



ProSafe M5300 Managed Switch

Software Administration Manual

10.0.0

350 East Plumeria Drive
San Jose, CA 95134
USA

December 2012
202-11153-03

©NETGEAR, Inc. All rights reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NETGEAR, Inc.

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, or get support online, visit us at <http://support.netgear.com>.

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): See Support information card.

Trademarks

NETGEAR, the NETGEAR logo, ReadyNAS, ProSafe, Smart Wizard, Auto Uplink, X-RAID2, and NeoTV are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, Windows NT, and Vista are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-11153-03	v1.0	December 2012	Made minor changes throughout.
202-11153-02	v1.0	November 2012	Added mixed switch stacking feature.
202-11153-01	v1.0	August 2012	Added Private VLAN features.
202-10515-05	v1.0	August 2012	Added MVR feature.
202-10515-05	v1.0	July 2011	Added DHCPv6 and DHCPv6 mode features.
202-10515-04	v1.0	November 2010	New document template.
202-10515-03	v 1.0	June 2010	Move some content to the <i>Software Setup Guide</i> .
202-10515-02			Software release 8.0.2: new firmware with DHCP L3 Relay, color conform policy, DHCP server in dynamic mode, and configuring a stacking port as an Ethernet port.
202-10515-01			Original publication.

Table of Contents

Chapter 1 Documentation Resources

Chapter 2 VLANs

Create Two VLANs	17
CLI: Create Two VLANs	17
Web Interface: Create Two VLANs	18
Assign Ports to VLAN2	19
CLI: Assign Ports to VLAN2	19
Web Interface: Assign Ports to VLAN2	19
Create Three VLANs	20
CLI: Create Three VLANs	20
Web Interface: Create Three VLANs	20
Assign Ports to VLAN3	22
CLI: Assign Ports to VLAN3	22
Web Interface: Assign Ports to VLAN3	23
Assign VLAN3 as the Default VLAN for Port 1/0/2	24
CLI: Assign VLAN3 as the Default VLAN for Port 1/0/2	24
Web Interface: Assign VLAN3 as the Default VLAN for Port 1/0/2	24
Create a MAC-Based VLAN	25
CLI: Create a MAC-Based VLAN	25
Web Interface: Assign a MAC-Based VLAN	26
Create a Protocol-Based VLAN	28
CLI: Create a Protocol-Based VLAN	28
Web Interface: Create a Protocol-Based VLAN	29
Virtual VLANs: Create an IP Subnet–Based VLAN	30
CLI: Create an IP Subnet–Based VLAN	31
Web Interface: Create an IP Subnet–Based VLAN	32
Voice VLANs	33
CLI: Configure Voice VLAN and Prioritize Voice Traffic	34
Web Interface: Configure Voice VLAN and Prioritize Voice Traffic	36
Private VLANs	43
Assign Private-VLAN Types (Primary, Isolated, Community)	45
CLI: Assign Private-VLAN Type (Primary, Isolated, Community)	45
Web Interface: Assign Private-VLAN Type (Primary, Isolated, Community)	45
Configure Private-VLAN Association	47
CLI: Configure Private-VLAN Association	47
Web Interface: Configure Private-VLAN Association	47
Configure Private-VLAN Port Mode (Promiscuous, Host)	48
CLI: Configure Private-VLAN Port Mode (Promiscuous, Host)	48
Web Interface: Configure Private-VLAN Port Mode (Promiscuous, Host)	48

Configure Private-VLAN Host Ports	49
CLI: Configure Private-VLAN Host Ports	49
Web Interface: Assign Private-VLAN Port Host Ports	49
Map Private-VLAN Promiscuous Port	51
CLI: Map Private-VLAN Promiscuous Port.	51
Web Interface: Map Private-VLAN Promiscuous Port	51

Chapter 3 LAGs

Create Two LAGs.	54
CLI: Create Two LAGs	54
Web Interface: Create Two LAGs.	54
Add Ports to LAGs	55
CLI: Add Ports to the LAGs	56
Web Interface: Add Ports to LAGs	57
Enable Both LAGs	58
CLI: Enable Both LAGs	58
Web Interface: Enable Both LAGs	58

Chapter 4 Port Routing

Port Routing Configuration	60
Enable Routing for the Switch	61
CLI: Enable Routing for the Switch.	61
Web Interface: Enable Routing for the Switch	61
Enable Routing for Ports on the Switch	61
CLI: Enable Routing for Ports on the Switch	62
Web Interface: Enable Routing for Ports on the Switch	62
Add a Default Route	64
CLI: Add a Default Route	64
Web Interface: Add a Default Route.	64
Add a Static Route	65
CLI: Add a Static Route	65
Web Interface: Add a Static Route	66

Chapter 5 VLAN Routing

Create Two VLANs.	67
CLI: Create Two VLANs.	68
Web Interface: Create Two VLANs	69
Set Up VLAN Routing for the VLANs and the Switch.	72
CLI: Set Up VLAN Routing for the VLANs and the Switch.	72
Web Interface: Set Up VLAN Routing for the VLANs and the Switch	73

Chapter 6 RIP

Routing for the Switch	75
CLI: Enable Routing for the Switch.	75
Web Interface: Enable Routing for the Switch	75
Routing for Ports	76

CLI: Enable Routing and Assigning IP Addresses for Ports 1/0/2 and 1/0/376	
Web Interface: Enable Routing for the Ports	76
RIP for the Switch	77
CLI: Enable RIP on the Switch	77
Web Interface: Enable RIP on the Switch	78
RIP for Ports 1/0/2 and 1/0/3	78
CLI: Enable RIP for Ports 1/0/2 and 1/0/3	78
Web Interface: Enable RIP for Ports 1/0/2 and 1/0/3	79
VLAN Routing with RIP	80
CLI: Configure VLAN Routing with RIP Support	80
Web Interface: Configure VLAN Routing with RIP Support	82

Chapter 7 OSPF

Inter-area Router	85
CLI: Configure an Inter-area Router	85
Web Interface: Configure an Inter-area Router	87
OSPF on a Border Router	90
CLI: Configure OSPF on a Border Router	90
Web Interface: Configure OSPF on a Border Router	91
Stub Areas	95
CLI: Configure Area 1 as a Stub Area on A1	96
Web Interface: Configure Area 1 as a Stub Area on A1	97
CLI: Configure Area 1 as a Stub Area on A2	100
Web Interface: Configure Area 1 as a Stub Area on A2	101
nssa Areas	104
CLI: Configure Area 1 as an nssa Area	104
Web Interface: Configure Area 1 as an nssa Area on A1	105
CLI: Configure Area 1 as an nssa Area on A2	108
Web Interface: Configure Area 1 as an nssa Area on A2	110
VLAN Routing OSPF	113
CLI: Configure VLAN Routing OSPF	114
Web Interface: Configure VLAN Routing OSPF	115
OSPFv3	118
CLI: Configure OSPFv3	118
Web Interface: Configure OSPFv3	120

Chapter 8 ARP

Proxy ARP Examples	123
CLI: show ip interface	123
CLI: ip proxy-arp	124
Web Interface: Configure Proxy ARP on a Port	124

Chapter 9 VRRP

VRRP on a Master Router	126
CLI: Configure VRRP on a Master Router	126
Web Interface: Configure VRRP on a Master Router	127
VRRP on a Backup Router	128

CLI: Configure VRRP on a Backup Router	128
Web Interface: Configure VRRP on a Backup Router	129

Chapter 10 ACLs

MAC ACLs	132
IP ACLs	132
ACL Configuration	132
Set Up an IP ACL with Two Rules	133
CLI: Set Up an IP ACL with Two Rules	133
Web Interface: Set Up an IP ACL with Two Rules	134
One-Way Access Using a TCP Flag in an ACL	137
CLI:Configure One-Way Access Using a TCP Flag in an ACL	137
Web Interface: Configure One-Way Access Using a TCP Flag in an ACL	141
Use ACLs to Configure Isolated VLANs on a Layer 3 Switch	152
CLI: Configure One-Way Access Using a TCP Flag in ACL Commands	153
Web Interface: Configure One-Way Access Using a TCP Flag in an ACL	155
Set up a MAC ACL with Two Rules	164
CLI: Set up a MAC ACL with Two Rules	164
Web Interface: Set up a MAC ACL with Two Rules	165
ACL Mirroring	167
CLI: Configure ACL Mirroring	167
Web Interface: Configure ACL Mirroring	168
ACL Redirect	172
CLI: Redirect a Traffic Stream	172
Web Interface: Redirect a Traffic Stream	173
Configure IPv6 ACLs	177
CLI: Configure an IPv6 ACL	178
Web Interface: Configure an IPv6 ACL	180

Chapter 11 CoS Queuing

CoS Queue Mapping	185
Trusted Ports	185
Untrusted Ports	185
CoS Queue Configuration	186
Show classofservice Trust	186
CLI: Show classofservice Trust	186
Web Interface: Show classofservice Trust	187
Set classofservice Trust Mode	187
CLI: Set classofservice Trust Mode	187
Web Interface: Set classofservice Trust Mode	187
Show classofservice IP-Precedence Mapping	188
CLI: Show classofservice IP-Precedence Mapping	188
Web Interface: Show classofservice ip-precedence Mapping	188
Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode	189
CLI: Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode	189
Web Interface: Configure CoS-queue Min-bandwidth and Strict Priority Scheduler Mode	189

Set CoS Trust Mode for an Interface	190
CLI: Set CoS Trust Mode for an Interface	191
Web Interface: Set CoS Trust Mode for an Interface	191
Configure Traffic Shaping.	191
CLI: Configure traffic-shape	192
Web Interface: Configure Traffic Shaping.	192

Chapter 12 DiffServ

DiffServ.	194
CLI: Configure DiffServ.	195
Web Interface: Configure DiffServ	197
DiffServ for VoIP.	210
CLI: Configure DiffServ for VoIP.	210
Web Interface: Diffserv for VoIP	212
Auto VoIP	217
CLI: Configure Auto VoIP	218
Web Interface: Configure Auto-VoIP	220
DiffServ for IPv6	221
CLI: Configure DiffServ for IPv6	221
Web Interface: Configure DiffServ for IPv6.	222
Color Conform Policy	228
CLI: Configure a Color Conform Policy.	228
Web Interface: Configure a Color Conform Policy	229

Chapter 13 IGMP Snooping and Querier

IGMP Snooping	236
CLI: Enable IGMP Snooping on VLAN 100	236
Web Interface: Enable IGMP Snooping on VLAN 100	237
Show igmpsnooping	238
CLI: Show igmpsnooping	238
Web Interface: Show igmpsnooping	238
Show mac-address-table igmpsnooping	239
CLI: Show mac-address-table igmpsnooping.	239
Web Interface: Show mac-address-table igmpsnooping	239
External Multicast Router	239
CLI: Configure the Switch with an External Multicast Router	240
Web Interface: Configure the Switch with an External Multicast Router	240
Multicast Router Using VLAN.	240
CLI: Configure the Switch with a Multicast Router Using VLAN.	240
Web Interface: Configure the Switch with a Multicast Router Using VLAN	241
IGMP Querier	241
Enable IGMP Querier	242
CLI: Enable IGMP Querier	242
Web Interface: Enable IGMP Querier.	243
Show IGMP Querier Status	245
CLI: Show IGMP Querier Status.	245
Web Interface: Show IGMP Querier Status	245

Chapter 14 MVR (Multicast VLAN Registration)

Configure MVR in Compatible Mode	247
CLI: Configure MVR in Compatible Mode	248
Web Interface: Configure MVR in Compatible Mode	250
Configure MVR in Dynamic Mode	254
CLI: Configure MVR in Dynamic Mode.	254
Web Interface: Configure MVR in Dynamic Mode	256
.	259

Chapter 15 Security Management

Port Security	260
Set the Dynamic and Static Limit on Port 1/0/1	261
CLI: Set the Dynamic and Static Limit on Port 1/0/1	261
Web Interface: Set the Dynamic and Static Limit on Port 1/0/1	262
Convert the Dynamic Address Learned from 1/0/1 to a Static Address	263
CLI: Convert the Dynamic Address Learned from 1/0/1 to the Static Address	263
Web Interface: Convert the Dynamic Address Learned from 1/0/1 to the Static Ad-	
dress.	263
Create a Static Address	264
CLI: Create a Static Address	264
Web Interface: Create a Static Address	264
Protected Ports	264
CLI: Configure a Protected Port to Isolate Ports on the Switch	265
Web Interface: Configure a Protected Port to Isolate Ports on the Switch	267
802.1x Port Security	271
CLI: Authenticating dot1x Users by a RADIUS Server	271
Web Interface: Authenticating dot1x Users by a RADIUS Server	272
Create a Guest VLAN	277
CLI: Create a Guest VLAN	278
Web Interface: Create a Guest VLAN	279
Assign VLANs Using RADIUS	282
CLI: Assign VLANs Using RADIUS	283
Web Interface: Assign VLANs Using RADIUS.	285
Dynamic ARP Inspection	288
CLI: Configure Dynamic ARP Inspection	289
Web Interface: Configure Dynamic ARP Inspection.	290
Static Mapping	294
CLI: Configure Static Mapping	294
Web Interface: Configure Static Mapping.	295
DHCP Snooping	296
CLI: Configure DHCP Snooping	296
Web Interface: Configure DHCP Snooping	297
Enter Static Binding into the Binding Database	299
CLI: Enter Static Binding into the Binding Database	299
Web Interface: Enter Static Binding into the Binding Database	300
Maximum Rate of DHCP Messages.	300
CLI: Configure the Maximum Rate of DHCP Messages.	301

Web Interface: Configure the Maximum Rate of DHCP Messages . . .	301
IP Source Guard	302
CLI: Configure Dynamic ARP Inspection	302
Web Interface: Configure Dynamic ARP Inspection	303

Chapter 16 SNTP

Show SNTP (CLI Only)	307
show sntp	307
show sntp client	308
show sntp server	308
Configure SNTP	309
CLI: Configure SNTP	309
Web Interface: Configure SNTP	310
Set the Time Zone (CLI Only)	311
Set the Named SNTP Server	311
CLI: Set the Named SNTP Server	312
Web Interface: Set the Named SNTP Server	312

Chapter 17 Tools

Traceroute	314
CLI: Traceroute	315
Web Interface: Traceroute	316
Configuration Scripting	316
script	317
script list and script delete	317
script apply running-config.scr	318
Create a Configuration Script	318
Upload a Configuration Script	318
Pre-Login Banner	319
Create a Pre-Login Banner (CLI Only)	319
Port Mirroring	320
CLI: Specify the Source (Mirrored) Ports and Destination (Probe) . . .	320
Web Interface: Specify the Source (Mirrored) Ports and Destination (Probe)	321
Dual Image	321
CLI: Download a Backup Image and Make It Active	322
Web Interface: Download a Backup Image and Make It Active	323
Outbound Telnet	324
CLI: show network	325
CLI: show telnet	325
CLI: transport output telnet	326
Web Interface: Configure Telnet	326
CLI: Configure the session-limit and session-timeout	327
Web Interface: Configure the Session Timeout	327

Chapter 18 Syslog

Show Logging	329
CLI: Show Logging	329

Web Interface: Show Logging	329
Show Logging Buffered	331
CLI: Show Logging Buffered	331
Web Interface: Show Logging Buffered	332
Show Logging Traplogs	332
CLI: Show Logging Traplogs	332
Web Interface: Show Logging Trap Logs	332
Show Logging Hosts	333
CLI: Show Logging Hosts	333
Web Interface: Show Logging Hosts	334
Configure Logging for a Port	334
CLI: Configure Logging for the Port	334
Web Interface: Configure Logging for the Port	335
Email Alerting	336
CLI: Send Log Messages to admin@switch.com Using Account aaaa@net-gear.com	337

Chapter 19 Switch Stacks

Switch Stack Management and Connectivity	338
The Stack Master and Stack Members	339
Stack Master	339
Stack Members	340
Stack Member Numbers	340
Stack Member Priority Values	341
Install and Power-up a Stack	341
Compatible Switch Models	341
Install a Switch Stack	342
Switch Firmware	342
Code Mismatch	343
Upgrade the Firmware	343
Migrate Configuration with a Firmware Upgrade	343
Copy Master Firmware to a Stack Member (Web Interface)	344
Configure a Stacking Port as an Ethernet Port	344
CLI: Configure a Stacking Port as an Ethernet Port	345
Web Interface: Configure a Stacking Port as an Ethernet Port	346
Stack Switches Using 10G Fiber	347
CLI: Stack Switches Using 10G Fiber	348
Web Interface: Stack Switches Using 10G Fiber	349
Add, Remove, or Replace a Stack Member	350
Add Switches to an Operating Stack	350
Remove a Switch from the Stack	351
Replace a Stack Member	351
Switch Stack Configuration Files	352
Preconfigure a Switch	353
Renumber Stack Members	354
CLI: Renumber Stack Members	354
Web Interface: Renumber Stack Members	355
Move the Stack Master to a Different Unit	356

CLI: Move the Stack Master to a Different Unit	356
Web Interface: Move the Stack Master to a Different Unit	356
M5300 and GSM73xxSv2 Mixed Stacking	357
Create a Mixed Stack with an M5300-28G3 Switch and a GSM7328Sv2 Switch	358
CLI: Change the SDM template on the M5300 switch to match the one on the GSM7328Sv2 switch.:	359
Web Interface: Change the SDM template on the M5300 switch to match the one on the GSM7328Sv2 switch.	359
Change the SDM template back to the default.	360
CLI: Change the SDM template back to the default	360
Web Interface: Change the SDM template back to the default.	360

Chapter 20 SNMP

Add a New Community	361
CLI: Add a New Community	361
Web Interface: Add a New Community.	362
Enable SNMP Trap	362
CLI: Enable SNMP Trap	362
Web Interface: Enable SNMP Trap	363
SNMP V3	363
CLI: Configure SNMP V3	364
Web Interface: Configure SNMP V3	364
sFlow	365
CLI: Configure Statistical Packet-Based Sampling of Packet Flows with sFlow366	
Web Interface: Configure Statistical Packet-based Sampling with sFlow367	
Time-Based Sampling of Counters with sFlow.	369
CLI: Configure Time-Based Sampling of Counters with sFlow.	369
Web Interface: Configure Time-Based Sampling of Counters with sFlow369	

Chapter 21 DNS

Specify Two DNS Servers	370
CLI: Specify Two DNS Servers.	370
Web Interface: Specify Two DNS Servers	371
Manually Add a Host Name and an IP Address	371
CLI: Manually Add a Host Name and an IP Address	371
Web Interface: Manually Add a Host Name and an IP Address.	372

Chapter 22 DHCP Server

Configure a DHCP Server in Dynamic Mode	373
CLI: Configure a DHCP Server in Dynamic Mode	373
Web Interface: Configure a DHCP Server in Dynamic Mode	374
Configure a DHCP Reservation	376
CLI: Configure a DHCP Reservation	377
Web Interface: Configure a DHCP Reservation	377

Chapter 23 DHCPv6 Server

CLI: Configure DHCPv6	381
Web Interface: Configure an Inter-area Router	382
Configure Stateless DHCPv6 Server	386
CLI: Configure Stateless DNS Server	386
Web Interface: Configure Stateless DHCPv6 Server	387

Chapter 24 Double VLANs and Private VLAN Groups

Double VLANs	390
CLI: Enable a Double VLAN	391
Web Interface: Enable a Double VLAN	391
Private VLAN Groups	394
CLI: Create a Private VLAN Group	395
Web Interface: Create a Private VLAN Group	396

Chapter 25 Spanning Tree Protocol

Configure Classic STP (802.1d)	400
CLI: Configure Classic STP (802.1d)	400
Web Interface: Configure Classic STP (802.1d)	401
Configure Rapid STP (802.1w)	402
CLI: Configure Rapid STP (802.1w)	402
Web Interface: Configure Rapid STP (802.1w)	402
Configure Multiple STP (802.1s)	403
CLI: Configure Multiple STP (802.1s)	403
Web Interface: Configure Multiple STP (802.1s)	404

Chapter 26 Tunnel

CLI: Create a Tunnel	407
Configure Switch GSM7328S_1	407
Configure Switch GSM7328S_2	408
Web Interface: Create a Tunnel	409
Configure Switch GSM7328S_1	409
Configure Switch GSM7328S_2	411

Chapter 27 IPv6 Interface Configuration

Create an IPv6 Routing Interface	414
CLI: Create an IPv6 Routing Interface	414
Web Interface: Create an IPv6 Routing Interface	416
Create an IPv6 Network Interface	417
CLI: Configure the IPv6 Network Interface	418
Web Interface: Configure the IPv6 Network Interface	418
Create an IPv6 Routing VLAN	419
CLI: Create an IPv6 Routing VLAN	419
Web Interface: Create an IPv6 VLAN Routing Interface	421
Configure DHCPv6 Mode on the Routing Interface	424

CLI: Configure DHCPv6 mode on routing interface	424
Web Interface: Configure DHCPv6 mode on routing interface.	425

Chapter 28 PIM

PIM-DM	427
CLI: Configure PIM-DM	429
Web Interface: Configure PIM-DM	433
PIM-SM.	451
CLI: Configure PIM-SM.	452
Web Interface: Configure PIM-SM	456

Chapter 29 DHCP L2 Relay and L3 Relay

DHCP L2 Relay	478
CLI: Enable DHCP L2 Relay.	479
Web Interface: Enable DHCP L2 Relay	480
DHCP L3 Relay	484
Configure the DHCP Server Switch	484
Configure a DHCP L3 Switch	489

Chapter 30 MLD

Configure MLD	495
CLI: Configure MLD	495
Web Interface: Configure MLD	497
MLD Snooping	508
CLI: Configure MLD Snooping	509
Web Interface: Configure MLD Snooping.	510

Chapter 31 DVMRP

CLI: Configure DVMRP	514
Web Interface: Configure DVMRP	520

Chapter 32 Captive Portal

Captive Portal Configuration.	532
Enable Captive Portal.	532
CLI: Enable Captive Portal	532
Web Interface: Enable Captive Portal.	533
Client Access, Authentication, and Control	534
Block a Captive Portal Instance	535
CLI: Block a Captive Portal Instance	535
Web Interface: Block a Captive Portal Instance	535
Local Authorization, Create Users and Groups	535
CLI: Create Users and Groups	536
Web Interface: Create Users and Groups	536
Remote Authorization (RADIUS) User Configuration	537
CLI: Configure RADIUS as the Verification Mode	538

Web Interface: Configure RADIUS as the Verification Mode 539
SSL Certificates 539

Index

Documentation Resources

1

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

- The NETGEAR installation guide for your switch
- *Hardware Installation Guide*
- *Software Setup Guide*
- *NETGEAR CLI Reference for the Prosafe 7X00 Series Managed Switch*. Refer to the *Command Line Reference* for information about the command structure. There are different documents in this series; choose the appropriate one for your product.
 - The *Command Line Reference* provides information about the CLI commands used to configure the switch and the stack. The document provides CLI descriptions, syntax, and default values.
 - The *ProSafe Managed Stackable Switch CLI Manual* provides information about the CLI commands used to configure the switch. The document provides CLI descriptions, syntax, and default values.

2 VLANs

2

Virtual LANs

This chapter provides the following examples:

- *Create Two VLANs* on page 17
- *Assign Ports to VLAN2* on page 19
- *Create Three VLANs* on page 20
- *Assign Ports to VLAN3* on page 22
- *Assign VLAN3 as the Default VLAN for Port 1/0/2* on page 24
- *Create a MAC-Based VLAN* on page 25
- *Create a Protocol-Based VLAN* on page 28
- *Virtual VLANs: Create an IP Subnet–Based VLAN* on page 30
- *Voice VLANs* on page 33
- *Private VLANs* on page 43
- *Assign Private-VLAN Types (Primary, Isolated, Community)* on page 45
- *Configure Private-VLAN Association* on page 47
- *Configure Private-VLAN Port Mode (Promiscuous, Host)* on page 48
- *Configure Private-VLAN Host Ports* on page 49
- *Map Private-VLAN Promiscuous Port* on page 51

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

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

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

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

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

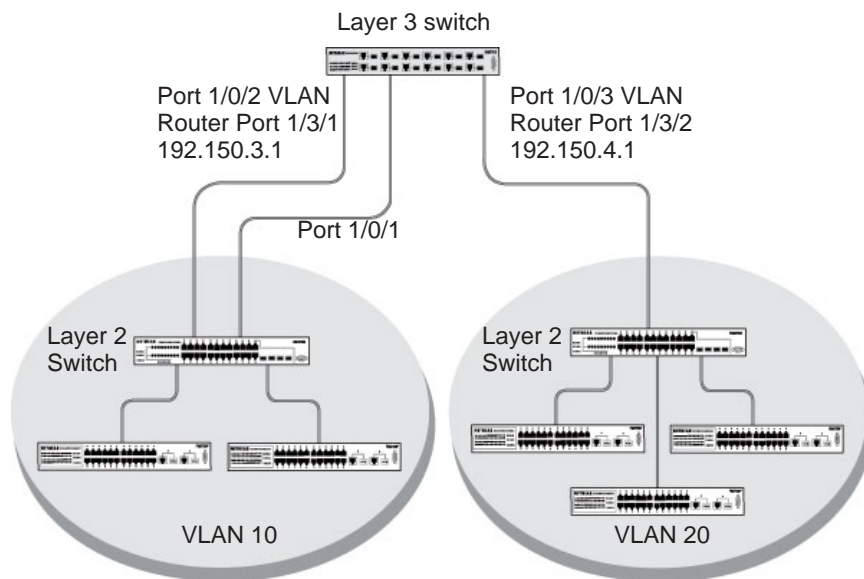


Figure 1. Switch with 4 ports configured for traffic from 2 VLANs

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

Create Two VLANs

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

CLI: Create Two VLANs

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

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

Web Interface: Create Two VLANS

1. Create VLAN2.
 - a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays.

The screenshot shows the 'VLAN Configuration' page in the ProSafe Managed Switch web interface. The page has a navigation menu at the top with tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. Below the navigation is a sub-menu for VLAN, STP, Multicast, Address Table, Ports, and LAG. The main content area shows the 'VLAN Configuration' page with a 'Reset' section and a table for VLAN configuration. The table has columns for VLAN ID, VLAN Name, and VLAN Type. The first row shows VLAN ID 2, VLAN Name VLAN2, and VLAN Type Static. The second row shows VLAN ID 1, VLAN Name Default, and VLAN Type Default.

- b. Enter the following information:
 - In the **VLAN ID** field, enter **2**.
 - In the **VLAN Name** field, enter **VLAN2**.
 - In the **VLAN Type** list, select **Static**.
 - c. Click **Add**.
2. Create VLAN3.
 - a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays.

The screenshot shows the 'VLAN Configuration' page in the ProSafe Managed Switch web interface. The page has a navigation menu at the top with tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. Below the navigation is a sub-menu for VLAN, STP, Multicast, Address Table, Ports, and LAG. The main content area shows the 'VLAN Configuration' page with a 'Reset' section and a table for VLAN configuration. The table has columns for VLAN ID, VLAN Name, and VLAN Type. The first row shows VLAN ID 3, VLAN Name VLAN3, and VLAN Type Static. The second row shows VLAN ID 1, VLAN Name Default, and VLAN Type Default. The third row shows VLAN ID 2, VLAN Name VLAN2, and VLAN Type Static.

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

Assign Ports to VLAN2

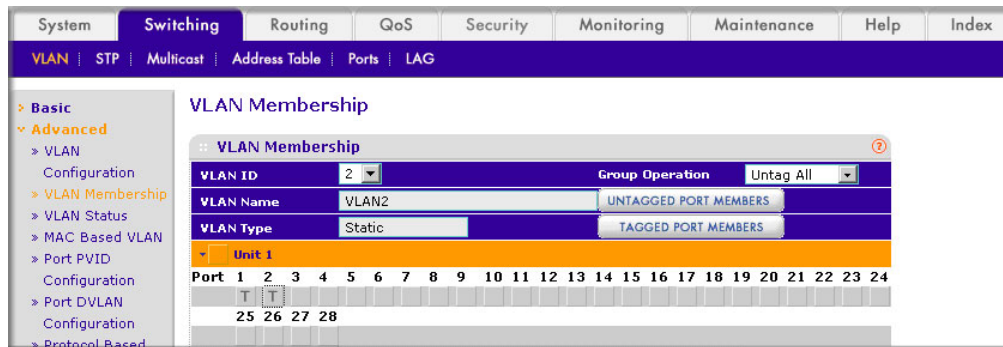
This sequence shows how to assign ports to VLAN2, and to specify that frames will always be transmitted tagged from all member ports and that untagged frames will be rejected on receipt.

CLI: Assign Ports to VLAN2

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

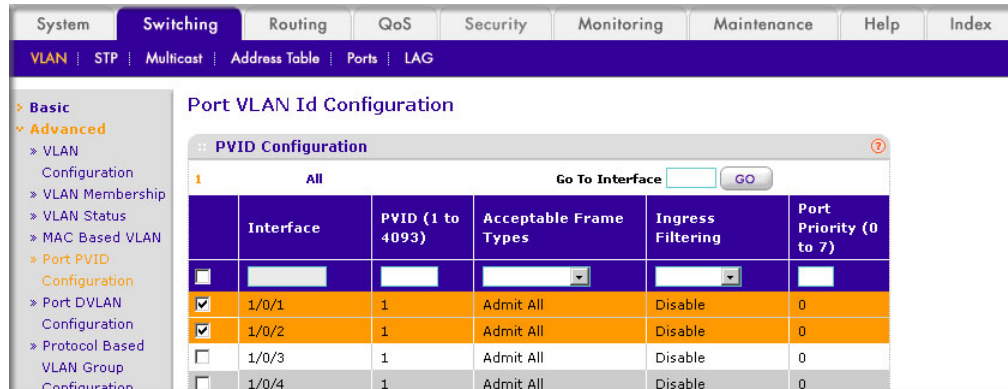
Web Interface: Assign Ports to VLAN2

1. Assign ports to VLAN2.
 - a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays.



- b. In the **VLAN ID** list, select **2**.
 - c. Click **Unit 1**. The ports display.
 - d. Click the gray boxes under ports **1** and **2** until **T** displays. The T specifies that the egress packet is tagged for the ports.
 - e. Click **Apply** to save the settings.
2. Specify that only tagged frames will be accepted on ports 1/0/1 and 1/0/2.

- a. Select **Switching > VLAN > Advanced > Port PVID Configuration**. A screen similar to the following displays.



- b. Under PVID Configuration, scroll down and select the check box for Interface **1/0/1**. Then scroll down and select the Interface **1/0/2** check box.
- c. Enter the following information:
- In the **Acceptable Frame Type polyhedron** list, select **VLAN Only**.
 - In the **PVID (1 to 4093)** field, enter **2**.
- d. Click **Apply** to save the settings.

Create Three VLANs

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

CLI: Create Three VLANS

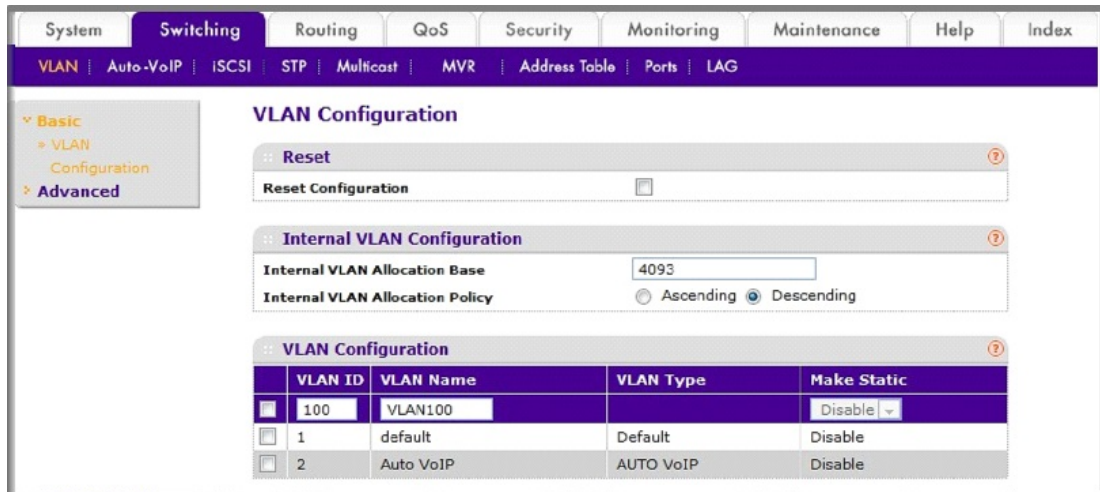
Use the following commands to create three VLANs and to assign the VLAN IDs while leaving the names blank.

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

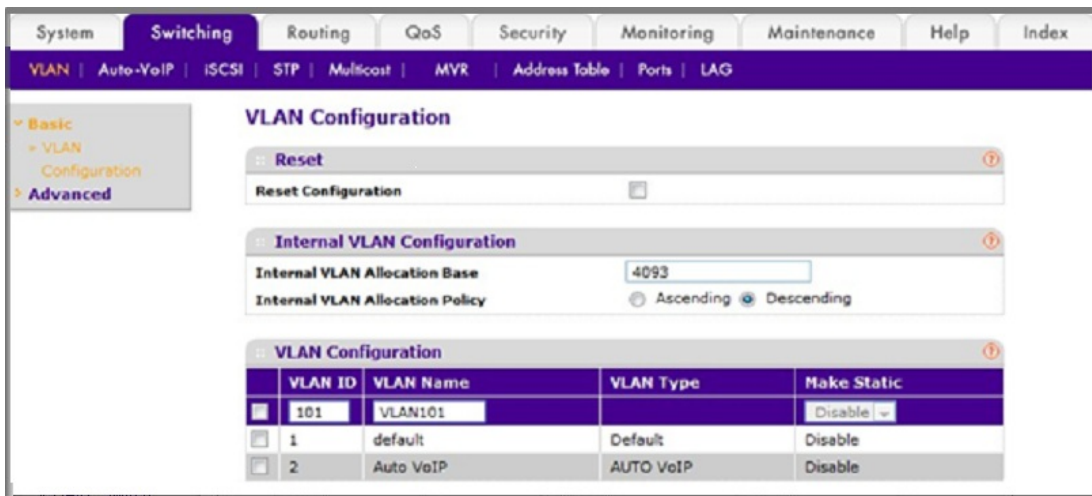
Web Interface: Create Three VLANS

1. Create VLAN100.

- a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays.

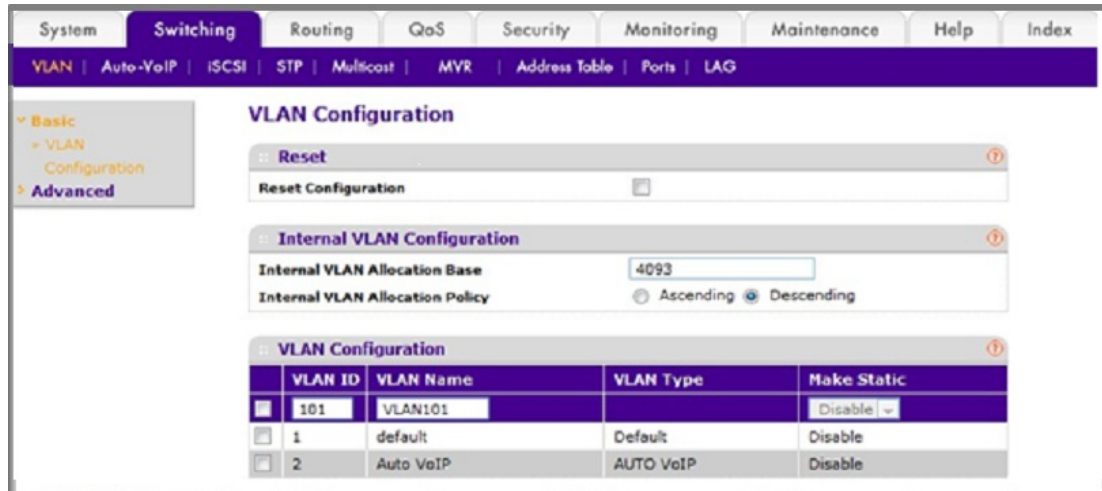


- b. Enter the following information:
 - In the **VLAN ID** field, enter **100**.
 - In the **VLAN Name** field, enter **VLAN100**.
 - c. Click **Add**.
2. Create VLAN101.
 - a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays.



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

3. Create VLAN102.
 - a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays.



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

Assign Ports to VLAN3

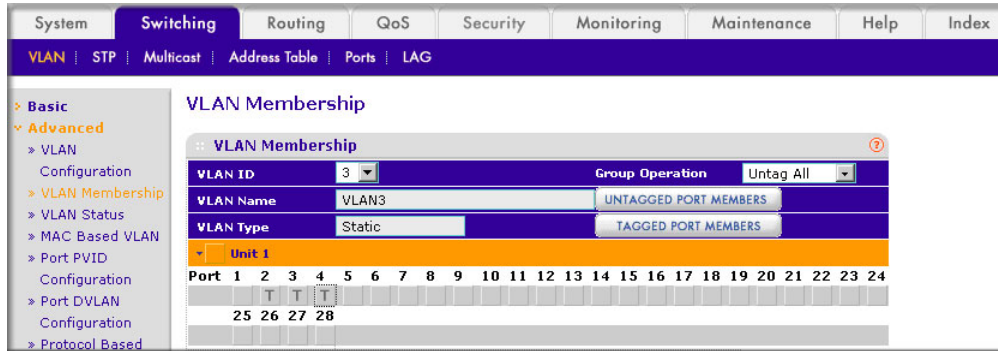
This example shows how to assign the ports that will belong to VLAN 3, and to specify that untagged frames will be accepted on port 1/0/4. Note that port 1/0/2 belongs to both VLANs and that port 1/0/1 can never belong to VLAN 3.

CLI: Assign Ports to VLAN3

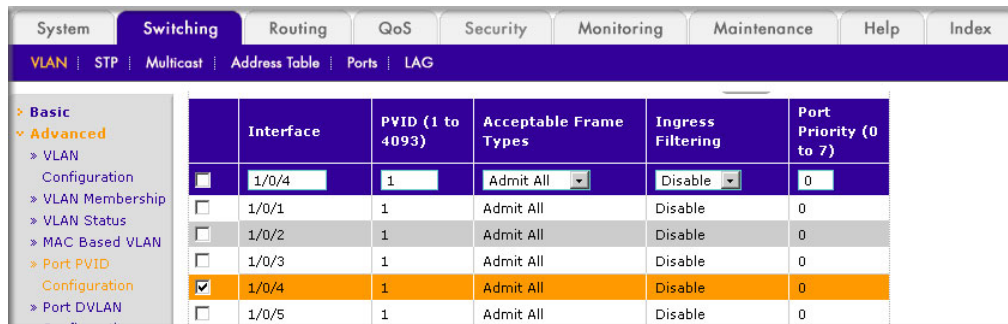
```
(Netgear Switch) (Config)#interface range 1/0/2-1/0/4
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#vlan participation include 3
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#exit
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#vlan acceptframe all
(Netgear Switch) (Interface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

Web Interface: Assign Ports to VLAN3

1. Assign ports to VLAN3.
 - a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays.



- b. In the **VLAN ID** list, select **3**.
 - c. Click **Unit 1**. The ports display.
 - d. Click the gray boxes under ports **2, 3** and **4** until **T** displays. The T specifies that the egress packet is tagged for the ports.
 - e. Click **Apply** to save the settings.
2. Specify that untagged frames will be accepted on port 1/0/4.
 - a. Select **Switching > VLAN > Advanced > Port PVID Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Interface **1/0/4** check box. Now 1/0/4 appears in the Interface field at the top.
 - c. In the **Acceptable Frame Types** list, select **Admit All**.
 - d. Click **Apply** to save the settings.

Assign VLAN3 as the Default VLAN for Port 1/0/2

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

CLI: Assign VLAN3 as the Default VLAN for Port 1/0/2

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

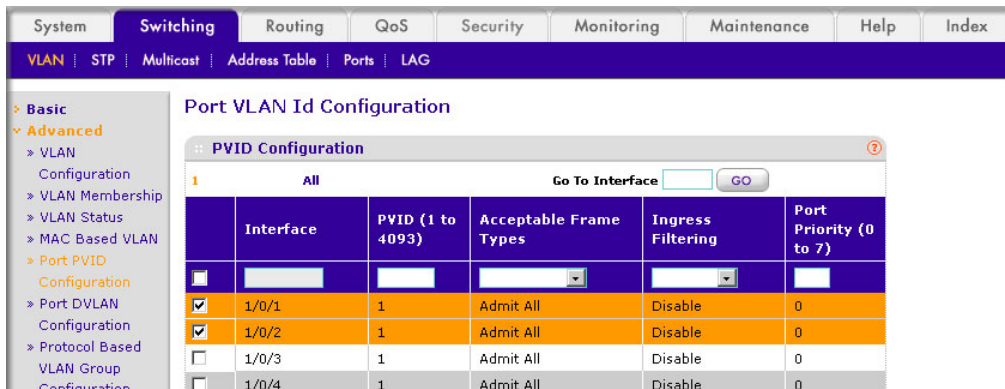
Web Interface: Assign VLAN3 as the Default VLAN for Port 1/0/2

1. Assign VLAN3 as the default VLAN for port 1/0/2.
 - a. Select **Switching > VLAN > Advanced > Port PVID Configuration**. A screen similar to the following displays.

Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)
<input type="checkbox"/> 1/0/1	1	Admit All	Disable	0
<input checked="" type="checkbox"/> 1/0/2	3	Admit All	Disable	0
<input type="checkbox"/> 1/0/3	1	Admit All	Disable	0
<input type="checkbox"/> 1/0/4	1	Admit All	Disable	0
<input type="checkbox"/> 1/0/5	1	Admit All	Disable	0
<input type="checkbox"/> 1/0/6	1	Admit All	Disable	0
<input type="checkbox"/> 1/0/7	1	Admit All	Disable	0

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

Create a MAC-Based VLAN



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

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

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

CLI: Create a MAC-Based VLAN

1. Create VLAN3.

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

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

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

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

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

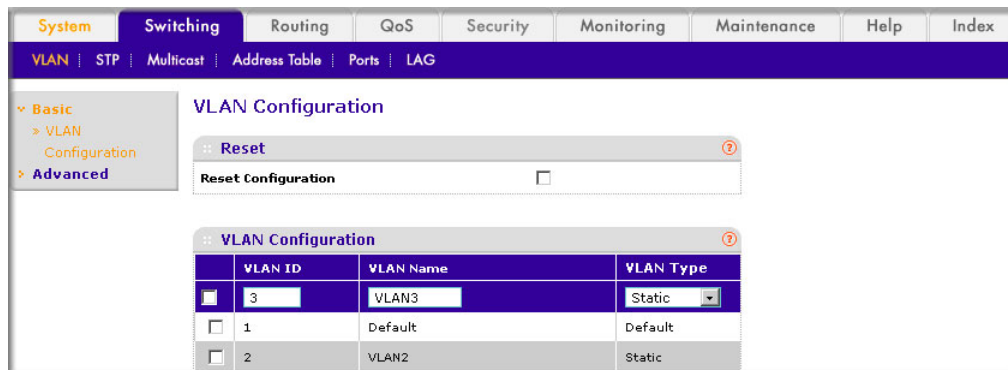
4. Add all the ports to VLAN3.

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

Web Interface: Assign a MAC-Based VLAN

1. Create VLAN3.

- a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays.

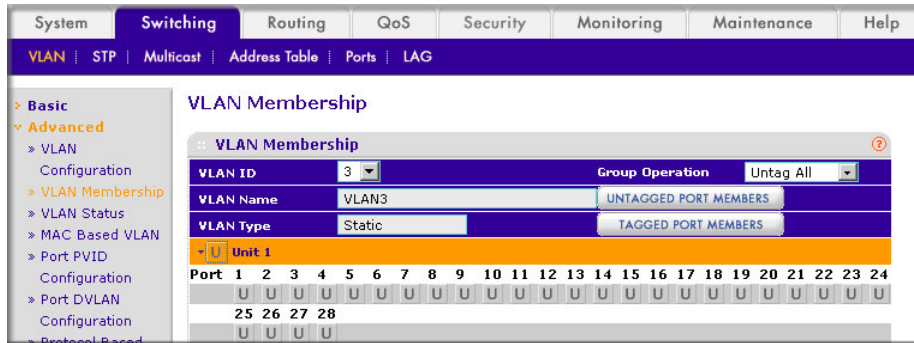


- b. Enter the following information:
 - In the **VLAN ID** field, enter **3**.
 - In the **VLAN Name** field, enter **VLAN3**.
 - In the **VLAN Type** list, select **Static**.

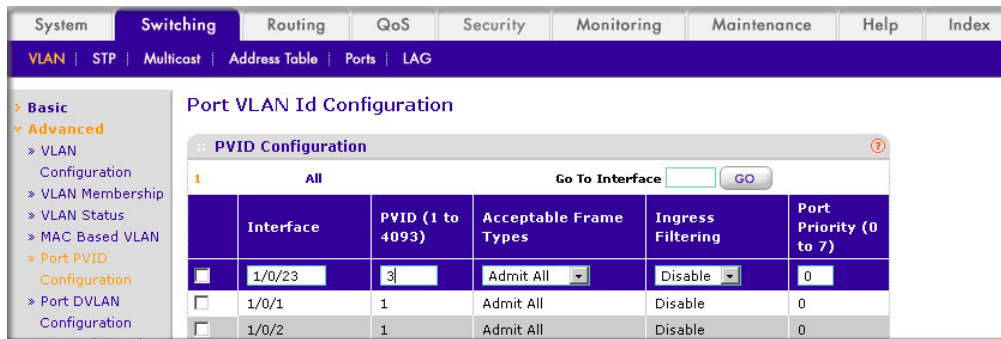
- c. Click **Add**.

2. Assign ports to VLAN3.

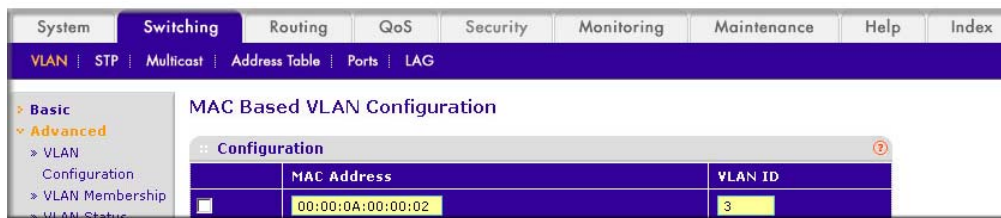
- a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays.



- b. In the **VLAN ID** list, select **3**.
 - c. Click **Unit 1**. The ports display.
 - d. Click the gray box before Unit 1 until **U** displays.
 - e. Click **Apply**.
3. Assign VPID3 to port 1/0/23.
 - a. Select **Switching > VLAN > Advanced > Port PVID Configuration**. A screen similar to the following displays.



- b. Scroll down and select the **1/0/23** check box.
 - c. In the **PVID (1 to 4093)** field, enter **3**.
 - d. Click **Apply** to save the settings.
4. Map the specific MAC to VLAN3.
 - a. Select **Switching > VLAN > Advanced > MAC based VLAN**. A screen similar to the following displays.



- b. Enter the following information:
 - In the **MAC Address** field, enter **00:00:0A:00:00:02**.
 - In the **PVID (1 to 4093)** field, enter **3**.
- c. Click **Add**.

Create a Protocol-Based VLAN

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

CLI: Create a Protocol-Based VLAN

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

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

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

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

3. Assign VLAN protocol group 1 to VLAN 4.

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

4. Assign VLAN protocol group 2 to VLAN 5.

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

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

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

Web Interface: Create a Protocol-Based VLAN

1. Create the protocol-based VLAN group `vlan_ipx`.

- a. Select **Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration**. A screen similar to the following displays.

Group Name	Group ID	Protocol	VLAN ID	Ports
<input type="checkbox"/> vlan_ipx		IP ARP IPX	4	

Enter the following information:

- In the **Group Name** field, enter `vlan_ipx`.
- In the **Protocol** list, select **IPX**.
- In the **VLAN ID** field, enter **4**.

- b. Click **Add**.

2. Create the protocol-based VLAN group `vlan_ip`.

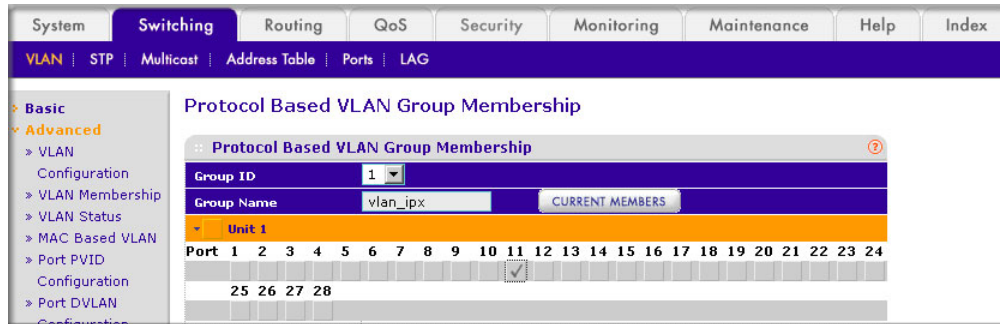
- a. Select **Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration**. A screen similar to the following displays.

Group Name	Group ID	Protocol	VLAN ID	Ports
<input type="checkbox"/> vlan_ip		IP ARP IPX	5	
<input type="checkbox"/> vlan_ipx	1	IPX	4	

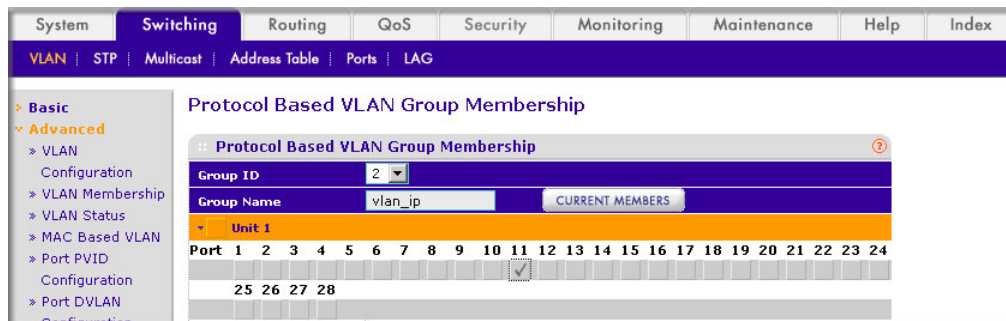
- b. Enter the following information:

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

- In the **VLAN** field, enter **5**.
 - c. Click **Add**.
3. Add port 11 to the group vlan_ipx.
- a. Select **Switching > VLAN > Advanced > Protocol Based VLAN Group Membership**. A screen similar to the following displays.



- b. In the **Group ID** list, select **1**.
 - c. Click the gray box under port **11**. A check mark displays in the box.
 - d. Click the **Apply** button.
4. Add port 11 to the group vlan_ip.
- a. Select **Switching > VLAN > Advanced > Protocol Based VLAN Group Membership**. A screen similar to the following displays.



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

Virtual VLANs: Create an IP Subnet–Based VLAN

In an IP subnet–based VLAN, all the end workstations in an IP subnet are assigned to the same VLAN. In this VLAN, users can move their workstations without reconfiguring their network addresses. IP subnet VLANs are based on Layer 3 information from packet headers. The switch makes use of the network-layer address (for example, the subnet address for TCP/IP networks) in determining VLAN membership. If a packet is untagged or priority

tagged, the switch associates the packet with any matching IP subnet classification. If no IP subnet classification can be made, the packet is subjected to the normal VLAN classification rules of the switch. This IP subnet capability does not imply a *routing* function or that the VLAN is routed. The IP subnet classification feature affects only the VLAN assignment of a packet. Appropriate 802.1Q VLAN configuration must exist in order for the packet to be switched.

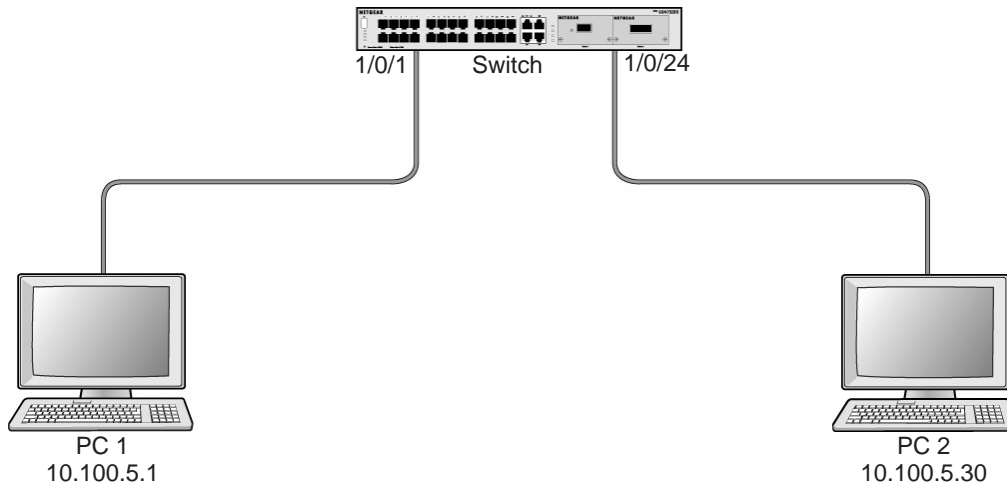


Figure 2. IP subnet-based VLAN

CLI: Create an IP Subnet-Based VLAN

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

Create an IP subnet-based VLAN 2000.

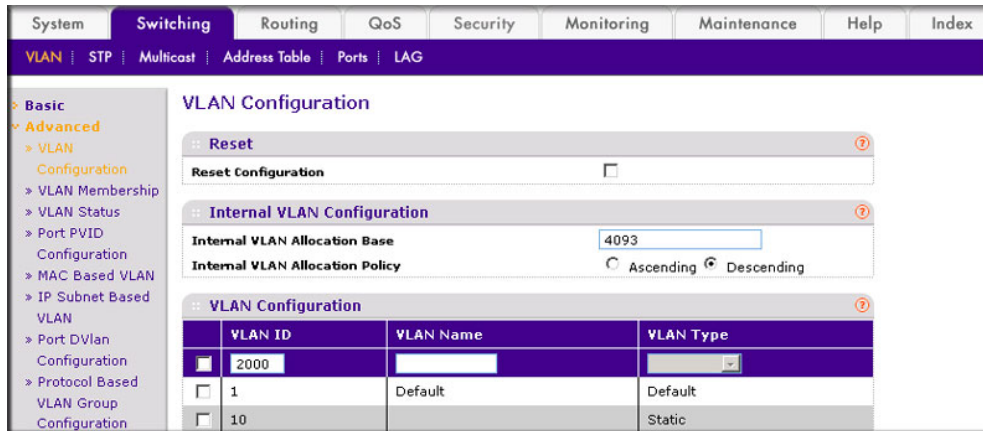
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface range 1/0/1-1/0/24
(Netgear Switch) (conf-if-range-1/0/1-1/0/24)# vlan participation include 2000
(Netgear Switch) (conf-if-range-1/0/1-1/0/24)#exit
(Netgear Switch) (Config)#
```

Assign all the ports to VLAN 2000.

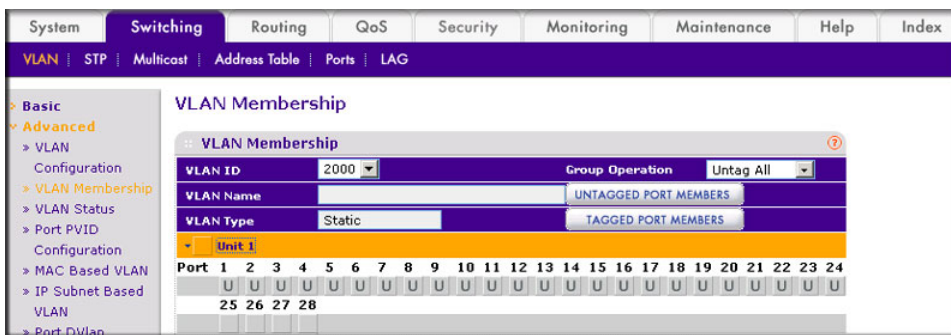
```
(Netgear Switch) #show mac-addr-table vlan 2000
MAC Address      Interface      Status
-----
00:00:24:58:F5:56 1/0/1         Learned
00:00:24:59:00:62 1/0/24        Learned
```

Web Interface: Create an IP Subnet–Based VLAN

1. Create VLAN 2000.
 - a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays.



- b. Enter the following information:
 - In the **VLAN ID** field, enter **2000**.
 - In the **VLAN Type** list, select **Static**.
 - c. Click **Add**.
2. Assign all the ports to VLAN 2000.
 - a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays.



management control and that clients attached to the network cannot initiate a direct attack on voice components.

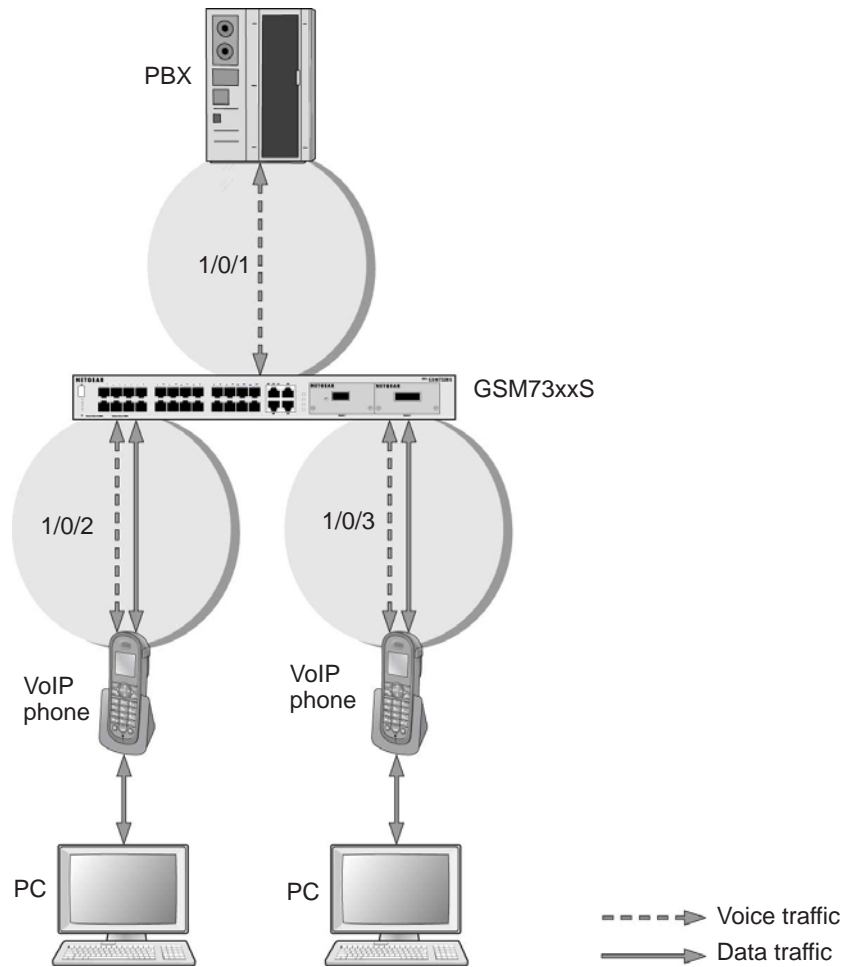


Figure 3. Voice VLAN

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

CLI: Configure Voice VLAN and Prioritize Voice Traffic

1. Create VLAN 10.

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

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

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

3. Configure Voice VLAN globally.

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

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

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

5. Create the DiffServ class ClassVoiceVLAN.

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

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

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

7. Create the DiffServ policy PolicyVoiceVLAN.

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

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

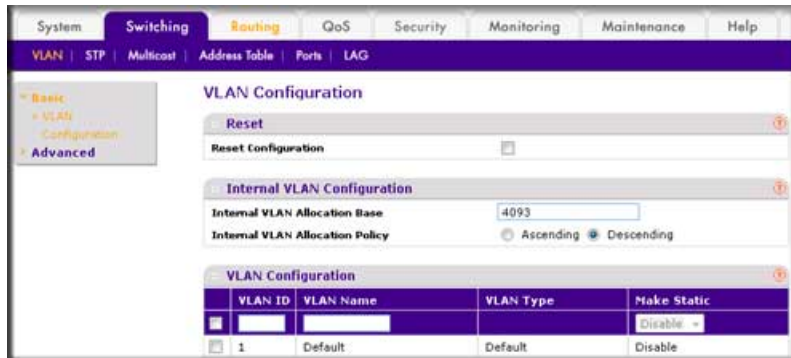
```
(Netgear Switch) (Config-policy-map)#class ClassVoiceVLAN
(Netgear Switch) (Config-policy-classmap)#assign-queue 3
(Netgear Switch) (Config-policy-classmap)#exit
```

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

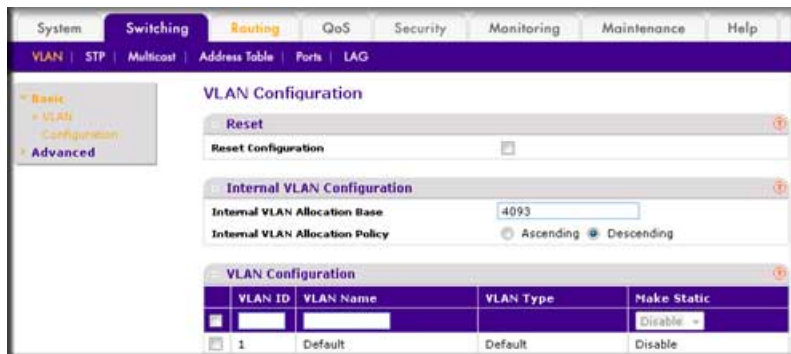
```
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)# service-policy in PolicyVoiceVLAN
```

Web Interface: Configure Voice VLAN and Prioritize Voice Traffic

1. Create VLAN 10.
 - a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays.



- b. In the **VLAN ID** field, enter **10**.
- c. In the **VLAN Name** field, enter **Voice VLAN**.
- d. Click **Add**. A screen similar to the following displays.



2. Include ports 1/0/1 and 1/0/2 in VLAN 10.
 - a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays.

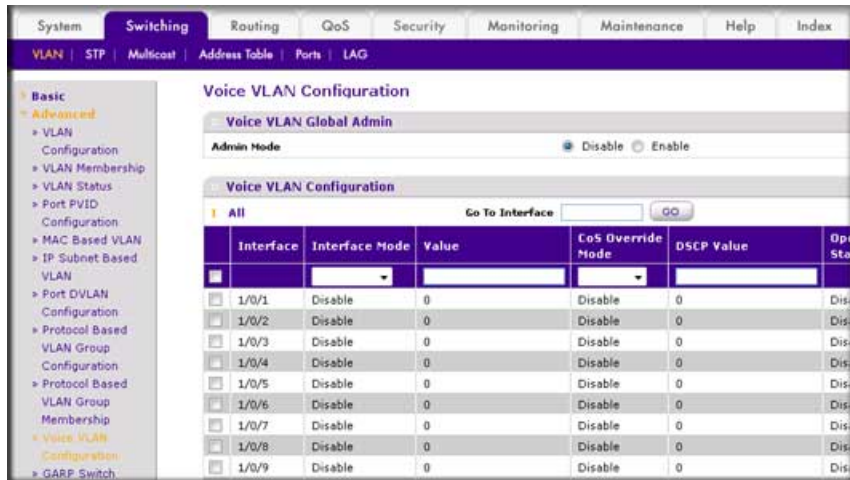


- b. In the VLAN Membership table, in the **VLAN ID** list, select **10**.

- c. Select Port 1 and Port 2 as tagged. A screen similar to the following displays.

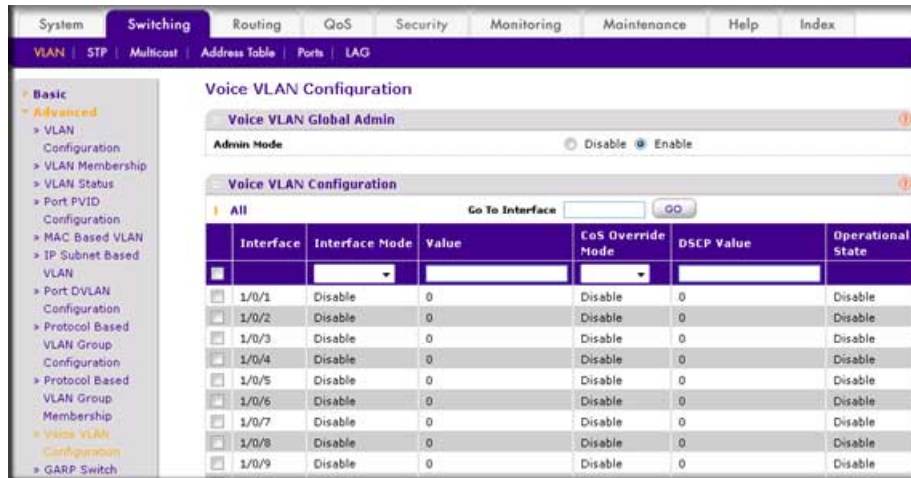


- d. Click **Apply**.
3. Configure Voice VLAN globally.
- a. Select **Switching > VLAN > Advanced > Voice VLAN Configuration**. A screen similar to the following displays.

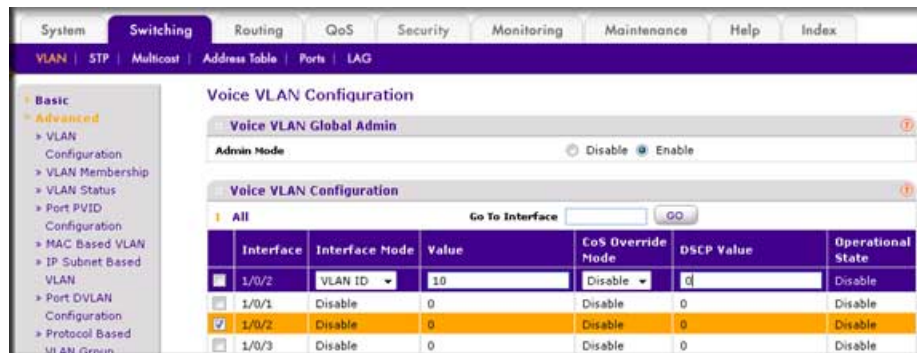


- b. For Admin Mode, select the **Enable** radio button.

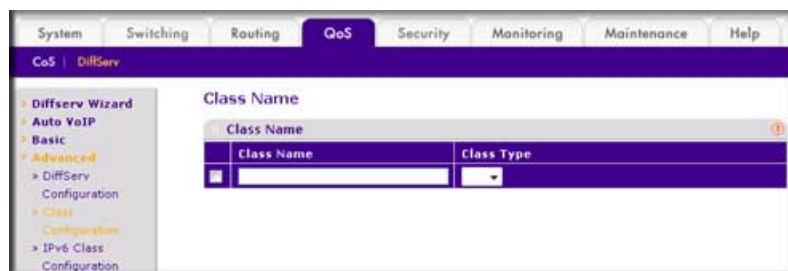
- c. Click **Apply**. A screen similar to the following displays.



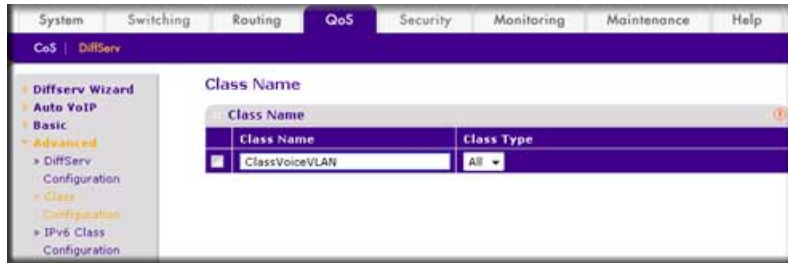
4. Configure Voice VLAN mode in interface 1/0/2.
- Select **Switching > VLAN > Advanced > Voice VLAN Configuration**.
 - Select the **1/0/2** check box.
 - In the **Interface Mode** list, select **VLAN ID**.
 - In the **Value** field, enter **10**. A screen similar to the following displays.



- Click **Apply**.
5. Create the DiffServ class ClassVoiceVLAN.
- Select **QoS > Advanced > DiffServ > Class Configuration**. A screen similar to the following displays.



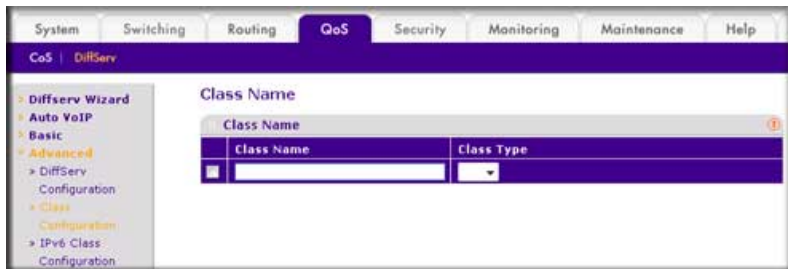
- b. In the **Class Name** field, enter **ClassVoiceVLAN**.
- c. In the **Class Type** list, select **All**. A screen similar to the following displays.



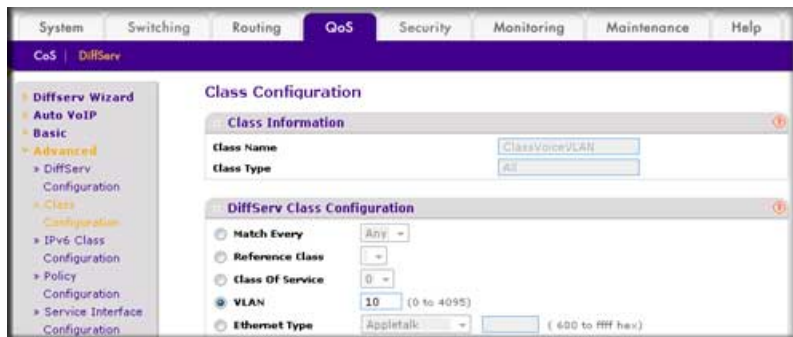
- d. Click **Add**. The Class Name screen displays, as shown in the next step in this procedure.
6. Configure matching criteria for the class as **VLAN 10**.
- a. Select **QoS > DiffServ > Advanced > Class Configuration**. A screen similar to the following displays.



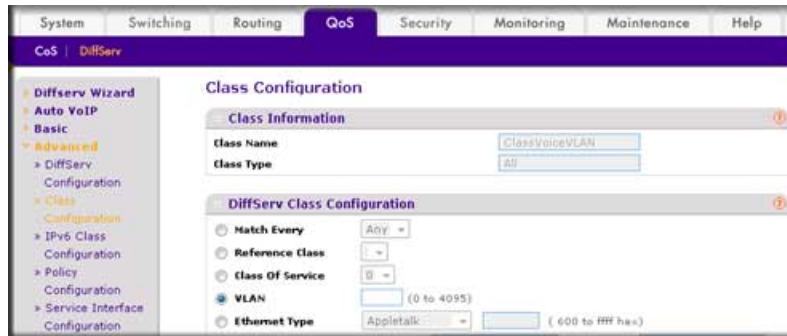
- b. Click the class **ClassVoiceVLAN**. A screen similar to the following displays.



- c. In the DiffServ Class Configuration table, select **VLAN**.
- d. In the **VLAN ID** field, enter **10**. A screen similar to the following displays.

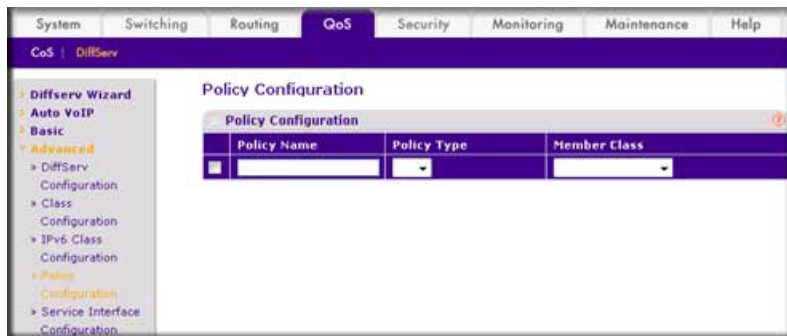


- e. Click **Apply**. A screen similar to the following displays.



7. Create the DiffServ policy PolicyVoiceVLAN.

- a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.



- b. In the **Policy Name** field, enter **PolicyVoiceVLAN**.
 c. In the **Policy Type** list, select **In**.
 d. In the **Member Class** list, select **ClassVoiceVLAN**. A screen similar to the following displays.



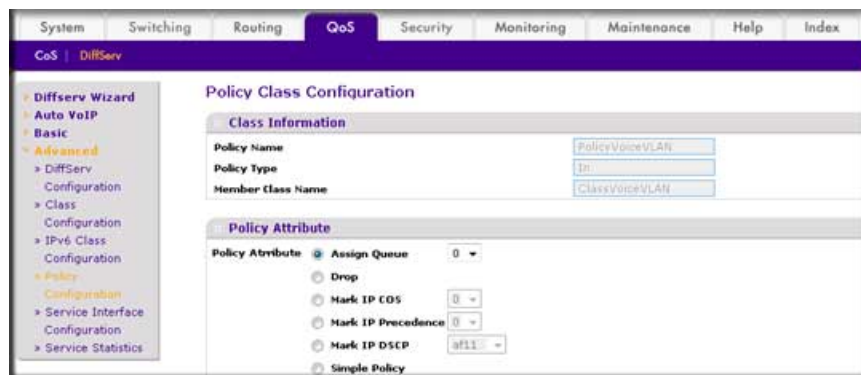
- e. Click **Add**. The Policy Configuration screen displays, as shown in the next step in this procedure.

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

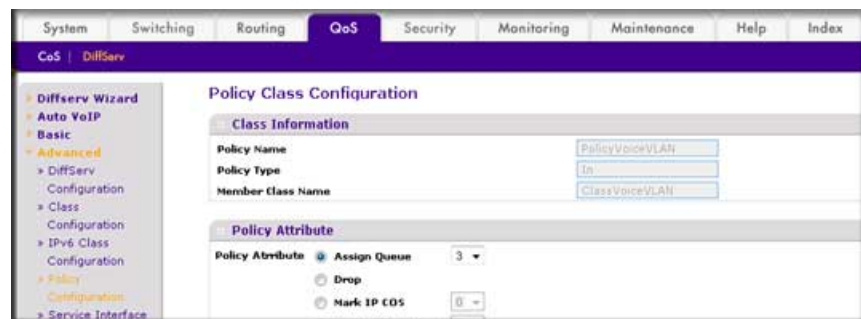
- a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.



- b. Click the **Policy PolicyVoiceVLAN**. A screen similar to the following displays.



- c. In the field next to the **Assign Queue** radio button, select **3**. A screen similar to the following displays.



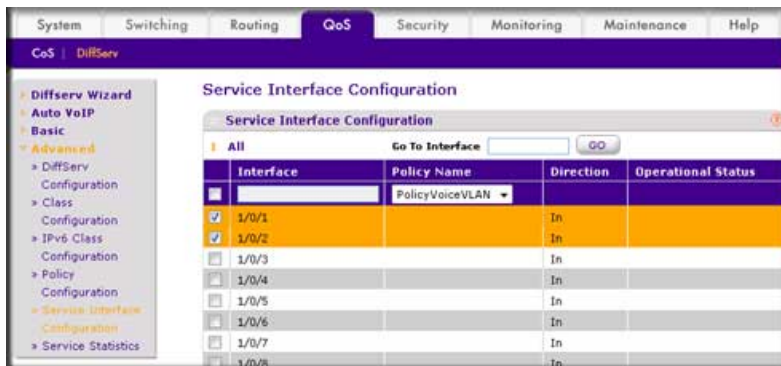
- d. Click **Apply**.

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

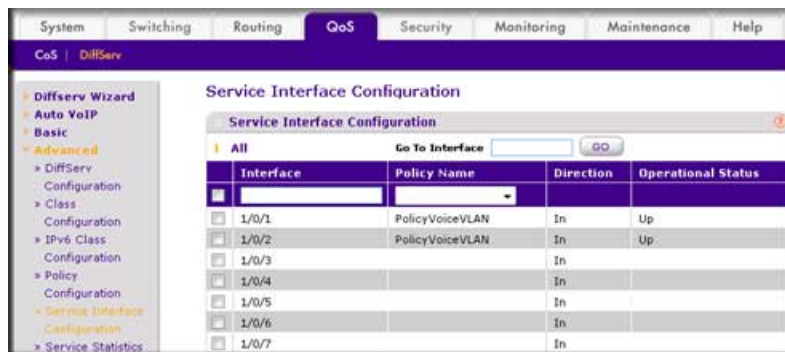
- a. Select **QoS > DiffServ > Advanced > Service Interface Configuration**. A screen similar to the following displays.



- b. Select the check boxes for Interfaces **1/0/1** and **1/0/2**.
- c. Set the **Policy Name** field as **PolicyVoiceVLAN**. A screen similar to the following displays.



- d. Click **Apply**. A screen similar to the following displays.



Private VLANs

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

There are three types of VLAN within a private VLAN:

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

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

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

The Private VLANs can be extended across multiple switches through inter-switch/stack links that transport primary, community and isolated VLANs between devices. See figure 1.

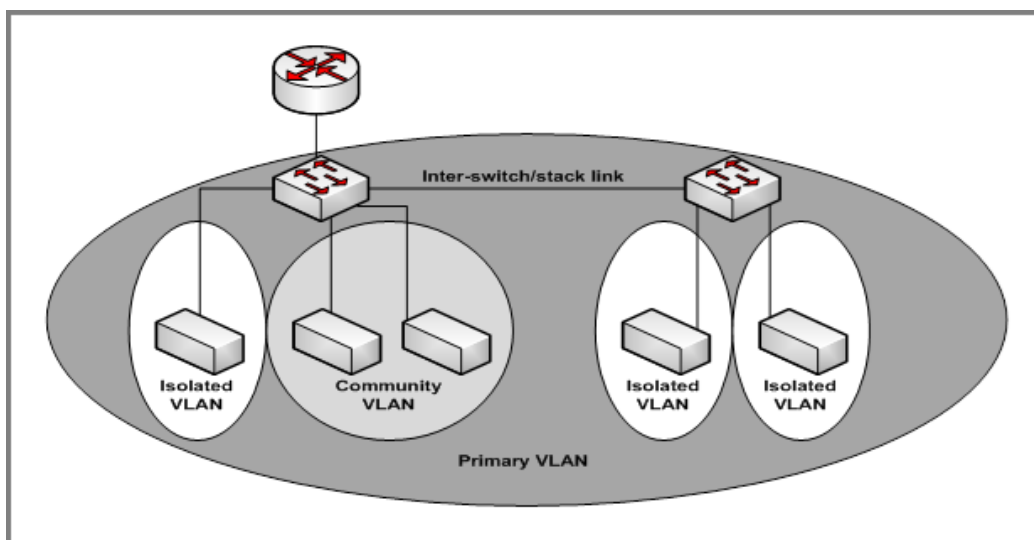


Figure 4. Private VLANs

Figure 2 illustrates the private VLAN traffic flow. Five ports A, B, C, D, and E make up a private VLAN. Port A is a promiscuous port which is associated with the primary VLAN 100. Ports B and C are the host ports which belong to the isolated VLAN 101. Ports D and E are the community ports which are associated with community VLAN 102. Port F is the inter-switch/stack link. It is configured to transmit VLANs 100, 101 and 102. Colored arrows represent possible packet flow paths in the private VLAN domain.

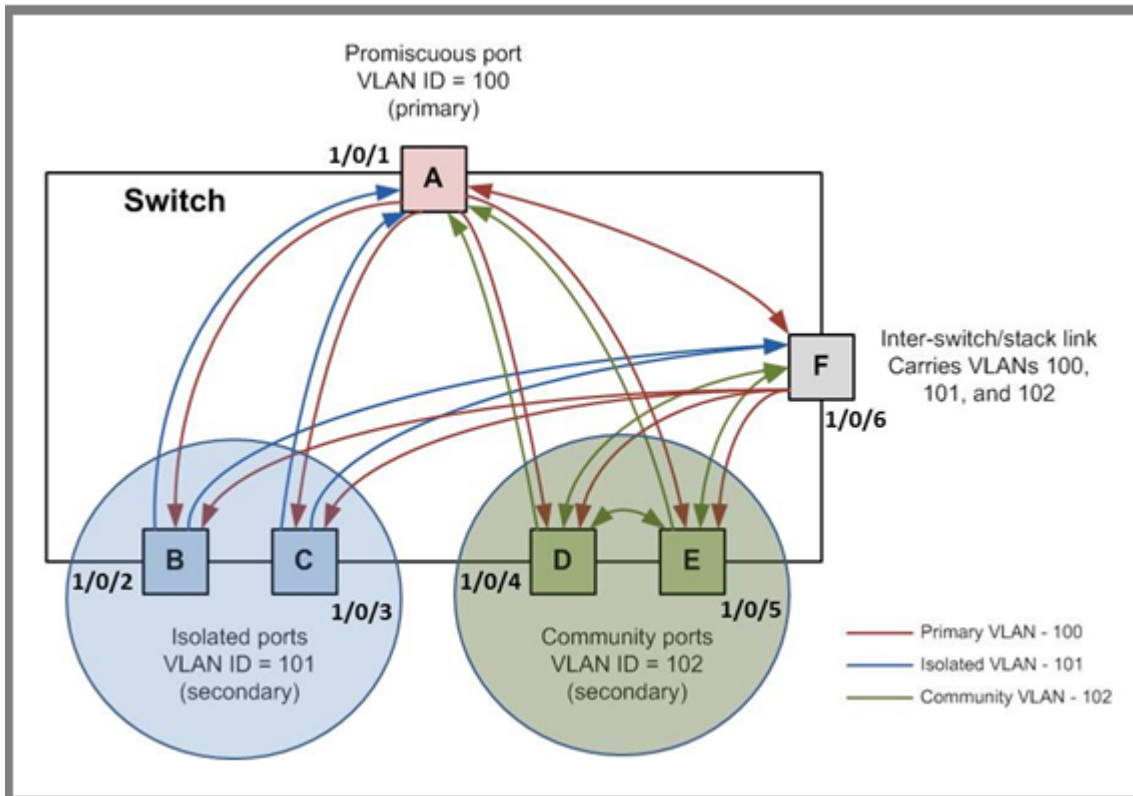


Figure 5. Packet flow within a Private VLAN domain

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

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

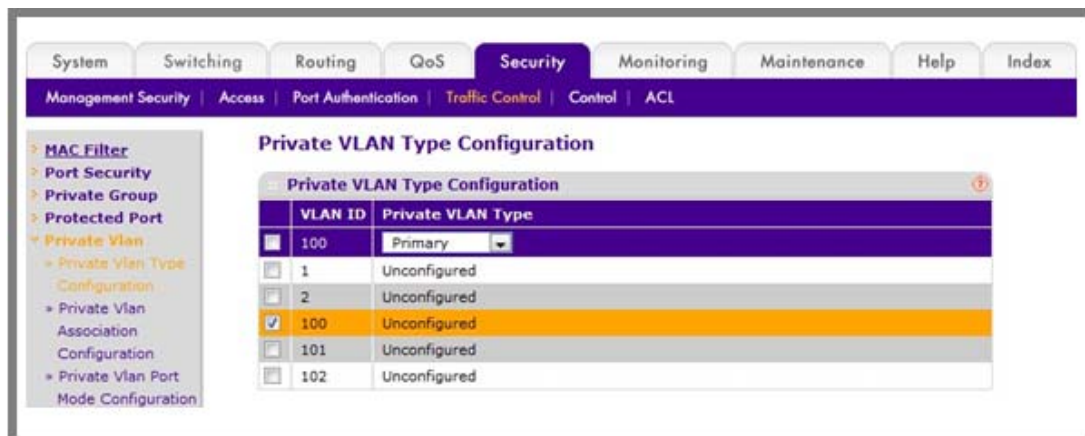
CLI: Assign Private-VLAN Type (Primary, Isolated, Community)

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

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

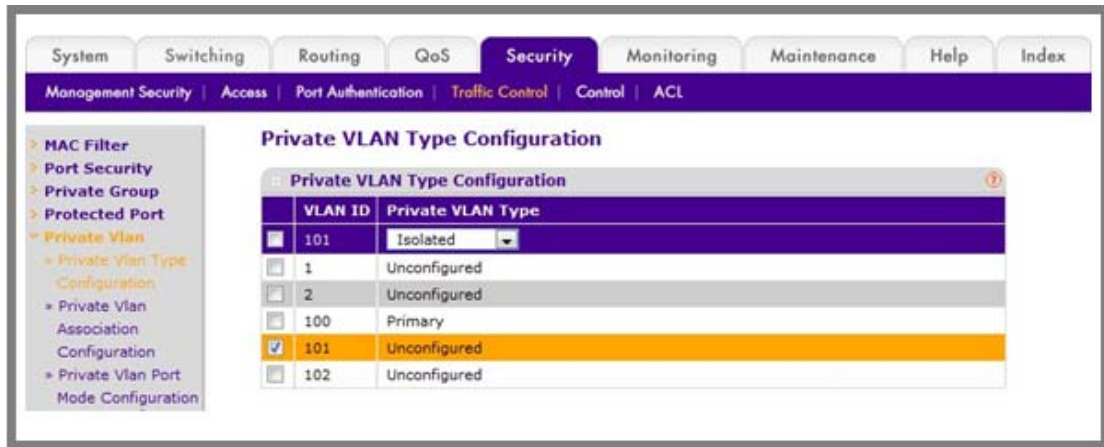
Web Interface: Assign Private-VLAN Type (Primary, Isolated, Community)

1. Create VLAN 10.
 - a. Select **Security > Traffic Control > Private VLAN > Private VLAN Type Configuration**. A screen similar to the following displays.

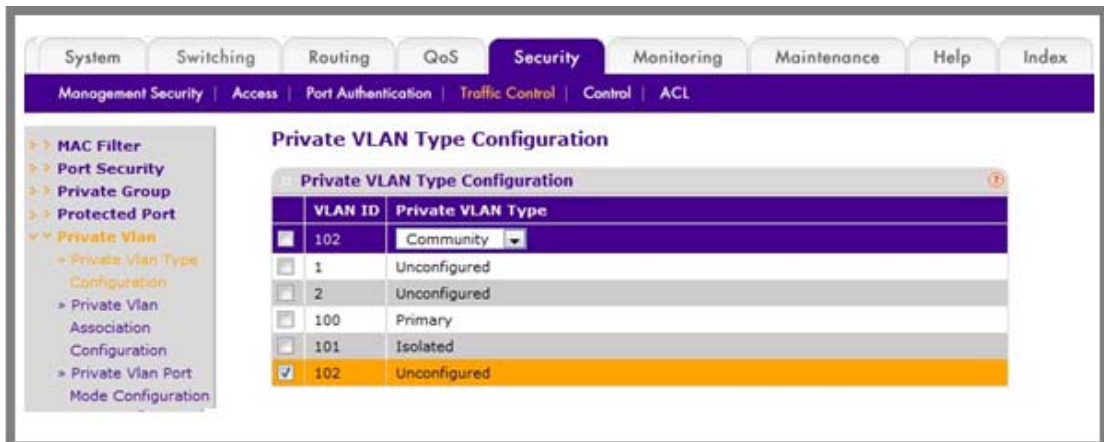


- b. Under **Private VLAN Type Configuration**, select the **VLAN ID 100** check box. Now 100 appears in the interface field at the top.
 - c. In the **Private VLAN Type** field, select **Primary** from the pull-down menu.
 - d. Click **Apply** to save the settings

2. Assign VLAN 101 as an isolated VLAN.
 - a. Select **Security > Traffic Control > Private VLAN > Private VLAN Type Configuration**. A screen similar to the following displays.



- b. Under **Private VLAN Type Configuration**, select the **VLAN ID 101** check box. Now 101 appears in the interface field at the top.
 - c. In the **Private VLAN Type** field, select **Isolated** from the pull-down menu.
 - d. Click **Apply** to save the settings
3. Assign VLAN 102 to community VLAN.
 - a. Select **Security > Traffic Control > Private VLAN > Private VLAN Type Configuration**. A screen similar to the following displays.



- b. Under **Private VLAN Type Configuration**, select the **VLAN ID 102** check box. Now 102 appears in the interface field at the top.
 - c. In the **Private VLAN Type** field, select **Community** from the pull-down menu.
 - d. Click **Apply** to save the settings.

Configure Private-VLAN Association

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

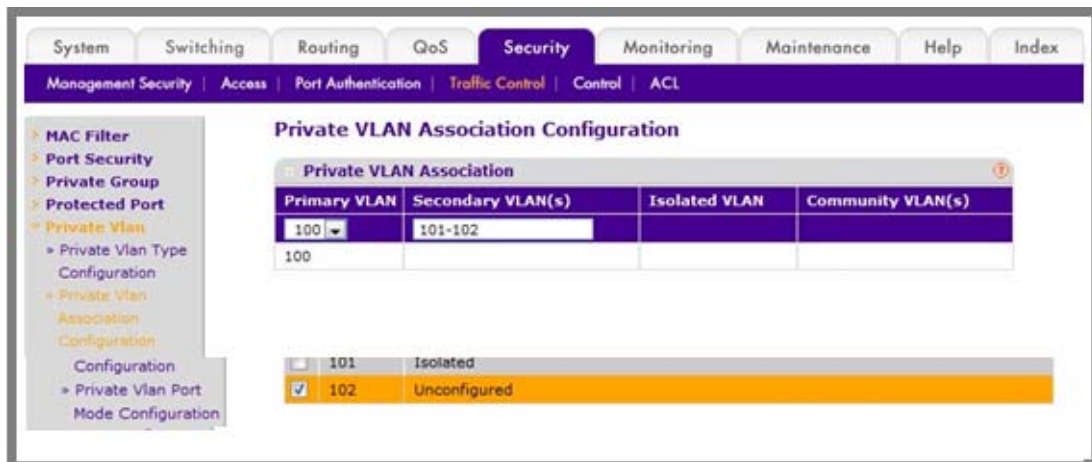
CLI: Configure Private-VLAN Association

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

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

Web Interface: Configure Private-VLAN Association

1. Associate VLAN 101-102 (secondary VLAN) to VLAN 100 (primary VLAN).
 - a. Select **Security > Traffic Control > Private VLAN > Private VLAN Association Configuration**. A screen similar to the following displays.



- b. Under **Private VLAN Association Configuration**, select the VLAN ID 100.
- c. In the **Secondary VLAN(s)** field, type 101-102.
- d. Click **Apply** to save the settings.

Configure Private-VLAN Port Mode (Promiscuous, Host)

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

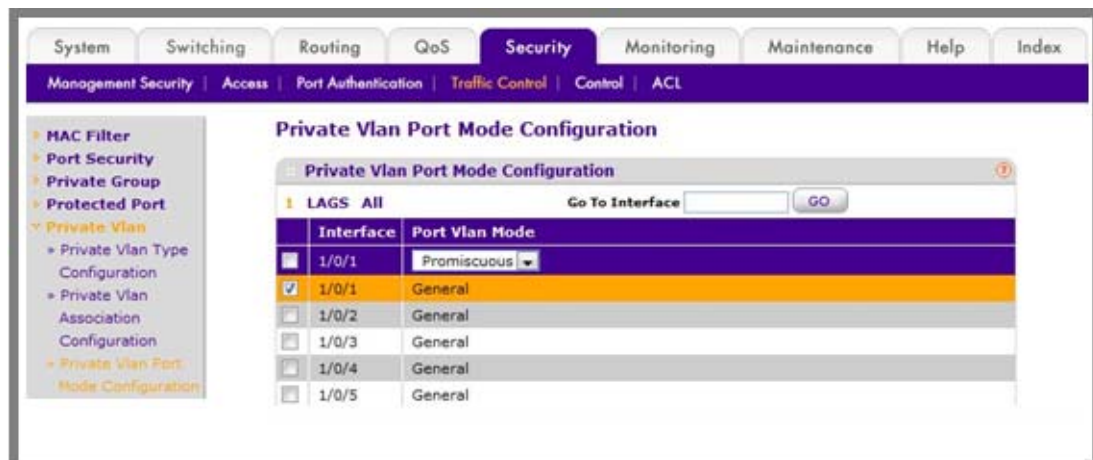
CLI: Configure Private-VLAN Port Mode (Promiscuous, Host)

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

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

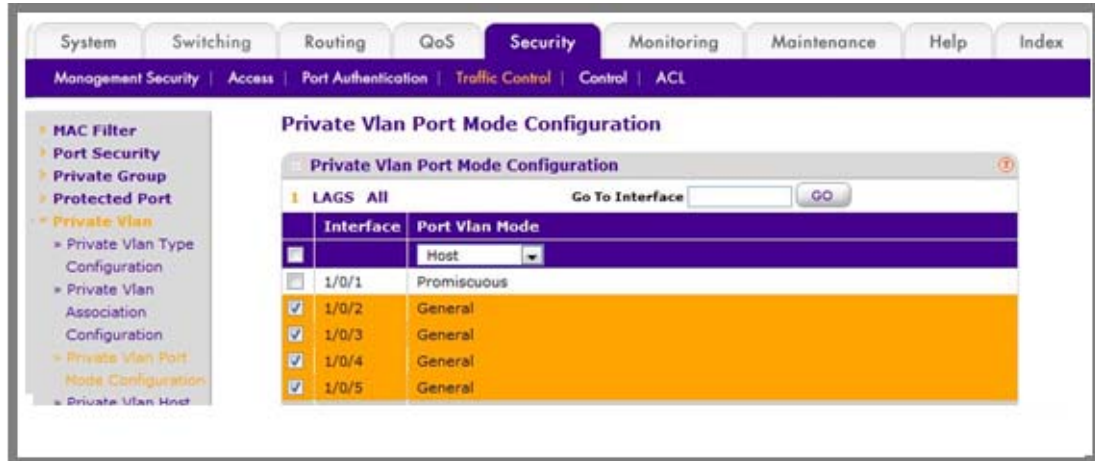
Web Interface: Configure Private-VLAN Port Mode (Promiscuous, Host)

1. Configure port 1/0/1 to promiscuous port mode.
 - a. Select **Security > Traffic Control > Private VLAN > Private VLAN Port Mode Configuration**. A screen similar to the following displays.



- b. Under **Private VLAN Port Mode Configuration**, select the 1/0/1 interface check box. Now 1/0/1 appears in the **Interface** field at the top.
 - c. In the **Port VLAN Mode** field, select **Promiscuous** from the pull-down menu.
 - d. Click **Apply** to save the settings.

2. Configure ports 1/0/2-1/0/5 to host port mode.
 - a. Select **Security > Traffic Control > Private VLAN > Private VLAN Port Mode Configuration**. A screen similar to the following displays.



- b. Under **Private VLAN Port Mode Configuration**, select the 1/0/2 to 1/0/5 interface check box.
- c. In the **Port VLAN Mode** field, select Host from the pull-down menu.
- d. Click **Apply** to save the settings.

Configure Private-VLAN Host Ports

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

CLI: Configure Private-VLAN Host Ports

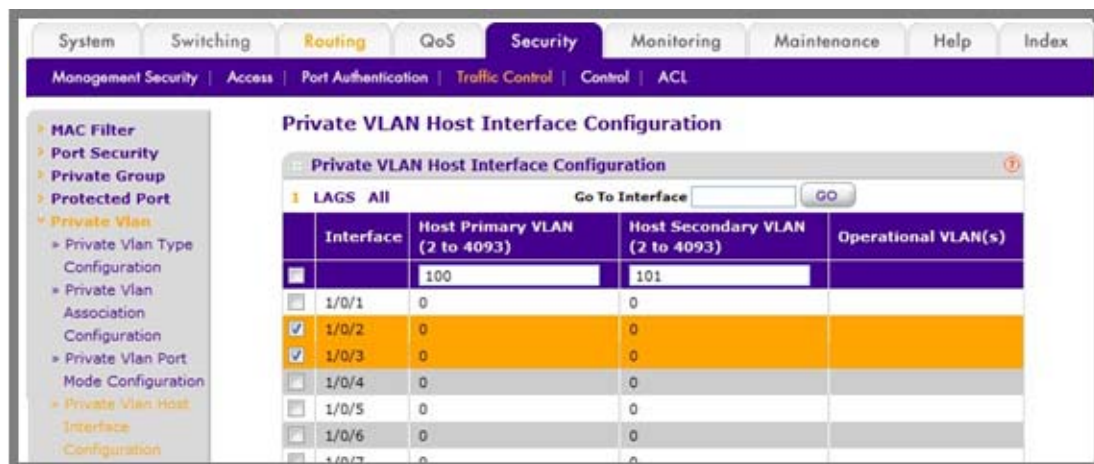
Use the following commands to associate isolated ports 1/0/2-1/0/3 to a private-VLAN (primary=100, secondary=101). Community ports 1/0/4-1/0/5 to a private-VLAN (primary=100, secondary=102).

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

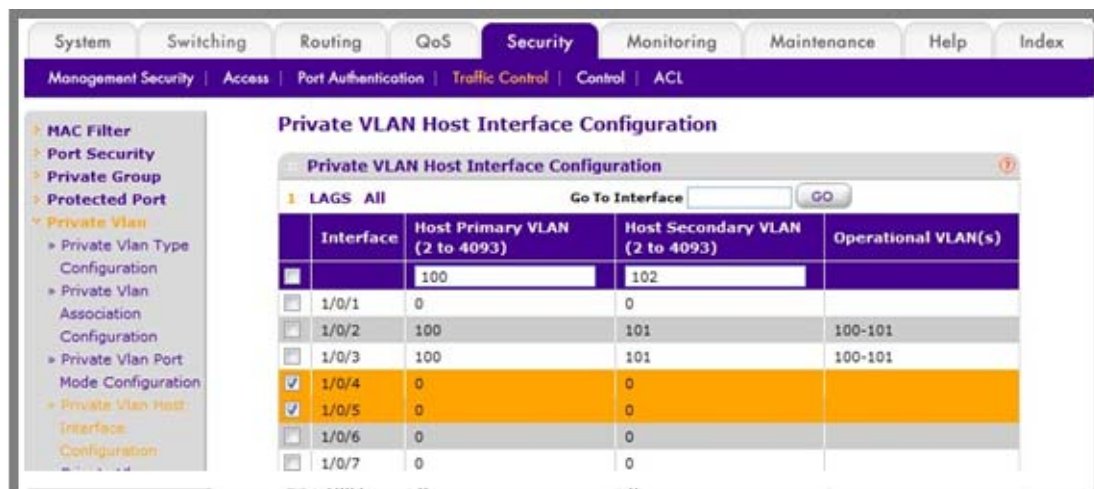
Web Interface: Assign Private-VLAN Port Host Ports

1. Associate isolated ports 1/0/2-1/0/3 to a private-VLAN (primary=100, secondary=101).

- a. Select **Security > Traffic Control > Private VLAN > Private VLAN Host Interface Configuration**. A screen similar to the following displays.



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



- b. Under **Private VLAN Host Interface Configuration**, select the 1/0/4 and 1/0/5 interface check box.
- c. In the **Host Primary VLAN** field, enter 100.
- d. In the **Host Secondary VLAN** field, enter 102.
- e. Click **Apply** to save the settings.

Map Private-VLAN Promiscuous Port

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

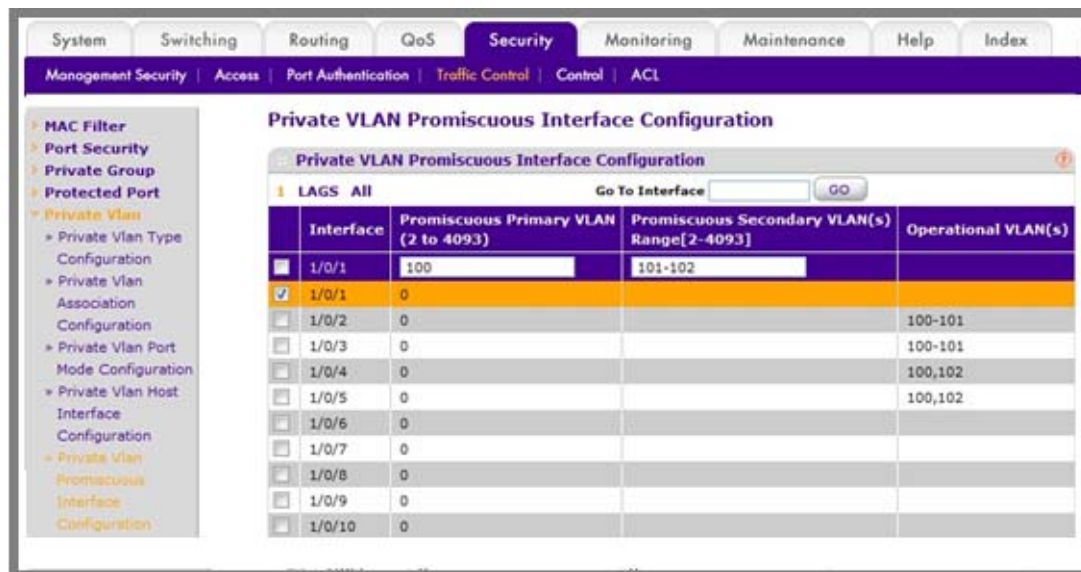
CLI: Map Private-VLAN Promiscuous Port

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

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

Web Interface: Map Private-VLAN Promiscuous Port

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



- b. Under **Private VLAN Promiscuous Interface Configuration**, select the 1/0/1 interface check box. Now 1/0/1 appears in the **Interface** field at the top.
- c. In the **Promiscuous Primary VLAN** field, enter 100.
- d. In the **Promiscuous Secondary VLAN** field, enter 101-102.
- e. Click **Apply** to save the settings.

Link Aggregation Groups

This chapter provides the following examples:

- *Create Two LAGs* on page 54
- *Add Ports to LAGs* on page 55
- *Enable Both LAGs* on page 58

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

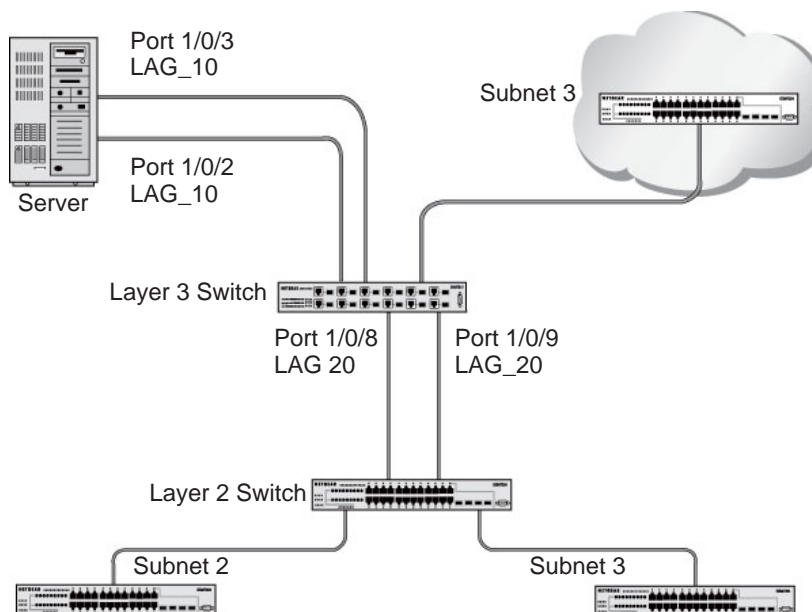


Figure 6. Example network with two LAGs

LAGs offers 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 two- or fivefold increase, useful if only a small increase is needed.

Create Two LAGs

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

CLI: Create Two LAGs

```
(Netgear Switch) #config
(Netgear Switch) (Config)#port-channel lag_10
(Netgear Switch) (Config)#port-channel lag_20
(Netgear Switch) (Config)#exit
```

Use the `show port-channel all` command to show the logical interface IDs you will use to identify the LAGs in subsequent commands. Assume that `lag_10` is assigned ID 1/1, and `lag_20` is assigned ID 1/2.

```
(Console) #show port-channel all
```

Log. Intf	Port-Channel Name	Link Link	Link			Mbr Type	Port Ports	Port Speed	Port Active
			Adm. Mode	Trap Mode	STP Mode				
1/1	lag_10	Down	En.	En.	Dis.	Dynamic			
1/2	lag_20	Down	En.	En.	Dis.	Dynamic			

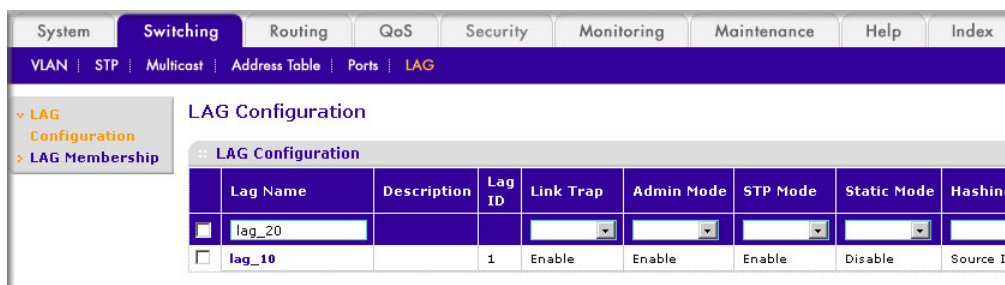
Web Interface: Create Two LAGs

1. Create LAG `lag_10`.

- a. Select **Switching > LAG > LAG Configuration**. A screen similar to the following displays.



- b. In the **Lag Name** field, enter **lag_10**.
 - c. Click **Add**.
2. Create LAG lag_20.
- a. Select **Switching > LAG > LAG Configuration**. A screen similar to the following displays.



- b. In the **Lag Name** field, enter **lag_20**.
- c. Click **Add**.

Add Ports to LAGs

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

CLI: Add Ports to the LAGs

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


Web Interface: Add Ports to LAGs

1. Add ports to lag_10.
 - a. Select **Switching > LAG > LAG Membership**. A screen similar to the following displays.

The screenshot shows the 'LAG Membership' configuration page for 'Lag 1' (LAG Name: lag_10). The configuration includes:

- LAG ID: Lag 1
- LAG Name: lag_10
- LAG Description: (empty)
- Admin Mode: Enable
- Link Trap: Enable
- STP Mode: Enable
- Static Mode: Disable
- Hash Mode: Source IP and Source TCP/UDP Port

 The 'Port Selection Table' shows 'Unit 1' expanded, with a grid of ports 1 through 24. Checkmarks are visible in the boxes for ports 2 and 3.

- b. In the **LAG ID** list, select **LAG 1**.
 - c. Click **Unit 1**. The ports display.
 - d. Click the gray boxes under port **2** and **3**. Two check marks display in the box.
 - e. Click **Apply** to save the settings.
2. Add ports to lag_20.

- a. Select **Switching > LAG > LAG Membership**. A screen similar to the following displays.

The screenshot shows the 'LAG Membership' configuration page for 'Lag 2' (LAG Name: lag_20). The configuration includes:

- LAG ID: Lag 2
- LAG Name: lag_20
- LAG Description: (empty)
- Admin Mode: Enable
- Link Trap: Enable
- STP Mode: Enable
- Static Mode: Disable
- Hash Mode: Source IP and Source TCP/UDP Port

 The 'Port Selection Table' shows 'Unit 1' expanded, with a grid of ports 1 through 24. Checkmarks are visible in the boxes for ports 8 and 9.

- b. Under LAG Membership, in the **LAG ID** list, select **LAG 2**.
 - c. Click **Unit 1**. The ports display.
 - d. Click the gray boxes under ports **8** and **9**. Two check marks display in the boxes.
 - e. Click **Apply** to save the settings.

Enable Both LAGs

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

CLI: Enable Both LAGs

By default, the system enables link trap notification.

```
(Console) #config
(Console) (Config)#port-channel adminmode all
(Console) (Config)#exit
```

At this point, the LAGs could be added to VLANs.

Web Interface: Enable Both LAGs

- a. Select **Switching > LAG > LAG Configuration**. A screen similar to the following displays.

	Lag Name	Description	Lag ID	Link Trap	Admin Mode	STP Mode	Static Mode	Hashing
<input checked="" type="checkbox"/>					Enable			
<input checked="" type="checkbox"/>	lag_10		1	Enable	Enable	Enable	Disable	Source IP
<input checked="" type="checkbox"/>	lag_20		2	Enable	Enable	Enable	Disable	Source IP

- b. Select the top check box and the check boxes for **lag_10** and **lag_20** are selected.
- c. In the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.

This chapter provides the following sections:

- *Port Routing Configuration* on page 60
- *Enable Routing for the Switch* on page 61
- *Enable Routing for Ports on the Switch* on page 61
- *Add a Default Route* on page 64
- *Add a Static Route* on page 65

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 7000 Series Managed 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 7000 Series Managed Switch always supports Layer 2 bridging, but Layer 3 routing must be explicitly enabled, first for the 7000 Series Managed Switch as a whole, and then for each port that is to be part of the routed network.

The configuration commands used in the example in this section enable IP routing on ports 1/0/2, 1/0/3, and 1/0/5. The router ID will be set to the 7000 Series Managed Switch's management IP address, or to that of any active router interface if the management address is not configured.

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

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

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

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

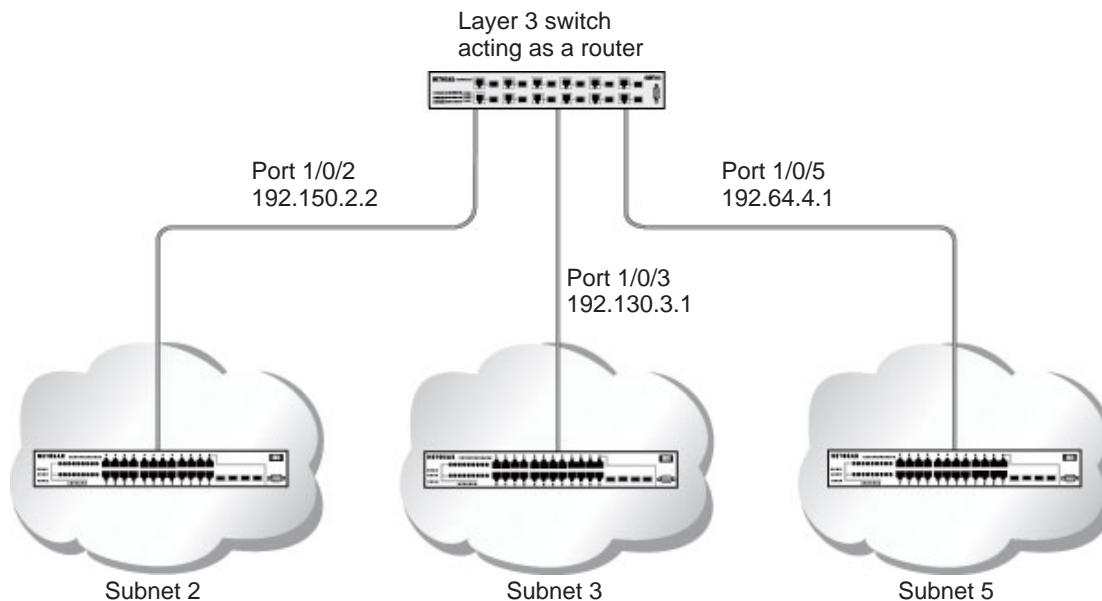


Figure 7. Layer 3 switch configured for port routing

Enable Routing for the Switch

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

CLI: Enable Routing for the Switch

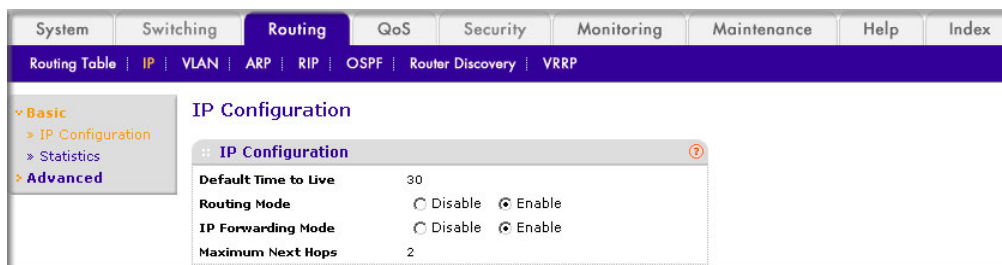
The following script shows the commands you would use to configure a 7000 Series Managed Switch to provide the port routing support shown in [Figure 7, Layer 3 switch configured for port routing](#) on page 60.

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

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

Web Interface: Enable Routing for the Switch

1. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.



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

Enable Routing for Ports on the Switch

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

CLI: Enable Routing for Ports on the Switch

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

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

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

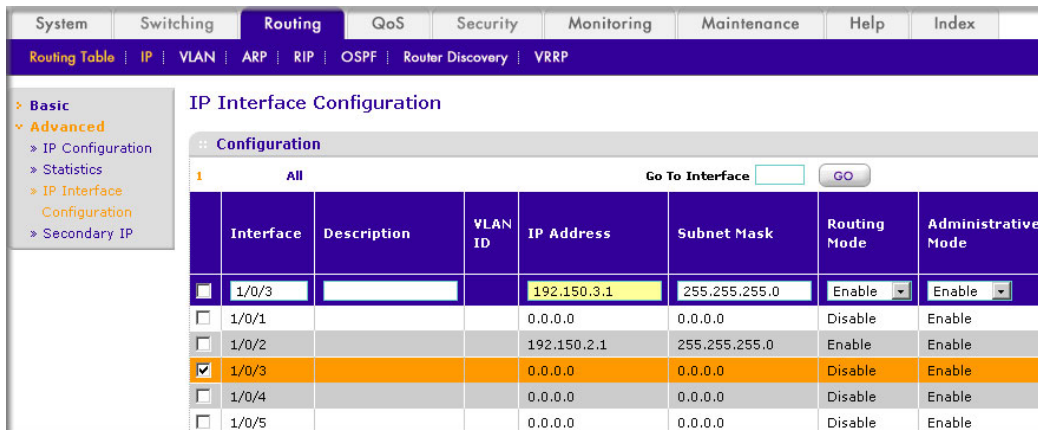
Web Interface: Enable Routing for Ports on the Switch

1. Assign IP address 192.150.2.1/24 to interface 1/0/2.
 - a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

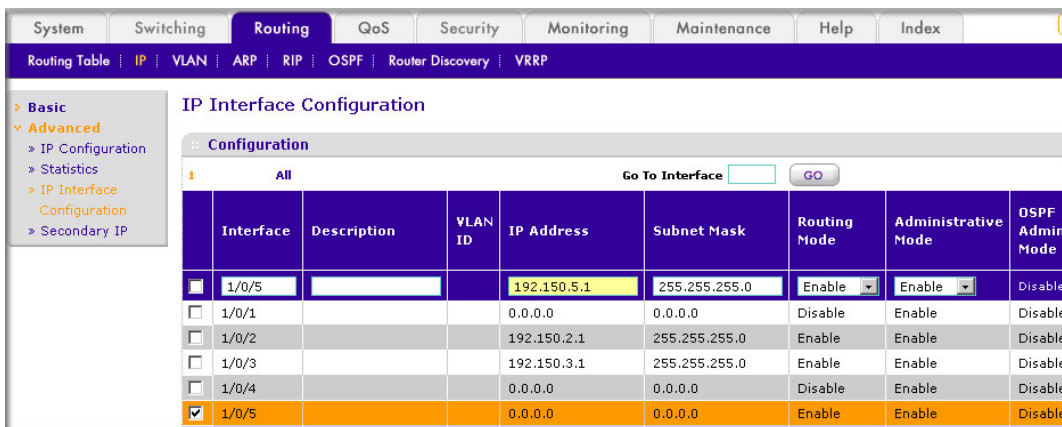
Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable
<input checked="" type="checkbox"/> 1/0/2			192.150.2.1	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/3			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 1/0/4			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the interface **1/0/2** check box. Now 1/0/2 appears in the Interface field at the top.
- c. Under the IP Interface Configuration, enter the following information:
 - In the **IP Address** field, enter **192.150.2.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.

2. Assign IP address 192.150.3.1/24 to interface 1/0/3.
 - a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the interface **1/0/3** check box. Now 1/0/3 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.150.3.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
3. Assign IP address 192.150.5.1/24 to interface 1/0/5.



- b. Scroll down and select the interface **1/0/5** check box. Now 1/0/5 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.150.5.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.

- In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.

Add a Default Route

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

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

CLI: Add a Default Route

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

Note that IP subnet 10.10.10.0 should be configured using either port routing ([Enable Routing for Ports on the Switch](#) on page 61) or VLAN routing (see [Set Up VLAN Routing for the VLANs and the Switch](#) on page 72).

Web Interface: Add a Default Route

1. Select **Routing > Routing Table > Basic > Route Configuration**. The Route Configuration screen displays.

The screenshot shows the 'Route Configuration' page in the web interface. The 'Route Type' dropdown menu is open, showing 'DefaultRoute' selected. The 'Next Hop IP Address' field is populated with '10.10.10.2'. Below the configuration table, there is a section for 'Learned Routes' with a table structure.

Route Type	Network Address	Subnet mask	Protocol	Next Hop Interface	Next Hop IP Address	Preference	Metric
DefaultRoute					10.10.10.2		

2. In the **Route Type** list, select **DefaultRoute**.
3. In the **Next Hop IP Address** field, enter one of the routing interface's IP addresses.
 - The **Network Address** and **Subnet Mask** fields will not accept input as they are not needed.

- The **Preference** field is optional. A value of 1 (highest) will be assigned by default if not specified.
4. Click the **Add** button on the bottom of the screen. This creates the default route entry in the routing table.

Add a Static Route

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

CLI: Add a Static Route

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

```
(FSM7328S) #show ip route

Total Number of Routes.....1

Network Subnet Next Hop Next Hop
AddressMaskProtocolIntfIP Address
-----
10.10.10.0 255.255.255.0 Local 1/0/3 10.10.10.1
```

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

Web Interface: Add a Static Route

1. Select **Routing > Routing Table > Basic > Route Configuration** to display the Route Configuration screen.

Route Type	Network Address	Subnet mask	Next Hop IP Address	Preference
<input checked="" type="checkbox"/> Static	10.10.20.0	255.255.255.0	192.168.1.1	
<input type="checkbox"/> Static DefaultRoute	0.0.0.0	0.0.0.0	10.10.10.2	1

Route Type	Network Address	Subnet mask	Protocol	Next Hop Interface	Next Hop IP Address	Preference	Metric
------------	-----------------	-------------	----------	--------------------	---------------------	------------	--------

2. In the **Route Type** list, select **Static**.
3. Fill in the **Network Address** field. Note that this field should have a network IP address, not a host IP address. Do not enter something like *10.100.100.1*. The last number should always be 0 (zero).
4. In the **Subnet Mask** field, enter a value that matches the subnet range that you want to use.
5. The **Preference** field is optional. A value of 1 is entered by default if you do not enter a number.
6. Click the **Add** button on the bottom of the screen. The screen is updated with the static route shown in the routing table.
7. To remove a route entry, either static or default, select the check box to the left of the entry, and click the **Delete** button on the bottom of the screen.

This chapter provides the following examples:

- *Create Two VLANs* on page 67
- *Set Up VLAN Routing for the VLANs and the Switch* on page 72

You can configure the 7000 Series Managed 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 additional segmentation or security is required.

The next section shows you how to configure the 7000 Series Managed Switch to support VLAN routing and how to use RIP and OSPF. A port can be either a VLAN port or a router port, but not both. However, a VLAN port can be part of a VLAN that is itself a router port.

Create Two VLANs

This section provides an example of how to configure the 7000 Series Managed Switch to support VLAN routing. The configuration of the VLAN router port is similar to that of a physical port. The main difference is that, after the VLAN has been created, you must use the *show ip vlan* command to determine the VLAN's interface ID so that you can use it in the router configuration commands.

The diagram in this section shows a Layer 3 switch configured for port routing. It connects two VLANs, with two ports participating in one VLAN, and one port in the other. The script

shows the commands you would use to configure a 7000 Series Managed Switch to provide the VLAN routing support shown in the diagram.

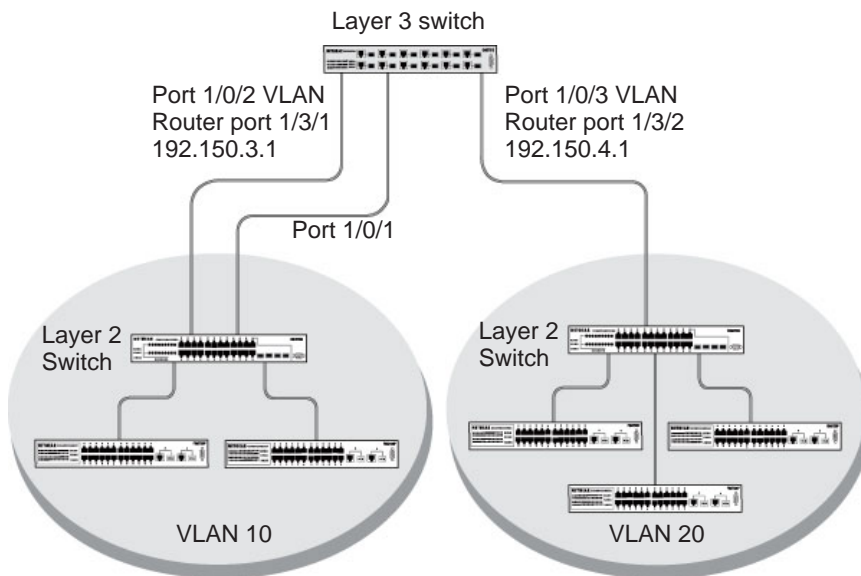


Figure 8. Layer 3 switch configured for port routing

CLI: Create Two VLANs

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

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

Web Interface: Create Two VLANs

1. Create VLAN 10 and VLAN20.

- a. Select **Switching > VLAN > Advanced > VLAN Configuration**. A screen similar to the following displays.

The screenshot shows the 'VLAN Configuration' page in the web interface. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. Under 'Switching', there are links for VLAN, STP, Multicast, Address Table, Ports, and LAG. The left sidebar shows a tree view with 'Basic' and 'Advanced' sections. Under 'Advanced', 'VLAN' is expanded to show 'Configuration', 'VLAN Membership', 'VLAN Status', 'MAC Based VLAN', 'Port PVID Configuration', 'Port DVLAN Configuration', and 'Protocol Based'. The main content area is titled 'VLAN Configuration' and includes a 'Reset Configuration' checkbox and a table for VLAN configuration.

	VLAN ID	VLAN Name	VLAN Type
<input checked="" type="checkbox"/>	10	VLAN10	Static
<input type="checkbox"/>	1	Default	Default

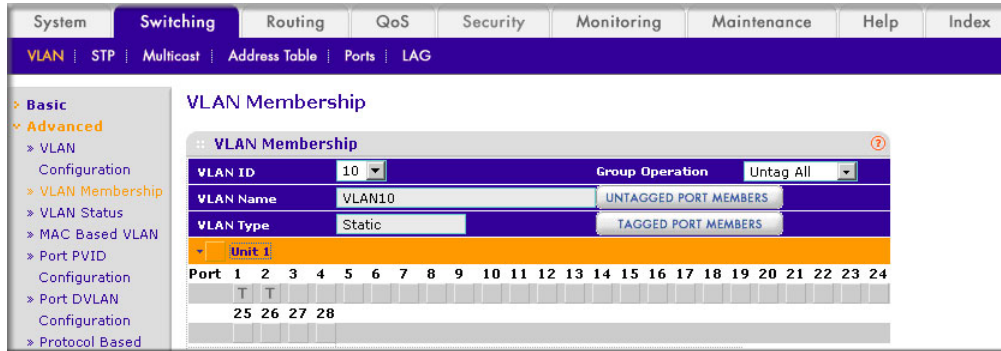
- b. In the **VLAN ID** field, enter **10**.
- c. In the **VLAN Name** field, enter **VLAN10**.
- d. In the **VLAN Type** list, select **Static**.
- e. Click **Add**.
- f. Select **Switching > VLAN > Advanced > VLAN Configuration**. A screen similar to the following displays.

The screenshot shows the 'VLAN Configuration' page in the web interface, similar to the previous one. The 'VLAN ID' field is now set to 20, and the 'VLAN Name' is VLAN20. The 'VLAN Type' is still Static. The table now shows two entries: one for VLAN 20 and one for VLAN 10.

	VLAN ID	VLAN Name	VLAN Type
<input checked="" type="checkbox"/>	20	VLAN20	Static
<input type="checkbox"/>	1	Default	Default
<input type="checkbox"/>	10	VLAN10	Static

- g. In the **VLAN ID** field, enter **20**.
 - h. In the **VLAN Name** field, enter **VLAN20**.
 - i. In the **VLAN Type** list, select **Static**.
 - j. Click **Add**.
2. Add ports to the VLAN10 and VLAN20.

- a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays.

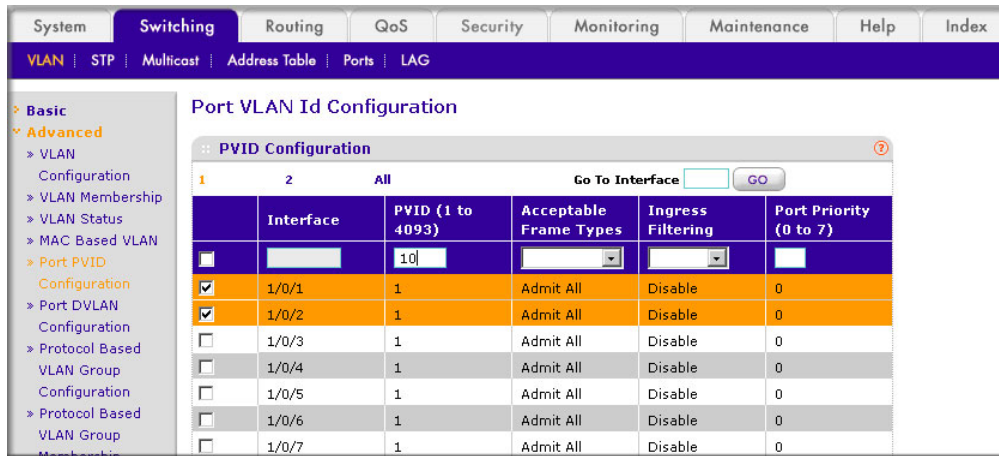


- b. In the **VLAN ID** field, select **10**.
- c. Click the **Unit 1**. The ports display.
- d. Click the gray boxes under ports **1** and **2** until **T** displays. The T specifies that the egress packet is tagged for the port.
- e. Click **Apply**.
- f. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays.

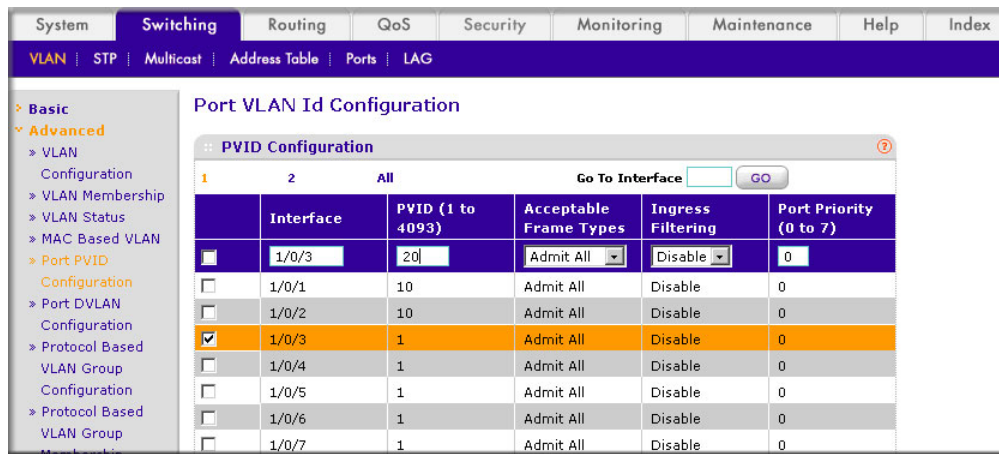


- g. In the **VLAN ID** list, select **20**.
- h. Click **Unit 1**. The ports display.
- i. Click the gray box under port **3** until **T** displays. The T specifies that the egress packet is tagged for the port.
- j. Click **Apply**.
3. Assign PVID to VLAN10 and VLAN20.

- a. Select **Switching > VLAN > Advanced > Port PVID Configuraton**. A screen similar to the following displays.



- b. Scroll down and select **1/0/1** and **1/0/2** check boxes.
- c. In the **PVID (1 to 4093)** field, enter **10**.
- d. Click **Apply** to save the settings.
- e. Select **Switching > VLAN > Advanced > Port PVID Configuraton**. A screen similar to the following displays.



- f. Scroll down and select the **1/0/3** check box.
- g. In the **PVID (1 to 4093)** field, enter **20**.
- h. Click **Apply** to save the settings.

Set Up VLAN Routing for the VLANs and the Switch

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

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

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

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

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

2. Enable routing for the switch.

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

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

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


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

1. Select **Routing > VLAN > VLAN Routing**. A screen similar to the following displays.

The screenshot shows the 'VLAN Routing Configuration' page. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. Under 'Routing', there are links for Routing Table, IP, VLAN, ARP, RIP, OSPF, Router Discovery, and VRRP. The 'VLAN Routing' section is expanded, showing a table with the following data:

	VLAN ID (1 to 4093)	Port	MAC Address	IP Address	Subnet Mask
<input type="checkbox"/>	10			192.150.3.1	255.255.255.0

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

The screenshot shows the 'VLAN Routing Configuration' page after adding a second entry. The table now contains two rows:

	VLAN ID (1 to 4093)	Port	MAC Address	IP Address	Subnet Mask
<input type="checkbox"/>	20			192.150.4.1	255.255.255.0
<input type="checkbox"/>	10	0/2/1	00:14:6c:e8:7e:1b	192.150.3.1	255.255.255.0

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

Routing Information Protocol

This chapter provides the following examples:

- *Routing for the Switch* on page 75
- *Routing for Ports* on page 76
- *RIP for the Switch* on page 77
- *RIP for Ports 1/0/2 and 1/0/3* on page 78
- *VLAN Routing with RIP* on page 80

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 managed switch supports both):

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

You can configure a given port to do the following:

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

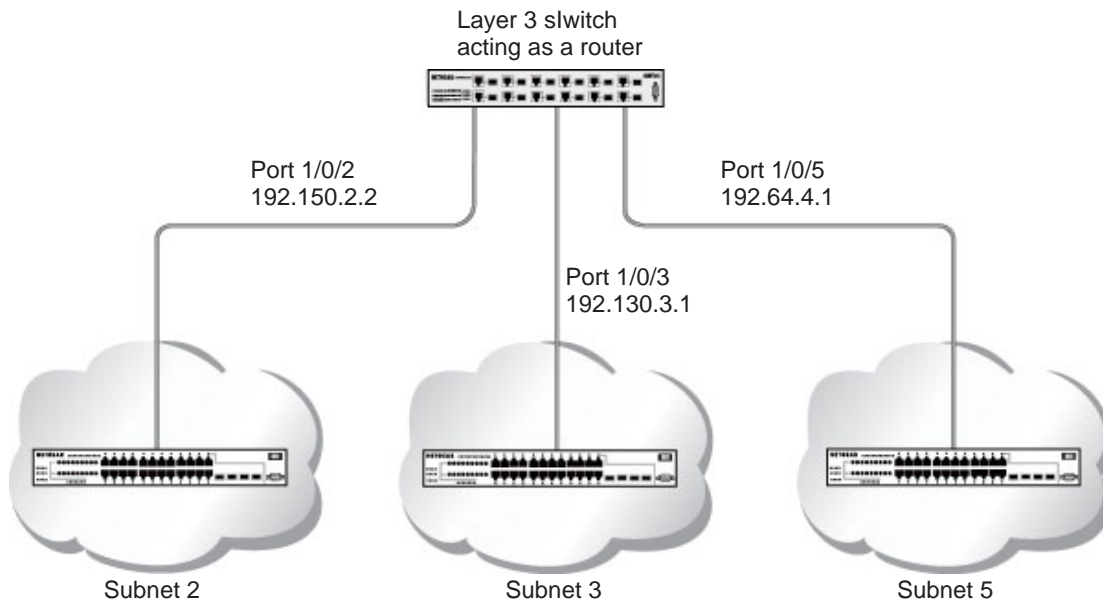


Figure 9. Network with RIP on ports 1/0/2 and 1/0/3

Routing for the Switch

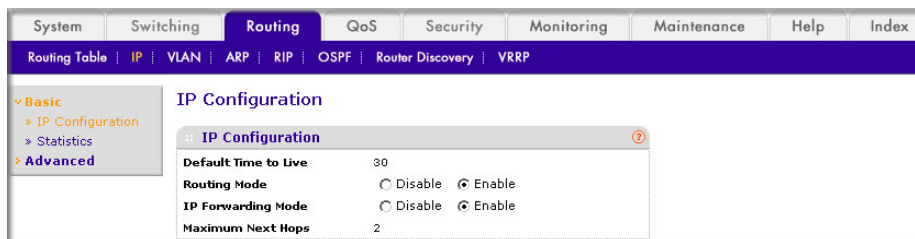
The example is shown as CLI commands and as a Web interface procedure.

CLI: Enable Routing for the Switch

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

Web Interface: Enable Routing for the Switch

1. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.



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

Routing for Ports

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

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

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

Web Interface: Enable Routing for the Ports

1. Assign IP address 192.150.2.1/24 to interface 1/0/2.
 - a. Select **Routing > Advanced > IP Interface Configuration**. A screen similar to the following displays.

Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable
<input checked="" type="checkbox"/> 1/0/2			192.150.2.1	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/3			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 1/0/4			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the Interface **1/0/2** check box. Now 1/0/2 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.150.2.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.

2. Assign IP address 192.150.3.1/24 to interface 1/0/3.
 - a. Select **Routing > Advanced > IP Interface Configuration**. A screen similar to the following displays.

Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/3			192.150.3.1	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 1/0/2			192.150.2.1	255.255.255.0	Enable	Enable
<input checked="" type="checkbox"/> 1/0/3			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 1/0/4			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 1/0/5			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the interface **1/0/3** check box. Now 1/0/3 appears in the Interface field at the top.
- c. Enter the following information:
 - In the **IP Address** field, enter **192.150.3.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.

RIP for the Switch

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

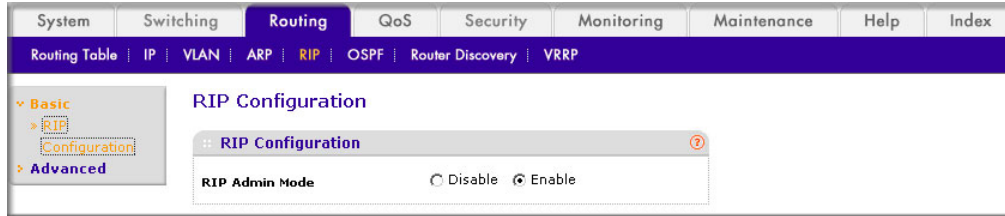
CLI: Enable RIP on the Switch

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

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

Web Interface: Enable RIP on the Switch

1. Select **Routing > RIP > Basic > RIP Configuration**. A screen similar to the following displays.



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

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

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

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

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

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

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

1. Select **Routing > RIP > Advanced > RIP Configuration**. A screen similar to the following displays.

The screenshot shows the web interface for configuring RIP on a switch. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. Under Routing, the path is RIP > OSPF > Router Discovery > VRRP. The left sidebar shows a tree view with Basic, Advanced, RIP Configuration, Interface Configuration, Route, and Redistribution. The main content area is titled 'Interface Configuration' and shows settings for interface 1/0/2. The 'Send Version' is set to RIP-2, 'Receive Version' is Both, and 'RIP Admin Mode' is Enable. Below the configuration fields is a 'Status' table.

Interface	IP Address	Send Version	Receive Version	Admin Mode	Link State	Bad Packets Received	Bad Routes Received	Updates Sent
1/0/2	0.0.0.0	RIP-2	Both	Disable	Link Down	0	0	0
1/0/3	0.0.0.0	RIP-2	Both	Disable	Link Down	0	0	0

2. Enter the following information:
 - In the **Interface** field, select **1/0/2**.
 - For RIP Admin Mode, select the **Enable** radio button.
 - In the **Send Version** field, select **RIP-2**.
3. Click **Apply** to save the settings.
4. Select **Routing > RIP > Advanced > RIP Configuration**. A screen similar to the following displays.

The screenshot shows the web interface for configuring RIP on a switch. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. Under Routing, the path is RIP > OSPF > Router Discovery > VRRP. The left sidebar shows a tree view with Basic, Advanced, RIP Configuration, Interface Configuration, Route, and Redistribution. The main content area is titled 'Interface Configuration' and shows settings for interface 1/0/3. The 'Send Version' is set to RIP-2, 'Receive Version' is Both, and 'RIP Admin Mode' is Disable. Below the configuration fields is a 'Status' table.

Interface	IP Address	Send Version	Receive Version	Admin Mode	Link State	Bad Packets Received	Bad Routes Received	Updates Sent
1/0/2	0.0.0.0	RIP-2	Both	Disable	Link Down	0	0	0
1/0/3	0.0.0.0	RIP-2	Both	Disable	Link Down	0	0	0

5. Enter the following information:
 - In the **Interface** field, select **1/0/3**.
 - For RIP Admin Mode, select the **Enable** radio button.
 - In the **Send Version** list, select **RIP-2**.

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

VLAN Routing with RIP

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.

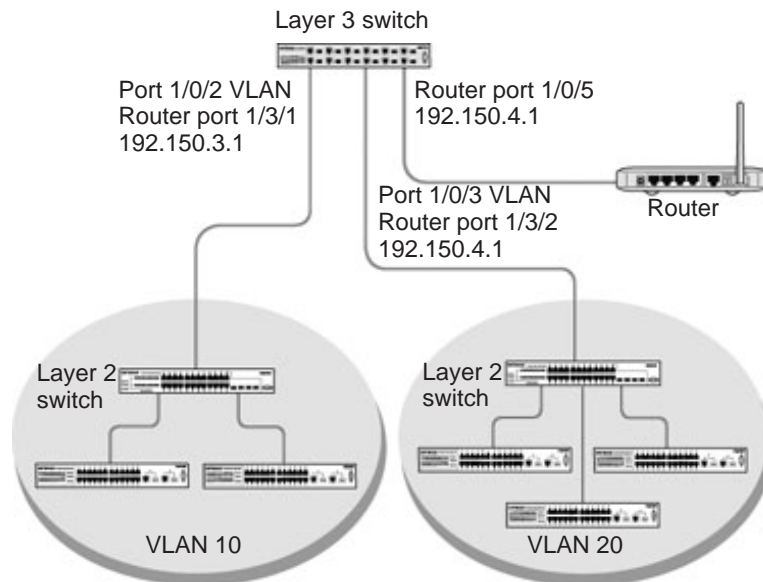


Figure 10. VLAN routing RIP configuration example

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

- Configure VLAN routing with RIP support on a 7000 Series Managed Switch.

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



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

2. Enable RIP for the switch. The route preference defaults to 15.

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

3. Configure the IP address and subnet mask for a 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
```

Web Interface: Configure VLAN Routing with RIP Support

1. Configure a VLAN and include ports 1/0/2 in the VLAN:
 - a. Select **Routing > VLAN > VLAN Routing Wizard**. A screen similar to the following displays.

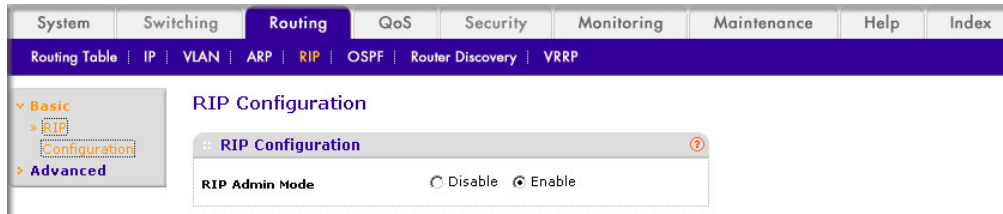
System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index																
Routing Table IP VLAN ARP RIP OSPF Router Discovery VRRP																								
VLAN Routing Wizard :: VLAN Routing Wizard																								
Vlan ID			10																					
LAG Enabled			<input type="checkbox"/>																					
IP Address			192.150.3.1			Network Mask			255.255.255.0															
Unit 1																								
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
		T																						
		25	26	27	28																			

- b. Enter the following information:
 - In the **Vlan ID** field, enter **10**.
 - In the **IP Address** field, enter **192.150.3.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.
 - c. Click **Unit 1**. The ports display:
 - d. Click the gray box under port **2** until **T** displays. The T specifies that the egress packet is tagged for the port.
 - e. Click **Apply** to save the VLAN that includes ports 2.
2. Configure a VLAN, and include port 1/0/3 in the VLAN:
 - a. Select **Routing > VLAN > VLAN Routing Wizard**. A screen similar to the following displays.

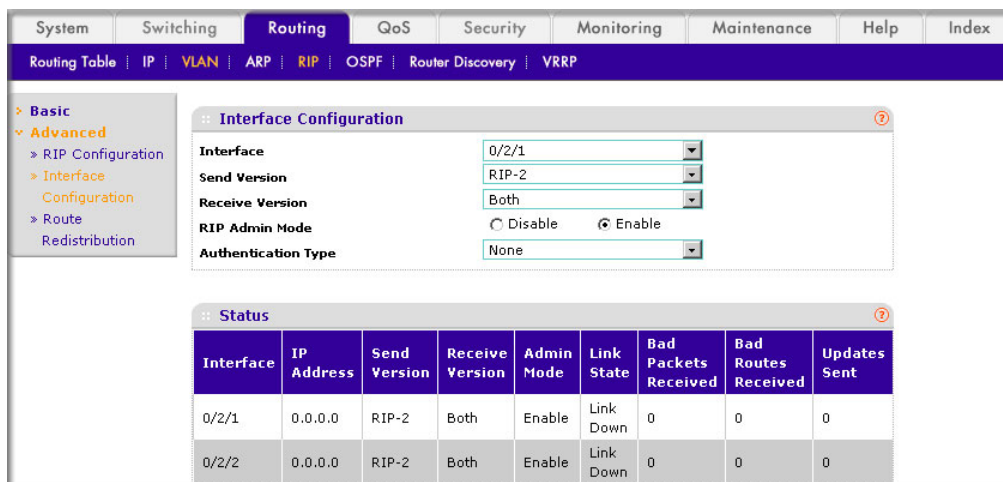
System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index																
Routing Table IP VLAN ARP RIP OSPF Router Discovery VRRP																								
VLAN Routing Wizard :: VLAN Routing Wizard																								
Vlan ID			20																					
LAG Enabled			<input type="checkbox"/>																					
IP Address			192.150.4.1			Network Mask			255.255.255.0															
Unit 1																								
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
			T																					
			25	26	27	28																		

- b. Enter the following information:
 - In the **Vlan ID** field, enter **20**.
 - In the **IP Address** field, enter **192.150.4.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.
 - c. Click **Unit 1**. The ports display.

- d. Click the gray box under port **3** until **T** displays. The T specifies that the egress packet is tagged for the port.
- e. Click **Apply** to save the VLAN that includes port 3.
3. Enable RIP on the switch (you can skip this step since the RIP is enabled by default).
 - a. Select **Routing > RIP > Basic > RIP Configuration**. A screen similar to the following displays.



- b. For RIP Admin Mode, select the **Enable** radio button.
- c. Click **Apply** to save the setting.
4. Enable RIP on VLANs 10 and 20.
 - a. Select **Routing > RIP > Advanced > RIP Configuration**. A screen similar to the following displays.



- b. Enter the following information:
 - In the **Interface** list, select **0/2/1**.
 - For RIP Admin Mode, select the **Enable** radio button.
- c. Click **Apply** to save the settings.

OSPF

7

Open Shortest Path First

This chapter provides the following examples:

- *Inter-area Router* on page 85
- *OSPF on a Border Router* on page 90
- *Stub Areas* on page 95
- *nssa Areas* on page 104
- *VLAN Routing OSPF* on page 113
- *OSPFv3* on page 118

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

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

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

The 7000 Series Managed Switch operating as a router and running OSPF determines the best route using the assigned cost and the type of the OSPF route. The order for choosing a route if more than one type of route exists is as follows:

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

Inter-area Router

The examples in this section show you how to configure a 7000 Series Managed Switch first as an inter-area router and then as a border router. They show two areas, each with its own border router connected to one inter-area router.

The following figure shows a network segment with an inter-area router connecting areas 0.0.0.2 and 0.0.0.3. The sample script shows the commands used to configure a 7000 Series Managed 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.

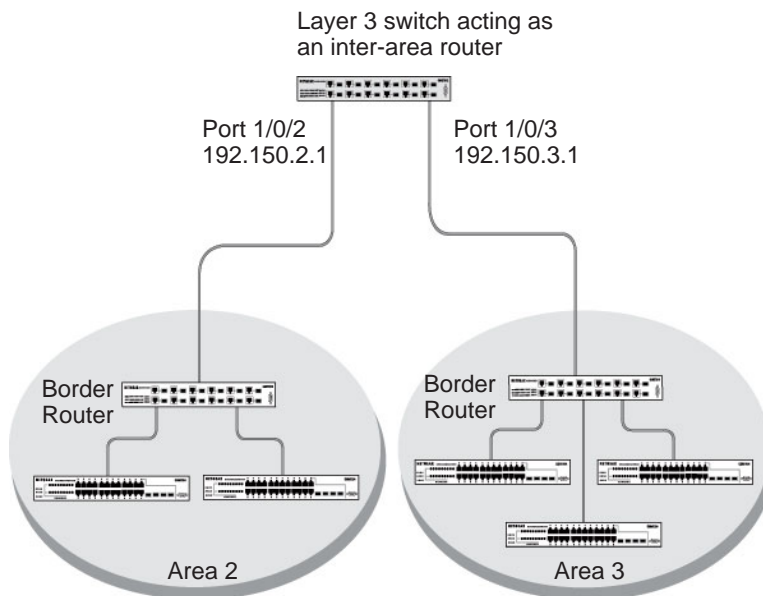


Figure 11. Network segment with an inter-area router connecting areas 0.0.0.2 and 0.0.0.3

CLI: Configure an Inter-area Router

1. Enable routing for the switch.

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

2. Assign IP addresses to ports.

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

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

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

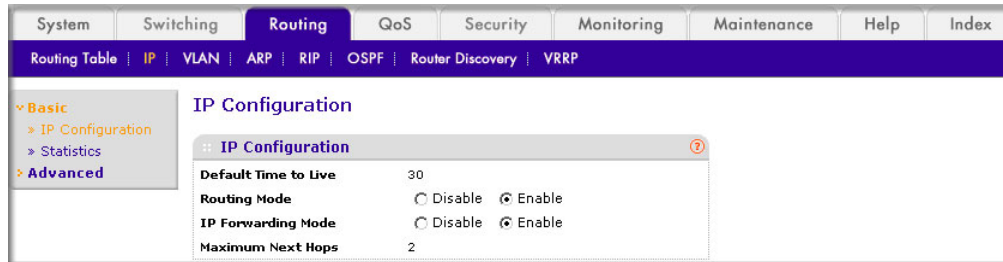
4. Enable OSPF, and set the OSPF priority and cost for the ports.

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

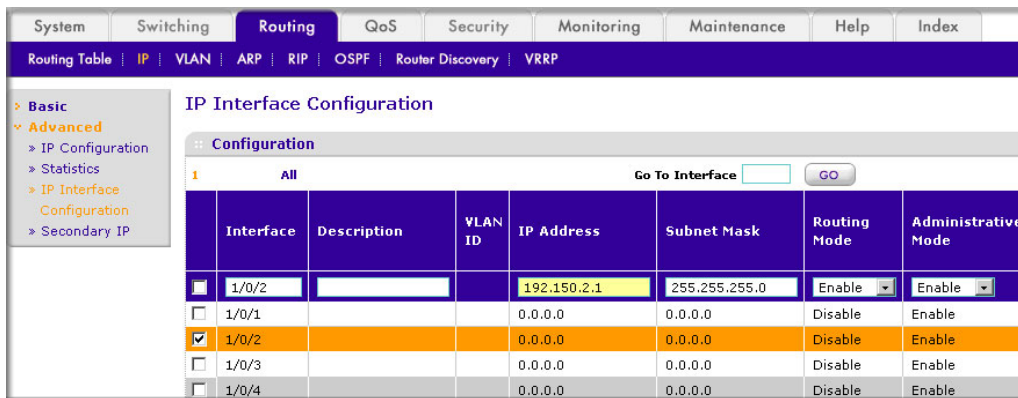
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip ospf
(Netgear Switch) (Interface 1/0/3)#ip ospf areaid 0.0.0.3
(Netgear Switch) (Interface 1/0/3)#ip ospf priority 255
(Netgear Switch) (Interface 1/0/3)#ip ospf cost 64
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch)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

Web Interface: Configure an Inter-area Router

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.



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



- b. Scroll down and select the interface **1/0/2** check box. Now 1/0/2 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.150.2.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Administrative Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
3. Assign IP address 192.150.3.1 to port 1/0/3:

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

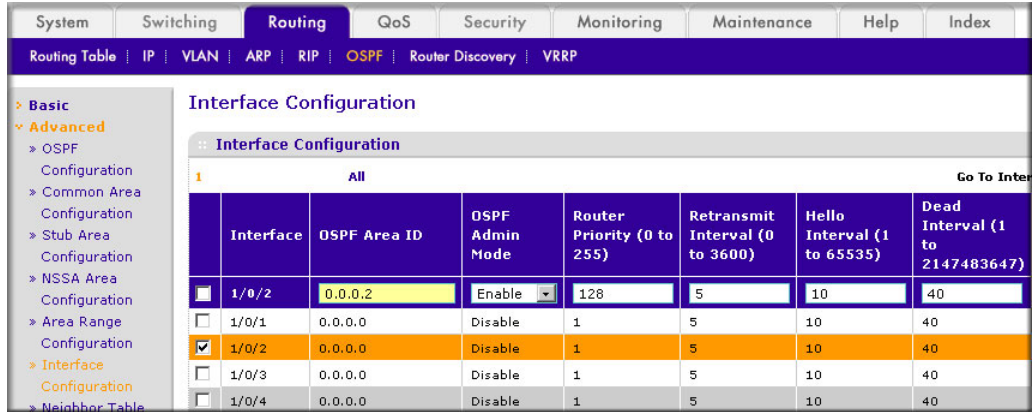
Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/3			192.150.3.1	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 1/0/2			192.150.2.1	255.255.255.0	Enable	Enable
<input checked="" type="checkbox"/> 1/0/3			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 1/0/4			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the interface **1/0/3** check box. Now 1/0/3 appears in the Interface field at the top.
- c. Enter the following information:
- In the **IP Address** field, enter **192.150.3.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.
 - In the **Administrative Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
4. Specify the router ID, and enable OSPF for the switch.
- a. Select **Routing > OSPF > Advanced > OSPF Configuration**. A screen similar to the following displays.

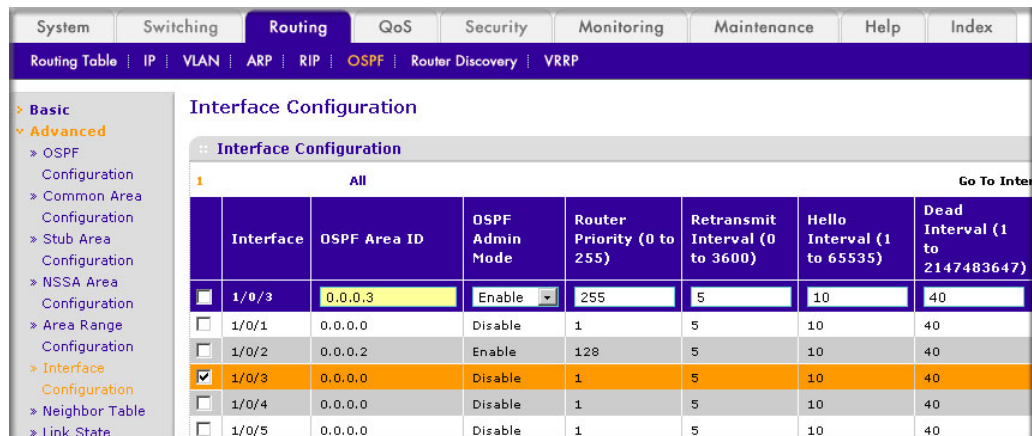
Field	Value
Default Information Originate	Disable
Always	False
Metric	(1 to 16777215)
Metric Type	External Type 2
Router ID	192.150.9.9
OSPF Admin Mode	Enable
ASBR Mode	Disabled
RFC 1583 Compatibility	Disable
ABR Status	
Exit Overflow Interval (secs)	0 (0 to 2147483647)
External LSA Count	

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

- c. Click **Apply** to save the settings.
5. Enable OSPF on port 1/0/2.
 - a. Select **Routing > OSPF > Advanced > Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the interface **1/0/2** check box. Now 1/0/2 appears in the Interface field at the top.
 - In the **OSPF Area ID** field, enter **0.0.0.2**.
 - In the the **OSPF Admin Mode** field, select **Enable**.
 - In the **Priority** field, enter **128**.
 - In the **Metric Cost** field, enter **32**.
- c. Click **Apply** to save the settings.
6. Enable OSPF on port 1/0/3.
 - a. Select **Routing > OSPF > Advanced > Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the interface **1/0/3** check box. Now 1/0/3 appears in the Interface field at the top.
 - In the **OSPF Area ID** field, enter **0.0.0.3**.
 - In the the **OSPF Admin Mode** field, select **Enable**.

- In the **Priority** field, enter **255**.
 - In the **Metric Cost** field, enter **64**.
- c. Click **Apply** to save the settings.

OSPF on a Border Router

The example is shown as CLI commands and as a Web interface procedure. For an OSPF sample network, see [Figure 11](#) on page 85.

CLI: Configure OSPF on a Border Router

1. Enable routing for the switch.

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

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

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

3. Specify the router ID, and enable OSPF for the switch. Set disable 1583compatibility to prevent a routing loop.

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

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

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

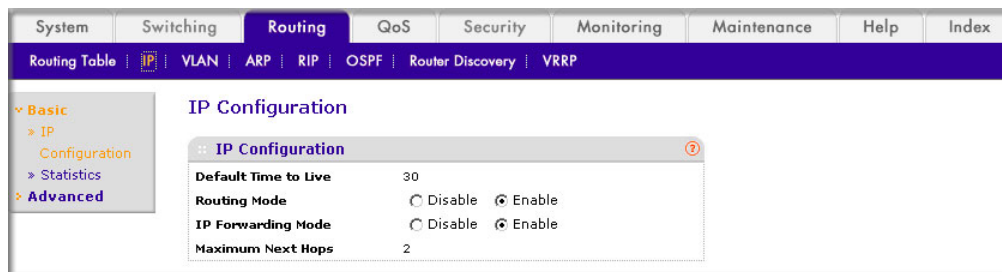
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip ospf
(Netgear Switch) (Interface 1/0/3)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/3)#ip ospf priority 255
(Netgear Switch) (Interface 1/0/3)#ip ospf cost 64
(Netgear Switch) (Interface 1/0/3)#exit

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

Web Interface: Configure OSPF on a Border Router

1. Enable IP routing on the switch.

- a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.



- b. For Routing Mode, select the **Enable** radio button.
 - c. Click **Apply** to save the settings.
- ### 2. Assign IP address 192.150.2.2 to port 1/0/2.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

The screenshot shows the 'IP Interface Configuration' page. The 'Configuration' table is as follows:

Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/2			192.150.2.2	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable
<input checked="" type="checkbox"/> 1/0/2			0.0.0.0	0.0.0.0	Disable	Enable

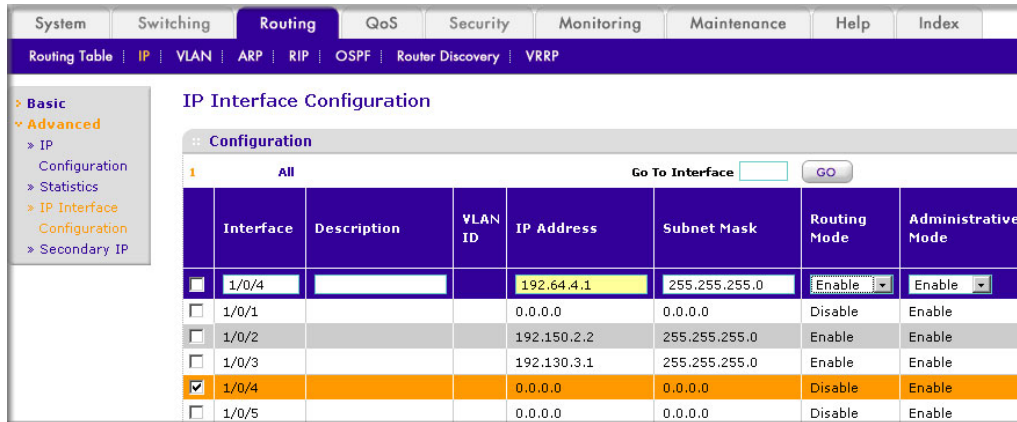
- b. Scroll down and select the interface **1/0/2** check box. Now 1/0/2 appears in the Interface field at the top.
- c. Enter the following information:
- In the **IP Address** field, enter **192.150.2.2**.
 - In the **Network Mask** field, enter **255.255.255.0**.
 - In the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
3. Assign IP address 192.130.3.1 to port 1/0/3:
- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

The screenshot shows the 'IP Interface Configuration' page. The 'Configuration' table is as follows:

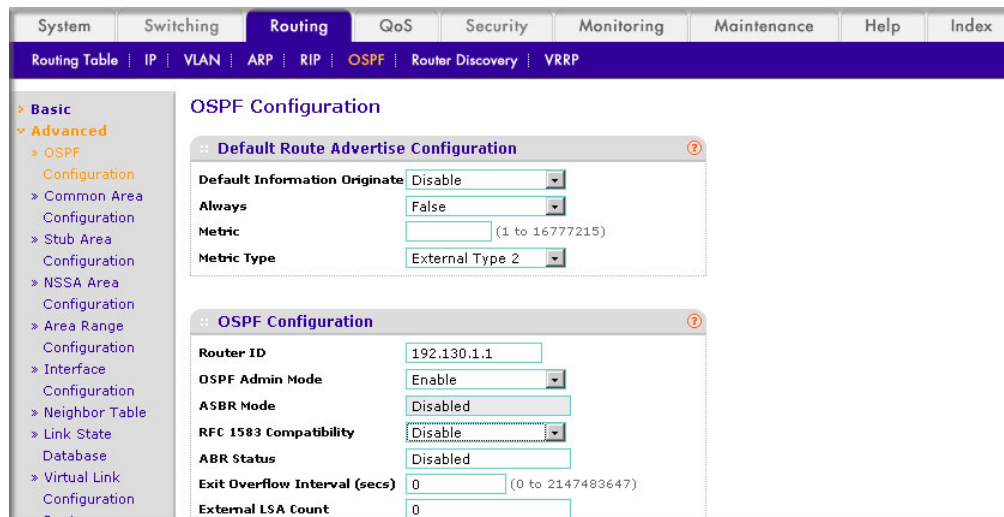
Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/3			192.130.3.1	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 1/0/2			192.150.2.2	255.255.255.0	Enable	Enable
<input checked="" type="checkbox"/> 1/0/3			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 1/0/4			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the interface **1/0/3** check box. Now 1/0/3 appears in the Interface field at the top.
- c. Enter the following information:
- In the **IP Address** field, enter **192.130.3.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.
 - In the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
4. Assign IP address 192.64.4.1 to port 1/0/4.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the interface **1/0/4** check box. Now 1/0/4 appears in the Interface field at the top.
- c. Enter the following information:
- In the **IP Address** field, enter **192.64.4.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.
 - In the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
5. Specify the router ID, and enable OSPF for the switch.
- a. Select **Routing > OSPF > Advanced > OSPF Configuration**. A screen similar to the following displays.



- b. Under OSPF Configuration, enter the following information:
- In the **Router ID** field, enter **192.130.1.1**.
 - In the **OSPF Admin Mode** field, select **Enable**.
 - In the **RFC 1583 Compatibility** field, select **Disable**.

- c. Click **Apply** to save the settings.
6. Enable OSPF on the port 1/0/2.
- a. Select **Routing > OSPF > Advanced > Interface Configuration**. A screen similar to the following displays.

Interface	OSPF Area ID	OSPF Admin Mode	Router Priority (0 to 255)	Retransmit Interval (0 to 3600)	Hello Interval (1 to 65535)	Dead Interval (1 to 2147483647)
<input type="checkbox"/> 1/0/2	0.0.0.2	Enable	128	5	10	40
<input type="checkbox"/> 1/0/1	0.0.0.0	Disable	1	5	10	40
<input checked="" type="checkbox"/> 1/0/2	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 1/0/3	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 1/0/4	0.0.0.0	Disable	1	5	10	40

- b. Under Interface Configuration, scroll down and select the interface **1/0/2** check box. Now 1/0/2 appears in the Interface field at the top.
- In the **OSPF Area ID** field, enter **0.0.0.2**.
 - In the **OSPF Admin Mode** field, select **Enable**.
 - In the **Router Priority (0 to 255)** field, enter **128**.
 - In the **Metric Cost** field, enter **32**.
- c. Click **Apply** to save the settings.
7. Enable OSPF on port 1/0/3.
- a. Select **Routing > OSPF > Advanced > Interface Configuration**. A screen similar to the following displays.

Interface	OSPF Area ID	OSPF Admin Mode	Router Priority (0 to 255)	Retransmit Interval (0 to 3600)	Hello Interval (1 to 65535)	Dead Interval (1 to 2147483647)
<input type="checkbox"/> 1/0/3	0.0.0.3	Enable	255	5	10	40
<input type="checkbox"/> 1/0/1	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 1/0/2	0.0.0.2	Enable	128	5	10	40
<input checked="" type="checkbox"/> 1/0/3	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 1/0/4	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 1/0/5	0.0.0.0	Disable	1	5	10	40

- b. Under Interface Configuration, scroll down and select the interface **1/0/3** check box. Now 1/0/3 appears in the Interface field at the top.
- In the **OSPF Area ID** field, enter **0.0.0.3**.
 - In the **OSPF Admin Mode** field, select **Enable**.

- In the **Priority** field, enter **255**.
 - In the **Metric Cost** field, enter **64**.
- c. Click **Apply** to save the settings.
8. Enable OSPF on port 1/0/4.
- a. Select **Routing > OSPF > Advanced > Interface Configuration**. A screen similar to the following displays.

Interface	OSPF Area ID	OSPF Admin Mode	Router Priority (0 to 255)	Retransmit Interval (0 to 3600)	Hello Interval (1 to 65535)	Dead Interval (1 to 2147483647)
<input checked="" type="checkbox"/> 1/0/4	0.0.0.2	Enable	255	5	10	40
<input type="checkbox"/> 1/0/1	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 1/0/2	0.0.0.2	Enable	128	5	10	40
<input type="checkbox"/> 1/0/3	0.0.0.3	Enable	255	5	10	40
<input type="checkbox"/> 1/0/5	0.0.0.0	Disable	1	5	10	40

- b. Under Interface Configuration, scroll down and select the interface **1/0/4** check box. Now 1/0/4 appears in the Interface field at the top.
- In the **OSPF Area ID** field, enter **0.0.0.2**.
 - In the **OSPF Admin Mode** field, select the **Enable**.
 - In the **Priority** field, enter **255**.
 - In the **Metric Cost** field, enter **64**.
- c. Click **Apply** to save the settings.

Stub Areas

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

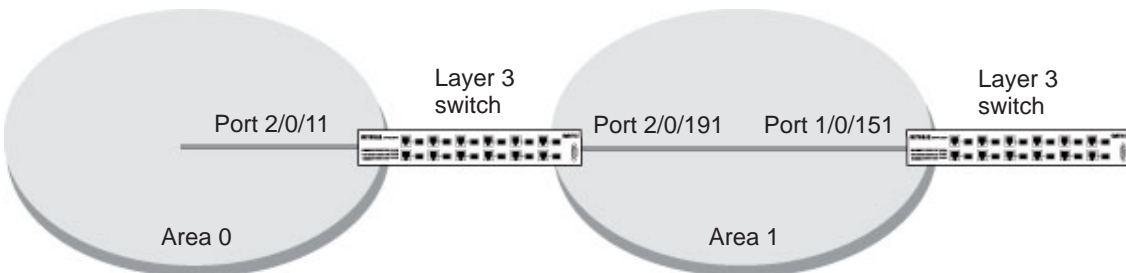


Figure 12. Area 1 is a stub area

CLI: Configure Area 1 as a Stub Area on A1

1. Enable routing on the switch.

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

2. Set the router ID to 1.1.1.1.

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

3. Configure area 0.0.0.1 as a stub area.

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

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

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

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

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

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

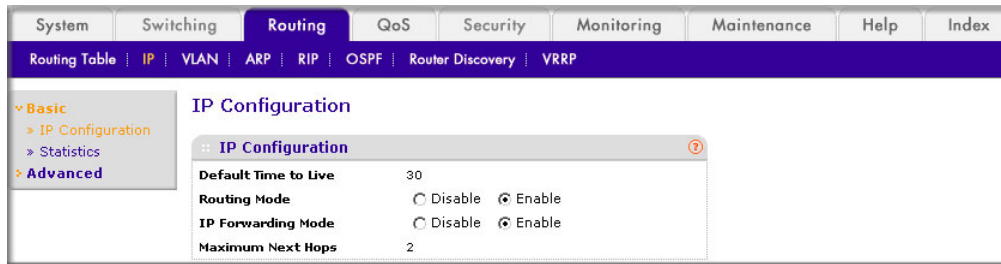
```
(Netgear Switch) (Config)#interface 2/0/19  
(Netgear Switch) (Interface 2/0/19)#routing  
(Netgear Switch) (Interface 2/0/19)#ip address 192.168.20.1 255.255.255.0  
(Netgear Switch) (Interface 2/0/19)#ip ospf  
(Netgear Switch) (Interface 2/0/19)#ip ospf areaid 0.0.0.1  
(Netgear Switch) (Interface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



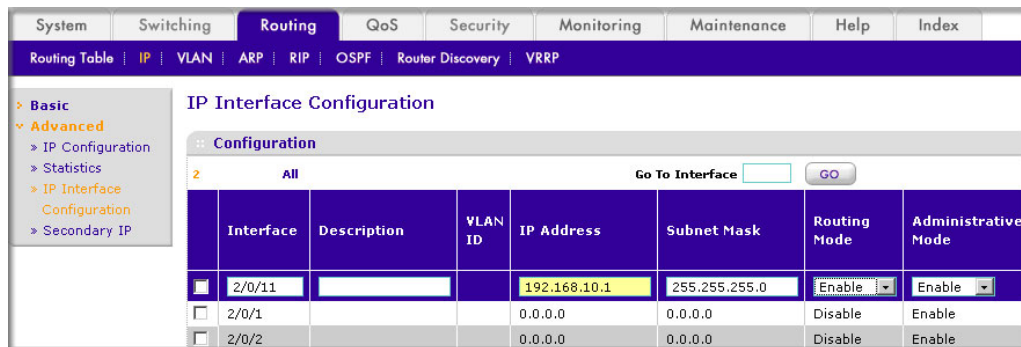
```
(Netgear Switch) (Config)#ex
(Netgear Switch) #show ip ospf neighbor interface all
  Router ID      IP Address      Neighbor Interface  State
-----
4.4.4.4         192.168.10.2   2/0/11              Full
2.2.2.2         192.168.20.2   2/0/19              Full
(Netgear Switch) #show ip route
Total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

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

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.



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



- b. Scroll down and select the interface **2/0/11** check box. Now 2/0/11 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.10.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.
 - In the the **Admin Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
3. Assign IP address 192.168.20.1 to port 2/0/19:
 - a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 2/0/19			192.168.20.1	255.255.255.0	Enable	Enable
<input type="checkbox"/> 2/0/1			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 2/0/2			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 2/0/3			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the interface **2/0/19** check box. Now 2/0/19 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.20.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.
 - In the the **Admin Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
4. Specify the router ID, and enable OSPF for the switch.
 - a. Select **Routing > OSPF > Basic > OSPF Configuration**. A screen similar to the following displays.

OSPF Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Router ID	1.1.1.1

- b. Under OSPF Configuration, in the **Router ID** field, enter **1.1.1.1**.
 - c. Click **Apply** to save the settings.
5. Enable OSPF on the port 2/0/11.

- a. Select **Routing > OSPF > Advanced > Interface Configuration**. A screen similar to the following displays.

Interface	OSPF Area ID	Admin Mode	Priority (0 to 255)	Interval (0 to 3600)	Interval (1 to 65535)	Interval (1 to 2147483647)
<input checked="" type="checkbox"/> 2/0/11	0.0.0.0	Enable	1	5	10	40
<input type="checkbox"/> 2/0/1	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 2/0/2	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 2/0/3	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 2/0/4	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 2/0/5	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 2/0/6	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 2/0/7	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 2/0/8	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 2/0/9	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 2/0/10	0.0.0.0	Disable	1	5	10	40

- b. Under Interface Configuration, scroll down and select the interface **2/0/11** check box. Now 2/0/11 appears in the Interface field at the top.
- In the **OSPF Area ID** field, enter **0.0.0.0**.
 - In the the **Admin Mode** field, select **Enable**.

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

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

- a. Select **Routing > OSPF > Advanced > Interface Configuration**. A screen similar to the following displays.

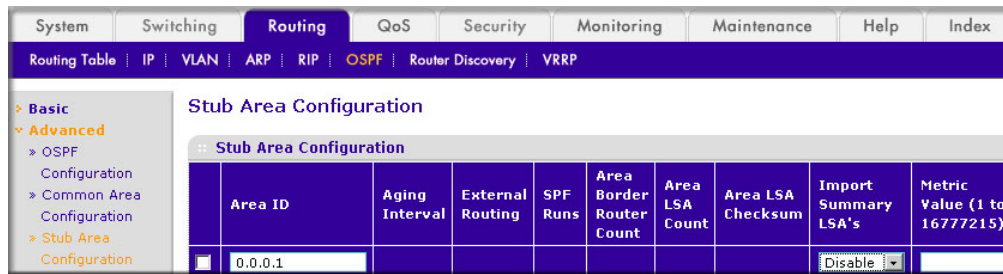
Interface	OSPF Area ID	OSPF Admin Mode	Router Priority (0 to 255)	Retransmit Interval (0 to 3600)	Hello Interval (1 to 65535)	Dead Interval (1 to 2147483647)	Iftransit Delay Interval (1 to 3600)
<input checked="" type="checkbox"/> 2/0/19	0.0.0.1	Enable	1	5	10	40	1
<input type="checkbox"/> 2/0/1	0.0.0.0	Disable	1	5	10	40	1
<input type="checkbox"/> 2/0/2	0.0.0.0	Disable	1	5	10	40	1
<input type="checkbox"/> 2/0/3	0.0.0.0	Disable	1	5	10	40	1

- b. Under Interface Configuration, scroll down and select the interface **2/0/19** check box. Now 2/0/19 appears in the Interface field at the top.
- In the **OSPF Area ID** field, enter **0.0.0.1**.
 - In the the **OSPF Admin Mode** field, select **Enable**.

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

7. Configure area 0.0.0.1 as a stub area.

- a. Select **Routing > OSPF > Advanced > Stub Area Configuration**. A screen similar to the following displays.



- b. Enter the following information:
- In the **Area ID** field, enter **0.0.0.1**.
 - In the **Import Summary LSAs** field, select **Disable**.
- c. Click **Add** to save the settings.

CLI: Configure Area 1 as a Stub Area on A2

1. Enable routing on the switch.

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

2. Set the router ID to 2.2.2.2.

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

3. Configure area 0.0.0.1 as a stub area.

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

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

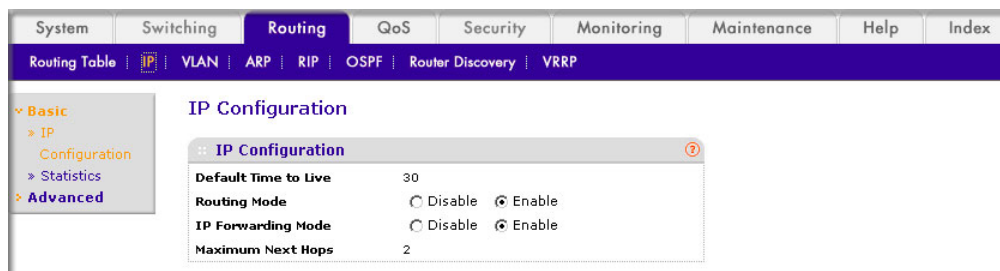
```
(Netgear Switch) (Config-router)#exit
(Netgear Switch) (Config-router)#exit
(Netgear Switch) (Config)#interface 1/0/15
(Netgear Switch) (Interface 1/0/15)#routing
(Netgear Switch) (Interface 1/0/15)#ip address 192.168.20.2 255.255.255.0
(Netgear Switch) (Interface 1/0/15)#ip ospf
(Netgear Switch)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

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

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

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

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.



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

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/15			192.168.20.2	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 1/0/2			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the interface **1/0/15** check box. Now 1/0/15 appears in the Interface field at the top.
- c. Enter the following information:
- In the **IP Address** field, enter **192.168.20.2**.
 - In the **Network Mask** field, enter **255.255.255.0**.
 - In the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
3. Specify the router ID, and enable OSPF for the switch.
- a. Select **Routing > OSPF > Basic > OSPF Configuration**. A screen similar to the following displays.

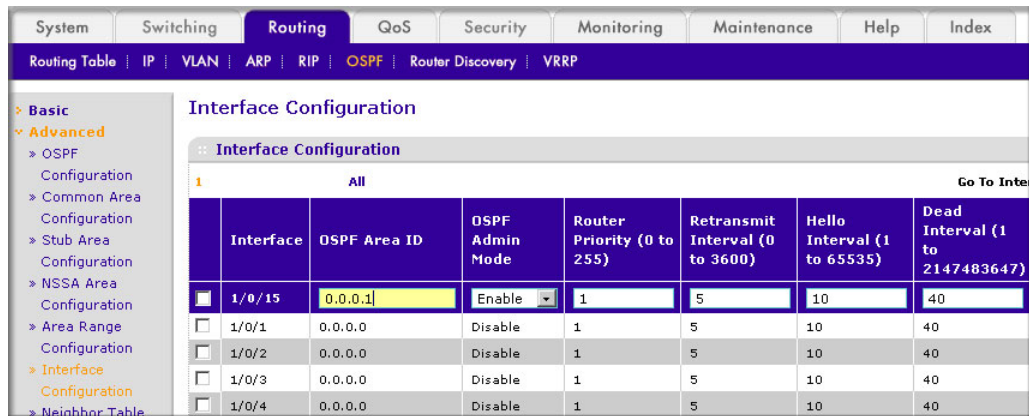
OSPF Configuration

OSPF Admin Mode Disable Enable

Router ID

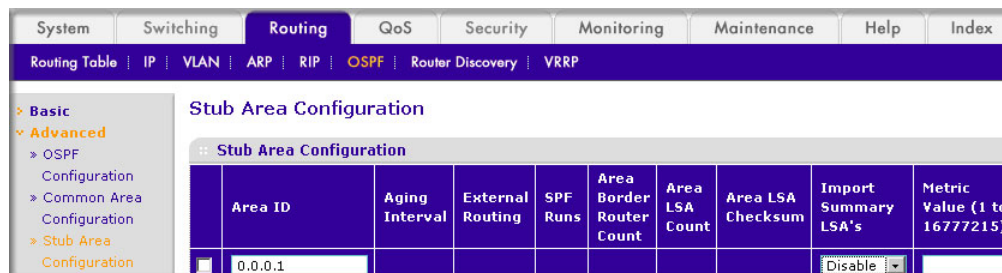
- b. In the **Router ID** field, enter **2.2.2.2**.
- c. Click **Apply** to save the settings.
4. Enable OSPF on port 1/0/15.

- a. Select **Routing > OSPF > Advanced > Interface Configuration**. A screen similar to the following displays.



- b. Under Interface Configuration, scroll down and select the interface **1/0/15** check box. Now 1/0/15 appears in the Interface field at the top.
- In the **OSPF Area ID** field, enter **0.0.0.1**.
 - In the **OSPF Admin Mode** field, select **Enable**.
- c. Click **Apply** to save the settings.
5. Configure area 0.0.0.1 as a stub area.

- a. Select **Routing > OSPF > Advanced > Stub Area Configuration**. A screen similar to the following displays.



- b. In the **Area ID** field, enter **0.0.0.1**.
- c. Click **Add** to save the settings.

nssa Areas

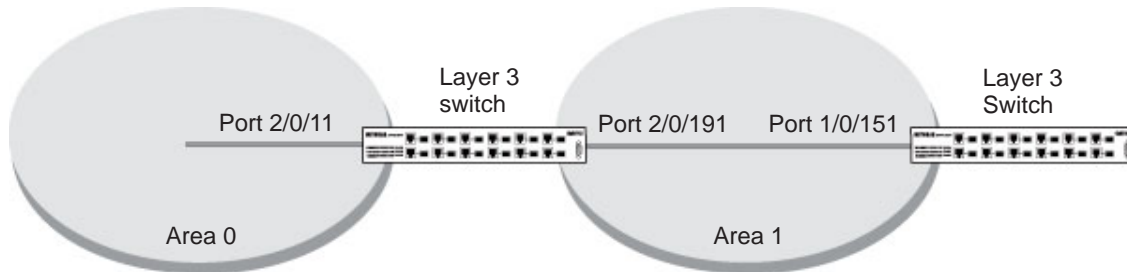


Figure 13. nssa Area

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

CLI: Configure Area 1 as an nssa Area

1. Enable routing on the switch.

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

2. Configure area 0.0.0.1 as an nssa area.

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

3. Stop importing summary LSAs to area 0.0.0.1.

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


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

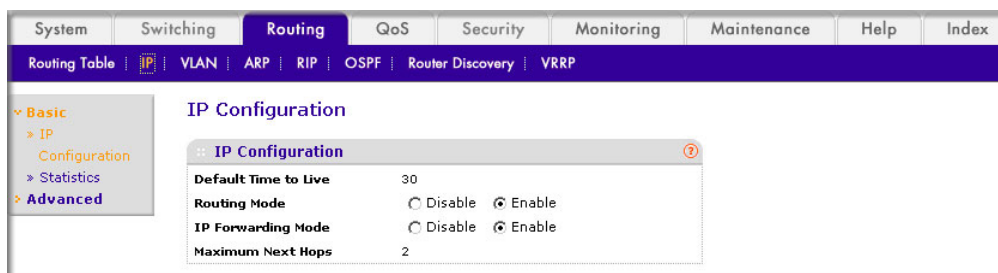
```
(Netgear Switch) (Config-router)#exit
(Netgear Switch) (Config)#interface 2/0/11
(Netgear Switch) (Interface 2/0/11)#routing
(Netgear Switch) (Interface 2/0/11)#ip address 192.168.10.1 255.255.255.0
(Netgear Switch) (Interface 2/0/11)#ip ospf
(Netgear Switch) (Interface 2/0/11)#exit
(Netgear Switch)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

(Netgear Switch) (Interface 2/0/19)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #show ip route
Total Number of Routes..... 2
```

Network Address	Subnet Mask	Protocol	Next Hop Intf	Next Hop IP Address
14.1.1.0	255.255.255.0	OSPF Inter	2/0/11	192.168.10.2
14.1.2.0	255.255.255.0	OSPF Inter	2/0/11	192.168.10.2
192.168.10.0	255.255.255.0	Local	2/0/11	192.168.10.1
192.168.20.0	255.255.255.0	Local	2/0/19	192.168.20.1
192.168.40.0	255.255.255.0	OSPF NSSA T2	2/0/19	192.168.20.2
192.168.41.0	255.255.255.0	OSPF NSSA T2	2/0/19	192.168.20.2
192.168.42.0	255.255.255.0	OSPF NSSA T2	2/0/19	192.168.20.2

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

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.



- b. For Routing Mode, select the **Enable** radio button.
 - c. Click **Apply** to save the settings.

2. Assign IP address 192.168.10.1 to port 2/0/11.
 - a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

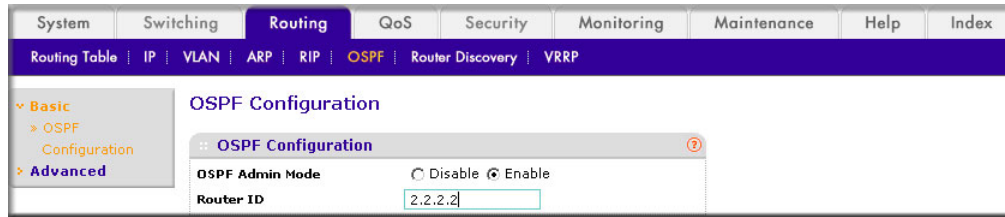
Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/15			192.168.20.2	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 1/0/2			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the interface **2/0/11** check box. Now 2/0/11 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.10.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.
 - In the **Admin Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
3. Assign IP address 192.168.20.1 to port 2/0/19.
 - a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

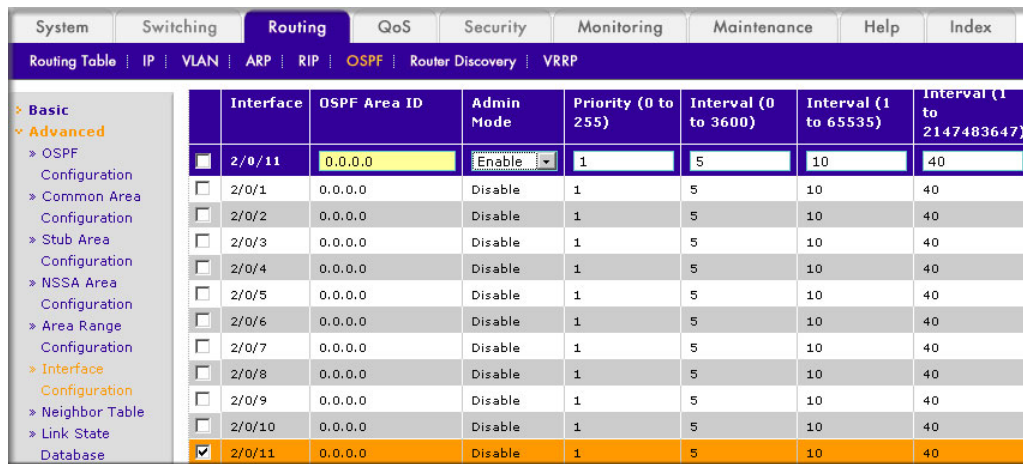
Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 2/0/19			192.168.20.1	255.255.255.0	Enable	Enable
<input type="checkbox"/> 2/0/1			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 2/0/2			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 2/0/3			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the interface **2/0/19** check box. Now 2/0/19 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.20.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Admin Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.

4. Specify the router ID, and enable OSPF for the switch.
 - a. Select **Routing > OSPF > Basic > OSPF Configuration**. A screen similar to the following displays.



- b. Under OSPF Configuration, in the **Router ID** field, enter **2.2.2.2**.
 - c. Click **Apply** to save the settings.
5. Enable OSPF on port 2/0/11.
 - a. Select **Routing > OSPF > Advanced > Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the interface **2/0/11** check box. Now 2/0/11 appears in the Interface field at the top.
 - In the **OSPF Area ID** field, enter **0.0.0.0**.
 - In the **OSPF Admin Mode** field, select **Enable**.
 - c. Click **Apply** to save the settings.
6. Enable OSPF on port 2/0/19.

- a. Select **Routing > OSPF > Advanced > Interface Configuration**. A screen similar to the following displays.

Interface	OSPF Area ID	OSPF Admin Mode	Router Priority (0 to 255)	Retransmit Interval (0 to 3600)	Hello Interval (1 to 65535)	Dead Interval (1 to 2147483647)	Iftransit Delay Interval (1 to 3600)
<input checked="" type="checkbox"/> 2/0/19	0.0.0.1	Enable	1	5	10	40	1
<input type="checkbox"/> 2/0/1	0.0.0.0	Disable	1	5	10	40	1
<input type="checkbox"/> 2/0/2	0.0.0.0	Disable	1	5	10	40	1
<input type="checkbox"/> 2/0/3	0.0.0.0	Disable	1	5	10	40	1

- b. Scroll down and select the interface **2/0/19** check box. 2/0/19 now appears in the Interface field at the top.
- c. Enter the following information:
- In the **OSPF Area ID** field, enter **0.0.0.1**.
 - In the **OSPF Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
7. Configure area 0.0.0.1 as a nssa area.
- a. Select **Routing > OSPF > Advanced > NSSA Area Configuration**. A screen similar to the following displays.

Area ID	Aging Interval	External Routing	SPF Runs	Area Border Router Count	Area LSA Count	Area LSA Checksum	Import Summary LSA's	Metric Value (1 to 16777215)
<input checked="" type="checkbox"/> 0.0.0.1							Disable	

- b. Enter the following information.
- In the **Area ID** field, enter **0.0.0.1**.
 - In the **Import Summary LSA's** field, select **Disable**.
- c. Click **Add** to save the settings.

CLI: Configure Area 1 as an nssa Area on A2

1. Enable routing on the switch.

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

2. Set the router ID to 2.2.2.2.

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

3. Configure the area 0.0.0.1 as an nssa area.

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

4. Redistribute the RIP routes into the OSPF.

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

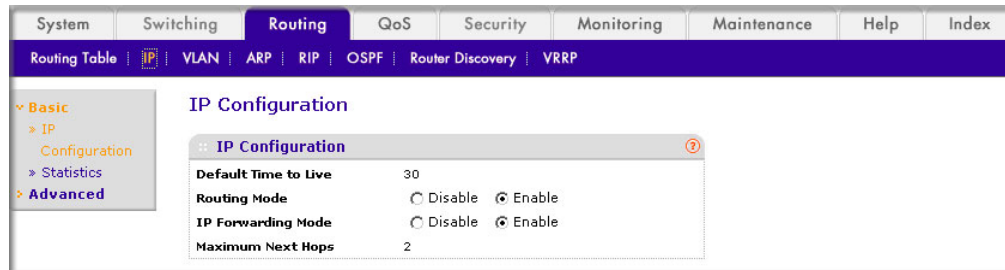
5. Enable OSPF area 0.0.0.1 on port 1/0/15.

```
(Netgear Switch) (Config-router)#exit  
(Netgear Switch) (Config)#interface 1/0/11  
(Netgear Switch) (Interface 1/0/11)#routing  
(Netgear Switch) (Interface 1/0/11)#ip address 192.168.30.1 255.255.255.0  
(Netgear Switch) (Interface 1/0/11)#ip rip  
(Netgear Switch) (Interface 1/0/11)#exit  
(Netgear Switch) (Config)#interface 1/0/15  
(Netgear Switch) (Interface 1/0/15)#routing  
(Netgear Switch) (Interface 1/0/15)#ip address 192.168.20.2 255.255.255.0  
(Netgear Switch) (Interface 1/0/15)#ip ospf  
(Netgear Switch) (Interface 1/0/15)#ip ospf areaid 0.0.0.1  
(Netgear Switch) (Interface 1/0/15)#exit  
(Netgear Switch) (Config)#exit  
(Netgear Switch) #show ip route  
Total Number of Routes..... 6
```

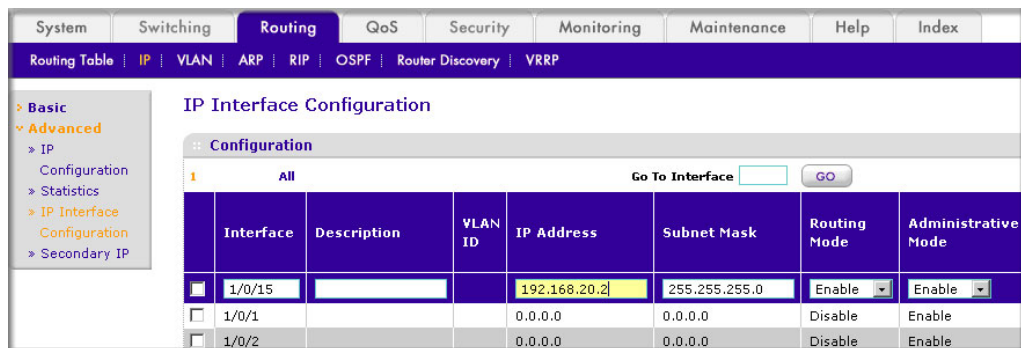
Network Address	Subnet Mask	Protocol	Next Hop Intf	Next Hop IP Address
0.0.0.0	0.0.0.0	OSPF Inter	1/0/15	192.168.20.1
192.168.20.0	255.255.255.0	Local	1/0/15	192.168.20.2
192.168.30.0	255.255.255.0	Local	1/0/11	192.168.30.1
192.168.40.0	255.255.255.0	RIP	1/0/11	192.168.30.2
192.168.41.0	255.255.255.0	RIP	1/0/11	192.168.30.2
192.168.42.0	255.255.255.0	RIP	1/0/11	192.168.30.2

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

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.

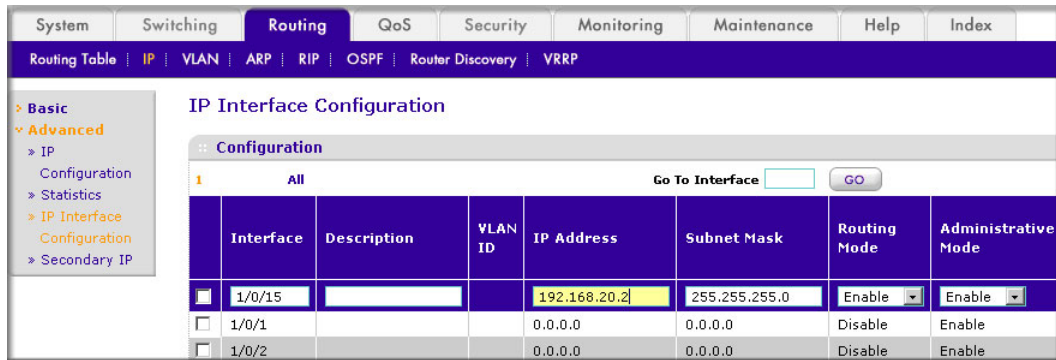


- b. For Routing Mode, select the **Enable** radio button.
 - c. Click **Apply** to save the settings.
2. Assign IP address 192.168.30.1 to port 1/0/11.
 - a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

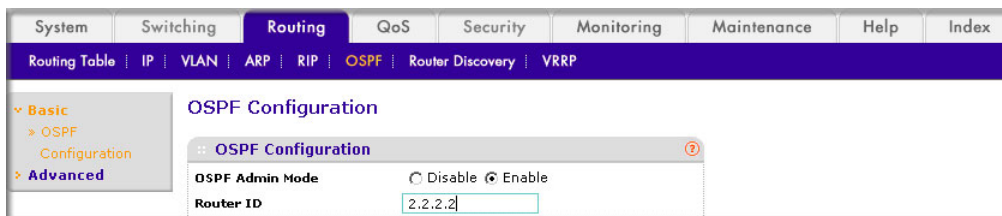


- b. Scroll down and select the interface **1/0/11** check box. Now 1/0/11 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.30.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
3. Assign IP address 192.168.20.2 to port 1/0/15.

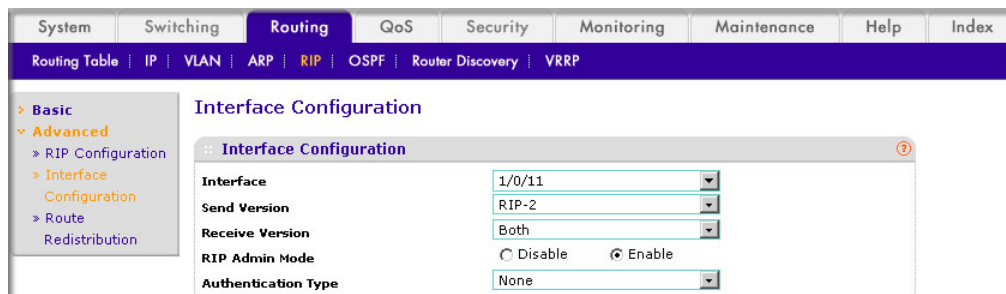
- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Under Configuration, scroll down and select the interface **1/0/15** check box. Now 1/0/15 appears in the Interface field at the top.
- c. Enter the following information:
- In the **IP Address** field, enter **192.168.20.2**.
 - In the **Network Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
4. Specify the router ID, and enable OSPF for the switch.
- a. Select **Routing > OSPF > Basic > OSPF Configuration**. A screen similar to the following displays.



- b. Under OSPF Configuration, in the **Router ID** field, enter **2.2.2.2**.
- c. Click **Apply** to save the settings.
5. Enable RIP on port 1/0/11.
- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.



- b. Enter the following information:
 - In the **Interface** field, select **1/0/11**.
 - For RIP Admin Mode, select the **Enable** radio button.
 - c. Click **Apply** to save the settings.
6. Enable OSPF on port 1/0/15.
- a. Select **Routing > OSPF > Advanced > Interface Configuration**. A screen similar to the following displays.

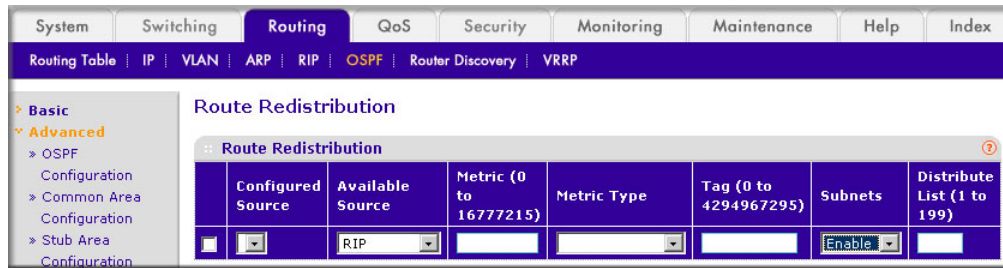
Interface	OSPF Area ID	OSPF Admin Mode	Router Priority (0 to 255)	Retransmit Interval (0 to 3600)	Hello Interval (1 to 65535)	Dead Interval (1 to 2147483647)
<input checked="" type="checkbox"/> 1/0/15	0.0.0.1	Enable	1	5	10	40
<input type="checkbox"/> 1/0/1	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 1/0/2	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 1/0/3	0.0.0.0	Disable	1	5	10	40
<input type="checkbox"/> 1/0/4	0.0.0.0	Disable	1	5	10	40

- b. Scroll down and select the interface **1/0/15** check box. Now 1/0/15 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the **OSPF Area ID** field, enter **0.0.0.1**.
 - In the **OSPF Admin Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
7. Configure area 0.0.0.1 as an nssa area.
- a. Select **Routing > OSPF > Advanced > NSSA Area Configuration**. A screen similar to the following displays.

Area ID	Aging Interval	External Routing	SPF Runs	Area Border Router Count	Area LSA Count	Area LSA Checksum	Import Summary LSA's	Metric Value (1 to 16777215)
<input checked="" type="checkbox"/> 0.0.0.1							Disable	

- b. In the **Area ID** field, enter **0.0.0.1**.
 - c. Click **Add** to save the settings.
8. Redistribute the RIP routes into the OSPF area.

- a. Select **Routing > OSPF > Advanced > Route Redistribution**. A screen similar to the following displays.



- b. Under Route Redistribution, in the **Available Source** list, select **RIP**.
- c. Click **Add** to add a route redistribution.

VLAN Routing OSPF

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

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

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

The 7000 Series Managed Switch operating as a router and running OSPF will determine the best route using the assigned cost and the type of the OSPF route. The order for choosing a route if more than one type of route exists is as follows:

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

CLI: Configure VLAN Routing OSPF

This example adds support for OSPF to the configuration created in the base VLAN routing example in [Figure 8, Layer 3 switch configured for port routing](#) on page 68.

1. Configure the 7000 Series Managed Switch as an inter-area router.

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

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

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

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

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

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

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

Web Interface: Configure VLAN Routing OSPF

1. Configure a VLAN and include ports 1/0/2 in the VLAN.
 - a. Select **Routing > VLAN > VLAN Routing Wizard**. A screen similar to the following displays.

The screenshot shows the 'VLAN Routing Wizard' configuration page. At the top, there are navigation tabs: System, Switching, Routing (selected), QoS, Security, Monitoring, Maintenance, Help, and Index. Below these are sub-tabs: Routing Table, IP, VLAN (selected), ARP, RIP, OSPF, Router Discovery, and VRRP. The main content area is titled 'VLAN Routing Wizard' and contains the following fields and options:

- Vlan ID:** 10
- LAG Enabled:**
- IP Address:** 192.150.3.1
- Network Mask:** 255.255.255.0
- Unit 1:** A table of ports from 1 to 28. Port 2 is selected.

- b. Enter the following information:
 - In the **Vlan ID** field, enter **10**.
 - In the **IP Address** field, enter **192.150.3.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.
- c. Click **Unit 1**. The ports display:

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

- d. Click **Apply** to save the VLAN that includes ports 2.
2. Configure a VLAN, and include port 1/0/3 in the VLAN.
 - a. Select **Routing > VLAN > VLAN Routing Wizard**. A screen similar to the following displays.

The screenshot shows the 'VLAN Routing Wizard' configuration page. The 'Vlan ID' is 20, 'IP Address' is 192.150.4.1, and 'Network Mask' is 255.255.255.0. The 'LAG Enabled' checkbox is unchecked. Under 'Unit 1', a table of ports 1 through 24 is shown. Port 3 has a 'T' in a gray box, indicating it is tagged for egress.

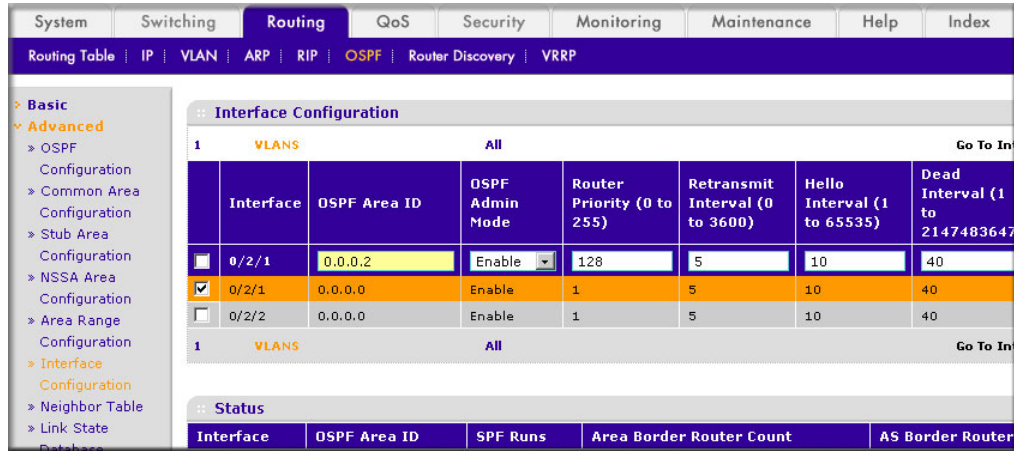
- b. Enter the following information:
 - In the **Vlan ID** field, enter **20**.
 - In the **IP Address** field, enter **192.150.4.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.
 - c. Click **Unit 1**. The ports display:

Click the gray box under port **3** until **T** displays. The T specifies that the egress packet is tagged for the port.
 - d. Click **Apply** to save the VLAN that includes port 3.
3. Enable OSPF on the switch.
 - a. Select **Routing > OSPF > Basic > OSPF Configuration**. A screen similar to the following displays.

The screenshot shows the 'OSPF Configuration' page. The 'OSPF Admin Mode' is set to 'Enable' (radio button selected), and the 'Router ID' is 192.150.9.9.

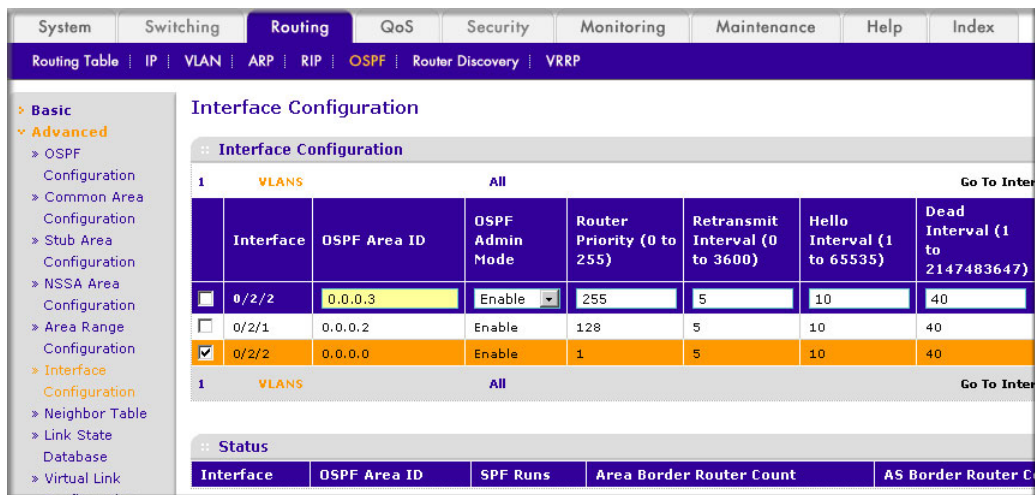
- b. For **OSPF Admin Mode**, select the **Enable** radio button.
 - c. In the **Router ID** field, enter **192.150.9.9**.
 - d. Click **Apply** to save the setting.
4. Enable OSPF on VLAN 10.

- a. Select **Routing > OSPF > Advanced > Interface Configuration**. A screen similar to the following displays.



- b. Under Interface Configuration, click **VLANS** to show all the VLAN interfaces.
- c. Scroll down and select the interface **0/2/1** check box. Now 0/2/1 appears in the Interface field at the top.
- d. Enter the following information:
- In the **OSPF Area ID** field, enter **0.0.0.2**.
 - In the **OSPF Admin Mode** field, select **Enable**.
 - In the **Priority** field, enter **128**.
 - In the **Metric Cost** field, enter **32**.
- e. Click **Apply** to save the settings.
5. Enable OSPF on VLAN 20.

- a. Select **Routing > OSPF > Advanced > Interface Configuration**. A screen similar to the following displays.



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

- c. Scroll down and select the interface **0/2/2** check box. Now 0/2/2 appears in the Interface field at the top.
- d. Enter the following information:
 - In the **OSPF Area ID** field, enter **0.0.0.3**.
 - In the **OSPF Admin Mode** field, select the **Enable**.
 - In the **Priority** field, enter **255**.
 - In the **Metric Cost** field, enter **64**.
- e. Click **Apply** to save the settings.

OSPFv3

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

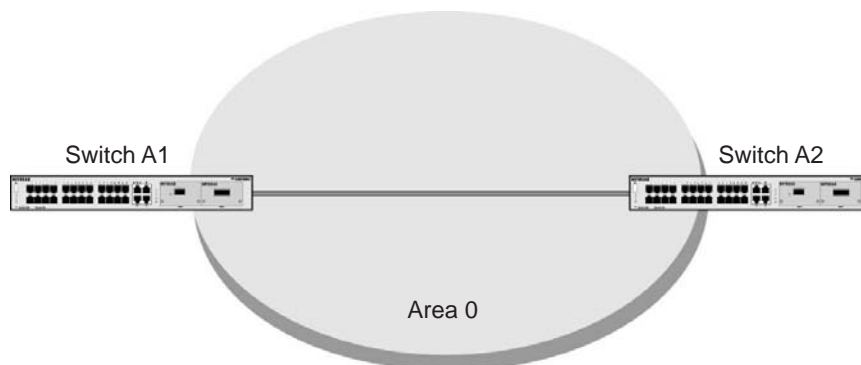


Figure 14. OSPFv3 Protocol for IPv6

CLI: Configure OSPFv3

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

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

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

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

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

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

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

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

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

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

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

6. Enable OSPFv3, and assign 2.2.2.2 as the router ID.

```
(Netgear Switch) (Config)#ipv6 router ospf
(Netgear Switch) (Config-rtr)#enable
(Netgear Switch) (Config-rtr)#router-id 2.2.2.2
(Netgear Switch) (Config-rtr)#exit
```

7. Enable routing mode on interface 1/0/13, and assign the IP address 2000::2 to IPv6.

```
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ipv6 address 2000::2/64
(Netgear Switch) (Interface 1/0/13)#ipv6 enable
```

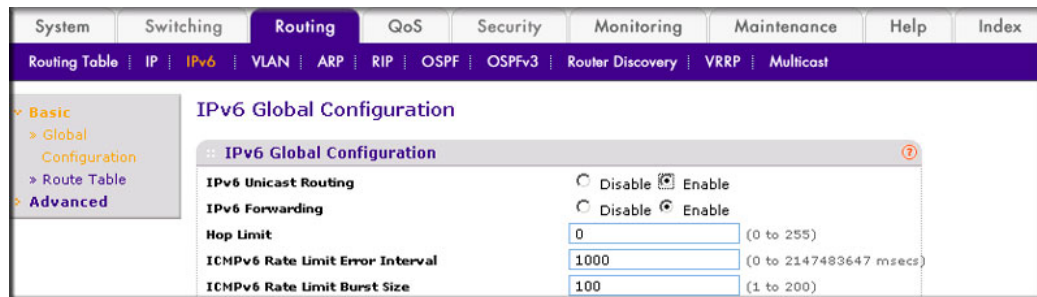
8. Enable OSPFv3 on interface 1/0/13, and set the OSPF network mode to broadcast.

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

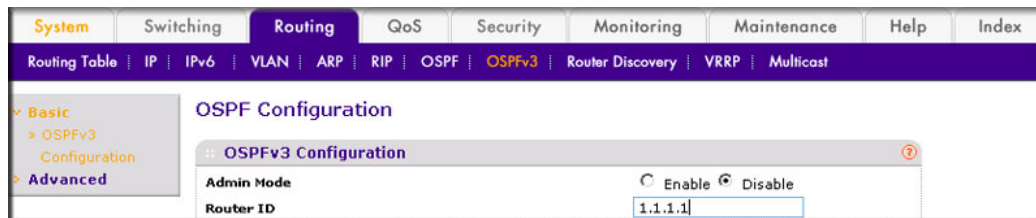
Router ID	Priority	IntfID	Interface	State	DeadTime
1.1.1.1	1	1	1/0/13	Full/ DR	34

Web Interface: Configure OSPFv3

1. Enable IPv6 unicast routing on the switch.
 - a. Select **Routing > IPv6 > Basic > IPv6 Global Configuration**. A screen similar to the following displays.

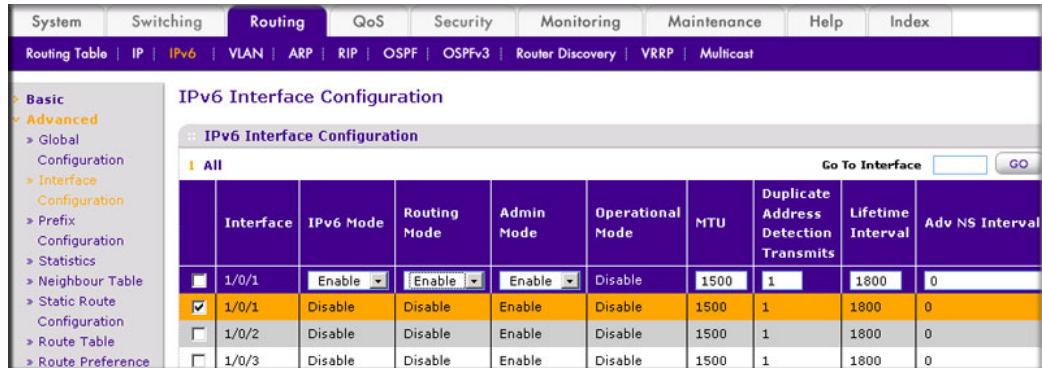


- b. For IPv6 Unicast Routing Mode, select the **Enable** radio button.
 - c. Click **Apply** to save the settings.
2. Specify the router ID, and enable OSPFv3 for the switch.
 - a. Select **Routing > OSPFv3 > Basic > OSPFv3 Configuration**. A screen similar to the following displays.

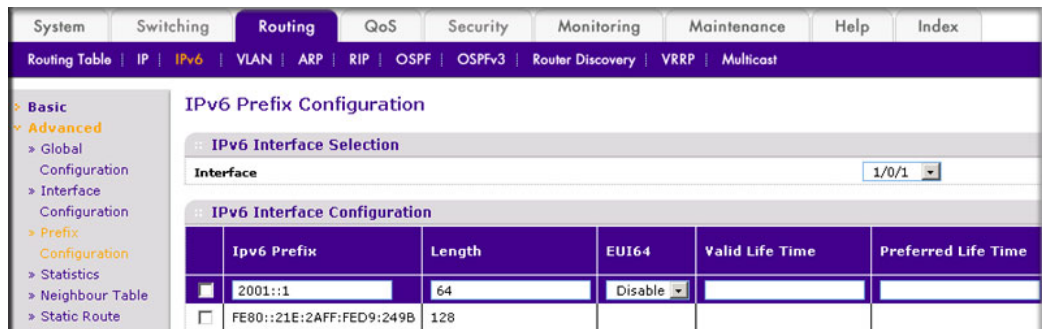


- b. Under the OSPF Configuration, enter the following information:
 - In the **Router ID** field, enter **1.1.1.1**.
 - For Admin Mode, select the **Enable** radio button.
 - c. Click **Apply** to save the settings.
3. Enable IPv6 on port 1/0/1.

- a. Select **Routing > IPv6 > Advanced > IP Interface Configuration**. A screen similar to the following displays.

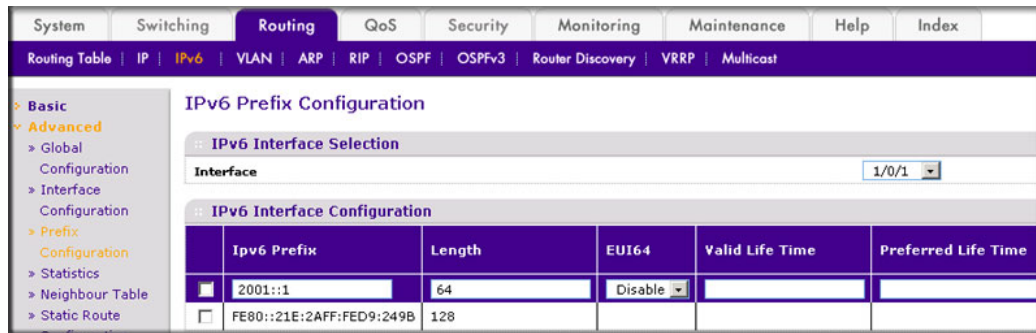


- b. Scroll down and select the interface **1/0/1** check box. Now 1/0/1 appears in the Interface field at the top.
- c. Enter the following information:
- In the **IPv6 Mode** field, select **Enable**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
4. Assign the IP address 2001::1 to port 1/0/1.
- a. Select **Routing > IPv6 > Advanced > IP Interface Configuration**. A screen similar to the following displays.

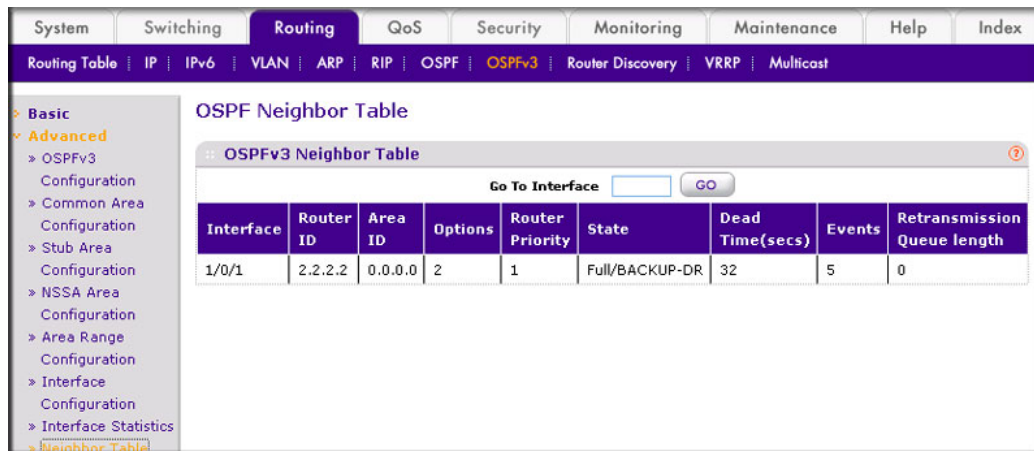


- b. Under IPv6 Prefix Selection, in the **Interface** list, select **1/0/1**.
- c. Under IPv6 Interface Configuration, enter the following information:
- In the **IPv6 Prefix** field, enter **2001::1**.
 - In the **Length** field, enter **64**.
 - In the **EUI64** field, select **Disable**.
 - In the the **Onlink Flag** field, select **Disable**.
 - In the **Autonomous Flag** field, select **Disable**.
- d. Click **Add** to save the settings.
5. Enable OSPFv3 on port 1/0/1.

- a. Select **Routing > OSPFv3 > Advanced > Interface Configuration**. A screen similar to the following displays.



- b. Under IP Interface Configuration, scroll down and select the interface **1/0/1** check box. Now 1/0/1 appears in the Interface field at the top.
 - In the **OSPF Area ID** field, enter **0.0.0.0**.
 - In the **Admin Mode** field, select **Enable**.
 - c. Click **Apply** to save the settings.
6. Display the OSPFv3 Neighbor Table.
 - a. Select **Routing > OSPFv3 > Advanced > Neighbor Table**. A screen similar to the following displays.



To use the Web interface to configure OSPF on switch A2, repeat this process for switch A2.

Proxy Address Resolution Protocol

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

Proxy ARP Examples

The following are examples of the commands used in the proxy ARP feature.

CLI: show ip interface

```
(Netgear Switch) #show ip interface ?

<slot/port>          Enter an interface in slot/port format.
brief                Display summary information about IP configuration
                    settings for all ports.

(Netgear Switch) #show ip interface 0/24

Routing Mode..... Disable
Administrative Mode..... Enable
Forward Net Directed Broadcasts..... Disable
Proxy ARP..... Disable
Active State..... Inactive
Link Speed Data Rate..... Inactive
MAC Address..... 08:00:17:05:05:02
Encapsulation Type..... Ethernet
IP MTU..... 1500
```

CLI: ip proxy-arp

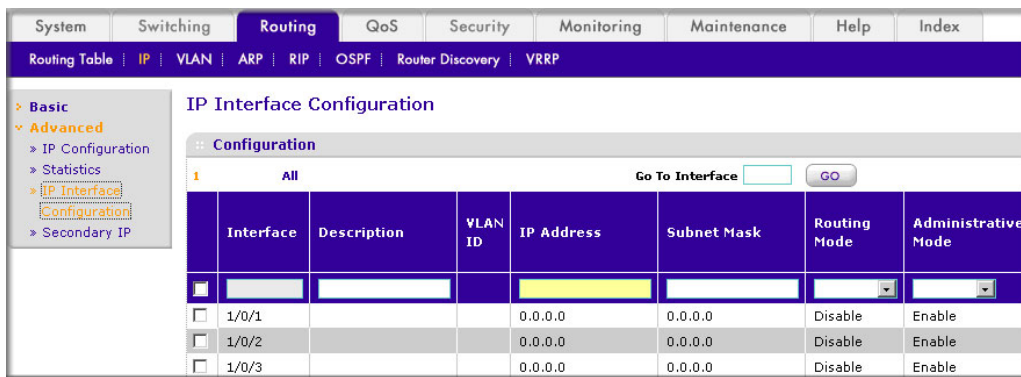
```
(Netgear Switch) (Interface 0/24)#ip proxy-arp ?

<cr>                               Press Enter to execute the command.

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

Web Interface: Configure Proxy ARP on a Port

1. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



2. Under Configuration, scroll down and select the Interface **1/0/3** check box. Now 1/0/3 appears in the Interface field at the top.
3. In the **Proxy Arp** field, select **Enable**.
4. Click **Apply** to save the settings.

Virtual Router Redundancy Protocol

This chapter provides the following examples:

- *VRRP on a Master Router* on page 126
- *VRRP on a Backup Router* on page 128

When an end station is statically configured with the address of the router that will handle its routed traffic, a single point of failure is introduced into the network. If the router goes down, the end station is unable to communicate. Since static configuration is a convenient way to assign router addresses, Virtual Router Redundancy Protocol (VRRP) was developed to provide a backup mechanism.

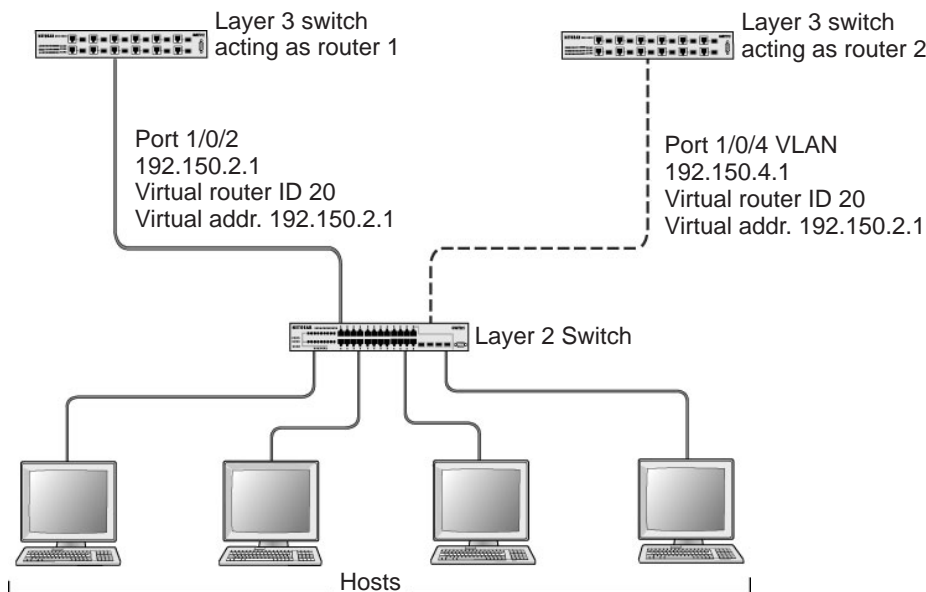


Figure 15. VRRP

VRRP eliminates the single point of failure associated with static default routes by enabling a backup router to take over from a master router without affecting the end stations using the route. The end stations use a virtual IP address that is recognized by the backup router if the master router fails. Participating routers use an election protocol to determine which router is the master router at any given time. A given port could appear as more than one virtual router to the network. Also, more than one port on a 7000 Series Managed Switch can be configured as a virtual router. Either a physical port or a routed VLAN can participate.

VRRP on a Master Router

This example shows how to configure the 7000 Series Managed Switch to support VRRP. Router 1 is the default master router for the virtual route, and Router 2 is the backup router.

CLI: Configure VRRP on a Master Router

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

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

2. Configure the IP addresses and subnet masks for the port that will participate in the protocol.

```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.0.0
(Netgear Switch) (Interface 1/0/2)#exit
```

3. Enable VRRP for the switch.

```
(Netgear Switch) (Config)#ip vrrp
```

4. Assign virtual router IDs to port that will participate in the protocol.

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

5. Specify the IP address that the virtual router function will recognize. Note that the virtual IP address on port 1/0/2 is the same as the port's actual IP address therefore, this router will always be the VRRP master when it is active. The default priority is 255.

```
(Netgear Switch) (Interface 1/0/2)#ip vrrp 20 ip 192.150.2.1
```

6. Enable VRRP on the port.

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

Web Interface: Configure VRRP on a Master Router

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.

The screenshot shows the 'IP Configuration' page in the web interface. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. Under 'Routing', there are links for Routing Table, IP, VLAN, ARP, RIP, OSPF, Router Discovery, and VRRP. The left sidebar shows a tree view with 'Basic' expanded to 'IP', then 'Configuration', 'Statistics', and 'Advanced'. The main content area is titled 'IP Configuration' and contains the following settings:

Default Time to Live	30
Routing Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IP Forwarding Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Maximum Next Hops	2

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

The screenshot shows the 'IP Interface Configuration' page in the web interface. The navigation menu is the same as in the previous screenshot. The left sidebar shows a tree view with 'Basic' expanded to 'Advanced', then 'IP Configuration', 'Statistics', 'IP Interface Configuration', and 'Secondary IP'. The main content area is titled 'IP Interface Configuration' and displays a table of interfaces. The table has columns for Interface, Description, VLAN ID, IP Address, Subnet Mask, Routing Mode, and Administrative Mode. The interface 1/0/2 is selected, and its IP Address is 192.150.2.1 and Subnet Mask is 255.255.0.0.

Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/2			192.150.2.1	255.255.0.0	Enable	Enable
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 1/0/3			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 1/0/4			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the Interface **1/0/2** check box. Now 1/0/2 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.150.2.1**.
 - In the **Network Mask** field, enter **255.255.0.0**.
 - In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
3. Enable VRRP on port 1/0/2.

- a. Select **Routing > VRRP > Advanced > VRRP Configuration**. A screen similar to the following displays.

VRID	Interface	Interface IP Address	Primary IP Address	Mode	State
20	1/0/2		192.150.2.1	Active	

- b. Under Global Configuration, next to the Admin Mode, select **Enable** radio button.
- c. Enter the following information in the VRRP Configuration:
- In the **VRID (1 to 255)** field, enter **20**.
 - In the **Interface** field, select **1/0/2**.
 - In the **Primary IP Address** field, enter **192.150.2.1**.
 - In the **Mode** field, select **Active**.
- d. Click **Apply** to save the settings.

VRRP on a Backup Router

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

CLI: Configure VRRP on a Backup Router

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

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

2. Configure the IP addresses and subnet masks for the port that will participate in the protocol.

```
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#routing
(Netgear Switch) (Interface 1/0/4)#ip address 192.150.4.1 255.255.0.0
(Netgear Switch) (Interface 1/0/4)#exit
```


3. Enable VRRP for the switch.

```
(Netgear Switch) (Config)#ip vrrp
```

4. Assign virtual router IDs to port that will participate in the protocol.

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

5. Specify the IP address that the virtual router function will recognize. Since the virtual IP address on port 1/0/4 is the same as Router 1's port 1/0/2 actual IP address, this router will always be the VRRP backup when Router 1 is active.

```
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20 ip 192.150.2.1
```

6. Set the priority for the port. The default priority is 100.

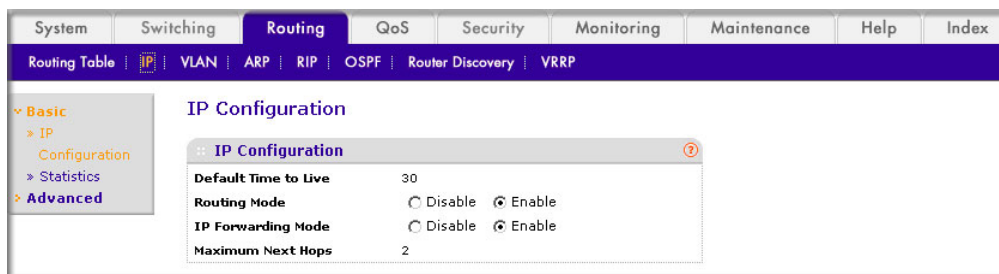
```
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20 priority 254
```

7. Enable VRRP on the port.

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

Web Interface: Configure VRRP on a Backup Router

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > IP Configuration**. A screen similar to the following displays.



- b. For Routing Mode, select the **Enable** radio button.
 - c. Click **Apply** to save the settings.
2. Assign IP address 192.150.4.1 to port 1/0/4.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/4			192.150.4.1	255.255.0.0	Enable	Enable
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 1/0/2			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 1/0/3			0.0.0.0	0.0.0.0	Disable	Enable
<input checked="" type="checkbox"/> 1/0/4			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 1/0/5			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/> 1/0/6			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the Interface **1/0/4** check box. Now 1/0/4 appears in the Interface field at the top.
- c. Enter the following information:
- In the **IP Address** field, enter **192.150.4.1**.
 - In the **Network Mask** field, enter **255.255.0.0**.
 - In the **Administrative Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
3. Enable VRRP on port 1/0/4.
- a. Select **Routing > VRRP > Basic > VRRP Configuration**. A screen similar to the following displays.

VRID (1 to 255)	Interface	Pre-empt Mode	Priority (1 to 255)	Advertisement Interval (secs) (1 to 255)	Interface IP Address	Owner
<input checked="" type="checkbox"/> 20	1/0/4	Disable	254	1		

- b. Under Global Configuration, for Admin Mode, select the **Enable** radio button.
- c. Enter the following information:
- In the **VRID (1 to 255)** field, enter **20**.
 - In the **Interface** field, select **1/0/4**.
 - In the **Priority (1 to 255)**, enter **254**.
 - In the **Primary IP Address** field, enter **192.150.2.1**.
 - In the **Status** list, select **Active**.
- d. Click **Add** to save the settings.

Access Control Lists

This chapter describes the Access Control Lists (ACLs) feature. The following examples are provided:

- *MAC ACLs* on page 132
- *Set Up an IP ACL with Two Rules* on page 133
- *One-Way Access Using a TCP Flag in an ACL* on page 137
- *Use ACLs to Configure Isolated VLANs on a Layer 3 Switch* on page 152
- *Set up a MAC ACL with Two Rules* on page 164
- *ACL Mirroring* on page 167
- *ACL Redirect* on page 172
- *Configure IPv6 ACLs* on page 177

Access control lists (ACLs) can control the traffic entering a network. Normally ACLs reside in a firewall router or in a router connecting two internal networks. When you configure ACLs, you can selectively admit or reject inbound traffic, thereby controlling access to your network or to specific resources on your network.

You can set up ACLs to control traffic at Layer 2-, or Layer 3. MAC ACLs are used for Layer 2. IP ACLs are used for Layer 3. Each ACL contains a set of rules that apply to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and may apply to one or more of the fields within a packet.

The following limitations apply to ACLs. These limitations are platform dependent.

- The maximum of number of ACLs is 100.
- The maximum number of rules per ACL is 8–10.
- Stacking systems do not support redirection.
- The system does not support MAC ACLs and IP ACLs on the same interface.
- The system supports ACLs set up for inbound traffic only.

MAC ACLs

MAC ACLs are Layer 2 ACLs. You can configure the rules to inspect the following fields of a packet (limited by platform):

- Source MAC address with mask.
- Destination MAC address with mask.
- VLAN ID (or range of IDs).
- Class of Service (CoS) (802.1p) .
- EtherType:
 - Secondary CoS (802.1p).
 - Secondary VLAN (or range of IDs).
- L2 ACLs can apply to one or more interfaces.
- Multiple access lists can be applied to a single interface: the sequence number determines the order of execution.
- You cannot configure a MAC ACL and an IP ACL on the same interface.
- You can assign packets to queues using the assign queue option.
- You can redirect packets using the redirect option.

IP ACLs

IP ACLs classify for Layer 3. Each ACL is a set of up to 10 rules applied to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and can apply to one or more of the following fields within a packet:

- Source IP address
- Destination IP address
- Source Layer 4 port
- Destination Layer 4 port
- ToS byte
- Protocol number

Note that the order of the rules is important: When a packet matches multiple rules, the first rule takes precedence. Also, once you define an ACL for a given port, all traffic not specifically permitted by the ACL is denied access.

ACL Configuration

To configure ACLs:

1. Create an ACL by specifying a name (MAC ACL) or a number (IP ACL).
2. Add new rules to the ACL.
3. Configure the match criteria for the rules.

4. Apply the ACL to one or more interfaces.

Set Up an IP ACL with Two Rules

This section shows you how to set up an IP ACL with two rules, one applicable to TCP traffic and one to UDP traffic. The content of the two rules is the same. TCP and UDP packets will be accepted by the 7000 Series Managed Switch only if the source and destination stations have IP addresses within the defined sets.

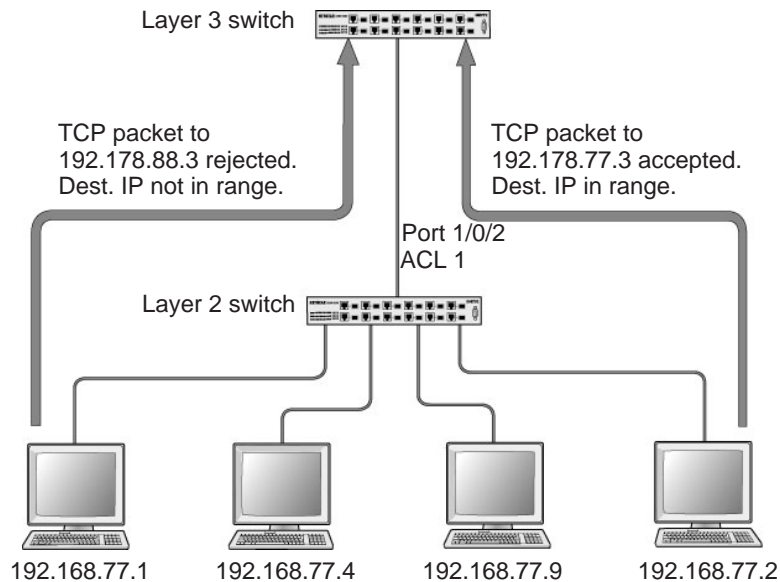


Figure 16. IP ACL with rules for TCP traffic and UDP traffic

CLI: Set Up an IP ACL with Two Rules

The following is an example of configuring ACL support on a 7000 Series Managed Switch.

Create ACL 101. Define the first rule: The ACL will permit packets that match the specified source IP address (after the mask has been applied), that are carrying TCP traffic, and that are sent to the specified destination IP address.

1. Enter these commands:

```
(Netgear Switch) #config
(Netgear Switch) (Config)#access-list 101 permit tcp 192.168.77.0 0.0.0.255
192.178.77.0 0.0.0.255
```

- Define the second rule for ACL 101 to set conditions for UDP traffic similar to those for TCP traffic.

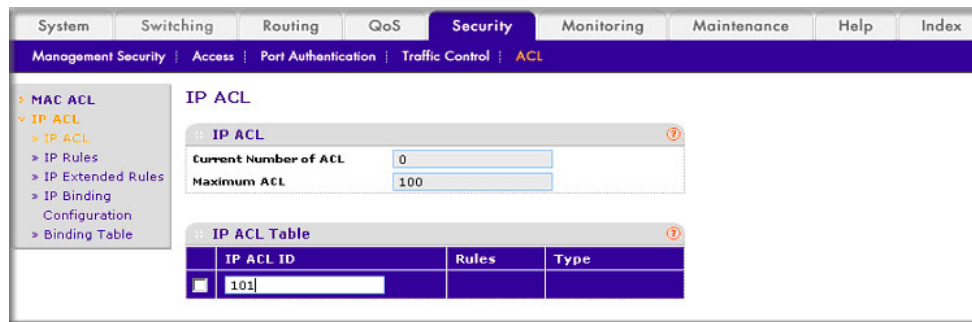
```
(Netgear Switch) (Config)#access-list 101 permit udp 192.168.77.0 0.0.0.255
192.178.77.0 0.0.0.255
```

- Apply the rule to inbound traffic on port 1/0/2. Only traffic matching the criteria will be accepted.

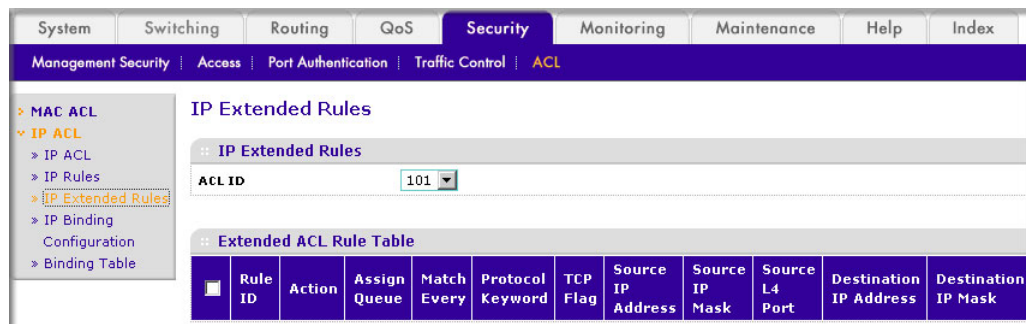
```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip access-group 101 in
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Set Up an IP ACL with Two Rules

- Create IP ACL 101 on the switch.
 - Select **Security > ACL > IP ACL**. A screen similar to the following displays.



- In the **IP ACL ID** field, enter **101**.
 - Click **Add** to create ACL 101.
- Create a new rule associated with ACL 101.
 - Select **Security > ACL > IP ACL > IP Extended Rules**. A screen similar to the following displays.



- For ACL ID, select **101**.

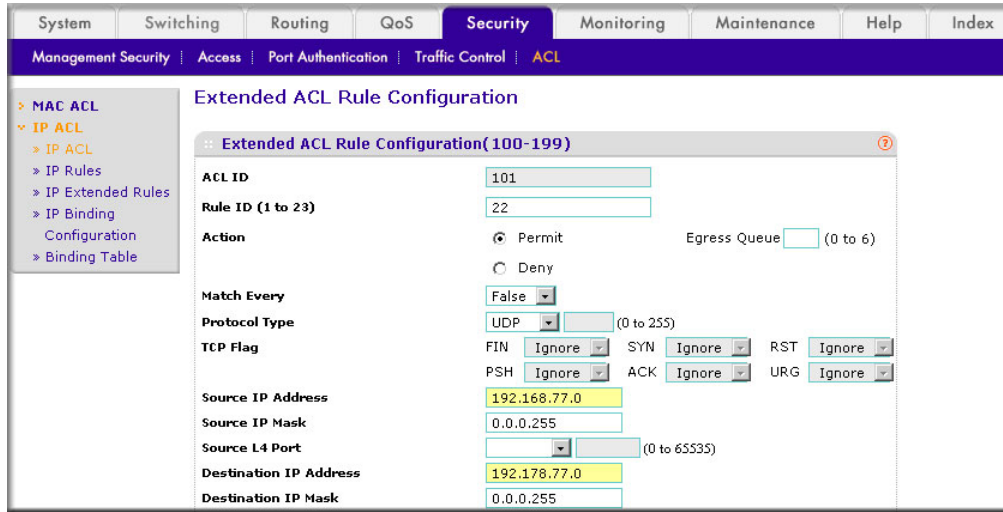
- c. Click **Add** to create a new rule.
3. Create a new ACL rule and add it to ACL 101.
 - a. After you click the Add button in step 2, A screen similar to the following displays.

The screenshot displays the 'Extended ACL Rule Configuration(100-199)' window. The left sidebar shows a navigation tree with 'IP ACL' expanded to 'IP Extended Rules'. The main configuration area includes the following fields and options:

- ACL ID:** 101
- Rule ID (1 to 23):** 1
- Action:** Permit, Deny. Egress Queue: (0 to 6)
- Match Every:** False
- Protocol Type:** TCP (0 to 255)
- TCP Flag:** FIN Ignore, SYN Ignore, RST Ignore, PSH Ignore, ACK Ignore, URG Ignore
- Source IP Address:** 192.168.77.0
- Source IP Mask:** 0.0.0.255
- Source L4 Port:** (0 to 65535)
- Destination IP Address:** 192.178.77.0
- Destination IP Mask:** 0.0.0.255
- Destination L4 Port:** (0 to 65535)
- Service Type:** IP DSCP (0 to 63)

- a. In the Extended ACL Rule Configuration, enter the following information:
 - In the **Rule ID (1 to 23)** field, enter **1**.
 - For Action, select the **Permit** radio button.
 - In the **Protocol Type** list, select **TCP**.
 - In the **Source IP Address** field, enter **192.168.77.0**.
 - In the **Source IP Mask** field, enter **0.0.0.255**.
 - In the **Destination IP Address** field, enter **192.178.77.0**.
 - In the **Destination IP Mask** field, enter **0.0.0.255**.
- b. Click **Apply** to save the settings.
4. Create another ACL rule and add it to the ACL 101.

a. After you click the Add button in step 3, a screen similar to the following displays.



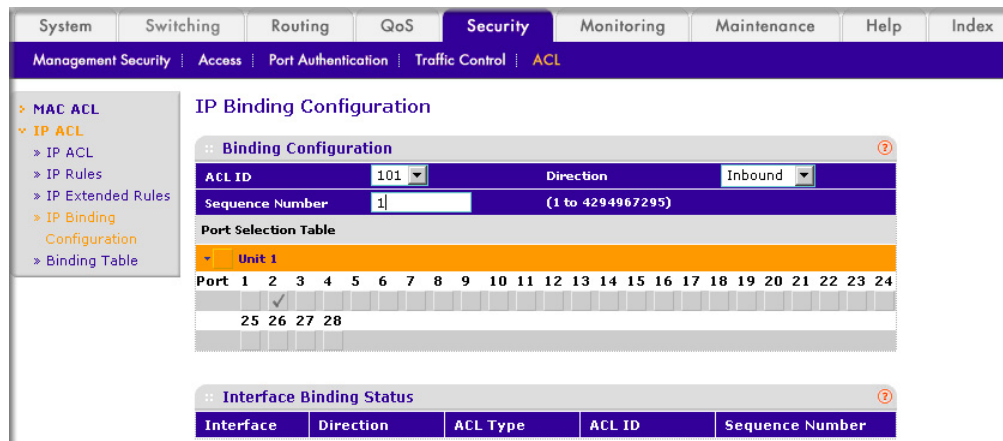
b. Under Extended ACL Rule Configuration, enter the following information:

- In the **Rule ID (1 to 23)** field, enter **22**.
- For Action, select the **Permit** radio button.
- In the **Protocol Type** list, select **UDP**.
- In the **Source IP Address** field, enter **192.168.77.0**.
- In the **Source IP Mask** field, enter **0.0.0.255**.
- In the **Destination IP Address** field, enter **192.178.77.0**.
- In the **Destination IP Mask** field, enter **0.0.0.255**.

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

5. Apply ACL 101 to port 2.

a. Select **Security > ACL > IP ACL > IP Binding Configuration**. A screen similar to the following displays.



b. Under IP Binding Configuration, enter the following information:

- In the **ACL ID** list, select **10**.
 - In the **Sequence Number** field, enter **1**.
- c. Click **Unit 1**. The ports display.
- d. Click the gray box under port **2**. A check mark displays in the box.
- e. Click **Apply** to save the settings.

One-Way Access Using a TCP Flag in an ACL

This example shows how to set up one-way Web access using a TCP flag in an ACL. PC 1 can access FTP server 1 and FTP server 2, but PC 2 can access only FTP server 2.

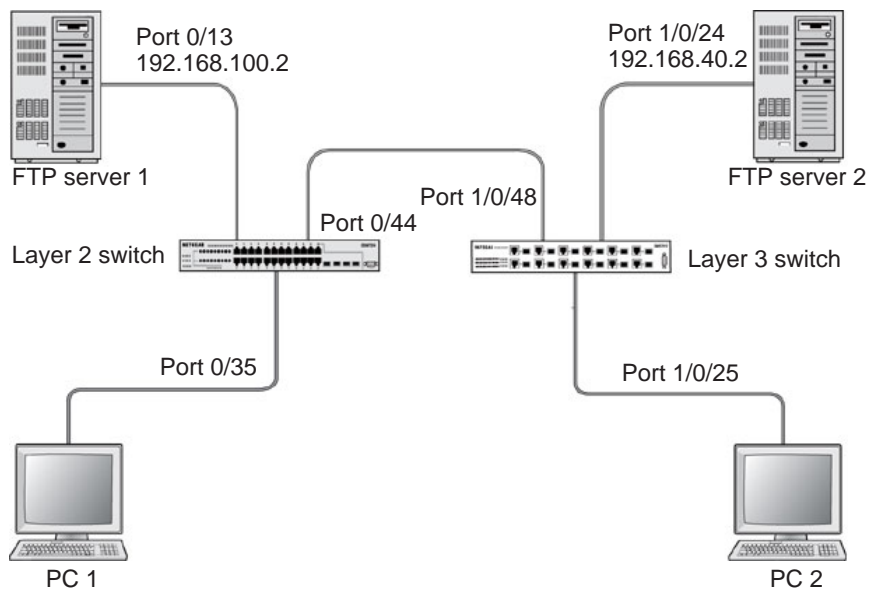


Figure 17. One-Way Web access using a TCP flag in an ACL

CLI:Configure One-Way Access Using a TCP Flag in an ACL

This is a two-step process:

- *Step 1: Configure the Switch* on page 137
- *Step 2: Configure the GSM7352S* on page 139

Step 1: Configure the Switch

(See *Figure 17, One-Way Web access using a TCP flag in an ACL.*)

1. Create VLAN 30 with port 0/35 and assign IP address 192.168.30.1/24.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 30
(Netgear Switch) (Vlan)#vlan routing 30
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 0/35
(Netgear Switch) (Interface 0/35)#vlan pvid 30
(Netgear Switch) (Interface 0/35)#vlan participation include 30
(Netgear Switch) (Interface 0/35)#exit
(Netgear Switch) (Config)#interface vlan 30
(Netgear Switch) (Interface-vlan 30)#routing
(Netgear Switch) (Interface-vlan 30)#ip address 192.168.30.1 255.255.255.0
(Netgear Switch) (Interface-vlan 30)#exit
(Netgear Switch) (Config)#exit
```

2. Create VLAN 100 with port 0/13 and assign IP address 192.168.100.1/24.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 100
(Netgear Switch) (Vlan)#vlan routing 100
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 0/13
(Netgear Switch) (Interface 0/13)#vlan pvid 100
(Netgear Switch) (Interface 0/13)#vlan participation include 100
(Netgear Switch) (Interface 0/13)#exit
(Netgear Switch) (Config)#interface vlan 100
(Netgear Switch) (Interface-vlan 100)#routing
(Netgear Switch) (Interface-vlan 100)#ip address 192.168.100.1 255.255.255.0
(Netgear Switch) (Interface-vlan 100)#exit
(Netgear Switch) (Config)#exit
```

3. Create VLAN 200 with port 0/44 and assign IP address 192.168.200.1/24.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#vlan routing 200
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 0/44
(Netgear Switch) (Interface 0/44)#vlan pvid 200
(Netgear Switch) (Interface 0/44)#vlan participation include 200
(Netgear Switch) (Interface 0/44)#exit
(Netgear Switch) (Config)#interface vlan 200
(Netgear Switch) (Interface-vlan 200)#routing
(Netgear Switch) (Interface-vlan 200)#ip address 192.168.200.1 255.255.255.0
(Netgear Switch) (Interface-vlan 200)#exit
```

4. Add two static routes so that the switch forwards the packets for which the destinations are 192.168.40.0/24 and 192.168.50.0/24 to the correct next hops.

```
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip route 192.168.40.0 255.255.255.0 192.168.200.2
(Netgear Switch) (Config)#ip route 192.168.50.0 255.255.255.0 192.168.200.2
```

5. Create an ACL that denies all the packets with TCP flags +syn-ack.

```
(Netgear Switch) (Config)#access-list 101 deny tcp any flag +syn -ack
```

6. Create an ACL that permits all the IP packets.

```
(Netgear Switch) (Config)#access-list 102 permit ip any
```

7. Apply ACLs 101 and 102 to port 0/44; the sequence of 101 is 1 and of 102 is 2.

Step 2: Configure the GSM7352S

(See [Figure 17, One-Way Web access using a TCP flag in an ACL](#) on page 137.)

1. Enter the following commands.

```
(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
```

2. 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
```

3. Create VLAN 50 with port 1/0/25 and assign IP address 192.168.50.1/24.

```
(Netgear Switch) (Config)#exit
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 50
(Netgear Switch) (Vlan)#vlan routing 50
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/25
(Netgear Switch) (Interface 1/0/25)#vlan pvid 50
(Netgear Switch) (Interface 1/0/25)#vlan participation include 50
(Netgear Switch) (Interface 1/0/25)#exit
(Netgear Switch) (Config)#interface vlan 50
(Netgear Switch) (Interface-vlan 50)#routing
(Netgear Switch) (Interface-vlan 50)#ip address 192.168.50.1 255.255.255.0
(Netgear Switch) (Interface-vlan 50)#exit
(Netgear Switch) (Config)#exit
```

4. 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
```

5. Add two static routes so that the switch forwards the packets with destinations 192.168.100.0/24 and 192.168.30.0/24 to the correct next hops.

```
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip route 192.168.100.0 255.255.255.0 192.168.200.1
(Netgear Switch) (Config)#ip route 192.168.30.0 255.255.255.0 192.168.200.1
```

Web Interface: Configure One-Way Access Using a TCP Flag in an ACL

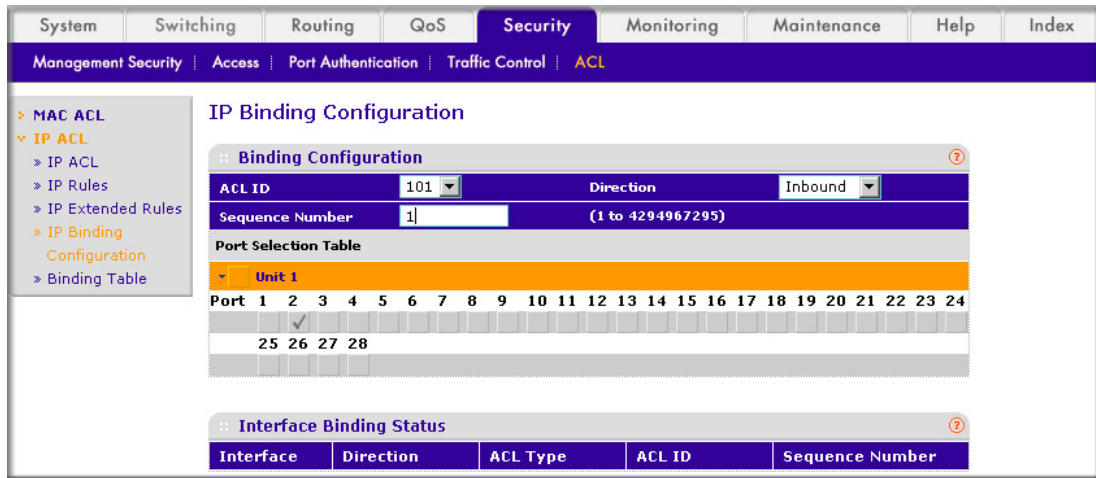
This is a two-part process:

- [Configuring the Switch](#) on page 141
- [Configuring the GSM7342S Switch](#) on page 149

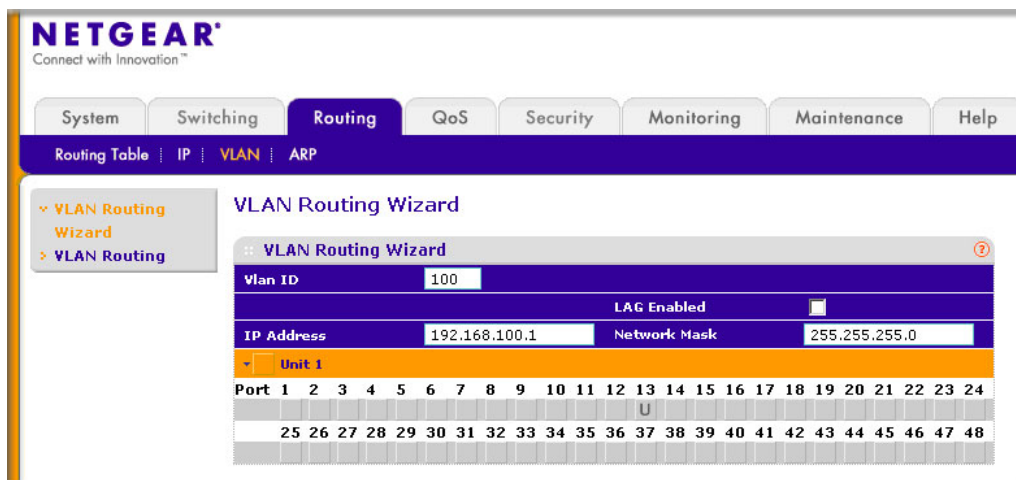
Configuring the Switch

1. Create VLAN 30 with IP address 192.168.30.1/24.

- a. Select **Routing > VLAN > VLAN Routing Wizard**. A screen similar to the following displays.

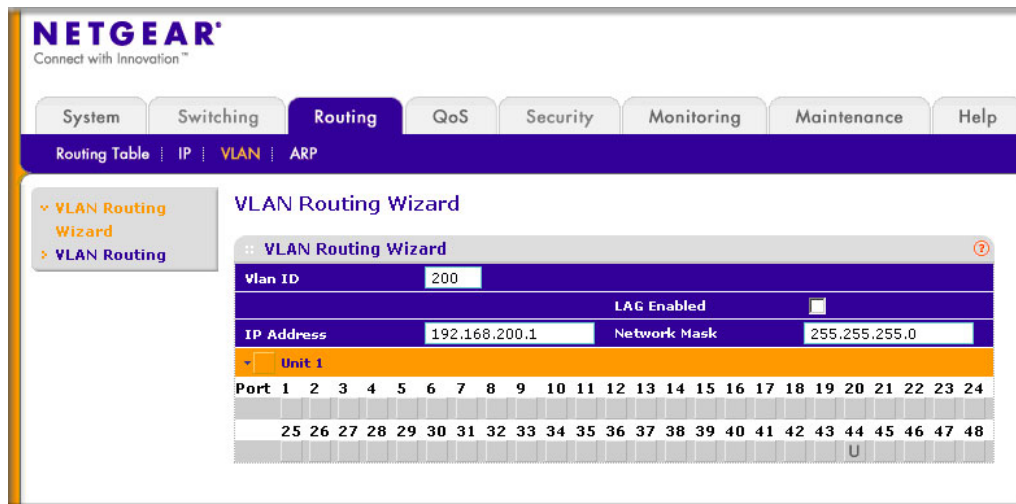


- b. In the VLAN Routing Wizard, enter the following information:
- In the **Vlan ID** field, enter **30**.
 - In the **IP Address** field, enter **192.168.30.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.
- c. Click **Unit 1**. The ports display.
- d. Click the gray box under port **35** twice until **U** displays. The U specifies that the egress packet is untagged for the port.
- e. Click **Apply** to save VLAN 30.
2. Create VLAN 100 with IP address 192.168.100.1/24.
- a. Select **Routing > VLAN > VLAN Routing Wizard**. A screen similar to the following displays.



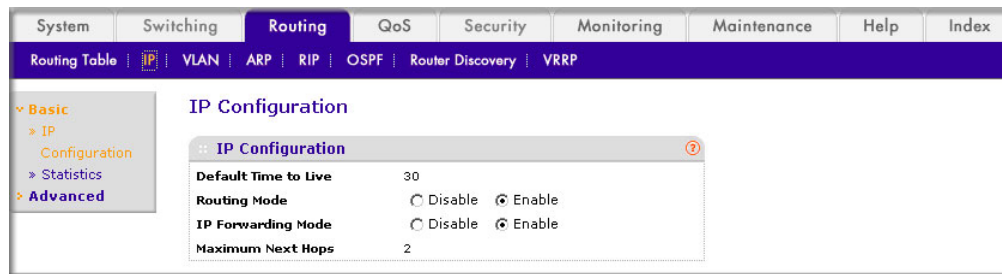
- b. Enter the following information:
- In the **Vlan ID** field, enter **100**.

- In the **IP Address** field, enter **192.168.100.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.
- c. Click **Unit 1**. The ports display.
 - d. Click the gray box under port **13** twice until **U** displays. The U specifies that the egress packet is untagged for the port.
 - e. Click **Apply** to save VLAN 100.
3. Create VLAN 200 with IP address 192.168.200.1/24.
 - a. Select **Routing > VLAN > VLAN Routing Wizard**. A screen similar to the following displays.

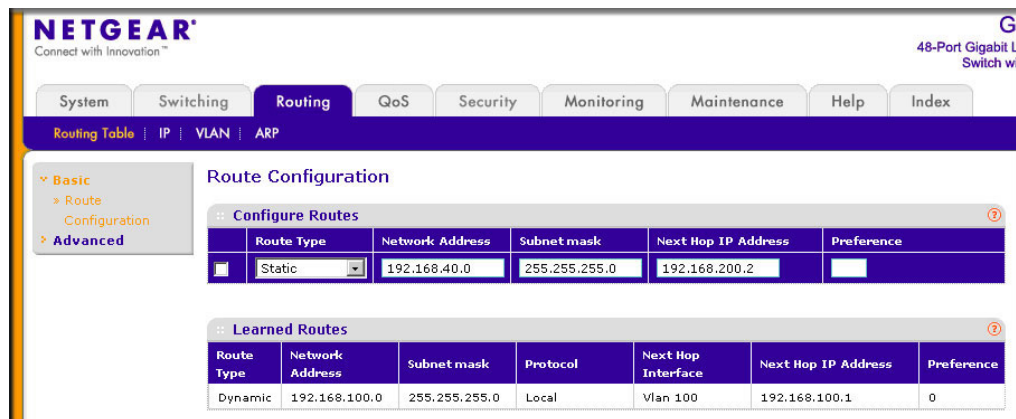


- b. Enter the following information:
 - In the **Vlan ID** field, enter **200**.
 - In the **IP Address** field, enter **192.168.200.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.
 - c. Click **Unit 1**. The ports display.
 - d. Click the gray box under port **44** twice until **U** displays. The U specifies that the egress packet is untagged for the port.
 - e. Click **Apply** to save VLAN 200.
4. Enable IP routing.

- a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.

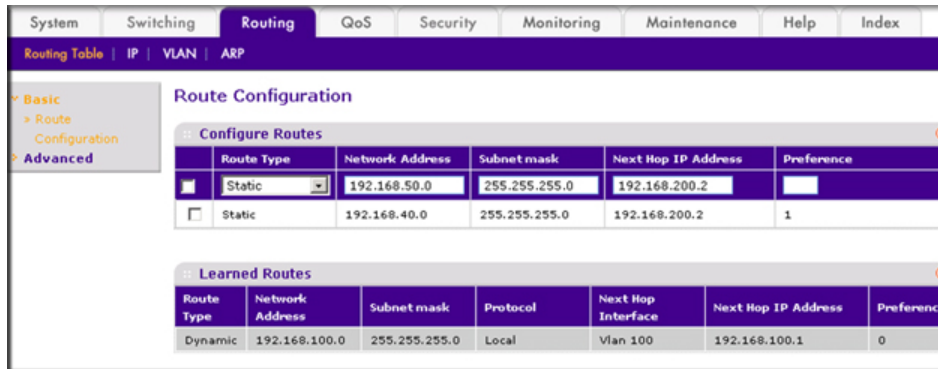


- b. Under IP Configuration, make the following selections:
- For Routing Mode, select the **Enable** radio button.
 - For IP Forwarding Mode, select the **Enable** radio button.
- c. Click **Apply** to enable IP routing.
5. Add a static route with IP address 192.268.40.0/24:
- a. Select **Routing > Routing Table > Basic > Route Configuration**. A screen similar to the following displays.



- b. Under Configure Routes, make the following selection and enter the following information:
- In the Route Type list, select **Static**.
 - In the **Network Address** field, enter **192.168.40.0**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Next Hop IP Address** field, enter **192.168.200.2**.
- c. Click **Add**.
6. Create a static route with IP address 192.168.50.0/24:

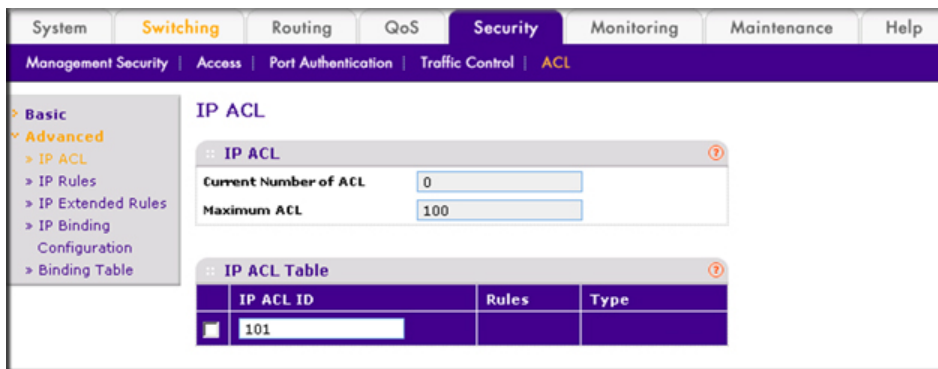
- a. Select **Routing > Routing Table > Basic > Route Configuration**. A screen similar to the following displays.



- b. Under Configure Routes, make the following selection and enter the following information:
- In the **Route Type** list, select **Static**.
 - In the **Network Address** field, enter **192.168.50.0**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Next Hop IP Address** field, enter **192.168.200.2**.
- c. Click **Add**.

7. Create an ACL with ID 101.

- a. Select **Security > ACL > Advanced > IP ACL**. A screen similar to the following displays.

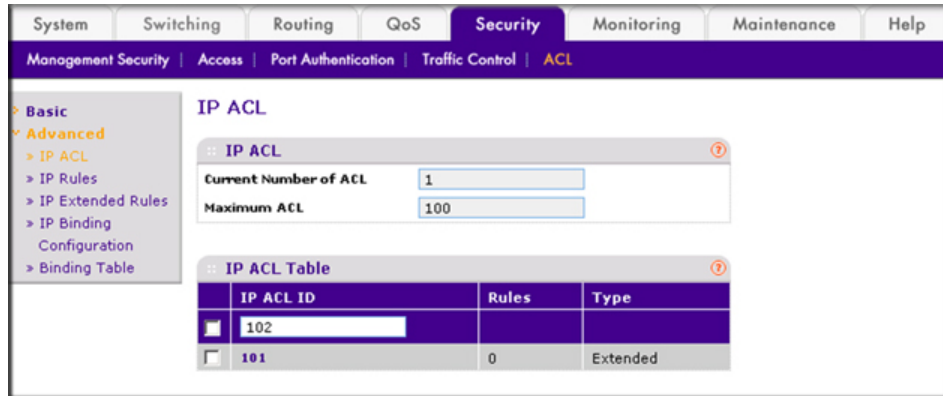


- b. In the IP ACL Table, in the **IP ACL ID** field, enter **101**.

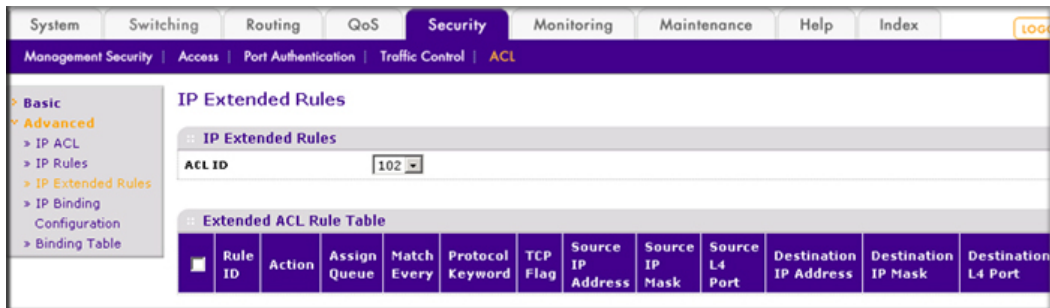
- c. Click **Add**.

8. Create an ACL with ID 102.

- a. Select **Security > ACL > Advanced > IP ACL**. A screen similar to the following displays.

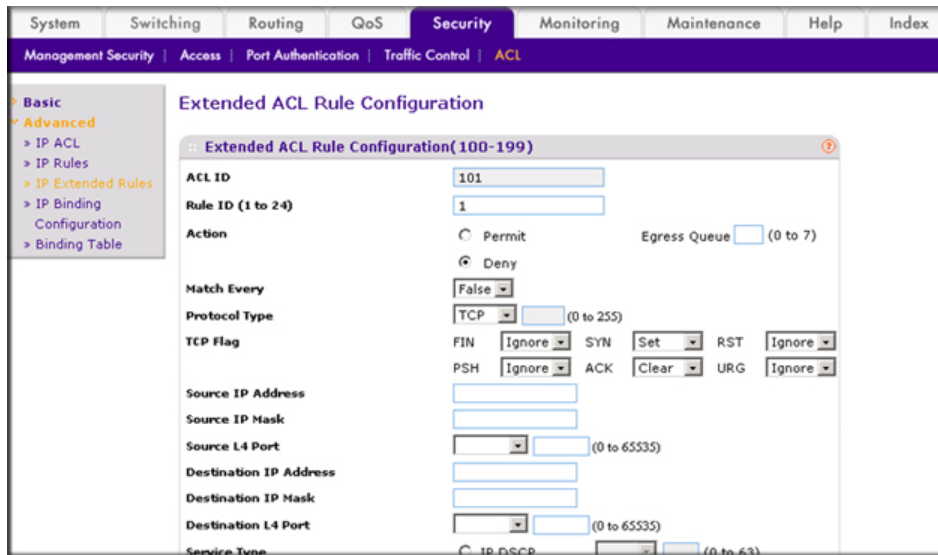


- b. In the IP ACL Table, in the **IP ACL ID** field, enter **102**.
- c. Click **Add**.
9. Add and configure an IP extended rule that is associated with ACL 101.
- a. Select **Security > ACL > Advanced > IP Extended Rules**. A screen similar to the following displays.



- b. Under IP Extended Rules, in the **ACL ID** list, select **10**.

c. Click **Add**. The Extended ACL Rule Configuration screen displays.



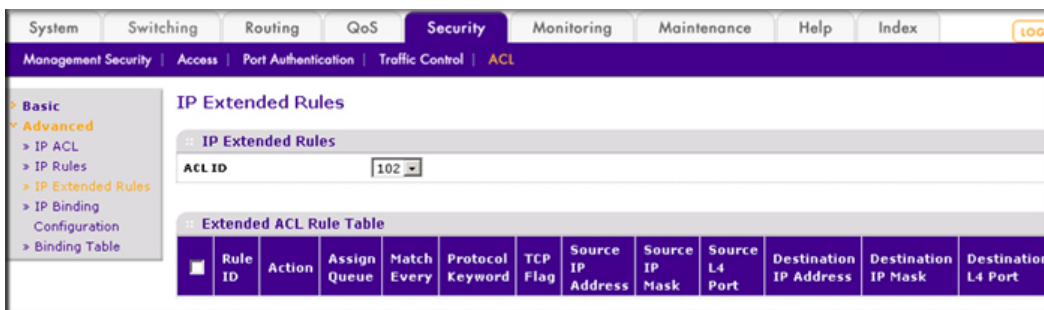
d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

- In the **Rule ID** field, enter **1**.
- For Action mode, select the **Deny** radio button.
- In the **Match Every** field, select **False**.
- In the **Protocol Type** list, select **TCP**.
- For TCP Flag, in the **SYN** field, select **Set**, and in the **ACK** field, select **Clear**.

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

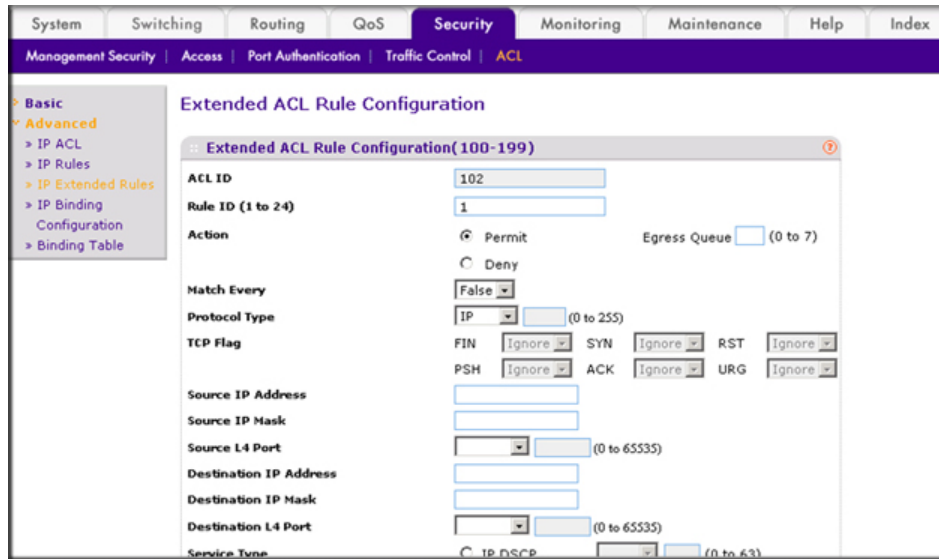
10. Add and configure an IP extended rule that is associated with ACL 102.

a. Select **Security > ACL > Advanced > IP Extended Rules**. A screen similar to the following displays.



b. Under IP Extended Rules, in the **ACL ID** list, select **102**.

c. Click **Add**. The Extended ACL Rule Configuration screen displays.



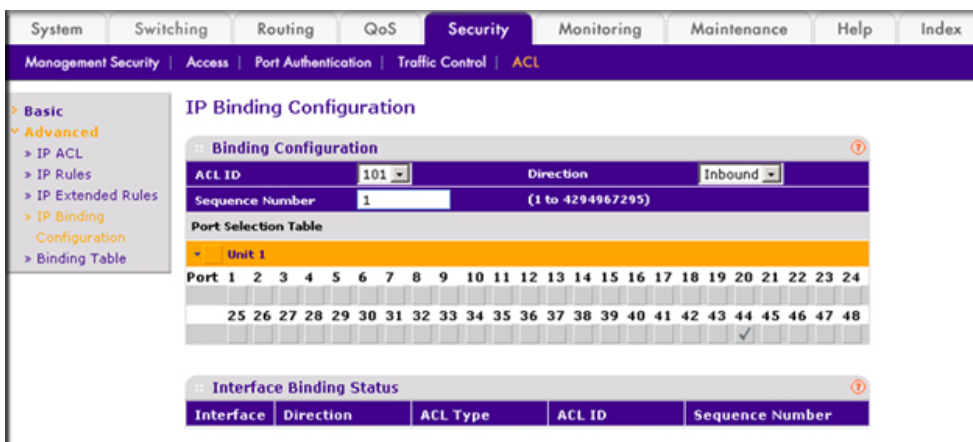
d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

- In the **Rule ID** field, enter **1**.
- For Action, select the **Permit** radio button.
- In the **Match Every** field, select **False**.
- In the **Protocol Type** list, select **IP**.

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

11. Apply ACL 101 to port 44.

a. Select **Security > ACL > Advanced > IP Binding Configuration**. A screen similar to the following displays.



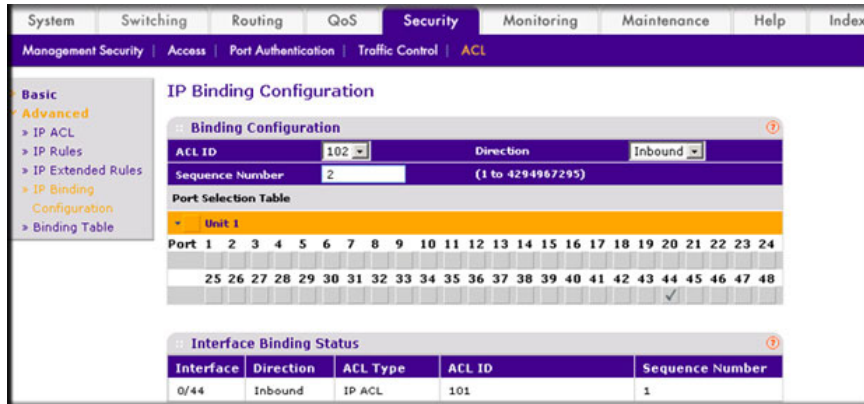
b. Under Binding Configuration, specify the following:

- In the **ACL ID** list, select **101**.
- In the **Sequence Number** field, enter **1**.

- c. Click **Unit 1**. The ports display.
- d. Click the gray box under port **44**. A check mark displays in the box.
- e. Click **Apply** to save the settings.

12. Apply ACL 102 to port 44.

- a. Select **Security > ACL > Advanced > IP Binding Configuration**. A screen similar to the following displays.



- b. Under Binding Configuration, make the following selection and enter the following information:
 - In the **ACL ID** list, select **102**.
 - In the **Sequence Number** field, enter **2**.
- c. Click **Unit 1**. The ports display.
- d. Click the gray box under port **44**. A check mark displays in the box.
- e. Click **Apply** to save the settings.

Configuring the GSM7342S Switch

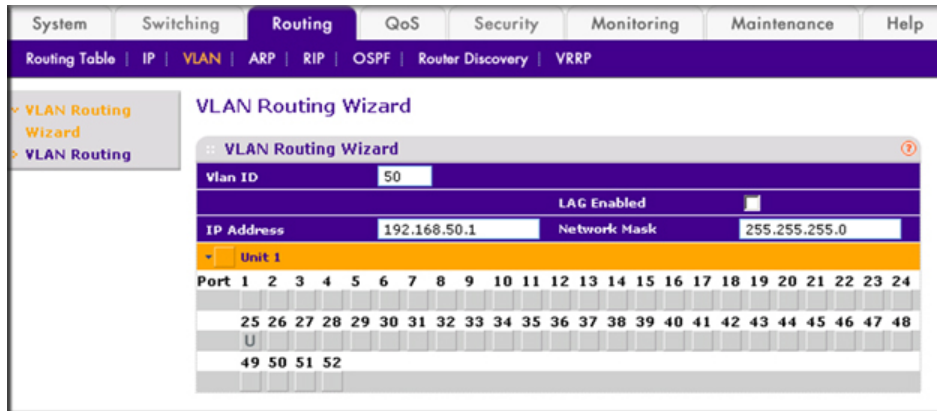
1. Create VLAN 40 with IP address 192.168.40.1/24.

- a. Select **Routing > VLAN > VLAN Routing Wizard**. A screen similar to the following displays.



- b. Enter the following information:
 - In the **Vlan ID** field, enter **40**.

- In the **IP Address** field, enter **192.168.40.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.
- c. Click **Unit 1**. The ports display.
 - d. Click the gray box under port **24** twice until **U** displays. The U specifies that the egress packet is untagged for the port.
 - e. Click **Apply** to save VLAN 40.
2. Create VLAN 50 with IP address 192.168.50.1/24:
 - a. Select **Routing > VLAN > VLAN Routing Wizard**. A screen similar to the following displays.

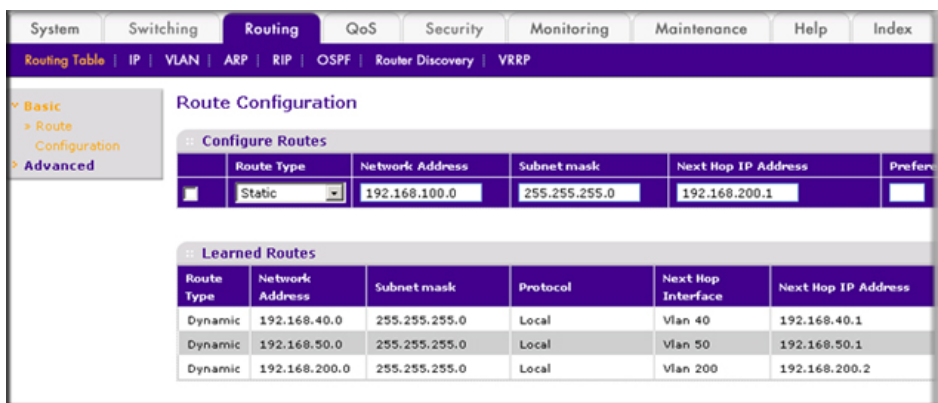


- b. Enter the following information:
 - In the **Vlan ID** field, enter **50**.
 - In the **IP Address** field, enter **192.168.50.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.
 - c. Click **Unit 1**. The ports display.
 - d. Click the gray box under port **25** twice until **U** displays. The U specifies that the egress packet is untagged for the port.
 - e. Click **Apply** to save VLAN 50.
3. Create VLAN 200 with IP address 192.168.200.2/24.

- a. Select **Routing > VLAN > VLAN Routing Wizard**. A screen similar to the following displays.

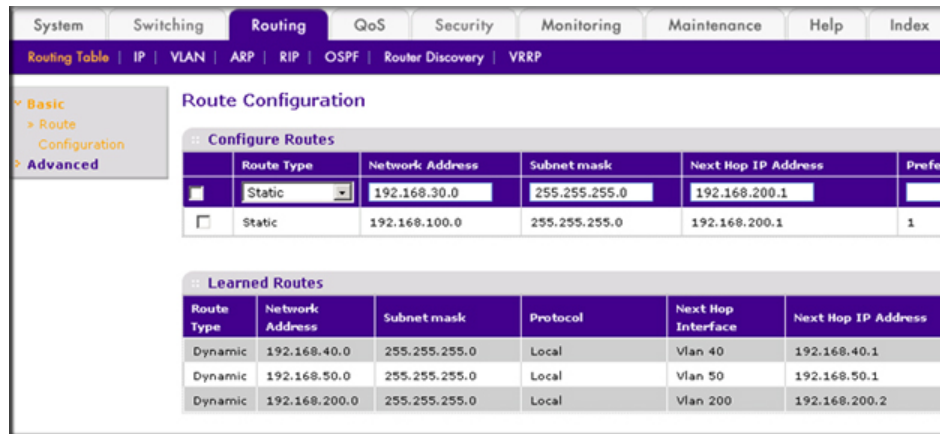


- b. Enter the following information:
- In the **Vlan ID** field, enter **200**.
 - In the **IP Address** field, enter **192.168.200.2**.
 - In the **Network Mask** field, enter **255.255.255.0**.
- c. Click **Unit 1**. The ports display.
- d. Click the gray box under port **48** twice until U displays. The U specifies that the egress packet is untagged for the port.
- e. Click **Apply** to save VLAN 200.
4. Create a static route with IP address 192.168.100.0/24:
- a. Select **Routing > Routing Table > Basic > Route Configuration**. A screen similar to the following displays.



- b. Under Configure Routes, make the following selections and enter the following information:
- Select **Static** in the **Route Type** field.
 - In the **Network Address** field, enter **192.168.100.0**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Next Hop IP Address** field, enter **192.168.200.1**.

- c. Click **Add**.
5. Create a static route with IP address 192.168.30.0/24:
- a. Select **Routing > Routing Table > Basic > Route Configuration**. A screen similar to the following displays.



Route Type	Network Address	Subnet mask	Next Hop IP Address	Preference
Static	192.168.30.0	255.255.255.0	192.168.200.1	
Static	192.168.100.0	255.255.255.0	192.168.200.1	1

Route Type	Network Address	Subnet mask	Protocol	Next Hop Interface	Next Hop IP Address
Dynamic	192.168.40.0	255.255.255.0	Local	Vlan 40	192.168.40.1
Dynamic	192.168.50.0	255.255.255.0	Local	Vlan 50	192.168.50.1
Dynamic	192.168.200.0	255.255.255.0	Local	Vlan 200	192.168.200.2

- b. Under Configure Routes, make the following selection and enter the following information:
- In the **Route Type** field, select **Static**.
 - In the **Network Address** field, enter **192.168.30.0**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Next Hop IP Address** field, enter **192.168.200.1**.
- c. Click **Add**.

Use ACLs to Configure Isolated VLANs on a Layer 3 Switch

This example shows how to isolate VLANs on a Layer 3 switch by using ACLs. In this example, PC 1 is in VLAN 24, PC 2 is in VLAN 48, and the server is in VLAN 38. PC 1 and

PC 2 are isolated by an ACL but can both access the server. The example is shown as CLI commands and as a Web interface procedure.

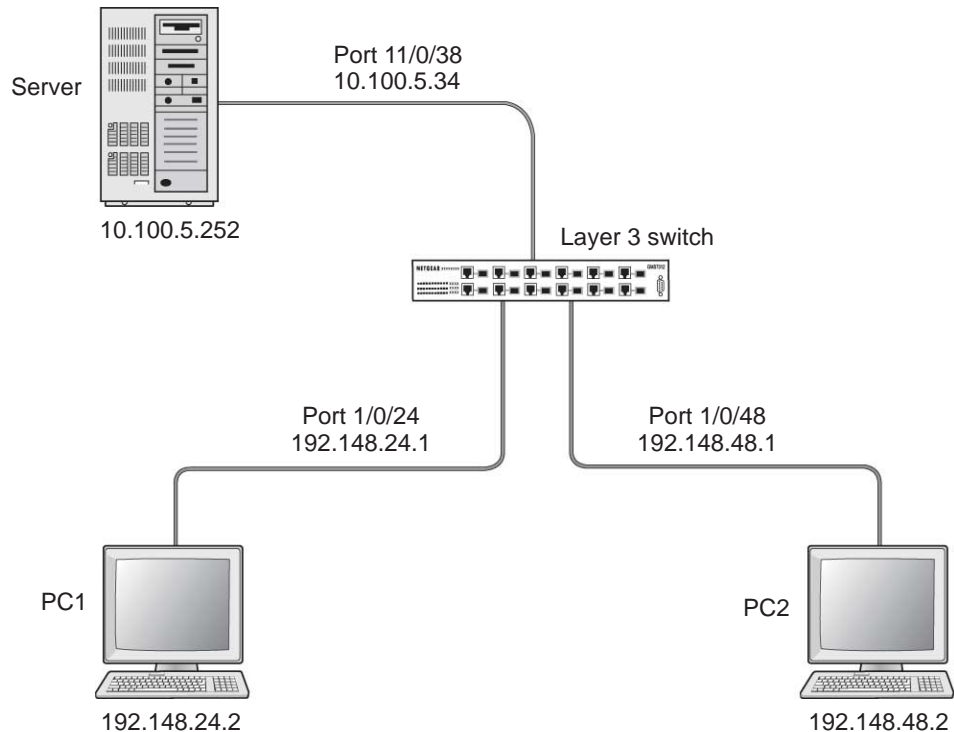


Figure 18. Using ACLs to isolate VLANs on a Layer 3 switch

CLI: Configure One-Way Access Using a TCP Flag in ACL Commands

1. Enter the following CLI commands.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 24
(Netgear Switch) (Vlan)#vlan routing 24
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan participation include 24
(Netgear Switch) (Interface 1/0/24)#vlan pvid 24
(Netgear Switch) (Interface 1/0/24)#exit

(Netgear Switch) (Config)#interface vlan 24
(Netgear Switch) (Interface-vlan 24)#routing
(Netgear Switch) (Interface-vlan 24)#ip address 192.168.24.1 255.255.255.0
(Netgear Switch) (Interface-vlan 24)#exit
(Netgear Switch) (Config)#exit
```

2. Create VLAN 48, add port 1/0/48 to it, and assign IP address 192.168.48.1 to it.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 48
(Netgear Switch) (Vlan)#vlan routing 48
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan participation include 48
(Netgear Switch) (Interface 1/0/48)#vlan pvid 48
(Netgear Switch) (Interface 1/0/48)#exit

(Netgear Switch) (Config)#vlan interface vlan 48
(Netgear Switch) (Interface-vlan 48)#routing
(Netgear Switch) (Interface-vlan 48)#ip address 192.168.48.1 255.255.255.0
(Netgear Switch) (Interface-vlan 48)#exit
(Netgear Switch) (Config)#exit
```

3. Create VLAN 38, add port 1/0/38 to it, and assign IP address 10.100.5.34 to it.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 38
(Netgear Switch) (Vlan)#vlan routing
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/38
(Netgear Switch) (Interface 1/0/38)#vlan participation include 38
(Netgear Switch) (Interface 1/0/38)#vlan pvid 38
(Netgear Switch) (Interface 1/0/38)#exit
(Netgear Switch) (Config)#interface vlan 38
(Netgear Switch) (Interface-vlan 38)#routing
(Netgear Switch) (Interface-vlan 38)#ip address 10.100.5.34 255.255.255.0
(Netgear Switch) (Interface-vlan 38)#exit
```

4. Enable IP routing on the switch.

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

5. Add a default route so that all the traffic without a destination is forwarded according to this default route.

```
(Netgear Switch) (Config)#ip route default 10.100.5.252
```

6. Create ACL 101 to deny all traffic that has the destination IP address 192.168.24.0/24.

```
(Netgear Switch) (Config)#access-list 101 deny ip any 192.168.24.0 0.0.0.255
```

7. Create ACL 102 to deny all traffic that has the destination IP address 192.168.48.0/24.

```
(Netgear Switch) (Config)#access-list 102 deny ip any 192.168.48.0 0.0.0.255
```

8. Create ACL 103 to permit all other traffic.

```
(Netgear Switch) (Config)#access-list 103 permit ip any any
```

9. Deny all traffic with the destination IP address 192.168.48.0/24, and permit all other traffic.

```
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#ip access-group 102 in 1
(Netgear Switch) (Interface 1/0/24)#ip access-group 103 in 2
(Netgear Switch) (Interface 1/0/24)#exit
```

10. Deny all traffic with the destination IP address 192.168.24.0/24, and permit all other traffic.

```
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#ip access-group 101 in 1
(Netgear Switch) (Interface 1/0/48)#ip access-group 103 in 2
(Netgear Switch) (Interface 1/0/48)#exit
```

Web Interface: Configure One-Way Access Using a TCP Flag in an ACL

1. Create VLAN 24 with IP address 192.168.24.1.

- a. Select **Routing > VLAN > VLAN Routing Wizard**. A screen similar to the following displays.

The screenshot shows the 'VLAN Routing Wizard' configuration page. The 'Vlan ID' is set to 24. The 'IP Address' is 192.168.24.1 and the 'Network Mask' is 255.255.255.0. The 'LAG Enabled' checkbox is unchecked. Below the fields is a table for 'Unit 1' with columns for 'Port' and 'U' (untagged). The 'U' column has a 'U' under port 24.

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
																								U	

- b. Enter the following information:
- In the **Vlan ID** field, enter **24**.
 - In the **IP Address** field, enter **192.168.24.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.
- c. Click **Unit 1**. The ports display.
- d. Click the gray box under port **24** twice until **U** displays. The U specifies that the egress packet is untagged for the port.
- e. Click **Apply** to save VLAN 24.
2. Create VLAN 48 with IP address 192.168.48.1.
- a. Select **Routing > VLAN > VLAN Routing Wizard**. A screen similar to the following displays.

The screenshot shows the 'VLAN Routing Wizard' configuration page for VLAN 48. The 'Vlan ID' is set to 48. The 'IP Address' is 192.168.48.1 and the 'Network Mask' is 255.255.255.0. The 'LAG Enabled' checkbox is unchecked. Below the fields is a table for 'Unit 1' with columns for 'Port' and 'U' (untagged). The 'U' column has a 'U' under port 48.

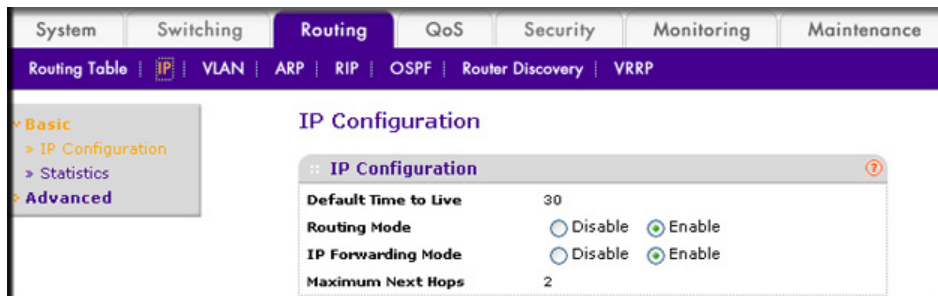
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	

- b. Enter the following information:
- In the **Vlan ID** field, enter **48**.
 - In the **IP Address** field, enter **192.168.48.1**.
 - In the **Network Mask** field, enter **255.255.255.0**.

- c. Click **Unit 1**. The ports display.
 - d. Click the gray box under port **48** twice until **U** displays. The U specifies that the egress packet is untagged for the port.
 - e. Click **Apply** to save VLAN 48.
3. Create VLAN 38 with IP address 10.100.5.34.
 - a. Select **Routing > VLAN > VLAN Routing Wizard**. A screen similar to the following displays.



- b. Enter the following information in the VLAN Routing Wizard:
 - In the **Vlan ID** field, enter **38**.
 - In the **IP Address** field, enter **10.100.5.34**.
 - In the **Network Mask** field, enter **255.255.255.0**.
 - c. Click **Unit 1**. The ports display.
 - d. Click the gray box under port **38** twice until **U** displays. The U specifies that the egress packet is untagged for the port.
 - e. Click **Apply** to save VLAN 38.
4. Enable IP routing:
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.



- b. Under IP Configuration, make the following selections:
 - For Routing Mode, select the **Enable** radio button.
 - For IP Forwarding Mode, select the **Enable** radio button.

- c. Click **Apply** to enable IP routing.
5. Create an ACL with ID 101.
 - a. Select **Security > ACL > Advanced > IP ACL**. A screen similar to the following displays.

The screenshot shows the IP ACL configuration page. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, and Help. The Security menu is expanded to show Management Security, Access, Port Authentication, Traffic Control, and ACL. The ACL configuration page has a left sidebar with a tree view showing Basic and Advanced options. The main content area is titled 'IP ACL' and contains two sections: 'IP ACL' and 'IP ACL Table'. The 'IP ACL' section has input fields for 'Current Number of ACL' (0) and 'Maximum ACL' (100). The 'IP ACL Table' section is a table with columns for IP ACL ID, Rules, and Type. A single row is visible with IP ACL ID 101, 0 rules, and an empty Type field.

IP ACL ID	Rules	Type
101		

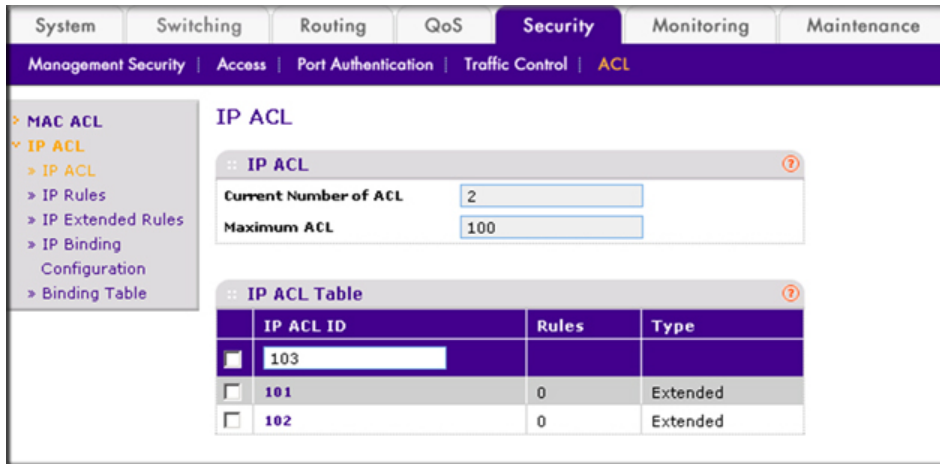
- b. In the IP ACL Table, in the **IP ACL ID** field, enter **101**.
 - c. Click **Add**.
6. Create an ACL with ID 102.
 - a. Select **Security > ACL > Advanced > IP ACL**. A screen similar to the following displays.

The screenshot shows the IP ACL configuration page. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, and Help. The Security menu is expanded to show Management Security, Access, Port Authentication, Traffic Control, and ACL. The ACL configuration page has a left sidebar with a tree view showing Basic and Advanced options. The main content area is titled 'IP ACL' and contains two sections: 'IP ACL' and 'IP ACL Table'. The 'IP ACL' section has input fields for 'Current Number of ACL' (1) and 'Maximum ACL' (100). The 'IP ACL Table' section is a table with columns for IP ACL ID, Rules, and Type. Two rows are visible: one with IP ACL ID 102, 0 rules, and an empty Type field; and another with IP ACL ID 101, 0 rules, and Type 'Extended'.

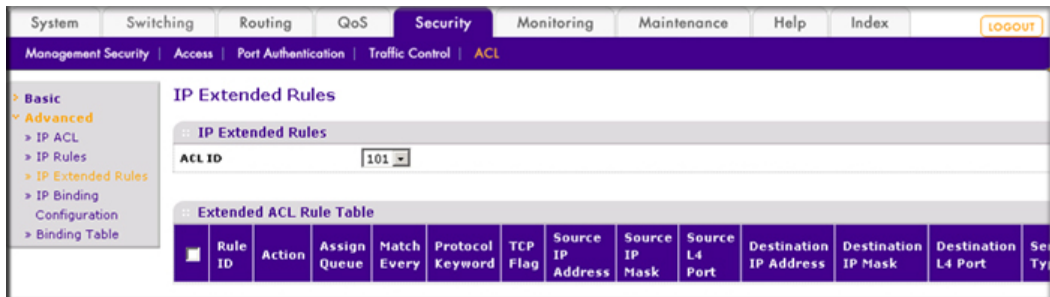
IP ACL ID	Rules	Type
102		
101	0	Extended

- b. In the IP ACL Table, in the **IP ACL ID** field, enter **102**.
 - c. Click **Add**.
7. Create an ACL with ID 103.

- a. Select **Security > ACL > Advanced > IP ACL**. A screen similar to the following displays.



- b. In the **IP ACL ID** field of the IP ACL Table, enter **103**.
 - c. Click **Add**.
8. Add and configure an IP extended rule that is associated with ACL 101:
 - a. Select **Security > ACL > Advanced > IP Extended Rules**. A screen similar to the following displays.



- b. Under IP Extended Rules, in the **ACL ID** field, select **101**.

- c. Click **Add**. The Extended ACL Rule Configuration screen displays.

The screenshot shows the 'Extended ACL Rule Configuration' window. The 'ACL ID' is set to 101 and 'Rule ID (1 to 23)' is set to 1. The 'Action' is 'Deny'. 'Match Every' is set to 'False'. The 'Protocol Type' is 'IP'. Under 'TCP Flag', 'FIN', 'PSH', 'SYN', 'ACK', 'RST', and 'URG' are all set to 'Ignore'. The 'Destination IP Address' is '192.168.24.0' and the 'Destination IP Mask' is '0.0.0.255'. Other fields like 'Source IP Address', 'Source IP Mask', and 'Source L4 Port' are empty.

- d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:
- In the **Rule ID** field, enter **1**.
 - For Action, select the **Deny** radio button.
 - In the **Match Every** field, select **False**.
 - In the **Destination IP Address** field, enter **192.168.24.0**.
 - In the **Destination IP Mask** field, enter **0.0.0.255**.
- e. Click **Apply** to save the settings.

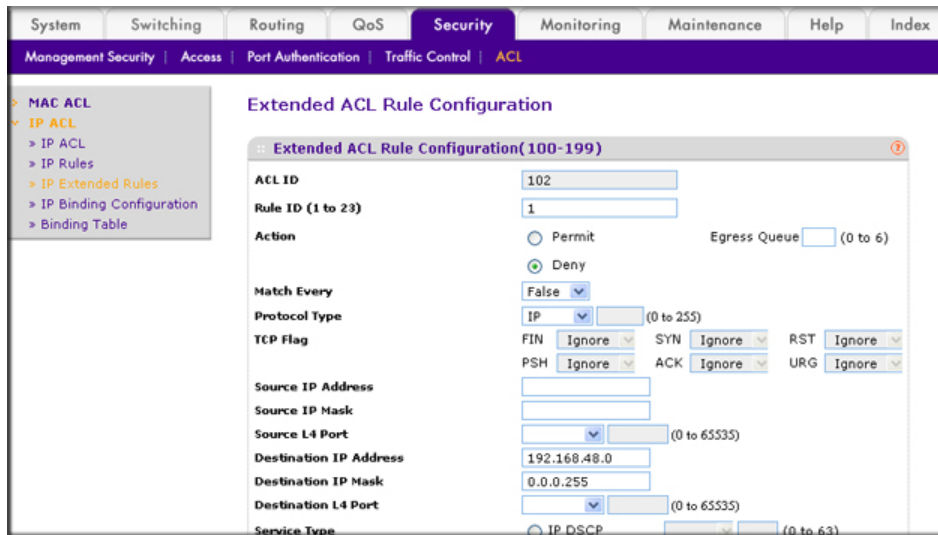
9. Add and configure an IP extended rule that is associated with ACL 102.

- a. Select **Security > ACL > Advanced > IP Extended Rules**. A screen similar to the following displays.

The screenshot shows the 'IP Extended Rules' configuration page. The 'ACL ID' is set to 102. Below it is a table titled 'Extended ACL Rule Table' with the following columns: Rule ID, Action, Assign Queue, Match Every, Protocol Keyword, TCP Flag, Source IP Address, Source IP Mask, Source L4 Port, Destination IP Address, Destination IP Mask, and Destination L4 Port. The table is currently empty.

- b. Under IP Extended Rules, in the **ACL ID** field, select **102**.

c. Click **Add**. The Extended ACL Rule Configuration screen displays.



d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

- In the **Rule ID** field, enter **1**.
- For Action mode, select the **Deny** radio button.
- In the **Match Every** field, select **False**.
- In the **Destination IP Address** field, enter **192.168.48.0**.
- In the **Destination IP Mask** field, enter **0.0.0.255**.

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

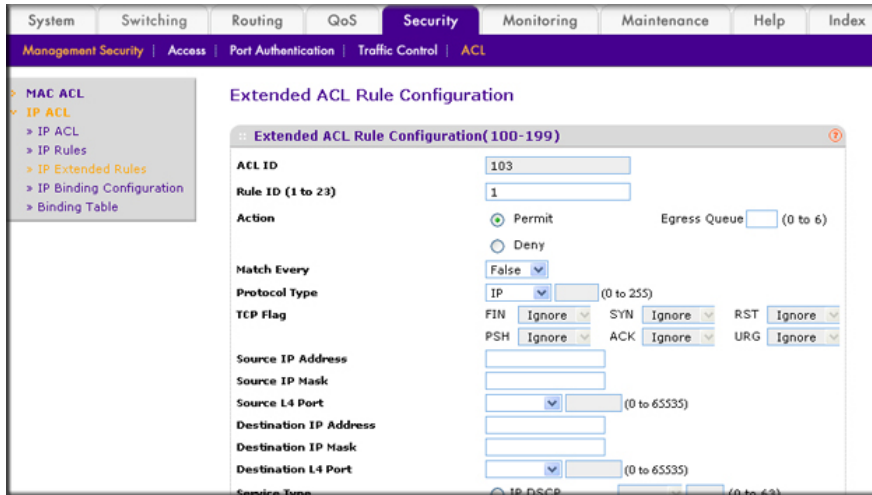
10. Add and configure an IP extended rule that is associated with ACL 103:

a. Select **Security > ACL > Advanced > IP Extended Rules**. A screen similar to the following displays.



b. Under IP Extended Rules, in the **ACL ID** field, select **103**.

c. Click **Add**. The Extended ACL Rule Configuration screen displays.



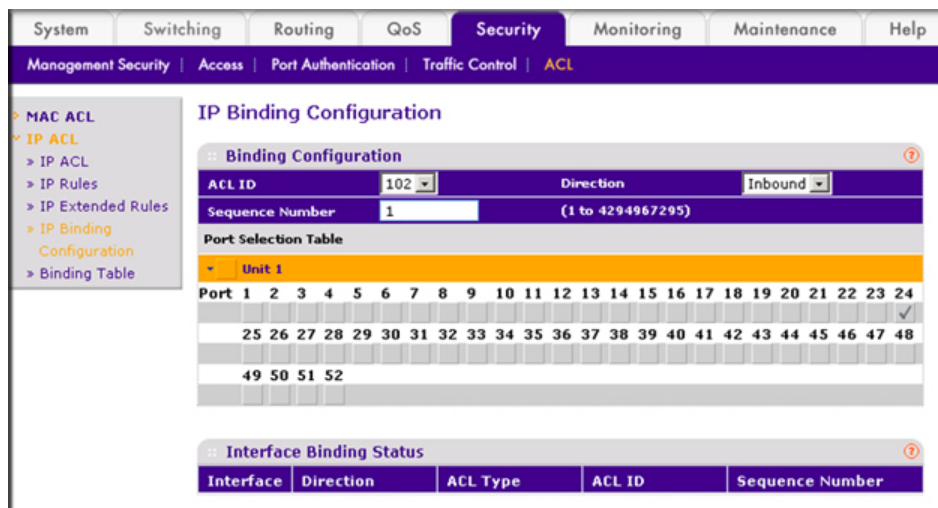
d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

- In the **Rule ID** field, enter **1**.
- For Action mode, select the **Permit** radio button.
- In the **Match Every** field, select **False**.
- In the **Protocol Type** field, select **IP**.

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

11. Apply ACL 102 to port 24:

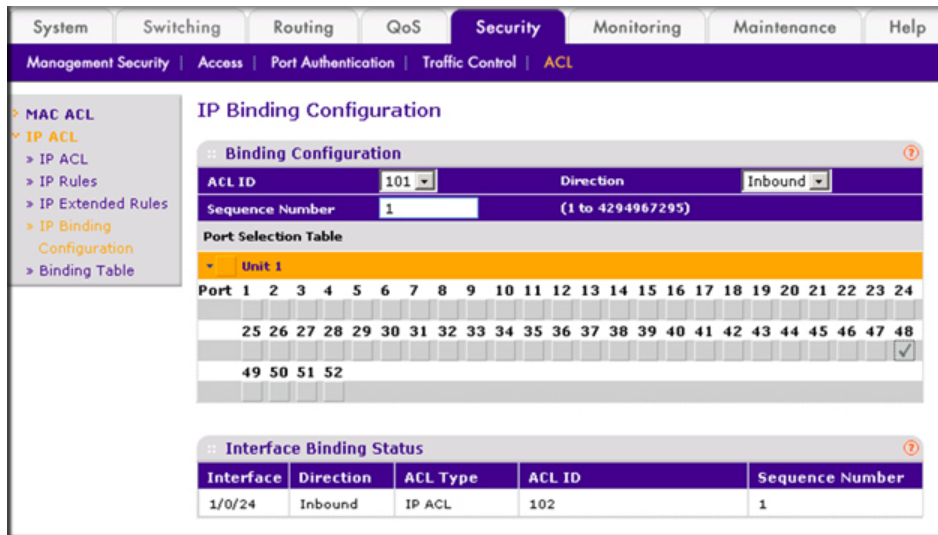
a. Select **Security > ACL > Advanced > IP Binding Configuration**. A screen similar to the following displays.



b. Under Binding Configuration, make the following selection and enter the following information:

- In the **ACL ID** field, select **102**.

- In the **Sequence Number** field, enter **1**.
 - c. Click **Unit 1**. The ports display.
 - d. Click the gray box under port **24**. A check mark displays in the box.
 - e. Click **Apply** to save the settings.
12. Apply ACL 101 to port 48:
- a. Select **Security > ACL > Advanced > IP Binding Configuration**. A screen similar to the following displays.



- b. Under Binding Configuration, make the following selection and enter the following information:
 - In the **ACL ID** field, select **101**.
 - In the **Sequence Number** field, enter **1**.
 - c. Click **Unit 1**. The ports display.
 - d. Click the gray box under port **48**. A check mark displays in the box.
 - e. Click **Apply** to save the settings.
13. Apply ACL 103 to port 24 and port 48:

- a. Select **Security > ACL > Advanced > IP Binding Configuration**. A screen similar to the following displays.

Interface	Direction	ACL Type	ACL ID	Sequence Number
1/0/24	Inbound	IP ACL	102	1
1/0/48	Inbound	IP ACL	101	1

- b. Under Binding Configuration, make the following selection and enter the following information:
- In the **ACL ID** field, select **103**.
 - In the **Sequence Number** field, enter **2**.
- c. Click **Unit 1**. The ports display. Configure the following ports:
- Click the gray box under port **24**. A check mark displays in the box.
 - Click the gray box under port **48**. A check mark displays in the box.
- d. Click **Apply** to save the settings.

Set up a MAC ACL with Two Rules

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

CLI: Set up a MAC ACL with Two Rules

1. Create a new MAC ACL `acl_bpdu`.

```
(Netgear Switch) #
(Netgear Switch) #config
(Netgear Switch) (Config)#mac access-list extended acl_bpdu
```

2. Deny all the traffic that has destination MAC `01:80:c2:xx:xx:xx`.

```
(Netgear Switch) (Config-mac-access-list)#deny any 01:80:c2:00:00:00 00:00:00:ff:ff:ff
```

3. Permit all the other traffic.

```
(Netgear Switch) (Config-mac-access-list)#permit any
(Netgear Switch) (Config-mac-access-list)#exit
```

4. Apply the MAC ACL acl_bpdu to port 1/0/2.

```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#mac access-group acl_bpdu in
```

Web Interface: Set up a MAC ACL with Two Rules

1. Create MAC ACL 101 on the switch.

- a. Select **Security > ACL > MAC ACL**. A screen similar to the following displays.

MAC ACL			
Current Number of ACL	0		
Maximum ACL	100		
MAC ACL Table			
Name	Rules	Direction	
<input checked="" type="checkbox"/> acl_bpdu			

- b. In the **Name** field, enter **acl_bpdu**.

- c. Click **Add** to create ACL acl_bpdu.

2. Create a new rule associated with the ACL acl_bpdu.

- a. Select **Security > ACL > MAC ACL > MAC Rules**. A screen similar to the following displays.

MAC Rules								
Rules								
ACL Name: acl_bpdu								
Rule Table								
ID	Action	Assign Queue Id	Match Every	CoS	Destination MAC	Destination MAC Mask	Ether	
<input checked="" type="checkbox"/> 1	Deny				01:80:c2:00:00:00	00:00:00:ff:ff:ff		

- a. In the **ACL Name** field, select **acl_bpdu**.

- b. In the **Action** field, select **Deny**.

- c. Enter the following information in the Rule Table.
 - In the **ID** field, enter 1.
 - In the **Destination MAC** field, enter **01:80:c2:00:00:00**.
 - In the **Destination MAC Mask** field, enter **00:00:00:ff:ff:ff**.
 - d. Click the **Add** button.
3. Create a another rule associated with the ACL acl_bpdu.
 - a. Select **Security > ACL > MAC ACL > MAC Rules**. A screen similar to the following displays.

ID	Action	Assign Queue Id	Match Every	CoS	Destination MAC	Destination MAC Mask	Ether
1	Deny		False		01:80:C2:00:00:00	00:00:00:FF:FF:FF	

- a. Select **acl_bpdu** in the **ACL Name** field.
 - b. Enter the following information in the Rule Table.
 - In the **ID** field, enter 2.
 - In the **Action** field, select the **Permit**.
 - c. Click the **Add** button.
4. Apply the ACL acl_bpdu to port 2.
 - a. Select **Security > ACL > MAC ACL > MAC Binding Configuration**. A screen similar to the following displays.

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
		<input checked="" type="checkbox"/>																										

- b. Enter the following information in the MAC Binding Configuration.
 - IN the **ACL ID** field, select **acl_bpdu**.

- In the **Sequence Number** field, enter **1**.
- c. Click the **Unit 1**. The ports display.
- d. Click the gray box under port **2**. A check mark displays in the box.
- e. Click **Apply** to save the settings.

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.

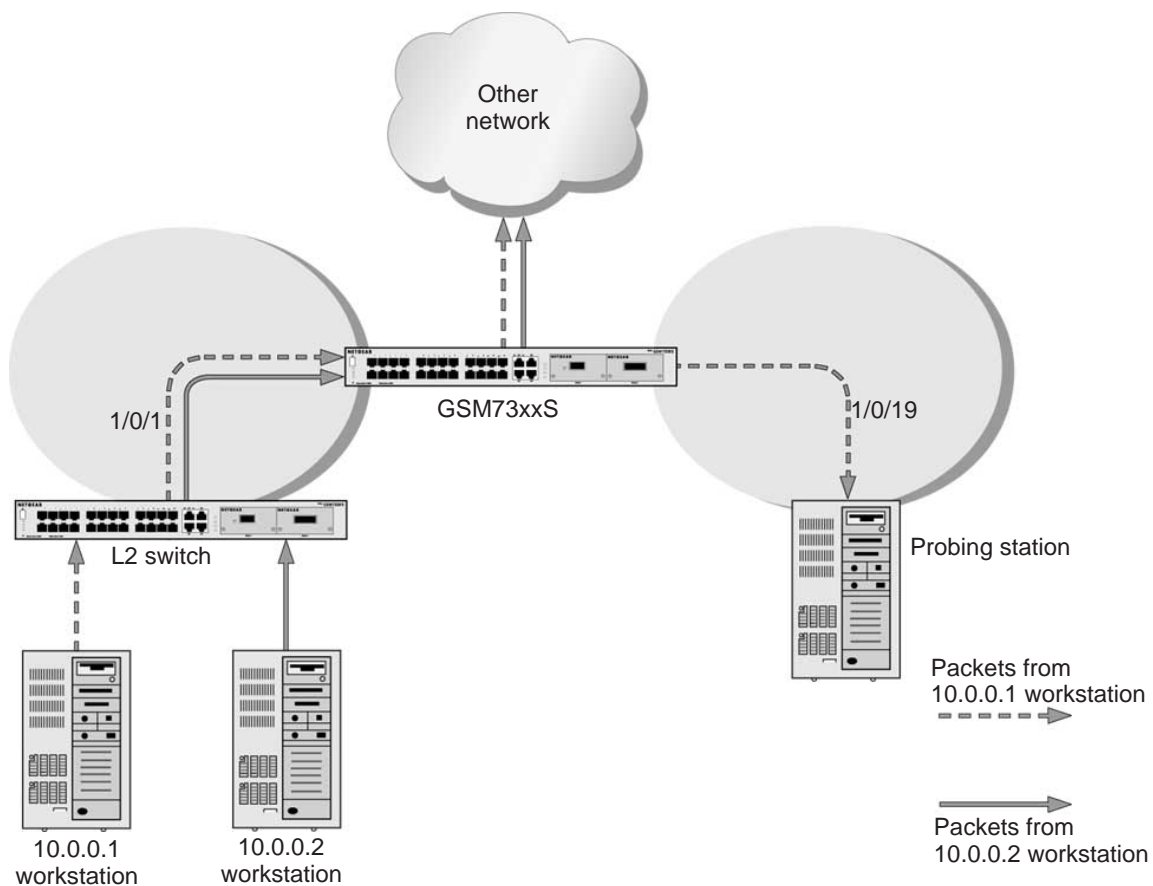


Figure 19. ACL mirroring

CLI: Configure ACL Mirroring

The script in this section shows how to mirror the traffic stream received from a host in an interface. These examples mirror the traffic from the host 10.0.0.1 connected to the interface 1/0/1.

1. Create an IP access control list with the name monitorHost.

```
(Netgear Switch) (Config)# ip access-list monitorHost
```

2. Define the rules to match host 10.0.0.1 and to permit all others.

```
(Netgear Switch) (Config-ipv4-acl)# permit ip 10.0.0.1 0.0.0.0 any mirror 1/0/19
(Netgear Switch) (Config-ipv4-acl)# permit every
```

3. Bind the ACL with interface 1/0/1.

```
(Netgear Switch) (Interface 1/0/1)#ip access-group monitorHost in 1
```

4. View the configuration.

```
(Netgear Switch) # show ip access-lists
Current number of ACLs: 1 Maximum number of ACLs: 100

ACL ID/Name          Rules  Direction      Interface(s)      VLAN(s)
-----
monitorHost          2      inbound        1/0/1

(Netgear Switch) #show ip access-lists monitorHost

ACL Name: monitorHost
Inbound Interface(s): 1/0/1

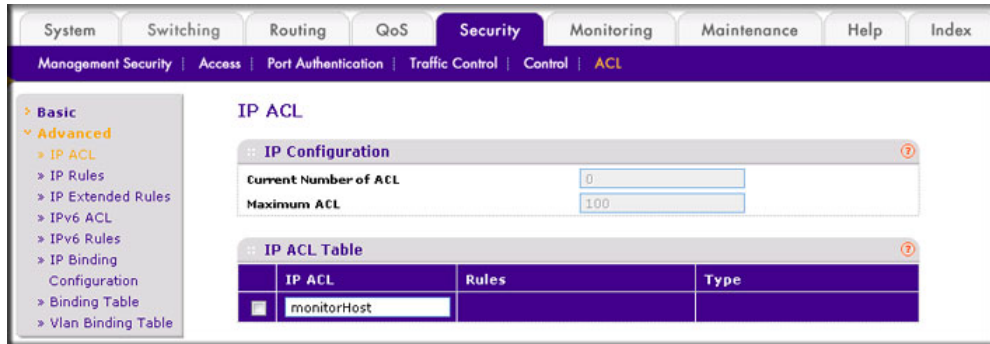
Rule Number: 1
Action..... permit
Match All..... FALSE
Protocol..... 255(ip)
Source IP Address..... 10.0.0.1
Source IP Mask..... 0.0.0.0
Mirror Interface..... 1/0/19

Rule Number: 2
Action..... permit
Match All..... TRUE
```

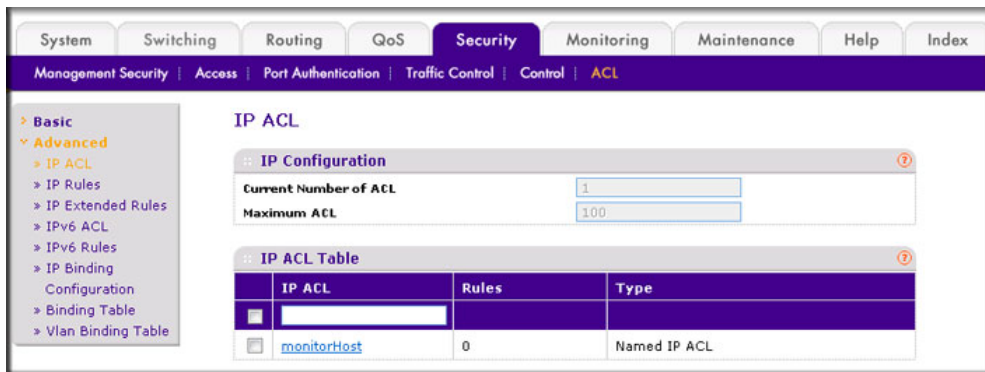
Web Interface: Configure ACL Mirroring

1. Create an IP access control list with the name monitorHost on the switch.

- a. Select **Security > ACL > Advanced > IP ACL**. A screen similar to the following displays.



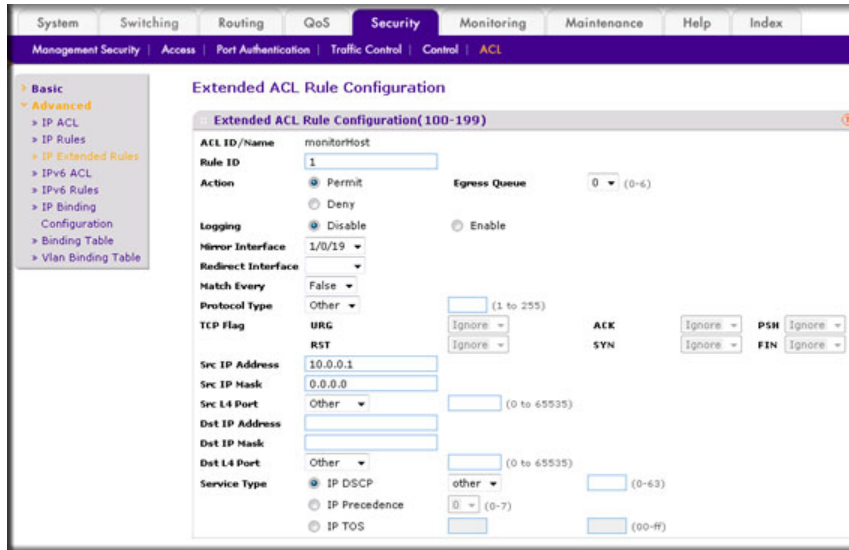
- b. In the **IP ACL ID** field, enter **monitorHost**.
- c. Click **Add** to create ACL monitorHost, and the following screen displays:



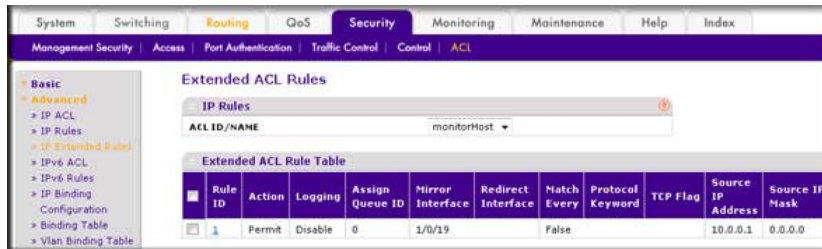
2. Create a rule to match host 10.0.0.1 in the ACL monitorHost.
 - a. Select **Security > ACL > Advanced > IP Extended Rules**. A screen similar to the following displays.



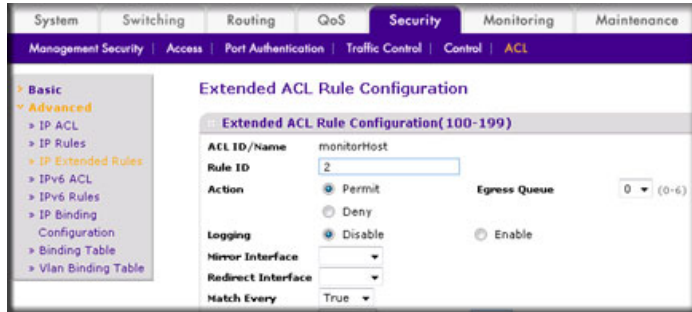
- b. Click **Add**, and the Extended ACL Rule Configuration screen displays.



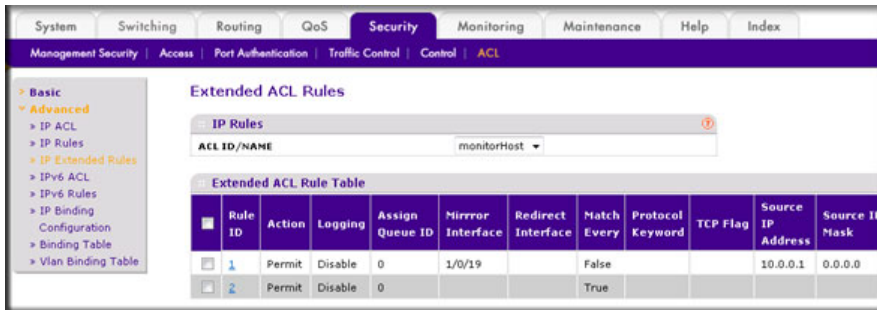
- c. In the **Rule ID** field, enter **1**.
 - d. For Action, select the **Permit** radio button.
 - e. In the **Mirror Interface** list, select **1/0/19**.
 - f. In the **Src IP Address** field, enter **10.0.0.1**.
 - g. In the **Src IP Mask** field, enter **0.0.0.0**.
 - h. Click **Apply**.
3. Create a rule to match every other traffic.
- a. Select **Security > ACL > Advanced > IP Extended Rules**. A screen similar to the following displays.



- b. Click **Add**, and a screen similar to the following displays.



- c. In the **Rule ID** field, enter **2**.
 d. Select the **Permit** radio button.
 e. In the **Match Every** field, select **True**.
 f. Click **Apply**. At the end of this configuration a screen similar to the following displays.

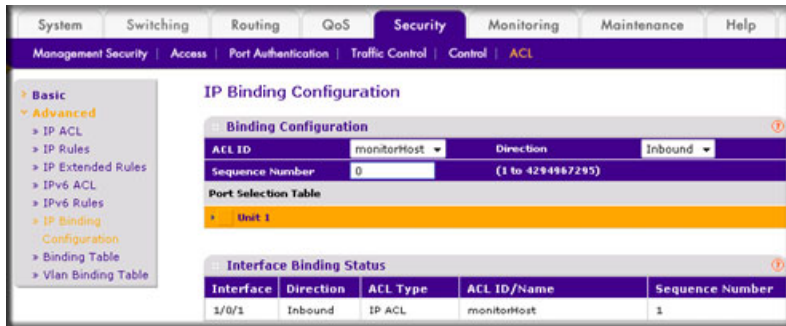


4. Bind the ACL with interface 1/0/1.
 a. Select **Security > ACL > Advanced > IP Binding Configuration**. A screen similar to the following displays.



- b. In the **Sequence Number** field, enter **1**.
 c. In the Port Selection Table, click **Unit 1** to display all the ports for the device.
 d. Select the **Port 1** check box.

e. Click **Apply**. A screen similar to the following displays.



ACL Redirect

This feature redirects a specified traffic stream to a specified interface.

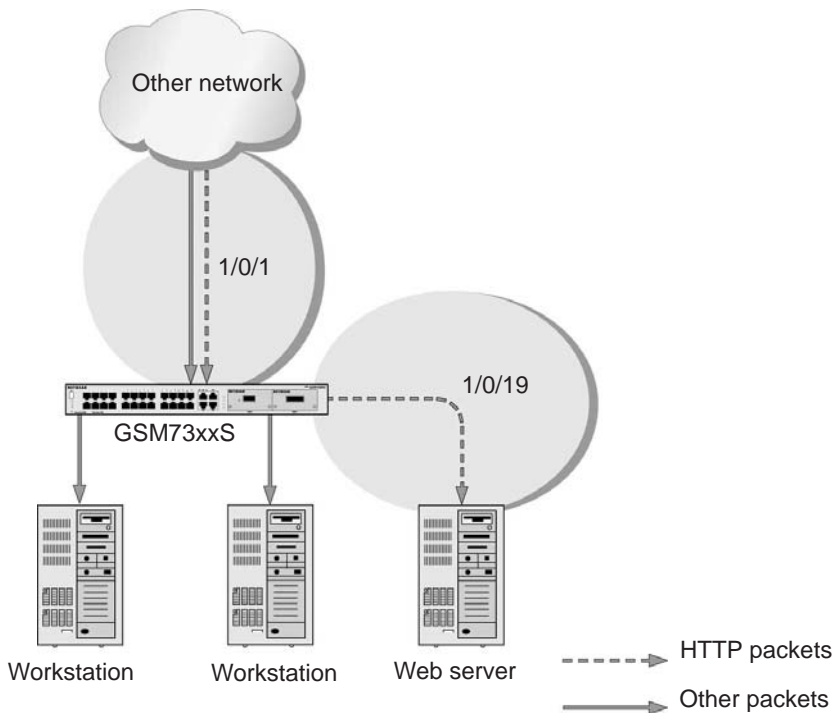


Figure 20. ACL Redirect

CLI: Redirect a Traffic Stream

The script in this section shows how to redirect an HTTP traffic stream received in an interface to the specified interface. This example redirects the HTTP traffic stream received in port 1/0/1 to port 1/0/19.

1. Create an IP access control list with the name redirectHTTP.

```
(Netgear Switch) (Config)#ip access-list redirectHTTP
```

2. Define a rule to match the HTTP stream and define a rule to permit all others.

```
(Netgear Switch) (Config-ipv4-acl)# permit tcp any any eq http redirect 1/0/19
(Netgear Switch) (Config-ipv4-acl)# permit every
```

3. Bind the ACL with interface 1/0/1.

```
(Netgear Switch) (Interface 1/0/1)#ip access-group redirectHTTP in 1
```

4. View the configuration.

```
(Netgear Switch) # show ip access-lists
Current number of ACLs: 1 Maximum number of ACLs: 100

ACL ID/Name          Rules  Direction  Interface(s)  VLAN(s)
-----
redirectHTTP         2      inbound    1/0/1

(Netgear Switch) #show ip access-lists redirectHTTP

ACL Name: redirectHTTP
Inbound Interface(s): 1/0/1

Rule Number: 1
Action..... permit
Match All..... FALSE
Protocol..... 6(tcp)
Destination L4 Port Keyword..... 80(www/http)
Redirect Interface..... 1/0/19

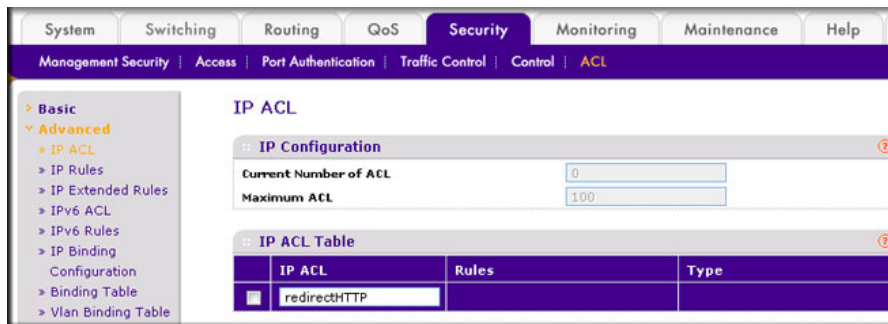
Rule Number: 2
Action..... permit
Match All..... TRUE
```

Web Interface: Redirect a Traffic Stream

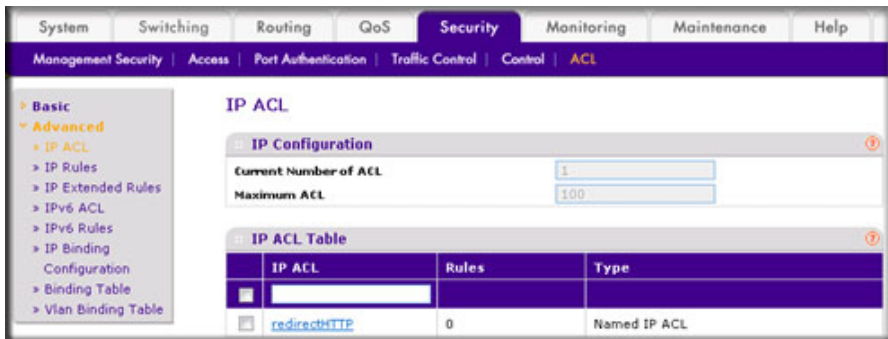
This example redirects the HTTP traffic stream received in port 1/0/1 to port 1/0/19.

1. Create an IP access control list with the name redirectHTTP.

- a. Select **Security > ACL > Advanced > IP ACL**. A screen similar to the following displays.



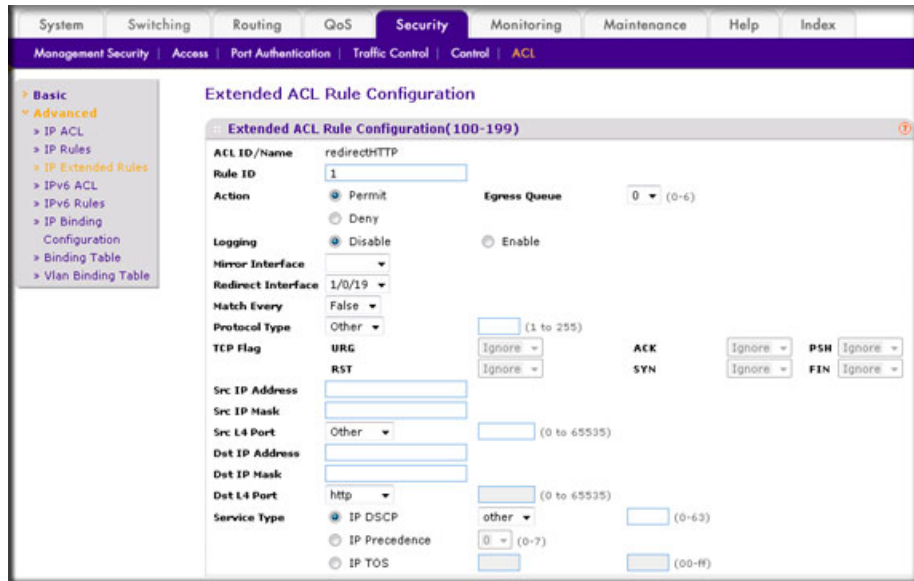
- b. In the **IP ACL** field, enter **redirectHTTP**.
- c. Click **Add** to create the IP ACL **redirectHTTP**. A screen similar to the following displays.



2. Create a rule to redirect HTTP traffic.
 - a. Select **Security > ACL > Advanced > IP Extended Rules**. A screen similar to the following displays.



b. Click **Add**, and the Extended ACL Rule Configuration screen displays.



c. In the **Rule ID** field, enter **1**.

d. For Action, select the **Permit** radio button.

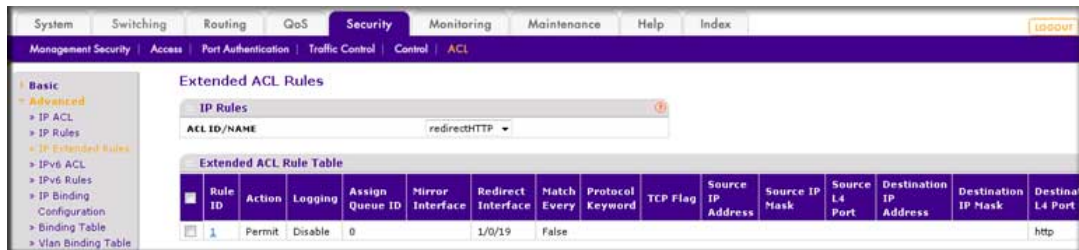
e. In the **Redirect Interface** list, select **1/0/19**.

f. In the **Dst L4 Port** list, select **http**.

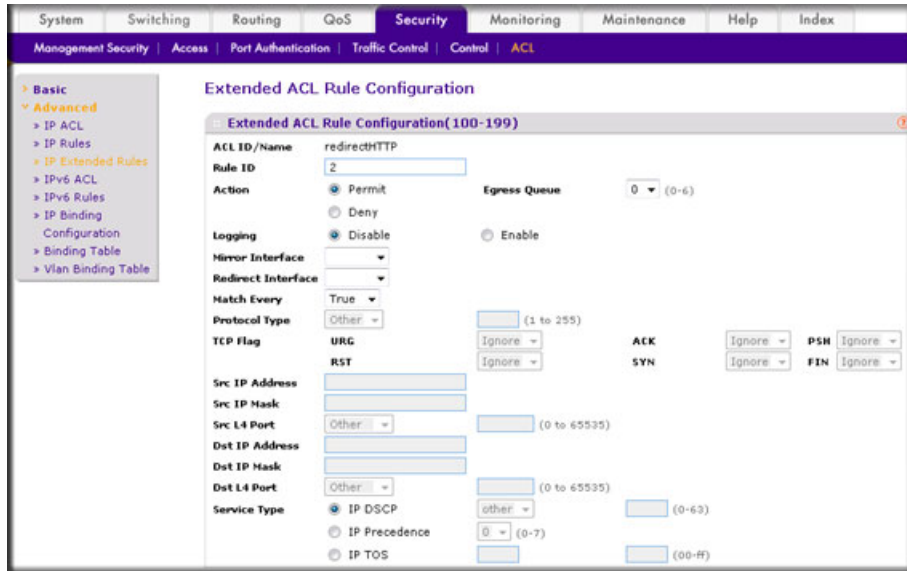
g. Click **Apply**. The Extended ACL Rules screen displays, as described in the next step in this procedure.

3. Create a rule to match every other traffic.

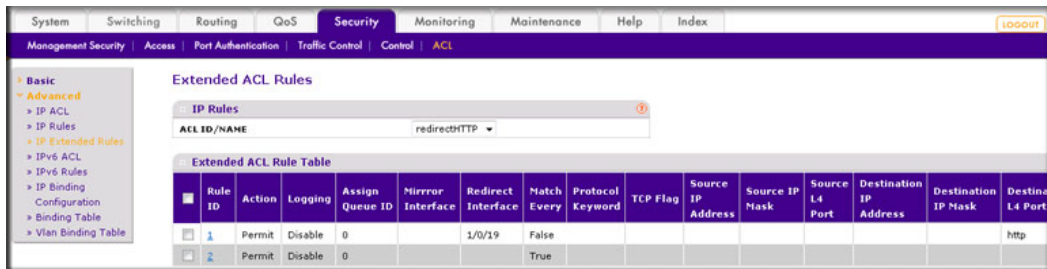
a. Select **Security > ACL > Advanced > IP Extended Rules**. A screen similar to the following displays.



- b. Click **Add**, and the Extended ACL Rule Configuration screen displays.



- c. In the **Rule ID** field, enter **2**.
 d. For Action, select the **Permit** radio button.
 e. In the **Match Every** field, select **True**.
 f. Click **Apply**. A screen similar to the following displays.



4. Bind the ACL with interface 1/0/1.
 a. Select **Security > ACL > Advanced > IP Binding Configuration**. A screen similar to the following displays.



- b. In the **Sequence Number** field, enter **1**.
 c. In the Port Selection Table, click **Unit 1** to display all the ports.

- d. Select the check box below Port 1.
- e. Click **Apply**. At the end of this configuration a screen similar to the following displays.



Configure IPv6 ACLs

This feature extends the existing IPv4 ACL by providing support for IPv6 packet classification. Each ACL is a set of up to 12 rules applied to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and can apply to one or more of the following fields within a packet:

- Source IPv6 prefix
- Destination IPv6 prefix
- Protocol number
- Source Layer 4 port
- Destination Layer 4 port
- DSCP value
- Flow label

Note that the order of the rules is important: When a packet matches multiple rules, the first rule takes precedence. Also, once you define an ACL for a given port, all traffic not specifically permitted by the ACL is denied access.

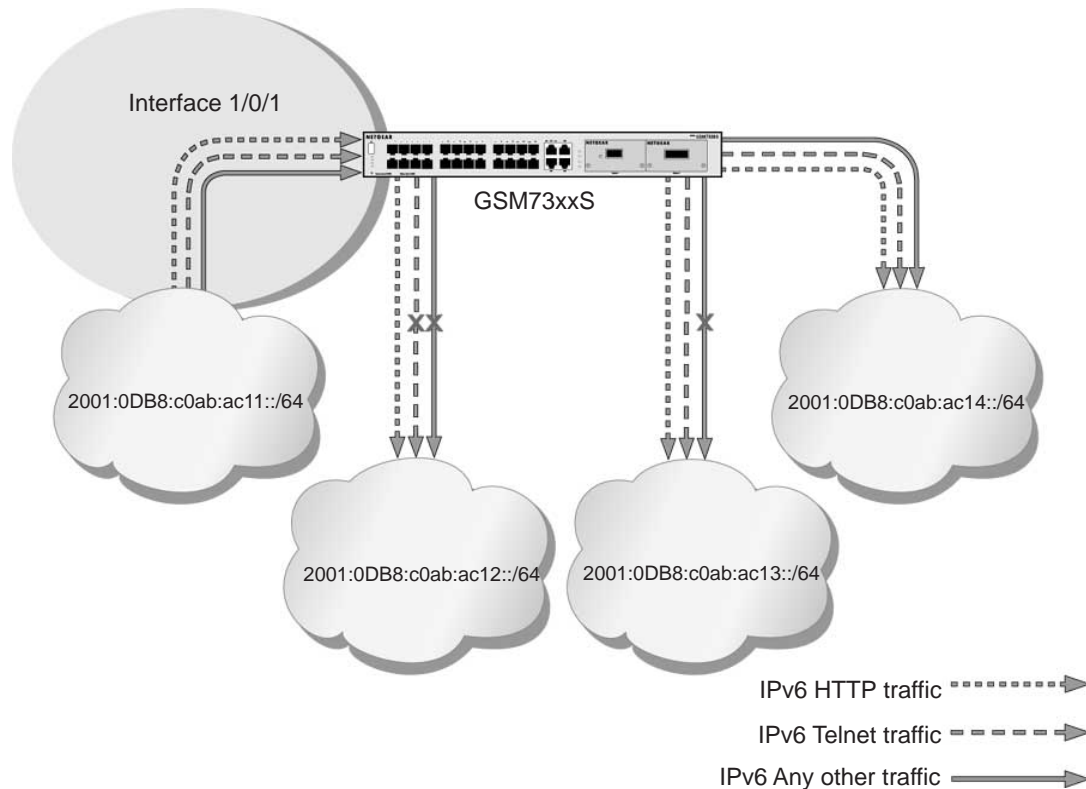


Figure 21. IPv6 ACLs

The script in this section shows you how to set up an IPv6 ACL with the following three rules:

- **Rule-1.** Permits every traffic to the destination network 2001:DB8:C0AB:AC14::/64.
- **Rule-2.** Permits IPv6 TELNET traffic to the destination network 2001:DB8:C0AB:AC13::/64.
- **Rule-3.** Permits IPv6 HTTP traffic to any destination.

CLI: Configure an IPv6 ACL

1. Create the access control list with the name `ipv6-acl`.

```
(Netgear Switch) (Config)# ipv6 access-list ipv6-acl
```

2. Define three rules to:

- Permit *any* IPv6 traffic to the destination network 2001:DB8:C0AB:AC14::/64 from the source network 2001:DB8:C0AB:AC11::/64.

- Permit IPv6 *Telnet* traffic to the destination network 2001:DB8:C0AB:AC13::/64 from the source network 2001:DB8:C0AB:AC11::/64.
- Permit IPv6 HTTP traffic to *any* destination network from the source network 2001:DB8:C0AB:AC11::/64.

```
(Netgear Switch) (Config-ipv6-acl)# permit ipv6 2001:DB8:C0AB:AC11::/64
2001:DB8:C0AB:AC14::/64
(Netgear Switch) (Config-ipv6-acl)# permit tcp 2001:DB8:C0AB:AC11::/64
2001:DB8:C0AB:AC13::/64 eq telnet
(Netgear Switch) (Config-ipv6-acl)# permit tcp 2001:DB8:C0AB:AC11::/64 any eq http
```

3. Apply the rules to inbound traffic on port 1/0/1. Only traffic matching the criteria will be accepted.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ipv6 traffic-filter ipv6-acl in
(Netgear Switch) (Interface 1/0/1)# exit
(Netgear Switch) (Config)#exit
```

4. View the configuration.

```
(Netgear Switch) #show ipv6 access-lists
Current number of all ACLs: 1 Maximum number of all ACLs: 100
IPv6 ACL Name          Rules  Direction  Interface(s)  VLAN(s)
-----
ipv6-acl                3     inbound    1/0/1
(Netgear Switch) #show ipv6 access-lists ipv6-acl

ACL Name: ipv6-acl
Inbound Interface(s): 1/0/1

Rule Number: 1
Action..... permit
Protocol..... 255(ipv6)
Source IP Address..... 2001:DB8:C0AB:AC11::/64
Destination IP Address..... 2001:DB8:C0AB:AC14::/64

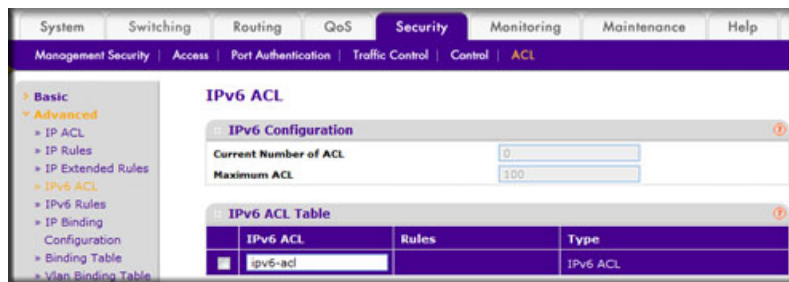
Rule Number: 2
Action..... permit
Protocol..... 6(tcp)
Source IP Address..... 2001:DB8:C0AB:AC11::/64
Destination IP Address..... 2001:DB8:C0AB:AC13::/64
Destination L4 Port Keyword..... 23(telnet)
```

```

Rule Number: 3
Action..... permit
Protocol..... 6(tcp)
Source IP Address..... 2001:DB8:C0AB:AC11::/64
Destination L4 Port Keyword..... 80(www/http)
    
```

Web Interface: Configure an IPv6 ACL

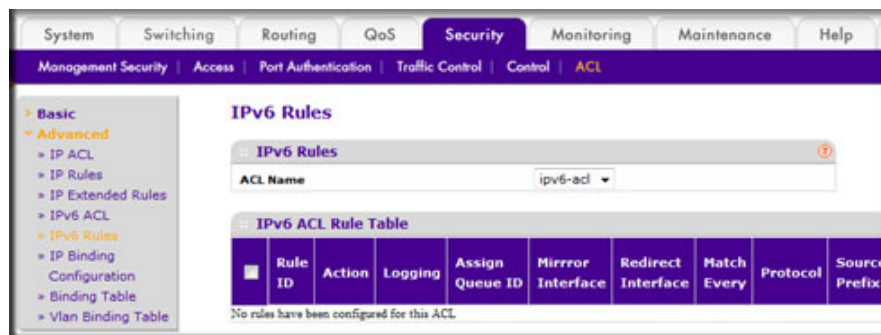
1. Create the access control list with the name ipv6-acl
 - a. Select **Security > ACL > Advanced > IPv6 ACL**.
 - b. In the IPv6 ACL Table, in the **IPv6 ACL** field, enter **ipv6-acl** . A screen similar to the following displays.



- c. Click **Add**. A screen similar to the following displays.



2. Define the first rule (1 of 3).
 - a. Select **Security > ACL > Advanced > IPv6 Rules**. A screen similar to the following displays.



- b. In the **ACL Name** list, select **ipv6-acl**.

- c. Click **Add**.
- d. In the **Rule ID** field, enter **1**.
- e. For Action, select the **Permit** radio button.
- f. In the **Source Prefix** field, enter **2001:DB8:C0AB:AC11::**.
- g. In the **Source Prefix Length** field, enter **64**.
- h. In the **Destination Prefix** field, enter **2001:DB8:C0AB:AC14::**.
- i. In the **Destination Prefix Length** field, enter **64**. A screen similar to the following displays.

The screenshot displays the 'IPv6 ACL Rule Configuration' page. The configuration is as follows:

Field	Value
ACL Name	ipv6-acl
Rule ID	1
Action	Permit
Egress Queue	(0-6)
Logging	Disable
Mirror Interface	(Empty)
Redirect Interface	(Empty)
Match Every	Disable
Protocol Type	Other
Source Prefix/PrefixLength	2001:DB8:C0AB:AC11:: 64
Source L4 Port	Other (0 to 65535)
Destination Prefix/PrefixLength	2001:DB8:C0AB:AC14:: 64
Destination L4 Port	Other (0 to 65535)
Flow Label	(0 to 1048575)
IP DSCP Service	(Empty)

- j. Click **Apply**.
3. Add Rule 2.
 - a. In the **Rule ID** field, enter **2**.
 - b. For Action, select the **Permit** radio button.
 - c. In the **Protocol Type** list, select **TCP**.
 - d. In the **Source Prefix** field, enter **2001:DB8:C0AB:AC11::**.
 - e. In the **Source Prefix Length** field, enter **64**.
 - f. In the **Destination Prefix** field, enter **2001:DB8:C0AB:AC13::**.
 - g. In the **Destination Prefix Length** field, enter **64**.

- h. In the **Destination L4 Port** list, select **telnet**. A screen similar to the following displays.

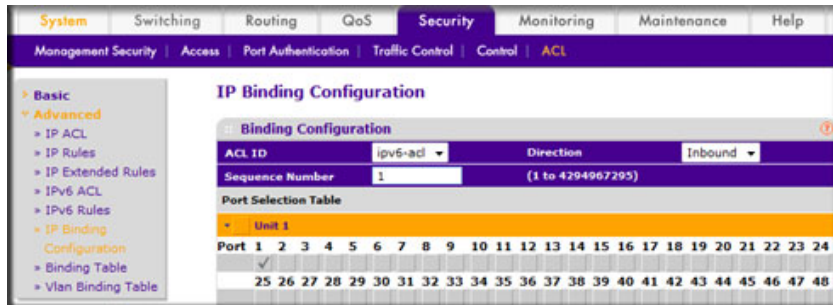
The screenshot shows the IPv6 ACL Rule Configuration page. The ACL Name is 'ipv6-acl' and the Rule ID is '2'. The Action is set to 'Permit'. The Protocol Type is 'TCP'. The Source Prefix/PrefixLength is '2001:DB8:C0AB:AC11::' with a length of '64'. The Destination Prefix/PrefixLength is '2001:DB8:C0AB:AC13::' with a length of '64'. The Destination L4 Port is set to 'telnet'. The Egress Queue is '(0-6)'. The Logging is set to 'Disable'. The Mirror Interface and Redirect Interface are both set to 'Disable'. The Match Every checkbox is checked. The IP DSCP Service is set to 'Other'.

- i. Click **Apply**.
4. Add Rule 3.
- In the **Rule ID** field, enter **3**.
 - For Action, select the **Permit** radio button.
 - In the **Protocol Type** list, select **TCP**.
 - In the **Source Prefix** field, enter **2001:DB8:C0AB:AC11::**.
 - In the **Source Prefix Length** field, enter **64**.
 - In the **Destination L4 Port** list, select **http**. A screen similar to the following displays.

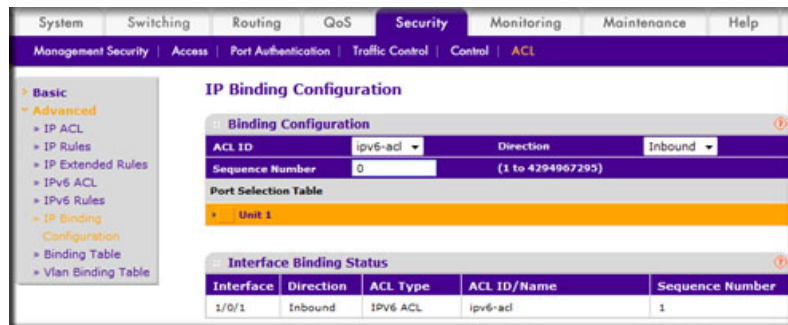
The screenshot shows the IPv6 ACL Rule Configuration page. The ACL Name is 'ipv6-acl' and the Rule ID is '3'. The Action is set to 'Permit'. The Protocol Type is 'TCP'. The Source Prefix/PrefixLength is '2001:DB8:C0AB:AC11::' with a length of '64'. The Source L4 Port is set to 'http'. The Destination Prefix/PrefixLength is '2001:DB8:C0AB:AC13::' with a length of '64'. The Destination L4 Port is set to 'Other'. The Egress Queue is '(0-6)'. The Logging is set to 'Disable'. The Mirror Interface and Redirect Interface are both set to 'Disable'. The Match Every checkbox is checked. The IP DSCP Service is set to 'Other'.

- g. Click **Apply**.
5. Apply the rules to inbound traffic on port 1/0/1. Only traffic matching the criteria will be accepted.
- Select **Security > ACL > Advanced > IP Binding Configuration**.

- b. In the **ACL ID** list, select **ipv6-acl**.
- c. In the **Sequence Number** list, select **1**.
- d. Click **Unit 1**.
- e. Select **Port 1**. A screen similar to the following displays.

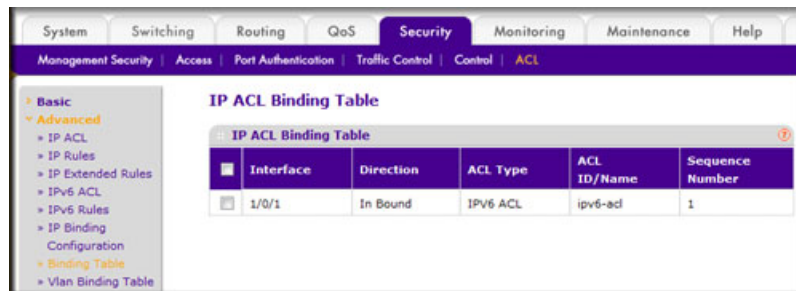


- f. Click **Apply**. A screen similar to the following displays.



6. View the binding table.

Select **Security > ACL > Advanced > Binding Table**. A screen similar to the following displays.



CoS Queuing

11

Class of Service Queuing

This chapter describes Class of Service (CoS) queue mapping, CoS Configuration, and traffic shaping features. This chapter provides the following examples:

- *Show classofservice Trust* on page 186
- *Set classofservice Trust Mode* on page 187
- *Show classofservice IP-Precedence Mapping* on page 188
- *Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode* on page 189
- *Set CoS Trust Mode for an Interface* on page 190
- *Configure Traffic Shaping* on page 191

Each port has one or more queues for packet transmission. During configuration, you can determine the mapping and configuration of these queues.

Based on the service rate and other criteria you configure, queues provide preference to specified packets. If a delay is necessary, the system holds packets until the scheduler authorizes transmission. As queues become full, packets are dropped. Packet drop precedence indicates the packet's sensitivity to being dropped during queue congestion.

Select per interface configuration scheme:

You can configure CoS mapping, queue parameters, and queue management are configurable per interface.

Queue management is configurable per interface.

Some hardware implementations allow queue depth management using tail dropping or weighted random early discard (WRED).

Some hardware implementations allow queue depth management using tail dropping.

The operation of CoS queuing involves queue mapping and queue configuration.

CoS Queue Mapping

CoS queue mapping uses trusted and untrusted ports.

Trusted Ports

- The system takes at face value certain priority designations for arriving packets.
- Trust applies only to packets that have that trust information.
- There can be only one trust field at a time - per port.
 - 802.1p user priority (This is the default trust mode and is managed through switching configuration.)
 - IP precedence
 - IP DiffServ Code Point (DSCP)

The system can assign the service level based upon the 802.1p priority field of the L2 header. You configure this by mapping the 802.1p priorities to one of three traffic class queues. These queues are:

- **Queue 2.** Minimum of 50 percent of available bandwidth
- **Queue 1.** Minimum of 33 percent of available bandwidth
- **Queue 0.** Lowest priority, minimum of 17 percent of available bandwidth

For untagged traffic, you can specify the default 802.1p priority on a per-port basis.

Untrusted Ports

- No incoming packet priority designation is trusted; therefore, the default priority value for the port is used.
- All ingress packets from untrusted ports, where the packet is classified by an ACL or a DiffServ policy, are directed to specific CoS queues on the appropriate egress port. That specific CoS queue is determined by either the default priority of the port or a DiffServ or ACL-assigned queue attribute.
- Used when trusted port mapping is unable to be honored - for instance, when a non-IP DSCP packet arrives at a port configured to trust IP DSCP.

CoS Queue Configuration

CoS queue configuration involves port egress queue configuration and drop precedence configuration (per queue). The design of these on a per-queue, per-drop precedence basis allows you to create the service characteristics that you want for different types of traffic.

Port egress queue configuration:

- Scheduler type, strict vs. weighted
- Minimum guaranteed bandwidth
- Maximum allowed bandwidth per-queue shaping
- Queue management type, tail drop vs. WRED

Drop precedence configuration (per queue):

- WRED parameters
 - Minimum threshold
 - Maximum threshold
 - Drop probability
 - Scale factor
- Tail drop parameters, threshold

Per-interface basis:

- Queue management type, tail Drop vs. WRED

Only if per-queue configuration is not supported

- WRED decay exponent
- Traffic shaping for an entire interface

Show classofservice Trust

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

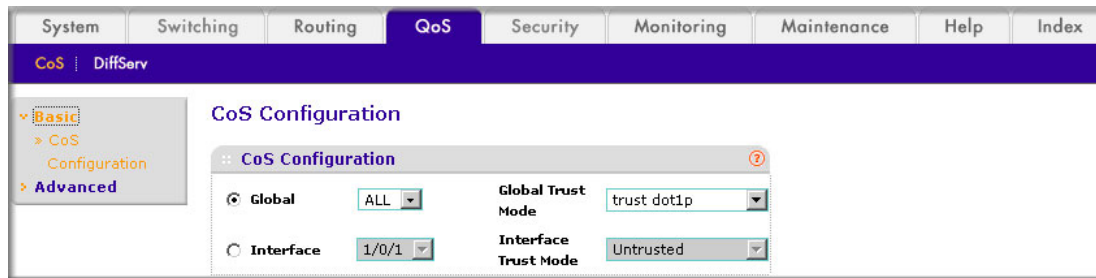
CLI: Show classofservice Trust

To use the CLI to show CoS trust mode, use these commands:

```
(Netgear Switch) #show classofservice trust?
<cr> Press Enter to execute the command.
(Netgear Switch) #show classofservice trust
Class of Service Trust Mode: Dot1P
```

Web Interface: Show classofservice Trust

Select **QoS > CoS > Basic > CoS Configuration**. A screen similar to the following displays.



Set classofservice Trust Mode

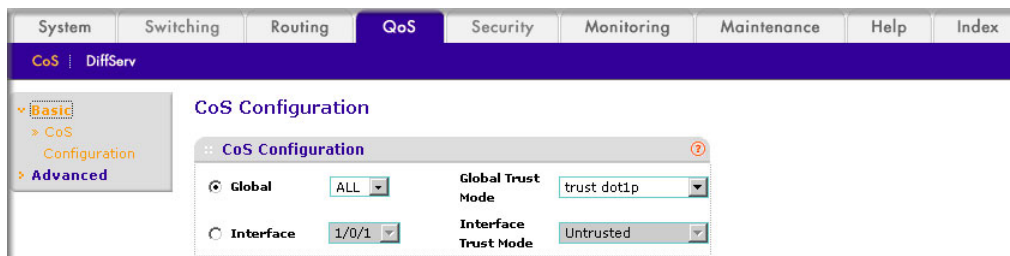
The example is shown as CLI commands and as a Web interface procedure.

CLI: Set classofservice Trust Mode

```
(Netgear Switch) (Config)#classofservice?
dot1p-mapping      Configure dot1p priority mapping.
ip-dscp-mapping   Maps an IP DSCP value to an internal traffic class.
trust              Sets the Class of Service Trust Mode of an Interface.
(Netgear Switch) (Config)#classofservice trust?
dot1p              Sets the Class of Service Trust Mode of an Interface
                  to 802.1p.
ip-dscp            Sets the Class of Service Trust Mode of an Interface
                  to IP DSCP.
(Netgear Switch) (Config)#classofservice trust dot1p?
<cr>              Press Enter to execute the command.
(Netgear Switch) (Config)#classofservice trust dot1p
```

Web Interface: Set classofservice Trust Mode

1. Select **QoS > CoS > Basic > CoS Configuration**. A screen similar to the following displays.



2. Select the **Global** radio button.
3. In the **Global Trust Mode** list, select **trust dot1p**.
4. Click **Apply** to save the settings.

Show classofservice IP-Precedence Mapping

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

CLI: Show classofservice IP-Precedence Mapping

```
(Netgear Switch) #show classofservice ip-precedence-mapping
```

IP Precedence	Traffic Class
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

Web Interface: Show classofservice ip-precedence Mapping

1. Select **QoS > CoS > Advanced > IP Precedence Queue Mapping**. A screen similar to the following displays.

IP Precedence	0	1	2	3	4	5	6	7
Queue	1	0	0	1	2	2	3	3

2. In the Interface list, select **All**.
The global IP precedence to queue mapping is displayed.
3. In the **Interface** list, select the specific interface (such as **1/0/1**).

The IP precedence to queue mapping of the interface is displayed.

Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode

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

CLI: Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode

```
(Netgear Switch) (Config)#cos-queue min-bandwidth?
<bw-0>                Enter the minimum bandwidth percentage for Queue 0.
(Netgear Switch) (Config)#cos-queue min-bandwidth 15
Incorrect input! Use 'cos-queue min-bandwidth <bw-0>..<bw-7>'.
(Netgear Switch) (Config)#cos-queue min-bandwidth 15 25 10 5 5 20 10 10
(Netgear Switch) (Config)#cos-queue strict?
<queue-id>           Enter a Queue Id from 0 to 7.
(Netgear Switch) (Config)#cos-queue strict 1?
<cr>                 Press Enter to execute the command.
<queue-id>           Enter an additional Queue Id from 0 to 7.
(Netgear Switch) (Config)#cos-queue strict 1
```

Web Interface: Configure CoS-queue Min-bandwidth and Strict Priority Scheduler Mode

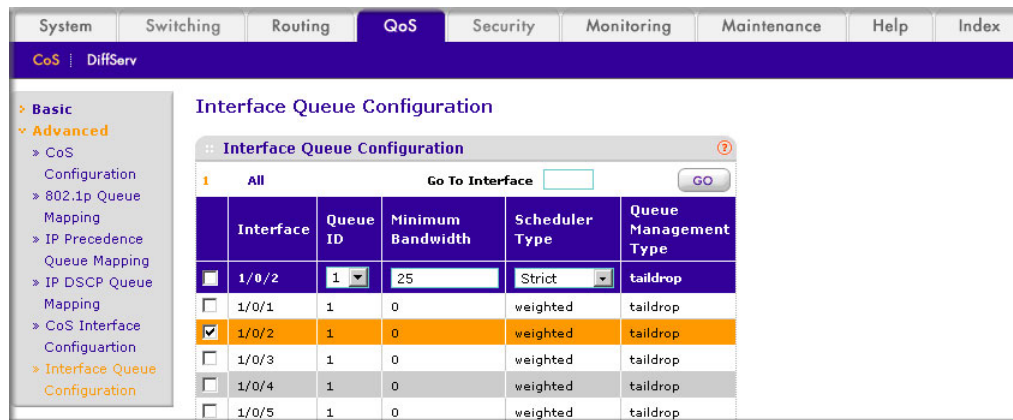
1. For Interface 1/0/2, set the minimum bandwidth to 15 for queue 0.
 - a. Select **QoS > CoS > Advanced > Interface Queue Configuration**. A screen similar to the following displays.

The screenshot shows the 'Interface Queue Configuration' page in the web interface. The page is under the 'QoS' tab and shows a table of queue configurations for various interfaces. The interface 1/0/2 is selected, and queue 0 is highlighted with a minimum bandwidth of 15.

Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
<input type="checkbox"/> 1/0/1	0	0	weighted	taildrop
<input checked="" type="checkbox"/> 1/0/2	0	15	weighted	taildrop
<input type="checkbox"/> 1/0/3	0	0	weighted	taildrop
<input type="checkbox"/> 1/0/4	0	0	weighted	taildrop
<input type="checkbox"/> 1/0/5	0	0	weighted	taildrop

- b. In the **Queue ID** list, select **0**.

- c. Under Interface Queue Configuration, scroll down and select the interface **1/0/2** check box. Now 1/0/2 appears in the Interface field at the top.
 - d. Enter the following information:
 - In the **Minimum Bandwidth** field, enter **15**.
 - In the **Scheduler Type** list, select **Weighted**.
 - e. Click **Apply** to save the settings.
2. For interface 1/0/2, set the minimum bandwidth 25 for queue 1, and set the scheduler type to strict.
 - a. Select **QoS > CoS > Advanced > Interface Queue Configuration**. A screen similar to the following displays.



- b. In the **Queue ID** list, select **1**.
- c. Under Interface Queue Configuration, scroll down and select the interface **1/0/2** check box. Now 1/0/2 appears in the Interface field at the top.
- d. Enter the following information:
 - In the **Minimum Bandwidth** field, enter **25**.
 - In the **Scheduler Type** list, select **Strict**.
- e. Click **Apply** to save the settings.

Set CoS Trust Mode for an Interface

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

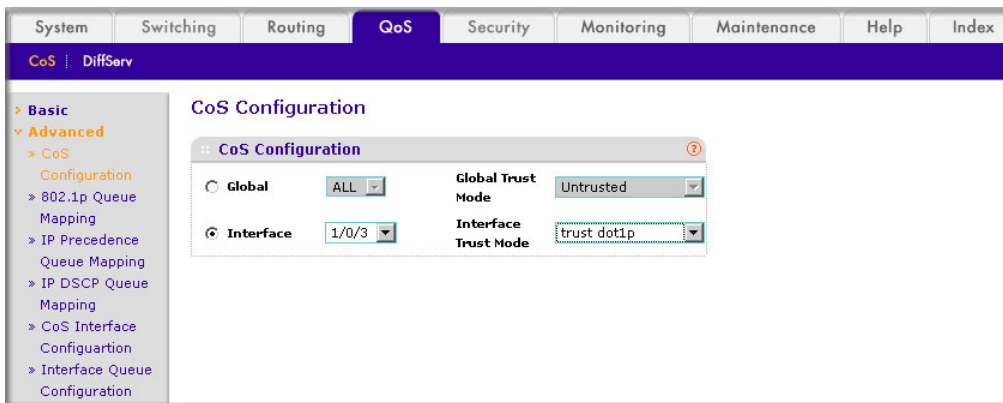
CLI: Set CoS Trust Mode for an Interface

```
(Netgear Switch) (Interface 1/0/3)#classofservice trust?
dot1p                Sets the Class of Service Trust Mode of an Interface
                     to 802.1p.
ip-dscp              Sets the Class of Service Trust Mode of an Interface
                     to IP DSCP.
(Netgear Switch) (Interface 1/0/3)#classofservice trust dot1p?
<cr>                Press Enter to execute the command.
(Netgear Switch) (Interface 1/0/3)#classofservice trust dot1p
```

Note: The traffic class value range is 0–6 instead of 0–7 because queue 7 is reserved in a stacking build for stack control, and therefore you cannot configure it.

Web Interface: Set CoS Trust Mode for an Interface

1. Select **QoS > CoS > Advanced > CoS Configuration**. A screen similar to the following displays.



2. Under CoS Configuration, select the **Interface** radio button.
3. In the **Interface** list, select **1/0/3**.
4. In the **Interface Trust Mode** list, select **trust dot1p**.
5. Click **Apply** to save the settings.

Configure Traffic Shaping

Traffic shaping controls the amount and volume of traffic transmitted through a network. This has the effect of smoothing temporary traffic bursts over time. Use the traffic-shape

command to enable traffic shaping by specifying the maximum transmission bandwidth limit for all interfaces (Global Config) or for a single interface (Interface Config).

The <bw> value is a percentage that ranges from 0 to 100 in increments of 5. The default bandwidth value is 0, meaning no upper limit is enforced, which allows the interface to transmit up to its maximum line rate.

The bw value is independent of any per-queue maximum bandwidth values in effect for the interface and should be considered as a second-level transmission rate control mechanism that regulates the output of the entire interface regardless of which queues originate the outbound traffic.

CLI: Configure traffic-shape

```
(Netgear Switch) (Config)#traffic-shape?
<bw>                               Enter the shaping bandwidth percentage from 0 to 100
                                   in increments of 5.
(Netgear Switch) (Config)#traffic-shape 70?
<cr>                               Press Enter to execute the command.
(Netgear Switch) (Config)#traffic-shape 70
(Netgear Switch) (Config)#
```

Web Interface: Configure Traffic Shaping

1. Set the shaping bandwidth percentage to 70 percent.
 - a. Select **QoS > CoS > Advanced > CoS Interface Configuration**. A screen similar to the following displays.

The screenshot shows the web interface for configuring CoS. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The main content area is titled 'CoS Interface Configuration' and contains a table with the following data:

Interface	Interface Trust Mode	Interface Shaping Rate (0 to 100)
<input checked="" type="checkbox"/> 1/0/3	Dot1p	70
<input type="checkbox"/> 1/0/1	Dot1p	0
<input type="checkbox"/> 1/0/2	Dot1p	0
<input type="checkbox"/> 1/0/4	Dot1p	0
<input type="checkbox"/> 1/0/5	Dot1p	0

- b. Under CoS Interface Configuration, scroll down and select the interface **1/0/3** check box. Now 1/0/3 appears in the Interface field at the top.
 - c. In the **Interface Shaping Rate (0 to 100)** field, enter **70**.
 - d. Click **Apply** to save the settings.

Differentiated Services

This chapter provides the following examples:

- *DiffServ* on page 194
- *DiffServ for VoIP* on page 210
- *Auto VoIP* on page 217
- *DiffServ for IPv6* on page 221
- *Color Conform Policy* on page 228

Differentiated services (DiffServ) is one technique for implementing Quality of Service (QoS) policies. Using DiffServ in your network allows you to directly configure the relevant parameters on the switches and routers rather than using a resource reservation protocol. This section explains how to configure the 7000 Series Managed Switch to identify which traffic class a packet belongs to, and how it should be handled to provide the quality of service you want. As implemented on the 7000 Series Managed Switch, DiffServ allows you to control what traffic is accepted and what traffic is discarded.

How you configure DiffServ support on a 7000 Series Managed Switch varies depending on the role of the switch in your network:

- **Edge device.** An edge device handles ingress traffic, flowing toward the core of the network, and egress traffic, flowing away from the core. An edge device segregates inbound traffic into a small set of traffic classes, and is responsible for determining a packet's classification. Classification is based primarily on the contents of the Layer 3 and Layer 4 headers, and is recorded in the Differentiated Services Code Point (DSCP) added to a packet's IP header.
- **Interior node.** A switch in the core of the network is responsible for forwarding packets, rather than for classifying them. It decodes the DSCP code point in an incoming packet, and provides buffering and forwarding services using the appropriate queue management algorithms.

Before configuring DiffServ on a particular 7000 Series Managed Switch, you must determine the QoS requirements for the network as a whole. The requirements are expressed in terms of rules, which are used to classify inbound traffic on a particular interface. The switch software does not support DiffServ in the outbound direction.

Rules are defined in terms of classes, policies, and services:

- **Class.** A class consists of a set of rules that identify which packets belong to the class. Inbound traffic is separated into traffic classes based on Layer 3 and Layer 4 header data and the VLAN ID, and marked with a corresponding DSCP value. One type of class is supported: All, which specifies that every match criterion defined for the class must be true for a match to occur.
- **Policy.** Defines the QoS attributes for one or more traffic classes. An example of an attribute is the ability to mark a packet at ingress. The 7000 Series Managed Switch supports a traffic conditions policy. This type of policy is associated with an inbound traffic class and specifies the actions to be performed on packets meeting the class rules:
 - Marking the packet with a given DSCP code point, IP precedence, or CoS
 - Policing packets by dropping or re-marking those that exceed the class's assigned data rate
 - Counting the traffic within the class
- **Service.** Assigns a policy to an interface for inbound traffic.

DiffServ

This example shows how a network administrator can provide equal access to the Internet (or other external network) to different departments within a company. Each of four departments has its own Class B subnet that is allocated 25 percent of the available bandwidth on the port accessing the Internet.

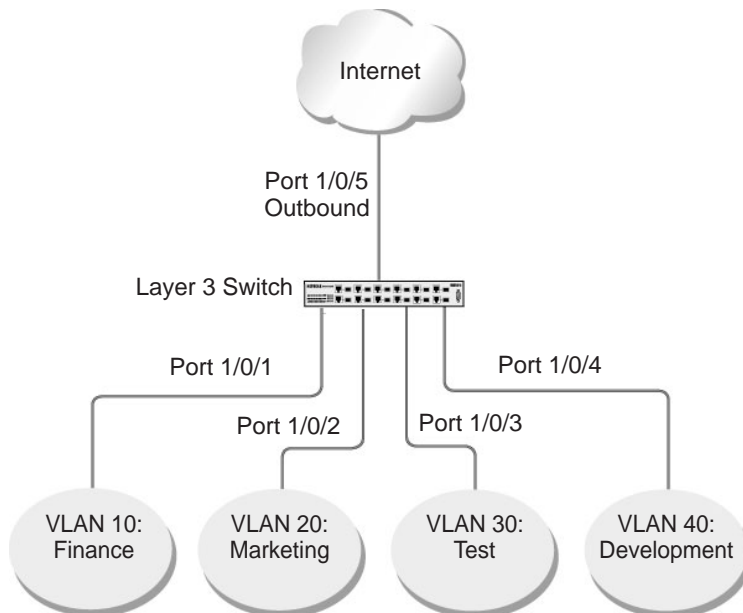


Figure 22. Class B subnet with differentiated services

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

CLI: Configure DiffServ

1. Ensure that the DiffServ operation is enabled for the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#diffserv
```

2. Create a DiffServ class of type all for each of the departments, and name them. Define the match criteria of source IP address for the new classes.

```
(Netgear Switch) (Config)#class-map match-all finance_dept
(Netgear Switch) (Config class-map)#match srcip 172.16.10.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit

(Netgear Switch) (Config)#class-map match-all marketing_dept
(Netgear Switch) (Config class-map)#match srcip 172.16.20.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit

(Netgear Switch) (Config)#class-map match-all test_dept
(Netgear Switch) (Config class-map)#match srcip 172.16.30.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit

(Netgear Switch) (Config)#class-map match-all development_dept
(Netgear Switch) (Config class-map)#match srcip 172.16.40.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit
```

3. Create a DiffServ policy for inbound traffic named 'internet_access', adding the previously created department classes as instances within this policy.

This policy uses the assign-queue attribute to put each department's traffic on a different egress queue. This is how the DiffServ inbound policy connects to the CoS queue settings established in the following example.

```
(Netgear Switch) (Config)#policy-map internet_access in
(Netgear Switch) (Config policy-map)#class finance_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 1
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class marketing_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 2
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class test_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 3
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class development_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 4
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#exit
```

4. Attach the defined policy to interfaces 1/0/1 through 1/0/4 in the inbound direction.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/1)#exit

(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/2)#exit

(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/3)#exit

(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/4)#exit
```

5. Set the CoS queue configuration for the (presumed) egress interface 1/0/5 such that each of queues 1, 2, 3, and 4 gets a minimum guaranteed bandwidth of 25 percent. All queues for this interface use weighted round robin scheduling by default. The DiffServ inbound policy designates that these queues are to be used for the departmental traffic through the

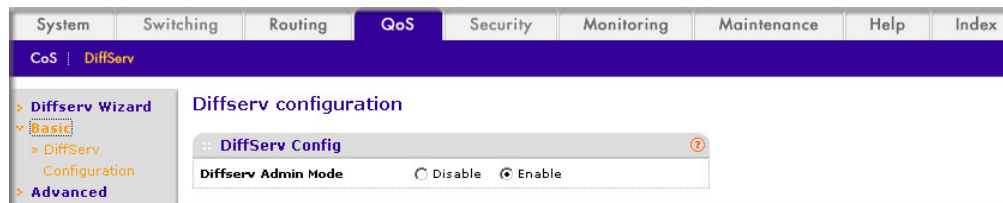
assign-queue attribute. It is presumed that the switch will forward this traffic to interface 1/0/5 based on a normal destination address lookup for Internet traffic.

```
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#cos-queue min-bandwidth 0 25 25 25 25 0 0 0
(Netgear Switch) (Interface 1/0/5)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Configure DiffServ

1. Enable Diffserv.

- a. Select **QoS > DiffServ > Basic > DiffServ Configuration**. A screen similar to the following displays.

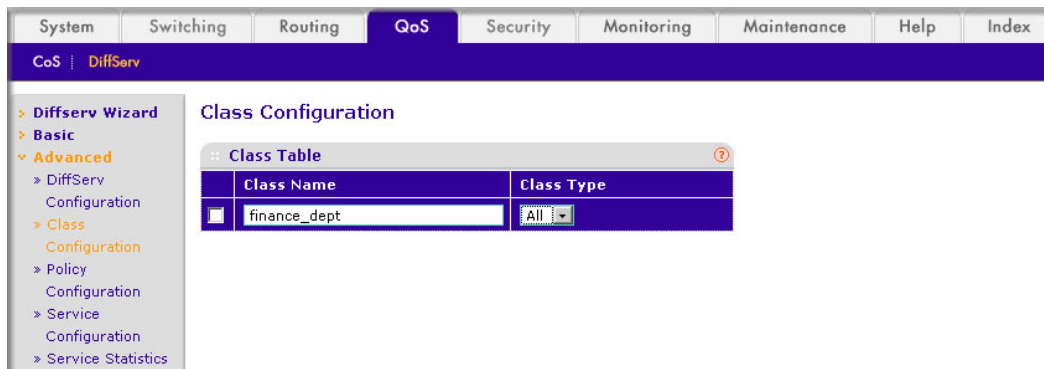


- b. For Diffserv Admin Mode, select the **Enable** radio button.

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

2. Create the class finance_dept.

- a. Select **QoS > DiffServ > Advanced > Class Configuration**. A screen similar to the following displays.



- b. Enter the following information:

- In the **Class Name** field, enter **finance_dept**.
- In the **Class Type** list, select **All**.

- c. Click **Add** to create a new class finance_dept.

- d. Click the **finance_dept** to configure this class.

The screenshot shows the DiffServ Class Configuration page for the **finance_dept** class. The page is divided into two main sections: **Class Information** and **Diffserv Class Configuration**.

Class Information:

- Class Name:
- Class Type:

Diffserv Class Configuration:

- Match Every:
- Reference Class:
- Class of Service:
- VLAN: (1 - 4093)
- Ethernet Type: (0600 - FFFF)
- Source MAC:
- Source MAC Mask:
- Destination MAC:
- Destination MAC Mask:
- Protocol Type: (0 - 255)
- Source IP Address:
- Source Mask:
- Source L4 Port: (0 - 65535)
- Destination IP Address:

- e. Under Diffserv Class Configuration, enter the following information:

- In the **Source IP Address** field, enter **172.16.10.0**.
- In the **Source Mask** field, enter **255.255.255.0**.

- f. Click **Apply**.

3. Create the class **marketing_dept**:

- a. Select **QoS > DiffServ > Advanced > Class Configuration**. A screen similar to the following displays.

The screenshot shows the Class Configuration page. The page is divided into two main sections: **Class Information** and **Class Table**.

Class Table:

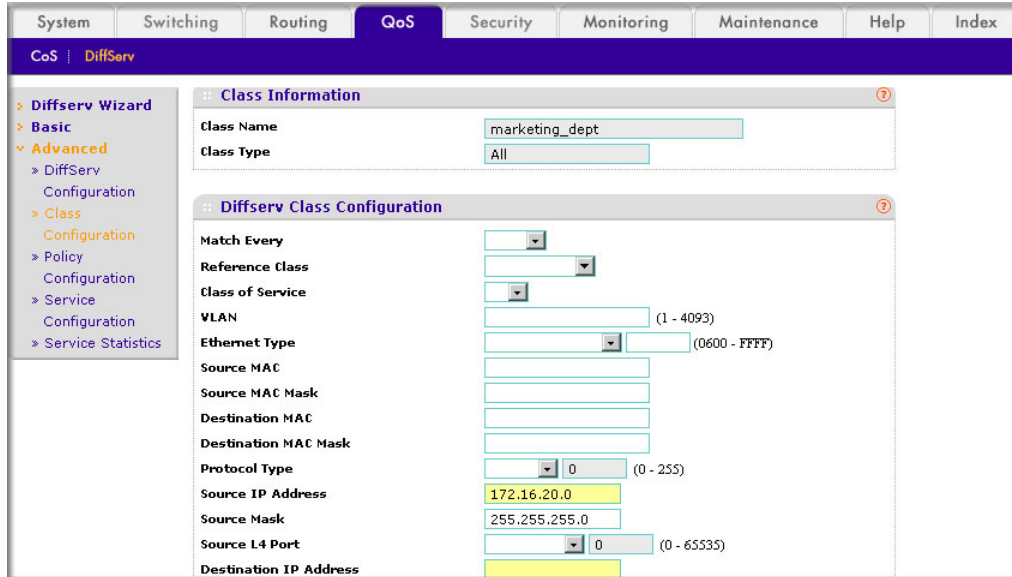
Class Name	Class Type
<input type="checkbox"/> marketing_dept	All
<input type="checkbox"/> finance_dept	All

- b. Enter the following information:

- In the **Class Name** field, enter **marketing_dept**.
- In the **Class Type** list, select **All**.

- c. Click **Add** to create a new class **marketing_dept**.

d. Click **marketing_dept** to configure this class.



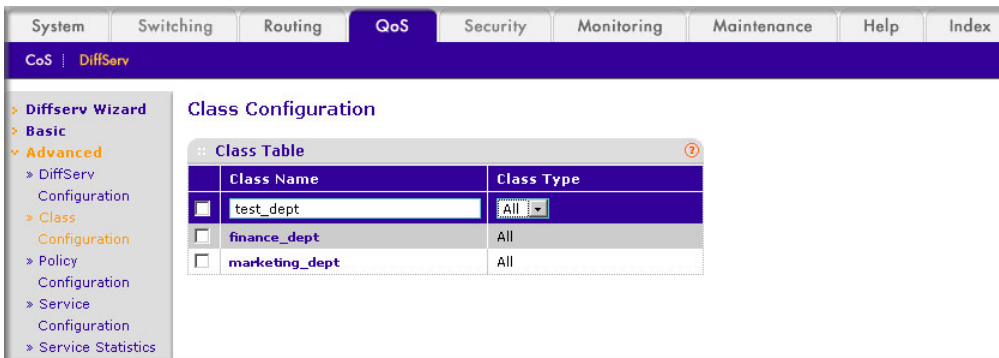
e. Under Diffserv Class Configuration, enter the following information:

- In the **Source IP Address** field, enter **172.16.20.0**.
- In the **Source Mask** field, enter **255.255.255.0**.

f. Click **Apply**.

4. Create the class test_dept:

a. Select **QoS > DiffServ > Advanced > Class Configuration**. A screen similar to the following displays.



b. Enter the following information:

- In the **Class Name** field, enter **test_dept**.
- In the **Class Type** list, select **All**.

c. Click **Add** to create a new class test_dept.

- d. Click **test_dept** to configure this class.

System Switching Routing **QoS** Security Monitoring Maintenance Help Index

CoS | DiffServ

DiffServ Wizard
 Basic
 Advanced
 DiffServ Configuration
 Class Configuration
 Policy Configuration
 Service Configuration
 Service Statistics

Class Information

Class Name: test_dept
 Class Type: All

DiffServ Class Configuration

Match Every: [Dropdown]
 Reference Class: [Dropdown]
 Class of Service: [Dropdown]
 VLAN: [Text] (1 - 4093)
 Ethernet Type: [Dropdown] [Text] (0600 - FFFF)
 Source MAC: [Text]
 Source MAC Mask: [Text]
 Destination MAC: [Text]
 Destination MAC Mask: [Text]
 Protocol Type: [Dropdown] [Text] (0 - 255)
 Source IP Address: 172.16.30.0
 Source Mask: 255.255.255.0
 Source L4 Port: [Dropdown] [Text] (0 - 65535)
 Destination IP Address: [Text]

- e. Under Diffserv Class Configuration, enter the following information:

- In the **Source IP Address** field, enter **172.16.30.0**.
- In the **Source Mask** field, enter **255.255.255.0**.

- f. Click **Apply**.

5. Create class development_dept.

- a. Select **QoS > DiffServ > Advanced > Class Configuration**. A screen similar to the following displays.

System Switching Routing **QoS** Security Monitoring Maintenance Help Index

CoS | DiffServ

DiffServ Wizard
 Basic
 Advanced
 DiffServ Configuration
 Class Configuration
 Policy Configuration
 Service Configuration
 Service Statistics

Class Configuration

Class Table

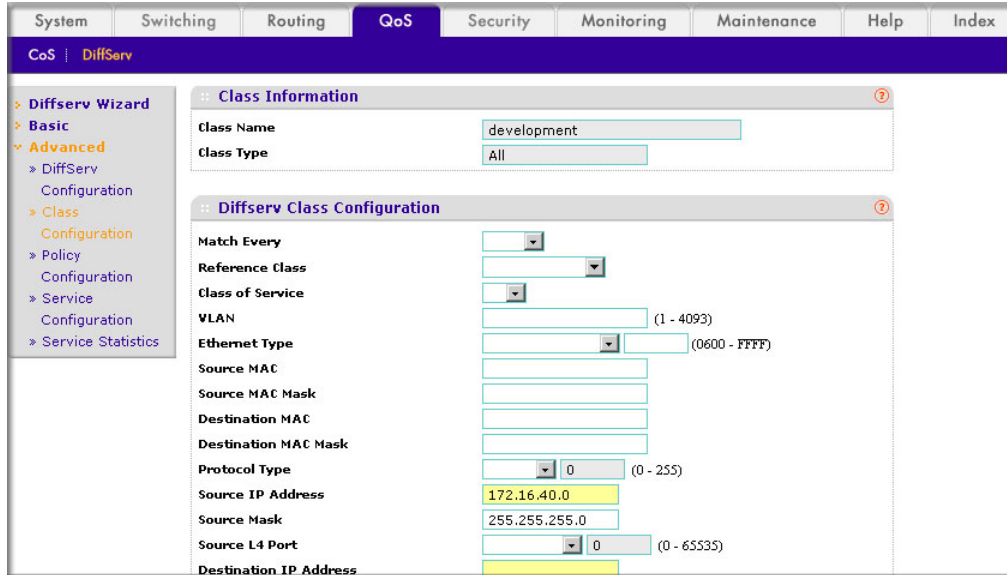
Class Name	Class Type
<input checked="" type="checkbox"/> development	All
<input type="checkbox"/> finance_dept	All
<input type="checkbox"/> marketing_dept	All
<input type="checkbox"/> test_dept	All

- b. Enter the following information:

- In the **Class Name** field, enter **development_dept**.
- In the **Class Type** list, select **All**.

- c. Click the **Add** to create a new class development_dept.

d. Click **development_dept** to configure this class.



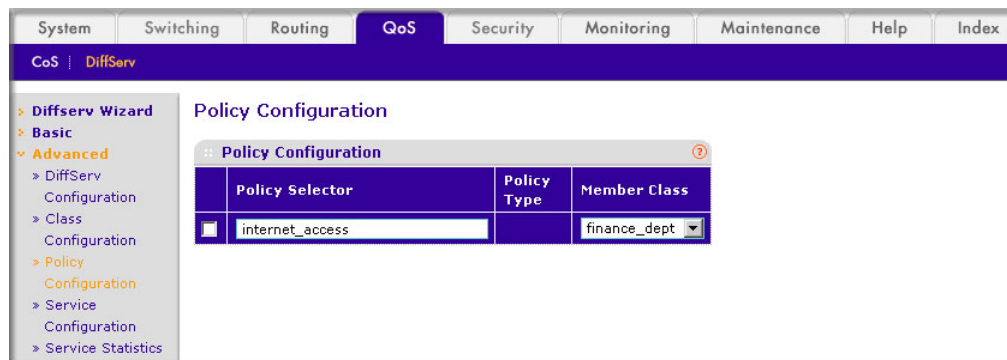
e. Under Diffserv Class Configuration, enter the following information:

- In the **Source IP Address** field, enter **172.16.40.0**.
- In the **Source Mask** field, enter **255.255.255.0**.

f. Click **Apply**.

6. Create a policy named internet_access and add the class finance_dept to it.

a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.



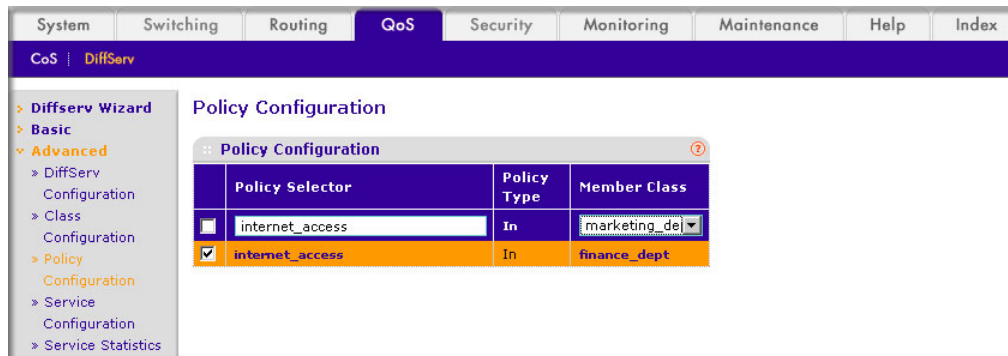
b. Enter the following information:

- In the **Policy Selector** field, enter **internet_access**.
- In the **Member Class** list, select the **finance_dept**.

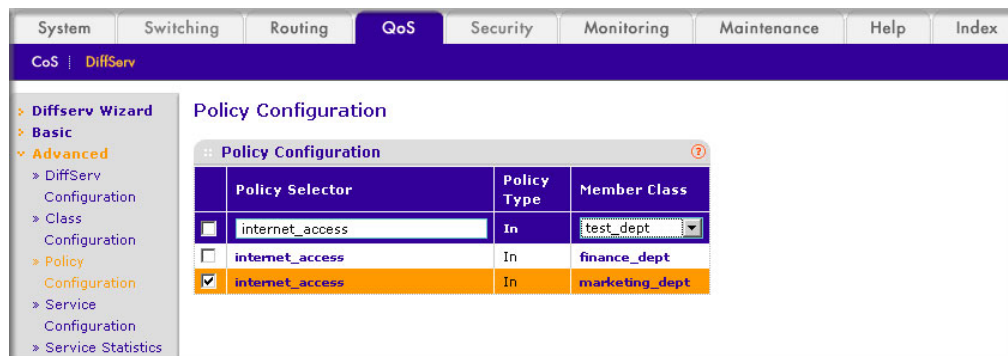
c. Click **Add** to create a new policy internet_access.

7. Add the class marketing_dept into the policy internet_access.

- a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.

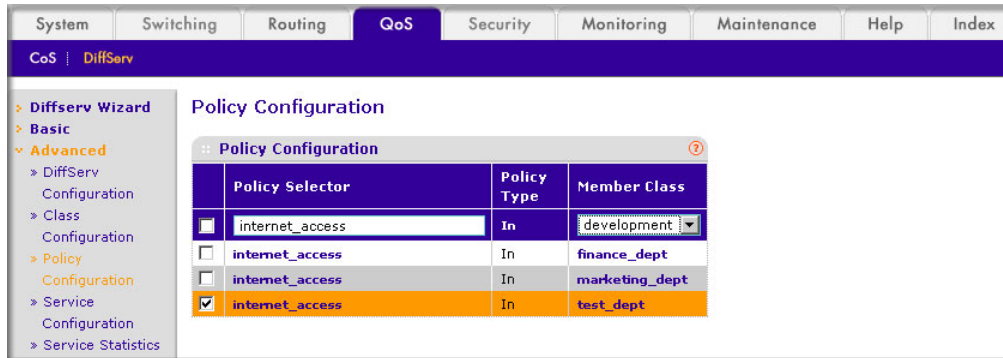


- b. Under Policy Configuration, scroll down and select the **internet_access** check box. internet_access now appears in the Policy Selector field at the top.
- c. In the **Member Class** list, select **marketing_dept**.
- d. Click **Apply** to add the class marketing_dept to the policy internet_access.
8. Add the class test_dept into the policy internet_access.
- a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.



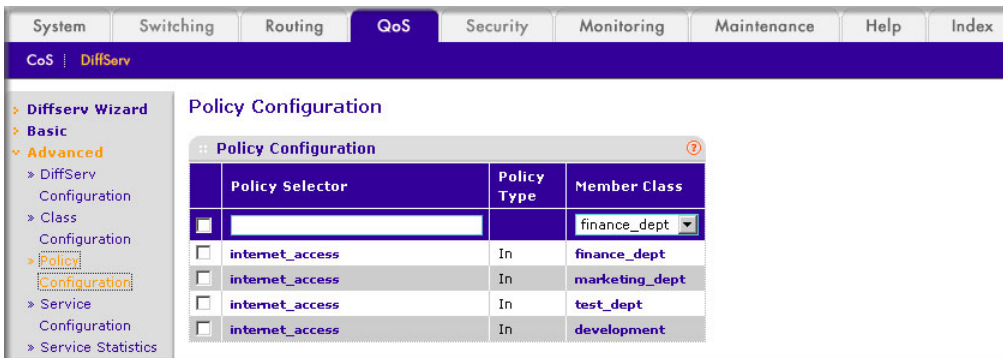
- b. Under Policy Configuration, scroll down and select the **internet_access** check box. Internet_access now appears in the Policy Selector field at the top.
- c. In the **Member Class** list, select **test_dept**.
- d. Click **Apply** to add the class test_dept to the policy internet_access.
9. Add the class development_dept into the policy internet_access.

- a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.

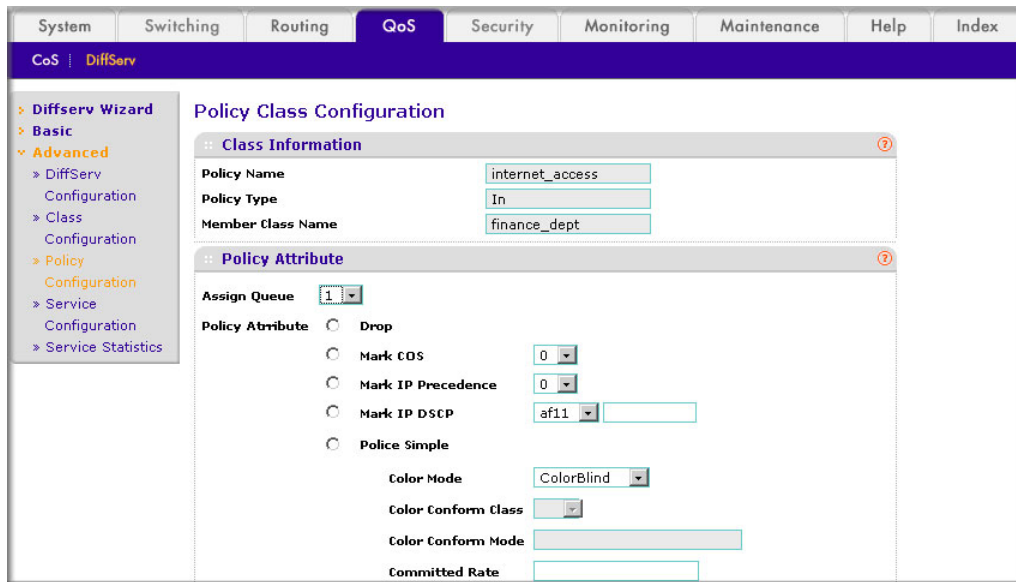


- b. Under Policy Configuration, scroll down and select the **internet_access** check box. Now internet_access appears in the Policy Selector field at the top.
 - c. In the **Member Class** list, select **development_dept**.
 - d. Click **Apply** to add the class development_dept to the policy internet_access.
10. Assign queue 1 to finance_dept.

- a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.



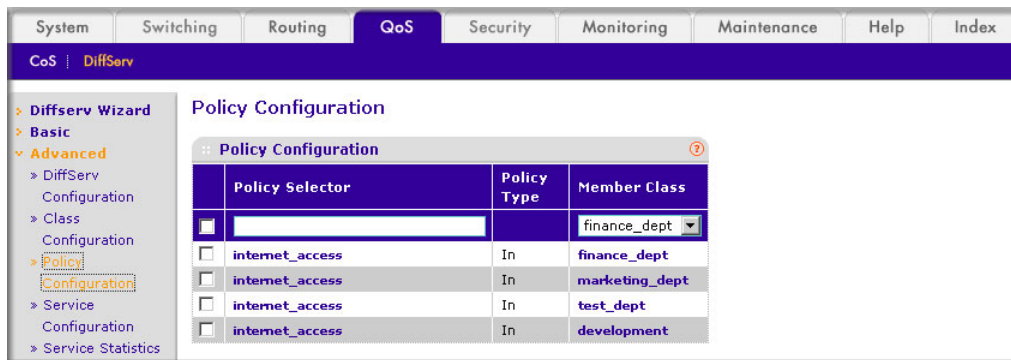
- b. Click the **internet_access** check box for the member class `finance_dept`. A screen similar to the following displays.



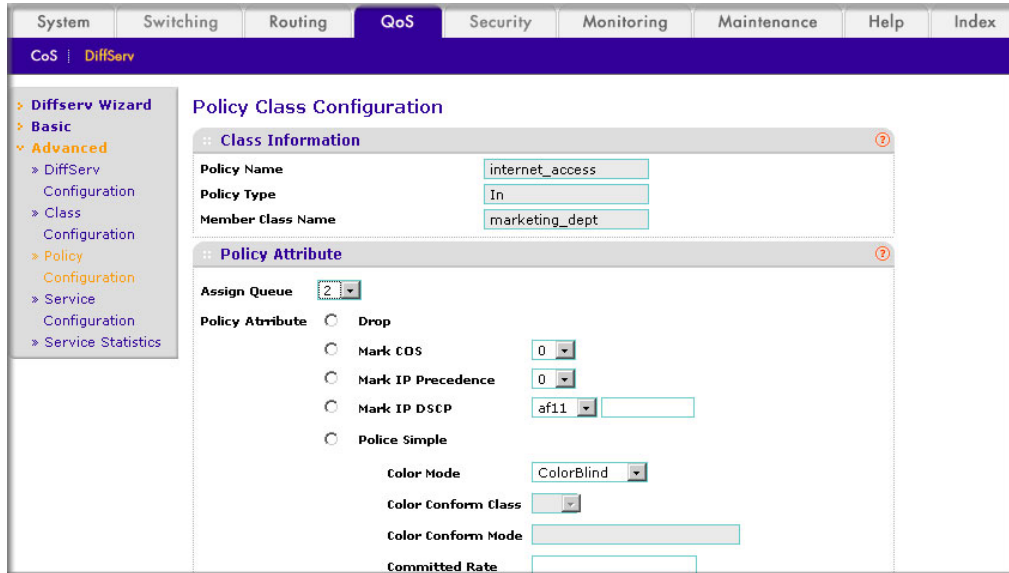
- c. In the **Assign Queue** list, select **1**.
- d. Click **Apply**.

11. Assign queue 2 to `marketing_dept`.

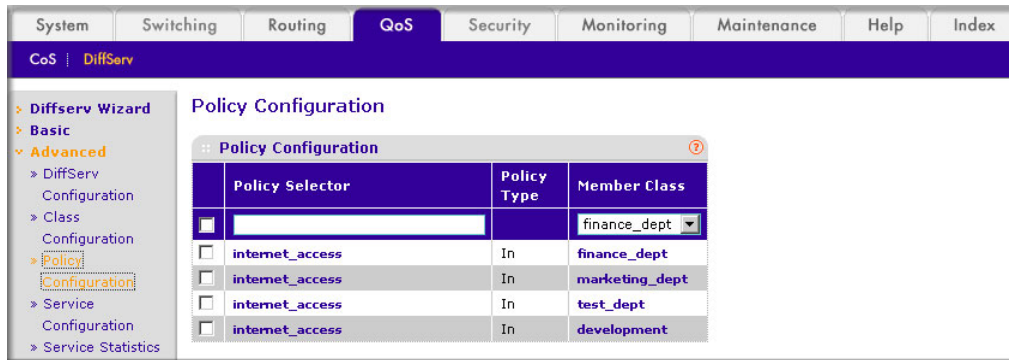
- a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.



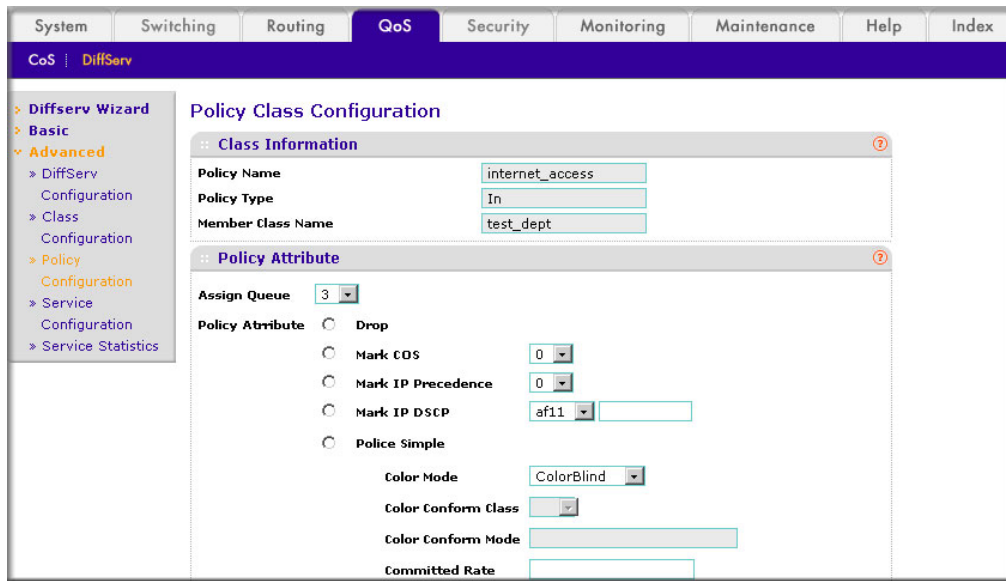
- b. Click the **internet_access** check box for marketing_dept. A screen similar to the following displays.



- c. In the **Assign Queue** list, select 2.
 - d. Click **Apply**.
12. Assign queue 3 to test_dept.
- a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.



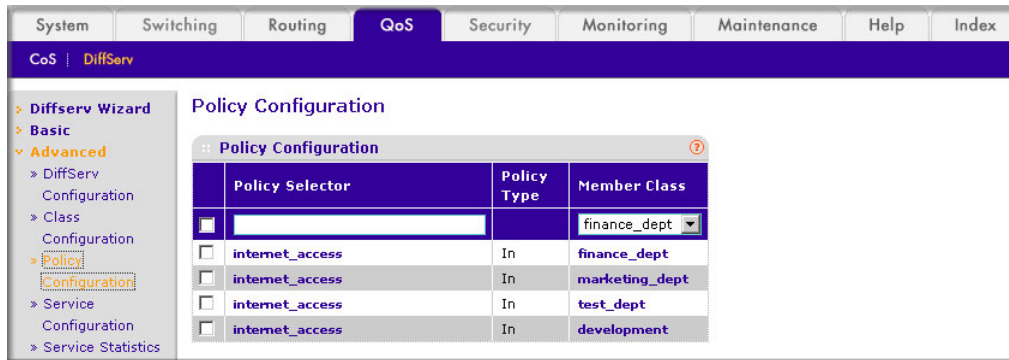
- b. Click the **internet_access** check mark for test_dept. A screen similar to the following displays.



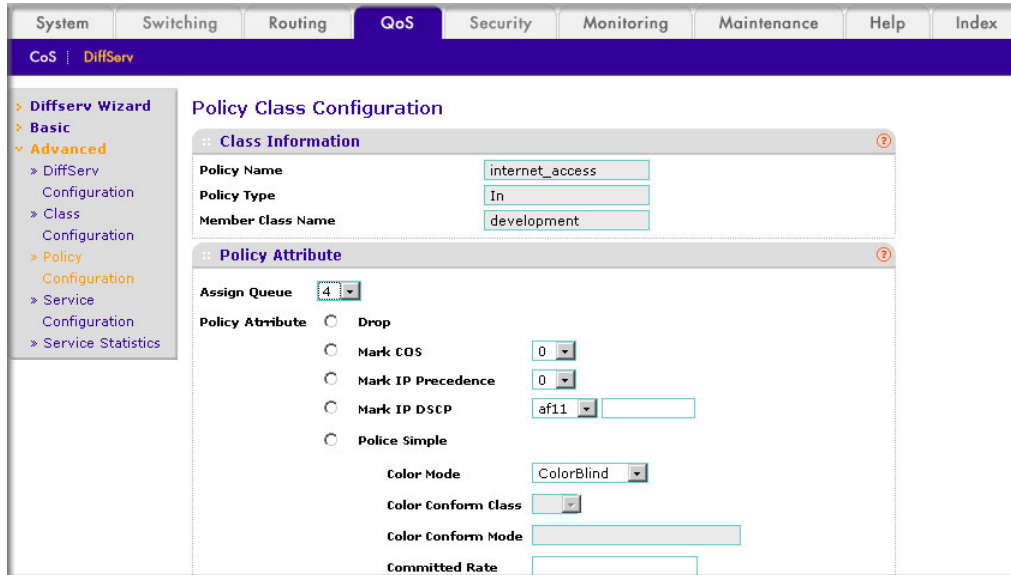
- c. In the **Assign Queue** list, select 3.
- d. Click **Apply**.

13. Assign queue 4 to development_dept.

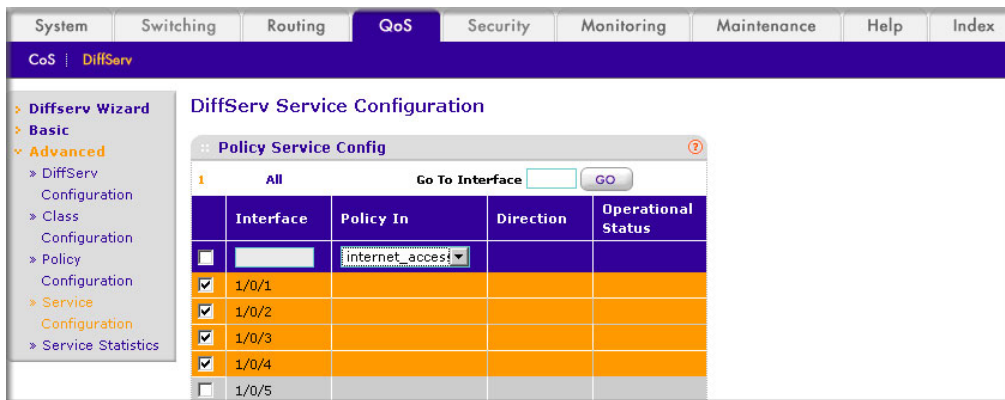
- a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.



- b. Click the **internet_access** check mark for development_dept. A screen similar to the following displays.



- c. In the **Assign Queue** list, select **4**.
- d. Click **Apply**.
14. Attach the defined policy to interfaces 1/0/1 through 1/0/4 in the inbound direction.
- a. Select **QoS > DiffServ > Advanced > Service Configuration**. A screen similar to the following displays.



- b. Scroll down and select the check boxes for interfaces **1/0/1**, **1/0/2**, **1/0/3**, and **1/0/4**.
- c. In the **Policy In** list, select **internet_access**.
- d. Click **Apply**.
15. Set the CoS queue 1 configuration for interface 1/0/5.

- a. Select **QoS > CoS > Advanced > Interface Queue Configuration**. A screen similar to the following displays.

The screenshot shows the 'Interface Queue Configuration' page. The left sidebar has a tree view with 'Advanced > CoS > Interface Queue Configuration' selected. The main content area shows a table with the following data:

Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
<input checked="" type="checkbox"/> 1/0/5	1	25	Weighted	taildrop
<input type="checkbox"/> 1/0/1	0	0	weighted	taildrop
<input type="checkbox"/> 1/0/2	0	0	weighted	taildrop
<input type="checkbox"/> 1/0/3	0	0	weighted	taildrop
<input type="checkbox"/> 1/0/4	0	0	weighted	taildrop
<input checked="" type="checkbox"/> 1/0/5	0	0	weighted	taildrop

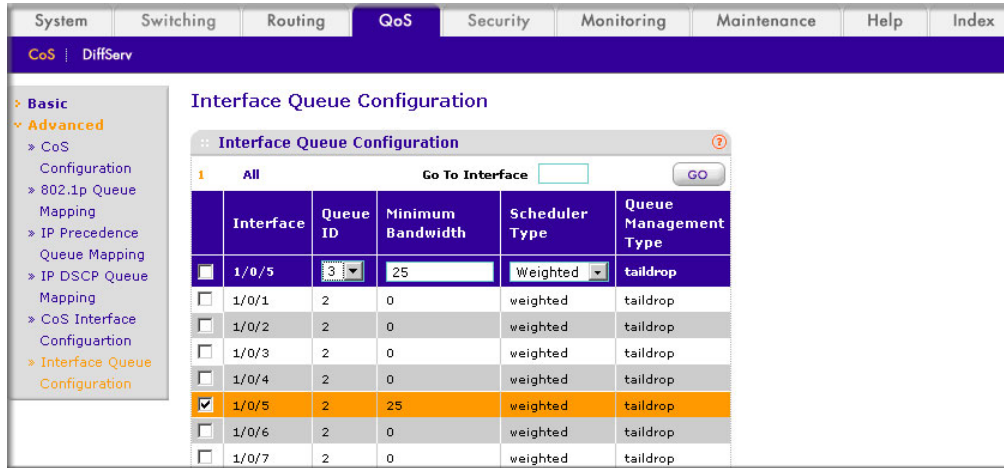
- b. Scroll down and select the Interface **1/0/5** check box. Now 1/0/5 appears in the Interface field at the top.
- c. In the **Queue ID** list, select **1**.
- d. In the **Minimum Bandwidth** field, enter **25**.
- e. Click **Apply**.
16. Set the CoS queue 2 configuration for interface 1/0/5.
- a. Select **QoS > CoS > Advanced > Interface Queue Configuration**. A screen similar to the following displays.

The screenshot shows the 'Interface Queue Configuration' page. The left sidebar has a tree view with 'Advanced > CoS > Interface Queue Configuration' selected. The main content area shows a table with the following data:

Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
<input checked="" type="checkbox"/> 1/0/5	2	25	Weighted	taildrop
<input type="checkbox"/> 1/0/1	1	0	weighted	taildrop
<input type="checkbox"/> 1/0/2	1	0	weighted	taildrop
<input type="checkbox"/> 1/0/3	1	0	weighted	taildrop
<input type="checkbox"/> 1/0/4	1	0	weighted	taildrop
<input checked="" type="checkbox"/> 1/0/5	1	25	weighted	taildrop

- b. Under Interface Queue Configuration, scroll down and select the interface **1/0/5** check box. Now 1/0/5 appears in the Interface field at the top.
- c. In the **Queue ID** list, select **2**.
- d. In the **Minimum Bandwidth** field, enter **25**.
- e. Click **Apply**.
17. Set the CoS queue 3 configuration for interface 1/0/5.

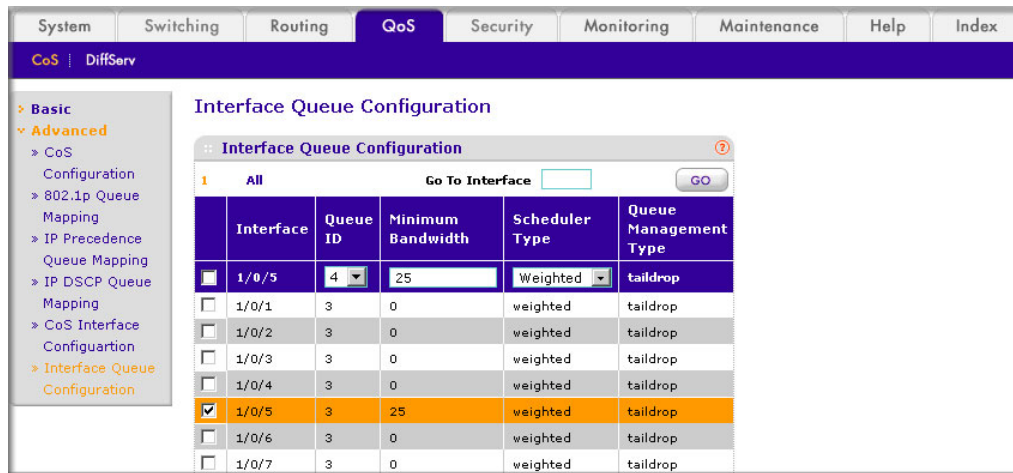
- a. Select **QoS > CoS > Advanced > Interface Queue Configuration**. A screen similar to the following displays.



- b. Under Interface Queue Configuration, scroll down and select the interface **1/0/5** check box. Now 1/0/5 appears in the Interface field at the top.
- c. In the **Queue ID** list, select **3**.
- d. In the **Minimum Bandwidth** field, enter **25**.
- e. Click **Apply**.

18. Set the CoS queue 4 configuration for interface 1/0/5.

- a. Select **QoS > CoS > Advanced > Interface Queue Configuration**. A screen similar to the following displays.



- b. Under Interface Queue Configuration, scroll down and select the Interface **1/0/5** check box. Now 1/0/5 appears in the Interface field at the top.
- c. In the **Queue ID** list, select **4**.
- d. In the **Minimum Bandwidth** field, enter **25**.
- e. Click **Apply**.

DiffServ for VoIP

One of the most valuable uses of DiffServ is to support Voice over IP (VoIP). VoIP traffic is inherently time sensitive: For a network to provide acceptable service, a guaranteed transmission rate is vital. This example shows one way to provide the necessary quality of service: how to set up a class for UDP traffic, have that traffic marked on the inbound side, and then expedite the traffic on the outbound side. The configuration script is for Router 1 in the accompanying diagram: A similar script should be applied to Router 2.

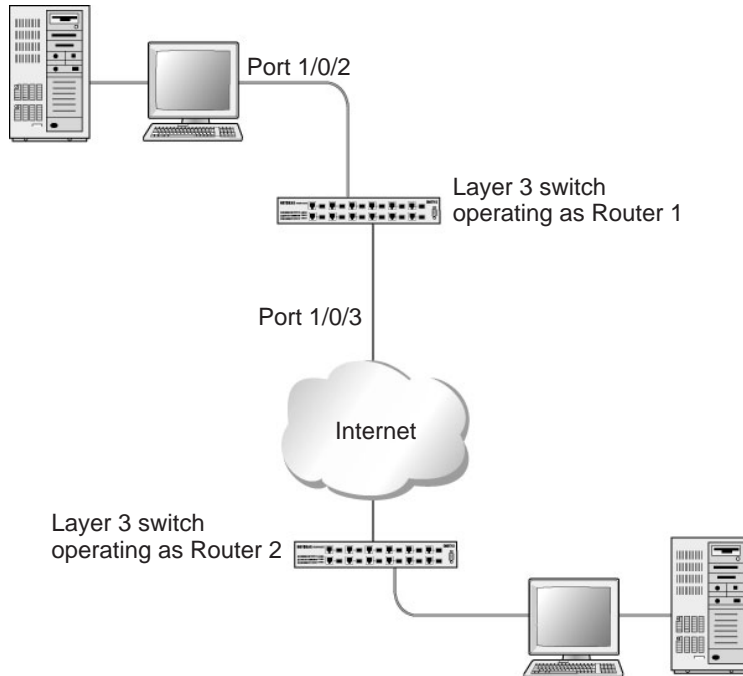


Figure 23. Diffserv for VoIP in Router 1

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

CLI: Configure DiffServ for VoIP

1. Enter Global configuration mode. Set queue 5 on all ports to use strict priority mode. This queue will be used for all VoIP packets. Activate DiffServ for the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#cos-queue strict 5
(Netgear Switch) (Config)#diffserv
```

2. Create a DiffServ classifier named `class_voip` and define a single match criterion to detect UDP packets. The class type `match-all` indicates that all match criteria defined for the class must be satisfied in order for a packet to be considered a match.

```
(Netgear Switch) (Config)#class-map match-all class_voip
(Netgear Switch) (Config class-map)#match protocol udp
(Netgear Switch) (Config class-map)#exit
```

3. Create a second DiffServ classifier named `class_ef` and define a single match criterion to detect a DiffServ code point (DSCP) of `EF` (expedited forwarding). This handles incoming traffic that was previously marked as expedited somewhere in the network.

```
(Netgear Switch) (Config)#class-map match-all class_ef
(Netgear Switch) (Config class-map)#match ip dscp ef
(Netgear Switch) (Config class-map)#exit
```

4. Create a DiffServ policy for inbound traffic named `pol_voip`, then add the previously created classes `class_ef` and `class_voip` as instances within this policy.

This policy handles incoming packets already marked with a DSCP value of `EF` (according to the `class_ef` definition), or marks UDP packets according to the `class_voip` definition) with a DSCP value of `EF`. In each case, the matching packets are assigned internally to use queue 5 of the egress port to which they are forwarded.

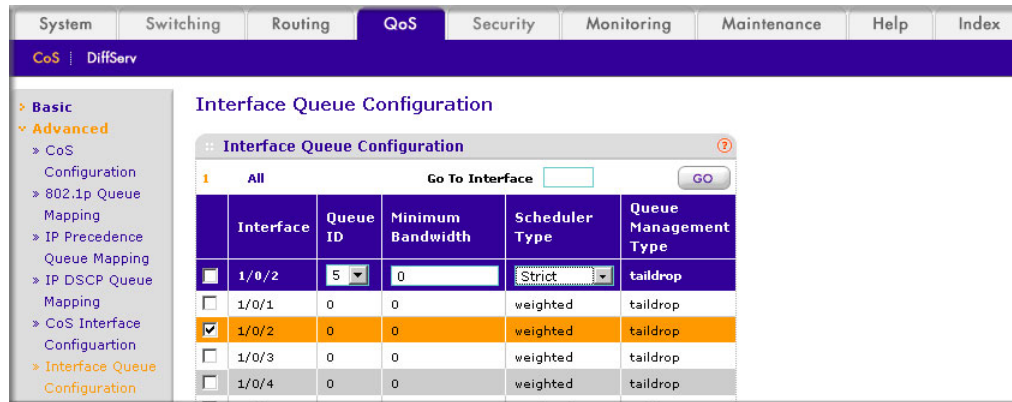
```
(Netgear Switch) (Config)#policy-map pol_voip in
(Netgear Switch) (Config policy-map)#class class_ef
(Netgear Switch) (Config policy-class-map)#assign-queue 5
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class class_voip
(Netgear Switch) (Config policy-class-map)#mark ip-dscp ef
(Netgear Switch) (Config policy-class-map)#assign-queue 5
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#exit
```

5. Attach the defined policy to an inbound service interface.

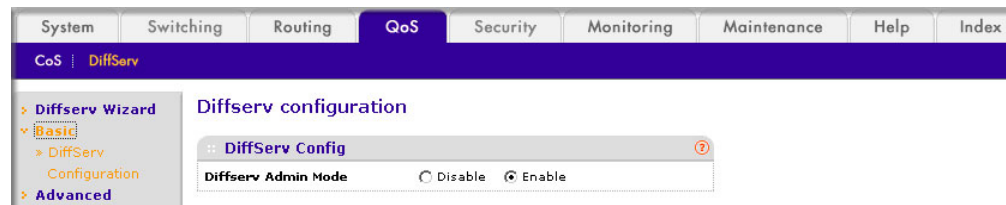
```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#service-policy in pol_voip
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Diffserv for VoIP

1. Set queue 5 on all interfaces to use strict mode.
 - a. Select **QoS > CoS > Advanced > CoS Interface Configuration**. A screen similar to the following displays.

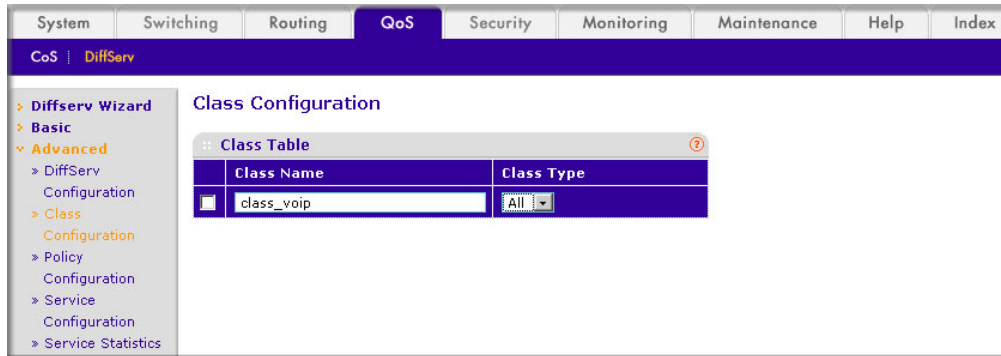


- b. Under Interface Queue Configuration, select all the interfaces.
 - c. In the **Queue ID** list, select **5**.
 - d. In the **Scheduler Type** list, select **Strict**.
 - e. Click **Apply** to save the settings.
2. Enable DiffServ.
 - a. Select **QoS > DiffServ > Basic > DiffServ Configuration**. A screen similar to the following displays.

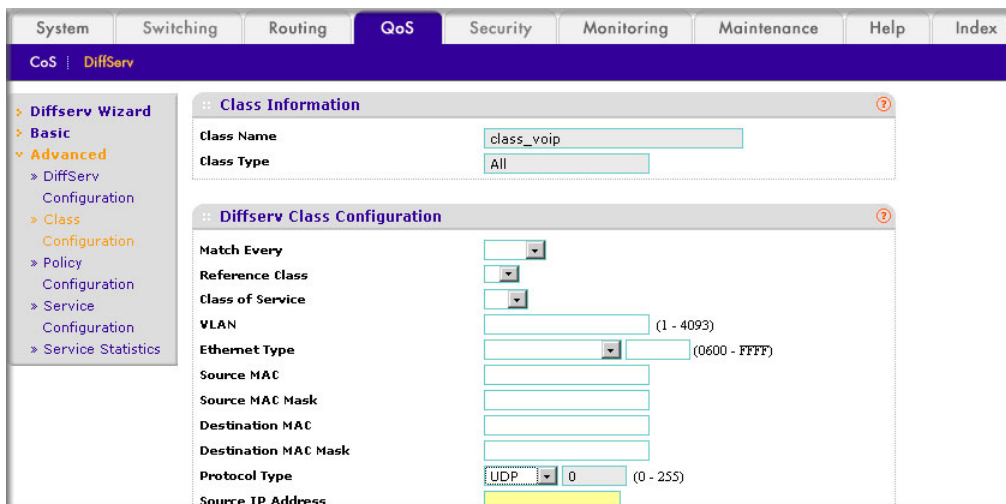


- b. For Diffserv Admin Mode, select the **Enable** radio button.
 - c. Click **Apply** to save the settings.
3. Create a class class_voip.

- a. Select **QoS > DiffServ > Advanced > DiffServ Configuration**. A screen similar to the following displays.

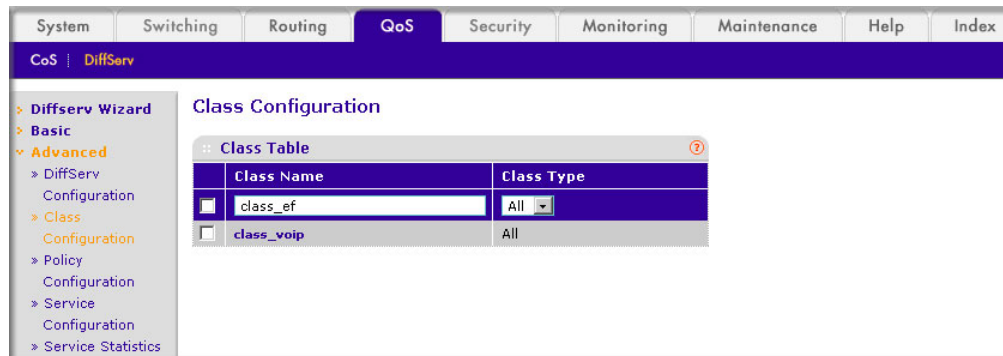


- b. In the **Class Name** field, enter **class_voip**.
- c. In the **Class Type** list, select **All**.
- d. Click **Add** to create a new class.
- e. Click **class_voip**. A screen similar to the following displays:

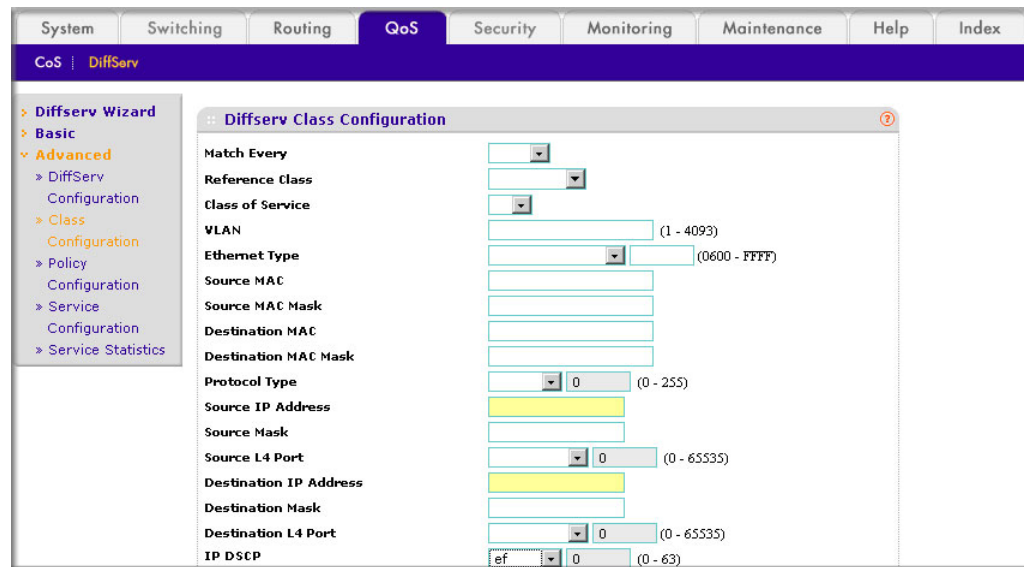


- f. In the **Protocol Type** list, select **UDP**.
 - g. Click **Apply** to create a new class.
4. Create a class class_ef:

- a. Select **QoS > DiffServ > Advanced > DiffServ Configuration**. A screen similar to the following displays.

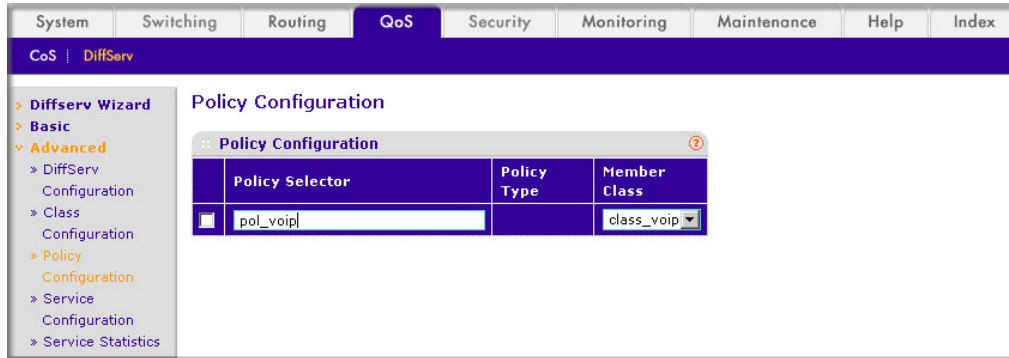


- b. In the **Class Name** field, enter **class_ef**.
 c. In the **Class Type** list, select **All**.
 d. Click **Add** to create a new class.
 e. Click **class_ef**. Another screen similar to the following displays:

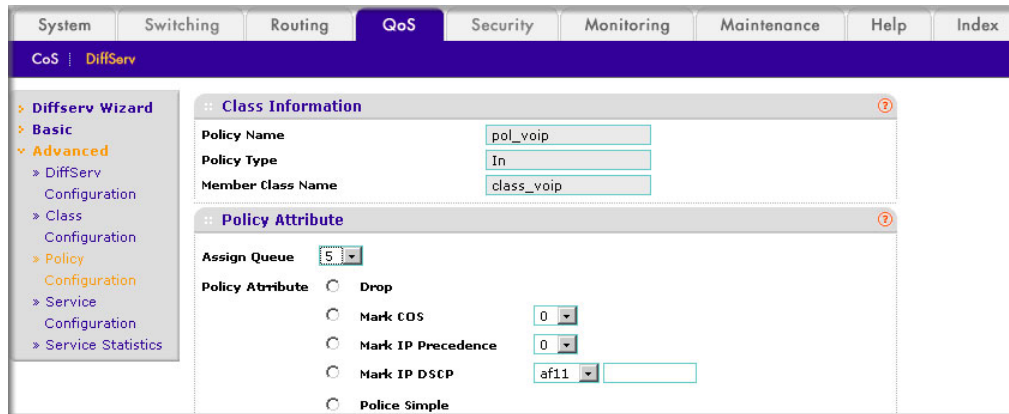


- f. In the **IP DSCP** list, select **ef**.
 g. Click **Apply** to create a new class.
 5. Create a policy **pol_voip**. and add **class_voip** to this policy.

- a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.



- b. In the **Policy Selector** field, enter **pol_voip**.
- c. In the **Member Class** list, select **class_voip**.
- d. Click **Add** to create a new policy.
- e. Click the **pol_voip** whose class member is class_voip. A screen similar to the following displays.



- f. In the **Assign Queue** list, select **5**.
 - g. For Policy Attribute, select the **Mark IP DSCP** radio button, and select **ef**.
 - h. Click **Apply** to create a new policy.
6. Add class_ef to the policy pol_voip.

- a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.

Policy Selector	Policy Type	Member Class
<input type="checkbox"/> pol_voip	In	class_ef
<input checked="" type="checkbox"/> pol_voip	In	class_voip

- b. Under Policy Configuration, scroll down and select the **pol_voip** check box. Pol_voip now appears in the Policy Selector field at the top.
- c. In the **Member Class** list, select **class_ef** in.
- d. Click **Apply** to add the class class_ef to the policy pol_voip.
- e. Click the **pol_voip** whose class member is class_ef, and a screen similar to the following displays.

Class Information

Policy Name: pol_voip

Policy Type: In

Member Class Name: class_ef

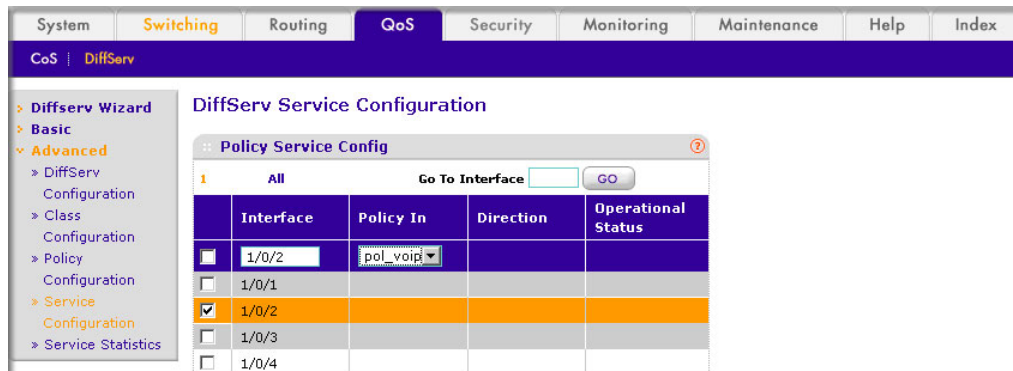
Policy Attribute

Assign Queue: 5

Policy Attribute: Drop Mark COS (0) Mark IP Precedence (0) Mark IP DSCP (ef)

- f. In the **Assign Queue** list, select **5**.
- g. Click **Apply** to create a new policy.
7. Attach the defined policy to interface 1/0/2 in the inbound direction.

- a. Select **QoS > DiffServ > Advanced > Service Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Interface **1/0/2** check box. Now 1/0/2 appears in the Interface field at the top.
- c. In the **Policy In** list, select **pol_voip**.
- d. Click **Apply** to create a new policy.

Auto VoIP

The Auto-VoIP feature makes it easy to set up VoIP for IP phones on a switch. This functionality copies VoIP signaling packets to the CPU to get the source and destination IP address and Layer 4 port of the current session. Based on these parameters a filter is

installed to assign the highest priority to VOIP data packets. As soon as the call ends, the filters are removed.

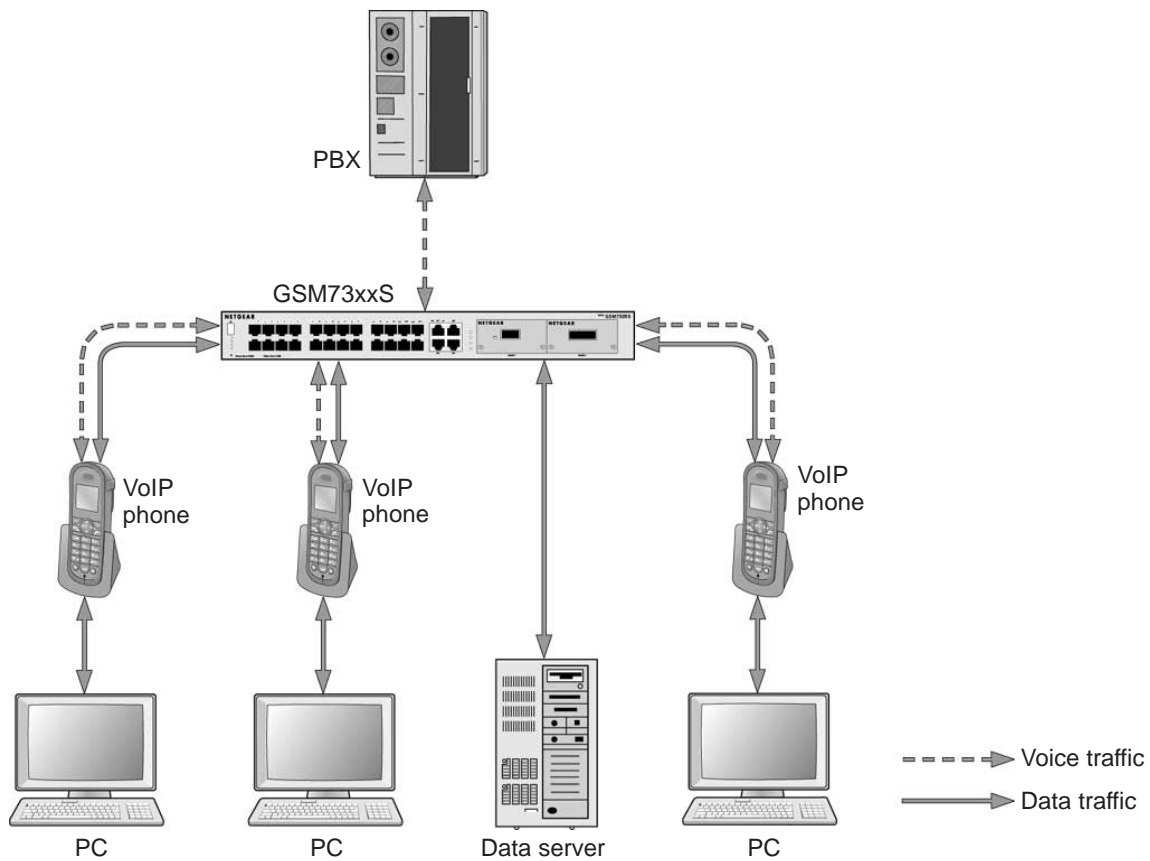


Figure 24. Auto VoIP

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

CLI: Configure Auto VoIP

This script in this section shows how to set up auto VoIP system-wide.

1. Enable auto VoIP on all the interfaces in the device.

```
(Netgear Switch) (Config)# auto-voip all
```

2. View the auto VoIP information:

```
(Netgear Switch) # show auto-voip interface all
```

Interface	Auto VoIP Mode	Traffic Class
1/0/1	Enabled	6
1/0/2	Enabled	6
1/0/3	Enabled	6
1/0/4	Enabled	6
1/0/5	Enabled	6
1/0/6	Enabled	6
1/0/7	Enabled	6
1/0/8	Enabled	6
1/0/9	Enabled	6
1/0/10	Enabled	6
1/0/11	Enabled	6
1/0/12	Enabled	6
1/0/13	Enabled	6
1/0/14	Enabled	6
1/0/15	Enabled	6
1/0/16	Enabled	6
1/0/17	Enabled	6
1/0/18	Enabled	6
1/0/19	Enabled	6
1/0/20	Enabled	6

```
--More-- or (q)uit
```

Interface	Auto VoIP Mode	Traffic Class
1/0/21	Enabled	6
1/0/22	Enabled	6
1/0/23	Enabled	6
1/0/24	Enabled	6
1/0/25	Enabled	6
1/0/26	Enabled	6
1/0/27	Enabled	6
1/0/28	Enabled	6

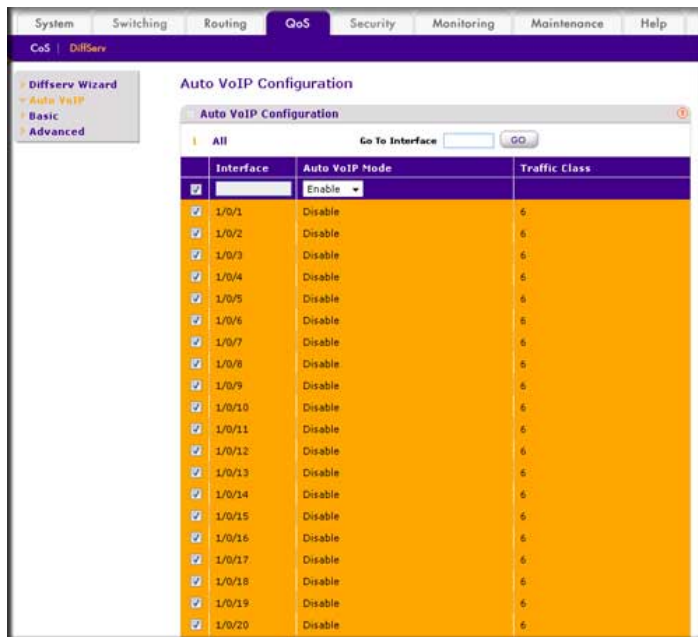
Auto VoIP classifies and prioritizes the packets and places only the packets in the higher-priority queue. In the previous example, they are placed in queue 6. You can override the egress queue setting using the commands `cos-queue strict` or `cos-queue min-bandwidth` if you want.

Web Interface: Configure Auto-VoIP

1. Enable auto VoIP for all the interfaces in the device.
 - a. Select **QoS > DiffServ > Auto VoIP**. A screen similar to the following displays.



- b. Select the check box in the first row to select all the interfaces.
 - c. In the **Auto VoIP Mode** field, select **Enable**. A screen similar to the following displays.



- d. Click **Apply**. A screen similar to the following displays.



DiffServ for IPv6

This feature extends the existing QoS ACL and DiffServ functionality by providing support for IPv6 packet classification.

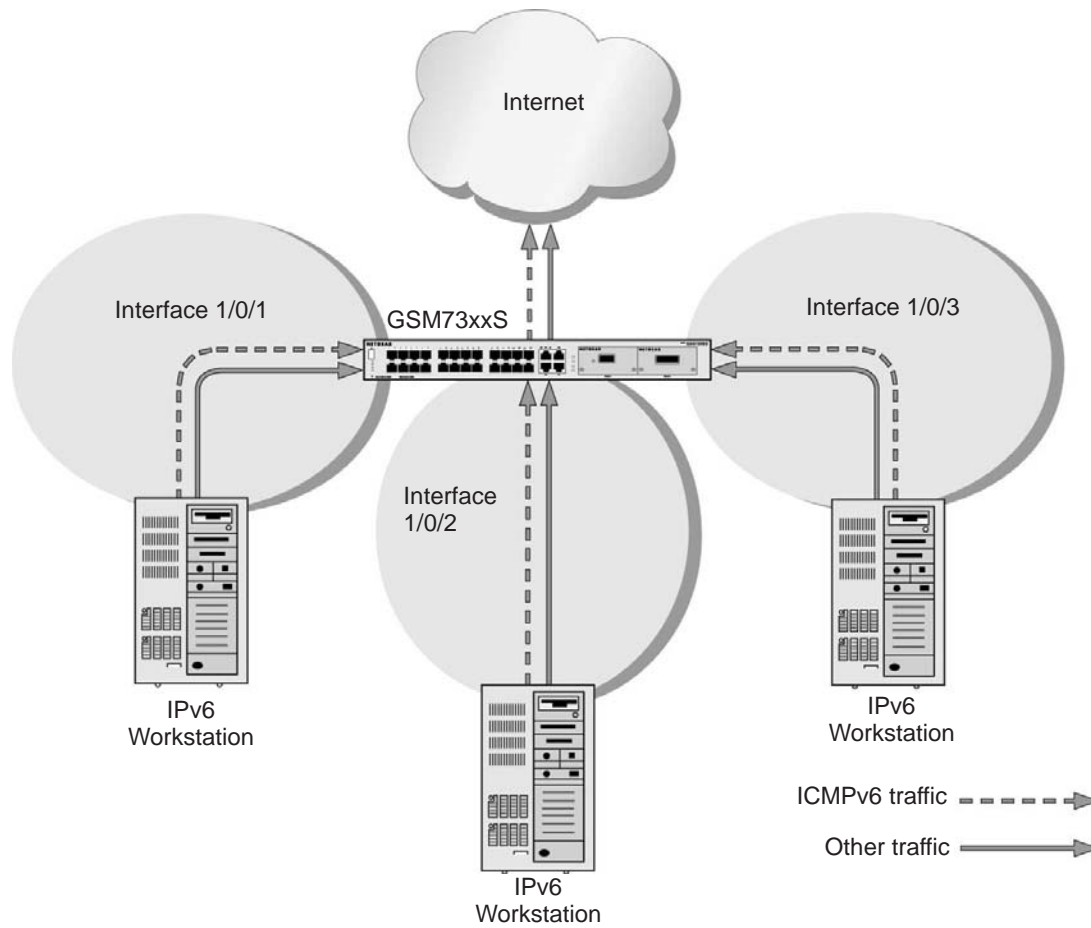


Figure 25. DiffServ for IPv6

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

CLI: Configure DiffServ for IPv6

The script in this section shows how to prioritize ICMPv6 traffic over other IPv6 traffic.

1. Create the IPv6 class classicmpv6.

```
(Netgear Switch) (Config)# class-map match-all classicmpv6 ipv6
```

2. Define matching criteria as protocol ICMPv6.

```
(Netgear Switch) (Config-classmap) # match protocol 58
(Netgear Switch) (Config-classmap) # exit
```

3. Create the policy policyicmpv6.

```
(Netgear Switch) (Config)# policy-map policyicmpv6 in
```

4. Associate the previously created class classicmpv6.

```
(Netgear Switch) (Config-policy-map)# class classicmpv6
```

5. Set the attribute as assign queue 6.

```
(Netgear Switch) (Config-policy-classmap)# assign-queue 6
(Netgear Switch) (Config-policy-map)# exit
```

6. Attach the policy policy_icmpv6 to interfaces 1/0/1,1/0/2 and 1/0/3:

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# service-policy in policyicmpv6
(Netgear Switch) (Interface 1/0/1)# exit

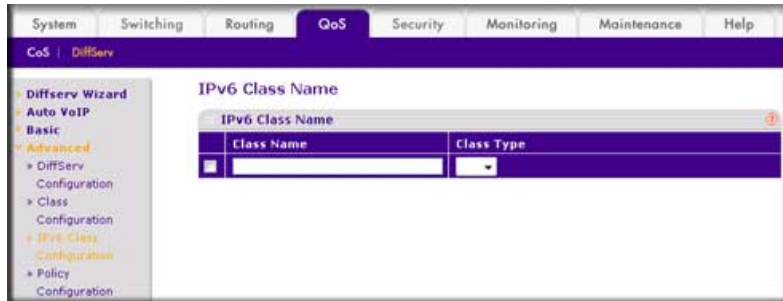
(Netgear Switch) (Config)# interface 1/0/2
(Netgear Switch) (Interface 1/0/2)# service-policy in policyicmpv6
(Netgear Switch) (Interface 1/0/2)# exit

(Netgear Switch) (Config)# interface 1/0/3
(Netgear Switch) (Interface 1/0/3)# service-policy in policyicmpv6
(Netgear Switch) (Interface 1/0/3)# exit
```

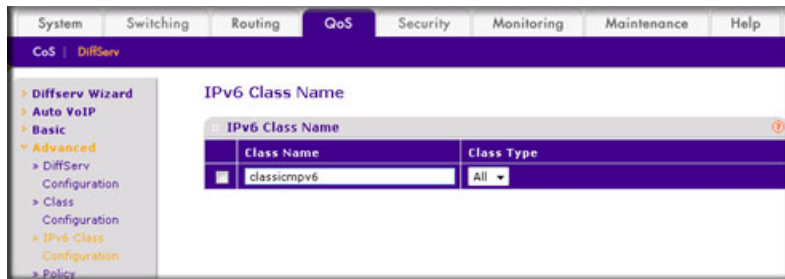
Web Interface: Configure DiffServ for IPv6

1. Create the IPv6 class classicmpv6.

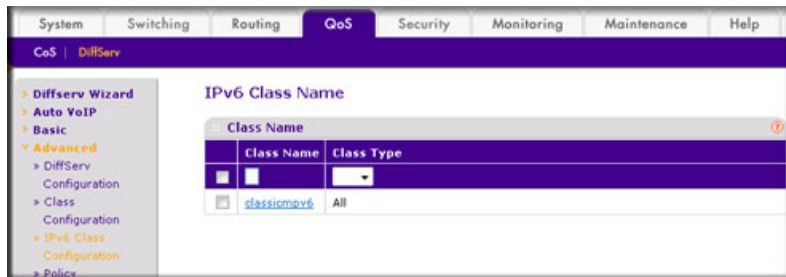
- a. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**. A screen similar to the following displays.



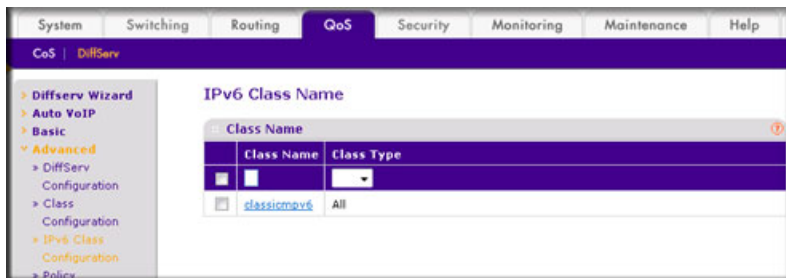
- b. In the **Class Name** field, enter **classicmpv6**.
- c. In the **Class Type** list, select **All**. A screen similar to the following displays.



- d. Click **Add** to create the IPv6 class. A screen similar to the following displays.



2. Define matching criteria as protocol ICMPv6.
 - a. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**. A screen similar to the following displays.



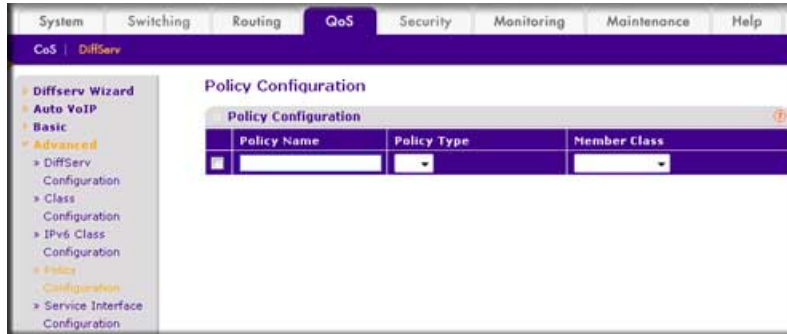
- b. Click the class **classicmpv6**. A screen similar to the following displays.

- c. Select the **Protocol Type** radio button, select **Other**, and enter **58**. A screen similar to the following displays.

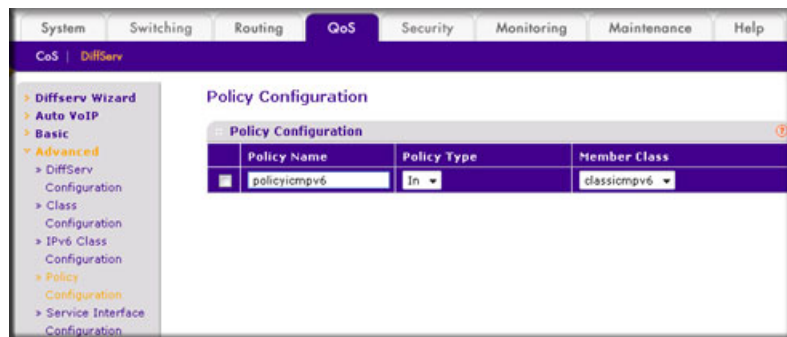
- d. Click **Apply**. A screen similar to the following displays.

3. Create the policy **policyicmpv6**, and associate the previously created class **classicmpv6**.

- a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.



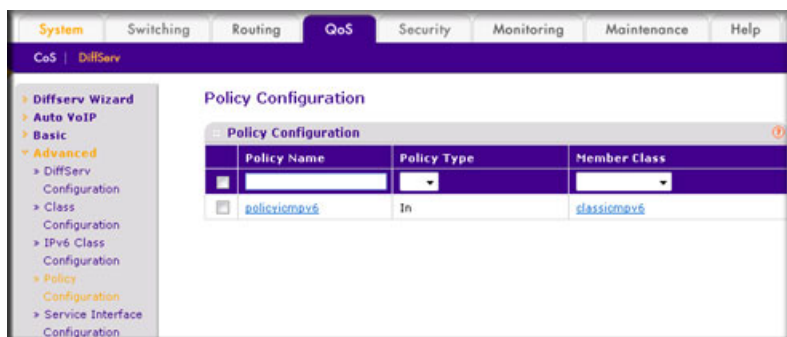
- b. In the **Policy Name** field, enter **policyicmpv6**.
- c. In the **Policy Type** list, select **In**.
- d. In the **Member Class** list, select **classicmpv6**. A screen similar to the following displays.



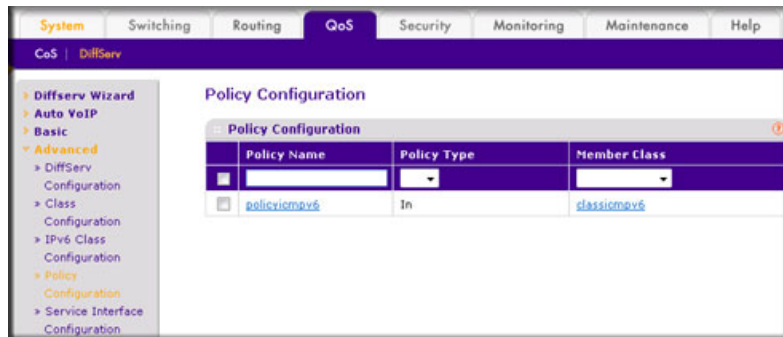
- e. Click **Add**.

4. Set the attribute as assign queue 6.

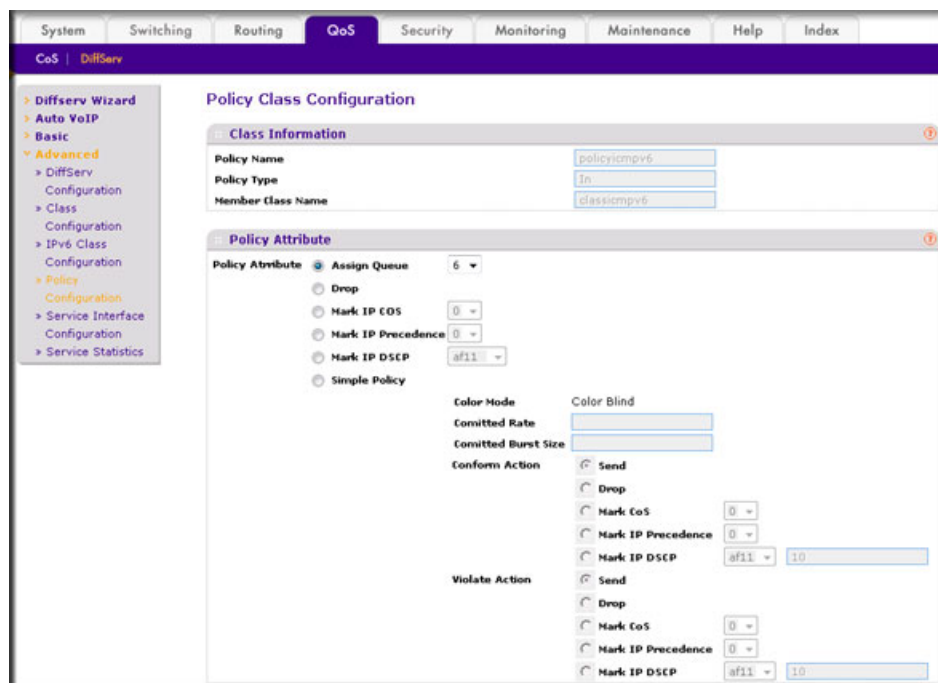
- a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.



- b. Click the policy **policyicmpv6**. A screen similar to the following displays.



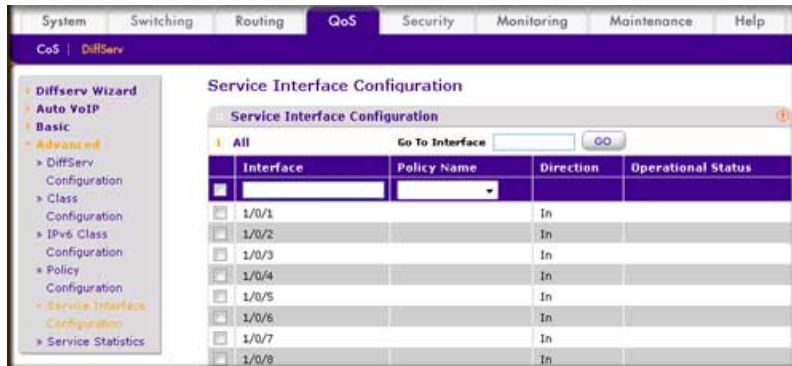
- c. In the **Assign Queue** list, select **6**.



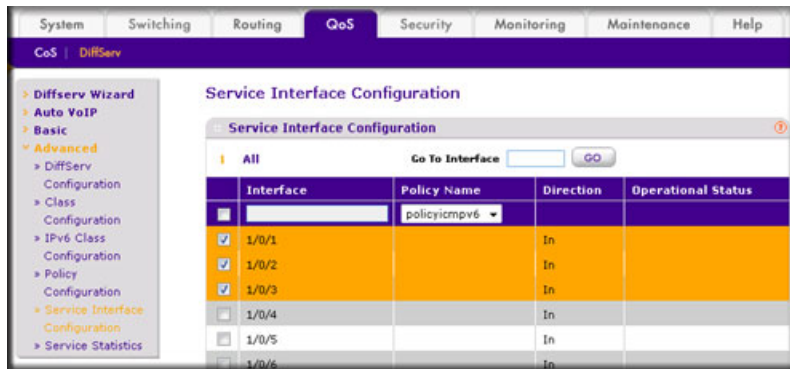
- d. Click **Apply**.

5. Attach the policy **policyicmpv6** to interfaces 1/0/1, 1/0/2 and 1/0/3.

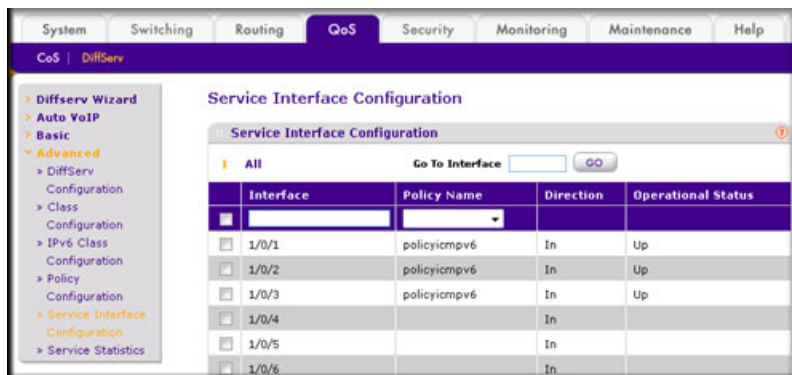
- a. Select **QoS > DiffServ > Advanced > Service Interface Configuration**. A screen similar to the following displays.



- b. In the **Policy Name** list, select **policyicmpv6**.
- c. Select the Interface **1/0/1**, **1/0/2**, and **1/0/3** check boxes. A screen similar to the following displays.



- d. Click **Apply**. A screen similar to the following displays.



Color Conform Policy

This example shows how to create a policy to police the traffic to a committed rate. The packets with IP precedence value of 7 are colored green to ensure that these packets are the last to be dropped when there is congestion. The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure a Color Conform Policy

1. Create a VLAN 5 and configure ports 1/0/13 and 1/0/25 as its members.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 5
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#vlan participation include 5
(Netgear Switch) (Interface 1/0/13)#vlan tagging 5
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#interface 1/0/25
(Netgear Switch) (Interface 1/0/25)#vlan participation include 5
(Netgear Switch) (Interface 1/0/25)#vlan tagging 5
(Netgear Switch) (Interface 1/0/25)#exit
```

2. Create classes class_vlan and class_color.

Note: DiffServ service is enabled by default.

```
(Netgear Switch) (Config)#class-map match-all class_vlan
(Netgear Switch) (Config-classmap)#match vlan 5
(Netgear Switch) (Config-classmap)#exit
(Netgear Switch) (Config)#class-map match-all class_color
(Netgear Switch) (Config-classmap)#match ip precedence 7
(Netgear Switch) (Config-classmap)#exit
```

3. Create a policy to police the traffic to a rate of 1000 kbps with an allowed burst size of 64 KB. Furthermore, the packets with IP precedence value of 7 will be colored green. That

means these packets will be the last packets to be dropped in the event of congestion beyond the policed rate.

```
(Netgear Switch) (Config)#policy-map policy_vlan in
(Netgear Switch) (Config-policy-map)#class class_vlan
(Netgear Switch) (Config-policy-classmap)#police-simple 1000 64 conform-action transmit
violate-action drop
(Netgear Switch) (Config-policy-classmap)#conform-color class_color
(Netgear Switch) (Config-policy-classmap)#exit
(Netgear Switch) (Config-policy-map)#exit
```

4. Apply this policy to port 1/0/13.

```
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#service-policy in policy_vlan
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Configure a Color Conform Policy

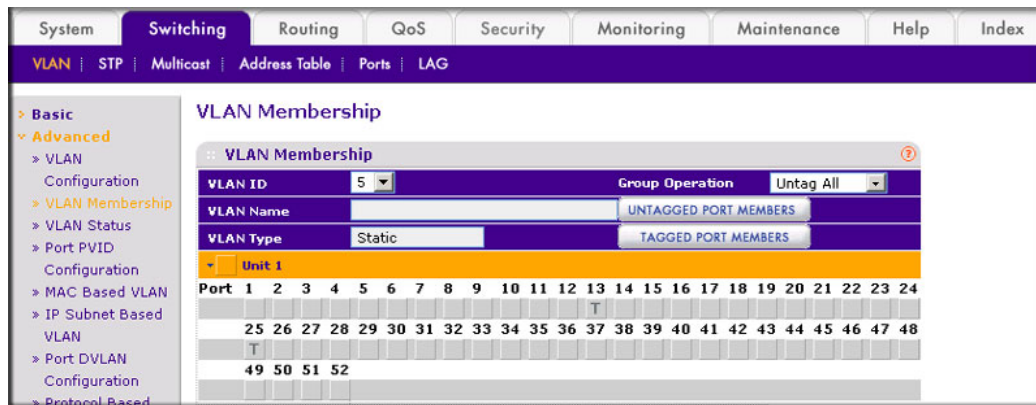
1. Create a VLAN.

- a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays.

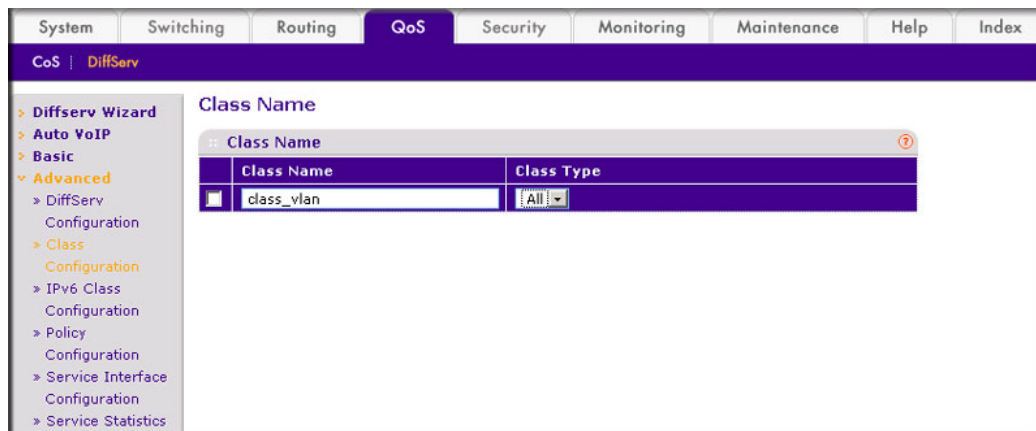
VLAN ID	VLAN Name	VLAN Type	Make Static
1	Default	Default	Disable

- b. In the **VLAN ID** field, enter **5**.
 - c. Click **Add**.
- ### 2. Add ports 1/0/13 and 1/0/25 to VLAN 5.

- a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays.

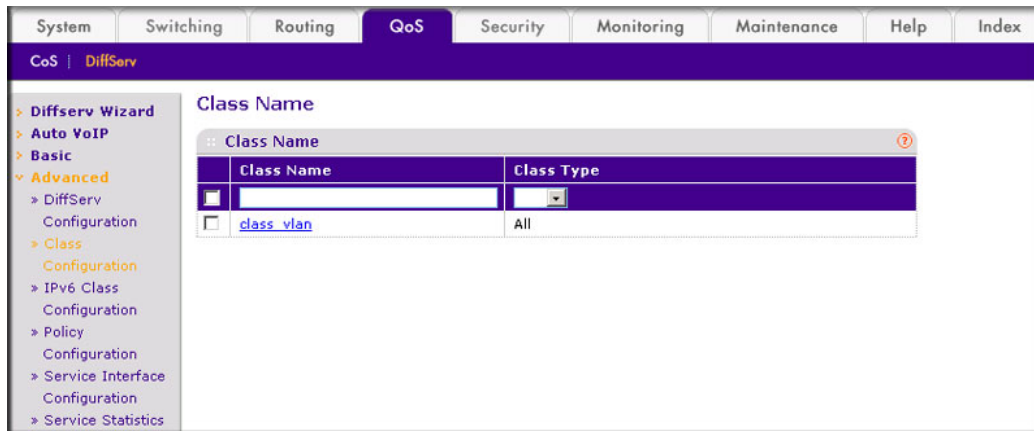


- b. In the **VLAN ID** list, select **5**.
- c. Click **Unit 1**. The ports display.
- d. Click the gray boxes under ports **13** and **25** until **T** displays. The T specifies that the egress packet is tagged for the port.
- e. Click **Apply**.
3. Create a class `class_vlan`:
- a. Select **QoS > DiffServ > Advanced > Class Configuration**. A screen similar to the following displays.

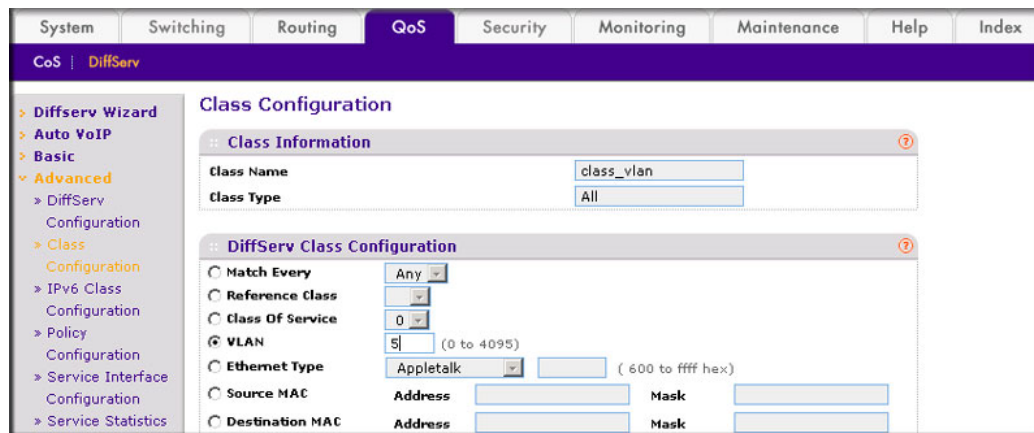


- b. Enter the following information:
- In the **Class Name** field, enter **class_vlan**.
 - In the **Class Type** list, select **All**.

- c. Click **Add** to create a new class class_vlan.



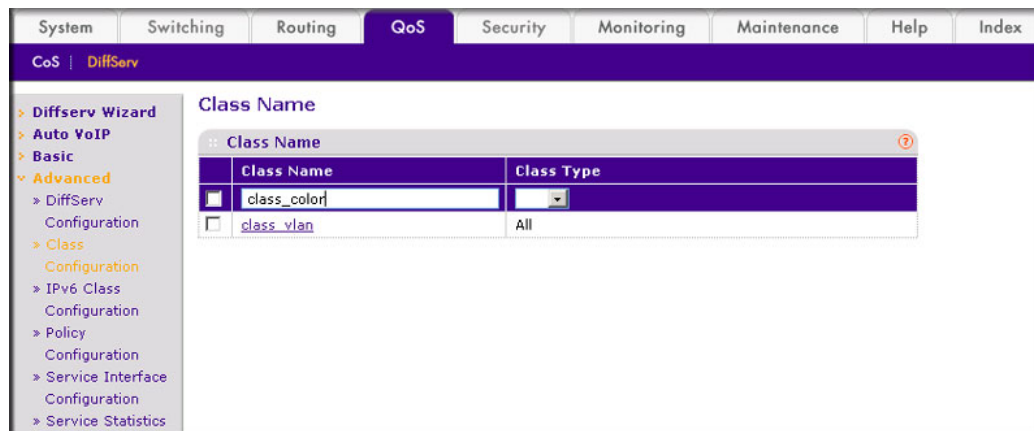
- d. Click **class_vlan** to configure this class. A screen similar to the following displays:



- e. Under Diffserv Class Configuration, in the **VLAN** field, enter **5**.
- f. Click **Apply**.

4. Create a class class_color.

- a. Select **QoS > DiffServ > Advanced > Class Configuration**. A screen similar to the following displays.



- b. Enter the following information:
 - In the **Class Name** field, enter **class_color**.
 - In the **Class Type** list, select **All**.
- c. Click **Add** to create a new class class_color.

The screenshot shows the 'Class Name' configuration page in the DiffServ section. The 'Class Name' field is populated with 'class_color' and the 'Class Type' dropdown is set to 'All'. A table below shows the current configuration:

Class Name	Class Type
class_vlan	All
class_color	All

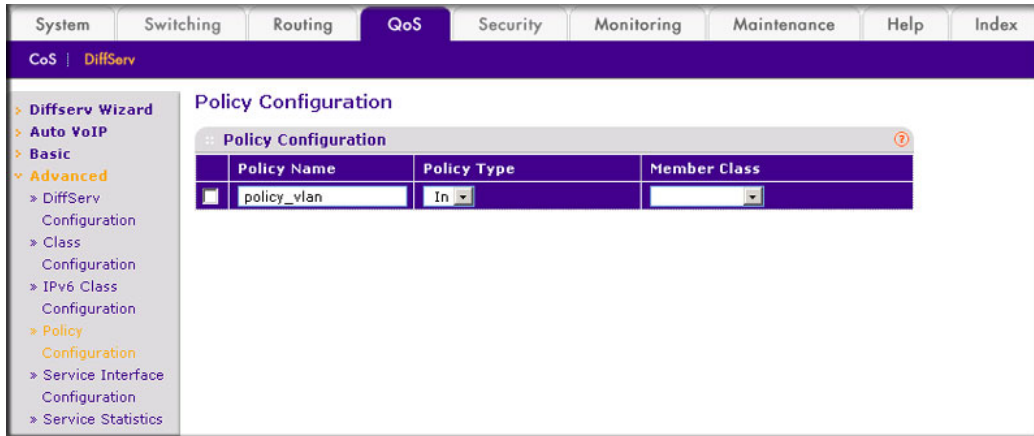
- d. Click **class_color** to configure this class. A screen similar to the following displays:

The screenshot shows the 'DiffServ Class Configuration' page for the class 'class_color'. The 'Precedence Value' is set to 7. The configuration options are as follows:

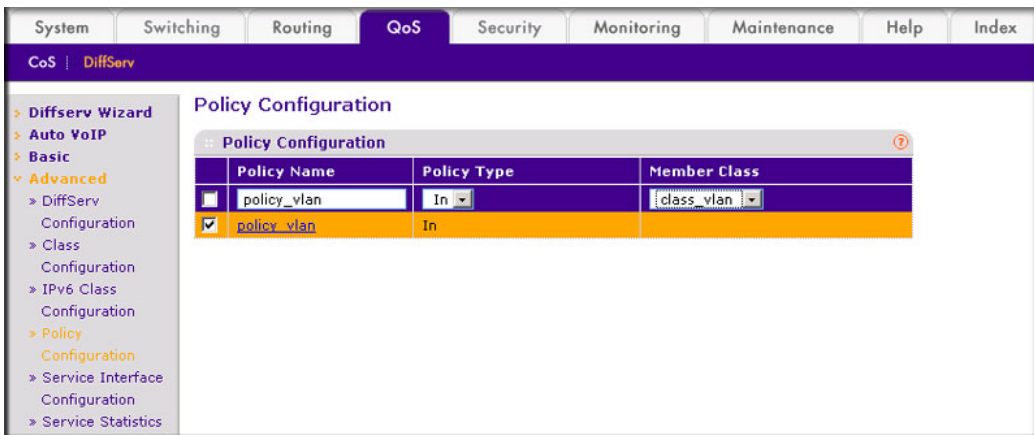
- Match Every: Any
- Reference Class: class_vlan
- Class Of Service: 0
- VLAN: (0 to 4095)
- Ethernet Type: Appletalk (600 to ffff hex)
- Source MAC: Address, Mask
- Destination MAC: Address, Mask
- Protocol Type: ICMP (0 to 255)
- Source IP: Address, Mask
- Source L4 Port: domain (0 to 65535)
- Destination IP: Address, Mask
- Destination L4 Port: domain (0 to 65535)
- IP DSCP: af11 (0 to 63)
- Precedence Value: 7 (0 to 7)
- IP ToS: Bit Value, Bit Mask

- e. Under Diffserv Class Configuration, in the **Precedence Value** list, select **7**.
 - f. Click **Apply**.
5. Create a policy policy_vlan.

- a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.



- b. In the **Policy Name** field, enter **policy_vlan**.
 - c. In the **Policy Type** list, select **In**.
 - d. Click **Add**.
6. Associate policy_vlan with class_vlan.
 - a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.



- b. Under Policy Configuration, scroll down and select the **policy_vlan** check box.
 - c. In the **Member Class** field, enter **class_vlan**.
 - d. Click **Apply**.
7. Configure policy_vlan.

- a. Select **QoS > DiffServ > Advanced > Policy Configuration**. Click **policy_vlan**. A screen similar to the following displays.

The screenshot shows the 'Policy Class Configuration' page. The navigation menu on the left includes 'DiffServ Wizard', 'Auto VoIP', 'Basic', and 'Advanced'. Under 'Advanced', there are sub-menus for 'DiffServ Configuration', 'Class Configuration', 'IPv6 Class Configuration', 'Policy Configuration', 'Service Interface Configuration', and 'Service Statistics'. The main content area is divided into two sections: 'Class Information' and 'Policy Attribute'.

Class Information:

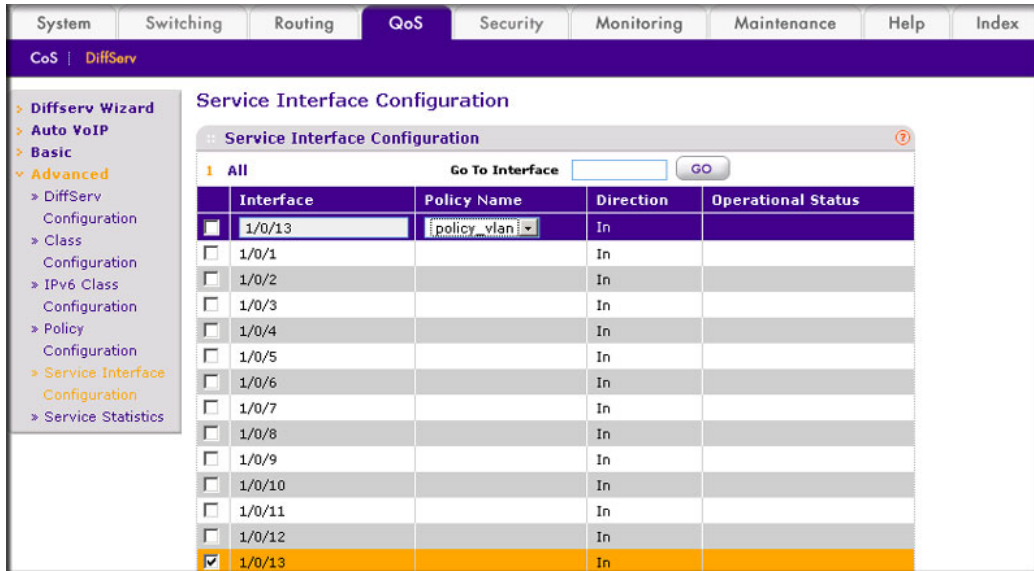
- Policy Name: policy_vlan
- Policy Type: In
- Member Class Name: class_vlan

Policy Attribute:

- Policy Attribute: Assign Queue (0), Drop, Mark IP CoS (0), Mark IP Precedence (0), Mark IP DSCP (af11), Simple Policy
- Color Conform Class: class_color
- Color Mode: Color Aware
- Committed Rate: 1000
- Committed Burst Size: 64
- Conform Action: Send, Drop, Mark CoS (0), Mark IP Precedence (0)

- b. Select the **Simple Policy** radio button.
- c. In the **Color Mode** list, select **Color Aware**.
- d. In the **Color Conform Class** list, select **class_color**.
- e. In the **Committed Rates** field, enter **1000**.
- f. In the **Committed Burst Size** field, enter **64**.
- g. For Conform Action, select the **Send** radio button.
- h. For Violate Action, select the **Drop** radio button.
- i. Click **Apply**.
8. Apply policy_vlan to interface 1/0/13.

- a. Select **QoS > DiffServ > Advanced > Service Interface Configuration**. A screen similar to the following displays.



- b. Under Service Interface Configuration, scroll down and select the Interface **1/0/13** check box.
- c. In the **Policy Name** list, select **policy_vlan**.
- d. Click **Apply** to save the settings.

13. IGMP Snooping and Querier

13

This chapter provides the following examples:

- *IGMP Snooping*
- *Show igmpsnooping* on page 238
- *Show mac-address-table igmpsnooping* on page 239
- *External Multicast Router* on page 239
- *Multicast Router Using VLAN* on page 240
- *IGMP Querier* on page 241
- *Enable IGMP Querier* on page 242
- *Show IGMP Querier Status* on page 245

IGMP:

- Uses version 3 of IGMP.
- Includes snooping.
- Snooping can be enabled per VLAN.

IGMP Snooping

The following are examples of the commands used in the IGMP snooping feature.

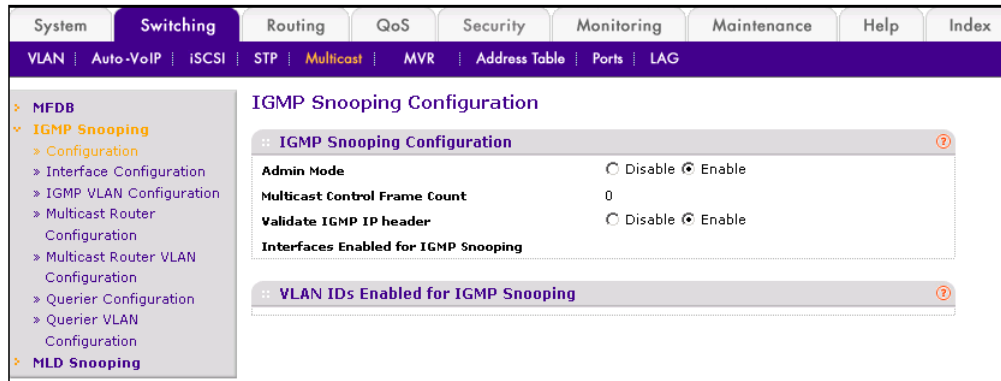
CLI: Enable IGMP Snooping on VLAN 100

The following example shows how to enable IGMP snooping.

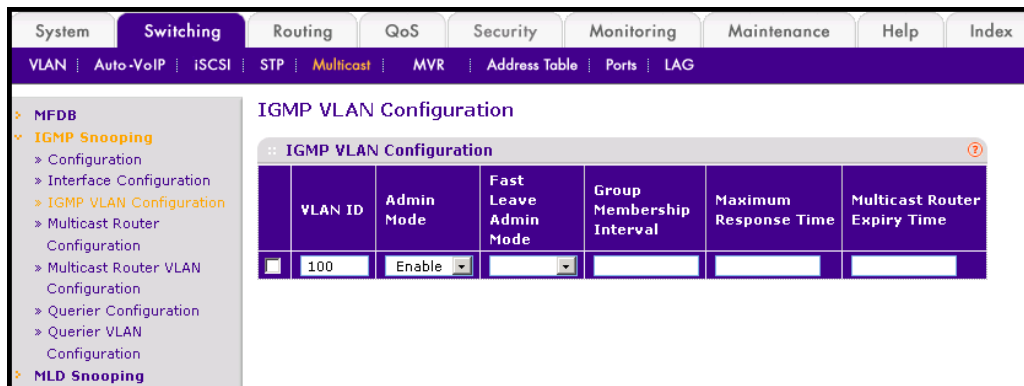
```
(Netgear Switch) #config
(Netgear Switch) (Config)#set igmp
(Netgear Switch) (Config)#set igmp 100
(Netgear Switch) (Config)# mac address-table multicast forbidden-unregistered vlan 100
(Netgear Switch) (Config)#exit
```

Web Interface: Enable IGMP Snooping on VLAN 100

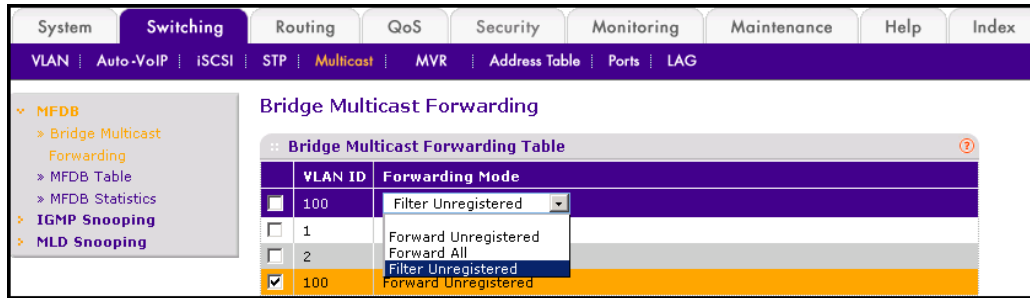
1. Configure IGMP snooping Admin Mode:
 - a. Select **Switching > Multicast > IGMP Snooping > Configuration**. A screen similar to the following displays.



- b. For Admin Mode select the **Enable** radio button.
 - c. Click **Apply**.
2. Configure IGMP Snooping on VLAN 100:
 - a. Select **Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration**. A screen similar to the following displays.



- b. In the VLAN ID field, enter **100**.
 - c. For Admin Mode, select the **Enable** from dropdown menu.
 - d. Click **Add**.
3. Configure IGMP Snooping filter on VLAN 100:
 - a. Select **Switching > Multicast > MFDB > Bridge Multicast Forwarding**. A screen similar to the following displays.



- b. Under Bridge Multicast Forwarding, scroll down and select the VLAN 100 check box. Now vlan 100 appears in the VLAN ID field at the top.
- c. In the Forwarding Mode field, select **Filter Unregistered**.
- d. Click **Apply**.

Show igmpsnooping

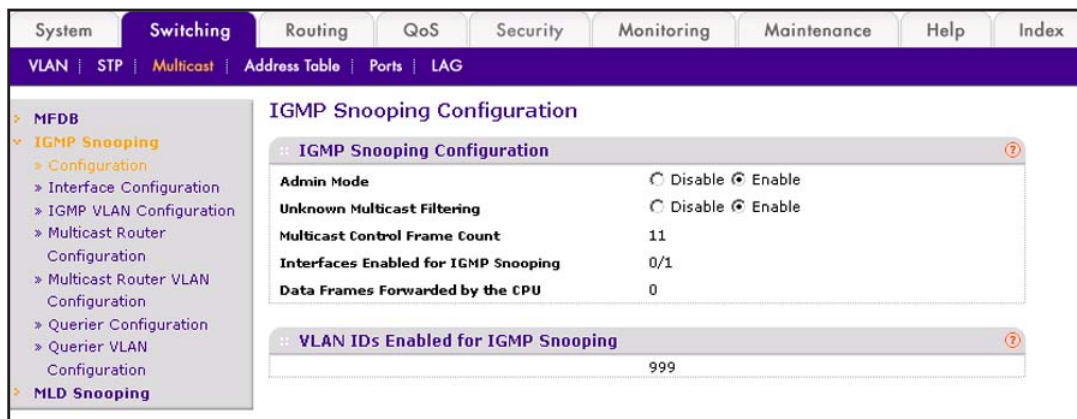
The example is shown as CLI commands and as a Web interface procedure.

CLI: Show igmpsnooping

```
(Netgear Switch) #show igmpsnooping
Admin Mode..... Disable
Unknown Multicast Filtering..... Disable
Multicast Control Frame Count..... 0
Interfaces Enabled for IGMP Snooping..... None
VLANs enabled for IGMP snooping..... None
```

Web Interface: Show igmpsnooping

Select **Switching > Multicast > IGMP Snooping Configuration**. A screen similar to the following displays.



Show mac-address-table igmpsnooping

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

CLI: Show mac-address-table igmpsnooping

```
(Netgear Switch) #show mac-address-table igmpsnooping ?

<cr>                               Press Enter to execute the command.

(Netgear Switch) #show mac-address-table igmpsnooping

Type          Description          Interfaces
-----
00:01:01:00:5E:00:01:16  Dynamic  Network Assist  Fwd: 1/0/47
00:01:01:00:5E:00:01:18  Dynamic  Network Assist  Fwd: 1/0/47
00:01:01:00:5E:37:96:D0   Dynamic  Network Assist  Fwd: 1/0/47
00:01:01:00:5E:7F:FF:FA   Dynamic  Network Assist  Fwd: 1/0/47
00:01:01:00:5E:7F:FF:FE   Dynamic  Network Assist  Fwd: 1/0/47
```

Web Interface: Show mac-address-table igmpsnooping

Select **Switching > Multicast > IGMP Snooping Table**. A screen similar to the following displays.

The screenshot shows the web interface for the MFDB Table. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. Under Switching, there are sub-tabs for VLAN, STP, Multicast, Address Table, Ports, and LAG. The Multicast tab is active, and the MFDB Table sub-tab is selected. The main content area shows the MFDB Table with a search bar and a table of entries.

MAC Address	VLAN ID	Component	Type	Description	Forwarding Interfaces
01:00:5e:01:02:03	999	IGMP	DYNAMIC	Network Assist	0/1

External Multicast Router

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

CLI: Configure the Switch with an External Multicast Router

This example configures the interface as the one the multicast router is attached to. All IGMP packets snooped by the switch is forwarded to the multicast router reachable from this interface.

```
(Netgear Switch)(Interface 1/0/3)# set igmp mrouter interface
```

Web Interface: Configure the Switch with an External Multicast Router

1. Select **Switching > Multicast > Multicast Router Configuration**. A screen similar to the following displays.

The screenshot shows the 'IGMP Snooping Interface Configuration' page. The left sidebar has a tree view with 'IGMP Snooping' expanded to 'Interface Configuration'. The main content area shows a table of interfaces with columns: Interface, Admin Mode, Group Membership Interval(secs), Max Response Time(secs), Present Expiration Time(secs), and Fast Leave Admin Mode. The row for interface 1/0/3 is highlighted in orange, and its 'Admin Mode' is set to 'Enable'.

Interface	Admin Mode	Group Membership Interval(secs)	Max Response Time(secs)	Present Expiration Time(secs)	Fast Leave Admin Mode
<input checked="" type="checkbox"/> 1/0/3	Enable	260	10	0	Disable
<input type="checkbox"/> 1/0/1	Disable	260	10	0	Disable
<input type="checkbox"/> 1/0/2	Disable	260	10	0	Disable
<input type="checkbox"/> 1/0/4	Disable	260	10	0	Disable
<input type="checkbox"/> 1/0/5	Disable	260	10	0	Disable

2. Under Multicast Router Configuration, scroll down and select the Interface **1/0/3** check box. Now 1/0/3 appears in the Interface field at the top.
3. In the Admin Mode field, select **Enable**.
4. Click **Apply**.

Multicast Router Using VLAN

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

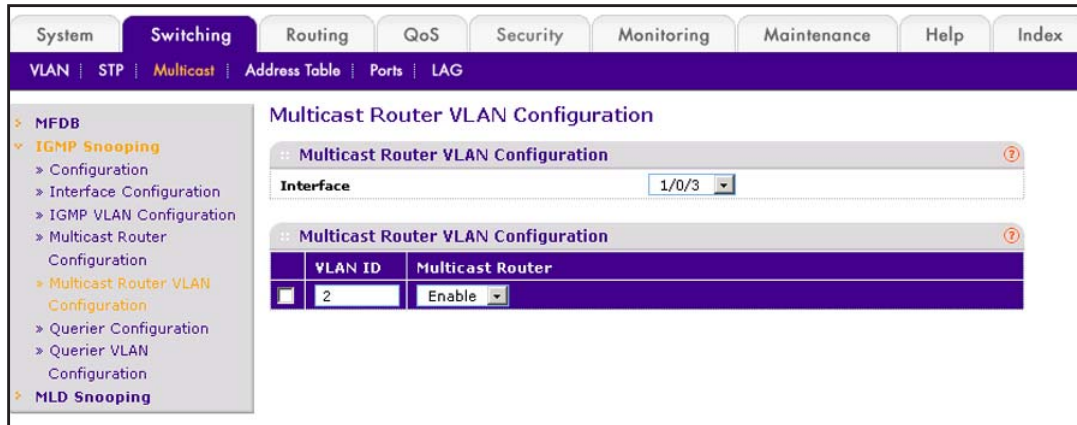
CLI: Configure the Switch with a Multicast Router Using VLAN

This example configures the interface to forward only the snooped IGMP packets that come from VLAN ID (<VLAN Id>) to the multicast router attached to this interface.

```
(Netgear Switch)(Interface 1/0/3)# set igmp mrouter 2
```


Web Interface: Configure the Switch with a Multicast Router Using VLAN

1. Select **Switching > Multicast > Multicast Router VLAN Configuration**. A screen similar to the following displays.



2. Under Multicast Router VLAN Configuration, scroll down and select the Interface **1/0/3** check box.
3. Enter the following information in the Multicast Router VLAN Configuration.
 - In the **VLAN ID** field, enter **2**.
 - In the **Multicast Router** field, select **Enable**.
4. Click **Apply**.

IGMP Querier

When the switch is used in network applications where video services such as IPTV, video streaming, and gaming are deployed, the video traffic is normally flooded to all connected ports because such traffic packets usually have multicast Ethernet addresses. IGMP snooping can be enabled to create a multicast group to direct that traffic only to those users that require it.

However, the IGMP snooping operation usually requires an extra network device—usually a router—that can generate an IGMP membership query and solicit interested nodes to

respond. With the built-in IGMP querier feature inside the switch, such an external device is no longer needed.

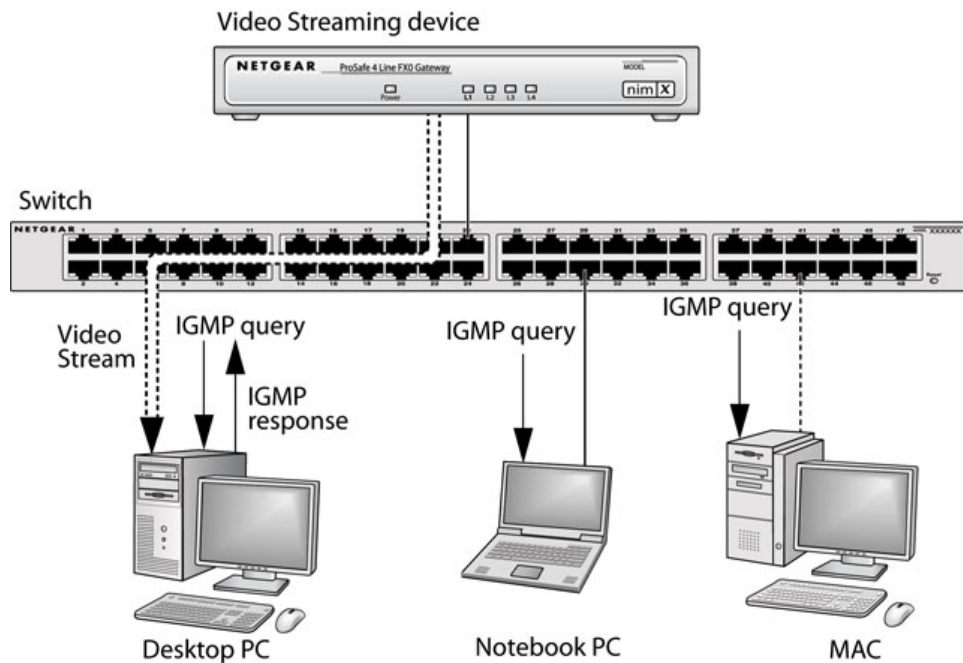


Figure 26. IGMP querier

Since the IGMP querier is designed to work with IGMP snooping, it is necessary to enable IGMP snooping when using it. The following figure shows a network application for video streaming service using the IGMP querier feature.

Enable IGMP Querier

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

CLI: Enable IGMP Querier

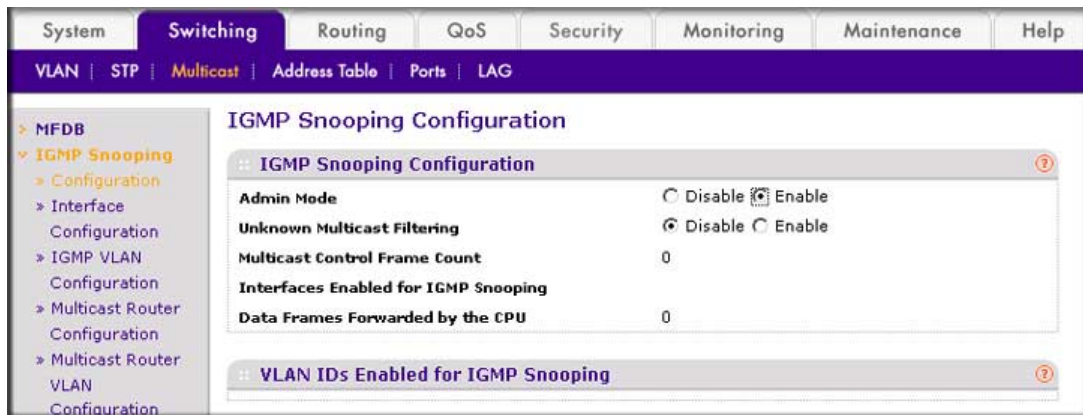
Use the following CLI commands to set up the switch to generate an IGMP querier packet for a designated VLAN. The IGMP packet will be transmitted to every port on the VLAN. The following example enables the querier for VLAN 1 and uses 10.10.10.1 as the source IP

address in querier packets. See the *Command Line Reference* for more details about other IGMP querier command options.

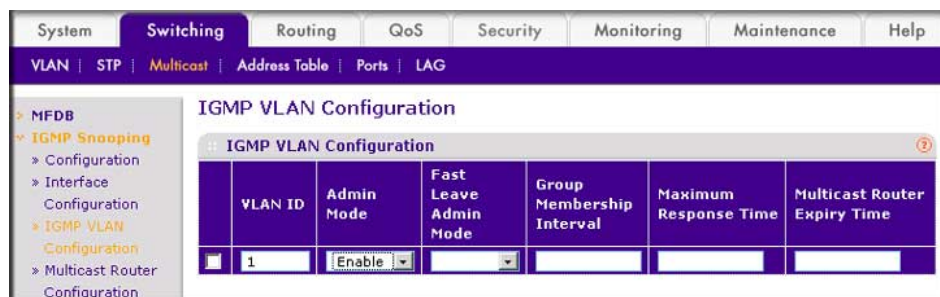
```
(Netgear switch) #vlan database
(Netgear switch) (vlan)#set igmp 1
(Netgear switch) (vlan)#set igmp querier 1
(Netgear switch) (vlan)#exit
(Netgear switch) #config
(Netgear switch) (config)#set igmp querier
(Netgear switch) (config)#set igmp querier address 10.10.10.1
(Netgear switch) (config)#exit
```

Web Interface: Enable IGMP Querier

1. Select **Switching > Multicast > IGMP VLAN Configuration**. A screen similar to the following displays.



2. Enable IGMP snooping on VLAN 1.
 - a. Select **Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration**. A screen similar to the following displays.



- b. Enter the following information:
 - In the **VLAN ID** field, enter 1.
 - In the **Admin Mode** field, select **Enable**.

- c. Click **Add**.
3. Enable the IGMP snooping querier globally.
 - a. Select **Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration**. A screen similar to the following displays.

System | **Switching** | Routing | QoS | Security | Monitoring | Maintenance | Help

VLAN | STP | **Multicast** | Address Table | Ports | LAG

MFDB

IGMP Snooping

IGMP Snooping Querier Configuration

IGMP Snooping Querier Configuration

Querier Admin Mode: Disable Enable

Querier IP Address: 10.10.10.1

IGMP Version: 2

Query Interval(secs): 60 (1 to 1800)

Querier Expiry Interval(secs): 60 (60 to 300)

VLAN Ids Enabled for IGMP Snooping Querier

- b. Enter the following information:
 - For Querier Admin Mode, select the **Enable** radio button.
 - In the **Querier IP Address** field, enter **10.10.10.1**.
- c. Click **Apply**.
4. Enable the IGMP snooping querier on VLAN 1.
 - a. Select **Switching > Multicast > IGMP Snooping Querier VLAN Configuration**. A screen similar to the following displays.

System | **Switching** | Routing | QoS | Security | Monitoring | Maintenance | Help | Index

VLAN | STP | **Multicast** | Address Table | Ports | LAG

MFDB

IGMP Snooping

IGMP Snooping Querier VLAN Configuration

IGMP Snooping Querier VLAN Configuration

VLAN ID	Querier Election Participate Mode	Querier VLAN Address	Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Max Response Time
1							

- b. In the **VLAN ID** field, enter **1**.
5. Click **Add**.

Show IGMP Querier Status

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

CLI: Show IGMP Querier Status

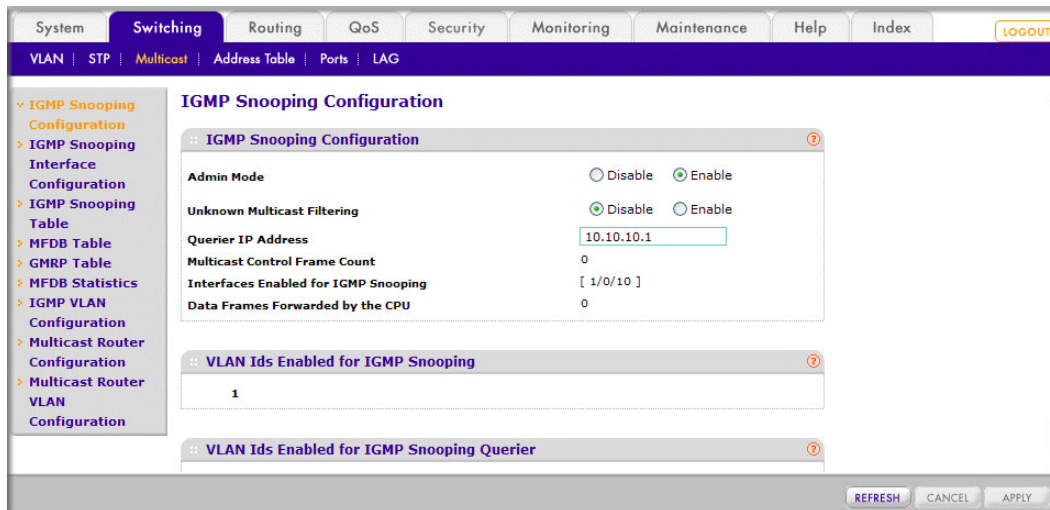
To see the IGMP querier status, use the following command.

```
(Netgear Switch) #show igmpsnooping querier vlan 1
VLAN 1 : IGMP Snooping querier status
-----
IGMP Snooping Querier VLAN Mode..... Enable
Querier Election Participate Mode..... Disable
Querier VLAN Address..... 0.0.0.0
Operational State..... Disabled
Operational version..... 2
```

The command shows that the IGMP admin mode is Active. The mode is controlled by the **set igmp** command. If the mode is inactive, no query packet is sent.

Web Interface: Show IGMP Querier Status

1. Select **Switching > Multicast > IGMP Snooping Configuration**. A screen similar to the following displays.



2. Click **Refresh**.

This chapter provides the following examples:

- *Configure MVR in Compatible Mode*
- *Configure MVR in Dynamic Mode*

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 multicasts traffic to all ports even if there are receivers connected to only a few ports.

To fix this problem, the IGMP Snooping protocol was developed. But the problem reappears when receivers are in different VLANs. Multicast VLAN Registration (MVR) is intended to solve the problem of receivers in different VLANs. It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.

MVR, like the IGMP Snooping protocol, allows a Layer 2 switch to snoop on the IGMP control protocol. Both protocols operate independently of each other. Both protocols can be enabled on the switch interfaces at the same time. In such a case, MVR listens to the join and report messages only for groups configured statically. All other groups are managed by IGMP snooping.

There are two types of MVR ports: source and receiver.

- The source port is the port to which the multicast traffic flows using the multicast VLAN.
- The receiver port is the port where a listening host is connected to the switch. It can utilize any (or no) VLAN, except the multicast VLAN. This implies that the MVR switch performs VLAN tag substitution from the multicast VLAN source port to the VLAN tag used by the receiver port.

The Multicast VLAN is the VLAN that is configured in the specific network for MVR purposes. It has to be manually specified by the operator for all source ports in the network. It is a VLAN that is used to transfer multicast traffic over the network to avoid duplication of

multicast streams for clients in different VLANs. A diagram of a network configured for MVR is shown in the following illustration. SP is the source port and RP is the receiver port.

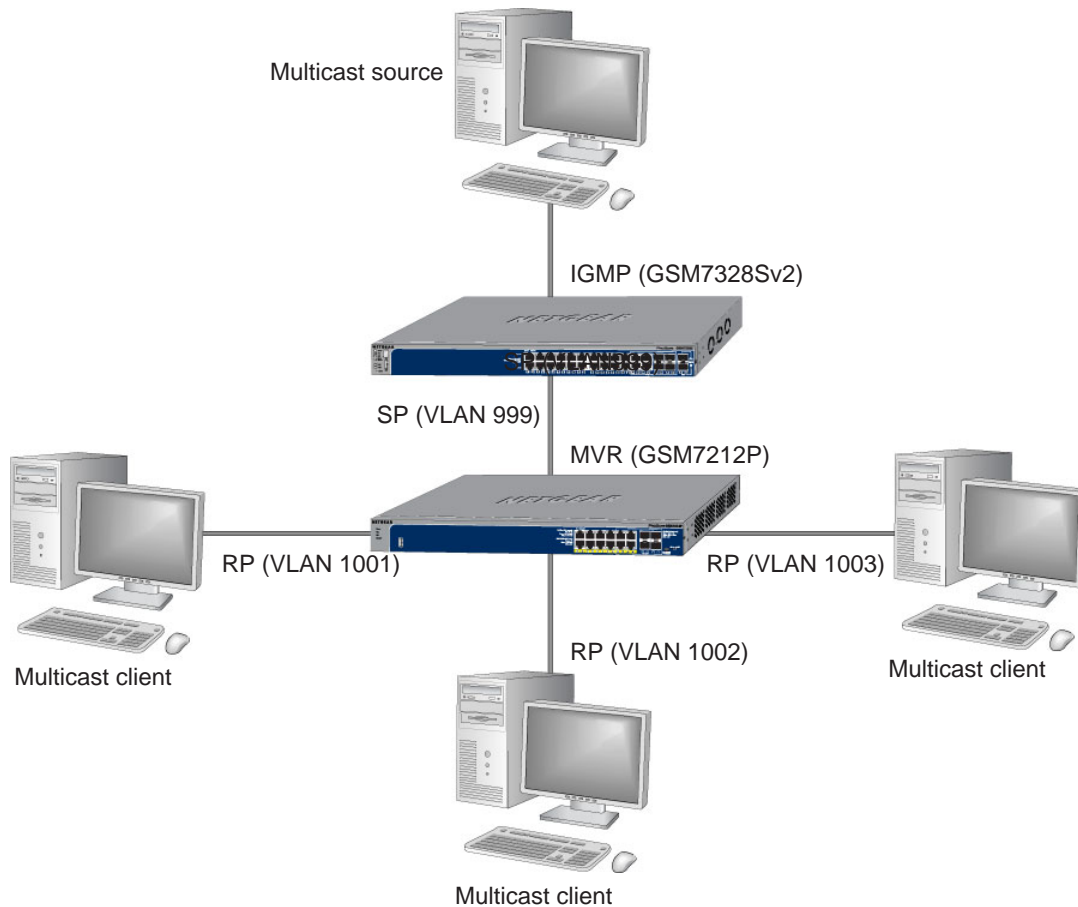


Figure 27. Network configured for MVR

Note: The following examples show how to configure the MVR on the MVR switch (GSM7212P in this case).

Configure MVR in Compatible Mode

In compatible mode, the MVR switch does not learn multicast groups; the groups have to be configured by the operator as the MVR does not forward IGMP reports from the hosts (RP port) to the IGMP router (SP port). To operate in this mode, the IGMP router has to be statically configured to transmit all required multicast streams to the MVR switch.

CLI: Configure MVR in Compatible Mode

1. Create MVlan, VLAN1, VLAN2, and VLAN3.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 999,1001, 1002, 1003
(Netgear Switch) (Vlan)#vlan name 999 mVlan
(Netgear Switch) (Vlan)#vlan name 1001 Vlan1
(Netgear Switch) (Vlan)#vlan name 1002 Vlan2
(Netgear Switch) (Vlan)#vlan name 1003 Vlan3
(Netgear Switch) (Vlan)#exit
```

2. Enable MVR, configure VLAN 999 as a multicast VLAN, and add group 224.1.2.3 to MVR.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#mvr
(Netgear Switch) (Config)#mvr vlan 999
(Netgear Switch) (Config)#mvr group 224.1.2.3
```

3. Configure multicast VLAN on the source port.

```
(Netgear Switch) (Config)#interface 0/9
(Netgear Switch) (Interface 0/9)#vlan participation include 999
(Netgear Switch) (Interface 0/9)#vlan tagging 999
(Netgear Switch) (Interface 0/9)#mvr
(Netgear Switch) (Interface 0/9)#mvr type source
(Netgear Switch) (Interface 0/9)#exit
```

4. Configure the receive ports.

Note: The receive port can participate in only one VLAN.

```
(Netgear Switch) (Config)#interface 0/1
(Netgear Switch) (Interface 0/1)#vlan participation include 1001
(Netgear Switch) (Interface 0/1)#vlan pvid 1001
(Netgear Switch) (Interface 0/1)#vlan participation exclude 1
(Netgear Switch) (Interface 0/1)#mvr
(Netgear Switch) (Interface 0/1)#mvr type receiver
(Netgear Switch) (Interface 0/1)#mvr vlan 999 group 224.1.2.3
(Netgear Switch) (Interface 0/1)#exit

(Netgear Switch) (Config)#interface 0/5
(Netgear Switch) (Interface 0/5)#vlan participation include 1002
(Netgear Switch) (Interface 0/5)#vlan pvid 1002
(Netgear Switch) (Interface 0/5)#vlan participation exclude 1
(Netgear Switch) (Interface 0/5)#mvr
(Netgear Switch) (Interface 0/5)#mvr stype receiver
(Netgear Switch) (Interface 0/5)#mvr vlan 999 group 224.1.2.3
(Netgear Switch) (Interface 0/5)#exit

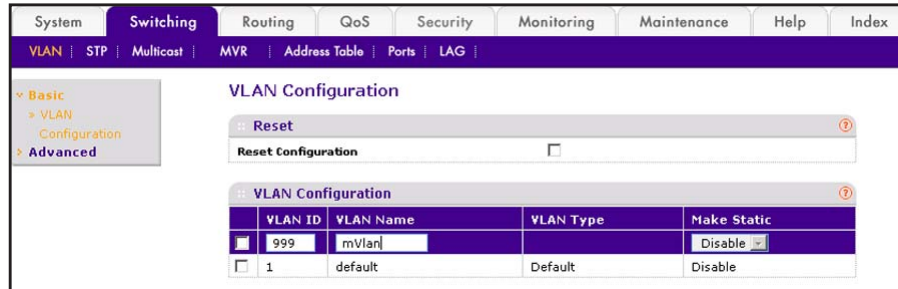
(Netgear Switch) (Config)#interface 0/7
(Netgear Switch) (Interface 0/7)#vlan participation include1003
(Netgear Switch) (Interface 0/7)#vlan pvid 1003
(Netgear Switch) (Interface 0/7)#vlan participation exclude 1
(Netgear Switch) (Interface 0/7)#mvr
(Netgear Switch) (Interface 0/7)#mvr type receiver
(Netgear Switch) (Interface 0/7)#mvr vlan 999 group 224.1.2.3
(Netgear Switch) (Interface 0/7)#exit
```

5. Show mvr status.

```
(Netgear Switch) #show mvr
MVR Running..... TRUE
MVR multicast VLAN..... 999
MVR Max Multicast Groups..... 256
MVR Current multicast groups..... 1
MVR Global query response time... 5 (tenths of sec)
MVR Mode..... compatible
(Netgear Switch) #show mvr interface
Port          Type          Status          Immediate Leave
-----
0/1           RECEIVER     ACTIVE/InVLAN   DISABLED
0/5           RECEIVER     ACTIVE/InVLAN   DISABLED
0/7           RECEIVER     ACTIVE/InVLAN   DISABLED
0/9           SOURCE       ACTIVE/InVLAN   DISABLED
```

Web Interface: Configure MVR in Compatible Mode

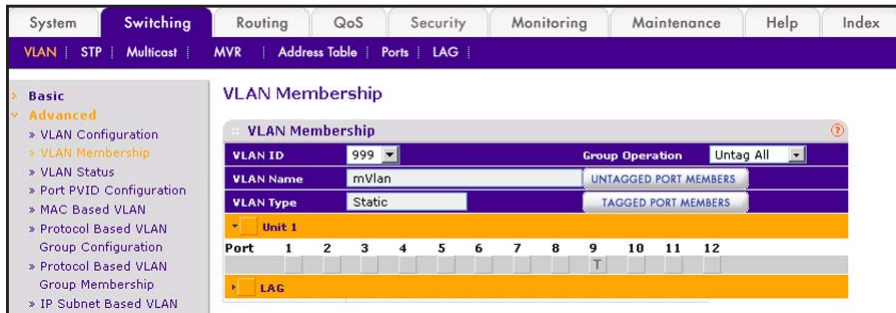
1. Create MVLAN 999, VLAN1 1001, VLAN2 1002 and VLAN3 1003.
 - a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays:



- b. In the VLAN ID field, enter **999**, and in the VLAN Name field, enter **mVlan**.
 - c. Click **Add**.
 - d. Repeat step b and c to create VLAN1 1001, VLAN2 1002, and VLAN3 1003.

2. Add port 9 into MVLAN 999 with tagged mode.

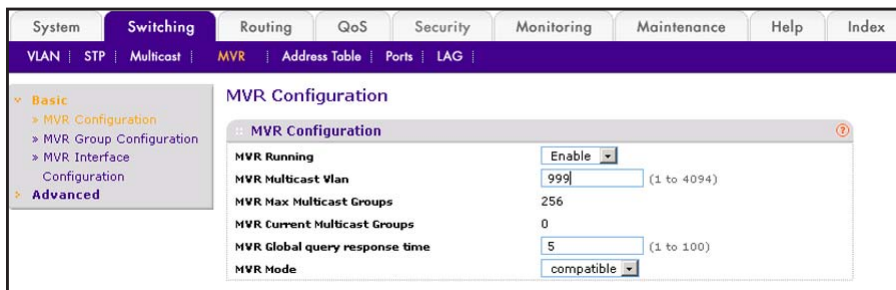
- a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays:



- b. In the VLAN ID list, select **999**.
- c. Click **Unit 1**. The ports display.
- d. Click the gray box under port 9 until T displays. The T specifies that the egress packet is tagged for the ports.
- e. Click **Apply** to save the settings.
- f. Repeat steps from b to e, add port 0/1 to VLAN1 1001, add port 0/5 to VLAN2 1002, and add port 0/7 to VLAN3 1003.

3. Enable MVR and multicast VLAN

- a. Select **Switching > MVR > Basic > MVR Configuration**. A screen similar to the following displays:



- b. For MVR Running, select **Enable**.
- c. In the MVR Multicast VLAN field, enter **999**.
- d. Click **Apply**.

4. Add multicast group 224.1.2.3 to MVR.
 - a. Select **Switching > MVR > Basic > MVR Group Configuration**. A screen similar to the following displays:

MVR Group IP	Status	Members
224.1.2.3		

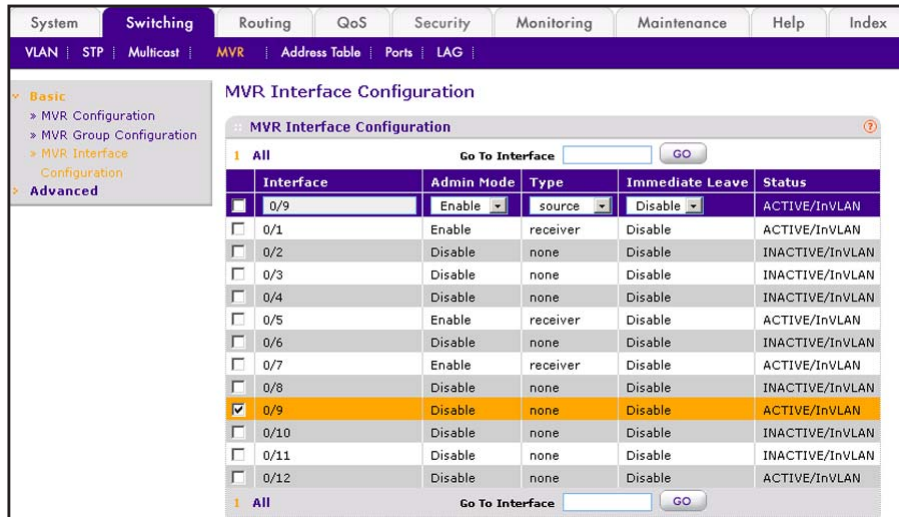
- b. In the the MVR Group IP field, enter **224.1.2.3**.
 - c. Click **Add**.
5. Configure a receiver on interface 0/1, 0/5, and 0/7.
 - a. Select **Switching > MVR > Basic > MVR Interface Configuration**. A screen similar to the following displays:

Interface	Admin Mode	Type	Immediate Leave	Status
<input checked="" type="checkbox"/> 0/1	Enable	Receiver	Disable	ACTIVE/InVLAN
<input type="checkbox"/> 0/2	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/> 0/3	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/> 0/4	Disable	none	Disable	INACTIVE/InVLAN
<input checked="" type="checkbox"/> 0/5	Disable	Receiver	Disable	ACTIVE/InVLAN
<input type="checkbox"/> 0/6	Disable	none	Disable	INACTIVE/InVLAN
<input checked="" type="checkbox"/> 0/7	Disable	Receiver	Disable	ACTIVE/InVLAN
<input type="checkbox"/> 0/8	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/> 0/9	Disable	none	Disable	ACTIVE/InVLAN
<input type="checkbox"/> 0/10	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/> 0/11	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/> 0/12	Disable	none	Disable	ACTIVE/InVLAN

- b. Under MVR Interface Configuration, scroll down and select the Interface **0/1**, **0/5** and **0/7** check boxes.
 - c. Enter the following information:
 - In the Admin Mode list, select **Enable**.
 - In the Type list, select **Receiver**.
 - d. Click **Apply** to save the settings.

6. Configure source interface.

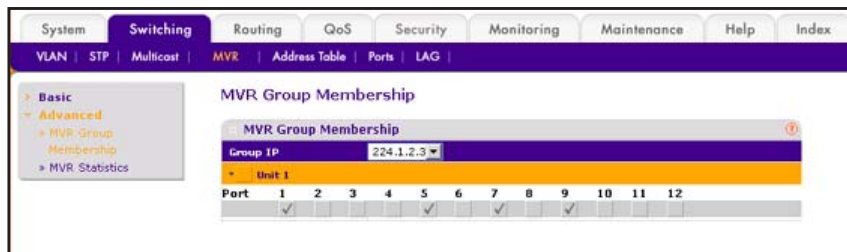
- a. Select **Switching > MVR > Basic > MVR Interface Configuration**. A screen similar to the following displays:



- b. Under MVR Interface Configuration, scroll down and select the Interface **0/9** check box.
- c. Enter the following information:
 - In the Admin Mode list, select **Enable**.
 - In the Type list, select **source**.
- d. Click **Apply** to save the settings.

7. Configure MVR Group Membership.

- a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays:



- b. In the Group IP list, select **224.1.2.3**.
- c. Click **Unit 1**. The ports display.
- d. Click the gray boxes under ports **1, 5, and 7**. (Port 9 is already in MVR group 224.1.2.3 because it is configured as the source port.)
- e. Click **Apply** to save the settings.

Configure MVR in Dynamic Mode

CLI: Configure MVR in Dynamic Mode

In dynamic mode, the MVR switch learns existing multicast groups by snooping the IGMP queries from router on source ports and forwarding the IGMP reports from the hosts to the IGMP router on the Multicast VLAN (with appropriate translation of the VLAN ID).

1. Create MVLAN, VLAN1, VLAN2, and VLAN3.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 999,1001, 1002, 1003
(Netgear Switch) (Vlan)#vlan name 999 mVlan
(Netgear Switch) (Vlan)#vlan name 1001 Vlan1
(Netgear Switch) (Vlan)#vlan name 1002 Vlan2
(Netgear Switch) (Vlan)#vlan name 1003 Vlan3
(Netgear Switch) (Vlan)#exit
```

2. Enable MVR, configure VLAN 999 as a multicast VLAN, and add group 224.1.2.3 to MVR.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#mvr
(Netgear Switch) (Config)#mvr vlan 999
(Netgear Switch) (Config)#mvr group 224.1.2.3
```

3. Configure MVR in dynamic mode.

```
(Netgear Switch) (Config)#mvr mode dynamic
```

4. Configure multicast VLAN on the source port.

```
(Netgear Switch) (Config)#interface 0/9
(Netgear Switch) (Interface 0/9)#vlan participation include 999
(Netgear Switch) (Interface 0/9)#vlan tagging 999
(Netgear Switch) (Interface 0/9)#mvr
(Netgear Switch) (Interface 0/9)#mvr type source
(Netgear Switch) (Interface 0/9)#exit
```

5. Configure the receive ports.

Note: A receive port can participate in only one VLAN.

```
(Netgear Switch) (Config)#interface 0/1
(Netgear Switch) (Interface 0/1)#vlan participation include 1001
(Netgear Switch) (Interface 0/1)#vlan pvid 1001
(Netgear Switch) (Interface 0/1)#vlan participation exclude 1
(Netgear Switch) (Interface 0/5)#mvr
(Netgear Switch) (Interface 0/1)#mvr type receiver
(Netgear Switch) (Interface 0/1)#exit

(Netgear Switch) (Config)#interface 0/5
(Netgear Switch) (Interface 0/5)#vlan participation include 1002
(Netgear Switch) (Interface 0/5)#vlan pvid 1002
(Netgear Switch) (Interface 0/5)#vlan participation exclude 1
(Netgear Switch) (Interface 0/5)#mvr
(Netgear Switch) (Interface 0/5)#mvr stype receiver
(Netgear Switch) (Interface 0/5)#exit

(Netgear Switch) (Config)#interface 0/7
(Netgear Switch) (Interface 0/7)#vlan participation include1003
(Netgear Switch) (Interface 0/7)#vlan pvid 1003
(Netgear Switch) (Interface 0/7)#vlan participation exclude 1
(Netgear Switch) (Interface 0/7)#mvr
(Netgear Switch) (Interface 0/7)#mvr type receiver
(Netgear Switch) (Interface 0/7)#exit
```

6. Show the MVR status.

```
(Netgear Switch) #show mvr
MVR Running..... TRUE
MVR multicast VLAN..... 999
MVR Max Multicast Groups..... 256
MVR Current multicast groups..... 1
MVR Global query response time... 5 (tenths of sec)
MVR Mode..... compatible
(Netgear Switch) #show mvr interface
```

Port	Type	Status	Immediate Leave
0/1	RECEIVER	ACTIVE/InVLAN	DISABLED
0/5	RECEIVER	ACTIVE/InVLAN	DISABLED
0/7	RECEIVER	ACTIVE/InVLAN	DISABLED
0/9	SOURCE	ACTIVE/InVLAN	DISABLED

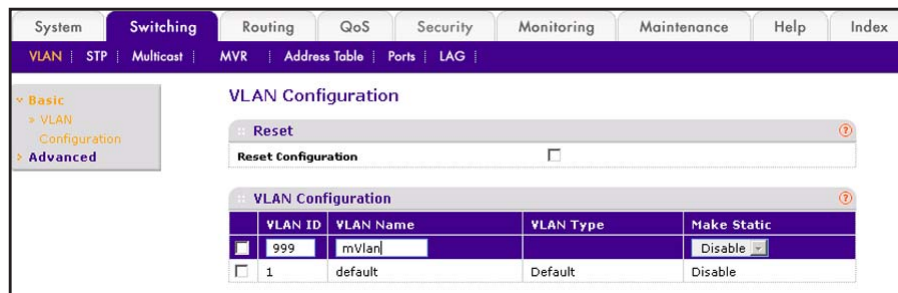
7. After port 0/1 receive IGMP report for Multicast Group 224.1.2.3, it will be added to the MVR Group 224.1.2.3.

```
(Netgear Switch) #show mvr members
```

MVR Group IP	Status	Members
224.1.2.3	ACTIVE	0/1(d)

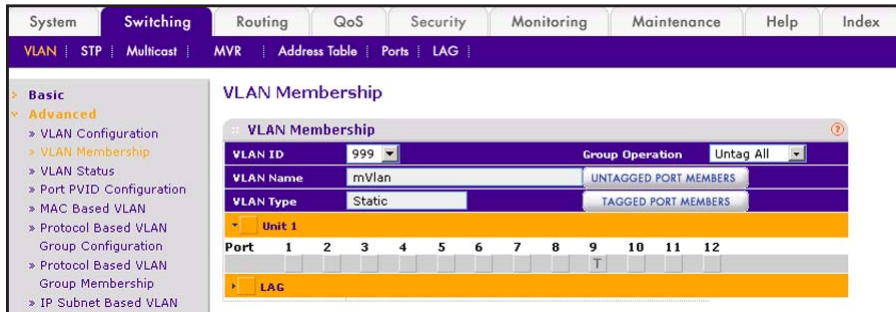
Web Interface: Configure MVR in Dynamic Mode

1. Create MVLAN 999, VLAN1 1001, VLAN2 1002, and VLAN3 1003.
 - a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays:

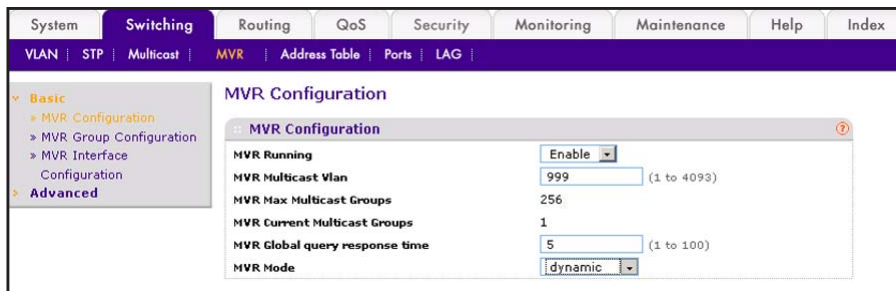


- b. In the VLAN ID field, enter **999**, and in the VLAN Name field, enter **mVlan**.
 - c. Click **Add**.
 - d. Repeat step b and c to create VLAN1 1001, VLAN2 1002, and VLAN3 1003.
 - e. Add port 9 into MVLAN 999 with tagged mode.

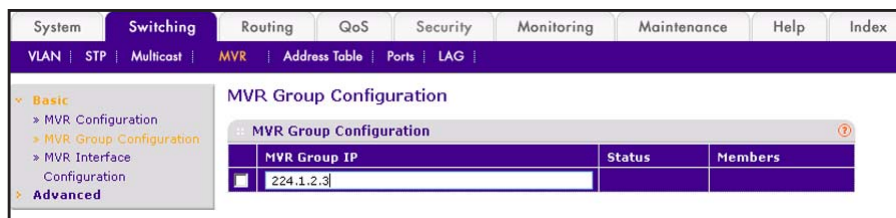
- f. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays:



- g. In the VLAN ID list, select **999**.
 - h. Click **Unit 1**. The ports display.
 - i. Click the gray boxes under port **9** until T displays. The T specifies that the egress packet is tagged for the ports.
 - j. Click **Apply** to save the settings.
 - k. Repeat steps from b to e, add port 0/1 to VLAN1 1001, add port 0/5 to VLAN2 1002, and add port 0/7 to VLAN3 1003.
2. Enable MVR and multicast VLAN.
 - a. Select **Switching > MVR > Basic > MVR Configuration**. A screen similar to the following displays:



- b. From the MVR Running list, select **Enable**.
 - c. In the MVR Multicast Vlan field, enter **999**.
 - d. From the MVR mode list, select **dynamic**.
 - e. Click **Apply**.
3. Add multicast group 224.1.2.3 to the MVR.
 - a. Select **Switching > MVR > Basic > MVR Group Configuration**. A screen similar to the following displays:



- b. In the MVR Group IP field, enter **224.1.2.3**.
 - c. Click **Add**.
4. Configure a receiver on interface 0/1, 0/5 and 0/7.
 - a. Select **Switching > MVR > Basic > MVR Interface Configuration**. A screen similar to the following displays:

The screenshot shows the 'MVR Interface Configuration' page. The table below represents the data shown in the interface:

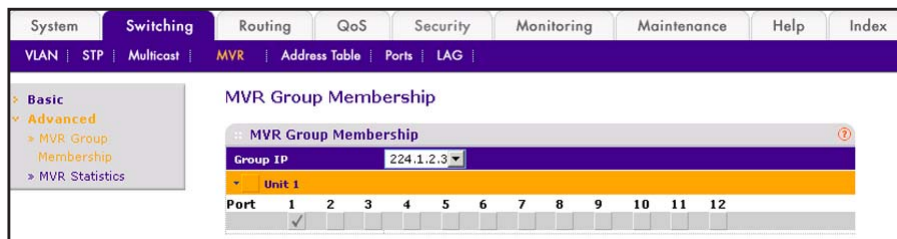
Interface	Admin Mode	Type	Immediate Leave	Status
<input checked="" type="checkbox"/> 0/1	Enable	receiver	Disable	ACTIVE/InVLAN
<input type="checkbox"/> 0/2	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/> 0/3	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/> 0/4	Disable	none	Disable	INACTIVE/InVLAN
<input checked="" type="checkbox"/> 0/5	Disable	none	Disable	ACTIVE/InVLAN
<input type="checkbox"/> 0/6	Disable	none	Disable	INACTIVE/InVLAN
<input checked="" type="checkbox"/> 0/7	Disable	none	Disable	ACTIVE/InVLAN
<input type="checkbox"/> 0/8	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/> 0/9	Disable	none	Disable	ACTIVE/InVLAN
<input type="checkbox"/> 0/10	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/> 0/11	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/> 0/12	Disable	none	Disable	ACTIVE/InVLAN

- b. Under MVR Interface Configuration, scroll down and select the Interface **0/1**, **0/5** and **0/7** check boxes
 - c. Enter the following information:
 - In the Admin Mode list, select **Enable**.
 - In the Type list, select **Receiver**.
 - d. Click **Apply** to save the settings.
5. Configure a source interface.
 - a. Select **Switching > MVR > Basic > MVR Interface Configuration**. A screen similar to the following displays:

The screenshot shows the 'MVR Interface Configuration' page. The table below represents the data shown in the interface:

Interface	Admin Mode	Type	Immediate Leave	Status
<input checked="" type="checkbox"/> 0/9	Enable	source	Disable	ACTIVE/InVLAN
<input type="checkbox"/> 0/1	Enable	receiver	Disable	ACTIVE/InVLAN
<input type="checkbox"/> 0/2	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/> 0/3	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/> 0/4	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/> 0/5	Enable	receiver	Disable	ACTIVE/InVLAN
<input type="checkbox"/> 0/6	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/> 0/7	Enable	receiver	Disable	ACTIVE/InVLAN
<input type="checkbox"/> 0/8	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/> 0/10	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/> 0/11	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/> 0/12	Disable	none	Disable	ACTIVE/InVLAN

- b. Under MVR Interface Configuration, scroll down and select the Interface **0/9** check box.
 - c. Enter the following information:
 - In the Admin Mode list, select **Enable**.
 - In the Type list, select **source**.
 - d. Click **Apply** to save the settings.
6. After port 1 receives an IGMP report for multicast group 224.1.2.3, it is added into MVR group 224.1.2.3.
- a. Select **Switching > MVR > Advanced > MVR Group Membership**. A screen similar to the following displays:



In this chapter, examples are provided for the following topics:

- *Port Security*
- *Set the Dynamic and Static Limit on Port 1/0/1* on page 261
- *Convert the Dynamic Address Learned from 1/0/1 to a Static Address* on page 263
- *Create a Static Address* on page 264
- *Protected Ports* on page 264
- *802.1x Port Security* on page 271
- *Create a Guest VLAN* on page 277
- *Assign VLANs Using RADIUS* on page 282
- *Dynamic ARP Inspection* on page 288
- *Static Mapping* on page 294
- *DHCP Snooping* on page 296
- *Enter Static Binding into the Binding Database* on page 299
- *Maximum Rate of DHCP Messages* on page 300
- *IP Source Guard* on page 302

Port Security

Port Security helps secure the network by preventing unknown devices from forwarding packets. When a link goes down, all dynamically locked addresses are freed. The port security feature offers the following benefits:

- You can limit the number of MAC addresses on a given port. Packets that have a matching MAC address (secure packets) are forwarded; all other packets (unsecure packets) are restricted.
- You can enable port security on a per port basis.

Port security implements two traffic filtering methods, dynamic locking and static locking. These methods can be used concurrently.

- **Dynamic locking.** You can specify the maximum number of MAC addresses that can be learned on a port. The maximum number of MAC addresses is platform dependent and is

given in the software Release Notes. After the limit is reached, additional MAC addresses are not learned. Only frames with an allowable source MAC addresses are forwarded.

Note: If you want to set a specific MAC address for a port, set the dynamic entries to 0, then allow only packets with a MAC address matching the MAC address in the static list.

Dynamically locked addresses can be converted to statically locked addresses. Dynamically locked MAC addresses are aged out if another packet with that address is not seen within the age-out time. You can set the time out value. Dynamically locked MAC addresses are eligible to be learned by another port. Static MAC addresses are not eligible for aging.

- **Static locking.** You can manually specify a list of static MAC addresses for a port. Dynamically locked addresses can be converted to statically locked addresses.

Set the Dynamic and Static Limit on Port 1/0/1

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

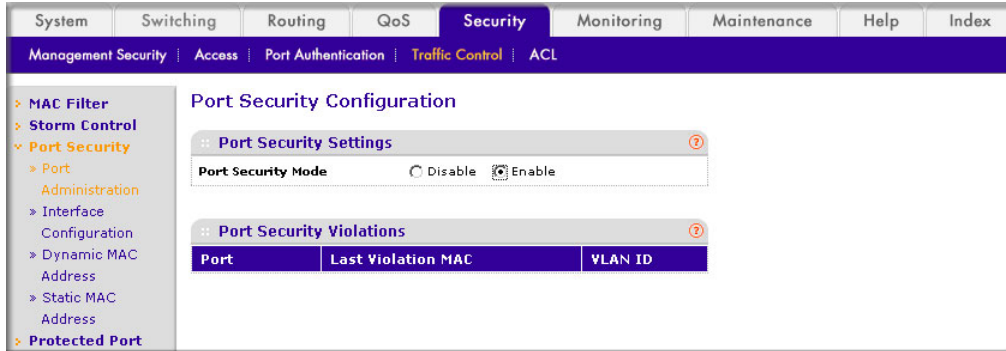
CLI: Set the Dynamic and Static Limit on Port 1/0/1

```
(Netgear Switch) (Config)#port-security
Enable port-security globally
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#port-security
Enable port-security on port 1/0/1
(Netgear Switch) (Interface 1/0/1)#port-security max-dynamic 10
Set the dynamic limit to 10
(Netgear Switch) (Interface 1/0/1)#port-security max-static 3
Set the static limit to 3
(Netgear Switch) (Interface 1/0/1)#ex
(Netgear Switch) (Config)#ex
(Netgear Switch) #show port-security 1/0/1
```

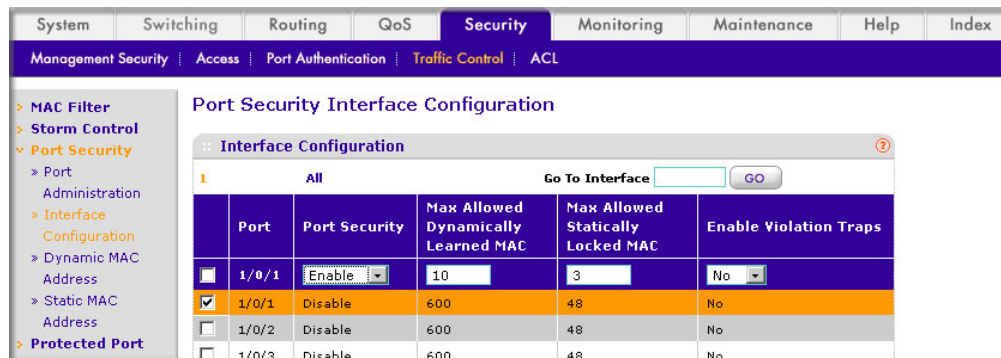
Intf	Admin Mode	Dynamic Limit	Static Limit	Violation Trap Mode
1/0/1	Disabled	10	3	Disabled

Web Interface: Set the Dynamic and Static Limit on Port 1/0/1

1. Select **Security > Traffic Control > Port Security >Port Administrator**. A screen similar to the following displays.



- b. Under Port Security Configuration, next to Port Security Mode, select the **Enable** radio button.
 - c. Click **Apply** to save the settings.
2. Set the dynamic and static limit on the port 1/0/1:
 - a. Select **Security > Traffic Control > Port Security >Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Interface **1/0/1** check box. Now 1/0/1 appears in the Interface field at the top.
- c. Enter the following information:
 - In the **Port Security** field, select **Enable**.
 - In the **Max Allowed Dynamically Learned MAC** field, enter **10**.
 - In the **Max Allowed Statically Locked MAC** field, enter **3**.
- d. Click **Apply** to save the settings.

Convert the Dynamic Address Learned from 1/0/1 to a Static Address

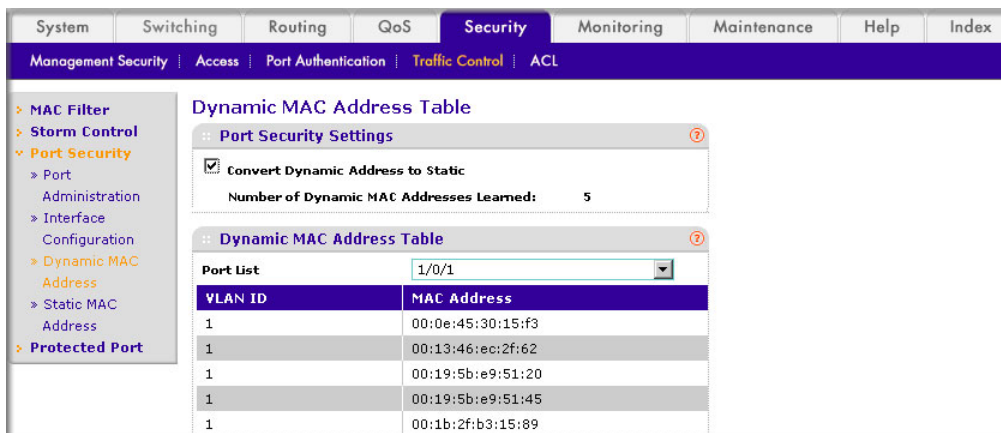
The example is shown as CLI commands and as a Web interface procedure.

CLI: Convert the Dynamic Address Learned from 1/0/1 to the Static Address

```
(Netgear Switch)(Interface 1/0/1)#port-security mac-address move
Convert the dynamic address learned from 1/0/1 to the static address
(Netgear Switch)(Interface 1/0/1)#exit
(Netgear Switch)(Config)#exit
(Netgear Switch)#show port-security static 1/0/1
Number of static MAC addresses configured: 3
Statically configured MAC Address VLAN ID
-----
00:0E:45:30:15:F3 1
00:13:46:EC:2F:62 1
00:14:6C:E8:81:23 1
```

Web Interface: Convert the Dynamic Address Learned from 1/0/1 to the Static Address

1. Select **Security > Traffic Control > Port Security > Dynamic MAC Address**. A screen similar to the following displays.



2. Under Port Security Configuration, in the **Port List** field, select **1/0/1**.
3. Select the **Convert Dynamic Address to Static** check box.
4. Click **Apply** to save the settings.

Create a Static Address

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

CLI: Create a Static Address

```
(Netgear Switch) (Interface 1/0/1)#port-security mac-address 00:13:00:01:02:03
```

Web Interface: Create a Static Address

1. Select **Security > Traffic Control > Port Security > Static MAC address**. A screen similar to the following displays.

Static MAC Address		Vlan ID
<input checked="" type="checkbox"/>	00:13:00:01:02:03	3
<input type="checkbox"/>	00:0E:45:30:15:F3	1
<input type="checkbox"/>	00:13:46:EC:2F:62	1
<input type="checkbox"/>	00:14:6C:E8:81:23	1

2. Under Port List, in the **Interface** list, select **1/0/1**.
3. In the Static MAC Address section of the screen, enter the following information:
 - In the **Static MAC Address** field, enter **00:13:00:01:02:03**.
 - In the **Vlan ID** list, select **3**.
4. Click **Add**.

Protected Ports

This section describes how to set up protected ports on the switch. Some situations might require that traffic is prevented from being forwarded between any ports at Layer 2 so that one user cannot see the traffic of another user on the same switch. Protected ports can:

- Prevent traffic from being forwarded between protected ports.
- Allow traffic to be forwarded between a protected port and a non-protected port.

In following example, PC 1 and PC 2 can access the Internet as usual, but PC 1 cannot see the traffic that is generated by PC 2, that is, no traffic is forwarded between PC 1 and PC 2.

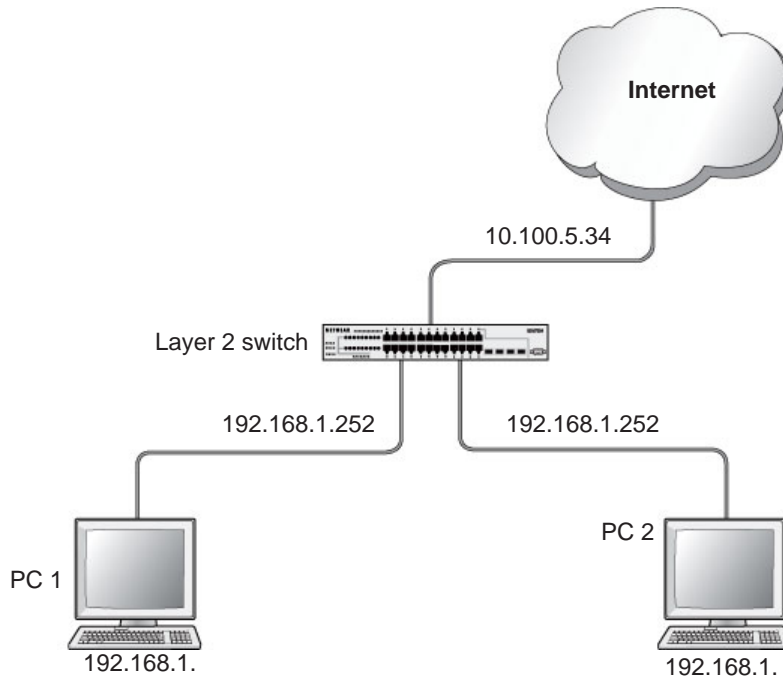


Figure 28. Protected ports

CLI: Configure a Protected Port to Isolate Ports on the Switch

1. Create one VLAN 192 including PC 1 and PC 2.

```
(Netgear Switch) #vlan database
(Netgear Switch) #vlan 192
(Netgear Switch) #vlan routing 192
(Netgear Switch) #exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/23
(Netgear Switch) (Interface 1/0/23)#vlan pvid 192
(Netgear Switch) (Interface 1/0/23)#vlan participation include 192
(Netgear Switch) (Interface 1/0/23)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan pvid 192
(Netgear Switch) (Interface 1/0/24)#vlan participation include 192
(Netgear Switch) (Interface 1/0/24)#exit
(Netgear Switch) (Interface-vlan 192)#interface vlan 192
(Netgear Switch) (Interface-vlan 192)#routing
(Netgear Switch) (Interface-vlan 192)#ip address 192.168.1.254 255.255.255.0
(Netgear Switch) (Interface-vlan 192)#exit
```

2. Create one VLAN 202 connected to the Internet.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 202
(Netgear Switch) (Vlan)#vlan routing 202
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan pvid 202
(Netgear Switch) (Interface 1/0/48)#vlan participation include 202
(Netgear Switch) (Interface 1/0/48)#exit
(Netgear Switch) (Config)#interface vlan 202
(Netgear Switch) (Interface-vlan 202)#routing
(Netgear Switch) (Interface-vlan 202)ip address 10.100.5.34 255.255.255.0
(Netgear Switch) (Interface-vlan 202)#exit
```

3. Create a DHCP pool to allocated IP addresses to PCs.

```
(Netgear Switch) (config)#service dhcp
(Netgear Switch) (config)#ip dhcp pool pool-a
(Netgear Switch) (Config-dhcp-pool)#dns-server 12.7.210.170
(Netgear Switch) (Config-dhcp-pool)#default-router 192.168.1.254
(Netgear Switch) (Config-dhcp-pool)#network 192.168.1.0 255.255.255.0
(Netgear Switch) (Config-dhcp-pool)#exit
```

4. Enable IP routing and configure a default route.

```
(Netgear Switch)(config)#ip routing
(Netgear Switch)(config)#ip route 0.0.0.0 0.0.0.0 10.100.5.252
```

5. Enable a protected port on 1/0/23 and 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/23
(Netgear Switch) (Interface 1/0/23)#switchport protected
(Netgear Switch) (Interface 1/0/23)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#switchport protected
(Netgear Switch) (Interface 1/0/24)#exit
```

Web Interface: Configure a Protected Port to Isolate Ports on the Switch

1. Create a DHCP pool:

Note: This example assumes that the DHCP service is enabled. For information about how to enable the DHCP service, see the Web interface procedure in *Configure a DHCP Server in Dynamic Mode* on page 373.

- a. Select **System > Services > DHCP Server > DHCP Server Configuration**. A screen similar to the following displays.

The screenshot shows the DHCP Pool Configuration web interface. The navigation menu on the left includes: System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Management, Device View, Services, Stacking, and SNMP. Under Services, the DHCP Server configuration options are: DHCP Server Configuration, DHCP Pool Configuration (selected), DHCP Pool Options, DHCP Server Statistics, DHCP Bindings, DHCP Conflicts, DHCP Relay, and UDP Relay. The DHCP Pool Configuration form includes the following fields:

- Pool Name: pool_a
- Type of Binding: Dynamic
- Network Number: 192.168.1.0
- Network Mask: 255.255.255.0
- Network Prefix Length: (0-32)
- Client Name: (empty)
- Hardware Address: (empty)
- Hardware Address Type: ethernet
- Client ID: (empty)
- Host Number: (empty)
- Host Mask: (empty)
- Host Prefix Length: (0-32)
- Lease Time: Specified Duration
- Days: 1 (0 to 59)
- Hours: 0 (0 to 1439)
- Minutes: 0 (0 to 86399)
- Default Router Addresses: 192.168.1.254
- DNS Server Addresses: 12.7.210.170

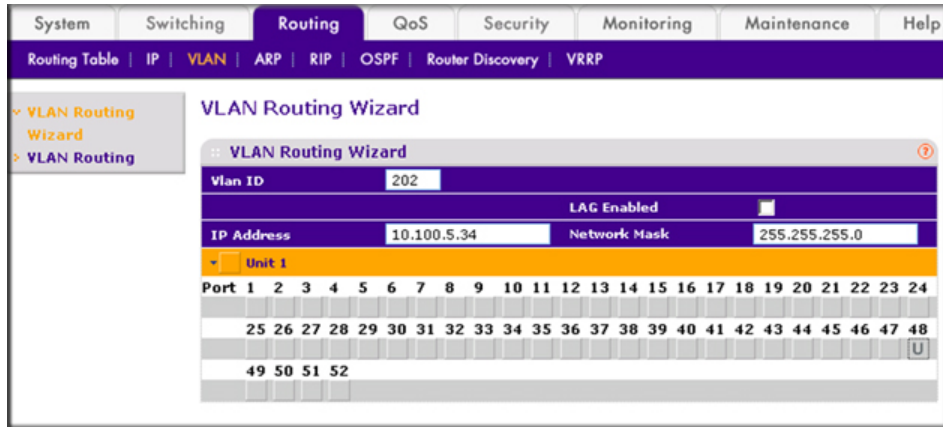
- b. Under DHCP Pool Configuration, enter the following information:
 - In the **Pool Name** field, select **Create**.
 - In the **Pool Name** field, enter **pool-a**.
 - In the **Type of Binding** field, select **Dynamic**.

- In the **Network Number** field, enter **192.168.1.0**.
 - In the **Network Mask** field, enter **255.255.255.0**.
 - In the **Days** field, enter **1**.
 - Click **Default Router Addresses**. The DNS server address fields display. In the first **Router Address** field, enter **192.168.1.254**.
 - Click **DNS Server Addresses**. The router address fields display. In the first **DNS Server Address** field, enter **12.7.210.170**.
- c. Click **Add**.
2. Configure a VLAN and include ports 1/0/23 and 1/0/24 in the VLAN:
- a. Select **Routing > VLAN > VLAN Routing Wizard**. A screen similar to the following displays.

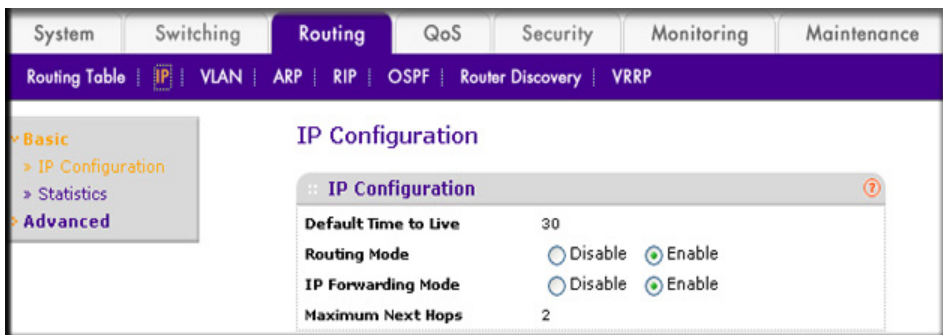
Vlan ID		IP Address		Network Mask	LAG Enabled																			
192		192.168.1.254		255.255.255.0	<input type="checkbox"/>																			
Unit 1																								
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
																							U	U
	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
	49	50	51	52																				

- b. Enter the following information:
- In the **Vlan ID** field, enter **192**.
 - In the **IP Address** field, enter **192.168.1.254**.
 - In the **Network Mask** field, enter **255.255.255.0**.
- c. Click **Unit 1**. The ports display:
- Click the gray box under port **23** twice until **U** displays.
 - Click the gray box under port **24** twice until **U** displays.
- The U specifies that the egress packet is untagged for the port.
- d. Click **Apply** to save the VLAN that includes ports 23 and 24.
3. Configure a VLAN and include port 1/0/48 in the VLAN:

- a. Select **Routing > VLAN > VLAN Routing Wizard**. A screen similar to the following displays.

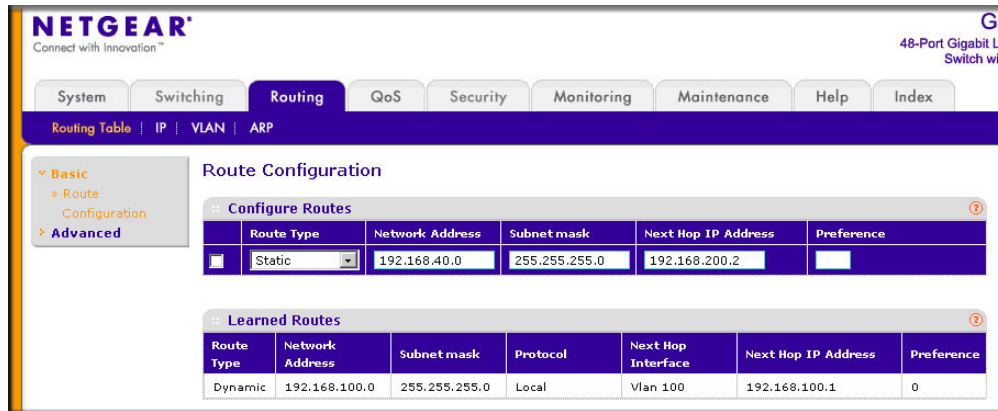


- b. Enter the following information:
- In the **Vlan ID** field, enter **202**.
 - In the **IP Address** field, enter **10.100.5.34**.
 - In the **Network Mask** field, enter **255.255.255.0**.
- c. Click **Unit 1**. The ports display:
- d. Click the gray box under port **48** twice until **U** displays. The U specifies that the egress packet is untagged for the port.
- e. Click **Apply** to save the VLAN that includes port 48.
4. Enable IP routing:
- a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.

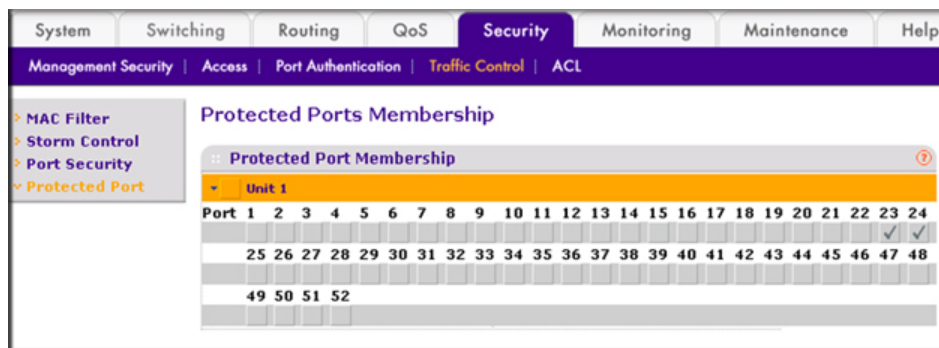


- b. Under IP Configuration, make the following selections:
- For Routing Mode, select the **Enable** radio button.
 - For IP Forwarding Mode, select the **Enable** radio button.
- c. Click **Apply** to enable IP routing.
5. Configure default route for VLAN 202:

- a. Select **Routing > Routing Table > Basic > Route Configuration**. A screen similar to the following displays.



- b. Under Configure Routes, in the **Route Type** list, select **Default Route**.
- c. In the **Next Hop IP Address** field, enter **10.100.5.252**.
- d. Click **Add** to add the route that is associated to VLAN 202 to the Learned Routes table.
6. Configure port 23 and port 24 as protected ports:
- a. Select **Security > Traffic Control > Protected Port**. A screen similar to the following displays.



- b. Under Protected Ports Configuration, click **Unit 1**. The ports display.
- Click the gray box under port **23**. A check mark displays in the box.
 - Click the gray box under port **24**. A check mark displays in the box.
- c. Click **Apply** to activate ports 23 and 24 as protected ports.

802.1x Port Security

This section describes how to configure the 802.1x port security feature on a switch port. IEEE 802.1x authentication prevents unauthorized clients from connecting to a VLAN unless these clients are authorized by the server. 802.1x port security prevent unauthorized clients from connecting to a VLAN. It can be configured on a per-port basis.

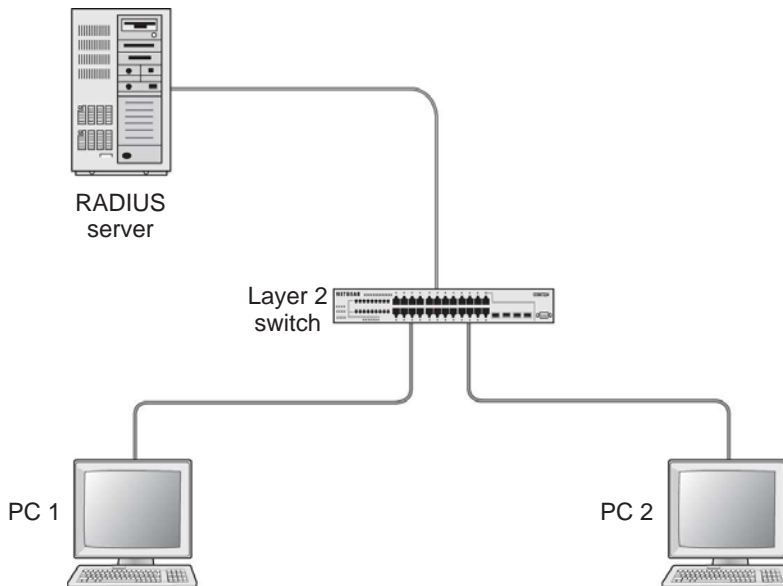


Figure 29. Using 802.1x port security

The following example shows how to authenticate the dot1x users by a RADIUS server. The management IP address is 10.100.5.33/24. The example is shown as CLI commands and as a Web interface procedure.

CLI: Authenticating dot1x Users by a RADIUS Server

1. Assign an IP address to 1/0/19, and set force authorized mode to this port, and create a user name list dot1xList.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.1.1 255.255.255.0
(Netgear Switch) (Config)#dot1x system-auth-control
(Netgear Switch) (Config)#interface 1/0/19
(Netgear Switch) (Interface 1/0/19)#routing
(Netgear Switch) (Interface 1/0/19)#ip address 10.100.5.33 255.255.255.0
(Netgear Switch) (Interface 1/0/19)#dot1x port-control force-authorized
```

2. Use RADIUS to authenticate the dot1x users.

```
(Netgear Switch) (Config)#aaa authentication dot1x default radius
```

3. Configure a RADIUS authentication server.

```
(Netgear Switch) (Config)#radius server host auth 10.100.5.17
```

4. Configure the shared secret between the RADIUS client and the server.

```
Netgear Switch) (Config)#radius server key auth 10.100.5.17  
Enter secret (16 characters max):123456  
Re-enter secret:123456
```

5. Set the RADIUS server as a primary server.

```
(Netgear Switch) (Config)#radius server msgauth 10.100.5.17  
(Netgear Switch) (Config)# radius server primary 10.100.5.17
```

6. Configure an accounting server.

```
(Netgear Switch) (Config)#radius accounting mode  
(Netgear Switch) (Config)#radius server host acct 10.100.5.17
```

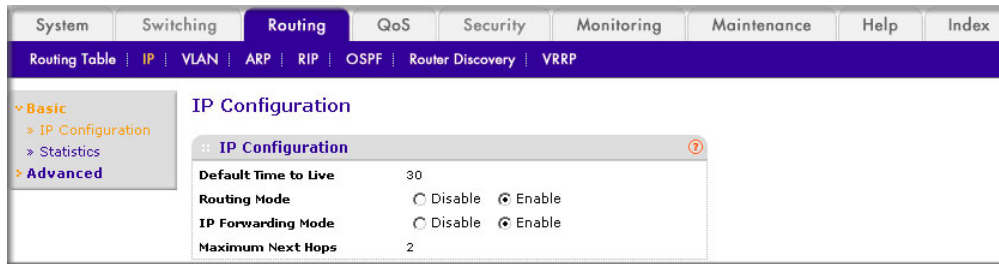
7. Configure the shared secret between the accounting server and the client.

```
(Netgear Switch) (Config)#radius server key acct 10.100.5.17  
Enter secret (16 characters max):123456  
Re-enter secret:123456
```

Web Interface: Authenticating dot1x Users by a RADIUS Server

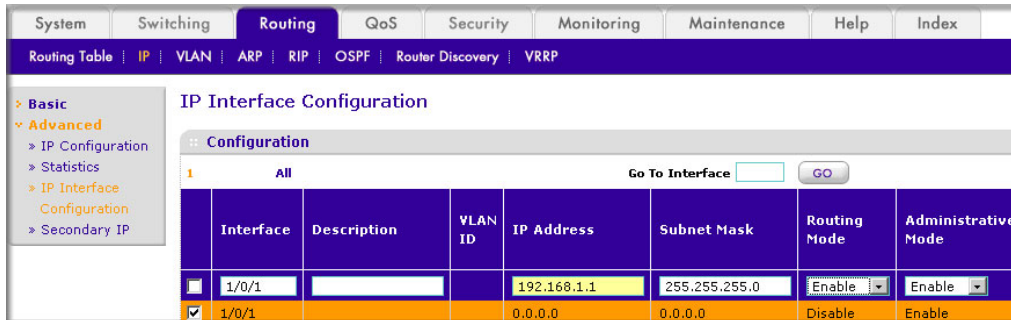
1. Enable routing for the switch.

- a. Select **Routing > Basic > IP Configuration**. A screen similar to the following displays.



- b. For Routing Mode, select the **Enable** radio button.
 c. Click **Apply** to save the settings.
2. Assign IP address 192.168.1.1/24 to the interface 1/0/1.

- a. Select **Routing > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Under IP Interface Configuration, scroll down and select the Interface **1/0/1** check box. Now 1/0/1 appears in the Interface field at the top.
- c. Enter the following information:
- In the **IP Address** field, enter **192.168.1.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
3. Assign IP address 10.100.5.33/24 to interface 1/0/19:

- a. Select **Routing > Advanced > IP Interface Configuration**. A screen similar to the following displays.

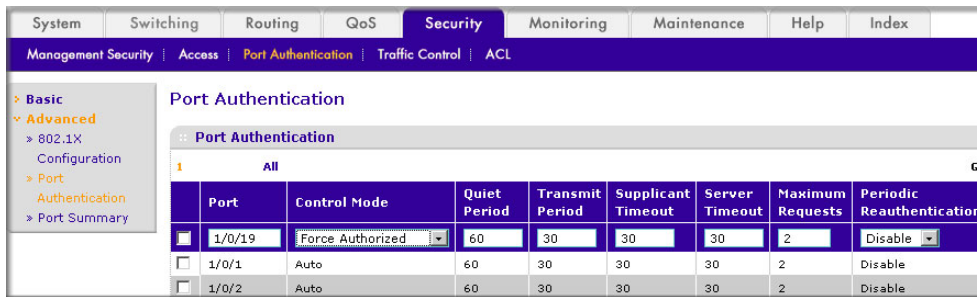
Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/19			10.100.5.33	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the interface **1/0/19** check box. Now 1/0/19 appears in the Interface field at the top.
- c. Enter the following information:
- In the **IP Address** field, enter **10.100.5.33**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
4. Create an authentication name list.
- a. Select **Security > Management Security > Login > Authentication List**. A screen similar to the following displays.

List Name	1	2	3
<input checked="" type="checkbox"/> dot1xList	Radius	Undefined	Undefined
<input type="checkbox"/> defaultList	Local	Undefined	Undefined

- b. Select the check box before **dot1xList**.
- c. In the **1** list, select **Radius**.
- d. Click **Apply**.
5. Set port 1/0/19 to force authorized mode. (In this case, the RADIUS server is connected to this interface.)

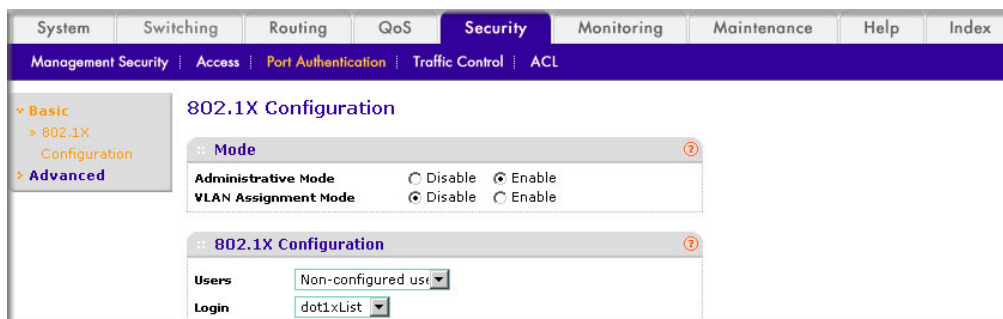
- a. Select **Security > Port Authentication > Advanced > Port Authentication**. A screen similar to the following displays.



- b. Scroll down and select the Interface **1/0/19** check box. Now 1/0/19 appears in the Interface field at the top.
- c. In the **Control Mode** list, select **Force Authorized**.
- d. Click **Apply** to save the settings.

6. Enable dot1x on the switch.

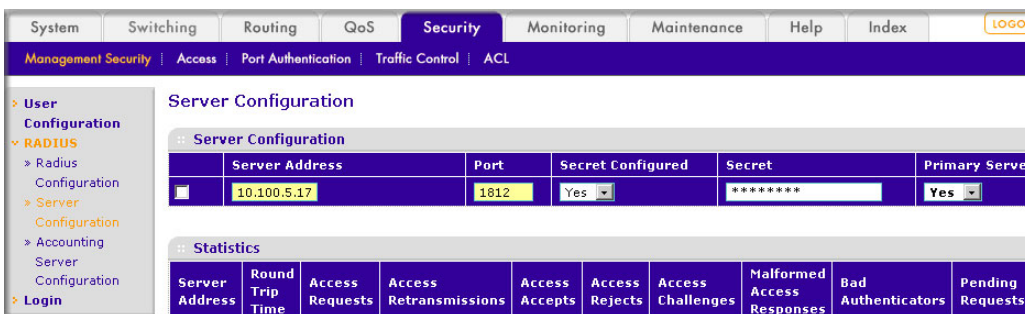
- a. Select **Security > Port Authentication > Server Configuration**. A screen similar to the following displays.



- b. For Administrative Mode, select the **Enable** radio button.
- c. In the **Login** list, select **dot1xList**.
- d. Click **Apply** to save settings.

7. Configure the RADIUS authentication server.

- a. Select **Security > Management Security > Server Configuration**. A screen similar to the following displays.



- b. In the **Server Address** field, enter **10.100.5.17**.

- c. In the **Secret Configured** field, select **Yes**.
 - d. In the **Secret** field, enter **123456**.
 - e. In the **Primary Server** field, select **Yes**.
 - f. In the **Message Authenticator** field, select **Enable**.
 - g. Click **Add**.
8. Enable accounting.
- a. Select **Security > Management Security > RADIUS > Radius Configuration**. A screen similar to the following displays.

The screenshot shows the 'Radius Configuration' page in the ProSafe Managed Switch web interface. The navigation tabs at the top include System, Switching, Routing, QoS, Security (selected), Monitoring, Maintenance, Help, and Index. Below the tabs, there are sub-tabs for Management Security, Access, Port Authentication, Traffic Control, and ACL. The left sidebar shows a tree view with 'RADIUS' selected. The main content area displays the 'Radius Configuration' form with the following fields:

Current Server Address	10.100.5.17
Number of Configured Servers	1
Max Number of Retransmits	4 (1 to 15)
Timeout Duration (secs)	5 (1 to 30)
Accounting Mode	Enable
RADIUS Attribute 4	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

- b. In the **Server Address** field, enter **10.100.5.17**.
 - c. In the **Accounting Mode** field, select **Enable**.
 - d. Click **Apply**.
9. Configure the accounting server.
- a. Select **Security > Management Security > RADIUS > Radius Accounting Server Configuration**. A screen similar to the following displays.

The screenshot shows the 'Accounting Server Configuration' page in the ProSafe Managed Switch web interface. The navigation tabs at the top include System, Switching, Routing, QoS, Security (selected), Monitoring, Maintenance, Help, and Index. Below the tabs, there are sub-tabs for Management Security, Access, Port Authentication, Traffic Control, and ACL. The left sidebar shows a tree view with 'Accounting Server Configuration' selected. The main content area displays the 'Accounting Server Configuration' form with the following fields:

Accounting Server Address	10.100.5.17
Port	1813
Secret Configured	Yes
Secret	*****
Accounting Mode	Enable

- b. In the **Accounting Server Address** field, enter **10.100.5.17**.
- c. In the **Accounting Mode** field, select **Enable**.
- d. Click **Apply**.

Create a Guest VLAN

The guest VLAN feature allows a switch to provide a distinguished service to dot1x unaware clients (not rogue users who fail authentication). This feature provides a mechanism to allow visitors and contractors to have network access to reach an external network with no ability to surf the internal LAN.

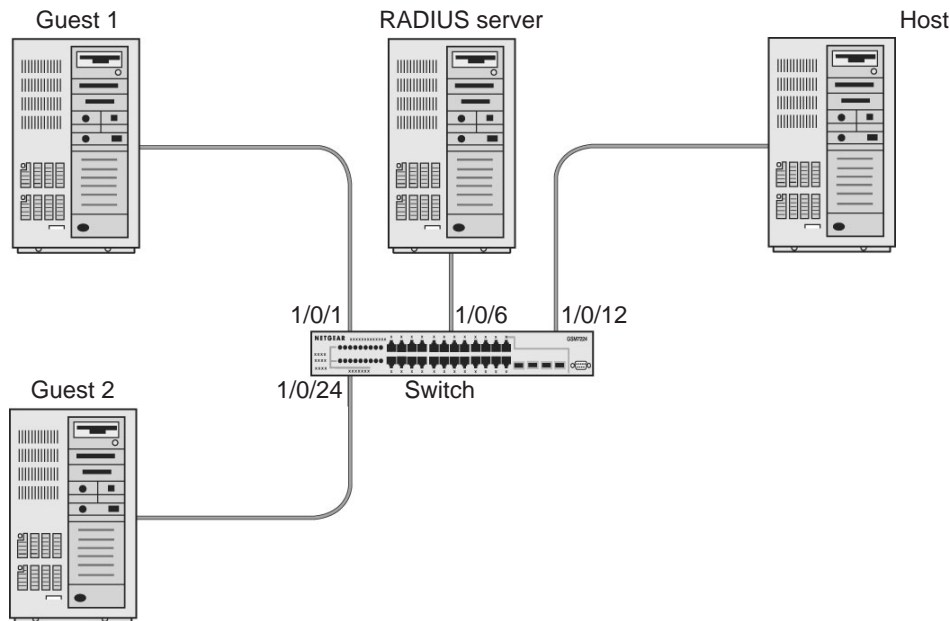


Figure 30. Guest VLAN

If a port is in port-based mode, and a client that does not support 802.1X is connected to an unauthorized port that has 802.1X enabled, the client does not respond to the 802.1X requests from the switch. The port remains in the unauthorized state, and the client is not granted access to the network. If the guest VLAN is configured for that port, then the port is placed in the configured guest VLAN and the port is moved to the authorized state, allowing access to the client after a certain amount of time (determined by the guest VLAN period). If the client attached is 802.1x aware, then this allows the client to respond to 802.1X requests from the switch.

For a port in MAC-based mode, if traffic from an unauthenticated client is noticed on a port then, if guest VLAN has been configured on the port, the guest VLAN timer is started for that client. If the client is 802.1x unaware and does not respond to any 802.1x requests, when the guest VLAN timer expires, the client is authenticated and associated with the guest VLAN. This ensures that traffic from the client is accepted and switched through the guest VLAN.

In this example, dot1x is enabled on all the ports so that all the hosts that are authorized are assigned to VLAN 1. On ports 1/0/1 and 1/0/24, guest VLAN is enabled. If guests connect to the port, they are assigned to VLAN 2000, so that guests cannot access the internal VLAN, but can access each other in the guest VLAN.

CLI: Create a Guest VLAN

1. Enter the following commands:

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

2. Create VLAN 2000, and have 1/0/1 and 1/0/24 as members of VLAN 2000.

```
(Netgear Switch) (Config)#aaa authentication dot1x default radius
(Netgear Switch) (Config)#dot1x system-auth-control
(Netgear Switch) (Config)#radius server host auth 192.168.0.1
(Netgear Switch) (Config)#radius server key auth 192.168.0.1
Enter secret (16 characters max):12345
Re-enter secret:12345
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)#dot1x port-control force-authorized
(Netgear Switch) (Interface 1/0/6)#exit
(Netgear Switch) (Config)#interface 1/0/12
(Netgear Switch) (Interface 1/0/12)#dot1x port-control force-authorized
(Netgear Switch) (Interface 1/0/12)#exit
```

3. Enable dot1x and RADIUS on the switch.

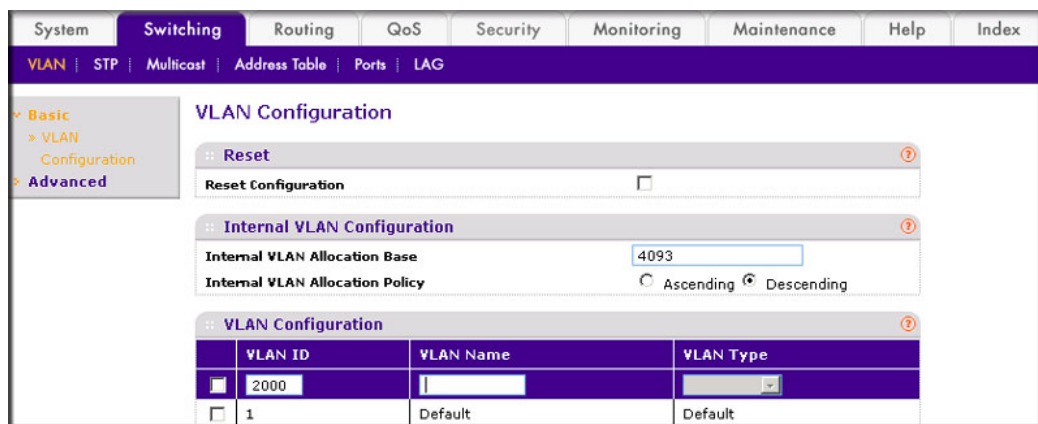
```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#dot1x guest-vlan 2000
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#dot1x guest-vlan 2000
(Netgear Switch) (Interface 1/0/24)#exit
```

4. Enable the guest VLAN on ports 1/0/1 and 1/0/24.

```
(Netgear Switch) #show dot1x detail 1/0/1
Protocol Version..... 1
PAE Capabilities..... Authenticator
Control Mode..... auto
Authenticator PAE State..... Authenticated
Backend Authentication State..... Idle
Quiet Period (secs)..... 60
Transmit Period (secs)..... 30
Guest VLAN ID..... 2000
Guest VLAN Period (secs)..... 90
Supplicant Timeout (secs)..... 30
Server Timeout (secs)..... 30
Maximum Requests..... 2
VLAN Id..... 2000
VLAN Assigned Reason..... Guest
Reauthentication Period (secs)..... 3600
Reauthentication Enabled..... FALSE
Key Transmission Enabled..... FALSE
Control Direction..... both
Maximum Users..... 16
Unauthenticated VLAN ID..... 0
Session Timeout..... 0
Session Termination Action..... Default
```

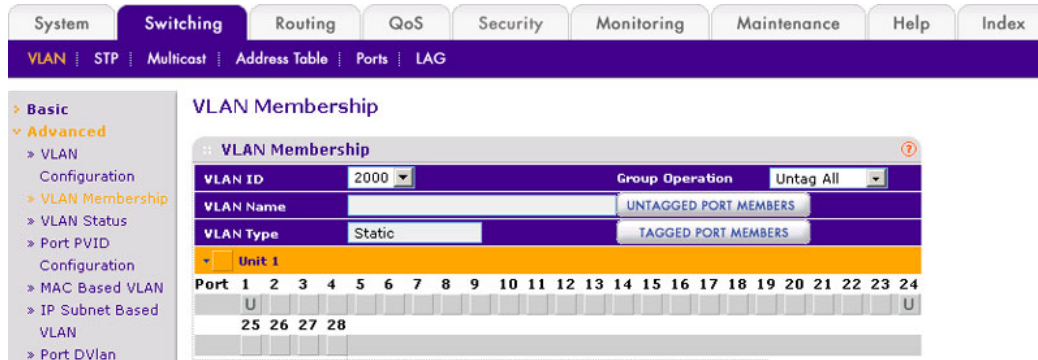
Web Interface: Create a Guest VLAN

1. Create VLAN 2000.
 - a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays.

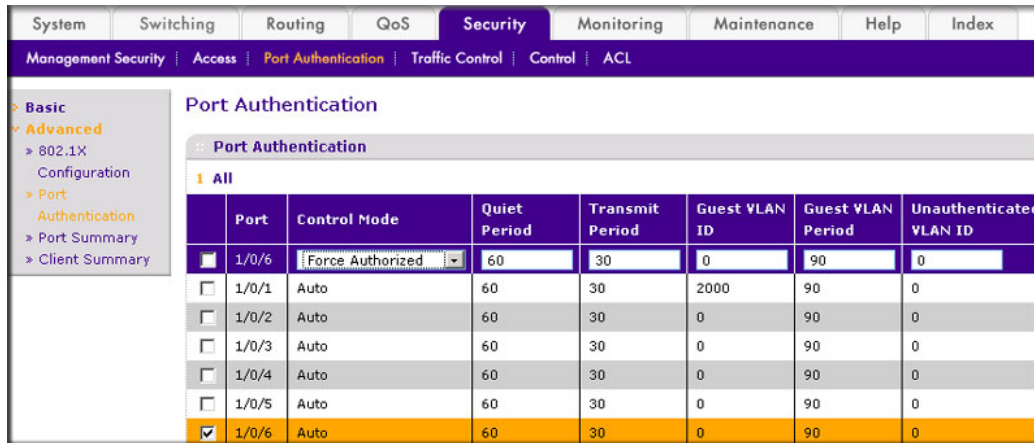


- b. In the **VLAN ID** field, enter **2000**.

- c. In the **VLAN Type** field, select **Static**.
 - d. Click **Add**.
2. Add ports to VLAN 2000.
- a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays.



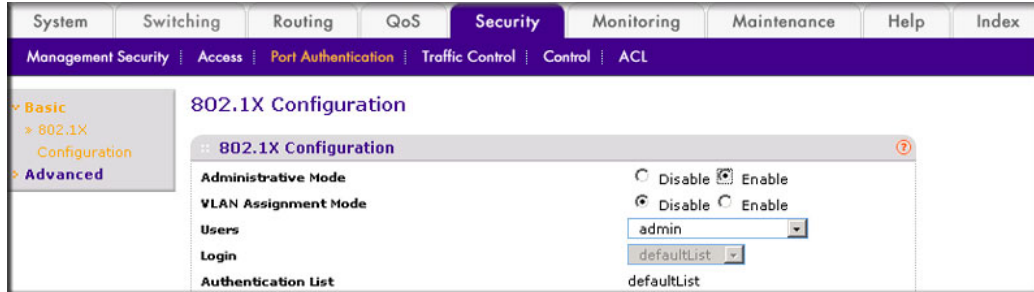
- b. In the **VLAN ID** list, select **2000**.
 - c. Click **Unit 1**. The ports display.
 - d. Click the gray boxes under ports **1** and **24** until **U** displays. The U specifies that the egress packet is untagged for the port.
 - e. Click **Apply**.
3. Set force authorized mode on ports 1/0/6 and 1/0/12.
- a. Select **Security > Port Authentication > Advanced > Port Authentication**. A screen similar to the following displays.



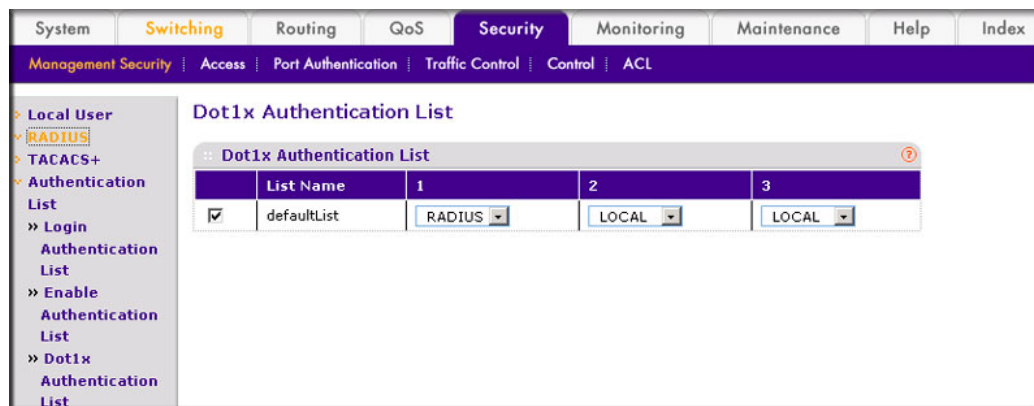
- b. Scroll down and select the Interface **1/0/6** and **1/0/12**, check boxes.
 - c. In the **Control Mode** list, select **Force Authorized**.
 - d. Click **Apply** to save settings.
4. Enable dot1x on the switch.

Make sure that 1/0/12 and 1/0/6 are configured as force authorized before you do this step; otherwise you cannot access the switch through the Web Interface.

- a. Select **Security > Port Authentication > Basic > 802.1x Configuration**. A screen similar to the following displays.



- b. For Administrative Mode, select the **Enable** radio button.
 - c. Click **Apply** to save settings.
5. Configure the dot1x authentication list.
 - a. Select **Security > Management Security > Authentication List > Dot1x Authentication List**. A screen similar to the following displays.



- b. Select the **defaultList** check box.
 - c. In the **1** list, select **RADIUS**.
 - d. Click **Add**.
6. Configure the RADIUS authentication server.

- a. Select **Security > Management Security > Radius > Server Configuration**. A screen similar to the following displays.

Radius Server IP Address	Radius Server Name	Current	Port	Secret Configured	Secret
<input checked="" type="checkbox"/> 192.168.0.1				Yes	12345

Radius Server	Round Trip Time	Access Requests	Access Retransmissions	Access Accepts	Access Rejects	Access Challenges	Malformed Access Responses	Bad Authenticators	Pending Requests

- b. In the **Radius Server IP Address** field, enter **192.168.0.1**.
 - c. In the **Secret Configured** field, select **Yes**.
 - d. In the **Secret** field, enter **12345**.
 - e. Click **Add**.
7. Configure the guest VLAN.
 - a. Select **Security > Port Authentication > Advanced > Port Authentication**. A screen similar to the following displays.

Port	Control Mode	Quiet Period	Transmit Period	Guest VLAN ID	Guest VLAN Period	Unauthenticated VLAN ID
<input checked="" type="checkbox"/> 1/0/1	Auto	60	30	2000	90	0
<input type="checkbox"/> 1/0/2	Auto	60	30	0	90	0

- b. Scroll down and select the port **1/0/1** and **1/0/24** check boxes.
- c. In the **Guest VLAN ID** field, enter **2000**.
- d. Click **Apply** to save your settings.

Assign VLANs Using RADIUS

This feature allows the client to connect from any port and be assigned to the appropriate VLAN assigned by the RADIUS server. This gives flexibility for the clients to move around the network without requiring the administrator to do static VLAN configuration. When multiple hosts are connected to the switch on the same port, only one host uses authentication. If any VLAN information is applied on the port based on the authenticated host, the VLAN applies that information to all the hosts that are connected to that port.

- After a port is in an authorized state, if any client initiates dot1x authentication, the port clears authenticated clients' states, and in the process clears the VLAN assigned to the port (if any). Then the port continues with the new client authentication and authorization process.
- When a client authenticates itself initially on the network, the switch acts as the authenticator to the clients on the network and forwards the authentication request to the RADIUS server in the network.

For use in VLAN assignment, the following tunnel attributes are used:

- Tunnel-Type = VLAN (13)
- Tunnel-Medium-Type = 802
- Tunnel-Private-Group-ID = VLANID where VLANID is 12 bits, with a value between 1 and 4094.

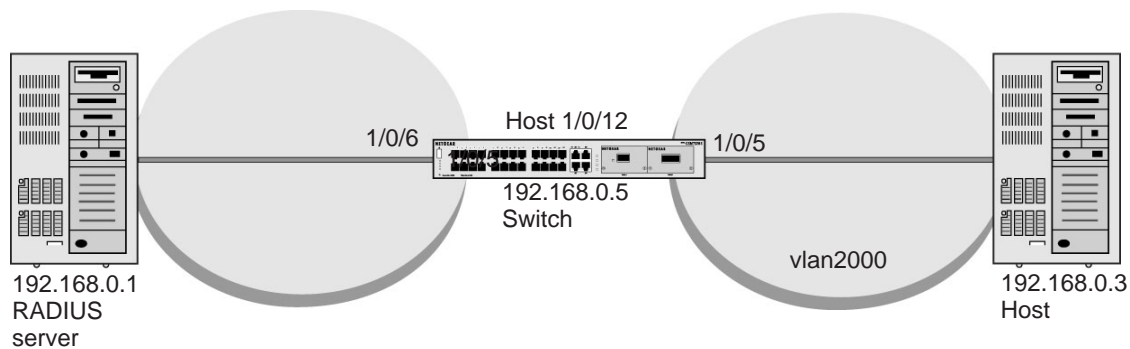


Figure 31. VLAN assignment using RADIUS

In the previous figure, the switch has placed the host in the VLAN (vlan2000) based on the user details of the clients.

The configuration on a RADIUS server for a user logged in as admin is:

- Tunnel-Type = VLAN (13)
- Tunnel-Medium-Type = 802
- Tunnel-Private-Group-ID = 2000

CLI: Assign VLANS Using RADIUS

1. Create VLAN 2000.

```
(Netgear Switch) #network protocol none
Changing protocol mode will reset ip configuration.
Are you sure you want to continue? (y/n) y
(Netgear Switch) #network parms 192.168.0.5 255.255.255.0
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 2000
(Netgear Switch) #exit
```

2. Enable dot1x authentication on the switch

```
(Netgear Switch) (Config)#dot1x system-auth-control
```

3. Use the RADIUS as the authenticator.

```
(Netgear Switch) (Config)#aaa authentication dot1x default radius
```

4. Enable the switch to accept VLAN assignment by the RADIUS server.

```
(Netgear Switch) (Config)#authorization network radius
```

5. Set the RADIUS server IP address.

```
(Netgear Switch) (Config)#radius server host auth 192.168.0.1
```

6. Set the NAS-IP address for the RADIUS server..

```
(Netgear Switch) (Config)#radius server key auth 192.168.0.1
Enter secret (16 characters max):12345
Re-enter secret:12345
Set the radius server key.
(Netgear Switch) (Config)#radius server attribute 4 192.168.0.1
```

7. Force 1/0/6 to be authorized for it to connect to the RADIUS server.

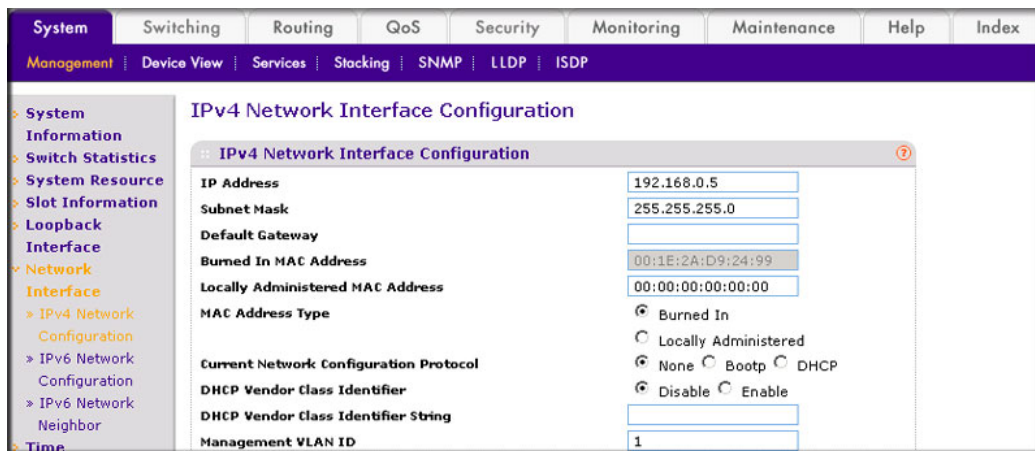
```
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)#dot1x port-control force-authorized
(Netgear Switch) (Interface 1/0/6)#exit
```

8. Show the dot1x detail for 1/0/5.

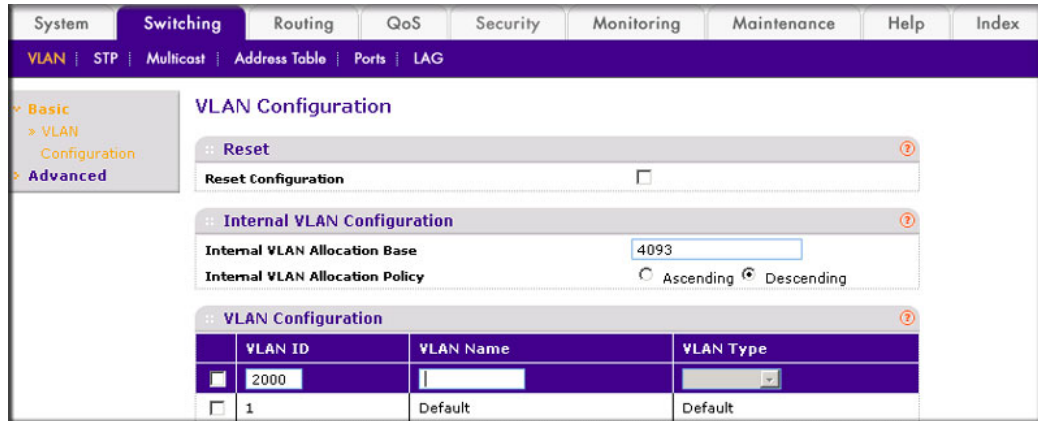
```
(Netgear Switch) #show dot1x detail 1/0/5
Port..... 1/0/5
Protocol Version..... 1
PAE Capabilities..... Authenticator
Control Mode..... auto
Authenticator PAE State..... Authenticated
Backend Authentication State..... Idle
Quiet Period (secs)..... 60
Transmit Period (secs)..... 30
Guest VLAN ID..... 0
Guest VLAN Period (secs)..... 90
Supplicant Timeout (secs)..... 30
Server Timeout (secs)..... 30
Maximum Requests..... 2
VLAN Id..... 2000
VLAN Assigned Reason..... RADIUS
Reauthentication Period (secs)..... 3600
Reauthentication Enabled..... FALSE
Key Transmission Enabled..... FALSE
Control Direction..... both
Maximum Users..... 16
Unauthenticated VLAN ID..... 0
Session Timeout..... 0
Session Termination Action..... Default
```

Web Interface: Assign VLANs Using RADIUS

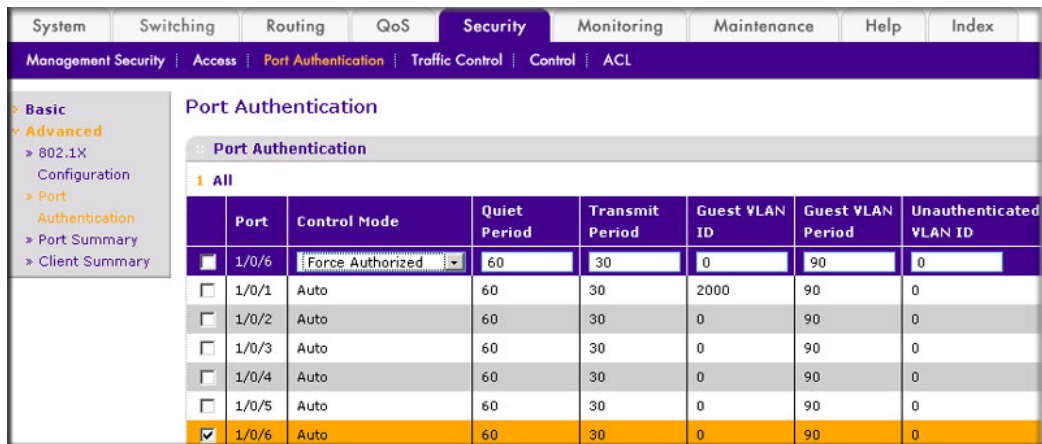
1. Assign the IP address for the Web Management Interface.
 - a. Select **System > Management > Network Interface > IPv4 Network Configuration**. A screen similar to the following displays.



- b. For Current Network Configuration Protocol, select the **None** radio button.
 - c. In the **IP Address** field, enter **192.168.0.5**.
 - d. In the **Subnet Mask** field, enter **255.255.255.0**.
 - e. Click **Apply**.
2. Create VLAN 2000.
- a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays.



- b. In the **VLAN ID** field, enter **2000**.
 - c. In the **VLAN Type** field, select **Static**.
 - d. Click **Add**.
3. Set force authorized mode on ports 1/0/6 and 1/0/12.
- a. Select **Security > Port Authentication > Advanced > Port Authentication**. A screen similar to the following displays.

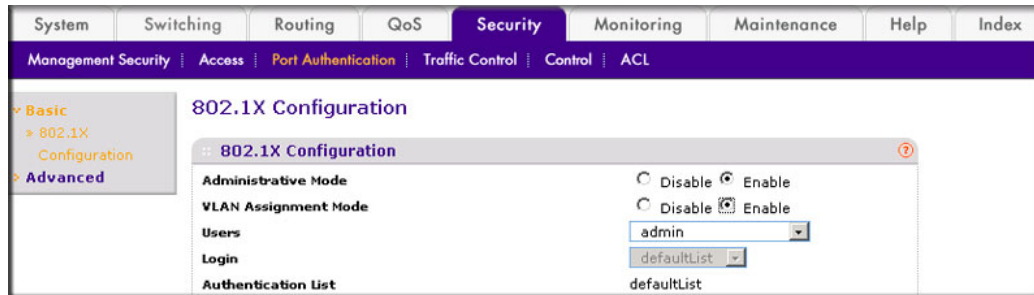


- b. Under Port Authentication, scroll down and select the 1/0/6 and 1/0/12 check boxes.
- c. In the **Control Mode** list, select **Force Authorized**.
- d. Click **Apply** to save settings.

4. Enable dot1x on the switch.

Make sure that 1/0/12 and 1/0/6 are configured as force authorized before you do this step; otherwise, you cannot access the switch through the Web Management Interface.

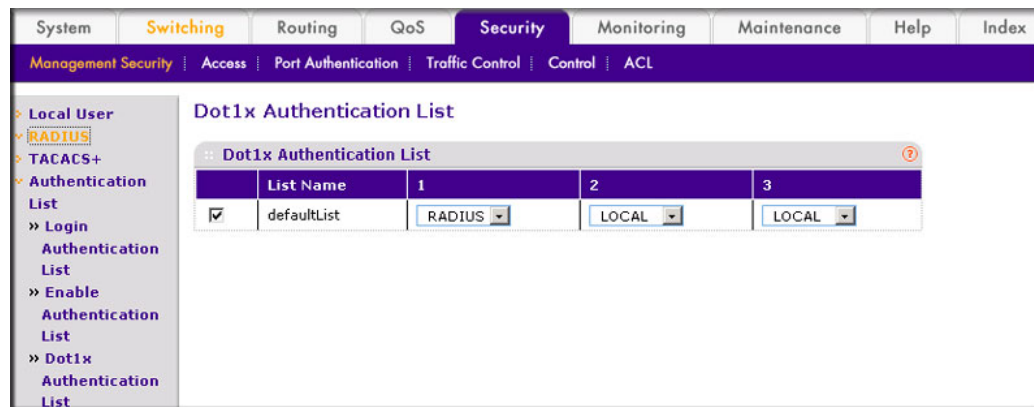
- a. Select **Security > Port Authentication > Basic > 802.1x Configuration**. A screen similar to the following displays.



- b. For Administrative Mode, select the **Enable** radio button.
- c. For VLAN Assignment Mode, select the **Enable** radio button.
- d. Click **Apply** to save settings.

5. Configure the dot1x authentication list.

- a. Select **Security > Management Security > Authentication List > Dot1x Authentication List**. A screen similar to the following displays.



- b. Select the **defaultList** check box.
- c. In the **1** list, select **RADIUS**.
- d. Click **Add**.

6. Configure the RADIUS authentication server.

- a. Select **Security > Management Security > Radius > Server Configuration**. A screen similar to the following displays.

Server Configuration						
Radius Server IP Address	Radius Server Name	Current	Port	Secret Configured	Secret	
<input type="checkbox"/>	192.168.0.1	<input type="text"/>	<input type="text"/>	Yes	*****	<input type="button" value="Add"/>

Statistics									
Radius Server	Round Trip Time	Access Requests	Access Retransmissions	Access Accepts	Access Rejects	Access Challenges	Malformed Access Responses	Bad Authenticators	Pending Requests

- b. In the **Radius Server IP Address** field, enter **192.168.0.1**.
- c. In the **Secret Configured** field, select **Yes**.
- d. In the **Secret** field, enter **12345**.
- e. Click **Add**.

Dynamic ARP Inspection

Dynamic ARP inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. The feature prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a bindings database of valid tuples (MAC address, IP address, VLAN interface).

When DAI is enabled, the switch drops ARP packet if the sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. However, it can be overcome through static mappings. Static mappings are useful when hosts configure static IP addresses, DHCP snooping cannot be run, or other switches in the network do not run

dynamic ARP inspection. A static mapping associates an IP address to a MAC address on a VLAN.

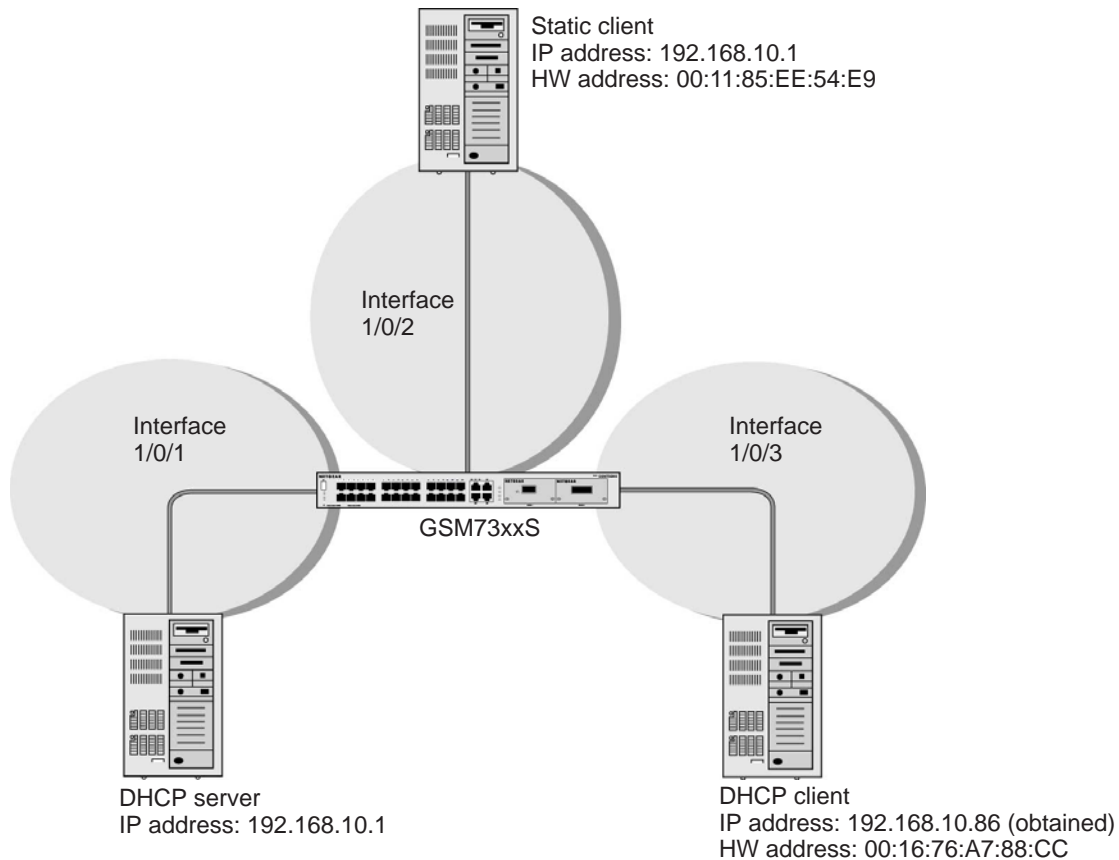


Figure 32. Dynamic ARP inspection

CLI: Configure Dynamic ARP Inspection

1. Enable DHCP snooping globally.

```
(Netgear Switch) (Config)# ip dhcp snooping
```

2. Enable DHCP snooping in a VLAN.

```
(Netgear Switch) (Config)# ip dhcp snooping vlan 1
```

3. Configure the port through which the DHCP server is reached as trusted.

```
(Netgear Switch) (Config)# interface 1/0/1  
(Netgear Switch) (Interface 1/0/1)# ip dhcp snooping trust
```

4. View the DHCP Snooping Binding table.

```
(GSM7328S) #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 there is a DHCP snooping entry; however ARP packets from the static client are dropped. It can be overcome by static configuration as described in [Static Mapping](#) on page 294.

Web Interface: Configure Dynamic ARP Inspection

1. Enable DHCP snooping globally.

- a. Select **Security > Control > DHCP Snooping Global Configuration**. A screen similar to the following displays.



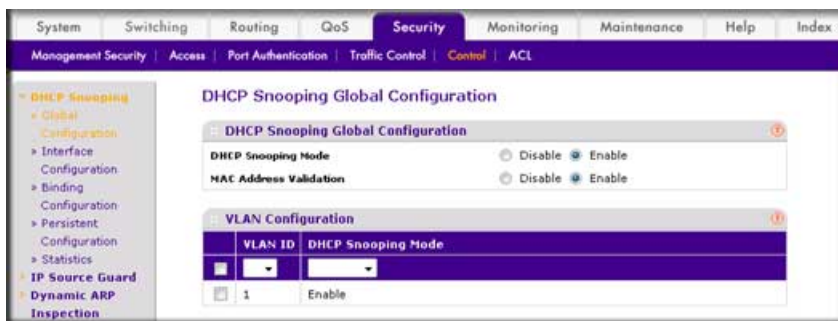
- b. For DHCP Snooping Mode, select the **Enable** radio button.
- c. Click **Apply**.

2. Enable DHCP snooping in a VLAN.

- a. Select **Security > Control > DHCP Snooping Global Configuration**. A screen similar to the following displays.

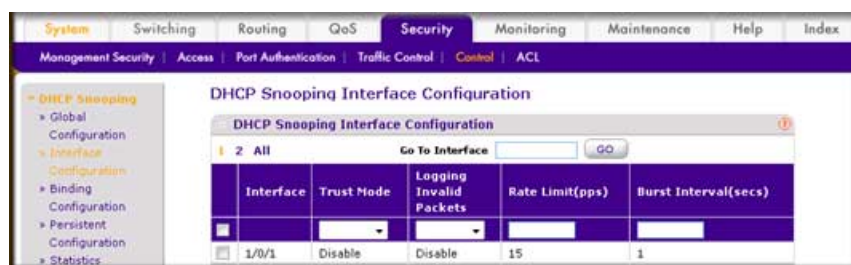


- b. In the **VLAN ID** field, enter 1.
- c. In the the **DHCP Snooping Mode** field, select **Enable**. A screen similar to the following displays.



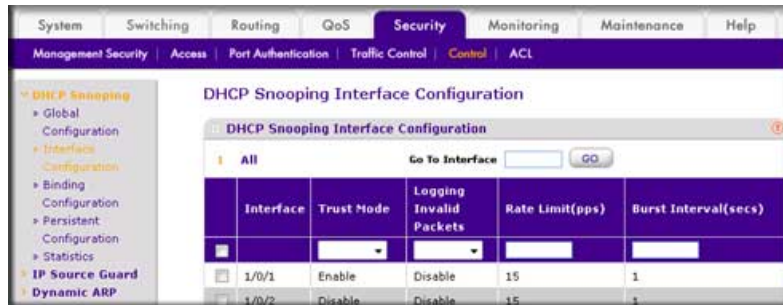
3. Configure the port through which the DHCP server is reached as trusted. Here interface 1/0/1 is trusted.

- a. Select **Security > Control > DHCP Snooping Interface Configuration**. A screen similar to the following displays.

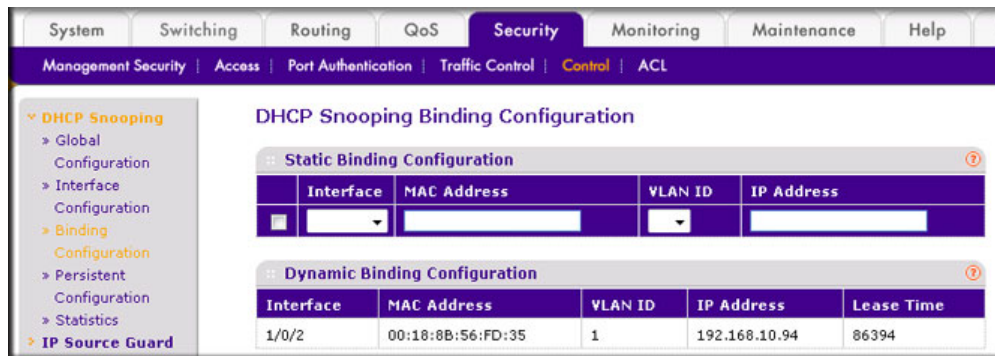


- b. Select the check box for Interface **1/0/1**.
- c. For Interface 1/0/1, set the Trust Mode as **Enable**.

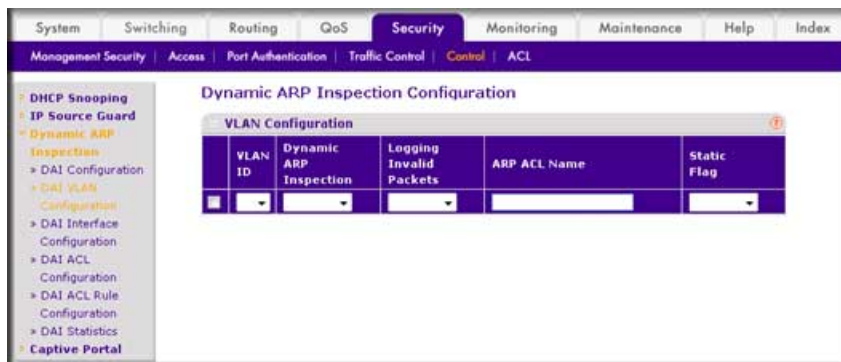
- d. Click **Apply**. A screen similar to the following displays.



4. View the DHCP Snooping Binding table.
- a. Select **Security > Control > DHCP Snooping Binding Configuration**. A screen similar to the following displays.



5. Enable ARP Inspection in VLAN 1.
- a. Select **Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration**. A screen similar to the following displays.



- b. In the **VLAN ID** field, enter 1.

- c. In the **Dynamic ARP Inspection** field, select **Enable**. A screen similar to the following displays.



- d. Click **Apply**. A screen similar to the following displays.



Now all the ARP packets received on the ports that are member of the VLAN are copied to the CPU for ARP inspection. If there are trusted ports, you can configure them as trusted in the next step. ARP packets received on the trusted ports are not copied to the CPU.

Note: Make sure the administrator PC has a DHCP snooping entry or can access the device through the trusted port for ARP. Otherwise, you might get disconnected from the device.

6. Configure port 1/0/1 as trusted.
 - a. Select **Security > Control > Dynamic ARP Inspection > DAI Interface Configuration**.
 - b. Select the Interface **1/0/1** check box.
 - c. For the **Trust Mode**, select **Enable**.

- d. Click **Apply**. A screen similar to the following displays.



Now ARP packets from the DHCP client will go through; however ARP packets from the static client are dropped, since it does not have a DHCP snooping entry. It can be overcome by static configuration as described in the following section, [Static Mapping](#) on page 294.

Static Mapping

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

CLI: Configure Static Mapping

1. Create an ARP ACL.

```
(Netgear Switch) (Config)# arp access-list ArpFilter
```

2. Configure the rule to allow the static client.

```
(Netgear Switch) (Config-arp-access-list)# permit ip host 192.168.10.2
mac host 00:11:85:ee:54:e9
```

3. Configure ARP ACL used for VLAN 1.

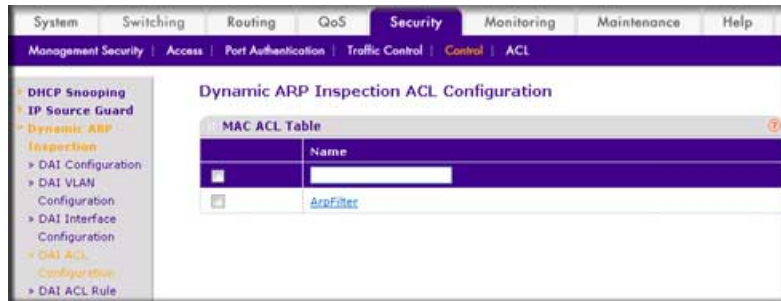
```
(Netgear Switch) (Config)# ip arp inspection filter ArpFilter vlan 1
```

4. Now the ARP packets from the static client will go through since it has an entry in the ARP ACL. ARP packets from the DHCP client also go through since it has a DHCP snooping entry.

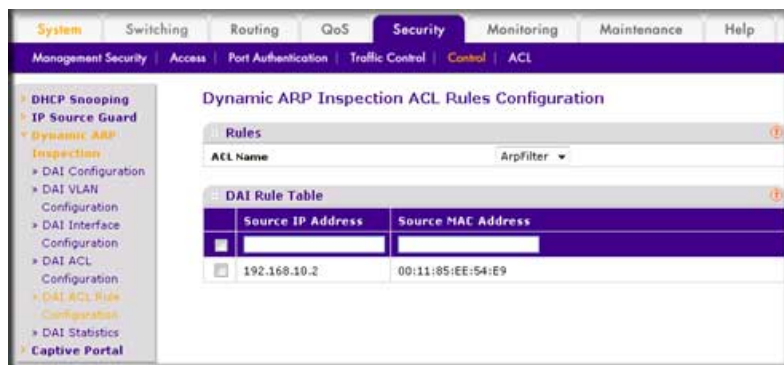
This command can include the optional `static` keyword. If the `static` keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings. In this example, ARP packets from the DHCP client are dropped since it does not have a matching rule, though it has a DHCP snooping entry.

Web Interface: Configure Static Mapping

1. Create an ARP ACL.
 - a. Select **Security > Control > Dynamic ARP Inspection > DAI ACL Configuration**.
 - b. In the **Name** field, enter **ArpFilter**.
 - c. Click **Add**. A screen similar to the following displays.



2. Configure a rule to allow the static client.
 - a. Select **Security > Control > Dynamic ARP Inspection > DAI ACL Rule Configuration**.
 - b. In the **ACL Name** list, select **ArpFilter**.
 - c. In the **Source IP Address** field, enter **192.168.10.2**.
 - d. In the **Source MAC Address** field, enter **00:11:85:EE:54:E9**.
 - e. Click **Add**. A screen similar to the following displays.



3. Configure the ARP ACL used for VLAN 1.
 - a. Select **Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration**.
 - b. In the **ARP ACL Name** field, enter **ArpFilter**.

- c. Click **Apply**. A screen similar to the following displays.



DHCP Snooping

DHCP snooping is a security feature that monitors DHCP messages between a DHCP client and DHCP server to filter harmful DHCP message and to build a bindings database of (MAC address, IP address, VLAN ID, port) tuples that are considered authorized. The network administrator enables DHCP snooping globally and on specific VLANs and configures ports within the VLAN to be trusted or untrusted. DHCP servers must be reached through trusted ports.

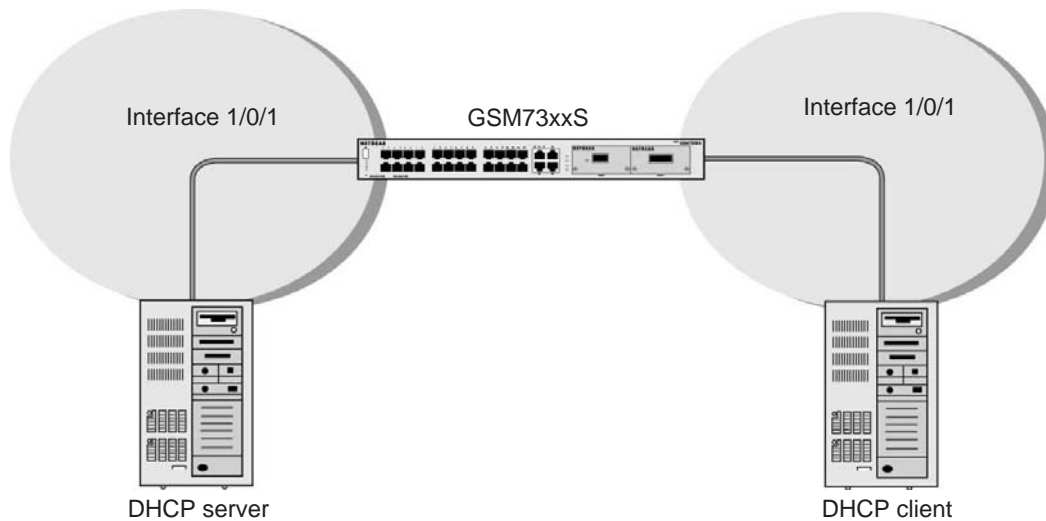


Figure 33. DHCP Snooping

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

CLI: Configure DHCP Snooping

1. Enable DHCP snooping globally.

```
(Netgear Switch) (Config)# ip dhcp snooping
```


2. Enable DHCP snooping in a VLAN.

```
(Netgear Switch) (Config)# ip dhcp snooping vlan 1
```

3. Configure the port through which the DHCP server is reached as trusted.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip dhcp snooping trust
```

4. View the DHCP Snooping Binding table.

```
(GSM7328S) #show ip dhcp snooping binding

Total number of bindings: 1

MAC Address          IP Address          VLAN  Interface  Type      Lease (Secs)
-----
00:16:76:A7:88:CC   192.168.10.89      1     1/0/2     DYNAMIC   86400
```

Web Interface: Configure DHCP Snooping

1. Enable DHCP snooping globally:

- a. Select **Security > Control > DHCP Snooping Global Configuration**. A screen similar to the following displays.



- b. For DHCP Snooping Mode, select **Enable**.
- c. Click **Apply**. A screen similar to the following displays:.



2. Enable DHCP snooping in a VLAN.

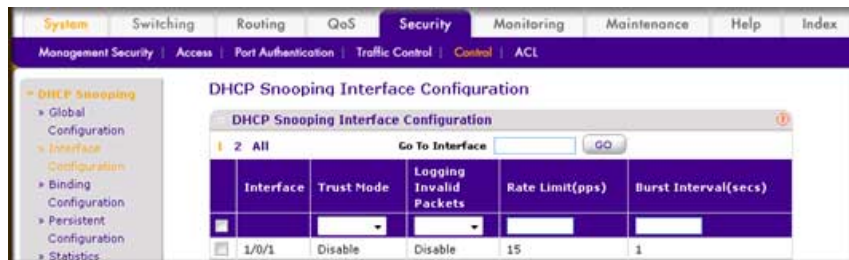
- a. Select **Security > Control > DHCP Snooping Global Configuration**. A screen similar to the following displays.



- b. In the **VLAN ID** list, select **1**.
- c. For DHCP Snooping Mode, select the **Enable** radio button. A screen similar to the following displays.



- d. Click **Apply**.
3. Configure the port through which DHCP server is reached as trusted.
- a. Select **Security > Control > DHCP Snooping Interface Configuration**. A screen similar to the following displays.



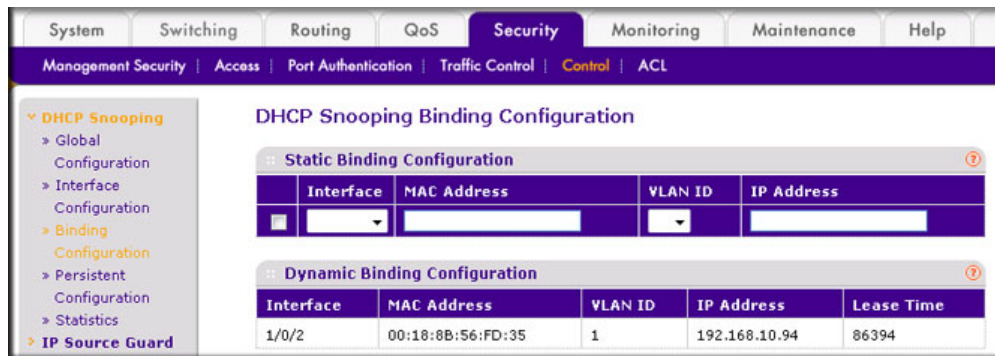
- b. Select the Interface **1/0/1** check box.
- c. For Interface 1/01/, in the Trust Mode field, select **Enable**.

- d. Click **Apply**. A screen similar to the following displays.



4. View the DHCP Snooping Binding configuration.

Select **Security > Control > DHCP Snooping Binding Configuration**. A screen similar to the following displays.



Enter Static Binding into the Binding Database

You can also enter the static binding into the binding database.

CLI: Enter Static Binding into the Binding Database

1. Enter the DHCP snooping static binding.

```
(Netgear Switch) (Config)# ip dhcp snooping binding 00:11:11:11:11:11
vlan 1 192.168.10 .1 interface 1/0/2
```

2. Check to make sure the binding database has the static entry.

```
(GSM7328S) #show ip dhcp snooping binding
Total number of bindings: 2

MAC Address          IP Address      VLAN  Interface      Type      Lease (Secs)
-----
00:11:11:11:11:11   192.168.10.1   1     1/0/2          STATIC
00:16:76:A7:88:CC   192.168.10.89  1     1/0/2          DYNAMIC   86348
```

Web Interface: Enter Static Binding into the Binding Database

1. Select **Security > Control > DHCP Snooping > Binding Configuration**.



2. Fill in the fields for the static binding and click **Apply**.
3. Check to make sure that the binding database shows the entry in the Static Binding Configuration table.



Maximum Rate of DHCP Messages

To prevent DHCP packets being used as DoS attachments when DHCP snooping is enabled, the snooping application enforces a rate limit for DHCP packets received on untrusted interfaces. DHCP snooping monitors the receive rate on each interface separately. If the receive rate exceeds the configured limit, DHCP snooping brings down the interface. The user must specify “no shutdown” on this interface to further work with that port.

CLI: Configure the Maximum Rate of DHCP Messages

1. Control the maximum rate of DHCP messages.

```
(Netgear Switch) (Interface 1/0/2)# ip dhcp snooping limit rate 5
```

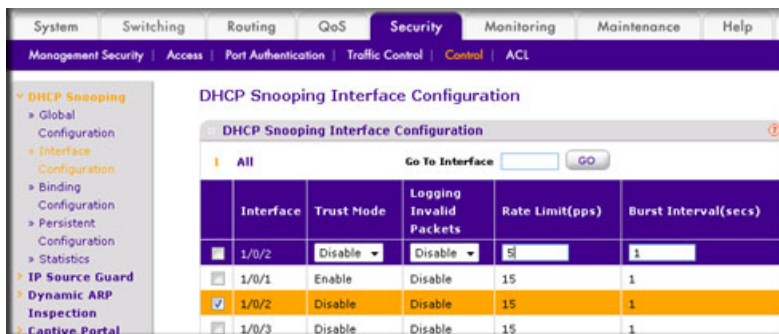
2. View the rate configured.

```
(GSM7328S) #show ip dhcp snooping interfaces 1/0/2
```

Interface	Trust State	Rate Limit (pps)	Burst Interval (seconds)
1/0/2	No	5	1

Web Interface: Configure the Maximum Rate of DHCP Messages

1. Select **Security > Control > DHCP Snooping > Interface Configuration**. A screen similar to the following displays:



2. Select the interface, fill in the **Rate Limit (pps)** field, and then click **Apply**.

The screen shows the new rate limit for the interface.



IP Source Guard

IP Source Guard uses the DHCP snooping bindings database. When IP Source Guard is enabled, the switch drops incoming packets that do not match a binding in the bindings database. IP Source Guard can be configured to enforce just the source IP address or both the source IP address and source MAC address.

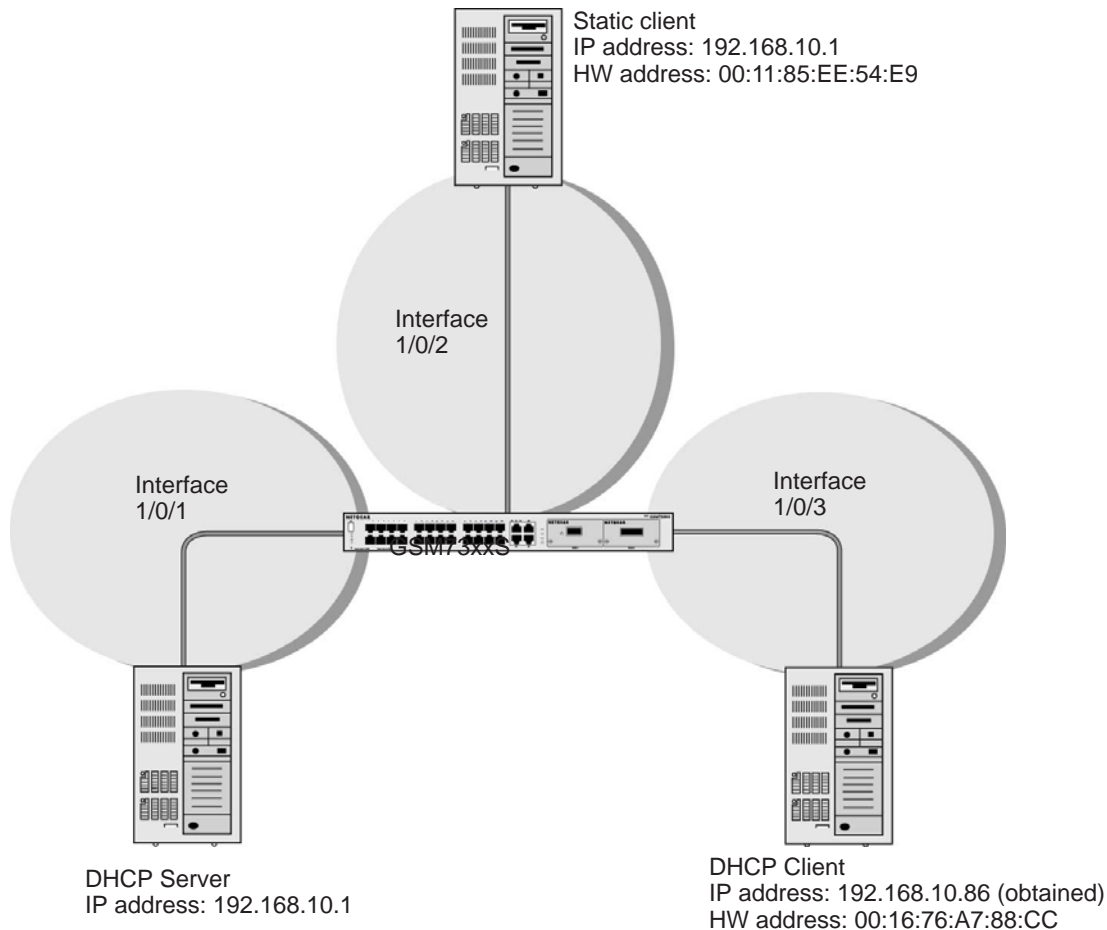


Figure 34. IP Source Guard

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

CLI: Configure Dynamic ARP Inspection

1. Enable DHCP snooping globally.

```
(Netgear Switch) (Config)# ip dhcp snooping
```

2. Enable DHCP snooping in a VLAN.

```
(Netgear Switch) (Config)# ip dhcp snooping vlan 1
```

3. Configure the port through which the DHCP server is reached as trusted.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip dhcp snooping trust
```

4. View the DHCP Snooping Binding table.

```
(GSM7328S) #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, it can statically added through the command `ip verify binding <mac-address> vlan <vlan id> <ip address> interface <interface id>` in global configuration mode.

5. Enable IP Source Guard in interface 1/0/2.

```
(GSM7352Sv2) (Interface 1/0/2)#ip verify source port-security
```

With this configuration, the device verifies both the source IP address and the source MAC address. If the port-security option is skipped, the device verifies only the source IP address.

Web Interface: Configure Dynamic ARP Inspection

1. Enable DHCP snooping globally.

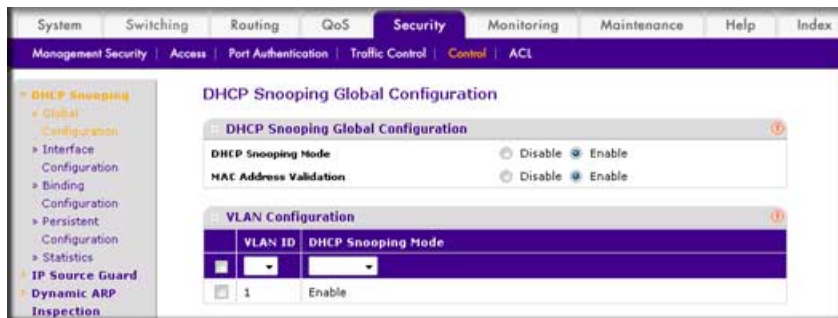
- a. Select **Security > Control > DHCP Snooping Global Configuration**. A screen similar to the following displays.



- b. For DHCP Snooping Mode, select the **Enable** radio button.
 - c. Click **Apply**.
 2. Enable DHCP snooping in a VLAN.
 - a. Select **Security > Control > DHCP Snooping Global Configuration**. A screen similar to the following displays.



- b. In the VLAN Configuration table, in the **VLAN ID** list, select **1**.
 - c. In the **DHCP Snooping Mode** field, select **Enable**. A screen similar to the following displays.



- d. Click **Apply**. A screen similar to the following displays.

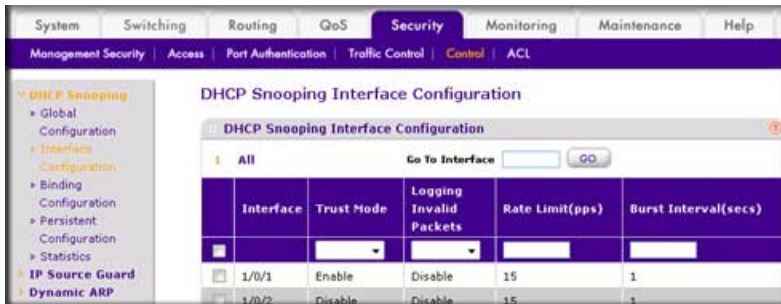


3. Configure the port through which the DHCP server is reached as trusted. Here interface 1/0/1 is trusted.

- a. Select **Security > Control > DHCP Snooping Interface Configuration**. A screen similar to the following displays.

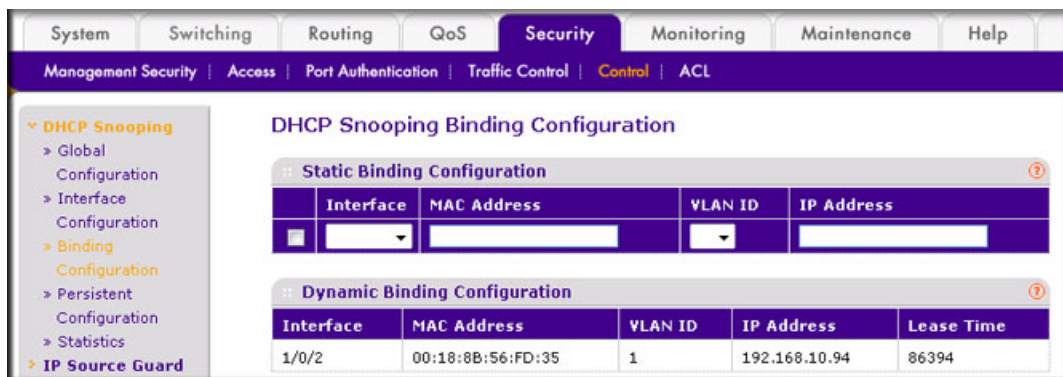


- b. Select Interface **1/0/1** check box.
- c. For interface 1/0/1, in the **Trust Mode** field, select **Enable**.
- d. Click **Apply**. A screen similar to the following displays.



4. View the DHCP Snooping Binding table.

Select **Security > Control > DHCP Snooping Binding Configuration**. A screen similar to the following displays.



5. Enable IP source guard in the interface 1/0/2.
 - a. Select **Security > Control > IP Source Guard > Interface Configuration**.
 - b. Select the Interface **1/0/2** check box.
 - c. For the IPSG mode, select **Enable**.

- d. Click **Apply**. A screen similar to the following displays.



6. Set up IP source guard static binding.
- Select **Security > Control > IP Source Guard > Binding Configuration**.
 - Select the Interface **1/0/2** check box.
 - In the **MAC Address** field, enter **00:05:05:05:05:05**.
 - In the **VLAN ID** field, enter **1**.
 - In the **IP Address** field, enter **192.168.10.80**.
 - Click **Add**. A screen similar to the following displays.



Simple Network Time Protocol

This chapter provides the following examples:

- *Show SNTP (CLI Only)*
- *Configure SNTP* on page 309
- *Set the Time Zone (CLI Only)* on page 311
- *Set the Named SNTP Server* on page 311

The SNTP feature offers these benefits:

- It can be used to synchronize network resources and for adaptation of NTP.
- SNTP provides synchronized network timestamp.
- It can be used in broadcast or unicast mode.
- It supports SNTP client implemented over UDP, which listens on port 123.

Show SNTP (CLI Only)

The following are examples of the commands used in the SNTP feature.

show sntp

```
(Netgear Switch Routing) #show sntp?  
  
<cr>      Press Enter to execute the command.  
client    Display SNTP Client Information.  
server    Display SNTP Server Information.
```

show sntp client

```
(Netgear Switch Routing) #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 Routing) #show sntp server

Server IP Address:        81.169.155.234
Server Type:              ipv4
Server Stratum:          3
Server Reference Id:      NTP Srv: 212.186.110.32
Server Mode:              Server
Server Maximum Entries:   3
Server Current Entries:   1

SNTP Servers
-----

IP Address:               81.169.155.234
Address Type:              IPV4
Priority:                  1
Version:                  4
Port:                     123
Last Update Time:         MAY 18 04:59:13 2005
Last Attempt Time:        MAY 18 11:59:33 2005
Last Update Status:       Other
Total Unicast Requests:   1111
Failed Unicast Requests:  361
```

Configure SNTP

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

CLI: Configure SNTP

NETGEAR switches do not have a built-in real-time clock. However, it is possible to use SNTP to get the time from a public SNTP/NTP server over the Internet. You may need permission from those public time servers. The following steps configure SNTP on the switch:

1. Configure the SNTP server IP address. The IP address can be either from the public NTP server or your own. You can search the Internet to locate the public server. The servers available could be listed in domain-name format instead of address format. In that case, use the `ping` command on the PC to find the server's IP address. The following example configures the SNTP server IP address to 208.14.208.19.

```
(Netgear Switch) (Config)#sntp server 208.14.208.19
```

2. After configuring the IP address, enable SNTP client mode. The client mode can be either broadcast mode or unicast mode. If the NTP server is not your own, you must use unicast mode.

```
(Netgear Switch) (Config)#sntp client mode unicast
```

3. Once SNTP client mode is enabled, the client waits for the polling interval to send the query to the server. The default value is approximately 1 minute. After this period, issue the `show`

command to confirm that the time has been received. The time will be used in all logging messages.

```
(Netgear Switch) #show sntp server
Server IP Address:          208.14.208.19
Server Type:                ipv4
Server Stratum:             4
Server Reference Id:        NTP Srv: 208.14.208.3
Server Mode:                Server
Server Maximum Entries:    3
Server Current Entries:    1
SNTP Servers
-----
IP Address: 208.14.208.19
Address Type: IPV4
Priority: 1
Version: 4
Port: 123
Last Update Time: Mar 26 03:36:09 2006
Last Attempt Time: Mar 26 03:36:09 2006
Last Update Status: Success
Total Unicast Requests: 2
Failed Unicast Requests: 0
```

Web Interface: Configure SNTP

1. Configure the SNTP server.
 - a. Select **System > Management > Time > SNTP Server Configuration**. A screen similar to the following displays.

The screenshot shows the Netgear web interface for SNTP Server Configuration. The navigation menu on the left includes System, Information, Switch Statistics, System Resource, IP Configuration, Slot Information, Time, and DNS. The main content area is titled "SNTP Server Configuration" and contains two tables.

SNTP Server Configuration Table:

Server Type	Address	Port	Priority	Version
IPv4	208.14.208.19	123	1	4
<input type="checkbox"/> DNS	time-d.netgear.com	123	1	4

SNTP Server Status Table:

Address	Last Update Time	Last Attempt Time	Last Attempt Status	Requests	Failed Requests
time-d.netgear.com		JAN 01 00:00:00 1970	Request Timed Out	0	70

- b. Enter the following information:

- In the **Server Type** field, select **IPv4**.
 - In the **Address** field, enter **208.14.208.19**.
 - In the **Port** field, enter **123**.
 - In the **Priority** field, enter **1**.
 - In the **Version** field, enter **4**.
- c. Click **Add**.
2. Configure SNMP globally.
- a. Select **System > Management > Time > SNMP Global Configuration**. A screen similar to the following displays.

- b. Enter the following information:
- For Client Mode, Select the **Unicast** radio button.
 - In the **Time Zone Name** field, enter **PST**.
 - In the **Offset Hours** field, enter **-8**.
- c. Click **Apply**.

Set the Time Zone (CLI Only)

The SNMP/NTP server is set to Coordinated Universal Time (UTC) by default. The following example shows how to set the time zone to Pacific Standard Time (PST), which is 8 hours behind GMT/UTC.

```
(Netgear switch)(config)#clock timezone PST -8
```

Set the Named SNMP Server

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

CLI: Set the Named SNTP Server

NETGEAR provides SNTP servers accessible by NETGEAR devices. Because NETGEAR might change IP addresses assigned to its time servers, it is best to access an SNTP server by DNS name instead of using a hard-coded IP address. The public time servers available are time-a, time-b, and time-c.

Enable a DNS name server and access a time server with the following commands:

```
(Netgear switch) (config)#ip domain-lookup
(Netgear switch) (config)#ip name-server 192.168.1.1
(Netgear switch) (config)#sntp server time-a.netgear.com
```

where *192.168.1.1* is the public network gateway IP address for your device.

This method of setting DNS name look-up can be used for any other applications that require a public IP address, for example, a RADIUS server.

Web Interface: Set the Named SNTP Server

1. Configure the SNTP server.
 - a. Select **System > Management > Time > SNTP Server Configuration**. A screen similar to the following displays.

Server Type	Address	Port	Priority	Version
<input checked="" type="checkbox"/> DNS	time-f.netgear.com	123	1	4
<input type="checkbox"/> DNS	time-d.netgear.com	123	1	4
<input type="checkbox"/> IPV4	208.14.208.19	123	1	4

Address	Last Update Time	Last Attempt Time	Last Attempt Status	Requests	Failed Requests

- b. Enter the following information:
 - In the **Server Type** list, select **DNS**.
 - In the **Address** field, enter **time-f.netgear.com**
 - In the **Port** field, enter **123**.
 - In the **Priority** field, enter **1**.
 - In the **Version** field, enter **4**.
 - c. Click **Add**.
 2. Configure the DNS server.

- a. Select **System > Management > DNS > DNS Configuration**. A screen similar to the following displays.

The screenshot shows a web-based configuration interface for a network switch. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. Below this, a secondary navigation bar shows Management, Device View, Services, Stacking, and SNMP. A left-hand sidebar contains a tree view with categories like System Information, Switch Statistics, System Resource, IP Configuration, Slot Information, Time, and DNS. The main content area is titled 'DNS Configuration' and contains two sections: 'DNS Configuration' with radio buttons for 'Disable' and 'Enable' (selected), and a text field for 'DNS Default Name'; and 'DNS Server Configuration' which is a table with columns for 'Serial No' and 'DNS Server'. The table contains one entry with '192.168.1.1' in the DNS Server field.

Serial No	DNS Server
	192.168.1.1

- b. Enter the following information:
- For DNS Status, select the **Enable** radio button
 - In the **DNS Server** field, enter **192.168.1.1**.
- c. Click **Add**.

This chapter provides the following examples:

- *Traceroute*
- *Configuration Scripting* on page 316
- *Pre-Login Banner* on page 319
- *Port Mirroring* on page 320
- *Dual Image* on page 321
- *Outbound Telnet* on page 324

Traceroute

This section describes the traceroute feature. Use traceroute to discover routes that packets take when traveling on a hop-by-hop basis to their destination through the network.

- Tracerout maps network routes by sending packets with small time-to-live (TTL) values and watches the ICMP time-out announcements.
- The tracerout command displays all L3 devices.
- It can be used to detect issues on the network .
- Tracerout tracks up to 20 hops.
- The default UPD port is used 33343 unless you specify otherwise in the `traceroute` command.

The following shows an example of using the `traceroute` command to determine how many hops there are to the destination. The command output shows each IP address the packet passes through and how long it takes to get there. In this example, the packet takes 16 hops to reach its destination.

CLI: Traceroute

```
(Netgear Switch) #traceroute?
<ipaddr>      Enter IP address.

(Netgear Switch) #traceroute 216.109.118.74 ?
<cr>         Press Enter to execute the command.
<port>       Enter port no.

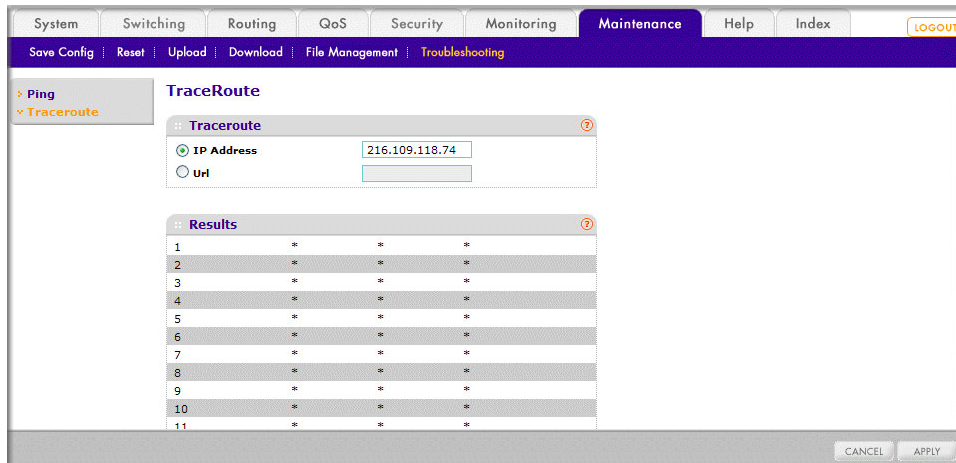
(Netgear Switch) #traceroute 216.109.118.74

racing route over a maximum of 20 hops

 1  10.254.24.1          40 ms      9 ms      10 ms
 2  10.254.253.1        30 ms      49 ms     21 ms
 3  63.237.23.33        29 ms      10 ms     10 ms
 4  63.144.4.1          39 ms      63 ms     67 ms
 5  63.144.1.141        70 ms      50 ms     50 ms
 6  205.171.21.89       39 ms      70 ms     50 ms
 7  205.171.8.154       70 ms      50 ms     70 ms
 8  205.171.8.222       70 ms      50 ms     80 ms
 9  205.171.251.34      60 ms      90 ms     50 ms
10  209.244.219.181     60 ms      70 ms     70 ms
11  209.244.11.9        60 ms      60 ms     50 ms
12  4.68.121.146        50 ms      70 ms     60 ms
13  4.79.228.2          60 ms      60 ms     60 ms
14  216.115.96.185     110 ms     59 ms     70 ms
15  216.109.120.203     70 ms      66 ms     95 ms
16  216.109.118.74      78 ms     121 ms     69 ms
```

Web Interface: Traceroute

1. Select **Maintenance > Troubleshooting > Traceroute**. A screen similar to the following displays.



Use this screen to tell the switch to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. Once you click the Apply button, the switch will send three traceroute packets each hop, and the results will be displayed in the result table.

2. In the **IP Address** field, enter **216.109.118.74**.
3. Click **Apply**.

Configuration Scripting

This section provides the following examples:

- *script* on page 317
- *script list and script delete* on page 317
- *script apply running-config.scr* on page 318
- *Create a Configuration Script* on page 318
- *Upload a Configuration Script* on page 318

Configuration scripting:

- Allows you to generate text-formatted files.
- Provides scripts that can be uploaded and downloaded to the system.
- Provides flexibility to create command configuration scripts.
- Can be applied to several switches.
- Can save up to 10 scripts or 500 K of memory.
- Provides script format of one CLI command per line.

Here are some considerations:

- The total number of scripts stored is limited by the NVRAM/FLASH size.
- Application of scripts is partial if a script fails. For example, if the script executes 5 of 10 commands and the script fails, the script stops at 5.
- Scripts cannot be modified or deleted while being applied.
- Validation of scripts checks for syntax errors only. It does not validate that the script will run successfully.

script

```
(Netgear Switch) #script ?

apply      Applies configuration script to the switch.
delete     Deletes a configuration script file from the switch.
list       Lists all configuration script files present on the switch.
show       Displays the contents of configuration script.
validate   Validate the commands of configuration script.
```

script list and script delete

```
(Netgear Switch) #script list

Configuration Script Name      Size(Bytes)
-----
basic.scr                      93
running-config.scr            3201

2 configuration script(s) found.
1020706 bytes free.

(Netgear Switch) #script delete basic.scr

Are you sure you want to delete the configuration script(s)? (y/n) y

1 configuration script(s) deleted.
```

script apply running-config.scr

```
(Netgear Switch) #script apply running-config.scr

Are you sure you want to apply the configuration script? (y/n) y

The system has unsaved changes.
Would you like to save them now? (y/n) y

Configuration Saved!
```

Create a Configuration Script

```
(Netgear Switch) #show running-config running-config.scr

Config script created successfully.

(Netgear Switch) #script list

Configuration Script Name      Size(Bytes)
-----
running-config.scr           3201

1 configuration script(s) found.
1020799 bytes free.
```

Upload a Configuration Script

```
(Netgear Switch) #copy nvram: script running-config.scr
tftp://192.168.77.52/running-config.scr

Mode..... TFTP
Set TFTP Server IP..... 192.168.77.52
TFTP Path..... ./
TFTP Filename..... running-config.scr
Data Type..... Config Script
Source Filename..... running-config.scr

Are you sure you want to start? (y/n) y

File transfer operation completed successfully.
```

Pre-Login Banner

Pre-login banner:

- Allows you to create message screens that display when a user logs in to the CLI.
- By default, no banner file exists.
- You can upload or download.
- File size cannot be larger than 2 K.

The Pre-Login Banner feature is only for the CLI interface.

Create a Pre-Login Banner (CLI Only)

1. On your PC, using Notepad create a banner.txt file that contains the banner to be displayed.

```
Login Banner - Unauthorized access is punishable by law.
```

2. Transfer the file from the PC to the switch using TFTP.

```
(Netgear Switch Routing) #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 Routing)#exit

(Netgear Switch Routing) >logout

Login Banner - Unauthorized access is punishable by law.
User:
```

Note: The `no clibanner` command removes the banner from the switch.

Port Mirroring

The port mirroring feature:

- Allows you to monitor network traffic with an external network analyzer.
- Forwards a copy of each incoming and outgoing packet to a specific port.
- Is used as a diagnostic tool, debugging feature, or means of fending off attacks.
- Assigns a specific port to copy all packets to.
- Allows inbound or outbound packets to switch to their destination and to be copied to the mirrored port.

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

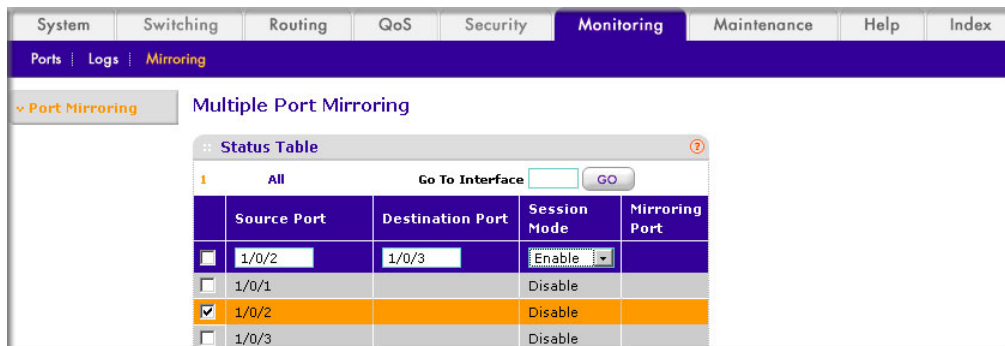
CLI: Specify the Source (Mirrored) Ports and Destination (Probe)

```
(Netgear Switch)#config
(Netgear Switch)(Config)#monitor session 1 mode
Enable mirror
(Netgear Switch)(Config)#monitor session 1 source interface 1/0/2
Specify the source interface.
(Netgear Switch)(Config)#monitor session 1 destination interface 1/0/3
Specify the destination interface.
(Netgear Switch)(Config)#exit
(Netgear Switch)#show monitor session 1
```

Session ID	Admin Mode	Probe Port	Mirrored Port
1	Enable	1/0/3	1/0/2

Web Interface: Specify the Source (Mirrored) Ports and Destination (Probe)

1. Select **Monitoring > Mirroring > Port Mirroring**. A screen similar to the following displays.



2. Scroll down and select the Source Port **1/0/2** check box. The value 1/0/2 now appears in the Interface field at the top.
3. Enter the following information:
 - In the **Destination Port** field, enter **1/0/3**.
 - In the **Session Mode** field, select **Enable**.
4. Click **Apply**.

Dual Image

Traditionally switches contain a single image in the permanent storage. This image is loaded into memory every time there is a reboot. The dual image feature allows switches to have two images in permanent storage. You can denote one of these images as an active image that will be loaded in subsequent reboots and the other image as a backup image. This feature provides for reduced down time for the switches, when the firmware is being upgraded or downgraded.

The images are stored in the file system with the file names `image1` and `image2`. These names are used in the CLI, Web, and SNMP interfaces. Each of the images can be associated with a textual description. The switch provides commands to associate and retrieve the text description for an image. A switch also provides commands to activate the backup image such that it is loaded in subsequent reboots. This activation command makes the current active image as the backup image for subsequent reboots.

On three successive errors executing the **active-image**, the switch attempts to execute the **backup-image**. If there are errors executing the **backup-image** as well, the bootloader will invoke the boot menu.

The Dual Image feature works seamlessly with the stacking feature. All members in the stack must be uniform in their support for the dual Image feature. The Dual Image feature works in the following way in a Stack.

- When an image is activated, the Management node notifies all the participating nodes. All nodes activate the specified image.
- When any node is unable to execute the **active-image** successfully, it attempts to execute the **backup-image**, as mentioned in the section above. Such cases will require user intervention to correct the problem, by using appropriate stacking commands.

CLI: Download a Backup Image and Make It Active

```
(Netgear Switch) #copy tftp://192.168.0.1/gsm73xxseps.stk image2
Mode..... TFTP
Set Server IP..... 192.168.0.1
Path..... /
Filename..... gsm73xxseps.stk
Data Type..... Code
Destination Filename..... image2
Management access will be blocked for the duration of the transfer Are you sure you want
to start? (y/n) y

TFTP code transfer starting
101888 bytes transferred...277504 bytes transferred...410112 bytes transferred...628224
bytes transferred...803328 bytes transferred...978944 bytes transferred...1154560 bytes
transferred...1330176 bytes transferred...1505280 bytes transferred...1680896 bytes
transferred...1861632 bytes transferred...2040320 bytes transferred...2215936 bytes
transferred...2391040 bytes transferred...2566656 bytes transferred...2741760 bytes
transferred...2916864 bytes transferred...3092992 bytes transferred...3268096 bytes
transferred...3443712 bytes transferred...3619328 bytes transferred...3794432 bytes
transferred...3970048 bytes transferred...4145152 bytes transferred...4320768 bytes
transferred...4496384 bytes transferred...4669952 bytes transferred...4849152 bytes
transferred...5027840 bytes transferred...5202944 bytes transferred...5378560 bytes
transferred...5554176 bytes transferred...5729280 by
tes transferred...5904896 bytes transferred...6078976 bytes transferred...6255616 bytes
transferred...6423040 bytes transferred...6606336 bytes transferred...6781952 bytes
transferred...6957056 bytes transferred...7111168 bytes transferred...7307776 bytes
transferred...7483392 bytes transferred...7658496 bytes transferred...

Verifying CRC of file in Flash File System
Distributing the code to the members of the stack!
File transfer operation completed successfully.
(Netgear Switch) #
(Netgear Switch) #show bootvar
Image Descriptions
  image1 : default image
  image2 :
Images currently available on Flash
```

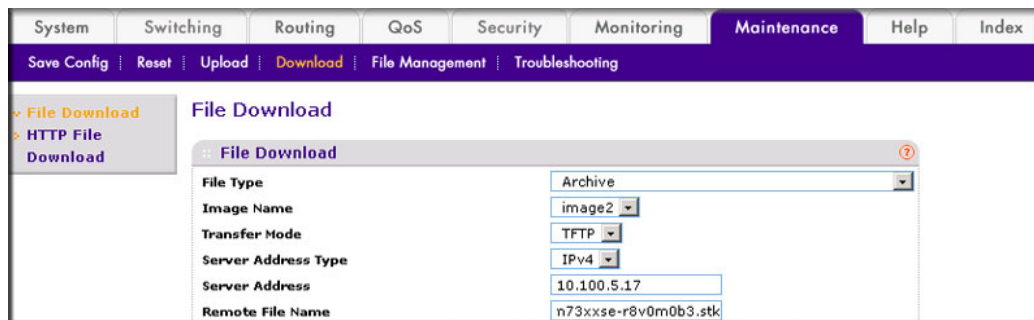
```

-----
unit      image1      image2      current-active      next-active
-----
1  5.11.2.51      8.0.0.2              image1              image1
(Netgear Switch) #boot system image2
Activating image image2 ..
(Netgear Switch) #show bootvar
Image Descriptions
image1 : default image
image2 :
Images currently available on Flash
-----
unit      image1      image2      current-active      next-active
-----
1  5.11.2.51      8.0.0.2              image1              image2
Image2 will be executed after reboot.

```

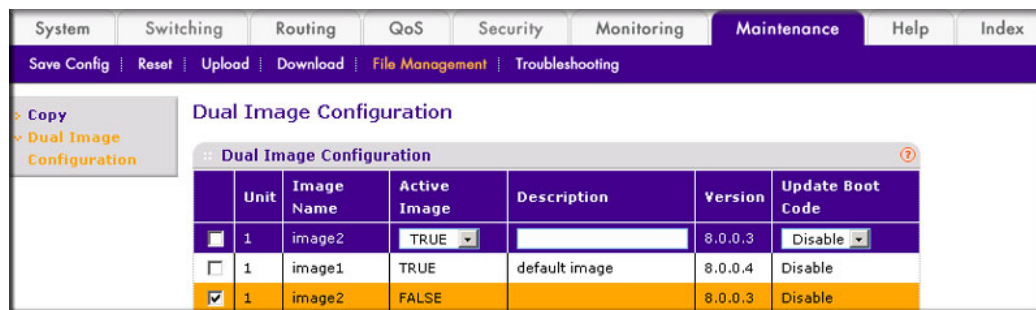
Web Interface: Download a Backup Image and Make It Active

1. Download a backup image using tftp.
 - a. Select **Maintenance > Download > File Download**. A screen similar to the following displays.



- b. In the **File Type** list, select **Archive**.
 - c. In the **Image Name** list, select **image2**.
 - d. In the **Transfer Mode** list, select **TFTP**.
 - e. In the **Server Address Type** list, select **IPv4**.
 - f. In the **Server Address** field, enter **10.100.5.17**(tftp server IP address).
 - g. In the **Remote File Name**, enter **gsm73xxse-r8v0m0b3.stk**.
 - h. Click **Apply**.
2. Activate image2.

- a. Select **Maintenance > File Management > Dual Image Configuration**. A screen similar to the following displays.



- b. Under Dual Image Configuration, scroll down and select the **Image 2** check box. The image2 now appears in the Image name field at the top.
- c. In the **Active Image** field, select **TRUE**.
- d. Click **Apply**.

Outbound Telnet

In this section, the following examples are provided:

- *CLI: show network* on page 325
- *CLI: transport output telnet* on page 326
- *Web Interface: Configure Telnet* on page 326
- *CLI: Configure the session-limit and session-timeout* on page 327
- *Web Interface: Configure the Session Timeout* on page 327

Outbound Telnet:

- Establishes an outbound Telnet connection between a device and a remote host.
- A Telnet connection is initiated, each side of the connection is assumed to originate and terminate at a network virtual terminal (NVT).
- Server and user hosts do not maintain information about the characteristics of each other's terminals and terminal handling conventions.
- Must use a valid IP address.

CLI: show network

```
(Netgear Switch Routing) >telnet 192.168.77.151
Trying 192.168.77.151...
(Netgear Switch Routing)
User:admin
Password:
(Netgear Switch Routing) >en
Password:

(Netgear Switch Routing) #show network

IP Address..... 192.168.77.151
Subnet Mask..... 255.255.255.0
Default Gateway..... 192.168.77.127
Burned In MAC Address..... 00:10:18.82.04:E9
Locally Administered MAC Address..... 00:00:00:00:00:00
MAC Address Type..... Burned In
Network Configuration Protocol Current... DHCP
Management VLAN ID..... 1
Web Mode..... Enable
Java Mode ..... Disable
```

CLI: show telnet

```
(Netgear Switch Routing)#show telnet

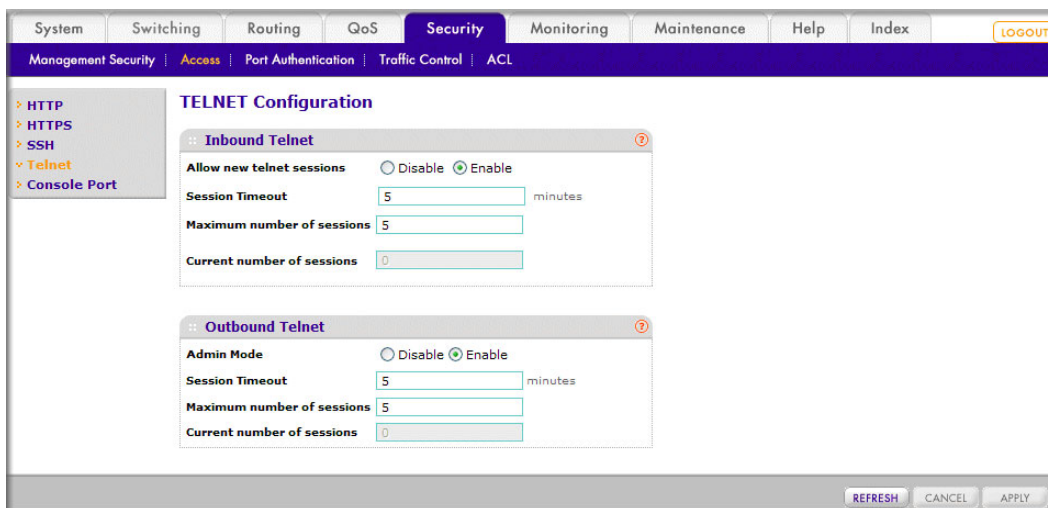
Outbound Telnet Login Timeout (minutes)..... 5
Maximum Number of Outbound Telnet Sessions..... 5
Allow New Outbound Telnet Sessions..... Yes
```

CLI: transport output telnet

```
(Netgear Switch Routing) (Config)#lineconfig ?
<cr>                               Press Enter to execute the command.
(Netgear Switch Routing) (Config)#lineconfig
(Netgear Switch Routing) (Line)#transport ?
input                               Displays the protocols to use to connect to a
                                   specific line of the router.
output                              Displays the protocols to use for outgoing
                                   connections from a line.
(Netgear Switch Routing) (Line)#transport output ?
telnet                              Allow or disallow new telnet sessions.
(Netgear Switch Routing) (Line)#transport output telnet ?
<cr>                               Press Enter to execute the command.
(Netgear Switch Routing) (Line)#transport output telnet
(Netgear Switch Routing) (Line)#
```

Web Interface: Configure Telnet

1. Select **Security > Access > Telnet**. A screen similar to the following displays.



- Under Outbound Telnet, for Admin Mode, select the **Enable** radio button.
- Click **Apply**.

CLI: Configure the session-limit and session-timeout

```
(Netgear Switch Routing) (Line)#session-limit ?
<0-5>          Configure the maximum number of outbound telnet sessions allowed.

(Netgear Switch Routing) (Line)#session-limit 5

(Netgear Switch Routing) (Line)#session-timeout ?
<1-160>       Enter time in minutes.

(Netgear Switch Routing) (Line)#session-timeout 15
```

Web Interface: Configure the Session Timeout

- Select **Security > Access > Telnet**. A screen similar to the following displays.

- Enter the following information:
 - In the **Session Timeout** field, enter **15**.
 - In the **Maximum number of sessions** field, enter **5**.
- Click **Apply**.

This chapter provides the following examples:

- *Show Logging* on page 329
- *Show Logging Buffered* on page 331
- *Show Logging Traplogs* on page 332
- *Show Logging Hosts* on page 333
- *Configure Logging for a Port* on page 334
- *Email Alerting* on page 336

The syslog feature:

- Allows you to store system messages and errors.
- Can store to local files on the switch or a remote server running a syslog daemon.
- Provides a method of collecting message logs from many systems.

The following illustration explains how to interpret log files.

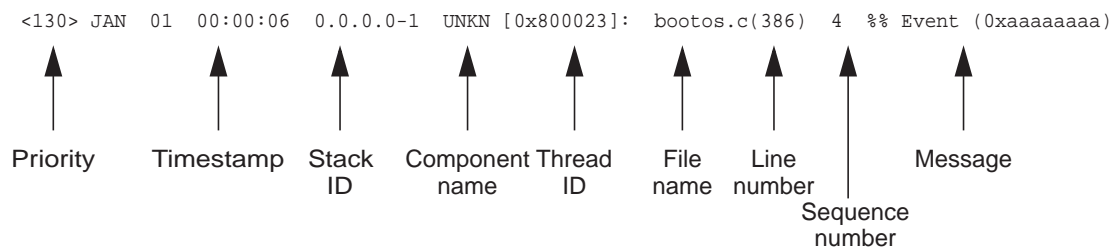


Figure 35. Log Files

Show Logging

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

CLI: Show Logging

```
(Netgear Switch Routing) #show logging

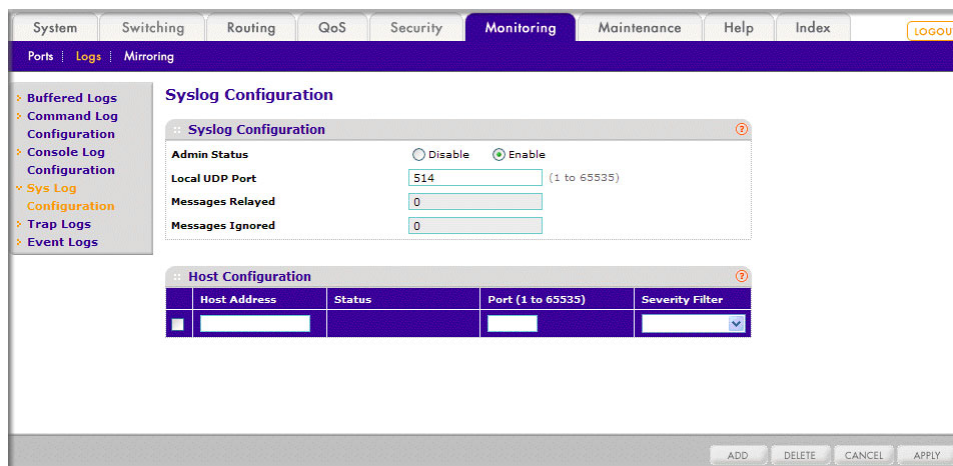
Logging Client Local Port      : 514
CLI Command Logging           : disabled
Console Logging               : disabled
Console Logging Severity Filter : alert
Buffered Logging              : enabled

Syslog Logging                 : enabled

Log Messages Received         : 66
Log Messages Dropped          : 0
Log Messages Relayed          : 0
Log Messages Ignored          : 0
```

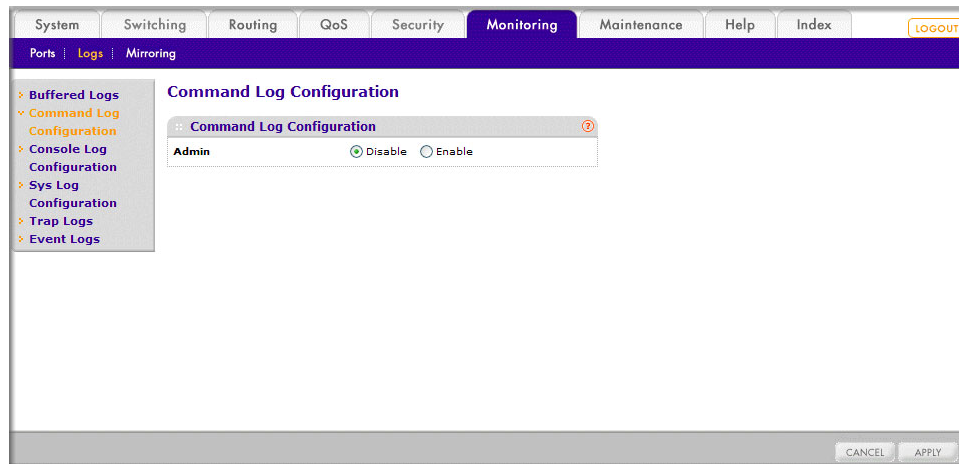
Web Interface: Show Logging

1. Configure the syslog.
 - a. From the main menu, select **Monitoring > Logs > Sys Log Configuration**.



- b. In the Syslog Configuration, next to the Admin Status, select the **Enable** radio button.
 - c. Click **Apply**.
 2. Configure the command log.

a. Select **Monitoring > Logs > Command Log**.

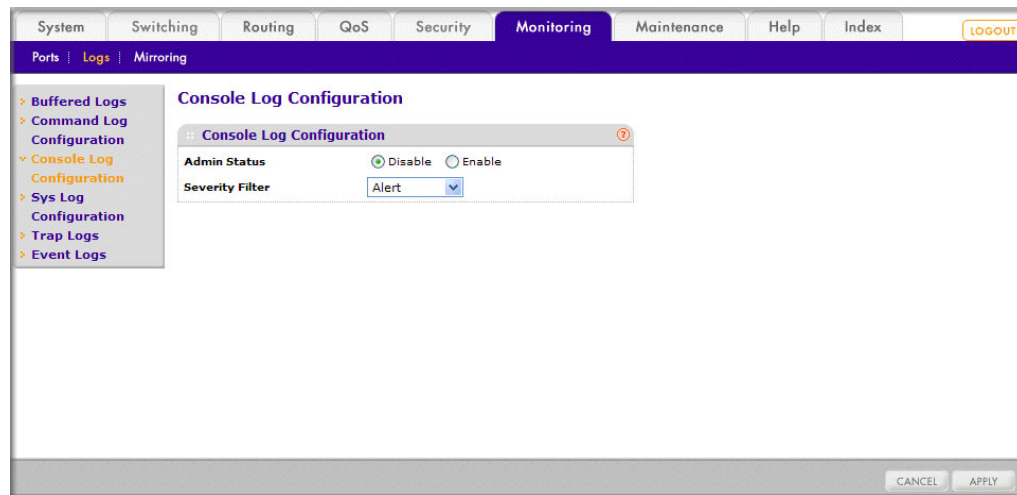


b. Under Command Log, for Admin Status, select the **Disable** radio button.

c. Click **Apply**.

3. Configure the console log.

a. Select **Monitoring > Logs > Console Log**.

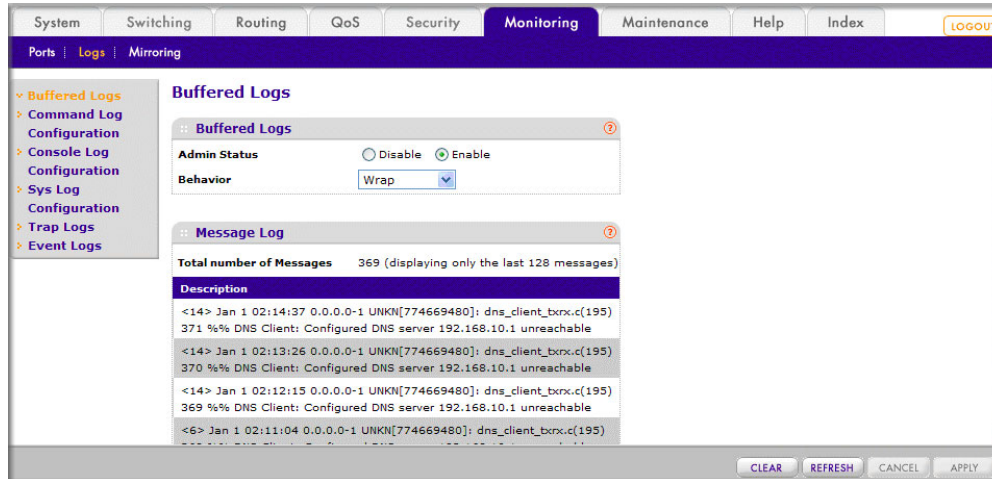


b. Under Console Log Configuration, for Admin Status, select the **Disable** radio button.

c. Click **Apply**.

4. Configure the buffer logs.

- a. Select **Monitoring > Logs > Buffer Logs**. A screen similar to the following displays.



- b. Under Buffer Logs, for Admin Status, select the **Enable** radio button.
c. Click **Apply**.

Show Logging Buffered

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

CLI: Show Logging Buffered

```
(Netgear Switch Routing) #show logging buffered ?

<cr>   Press Enter to execute the command.

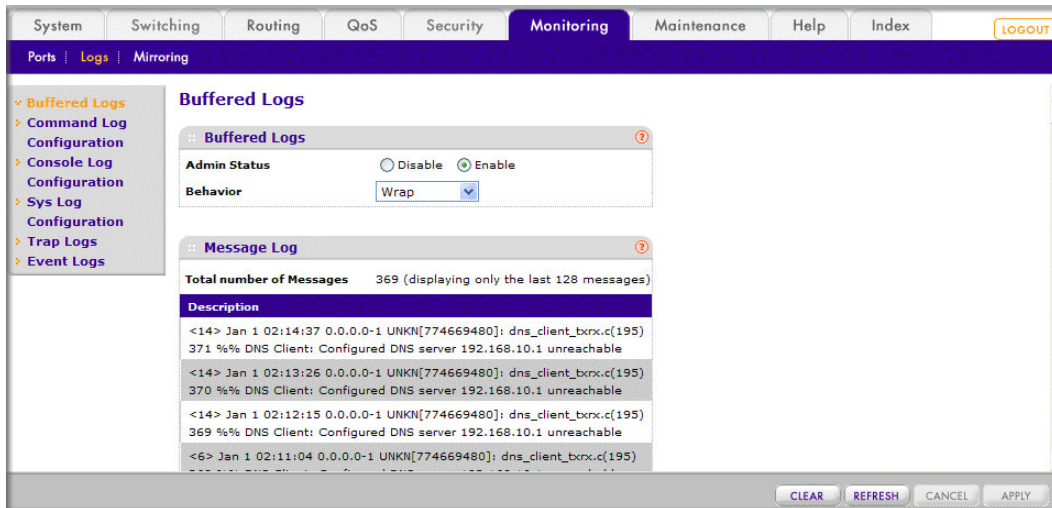
(Netgear Switch Routing) #show logging buffered

Buffered (In-Memory) Logging           :   enabled
Buffered Logging Wrapping Behavior     :   On
Buffered Log Count                     :   66

<1> JAN 01 00:00:02 0.0.0.0-0 UNKN[268434944]: usmdb_sim.c(1205) 1 %% Error 0 (0x0)
<2> JAN 01 00:00:09 0.0.0.0-1 UNKN[268434944]: bootos.c(487) 2 %% Event
(0xaaaaaaaa)
<6> JAN 01 00:00:09 0.0.0.0-1 UNKN[268434944]: bootos.c(531) 3 %% Starting code...
<6> JAN 01 00:00:16 0.0.0.0-3 UNKN[251627904]: cda_cnfgr.c(383) 4 %% CDA: Creating new
STK file.
<6> JAN 01 00:00:39 0.0.0.0-3 UNKN[233025712]: edb.c(360) 5 %% EDB Callback: Unit Join:
3.
<6> JAN 01 00:00:40 0.0.0.0-3 UNKN[251627904]: sysapi.c(1864) 6 %% File user_mgr_cfg:
same version (6) but the sizes (2312->7988) differ
```

Web Interface: Show Logging Buffered

Select **Monitoring > Logs > Buffer Logs**. A screen similar to the following displays.



Show Logging Traplogs

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

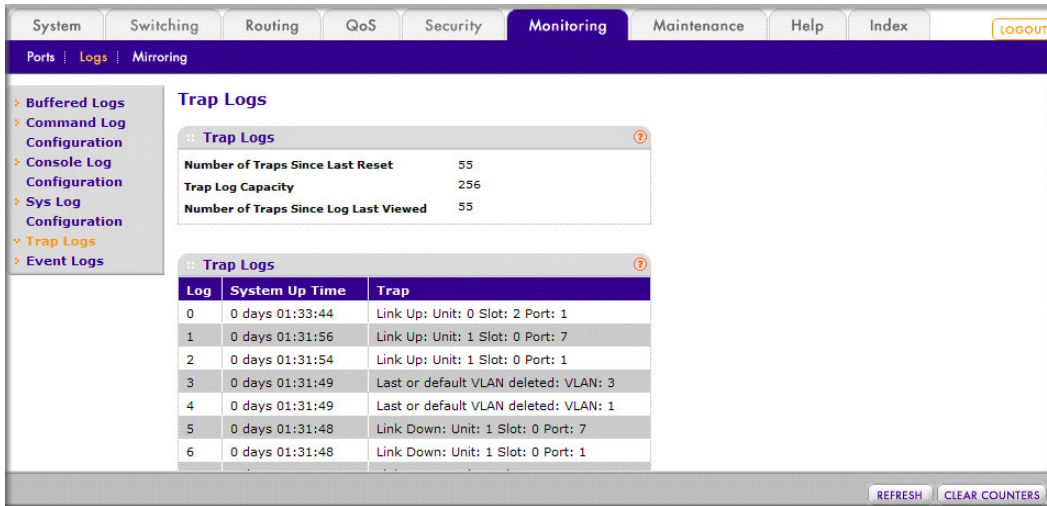
CLI: Show Logging Traplogs

```
(Netgear Switch Routing) #show logging traplogs ?
<cr> Press Enter to execute the command.
(Netgear Switch Routing) #show logging traplogs
Number of Traps Since Last Reset..... 6
Trap Log Capacity.....256
Number of Traps Since Log Last Viewed..... 6

Log System Up Time      Trap
-----
0  0 days 00:00:46      Link Up: Unit: 3 Slot: 0 Port: 2
1  0 days 00:01:01      Cold Start: Unit: 0
2  0 days 00:21:33      Failed User Login: Unit: 1 User ID: admin
3  0 days 18:33:31      Failed User Login: Unit: 1 User ID: \
4  0 days 19:27:05      Multiple Users: Unit: 0      Slot: 3 Port: 1
5  0 days 19:29:57      Multiple Users: Unit: 0      Slot: 3 Port: 1
```

Web Interface: Show Logging Trap Logs

Select **Monitoring > Logs > Trap Logs**. A screen similar to the following displays.



Show Logging Hosts

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

CLI: Show Logging Hosts

```
(Netgear Switch Routing) #show logging hosts ?

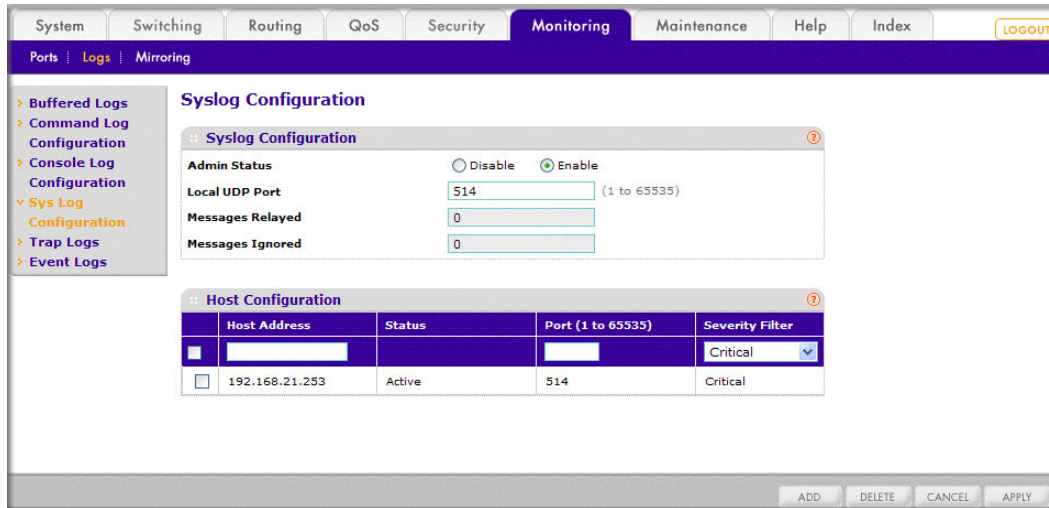
<cr>                               Press Enter to execute the command.

(Netgear Switch Routing) #show logging hosts

Index      IP Address      Severity  Port    Status
-----  -
1         192.168.21.253  critical  514    Active
```

Web Interface: Show Logging Hosts

Select **Monitoring > Logs > Sys Log Configuration**. A screen similar to the following displays.



Configure Logging for a Port

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

CLI: Configure Logging for the Port

```
(Netgear Switch Routing) #config

(Netgear Switch Routing) (Config)#logging ?

buffered          Buffered (In-Memory) Logging Configuration.
cli-command       CLI Command Logging Configuration.
console           Console Logging Configuration.
host              Enter IP Address for Logging Host
syslog            Syslog Configuration.

(Netgear Switch Routing) (Config)#logging host ?
<hostaddress>    Enter Logging Host IP Address
reconfigure       Logging Host Reconfiguration
remove           Logging Host Removal
(Netgear Switch Routing) (Config)#logging host 192.168.21.253 ?

<cr>             Press Enter to execute the command.
<port>           Enter Port Id
```

```
(Netgear Switch Routing) (Config)#logging host 192.168.21.253 4 ?

<cr>          Press Enter to execute the command.
<severitylevel> Enter Logging Severity Level (emergency|0, alert|1, critical|2,
error|3, warning|4, notice|5, info|6, debug|7).

(Netgear Switch Routing) (Config)#logging host 192.168.21.253 4 1 ?

<cr>          Press Enter to execute the command.

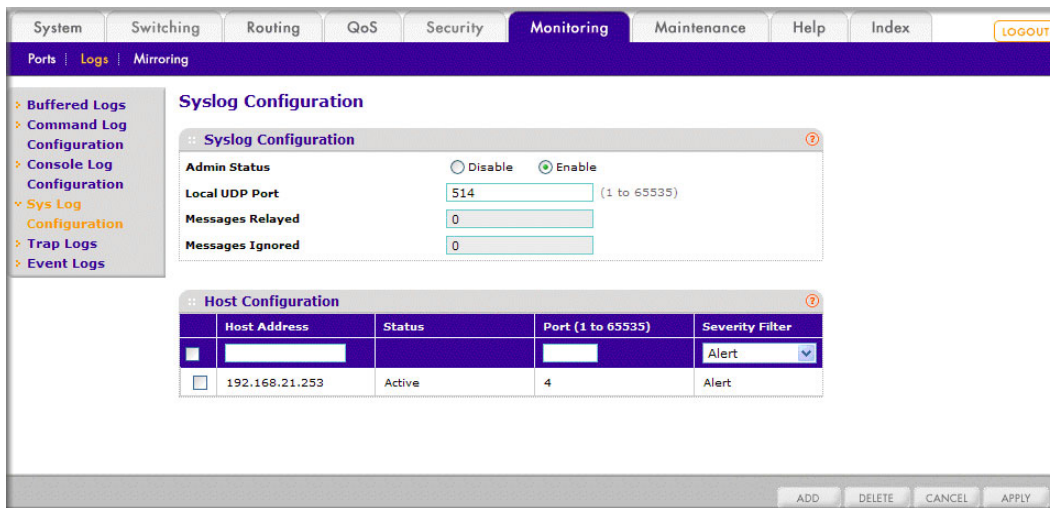
(Netgear Switch Routing) (Config)#logging host 192.168.21.253 4 1

(Netgear Switch Routing) #show logging hosts

Index      IP Address      Severity  Port      Status
-----
1          192.168.21.253  alert    4         Active
```

Web Interface: Configure Logging for the Port

1. Select **Monitoring > Logs > Sys Log Configuration**. A screen similar to the following displays.



2. Enter the following information:
 - In the **Host Address** field, enter your host address **192.168.21.253**.
 - In the **Port** field, enter **4**.
 - In the **Severity Filter** list, select **Alert**.
3. Click **Add**.

Email Alerting

Email Alerting is an extension of the logging system. The logging system allows you to configure a set of destinations for log messages. This feature adds the email configuration, through which the log messages are sent to a configured SMTP server such that an administrator may receive the log in an email account of their choice.

This feature is enabled globally. When email alerting is enabled, selected log messages are sent to an SMTP server. Log messages are divided into three groups by severity level: urgent, non-urgent, and never.

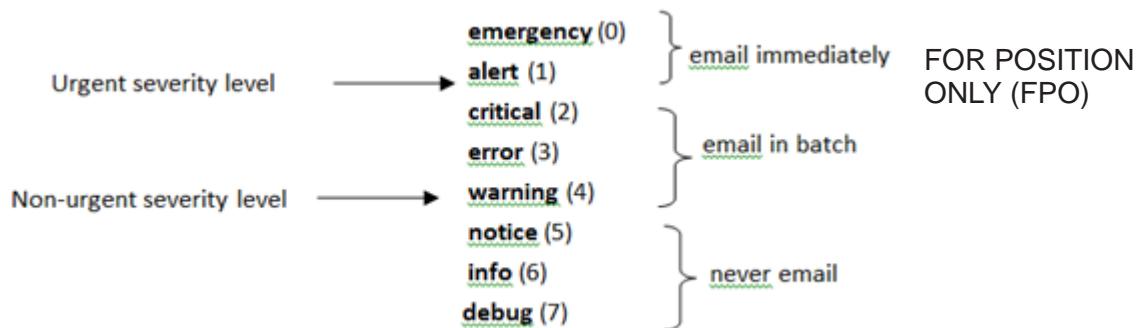


Figure 36. Log message severity levels

The network administrator can adjust the urgent and non-urgent severity levels. These levels are global and apply to all destination email addresses. Log messages in the urgent group are sent immediately to the SMTP server with each log message in a separate mail. Log messages in the non-urgent group are batched into a single email message and after a configurable delay.

Email alerting also provides a configuration option that allows the network administrator to specify the severity level at which SNMP traps are logged. Using this option, the administrator can put traps in the urgent group, the non-urgent group, or the never group for emailing. Traps are not emailed by default. For traps to be emailed, the network administrator has to either increase the severity at which traps are logged, or lower the severity level of log messages that are emailed.

The network administrator can configure multiple destination email addresses, and for each email address, specify whether to deliver urgent log messages, non-urgent log messages, or both.

There is an exception to the sending of the messages periodically to the SMTP server. When the log buffer is completely full before the expiry of the periodic timer sending of the log messages to the SMTP server does not until the expiry of the timer. When the log buffer is full, a connection is opened immediately with the SMTP server, and all the messages that have not previously been emailed are sent to it.

CLI: Send Log Messages to admin@switch.com Using Account aaaa@netgear.com

1. Configure an SMTP server, for example, smtp.netgear.com. Before you configure the smtp server, you need to have an account on SMTP server.

```
(Netgear Switch) (Config)#mail-server "smtp.netgear.com" port 465
(Netgear Switch) (Mail-Server)#security tlsv1
(Netgear Switch) (Mail-Server)# username aaaa
(Netgear Switch) (Mail-Server)# password xxxxxx
(Netgear Switch) (Mail-Server)#exit
```

2. Configure logging mail. From-addr is the source address of email and to-addr is the destination address of email.

```
(Netgear Switch) (Config)#logging email
(Netgear Switch) (Config)#logging email from-addr aaaa@netgear.com
(Netgear Switch) (Config)#logging email message-type urgent to-addr admin@switch.com
(Netgear Switch) (Config)#logging email message-type non-urgent to-addr admin@switch.com
```

3. Increase the severity of traps to 3 (error). By default, it is 6 (infor).

```
(Netgear Switch) (Config)#logging traps 3
```

This chapter describes the concepts and recommended operating procedures to manage NETGEAR stackable managed switches running release 4.x.x.x or newer.

This chapter includes the following topics:

- *Switch Stack Management and Connectivity*
- *The Stack Master and Stack Members* on page 339
- *Install and Power-up a Stack* on page 341
- *Switch Firmware* on page 342
- *Configure a Stacking Port as an Ethernet Port* on page 344
- *Stack Switches Using 10G Fiber* on page 347
- *Add, Remove, or Replace a Stack Member* on page 350
- *Switch Stack Configuration Files* on page 352
- *Preconfigure a Switch* on page 353
- *Renumber Stack Members* on page 354
- *Move the Stack Master to a Different Unit* on page 356
- *M5300 and GSM73xxSv2 Mixed Stacking* on page 357
- *Create a Mixed Stack with an M5300-28G3 Switch and a GSM7328Sv2 Switch* on page 358
- *Change the SDM template back to the default* on page 360

Switch Stack Management and Connectivity

You manage the switch stack through the stack master. You cannot manage stack members on an individual basis. To access the stack master, use either a serial connection to the switch master's console port, or a Telnet connection to the IP address of the stack.

You can use these methods to manage switch stacks:

- Web Management Interface.
- CLI (over a serial connection).
- A network management application through SNMP.

The Stack Master and Stack Members

A switch stack is a set of up to 8 switches connected through their stacking ports. The switch that controls the operation of the stack is the stack master. The stack master and the other switches in the stack are stack members. Stack members use stacking technology to behave and work together as a unified system. Layer 2 and Layer 3 protocols present the entire switch stack as a single entity to the network. The following figure shows an example of switches that are interconnected to form a stack.

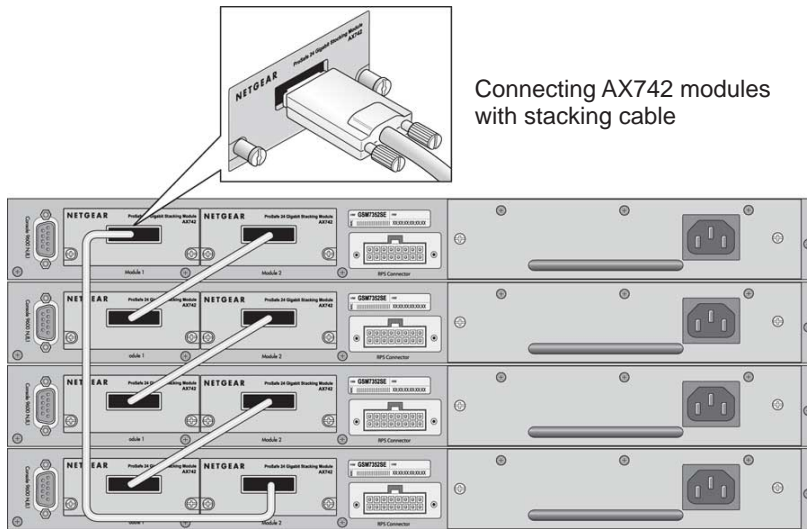


Figure 37. Stacked switches

Stack Master

The stack master is the single point of stack-wide management. From the stack master, you configure:

- System-level (global) features that apply to all stack members.
- Interface-level features for all interfaces on any stack member.

A switch stack is identified in the network by its network IP address. The network IP address is assigned according to the MAC address of the stack master. Every stack member is uniquely identified by its own *stack member number*.

The stack master contains the saved and running configuration files for the switch stack. The configuration files include the system-level settings for the switch stack and the interface-level settings for all stack members. Each stack member retains a copy of the saved file for backup purposes. If the master is removed from the stack, another member is elected master, and then runs from that saved configuration.

All stack members are eligible stack masters. If the stack master becomes unavailable, the remaining stack members participate in electing a new stack master. A set of factors determine which switch is elected the stack master. The stack master is elected or re-elected based on one of these factors and in the order listed:

1. The switch that is currently the stack master.
2. The switch with the highest stack member priority value.

Note: NETGEAR recommends assigning the highest priority value to the switch that you prefer to be the stack master. This ensures that the switch is re-elected as stack master if a re-election occurs.

3. The switch with the higher MAC address.

A stack master retains its role unless one of these events occurs:

- The stack master is removed from the switch stack
- The stack master is reset or powered off
- The stack master has failed
- The switch stack membership is increased by adding powered-on standalone switches or switch stacks

In the case of a master re-election, the new stack master becomes available after a few seconds. In the meantime, the switch stack uses the forwarding tables in memory to minimize network disruption. The physical interfaces on the other available stack members are not affected while a new stack master is elected. If a new stack master is elected and the previous stack master becomes available, the previous stack master does not resume its role as stack master.

Stack Members

A switch stack has up to 8 stack members connected through their stacking ports. A switch stack always has one stack master.

A standalone switch is a switch stack with one stack member that also operates as the stack master. You can connect one standalone switch to another to create a switch stack containing two stack members, with one of them being the stack master. You can connect standalone switches to an existing switch stack to increase the stack membership.

The operation of the switch stack continues uninterrupted during membership changes unless you remove the stack master or you add powered-on standalone switches or switch stacks.

Stack Member Numbers

A stack member number (1 to 8) identifies each member in the switch stack. The member number also determines the interface-level configuration that a stack member uses. You can display the stack member number by using the `show switch user EXEC` command.

A new, out-of-the-box switch (one that has not joined a switch stack or has not been manually assigned a stack member number) ships with a default stack member number of 1. When it

joins a switch stack, its default stack member number changes to the lowest available member number in the stack.

Stack members in the same switch stack cannot have 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.

See *Renumber Stack Members* on page 354.

Stack Member Priority Values

You can change a stack member priority. This is useful if you want to change the master of the stack. Use the following command (in the global config mode):

```
switch unit priority value
```

Install and Power-up a Stack

Note: Many switch models such as the GSM7200PS and GSM7300S series have a *Hardware Installation Guide* that includes additional information about rack mounting and stack cabling.

Compatible Switch Models

NETGEAR stackable managed switches include the following models:

- FSM7226RS
- FSM7250RS
- FSM7328S
- FSM7328PS
- FSM7352S
- FSM7352PS
- GSM7328S
- GSM7352S
- GSM7328FS
- GSM7228PS
- GSM7252PS
- M5300 Series

The FSM family, GSM family, and XSM72224S cannot be stacked together at this point.

Install a Switch Stack

Note: Many models of switches have a *Hardware Installation Guide* that includes additional information about rack mounting and switch stack cabling.

1. Install the switches in a rack.
2. Install all stacking cables, including the redundant stack link. It is highly recommended that a redundant link be installed.
3. Identify the switch to be the master. Power up this switch first.
4. Monitor the console port. Allow this switch to come up to the login prompt. If the switch has the default configuration, it should come up as unit #1, and automatically become a master switch. If not, renumber the units.
5. If you want to configure switches offline, preconfigure the other switches to be added to the stack. See [Preconfigure a Switch](#) on page 353.
6. Power on a second switch, making sure it is adjacent (the next physical switch in the stack) to the switch already powered up. This ensures that the second switch comes up as a member of the stack, and not a master of a separate stack.
7. Monitor the master switch to see that the second switch joins the stack. Use 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. Renumber this stack member, if you want. See [Renumber Stack Members](#) on page 354 for recommendations for renumbering stack members.

Repeat steps 6 through 8 to add members to the stack. Always power on a switch adjacent to the switches already in the stack.

Switch Firmware

All stack members must run the same firmware version. This helps ensure full compatibility in the stack protocol version among the stack members.

If a stack member is running a different firmware version than the stack master, that stack member is not allowed to join the stack. Use the `show switch` command to list the stack members and firmware versions. See the following section [Code Mismatch](#).

You can upgrade a switch that has an incompatible firmware image by using the command `copy xmodem | ymodem | zmodem | tftp://ip/filepath/filename`. 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.

Code Mismatch

If a switch is added to a stack and it does not have the same version of code as that of the master, the following occurs:

- The new unit boots up and becomes a member of the stack.
- Ports on the added unit remain in the detached state.
- A message displays on the CLI indicating a code mismatch with the newly added unit.
- To have the newly added unit to merge normally with the stack, use the `copy` command to load the correct code from the master to the newly added unit. Then reset the newly added member. It should reboot normally and join the stack.

Upgrade the Firmware

All stack members must run the same firmware version. Ports on stack members that don't match the master switch firmware version don't come up and the `show switch` command shows a code mismatch error.

1. NETGEAR recommends that you schedule the firmware upgrade when there is no excessive network traffic (such as a broadcast event).
2. Download new firmware using TFTP or xmodem to the master switch using the `copy` command.

Once the firmware is successfully loaded on the master switch, it automatically propagates to the other units in the stack.



CAUTION:

To avoid errors during code propagation, do not move stack cables or reconfigure units.

3. If an error occurs during code propagation, first check to make sure the master switch is running the correct firmware. Then issue the `copy` command (in stack configuration mode) to make another attempt to copy the firmware to the units that did not get updated.
4. Once code is loaded to all members of the stack, reset all the switches so that the new firmware starts running.

Migrate Configuration with a Firmware Upgrade

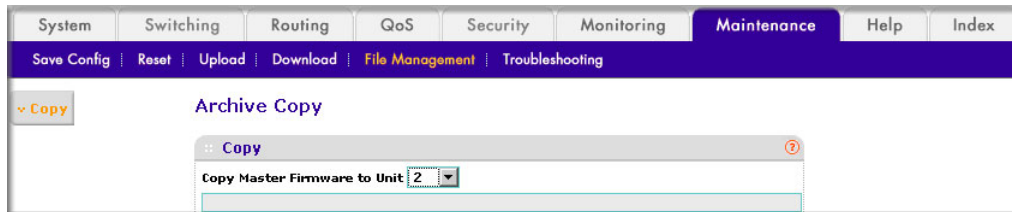
In some cases, a configuration might not be carried forward in a code update. For updates where this issue is to be expected, the following procedure should be followed:

1. Save the current configuration by uploading it from the stack, using the `copy` command from the CLI.
2. Load new code into the stack manager. Reboot the stack.
3. Upon reboot, go into the boot menu and erase the configuration (restore to factory defaults)

4. Continue with the boot of operational code.
5. Once the stack is up, download the saved configuration back to the master. This configuration should then be automatically propagated to all members of the stack.

Copy Master Firmware to a Stack Member (Web Interface)

1. Select **System > Management > Basic > Stack Configuration**. A screen similar to the following displays.



2. In the **Copy Master Firmware to Unit** list, select **2**.
3. Click **Apply**.

Configure a Stacking Port as an Ethernet Port

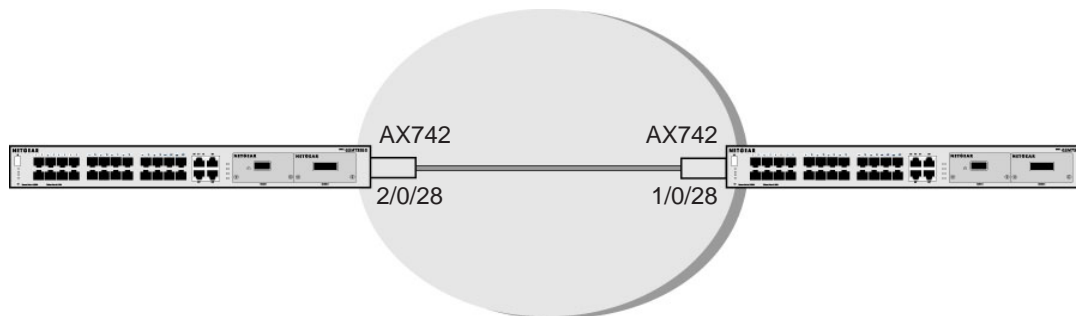


Figure 38. Configuring a stacking port as an Ethernet port

Follow these steps to set up the topology:

1. Insert the AX742 into the I/O module on the switch.
2. Configure the switch A and B as described in the following instructions.
3. Connect the AX 742 with stack cable.
4. Reboot Switch A and Switch B.

CLI: Configure a Stacking Port as an Ethernet Port

1. On Switch A, Configure the Stack Port and Reboot

```
(Netgear Switch) #show stack-port
```

Unit	Intf	SlotId	Type	XFP Adapter	Configured		Running		Link Speed (Gb/s)
					Stack Mode	Stack Mode	Link Status	Link Status	
2	0/27		None		Stack	Stack	Link Down	0	
2	0/28		AX742	(stack)	Stack	Stack	Link Down	12	

```
(Netgear Switch) #config
(Netgear Switch) (Config)#stack
(Netgear Switch) (Config-stack)#stack-port 2/0/28 ethernet
(Netgear Switch) (Config-stack)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #reload
Are you sure you want to reload the stack? (y/n) y
```

After Switch A reboots:

```
(Netgear Switch) #show port 2/0/28
```

Intf	Type	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	LACP Mode	Actor Timeout
2/0/28		Enable	10G Full	10G Full	Up	Enable	Enable	long

2. On Switch B, Configure the stack port and reboot.

```
(Netgear Switch) #
(Netgear Switch) #show stack-port
```

Unit	Intf	SlotId	Type	XFP Adapter	Configured		Running		Link Speed (Gb/s)
					Stack Mode	Stack Mode	Link Status	Link Status	
1	0/51		AX742	(stack)	Ethernet	Ethernet	Link Down	12	
1	0/52		AX741		Ethernet	Ethernet	Link Down	10	

```
(Netgear Switch) #config
(Netgear Switch) (Config)#stack
(Netgear Switch) (Config-stack)#stack-port 1/0/51 ethernet
(Netgear Switch) (Config-stack)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #reload
Are you sure you want to reload the stack? (y/n) y
```

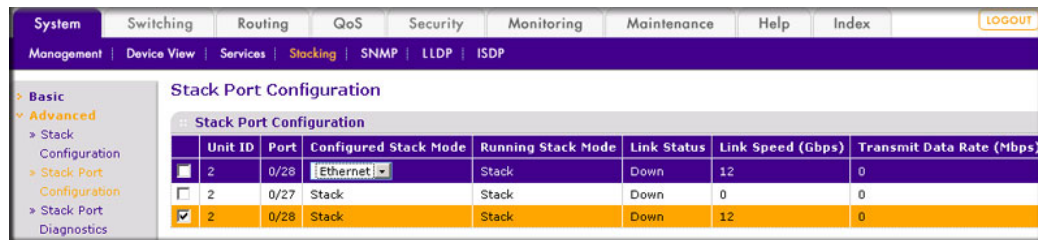
After Switch B reboots:

```
(Netgear Switch) #show port 2/0/28
```

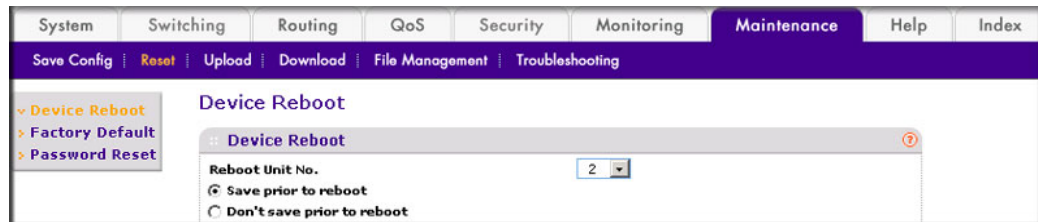
Intf	Type	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	LACP Mode	Actor Timeout
1/0/51	Enable	10G Full	10G Full	Up	Enable	Enable	long	

Web Interface: Configure a Stacking Port as an Ethernet Port

- On Switch A, configure a stack port as an Ethernet port.
 - Select **System > Stacking > Advanced > Stack Port Configuration**. A screen similar to the following displays.

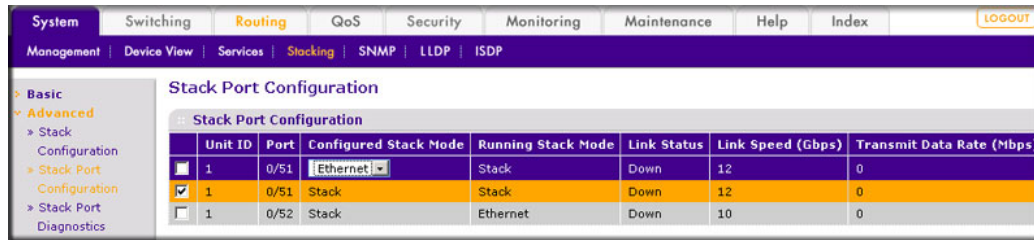


- Under Stack Port Configuration, scroll down and select the **2/0/28** check box.
 - In the **Configured Stack Mode** list, select **Ethernet**.
 - Click **Apply** to save the settings.
- Reboot the switch.
 - Select **Maintenance > Reset > Device Reboot**. A screen similar to the following displays.

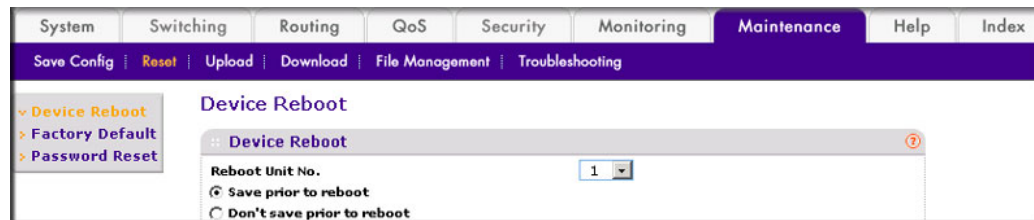


- In the **Reboot Unit No.** list, select **2**.
 - Click **Apply**.
- On Switch B, configure a stack port as an Ethernet port

- a. Select **System > Stacking > Advanced > Stack Port Configuration**. A screen similar to the following displays.



- b. Under Stack Port Configuration, scroll down and select the **1/0/51** check box.
 - c. In the Configured Stack Mode list, select **Ethernet**.
 - d. Click **Apply** to save the settings.
4. Reboot the switch.
 - a. Select **Maintenance > Reset > Device Reboot**. A screen similar to the following displays.



- b. In the **Reboot Unit No.** list, select **1**.
- c. Click **Apply**.

Stack Switches Using 10G Fiber

This example shows how to stack two switches in different buildings at long distance using 10G fiber. First insert AX741 to I/O slot on Switch A, and insert AX741 to I/O slot on Switch B. Then connect the two AX741 with fiber.

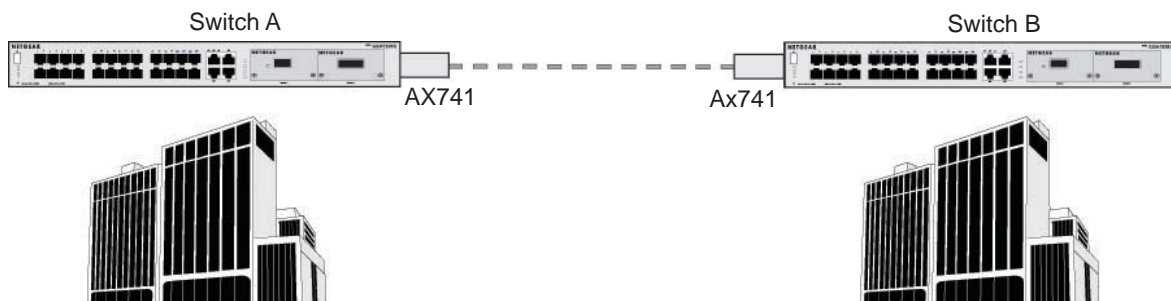


Figure 39. Using 10G fiber to stack switches in different buildings

CLI: Stack Switches Using 10G Fiber

1. On Switch A, show the port information.

```
(Netgear Switch) #show stack-port
```

Unit	Intf	SlotId	Type	XFP Adapter	Configured	Running	Link	Link Speed (Gb/s)
					Stack Mode	Stack Mode	Link Status	
1	0/51			None	Ethernet	Ethernet	Link Down	12
1	0/52			AX741	Stack	Stack	Link Down	0

In this case, port 1/0/52 has been configured as stack, so no action is needed.

2. On Switch B, show the stack port information.

```
(Netgear Switch) #show stack-port
```

Unit	Intf	SlotId	Type	XFP Adapter	Configured	Running	Link	Link Speed (Gb/s)
					Stack Mode	Stack Mode	Link Status	
2	0/27			None	Stack	Stack	Link Down	0
2	0/28			AX741	Ethernet	Ethernet	Link Down	12

3. Since 2/0/28 is in Ethernet mode, it must be changed to stack mode.

```
(Netgear Switch) (Config)#stack
(Netgear Switch) (Config-stack)#stack-port 2/0/28 stack
(Netgear Switch) (Config-stack)#exit
(Netgear Switch) (Config)
```

4. Reboot Switch B.

```
(Netgear Switch) #reload
Management switch has unsaved changes.
Would you like to save them now? (y/n) n
Configuration Not Saved!
Are you sure you want to reload the stack? (y/n) y
Reloading all switches.
```

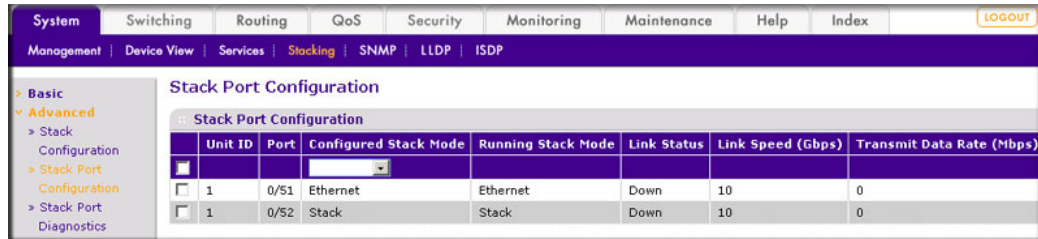
On Switch A, you see the following:

```
(Netgear Switch) #show switch
```

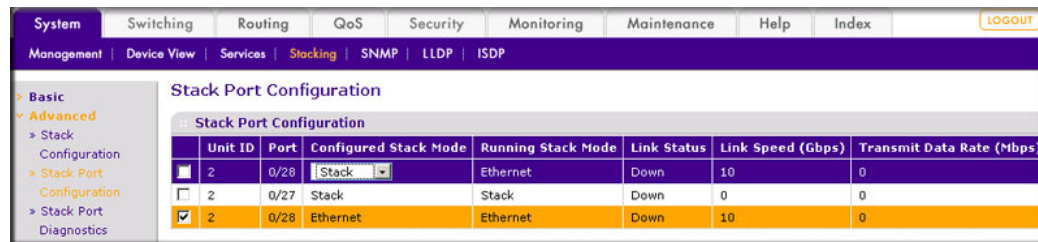
Management SW	Standby Switch	Preconfig Model ID	Plugged-in Model ID	Switch Status	Code Version
1	Mgmt Sw	GSM7352Sv2	GSM7352Sv2	OK	8.0.1.2
2	Stack Mbr	Oper Stby GSM7328Sv2	GSM7328Sv2	OK	8.0.1.2

Web Interface: Stack Switches Using 10G Fiber

1. On Switch A, show the Port Information.
 - a. Select **System > Stacking > Advanced > Stack Port Configuration**. A screen similar to the following displays.

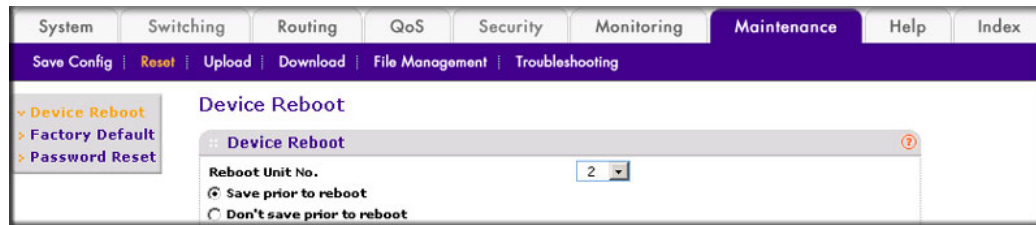


- b. Since the port 1/0/52 is stack mode already, nothing needs to be done.
2. On Switch B, configure port 2/0/28 as stacking port.
 - a. Select **System > Stacking > Advanced > Stack Port Configuration**. A screen similar to the following displays.



- b. Scroll down and select the **2/0/28** check box.
 - c. In the **Configured Stack Mode** list, select **Stack**.
 - d. Click **Apply** to save the settings.
3. Reboot the switch.

- a. Select **Maintenance > Reset > Device Reboot**. A screen similar to the following displays.



- b. In the **Reboot Unit No.** list, select **2**.
- c. Click **Apply**.

Add, Remove, or Replace a Stack Member

Add Switches to an Operating Stack

1. Make sure the redundant stack connection is in place and functional. All stack members should be connected in a logical ring.
2. Preconfigure the new switches, if desired.
3. Power off all new switches that will be joining the stack.



CAUTION:

If you cable one or more powered-on switches to the stack, the existing stack and the new switches assume two stacks are merging. They elect a single, new stack master, and you cannot specify which switch becomes the new master. All stack members assume configuration based on the new stack master. Stack members change their stack member numbers to the lowest available numbers.

4. Install the new switches in the rack. This procedure assumes installation below the bottom-most switch, or above the top-most switch.
5. Disconnect the redundant stack cable that connects the last switch in the stack back up to the first switch in the stack at the position in the ring where the new switch is to be inserted.

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. Verify, by monitoring the master switch console port, that the new switch joins the stack by issuing the `show switch` command. The new switch should join as a member (never as master; the existing master of the stack should not change).
8. If the firmware version of the newly added member is not the same as the existing stack, update the firmware as described in *Upgrade the Firmware* on page 343.

Remove a Switch from the Stack

1. Make sure the redundant stack connection is in place and functional. All stack members should be connected in a logical ring.
2. Power down the switch to be removed.

Note: Removing powered-on stack members can cause the switch stack to divide (partition) into two or more switch stacks, each with the same configuration. However, if cabled correctly, the switch stack should not divide.

3. Disconnect the stack cables.
4. If the switch is not to be replaced, reconnect the stack cable from the stack member above to the stack member below the switch being removed.
5. Remove the switch from the rack.
6. If you want to remove the switch from the stack configuration, issue the command:
`no member <unit-id>`.

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.

If you did not intend to partition the switch stack:

1. Power off the newly created switch stacks.
2. Reconnect them to the original switch stack through their stacking ports.
3. Power on the switches.

Replace a Stack Member

1. Make sure the redundant stack connection is in place and functional. All stack members should be connected in a logical ring.
2. Power down the switch to be removed and disconnect its stack cables.
3. Remove the switch from the rack.
4. If you will be installing a different model switch, remove the unit from the configuration by issuing the command `no member <unit-id>`.

5. Install the new switch in the rack:
 - If you are installing the same model switch, put it in the same position in the stack as the one that you just removed.
 - If you are installing a different model switch you can either put it in the same position as the previous switch, or at the bottom of the stack.
6. Cable the new switch, following the established order of stacking cables.
7. Power up the new switch. Verify, by monitoring the master switch console port, that the new switch successfully joins the stack by issuing the `show switch` command. The new switch should join as a member (never as master; the existing master of the stack should not change).
8. If the code version of the newly added member is not the same as the existing stack, update the code as described in [Upgrade the Firmware](#) on page 343.

Switch Stack Configuration Files

The configuration files record settings for all global and interface-specific settings that define the operation of the stack and individual members. Once a `save config` command is issued, all stack members store a copy of the configuration settings. If a stack master becomes unavailable, any stack member assuming the role of stack master will operate from the saved configuration files.

When a new, out-of-box switch joins a switch stack, it uses the system-level settings of that switch stack. However, if you want it to store this system level configuration, you must issue a `save config` command.

You back up and restore the stack configuration using the copy command the same way that you would for standalone switch configuration.

The following table provides switch stack configuration scenarios. Most of the scenarios assume at least two switches are connected through their stacking ports.

Table 1. Switch Stack Master Scenarios

Scenario	Action	Result
Stack master election specifically determined by existing stack masters. Note: This is not recommended.	Connect two powered-on switch stacks through the stacking ports.	Only one of the stack masters becomes the new stack master. No other stack members become the stack master.
Stack master election specifically determined by the stack member priority value.	<ul style="list-style-type: none"> • Connect two switches through their stacking ports. • Use the global configuration command <code>switch stack-member-number priority new-priority-number</code> to set a stack member to a higher member priority value. • Restart both stack members at the same time. 	The stack member with the higher-priority value is elected stack master.

Table 1. Switch Stack Master Scenarios (Continued)

Scenario	Action	Result
Stack master election specifically determined by the MAC address.	Assuming that both stack members have the same priority value and firmware image, restart both stack members at the same time.	The stack member with the higher MAC address is elected stack master.
Add a stack member.	<ul style="list-style-type: none"> • Power off the new switch • Through their stacking ports, connect the new switch to a powered-on switch stack. • Power on the new switch. 	The stack master is retained. The new switch is added to the switch stack.
Stack master failure.	Remove (or power off) the stack master.	One of the remaining stack members becomes the new stack master. All other members in the stack remain stack members and do not reboot.

Preconfigure a Switch

You can preconfigure (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 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.

1. Issue the `member <unit-id> <switchindex>` command. To view the supported unit types, use the `show supported switchtype` command.
2. Next, configure the unit you just defined with configuration commands, just as if the unit were physically present.

Ports for the preconfigured unit come up in a detached state.

3. To see the ports, use the `show port all` command. Now you can configure the detached ports for VLAN membership and any other port-specific configuration.

After you preconfigure a unit type for a specific unit number, attaching a unit with different unit type for this unit number causes the switch to report an error. The `show switch` command indicates config mismatch for the new unit and the ports on that unit don't come up. To resolve this situation, you can change the unit number of the mismatched unit or delete the preconfigured unit type using 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 occur when the switch stack compares the preconfigured configuration with the new switch.

Table 2. Preconfigured Switches Compared to Stack Configuration

Switch Type Is the Same	Stack Member Number	Result
Yes	Is the same.	The switch stack applies configuration to the preconfigured new switch and adds it to the stack.
Yes	Does not match.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • The switch stack applies the default configuration to the new switch and adds it to the stack. • The preconfigured information is changed to reflect the new information.
	Is not found in the preconfigured switch.	The switch stack applies the default configuration to the preconfigured switch and adds it to the stack.

Renumber Stack Members

This example is provided as CLI commands and a Web interface procedure.

CLI: Renumber Stack Members

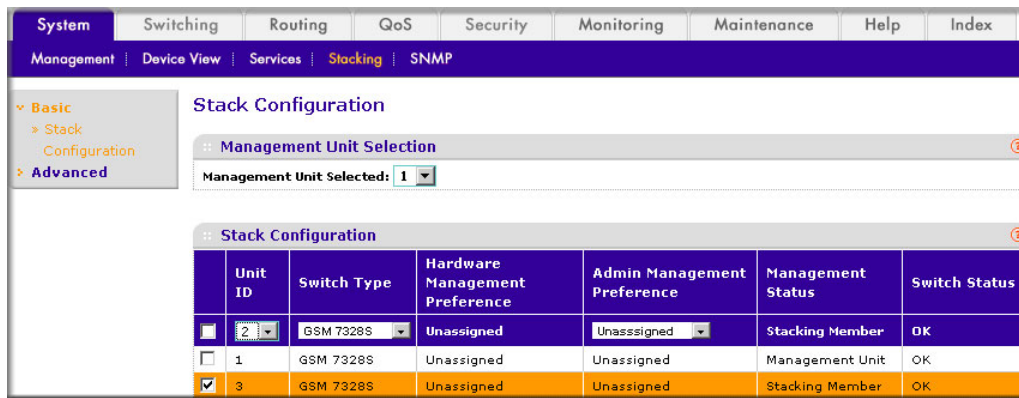
Note: When issuing a command (such as move management, or renumber), NETGEAR recommends that you wait until the command has fully executed before issuing the next command. For example, if a reset is issued to a stack member, use the `show port` command to verify that the switch has re-merged with the stack, and all ports are joined before issuing the next command.

- If specific numbering is required, NETGEAR recommends that you assign stack members their numbers when they are first installed and configured in the stack, if possible.
- If the stack unit number for a switch is unused, you can renumber the unit by using the `switch <oldunit-id> renumber <newunit-id>` CLI command. This command is found in global config mode.
- If the newunit-id has been preconfigured, you might need to remove the newunit-id from the configuration before renumbering the unit.

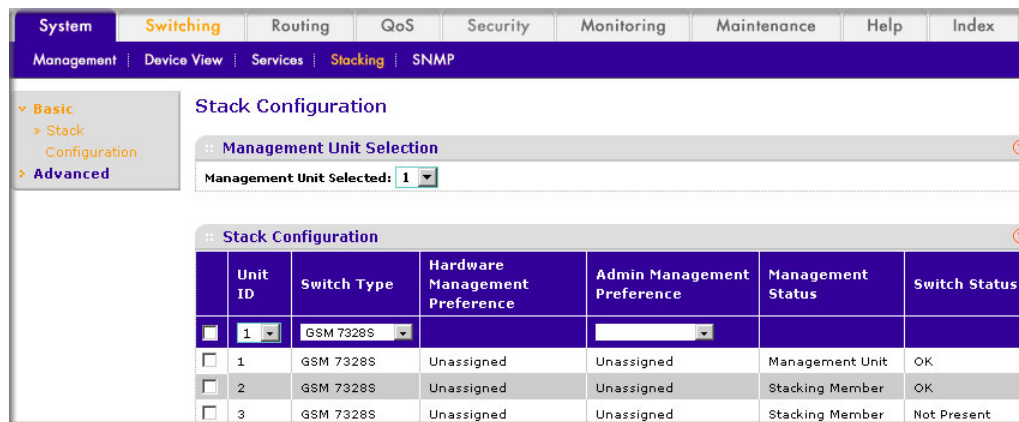
- If you need to reassign multiple existing stack unit numbers, the configuration could become mismatched. To avoid this situation, NETGEAR recommends that you power down all switches except the master, and then add them back one at a time using the procedure in Section *Add Switches to an Operating Stack* on page 350.

Web Interface: Renumber Stack Members

1. Renumber the stacking member's ID from 3 to 2.
 - a. Select **System > Management > Basic > Stack Configuration**. A screen similar to the following displays.



- b. Under Stack Configuration, scroll down and select the Unit ID 3 check box.
- c. In the Unit ID list, select 2.
- d. Click **Apply**.
- e. Now the unit ID of the stacking member is 2.



Move the Stack Master to a Different Unit

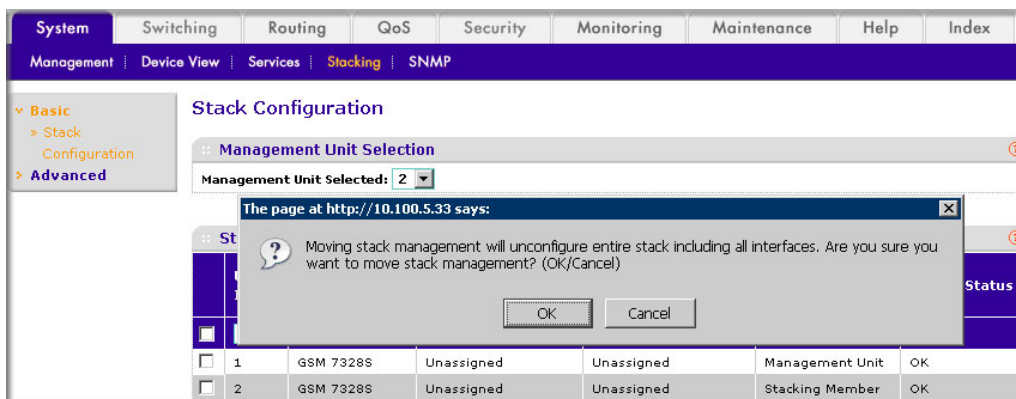
This example is provided as CLI commands and a Web interface procedure.

CLI: Move the Stack Master to a Different Unit

1. Using the `movemanagement` command, move the master to a different unit number. The operation takes between 30 seconds and 3 minutes depending on the stack size and configuration. The command is `movemanagement <fromunit-id> <tounit-id>`.
2. Make sure that you can log in on the console attached to the new master. Use the `show switch` command to verify that all units rejoined the stack.
3. NETGEAR recommends that you rest the stack with the `reload` command after moving the master.

Web Interface: Move the Stack Master to a Different Unit

1. Select **System > Management > Basic > Stack Configuration**. A screen similar to the following displays.



2. In the **Management Unit Selected** list, select **2**.

A warning window displays.

3. Click the **OK** button.
4. Click **Apply**.

Note: If you move a master to a different unit, you might lose the connection to the switch because the IP address could change if the switch gets its IP address using DHCP.

M5300 and GSM73xxSv2 Mixed Stacking

Normally stacking NETGEAR switches is limited to switches of similar types, for example, GSM7328S and GSM7352S, or GS728TS and GS752TPS. However, with the introduction of M5300 switches, you can stack M5300 switches with older GSM73xxSv2 (GSM7228PS, GSM7252PS, GSM7328Sv2, and GSM7352Sv2) switches. This section provides examples of mixed stacking.

The NETGEAR stacking architecture requires the capacities and capabilities of stacked switches to be compatible. Only switches with matching SDM templates can be stacked together before M5300 and GSM73xxSv2 switches can be joined to form a stack, the following steps are required:

1. Check the firmware release version installed on each switch. Make sure each is running release 10.0 firmware.
2. Review the available Switch Database Management (SDM) templates on the target switch.
3. Select the matching SDM template on the target switch.
4. Reboot the switch with newly selected template.
5. Connect the switches together to form the stack.

For more information on SDM, see the Command Line Interface Manual (CLI) , available on the resource CD shipped with your switch or the NETGEAR download website. SDM template matching is needed when mixing the following M5300 series switches with older switch models:

Table 3. Switches That can be Stacked Together

M5300 Series Switches	GSM7xxxSv2 Series Switches
M5300-28G	GSM7328SV2
M5300-52G	GSM7352SV2
M5300-28G3	GSM7228PS
M5300-52G3	GSM7252PS
M5300-28GF3	
M5300-28G-POE+	
M5300-52G-POE+	

Once the stack is formed successfully, all the normal stacking rules and procedures apply.

**CAUTION:**

Since the existing configuration might be invalid with the new SDM template, changing the SDM template on the switch causes the switch configuration be set to the factory defaults. A warning message is displayed in the browser window if the web GUI is used or on the console if the CLI is used. You are prompted to confirm that the current configuration will be cleared and the switch will be rebooted.

Create a Mixed Stack with an M5300-28G3 Switch and a GSM7328Sv2 Switch

The following example demonstrates how to stack an M5300-28G3 switch and a GSM7328Sv2 switch. Stacking other combinations of M5300 series switches and GSM73xxS switches use the same process.

Before an M5300 switch can be stacked with a GSM73xxSv2 switch, both switches must have the same 10.0 firmware version. The SDM templates are only available in release 10.0. If for example, the GSM7328Sv2 switch is running firmware version 8.0.3.25, the GSM7328Sv2 switch must first be upgraded to one of the version 10.0 images available from the NETGEAR product support website. The 10.0 version for the GSM7328Sv2 switch must be the same version that is used in the M5300 switch.

After the GSM7328Sv2 switch is upgraded to firmware version 10.0.0.23 (assuming this is the available version on GSM7328Sv2 website and version 10.0.0.23 is running on the M5300-28G3), use the `show sdm prefer` command to show the default SDM template setting:

```
(GSM7328Sv2) #show sdm prefer

The current template is the 'dual ipv4 and ipv6 smb' template.

ARP Entries..... 1024
IPv4 Unicast Routes..... 224
IPv6 NDP Entries..... 512
IPv6 Unicast Routes..... 128
ECMP Next Hops..... 4
IPv4 Multicast Routes..... 128
IPv6 Multicast Routes..... 128
```

By default, an M5300 switch using version 10.0 firmware has the SDM template set to 'dual ipv4 and ipv6 enterprise'. The GSM7328Sv2 switch using version 10.0.0.23 firmware has the SDM template set to 'dual ipv4 and ipv6 smb'. You need to change the SDM template on the M5300 switch to match the template on the GSM7328Sv2 switch.

CLI: Change the SDM template on the M5300 switch to match the one on the GSM7328Sv2 switch.:

```
(M5300) (Config)#sdm prefer ipv4-routing smb
```

After the command is issued, check the SDM template setting on the M5300 switch to make sure it is now set to 'dual ipv4 and ipv6 smb'. When the M5300-28G3 switch is verified to have the correct SDM template, you can connect the M5300-28G3 and GSM7328Sv2 switches together to form the stack.

Web Interface: Change the SDM template on the M5300 switch to match the one on the GSM7328Sv2 switch.

1. Select **System > Management > SDM Template Preference**

The screenshot shows the 'SDM Template Preference' configuration page. The 'SDM Current Template ID' is set to 'Dual IPv4 and IPv6 Enterprise'. The 'SDM Next Template ID' dropdown menu is also set to 'Dual IPv4 and IPv6 Enterprise'. Below this, a 'Summary' table lists various SDM templates and their associated metrics.

SDM Template	ARP Entries	IPv4 Unicast Routes	IPv6 NDP Entries	IPv6 Unicast Routes	ECMP Next Hops	IPv4 Multicast Routes	IPv6 Multicast Routes
Dual IPv4 and IPv6 SMB	1024	224	512	128	4	128	128
Dual IPv4 and IPv6 Enterprise	4096	6112	1024	3072	4	512	256
IPv4 SMB	2045	480	0	0	4	256	0
IPv4 Enterprise	6144	12256	0	0	4	1024	0
IPv4 Data Center Enterprise	4096	6112	0	0	16	1024	0
IPv4 Data Center Plus Enterprise	6144	12256	0	0	16	1024	0
Dual IPv4 and IPv6 Data Center Enterprise	4096	6112	1024	3072	16	512	256

2. Select **Default** from the drop-down menu next to **SDM Next Template ID** field.
3. Click **Apply**.

Change the SDM template back to the default

CLI: Change the SDM template back to the default

```
(M5300) (Config)#no sdm prefer
Startup-config will be deleted on the affected units and the
units will be force rebooted.
Are you sure you want to change the SDM Template ID? (y/n)y
```

Note: After this command is issued, the switch will remove the startup-config and reboot. Upload your start-config before issuing this command, and confirm you really want to issue the command.

Web Interface: Change the SDM template back to the default

1. Select **System > Management > SDM Template Preference**

The screenshot shows the 'SDM Template Preference' configuration page. The 'SDM Next Template ID' is set to 'Dual IPv4 and IPv6 Enterprise'. Below this is a 'Summary' table with the following data:

SDM Template	ARP Entries	IPv4 Unicast Routes	IPv6 NDP Entries	IPv6 Unicast Routes	ECMP Next Hops	IPv4 Multicast Routes	IPv6 Multicast Routes
Dual IPv4 and IPv6 SMB	1024	224	512	128	4	128	128
Dual IPv4 and IPv6 Enterprise	4096	6112	1024	3072	4	512	256
IPv4 SMB	2045	480	0	0	4	256	0
IPv4 Enterprise	6144	12256	0	0	4	1024	0
IPv4 Data Center Enterprise	4096	6112	0	0	16	1024	0
IPv4 Data Center Plus Enterprise	6144	12256	0	0	16	1024	0
Dual IPv4 and IPv6 Data Center Enterprise	4096	6112	1024	3072	16	512	256

2. Select **Default** from the drop-down menu for **SDM Next Template ID**.
3. Click **Apply**.

This chapter provides the following examples:

- *Add a New Community*
- *Enable SNMP Trap* on page 362
- *SNMP V3* on page 363
- *sFlow* on page 365
- *Time-Based Sampling of Counters with sFlow* on page 369

Add a New Community

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

CLI: Add a New Community

```
(Netgear switch) #config  
(Netgear switch) (Config)#snmp-server community rw public@4
```

Web Interface: Add a New Community

1. Select **System > SNMP > SNMP V1/V2 > Community Configuration**. A screen similar to the following displays.

	Community Name	Client Address	Client IP Mask	Access Mode	Status
<input checked="" type="checkbox"/>	public@4	0.0.0.0	0.0.0.0	Read/Write	Enable
<input type="checkbox"/>	public	0.0.0.0	0.0.0.0	ReadOnly	Enable
<input type="checkbox"/>	private	0.0.0.0	0.0.0.0	ReadWrite	Enable
<input type="checkbox"/>	public@1	0.0.0.0	0.0.0.0	ReadOnly	Enable
<input type="checkbox"/>	public@2	0.0.0.0	0.0.0.0	ReadOnly	Enable
<input type="checkbox"/>	public@3	0.0.0.0	0.0.0.0	ReadOnly	Enable

2. In the **Community Name** field, enter **public@4**.
3. In the **Client Address** field, enter **0.0.0.0**.
4. In the **Client IP Mask** field, enter **0.0.0.0**.
5. In the **Access Mode** field, select **Read/Write**.
6. In the **Status** field, select **Enable**.
7. Click **Add**.

Enable SNMP Trap

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

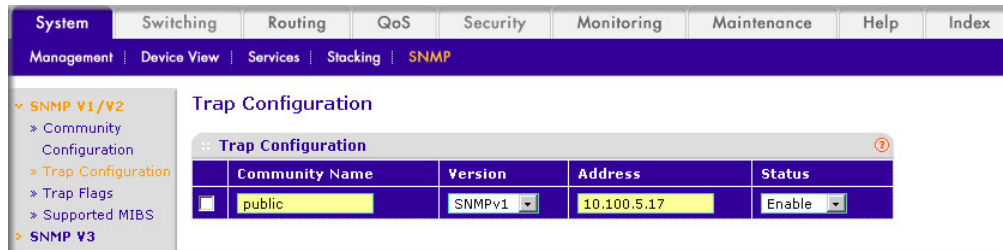
CLI: Enable SNMP Trap

This example shows how to send SNMP trap to the SNMP server.

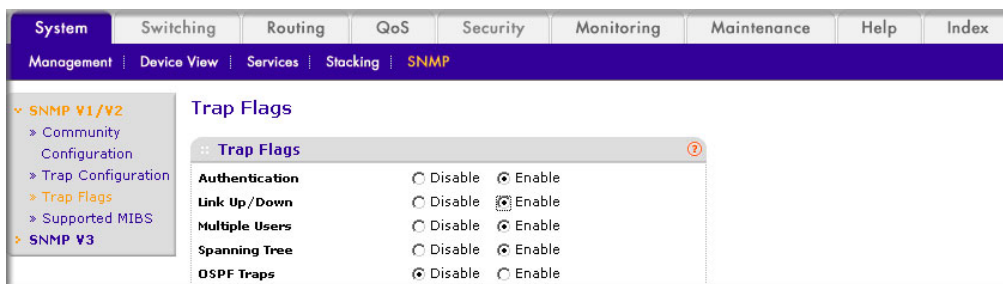
```
(Netgear switch) #config
(Netgear switch) (Config)# snmptrap public 10.100.5.17
                                Enable send trap to SNMP server 10.100.5.17
(Netgear switch) (Config)#snmp-server traps linkmode
                                Enable send link status to the SNMP server when
link status changes.
```

Web Interface: Enable SNMP Trap

1. Enable SNMP trap for the server 10.100.5.17.
 - a. Select **System > SNMP > SNMP V1/V2 > Trap Configuration**. A screen similar to the following displays.



- b. In the **Community Name** field, enter **public**.
 - c. In the **Version** list, select **SNMPv1**.
 - d. In the **Address** field, enter **10.100.5.17**.
 - e. In the **Status** field, select **Enable**.
 - f. Click the **Add** button.
2. Set the Link Up/Down flag.
 - a. Select **System > SNMP > SNMP V1/V2 > Trap Flags**. A screen similar to the following displays.



- b. For Link Up/Down, select the **Enable** radio button.
 - c. Click **Apply**.

SNMP V3

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

CLI: Configure SNMP V3

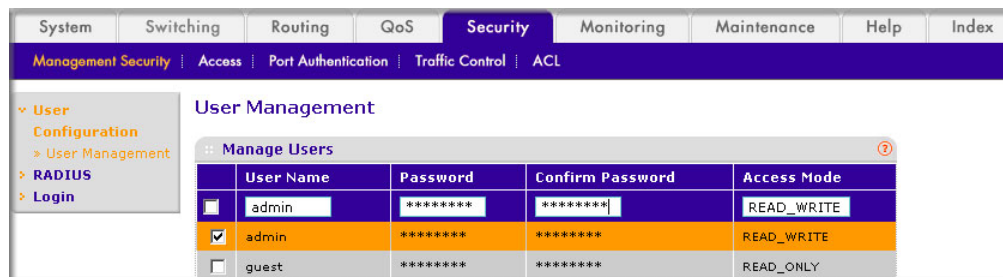
```
(Netgear Switch) #config
(Netgear Switch) (Config)#users passwd admin
Enter old password:
Enter new password:12345678
Confirm new password:12345678
Password Changed!
change the password to "12345678"
(Netgear Switch) (Config)#users snmpv3 authentication admin md5
Set the authentication mode to md5
(Netgear Switch) (Config)#users snmpv3 encryption admin des 12345678
Set the encryption mode to des and the key is "12345678"
```

Web Interface: Configure SNMP V3

1. Change the user password.

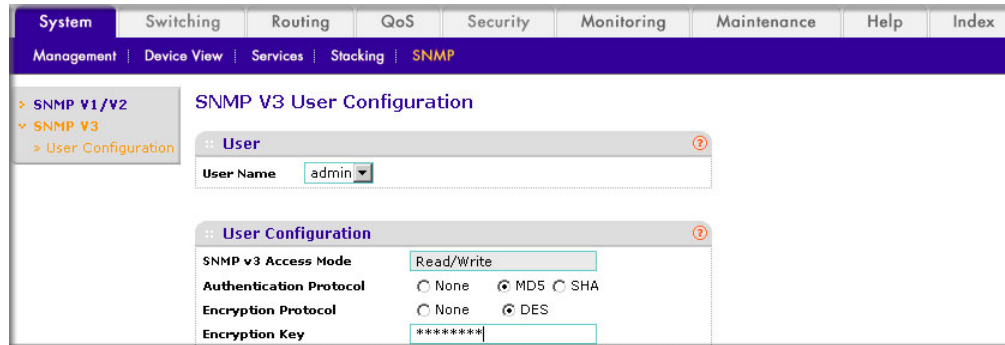
If you set the authentication mode to MD5, you must make the length of password longer than 8 characters.

- a. Select **Security > Management Security > User Configuration > User Management**. A screen similar to the following displays.



- b. Under User Management, scroll down and select the User Name **admin** check box. Now admin appears in the User Name field at the top.
 - c. In the **Password** field, enter **12345678**.
 - d. In the **Confirm Password** field, enter **12345678**.
 - e. Click **Apply** to save the settings.
2. Configure the SNMP V3 user.

- a. Select **System > Management > User Configuration**. A screen similar to the following displays.



The screenshot shows the 'SNMP V3 User Configuration' page in a web browser. The navigation menu at the top includes 'System', 'Switching', 'Routing', 'QoS', 'Security', 'Monitoring', 'Maintenance', 'Help', and 'Index'. Below the menu, there are tabs for 'Management', 'Device View', 'Services', 'Stacking', and 'SNMP'. The left sidebar shows a tree view with 'SNMP v1/v2', 'SNMP v3', and 'User Configuration' expanded. The main content area is titled 'SNMP V3 User Configuration' and contains two sections: 'User' and 'User Configuration'. The 'User' section has a 'User Name' dropdown menu set to 'admin'. The 'User Configuration' section has several fields: 'SNMP v3 Access Mode' set to 'Read/Write', 'Authentication Protocol' with radio buttons for 'None', 'MD5' (selected), and 'SHA', 'Encryption Protocol' with radio buttons for 'None' and 'DES' (selected), and an 'Encryption Key' field containing '*****'.

- b. In the **User Name** field, select the **admin**.
- c. For Authentication Protocol, select the **MD5** radio button.
- d. For Encryption Protocol, select the **DES** radio button.
- e. In the **Encryption Key** field, enter **12345678**.
- f. Click **Apply** to save the settings.

sFlow

sFlow is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

The sFlow monitoring system consists of an sFlow agent (embedded in a switch or router or in a standalone probe) and a central sFlow collector. The sFlow agent uses sampling technology to capture traffic statistics from the device it is monitoring. The sFlow datagrams are used to immediately forward the sampled traffic statistics to an sFlow collector for analysis.

The sFlow agent uses two forms of sampling: statistical packet-based sampling of switched or routed packet flows, and time-based sampling of counters.

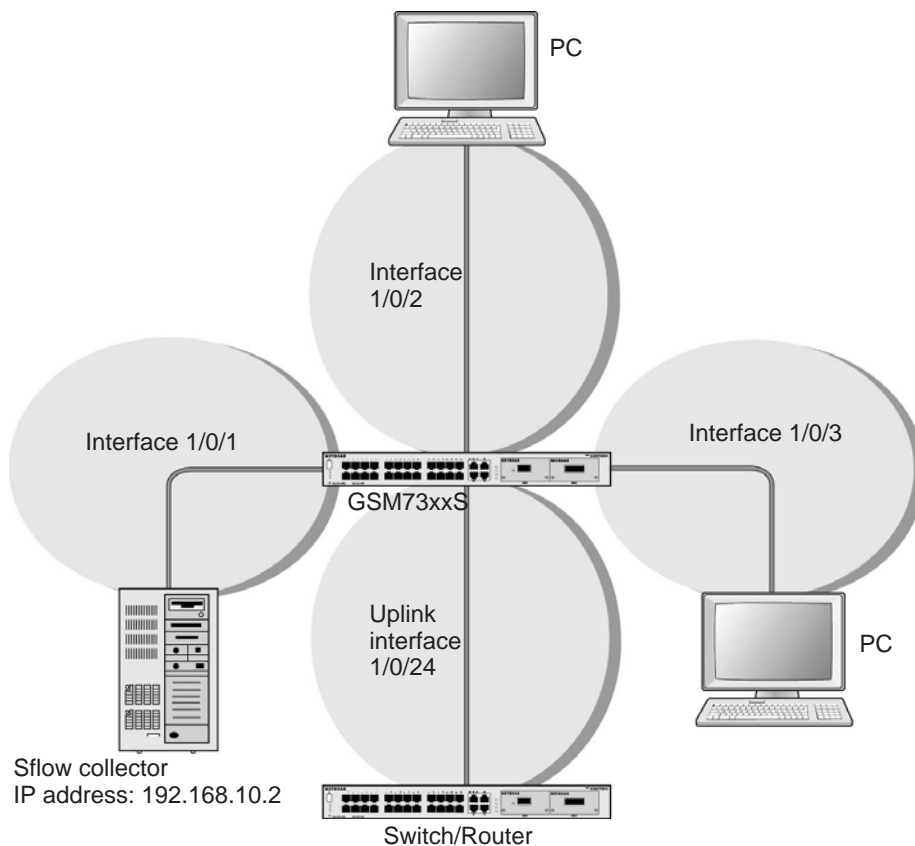


Figure 40. sFlow

CLI: Configure Statistical Packet-Based Sampling of Packet Flows with sFlow

1. Configure the sFlow receiver (sFlow collector) IP address. In this example, sFlow samples will be sent to the destination address 192.168.10.2.

```
(Netgear Switch) (Config)# sflow receiver 1 ip 192.168.10.2
```

2. Configure the sFlow receiver timeout. Here sFlow samples will be sent to this receiver for the duration of 31536000 seconds. That is approximately 1 year.

```
(Netgear Switch) (Config)# sflow receiver 1 owner NetMonitor timeout 31536000
```

3. Here the default maximum datagram size is 1400. It can be modified to a value between 200 and 9116 using the command `sflow receiver 1 maxdatagram <size>`.

```
(GSM7328S) #show sflow receivers
```

Receiver Index	Owner String	Time out	Max Datagram Size	Port	IP Address
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

```
(GSM7328S) #
```

4. Configure the sampling port sFlow receiver index, sampling rate, and sampling maximum header size. You need to repeat these for all the ports to be sampled.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# sflow sampler 1
(Netgear Switch) (Interface 1/0/1)# sflow sampler rate 1024
(Netgear Switch) (Interface 1/0/1)# sflow sampler maxheadersize 64
```

5. View the sampling port configurations.

```
(GSM7328S) #show sflow samplers
```

Sampler Data Source	Receiver Index	Packet Sampling Rate	Max Header Size
1/0/1	1	1024	64

Web Interface: Configure Statistical Packet-based Sampling with sFlow

1. Configure the sFlow receiver IP address.
 - a. Select **Monitoring > sFlow > Advanced > sFlow Receiver Configuration**.
 - b. Select the **1** check box.
 - c. In the **Receiver Owner** field, enter **NetMonitor**.
 - d. In the **Receiver Timeout** field, enter **31536000**.

- e. In the **Receiver Address** field, enter **192.168.10.2**. A screen similar to the following displays.

Receiver Index	Receiver Owner	Receiver Timeout	Maximum Datagram Size	Receiver Address	Receiver Port	Datagram Version
<input type="checkbox"/>	NetMonitor	31536000	1400	192.168.10.2	6343	5
<input checked="" type="checkbox"/>		0	1400	0.0.0.0	6343	5
<input type="checkbox"/>		0	1400	0.0.0.0	6343	5

- f. Click **Apply**. A screen similar to the following displays.

Receiver Index	Receiver Owner	Receiver Timeout	Maximum Datagram Size	Receiver Address	Receiver Port	Datagram Version
<input type="checkbox"/>						
<input type="checkbox"/>	NetMonitor	31535999	1400	192.168.10.2	6343	5
<input type="checkbox"/>		0	1400	0.0.0.0	6343	5

2. Configure the sampling ports sFlow receiver index, sampling rate, and sampling maximum header size.

- a. Select **Monitoring > sFlow > Advanced > sFlow Interface Configuration**. A screen similar to the following displays.

Interface	Poller		Sampler		
	Receiver Index	Poller Interval	Receiver Index	Sampling Rate	Maximum Header Size
<input type="checkbox"/>	0	0	1	1024	64
<input checked="" type="checkbox"/>	0	0	0	0	128
<input type="checkbox"/>	0	0	0	0	128

- b. Select the **Interface 1/0/1** check box.
- c. In the **Sampling Rate** field, enter **1024**.
- d. In the **Maximum Header Size** field, enter **64**.
- e. Click **Apply**. A screen similar to the following displays.

Interface	Poller		Sampler		
	Receiver Index	Poller Interval	Receiver Index	Sampling Rate	Maximum Header Size
<input type="checkbox"/>					
<input type="checkbox"/>	0	0	1	1024	64

Time-Based Sampling of Counters with sFlow

CLI: Configure Time-Based Sampling of Counters with sFlow

1. Configure the sampling port sFlow receiver index, and polling interval. You need to repeat this for all the ports to be polled.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# sflow poller 1
(Netgear Switch) (Interface 1/0/1)# sflow poller interval 300
```

2. View the polling port configurations.

```
(GSM7328S) #show sflow pollers
Poller          Receiver          Poller
Data Source     Index             Interval
-----
1/0/1           1                 300
```

Web Interface: Configure Time-Based Sampling of Counters with sFlow

1. Configure the sampling ports sFlow receiver index, and polling interval.
 - a. Select **Monitoring > sFlow > Advanced > sFlow Interface Configuration**.
 - b. Select the Interface **1/0/1** check box.
 - c. In the **Poller Interval** field, enter **300**. A screen similar to the following displays.

Interface	Poller			Sampler	
	Receiver Index	Poller Interval	Receiver Index	Sampling Rate	Maximum Header Size
<input checked="" type="checkbox"/> 1/0/1	1	300	1	1024	64
<input type="checkbox"/> 1/0/2	0	0	0	0	128

- d. Click **Apply**.

Domain Name System

This chapter provides the following examples:

- *Specify Two DNS Servers*
- *Manually Add a Host Name and an IP Address* on page 371

This section describes the Domain Name System (DNS) feature. The DNS protocol maps a host name to an IP address, allowing you to replace the IP address with the host name for IP commands such as a ping and a traceroute, and for features such as RADIUS, DHCP relay, SNTP, SNMP, TFTP, SYSLOG, and UDP relay.

You can obtain the DNS server IP address from your ISP or public DNS server list. DNS is used to resolve the host's IP address. It enables a static host name entry to be used to resolve the IP address. The following are examples of how the DNS feature is used.

Specify Two DNS Servers

The following example shows how to specify two DNS servers (that is, two IP addresses for DNS servers) and to resolve an IP address using the DNS server. The example is shown as CLI commands and as a Web interface procedure.

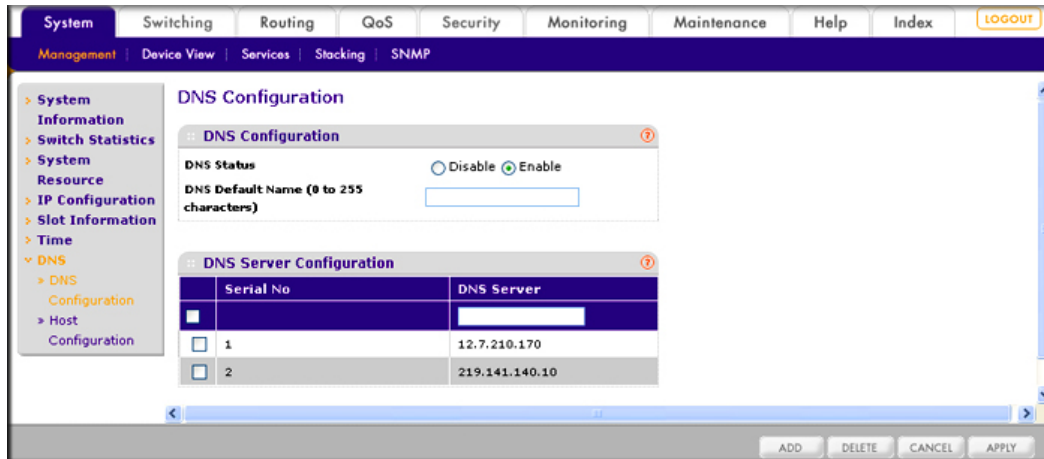
CLI: Specify Two DNS Servers

```
(Netgear Switch)#config
(Netgear Switch) (Config)#ip name-server 12.7.210.170 219.141.140.10
(Netgear Switch) (Config)#ip domain-lookup
(Netgear Switch) (Config)#exit
(Netgear Switch)#ping www.netgear.com

Send count=3, Receive count=3 from 206.82.202.46
```

Web Interface: Specify Two DNS Servers

1. Select **System > Management > DNS > DNS Configuration**. A screen similar to the following displays.



2. Under DNS Server Configuration, in the **DNS Server** field, enter **12.7.210.170**.
3. Click **Add**.
4. In the **DNS Server** field, enter **219.141.140.10**.
5. Click **Add**.

Both DNS servers now show in the DNS Server Configuration table.

Manually Add a Host Name and an IP Address

The following example shows commands to add a static host name entry to the switch so that you can use this entry to resolve the IP address. The example is shown as CLI commands and as a Web interface procedure.

CLI: Manually Add a Host Name and an IP Address

```
(Netgear Switch)#config
(Netgear Switch) (Config)#ip host www.netgear.com 206.82.202.46
(Netgear Switch) (Config)#ip domain-lookup
(Netgear Switch) (Config)#ping www.netgear.com

Send count=3, Receive count=3 from 206.82.202.46
```

Web Interface: Manually Add a Host Name and an IP Address

1. Select **System > Management > DNS > Host Configuration**. A screen similar to the following displays.

The screenshot shows the 'DNS Host Configuration' page in a web interface. The top navigation bar includes 'System', 'Switching', 'Routing', 'QoS', 'Security', 'Monitoring', and 'Maintenance'. Below this is a secondary bar with 'Management', 'Device View', 'Services', 'Stacking', and 'SNMP'. The left sidebar has a tree view with 'System' expanded to 'DNS Configuration'. The main content area has a title 'DNS Host Configuration' and a table with two columns: 'Host Name (1-158 characters)' and 'IP Address'. The table contains one entry: 'www.netgear.com' and '206.82.202.46'. Below this is a 'Dynamic Host Mapping' section with a table with columns: 'Host', 'Total', 'Elapsed', 'Type', and 'Addresses'.

2. Under DNS Host Configuration, enter the following information:
 - In the **Host Name** field, enter **www.netgear.com**.
 - In the **IP Address** field, enter **206.82.202.46**.
3. Click **Add**.

The host name and IP address now show in the DNS Host Configuration table.

This chapter provides the following examples:

- *Figure* on page 373
- *Configure a DHCP Reservation* on page 376

When a client sends a request to a DHCP server, the DHCP server assigns the IP address from address pools that are specified on the switch. The network in the DHCP pool must belong to the same subnet.

DHCP server allows the switch to dynamically assign an IP address to a DHCP client that is attached to the switch. It also enables the IP address to be assigned based on the client's MAC address. The following are examples of how the DHCP Server feature is used.

Configure a DHCP Server in Dynamic Mode

The following example shows how to create a DHCP server with a dynamic pool. The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure a DHCP Server in Dynamic Mode

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#vlan routing 200
(Netgear Switch) (Vlan)#exit
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#vlan participation include 200
(Netgear Switch) (Interface 1/0/1)#vlan pvid 200
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface vlan 200
(Netgear Switch) (Interface-vlan 200)#routing
(Netgear Switch) (Interface-vlan 200)#ip address 192.168.100.1 255.255.255.0
(Netgear Switch) #config
(Netgear Switch) (Config)#service dhcp
(Netgear Switch) (Config)#ip dhcp pool pool_dynamic
(Netgear Switch) (Config)#network 192.168.100.0 255.255.255.0
```

Note: If there is no DHCP L3 relay between client PC and DHCP server, there must be an active route whose subnet is the same as the DHCP dynamic pool's subnet.

Web Interface: Configure a DHCP Server in Dynamic Mode

1. Create VLAN 200.
 - a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays.

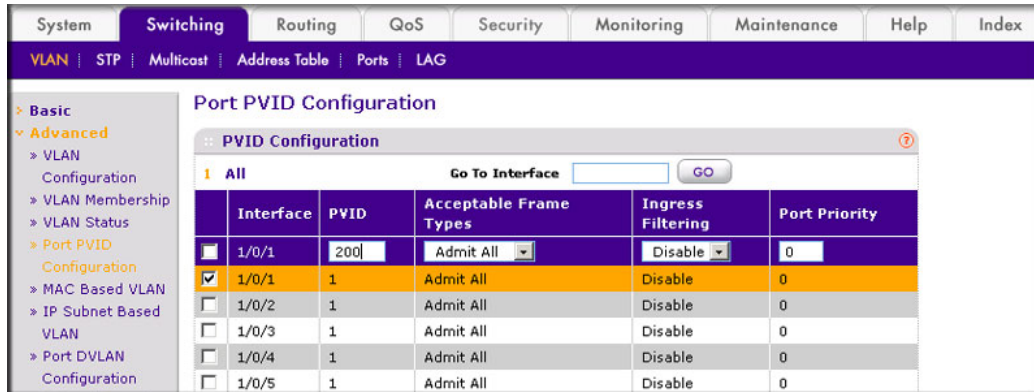
VLAN ID	VLAN Name	VLAN Type	Make Static
200			Disable
1	Default	Default	Disable

- b. Under VLAN Configuration, in the **VLAN ID** field, enter **200**.
 - c. Click **Add**.
2. Add port 1/0/1 to VLAN 200.
 - a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays.

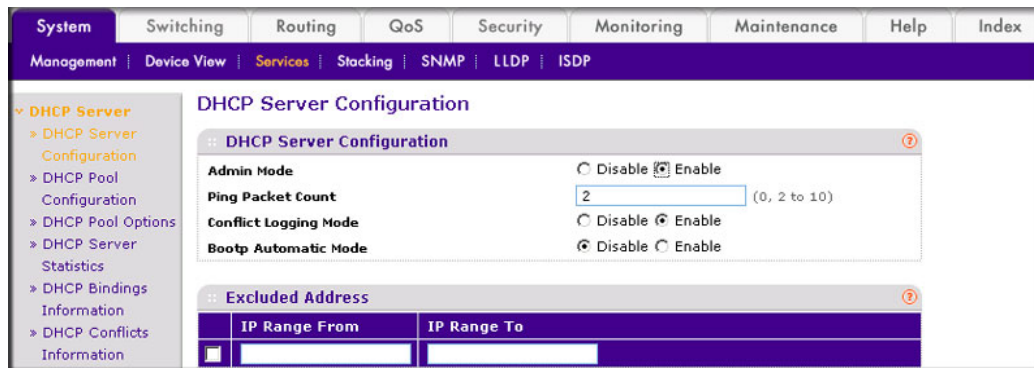
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	U																							
	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
	49	50	51	52																				

- b. In the **VLAN ID** field, select **200**.
 - c. Click **Unit 1**. The ports display.

- d. Click the gray boxes under ports **1** and **24** until **U** displays. The U specifies that the egress packet is untagged for the port.
 - e. Click **Apply**.
3. Assign PVID to the VLAN 200.
- a. Select **Switching > VLAN > Advanced > Port PVID Configuration**. A screen similar to the following displays.



- b. Under Port PVID Configuration, scroll down and select the **1/0/1** check box.
 - c. In the **PVID (1 to 4093)** field, enter **200**.
 - d. Click **Apply** to save the settings.
4. Create a new DHCP pool.
- a. Select **System > Services > DHCP Server > DHCP Server Configuration**. A screen similar to the following displays.



- b. For Admin Mode, select the **Enable** radio button.
- c. Click **Apply** to enable the DHCP service.

- d. Select **System > Services > DHCP Server > DHCP Pool Configuration**. A screen similar to the following displays.

- e. Under DHCP Pool Configuration, enter the following information:
- In the **Pool Name** list, select **Create**.
 - In the **Pool Name** field, enter **pool_dynamic**.
 - In the **Type of Binding** list, select **Dynamic**.
 - In the **Network Number** field, enter **192.168.100.0**.
 - In the **Network Mask** field, enter **255.255.255.0**. As an alternate, you can enter **24** in the **Network Prefix Length** field. Do not fill in both the Network Mask field and Network Prefix Length fields.
 - In the **Days** field, enter **1**.
- f. Click **Add**.

The pool_dynamic name is now added to the Pool Name drop-down list.

Configure a DHCP Reservation

The following example shows how to create a DHCP server with an IP address pool that is makes fixed IP to MAC address assignments. The example is shown as CLI commands and as a Web interface procedure.

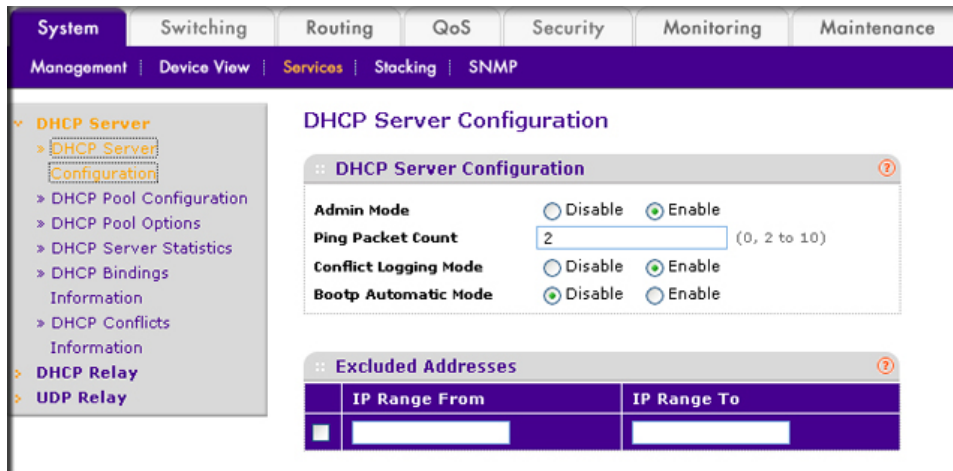
CLI: Configure a DHCP Reservation

```
(Netgear Switch)#config
(Netgear Switch) (Config)#service dhcp
(Netgear Switch) (Config)#ip dhcp pool pool_manual
(Netgear Switch) (Config)#client-name dhcpcplint
(Netgear Switch) (Config)#hardware-address 00:01:02:03:04:05
(Netgear Switch) (Config)#host 192.168.200.1 255.255.255.0
(Netgear Switch) (Config)#client-identifier 01:00:01:02:03:04:05
```

Note: The unique identifier is a concatenation of the media type and MAC addresses. For example, the Microsoft client identifier for Ethernet address c8:19:24:88:f1:77 is 01:c8:19:24:88:f1:77, where 01 represents the Ethernet media type. For more information, see the “Address Resolution Protocol Parameters” section of RFC 1700.

Web Interface: Configure a DHCP Reservation

1. Select **System > Services > DHCP Server > DHCP Server Configuration**. A screen similar to the following displays.



2. For Admin Mode, select the **Enable** radio button.
3. Click **Apply** to enable the DHCP service.

4. Select **System > Services > DHCP Server > DHCP Pool Configuration**. A screen similar to the following displays.

5. Under DHCP Pool Configuration, enter the following information:
- In the **Pool Name** list, select **Create**.
 - In the **Pool Name** field, enter **pool_manual**.
 - In the **Type of Binding** list, select **Manual**.
 - In the **Client Name** field, enter **dhcpclient**.
 - In the **Hardware Address** field, enter **00:01:02:03:04:05**.
 - In the **Hardware Type** list, select **ethernet**.
 - In the **Host Number** field, enter **192.168.200.1**.
 - In the **Network Mask** field, enter **255.255.255.0**. As an alternate, you can enter **24** in the **Network Prefix Length** field.
 - In the **Days** field, enter **1**.
6. Click **Add**. The pool_manual name is now added to the Pool Name drop-down list.

This chapter provides the following examples:

- *CLI: Configure DHCPv6* on page 381
- *Web Interface: Configure an Inter-area Router* on page 382
- *Configure Stateless DHCPv6 Server* on page 386

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is used to assign IPv6 addresses statefully and distribute other configuration information such as domain name or DNS server.

Although DHCPv6 supports stateful address allocation, prefix delegation and stateless services, only prefix delegation mode and stateless service are supported on managed switches. This chapter shows how to configure prefix delegation mode using DHCPv6 pool. When create a DHCPv6 pool, user needs to assign a prefix to client 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:

- a. Link-layer address plus time:**
 - 00:01:hardware type:time:link-layer address
 - Hardware type - 16 bit hardware type reserved by IANA. 1 means an Ethernet device.
 - Time: 32-bit unsigned integer. The time in seconds when this DUID was generated since 00:00:00 1/1/2000.
 - Link-layer address - The link layer address of a device generating the DUID.
- b. 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
- c. Link-layer address:**
 - 00:03:hardware type:link-layer address
 - Hardware type - 16 bit hardware type reserved by IANA. 1 means an Ethernet device.
 - Link-layer address - The link layer address of a device generating the DUID.

In the following case, the CPE router requests prefix from the PE router. The PE router chooses prefix (2001:1::/64) for delegation, and responds with the prefix to the requesting CPE router. The CPE router subnets the prefix and assigns the longer prefixes to links in the user's network. The CPE router is then responsible to assign the 2001:1:1::/96 to one user's network and 2001:1:2::/96 to another user's network.

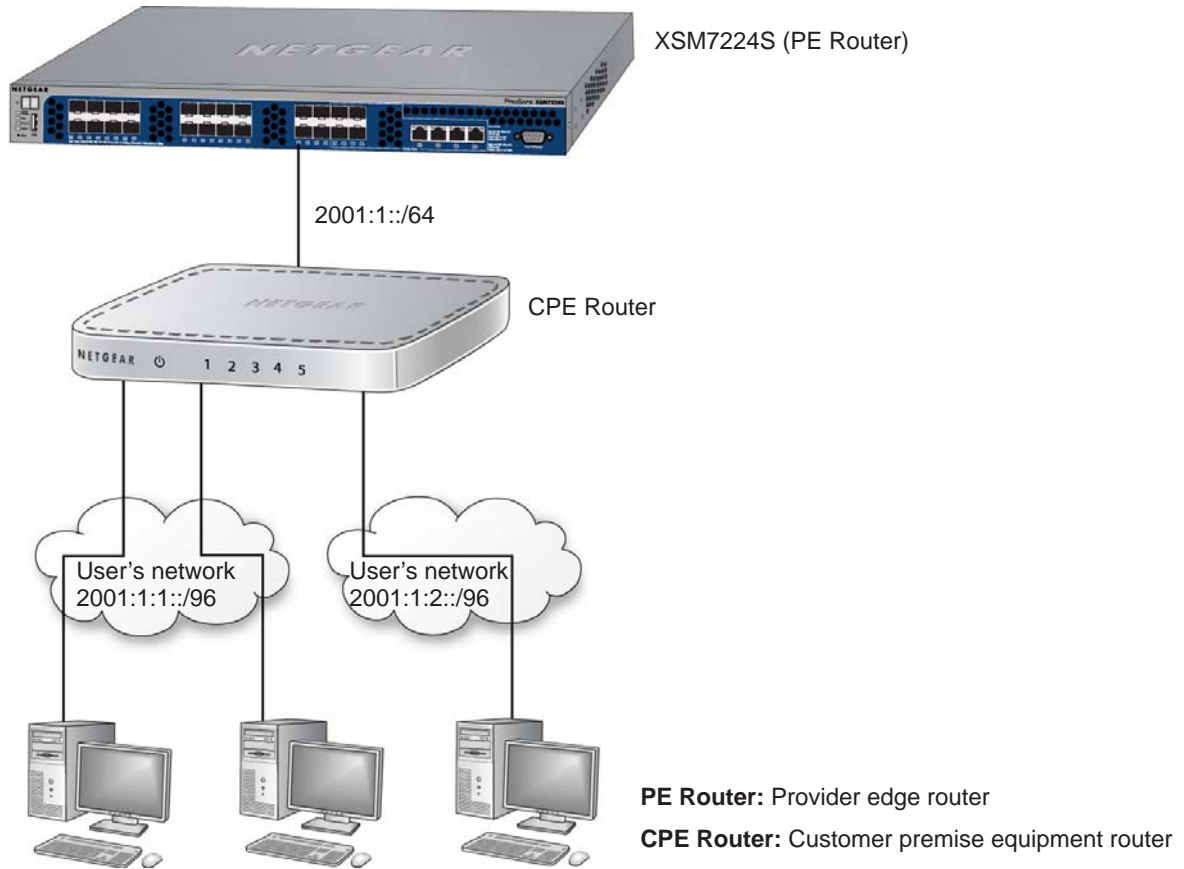


Figure 41. DHCPv6 stateful IPv6 address assignment

CLI: Configure DHCPv6

1. Enable IPv6 routing.

```
(Netgear Switch) #configure
(NETGEAR SWITCH) (Config)#ip routing
(NETGEAR SWITCH) (Config)#ipv6 unicast routing
```

2. Create a DHCPv6 pool and enable DHCP service.

```
(NETGEAR SWITCH) (Config)#service dhcpv6
(NETGEAR SWITCH) (Config)#ipv6 dhcp pool pool1
(NETGEAR SWITCH) (Config dhcp6 pool)#domain name netgear.com
(NETGEAR SWITCH) (Config dhcp6s pool)#prefix delegation 2001:1::/64
00:01:00:01:15:40:14:4f:00:00:00:4d:aa:d0
(NETGEAR SWITCH) (Config dhcp6s pool)#exit
```

3. Enable DHCPv6 service on port 1/0/9.

```
(NETGEAR SWITCH) (Config)#interface 1/0/9
(NETGEAR SWITCH) (Interface 1/0/9)#routing
(NETGEAR SWITCH) (Interface 1/0/9)#ipv6 address 2001:1::1/64
(NETGEAR SWITCH) (Interface 1/0/9)#ipv6 enable
(NETGEAR SWITCH) (Interface 1/0/9)#ipv6 dhcp server pool1 preference 20
(NETGEAR SWITCH) (Interface 1/0/9)#exit
```

4. Show DHCPv6 binding.

```
(NETGEAR SWITCH) #show ipv6 dhcp binding
Client Address..... FE80::200:FF:FE4D:AAD0
Client Interface..... 1/0/9
Client DUID.....
00:01:00:01:15:40:14:4f:00:00:00:4d:aa:d0
Identity Association ID..... 5090000
Binding Prefix Address/Length..... 2001:1::/64
Binding Prefix Type ..... IA_PD
Binding Expiration (secs)..... 4294967284
Binding Prefix Valid Lifetime (secs)..... infinite
Binding Prefix Preferred Lifetime (secs)..... infinit
```

Web Interface: Configure an Inter-area Router

1. Enable IP routing globally
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.

The screenshot shows the 'IP Configuration' page in the web interface. The navigation menu includes System, Switching, Routing (selected), QoS, Security, Monitoring, Maintenance, and Help. Under Routing, there are sub-menus for Routing Table, IP, IPv6, VLAN, ARP, RIP, OSPF, OSPFv3, Router Discovery, VRRP, Multicast, and IPv6 Multicast. The left sidebar shows a tree view with Basic, IP, Configuration, Statistics, and Advanced. The main content area is titled 'IP Configuration' and contains the following settings:

Default Time to Live	64
Routing Mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
ICMP Echo Replies	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ICMP Redirects	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
ICMP Rate Limit Interval	<input type="text" value="1000"/> (0 to 2147483647 ms)
ICMP Rate Limit Burst Size	<input type="text" value="100"/> (1 to 200)
Maximum Next Hops	4
Maximum Routes	6112
Select to configure Global Default Gateway	<input type="checkbox"/>
Global Default Gateway	<input type="text" value="0.0.0.0"/>

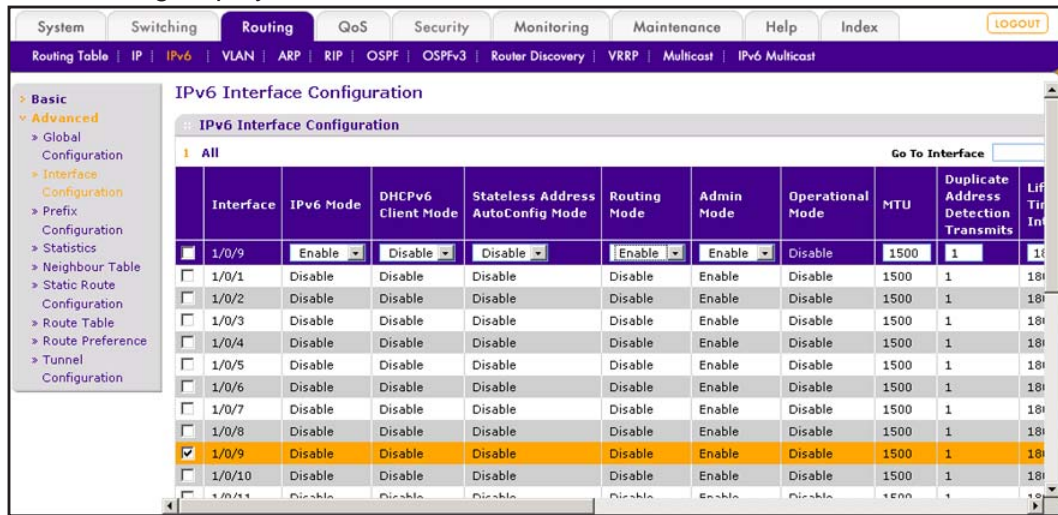
- b. For Routing Mode, select the **Enable** radio button.
 - c. Click **Apply** to apply the settings.
2. Enable IPv6 unicast globally
 - a. Select **Routing > IPv6 > Basic > Global Configuration**. A screen similar to the following displays.

The screenshot shows the 'IPv6 Global Configuration' page in the web interface. The navigation menu is the same as in the previous screenshot. Under Routing, the sub-menu 'IPv6' is selected. The left sidebar shows a tree view with Basic, Global, Configuration, Route Table, and Advanced. The main content area is titled 'IPv6 Global Configuration' and contains the following settings:

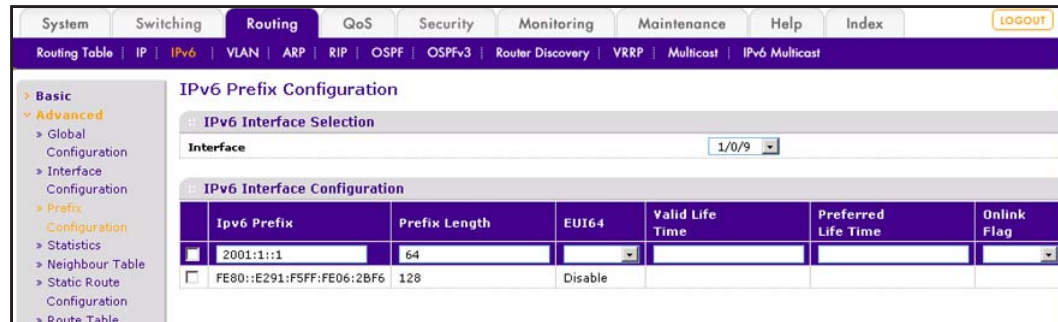
IPv6 Unicast Routing	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IPv6 Forwarding	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Hop Limit	<input type="text" value="0"/> (0 to 255)
ICMPv6 Rate Limit Error Interval	<input type="text" value="1000"/> (0 to 2147483647 msecs)
ICMPv6 Rate Limit Burst Size	<input type="text" value="100"/> (1 to 200)

- b. For IPv6 Unicast Routing, select the **Enable** radio button.
 - c. Click **Apply** to apply the setting.
3. Enable IPv6 address on interface 1/0/9.

- a. Select **Routing > IPv6 > Advanced > Interface Configuration**. A screen similar to the following displays.

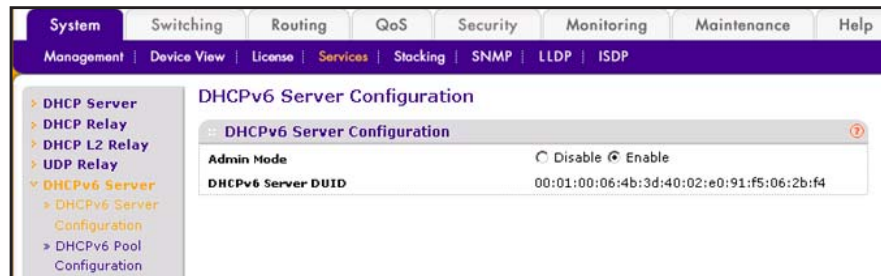


- b. Scroll down and select the interface **1/0/9** check box. Now 1/0/9 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the IPv6 Mode field, select **Enable**.
 - In the Routing Mode field, select **Enable**.
 - d. Click **Apply** to apply the settings.
4. Configure prefix on interface 1/0/9.
 - a. Select **Routing > IPv6 > Advanced > Prefix Configuration**. A screen similar to the following displays.

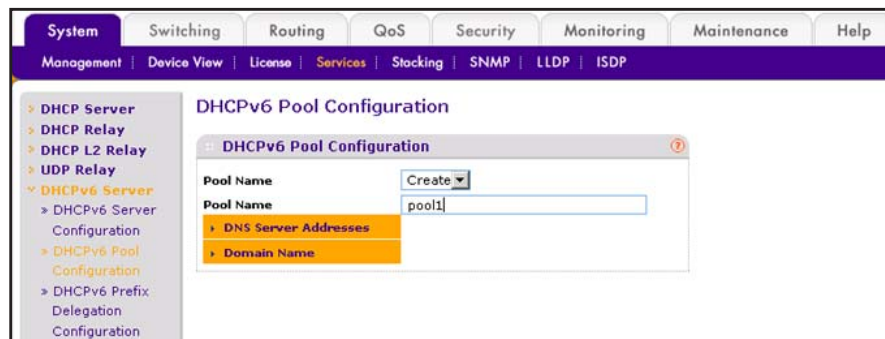


- b. Scroll down and select interface **1/0/9**.
 - c. Enter the following information:
 - In the IPv6 Prefix field, enter **2001::1::1**.
 - In the Prefix Length field, select **64**.
 - d. Click **Add** to create IPv6 prefix to interface 1/0/9.
5. Enable DHCPv6 Server Configuration

- a. Select **System > Services > DHCPv6 Server > DHCPv6 Server Configuration**. A screen similar to the following displays.



- b. For Admin Mode, Select the **Enable** radio button.
 - c. Click **Apply** to apply the setting.
6. Create a DHCPv6 pool named pool1.
 - a. Select **System > Services > DHCP Server > DHCPv6 Pool Configuration**. A screen similar to the following displays.

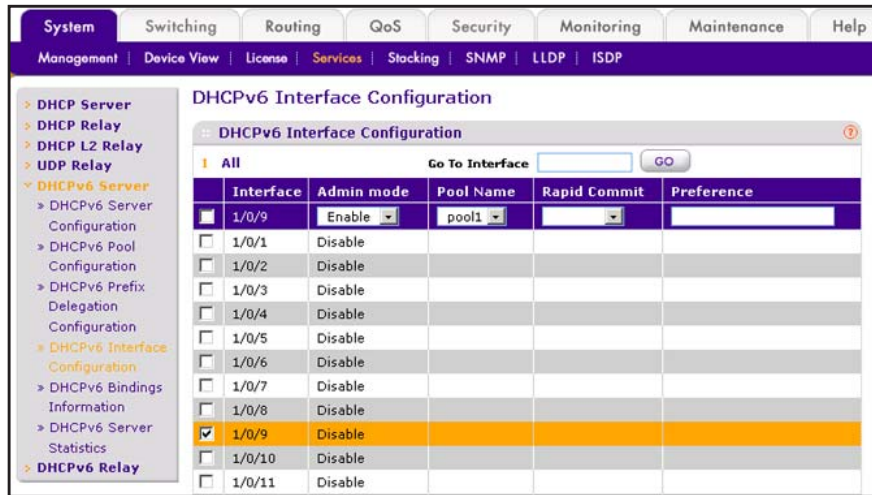


- b. From the Pool Name drop-down list, select **Create**.
 - c. In the Pool Name field, enter **pool1**.
 - d. Click **Apply** to apply the setting.
7. Configure prefix in the pool1
 - a. Select **System > Services > DHCPv6 Server > DHCPv6 Pool Configuration**. A screen similar to the following displays.



- b. From the Pool Name drop-down list, select **Pool1**.

- c. Enter **2001:1::** in the Prefix field.
 - d. in the Prefix Length field, enter **64**.
 - e. In the Prefix field, enter **00:01:00:01:15:40:14:4f:00:00:00:4d:aa:d0**.
 - f. Click **Apply** to apply the setting.
8. Configure DHCPv6 on interface 1/0/9.
- a. Select **System > Services > DHCPv6 Server > DHCPv6 Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the interface **1/0/9** check box. Now 1/0/9 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the Admin mode field, select **Enable**.
 - In the Pool Name field, enter **pool1**.
 - In the Administrative Mode field, select **Enable**.
 - d. Click **Apply** to apply the settings.
9. Show DHCPv6 binding.

- a. Select **System > Services > DHCPv6 Server > DHCPv6 Binding Information**. A screen similar to the following displays.

The screenshot shows the web interface for DHCPv6 Bindings Information. The navigation menu on the left includes: System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, Index, and a LOGOUT button. Below the navigation menu are tabs for Management, Device View, License, Services, Stacking, SNMP, LLDP, and ISDP. The main content area is titled 'DHCPv6 Bindings Information' and features a search bar labeled 'Search By Binding IP' with a 'GO' button. Below the search bar is a table with the following columns: Client Address, Client Interface, Client DUID, Prefix, Prefix Length, Prefix Type, Expiry Time, and Valid Lifetime. The table contains one entry:

Client Address	Client Interface	Client DUID	Prefix	Prefix Length	Prefix Type	Expiry Time	Valid Lifetime
FE80::200:FF:FE4D:AAD0	1/0/9	00:01:00:01:15:40:14:4f:00:00:00:4d:aa:d0	2001:1::	64	IA_PD	4294908066	4294967295

Configure Stateless DHCPv6 Server

This example uses the DHCPv6 server to configure the information about DNS server to those clients which get IPv6 in autoconfig mode or manual mode. The configured DHCP pool doesn't contain a prefix pool but contains DNS server to be passed to clients. The IPv6 interface must have the 'ipv6 nd other-config-flag' command enabled.

CLI: Configure Stateless DNS Server

This example shows how to configure a DNS server to clients with stateless IPv6 address using DHCPv6 server.

1. Enable ipv6 routing.

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

2. Create an IPv6 pool with DNS server and enable 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 IPv6 DHCP server on interface 2/0/21.

Note: In this case, you have to configure the command `ipv6 nd other-config-flag` on the interface, otherwise, the host cannot update the DNS with it.

```
(Netgear Switch) (Config)#interface 2/0/21
(Netgear Switch) (Interface 2/0/21)#routing
(Netgear Switch) (Interface 2/0/21)#ipv6 address 2003:1000::1/64
(Netgear Switch) (Interface 2/0/21)#ipv6 enable
(Netgear Switch) (Interface 2/0/21)#ipv6 nd other-config-flag
(Netgear Switch) (Interface 2/0/21)#ipv6 dhcp server ipv6_server
(Netgear Switch) (Interface 2/0/21)#exit
```

Web Interface: Configure Stateless DHCPv6 Server

1. Enable ipv6 routing.

- a. Select **Routing > IPv6 > Basic > Global Configuration**. A screen similar to the following displays:

The screenshot shows the 'IPv6 Global Configuration' page. The 'IPv6 Unicast Routing' section has a radio button for 'Enable' selected. Other settings include 'Hop Limit' set to 0, 'ICMPv6 Rate Limit Error Interval' set to 1000, and 'ICMPv6 Rate Limit Burst Size' set to 100.

- b. For IPv6 Unicast Routing, select the **Enable** radio button.

- c. Click **Apply**.

2. Enable ipv6 routing on the interface 2/0/21.

- a. Select **Routing > IPv6 > Advanced > Interface Configuration**. A screen similar to the following displays:

The screenshot shows the 'IPv6 Interface Configuration' page with a table of interface settings. The '2/0/21' interface is selected and highlighted.

Interface	IPv6 Mode	DHCPv6 Client Mode	Stateless Address AutoConfig Mode	Routing Mode	Admin Mode	Operational Mode	MTU	Duplicate Address Detection Transmits	Life Time Interval	Adv NS Interval
<input checked="" type="checkbox"/> 2/0/21	Enable	Disable	Disable	Enable	Enable	Disable	1500	1	1800	0
<input type="checkbox"/> 2/0/1	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
<input type="checkbox"/> 2/0/2	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
<input type="checkbox"/> 2/0/3	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0

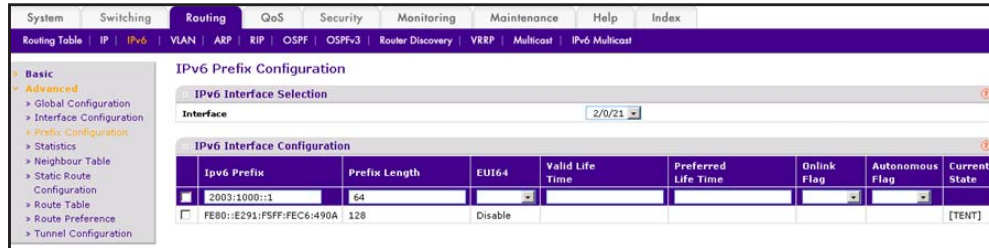
- b. Under IPv6 Interface Configuration, scroll down and select the Interface **2/0/21** check box. Now 2/0/21 appears in the Interface field at the top.

- c. In the IPv6 Mode field, select **Enable**.

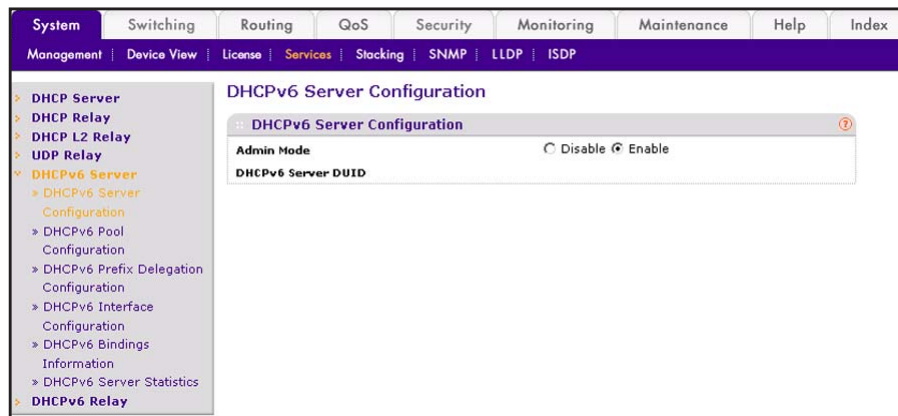
- d. In the Routing Mode field, select **Enable**.

- e. In the Adv Other Config Flag field, select **Enable**.

- f. Click **Apply** to save the settings.
3. Configure IPv6 address on the interface 2/0/21.
 - a. Select **Routing > IPv6 > Advanced > Prefix Configuration**. A screen similar to the following displays:



- b. In the Interface list, select **1/0/21**.
- c. In the IPv6 Prefix field, enter **2003:1000::1**.
- d. In the Length field, enter **64**.
- e. In the EUI64 field, select **Disable**.
- f. Click **Add**.
4. Enable DHCPv6 service.
 - a. Select **System > Services > DHCPv6 Server > DHCPv6 Server Configuration**. A screen similar to the following displays:



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

5. Create DHCPv6 pool.
 - a. Select **System > Services > DHCP Server > DHCPv6 Pool Configuration**. A screen similar to the following displays:

- b. From the Pool Name drop-down list, select **Create**.
 - c. In the Pool Name field, enter **ipv6_server**.
 - d. In the DNS Server Addresses fields, enter **2011:9:18::1** (the DNS server IPv6 address).
 - e. Click **Apply**.
6. Enable DHCPv6 pool on the interface 2/0/21.
 - a. Select **System > Services > DHCPv6 Server > DHCPv6 Interface Configuration**. A screen similar to the following displays:

Interface	Admin mode	Pool Name	Rapid Commit	Preference
<input checked="" type="checkbox"/> 2/0/21	Enable	ipv6_server	Disable	20
<input type="checkbox"/> 2/0/1	Disable			
<input type="checkbox"/> 2/0/2	Disable			
<input type="checkbox"/> 2/0/3	Disable			
<input type="checkbox"/> 2/0/4	Disable			
<input type="checkbox"/> 2/0/5	Disable			
<input type="checkbox"/> 2/0/6	Disable			
<input type="checkbox"/> 2/0/7	Disable			
<input type="checkbox"/> 2/0/8	Disable			
<input type="checkbox"/> 2/0/9	Disable			

- b. Scroll down and select the interface **2/0/21** check box. Now 2/0/21 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the Admin mode field, select **Enable**.
 - In the Pool Name field, enter **ipv6_server**.
 - d. Click **Apply**.

24 Double VLANs and Private VLAN Groups

24

This chapter includes the following examples:

- *Double VLANs*
- *Private VLAN Groups* on page 394

Double VLANs

This section describes how to enable the double DVLAN feature. Double VLANs pass traffic from one customer domain to another through the metro core. Custom VLAN IDs are preserved and a provider service VLAN ID is added to the traffic so the traffic can pass the metro core in a simple and cost-effective manner. You can use VLANs to specify customer ports and a service provider port. In this example, the switches have the same configuration.

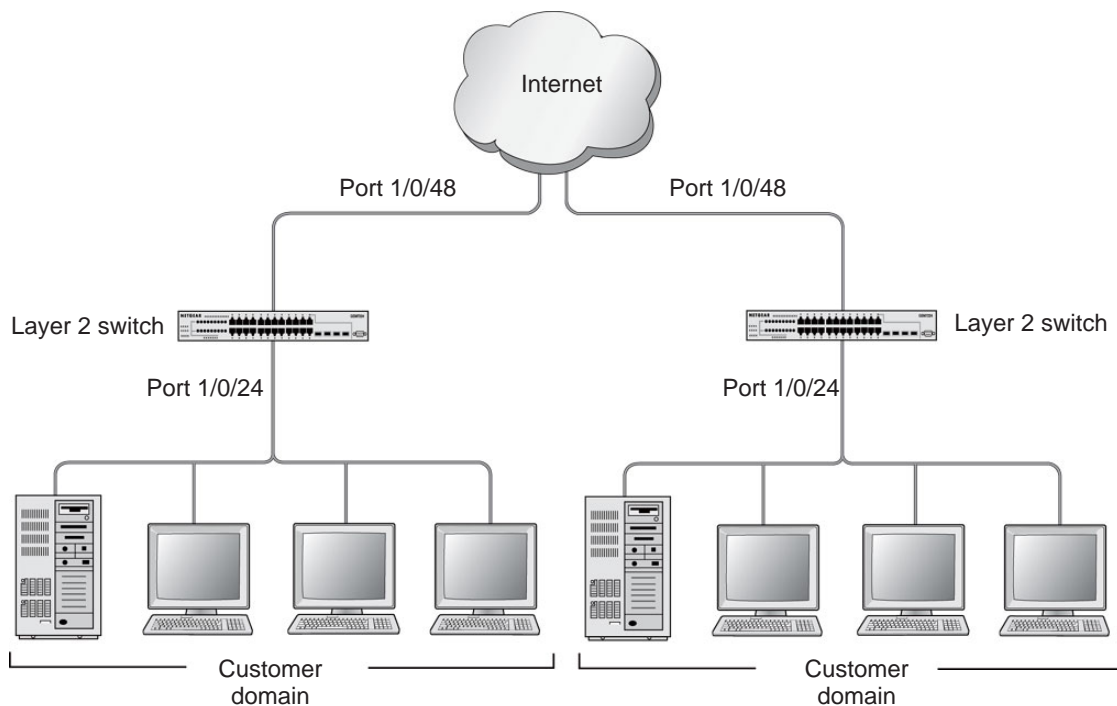


Figure 42. Double VLANS

The following example shows how to configure the NETGEAR switch shown in the preceding figure to add a double VLAN tag for traffic going from the subnet domain connected to port 1/0/24. This example assumes there is a Layer 2 switch connecting all these devices in your domain. The Layer 2 switch tags the packet going to the NETGEAR switch port 1/0/24. The example is shown as CLI commands and as a Web interface procedure.

CLI: Enable a Double VLAN

```
Create a VLAN 200.
(Netgear Switch)#vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#exit

Add interface 1/0/24 to VLAN 200, add pvid 200 to port.
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan pvid 200
(Netgear Switch) (Interface 1/0/24)#vlan participation include 200
(Netgear Switch) (Interface 1/0/24)#exit

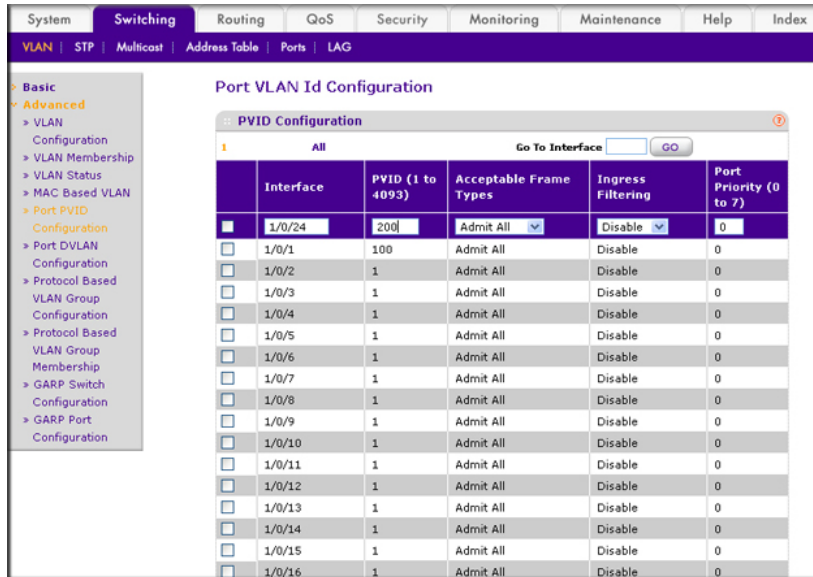
Add interface 1/0/48 to the VLAN 200 in a tagging mode.
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan participation include 200
(Netgear Switch) (Interface 1/0/48)#vlan tagging 200
(Netgear Switch) (Interface 1/0/48)#exit

Select interface 1/0/48 as the provider port.
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#mode dvlan-tunnel
(Netgear Switch) (Interface 1/0/48)#exit
```

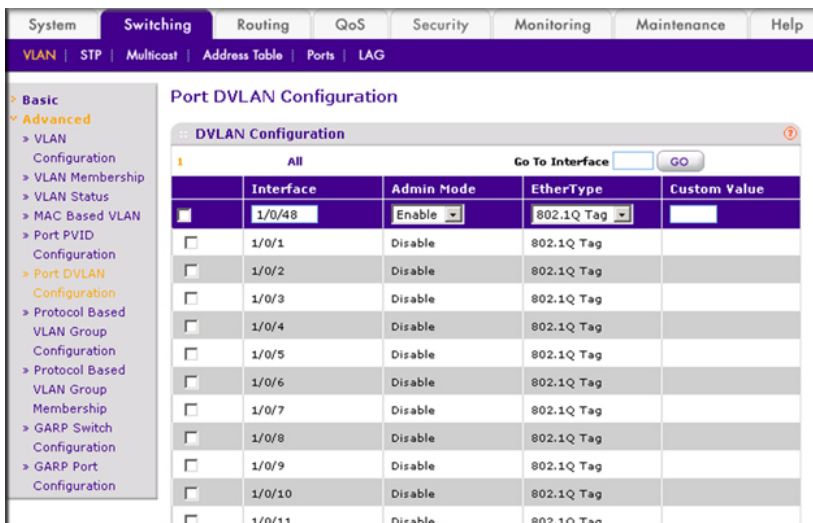
Web Interface: Enable a Double VLAN

1. Create static VLAN 200:

- Click the gray box under port **48** once until **T** displays. The T specifies that the egress packet is tagged for the port.
 - d. Click **Apply** to save the settings.
3. Change the port VLAN ID (PVID) of port 24 to 200:
- a. Select **Switching > VLAN > Advanced > Port PVID Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Interface **1/0/24** check box. Now 1/0/24 appears in the Interface field at the top.
 - c. In the **PVID (1 to 4093)** field, enter **200**.
 - d. Click **Apply** to save the settings.
4. Configure port 48 as the provider service port:
- a. Select **Switching > VLAN > Advanced > Port DVLAN Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Interface **1/0/48** check box. Now 1/0/48 appears in the Interface field at the top.
- c. In the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.

Private VLAN Groups

The private VLAN group allows you to create groups of users within a VLAN that cannot communicate with members in different groups but only within the same group. There are two modes for the private group. The mode can be either isolated or community. When in isolated mode, the member port in the group cannot forward its egress traffic to any other members in the same group. The default mode is community, in which each member port can forward traffic to other members in the same group, but not to members in other groups. The following examples show how to create a private group.

The following example creates two groups. Group 1 is in community mode, and Group 2 is in isolated mode.

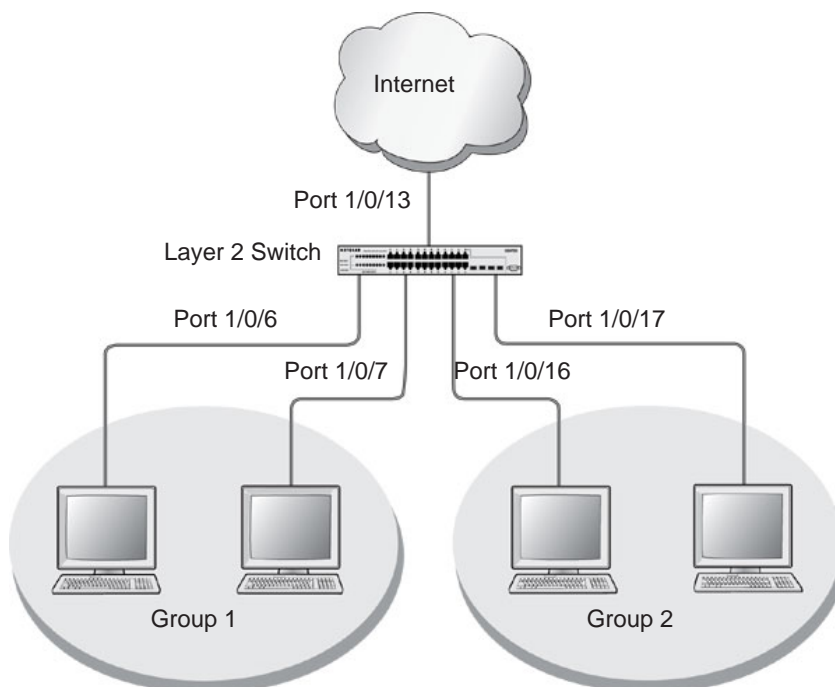


Figure 43. Private VLAN groups in community mode and isolated mode

CLI: Create a Private VLAN Group

1. Enter the following commands.

```
(Netgear Switch) #
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#exit

(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)#vlan participation include 200
(Netgear Switch) (Interface 1/0/6)#vlan pvid 200
(Netgear Switch) (Interface 1/0/6)#exit

(Netgear Switch) (Config)#interface 1/0/7
(Netgear Switch) (Interface 1/0/7)#vlan participation include 200
(Netgear Switch) (Interface 1/0/7)#vlan pvid 200
(Netgear Switch) (Interface 1/0/7)#exit
(Netgear Switch) (Config)#interface 1/0/16
(Netgear Switch) (Interface 1/0/16)#vlan participation include 200
(Netgear Switch) (Interface 1/0/16)#vlan participation pvid 200
(Netgear Switch) (Interface 1/0/16)#exit

(Netgear Switch) (Config)#interface 1/0/17
(Netgear Switch) (Interface 1/0/17)#vlan participation include 200
(Netgear Switch) (Interface 1/0/17)#vlan pvid 200
(Netgear Switch) (Interface 1/0/17)#exit
```

2. Create a VLAN 200 and include 1/0/6,1/0/7, 1/0/16, and 1/0/17.

```
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#private-group name group1 1 mode community
```

3. Create a private group in community mode.

```
(Netgear Switch) (Config)#private-group name group2 2 mode isolated
```

4. Create a private group in isolated mode.

```
(Netgear Switch) (Config)#interface range 1/0/6-1/0/7
(Netgear Switch) (conf-if-range-1/0/6-1/0/7)#switchport private-group 1
(Netgear Switch) (conf-if-range-1/0/6-1/0/7)#exit
```

5. Add 1/0/16 and 1/0/7 to the private group 1.

```
(Netgear Switch) (Config)#interface range 1/0/16-1/0/17
(Netgear Switch) (conf-if-range-1/0/16-1/0/17)#switchport private-group 2
```

6. Add 1/0/16 and 1/0/7 to the private group 2.

```
(Netgear Switch) (conf-if-range-1/0/16-1/0/17)#exit
```

Web Interface: Create a Private VLAN Group

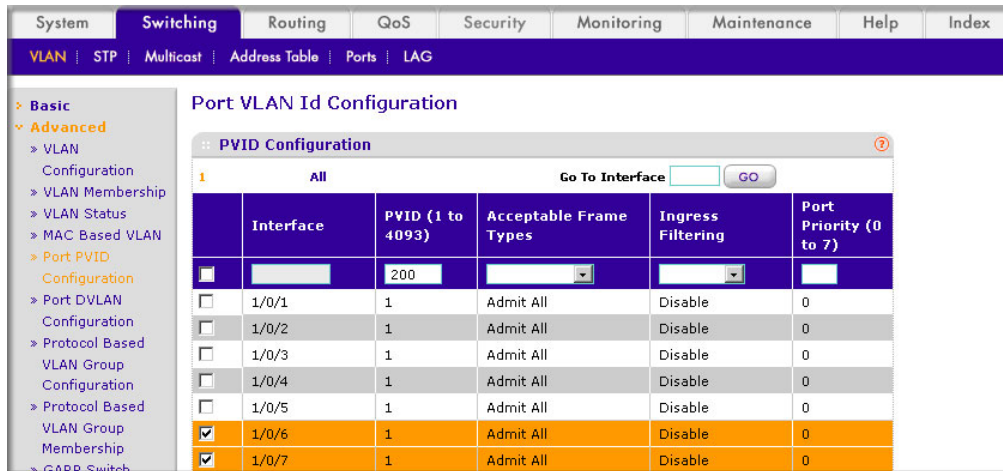
1. Create VLAN 200.
 - a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays.

VLAN ID	VLAN Name	VLAN Type
200	VLAN200	Static
1	Default	Default

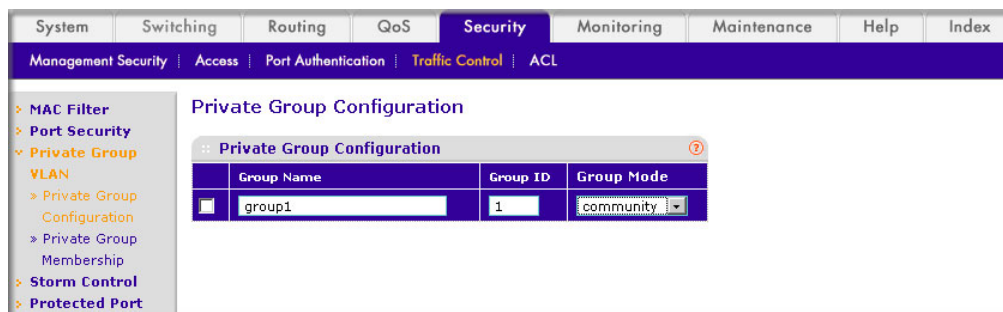
- b. Enter the following information:
 - In the **VLAN ID** field, enter **200**.
 - In the **VLAN Name** field, enter **VLAN200**.
 - In the **VLAN Type** field, select **Static**.
 - c. Click **Add**.
2. Add ports 1/0/6, 1/0/7, 1/0/16, and 1/0/17 to VLAN 200.
 - a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays.

Port	Unit 1
1	
2	
3	
4	
5	
6	U
7	U
8	
9	
10	
11	
12	
13	
14	
15	
16	U
17	U
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	

- b. Under VLAN Membership, in the **VLAN ID** list, select **200**.
 - c. Click **Unit 1**. The ports display.
 - d. Click the gray boxes under ports **6, 7, 16** and **17** until **U** displays. The U specifies that the egress packet is untagged for the port.
 - e. Click **Apply**.
3. Specify the PVID on ports 1/0/6, 1/0/7, 1/0/16, and 1/0/17.
- a. Select **Switching > VLAN > Advanced > Port PVID Configuration**. A screen similar to the following displays.

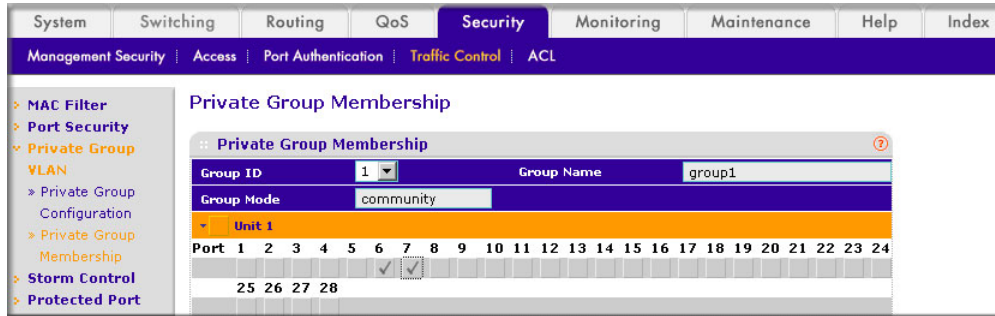


- b. Under PVID Configuration, scroll down and select the Interface **1/0/6,1/0/7,1/0/16,** and **1/0/17** check boxes.
 - c. In the **PVID (1 to 4093)** field, enter **200**.
 - d. In the **Acceptable Frame Type** list, select **Admit All**.
 - e. Click **Apply** to save the settings.
4. Create a private group, group1.
- a. Select **Security > Traffic Control > Private Group VLAN > Private Group VLAN > Private Group Configuration**. A screen similar to the following displays.

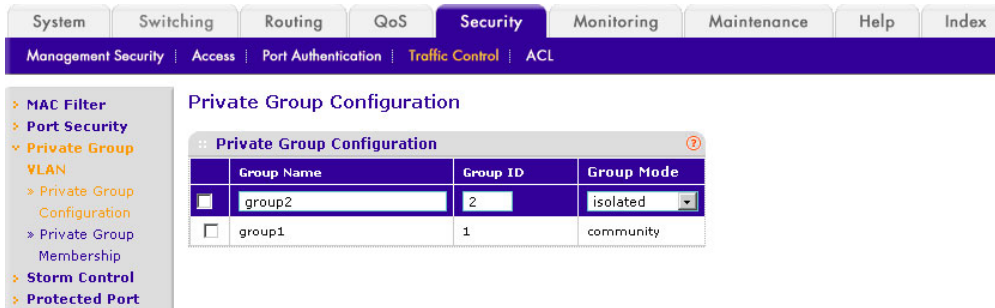


- b. In the **Group Name** field, enter **group1**.
- c. In the **Group ID** field, enter **1**.
- d. In the **Group Mode** list, select **community**.

- e. Click **Add**.
5. Add port 6 and 7 to group1.
 - a. Select **Security > Traffic Control > Private Group VLAN > Private Group Membership**. A screen similar to the following displays.

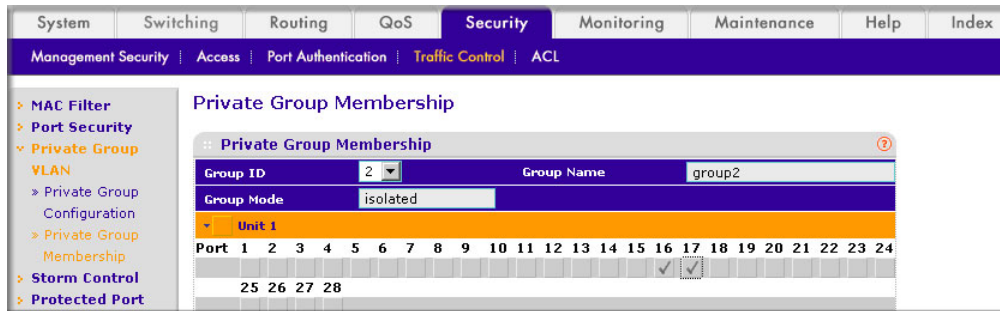


- b. In the **Group ID** list, select 1.
- c. Click **Unit 1**. The ports display.
- d. Click the gray boxes under ports **6** and **7**. A check mark displays in each box.
- e. Click **Apply**.
6. Create a private group, group2.
 - a. Select **Security > Traffic Control > Private Group VLAN > Private Group Configuration**. A screen similar to the following displays.



- b. In the **Group Name** field, enter **group2**.
- c. In the **Group ID** field, enter **2**.
- d. In the **Group Mode** field, select **isolated**.
- e. Click **Add**.
7. Add ports 16 and 17 to group2.

- a. Select **Security > Traffic Control > Private Group VLAN > Private Group VLAN > Private Group Membership**. A screen similar to the following displays.



- b. In the **Group ID** list, select **2**.
- c. Click **Unit 2**. The ports display.
- d. Click the gray boxes under ports **16** and **17**, and a check mark displays in each box.
- e. Click **Apply**.

This chapter provides the following examples:

- *Configure Classic STP (802.1d)*
- *Configure Rapid STP (802.1w)* on page 402
- *Configure Multiple STP (802.1s)* on page 403

The purpose of Spanning Tree is to eliminate loops in the switch system. There are three STPs: Classic STP (802.1d), Rapid STP (RSTP, 802.1w), and Multiple STP (MSTP, 802.1s).

While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a few seconds. RSTP can revert back to 802.1d in order to interoperate with legacy bridges on a per-port basis. This drops the benefits it introduces.

In Multiple Spanning Tree Protocol (MSTP), each Spanning Tree instance can contain several VLANs. Each Spanning Tree instance is independent of other instances. This approach provides multiple forwarding paths for data traffic, enabling load balancing, and reducing the number of Spanning Tree instances required to support a large number of VLANs.

Configure Classic STP (802.1d)

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

CLI: Configure Classic STP (802.1d)

```
(Netgear Switch) (Config)# spanning-tree
(Netgear Switch) (Config)# spanning-tree forceversion 802.1d
(Netgear switch) (Interface 1/0/3)# spanning-tree port mode
```


Web Interface: Configure Classic STP (802.1d)

1. Enable 802.1d on the switch.
 - a. Select **Switching > STP > STP Configuration**. A screen similar to the following displays.

STP Configuration

Spanning Tree Admin Mode: Disable Enable

Force Protocol Version: IEEE 802.1d IEEE 802.1w IEEE 802.1s

Configuration Name: 00-14-6C-53-62-8E (0 to 65535)

Configuration Revision Level: 0 (0 to 65535)

Forward BPDU while STP Disabled: Disable Enable

Configuration Digest Key: 0xac36177f50283cd4b83821d8ab26de62

STP Status

MST ID	VID	FID
CST	1	1

CANCEL REFRESH APPLY

- b. Enter the following information:
 - For Spanning Tree Admin Mode, select the **Enable** radio button.
 - For Force Protocol Version, select the **IEEE 802.1d** radio button.
 - c. Click **Apply**.
 2. Configure the CST port.
 - a. Select **Switching > STP > CST Port Configuration**. A screen similar to the following displays.

CST Port Configuration

LAGS: All

Interface	Port Priority	Admin Edge Port	Port Path Cost	Auto Calculated Port Path Cost	Hello Timer	External Port Path Cost	Auto Calculated External Port Path Cost	Port ID	Port Mode	Port Forwarding State
1/0/3	128	True	0	Disable	Not Configured	0	Disabled	32771	Enable	Discarding
<input type="checkbox"/> 1/0/1	128	True	0	Enable	Not Configured	0	Enabled	32769	Enable	Disabled
<input type="checkbox"/> 1/0/2	128	True	0	Enable	Not Configured	0	Enabled	32770	Enable	Disabled
<input checked="" type="checkbox"/> 1/0/3	128	True	0	Disable	Not Configured	0	Enabled	32771	Enable	Discarding
<input type="checkbox"/> 1/0/4	128	True	0	Enable	Not Configured	0	Enabled	32772	Enable	Disabled
<input type="checkbox"/> 1/0/5	128	True	0	Enable	Not Configured	0	Enabled	32773	Enable	Disabled
<input type="checkbox"/> 1/0/6	128	True	0	Enable	Not Configured	0	Enabled	32774	Enable	Disabled
<input type="checkbox"/> 1/0/7	128	True	0	Enable	Not Configured	0	Enabled	32775	Enable	Disabled
<input type="checkbox"/> 1/0/8	128	True	0	Enable	Not Configured	0	Enabled	32776	Enable	Disabled
<input type="checkbox"/> 1/0/9	128	True	0	Enable	Not Configured	0	Enabled	32777	Enable	Disabled
<input type="checkbox"/> 1/0/10	128	True	0	Enable	Not Configured	0	Enabled	32778	Enable	Disabled
<input type="checkbox"/> 1/0/11	128	True	0	Enable	Not Configured	0	Enabled	32779	Enable	Disabled
<input type="checkbox"/> 1/0/12	128	True	0	Enable	Not Configured	0	Enabled	32780	Enable	Disabled
<input type="checkbox"/> 1/0/13	128	True	0	Enable	Not Configured	0	Enabled	32781	Enable	Disabled

CANCEL REFRESH APPLY

- b. Under CST Port Configuration, scroll down and select the Interface **1/0/3** check box. Now 1/0/3 appears in the Interface field at the top.
 - c. In the **Port Mode** field, select **Enable**.
 - d. Click **Apply**.

Configure Rapid STP (802.1w)

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

CLI: Configure Rapid STP (802.1w)

```
(Netgear switch) (Config)# spanning-tree
(Netgear switch) (Config)# spanning-tree forceversion 802.1w
(Netgear switch) (Interface 1/0/3)# spanning-tree port mode
```

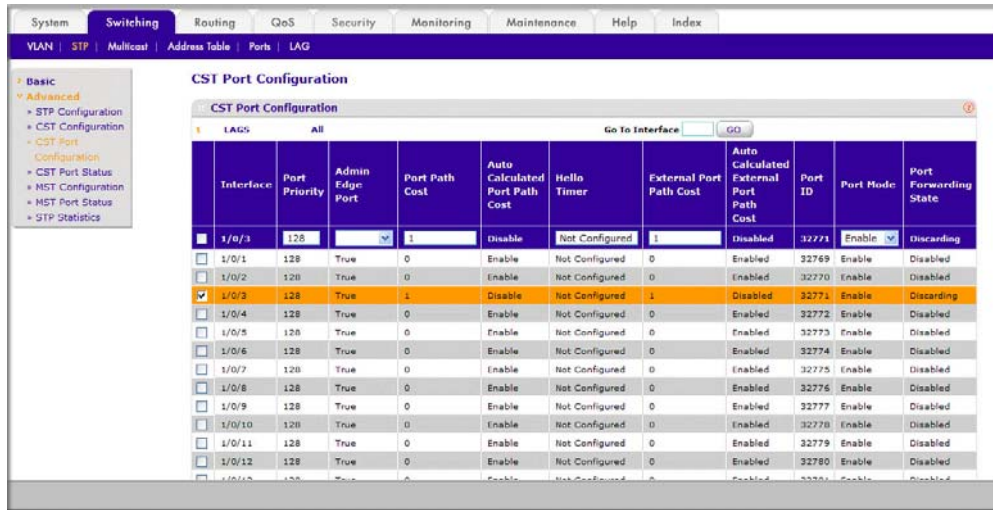
Web Interface: Configure Rapid STP (802.1w)

1. Enable 802.1w on the switch:
 - a. Select **Switching > STP > STP Configuration**. A screen similar to the following displays.

MST ID	VID	FID
CST	1 2 3 4 10 20 30 40 50 100 111	1 2 3 4 10 20 30 40 50 100 111

- b. Enter the following information:
 - For Spanning Tree Admin Mode, select the **Enable** radio button.
 - For Force Protocol Version, select the **IEEE 802.1w** radio button.
 - c. Click **Apply**.
 2. Configure the CST port.

- a. Select **Switching > STP > CST Port Configuration**. A screen similar to the following displays.



- b. Under CST Port Configuration, scroll down and select the Interface **1/0/3** check box. Now 1/0/3 appears in the Interface field at the top.
- c. In the **Port Mode** field, select **Enable**.
- d. Click **Apply**.

Configure Multiple STP (802.1s)

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

CLI: Configure Multiple STP (802.1s)

```
(Netgear switch) (Config)# spanning-tree
(Netgear switch) (Config)# spanning-tree forceversion 802.1s
(Netgear switch) (Config)# spanning-tree mst instance 1
Create a mst instance 1
(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
Associate the mst instance 1 with the VLAN 2 and 3
(Netgear switch) (Config)# spanning-tree mst instance 2
Create a mst instance 2
(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
Associate the mst instance 2 with the VLAN 11 and 12
(Netgear switch) (Interface 1/0/3)# spanning-tree mst 1 port-priority 128
(Netgear switch) (Interface 1/0/3)# spanning-tree mst 1 cost 0
```

Web Interface: Configure Multiple STP (802.1s)

1. Enable 802.1s on the switch.
 - a. Select **Switching > STP > STP Configuration**. A screen similar to the following displays.

STP Configuration

Spanning Tree Admin Mode Disable Enable

Force Protocol Version IEEE 802.1d IEEE 802.1w IEEE 802.1s

Configuration Name 00-14-6C-53-62-8E

Configuration Revision Level 0 (0 to 65535)

Forward BPDUs while STP Disabled Disable Enable

Configuration Digest Key 0xe9ab4722864c0c015adf6a12df3494ca

STP Status

MST ID	VID	FID
CST	1	1
1	2 3	2 3
2	11 12	11 12

- b. Enter the following information:
 - For Spanning Tree Admin Mode, select the **Enable** radio button.
 - For Force Protocol Version, select the **IEEE 802.1s** radio button.
 - c. Click **Apply**.
2. Configure MST.
 - a. Select **Switching > STP > MST Configuration**. A screen similar to the following displays.

MST Configuration

MST ID	Priority	Vlan Id	Bridge Identifier	Time Since Topology Change	Topology Change Count	Topology Change	Designated Root
1	4096	2, 3	10:01:00:14:6c:53:62:8e	0 day 2 hr 45 min 35 sec	0	False	10:01:00:14:6c:53:62:8e
2	4096	11, 12	10:02:00:14:6c:53:62:8e	0 day 2 hr 45 min 35 sec	0	False	10:02:00:14:6c:53:62:8e

- b. Configure MST ID 1.
 - In the **MST ID** field, enter **1**.
 - In the **Priority** field, enter **4096**.

- In the **VLAN Id** field, enter **2**.
 - Click **Add**.
 - In the **VLAN Id** field, enter **3**.
 - Click **Apply**.
- c. Configure MST ID 2.
- In the **MST ID** field, enter **2**.
 - In the **Priority** field, enter **4096**.
 - In the **VLAN Id** field, enter **11**.
 - Click **Add**.
 - In the **VLAN Id** field, enter **12**.
 - Click **Apply**.
3. Configure the MST port.
- a. Select **Switching > STP > MST Port Status**. A screen similar to the following displays.

Interface	Port Priority	Port Path Cost	Auto Calculated Port Path Cost	Port ID	Port Uptime Since Last Clear Counters	Port Mode	Port Forwarding State	Port Role	Designated
<input checked="" type="checkbox"/> 1/0/3	128	0	Enable	32771	0 day 0 hr 3 min 14 sec	Enabled	Disabled	Disabled	80:01:01:00:00:00
<input type="checkbox"/> 1/0/1	128	200000	Enable	32769	0 day 0 hr 3 min 13 sec	Enabled	Forwarding	Designated	10:01:01:00:00:00
<input type="checkbox"/> 1/0/2	128	0	Enable	32770	0 day 0 hr 3 min 14 sec	Enabled	Disabled	Disabled	80:01:01:00:00:00
<input type="checkbox"/> 1/0/4	128	0	Enable	32772	0 day 0 hr 3 min 14 sec	Enabled	Disabled	Disabled	80:01:01:00:00:00
<input type="checkbox"/> 1/0/5	128	0	Enable	32773	0 day 0 hr 3 min 15 sec	Enabled	Disabled	Disabled	80:01:01:00:00:00
<input type="checkbox"/> 1/0/6	128	0	Enable	32774	0 day 0 hr 3 min 15 sec	Enabled	Disabled	Disabled	80:01:01:00:00:00
<input type="checkbox"/> 1/0/7	128	200000	Enable	32775	0 day 0 hr 3 min 14 sec	Enabled	Forwarding	Designated	10:01:01:00:00:00
<input type="checkbox"/> 1/0/8	128	0	Enable	32776	0 day 0 hr 3 min 15 sec	Enabled	Disabled	Disabled	80:01:01:00:00:00
<input type="checkbox"/> 1/0/9	128	0	Enable	32777	0 day 0 hr 3 min 15 sec	Enabled	Disabled	Disabled	80:01:01:00:00:00

4. Under MST Port Configuration, scroll down and select the Interface **1/0/3** check box. Now 1/0/3 appears in the Interface field at the top.
5. Enter the following information:
- In the **Port Priority** field, enter **128**.
 - In the **Port Path Cost** field, enter **0**.
6. Click **Apply**.

There are two methods for IPv6 sites to communicate with each other over the IPv4 network: 6in4 tunnel and 6to4 tunnel. The 6in4 tunnel encapsulates IPv6 traffic over an explicitly configured IPv4 destination or end port of the tunnel with the IP protocol number set to 41. The 6to4 tunnel IPv6 prefix is constructed by prepending 2002 (hex) to the global IPv4 address. For example, if the IPv4 address is 4.4.4.1, the tunnel IPv6 prefix would be 2002:404:401::/16.

The 6to4 tunnels are automatically formed IPv4 tunnels carrying IPv6 traffic. The automatic tunnel's IPv4 destination address is derived from the 6to4 IPv6 address of the tunnel's nexthop. It supports the functionality of a 6to4 border router that connects a 6to4 site to a 6to4 domain. It sends/receives tunneled traffic from routers in a 6to4 domain that includes other 6to4 border routers and 6to4 relay routers. The example creates a 6in4 tunnel between GSM7328S_1 and GSM7328S_2. The tunnel carries IPv6 packets over IPv4 packets.



Figure 44. 6in4 tunnel between two switches

CLI: Create a Tunnel

Configure Switch GSM7328S_1

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ipv6 forwarding
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.1.1 255.255.255.0
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface tunnel 0
(Netgear Switch) (Interface tunnel 0)#ipv6 enable
(Netgear Switch) (Interface tunnel 0)#ipv6 address 2000::1/64
(Netgear Switch) (Interface tunnel 0)#tunnel mode ipv6ip
(Netgear Switch) (Interface tunnel 0)#tunnel source 192.168.1.1
(Netgear Switch) (Interface tunnel 0)#tunnel destination 192.1.168.1.2
(Netgear Switch) (Interface tunnel 0)#exit
(Netgear Switch) (Config)#exit
```

This example is using 6in4 mode. If you want to use 6to4 mode, configure each unit as below and be sure the IPv6 prefix is constructed in the format of 2002:V4ADDR::/48.(V4ADDR is the IPv4 address of the tunnel source port). In this case, IPv4 and the address is 192.168.1.1 and IPv6 prefix is 2002:c0a8:0101..

```
(Netgear Switch) (Interface tunnel 0) # ipv6 enable
(Netgear Switch) (Interface tunnel 0) # tunnel mode ipv6ip 6to4
(Netgear Switch) (Interface tunnel 0) # tunnel source 192.168.1.1
(Netgear Switch) (Interface tunnel 0) # ipv6 address 2002:c0a8:0101::1/128
(Netgear Switch) (Interface tunnel 0) # exit
(Netgear Switch) (Config) # ipv6 route 2002::/16 interface tunnel 0
```

Configure Switch GSM7328S_2

```
(Netgear Switch) #show interface tunnel 0
Interface Link Status..... Up
IPv6 is enabled
IPv6 Prefix is ..... FE80::COA8:101/128
                               2000::1/64
MTU size..... 1280 bytes
#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
```

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ipv6 forwarding
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ip address 192.168.1.2 255.255.255.0
(Netgear Switch) (Interface 1/0/13)#exit

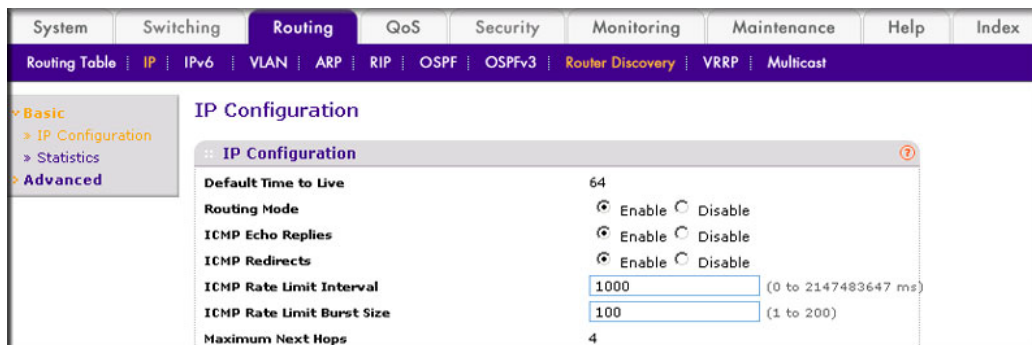
(Netgear Switch) (Config)#interface tunnel 0
(Netgear Switch) (Interface tunnel 0)#ipv6 enable
(Netgear Switch) (Interface tunnel 0)#ipv6 address 2000::2/64
(Netgear Switch) (Interface tunnel 0)#tunnel mode ipv6ip
(Netgear Switch) (Interface tunnel 0)#tunnel source 192.168.1.2
(Netgear Switch) (Interface tunnel 0)#tunnel destination 192.168.1.1
(Netgear Switch) (Interface tunnel 0)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #show interface tunnel

TunnelId  Interface  TunnelMode      SourceAddress    DestinationAddress
-----  -
0 tunnel  0         6 in 4 Configured  192.168.1.2     192.168.1.1
```


Web Interface: Create a Tunnel

Configure Switch GSM7328S_1

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.



System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index		
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast

IP Configuration

Default Time to Live: 64

Routing Mode: Enable Disable

ICMP Echo Replies: Enable Disable

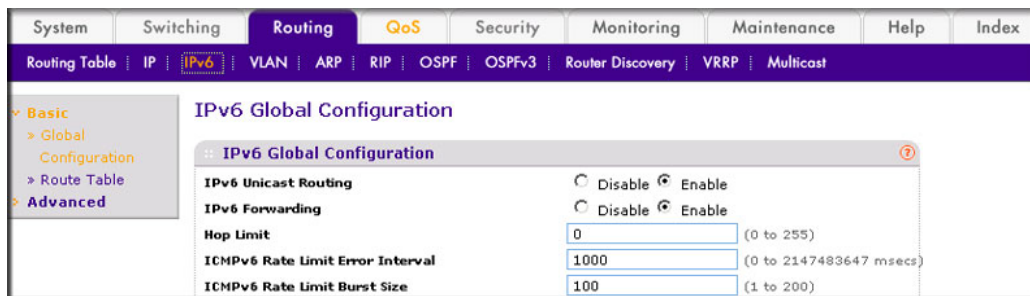
ICMP Redirects: Enable Disable

ICMP Rate Limit Interval: 1000 (0 to 2147483647 ms)

ICMP Rate Limit Burst Size: 100 (1 to 200)

Maximum Next Hops: 4

- b. For Routing Mode, select the **Enable** radio button.
 - c. Click **Apply**.
2. Enable IPv6 forwarding and unicast routing on the switch.
 - a. Select **Routing > IPv6 > Basic > Global Configuration**. A screen similar to the following displays.



System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index		
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast

IPv6 Global Configuration

IPv6 Unicast Routing: Disable Enable

IPv6 Forwarding: Disable Enable

Hop Limit: 0 (0 to 255)

ICMPv6 Rate Limit Error Interval: 1000 (0 to 2147483647 msecs)

ICMPv6 Rate Limit Burst Size: 100 (1 to 200)

- b. For IPv6 Unicast Routing, select the **Enable** radio button.
 - c. For IPv6 Forwarding, select the **Enable** radio button.
 - d. Click **Apply**.
3. Create a routing interface and assign an IP address to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input type="checkbox"/> 1/0/1			192.168.1.1	255.255.255.0	Enable	Enable
<input checked="" type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

- b. Under IP Interface Configuration, scroll down and select the Port **1/0/1** check box. Now 1/0/1 appears in the Interface field at the top.
- In the **IP Address** field, enter **192.168.1.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- c. Click **Apply**.

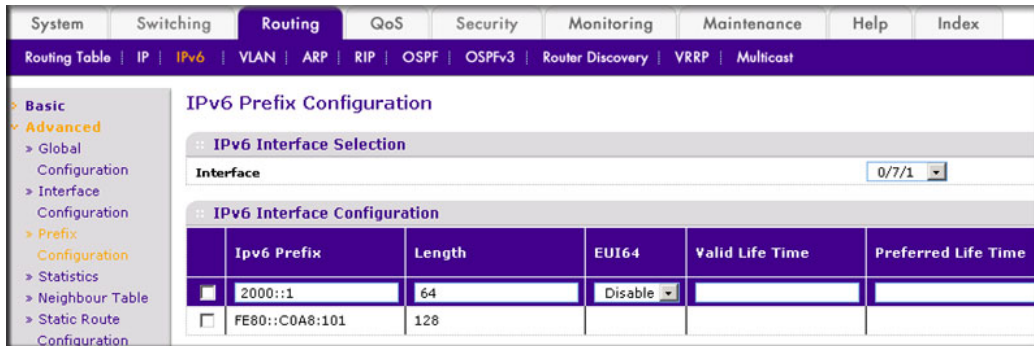
4. Create a 6-in-4 tunnel interface.

- a. Select **Routing > IPv6 > Advanced > Tunnel Configuration**. A screen similar to the following displays.

Tunnel Id	Mode	IPv6 Mode	IPv6 Unreachables	IPv6 Address	EUI64	Source Address	Source Interface	Desti
<input type="checkbox"/> 0	6-in-4-configured	Enable				192.168.1.1	192.168.1.1	

- b. In the **Tunnel Id** list, select **0**.
- c. In the **Mode** field, select **6-in-4-configured**.
- d. In the **Source Address** field, enter **192.168.1.1**.
- e. In the **Destination Address** field, enter **192.168.1.2**.
- f. Click **Apply**.
5. Assign an IPv6 address to the tunnel.

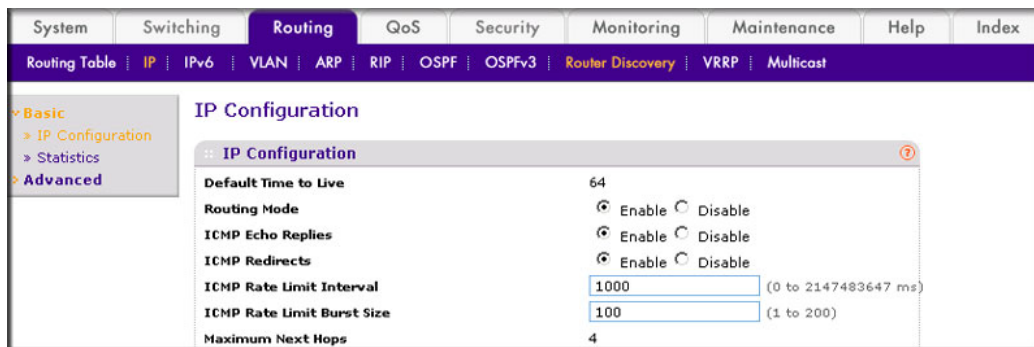
- a. Select **Routing > IPv6 > Advanced > Prefix Configuration**. A screen similar to the following displays.



- b. In the **Interface** list, select **0/7/1**.
- c. In the **IPv6 Prefix** field, enter **2000::1**.
- d. In the **Length** field, enter **64**.
- e. In the **EUI64** field, select **Disable**.
- f. Click **Add**.

Configure Switch GSM7328S_2

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.



- b. For Routing Mode, select the **Enable** radio button.
- c. Click **Apply**.
2. Enable IPv6 forwarding and unicast routing on the switch.

- a. Select **Routing > IPv6 > Basic > Global Configuration**. A screen similar to the following displays.

The screenshot shows the 'IPv6 Global Configuration' page. The navigation menu includes System, Switching, Routing (selected), QoS, Security, Monitoring, Maintenance, Help, and Index. Under Routing, there are sub-menus for Routing Table, IP, IPv6 (selected), VLAN, ARP, RIP, OSPF, OSPFv3, Router Discovery, VRRP, and Multicast. The left sidebar shows a tree view with Basic > Global > Configuration > Route Table > Advanced. The main content area is titled 'IPv6 Global Configuration' and contains the following settings:

- IPv6 Unicast Routing: Disable Enable
- IPv6 Forwarding: Disable Enable
- Hop Limit: (0 to 255)
- ICMPv6 Rate Limit Error Interval: (0 to 2147483647 msec)
- ICMPv6 Rate Limit Burst Size: (1 to 200)

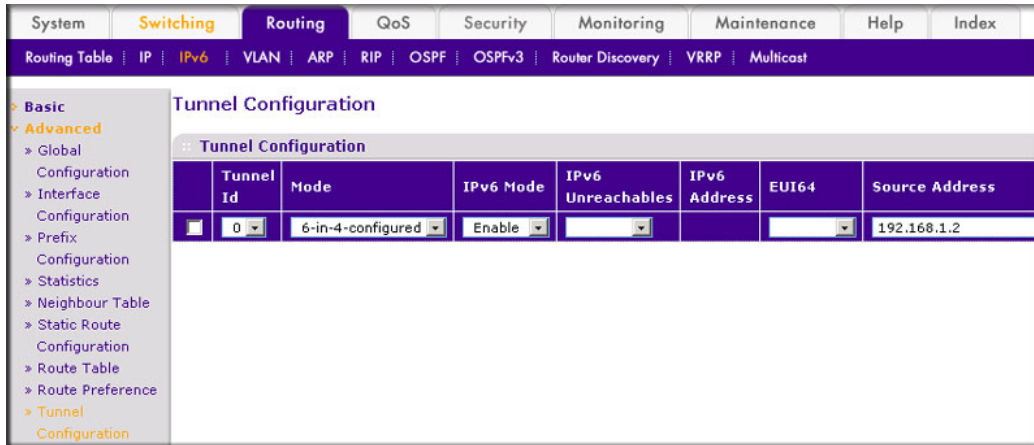
- b. For IPv6 Unicast Routing, select the **Enable** radio button.
- c. For IPv6 Forwarding, select the **Enable** radio button.
- d. Click **Apply**.
3. Create a routing interface and assign an IP address to it.
- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

The screenshot shows the 'IP Interface Configuration' page. The navigation menu includes System, Switching, Routing (selected), QoS, Security, Monitoring, Maintenance, Help, and Index. Under Routing, there are sub-menus for Routing Table, IP (selected), IPv6, VLAN, ARP, RIP, OSPF, OSPFv3, Router Discovery, VRRP, and Multicast. The left sidebar shows a tree view with Basic > Advanced > IP Configuration > Statistics > IP Interface > Configuration > Secondary IP. The main content area is titled 'IP Interface Configuration' and contains a table with the following data:

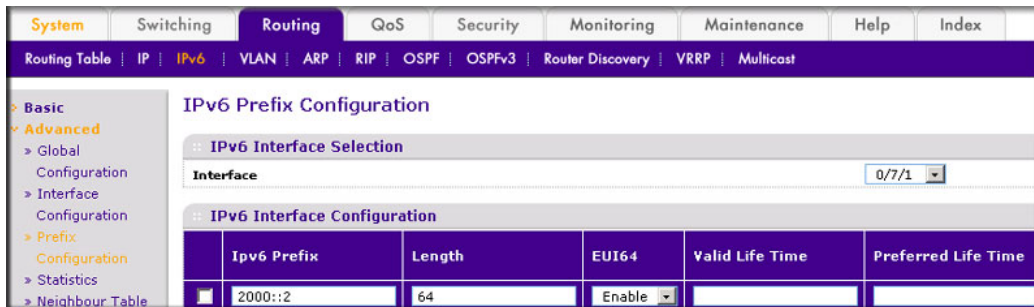
Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/13			192.168.1.2	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

- b. Under IP Interface Configuration, scroll down and select the Port **1/0/13** check box. Now 1/0/1 appears in the Port field at the top.
- In the **IP Address** field, enter **192.168.1.2**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- c. Click **Apply**.
4. Create a 6-in-4 tunnel interface.

- a. Select **Routing > IPv6 > Advanced > Tunnel Configuration**. A screen similar to the following displays.



- b. In the **Tunnel Id** list, select **0**.
 - c. In the **Mode** list, select **6-in-4-configured**.
 - d. In the **Source Address** field, enter **192.168.1.2**.
 - e. In the **Destination Address** field, enter **192.168.1.1**.
 - f. Click **Apply**.
5. Assign an IPv6 address to the tunnel.
 - a. Select **Routing > IPv6 > Advanced > Prefix Configuration**. A screen similar to the following displays.



- b. In the **Interface** list, select **0/7/1**.
- c. In the **IPv6 Prefix** field, enter **2000::2**.
- d. In the **Length** field, enter **64**.
- e. In the **EUI64** field, select **Disable**.
- f. Click **Add**.

27. IPv6 Interface Configuration



This chapter provides the following examples:

- *Create an IPv6 Routing Interface*
- *Create an IPv6 Network Interface* on page 417
- *Create an IPv6 Routing VLAN* on page 419
- *Configure DHCPv6 Mode on the Routing Interface* on page 424

Create an IPv6 Routing Interface

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

CLI: Create an IPv6 Routing Interface

1. Enable IPV6 forwarding and unicast routing on the switch.

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

2. Assign an IPv6 address to interface 1/0/1.

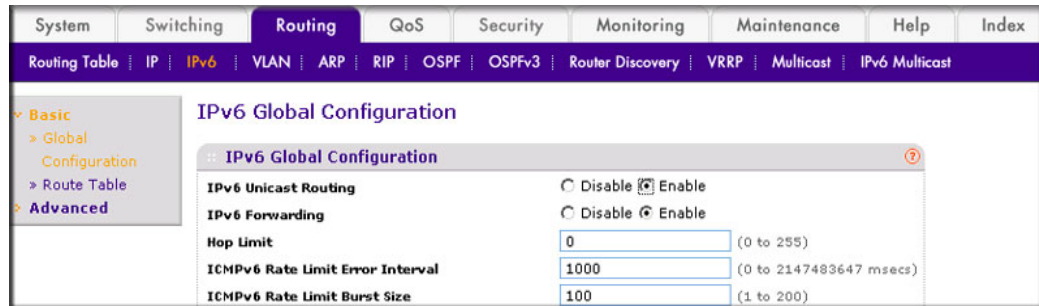
```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#ipv6 enable
(Netgear Switch) (Interface 1/0/1)#ipv6 address 2000::2/64
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) #ping ipv6 2000::2
Send count=3, Receive count=3 from 2000::2
Average round trip time = 1.00 ms
(Netgear Switch) #show ipv6 brief
IPv6 Forwarding Mode..... Enable
IPv6 Unicast Routing Mode..... Enable
IPv6 Hop Limit..... 0
ICMPv6 Rate Limit Error Interval..... 1000 msec
ICMPv6 Rate Limit Burst Size..... 100 messages
Maximum Routes..... 12
```

```
(Netgear Switch) #show ipv6 interface 1/0/1
IPv6 is enabled
IPv6 Prefix is ..... FE80::21E:2AFF:FED9:249B/128
                               2000::2/64 [TENT]
Routing Mode..... Enabled
Administrative Mode..... Enabled
IPv6 Routing Operational Mode..... Enabled
Bandwidth..... 1000000 kbps
Interface Maximum Transmit Unit..... 1500
Router Duplicate Address Detection Transmits... 1
Router Advertisement NS Interval..... 0
Router Advertisement Lifetime..... 1800
Router Advertisement Reachable Time..... 0
Router Advertisement Interval..... 600
Router Advertisement Managed Config Flag..... Disabled
Router Advertisement Other Config Flag..... Disabled
Router Advertisement Suppress Flag..... Disabled
IPv6 Destination Unreachables..... Enabled

Prefix 2000::2/64
Preferred Lifetime..... 604800
Valid Lifetime..... 2592000
Onlink Flag..... Enabled
Autonomous Flag..... Enabled
```

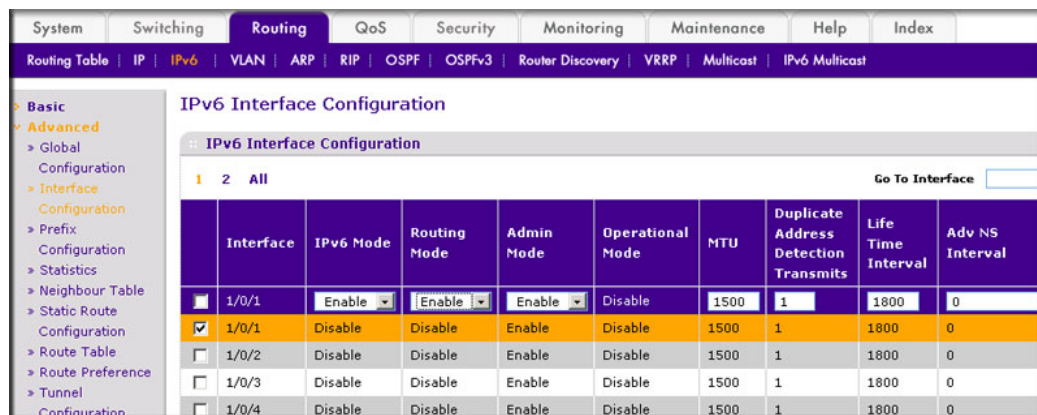
Web Interface: Create an IPv6 Routing Interface

1. Enable IPv6 forwarding and unicast routing on the switch.
 - a. Select **Routing > IPv6 > Basic > Global Configuration**. A screen similar to the following displays.



The screenshot shows the 'IPv6 Global Configuration' page. The 'IPv6 Unicast Routing' and 'IPv6 Forwarding' options are both set to 'Enable'. The 'Hop Limit' is set to 0, 'ICMPv6 Rate Limit Error Interval' is 1000, and 'ICMPv6 Rate Limit Burst Size' is 100.

- b. For IPv6 Unicast Routing, select the **Enable** radio button.
 - c. For IPv6 Forwarding, select the **Enable** radio button.
 - d. Click **Apply**.
2. Enable IPv6 routing on interface 1/0/1.
 - a. Select **Routing > IPv6 > Advanced > Interface Configuration**. A screen similar to the following displays.



The screenshot shows the 'IPv6 Interface Configuration' page. A table lists the interfaces and their configurations. The '1/0/1' interface is selected, and its 'IPv6 Mode' is set to 'Enable'.

	Interface	IPv6 Mode	Routing Mode	Admin Mode	Operational Mode	MTU	Duplicate Address Detection Transmits	Life Time Interval	Adv NS Interval
<input type="checkbox"/>	1/0/1	Enable	Enable	Enable	Disable	1500	1	1800	0
<input checked="" type="checkbox"/>	1/0/1	Disable	Disable	Enable	Disable	1500	1	1800	0
<input type="checkbox"/>	1/0/2	Disable	Disable	Enable	Disable	1500	1	1800	0
<input type="checkbox"/>	1/0/3	Disable	Disable	Enable	Disable	1500	1	1800	0
<input type="checkbox"/>	1/0/4	Disable	Disable	Enable	Disable	1500	1	1800	0

- b. Under IPv6 Interface Configuration, scroll down and select the Interface **1/0/1** check box. Now 1/0/1 appears in the Interface field at the top.
 - c. In the IPv6 Mode field, select **Enable**.
 - d. Click **Apply** to save the settings.
3. Assign an IPv6 address to the routing interface.

- a. Select **Routing > IPv6 > Advanced > Prefix Configuration**. A screen similar to the following displays.

IPv6 Prefix Configuration					
IPv6 Interface Selection					
Interface					1/0/1
IPv6 Interface Configuration					
	IPv6 Prefix	Length	EUI64	Valid Life Time	Preferred Life Time
<input type="checkbox"/>	2000::2	64	Disable		

- b. In the Interface list, select **1/0/1**.
- c. In the IPv6 Prefix field, enter **2000::2**.
- d. In the Length field, enter **64**.
- e. In the EUI64 field, select **Disable**.
- f. Click **Add**.

Create an IPv6 Network Interface

The IPv6 network interface is the logical interface used for in-band connectivity with the switch using any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

To access the switch over an IPv6 network you must first configure it with IPv6 information (IPv6 prefix, prefix length, and default gateway).

CLI: Configure the IPv6 Network Interface

```
(Netgear Switch) #network ipv6 enable
(Netgear Switch) #network ipv6 address 2001:1::1/64
(Netgear Switch) #network ipv6 gateway 2001:1::2
(Netgear Switch) #show network
Interface Status..... Always Up
IP Address..... 0.0.0.0
Subnet Mask..... 0.0.0.0
Default Gateway..... 0.0.0.0
IPv6 Administrative Mode..... Enabled
IPv6 Prefix is ..... FE80::2FF:F9FF:FE70:485/64
IPv6 Prefix is ..... 2001:1::1/64
IPv6 Default Router..... 2001:1::2
Burned In MAC Address..... 00:FF:F9:70:04:85
Locally Administered MAC address..... 00:00:00:00:00:00
MAC Address Type..... Burned In
Configured IPv4 Protocol..... None
Configured IPv6 Protocol..... None
IPv6 AutoConfig Mode..... Disabled
Management VLAN ID.....1
```

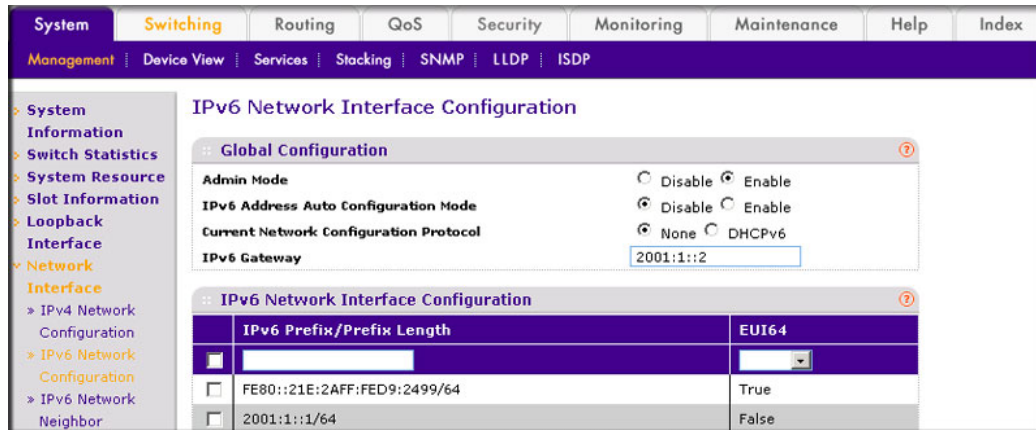
Web Interface: Configure the IPv6 Network Interface

1. Add an IPv6 address to the network interface.
 - a. Select **System > Management > Network Interface > IPv6 Network Configuration**. A screen similar to the following displays.

IPv6 Network Interface Configuration	
Global Configuration	
Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IPv6 Address Auto Configuration Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Current Network Configuration Protocol	<input checked="" type="radio"/> None <input type="radio"/> DHCPv6
IPv6 Gateway	<input type="text"/>
IPv6 Network Interface Configuration	
IPv6 Prefix/Prefix Length	EUI64
<input checked="" type="checkbox"/> 2001:1::1/64	False
<input type="checkbox"/> FE80::21E:2AFF:FED9:2499/64	True

- b. For Admin Mode, select the **Enable** radio button.
 - c. In the **IPv6 Prefix/Prefix Length** field, enter **2001:1::1/64**.
 - d. In the **EUI64** field, select **False**.
 - e. Click **Add**.

2. Add an IPv6 gateway to the network interface.
 - a. Select **System > Management > Network Interface > IPv6 Network Configuration**. A screen similar to the following displays.



- b. In the **IPv6 Gateway** field, enter **2001:1::2**.
- c. Click **Apply**.

Create an IPv6 Routing VLAN

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

CLI: Create an IPv6 Routing VLAN

1. Create a routing VLAN with VLAN ID 500.

```
Netgear Switch) (Vlan)#vlan 500
Netgear Switch) (Vlan)#vlan routing 500
Netgear Switch) (Vlan)#exit
```

2. Add interface 1/0/1 to VLAN 500.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#vlan participation include 500
(Netgear Switch) (Interface 1/0/1)#vlan participation pvid 500
(Netgear Switch) (Interface 1/0/1)#exit
```

3. Assign IPv6 address 2000::1/64 to VLAN 500 and enable IPv6 routing.

```
(Netgear Switch) (Config)#interface vlan 0/4/1
(Netgear Switch) (Interface 0/4/1)#routing
(Netgear Switch) (Interface 0/4/1)#ipv6 enable
(Netgear Switch) (Interface 0/4/1)#ipv6 address 2000::1/64
(Netgear Switch) (Interface 0/4/1)#exit
```

4. Enable IPV6 forwarding and unicast routing on the switch.

```
(Netgear Switch) (Config)#ipv6 forwarding
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) #ping ipv6 2000::2
Send count=3, Receive count=3 from 2000::2
Average round trip time = 1.00 ms
(Netgear Switch) #show ipv6 brief
IPv6 Forwarding Mode..... Enable
IPv6 Unicast Routing Mode..... Enable
IPv6 Hop Limit..... 0
ICMPv6 Rate Limit Error Interval..... 1000 msec
ICMPv6 Rate Limit Burst Size..... 100 messages
Maximum Routes..... 128
(Netgear Switch) #show ipv6 interface 0/4/1
IPv6 is enabled
IPv6 Prefix is ..... FE80::21E:2AFF:FED9:249B/128
                               2000::1/64
Routing Mode..... Enabled
Administrative Mode..... Enabled
IPv6 Routing Operational Mode..... Enabled
Bandwidth..... 10000 kbps
Interface Maximum Transmit Unit..... 1500
Router Duplicate Address Detection Transmits... 1
Router Advertisement NS Interval..... 0
Router Advertisement Lifetime..... 1800
Router Advertisement Reachable Time..... 0
Router Advertisement Interval..... 600
Router Advertisement Managed Config Flag..... Disabled
Router Advertisement Other Config Flag..... Disabled
Router Advertisement Suppress Flag..... Disabled
IPv6 Destination Unreachables..... Enabled
Prefix 2000::1/64
Preferred Lifetime..... 604800
Valid Lifetime..... 2592000
Onlink Flag..... Enabled
Autonomous Flag..... Enabled
```

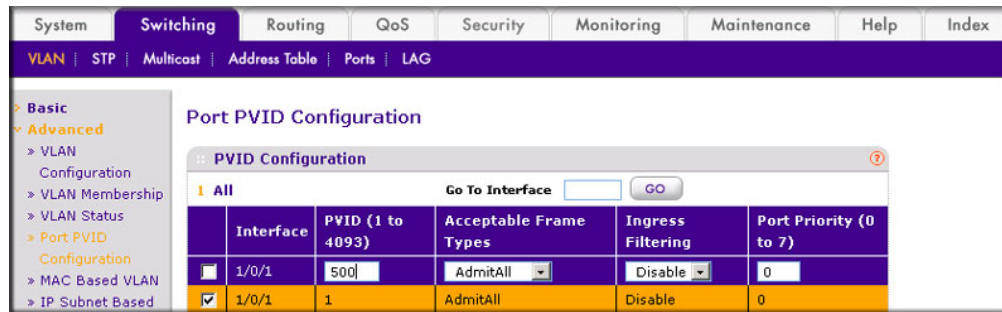
Web Interface: Create an IPv6 VLAN Routing Interface

1. Create VLAN 500.
 - a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays.

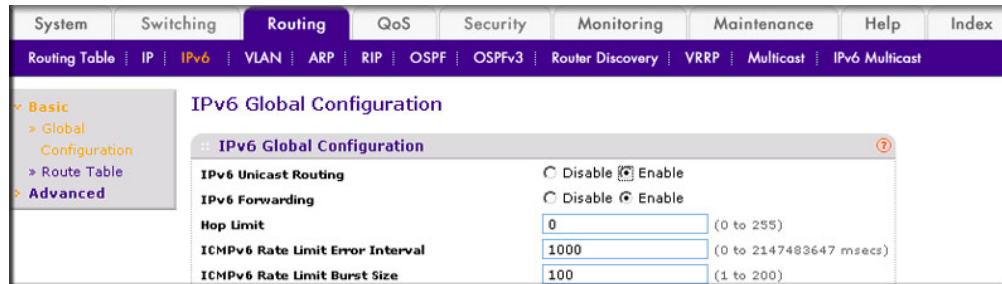
- b. In the **VLAN ID** field, enter **500**.
 - c. In the **VLAN Type** field, select **Static**.
 - d. Click **Add**.
2. Add ports to VLAN 500.
 - a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays.

- b. In the **VLAN ID** list, select **500**.
 - c. Click **Unit 1**. The ports display.
 - d. Click the gray box under port **1** until **U** displays, indicating that the egress packet is untagged for the port.
 - e. Click **Apply**.
3. Specify the PVID on port 1/0/1.

- a. Select **Switching > VLAN > Advanced > Port PVID Configuration**. A screen similar to the following displays.

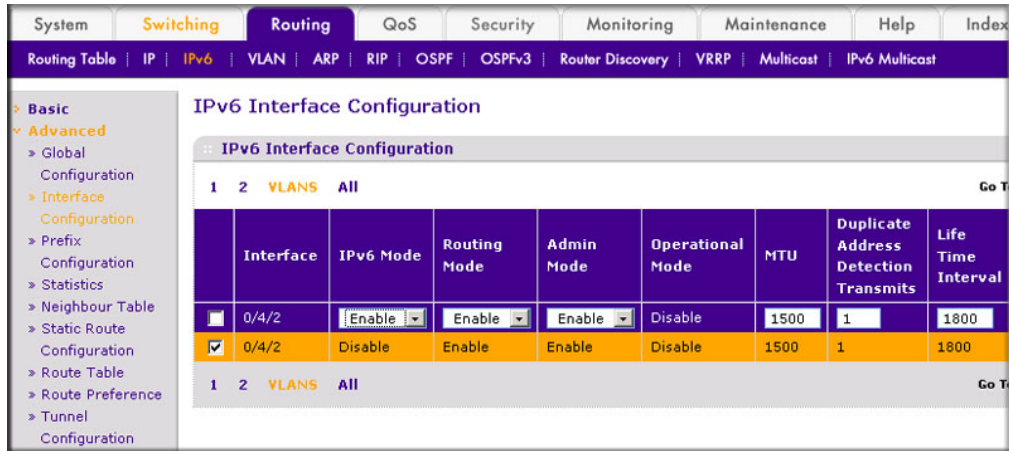


- b. Under PVID Configuration, scroll down and select the Interface **1/0/1** check box.
 c. In the **PVID (1 to 4093)** field, enter **500**.
 d. Click **Apply** to save the settings.
4. Enable IPv6 forwarding and unicast routing on the switch.
- a. Select **Routing > IPv6 > Basic > Global Configuration**. A screen similar to the following displays.



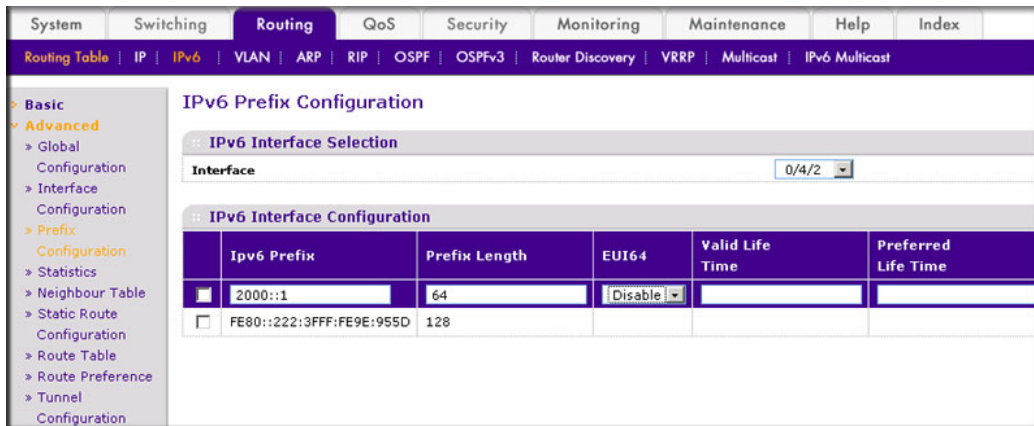
- b. For IPv6 Unicast Routing, select the **Enable** radio button.
 c. For IPv6 Forwarding, select the **Enable** radio button.
 d. Click **Apply**.
5. Enable IPv6 routing on the VLAN.

- a. Select **Routing > IPv6 > Advanced > Interface Configuration**. A screen similar to the following displays.



- b. Click **VLANS**. The logical VLAN interface 0/4/2 displays.
 - c. Select the **0/4/2** check box.
 - d. Under IPv6 Interface Configuration, in the **IPv6 Mode** field, select **Enable**.
 - e. Click **Apply**.
6. Assign an IPv6 address to the routing VLAN.

- a. Select **Routing > IPv6 > Advanced > Prefix Configuration**. A screen similar to the following displays.



- b. In the **Interface** field, select **0/4/2**.
- c. In the **IPv6 Prefix** field, enter **2000::1**.
- d. In the **Length** field, enter **64**.
- e. In the **EUI64** field, select **Disable**.
- f. Click **Add**.

Configure DHCPv6 Mode on the Routing Interface

The routing interface supports DHCPv6 mode, which can get the IPv6 address from a DHCPv6 server (address allocation).

Note: Before you enable DHCPv6 mode, you have to disable IPv6 unicast mode globally.

CLI: Configure DHCPv6 mode on routing interface

1. Enable IPv6 unicast globally.

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

2. Enable DHCPv6 on the interface 1/0/23.

```
(Netgear Switch) (Config)#interface 1/0/23
(Netgear Switch) (Interface 1/0/23)#routing
(Netgear Switch) (Interface 1/0/23)#ipv6 enable
(Netgear Switch) (Interface 1/0/23)#ipv6 address dhcp
(Netgear Switch) (Interface 1/0/23)
```

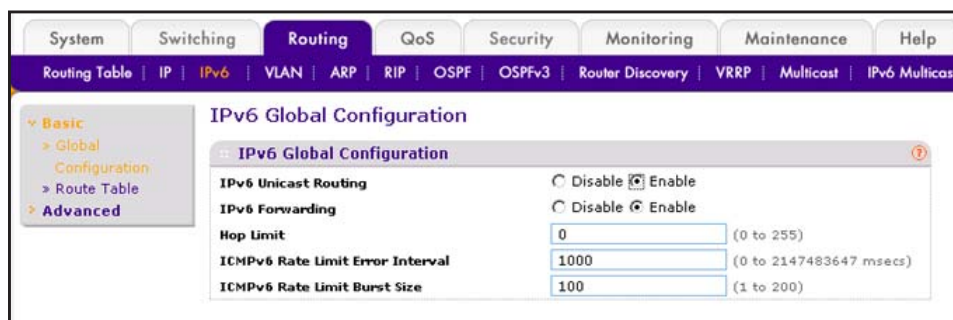

3. Show the ipv6 address assigned from 1/0/23.

```
(Netgear Switch) #show ipv6 interface 1/0/23
IPv6 is enabled
IPv6 Prefix is ..... FE80::E291:F5FF:FE06:2BF6/128
                                     2000::1D5C:7CFE:828F:8144/128 [DHCP]

Routing Mode..... Enabled
IPv6 Enable Mode..... Enabled
Administrative Mode..... Enabled
IPv6 Operational Mode..... Enabled
Bandwidth..... 1000000 kbps
Interface Maximum Transmit Unit..... 1500
Router Duplicate Address Detection Transmits... 1
Address DHCP Mode..... Enabled
Router Advertisement NS Interval..... 0
Router Advertisement Lifetime..... 1800
Router Advertisement Reachable Time..... 0
Router Advertisement Interval..... 600
Router Advertisement Managed Config Flag..... Disabled
Router Advertisement Other Config Flag..... Disabled
Router Advertisement Router Preference..... medium
Router Advertisement Suppress Flag..... Disabled
IPv6 Destination Unreachables..... Enabled
```

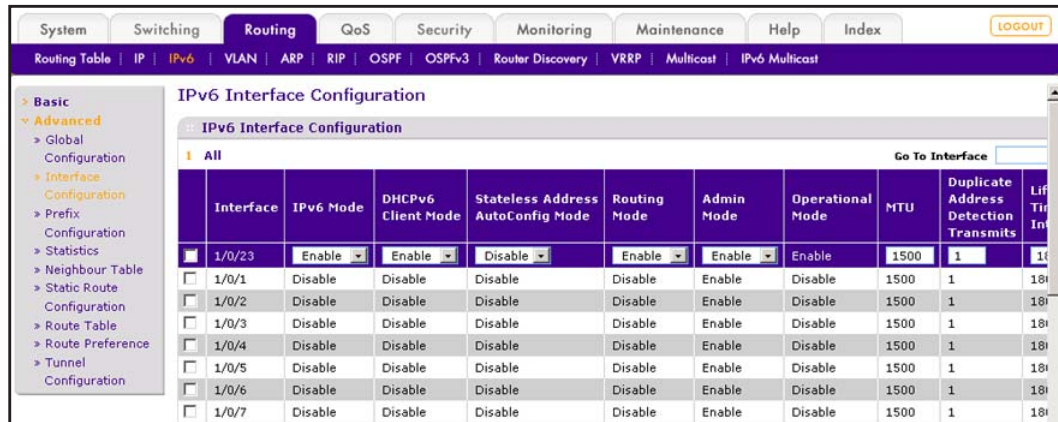
Web Interface: Configure DHCPv6 mode on routing interface

1. Enable IPv6 unicast globally.
 - a. Select **Routing > IPv6 > Basic > Global Configuration**. A screen similar to the following displays.



- b. For IPv6 Unicast Routing, select the **Enable** radio button.
 - c. Click **Apply** to apply the setting.
2. Enable DHCPv6 on the interface 1/0/23.

- a. Select **Routing > IPv6 > Advanced > Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the **interface 1/0/23** check box. Now 1/0/23 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the IPv6 Mode field, select **Enable**.
 - In the Routing Mode field, select **Enable**.
 - In the DHCPv6 Client Mode field, select **Enable**.
 - d. Click **Apply** to apply the settings.
3. Show the ipv6 address assigned from 1/0/23.

- a. Select **Routing > IPv6 > Advanced > Prefix Configuration**. A screen similar to the following displays.



- b. Scroll down and select the **interface 1/0/23**. You can see the IPv6 address assigned by the DHCPv6 server.

Protocol-Independent-Multicast

This chapter provides the following examples:

- *PIM-DM*
- *PIM-SM* on page 451

Note: The PIM protocol can be configured to operate on IPv4 and IPv6 networks. Separate CLI commands are provided for IPv4 and IPv6 operation; however, most configuration options are common to both protocols. Therefore, this section describes only IPv4 configuration; IPv6 configuration is similar to IPv4.

Multicast protocols are used to deliver multicast packets from one source to multiple receivers. They facilitate better bandwidth utilization, and use less host and router processing, making them ideal for usage in applications such as video and audio conferencing, whiteboard tools, stock distribution tickers, and so on. PIM is a widely used multicast routing protocol. Protocol Independent Multicast (PIM) is a standard multicast routing protocol that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. There are two types of PIM:

- PIM-Dense Mode (PIM-DM)
- PIM-Sparse Mode (PIM-SM)

PIM-DM

PIM-DM is appropriate for:

- Densely distributed receivers
- A ratio of few senders to many receivers (due to frequent flooding)
- High volume of multicast traffic
- Constant stream of traffic

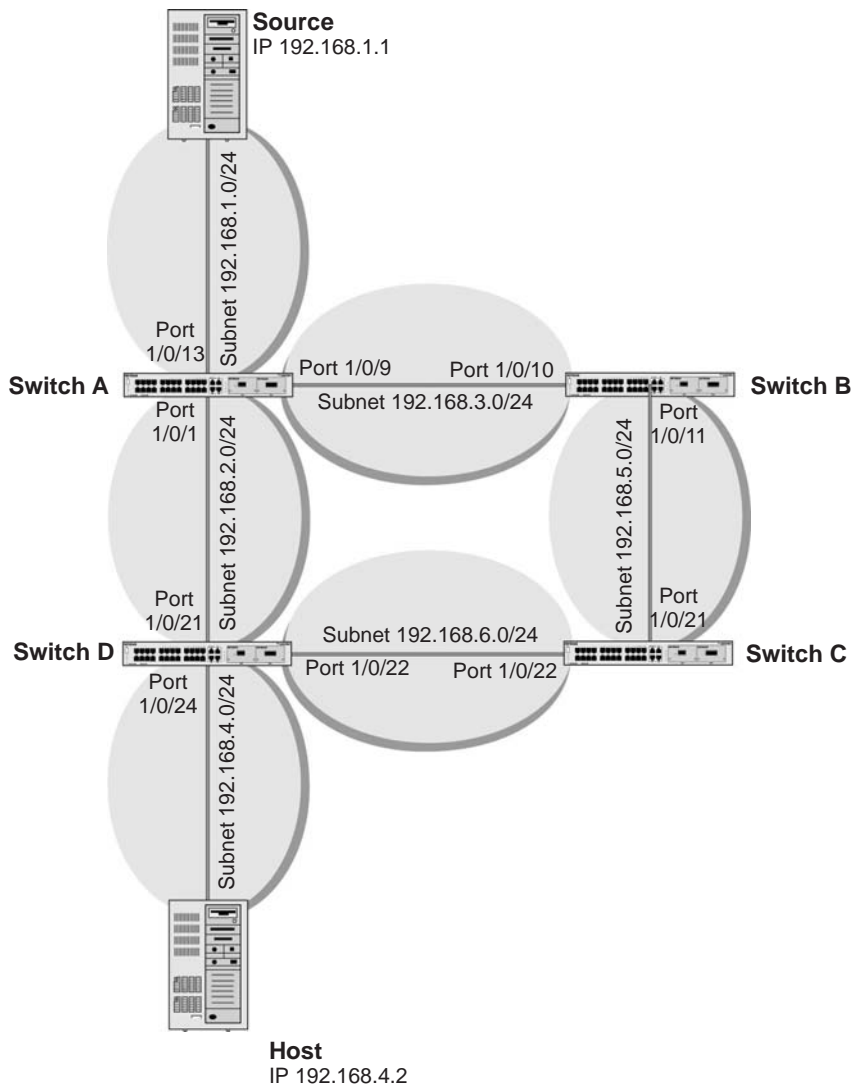


Figure 45. Configuring and Using PIM-DM

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 making use of reverse path forwarding (RPF). PIM-DM cannot be used to build a shared distribution tree, as PIM-SM can. PIM-DM assumes that when a sender starts sending data, all downstream routers and hosts want to receive a multicast datagram. PIM-DM initially floods multicast traffic throughout the network. Routers that do not have any downstream neighbors prune back the unwanted traffic. Apart from the prune messages, PIM-DM makes use of two more messages: graft and assert. Graft messages are used whenever a new host wants to join the group. Assert messages are used to shut off duplicate flows onto the same multi-access network.

To minimize the repeated flooding of datagrams and subsequent pruning associated with a particular (S,G) pair, PIM-DM uses a state refresh message. This message is sent by the routers directly connected to the source and is propagated throughout the network. When

received by a router on its RPF interface, the state refresh message causes an existing prune state to be refreshed. State refresh messages are generated periodically by the router directly attached to the source. There are two versions of PIM-DM. Version 2 does not use IGMP messages; instead, it uses a message that is encapsulated in IP packets with protocol number 103. In version 2, the Hello message is introduced in place of the query message.

CLI: Configure PIM-DM

PIM-DM on Switch A

1. Enable IP routing on the switch.

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

2. Enable pimdm on the switch.

```
(Netgear Switch) (Config)#ip pim dense
```

3. Enable IP multicast forwarding on the switch.

```
(Netgear Switch) (Config)#ip multicast
```

4. Enable RIP to build the unicast IP routing table.

```
(Netgear Switch) (Config)#interface 1/0/1  
(Netgear Switch) (Interface 1/0/1)#routing  
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.2.2 255.255.255.0  
(Netgear Switch) (Interface 1/0/1)#ip rip
```

5. Enable PIM-DM on the interface.

```
(Netgear Switch) (Interface 1/0/1)#ip pim dense
(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 dense
(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 dense
(Netgear Switch) (Interface 1/0/13)#exit
```

PIM-DM on Switch B

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim dense
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#interface 1/0/10
(Netgear Switch) (Interface 1/0/10)#routing
(Netgear Switch) (Interface 1/0/10)#ip address 192.168.3.2 255.255.255.0
(Netgear Switch) (Interface 1/0/10)#ip rip
(Netgear Switch) (Interface 1/0/10)#ip pim dense
(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 dense
(Netgear Switch) (Interface 1/0/11)#exit
```

PIM-DM on Switch C

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim dense
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address 192.168.5.2 255.255.255.0
(Netgear Switch) (Interface 1/0/21)#ip rip
(Netgear Switch) (Interface 1/0/21)#ip pim dense
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) (Config)#interface 1/0/22
(Netgear Switch) (Interface 1/0/22)#routing
(Netgear Switch) (Interface 1/0/22)#ip address 192.168.6.1 255.255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22)#ip pim dense
(Netgear Switch) (Interface 1/0/22)#exit
```

PIM-DM on Switch D

1. Enable IGMP on the switch.

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim dense
(Netgear Switch) (Config)#ip igmp
```

```
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address 192.168.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/21)#ip rip
(Netgear Switch) (Interface 1/0/21)#ip pim dense
(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 dense
(Netgear Switch) (Interface 1/0/22)#exit
```

2. Enable IGMP on 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#routing
(Netgear Switch) (Interface 1/0/24)#ip pim dense
(Netgear Switch) (Interface 1/0/24)#ip igmp
(Netgear Switch) (Interface 1/0/24)#ip rip
(Netgear Switch) (Interface 1/0/24)#ip address 192.168.4.1 255.255.255.0
(Netgear Switch) (Interface 1/0/24)#exit
```

3. PIM-DM builds the multicast routes table on each switch.

```
(A) #show ip mcast mroute summary
      Multicast Route Table Summary
      Incoming      Outgoing
Source IP  Group IP  Protocol  Interface  Interface List
-----
192.168.1.1  225.1.1.1  PIMDM    1/0/13    1/0/1

(B) #show ip mcast mroute summary
      Multicast Route Table Summary
      Incoming      Outgoing
Source IP  Group IP  Protocol  Interface  Interface List
-----
192.168.1.1  225.1.1.1  PIMDM    1/0/10

(C) #show ip mcast mroute summary
      Multicast Route Table Summary
      Incoming      Outgoing
Source IP  Group IP  Protocol  Interface  Interface List
-----
192.168.1.1  225.1.1.1  PIMDM    1/0/21

(D) #show ip mcast mroute summary
      Multicast Route Table Summary
      Incoming      Outgoing
Source IP  Group IP  Protocol  Interface  Interface List
-----
192.168.1.1  225.1.1.1  PIMDM    7/0/21    7/0/24
```


Web Interface: Configure PIM-DM

PIM-DM on Switch A

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.

The screenshot shows the 'IP Configuration' page in the web interface. The 'Routing Mode' is set to 'Enable' (radio button selected). Other settings include: Default Time to Live: 64; ICMP Echo Replies: Enable; ICMP Redirects: Enable; ICMP Rate Limit Interval: 1000; ICMP Rate Limit Burst Size: 100.

- b. For Routing Mode, select the **Enable** radio button.
 - c. Click **Apply**.
2. Configure 1/0/1 as a routing port and assign an IP address to it.
 - a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

The screenshot shows the 'IP Interface Configuration' page. A table lists the configured interfaces:

Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input type="checkbox"/> 1/0/1			192.168.2.2	255.255.255.0	Enable	Enable
<input checked="" type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

- b. Under IP Interface Configuration, scroll down and select the Port **1/0/1** check box. Now 1/0/1 appears in the Port field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.2.2**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
3. Configure 1/0/9 as a routing port and assign an IP address to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

The screenshot shows the 'IP Interface Configuration' page. The table below lists the configuration for various ports. Port 1/0/9 is highlighted in orange, indicating it is selected.

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/>	1/0/9			192.168.3.1	255.255.255.0	Enable	Enable
<input type="checkbox"/>	1/0/1			192.168.2.2	255.255.255.0	Enable	Enable
<input type="checkbox"/>	1/0/2			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/>	1/0/3			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/>	1/0/4			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/>	1/0/5			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/>	1/0/6			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/>	1/0/7			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/>	1/0/8			0.0.0.0	0.0.0.0	Disable	Enable
<input checked="" type="checkbox"/>	1/0/9			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the Port **1/0/9** check box. Now 1/0/9 appears in the Port field at the top.

- c. Enter the following information :

- In the **IP Address** field, enter **192.168.3.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

- d. Click **Apply**.

4. Configure 1/0/13 as a routing port and assign an IP address to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

The screenshot shows the 'IP Interface Configuration' page. The table below lists the configuration for various ports. Port 1/0/13 is highlighted in orange, indicating it is selected.

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/>	1/0/13			192.168.1.2	255.255.255.0	Enable	Enable
<input type="checkbox"/>	1/0/1			192.168.2.2	255.255.255.0	Enable	Enable
<input type="checkbox"/>	1/0/2			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/>	1/0/3			0.0.0.0	0.0.0.0	Disable	Enable
<input type="checkbox"/>	1/0/4			0.0.0.0	0.0.0.0	Disable	Enable

- b. Under IP Interface Configuration, scroll down and select the Port **1/0/13** check box. Now 1/0/13 appears in the Port field at the top.

- c. Enter the following information:

- In the **IP Address** field, enter **192.168.1.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.

- In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
5. Enable RIP on the interface 1/0/1.
- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

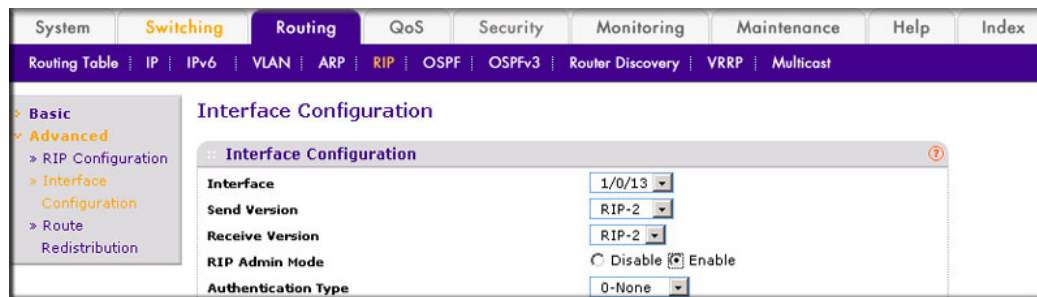


- b. In the **Interface** list, select **1/0/1**.
 - c. For RIP Admin Mode, select the **Enable** radio button.
 - d. Click **Apply**.
6. Enable RIP on interface 1/0/9.
- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

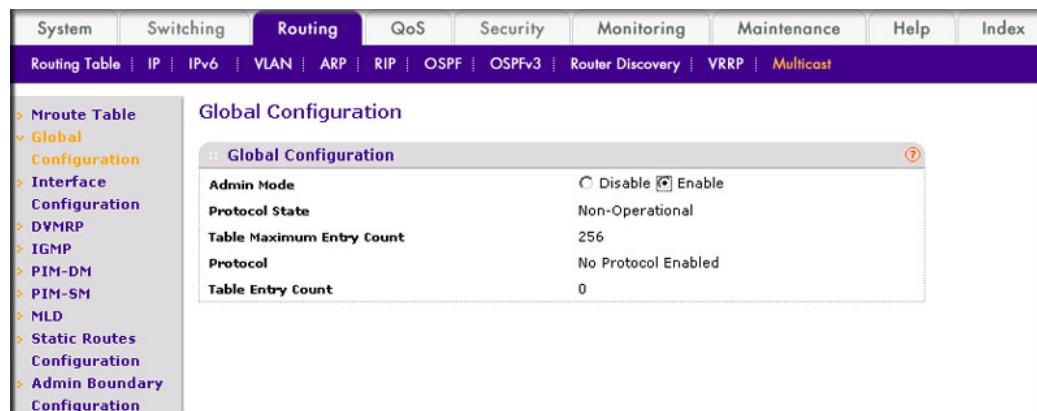


- b. In the **Interface** field, select **1/0/9**.
 - c. For RIP Admin Mode, select the **Enable** radio button.
 - d. Click **Apply**.
7. Enable RIP on interface 1/0/13.

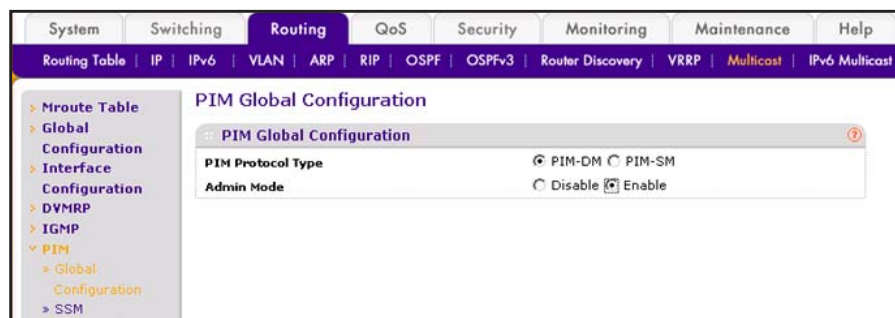
- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.



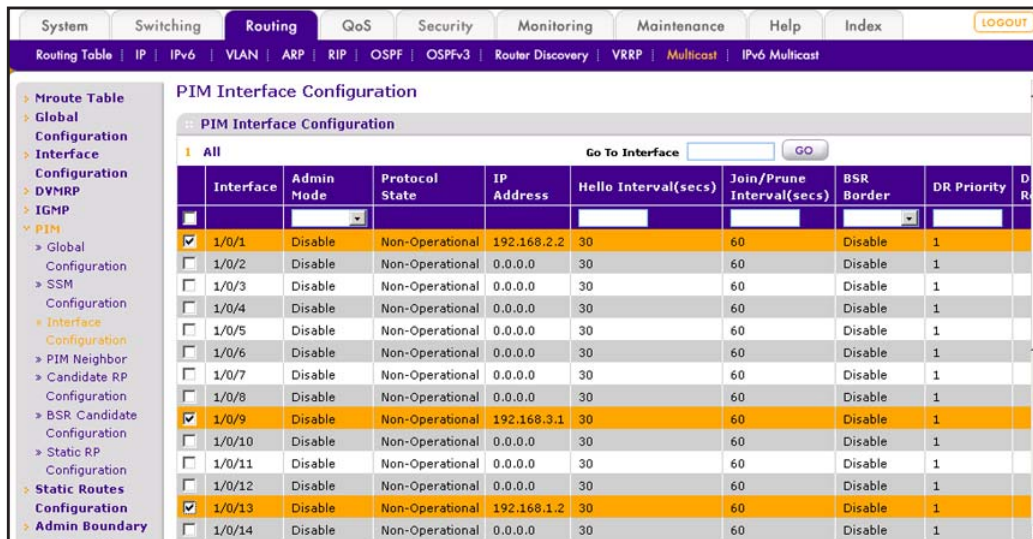
- b. In the **Interface** list, select **1/0/13**.
- c. For RIP Admin Mode, select the **Enable** radio button.
- d. Click **Apply**.
8. Enable multicast globally.
- a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.



- b. For Admin Mode, select the **Enable** radio button.
- c. Click **Apply**.
9. Enable PIM-DM globally.
- a. Select **Routing > Multicast > PIM > Global Configuration**. A screen similar to the following displays.



- b. For PIM Protocol Type, select the **PIM-DM** radio button.
 - c. For Admin Mode, select the **Enable** radio button.
 - d. Click **Apply**.
10. Enable PIM-DM on interfaces 1/0/1, 1/0/9, and 1/0/13.
- a. Select **Routing > Multicast > PIM > Interface Configuration**. A screen similar to the following displays.



- b. Under PIM Interface Configuration, scroll down and select the **1/0/1**, **1/0/9**, and **1/0/13** check boxes.
- c. In the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.

PIM-DM on Switch B:

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.

The screenshot shows the 'IP Configuration' page. The 'Routing Mode' is set to 'Enable'. The 'ICMP Echo Replies' and 'ICMP Redirects' are also set to 'Enable'. The 'ICMP Rate Limit Interval' is set to 1000 ms, and the 'ICMP Rate Limit Burst Size' is set to 100.

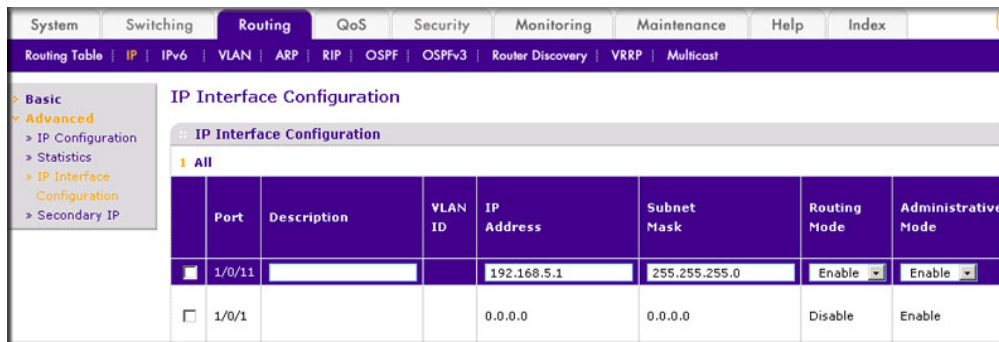
- b. For Routing Mode, select the **Enable** radio button.
 - c. Click **Apply**.
2. Configure 1/0/10 as a routing port and assign an IP address to it.
 - a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

The screenshot shows the 'IP Interface Configuration' page. The table below shows the configuration for interface 1/0/10.

Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/10			192.168.3.2	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

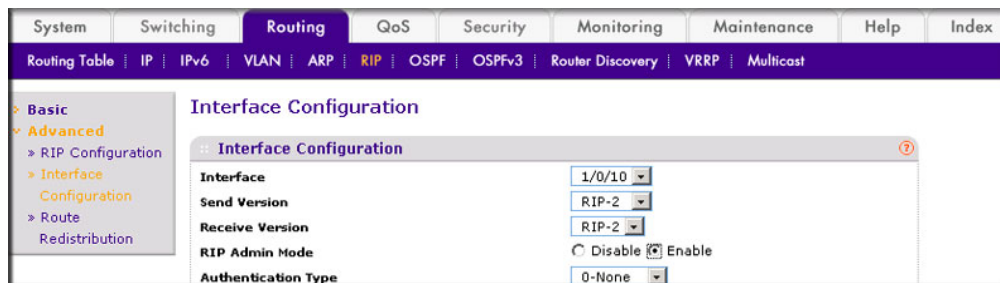
- b. Scroll down and select the Port **1/0/10** check box. Now 1/0/10 appears in the Port field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.3.2**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
3. Configure 1/0/11 as a routing port and assign an IP address to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Under IP Interface Configuration, scroll down and select the Port **1/0/11** check box. Now 1/0/11 appears in the Port field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.5.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
4. Enable RIP on interface 1/0/10.

- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

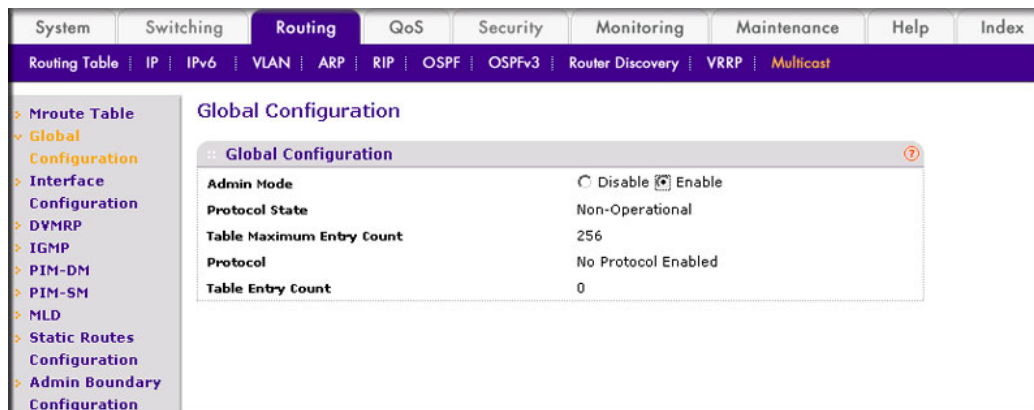


- b. In the **Interface** list, select **1/0/10**.
 - c. For RIP Admin Mode, select the **Enable** radio button.
 - d. Click **Apply**.
5. Enable RIP on interface 1/0/11.

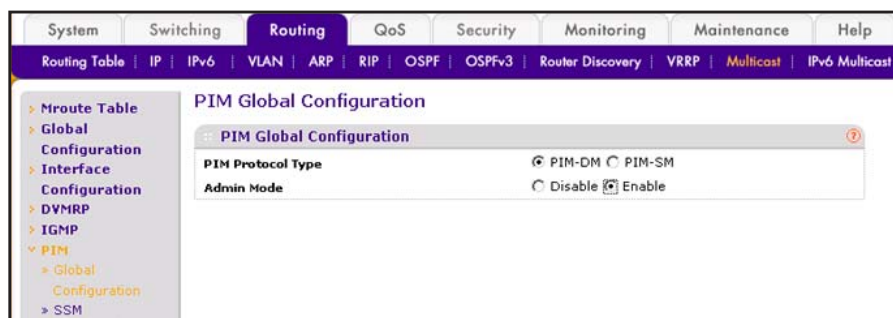
- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.



- b. In the **Interface** list, select **1/0/11**.
- c. For RIP Admin Mode, select the **Enable** radio button.
- d. Click **Apply**.
6. Enable multicast globally.
- a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.



- b. For Admin Mode, select the **Enable** radio button.
- c. Click **Apply**.
7. Enable PIM-DM globally.
- a. Select **Routing > Multicast > PIM > Global Configuration**. A screen similar to the following displays.



- b. For PIM Protocol Type, select the **PIM-DM** radio button.
 - c. For Admin Mode, select the **Enable** radio button.
 - d. Click **Apply**.
8. Enable PIM-SM on interfaces 1/0/10 and 1/0/11.
- a. Select **Routing > Multicast > PIM > Interface Configuration**. A screen similar to the following displays.

Interface	Admin Mode	Protocol Type	Address	Priority	Max Hops	Admin Distance	Operational Mode
1/0/5	<input type="checkbox"/>	Disable	Non-Operational	0.0.0.0	30	60	Disable 1
1/0/6	<input type="checkbox"/>	Disable	Non-Operational	0.0.0.0	30	60	Disable 1
1/0/7	<input type="checkbox"/>	Disable	Non-Operational	0.0.0.0	30	60	Disable 1
1/0/8	<input type="checkbox"/>	Disable	Non-Operational	0.0.0.0	30	60	Disable 1
1/0/9	<input type="checkbox"/>	Disable	Non-Operational	0.0.0.0	30	60	Disable 1
1/0/10	<input checked="" type="checkbox"/>	Disable	Non-Operational	192.168.3.2	30	60	Disable 1
1/0/11	<input checked="" type="checkbox"/>	Disable	Non-Operational	192.168.5.1	30	60	Disable 1
1/0/12	<input type="checkbox"/>	Disable	Non-Operational	0.0.0.0	30	60	Disable 1
1/0/13	<input type="checkbox"/>	Disable	Non-Operational	0.0.0.0	30	60	Disable 1
1/0/14	<input type="checkbox"/>	Disable	Non-Operational	0.0.0.0	30	60	Disable 1
1/0/15	<input type="checkbox"/>	Disable	Non-Operational	0.0.0.0	30	60	Disable 1
1/0/16	<input type="checkbox"/>	Disable	Non-Operational	0.0.0.0	30	60	Disable 1
1/0/17	<input type="checkbox"/>	Disable	Non-Operational	0.0.0.0	30	60	Disable 1
1/0/18	<input type="checkbox"/>	Disable	Non-Operational	0.0.0.0	30	60	Disable 1

- b. Scroll down and select the Interface **1/0/10** and **1/0/11** check box.
- c. In the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.

PIM-DM on Switch C

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.

IP Configuration

Default Time to Live: 64

Routing Mode: Disable **Enable**

ICMP Echo Replies: Disable **Enable**

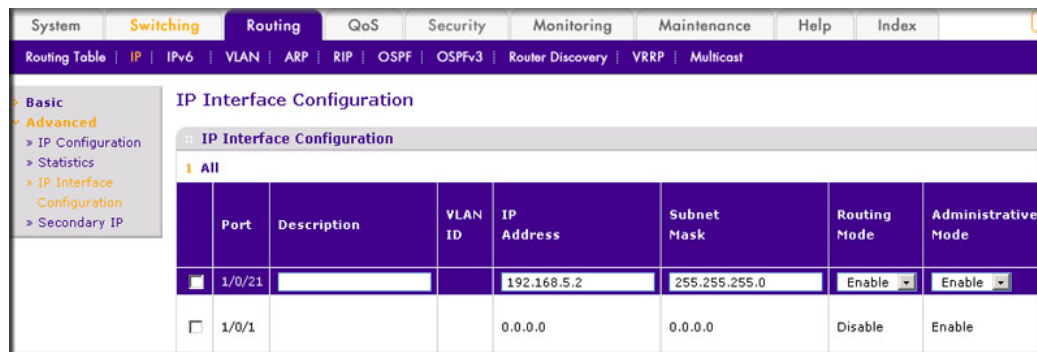
ICMP Redirects: Disable **Enable**

ICMP Rate Limit Interval: (0 to 2147483647 ms)

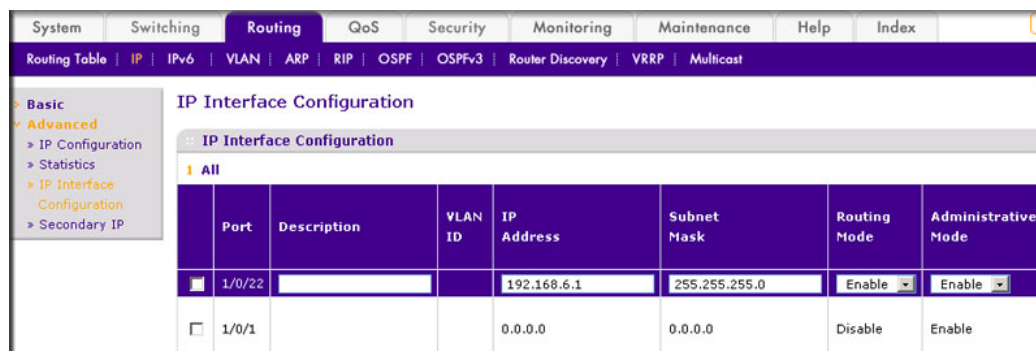
ICMP Rate Limit Burst Size: (1 to 200)

- b. For Routing Mode, select the **Enable** radio button.
 - c. Click **Apply**.
2. Configure 1/0/21 as a routing port and assign an IP address to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Scroll down select the Port **1/0/21** check box. Now 1/0/21 appears in the Interface field at the top.
- c. Enter the following information:
- In the **IP Address** field, enter **192.168.5.2**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
3. Configure 1/0/22 as a routing port and assign an IP address to it.
- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Port **1/0/22** check box. Now 1/0/22 appears in the Port field at the top.
- c. Enter the following information:
- In the **IP Address** field, enter **192.168.6.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
4. Enable RIP on interface 1/0/21.

- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

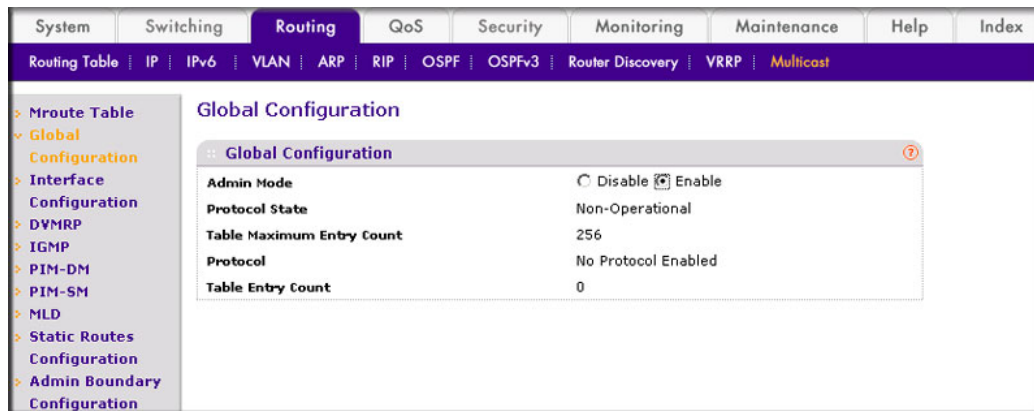


- b. In the **Interface** list, select **1/0/21**.
 - c. For RIP Admin Mode, select the **Enable** radio button.
 - d. Click **Apply**.
5. Enable RIP on interface 1/0/22.
 - a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

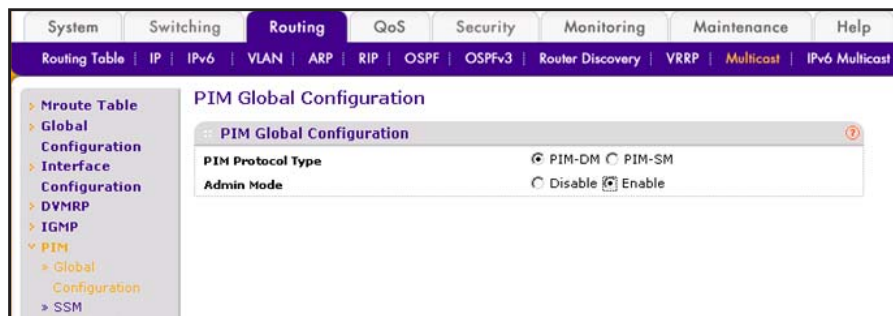


- b. In the **Interface** list, select **1/0/22**.
 - c. For RIP Admin Mode, select the **Enable** radio button.
 - d. Click **Apply**.
6. Enable multicast globally.

- a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.

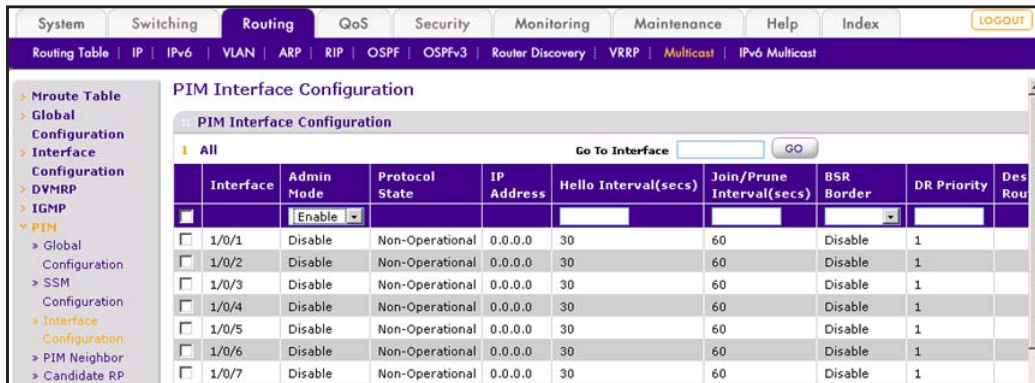


- b. For Admin Mode, select the **Enable** radio button.
- c. Click **Apply**.
7. Enable PIM-DM globally.
- a. Select **Routing > Multicast > PIM > Global Configuration**. A screen similar to the following displays.



- b. For PIM Protocol Type, select the **PIM-DM** radio button.
- c. For Admin Mode, select the **Enable** radio button.
- d. Click **Apply**.
8. Enable PIM-DM on interfaces 1/0/21 and 1/0/22.

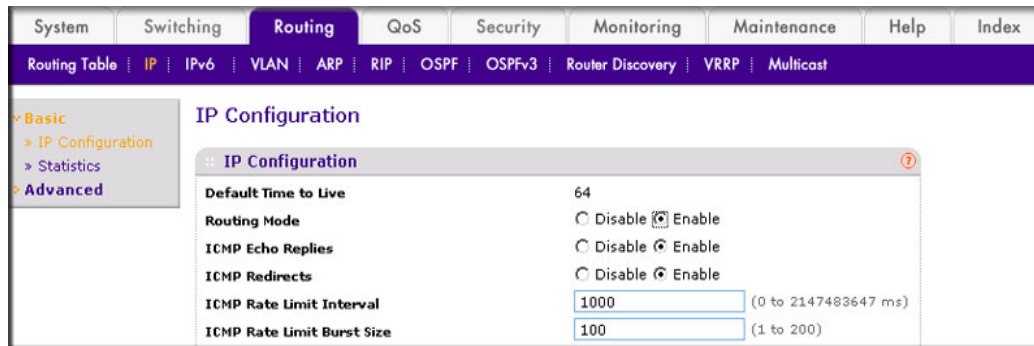
- a. Select **Routing > Multicast > PIM > Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the **1/0/21** and **1/0/22** check boxes.
- c. In the PIM Interface Configuration, in the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.

PIM-DM on Switch D:

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.



- b. For Routing Mode, select the **Enable** radio button.
- c. Click **Apply**.
2. Configure 1/0/21 as a routing port and assign an IP address to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

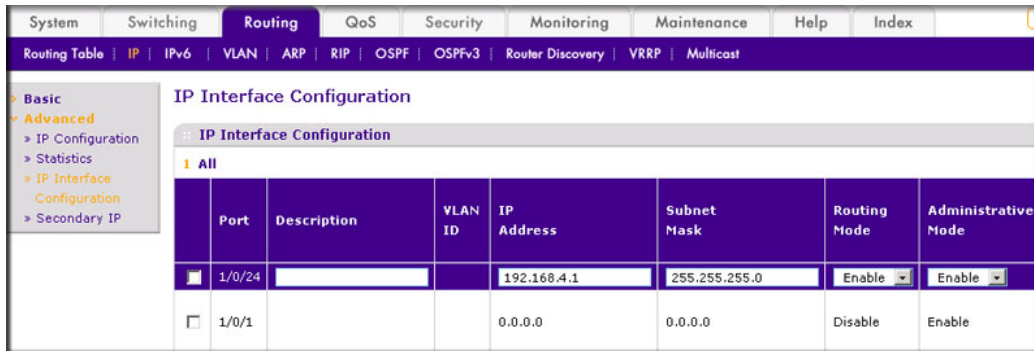
Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/21			192.168.2.1	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the Port **1/0/21** check box. Now 1/0/21 appears in the Port field at the top.
- c. Enter the following information in the IP Interface Configuration.
- In the **IP Address** field, enter **192.168.2.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
3. Configure 1/0/22 as a routing port and assign an IP address to it.
- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/22			192.168.6.2	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the Port **1/0/22** check box. Now 1/0/22 appears in the Interface field at the top.
- c. Enter the following information:
- In the **IP Address** field, enter **192.168.6.2**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
4. Configure 1/0/24 as a routing port and assign an IP address to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Port **1/0/24** check box. Now 1/0/24 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.4.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
5. Enable RIP on interface 1/0/21.
 - a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.



- b. In the **Interface** list, select t **1/0/21**.
 - c. For RIP Admin Mode, select the **Enable** radio button.
 - d. Click **Apply**.
6. Enable RIP on interface 1/0/22.

- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

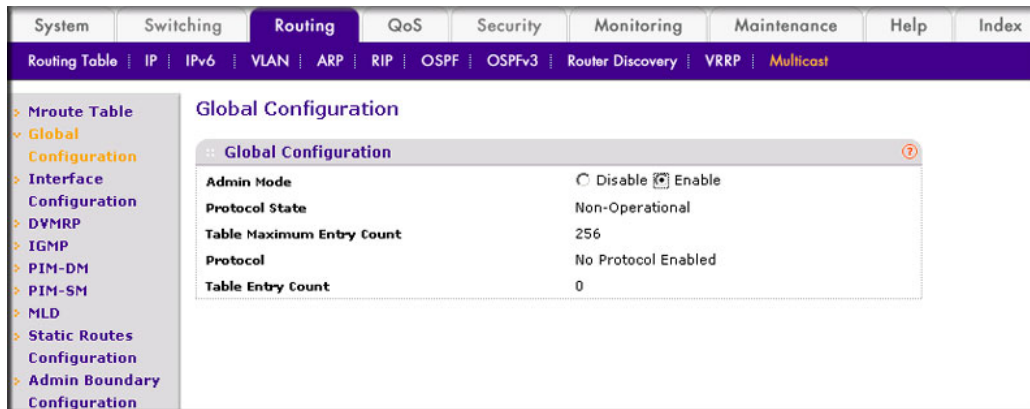
Interface Configuration	
Interface	1/0/22
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Authentication Type	0-None

- b. In the **Interface** list, select **1/0/22**.
- c. For RIP Admin Mode, select the **Enable** radio button.
- d. Click **Apply**.
7. Enable RIP on interface 1/0/24.
- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

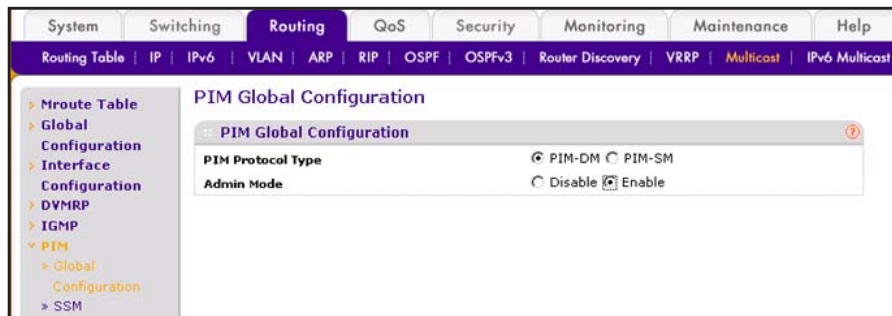
Interface Configuration	
Interface	1/0/24
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Authentication Type	0-None

- b. In the **Interface** list, select **1/0/24**.
- c. For RIP Admin Mode, select the **Enable** radio button.
- d. Click **Apply**.
8. Enable multicast globally.

- a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.

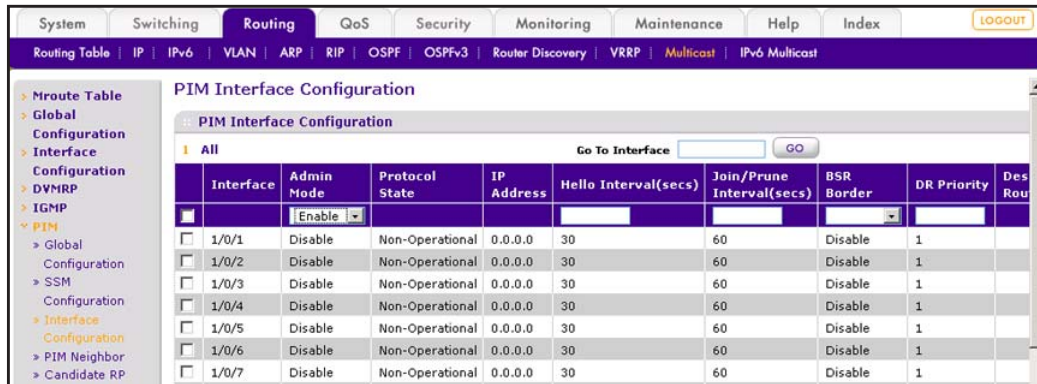


- b. For Admin Mode, select the **Enable** radio button.
- c. Click **Apply**.
9. Enable PIM-DM globally.
- a. Select **Routing > Multicast > PIM > Global Configuration**. A screen similar to the following displays.



- b. For PIM Protocol Type, select the **PIM-SM** radio button.
- c. For Admin Mode, select the **Enable** radio button.
- d. Click **Apply**.
10. Enable PIM-DM on interfaces 1/0/21, 1/0/22, and 1/0/24.

- a. Select **Routing > Multicast > PIM > Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Interface **1/0/21**, **1/0/22**, and **1/0/24** check boxes.
- c. In the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.

11. Enable IGMP globally.

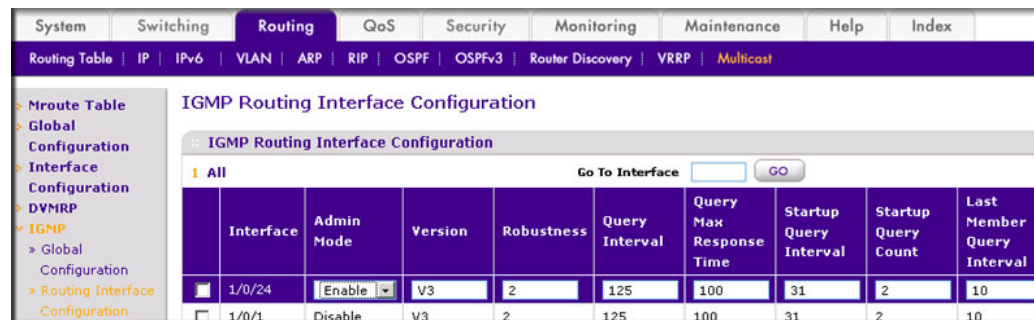
- a. Select **Routing > Multicast > IGMP > Global Configuration**. A screen similar to the following displays.



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

12. Enable IGMP on interface 1/0/24.

- a. Select **Routing > Multicast > IGMP > Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the interface **1/0/24** check box.
- c. In the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.

PIM-SM

Protocol-independent multicast sparse mode (PIM-SM) is used to efficiently route multicast traffic to multicast groups that can span wide area networks where bandwidth is a constraint.

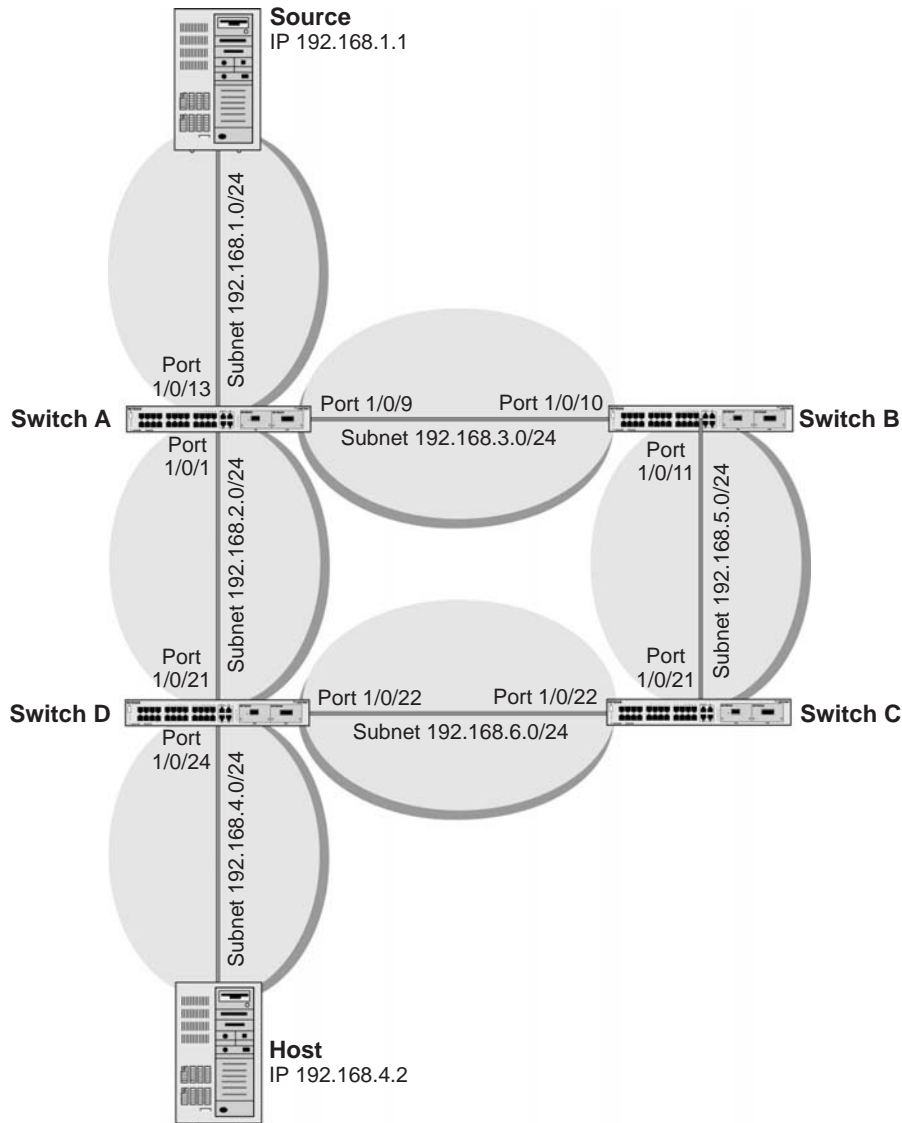


Figure 46. PIM-SM

PIM-SM uses shared trees by default and implements source-based trees for efficiency; it assumes that no hosts want the multicast traffic unless they specifically ask for it. It creates a shared distribution tree centered on a defined rendezvous point (RP). Traffic from this source

is relayed to the receivers. Senders first send the multicast data to the RP, which in turn sends the data down the shared tree to the receivers. Shared trees centered on an RP do not necessarily provide the shortest, most optimal path. In such cases PIM-SM provides a means to switch to more efficient source-specific trees. A data threshold rate is defined for toggling between trees. PIM-SM uses a bootstrap router (BSR), which advertises information to other multicast routers about the RP. In a given network, a set of routers can be administratively enabled as candidate bootstrap routers. If it is not apparent which router should be the BSR, the candidates flood the domain with advertisements. The router with the highest priority is elected. If all the priorities are equal, then the candidate with the highest IP address becomes the BSR. PIM-SM is defined in RFC 4601.

The following example describes how to configure and use PIM-SM. In this case, set the switch B,C,D as RP-candidate and BSR-candidate. Switch B will become the BSR because it has the highest priority. Switch D will become the RP after RP election.

CLI: Configure PIM-SM

PIM-SM on Switch A

1. Enable IP routing on the switch.

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

2. Enable PIM-SM on the switch.

```
(Netgear Switch) (Config)#ip pim sparse
```

3. Enable IP multicast forwarding on the switch.

```
(Netgear Switch) (Config)#ip multicast
```

4. Enable RIP to build a unicast IP routing table.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.2.2 255.255.255.0
(Netgear Switch) (Interface 1/0/1)#ip rip
```

```
(Netgear Switch) (Interface 1/0/1)#ip pim sparse
(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 sparse
(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 sparse
(Netgear Switch) (Interface 1/0/1)#exit
```

PIM-SM on Switch B

1. Enable the switch to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

```
(Netgear Switch)#configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim sparse
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#ip pim sparse rp-candidate interface 1/0/11 225.1.1.1
255.255.255.0
```

2. Enable the switch to announce its candidacy as a bootstrap router (BSR).

```
(Netgear Switch) (Config)#ip pim sparse bsr-candidate interface 1/0/10 30 7

(Netgear Switch) (Config)#interface 1/0/10
(Netgear Switch) (Interface 1/0/10)#routing
(Netgear Switch) (Interface 1/0/10)#ip address 192.168.3.2 255.255.255.0
(Netgear Switch) (Interface 1/0/10)#ip rip
(Netgear Switch) (Interface 1/0/10)#ip pim sparse
(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 sparse
(Netgear Switch) (Interface 1/0/11)#exit
```

PIM-SM on Switch C

```
(Netgear Switch)#configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim sparse
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#ip pim sparse rp-candidate interface 1/0/22 225.1.1.1
255.255.255.0
(Netgear Switch) (Config)#ip pim sparse bsr-candidate interface 1/0/21 30 5
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address 192.168.5.2 255.255.255.0
(Netgear Switch) (Interface 1/0/21)#ip rip
(Netgear Switch) (Interface 1/0/21)#ip pim sparse
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) (Config)#interface 1/0/22
(Netgear Switch) (Interface 1/0/22)#routing
(Netgear Switch) (Interface 1/0/22)#ip address 192.168.6.1 255.255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22)#ip pim sparse
(Netgear Switch) (Interface 1/0/22)#exit
```

PIM-SM on Switch D

```
(Netgear Switch)#configure
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip igmp
(Netgear Switch) (Config)#ip pim sparse
(Netgear Switch) (Config)#ip pim rp-candidate interface 1/0/22 225.1.1.1 255.255.255.0
(Netgear Switch) (Config)#ip pim bsr-candidate interface 1/0/22 30 3
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address 192.168.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/21)#ip rip
(Netgear Switch) (Interface 1/0/21)#ip pim sparse
(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 sparse
(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 sparse
(Netgear Switch) (Interface 1/0/24)#exit
```

PIM-SM builds the multicast route table on each switch. The following tables show the routes that are built after PIM-SM switches to the source-specific tree from the shared tree.

```
(A) #show ip mcast mroute summary
      Multicast Route Table Summary
      Incoming      Outgoing
Source IP      Group IP      Protocol      Interface      Interface List
-----
192.168.1.1    225.1.1.1    PIMSM        1/0/13        1/0/1

(B) #show ip mcast mroute summary
      Multicast Route Table Summary
      Incoming      Outgoing
Source IP      Group IP      Protocol      Interface      Interface List
-----
192.168.1.1    225.1.1.1    PIMSM        1/0/10

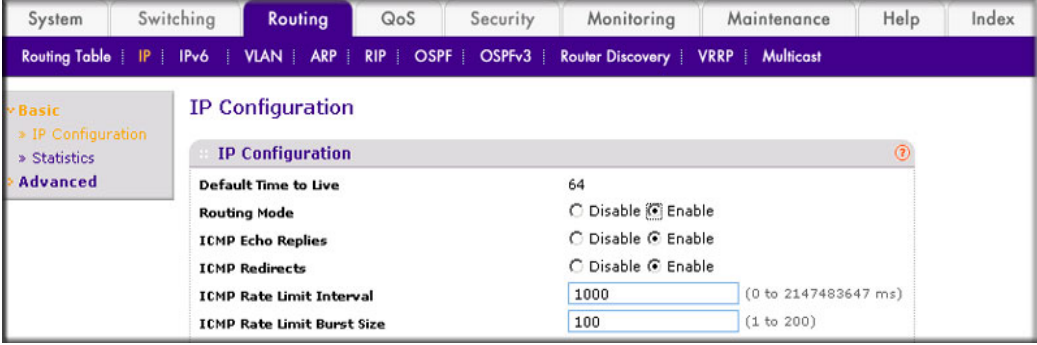
(C) #show ip mcast mroute summary
      Multicast Route Table Summary
      Incoming      Outgoing
Source IP      Group IP      Protocol      Interface      Interface List
-----
*              225.1.1.1    PIMSM        1/0/22
192.168.1.1    225.1.1.1    PIMSM        1/0/21

(D) #show ip mcast mroute summary
      Multicast Route Table Summary
      Incoming      Outgoing
Source IP      Group IP      Protocol      Interface      Interface List
-----
*              225.1.1.1    PIMSM        1/0/22        1/0/24
192.168.1.1    225.1.1.1    PIMSM        1/0/21        1/0/24
```

Web Interface: Configure PIM-SM

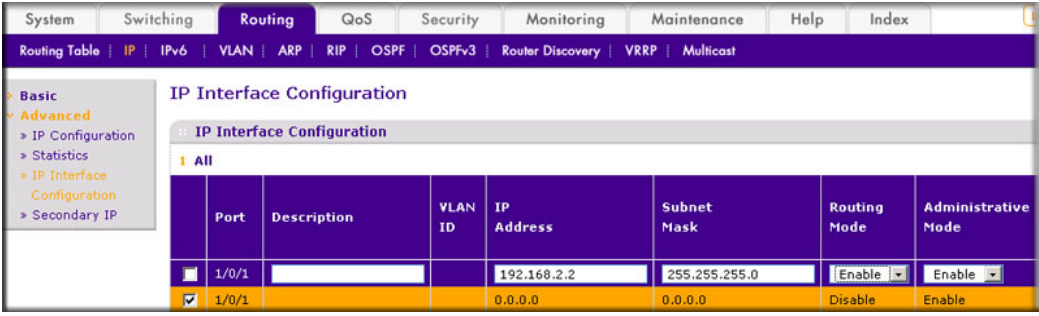
PIM-SM on Switch A

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.



The screenshot shows the 'IP Configuration' page in the web interface. The 'Routing Mode' is set to 'Enable' (radio button selected). Other settings include 'Default Time to Live' at 64, 'ICMP Echo Replies' at 'Enable', 'ICMP Redirects' at 'Enable', 'ICMP Rate Limit Interval' at 1000, and 'ICMP Rate Limit Burst Size' at 100.

- b. For Routing Mode, select the **Enable** radio button.
 - c. Click **Apply**.
2. Configure 1/0/1 as a routing port and assign an IP address to it.
 - a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

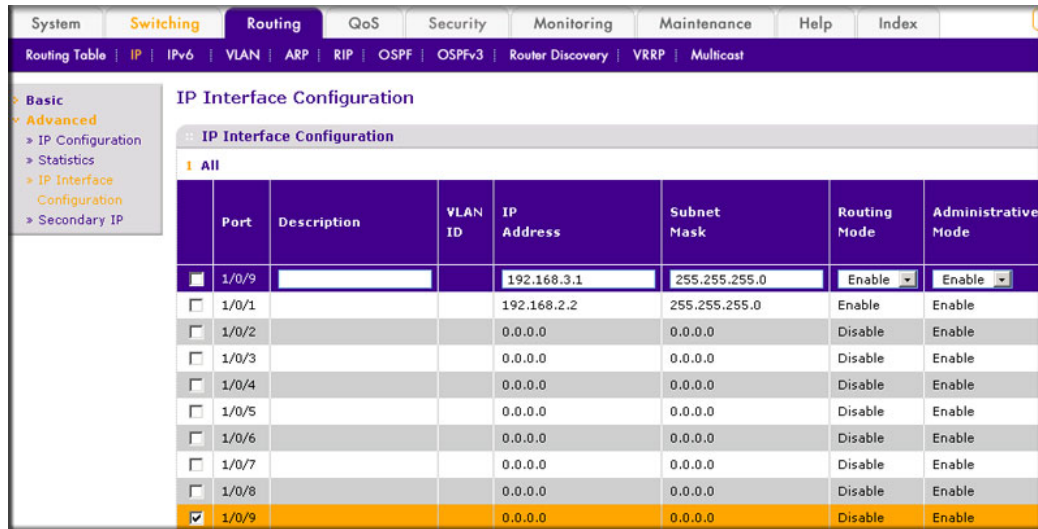


The screenshot shows the 'IP Interface Configuration' page. A table lists the interfaces, and the configuration for interface 1/0/1 is shown below. The configuration includes IP Address (192.168.2.2), Subnet Mask (255.255.255.0), Routing Mode (Enable), and Administrative Mode (Enable).

Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input type="checkbox"/>	1/0/1		192.168.2.2	255.255.255.0	Enable	Enable
<input checked="" type="checkbox"/>	1/0/1		0.0.0.0	0.0.0.0	Disable	Enable

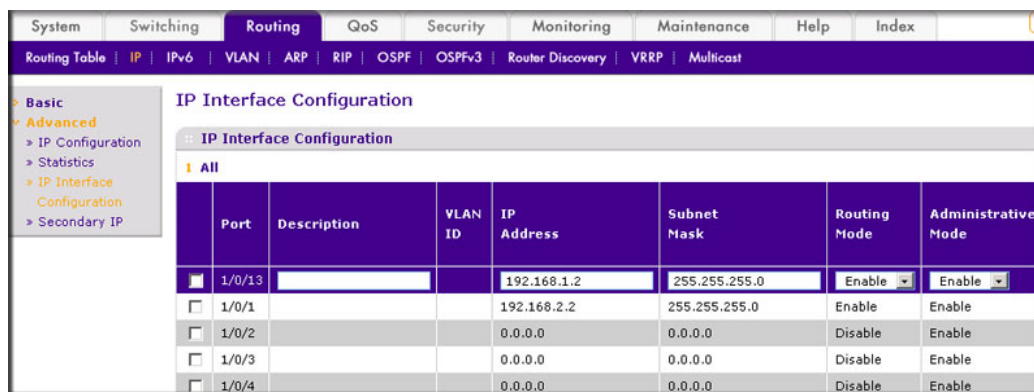
- b. Scroll down and select the interface **1/0/1** check box. Now 1/0/1 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.2.2**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
3. Configure 1/0/9 as a routing port and assign an IP address to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the interface **1/0/9** check box. Now 1/0/9 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.3.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply**.
4. Configure 1/0/13 as a routing port and assign an IP address to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the interface **1/0/13** check box. Now 1/0/13 appears in the Interface field at the top.
- c. Enter the following information:
 - In the **IP Address** field, enter **192.168.1.2**.

- In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
5. Enable RIP on interface 1/0/1.
- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.



- b. In the **Interface** field, select **1/0/1**.
- c. For RIP Admin Mode, select the **Enable** radio button.
- d. Click **Apply**.
6. Enable RIP on interface 1/0/9.
- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

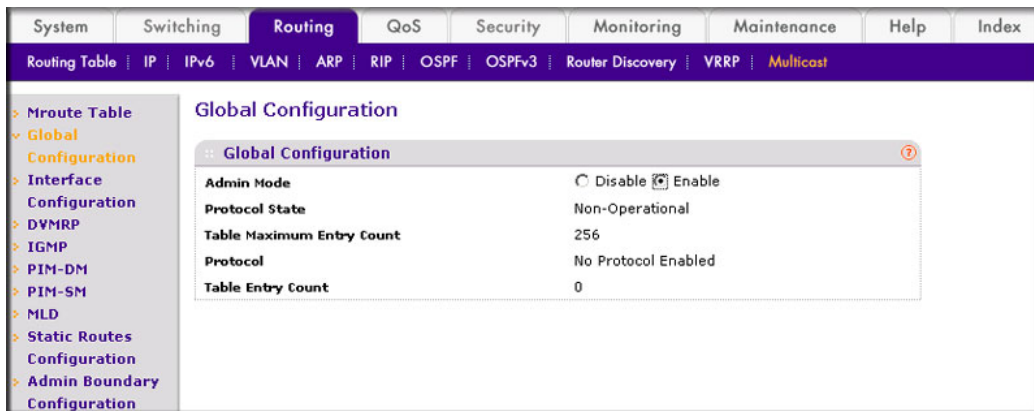


- b. In the **Interface** field, select **1/0/9**.
- c. For RIP Admin Mode, select the **Enable** radio button.
- d. Click **Apply**.
7. Enable RIP on interface 1/0/13.

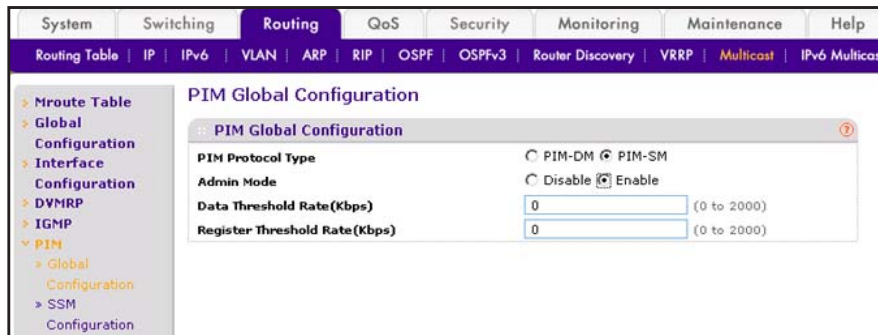
- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.



- b. Select **1/0/13** in the **Interface** field.
 - c. For RIP Admin Mode, select the **Enable** radio button.
 - d. Click **Apply**.
8. Enable multicast globally.
 - a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.



- b. For Admin Mode, select the **Enable** radio button.
 - c. Click **Apply**.
9. Enable PIM-SM globally.
 - a. Select **Routing > Multicast > PIM > Global Configuration**. A screen similar to the following displays.



- b. For PIM Protocol Type, select the **PIM-SM** radio button.
 - c. For Admin Mode, select the **Enable** radio button.
 - d. Click **Apply**.
10. Enable PIM-SM on interfaces 1/0/1, 1/0/9, and 1/0/13.
- a. Select **Routing > Multicast > PIM > Interface Configuration**. A screen similar to the following displays.

Interface	Admin Mode	Protocol State	IP Address	Hello Interval(secs)	Join/Prune Interval(secs)	BSR Border	DR Priority
<input checked="" type="checkbox"/> 1/0/1	Disable	Non-Operational	192.168.2.2	30	60	Disable	1
<input type="checkbox"/> 1/0/2	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
<input type="checkbox"/> 1/0/3	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
<input type="checkbox"/> 1/0/4	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
<input type="checkbox"/> 1/0/5	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
<input type="checkbox"/> 1/0/6	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
<input type="checkbox"/> 1/0/7	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
<input type="checkbox"/> 1/0/8	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
<input checked="" type="checkbox"/> 1/0/9	Disable	Non-Operational	192.168.3.1	30	60	Disable	1
<input type="checkbox"/> 1/0/10	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
<input type="checkbox"/> 1/0/11	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
<input type="checkbox"/> 1/0/12	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
<input checked="" type="checkbox"/> 1/0/13	Disable	Non-Operational	192.168.1.2	30	60	Disable	1
<input type="checkbox"/> 1/0/14	Disable	Non-Operational	0.0.0.0	30	60	Disable	1

- b. Scroll down and select the Interface **1/0/1**, **1/0/9**, and **1/0/13** check boxes.
- c. In the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.

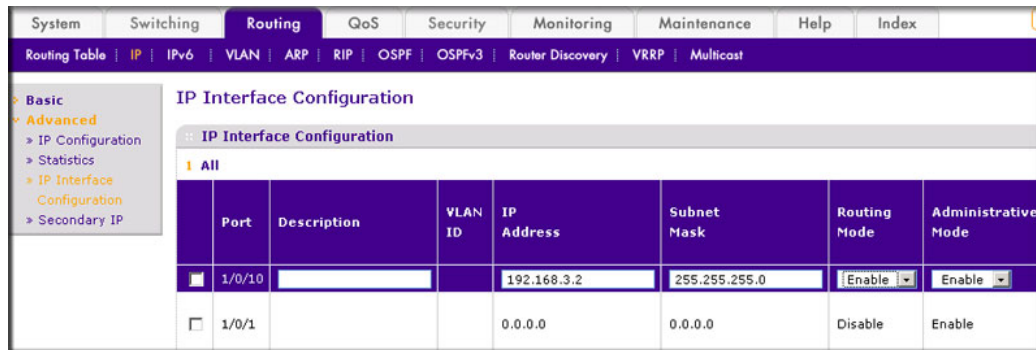
PIM-SM on Switch B:

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.

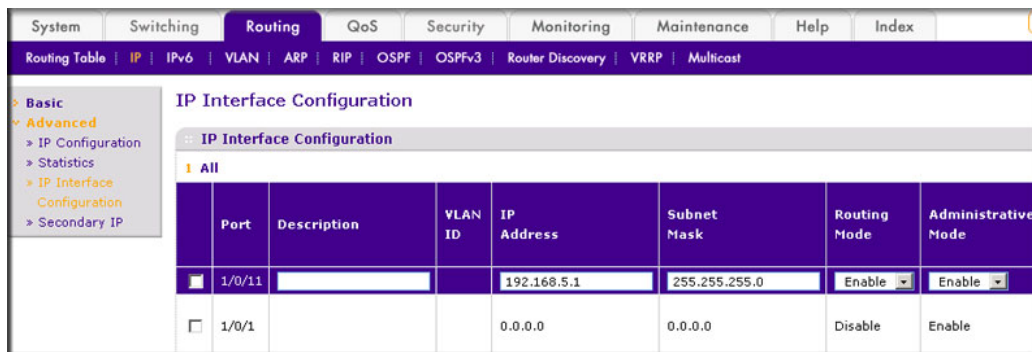
Default Time to Live	64
Routing Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
ICMP Echo Replies	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
ICMP Redirects	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
ICMP Rate Limit Interval	1000 (0 to 2147483647 ms)
ICMP Rate Limit Burst Size	100 (1 to 200)

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

2. Configure 1/0/10 as a routing port and assign an IP address to it.
 - a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the interface **1/0/10** check box. Now 1/0/10 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.3.2**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
3. Configure 1/0/11 as a routing port and assign an IP address to it.
 - a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Port **1/0/11** check box. Now 1/0/11 appears in the Port field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.5.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
4. Enable RIP on interface 1/0/10.

- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

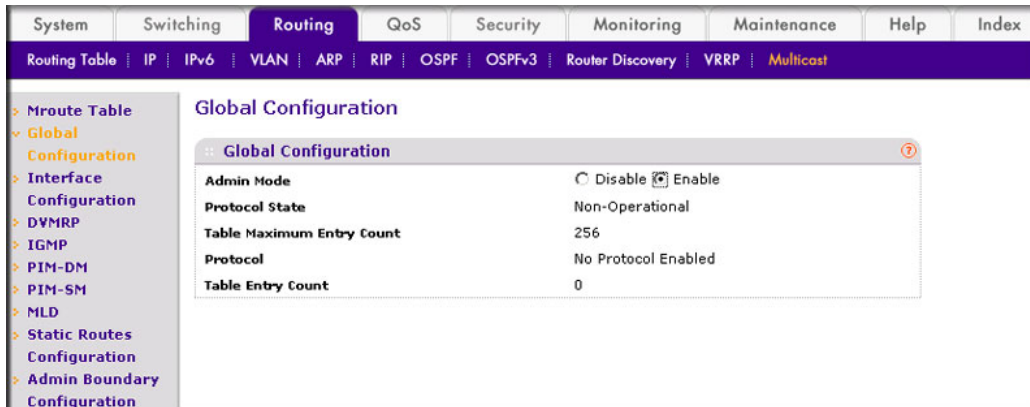


- b. In the **Interface** field, select **1/0/10**.
- c. For RIP Admin Mode, select the **Enable** radio button.
- d. Click **Apply**.
5. Enable RIP on interface 1/0/11.
- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

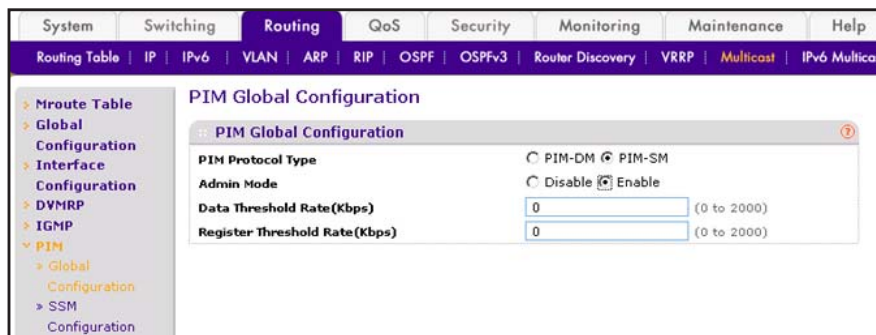


- b. In the **Interface** list, select **1/0/11**.
- c. For RIP Admin Mode, select the **Enable** radio button.
- d. Click **Apply**.
6. Enable multicast globally.

- a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.



- b. For Admin Mode, select the **Enable** radio button.
 - c. Click **Apply**.
7. Enable PIM-SM globally.
 - a. Select **Routing > Multicast > PIM > Global Configuration**. A screen similar to the following displays.



- b. For PIM Protocol Type, select the **PIM-SM** radio button.
 - c. For Admin Mode, select the **Enable** radio button.
 - d. Click **Apply**.
8. Enable PIM-SM on interfaces 1/0/10 and 1/0/11.

- a. Select **Routing > Multicast > PIM > Interface Configuration**. A screen similar to the following displays.

Interface	Admin Mode	Protocol State	IP Address	Hello Interval(secs)	Join/Prune Interval(secs)	BSR Border	DR Priority	DR
<input type="checkbox"/> 1/0/1	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	
<input type="checkbox"/> 1/0/2	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	
<input type="checkbox"/> 1/0/3	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	
<input type="checkbox"/> 1/0/4	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	
<input type="checkbox"/> 1/0/5	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	
<input type="checkbox"/> 1/0/6	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	
<input type="checkbox"/> 1/0/7	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	
<input type="checkbox"/> 1/0/8	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	
<input type="checkbox"/> 1/0/9	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	
<input checked="" type="checkbox"/> 1/0/10	Enable	Non-Operational	192.168.3.2	30	60	Disable	1	
<input checked="" type="checkbox"/> 1/0/11	Enable	Non-Operational	192.168.5.1	30	60	Disable	1	
<input type="checkbox"/> 1/0/12	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	
<input type="checkbox"/> 1/0/13	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	
<input type="checkbox"/> 1/0/14	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	

- b. Scroll down and select the Interface **1/0/10** and **1/0/11** check boxes.
- c. In the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
9. Set up the candidate RP configuration.
- a. Select **Routing > Multicast > PIM > Candidate RP Configuration**. A screen similar to the following displays.

PIM Candidate RP Configuration

PIM Interface Selection

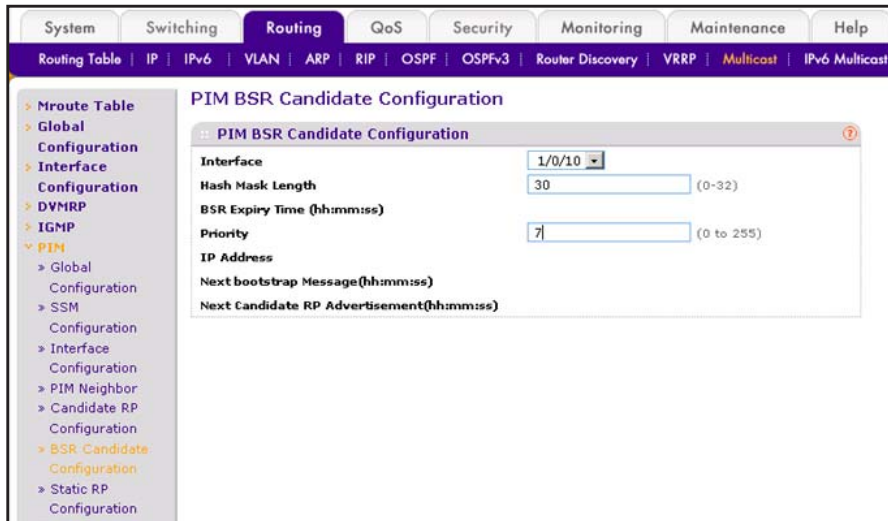
Interface: 1/0/11

PIM Candidate RP Configuration

Group Address	Group Mask
225.1.1.1	255.255.255.0

- b. In the **Interface** list, select **1/0/11**.
- c. In the **Group IP** field, enter **225.1.1.1**.
- d. In the **Group Mask** field, enter **255.255.255.0**.
- e. Click **Add**.
10. Set up the BSR candidate configuration.

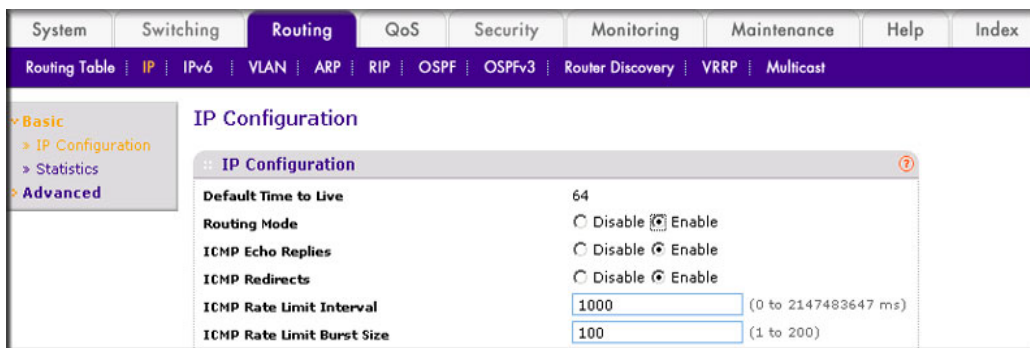
- a. Select **Routing > Multicast > PIM > BSR Candidate Configuration**. A screen similar to the following displays.



- b. In the **Interface** list, select the **1/0/10**.
- c. In the **Hash Mask Length** field, enter **30**.
- d. In the **Priority** field, enter **7**.
- e. Click **Apply**.

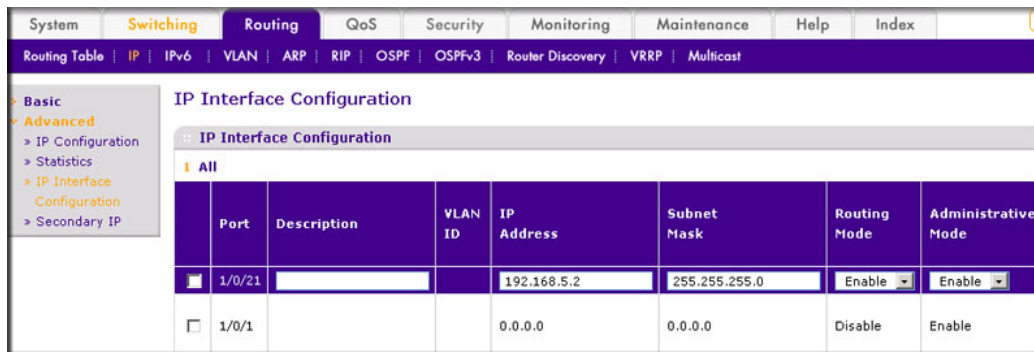
PIM-SM on Switch C:

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.

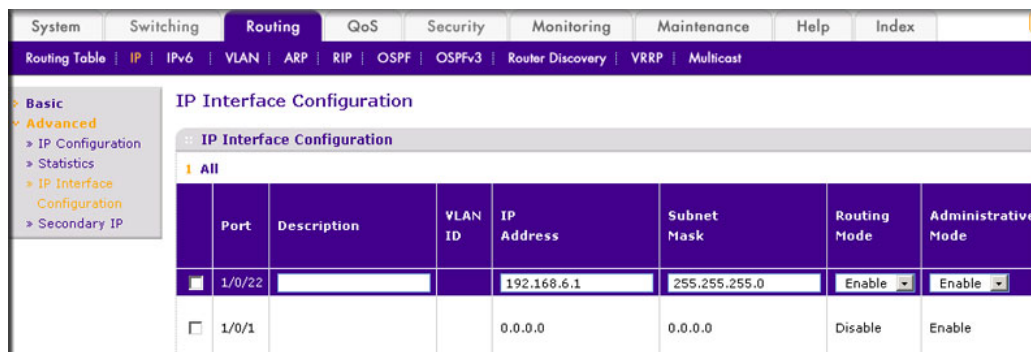


- b. For Routing Mode, select the **Enable** radio button.
- c. Click **Apply**.
2. Configure 1/0/21 as a routing port and assign an IP address to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

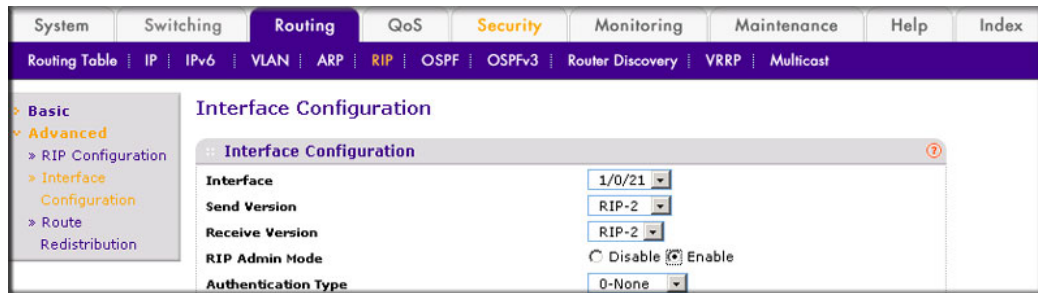


- b. Scroll down and select the Port **1/0/21** check box. Now 1/0/21 appears in the Interface field at the top.
- c. Enter the following information:
- In the **IP address**, enter **192.168.5.2**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
3. Configure 1/0/22 as a routing port and assign an IP address to it.
- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the **1/0/22** check box. Now 1/0/22 appears in the Interface field at the top.
- c. Enter the following information:
- In the **IP Address** field, enter **192.168.6.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
4. Enable RIP on the interface 1/0/21.

- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

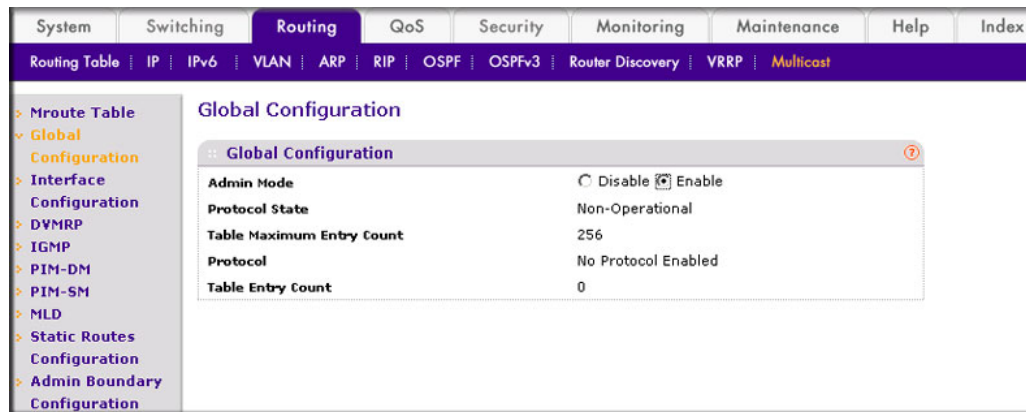


- b. In the **Interface** field, select **1/0/21**.
 - c. For RIP Admin Mode, select the **Enable** radio button.
 - d. Click **Apply**.
5. Enable RIP on interface 1/0/22.
 - a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

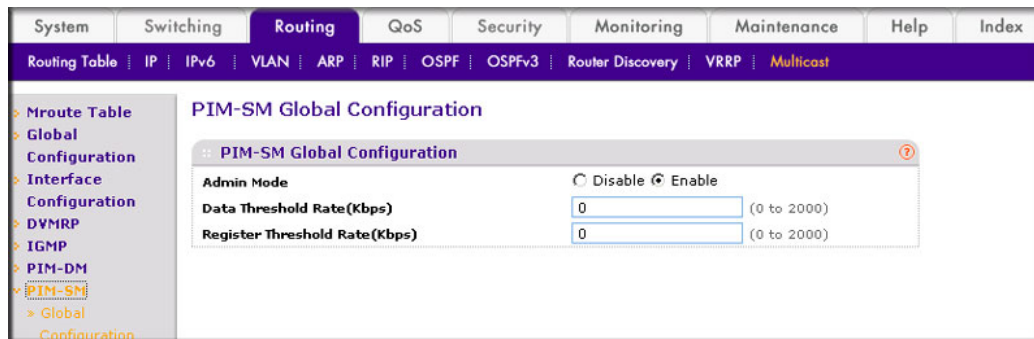


- b. In the **Interface** list, select **1/0/22**.
 - c. For RIP Admin Mode, select the **Enable** radio button.
 - d. Click **Apply**.
6. Enable multicast globally.

- a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.

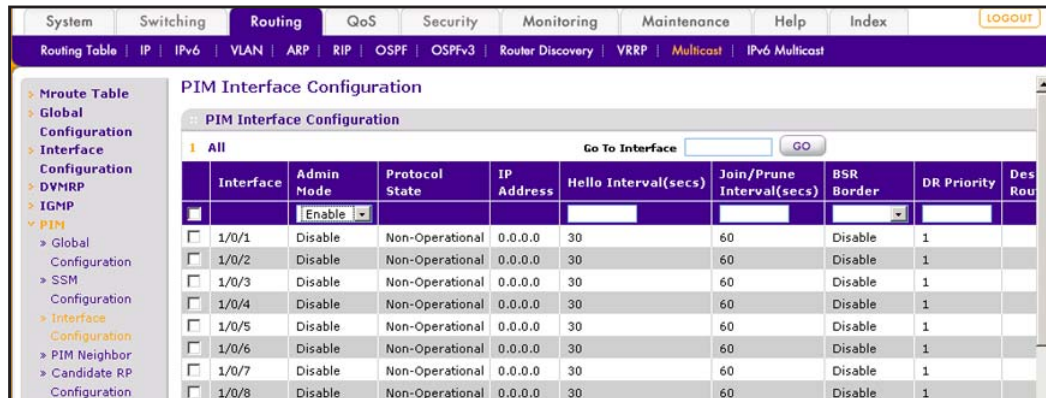


- b. For Admin Mode, select the **Enable** radio button.
- c. Click **Apply**.
7. Enable PIM-SM globally.
- a. Select **Routing > Multicast > PIM > Global Configuration**. A screen similar to the following displays.

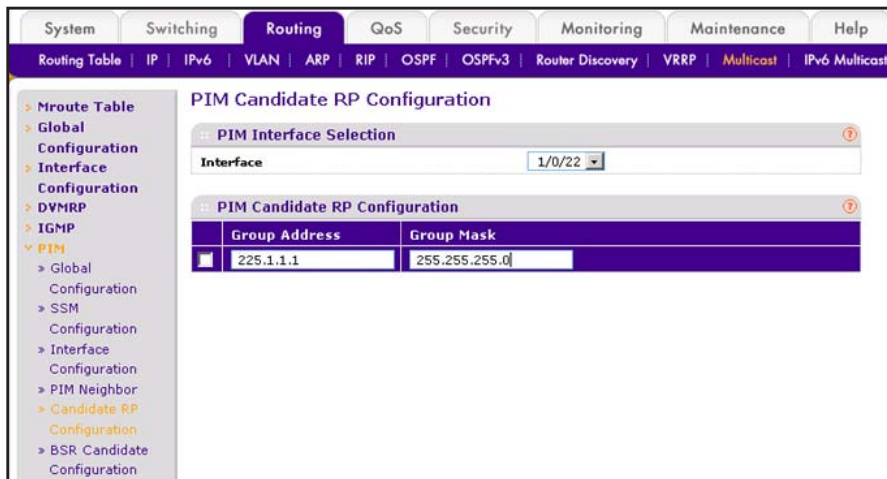


- b. For PIM Protocol Type, select the **PIM-SM** radio button.
- c. For Admin Mode, select the **Enable** radio button.
- d. Click **Apply**.
8. Enable PIM-SM on interfaces 1/0/21 and 1/0/22.

- a. Select **Routing > Multicast > PIM > Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Interface **1/0/21** and **1/0/22** check boxes.
 - c. In the **Admin Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
9. Candidate RP Configuration.
 - a. Select **Routing > Multicast > PIM > Candidate RP Configuration**. A screen similar to the following displays.



- b. In the **Interface** list, select **1/0/22**.
 - c. In the **Group IP** field, enter **225.1.1.1**.
 - d. In the **Group Mask** field, enter **255.255.255.0**.
 - e. Click **Add**.
10. BSR Candidate Configuration.

- a. Select **Routing > Multicast > PIM > BSR Candidate Configuration**. A screen similar to the following displays.

The screenshot shows the 'PIM BSR Candidate Configuration' page. The interface includes a top navigation bar with tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, and Help. Below this is a sub-navigation bar with links for Routing Table, IP, IPv6, VLAN, ARP, RIP, OSPF, OSPFv3, Router Discovery, VRRP, Multicast, and IPv6 Multicast. A left sidebar contains a tree view with categories like Mroute Table, Global Configuration, Interface Configuration, DVMRP, IGMP, PIM, and BSR Candidate Configuration. The main content area is titled 'PIM BSR Candidate Configuration' and contains the following fields:

Interface	1/0/21	
Hash Mask Length	30	(0-32)
BSR Expiry Time (hh:mm:ss)		
Priority	5	(0 to 255)
IP Address		
Next bootstrap Message(hh:mm:ss)		
Next Candidate RP Advertisement(hh:mm:ss)		

- b. In the **Interface** list, select the **1/0/21**.
- c. In the **Hash Mask Length** field, enter **30**.
- d. In the **Priority** field, enter **5**.
- e. Click **Apply**.

PIM-SM on Switch D

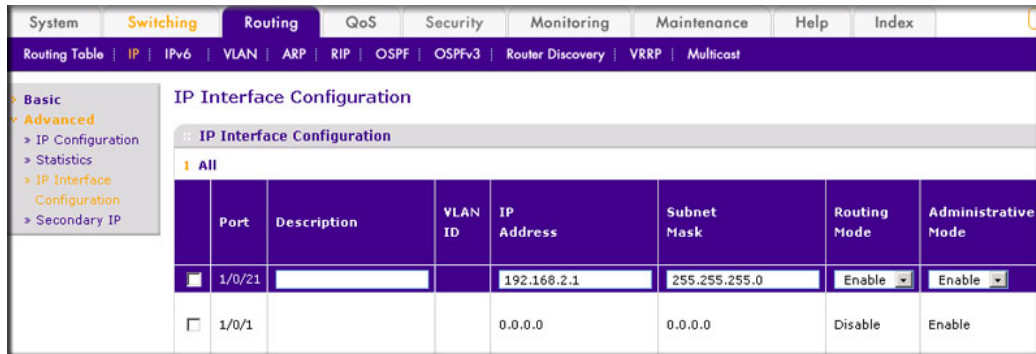
1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.

The screenshot shows the 'IP Configuration' page. The interface includes a top navigation bar with tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. Below this is a sub-navigation bar with links for Routing Table, IP, IPv6, VLAN, ARP, RIP, OSPF, OSPFv3, Router Discovery, VRRP, and Multicast. A left sidebar contains a tree view with categories like Basic, IP Configuration, Statistics, and Advanced. The main content area is titled 'IP Configuration' and contains the following fields:

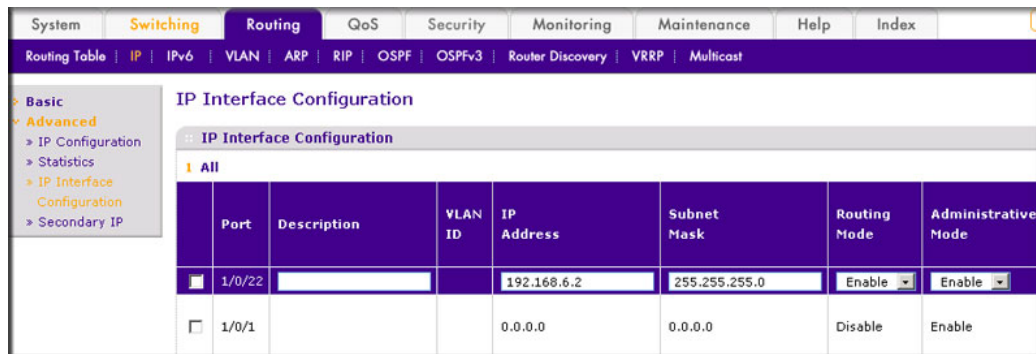
Default Time to Live	64
Routing Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
ICMP Echo Replies	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
ICMP Redirects	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
ICMP Rate Limit Interval	1000 (0 to 2147483647 ms)
ICMP Rate Limit Burst Size	100 (1 to 200)

- b. For Routing Mode, select the **Enable** radio button.
- c. Click **Apply**.
2. Configure 1/0/21 as a routing port and assign an IP address to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Interface **1/0/21** check box. Now 1/0/21 appears in the Interface field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.2.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
3. Configure 1/0/22 as a routing port and assign an IP address to it.
 - a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Port **1/0/22** check box. Now 1/0/22 appears in the Port field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.6.2**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
4. Configure 1/0/24 as a routing port and assign an IP address to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/>			192.168.4.1	255.255.255.0	Enable	Enable
<input type="checkbox"/>			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the Interface **1/0/24** check box. Now 1/0/24 appears in the Interface field at the top.
- c. Enter the following information:
- In the **IP Address** field, enter **192.168.4.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
5. Enable RIP on interface 1/0/21.
- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

Interface	1/0/21
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Authentication Type	0-None

- b. In the **Interface** list, select **1/0/21**.
- c. For RIP Admin Mode, select the **Enable** radio button.
- d. Click **Apply**.
6. Enable RIP on interface 1/0/22.

- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

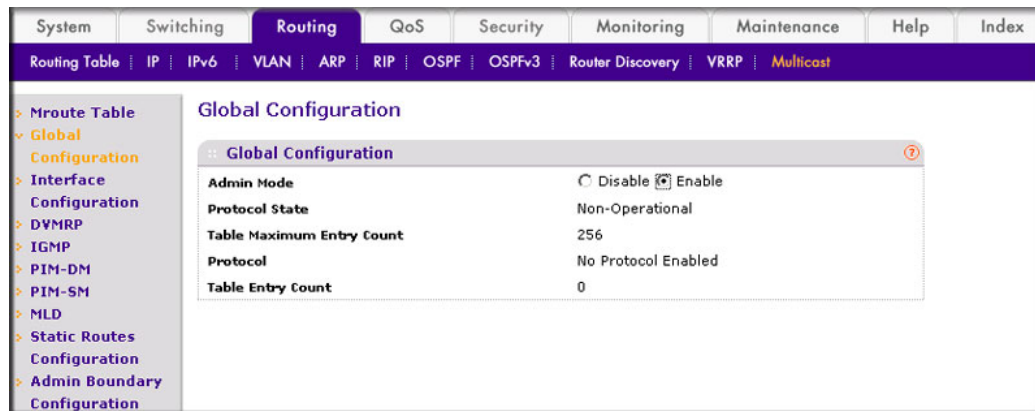


- b. In the **Interface** list, select **1/0/22**.
 - c. For RIP Admin Mode, select the **Enable** radio button.
 - d. Click **Apply**.
7. Enable RIP on interface 1/0/24.
 - a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.



- b. In the **Interface** list, select **1/0/24**.
 - c. For RIP Admin Mode, select the **Enable** radio button.
 - d. Click **Apply**.
8. Enable multicast globally.

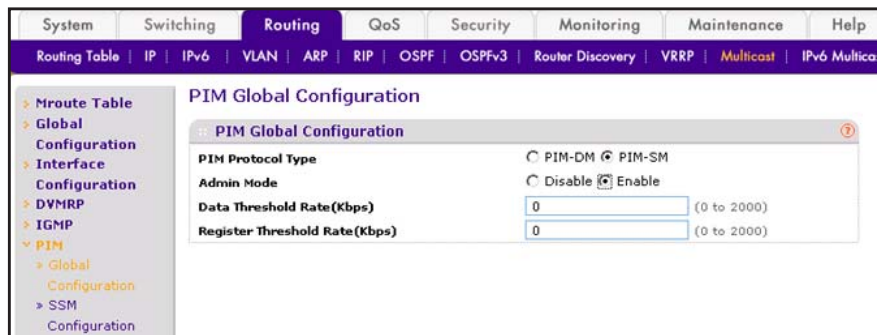
- a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.



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

9. Enable PIM-SM globally.

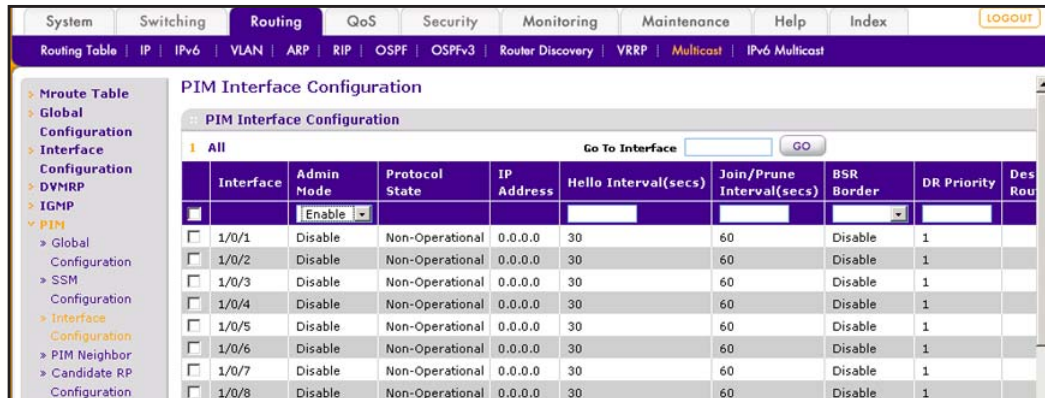
- a. Select **Routing > Multicast > PIM > Global Configuration**. A screen similar to the following displays.



- b. For PIM Protocol Type, select the **PIM-SM** radio button.
 c. For Admin Mode, select the **Enable** radio button.
 d. Click **Apply**.

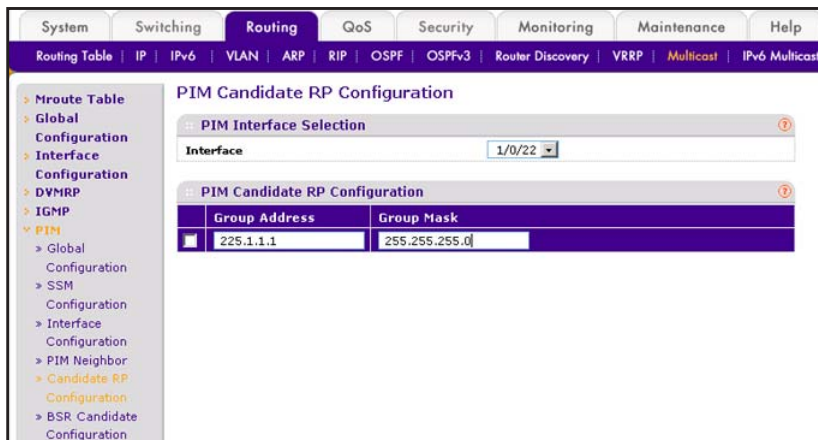
10. Enable PIM-SM on interfaces 1/0/21, 1/0/22, and 1/0/24.

- a. Select **Routing > Multicast > PIM > Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Interface **1/0/21**, **1/0/22**, and **1/0/24** check boxes.
 - c. In the **Admin Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
11. Set up Candidate RP configuration.

- a. Select **Routing > Multicast > PIM > Candidate RP Configuration**. A screen similar to the following displays.



- b. In the **Interface** list, select **1/0/22**.
 - c. In the **Group IP** field, enter **225.1.1.1**.
 - d. In the **Group Mask** field, enter **255.255.255.0**.
 - e. Click **Add**.
12. Set up BSR Candidate configuration.

- a. Select **Routing > Multicast > PIM > BSR Candidate Configuration**. A screen similar to the following displays.

The screenshot shows the 'PIM BSR Candidate Configuration' page. The left sidebar contains a navigation tree with 'PIM' expanded to 'BSR Candidate Configuration'. The main content area has a title 'PIM BSR Candidate Configuration' and a form with the following fields:

- Interface:** A dropdown menu showing '1/0/22'.
- Hash Mask Length:** A text input field containing '30', with '(0-32)' in parentheses to its right.
- BSR Expiry Time (hh:mm:ss):** An empty text input field.
- Priority:** A text input field containing '3', with '(0 to 255)' in parentheses to its right.
- IP Address:** An empty text input field.
- Next bootstrap Message(hh:mm:ss):** An empty text input field.
- Next Candidate RP Advertisement(hh:mm:ss):** An empty text input field.

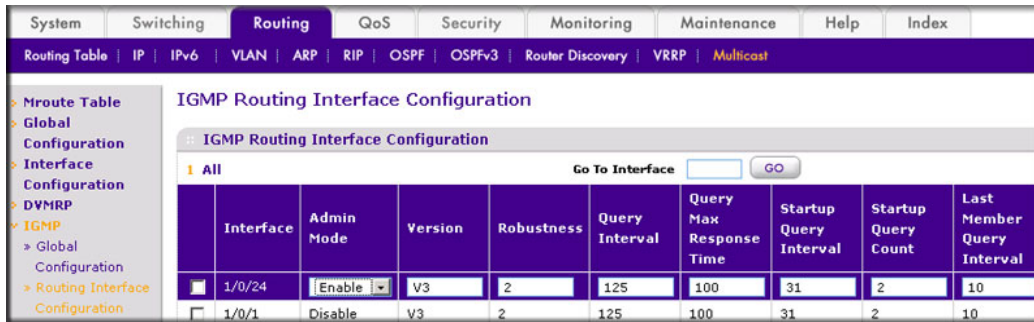
- b. In the **Interface** list, select **1/0/22**.
- c. In the **Hash Mask Length** field, enter **30**.
- d. In the **Priority** field, enter **3**.
- e. Click **Apply**.
13. Enable IGMP globally.
- a. Select **Routing > Multicast > IGMP > Global Configuration**. A screen similar to the following displays.

The screenshot shows the 'IGMP Global Configuration' page. The left sidebar contains a navigation tree with 'IGMP' expanded to 'Global Configuration'. The main content area has a title 'IGMP Global Configuration' and a form with the following field:

- Admin Mode:** A radio button group with 'Disable' and 'Enable' options. The 'Enable' radio button is selected.

- b. For Admin Mode, select the **Enable** radio button.
- c. Click **Apply**.
14. Enable IGMP on interface 1/0/24.

- a. Select **Routing > Multicast > IGMP > Interface Configuration**. A screen similar to the following displays.



- b. Under IGMP Routing Interface Configuration, scroll down and select the Interface **1/0/24** check box.
- c. In the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.

This chapter includes the following sections:

- *DHCP L2 Relay*
- *DHCP L3 Relay* on page 484
- *Configure a DHCP L3 Switch* on page 489

DHCP L2 Relay

DHCP relay agents eliminate the need to have a DHCP server on each physical network. Relay agents populate the `giaddr` field and also append the `Relay Agent Information` option to the DHCP messages. DHCP servers use this option for IP addresses and other parameter assignment policies. These DHCP relay agents are typically IP routing-aware devices and are referred to as Layer 3 relay agents.

In some network configurations, there is a need for Layer 2 devices to append the relay agent Information option as they are closer to the end hosts.

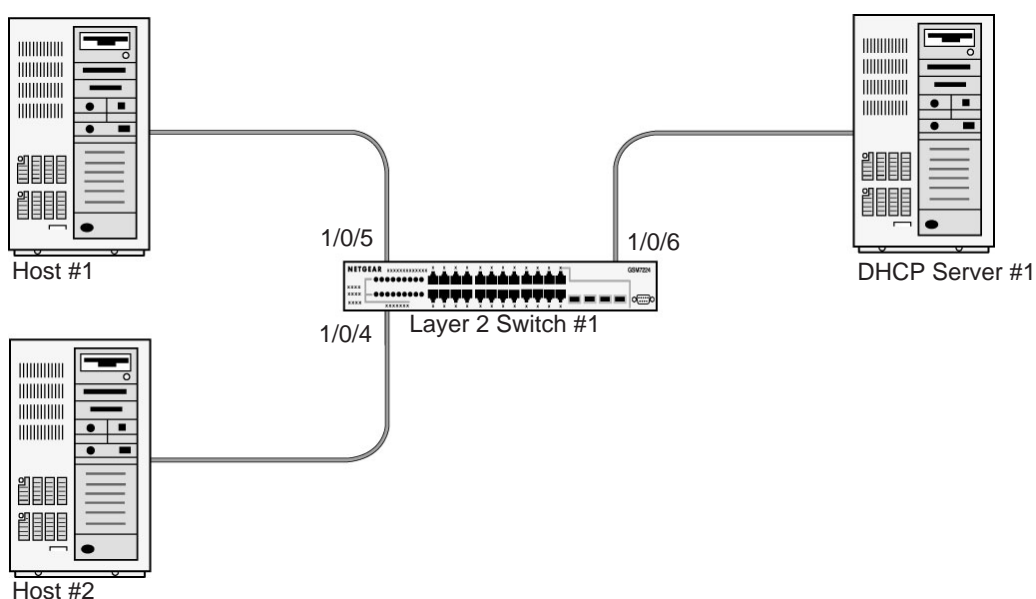


Figure 47. DHCP L2 Relay

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 located on another network. These Layer 2 devices append the Relay agent information option and broadcast the DHCP message. This section provides information about where a Layer 2 relay agent fits in and how it is used.

CLI: Enable DHCP L2 Relay

1. Enter the following commands:

```
(Netgear Switch)#vlan database
(Netgear Switch)(Vlan)#vlan 200
(Netgear Switch)(Vlan)#exit
```

2. Enable the DHCP L2 relay on the switch.

```
(Netgear Switch) (Config)#dhcp l2relay
(Netgear Switch) (Config)#dhcp l2relay vlan 200
```

3. Enable the Option 82 Circuit ID field.

```
(Netgear Switch) (Config)#dhcp l2relay circuit-id vlan 200
```

4. Enable the Option 82 Remote ID field.

```
(Netgear Switch) (Config)#dhcp l2relay remote-id rem_id vlan 200
```

5. Enable DHCP L2 relay on port 1/0/4.

```
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)# dhcp l2relay
```

```
(Netgear Switch) (Interface 1/0/4)# vlan pvid 200
(Netgear Switch) (Interface 1/0/4)# vlan participation include 200
(Netgear Switch) (Interface 1/0/4)# exit
```

6. Enable DHCP L2 relay on port 1/0/5.

```
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)# dhcp l2relay
(Netgear Switch) (Interface 1/0/5)# vlan pvid 200
(Netgear Switch) (Interface 1/0/5)# vlan participation include 200
(Netgear Switch) (Interface 1/0/5)# exit
```

7. Enable DHCP L2 relay on port 1/0/6.

```
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)# dhcp l2relay
```

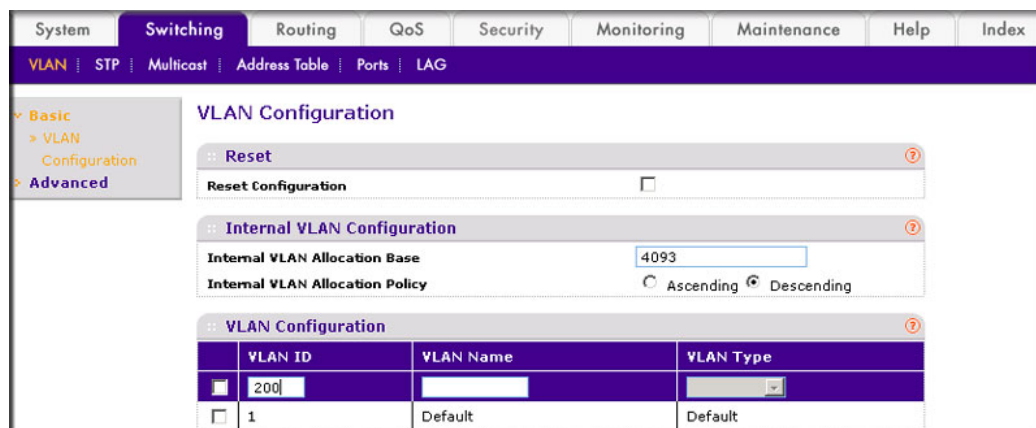
8. Trust packets with option 82 received on port 1/0/6.

```
(Netgear Switch) (Interface 1/0/6)# dhcp l2relay trust
(Netgear Switch) (Interface 1/0/6)# vlan pvid 200
(Netgear Switch) (Interface 1/0/6)# vlan participation include 200
(Netgear Switch) (Interface 1/0/6)# exit
```

Web Interface: Enable DHCP L2 Relay

1. Create VLAN 200.

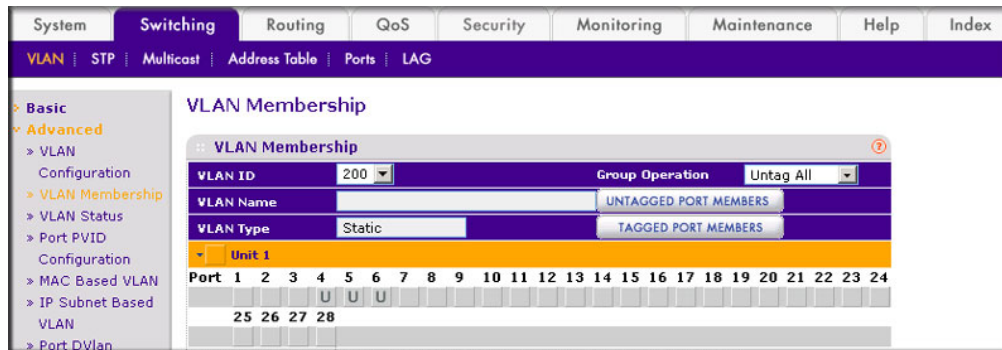
- a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays.



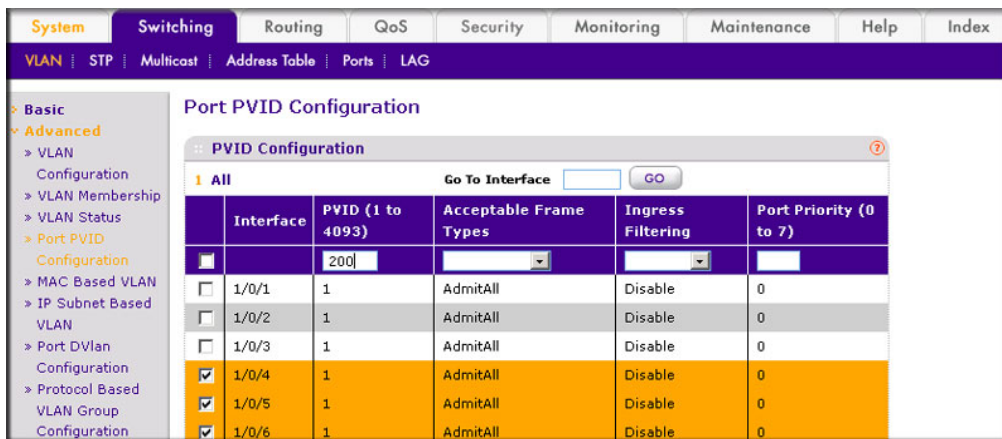
- b. In the **VLAN ID** field, enter **200**.
- c. In the **VLAN Type** field, select **Static**.
- d. Click **Add**.

2. Add ports to VLAN 200.

- a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays.



- b. In the **VLAN ID** field, select **200**.
 - c. Click **Unit 1**. The ports display.
 - d. Click the gray boxes under ports **4, 5, and 6** until **U** displays. The U specifies that the egress packet is untagged for the port.
 - e. Click **Apply**.
3. Specify the PVID on ports 1/0/4, 1/0/5 and 1/0/6.
 - a. Select **Switching > VLAN > Advanced > Port PVID Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Interface **1/0/4, 1/0/5, and 1/0/6** check boxes.
 - c. In the **PVID (1 to 4093)** field, enter **200**.
 - d. Click **Apply** to save the settings.
4. Enable DHCP L2 relay on VLAN 200.

- a. Select **System > Services > DHCP L2 Relay > DHCP L2 Relay Configuration**. A screen similar to the following displays.

DHCP L2 Relay Global Configuration				
Admin Mode <input type="radio"/> Disable <input checked="" type="radio"/> Enable				
DHCP L2 Relay VLAN Configuration				
	VLAN ID	Admin Mode	Circuit ID Mode	Remote ID String
<input type="checkbox"/>	200	Enable	Enable	rmt_id
<input type="checkbox"/>	1	Disable	Disable	
<input checked="" type="checkbox"/>	200	Disable	Disable	

- b. For Admin Mode, select the **Enable** radio button.
- c. Scroll down and select the VLAN ID **200** check box.
- d. Enter the following information:
- In the **Admin Mode** field, select **Enable**.
 - In the **Circuit ID Mode** field, select **Enable**.
 - In the **Remote ID String** field, enter `rmt_id`.
- e. Click **Apply** to save the settings.
5. Enable DHCP L2 Relay on interfaces 1/0/4, 1/0/5, and 1/0/6.
- a. Select **System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration**. A screen similar to the following displays.

DHCP L2 Relay Configuration			
1 All			
Go To Interface <input type="text"/> GO			
	Interface	Admin Mode	82 Option Trust Mode
<input type="checkbox"/>	1/0/1	Disable	Disable
<input type="checkbox"/>	1/0/2	Disable	Disable
<input type="checkbox"/>	1/0/3	Disable	Disable
<input checked="" type="checkbox"/>	1/0/4	Disable	Disable
<input checked="" type="checkbox"/>	1/0/5	Disable	Disable
<input checked="" type="checkbox"/>	1/0/6	Disable	Disable

- b. Scroll down and select the **1/0/4**, **1/0/5**, and **1/0/6** check boxes.
- c. In the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
6. Enable DHCP L2 relay trust on interface 1/0/6.

- a. Select **System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration**. A screen similar to the following displays.

The screenshot shows the DHCP L2 Relay Configuration page. The left sidebar contains a navigation tree with the following items: DHCP Server, DHCP Relay, DHCP L2 Relay (expanded), DHCP L2 Relay Global Configuration, DHCP L2 Relay Interface Configuration (expanded), DHCP L2 Relay Interface Statistics, UDP Relay, DHCPv6 Server, and DHCPv6 Relay. The main content area is titled "DHCP L2 Relay Configuration" and contains a table with the following data:

Interface	Admin Mode	82 Option Trust Mode
<input checked="" type="checkbox"/> 1/0/6	Enable	Enable
<input type="checkbox"/> 1/0/1	Disable	Disable
<input type="checkbox"/> 1/0/2	Disable	Disable
<input type="checkbox"/> 1/0/3	Disable	Disable
<input type="checkbox"/> 1/0/4	Enable	Disable
<input type="checkbox"/> 1/0/5	Enable	Disable
<input checked="" type="checkbox"/> 1/0/6	Enable	Disable

- b. Under DHCP L2 Relay Configuration, scroll down and select the Interface **1/0/6** check box.
- c. In the **82 Option Trust Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.

DHCP L3 Relay

This case has two steps, DHCP server configuration and DHCP L3 relay configuration. This example shows how to configure a DHCP L3 relay on a NETGEAR switch and how to configure DHCP pool to assign IP addresses to DHCP clients using DHCP L3 relay.

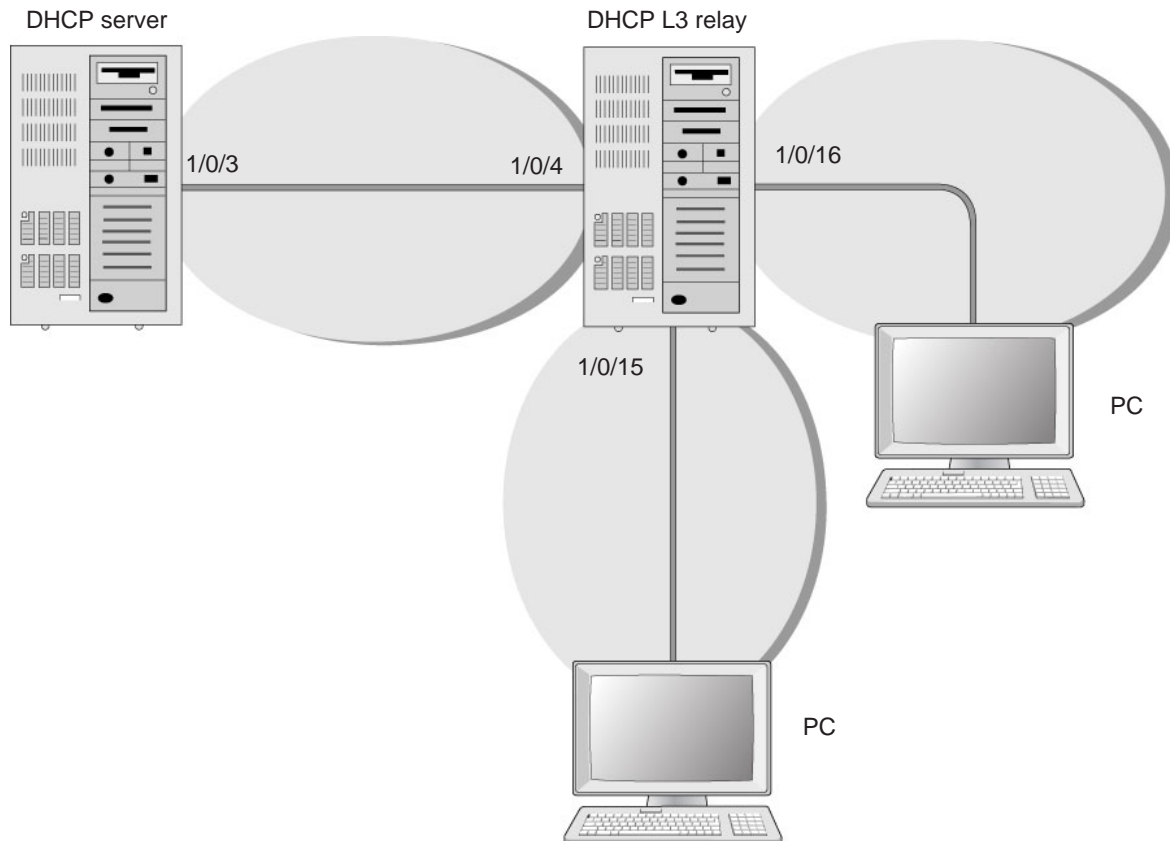


Figure 48. DHCP L3 relay

Configure the DHCP Server Switch

CLI: Configure a DHCP Server

1. Enable routing on the switch.

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

2. Create a routing interface and enable RIP on it so that the DHCP server learns the route 10.200.1.0/24 from the DHCP L3 relay.

```
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 10.100.1.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#ip rip
(Netgear Switch) (Interface 1/0/3)#exit
```

3. Create a DHCP pool.

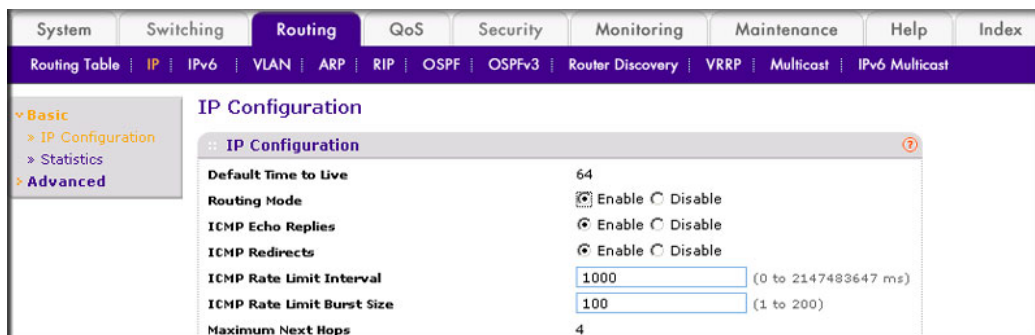
```
(Netgear Switch) (Config)#ip dhcp pool dhcp_server
(Netgear Switch) (Config-dhcp-pool)#network 10.200.1.0 255.255.255.0
(Netgear Switch) (Config-dhcp-pool)#exit
(Netgear Switch) (Config)#ip dhcp pool dhcp_server_second
(Netgear Switch) (Config-dhcp-pool)#network 10.200.2.0 255.255.255.0
(Netgear Switch) (Config-dhcp-pool)#exit
(Netgear Switch) (Config)#service dhcp
(Netgear Switch) (Config)#exit
```

4. Exclude the IP address 10.200.1.1 and 10.200.2.1 from the DHCP pool because it has been used on the DHCP L3 relay.

```
(Netgear Switch) (Config)#ip dhcp excluded-address 10.200.1.1
(Netgear Switch) (Config)#ip dhcp excluded-address 10.200.2.1
```

Web Interface: Configure a DHCP Server

1. Enable routing mode on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.



- b. For Routing Mode, select the **Enable** radio button.
 - c. Click **Apply**.
2. Create a routing interface and assign 10.100.1.1/24 to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

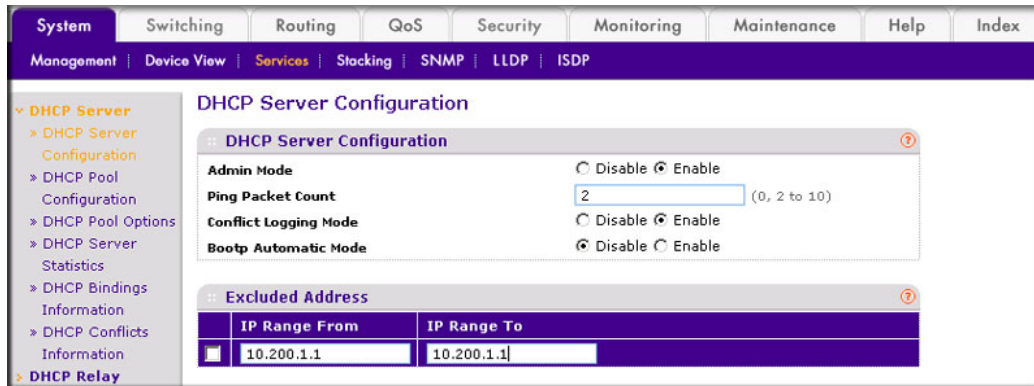
Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode	OSPF Admin Mode	Forward Net Directed Broadcasts
<input type="checkbox"/>	1/0/1		0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable
<input type="checkbox"/>	1/0/2		0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable
<input checked="" type="checkbox"/>	1/0/3		10.100.1.1	255.255.255.0	Enable	Enable	Disable	Disable

- b. Scroll down and select the **1/0/3** check box.
- c. In the **IP Address** field, enter **10.100.1.1**.
- d. In the **Subnet Mask** field, enter **255.255.255.0**.
- e. In the **Routing Mode** field, select **Enable**.
- f. Click **Apply** to save the settings.
3. Enable RIP on interface 1/0/3.
- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

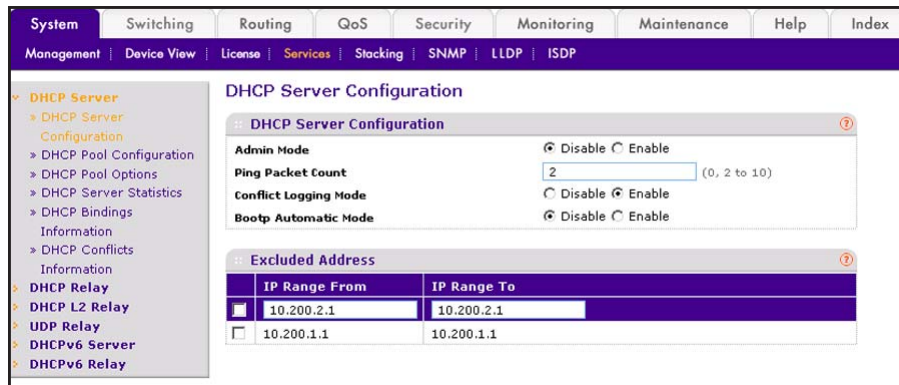
Interface	1/0/3
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Authentication Type	None

- b. In the **Interface** field, select **1/0/3**.
- c. For RIP Admin Mode, select the **Enable** radio button.
- d. Click **Apply** to save the settings.
4. Set up the DHCP global configuration.

- a. Select **System > Services > DHCP Server > DHCP Server Configuration**. A screen similar to the following displays.



- b. For Admin Mode, select the **Enable** radio button.
 - c. In the **IP Range From** field, enter **10.200.1.1**.
 - d. In the **IP Range To** field, enter **10.200.1.1**.
 - e. Click **Add**.
5. Exclude 10.200.2.1 from the DHCP pool.
 - a. Select **System > Services > DHCP Server > DHCP Server Configuration**. A screen similar to the following displays:



- b. In the IP Range From field, enter **10.200.2.1**.
 - c. In the IP Range To field, enter **10.200.2.1**.
 - d. Click **Add**.
6. Create a DHCP pool named `dhcp_server`.

- a. Select **System > Services > DHCP Server > DHCP Pool Configuration**. A screen similar to the following displays.

The screenshot shows the DHCP Pool Configuration page. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The left sidebar shows the DHCP Server configuration tree. The main form contains the following fields:

Field	Value	Constraints
Pool Name (list)	Create	
Pool Name (text)	dhcp_server	(1 to 31 Alphanumeric Characters)
Type of Binding (list)	Dynamic	
Network Address (text)	10.200.1.1	
Network Mask (text)	255.255.255.0	
Network Prefix Length (text)		(0 to 32)
Client Name (text)		
Hardware Address (text)	00:00:00:00:00:00	
Hardware Address Type (list)	Ethernet	
Client ID (text)		
Host Number (text)	0.0.0.0	
Host Mask (text)	0.0.0.0	
Host Prefix Length (text)		(0 to 32)

- b. Under DHCP Pool Configuration, enter the following information:
- In the **Pool Name** list, select **Create**.
 - In the **Pool Name** field, enter **dhcp_server**.
 - In the **Type of Binding** list, select **Dynamic**.
 - In the **Network Number** field, enter **10.200.1.0**.
 - In the **Network Mask** field, enter **255.255.255.0**. As an alternate, you can enter **24** in the **Network Prefix Length** field.

Note: Do not fill in the Network Mask field and Network Prefix Length field at the same time.

- c. Click **Add**. The pool_dynamic name is now added to the **Pool Name** drop-down list.
7. Create a DHCP pool named dhcp_server_second.

- a. Select **System > Services > DHCP Server > DHCP Pool Configuration**. A screen similar to the following displays.

- b. Under DHCP Pool Configuration, enter the following information:
- In the Pool Name list, select **Create**.
 - In the Pool Name field, enter **dhcp_server_second**.
 - In the Type of Binding list, select **Dynamic**.
 - In the Network Number field, enter **10.200.2.0**.
 - In the Network Mask field, enter **255.255.255.0**. As an alternate, you can enter **24** in the Network Prefix Length field.
- c. Click **Add**. The dhcp_server_second name is now added to the Pool Name drop-down list.

Configure a DHCP L3 Switch

CLI: Configure a DHCP L3 Relay

1. Enable routing on the switch.

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

2. Create a routing interface and enable RIP on 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)#ip rip
(Netgear Switch) (Interface 1/0/4)#exit
```

3. Create a routing interface connecting to the client.

```
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#interface 1/0/16
(Netgear Switch) (Interface 1/0/16)#routing
(Netgear Switch) (Interface 1/0/16)#ip address 10.200.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/16)#exit
```

4. Configure the DHCP Server IP address and enable the DHCP L3 relay.

```
(Netgear Switch) (Config)#ip helper-address 10.100.1.1 dhcp
(Netgear Switch) (Config)#ip helper enable
```

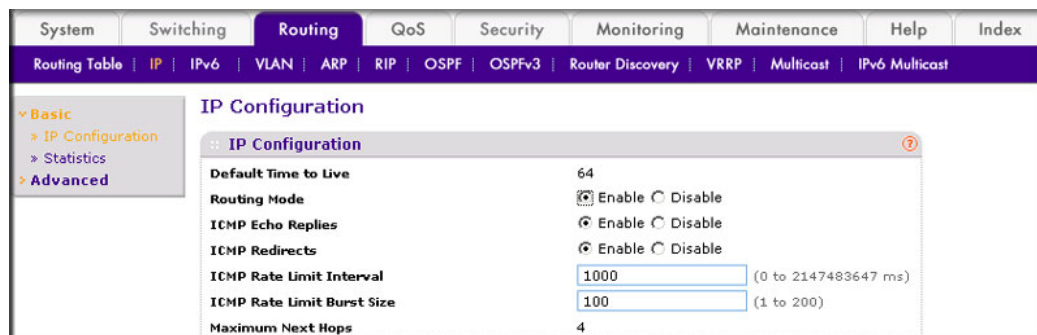
5. Redistribute 10.200.1.0/24 and 10.200.2.0/24 to the RIP such that RIP advertises this route to the DHCP server.

```
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#router rip
(Netgear Switch) (Config-router)#redistribute connected
(Netgear Switch) (Config-router)#exit
```

Web Interface: Configure a DHCP L3 Relay

1. Enable routing mode on the switch.

- a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.

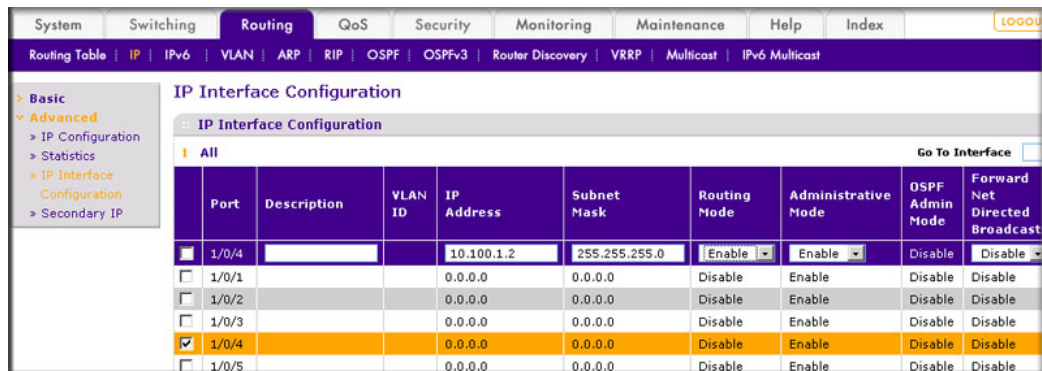


- b. For Routing Mode, select the **Enable** radio button.

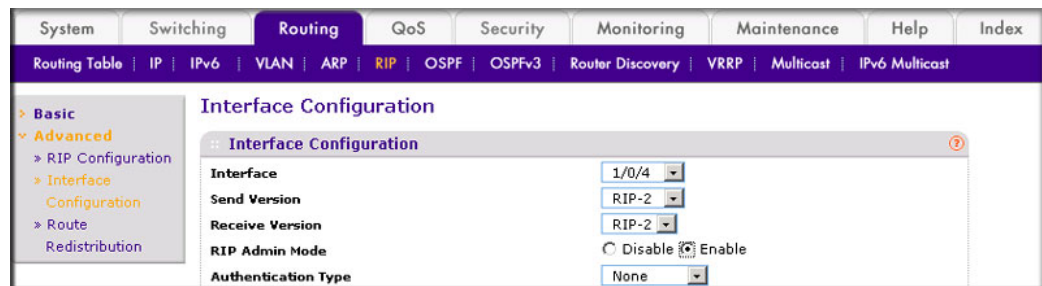
- c. Click **Apply**.

2. Create a routing interface and assign 10.100.1.2/24 to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Port **1/0/4** check box.
 c. In the **IP Address** field, enter **10.100.1.2**.
 d. In the **Subnet Mask** field, enter **255.255.255.0**.
 e. In the **Routing Mode** field, select **Enable**.
 f. Click **Apply** to save the settings.
3. Enable RIP on interface 1/0/4.
- a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.



- b. In the **Interface** list, select **1/0/4**.
 c. For RIP Admin Mode, select the **Enable** radio button.
 d. Click **Apply** to save the settings.
4. Create a routing interface and assign 10.200.1.1/24 to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

Port	Description	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Routing Mode	Administrative Mode	Link Speed Data Rate
<input checked="" type="checkbox"/>	1/0/15		Manual	10.200.1.1	255.255.255.0	Enable	Enable	Unknown
<input type="checkbox"/>	1/0/1		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
<input type="checkbox"/>	1/0/2		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
<input type="checkbox"/>	1/0/3		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
<input type="checkbox"/>	1/0/4		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
<input type="checkbox"/>	1/0/5		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
<input type="checkbox"/>	1/0/6		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
<input type="checkbox"/>	1/0/7		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
<input type="checkbox"/>	1/0/8		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
<input type="checkbox"/>	1/0/9		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown

- b. Under IP Interface Configuration, scroll down and select the Port **1/0/15** check box.
- c. In the **IP Address Configuration Method** field, enter **Manual**.
- d. In the **IP Address** field, enter **10.200.1.1**.
- e. In the **Subnet Mask** field, enter **255.255.255.0**.
- f. In the **Routing Mode** field, select **Enable**.
- g. Click **Apply** to save the settings.
5. Create a routing interface and assign 10.200.2.1/24 to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

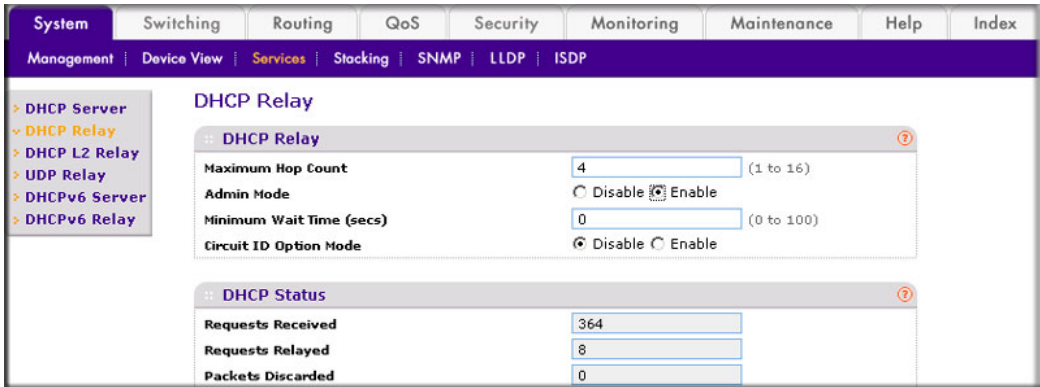
Port	Description	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Routing Mode	Administrative Mode	Link Speed Data Rate
<input checked="" type="checkbox"/>	1/0/16		Manual	10.200.2.1	255.255.255.0	Enable	Enable	Unknown
<input type="checkbox"/>	1/0/1		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
<input type="checkbox"/>	1/0/2		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
<input type="checkbox"/>	1/0/3		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
<input type="checkbox"/>	1/0/4		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
<input type="checkbox"/>	1/0/5		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
<input type="checkbox"/>	1/0/6		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
<input type="checkbox"/>	1/0/7		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
<input type="checkbox"/>	1/0/8		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
<input type="checkbox"/>	1/0/9		None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown

- b. Under IP Interface Configuration, scroll down and select the Port **1/0/16** check box.
- c. In the **IP Address Configuration Method** field, enter **Manual**.
- d. In the **IP Address** field, enter **10.200.2.1**.
- e. In the **Subnet Mask** field, enter **255.255.255.0**.
- f. In the **Routing Mode** field, select **Enable**.
- g. Click **Apply** to save the settings.
6. Redistribute the connected routes to RIP.

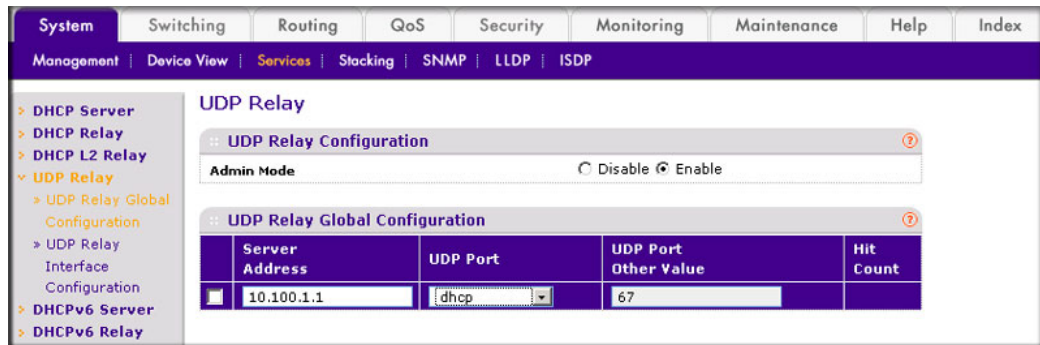
- a. Select **Routing > RIP > Advanced > Route Redistribution**. A screen similar to the following displays.



- b. In the **Source** field, select **Connected**.
 - c. In the **Redistribute Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
7. Enable DHCP L3 relay.
 - a. Select **System > Services > DHCP Relay**. A screen similar to the following displays.



- b. For Admin Mode, select the **Enable** radio button.
 - c. Click **Apply** to save the settings.
8. Configure the DHCP server IP address.
 - a. Select **System > Services > UDP Relay**. A screen similar to the following displays.



- b. In the **Server Address** field, enter **10.100.1.1**.
- c. In the **UDP Port** field, enter **dhcp**.
- d. Click **Add** to save the settings.

Multicast Listener Discovery

This chapter provides the following examples:

- *Configure MLD* on page 495
- *MLD Snooping* on page 508

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 makes decisions on the flow of multicast data packets. Periodically, the multicast router sends general queries requesting multicast address listener information from systems on an attached networks. These queries are used to build and refresh the multicast address listener state on the attached networks. In response to the queries, multicast listeners reply with membership reports. These membership reports specify their multicast addresses listener state and their desired set of sources with current-state multicast address records. The multicast router also processes unsolicited filter- mode-change records and source-list-change records from systems that want to indicate interest in receiving or not receiving traffic from particular sources.

Configure MLD

In this case, PIM-DM is enabled on Switch A and Switch B, and MLD is enabled on Switch B's port 1/0/24 to discover the multicast listeners.

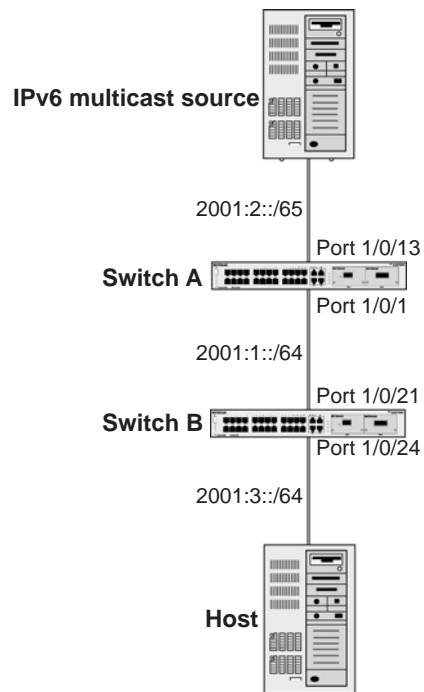


Figure 49. Configure MLD

CLI: Configure MLD

MLD on Switch A

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

```

(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) (Config)#ipv6 pim dense
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ipv6 address 2001:1::1/64
(Netgear Switch) (Interface 1/0/1)#ipv6 enable
(Netgear Switch) (Interface 1/0/1)#ipv6 pim dense
(Netgear Switch) (Interface 1/0/1)#ipv6 ospf
(Netgear Switch) (Interface 1/0/1)#exit

(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ipv6 address 2001:2::1/64
(Netgear Switch) (Interface 1/0/13)#ipv6 enable
(Netgear Switch) (Interface 1/0/13)#ipv6 pim dense
(Netgear Switch) (Interface 1/0/13)#ipv6 ospf
(Netgear Switch) (Interface 1/0/13)#exit

```

MLD on Switch B

1. Enable OSPFv3 to build a unicast route table.

```

(Netgear Switch)#configure
(Netgear Switch) (Config)#ipv6 router ospf
(Netgear Switch) (Config-rtr)#router-id 2.2.2.2
(Netgear Switch) (Config)#exit

```

2. Enable IPV6 unicast routing on the switch.

```

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

```

3. Enable IPV6 MLD on the switch.

```

(Netgear Switch) (Config)#ipv6 mld router

```

4. Enable IPV6 PIM-DM on the switch.

```

(Netgear Switch) (Config)#ipv6 pim dense

```


5. Enable IP multicast forwarding on the switch.

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

6. Enable MLD on interface 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ipv6 address 2001:1::2/64
(Netgear Switch) (Interface 1/0/21)#ipv6 enable
(Netgear Switch) (Interface 1/0/21)#ipv6 pim dense
(Netgear Switch) (Interface 1/0/21)#ipv6 ospf
(Netgear Switch) (Interface 1/0/21)#exit

(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#routing
(Netgear Switch) (Interface 1/0/24)#ipv6 address 2001:3::1/64
(Netgear Switch) (Interface 1/0/24)#ipv6 enable
(Netgear Switch) (Interface 1/0/24)#ipv6 mld router

(Netgear Switch) (Interface 1/0/24)#ipv6 pim dense
(Netgear Switch) (Interface 1/0/24)#exit

The MLD group information on switch B:
(B) #show ipv6 mld groups ff32::1

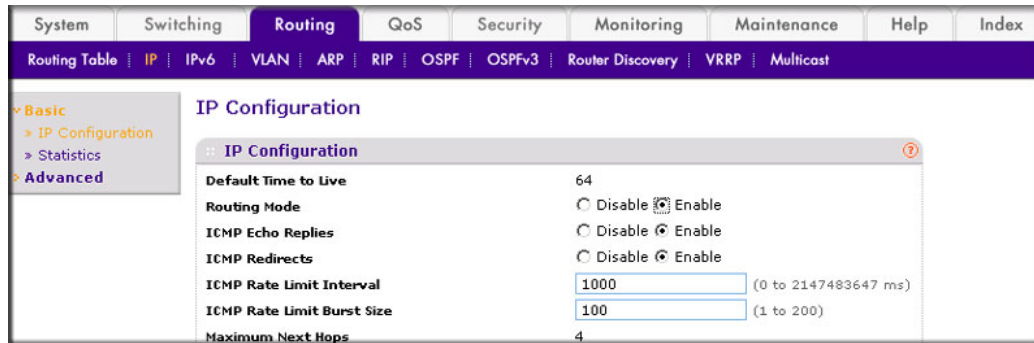
Interface..... 71/1/24
Group Address..... FF32::1
Last Reporter..... FE80::200:4FF:FEE8:5EFC
Up Time (hh:mm:ss)..... 00:00:18
Expiry Time (hh:mm:ss)..... -----
Filter Mode..... Include
Version1 Host Timer..... -----
Group compat mode..... v2
Source Address      ExpiryTime
-----
2001:2::2          00:04:02
```

Web Interface: Configure MLD

MLD on Switch A

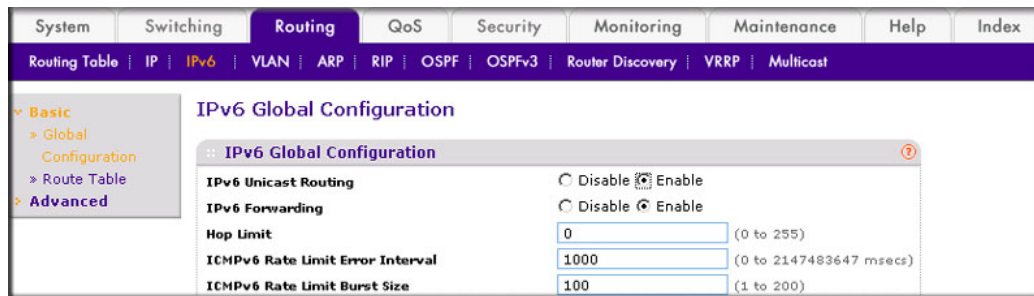
1. Enable IP routing on the switch.

- a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.



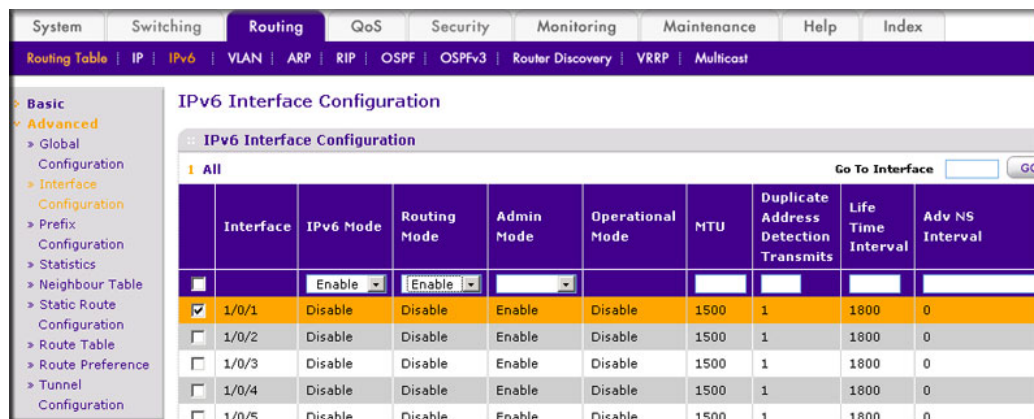
- b. For Routing Mode, select the **Enable** radio button.
 - c. Click **Apply**.
2. Enable IPv6 unicast routing on the switch.

- a. Select **Routing > IPv6 > Basic > Global Configuration**. A screen similar to the following displays.

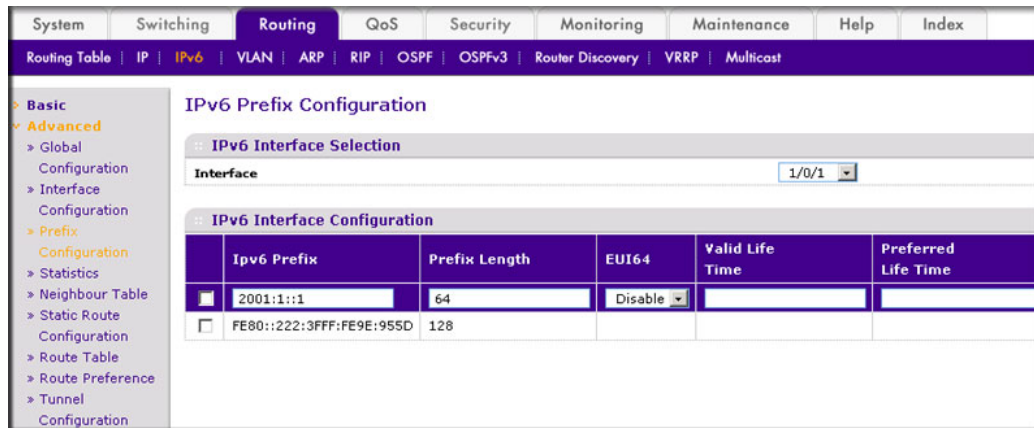


- b. For IPv6 Unicast Routing, select the **Enable** radio button.
 - c. Click **Apply**.
3. Configure 1/0/1 and 1/0/13 as a IPv6 routing ports.

- a. Select **Routing > IPv6 > Advanced > Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Interface **1/0/1** and **1/0/13** check boxes.
 - c. Enter the following information:
 - In the **IPv6 Mode** field, select **Enable**.
 - In the **Routing Mode** field, select **Enable**.
 - In the **Admin Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
4. Assign an IPv6 address to 1/0/1.
- a. Select **Routing > IPv6 > Advanced > Prefix Configuration**. A screen similar to the following displays.



- b. In the Interface field, select **1/0/1**.
 - c. Enter the following information:
 - In the **IPv6 Prefix** field, enter **2001:1::1**.
 - In the **Prefix Length** field, enter **64**.
 - In the **EUI64** field, select **Disable**.
 - d. Click **Add** to save the settings.
5. Assign an IPv6 address to 1/0/13.

- a. Select **Routing > IPv6 > Advanced > Prefix Configuration**. A screen similar to the following displays.

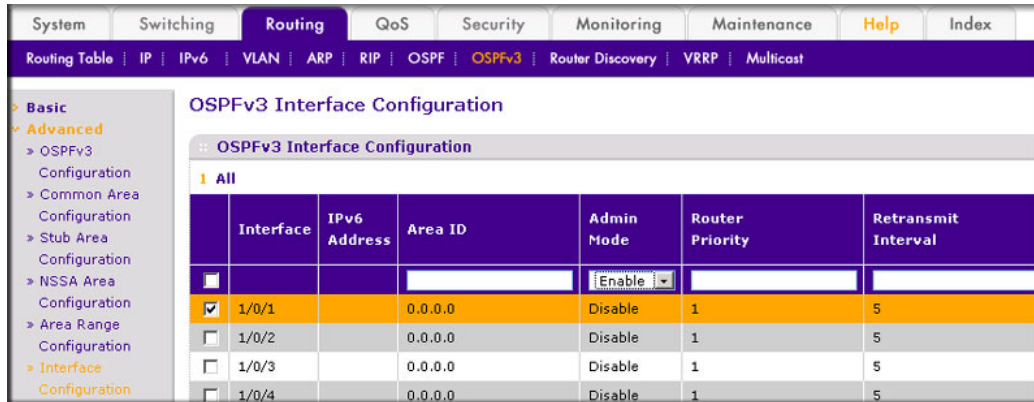
	Ipv6 Prefix	Prefix Length	EUI64	Valid Life Time	Preferred Life Time
<input checked="" type="checkbox"/>	2001:2::1	64	Disable		
<input type="checkbox"/>	FE80::222:3FFF:FE9E:955D	128			

- b. Select Interface **1/0/13**.
- c. Enter the following information:
- In the **IPv6 Prefix** field, enter **2001:2::1**.
 - In the **Prefix Length** field, enter **64**.
 - In the **EUI64** field, select **Disable**.
- d. Click **Add** to save the settings.
6. Configure the router ID of OSPFv3.
- a. Select **Routing > OSPFv3 > Basic > OSPFv3 Configuration**. A screen similar to the following displays.

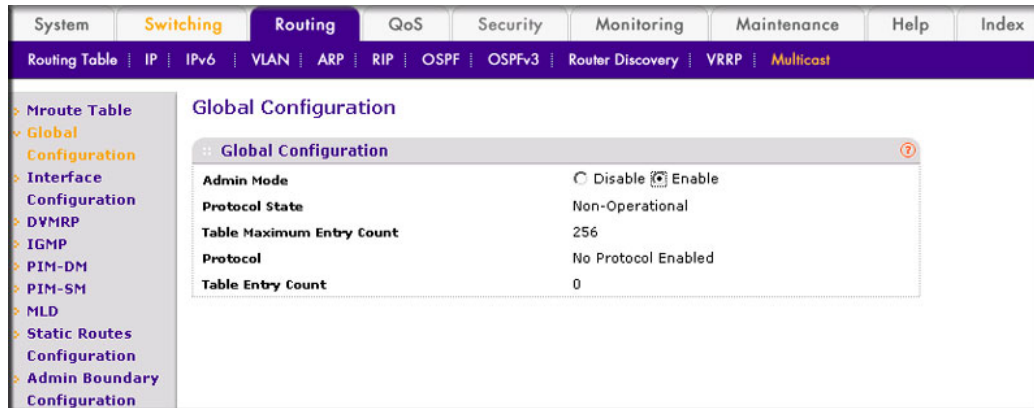
Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Router ID	1.1.1.1

- b. In the **Router ID** field, enter **1.1.1.1**.
- c. For Admin Mode, select the **Enable** radio button.
- d. Click **Apply**.
7. Enable OSPFv3 on interfaces 1/0/1 and 1/0/13.

- a. Select **Routing > OSPFv3 > Advanced > Interface Configuration**. A screen similar to the following displays.

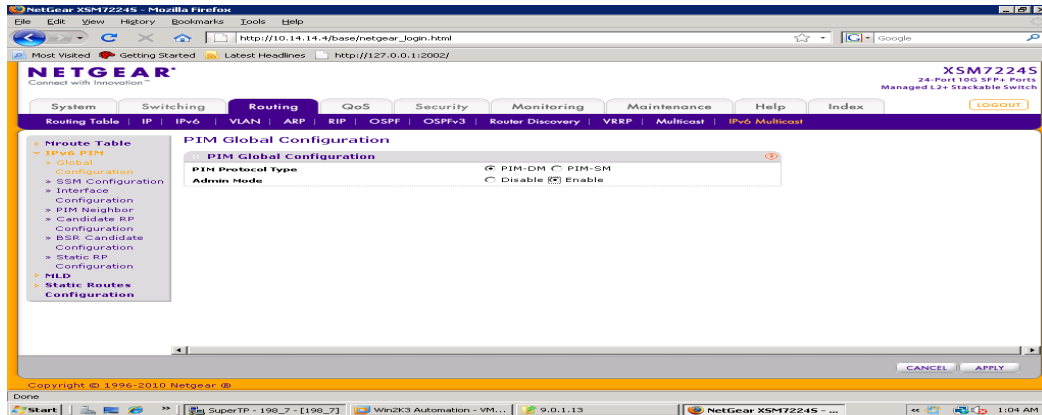


- b. Scroll down and select the Interface **1/0/1** and **1/0/13** check boxes.
 - c. In the **Admin Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
8. Enable multicast globally.
 - a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.



- b. For Admin Mode, select the **Enable** radio button.
 - c. Click **Apply**.
9. Enable PIM-DM globally.

- a. Select **Routing > IPv6 Multicast > IPv6 PIM > Global Configuration**. A screen similar to the following displays.

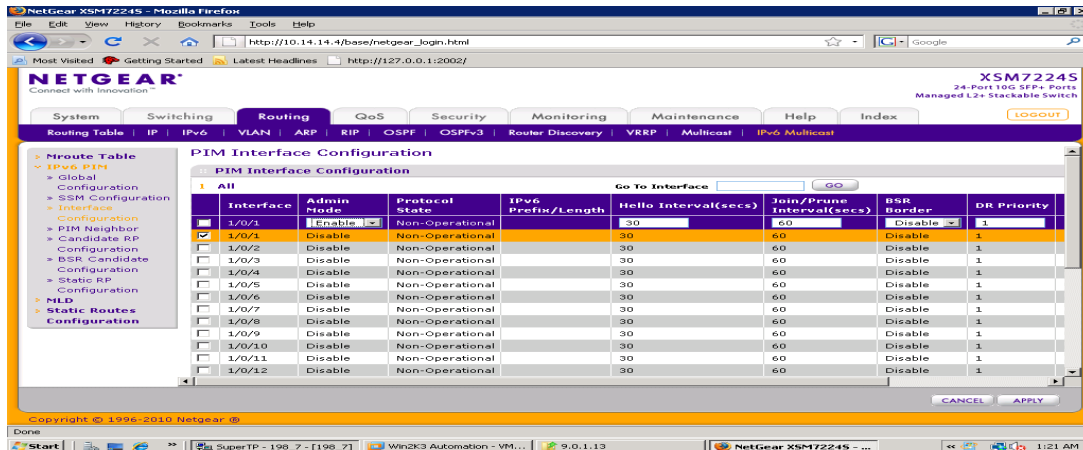


- b. For Admin Mode, select the **Enable** radio button.

- c. Click **Apply**.

10. Enable PIM-DM on interfaces 1/0/1 and 1/0/13.

- a. Select **Routing > IPv6 Multicast > IPv6 PIM > Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Interface **1/0/1** and **1/0/13** check boxes.

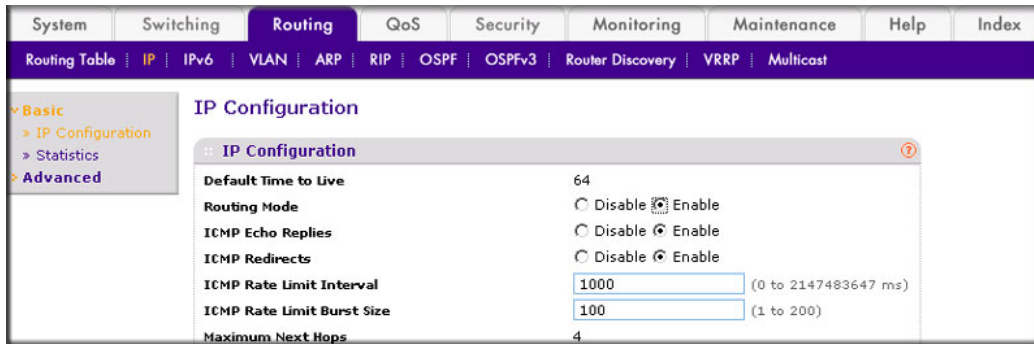
- c. In the **Admin Mode** field, select **Enable**.

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

MLD on Switch B

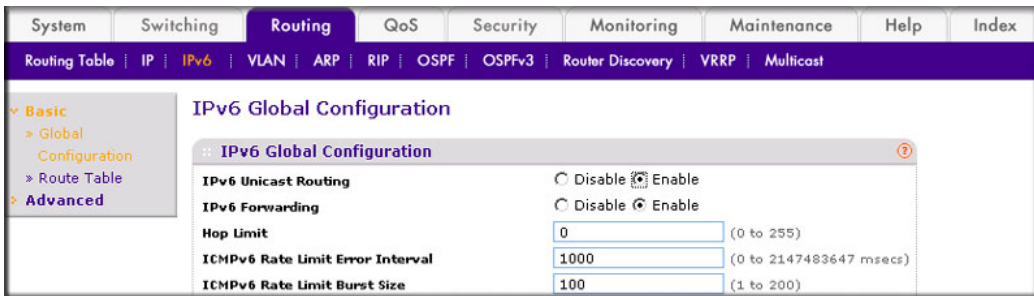
1. Enable IP routing on the switch.

- a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.



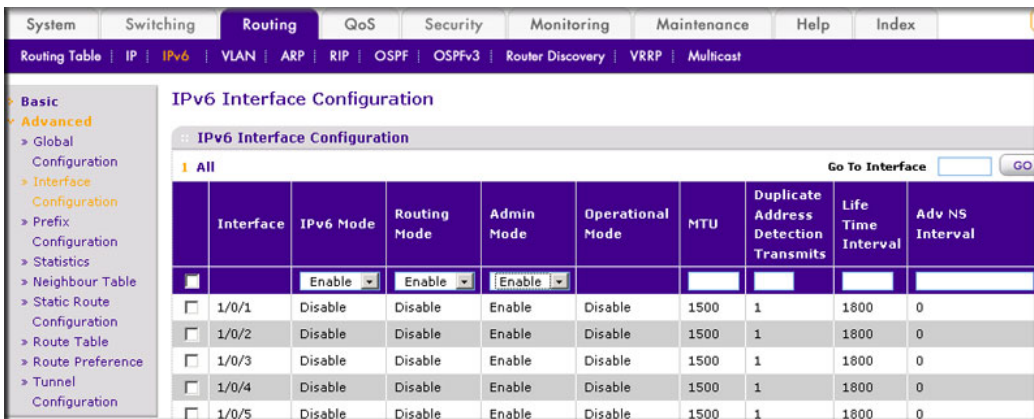
- b. For Routing Mode, select the **Enable** radio button.
 - c. Click **Apply**.
2. Enable IPv6 unicast routing on the switch.

- a. Select **Routing > IPv6 > Basic > Global Configuration**. A screen similar to the following displays.



- b. For IPv6 Unicast Routing, select the **Enable** radio button.
 - c. Click **Apply**.
3. Configure 1/0/21 and 1/0/24 as IPv6 routing ports.

- a. Select **Routing > IPv6 > Advanced > Interface Configuration**. A screen similar to the following displays.

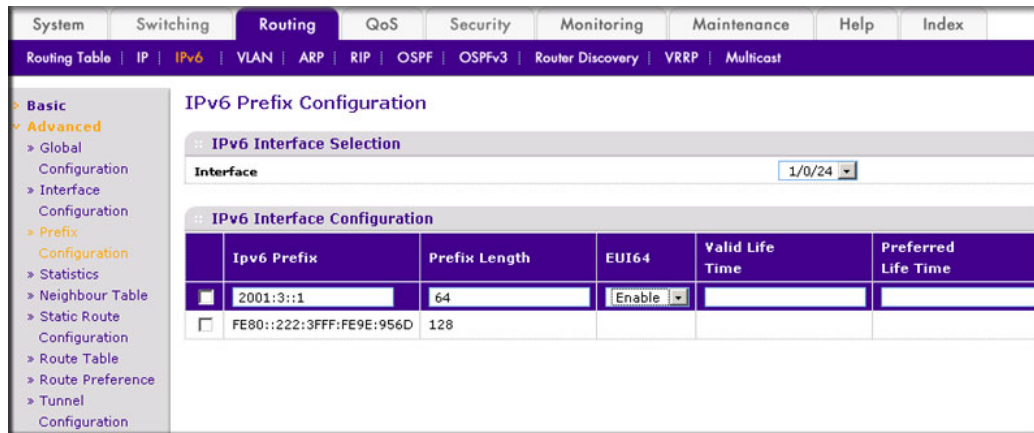


- b. Scroll down and select the Interface **1/0/21** and **1/0/24** check boxes.
 - c. Enter the following information:
 - In the **IPv6 Mode** field, select **Enable**.
 - In the **Routing Mode** field, select **Enable**.
 - In the **Admin Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
4. Assign an IPv6 address to 1/0/21.
 - a. Select **Routing > IPv6 > Advanced > Prefix Configuration**. A screen similar to the following displays.

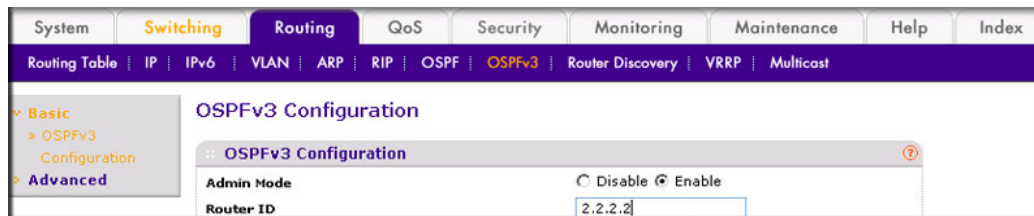
IPv6 Prefix Configuration					
:: IPv6 Interface Selection					
Interface		1/0/21			
:: IPv6 Interface Configuration					
	IPv6 Prefix	Prefix Length	EUI64	Valid Life Time	Preferred Life Time
<input checked="" type="checkbox"/>	2001:1::2	64	Disable		
<input type="checkbox"/>	FE80::222:3FFF:FE9E:956D	128			

- b. In the Interface field, select **1/0/21**.
 - c. Enter the following information:
 - In the **IPv6 Prefix** field, enter **2001:1::2**.
 - In the **Prefix Length** field, enter **64**.
 - In the **EUI64** field, select **Disable**.
 - d. Click **Add** to save the settings.
5. Assign an IPv6 address to 1/0/24.

- a. Select **Routing > IPv6 > Advanced > Prefix Configuration**. A screen similar to the following displays.



- b. Under IPv6 Interface Selection, in the **Interface** field, select **1/0/24**.
 - c. Enter the following information:
 - In the **IPv6 Prefix** field, enter **2001:3::1**.
 - In the **Prefix Length** field, enter **64**.
 - In the **EUI64** field, select **Disable**.
 - d. Click **Add** to save the settings.
6. Configure the router ID of OSPFv3.
 - a. Select **Routing > OSPFv3 > Basic > OSPFv3 Configuration**. A screen similar to the following displays.



- b. In the **Router ID** field, enter **2.2.2.2**.
 - c. For Admin Mode, select the **Enable** radio button.
 - d. Click **Apply**.
7. Enable OSPFv3 on interfaces 1/0/21 and 1/0/24.

- a. Select **Routing > OSPFv3 > Advanced > Interface Configuration**. A screen similar to the following displays.

The screenshot shows the OSPFv3 Interface Configuration page. The breadcrumb trail is Routing > OSPFv3 > Advanced > Interface Configuration. The page title is OSPFv3 Interface Configuration. The left sidebar shows the navigation menu with 'Interface Configuration' selected. The main content area displays a table with the following columns: Interface, IPv6 Address, Area ID, Admin Mode, Router Priority, and Retransmit Interval. The table contains four rows, each representing an interface (1/0/1, 1/0/2, 1/0/3, 1/0/4). The 'Admin Mode' dropdown is set to 'Enable'.

Interface	IPv6 Address	Area ID	Admin Mode	Router Priority	Retransmit Interval
<input type="checkbox"/>			Enable		
<input type="checkbox"/>	1/0/1	0.0.0.0	Disable	1	5
<input type="checkbox"/>	1/0/2	0.0.0.0	Disable	1	5
<input type="checkbox"/>	1/0/3	0.0.0.0	Disable	1	5
<input type="checkbox"/>	1/0/4	0.0.0.0	Disable	1	5

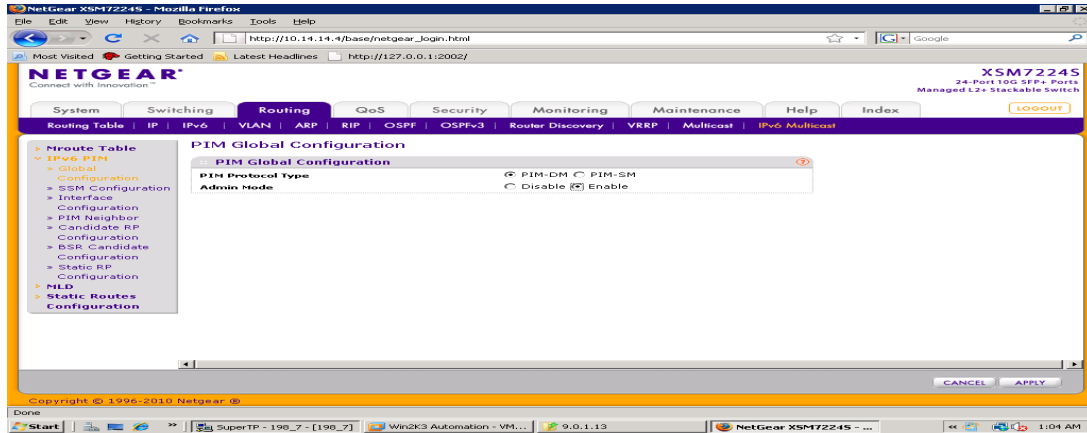
- b. Under OSPFv3 Interface Configuration, scroll down and select the Interface **1/0/21** and **1/0/24** check boxes.
- c. In the OSPFv3 Interface Configuration, in the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
8. Enable multicast globally.
- a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.

The screenshot shows the Global Configuration page. The breadcrumb trail is Routing > Multicast > Global Configuration. The page title is Global Configuration. The left sidebar shows the navigation menu with 'Global Configuration' selected. The main content area displays the Global Configuration settings. The 'Admin Mode' radio button is selected as 'Enable'.

Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Protocol State	Non-Operational
Table Maximum Entry Count	256
Protocol	No Protocol Enabled
Table Entry Count	0

- b. For Admin Mode, select the **Enable** radio button.
- c. Click **Apply**.
9. Enable PIM-DM globally.

- a. Select **Routing > IPv6 Multicast > IPv6PIM > Global Configuration**. A screen similar to the following displays.

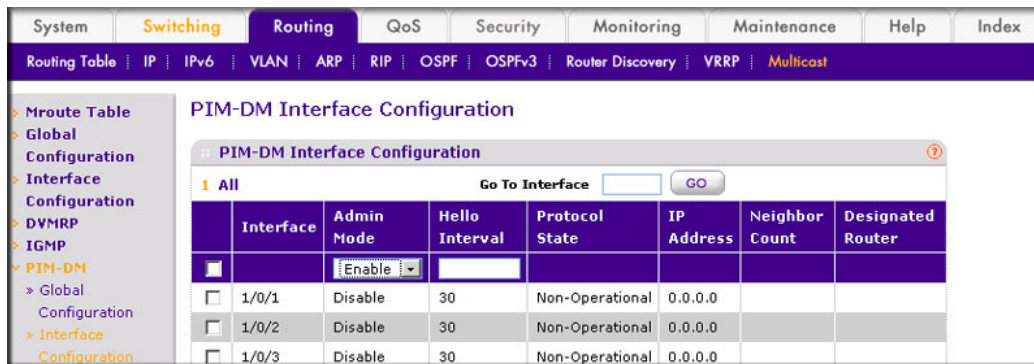


- b. For Admin Mode, select the **Enable** radio button.

- c. Click **Apply**.

10. Enable PIM-DM on interfaces 1/0/21 and 1/0/24.

- a. Select **Routing > IPv6 Multicast > IPv6 PIM > Interface Configuration**. A screen similar to the following displays.



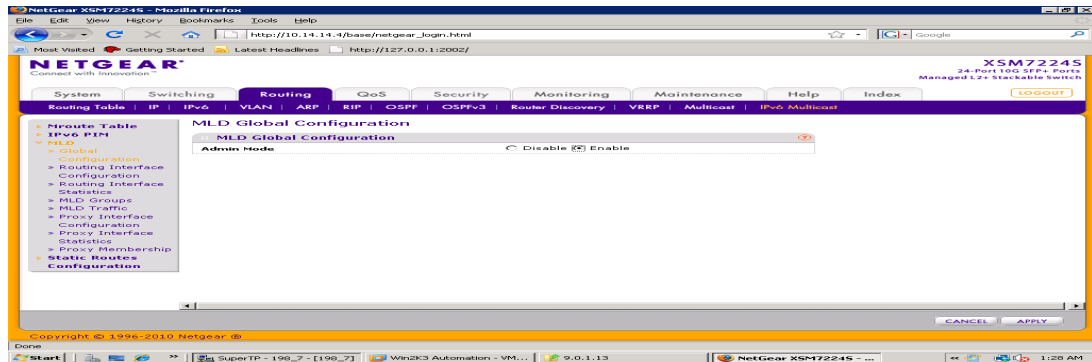
- b. Under PIM Interface Configuration, scroll down select the Interface **1/0/21** and **1/0/24** check boxes.

- c. In the **Admin Mode** field, select **Enable**.

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

11. Enable MLD on the switch.

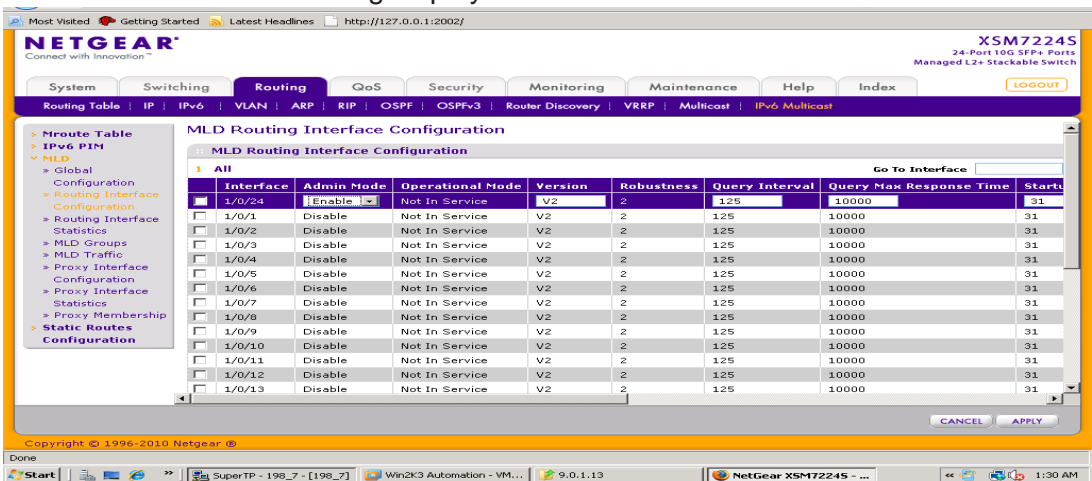
- a. Select **Routing > IPv6 Multicast > MLD > Global Configuration**. A screen similar to the following displays.



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

12. Enable MLD on interface 1/0/24.

- a. Select **Routing > IPv6 Multicast > MLD > Routing Interface Configuration**. A screen similar to the following displays.



- b. Under MLD Routing Interface Configuration, scroll down and select the **1/0/24** check box. Now 1/0/24 appears in the Interface field at the top.
c. In the **Admin Mode** field, select **Enable**.
d. Click **Apply**.

MLD Snooping

In IPv4, Layer 2 switches can use IGMP snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast address. In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes configured to receive IPv6 multicast packets) on its directly attached links and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD version 1 (MLDv1) is equivalent to IGMPv2, and MLD version 2 (MLDv2) is equivalent to IGMPv3. MLD is a subprotocol of Internet Control Message Protocol version 6 (ICMPv6), and MLD messages are a subset of ICMPv6 messages, identified in IPv6 packets by a preceding Next Header value of 58.

The switch can snoop on both MLDv1 and MLDv2 protocol packets and bridge IPv6 multicast data based on destination IPv6 multicast MAC addresses. The switch can be configured to perform MLD snooping and IGMP snooping simultaneously.

CLI: Configure MLD Snooping

1. Enter the following commands.

```
(Netgear Switch) #vlan da
(Netgear Switch) (Vlan)#vlan 300
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#vlan participation include 300
(Netgear Switch) (Interface 1/0/1)#vlan pvid 300
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan participation include 300
(Netgear Switch) (Interface 1/0/24)#vlan pvid 300
(Netgear Switch) (Interface 1/0/24)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) (Config)#set mld
(Netgear Switch) (Config)#exit
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#set mld 300
(Netgear Switch) (Vlan)#exit
```

2. Enable MLD snooping on VLAN 300.

```
(Netgear Switch) #show mldsnooping
Admin Mode..... Enable
Multicast Control Frame Count..... 0
Interfaces Enabled for MLD Snooping..... None
VLANs enabled for MLD snooping..... 300
(Netgear Switch) #
```

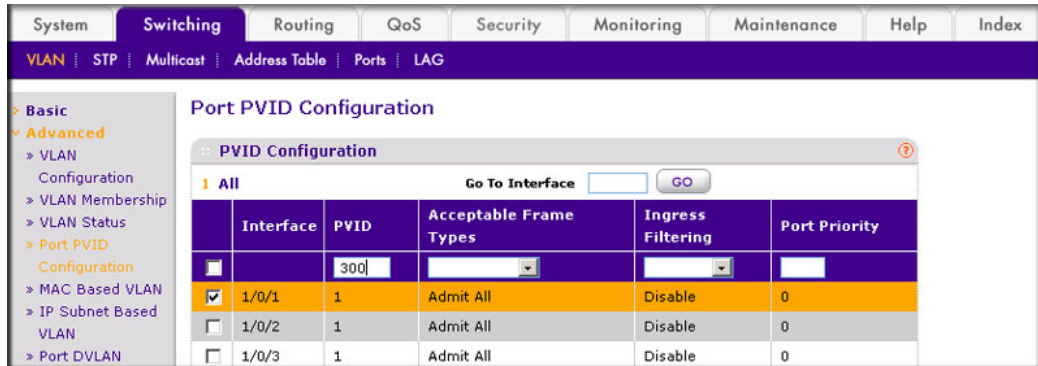
Web Interface: Configure MLD Snooping

1. Create VLAN 300.
 - a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays.

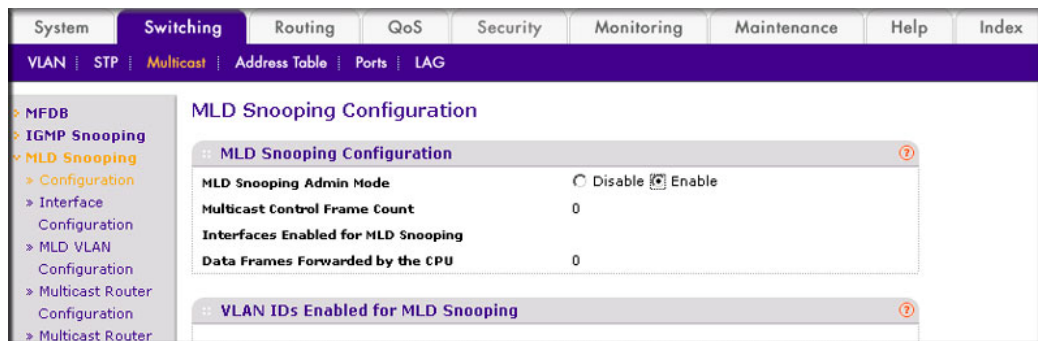
- b. In the **VLAN ID** field, enter **300**.
 - c. Click **Add**.
2. Assign all of the ports to VLAN 300.
 - a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays.

- b. In the **VLAN ID** list, select **300**.
 - c. Click **Unit 1**. The ports display.
 - d. Click the gray boxes under ports **1** and **24** until **U** displays. The U specifies that the egress packet is untagged for the port.
 - e. Click **Apply**.
3. Assign PVID to ports 1/0/1 and 1/0/24.

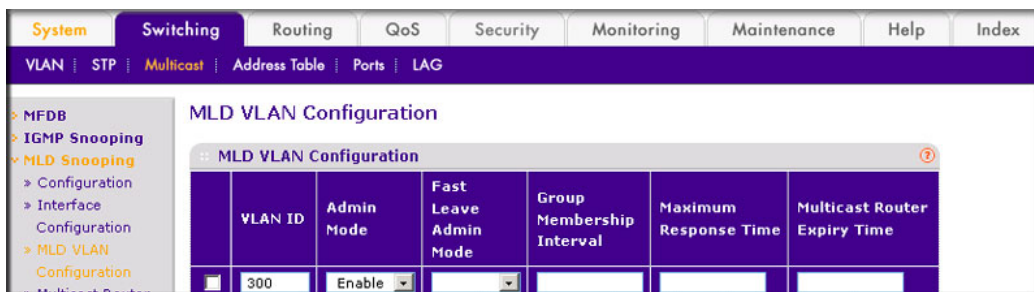
- a. Select **Switching > VLAN > Advanced > Port PVID Configuration**. A screen similar to the following displays.



- b. Scroll down and select the interface **1/0/1** and **1/0/24** check boxes.
 - c. In the **PVID (1 to 4093)** field, enter **300**.
 - d. Click **Apply** to save the settings.
4. Enable MLD snooping on the switch.
 - a. Select **Routing > Multicast > MLD Snooping > Configuration**. A screen similar to the following displays.



- b. For MLD Snooping Admin Mode, select the **Enable** radio button.
 - c. Click **Apply**.
5. Enable MLD snooping on the VLAN 300.
 - a. Select **Routing > Multicast > MLD Snooping > MLD VLAN Configuration**. A screen similar to the following displays.



- b. Enter the following information:
 - In the **VLAN ID** field, enter **300**.
 - In the **Admin Mode** field, select **Enable**.
6. Click **Add**.

Distance Vector Multicast Routing Protocol

The 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. DVMRP maintains a link-state database to keep track of the return paths to the source of multicast packages.

The DVMRP operates as follows:

- The first message for any source-group pair is forwarded to the entire multicast network, with respect to the time-to-live (TTL) of the packet.
- TTL restricts the area to be flooded by the message.
- All the leaf routers that do not have members on directly attached subnetworks send back prune messages to the upstream router.
- The branch that transmitted a prune message is deleted from the delivery tree.
- The delivery tree, which is spanning to all the members in the multicast group, is constructed.

In this example, DVMRP is running on switches A, B, and C. IGMP is also running on Switch C, which is connected to the host directly. After the host sends an IGMP report to switch C,

multicast streams are sent from the multicast resource to the host along the path built by DVMRP.

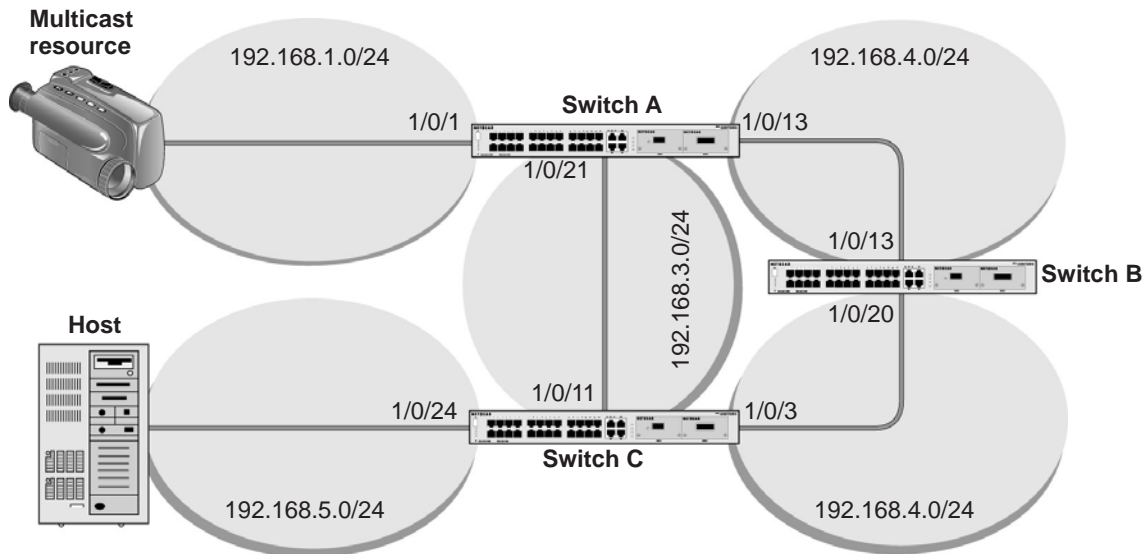


Figure 50. DVMRP

CLI: Configure DVMRP

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 the switch.

```
(Netgear Switch) (Config)#ip multicast
```

3. Enable DVMRP protocol on the switch.

```
(Netgear Switch) (Config)#ip dvmrp
```

4. Enable DVMRP mode on the interfaces 1/0/1, 1/0/13, and 1/0/21.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#ip dvmrp
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#ip dvmrp
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#ip dvmrp
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) #show ip dvmrp neighbor
Interface ..... 1/0/13
Neighbor IP Address ..... 192.168.2.2
State ..... Active
Up Time (hh:mm:ss) ..... 00:02:40
Expiry Time (hh:mm:ss) ..... 00:00:25
Generation ID ..... 1116347719
Major Version ..... 3
Minor Version ..... 255
Capabilities ..... Prune GenID Missing 11441
Received Routes ..... 0
Received Bad Packets ..... 0
Received Bad Routes ..... 0
Interface ..... 1/0/21
Neighbor IP Address ..... 192.168.3.1
State ..... Active
Up Time (hh:mm:ss) ..... 00:01:44
Expiry Time (hh:mm:ss) ..... 00:00:28
Generation ID ..... 1116595047
Major Version ..... 3
Minor Version ..... 255
More Entries or quit(q)
Capabilities ..... Prune GenID Missing 11441
Received Routes ..... 0
Received Bad Packets ..... 0
Received Bad Routes ..... 0
```

```
(Netgear Switch) #show ip mcast mroute summary
```

```

          Multicast Route Table Summary

Source IP      Group IP      Protocol      Incoming      Outgoing
-----      -
192.168.1.2    225.0.0.1    DVMRP         1/0/1         1/0/21

```

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 the switch.

```
(Netgear Switch) (Config)#ip multicast
```

3. Enable DVMRP protocol on the switch.

```
(Netgear Switch) (Config)#ip dvmrp
```

4. Enable DVMRP mode on interfaceS 1/0/13 and 1/0/20.

```

(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#ip dvmrp
(Netgear Switch) (Interface 1/0/13)#ex
(Netgear Switch) (Config)#interface 1/0/20
(Netgear Switch) (Interface 1/0/20)#ip dvmrp
(Netgear Switch) (Interface 1/0/20)#exit
(Netgear Switch) (Config)#exit

```

```
(Netgear Switch) #show ip dvmrp neighbor
Interface ..... 1/0/13
Neighbor IP Address ..... 192.168.2.1
State ..... Active
Up Time (hh:mm:ss) ..... 00:02:26
Expiry Time (hh:mm:ss) ..... 00:00:20
Generation ID ..... 88091
Major Version ..... 3
Minor Version ..... 255
Capabilities ..... Prune GenID Missing 11441
Received Routes ..... 0
Received Bad Packets ..... 0
Received Bad Routes ..... 0
Interface ..... 1/0/20
Neighbor IP Address ..... 192.168.4.2
State ..... Active
Up Time (hh:mm:ss) ..... 00:01:44
Expiry Time (hh:mm:ss) ..... 00:00:29
Generation ID ..... 1116595033
Major Version ..... 3
Minor Version ..... 255
Capabilities ..... Prune GenID Missing 11441
Received Routes ..... 0
Received Bad Packets ..... 0
Received Bad Routes ..... 0

(Netgear Switch) #show ip mcast mroute detail summary

                Multicast Route Table Summary
                Incoming      Outgoing
Source IP      Group IP      Protocol  Interface  Interface List
-----
192.168.1.2    225.0.0.1    DVMRP     1/0/13
```

DVRMP on Switch C:

1. Create routing interfaces 1/0/11, 1/0/3, and 1/0/24.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip interface 1/0/11
(Netgear Switch) (Interface 1/0/11)#ip routing
(Netgear Switch) (Interface 1/0/11)#ip address 192.168.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/11)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.168.4.2 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#routing
(Netgear Switch) (Interface 1/0/24)#ip address 192.168.5.1 255.255.255.0
(Netgear Switch) (Interface 1/0/24)#exit
```

2. Enable IP multicast forwarding on the switch.

```
(Netgear Switch) (Config)#ip multicast
```

3. Enable IP DVMRP protocol on the switch.

```
(Netgear Switch) (Config) #ip dvmrp
```

4. Enable DVMRP mode on interfaces 1/0/3, 1/0/11, and 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip dvmrp
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#interface 1/0/11
(Netgear Switch) (Interface 1/0/11)#ip dvmrp
(Netgear Switch) (Interface 1/0/11)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#ip dvmrp
(Netgear Switch) (Interface 1/0/24)#exit
```

5. Enable IGMP protocol on the switch.

```
(Netgear Switch) (Config)# ip igmp
```

6. Enable IGMP mode on the interface 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#ip igmp
(Netgear Switch) (Interface 1/0/24)#exit
```

```
(Netgear Switch) #show ip dvmrp neighbor
Interface ..... 1/0/11
Neighbor IP Address ..... 192.168.3.2
State ..... Active
Up Time (hh:mm:ss) ..... 00:01:03
Expiry Time (hh:mm:ss) ..... 00:00:24
Generation ID ..... 88099
Major Version ..... 3
Minor Version ..... 255
Capabilities ..... Prune GenID Missing 11441
Received Routes ..... 0
Received Bad Packets ..... 0
Received Bad Routes ..... 0
Interface ..... 1/0/3
Neighbor IP Address ..... 192.168.4.1
State ..... Active
Up Time (hh:mm:ss) ..... 00:01:17
Expiry Time (hh:mm:ss) ..... 00:00:23
Generation ID ..... 1116347728
Major Version ..... 3
Minor Version ..... 255

More Entries or quit(q)
Capabilities ..... Prune GenID Missing 11441
Received Routes ..... 0
Received Bad Packets ..... 0
Received Bad Routes ..... 0
(Netgear Switch) #show ip mcast mroute detail summary

                          Multicast Route Table Summary

Source IP      Group IP      Protocol      Incoming      Outgoing
-----      -
192.168.1.2    225.0.0.1    DVMRP         1/0/11        1/0/24
```

Web Interface: Configure DVMRP

DVMRP on Switch A

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.

The screenshot shows the 'IP Configuration' page in the web interface. The 'Routing Mode' is set to 'Enable' (radio button selected). Other settings include: Default Time to Live: 64; ICMP Echo Replies: Enable; ICMP Redirects: Enable; ICMP Rate Limit Interval: 1000; ICMP Rate Limit Burst Size: 100; Maximum Next Hops: 4.

- b. For Routing Mode, select the **Enable** radio button.
 - c. Click **Apply**.
2. Configure 1/0/1 as a routing port and assign an IP address to it.
 - a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

The screenshot shows the 'IP Interface Configuration' page. A table lists the configured interfaces:

Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input type="checkbox"/>	1/0/1		192.168.1.1	255.255.255.0	Enable	Enable
<input checked="" type="checkbox"/>	1/0/1		0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the Port **1/0/1** check box. Now 1/0/1 appears in the Port field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.1.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
3. Configure 1/0/13 as a routing port and assign an IP address to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

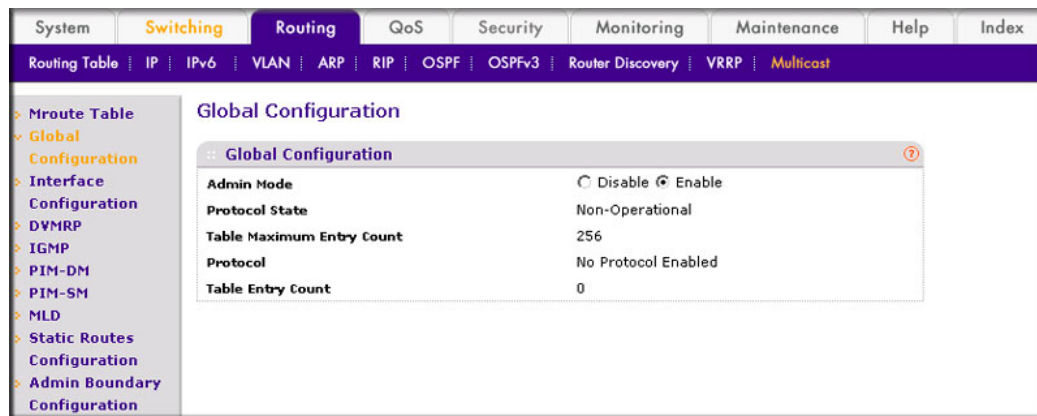
Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/13			192.168.2.1	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/1			192.168.1.1	255.255.255.0	Enable	Enable

- b. Scroll down and select the Port **1/0/13** check box. Now 1/0/13 appears in the Port field at the top.
- c. Enter the following information:
- In the **IP Address** field, enter **192.168.2.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
4. Configure 1/0/21 as a routing port and assign an IP address to it.
- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/21			192.168.3.2	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/1			192.168.1.1	255.255.255.0	Enable	Enable

- b. Scroll down and select the Port **1/0/13** check box. Now 1/0/13 appears in the Port field at the top.
- c. Enter the following information:.
- In the **IP Address** field, enter **192.168.3.2**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
5. Enable IP multicast on the switch.

- a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.

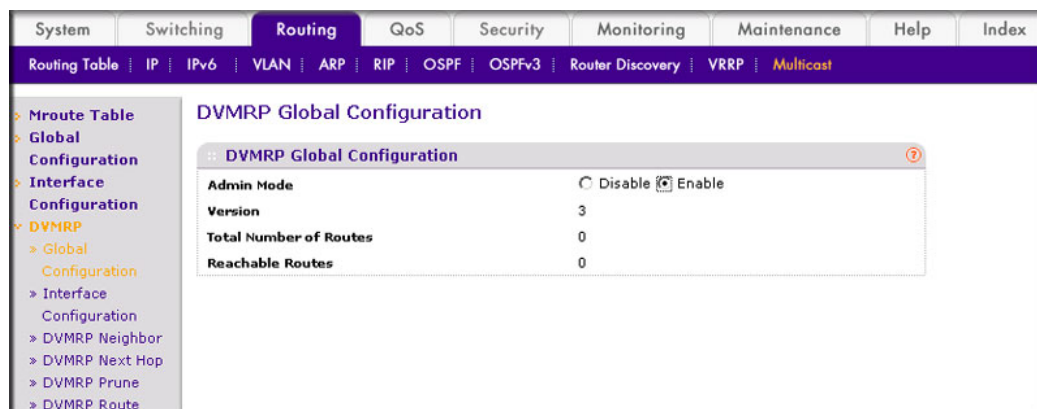


- b. For Admin Mode, select the **Enable** radio button.

- c. Click **Apply**.

6. Enable DVMRP on the switch.

- a. Select **Routing > Multicast > DVMRP > Global Configuration**. A screen similar to the following displays.

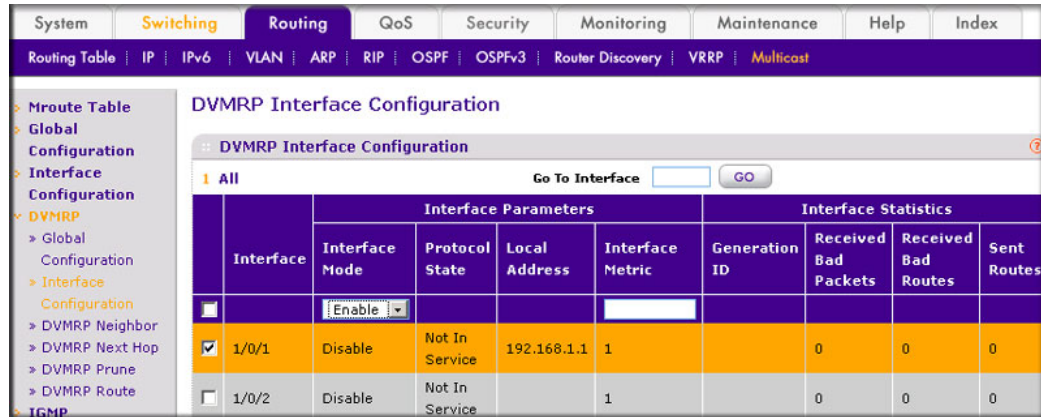


- b. For Admin Mode, select the **Enable** radio button.

- c. Click **Apply**.

7. Enable DVMRP on the interface.

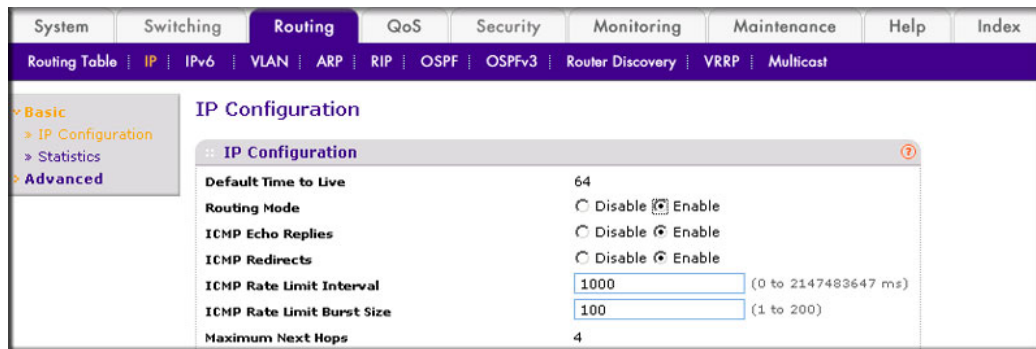
- a. Select **Routing > Multicast > DVMRP > Interface Configuration**. A screen similar to the following displays.



- b. Scroll down select the Interface **1/0/1, 1/0/13, and 1/0/21** check boxes.
- c. In the **Interface Mode** field, select **300**.
- d. Click **Apply** to save the settings.

DVMRP on Switch B

1. Enable IP routing on the switch.
 - a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.



- b. For Routing Mode, select the **Enable** radio button.
 - c. Click **Apply**.
2. Configure 1/0/13 as a routing port and assign and IP address to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

The screenshot shows the 'IP Interface Configuration' page. The 'Port' column has a checkmark next to '1/0/13'. The 'IP Address' field is '192.168.2.2' and the 'Subnet Mask' is '255.255.255.0'. The 'Routing Mode' is set to 'Enable' and the 'Administrative Mode' is 'Enable'. The '1/0/1' port is unchecked and has '0.0.0.0' for both IP and Subnet Mask, with 'Disable' for Routing Mode and 'Enable' for Administrative Mode.

Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/13			192.168.2.2	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the Port **1/0/13** check box. Now 1/0/13 appears in the Port field at the top.
- c. Enter the following information in the IP Interface Configuration.
- In the **IP Address** field, enter **192.168.2.2**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
3. Configure 1/0/20 as a routing port and assign an IP address to it.

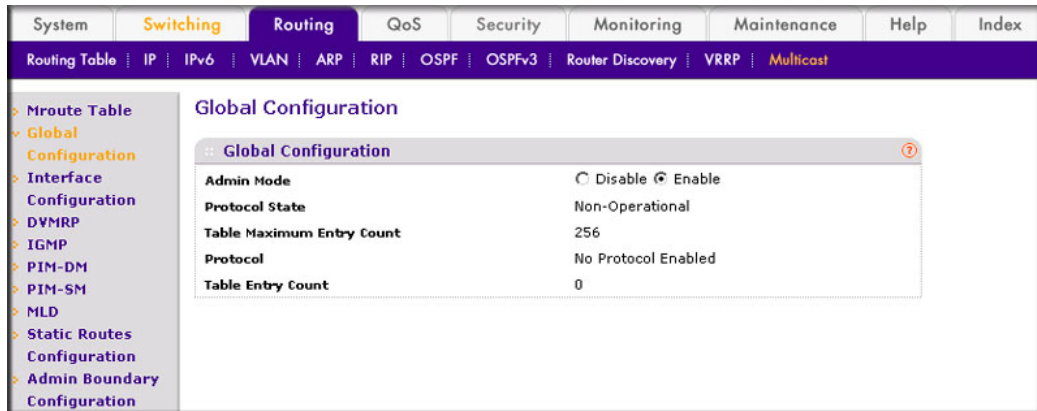
- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

The screenshot shows the 'IP Interface Configuration' page. The 'Port' column has a checkmark next to '1/0/20'. The 'IP Address' field is '192.168.4.1' and the 'Subnet Mask' is '255.255.255.0'. The 'Routing Mode' is set to 'Enable' and the 'Administrative Mode' is 'Enable'. The '1/0/1' port is unchecked and has '0.0.0.0' for both IP and Subnet Mask, with 'Disable' for Routing Mode and 'Enable' for Administrative Mode.

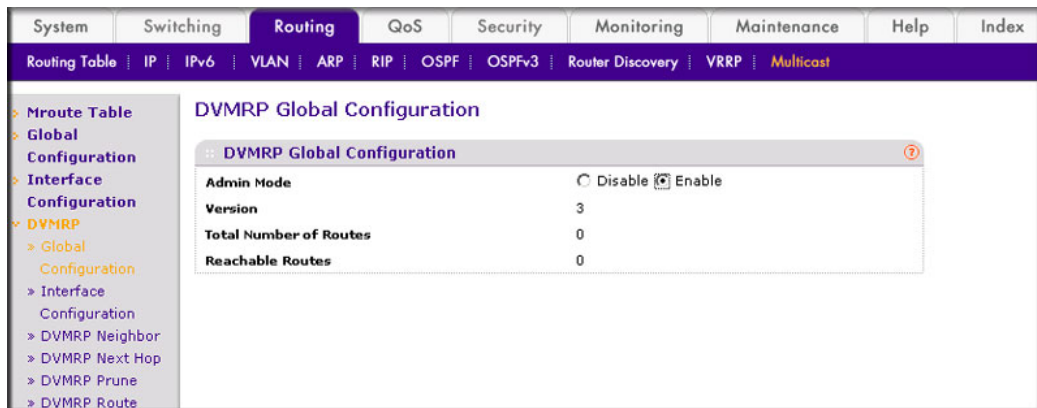
Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/20			192.168.4.1	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll and select the Port **1/0/20** check box. Now 1/0/20 appears in the Interface field at the top.
- c. Enter the following information:
- In the **IP Address** field, enter **192.168.4.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
4. Enable IP multicast on the switch.

- a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.



- b. For Admin Mode, select the **Enable** radio button.
 - c. Click **Apply**.
5. Enable DVMRP on the switch.
 - a. Select **Routing > Multicast > DVMRP > Global Configuration**. A screen similar to the following displays.



- b. For Admin Mode, select the **Enable** radio button.
 - c. Click **Apply**.
6. Enable DVMRP on the interface.

- a. Select **Routing > Multicast > DVMRP > Interface Configuration**. A screen similar to the following displays.

DVMRP Interface Configuration									
DVMRP Interface Configuration									
1 All									
Go To Interface <input type="text"/> <input type="button" value="GO"/>									
	Interface	Interface Parameters				Interface Statistics			
		Interface Mode	Protocol State	Local Address	Interface Metric	Generation ID	Received Bad Packets	Received Bad Routes	Sent Routes
<input type="checkbox"/>	1/0/1	Enable	Not In Service		1		0	0	0

- b. Scroll down and select the Interface **1/0/13** and **1/0/20** check boxes.
 c. In the **Interface Mode** field, select **Enable**.
 d. Click **Apply** to save the settings.

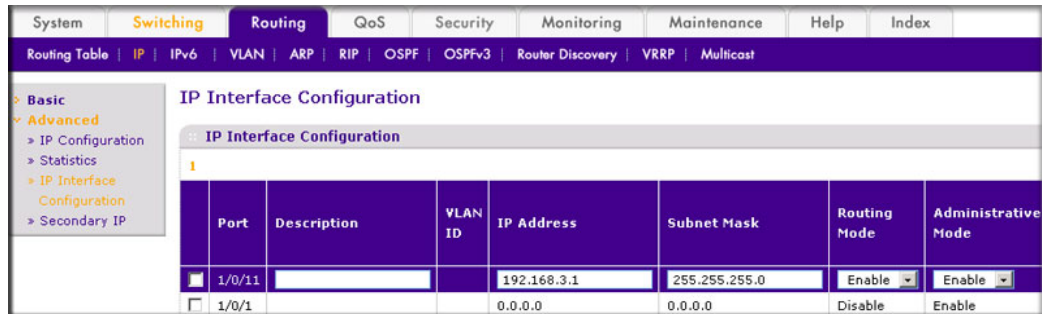
DVMRP on Switch C

- Enable IP routing on the switch.
 - Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.

IP Configuration	
Default Time to Live	64
Routing Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
ICMP Echo Replies	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
ICMP Redirects	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
ICMP Rate Limit Interval	<input type="text" value="1000"/> (0 to 2147483647 ms)
ICMP Rate Limit Burst Size	<input type="text" value="100"/> (1 to 200)
Maximum Next Hops	4

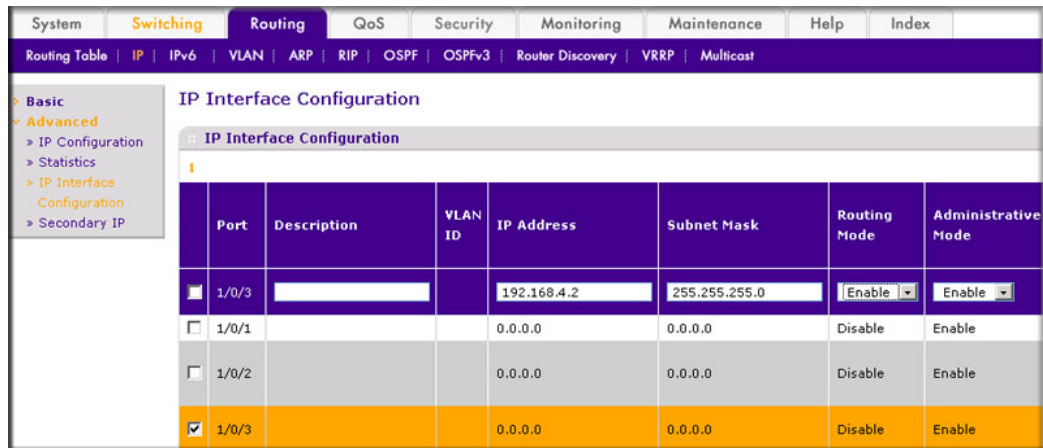
- For Routing Mode, select the **Enable** radio button.
 - Click **Apply**.
- Configure 1/0/11 as a routing port and assign an IP address to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Port **1/0/11** check box. Now 1/0/11 appears in the Port field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.3.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
3. Configure 1/0/3 as a routing port and assign an IP address to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Port **1/0/3** check box. Now 1/0/3 appears in the Port field at the top.
 - c. Enter the following information:
 - In the **IP Address** field, enter **192.168.4.2**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
 - d. Click **Apply** to save the settings.
4. Configure 1/0/24 as a routing port and assign an IP address to it.

- a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

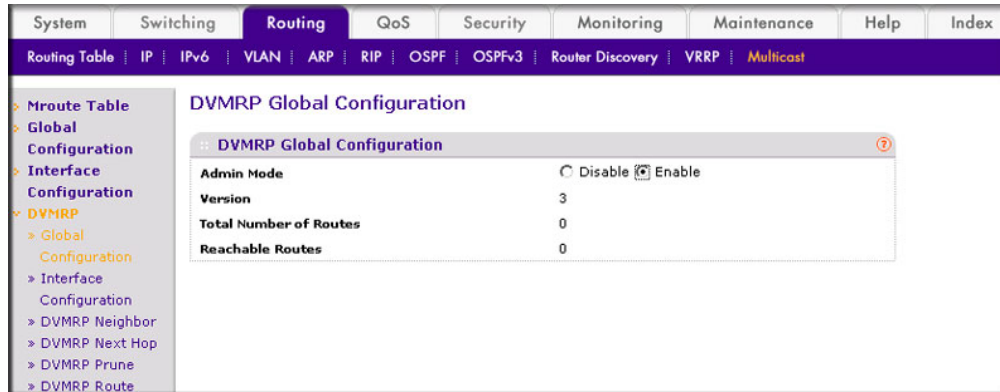
Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
<input checked="" type="checkbox"/> 1/0/24			192.168.5.1	255.255.255.0	Enable	Enable
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

- b. Scroll down and select the Port **1/0/24** check box. Now 1/0/24 appears in the Port field at the top.
- c. Enter the following information:
- In the **IP Address** field, enter **192.168.5.1**.
 - In the **Subnet Mask** field, enter **255.255.255.0**.
 - In the **Routing Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
5. Enable IP multicast on the switch.
- a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.

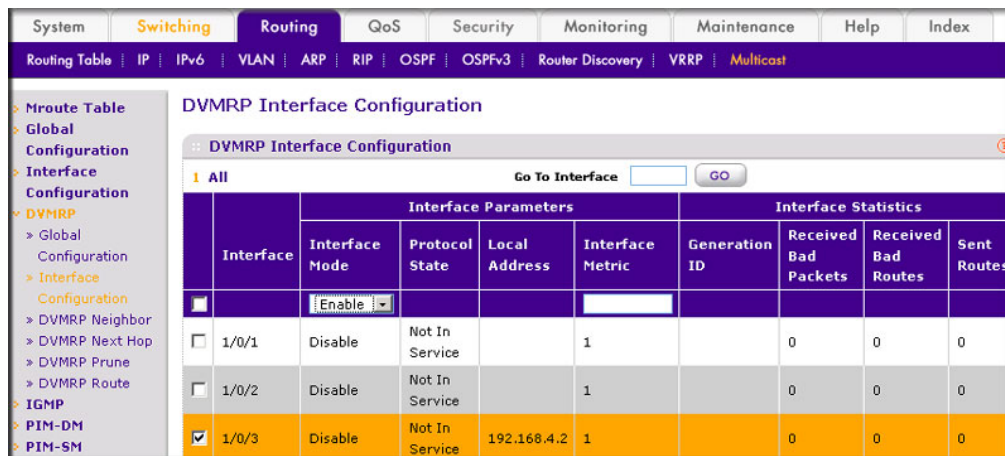
Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Protocol State	Non-Operational
Table Maximum Entry Count	256
Protocol	No Protocol Enabled
Table Entry Count	0

- b. For Admin Mode, select the **Enable** radio button.
- c. Click **Apply**.
6. Enable DVMRP on the switch.

- a. Select **Routing > Multicast > DVMRP > Global Configuration**. A screen similar to the following displays.

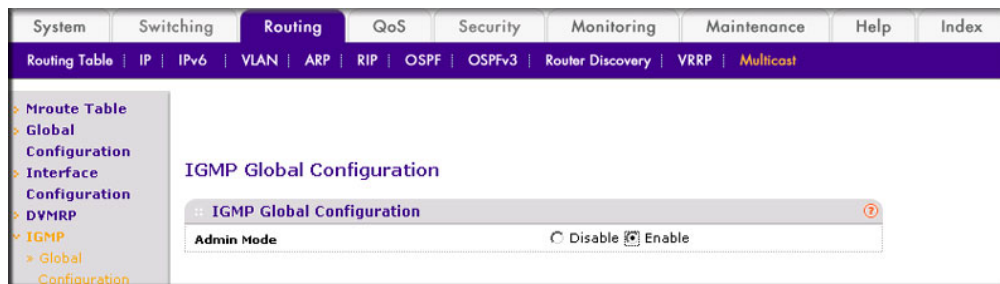


- b. For Admin Mode, select the **Enable** radio button.
 - c. Click **Apply**.
7. Enable DVMRP on the interface.
 - a. Select **Routing > Multicast > DVMRP > Interface Configuration**. A screen similar to the following displays.

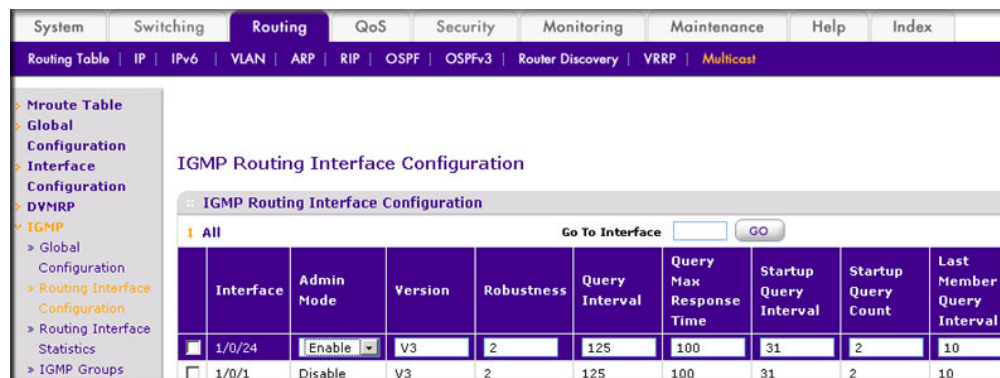


- b. Scroll down and select the Interface **1/0/3**, **1/0/11**, and **1/0/24** check boxes.
 - c. Select **Enable** in the **Interface Mode** field.
 - d. Click **Apply** to save the settings.
8. Enable IGMP on the switch.

- a. Select **Routing > Multicast > IGMP > Global Configuration**. A screen similar to the following displays.



- b. For Admin Mode, select the **Enable** radio button.
- c. Click **Apply**.
9. Enable IGMP on the interface.
- a. Select **Routing > Multicast > IGMP > Routing Interface Configuration**. A screen similar to the following displays.



- b. Scroll down and select the Interface **1/0/24** check box. Now 1/0/24 appears in the Interface field at the top.
- c. In the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.

This chapter includes the following sections:

- *Captive Portal Configuration* on page 532
- *Enable Captive Portal* on page 532
- *Client Access, Authentication, and Control* on page 534
- *Block a Captive Portal Instance* on page 535
- *Local Authorization, Create Users and Groups* on page 535
- *Remote Authorization (RADIUS) User Configuration* on page 537
- *SSL Certificates* on page 539

The captive portal feature is a software implementation that blocks clients from accessing the network until user verification has been established. You can set up verification to allow access for both guests and authenticated users. Authenticated users must be validated against a database of authorized captive portal users before access is granted.

The authentication server supports both HTTP and HTTPS Web connections. In addition, you can configure captive portal to use an optional HTTP port (in support of HTTP proxy networks). If configured, this additional port is then used exclusively by captive portal. Note that this optional port is in addition to the standard HTTP port 80, which is currently being used for all other Web traffic.

Captive portal for wired interfaces allows the clients directly connected to the switch to be authenticated using a captive portal mechanism before the client is given access to the network. When a wired physical port is enabled for captive portal, the port is set in captive-portal-enabled state such that all the traffic coming to the port from the unauthenticated clients is dropped except for the ARP, DHCP, DNS and NETBIOS packets. The switch forwards these packets so that unauthenticated clients can get an IP address and resolve the hostname or domain names. Data traffic from authenticated clients goes through, and the rules do not apply to these packets.

All the HTTP/HTTPS packets from unauthenticated clients are directed to the CPU on the switch for all the ports that are enabled for captive portal. When an unauthenticated client opens a Web browser and tries to connect to network, the captive portal redirects all the HTTP/HTTPS traffic from unauthenticated clients to the authenticating server on the switch. A captive portal Web page is sent back to the unauthenticated client. The client can authenticate. If the client successfully authenticates, the client is given access to port.

You can enable captive portal on all the physical ports on the switch. It is not supported for VLAN interfaces, loopback interfaces or logical interfaces. The captive portal feature uses MAC-address based authentication and not port-based authentication. This means that all the clients connected to the captive portal interface must be authenticated before they can get access to the network.

Clients connecting to the captive portal interface have three states; unknown, unauthenticated, and authenticated.

- **Unknown.** In the unknown state, the captive portal does not redirect HTTP/S traffic to the switch, but instead asks the switch whether the client is authenticated or unauthenticated.
- **Unauthenticated.** The captive portal directs the HTTP/S traffic to the switch so that the client can authenticate with the switch.
- **Authenticated.** After successful authentication, the client is placed in authenticated state. In this state, all the traffic emerging from the client is forwarded through the switch.

Captive Portal Configuration

This section introduces the objects that make up the captive portal and describes the interaction between the captive portal and the network administrator. It explains what configurations are visible to the network administrator and enumerates the events.

All the configurations included in this section are managed using the CLI, the Web Interface, and SNMP, with one exception; to customize the captive portal Web page, you must use the Web Interface.

The captive portal configuration provides the network administrator control over verification and authentication, assignment to interfaces, client sessions, and Web page customization.

You can create multiple captive portal configuration instances. Each captive portal configuration contains various flags and definitions used to control client access and content to customize the user verification Web page. A captive portal configuration can be applied to one or more interfaces. An interface can only be a physical port on the switch. Software release 8.0 and newer versions can contain up to 10 captive portal configurations.

Enable Captive Portal

CLI: Enable Captive Portal

1. Enable captive portal on the switch.

```
(Netgear Switch) (config)#captive-portal
(Netgear Switch) (Config-CP)#enable
```

2. Enable captive portal instance 1.

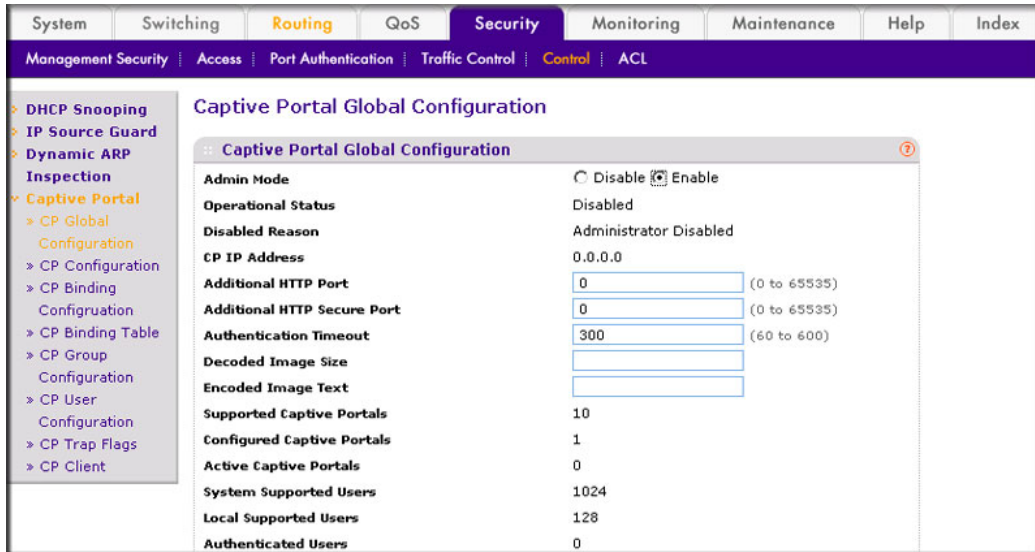
```
(Netgear Switch) (Config-CP)#configuration 1
(Netgear Switch) (Config-CP 1)#enable
```

3. Enable captive portal instance 1 on port 1/0/1.

```
(Netgear Switch) (Config-CP 1)#interface 1/0/1
```

Web Interface: Enable Captive Portal

1. Enable captive portal on the switch.
 - a. Select **Security > Control > Captive Portal > CP Global Configuration**. A screen similar to the following displays.



- b. For Admin Mode, Select the **Enable** radio button.
 - c. Click **Apply**.
2. Enable captive portal instance 1 on the switch.

- a. Select **Security > Control > Captive Portal > CP Configuration**. A screen similar to the following displays.

CP ID	CP Name	Admin Mode	Protocol	Verification	Block	Group
1	Default	Enable	http	Guest	Disable	0

- b. Scroll down and select the CP 1 check box. Now CP 1 appears in the CP ID field at the top.
- c. In the **Admin Mode** field, select **Enable**.
- d. Click **Apply** to save the settings.
3. Enable CP 1 on interface 1/0/1.
- a. Select **Security > Controls > Captive Portal > CP Binding Configuration**. A screen similar to the following displays.

CP ID	CP Name
1	Default

Unit 1	Port 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	<input checked="" type="checkbox"/>																							

- b. In the **CP ID** list, select **1**.
- c. Click **Unit 1**. The ports display.
- d. Click the gray box under port **1**.
- e. Click **Apply**.

Client Access, Authentication, and Control

User verification can be configured to allow access for guest users—users who do not have assigned user names and passwords. User verification can also be configured to allow access for authenticated users. Authenticated users are required to enter a valid user name and password that must first be validated against the local database or a RADIUS server. Network access is granted once user verification has been confirmed. The administrator can block access to a captive portal configuration. When an instance is blocked, no client traffic is allowed through any interfaces associated with that captive portal configuration. Blocking a

captive portal instance is a temporary command executed by the administrator and not saved in the configuration.

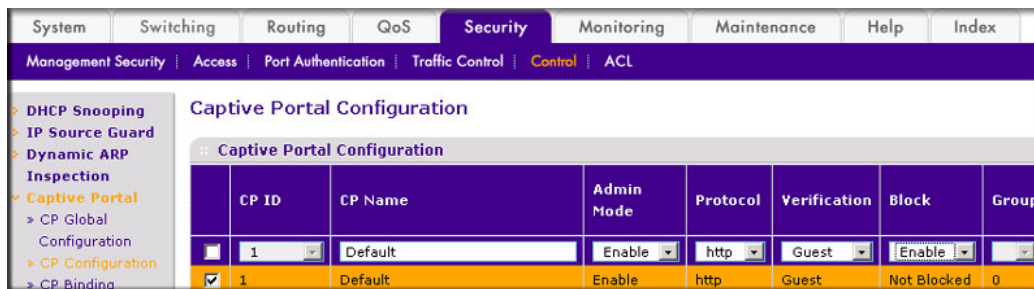
Block a Captive Portal Instance

CLI: Block a Captive Portal Instance

```
(Netgear Switch)(Config-CP 1)#block
```

Web Interface: Block a Captive Portal Instance

1. Select **Security > Control > Captive Portal > CP Configuration**. A screen similar to the following displays.



2. Under Captive Portal Configuration, scroll down and select the CP 1 check box. Now CP 1 appears in the CP ID field at the top.
3. In the **Block** field, select **Enable**.
4. Click **Apply** to save the settings.

Local Authorization, Create Users and Groups

When using local authentication, the administrator provides user identities for captive portal by adding unique user names and passwords to the local user database. This configuration is global to the captive portal component and can contain up to 128 user entries (a RADIUS server should be used if more users are required). A local user can belong to one or more groups. There is one group created by default with the group name *Default* to which all new users are assigned. All new captive portal instances are also assigned to the Default group. You can create new groups and modify the user/group association to allow only a subset of users access to a specific captive portal instance. Network access is granted upon successful user name, password, and group verification.

CLI: Create Users and Groups

1. Create a group whose group ID is 2.

```
(Netgear Switch) #config
(Netgear Switch) (config)#captive-portal
(Netgear Switch)(Config-CP)# user group 2
```

2. Create a user whose name is user1.

```
(Netgear Switch) (Config-CP)#user 2 name user1
```

3. Configure the user's password.

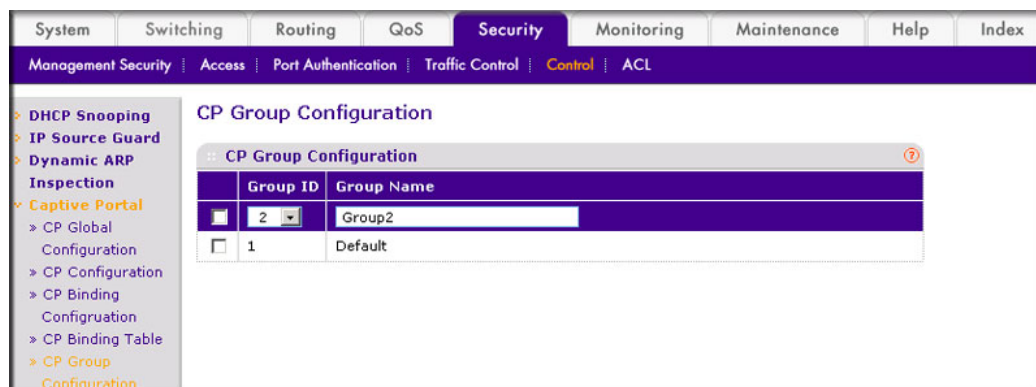
```
(Netgear Switch) (Config-CP)#user 2 password
Enter password (8 to 64 characters): 12345678
Re-enter password: 12345678
```

4. Add the user to the group.

```
(Netgear Switch) (Config-CP)#user 2 group 2
```

Web Interface: Create Users and Groups

1. Create a group.
 - a. Select **Security > Control > Captive Portal > CP Group Configuration**. A screen similar to the following displays.



- b. Enter the following information:
 - In the **Group ID** field, select **2**.
 - In the **Group Name** field, enter **Group2**.

- c. Click **Add**.
2. Create a user.
 - a. Select **Security > Control > Captive Portal > CP User Configuration**. A screen similar to the following displays.

User ID	User Name	Password	Confirm Password	Group	Session Timeout
2	user1	*****	*****	2	

- b. Enter the following information:
 - In the **User ID** Field, enter **2**.
 - In the **User Name** field, enter **user1**.
 - In the **Password** field, enter **12345678**.
 - In the **Confirm Password** field, enter **12345678**.
 - In the **Group** field, select **2**.
- c. Click **Add**.

Remote Authorization (RADIUS) User Configuration

A remote RADIUS server can be used for client authentication. In software release 8.0 (or newer), the RADIUS authentication and accounting servers are configured separate from the captive portal configuration. In order to perform authentication and accounting using RADIUS, you configure one or more RADIUS servers and then references the servers using their names in the captive portal configuration. Each captive portal instance can be assigned one RADIUS authentication server and one RADIUS accounting server.

If RADIUS is enabled for a captive portal configuration and no RADIUS servers are assigned, the captive portal activation status will indicate that the instance is disabled with an appropriate reason code.

The following table indicates the RADIUS attributes that are used to configure captive portal users. The table indicates both RADIUS attributes and vendor specific attributes (VSA) that

are used to configure captive portal. VSAs are denoted in the ID column and are comma delimited (vendor ID, attribute ID).

Table 4. RADIUS Attributes for Configuring Captive Portal Users

RADIUS Attribute	No.	Description	Range	Usage	Default
User-Name	1	User name to be authorized.	1–32 characters	Required	None
User-Password	2	User password.	8–64 characters	Required	None
Session-Timeout	27	Logout once session timeout is reached (seconds). If the attribute is 0 or not present then 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, then use the value configured for the captive portal.	Integer (seconds)	Optional	0
WISPr-Max-Band width-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, then use the value configured for the captive portal.	Integer	Optional	0
WISPr-Max-Band width-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, then use the value configured for the captive portal.	Integer	Optional	0

CLI: Configure RADIUS as the Verification Mode

```
(Netgear Switch) (Config-CP 1)#radius-auth-server Default-RADIUS-Server
(Netgear Switch) (Config-CP 1)#verification radius
```

Web Interface: Configure RADIUS as the Verification Mode

1. Select **Security > Control > Captive Portal > CP Configuration**. A screen similar to the following displays.

CP ID	CP Name	Admin Mode	Protocol	Verification	Block	Group
<input type="checkbox"/> 1	Default	Enable	http	RADIUS		1
<input checked="" type="checkbox"/> 1	Default	Enable	http	Local	Not Blocked	1

2. Scroll down and select the CP 1 check box. Now CP 1 appears in the CP ID field at the top.
3. Enter the following information:
 - In the **Verification** field, select **RADIUS**.
 - In the **Radius Auth Server** field, enter the RADIUS server name **Default-RADIUS-Server**.
4. Click **Apply**.

SSL Certificates

A captive portal instance can be configured to use the HTTPS protocol during its user verification process. The connection method for HTTPS uses the Secure Sockets Layer (SSL) protocol, which requires a certificate to provide encryption. The certificate is presented to the user at connection time.

In software release 8.0 (or newer), the captive portal uses the same certificate that is used for secure HTTP connections. You can generate this certificate using a CLI command. If a captive portal instance is configured for the HTTPS protocol and there is not a valid certificate present on the system, the captive portal instance status will show Disabled with an appropriate reason code.

Index

Numerics

6to4 tunnels **406**
802.1x port security **271**

A

ACL mirroring **167**
ACL redirect **172**
ACLs **131**
 IP ACL configuration **132**
 IPv6 **177**
 isolated VLANs on a Layer 3 switch **153**
 MAC ACLs **132, 164**
 TCP flag **137**
ARP **123**
 dynamic ARP inspection **288, 289, 290**
ARP, dynamic inspection **302, 303**
Auto VoIP **217, 218, 220**

B

banner, pre-login **319**

C

captive portal **531**
 configuration **532**
classic STP (802.1d) **400**
code mismatch (stacked switches) **343**
color conform policy
 DiffServ
 color conform policy **228, 229**
configuration scripting **316**
CoS
 cos-queue min-bandwidth **189**
 per-interface basis **186**
 set classofservice trust mode **187**
 setting Trust Mode **190**
 show classofservice ip-precedence mapping **188**
 show classofservice trust **186**
 traffic shaping **191**
CoS queue configuration **186**
CoS queue configuratoin **186**
CoS queue mapping **185**

CoS queueing **184**

D

default VLAN **24**
DHCP L2 relay **478, 479, 480**
DHCP L3 relay **484, 485**
DHCP messages, maximum rate **300, 301**
DHCP reservation, configuring **376**
DHCP server, dynamic mode **373**
DHCP snooping **296, 297**
DiffServ **193**
 Auto VoIP **217, 218, 220**
 edge device **193**
 interior node **193**
 IPv6 **221, 222**
 VoIP **210**
Diffserv
 VoIP **212**
distance vector multicast routing protocol (DVMRP) **513**
DNS **370**
 host name and IP address **371**
documentation **15**
dual image **321**
DVMRP **513, 514, 520**

E

Ethernet configuration for stacking ports **344**

F

firmware
 upgrading stacked switches **343, 344**
firmware for stacked switches **342**

G

gaming **241**
guest VLAN **277, 278, 279**

I

IGMP querier **241, 242**
 enable **242, 243**
 status **245**

IGMP snooping **237, 242**
 238
 external multicast router **239, 240**
 multicast router using VLAN **240, 241**
 show igmpsnooping **238**
 show ignpsnooping **238**
 show mac-address-table **239**
 show mac-address-table igmpsnooping **239**

IGMPv3 **236**

interpreting log files **328**

IP ACLs **132, 133**

IP routing
 port routing **59, 60**
 VLAN routing OSPF configuration **113**
 VLAN routing RIP configuration **80, 82**

IP source guard **302, 303**

IPTV **241**

IPv6 **414**
 network interface **417**
 routing interface **414**
 routing VLAN **419**

L

LAGS
 creating **54**

LAGs **53, 59**
 adding ports **55, 57**
 creating **54**
 enabling **58**

logs
 show logging hosts **333**

M

MAC ACLs **132, 164**

MLD **494, 495, 497**

MLD Snooping **508**

MLD snooping **508, 509, 510**

multicast listener discovery (MLD) **494**

N

NVT **324**

O

OSPF **60, 84, 113**
 border router configuration **90**
 inter-area router **85**
 nssa area **104**

 stub area configuration **95**
 VLAN routing **113**

OSPFv3 **118**

outbound Telnet **324**

P

PIM **427**

PIM-DM **427, 429, 433**

PIM-SM **451, 452, 456**

port mirroring **320, 321**
 activate backup image **322**
 dual image **321**

port routing
 adding a default route **64**
 adding a static route **65, 66**
 configuration **60**
 enabling routing for ports **61, 62**
 enabling routing for the switch **61**

port security
 802.1x **271, 272**
 convert dynamic to static address **263**
 static MAC address **264**

private edge VLANs **17**

private VLAN groups **394**

protected ports **264, 265, 267**

Protocol-independent multicast sparse mode **451**

Protocol-Independent-Multicast **427**

Proxy Address Resolution Protocol **123**

Q

QoS
 class **194**
 policy **194**
 service **194**

R

RADIUS
 assigning VLANs **282, 283, 285**

rapid STP (802.1w) **402**

RIP **60, 74, 80**
 VLAN routing **80, 82**

Routing Information Protocol (RIP) **74**

S

script **317**

script delete **317**

script list **317**

scripting, configuration **316**

security

- 802.1x port security [271](#), [272](#)
 - DHCP messages, maximum rate [300](#), [301](#)
 - DHCP snooping [296](#), [297](#)
 - IP source guard [302](#)
 - protected ports [264](#), [267](#)
 - static binding [299](#), [300](#)
 - static mapping [294](#), [295](#)
 - sFlow [365](#), [366](#), [367](#)
 - sFlow, time-based sampling of counters [369](#)
 - show logging [329](#)
 - show logging buffered [331](#)
 - show logging hosts [333](#)
 - show logging traplogs [332](#)
 - show network [325](#)
 - show SNTP (CLI only) [307](#)
 - show switch [342](#)
 - show telnet [325](#)
 - SNMP [361](#)
 - SNMP trap [362](#)
 - SNTP [307](#)
 - configure [309](#)
 - SNTP server [311](#)
 - Spanning Tree protocol [400](#)
 - stack members, renumbering [354](#)
 - stacking
 - moving a master to a different stack [356](#)
 - stacking ports, Ethernet configuration [344](#)
 - stacks
 - adding switches to [350](#)
 - code mismatch [343](#)
 - compatible switch models [341](#)
 - firmware [342](#)
 - installation [342](#)
 - removing switches from [351](#)
 - upgrading firmware [343](#), [344](#)
 - stacks, 10G fiber [347](#), [348](#), [349](#)
 - static binding [299](#), [300](#)
 - static host name [370](#)
 - static mapping [294](#), [295](#)
 - STP
 - multiple STP (802.1s) [403](#)
 - STPs [400](#)
 - switch
 - FSM family of switches [341](#)
 - GSM family of switches [341](#)
 - switch priority [341](#)
 - switch stack
 - configuration files [352](#)
 - member numbers [340](#)
 - member priority values [341](#)
 - membership [340](#)
 - software compatibility [352](#)
 - upgrading firmware [343](#)
 - Syslog
 - show logging [329](#)
 - show logging buffered [331](#)
 - syslog [328](#)
- ## T
- technical support [2](#)
 - Telnet
 - configure [326](#)
 - session-limit [327](#)
 - session-timeout [327](#)
 - Telnet, outbound [324](#)
 - time, set the time zone (CLI only) [311](#)
 - traceroute [314](#), [315](#), [316](#)
 - trademarks [2](#)
 - transport output telnet [326](#)
 - tunnel [406](#), [407](#), [409](#)
- ## V
- video streaming [241](#)
 - VLAN
 - guest VLAN [277](#)
 - IPv6 routing VLAN [419](#)
 - private VLAN groups [394](#)
 - VLAN routing [72](#), [73](#)
 - VLANs [16](#)
 - assigning ports [19](#), [22](#), [23](#)
 - creating two VLANs [17](#)
 - default [24](#)
 - guest VLANs [277](#), [278](#), [279](#)
 - IP subnet based [30](#)
 - IP subnet-based [30](#), [31](#), [32](#)
 - MAC-based [25](#), [26](#)
 - private edge [17](#)
 - protocol-based [28](#), [29](#)
 - using RADIUS to assign [282](#), [283](#), [285](#)
 - VRRP [125](#)
 - backup router [128](#)
 - master router [126](#)
- ## W
- WRED [184](#)