

M5300, M6100, and M7100 Series ProSAFE Managed Switches

Software Administration Manual

Software Version 11.0.0

November 2015 202-11527-02

350 East Plumeria Drive San Jose, CA 95134 USA



Support

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

Conformity

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

Compliance

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

See the regulatory compliance document before connecting the power supply.

Trademarks

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

Revision History

Publication Part Number	Publication Date	Comments
202-11527-02	October 2015	 Made minor changes to the following chapters: Chapter 4, MLAGs Chapter 10, PBR
202-11527-01	March 2015	 Added the following chapters: Chapter 24, Switch Stacks Chapter 39, Override Factory Defaults Added the following sections: VLAN Access Ports and Trunk Ports Find a Rogue DHCP Server Use the Authentication Manager to Set Up an Authentication Method List Configure a Stateful DHCPv6 Server Configure PVSTP and PVRSTP Create a 6to4 Tunnel Made changes and minor additions to various commands.
202-11460-01	October 2014	 Added the following chapters: Chapter 9, BGP Chapter 10, PBR Chapter 40, NETGEAR SFP Added the following sections: Full Memory Dump Replaced the Switch Stack chapter with Chapter 23, Chassis Switch Management. Updated most of the rest of the manual.

202-11331-01	September 2013	Added the following chapters: • Chapter 4, MLAGs • Chapter 19, MAB Added or revised the following sections: • Configure GARP VLAN Registration Protocol • Configure a Management ACL • Authorization and Accounting • Auto VoIP • Remote SPAN
202-11161-01	February 2013	Updated the document.
	October 2012	Added iSCSI features.
202-11153-01	August 2012	Added Private VLAN features.
202-10515-05	August 2012	Added the MVR feature.
202-10515-05	July 2011	Added DHCPv6 and DHCPv6 mode features.
202-10515-04	November 2010	Converted the book to a new format.
202-10515-03	June 2010	Moved some content to the Software Setup Guide.
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		Initial publication.

Table of Contents

Chapter 1 Documentation Resources

Chapter 2 VLANs

VLAN Concepts	21
Create Two VLANs.	22
CLI: Create Two VLANs	22
Web Interface: Create Two VLANs	22
Assign Ports to VLAN 2	23
CLI: Assign Ports to VLAN 2	23
Web Interface: Assign Ports to VLAN 2	24
Create Three VLANs	25
CLI: Create Three VLANs	25
Web Interface: Create Three VLANs	25
Assign Ports to VLAN 3	27
CLI: Assign Ports to VLAN 3	27
Web Interface: Assign Ports to VLAN 3	27
Assign VLAN 3 as the Default VLAN for Port 1/0/2	28
CLI: Assign VLAN 3 as the Default VLAN for Port 1/0/2	28
Web Interface: Assign VLAN 3 as the Default VLAN for Port 1/0/2	29
Create a MAC-Based VLAN	29
CLI: Create a MAC-Based VLAN	30
Web Interface: Assign a MAC-Based VLAN	31
Create a Protocol-Based VLAN	33
CLI: Create a Protocol-Based VLAN	33
Web Interface: Create a Protocol-Based VLAN	34
Virtual VLANs: Create an IP Subnet-Based VLAN	37
CLI: Create an IP Subnet–Based VLAN	38
Web Interface: Create an IP Subnet-Based VLAN	39
Voice VLANs	40
CLI: Configure Voice VLAN and Prioritize Voice Traffic	41
Web Interface: Configure Voice VLAN and Prioritize Voice Traffic	43
Configure GARP VLAN Registration Protocol	48
CLI: Enable GVRP	49
Web Interface: Configure GVRP on switch A	51
Web Interface: Configure GVRP on Switch B	53
Private VLANs	54
Assign Private-VLAN Types (Primary, Isolated, Community)	56
CLI: Assign Private-VLAN Type (Primary, Isolated, Community)	56
Web Interface: Assign Private-VLAN Type (Primary,	
Isolated, Community)	56

Managed Switches

Configure Private-VLAN Association
CLI: Configure Private-VLAN Association
Web Interface: Configure Private-VLAN Association
Configure Private-VLAN Port Mode (Promiscuous, Host)
CLI: Configure Private-VLAN Port Mode (Promiscuous, Host) 59
Web Interface: Configure Private-VLAN Port Mode
(Promiscuous, Host)59
Configure Private-VLAN Host Ports
CLI: Configure Private-VLAN Host Ports
Web Interface: Assign Private-VLAN Port Host Ports
Map Private-VLAN Promiscuous Port
CLI: Map Private-VLAN Promiscuous Port
Web Interface: Map Private-VLAN Promiscuous Port
VLAN Access Ports and Trunk Ports
CLI: Configure a VLAN Trunk64
Web Interface: Configure a VLAN Trunk

Chapter 3 LAGs

Link Aggregation Concepts	70
Add Ports to LAGs	71
CLI: Add Ports to the LAGs	71
Web Interface: Add Ports to LAGs	71

Chapter 4 MLAGs

Multichassis Link Aggregation Concepts
Create an MLAG
CLI: Create an MLAG on LAG2 and LAG377
Web Interface: Create an MLAG on LAG2, LAG3, and LAG4 80
Enable Static Routing on MLAG Interfaces
CLI: Enable Static Routing on MLAG83
Web Interface: Enable Routing on MLAG Interfaces
Enable DCPDP on MLAG Interfaces
CLI: Configure the DCPDP on the MLAG Interfaces
Web Interface: Configure the DCPDP on MLAG Interfaces
Troubleshoot the MLAG Configuration
The Creation of an MLAG Fails
Traffic Through an MLAG Is Not Forwarded Normally
A Ping to a VRRP Virtual IP Address Fails
The VRRP Is Not in the Master State on the Primary or
Secondary Device
DCPDP Does Not Detect the Peer101

Chapter 5 Port Routing

Port Routing Concepts	103
Port Routing Configuration	103
Enable Routing for the Switch	104

CLI: Enable Routing for the Switch	104
Web Interface: Enable Routing for the Switch	105
Enable Routing for Ports on the Switch	105
CLI: Enable Routing for Ports on the Switch	106
Web Interface: Enable Routing for Ports on the Switch	106
Add a Default Route	108
CLI: Add a Default Route	108
Web Interface: Add a Default Route	109
Add a Static Route	109
CLI: Add a Static Route	110
Web Interface: Add a Static Route	110

Chapter 6 VLAN Routing

VLAN Routing Concepts
Create Two VLANs
CLI: Create Two VLANs114
Web Interface: Create Two VLANs115
Set Up VLAN Routing for the VLANs and the Switch118
CLI: Set Up VLAN Routing for the VLANs and the Switch118
Web Interface: Set Up VLAN Routing for the VLANs and the Switch 119

Chapter 7 RIP

Routing Information Protocol Concepts12	21
Enable Routing for the Switch	22
CLI: Enable Routing for the Switch12	22
Web Interface: Enable Routing for the Switch	22
Enable Routing for Ports12	23
CLI: Enable Routing and Assigning IP Addresses for Ports	
1/0/2 and 1/0/3	23
Web Interface: Enable Routing for the Ports	23
Enable RIP on the Switch	25
CLI: Enable RIP on the Switch12	25
Web Interface: Enable RIP on the Switch12	25
Enable RIP for Ports 1/0/2 and 1/0/3 12	26
CLI: Enable RIP for Ports 1/0/2 and 1/0/312	26
Web Interface: Enable RIP for Ports 1/0/2 and 1/0/312	26
Configure VLAN Routing with RIP Support	27
CLI: Configure VLAN Routing with RIP Support	27
Web Interface: Configure VLAN Routing with RIP Support12	29

Chapter 8 OSPF

Open Shortest Path First Concepts	133
Inter-area Router	133
CLI: Configure an Inter-area Router	134
Web Interface: Configure an Inter-area Router	136
OSPF on a Border Router	140

CLI: Configure OSPF on a Border Router	140
Web Interface: Configure OSPF on a Border Router	141
Stub Areas	146
CLI: Configure Area 1 as a Stub Area on A1	146
Web Interface: Configure Area 1 as a Stub Area on A1	148
CLI: Configure Area 1 as a Stub Area on A2	152
Web Interface: Configure Area 1 as a Stub Area on A2	153
NSSA Areas	155
CLI: Configure Area 1 as an NSSA Area	155
Web Interface: Configure Area 1 as an NSSA Area on A1	157
CLI: Configure Area 1 as an NSSA Area on A2	160
Web Interface: Configure Area 1 as an NSSA Area on A2	162
VLAN Routing OSPF	166
CLI: Configure VLAN Routing OSPF	167
Web Interface: Configure VLAN Routing OSPF	169
OSPFv3	171
CLI: Configure OSPFv3	172
Web Interface: Configure OSPFv3	174

Chapter 9 BGP

Border Gateway Protocol Concepts	178
Example1: Configure BGP on Switches A, B, and C in the Same AS .	
Configure BGP on Switch A	180
Configure BGP on Switch B	181
Configure BGP on Switch C	182
Check the BGP Neighbor Status	182
Example 2: Create eBGP on Switches A and D	184
Configure eBGP on Switch A	184
Configure eBGP on Switch D	185
Check the eBGP Neighbor Status	185
Example 3: Create an iBGP Connection with a Loopback Interface	187
Configure iBGP on Switch D	187
Configure eBGP on Switch E	188
Check the iBGP Status	
Example 4: Configure Reflection for iBGP	190
Configure RR on Switch A	191
Configure RR on Switch B and C	191
Example 5: Filter Routes with NLRI	191
Example 6: Filter Routes with AS_PATH	193
Example 7: Filter Routes with Route Maps	194
Example 8: Exchange IPv6 Routes over an IPv4 BGP	196
Configure IPv6 BGP on Switch A	
Configure IPv6 BGP on Switch B	196

Chapter 10 PBR

Policy-Based Routing Concept	. 1	99
Route-Map Statements	. 1	99

PBR Processing Logic	. 200
PBR Configurations	. 201
PBR Example	. 202

Chapter 11 ARP

Proxy ARP Concepts	. 206
Proxy ARP Examples	. 206
CLI: show ip interface	. 206
CLI: ip proxy-arp	. 206
Web Interface: Configure Proxy ARP on a Port	. 207

Chapter 12 VRRP

Virtual Router Redundancy Protocol Concepts	209
VRRP on a Master Router	210
CLI: Configure VRRP on a Master Router	210
Web Interface: Configure VRRP on a Master Router	211
VRRP on a Backup Router	212
CLI: Configure VRRP on a Backup Router	212
Web Interface: Configure VRRP on a Backup Router	213

Chapter 13 ACLs

Access Control List Concepts	6
MAC ACLs	6
IP ACLs	7
ACL Configuration	7
Set Up an IP ACL with Two Rules	7
CLI: Set Up an IP ACL with Two Rules	8
Web Interface: Set Up an IP ACL with Two Rules	9
One-Way Access Using a TCP Flag in an ACL	2
CLI: Configure One-Way Access Using a TCP Flag in an ACL	2
Web Interface: Configure One-Way Access Using a TCP	
Flag in an ACL	6
Use ACLs to Configure Isolated VLANs on a Layer 3 Switch	7
CLI: Configure One-Way Access Using a TCP Flag in ACL	
Commands	8
Web Interface: Configure One-Way Access Using a TCP	
Flag in an ACL	0
Set up a MAC ACL with Two Rules24	8
CLI: Set up a MAC ACL with Two Rules24	8
Web Interface: Set up a MAC ACL with Two Rules	9
ACL Mirroring	1
CLI: Configure ACL Mirroring25	2
Web Interface: Configure ACL Mirroring 25	4
ACL Redirect	7
ACL Redirect	7 8

Configure a Management ACL	262
Example 1: Permit Any Host to Access the Switch Through	
Telnet or HTTP: 2	262
Example 2: Permit a Specific Host to Access the Switch	
Through SSH Only	263
Configure IPv6 ACLs	263
CLI: Configure an IPv6 ACL 2	264
Web Interface: Configure an IPv6 ACL 2	266

Chapter 14 CoS Queuing

CoS Queuing Concepts
CoS Queue Mapping
Trusted Ports
Untrusted Ports
CoS Queue Configuration273
Show classofservice Trust
CLI: Show classofservice Trust274
Web Interface: Show classofservice Trust
Set classofservice Trust Mode274
CLI: Set classofservice Trust Mode274
Web Interface: Set classofservice Trust Mode 275
Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode 275
Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode 275 CLI: Configure Cos-queue Min-bandwidth and Strict Priority
Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode 275 CLI: Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode
Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode 275 CLI: Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode
Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode 275 CLI: Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode
Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode. 275 CLI: Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode
Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode. 275 CLI: Configure Cos-queue Min-bandwidth and Strict Priority 275 Web Interface: Configure CoS-queue Min-bandwidth and 275 Strict Priority Scheduler Mode. 275 Set CoS Trust Mode for an Interface 277 CLI: Set CoS Trust Mode for an Interface 277
Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode. 275 CLI: Configure Cos-queue Min-bandwidth and Strict Priority 275 Web Interface: Configure CoS-queue Min-bandwidth and 275 Strict Priority Scheduler Mode. 275 Set CoS Trust Mode for an Interface 277 CLI: Set CoS Trust Mode for an Interface 277 Web Interface: Set CoS Trust Mode for an Interface. 277
Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode.275CLI: Configure Cos-queue Min-bandwidth and Strict Priority275Web Interface: Configure CoS-queue Min-bandwidth and275Strict Priority Scheduler Mode.275Set CoS Trust Mode for an Interface277CLI: Set CoS Trust Mode for an Interface277Web Interface: Set CoS Trust Mode for an Interface277Configure Traffic Shaping.278
Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode.275CLI: Configure Cos-queue Min-bandwidth and Strict Priority275Web Interface: Configure CoS-queue Min-bandwidth and275Strict Priority Scheduler Mode.275Set CoS Trust Mode for an Interface277CLI: Set CoS Trust Mode for an Interface277Web Interface: Set CoS Trust Mode for an Interface277Configure Traffic Shaping.278CLI: Configure traffic-shape278

Chapter 15 DiffServ

Differentiated Services Concepts DiffServ	281 282
CLI: Configure DiffServ	282
Web Interface: Configure DiffServ	285
DiffServ for VoIP	298
CLI: Configure DiffServ for VoIP	298
Web Interface: Diffserv for VoIP	300
Auto VoIP	305
Protocol-Based Auto VoIP	305
OUI-Based Auto VoIP	306
Example 1: Enable Protocol-Based Auto VoIP	307
Example 2: Change the Queue of Protocol-Based Auto VoIP	308
Example 3: Create an Auto VoIP VLAN	310

DiffServ for IPv6	312
CLI: Configure DiffServ for IPv6	312
Web Interface: Configure DiffServ for IPv6	313
Color Conform Policy	319
CLI: Configure a Color Conform Policy	320
Web Interface: Configure a Color Conform Policy	321

Chapter 16 IGMP Snooping and Querier

Internet Group Management Protocol Concepts	28
IGMP Snooping	28
CLI: Enable IGMP Snooping	28
Web Interface: Enable IGMP Snooping	28
Show igmpsnooping	29
CLI: Show igmpsnooping	29
Web Interface: Show igmpsnooping	29
Show mac-address-table igmpsnooping	30
CLI for IGMPv1 and IGMPv2: Show mac-address-table igmpsnooping 33	30
CLI for IGMPv3: show igmpsnooping ssm entries	30
Web Interface: Show mac-address-table igmpsnooping	31
External Multicast Router	31
CLI: Configure the Switch with an External Multicast Router	31
Web Interface: Configure the Switch with an External Multicast Router 33	31
Multicast Router Using VLAN	32
CLI: Configure the Switch with a Multicast Router Using VLAN	32
Web Interface: Configure the Switch with a Multicast Router	
Using VLAN	32
IGMP Querier Concepts	33
Enable IGMP Querier	34
CLI: Enable IGMP Querier	34
Web Interface: Enable IGMP Querier	34
Show IGMP Querier Status	36
CLI: Show IGMP Querier Status	36
Web Interface: Show IGMP Querier Status	37

Chapter 17 MVR

Multicast VLAN Registration	9
Configure MVR in Compatible Mode	0
CLI: Configure MVR in Compatible Mode	1
Web Interface: Configure MVR in Compatible Mode	3
Configure MVR in Dynamic Mode	6
CLI: Configure MVR in Dynamic Mode	6
Web Interface: Configure MVR in Dynamic Mode	.9

Chapter 18 Security Management

Port Security Concepts	354
Set the Dynamic and Static Limit on Port 1/0/1	355

Managed Switches

CLI: Set the Dynamic and Static Limit on Port 1/0/1	355
Web Interface: Set the Dynamic and Static Limit on Port 1/0/1	355
Convert the Dynamic Address Learned from 1/0/1 to a Static Address	356
CLI: Convert the Dynamic Address Learned from 1/0/1 to the	
Static Address	356
Web Interface: Convert the Dynamic Address Learned from	
1/0/1 to the Static Address	357
Create a Static Address.	357
CLI: Create a Static Address	357
Web Interface: Create a Static Address	358
Protected Ports	358
CLI: Configure a Protected Port to Isolate Ports on the Switch	359
Web Interface: Configure a Protected Port to Isolate Ports	
on the Switch	
802.1x Port Security	364
CLI: Authenticating dot1x Users by a RADIUS Server	365
Web Interface: Authenticating dot1x Users by a RADIUS Server	366
	370
CLI: Create a Guest VLAN	3/1
Web Interface: Create a Guest VLAN	3/2
	3/5
	376
Web Interface: Assign VLANS Using RADIUS	3/8
	381
CLI: Configure Dynamic ARP Inspection	382
Web Interface: Configure Dynamic ARP Inspection.	383
Static Mapping	386
CLI: Configure Static Mapping	386
	387
	388
	389
Web Interface: Configure DHCP Snooping Find a Dargue DHCD Service	389
	392
CLI: FIND & ROGUE DHCP Server	392
Web Interface: Find a Rogue DHCP server	
Chile Fater Static Diadian into the Binding Database	
CLI: Enter Static Binding Into the Binding Database	395
Meximum Pate of DUCD Messages	
CLI Configure the Maximum Date of DUCP Messages	
Web Interface: Configure the Maximum Pate of DHCP Messages	206
Web Interface. Comingule the Maximum Rate of DHCP Messages	
CLI Configure Dynamic ADD Inspection	
CLI: Configure Dynamic ARP Inspection	200
	402
	402
CUITINIANU AUDIOLIZATION Authorization by a TACACS - Server	4UZ
	403
	403

)4
)4
)5
)6
)7
)8
)9
)9

Chapter 19 MAB

Chapter 20 SNTP

Simple Network Time Protocol Concepts
Show SNTP (CLI Only)
show sntp
show sntp client
show sntp server
Configure SNTP
CLI: Configure SNTP
Web Interface: Configure SNTP433
Set the Time Zone (CLI Only)434
Set the Named SNTP Server
CLI: Set the Named SNTP Server434
Web Interface: Set the Named SNTP Server

Chapter 21 Tools

138
139
140
140
441
441
142

Managed Switches

Create a Configuration Script	
Upload a Configuration Script	
Pre-Login Banner.	
Create a Pre-Login Banner	
Port Mirroring	
CLI: Specify the Source (Mirrored) Ports and Destination (Probe)	
Web Interface: Specify the Source (Mirrored) Ports and	
Destination (Probe)	
Remote SPAN	
CLI: Enable RSPAN on a Switch	
Dual Image	
CLI: Download a Backup Image and Make It Active	
Web Interface: Download a Backup Image and Make It Active	450
Outbound Telnet	451
CLI: show network	452
CLI: show telnet	452
CLI: transport output telnet	453
Web Interface: Configure Telnet	453
CLI: Configure the Session Limit and Session Time-out	454
Web Interface: Configure the Session Time-out	454
Full Memory Dump	

Chapter 22 Syslog

Syslog Concepts
Show Logging
CLI: Show Logging457
Web Interface: Show Logging458
Show Logging Buffered
CLI: Show Logging Buffered460
Web Interface: Show Logging Buffered461
Show Logging Traplogs
CLI: Show Logging Traplogs461
Web Interface: Show Logging Trap Logs
Show Logging Hosts
CLI: Show Logging Hosts
Web Interface: Show Logging Hosts463
Configure Logging for a Port463
CLI: Configure Logging for the Port463
Web Interface: Configure Logging for the Port
Email Alerting
CLI: Send Log Messages to admin@switch.com Using
Account aaaa@netgear.com466

Chapter 23 Chassis Switch Management

Chassis Switch Management and Connectivity	468
Supervisor and Chassis Members	468
Supervisor	468

Chassis Members
Chassis Firmware
Code Mismatch
Configuration Mismatch
Upgrade the Firmware
Migrate Configuration with a Firmware Upgrade
Add, Remove, or Replace a Chassis Member
Add a Blade to an Operating Chassis471
Remove a Blade from the Chassis
Replace a Chassis Member471
Chassis Switch Configuration Files
Preconfigure a Switch
Move the Supervisor to a Different Blade
CLI: Move the Supervisor to a Different Blade
Web Interface: Move the Supervisor to a Different Blade

Chapter 24 Switch Stacks

	. – .
Switch Stack Management and Connectivity	. 476
Stack Master and Stack Members	. 476
Stack Master	. 477
Stack Members	. 478
Stack Member Numbers	. 478
Stack Member Priority Values	. 478
Install and Power-up a Stack	. 478
Compatible Switch Models	. 478
Install a Switch Stack	. 479
Switch Firmware and Firmware Mismatch.	. 480
Upgrade the Firmware	. 480
Migrate Configuration with a Firmware Upgrade	. 481
Web Interface: Copy Master Firmware to a Stack Member	. 481
Stack Switches Using Ethernet Ports and a Stack Cable	. 482
CLI: Configure the Stack Ports as Ethernet Ports	. 482
Web Interface: Configure the Stack Ports as Ethernet Ports	. 484
Stack Switches Using 10G Fiber	. 486
CLI: Stack Switches Using 10G Fiber	. 486
Web Interface: Stack Switches Using 10G Fiber	. 488
Add, Remove, or Replace a Stack Member	. 489
Add Switches to an Operating Stack	. 489
Remove a Switch from a Stack	. 490
Replace a Stack Member	. 491
Switch Stack Configuration Files	. 491
Preconfigure a Switch	. 492
Renumber Stack Members	. 494
CLI: Renumber Stack Members.	. 494
Web Interface: Renumber Stack Members	. 495
Move the Stack Master to a Different Unit	. 496
CLI: Move the Stack Master to a Different Unit	. 496

Web Interface: Move the Stack Mast	er to a Different Unit
------------------------------------	------------------------

Chapter 25 SNMP

Add a New Community
CLI: Add a New Community498
Web Interface: Add a New Community
Enable SNMP Trap
CLI: Enable SNMP Trap
Web Interface: Enable SNMP Trap499
SNMP Version 3
CLI: Configure SNMPv3500
Web Interface: Configure SNMPv3501
sFlow
CLI: Configure Statistical Packet-Based Sampling of Packet
Flows with sFlow
Web Interface: Configure Statistical Packet-based Sampling
with sFlow
Time-Based Sampling of Counters with sFlow
CLI: Configure Time-Based Sampling of Counters with sFlow505 Web Interface: Configure Time-Based Sampling of Counters
with sFlow

Chapter 26 DNS

508

Chapter 27 DHCP Server

511
511
511
512
514
514
515

Chapter 28 DHCPv6 Server

Dynamic Host Configuration Protocol Version 6 Concepts	. 518
CLI: Configure DHCPv6 Prefix Delegation	. 519
Web Interface: Configure DHCPv6 Prefix Delegation	. 520
Configure a Stateless DHCPv6 Server	. 524
CLI: Configure a Stateless DHCPv6 Server	. 524

Web Interface: Configure a Stateless DHCPv6 Server	525
Configure a Stateful DHCPv6 Server	528
CLI: Configure a Stateful DHCPv6 Server	528
Web Interface: Configure a Stateful DHCPv6 Server	529

Chapter 29 DVLANs and Private VLANs

Double VLANs
CLI: Enable a Double VLAN535
Web Interface: Enable a Double VLAN535
Private VLAN Groups
CLI: Create a Private VLAN Group539
Web Interface: Create a Private VLAN Group540

Chapter 30 STP

Spanning Tree Protocol Concepts	545
Configure Classic STP (802.1d)	545
CLI: Configure Classic STP (802.1d)	545
Web Interface: Configure Classic STP (802.1d)	545
Configure Rapid STP (802.1w)	546
CLI: Configure Rapid STP (802.1w).	546
Web Interface: Configure Rapid STP (802.1w)	547
Configure Multiple STP (802.1s)	548
CLI: Configure Multiple STP (802.1s)	548
Web Interface: Configure Multiple STP (802.1s)	549
Configure PVSTP and PVRSTP	550
CLI: Configure PVSTP	552
Web Interface: Configure PVSTP	555

Chapter 31 Tunnels for IPv6

Tunnel Concepts	560
Create a 6in4 Tunnel	560
CLI: Create a 6in4 Tunnel	561
Web Interface: Create a 6in4 Tunnel	562
Create a 6to4 Tunnel	566
CLI: Create a 6to4 Tunnel	567
Web Interface: Create a 6to4 Tunnel	572

Chapter 32 IPv6 Interface Configuration

Create an IPv6 Routing Interface	
CLI: Create an IPv6 Routing Interface	
Web Interface: Create an IPv6 Routing Interface	587
Create an IPv6 Routing VLAN	
CLI: Create an IPv6 Routing VLAN	
Web Interface: Create an IPv6 VLAN Routing Interface	591
Configure DHCPv6 Mode on the Routing Interface	593

CLI: Configure DHCPv6 mode on routing interface	594
Web Interface: Configure DHCPv6 mode on routing interface	595

Chapter 33 PIM

Protocol Independent Multicast Concepts5	598
PIM-DM	598
CLI: Configure PIM-DM	500
Web Interface: Configure PIM-DM6	504
PIM-SM	521
CLI: Configure PIM-SM6	522
Web Interface: Configure PIM-SM6	526

Chapter 34 DHCP L2 Relay and L3 Relay

DHCP L2 Relay	17
CLI: Enable DHCP L2 Relay64	17
Web Interface: Enable DHCP L2 Relay64	19
DHCP L3 Relay	52
Configure the DHCP Server Switch65	52
Configure a DHCP L3 Switch65	57

Chapter 35 MLD

Multicast Listener Discovery Concepts	53
Configure MLD	53
CLI: Configure MLD66	54
Web Interface: Configure MLD66	56
MLD Snooping	75
CLI: Configure MLD Snooping67	76
Web Interface: Configure MLD Snooping	77

Chapter 36 DVMRP

Distance Vector Multicast Routing Protocol Concepts	. 680
CLI: Configure DVMRP	. 681
Web Interface: Configure DVMRP	. 687

Chapter 37 Captive Portal

Captive Portal Concepts	698
Captive Portal Configuration Concepts	699
Enable a Captive Portal	
CLI: Enable a Captive Portal	
Web Interface: Enable a Captive Portal	700
Client Access, Authentication, and Control	701
Block a Captive Portal Instance	701
CLI: Block a Captive Portal Instance	701
Web Interface: Block a Captive Portal Instance	702
Local Authorization, Create Users and Groups	702

CLI: Create Users and Groups	702
Web Interface: Create Users and Groups	703
Remote Authorization (RADIUS) User Configuration	704
CLI: Configure RADIUS as the Verification Mode	705
Web Interface: Configure RADIUS as the Verification Mode	706
SSL Certificates	706

Chapter 38 iSCSI

708
709
710
710
710
711
711
711
712
712
713

Chapter 39 Override Factory Defaults

Override the Factory Default Configuration File	.715
CLI: Install Another Factory Defaults Configuration File	.715
CLI: Erase the Old Factory Default Configuration File	.716

Chapter 40 NETGEAR SFP

Index

Documentation Resources

1

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

- The NETGEAR installation guide for your switch
- Managed Switch Hardware Installation Guide
- Managed Switch Software Setup Manual
- ProSAFE Managed Switch Command Line Interface (CLI) User Manual
- ProSAFE Managed Switch Web Management User Manual

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

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

VLANs

Virtual LANs

This chapter includes the following sections:

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

2

VLAN Concepts

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

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

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

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

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



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

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

Create Two VLANs

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

CLI: Create Two VLANs

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

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

Web Interface: Create Two VLANs

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

Syste	em	Sv	vitching		Routing	QoS	Security	Monitori	ng	Maintenance	Help	Index	
VLAN	Auto-V	/olP	iSCSI	STP	Multicast	MVR	Address Table	Ports LAG	MLAC	3			
	VLA	N		Reset									
•Basic			~	Res	et Configurat	ion							
• VLAN	l Config	uration	R										
• Advance	ed		~										
		Internal VLAN Configuration											
				Inter	mal VLAN A	location Ba	se 4)93	1				
				Inter	mal VLAN A	location Po	licy 🔘	Ascending	Descendi	ng			
				VLAN	Configuratio	1							
					VLANID	/I AN Name	VI AN Type	Make Static					
				-	2	VI AN2		Dicable x					
					1	lefault	Default	Disable					

- **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.

Syste	em	Switching		Routing	QoS	Security	Monitorir	ıg	Maintenance	Help	Index		
	Auto-VolF	o iscsi	STP	Multicast	MVR	Address Table	Ports LAG	MLAG					
	VLAN		Reset										
• Basic		^	Res	et Configurat	tion								
• VLAN	I Configurat	ion											
• Advanc	ed	~											
	Internal VLAN Configuration												
			Inte	rnal VLAN AI	llocation Ba	ase 40	93						
			Inte	rnal VLAN AI	llocation Po	olicy 🔘	Ascending	escending					
			VLAN	Configuration	n								
				VLAN ID	VLAN Nam	e VLAN Type	Make Static						
				3	VLAN3		Disable 🛩						
				1 0	default	Default	Disable						
				2	VLAN2	Static	Disable						

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

Assign Ports to VLAN 2

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

CLI: Assign Ports to VLAN 2

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

Web Interface: Assign Ports to VLAN 2

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

A screen similar to the following displays.

Basic	-	12	3 LAGS A	1					Go To Interface	Go
Advanced VLAN Configuration	^	•	Interface	PVID	VLAN Member	VLAN Tag	Acceptable Frame Types	Configured Ingress Filtering	Gurrent Ingress Filtering	Port Priority (0 to 7)
• VLAN Membership				2			÷	14		
VLAN Status		ø	1/0/1	ð.,	1,2	2	Admit All	Disable	Disable	0
Port PVID Configuration			1/0/2 1/0/3	1	1,2	2 None	Admit All Admit All	Disable Disable	Disable Disable	0
		10	000			Hone	Palitic Pa	Disable	Disable	0

- 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.

Syste	em	Sv	vitching		Routing	QoS		Security		Monitorin	g	Maintenance	Help	Index
VLAN	Auto-	VolP	iSCSI	STP	Multicas	t MVR	Addr	ess Table	Ports	LAG	MLAG			· · · · · · · · · · · · · · · · · · ·
	VLAM	N		VLAN M	Vembershi	р								
• Basic			~	VLAN	ID							2		
• Advanc	ed		^	Group	Operation							Unta	ag All 🗸	
• VLAN	I Config	uration	1	VLAN	Name							VLAN	12	
• VLAN	I Memb	ership		VLAN	Туре							Statio	c	
• VLAN	I Status	5		U	nit 1									
Port I Confi	PVID guration	1		Ports	1 3	5 7	9 11	13 15	17 1	9 21 2	23			
• MAC	Based	VLAN			T									
• Proto	col Bas	ed VL	AN				10 12		18 2					
Citta	p ooning	Juration			2 7	0 0	10 12	14 10	10 2	0 22 2				

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.

Syst	em 🚺	Swi	tching		Routing	QoS	Security	Monitorin	g Maintena	nce Help	Index
	Auto-V	olP	iscsi	STP	Multicast	MVR	Address Table	Ports LAG	MLAG		
	VLAN			Reset							
• Basic			~	Res	et Configurati	ion					
• Advanc	ed:		^								
• VLAN	N Configu	ration									
• VLAN	√ Membe	ership		Interna	I VLAN Conf	iguration					
- VLAN	√ Status			Inter	mal VLAN All	location Ba	se 40	193			
• Port F Confi	PVID guration			Inter	mal VLAN All	location Pol	licy O	Ascending	escending		
• MAC	Based V	/LAN									
• Proto Grou	icol Base p Configu	ed VLA	N	VLAN	Configuration	i					
• Proto Grou	icol Base p Membe	ed VLA	Ň		VLAN ID V	/LAN Name	VLAN Type	Make Static			
• IP Su	ubnet Bas	sed			100	√LAN100		Disable 🛩			
• Port	DVLAN				1 d	lefault	Default	Disable			

- **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.

System	n	Switching	li.	Routing	QoS	Security	Monitorin	g Maintenance	Help	Index
VLAN A	Auto-VolF	iscs	STP	Multicast	MVR /	Address Table	Ports LAG	MLAG		16
1	VLAN		Reset							
•Basic		~	Res	et Configurat	tion					
• Advanced	ł	^								
• VLAN C	Configural	tion								
VLAN N	Vembers	nip	Interna	al VLAN Con	figuration					
- VLAN S	Status		Inte	mal VLAN A	llocation Bas	e 40	03			
Port PV Configu	/ID iration		Inte	mal VLAN A	llocation Poli	icy O	Ascending 💿 De	escending		
• MAC B	ased VLA	AN								
Protoco Group (ol Based ' Configurat	VLAN tion	VLAN	Configuratio	n					
 Protoco Group N 	ol Based Members	VLAN hip		VLAN ID	VLAN Name	VLAN Type	Make Static			
• IP Subr VLAN	net Based	ł		101	VLAN101		Disable 👻			
Port DV Configu	/LAN iration			1 100	default VLAN100	Default Static	Disable Disable			

- **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.

Syste	m	Switching		Routing	QoS	Security	Monitorin	ng Maintenance	Help	Index
	Auto-VolF	iscsi	STP	Multicas	t MVR A	Address Table	Ports LAG	MLAG		
	VLAN									
• Basic		*	Interna	al VLAN Cor	nfiguration					
• Advance	d	~	Inter	mal VLAN A	Allocation Bas	e 40	93			
- VLAN	Configurat	ion	Inter	mal VLAN A	Allocation Poli	су	Ascending Description	escending		
• VLAN	Membersh	nip								
• VLAN	Status									
• Port P Config	VID uration		VLAN	Configuratio	on					
• MAC E	Based VLA	N		VLAN ID	VLAN Name	VLAN Type	Make Static			
• Protoc	ol Based V	VIAN		102	VLAN102		Disable 🗸			
Group	Configurat	ion		1	default	Default	Disable			
• Protoc	ol Based \	VLAN		100	VLAN100	Static	Disable			
Group	Membersh	nip		101	VLAN101	Static	Disable			
• IP Sub VLAN	onet Based	ł								

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

Assign Ports to VLAN 3

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

CLI: Assign Ports to VLAN 3

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

Web Interface: Assign Ports to VLAN 3

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

A screen similar to the following displays.

Syst	em	Sw	ritching		Routing	QoS	Securi	у	Monitorir	ig 📗	Maintenance	Help	Index
	Auto-V	/olP	iSCSI	STP	Multicast	MVR	Address Tab	e Ports	LAG	MLAC	3		
	VLAN			VLAN I	Vembership								
• Basic			~	VLAN	ID						2.	í.	
• Advanc	ed		^	Group	Operation						Unta	ag All 🗸 🗸	
• VLAI	v Contigu	Iration		VLAN	Name						VLAN	13	
- 1/1 /1	V Wembe	asnip		VLAN	Type						Static	2	
Port Confi	PVID guration Based \	/LAN		Ports	nit 1	5 7 9		5 17 1	9 <u>21</u> 2	23			
• Proto Grou	ocol Base p Configu	ed VLA	AN		T T 2 4	3 8 10	0 12 14	6 18 2	0 22 2	24			

- 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.

System Switching		Routing	9	Security	Monitoring	Maintenance Help	Index		
VIEAL Auto-VolP ISCSI	STP	Multica	at MV	R Address Table	Ports LAG MLA	G			
VLAN	PVID	Configuratio	on						
Basic -	12	3 LAGS A	JI					Go To Interface	Go
Advanced A		-	-						0.00
VLAN Configuration		Interface.	FVID	VLAN Member	VLAN Tag	Acceptable Frame Types	Configured Ingress Filtering	Current Ingress Filtering	(0 to 7)
VLAN Membership		1/0/4	1	1	None	Admit All 👻	Disable +	Disable	0
VLAN Status		1/0/1	1	1	None	Admit All	Disable	Disable	0
Port PVID	1	1/0/2	1	1	None	Admit All	Disable	Disable	0
Configuration		1/0/3	1	1	None	Admit All	Disable	Disable	0
MAC Based VLAN	2	1/0/4	1	1	None	Admit All	Disable	Disable	0
Protocol Based VI AN	0	1/0/5	1	1	None	Admit All	Disable.	Disable	0
Group Configuration		1/0/6	1	1	None	Admit All	Disable	Disable	0
Protocol Resear VI AN	8	1/0/7	1	1	None	Admit All	Disable	Disable	0
Group Membership	8	1/0/8	1	1	None	Admit All	Disable	Disable	0
- IP Subnet Based	- 10	1/0/9	1	1	None	Admit All	Disable	Disable	0
VLAN	8	1/0/10	1	1	None	Admit All	Disable	Disable	0

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

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

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

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

(Netgear	Switch)	#config	
(Netgear	Switch)	(Config)#ir	nterface 1/0/2
(Netgear	Switch)	(Interface	1/0/2)#vlan pvid 3
(Netgear	Switch)	(Interface	1/0/2)#exit
(Netgear	Switch)	(Config)#e>	xit

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

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

A screen similar to the following displays.

System	Switching		Routing	Qo	S Security	Monitoring	Maintenance Help	Index		
IoV-otuA Really	P ISCSI	STP	Multicas	it MVR	Address Table	Ports LAG MLA	G			
VLAN		PVID	Configuratio	20						
Basic		12	I LAGS A	ñ.					Go To Interface	Go
Advanced				-						Dec 2010
• VLAN Configura	tion		Interface	PVID	VLAN Member	VLAN Tag	Acceptable Frame Types	Configured Ingress Filtering	Current Ingress Filtering	(0 to 7)
• VLAN Members	hip		1/0/2	3	3	None	Admit All 👻	Disable +	Disable	0
VLAN Status			1/0/1	1	1	None	Admit All	Disable	Disable	0
+Port PVID			1/0/2	1	1	None	Admit All	Disable	Disable	0
Configuration		0	1/0/3	1	1	None	Admit All	Disable	Disable	0
·MAC Based VL	AN		1/0/4	1	1	None	Admit All	Disable	Disable	0
+ Distocal Based	VCAN.	- 83	1/0/5	1	1	None	Admit All	Disable	Disable	0
Group Configura	ation	8	1/0/6	1	1	None	Admit All	Disable	Disable	0
*Protocol Flagad	W.AN	8	1/0/7	1	4	None	Admit All	Disable	Disable	0
Group Members	ship	13	1/0/8	1	1	None	Admit All	Disable	Disable	0
• IP Subnet Base	d	8	1/0/9	1	1	None	Admit All	Disable	Disable	0
VLAN	×	B	1/0/10	1	1	None	Admit All	Disable	Disable	0

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

Create a MAC-Based VLAN

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

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

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

CLI: Create a MAC-Based VLAN

1. Create VLAN3.

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

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

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

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

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

4. Add all the ports to VLAN3.

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

Web Interface: Assign a MAC-Based VLAN

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

A screen similar to the following displays.

Syste		Sw	itching		Routing	QoS	Security	Monitori	ng	Maintenance	Help	Index
	Auto-V	/olP	iSCSI	STP	Multicast	MVR	Address Table	Ports LAG	MLAG			
	VLAN			Reset								
Basic			~	Res	et Configurati	on						
Advance	ed		^									
• VLAN	Configu	iration										
• VLAN	Membe	ership		Interna	I VLAN Conf	guration						
- VLAN	Status			Inter	nal VLAN All	ocation Ba	se 40	13				
Port F Config	VID Juration			Inter	nal VLAN All	ocation Pol	icy 🔘	Ascending 🖲 🛙)escendir	ıg		
• MAC	Based \	/L AN										
Protoc Group	col Base Configu	ed VLA uration	N	VLAN	Configuration							
• Protoc Group	col Base Membe	ed VLA ership	N		VLAN ID V	LAN Name	VLAN Type	Make Static				
• IP Sul VLAN	bnet Ba	sed			3	/LAN3		Disable 👻				
Port D Config	VLAN Juration				1 d	efault	Default	Disable				

- **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.

System	Sv	vitching		Routing	QoS	Security		/lonitoring	g	Maintenance	Help	Index
VLAN Auto	-VoIP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAG			a
VL	AN		VLAN I	Vembership								
 Basic 		~	VLAN	ID						3 ~		
Advanced		^	Group	Operation						Unta	ia All 🗸	
VLAN Cont	iguration	0	VLAN	Name						VLAN	3	
VLAN Men	nbership		VLAN	Туре						Static		
• VLAN Stat	JS			nit 1								1
 Port PVID Configuration 	on		Ports	1 3 5	79) 11 13 15	17 19	21 2	3			
• MAC Base	d VLAN			υυι	ี่ [บ] [เ	U U U U	UU	UUU	J			
 Protocol B: Group Con 	ased VL iguratior	AN 1		UUU 246	1 U L	JUUUU 0 12 14 16	U U 18 20	U U 22 2	J 4			

- 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.

System Swi	tching		Routing	Qo	S Security	Monitoring	Maintenance Help	Index		
VILMI Auto-VolP	SCSI	STP	Multica	at MVR	Address Table	Ports LAG MLA	G			
VLAN		PVID	Configurati	on						
*Basic	*	12	J LAGS A	UI I					Go To Interface	Go
Advanced VLAN Configuration	^		Interface	PVID	VLAN Member	VLAN Tag	Acceptable Frame Types	Configured Ingress Filtering	Current Ingress Filtering	Port Priority (0 to 7)
*VLAN Membership			1/0/23	1.	1,3	None	Admit All 👻	Disable 👻	Disable	0
*VLAN Status		1	1/0/1	1	1.3	None	Admit All	Disable	Disable	0
+Port PVID		13	1/0/2	1	1,3	None	Admit All	Disable	Disable	0
Configuration		8	1/0/3	1	1,3	None	Admit All	Disable	Disable	0
MAC Based VLAN			1/0/4	1	1,3	None	Admit All	Disable	Disable	0
Protocol Based VI A	n	- 83	1/0/5	1	1,3	None	Admit All	Disable	Disable	0
Group Configuration		8	1/0/6	1	1,3	None	Admit All	Disable	Disable	0
Protocol Flased VLA	N I	8	1/0/7	1	1,3	None	Admit All	Disable	Disable	0
Group Membership	2	0	1/0/8	1	1,3	None	Admit All	Disable	Disable	0

- **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.

System	S	witching		Routing	QoS	Security	×	Monitorin	Ig	Maintenance	Help	Index
VLAN Aut	o-VolP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLA	G		· · · · · · · · · · · · · · · · · · ·
VL	AN		MAC B	ased VLAN (Configurat	ion						
• Basic		~		MAC Addres	is	VLAN ID		- 27				
 Advanced 		^		00:00:0A:00:	00:02	3						
• VLAN Con	figuratio	n										
• VLAN Mer	nbership											
• VLAN Stat	us											
 Port PVID Configurati 	on											
• MAC Base	d VLAN											
 Protocol B Group Con 	ased VL figuratio	AN n										
 Protocol B Group Mer 	ased VL nbership	AN										

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

Create a Protocol-Based VLAN

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

CLI: Create a Protocol-Based VLAN

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

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

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

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

3. Assign VLAN protocol group 1 to VLAN 4.

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

4. Assign VLAN protocol group 2 to VLAN 5.

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

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

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

Web Interface: Create a Protocol-Based VLAN

1. Create VLAN4 and VLAN5.

Create VLAN4.

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

A screen similar to the following displays.

Syste	em	Sw	vitching		Routing	QoS	Security	Monitorin	ig Mainte	enance	Help	Index
VLAN	Auto-V	olP	iSCSI	STP	Multicast	MVR	Address Table	Ports LAG	MLAG			
	VLAN	1		Reset								
• Basic			^	Res	et Configurat	ion						
• VLAN	I Configu	iration	ř.									
• Advance	ed		~									
				Interna	I VLAN Con	iguration						
				Inter	nal VLAN A	location Ba	ase 40	93				
				Inter	mal VLAN AI	location Po	olicy 🔘	Ascending 💿 D	escending			
				VLAN	Configuratio	1						
					VLAN ID	/LAN Nam	e VLAN Type	Make Static				
					4	/LAN4		Disable 🛩				
					1 0	lefault	Default	Disable				

b. Enter the following information:

In the VLAN ID field, enter 4.

In the VLAN Name field, enter VLAN4.

In the VLAN Type list, select Static.

c. Click Add.

Create VLAN5.

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

Syste	m 🥵	Switching		Routing	QoS	Security	Monitorin	ng Maintenance	Help	Index			
VLAN	Auto-VolP	iSCSI	STP	Multicast	MVR	Address Table	Ports LAG	MLAG					
	VLAN		Reset										
• Basic		^	Res	et Configurat	tion								
• VLAN	Configurati	on											
• Advance	d	~											
			Interna	al VLAN Con	figuration								
	Internal VLAN Allocation Base 4093												
			Inte	mal VLAN A	llocation Po	licy 💿	Ascending D	escending					
			VLAN	Configuratio	n								
				VLAN ID	VLAN Name	VLAN Type	Make Static						
				5	VLAN5		Disable 🛩						
				1	default	Default	Disable						
				4	VLAN4	Static	Disable						

b. Enter the following information:

In the VLAN ID field, enter 5.

In the VLAN Name field, enter VLAN5.

In the VLAN Type list, select Static.

- c. Click Add.
- 2. Create the protocol-based VLAN group vlan_ipx.
 - a. Select Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration.

A screen similar to the following displays.

Syst	em	Sw	itching		Routing	QoS	Security	N	Nonitoring	Maintenance	Help	Index
VLAN	Auto-V	/olP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG MI	LAG		
	VLAN	1		Protoc	ol Based VL	AN Group	Configuration					
• Basic			~		Group ID	Group Nan	ne Protocol		VLAN I) Ports		
• Advanc	ed		^		1	vlan_ipx	ipx		4			
• VLAN	Config	uration										
. VLAN	Memb	ership										
• VLAN	V Status											
• Port I Confi	PVID guration											
- MAC	Based '	VLAN										
• Proto Grou	col Bas p Config	ed VLA uration	٨N									
• Proto Grou	col Bas p Memb	ed VLA ership	NN .									

Enter the following information:

- In the Group ID field, enter 1.
- In the Group Name field, enter vlan_ipx.
- In the **Protocol** list, enter **ipx**.
- In the VLAN ID field, enter 4.
- b. Click Add.
- 3. Create the protocol-based VLAN group vlan_ip.
 - a. Select Switching > VLAN >Advanced > Protocol Based VLAN Group Configuration.

A screen similar to the following displays.

System	Swit	ching		Routing	QoS	Security	ľ	Monitorin	ig	Maintenance	Help	Ind
VLAN Auto-Vo	olP i	SCSI	STP	Multicas	t MVR	Address Table	Ports	LAG	MLA	κG		
VLAN			Protoc	ol Based V	LAN Group (Configuration						
Basic		~		Group ID	Group Name	e Protocol		VL/	AN ID	Ports		
Advanced		^		2	vlan ip	ip.arp		5				
VLAN Configur	ration			1	vlan_ipx	IPX		4				
• VLAN Member	rship											
 VLAN Status 												
Port PVID Configuration												
• MAC Based V	LAN											
Protocol Base Group Configure	d VLAN ration	Ň										
Protocol Base Group Mombo	d VLAN rship	J.										

- **b.** Enter the following information:
 - In the Group ID field, enter 2.
 - In the Group Name field, enter vlan_ip.
 - In the **Protocol** list, select **IP** and **ARP** while holding down the **Ctrl** key.
 - In the VLAN field, enter 5.
- c. Click Add.
- 4. Add port 11 to the group vlan_ipx.
 - a. Select Switching > VLAN > Advanced > Protocol Based VLAN Group Membership.

System Swi	tching		Routing	1	QoS		Secu	rity	6	Mc	nitorir	ig	N	lainter	nance		ł	lelp		li	ıdex		
VLAN Auto-VolP	iscsi	STP	Multica	ast	MVR	Addre	ess Tal	ole	Port	S	LAG	ML	AG										
VLAN		Protoco	Based	VLA	V Group	Memb	ership																
•Basic	~	Group	ID												4	~							
 Advanced 	^	Group	Name												vlan	ipx							
 VLAN Configuration 															Cu	irrent	mer	nber	5				
 VLAN Membership 		U 💼	nit 1												10								
 VLAN Status 		Ports	1 3	5	7	9 11	13	15	17	19	21 :	23											
 Port PVID Configuration 				1							1												
MAC Based VLAN			2 4	6	8	10 12	14	16	18	20	22	24											
 Protocol Based VLA Group Configuration 	N	U 📕	nit 2																				
Protocol Based VLA Group Membership	N	Ports	1 3	5	7	9 11	13	15	17	19	21	23 2	5 27	29	31	33	35	37	39	41	43	45	47
 IP Subnet Based VLAN 																					22 A		
			2 4	6	8	10 12	14	16	18	20	22 3	24 2	6 28	30	32	34	36	38	40	42	44	46	48

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

System	Sw	itching	ļ	Routing]	QoS	1	Se	curity		M	onitor	ing		Ma	ainten	ance	4		Help		lr	ıdex	32	
VLAN Auto-	VolP	iSCSI	STP	Multi	cast	MVR	Add	iress 1	Table	Po	rts	LAG	i N	ILAG	5										
VLAI	N		Protoco	l Base	d VLA	N Grou	p Merr	bersh	ip																
• Basic		~	Group	ID													2 .								
 Advanced 		^	Group	Name													vlan	ip							
 VLAN Config 	guration																Cu	rren	t me	mber	IS				
• VLAN Memb	bership		Πu	nit 1												3	-								
VLAN Status	s		Ports	1	3 5	7	9 1	1 13	15	17	19	21	23												
 Port PVID Configuration 	n							1																	
• MAC Based	VLAN			2	4 6		10 1	2 14	16	18	20	22	24												
 Protocol Bas Group Config 	sed VLA guration	N.	U	nit 2																					
Protocol Bas Group Memb	sed VLA bership	JN .	Ports		35	7	9 1	1 13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
 IP Subnet B: VLAN 	ased					j, j														a (12				6 (j)	
				2	4 6	8	10 1	2 14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48

- 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 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.

Managed Switches



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-ad	dr-table vlan 2000
MAC Address In	nterface	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.

Syster	m 😵	Switching		Routing	QoS	Security	Monitorin	g Maintenance	Help	Index
VLAN	Auto-VolP	iSCSI	STP	Multicast	MVR	Address Table	Ports LAG	MLAG		
	VLAN		Reset							
• Basic		^	Res	et Configurat	tion					
• VLAN	Configuration	on								
Advance	d	~								
			Interna	I VLAN Con	figuration					
			Inter	mal VLAN A	llocation Bas	se 40	93			
			Inter	mal VLAN A	llocation Pol	icy 🔘	Ascending 💿 D	escending		
			VLAN	Configuration	n					
				VLAN ID	VLAN Name	VLAN Type	Make Static			
				2000			Disable 👻			
				1 0	default	Default	Disable			

- **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.

System	S	witching		Routing	QoS	Security	6	Monitorin	g	Maintenance	Help	Index
VLAN Au	to-VolP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAG			й.
VL	LAN		VLAN I	/lembership	9							
Basic		~	VLAN	ID						2000) ~	
Advanced		^	Group	Operation						Unta	aq All 🗸	
VLAN Cor	nfiguration	1	VLAN	Name						VLAN	12000	
VLAN Me	mbership)	VLAN	Туре						Static	:	
• VLAN Sta	itus			nit 1								
Port PVID Configurat	ion		Ports	1 3	57	9 11 13 15	17 1	9 21 2	23			
• MAC Bas	ed VLAN			υυ	UU	ບັບບັບ	UU	U	J			
Protocol E Group Cor	Based VL nfiguration	AN n		2 4	U U [UUUU 10 12 14 16	U U 18 20	0 0 1	J 4			

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

- e. Click Apply.
- 3. Associate the IP subnet with VLAN 2000.
 - a. Select Switching > VLAN > Advanced > IP Subnet Based VLAN.

Syste	em 📄	Switching		Routing	QoS	Security	N	lonitorin	g Mair	itenance	Help	Index
VLAN	Auto-VolP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAG			
Common State Sta	VLAN		IP Sub	net Based VL	AN Confi	guration						
• Basic		~		IP Address		Subnet Mask		VLAN	ID			
* Advanc	ed	^		10.100.0.0		255.255.0.0		2000				
• VLAN	l Configurati	on				1						
• VLAN	l Membersh	ip										
• VLAN	l Status											
Port F Config	⊃VID guration											
• MAC	Based VLA	N										
• Proto Group	col Based V configurati	/LAN on										
• Proto Group	col Based V Membersh	'LAN ip										
• IP Su VLAN	bnet Based I											
1												

- **b.** Enter the following information:
 - In the IP Address field, enter 10.100.0.0.
 - In the Subnet Mask field, enter 255.255.0.0.
 - In the VLAN (1 to 4093) field, enter 2000.
- c. Click Add.

Voice VLANs

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

Note: For more information about voice VLANs, see*Auto VoIP* on page 305.

Managed Switches



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.

Syste	em	Sw	vitching		Routing	QoS	Security	Monitorin	g Maintenance	Help	Index
VLAN	Auto-V	/olP	iSCSI	STP	Multicast	MVR	Address Table	Ports LAG	MLAG		
	VLA	N		Reset							
 Basic 			^	Res	et Configurat	ion					
• VLAN	I Config	uration	R								
Advance	ed		~								
				Interna	I VLAN Con	figuration					
				Inter	mal VLAN A	location Ba	se 40)93			
				Inter	mal VLAN A	location Pol	icy 🔘	Ascending	escending		
				VLAN	Configuration	n					
					MANID	/ AN Nama	VI AN TUDO	Make Static			
				-	VLANID	VLAN Name	VLAN Type	Wake Static			
					10	Voice VLAN	_	Disable Y			
					1 (default	Default	Disable			

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

System	SI	witching		Routing	QoS	Security		Monitorin	ıg	Maintenance	Help	Index
VLAN Auto	-VolP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAG		2	
VLA	N		VLAN I	Vlembership								
• Basic		~	VLAN	ID						10	Y	
 Advanced 		^	Group	Operation						Unt	ag All 🗸	
VLAN Confi	guration	1	VLAN	Name						Voic	e VLAN	
 VLAN Mem 	bership		VLAN	Туре						Stati	c	
• VLAN Statu • Port PVID Configuratio • MAC Based • Protocol Ba	is in 1 VLAN ised VI	AN	Ports	nit 1 1 3 ! T		9 11 13 15	17 1	9 21 2	23			
Group Confi	iguratio	n		2 4 1	8	10 12 14 16	18 2	0 22 2	24			

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

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

Syste	em	Sw	itching		Routing	QoS	Security	M	lonitoring	Maintenance	Help	Index	
VLAN	Auto-	VolP	iSCSI	STP	Multica	st MVR A	ddress Table	Ports	LAG MLA	.G			
• VLAN	Memb	ership		Voice	VLAN Glo	al Admin							
-VLAM	Status	6		Adn	nin Mode	🔘 Disa	ble 💽 Enable						
• Port I Confi	PVID guration	D.											
• MAC	Based	VLAN											
• Proto	col Bas	ed VLA	N	Voice	VLAN Con	figuration							
Grou	p Config	uration		12	3 All						Go To Interfac	e	Go
• Proto Grou	p Memb	ed VLA ership	N		Interface	Interface Mode	Value		CoS Over	ride Operational	Authentication	DSCP Val	ue
· IP SU	ibnet Ba	ased		-		-	_		woue	State	Wode	-	
VLA	4 .					~				~	~		
Port I	DVLAN				1/0/1	Disable	0		Disable	Disable	Enable	0	
Conn	guration	E	_		1/0/2	Disable	0		Disable	Disable	Enable	0	
Voice	VLAN				1/0/3	Disable	0		Disable	Disable	Enable	0	
Com	guration	<u>u</u>			1/0/4	Disable	0		Disable	Disable	Enable	0	
• GAR	P Switc	h			1/0/5	Disable	0		Disable	Disable	Enable	0	
South	guidtion				1/0/6	Disable	0		Disable	Disable	Enable	0	
 GARI Confi 	P Port guration	1			1/0/7	Disable	0		Disable	Disable	Enable	0	

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

A screen similar to the following displays.

Syst	em	Swi	tching		Routing	QoS	Security	M	onitoring]	Maintenance	Help	Index	
VLAN	Auto-V	/olP	iSCSI	STP	Multica	st MVR	Address Table	Ports	LAG	MLAG				
• VLAN	N Membe	ership		Voice	VLAN Glob	bal Admin								
• VLAN	V Status			Adn	nin Mode	O Dis	sable 🖲 Enable							
• Port Confi	PVID guration													
• MAC	Based \	VLAN		Victor	MAN Ore	Converting of								
• Proto Grou	p Configu	ed VLA uration	N	voice	2 All	Iguration						Co To Istadao		Co
• Proto	col Base	ed VI A	N	12	5 All							Go to intenac	e	60
Grou	p Membe	ership			Interface	Interface Mod	de Value		CoS	Override	Operational	Authentication Mode	DSCP Val	ue
· IP SL	ubnet Ba V	ised		and a		VLANID	× 10			~	otato	×	-	
• Port	DVLAN			2	1/0/1	Disable	0		Dies	blo	Disable	Enable	0	
Confi	guration		_		1/0/2	Disable	0		Disa	ible	Disable	Enable	0	
- Voice	e VLAN				1/0/3	Disable	0		Disa	ible	Disable	Enable	0	
Com	guration	6	-		1/0/4	Disable	0		Disa	ible	Disable	Enable	0	
• GAR	P Switch	n			1/0/5	Disable	0		Disa	ible	Disable	Enable	0	
0000	garation				1/0/6	Disable	0		Disa	ible	Disable	Enable	0	
• GAR Confi	P Port guration				1/0/7	Disable	0		Disa	ible	Disable	Enable	0	

e. Click Apply.

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

DiffServ	Cla	iss Name					
Diffserv Wizard		Class Name	9	Cla	ss Type		
Basic	*	ClassVoice	VLAN	ΔΙ	~		
Advanced	~			7.0			
DiffServ Configura	ation						
- Class Configurati	ion						
• IPv6 Class Config	guration						
Policy Configurat	lion						
 Service Interface Configuration 							
	5						

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

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
DiffSe	erv Cla	iss Name						
• Diffserv Wizard				Cla	as Tuno			
Basic	×	Class Warm	P.	Cia	ss type			
Advanced	~		VLAN	All	•			
DiffServ Confi	iguration		VLAN	All				
Class Config	uration							
• IPv6 Class C	onfiguration							
 Policy Config 	juration							
 Service Interf Configuration 	ace							
Service Stati	stics							

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

System Sw	<i>i</i> itching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
DiffServ	0	Class Information						
Diffserv Wizard	100	Class Name	Class	oiceVLAN				
Basic	~	Class Type	All					
 Advanced 	^							
 DiffServ Configuration 	n							
Class Configuration	6	DiffServ Class Confi	iguration					
 IPv6 Class Configur 	ation	Match Every		1				
 Policy Configuration 	ı	Reference Cla	99	Any	×			
Service Interface Configuration		Class Of Servi	ice	clas	51 Y			
Conliguration				0 ×				
- Service Statistics		© VLAN		10	(1 to 4093)			
		Secondary Cla	ass of Servici	° 0 ~				
		Secondary VL	AN		(1 to 4093)			
		Ethernet Type		Appl	etalk 🗸 🗸			
		Source MAC		Addr	ess			

- e. Click Apply.
- 7. Create the DiffServ policy PolicyVoiceVLAN.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DillSen	<i>,</i>							
DiffS	erv Po	licy Configuratio	n					
Diffserv Wizard	i	Policy Nam	e	Policy Type	Member Class			
 Basic Advanced DiffServ Config Class Config IPv6 Class C 	figuration Juration Configuration	PolicyVoice	Vlan	ln ×	ClassVoiceVLAN v			
Policy Config Service Interf Configuration Service Stati	face 1 istics							

- b. In the Policy Name field, enter PolicyVoiceVLAN.
- c. In the Policy Type list, select In.
- d. In the Member Class list, select ClassVoiceVLAN.
- e. Click Add.

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

- 8. Map the policy and class and assign them to the higher-priority queue.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
DiffSe	erv P	olicy Configuration	1					
Diffserv Wizard		Rolicy Name		Policy Type	Momber Class	1		
Basic	~		-	r oncy rype	Weinber Class			
 Advanced 	^	Policy//oice	Vlan	In				
DiffServ Confi	iguration	- I oney voice	VIGH .		010304010040144			
Class Configu	uration							
• IPv6 Class Co	onfiguration							
Policy Config	juration							
 Service Interface Configuration 	ace							
Service Statis	stics							

b. Click the **Policy PolicyVoiceVLAN**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
DiffSe	IV	Class Information						
Diffserv Wizard		Policy Name		Polic/VoiceVlan				
•Basic	~	Policy Type		In				
 Advanced 	~	Member Class N	ame	ClassVoiceVLA	N			
DiffServ Config	guration							
Class Configu	iration							
• IPv6 Class Co	onfiguration	Policy Attribute						
Policy Configu	uration	Policy Attribute	۲	Assign Queue		3 ×		
 Service Interfa Configuration 	ace		0	Drop				
Service Statis	stics		0	Mark VLAN CoS		0 ~		
			۲	Mark CoS As Se	condary CoS			
			0	Mark IP Precede	nce	0 ~		

- c. In the field next to the Assign Queue radio button, select 3.
- d. Click Apply.
- 9. Assign it to interfaces 1/0/1 and 1/0/2.
 - a. Select QoS > DiffServ > Advanced > Service Interface Configuration.

DiffServ	Servic	e Interface Confi	guration				
Diffserv Wizard	1 2	3 LAGS All			Go To Ir	nterface	Go
Basic · Advanced ·	~ •	Interface		Policy In Name	Policy Out Name	Direction	Operational Status
 DiffServ Configuration 				PolicyVoiceVlan ~	~		
 Class Configuration 	•	1/0/1					
 IPv6 Class Configuration 	2	1/0/2					
 Policy Configuration 		1/0/3					
Service Interface		1/0/4					
Configuration		1/0/6					
 Service Statistics 		1/0/7					

- b. Select the check boxes for Interfaces 1/0/1 and 1/0/2.
- c. Set the Policy Name field as PolicyVoiceVLAN.
- d. Click Apply.

Configure GARP VLAN Registration Protocol

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



Figure 4. GVRP configuration

CLI: Enable GVRP

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

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

2. On Switch A, enable GVRP.

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

3. On Switch B, enable GVRP.

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

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

(Netgear Switch) #show vlan Maximum VLAN Entries..... 1024 VLAN Entries Currently in Use..... 5 VLAN ID VLAN Name VLAN Type _____ _ ____ 1 default Default 2 Auto VoIP AUTO VOIP 1000 Dynamic (GVRP) 2000 Dynamic (GVRP) 3000 Dynamic (GVRP) (Netgear Switch) #show vlan 1000 VLAN ID: 1000 VLAN Name: VLAN Type: Dynamic (GVRP) Interface Current Configured Tagging ----- ----- ------ ------1/0/1 Exclude Autodetect Untagged 1/0/2 Exclude Autodetect Untagged 1/0/3 Exclude Autodetect Untagged 1/0/4 Exclude Autodetect Untagged 1/0/5 Exclude Autodetect Untagged 1/0/6 Exclude Autodetect Untagged 1/0/7 Exclude Autodetect Untagged 1/0/8 Exclude Autodetect Untagged 1/0/9 Exclude Autodetect Untagged 1/0/10 Exclude Autodetect Untagged 1/0/11 Include Autodetect Tagged 1/0/12 Exclude Autodetect Untagged 1/0/13 Exclude Autodetect Untagged 1/0/14 Exclude Autodetect Untagged 1/0/15 Exclude Autodetect Untagged 1/0/16 Exclude Untagged Autodetect

Web Interface: Configure GVRP on switch A

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

A screen similar to the following displays.

Syst	em	Sw	ritching		Routing	QoS	Security	Monitorin	ng Maintenance	Help	Index
VLAN	Auto-	VolP	iSCSI	STP	Multicast	MVR	Address Table	Ports LAG	MLAG		
	VLA	JN .		Reset							
Basic			^	Rese	et Configurat	ion					
• VLAI	V Config	uration	Ŕ,								
 Advance 	ed		~								
				Interna	VLAN Cont	iguration					
				Inter	na <mark>l VLAN A</mark> I	location Ba	ise 40	93			
				Inter	nal VLAN Al	location Po	olicy 🔘	Ascending 💿 D	escending		
				VLAN	Configuration	1					
					VLAN ID	/LAN Nam	e VLAN Type	Make Static			
					1000			Disable ×			
					1 c	lefault	Default	Disable			

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

A screen similar to the following displays.

Syst	em 🤤	Switching	R	Routing	QoS	Security		Monitorin	g	Maintenance	Help	Index
VLAN	Auto-VolP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAG			
	VLAN		VLAN I	Vembership								
 Basic 		~	VLAN	ID						1000	v	
 Advance 	ed	^	Group	Operation						Unta	g All 🗸	
• VLAN	I Configuration	on	VLAN	Name						VLAN	1000	
• VLAI	I Membershi	p	VLAN	Туре						Static		
Port Confi MAC Proto	PVID guration Based VLAI col Based V	N LAN	Ports	nit 1		9 11 13 15 1 1 1			3			
Grou	o Configuratio	on		2 4 1	581	10 12 14 16	18 20) 22 2	4			

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

The ports display.

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

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

- d. Click Apply.
- 3. Enable GVRP globally:
 - a. Select Switching > VLAN > Advanced > GARP Switch Configuration.

A screen similar to the following displays.

System	S	witching		Routing	QoS	Security	٨	Aonitorin	g	Maintenance	Help	Index
VLAN Au	to-VoIP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLA	G		
 Advanced 		^	GARP	Switch Confi	guration							
• VLAN Cor	nfiguratio	n	GVR	P Mode	0	Disable 🖲 Enable						
• VLAN Me	mbership		GMR	P Mode	۲	Disable 🔘 Enable						
VLAN Sta	atus											
Port PVID Configurat) tion											
• MAC Bas	ed VLAN											
 Protocol E Group Co 	Based VL nfiguratio	AN										
 Protocol E Group Me 	Based VL embership	AN										
 IP Subnet VLAN 	t Based											
 Port DVL/ Configurat 	AN tion											
 Voice VL/ Configurat 	AN tion											
GARP Sy Configurat	vitch tion											

- **b.** Next to GVRP Mode, select the **Enable** radio button.
- c. Click Apply.
- 4. Enable GVRP on port 1/0/24.
 - a. Select Switching > VLAN > Advanced > GARP Port Configuration.

A screen similar to the following displays.

Syst	em	Switching		Routing	QoS	Security M	onitoring	Maintenar	nce Help
	Auto-Voll	P iSCSI	STP	Multica	st MVR Addre	ss Table Ports	LAG ML	AG	
Advanc	ed:	^		Doct Confi	auration				
1/I AT		ion	GAR	Fort Com	guration				
V L/U	v configura		12	3 LAGS A	I		Go To Ir	iterface	Go
• VLAI	Mémbers	nip	1000					(B	
• VLA	V Status			Interface	Port GVRP Mode	Port GMRP Mode	Join Timer	Leave Timer	Leave All Timer
• Port	PVID			1/0/24	Enable 🗸	Disable 🗸	20	60	1000
Confi	guration			1/0/1	Disable	Disable	20	60	1000
• MAC	Based VL	AN		1/0/2	Disable	Disable	20	60	1000
• Prote	col Based	VLAN		1/0/3	Disable	Disable	20	60	1000
Grou	p Configura	tion		1/0/4	Disable	Disable	20	60	1000
• Proto	col Based	VLAN		1/0/5	Disable	Disable	20	60	1000
Grou	p Members	hip		1/0/6	Disable	Disable	20	60	1000
• IP St	ubnet Base	i i		1/0/7	Disable	Disable	20	60	1000
VLA	V			1/0/8	Disable	Disable	20	60	1000
• Port	DVLAN			1/0/9	Disable	Disable	20	60	1000
Confi	guration			1/0/10	Disable	Disable	20	60	1000
• Voice	e VLAN			1/0/11	Disable	Disable	20	60	1000
Confi	guration			1/0/12	Disable	Disable	20	60	1000
GAR	P Switch			1/0/13	Disable	Disable	20	60	1000
Confi	guration			1/0/14	Disable	Disable	20	60	1000
• GAR	P Port			1/0/15	Disable	Disable	20	60	1000
Com	guration			410140	mission.	D:	20	c0	4000

b. Scroll down and select the check box that corresponds to interface 1/0/24.
 The Interface field in the table heading displays 1/0/24.

- c. From the Port GVRP Mode menu, select Enable.
- d. Click Apply.

Web Interface: Configure GVRP on Switch B

- **1.** Enable GVRP globally:
 - a. Select Switching > VLAN > Advanced > GARP Switch Configuration.

A screen similar to the following displays.

Syster	m S	witching		Routing	QoS	Security		Monitorin	g	Maintenance	Help	Index
VLAN	Auto-VoIP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAG	G		s 1.1 se
VLAN • Advance • VLAN • VLAN • VLAN • VLAN • Port P' Configu • MAC E • Protoc Group	Auto-VoIP d Configuratio Membershi Status VID uration Based VLAM ol Based VLAM configuratio	iSCSI	GARP GVR GMR	Multicast Switch Confi IP Mode RP Mode	MVR guration © [@ [Address Table	Ports	LAG	MLAG	G		
Protoc Group IP Sub VLAN Port D Configu Voice Configu GARP Configu	ol Based VI Membershi onet Based VLAN uration VLAN uration Switch uration	ΔAN p										

- **b.** Next to GVRP Mode, select the **Enable** radio button.
- c. Click Apply.
- 2. Enable GVRP on port 1/0/11:
 - a. Select Switching > VLAN > Advanced > GARP Port Configuration.

Syst	em	Swite	hing		Routing	QoS	Security M	onitoring	Maintenar	nce Help	Index
	Auto-Voll	P iS	SCSI	STP	Multica	st MVR Addre	ess Table Ports	LAG ML	AG		
Advanc • VLAI • VLAI	ced N Configurat N Members	tion hip	^	GARF	Port Confi 3 LAGS A	guration		Go To In	terface	Go	
• VI AI	V Status				Interface	Port GVRP Mode	Port GMRP Mode	Join Timer	Leave Timer	Leave All Timer	
• Port	PVID				1/0/11	Enable Y	Disable 🗸	20	60	1000	
Confi	iguration				1/0/1	Disable	Disable	20	60	1000	
• MAC	Based VL	AN			1/0/2	Disable	Disable	20	60	1000	
• Prote	ncol Based	VIAN			1/0/3	Disable	Disable	20	60	1000	
Grou	p Configura	tion			1/0/4	Disable	Disable	20	60	1000	
• Proto	col Based	VLAN			1/0/5	Disable	Disable	20	60	1000	
Grou	p Members	hip			1/0/6	Disable	Disable	20	60	1000	
• IP St	ubnet Baser	d			1/0/7	Disable	Disable	20	60	1000	
VLA	N				1/0/8	Disable	Disable	20	60	1000	
• Port	DVLAN				1/0/9	Disable	Disable	20	60	1000	
Confi	iguration				1/0/10	Disable	Disable	20	60	1000	
• Voice	e VLAN				1/0/11	Disable	Disable	20	60	1000	
Confi	iguration				1/0/12	Disable	Disable	20	60	1000	
• GAR	P Switch				1/0/13	Disable	Disable	20	60	1000	
Confi	iguration				1/0/14	Disable	Disable	20	60	1000	
- GAR	P Port				1/0/15	Disable	Disable	20	60	1000	
Confi	iguration				410140	Dissue.	Dissel	20	C0	4000	

- **b.** Scroll down and select the check box that corresponds to interface 1/0/11. The Interface field in the table heading displays 1/0/11.
- c. From the Port GVRP Mode menu, select Enable.
- d. Click Apply.

Private VLANs

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

There are three types of VLAN within a private VLAN:

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

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

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

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



Figure 5. Private VLANs

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



Figure 6. Packet flow within a Private VLAN domain

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

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

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

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

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

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Se	curity Acce	ss Port Aut	nentication Tra	flic Control Cor	ntrol ACL			
Traffic Con	itrol	Private VLAN	Fype Configuratio	1				
• MAC Filter	~	VIANI	D Private VI AN	Туре				
 Port Security 	~	100	Primany	* .)}po				
Private Group	~		Unconfigured	6				
Protected Port		100	Unconfigured					
Private Vlan	~	101	Unconfigured					
Private Vlan Tr Configuration	ype	102	Unconfigured					
 Private Vlan Association Configuration 								

- **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.

System	Swit	ching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	Security	Access	Port Authe	ntication Tra	fic Control Cor	ntrol ACL			
Traffic Co	ontrol	Priv	vate VLAN Ty	pe Configuration					
• MAC Filter		×	VLAN ID	Private VI AN	Type				
Port Security		~	101	Isolated	v				
Private Group		×	1	Unconfigured					
Protected Port			100	Primary					
• Private Vlan		~ 1	101	Unconfigured					
Private Vlan Configuration	Туре		102	Unconfigured					
Conliguration	a:								

- **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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Se	curity Access	Port Authe	ntication Trai	fic Control Cor	itrol ACL			
Traffic Cor	ntrol Priv	ate VLAN Ty	pe Configuration					
• MAC Filter	× 1		Private VI AN	Τιγρο				
 Port Security 	v	402	Community	, ypc				
Private Group	v	102	Unconfigured	·				
Protected Port		100	Primary					
• Private Vlan	~ 1	101	Isolated					
Private Vlan T	ype	102	Unconfigured					
Configuration								

- **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.

System	Swit	ching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	lecurity	Access	Port Authenti	ication Trai	fic Control Co	introl ACL			
-									
Traffic Co	ontrol	Pri	vate VLAN Asso	ociation					
• MAC Filter		~	Primary VL	AN Seconda	ary VLAN(s)	Isolated VLAN	Community VLAN(s)		
Port Security		~	100 ~	101-102	2				
 Private Group 		¥	100						
Protected Port									
 Private Vlan 		^							
 Private Vlan Configuration 	Type 1								
 Private Vlan Association Configuration 	1								

- 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.

System	Swite	ching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	Security	Acces	s I	Port Authe	ntication Trafi	ic Control Co	ntrol ACL			
Traffic C	ontrol	P	rivate	e Vlan Port	Mode Configura	ation				
• MAC Filter		~	12	3 LAGS A	II Go To Interfac	e	Go			
Port Security		~		Interface	Port Vlan Mod					
Private Group		~	-	Intenace	Port vian woo	e				
Protected Port				1/0/1	Promiscuous	~				
- intected i on			1/0/1	General						
Private Vlan		^		1/0/2	General					
Private Vlan	Туре			1/0/3	General					
Configuration	1			1/0/4	General					
Private Vlan				1/0/5	General					
Association	2			1/0/6	General					
Comguration				1/0/7	General					
 Private Vlan Configuration 	Port Mod n	e		1/0/8	General					
- Deivete Miere	l la ak	-		1/0/9	General					
Interface Co	nfiguration	1		1/0/10	General					
- Driveta Mare				1/0/11	General					
Promiscuou	s Interface	е		1/0/12	General					
Configuration	n			1/0/13	General					

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.

System	Swit	ching	Routi	ig	loS	Security	Monitoring	Maintenance	Help	Index
Management S	Security	Access	Port A	Ithenticatio	i Tra	affic Control Co	entrol ACL			
Traffic Co	ontrol	Pr	vate Vlan	⊃ort Mode	Configui	ration				
• MAC Filter		× .	1 2 3 LAC	S All Go T	Interfa	ice	Go			
Port Security		~								
• Private Group		~	lnterf	ice Port \	lan Mo	de				
- Destanted Dest				Host		~				
· Protected Port			1/0/1	Promi	scuous					
• Private Vlan		^	1/0/2	Gener	al					
Private Vlan	Туре		1/0/3	Gener	al					
Configuration	1		☑ 1/0/4	Gener	al					
Private Vlan			1/0/5	Gener	al					
Configuration	1		1/0/6	Gener	al					
• Prinoto Vion	Port Mor		1/0/7	Gener	al					
Configuration		e	1/0/8	Gener	al					
Private Vlan	Host		1/0/9	Gener	al					
Interface Cor	nfiguration	1	1/0/1) Gener	al					

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

System	Swite	ching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Se	curity	Access	Port Authe	ntication Traffic	Control Co	ntrol ACL			
Traffic Con	itrol	Pri	vate VLAN Ho	ost Interface Config	uration				
• MAC Filter		• T	1 2 3 LAGS A	All		Go To Interface	Go		
 Port Security 		~		11		5 I 3/1 ANI			
Private Group		~	Interface	(2 to 4093)	AN Host : (2 to 4	Secondary VLAN 1093)	Operational VLAN(s)		
Protected Port				100	101				
Private Vlan		~	1/0/1	0	0				
• Private Vlan Tr	vne		1/0/2	0	0				
Configuration	ypo		✓ 1/0/3	0	0				
• Private Vlan			1/0/4	0	0				
Association			1/0/5	0	0				
Configuration			1/0/6	0	0				
• Private Vlan P	ort Mod	e	1/0/7	0	0				
Configuration	Configuration		1/0/8	0	0				
Private Vlan H	Private Vlan Host		1/0/9	0	0				
Interface Configuration			1/0/10	0	0				

- **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.

System	Switch	ing	Routing	QoS	Security	Monitoring	Maintenance	Help	Inde
Management Secu	rity	Access	Port Authe	ntication Traffic	Control Con	trol ACL			
Traffic Contro	ol	Priv	rate VLAN Ho	ist Interface Config	uration				
MAC Filter	2	1	2 3 LAGS A	All		Go To Interface	Go		
Port Security				11 . D	ANI 11 1 0	1			
Private Group		-	Interface	(2 to 4093)	AN Host 5 (2 to 4	econdary vLAN 093)	Operational VLAN(s)		
Protected Port				100	102				
Private Vlan		د آ	1/0/1	0	0				
• Private Vlan Tvn		1	1/0/2	100	101		100-101		
Configuration		1	1/0/3	100	101		100-101		
Drivato Vilan			✓ 1/0/4	0	0				
Association			1/0/5	0	0				
Configuration		1	1/0/6	0	0				
Private Vlan Por	t Mode		1/0/7	0	0				
Configuration			1/0/8	0	0				
Private Vlan Hos			1/0/9	0	0				
Interface Configuration			1/0/10	0	0				

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

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

Map Private-VLAN Promiscuous Port

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

CLI: Map Private-VLAN Promiscuous Port

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

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

Web Interface: Map Private-VLAN Promiscuous Port

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

System	Switching		Routing	QoS	Security	Monitoring	Maintenar	ice Help	Index
Management S	ecurity Acc	ess	Port Authe	ntication Tre	Tic Control Co	introl ACL			
Traffic Co	ntrol	Private	e VLAN Pre	omiscuous Inte	face Configuration	n			
• MAC Filter	~	1 2	3 LAGS A	ll		G	o To Interface	Go	
Port Security	~	1							7
Private Group	~		Interface	(2 to 4093)	Primary VLAN	Promiscuous Seco Range[2-4093]	ndary VLAN(s)	Operational VLAN(s)	
Protected Port			1/0/1	100		101-102			
Private Vlan	~		1/0/1	0					
• Private Vlan]	Type		1/0/2	0				100-101	
Configuration	ypo		1/0/3	0				100-101	
• Private Vlan			1/0/4	0				100,102	
Association			1/0/5	0				100,102	
Configuration			1/0/6	0					
Private Vlan	Port Mode		1/0/7	0					
Configuration			1/0/8	0					
Private Vlan I	lost		1/0/9	0					
Interface Con	tiguration		1/0/10	0					
Private Vlan	Interface		1/0/11	0					
Configuration	intenace		1/0/12	0					

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

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

VLAN Access Ports and Trunk Ports

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

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

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

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

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

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



Figure 7. Access and trunk ports

CLI: Configure a VLAN Trunk

1. Create VLAN 1000 and 2000.

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

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

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

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

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

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

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

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

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

Web Interface: Configure a VLAN Trunk

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

Syste	em	Sw	itc hing		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
	Auto-V	olP	iSCSI	STP	Multicast	MVR	Address Table	Ports LAG	MLAG MRP		
	VLAN	١		Reset							1.1
Basic			^	Res	et Configura	ation					
• VLAN	I Configu	uration	ы.		1						
Advanc	ed		~								
				Internal	VLAN Con	figuration					
				Inte		loc ation B	926	1003			20
				Inte		Illesation D	ase	According @ D	assanding		
				inte	mai vlan P	Allocation P	olicy	Ascending 💿 D	escenaing		
				VLAN (Configuration	n					
					VLAN ID	VLAN Nan	ne VLAN Typ	Make Static			
					1000	L		Disable 🗸			
					1	default	Default	Disable			

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

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

A screen similar to the following displays.

System Swit	tching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VLAN Auto-VoIP	ISCSI STR	Multicast	MVR Ad	idress Table	Ports LAG	MLAG MRP		
VLAN	Reset							
Basic	^ Re	set Configura	tion					
 VLAN Configuration 				-				
Advanced	¥							
	Interna	al VLAN Conf	iguration					
	1.0		Ilexation Deca	10	22			
	Int	emai VLAN A	liocation base	40	assessing @ D			
	Int	emai vlan A	liocation Polic	y Of	Ascending 🖲 De	escending		
	VLAN	Configuration						
		Configuration						
		VLAN ID	VLAN Name	VLAN Type	Make Static			
		2000			Disable 🗸			
		1	default	Default	Disable			
		1000	VLAN1000	Static	Disable			

- b. In the VLAN ID field, enter 2000.
- c. Click Add.
- 2. Configure port 1/0/1 as an access port in VLAN 1000.
 - a. Select Switching > VLAN > Advanced > VLAN Trunking Configuration.

System	Switch	ning		Routing	QoS	Security Monito	ring Mainter	ance Help	Index
VLAN Auto-	-VolP iS	CSI	STP	Multicas	t MVR Addr	ess Table Ports LA	G MLAG MRP		
1									
5			Cuitala	and Canton	and an				
VL	AN		Switch	Jon Coning	uration				
Basic		~	12	3 LAG All				Go To Interfac	Go
 Advanced 		^		Interface	Switchport Mode	Native VLAN Tagging	Access VLAN ID	Native VLAN ID	Trunk Allowed VLANs
·VLAN Confi	guration			1/0/1	Access v	Disable	1000 ×	1 ×	1-4093
VLAN Trunking				1/0/1	General	Disable	1	1	1_4093
Configuratio	Configuration			1/0/2	General	Disable	1	1	1-4093
 VLAN Memi 	bership			1/0/3	General	Disable	1	1	1-4093
·VLAN Statu	S			1/0/4	General	Disable	1	1	1-4093
• Port PVID (- Port DV/D Configuration			1/0/5	General	Disable	1	1	1-4093
MAG Based		³⁷		1/0/6	General	Disable	1	1	1-4093
• MAC Based	VLAN			1/0/7	General	Disable	1	1	1-4093
Protocol Bas	sed VLAN			1/0/8	General	Disable	1	1	1-4093
Group Conn	guration			1/0/9	General	Disable	1	1	1-4093
Protocol Bas	sed VLAN			1/0/10	General	Disable	1	1	1-4093
Gloup Merri	bership			1/0/11	General	Disable	1	1	1-4093
 IP Subnet B 	ased VLAN	1		1/0/12	General	Disable	1	1	1-4093
· Port DVLAN	1			1/0/13	General	Disable	1	1	1-4093
Configuratio	n			1/0/14	General	Disable	1	1	1-4093
Voice VLAN	I			1/0/15	General	Disable	1	1	1-4093
Configuratio	n			1/0/16	General	Disable	1	1	1-4093
· GARP Swite	ch			1/0/17	General	Disable	1	1	1-4093
Configuratio	n			1/0/18	General	Disable	1	1	1-4093
• GARP Port				1/0/19	General	Disable	1	1	1-4093
Configuration				1/0/20	General	Disable	1	1	1-4093

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

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

- c. In the Switchport Mode field, select Access.
- d. In the Access VLAN ID field, select 1000.
- e. Click Apply.
- 3. Configure port 1/0/2 as an access port in VLAN 2000.
 - a. Select Switching > VLAN > Advanced > VLAN Trunking Configuration.

A screen similar to the following displays.

System Switching			Routing QoS Secur		Security Monitor	ring Mainter	hance Help	Index			
VLAN Auto-VoIP	iscsi	STP	Multicas	t MVR Addre	ss Table Ports LA	G MLAG MRP					
VLAN	1	Switch	port Config	uration							
Basic	~	1 2 3 LAG All Go To Interface Go									
Advanced	^		Interface	Switchport Mode	Native VLAN Tagging	Access VLAN ID	Native VLAN ID	Trunk Allowed VLANs			
VLAN Configuration			1/0/2	Access *	Disable	2000 ¥	1 *	1-4093			
VLAN Trunking			1/0/1	Access	Disable	1000	1	1-4093			
Configuration			1/0/2	General	Disable	1	1	1-4093			
 VLAN Membership 			1/0/3	General	Disable	1	1	1-4093			
VLAN Status			1/0/4	General	Disable	1	1	1-4093			
• Port PVID Configura	ation		1/0/5	General	Disable	1	1	1-4093			
-Poitr vib oomgaa	aton		1/0/6	General	Disable	1	1	1-4093			
 MAC Based VLAN 			1/0/7	General	Disable	1	1	1-4093			
Protocol Based VLA	N		1/0/8	General	Disable	1	1	1-4093			
Group Configuration			1/0/9	General	Disable	1	1	1-4093			
Protocol Based VLA	N		1/0/10	General	Disable	1	1	1-4093			
Gloup membership			1/0/11	General	Disable	1	1	1-4093			
 IP Subnet Based VL 	AN		1/0/12	General	Disable	1	1	1-4093			
Port DVLAN			1/0/13	General	Disable	1	1	1-4093			
Configuration			1/0/14	General	Disable	1	1	1-4093			
Voice VLAN			1/0/15	General	Disable	1	1	1-4093			
Configuration			1/0/16	General	Disable	1	1	1-4093			
· GARP Switch			1/0/17	General	Disable	1	1	1-4093			
Configuration			1/0/18	General	Disable	1	1	1-4093			
GARP Port			1/0/19	General	Disable	1	1	1-4093			
Connguration			1/0/20	General	Disable	1	1	1-4093			
			1/0/21	General	Disable	1	1	1-4093			

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

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

- c. In the Switchport Mode field, select Access.
- d. In the Access VLAN ID field, select 2000.
- e. Click Apply.
- 4. Configure port 1/0/3 as a trunk port that allows VLANs 1000 and 2000.
 - a. Select Switching > VLAN > Advanced > VLAN Trunking Configuration.

Managed Switches

System Switching	i i	Routing	QoS	Security Monito	ring Mainter	ance Help	Index	
VLAN Auto-VolP iSCS	STP	Multicas	at MVR Addre	ss Table Ports LA	G MLAG MRP	6		
VLAN	Switch	port Config	uration					
Basic ~	12	3 LAG All				Go To Interfa	ce Go	
Advanced ^	Interface Switchport Mr		Switchport Mode	Native VLAN Tagging	Access VLAN ID	Native VLAN ID	Trunk Allowed VLANs	
 VLAN Configuration 		1/0/3	Trunk	Disable	1 ×	2000 ×	1000,2000	
VLAN Trunking	0	1/0/1	Access	Disable	1000	1	1-4093	
Configuration		1/0/2	Access	Disable	2000	1	1-4093	
 VLAN Membership 	1	1/0/3	General	Disable	1	1	1-4093	
VLAN Status		1/0/4	General	Disable	1	1	1-4093	
Port PVID Configuration		1/0/5	General	Disable	1	1	1-4093	
MAC Development		1/0/6	General	Disable	1	1	1-4093	
• MAC Based VLAN		1/0/7	General	Disable	1	1	1-4093	
Protocol Based VLAN		1/0/8	General	Disable	1	1	1-4093	
Group Conliguration		1/0/9	General	Disable	1	1	1-4093	
Protocol Based VLAN Group Membership		1/0/10	General	Disable	1	1	1-4093	
Group Membership		1/0/11	General	Disable	1	1	1-4093	
IP Subnet Based VLAN		1/0/12	General	Disable	1	1	1-4093	
Port DVLAN		1/0/13	General	Disable	1	1	1-4093	
Configuration		1/0/14	General	Disable	1	1	1-4093	
Voice VLAN		1/0/15	General	Disable	1	1	1-4093	
Configuration		1/0/16	General	Disable	1	1	1-4093	
GARP Switch		1/0/17	General	Disable	1	1	1-4093	
Configuration		1/0/18	General	Disable	1	1	1-4093	
GARP Port		1/0/19	General	Disable	1	1	1-4093	
Configuration		1/0/20	General	Disable	1	1	1-4093	
		1/0/21	General	Disable	1	1	1-4093	

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

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

- c. In the Switchport Mode field, select Trunk.
- d. In the Native VLAN ID field, select 2000.
- **Note:** In this step, you configure incoming untagged packets to be tagged with VLAN ID 2000. If you want the switch to drop untagged packets, ignore this step.
- e. In the Trunk Allowed VLANs field, enter 1000,2000.
- f. Click Apply.

LAGs

Link Aggregation Groups

This chapter includes the following sections:

- Link Aggregation Concepts
- Add Ports to LAGs



Link Aggregation Concepts

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



Figure 8. Example network with two LAGs

LAGs offer the following benefits:

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

Add Ports to LAGs

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

CLI: Add Ports to the LAGs

(Netgear	Switch)	#config		
(Netgear	Switch)	(Config)#ir	nterface 0/2	
(Netgear	Switch)	(Interface	0/2)#addport	1/1
(Netgear	Switch)	(Interface	0/2)#exit	
(Netgear	Switch)	(Config)#ir	nterface 0/3	
(Netgear	Switch)	(Interface	0/3)#addport	1/1
(Netgear	Switch)	(Interface	0/3)#exit	
(Netgear	Switch)	(Config)#ir	nterface 0/8	
(Netgear	Switch)	(Interface	0/8)#addport	1/2
(Netgear	Switch)	(Interface	0/8)#exit	
(Netgear	Switch)	(Config)#ir	nterface 0/9	
(Netgear	Switch)	(Interface	0/9)#addport	1/2
(Netgear	Switch)	(Interface	0/9)#exit	
(Netgear	Switch)	(Config)#ex	kit	

Web Interface: Add Ports to LAGs

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

Syste	System		Switching		Routing	QoS	Sec	urity	Mc	onitoring	3	Maintenance	Help	Index	
VLAN	Auto-\	VolP	iSCSI	STP	Multicast	MVR	Address Ta	ible P	orts		MLA	G			
	LAG	3		LAG M	lembership										
LAG Configuration				LAG	D				12						
LAG M	embersl	hip						Lag 1 👻							
			LAG	ch1											
			Admin Mada												
				Admi	n wode			Enable	e v						
				Link	Irap			Disabl	le v						
				STP I	Mode			Enabl	e ¥						
			Statio	Mode	Disabl	le 🛩									
				Hash	Mode	Src/Dest MAC, VLAN, EType, incoming port 👻						ort 🗸			
		Unit 1										^			
			Ports 1 3 5 7 9 11 13 15 17 19 21 23												
					2 4 6	5 8	10 12 14	16 18	20	22 2	4				

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

Two check marks display in the box.

- e. Click the Apply button to save the settings.
- 2. Add ports to lag_20.
 - a. Select Switching > LAG > LAG Membership.

Syst	em	Switching	Routing	QoS	Security	Monitorin	g Maintenance	Help	Index	
VLAN	Auto-Vo	olP iSCSI	STP Multicas	t MVR	Address Table	Ports LAG	MLAG			
	LAG		LAG Membership							
•LAG C	onfiguratio	n	LAG ID	9	1.55	0				
LAG Membership		р	LAG Name	Lag	Lag 2 ×					
			LAG Description		GIZ					
			Admin Mode		Ena	ble 👻				
			Link Trap		Disa	able 🗸				
			STP Mode		Ena	ble 🛩				
			Static Mode		Disa	able 🛩				
			Hash Mode		Src	Dest MAC, VL	AN, EType, incoming port	~		
			Unit 1			^				
			Ports 1 3	5 7 9 	11 13 15 15 15 15 16 12 14	17 19 21 2 1 1 1 2 1 1 1 2 1 1 2 2 2	23 24			

- 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.
MLAGs



Multichassis Link Aggregation Groups

This chapter includes the following sections:

- Multichassis Link Aggregation Concepts
- Create an MLAG
- Enable Static Routing on MLAG Interfaces
- Enable DCPDP on MLAG Interfaces
- Troubleshoot the MLAG Configuration

Note: MLAGs are available on the M6100 and M7100 series switches only.

Multichassis Link Aggregation Concepts

In a Layer 2 network, Spanning Tree Protocol (STP) is deployed to avoid network loops. With STP running, ports can either be in forwarding or in blocked state. When a topology change occurs, STP reconverges the network to a new stable loop-free network. STP is successful in managing Layer 2 networks and mitigating loops in the network.

However, because STP marks ports as forwarding or blocking, a significant percentage of the links in a network do not carry data traffic. Also, any disruption in existing links causes a reconvergence of up to several seconds.

New loop management technologies include Spanning Tree Bridges and Transparent Interconnection of Lots of Links (TRILL), and a multichassis LAG (MLAG) solution such as Virtual Private Cloud (VPC).

To avoid using STP, you can bundle together multiple links between two adjacent switches using a link aggregation group (LAG). The advantages of a LAG are that all member links are in forwarding state and a link failure does not cause disruptions in the order of seconds (a LAG handles a link failure in less than one second). However, if a device failure occurs in a typical LAG setting, the network can go down.

A multichassis LAG (MLAG) carries the advantages of a LAG across multiple devices. An MLAG enables links that are on two different switches to pair with links on a partner device. The remote partner device does not detect that it is pairing with two different devices to form a LAG. The advantages of an MLAG are that all links can carry data traffic simultaneously, and if a link or device failure occurs, the network can be resolved and the traffic can resume quickly.

The following figure shows an example of an MLAG deployment topology.



Figure 9. Example of an MLAG deployment topology

In the MLAG deployment topology example:

- P and S are MLAG-aware peer devices. P stands for primary device and S stands for secondary device. The roles are elected after the devices exchanged keep-alive messages. The primary device owns the MLAG member ports on the secondary device. The primary device handles the control plane functionality of supported protocols for the MLAG member ports on the secondary.
- The two devices are connected with a peer link. The peer link must be configured on a port-channel interface (that is, a LAG). Only one peer link is allowed per switch. All instances of MLAG running on the two peer switches share this peer link. The peer link is used for the following purposes:
 - Carry keep-alive messages to the peer.
 - Syncing forwarding database (FDB) entries that are learned on MLAG interfaces between the two MLAG peer switches.

- STP Bridge Protocol Data Units (BPDUs) and Link Aggregation Control Protocol Data Units (LACPDUs) that are received on secondary MLAG member ports are forwarded to the primary MLAG component over the peer link.
- Interface events that are related to the MLAG interface and its member ports and that occur on the secondary device are transferred over the peer link to the primary device for handling.
- MLAG control information between the primary device and the secondary MLAG switches is carried over the peer link.
- When all member ports of an MLAG interface are down on one MLAG switch, the traffic that is received on that switch and that is destined for the MLAG is sent over the peer link to the peer MLAG switch for forwarding.

The MLAG deployment topology example also includes the following ports and devices:

- P21, P22, P23, P24, S21, S22, S23, and S24 are the port-channel ports that form the peer link.
- Ports P11, S11 are members of MLAG1 and ports P12, S12 are members of MLAG2.
- A, B, and C, are LAG devices.
- A and B are partner devices that form an MLAG with P and S. On A and B, the LAG1 is a regular LAG.

In the MLAG deployment topology example, the following restrictions and limitations apply:

- Layer 3 dynamic routing protocols such as OSPF and RIP are not supported on an MLAG interface.
- IGMP snooping is not supported with an MLAG.
- The peer link is a crucial link. You must configure a port channel as the peer link. If the peer link is overwhelmed with data, traffic is disrupted.
- If the FBD on the primary device has the same limit (that is, the same number of maximum supported MAC addresses) as on the secondary device, both devices are in synchronization until the limit is reached. When the limit is exceeded, the primary and secondary devices do not learn the same set of FDB entries, and the FBD tables are no longer in synchronization.
- Traffic might be disrupted during the time when an MLAG interface goes down on one device and the peer device is programmed to forward the traffic over this MLAG on the peer device.
- An MLAG cannot be formed between more than two devices. All instances of MLAG must run on the same two devices.
- All primary instances of MLAG are handled on one device.
- Keep-alive links and peer links are shared across all instances of MLAG that are running between the two devices.
- The virtual IP addresses of the Virtual Router Redundancy Protocol (VRRP) routers must be different from the physical IP address of either peer. Following this requirement ensures that the packets that are generated at either of the peers are transmitted with the source MAC address as the physical MAC address and not the virtual MAC address.

Create an MLAG

In this configuration example, each MLAG switch has three LAGs:

- Two LAGs to the remote LAG partner: LAG2 and LAG3
- One LAG to the peer MLAG device: LAG1

If more remote devices are needed, follow the steps in the following sections to add them.

This configuration example is presented as CLI commands and as a web interface procedure.

CLI: Create an MLAG on LAG2 and LAG3

1. Enable MLAG globally.

```
(Switch P or S) #config
(Switch P or S) (Config)#feature vpc
```

2. Enable the MLAG keep-alive protocol in the MLAG (VPC) domain.

This step is mandatory.

```
(Switch P or S) (Config)#vpc domain 1
(Switch P or S) (Config-VPC 1)#peer-keepalive enable
(Switch P or S) (Config-VPC 1)#exit
```

3. Enable the MLAG peer link on LAG1 that is used to connect the MLAG peers.

After you have configured a peer link, the traffic from the peer link is prevented from leaving any MLAG member port. When a failure occurs on one MLAG peer switch and the traffic has to flow through the MLAG member ports of the peer, the traffic that arrives from the peer link on the second MLAG device can leave only from select MLAG interfaces. Therefore, you need to configure the following options on the port channel of the peer link:

- Disable STP on the peer link.
- Include the peer link in all the VLANs that are configured on all MLAG interfaces on the device.
- Enable egress tagging on the peer link.
- NETGEAR recommends that you use dynamic LAGs as port channels.
- NETGEAR recommends that you configure Unidirectional Link Detection (UDLD) to detect and shut down any unidirectional links.

```
(Switch P or S) (Config)#interface lag 1
(Switch P or S) (Interface lag 1)#vpc peer-link
(Switch P or S) (Config)#exit
```

4. Disable STP on the peer link (LAG1).

This step is mandatory.

```
(Switch P or S) (Config)#interface lag 1
(Switch P or S) (Interface lag 1)#no spanning-tree port mode
```

5. Enable UDLD on the member of LAG 1 (peer link).

This step is not mandatory but recommended.

```
(Switch P or S) (Config)#udld enable
(Switch P or S) (Interface 0/21-0/24)#udld enable
```

6. Create MLAG1 on LAG2.

```
(Switch P or S) (Config)#interface lag 2
(Switch P or S) (Interface lag 2)#vpc 1
(Switch P or S) (Config)#exit
```

7. Create MLAG2 on LAG3.

```
(Switch P or S) (Config)#interface lag 3
(Switch P or S) (Interface lag 3)#vpc 2
(Switch P or S) (Config)#exit
```

8. Create MLAG3 on LAG4.

```
(Switch P or S) (Config)#interface lag 4
(Switch P or S) (Interface lag 4)#vpc 3
(Switch P or S) (Config)#exit
```

9. Check the status of VPC1, VPC2, and VPC3.

```
(Switch P or S) #show vpc 1
VPC id# 1
_____
Config mode..... Enabled
Operational mode..... Enabled
Port channel..... lag 2
Self member ports Status
----- -----
0/11
           ΠP
Peer member ports Status
----- -----
0/11
           IID
(Switch P or S) #show vpc 2
VPC id# 2
_____
Config mode..... Enabled
Operational mode..... Enabled
Port channel..... lag 3
Self member ports Status
_____ _
0/12
           UP
Peer member ports Status
----- -----
0/12
           UP
(Switch P or S) #show vpc 3
VPC id# 2
_____
Config mode..... Enabled
Operational mode..... Enabled
Port channel..... lag 4
Self member ports Status
----- -----
0/1
           UP
Peer member ports Status
_____ ____
0/1
           UP
```

Web Interface: Create an MLAG on LAG2, LAG3, and LAG4.

- 1. Enable MLAG and configure LAG1 as the peer link.
 - a. Select Switching > MLAG > Basic > VPC Global Configuration.

A screen similar to the following displays.

Syst	em	Sv	vitching		Routing	QoS	Security		Monitorin	g	Maintenance	Help	Index
VLAN	Auto-\	VolP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	ML	AG		
	MLA	G		VPC G	lobal Configu	uration							
Basic			^	Dom	ain ID	1							
• VPC Confi	Global			VPC	Mode) (©	Disable 💿 Enabl	Э					
• Advanc	ed:		.*	Devic Syste Keepali	e Role em MAC ve Paramete	Nor 6C: ers	ne B0:CE:19:AE:3E						
				Keep	alive Priority		100			(1 to	255) secs		
				Keep	alive Timeou	ıt	5			(2 to	15) secs		
				Keep	alive Admin	Mode	Di	able 🔘	Enable				
				Keep	alive Operat	ional Mode	e Disab	led					
				Peer Li Enab Port	nk le Modificati Channel	on	None Y]					
				Peer	Link Status		Down						
				Peer	Keepalive P	riority	0						
				Peer	Link STP M	ode							

- **b.** For VPC Mode, select the **Enable** radio button.
- c. Select the Enable Modification check box.
- d. From the Port Channel menu, select lag 1.
- e. Click Apply.
- 2. Disable STP on LAG 1.
 - a. Select Switching > MLAG > Basic > VPC Global Configuration.

Syst	em	Switching		Routing	QoS	Security	Λ	Ionitoring	Maintenance	Help	Index
VLAN	Auto-Vol	P iSCSI	STP	Multicast	MVR.	Address Table	Ports	LAG	MLAG		
	MLAG		VPC G	lobal Configu	ration						
Basic		^	Dom	ain ID	1						
VPC Confi	Global		VPC	Mode	0[Disable 🖲 Enable	e				
= Advanc	od	×	Devic	e Role	Nor	ie					
Auvano	.eu		Syste	em <mark>M</mark> AC	20:0	DC:C8:4D:95:96					
			Keepali	ve Paramete	rs						
			Keep	alive Priority		100		('1 to 255) secs		
			Keep	alive Timeou	t	5		('2 to 15) secs		
			Keep	alive Admin I	Vode	🖲 Dis	able 🔘 🛙	Enable			
			Keep	alive Operati	onal Mode	e Disab	ed				

b. Scroll down and select the interface **lag1** check box.

The Interface field in the table heading displays lag1.

- c. In the Port Mode field, select **Disable**.
- d. Click Apply.
- 3. Enable UDLD on the members of LAG1.

The web management interface does not support UDLD so you need to use the CLI. For more information, see *CLI: Create an MLAG on LAG2 and LAG3* on page 77.

- 4. Create MLAG on LAG2.
 - a. Select Switching > MLAG > Advanced > VPC Interface Configuration.

Syste	em	Sv	witching		Routing	QoS	Security	N	Aonitorin	g	Maintenance	Help	Index
VLAN	Auto-	VolP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAG			
	MLA	١G		VPC In	terface Config	guration							
• Basic			~		LAG Interface	e State	VPC Identifier						
 Advanc 	ed		~		lag 2 →		1						
• VPC Confi	Global guration	1											
• VPC Confi	Interfac guration	:e 1											
• VPC	Interfac	e Deta	uls										
• VPC Statis	Keepal stics	ive											
• VPC Statis	Peer Li stics	nk											

- **b.** From the LAG Interface menu, select **lag 2**.
- c. In the VPC Identifier field, enter 1.
- d. Click Add.
- 5. Create MLAG on LAG3.
 - a. Select Switching > MLAG > Advanced > VPC Interface Configuration.

Syst	em	Swite	hing		Routing		QoS	Security		M	lonitorin	ıg	Mainte	папсе	lelp	Index
VLAN	Auto-VolF	o is	SCSI	STP	Multi	cast	MVR	Address Table	Po	rts	LAG					
	MLAG			VPC Ir	nterface	Config	uration									
 Basic 			~		LAG Int	erface	State	VPC Identi	fier							
• Advanc	ed		^		lag 3	~		2								
• VPC Confi	Global guration				lag 2		Disable	ed 1								
• VPC Confi	Interface guration															
• VPC	Interface D	etails														
• VPC Stati:	Keepalive stics															
• VPC Stati	Peer Link stics															

- **b.** From the LAG Interface menu, select **lag 3**.
- c. In the VPC Identifier field, enter 2.
- d. Click Add.
- 6. Create MLAG on LAG4.
 - a. Select Switching > MLAG > Advanced > VPC Interface Configuration.

System	S	witching		Routing	QoS	Security	Monitorin	g Maintenance	Help	Index
VLAN Au	to-VoIP	iSCSI	STP	Multicast	MVR A	ddress Table	Ports LAG			
Ν	ILAG		VPC I	nterface Conf	iguration					
• Basic		~		LAG Interfac	ce State	VPC Identifie	er			
 Advanced 		^		lag 4 🗸 🗸		3				
 VPC Glol Configura 	oal tion			lag 2	Disabled	1				
VPC Inte Configura	face tion			lag 3	Disabled	2				
VPC Inte	face Deta	ails								
 VPC Kee Statistics 	palive									
VPC Pee Statistics	r Link									
VPC Inte VPC Kee Statistics VPC Pee Statistics	face Deti palive r Link	ails								

- **b.** From the LAG Interface menu, select **lag 4**.
- c. In the VPC Identifier field, enter 3.
- d. Click Add.

Enable Static Routing on MLAG Interfaces

You can make MLAG interfaces members of VLAN routing interfaces. Static routing is supported on these VLAN interfaces. Routing interfaces that have MLAG interfaces as members do nor support routing protocols such as OSPF and RIP. You need to configure VRRP on these routing interfaces to provide redundancy for virtual IP addresses and virtual MAC addresses. After you have VRRP enabled on a VLAN that has an MLAG port as its member, each VRRP router functions as master in that VLAN.

Note: The virtual IP address of the VRRP routers must be different from the physical IP addresses of the peers.

The following configuration steps assume that you created an MLAG as described in *Create an MLAG* on page 77.

CLI: Enable Static Routing on MLAG

The following steps assume that you created an MLAG as described in *Create an MLAG* on page 77.

Configure Switch P

Note: For information about switch P, see *Figure 9* on page 75 and the description following the figure.

1. Add LAG1 and LAG2 to VLAN 100, LAG1 and LAG4 to VLAN 200, and LAG1 and LAG3 to VLAN 300.

For information about how to add a LAG to a VLAN, see Chapter 2, VLANs.

2. Enable IP routing globally.

```
(Switch P) # configure
(Switch P) (Config)#ip routing
```

3. Enable IP VRRP globally.

```
(Switch P) # configure
(Switch P) (config)#ip vrrp
```

4. Configure the IP address and VRRP IP address on VLAN 100.

```
(Switch P) # configure
(Switch P) (config)# interface vlan 100
(Switch P) (Interface vlan 100)#routing
(Switch P) (Interface vlan 100)ip address 192.168.100.1 255.255.255.0
(Switch P) (Interface vlan 100)ip vrrp 1
(Switch P) (Interface vlan 100)ip vrrp 1 mode
(Switch P) (Interface vlan 100)ip vrrp 1 ip 192.168.100.3
(Switch P) (Interface vlan 100)exit
```

5. Check the VRRP status on VLAN 100, and make sure that the state is master.

```
(Switch P) #show ip vrrp interface vlan 100 1
Primary IP address..... 192.168.100.3
Authentication Type..... None
Priority...... 1
Configured Priority..... 1
Advertisement Interval (secs)..... 1
Pre-empt Mode..... Enable
Administrative Mode..... Enable
Accept Mode..... Disable
State..... Master
Track Interface State DecrementPriority
_____
No interfaces are tracked for this vrid and interface combination
Track Route(pfx/len) Reachable DecrementPriority
_____
No routes are tracked for this vrid and interface combination
```

6. Configure the IP address and VRRP IP address on VLAN 200.

```
(Switch P) # configure
(Switch P) (config)# interface vlan 200
(Switch P) (Interface vlan 200)#routing
(Switch P) (Interface vlan 200)ip address 192.168.102.1 255.255.255.0
(Switch P) (Interface vlan 200)ip vrrp 1
(Switch P) (Interface vlan 200)ip vrrp 1 mode
(Switch P) (Interface vlan 200)ip vrrp 1 ip 192.168.102.3
(Switch P) (Interface vlan 200)exit
```

7. Check the VRRP status on VLAN 200, and make sure that the state is master.

```
(Switch P) #show ip vrrp interface vlan 200 1
Primary IP address..... 192.168.102.3
Authentication Type..... None
Priority...... 1
Configured Priority..... 1
Advertisement Interval (secs)..... 1
Pre-empt Mode..... Enable
Administrative Mode..... Enable
Accept Mode..... Disable
State..... Master
Track Interface State DecrementPriority
-----
No interfaces are tracked for this vrid and interface combination
Track Route(pfx/len) Reachable DecrementPriority
_____
             _____
No routes are tracked for this vrid and interface combination
```

8. Configure the IP address and VRRP IP address on VLAN 300.

```
(Switch P) # configure
(Switch P) (config)#interface vlan 300
(Switch P) (Interface vlan 300)routing
(Switch P) (Interface vlan 300)ip address 192.168.103.1 255.255.255.0
(Switch P) (Interface vlan 300)ip vrrp 1
(Switch P) (Interface vlan 300)ip vrrp 1 mode
(Switch P) (Interface vlan 300)ip vrrp 1 ip 192.168.103.3
(Switch P) (Interface vlan 300)exit
```

9. Check the VRRP status on VLAN 300, make sure that the state is master.

```
(Switch P) #show ip vrrp interface vlan 300 1
Primary IP address..... 192.168.103.3
Authentication Type..... None
Priority...... 1
Configured Priority..... 1
Advertisement Interval (secs)...... 1
Pre-empt Mode..... Enable
Administrative Mode..... Enable
Accept Mode..... Disable
State..... Master
Track Interface State DecrementPriority
_____
No interfaces are tracked for this vrid and interface combination
Track Route(pfx/len) Reachable DecrementPriority
_____ ____
No routes are tracked for this vrid and interface combination
```

Configure Switch S

Note: For information about switch S, see *Figure 9* on page 75 and the description following the figure.

1. Add LAG2 in VLAN100, LAG3 in VLAN 300, and LAG1 in both VLAN 100 and VLAN 300.

For information about how to add a LAG to a VLAN, see Chapter 2, VLANs.

2. Enable IP routing globally.

```
(Switch S) # configure
(Switch S) (Config)#ip routing
```

3. Enable IP VRRP globally.

(Switch S) # configure
(Switch S) (config)#ip vrrp

4. Configure the IP address and VRRP IP address on VLAN 100.

```
(Switch S) # configure
(Switch S) (config)# interface vlan 100
(Switch S) (Interface vlan 100)#routing
(Switch S) (Interface vlan 100)ip address 192.168.100.2 255.255.255.0
(Switch S) (Interface vlan 100)ip vrrp 1
(Switch S) (Interface vlan 100)ip vrrp 1 mode
(Switch S) (Interface vlan 100)ip vrrp 1 ip 192.168.100.3
(Switch S) (Interface vlan 100)exit
```

5. Check the VRRP status on VLAN 100, and make sure that the VRRP state is master.

```
(Switch S) #show ip vrrp interface vlan 100 1
Primary IP address..... 192.168.100.3
Authentication Type..... None
Priority..... 100
Configured Priority..... 100
Advertisement Interval (secs)..... 1
Pre-empt Mode..... Enable
Administrative Mode..... Enable
Accept Mode..... Disable
State..... Master
Track Interface State DecrementPriority
_____
No interfaces are tracked for this vrid and interface combination
Track Route(pfx/len) Reachable DecrementPriority
_____ ____
No routes are tracked for this vrid and interface combination
```

6. Configure the IP address and VRRP IP address on VLAN 200.

```
(Switch S) # configure
(Switch S) (config)# interface vlan 200
(Switch S) (Interface vlan 200)#routing
(Switch S) (Interface vlan 200)ip address 192.168.102.2 255.255.255.0
(Switch S) (Interface vlan 200)ip vrrp 1
(Switch S) (Interface vlan 200)ip vrrp 1 mode
(Switch S) (Interface vlan 200)ip vrrp 1 ip 192.168.102.3
(Switch S) (Interface vlan 200)exit
```

- 7. Check the VRRP status on VLAN 200, and make sure that the state is master.
 - **Note:** The VRRP state is master on both switch P and switch S (see *Figure 9* on page 75).

```
(Switch S) #show ip vrrp interface vlan 200 1
Primary IP address..... 192.168.102.3
Authentication Type..... None
Priority...... 1
Configured Priority..... 1
Advertisement Interval (secs)..... 1
Pre-empt Mode..... Enable
Administrative Mode..... Enable
Accept Mode..... Disable
State..... Master
Track Interface State DecrementPriority
-----
No interfaces are tracked for this vrid and interface combination
Track Route(pfx/len)
             Reachable DecrementPriority
_____
             _____
No routes are tracked for this vrid and interface combination
```

8. Configure the IP address and VRRP IP address on VLAN 300.

```
(Switch S) # configure
(Switch S) (config)#interface vlan 300
(Switch S) (Interface vlan 300)routing
(Switch S) (Interface vlan300)ip address 192.168.103.2 255.255.255.0
(Switch S) (Interface vlan 300)ip vrrp 1
(Switch S) (Interface vlan 300)ip vrrp 1 mode
(Switch S) (Interface vlan 300)ip vrrp 1 ip 192.168.103.3
(Switch S) (Interface vlan 300)exit
```

9. Check the VRRP status on VLAN 300, and make sure that the VRRP state is master.

```
(Switch S) #show ip vrrp interface vlan 300 1
Primary IP address..... 192.168.103.3
Authentication Type..... None
Priority..... 100
Configured Priority..... 100
Advertisement Interval (secs)...... 1
Pre-empt Mode..... Enable
Administrative Mode..... Enable
Accept Mode..... Disable
State..... Master
Track Interface State DecrementPriority
_____
No interfaces are tracked for this vrid and interface combination
Track Route(pfx/len)
             Reachable DecrementPriority
_____
             _____
No routes are tracked for this vrid and interface combination
```

Web Interface: Enable Routing on MLAG Interfaces

The following configuration steps assume that you created an MLAG as described in *Create an MLAG* on page 77.

Configure Switch P

Note: For information about switch P, see *Figure 9* on page 75 and the description following the figure.

1. On switch P, configure IP address 192.168.100.1 on VLAN 100, IP address 192.168.102.1 on VLAN 200, and IP address 192.168.103.1 on VLAN 300.

For information about configuring IP addresses, see *Chapter 5, Port Routing* and *Chapter 6, VLAN Routing*.

- 2. Configure VRRP on VLAN 100 on switch P.
 - a. Select Routing > VRRP > Basic > VRRP Configuration.

System	Sv	vitching		Routing		QoS	Security	r I	Monitoring		Maintenance		Help		ndex
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router	Discovery	VRRP	Multicast	IPv6	Multicast		
VRR	P		Global	Configur	ation										
• Basic		^	Adm	nin Mode	8	Dis	able 🔵 Enabl	e							
VRRP Config	guration	n:													
 Advanced 		~													
			Table (Configura	tion										
				VRID (1	to 255		Interface	Interfa	ace IP Addres	s Prir	mary IP Addre	ss	Mode		State
				1			vlan 100 👻			193	2.168.100.3		Active	~	

- **b.** Under Global Configuration, next to the Admin Mode, select the **Enable** radio button.
- **c.** For the VRRP configuration, enter the following information:
 - In the VRID (1 to 255) field, enter 1.
 - From the Interface menu, select VLAN 100.
 - In the Primary IP Address field, enter **192.168.100.3**.
 - From the Mode menu, select Active.
- d. Click Add.
- 3. Configure VRRP on VLAN 200 on switch P.
 - a. Select Routing > VRRP > Basic > VRRP Configuration.

A screen similar to the following displays.

System	S	witching		Routing		QoS	Securit	ty	Monitoring		Maintenance		Help		Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Ro	outer Discovery		Multicast	IPv6	Multicast		
VRI	٦P		Global	Configur	ation										
•Basic		^	Adn	nin Mode	1	Disa	able 🔘 Enal	ble							
VRRP Confi	guratio	n:													
 Advanced 		~													
			Table	Configura	tion										
				VRID (1	to 255)		Interface	l	nterface IP Addre	s Pri	mary IP Addre	ess	Mode		State
				2			vlan 200 ·	~		19	2.168.102.3		Active	~	
				1		2	vlan 100	1	192.168.100.2	192	2.168.100.3		Active		Initialize

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

- **c.** For the VRRP configuration, enter the following information:
 - In the VRID (1 to 255) field, enter 1.
 - From the Interface menu, select VLAN 200.
 - In the Primary IP Address field, enter **192.168.102.3**.
 - From the Mode menu, select **Active**.
- d. Click Add.
- 4. Configure VRRP on VLAN 300 on switch P.
 - a. Select Routing > VRRP > Basic > VRRP Configuration.

System	Sv	vitching		Routing		QoS	Security	Monitoring	Ma	intenance	Help	1000	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP I	Multicast	IPv6 Multicast		
VRF	RΒ		Globa	l Configura	ation								
• Basic		^	Adn	nin Mode		Ois:	able 🔘 Enabl	e					
VRRP Config	guration	¥.											
 Advanced 		~											
			Table	Configura	tion								
				VRID (1	to 255)		Interface	Interface IP Address	s Primar	y IP Addre	ss Mode		State
				3			vlan 300 👻		192.16	68.103.3	Active	~	
				1		2	vlan 100	192.168.100.2	192.16	8.100.3	Active		Initialize
				2			vlan 200	192.168.102.2	192.16	8.102.3	Active		Initialize
1													

- **b.** Under Global Configuration, next to the Admin Mode, select the **Enable** radio button.
- **c.** For the VRRP configuration, enter the following information:
 - In the VRID (1 to 255) field, enter **1**.
 - From the Interface menu, select VLAN 300.
 - In the Primary IP Address field, enter **192.168.103.3**.
 - From the Mode menu, select **Active**.
- d. Click Add.

Configure Switch S

Note: For information about switch S, see *Figure 9* on page 75 and the description following the figure.

1. On switch S, configure IP address 192.168.100.2 on VLAN 100, IP address 192.168.102.2 on VLAN 200, and IP address 192.168.103.2 on VLAN 300.

For information about configuring IP addresses, see *Chapter 5, Port Routing* and *Chapter 6, VLAN Routing*.

- 2. Configure VRRP on VLAN 100 on switch S.
 - a. Select Routing > VRRP > Basic > VRRP Configuration.

System	Sv	vitching	i i	Routing		QoS	Security	Monitoring	*	Maintenance	H	lelp	In	dex
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Mu	Ilticast	8	, i
VRF	۹۶		Global	Configur	ation									
• Basic		^	Adn	nin Mode		O Dis	able 🖲 Enab	e						
VRRP Config	guratio	n												
 Advanced 		~												
			Table	Configura	tion									
				VRID (1	to 255)		Interface	Interface IP Addre	ess Pri	mary IP Addre	ess M	lode	S	State
				1			vlan 100 🗸		19	2.168.100.3		Active	~	
			_											

- **b.** Under Global Configuration, next to the Admin Mode, select the **Enable** radio button.
- **c.** For the VRRP configuration, enter the following information:
 - In the VRID (1 to 255) field, enter 1.
 - From the Interface menu, select VLAN 100.
 - In the Primary IP Address field, enter **192.168.100.3**.
 - From the Mode menu, select **Active**.
- d. Click Add.
- 3. Configure VRRP on VLAN 200 on switch S.
 - a. Select Routing > VRRP > Basic > VRRP Configuration.

A screen similar to the following displays.

System	Sv	vitching		Routing		QoS	Security	/ Monit	oring	Ma	iintenance	Help		Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discov	ery VI	RRP I	Multicast	IPv6 Multicas	st	
VRR	P		Globa	l Configur	ation									
• Basic		^	Adn	nin Mode		Ois	able 🔘 Enab	e						
VRRP Config	juratio	n												
 Advanced 		~												
			Table	Configura	tion									
				VRID (1	to 255)	Interface	Interface IP	Address	Primar	v IP Addre	ess Mode		State
			-	1			vlan 200 🗸			192.10	58.102.3	Active	• •	
				1			vlan 100	192.168.100	.3	192.16	8.100.3	Active		Initialize

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

- **c.** For the VRRP configuration, enter the following information:
 - In the VRID (1 to 255) field, enter 1.
 - From the Interface mode, select **VLAN 200**.
 - In the Primary IP Address field, enter **192.168.102.3**.
 - From the Mode menu, select **Active**.
- d. Click Add.
- 4. Configure VRRP on VLAN 300 on switch S.
 - a. Select Routing > VRRP > Basic > VRRP Configuration.

System	S	witching		Routing		QoS	Security	Monitoring	Maintenance	e Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	/RRP Multicast	IPv6 Multicast	
VR	٩P		Global	Configur	ation						
• Basic			Adm	in Mode	2	Dis	able 🔘 Enabl	e			
VRRP Confi	guratio	n:									
 Advanced 		v									
			Table (Configura	tion						
				VRID (1	to 255))	Interface	Interface IP Address	Primary IP Add	ess Mode	State
				1			vlan 300 🐱		192.168.103.3	Active	~
				1			vlan 100	192.168.100.3	192.168.100.3	Active	Initialize
				1			vlan 200	192.168.102.3	192.168.102.3	Active	Initialize

- **b.** Under Global Configuration, next to the Admin Mode, select the **Enable** radio button.
- **c.** For the VRRP configuration, enter the following information:
 - In the VRID (1 to 255) field, enter **1**.
 - From the Interface menu, select VLAN 300.
 - In the Primary IP Address field, enter **192.168.103.3**.
 - From the Mode menu, select **Active**.
- d. Click Add.

Enable DCPDP on MLAG Interfaces

The Dual Control Plane Detection Protocol (DCPDP) s a UDP-based protocol. When a secondary device in an MLAG configuration does not receive keep-alive messages from the primary device, the secondary device takes on the role of primary device as well. Eventually, the MLAG configuration contains two primary devices, which can cause unexpected behavior. For example, if the MLAGs are static, a non-MLAG device can detect two BPDUs with two different MAC addresses on the same interface and sends STP BPDUs through one of the LAG members. (Because the LAGs are static, all of its members are operational). In the worst-case scenario, STP can go through a continuous reconvergence. The DCPDP can

resolve a configuration with two primary devices by identifying the presence of another peer and taking appropriate action.

You must configure the DCPDP on an IP interface that none of the MLAG interfaces share. After you have enabled DCPDP, it sends a control plane detection message to the peer once every second. The message is unidirectional and contains the senders MAC address. When a switch receives a control plane detection message, it sets the *peer is UP* variable to TRUE to indicate that a peer is detected.

The DCPDP configuration includes the following components:

- **Peer IP address**. The IP address of the peer switch, which you must configure before you enable DCPDP.
- **Source IP address**. The IP address from which the DCPDP packets are sent. This configuration is also mandatory. On the receiving side, DCPDP checks if the source IP address of the packet matches the configured peer IP address. Packets with an IP address that does not match the configured peer IP address are discarded.
- **UDP Port**. The port number to which messages are sent. The default port number is 50000. This configuration is optional.

CLI: Configure the DCPDP on the MLAG Interfaces

1. Configure the destination and source IP addresses of the peer on switch P.

For this configuration, switch P has an IP address of 192.168.105.1 and switch S has an IP address of 192.168.104.1. Both switches can reach each other on the network.

Note: For information about switch P and switch S, see *Figure 9* on page 75 and the description following the figure.

```
(Switch P) (Config)#vpc domain 1
(Switch P) (Config-VPC 1)#peer-keepalive destination 192.168.104.1 source
192.168.105.1
(Switch P) (Config-VPC 1)#peer detection enable
```

2. Check the status of the DCPDP peer.

3. Configure the destination and source IP addresses of the peer on switch S.

```
(Switch S) (Config)#vpc domain 1
(Switch S) (Config-VPC 1)#peer-keepalive destination 192.168.105.1 source
192.168.104.1
```

4. Check the status of the DCPDP peer.

```
(M7100-24X) #show vpc peer-keepalive
Peer IP address...... 192.168.105.1
Source IP address...... 192.168.104.1
UDP port..... 50000
Peer detection..... Enabled
Peer detection operational status..... Up
Peer is detected..... TRUE
```

Web Interface: Configure the DCPDP on MLAG Interfaces

1. Configure the DCPDP on switch P.

For information about switch P, see *Figure 9* on page 75 and the description following the figure.

a. Select Routing > VRRP > Basic > VRRP Configuration.

Syst	em	S	vitching		Routing	QoS	Security	Δ	lonitoring	ñ (Maintenance	Help	Index
VLAN	Auto-	VolP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG				
	MLA	١G		Port	Channel		lag 1 x						
 Basic 			^	Peer	Link Status		Down						
• VPC Confi	Global guration	1		Peer	Keepalive P	riority	0						
• Advanc	ed		~	Peer	Link STP M	ode	Enable						
				Peer D	etection								
				Peer	Detection M	lode	Disable () Enable	e				
				Peer	Detection S	tatus	Disable						
				Peer	IP Address		192.168.10	4.1	(X.X.)	(. <i>X</i>)			
				Sour	ce IP Addres	s	192.168.10	5.1	(X.X.)	K.X)			
				UDP	Port		50000		(1 to 6	35535)			

- **b.** Under Peer Detection, next to Peer Detection Mode, select the **Enable** radio button.
- c. Enter the following information in the Peer Detection section:
 - In the Peer IP Address field, enter **192.168.104.1**.
 - In the Source IP Address field, select **192.168.105.1**.
 - In the UDP Port field, enter **50000**.

- d. Click Apply.
- 2. Configure DCPDP on switch S.

For information about switch S, see *Figure 9* on page 75 and the description following the figure.

a. Select Switching > MLAG > Basic > VPC Global Configuration.

Syst	em	Swi	tching		Routing	QoS	Security	N	Ionitoring	M	laintenance	Help	Index
VLAN	Auto-Vo	olP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAG			·
	MLAG	3		Port	Channel		-						
• Basic			^	Peer	Link Status		lag 1 ~						
• VPC	Global			Peer	Keepalive P	riority	0						
Confi	guration			Peer	Link STP M	nde	Enable						
 Advance 	ed		~	1 001	Lanc off the	540	Lindbro						
				Peer D	etection								
				Peer	Detection M	ode	Disable () Enable	3				
				Peer	Detection St	tatus	Disable						
				Peer	IP Address		192.168.105	5.1	(X.X.X	(.X)			
				Sour	ce IP Addres	S	192.168.104	1.1	(X.X.X)	(.X)			
				UDP	Port		50000		(1 to 6	5535)			

- **b.** Under Peer Detection, next to Peer Detection Mode, select the **Enable** radio button.
- c. Enter the following information in the Peer Detection section:
 - In the Peer IP Address field, enter **192.168.105.1**.
 - In the Source IP Address field, select **192.168.104.1**.
 - In the UDP Port field, enter **50000**.
- 3. Click Apply.

Troubleshoot the MLAG Configuration

The Creation of an MLAG Fails

If an MLAG is not created correctly, either the physical port link is not up or the configuration is inconsistent between two peers. First, check the peer link. Then, check the status of the MLAG interface.

Step 1: Check the Peer Link

- 1. Check if the MLAG is enabled globally.
- 2. Check if keep-alives are enabled in the VPC domain.
- 3. Check if the peer link is a LAG.
- 4. Check the status of the ports of the peer link.
- 5. If the ports links are up, check the status of the LAG.

If the LAG is up, skip the following step.

- 6. If the LAG is down, check if the following parameters are identical on the peer link:
 - Port-channel mode
 - Link speed
 - Duplex mode
 - MTU
 - Bandwidth
 - VLAN configuration
 - LACP parameters:
 - Actor parameters
 - Admin key
 - Collector max-delay
 - Partner parameters

- 7. If the LAG is up, check if the peer link is enabled on the LAG by entering the **show vpc role** command.
- 8. Check if STP is disabled on peer link.

Step 2: Check the MLAG Interface Status

- 1. Check if the MLAG has member ports.
- 2. Check the status of the members of the MLAG.
- 3. If the ports links are up, check the status of the LAG.

If the LAG is up, skip the following step.

- 4. If the LAG is down, check if the following parameters are identical on the peer link:
 - Port-channel mode
 - Link speed
 - Duplex mode
 - MTU
 - Bandwidth
 - VLAN configuration
 - LACP parameters
 - Actor parameters
 - Admin key
 - Collector max-delay
 - Partner parameters
- 5. If the LAG is up, check if the MLAG is configured on the LAG.
- 6. Check if STP is enabled on the MLAG. The following STP configuration parameters must be identical on the primary and secondary devices:
 - Bpdufilter
 - Bpduflood
 - Auto-edge
 - Tcnguard
 - Cost
 - Edgeport
 - STP version
 - STP MST VLAN configuration
 - STP MST instance configuration (MST instance ID/port priority/port cost/mode)
 - Root guard
 - Loop guard

Traffic Through an MLAG Is Not Forwarded Normally

If the traffic is not forwarded normally, check if the following settings are identical on the primary and slave devices.

- FDB entry aging timers
- Static MAC entries.
- ACL configuration

A Ping to a VRRP Virtual IP Address Fails

If you ping the VRRP virtual IP address and do not see the response, use the CLI or web management interface to check if the accept mode is enabled. By default, the accept mode is disabled. It should be enabled before you ping the VRRP virtual IP address.

CLI: Check the Accept Mode

1. Check the accept mode.

(Netgear Switch) #show ip vrrp interface vlan 10	00 1
Primary IP address	192.168.100.3
VMAC Address	00:00:5e:00:01:01
Authentication Type	None
Priority	1
Configured Priority	1
Advertisement Interval (secs)	1
Pre-empt Mode	Enable
Administrative Mode	Enable
Accept Mode	Disable
State	Initialized

2. Enable the accept mode.

(Netgear Switch) (Interface vlan 100)#ip vrrp 1 accept-mode

Web Interface: Check the Accept Mode

1. Select Routing > VRRP > Advanced > VRRP Configuration.

A screen similar to the following displays.

Resting Table IP PAGe VLN ARP RIP OSPF OSPF Restar Discovery VRIP Multicast PAGe Adds Cancet Adds VRIP Configuration Configuration * VRIP Configuration Configuration * VRIP Restar Configuration * VRIP Configuration * VRIP Configuration * VRIP Restar Configuration * VRIP Configuration * VRIP Configuration * VRIP Configuration * VRIP Configuration <t< th=""><th>System Switching</th><th></th><th>Routing</th><th>DoS Se</th><th>cunity</th><th>Monitoring</th><th>Maintenance</th><th>Help</th><th>Index</th><th></th><th></th><th></th><th>1</th></t<>	System Switching		Routing	DoS Se	cunity	Monitoring	Maintenance	Help	Index				1
VRRP Global Configuration Configurat	Routing Table IP IPv6	VLAN	ARP RIP	OSPF OSPI	Fv3 Router I	Discovery Vil	E Multicast I	Pv6 Multicast					
VR8P Global Configuration Configurat												Add Delete	Cancel Apply
* Bisic • Admin Mode • Disable & Enable * Admin Mode • Disable & Enable * Admin Mode • Disable & Enable * VR0P Secondariano • VR0P Secondariano * VR0P Secondariano • VR0P (110 :255) • VR0P Secondariano • VR0P (110 :255) • VR0P Secondariano • • • • • • • • • • • • • • • • • • •	VRRP	Globa	I Configuration										c
*Advanced * *VR80 ² Configuration *VR80 ² Secondary P, Address Configuration *VR80 ² Secondary P, Address Configuration *VR80 ² Table Configuration *VR80 ²	•Basic ~	Adr	nin Mode	🕒 Disable 🛞	Enable								
• VR8P Configuration • VR8P Secondary P Address Configuration Table Configuration • VR8P Statistics Table Configuration • C	*Advanced ^												
*VRRP Secondary IP Address Configuration Table Configuration Pre-secondary IP (10 256) Operational (10 256) Address Configuration Interface (P) Address Owner VMAC Address Primary IP Address •VRRP Statistics Image (P) (10 256) Image (P) (10 256) Image (P) (10 256) Image (P) (10 256) Operational (10 256) Address (P) (10 256) Owner VMAC Address (P) (10 256) Primary IP Address Primary I	VRRP Configuration												
• VRRP Statistics Image: Configuration VRRP Statistics VRR	VRRP Secondary IP Address Configuration	Table	Configuration										C
•VRRP Statistics v v v	VRRP Tracking Configuration		VRID (1 to 255)	Interlace	Pre-empt Mode	Accept Mode	Configured Priority (110-254)	Operational Phonty	Advertisement Interval (1 to 255)	Interface IP Address	Owner	VMAC Address	Primary IP Address
1 stan 100 Enable Enable 100 100 1 192 (168 100 2) FALSE 00.00 5E:00:01:01 192 (168 100 2) 2 stan 200 Enable 100 100 1 192 (168 100 2) FALSE 00.00 5E:00:01:01 192 (168 100 2) 3 stan 200 Enable Enable 100 100 1 192 (168 100 2) 192 (168 100 3) FALSE 00.00 5E:00:01:01 192 (168 100 3)	VRRP Statistics												-
2 vian 200 Enable Enable 100 100 1 192 168 102.2 FALSE 00.00 56:00.01.02 192 168 102.3 3 vian 300 Enable Enable 100 100 1 192 168 103.2 FALSE 00.00 56:00.01.02 192 168 103.3			1	stan 100	Enable	Enable	100	100	1	192 168 100 2	FALSE	00:00 5E 00:01:01	192 168 100 3
3 vlan 300 Enable Enable 100 100 1 192.168.103.2 FALSE 00:00:5E:00:01:03 192.168.103.3			2	vian 200	Enable	Enable	100	100	1	192.168.102.2	FALSE	00:00:5E:00:01:02	192 168 102.3
			3	vlan 300	Enable	Enable	100	100	1	192.168.103.2	FALSE	00:00:5E:00:01:03	192.165.103.3

- 2. Under Global Configuration, next to Accept Mode, select the **Enable** radio button.
- 3. Click Apply.

The VRRP Is Not in the Master State on the Primary or Secondary Device

If the state of VRRP is Initialize (for example, the VRRP on VLAN 300), check the following:

- 1. Check if the peer link is up. If it is not, get up the peer link.
- 2. Check if the MLAG is member of VLAN 300. If it is not, add the MLAG to the VLAN.

(M7100-24X)	#show ip	vrrp interface brie	ef	
Interface	VRID	IP Address	Mode	State
vlan 100	1	192.168.100.3	Enable	Master
vlan 200	1	192.168.102.3	Enable	Master
vlan 300	1	192.168.103.3	Enable	Initialize

DCPDP Does Not Detect the Peer

If the Dual Control Plane Detection Protocol (DCPDP) does not detect the peer, check the following:

- 1. Check if DCPDP is enabled in the VPC domain.
- 2. If DCPDP is enabled, check the destination IP address, source IP address, and port number. of the DCPDP.
- 3. Ping the destination address of the DCPDP to verify that it is reachable.

Port Routing

Port routing, default routes, and static routes

5

This chapter includes the following sections:

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

Port Routing Concepts

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

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

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

The router's IP address is often statically configured in the end station, although the 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 managed switch always supports Layer 2 bridging, but Layer 3 routing must be explicitly enabled, first for the 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 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 10. Layer 3 switch configured for port routing

Enable Routing for the Switch

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

CLI: Enable Routing for the Switch

The following script shows the commands that you use to configure the managed switch to provide the port routing support shown in *Figure 10, Layer 3 switch configured for port routing* on page 104.

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.

System	S	witching		Routing		QoS	Securi	y	Monitoring]	Maintenance		Help	Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRF	P Multicast	IPv	6 Multicast	
IP			IP Con	figuration										
• Basic		^	Defa	ult Time	o Live				64					
• IP Configurat	tion		Rout	ing Mode	E9				Enab	le 🖲 Dis	sable			
 Statistics 			ICM	Echo F	eplies				Enable	le 🔘 Dis	able			
 Advanced 		¥	ICM	P Redired	ts				Enab	le 🖲 Dis	able			
			ICM	P Rate Li	mit Int	erval			1000		(0 to 2	14748	33647 ms)	
			ICM	P Rate Li	mit Bu	rst Size			100		(1 to 2	00)		
			Max	imum Ne	xt Hop	s			16					
			Max	imum Ro	utes				12288					
			Sele	ct to con	figure (Global Def	fault Gatewa	y						
			Glob	al Defaul	Gate	way			0.0.0.0					

- 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)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit
(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)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Interface 1/0/5)#routing
(Netgear Switch) (Interface 1/0/5)#routing
(Netgear Switch) (Interface 1/0/5)#routing
(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) (Interface 1/0/5)#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.

System	Sw	ritching		Routing		QoS	Securit	y Monitoring	1	Maintenance	Help	Index		
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast			
IP			IP Int	erface Co	onfigurat	ion								
Basic		*	1 2	3 VLAN	S All									
Advanced IP Configuratio	on	^		Port	Descri	iption	VLAN ID	IP Address Config Method	uration	IP Address	Subnet Mask	Ro Mo	uting de	Administrative Mode
 Statistics 				1/0/2				Manual 🗸		192.150.2.1	255.255.	255.0 E	nable 🗸	Enable v
IP Interface Configuration				1/0/1				None		0.0.0.0	0.0.0.0	Dis	able	Enable
Secondary IP				1/0/2 1/0/3 1/0/4				None None		0.0.0.0	0.0.0.0	Dis	able able able	Enable Enable Enable
				1/0/5				None		0.0.0.0	0.0.0.0	Dis	able	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.

System Swite	ching		Routing	6	QoS	Security	/ Monitoring	10	Maintenance	Help	Index			
Routing Table IP IF	Pv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast				
IP		IP Inte	rface Co	nfigurati	on									
•Basic	~	12	3 VLAN:	s All										
IP Configuration	^		Port	Descri	ption	VLAN ID	IP Address Config Method	uration	IP Address	Subnet Mask	Routing Mode		Administrativ Mode	ve
 Statistics 							~					v	~	
 IP Interface Configuration 			1/0/1				None Manual		0.0.0.0	0.0.0.0	Disable 255.0 Enable		Enable	
 Secondary IP 			1/0/2				Manual		192.150.3.1	255.255.2	255.0 Enable		Enable	
			1/0/4 1/0/5				None None		0.0.0.0	0.0.0.0	Disable 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.
- 3. Assign IP address 192.150.5.1/24 to interface 1/0/5.
 - a. Select Routing > IP > Advanced > IP Interface Configuration.

System	Sv	<i>i</i> itching	E .	Routing		QoS	Securit	y Monit	oring	Maintenance	Help	Index	X	
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discov	ery VRR	P Multicast	IPv6 Multicast			
IP			IP Inte	erface Co	onfigurat	ion								
• Basic		~	12	3 VLAN	S All									
 Advanced IP Configuration 	on	^		Port	Descri	ption	VLAN ID	IP Address C Method	Configuration	n IP Address	Subnet Mask	Ro Me	outing ode	Administrative Mode
 Statistics 				1/0/5				Manual 🗸		192.150.5.1	255.255	.255.0 E	nable 🗸	Enable v
IP Interface Configuration				1/0/1				None Manual		0.0.0.0	0.0.0.0	255.0 Er	sable Jable	Enable Enable
 Secondary IP 				1/0/3				Manual		192.150.3.1	255.255	.255.0 Er	able sable	Enable
				1/0/5				None		0.0.0.0	0.0.0.0	Di	sable	Enable
		2												

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

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

- c. Enter the following information:
 - In the IP Address field, enter 192.150.5.1.
 - In the Subnet Mask field, enter 255.255.255.0.
 - In the Routing Mode field, select Enable.
- d. Click Apply to save the settings.

Add a Default Route

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

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

CLI: Add a Default Route

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

Note: IP subnet 10.10.10.0 should be configured using either port routing (*Enable Routing for Ports on the Switch* on page 105) or VLAN routing (see Set Up VLAN Routing for the VLANs and the Switch on page 118).
Web Interface: Add a Default Route

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

A screen similar to the following displays.

System	Switchin	g	Routing		QoS	Security	Monitori	ıg	Maintenand	ce Help	Index	
Routing Table	IP IPv6	VLAN	ARP	RIP	OSPF 0	SPFv3 F	Router Discover	VRRF	Multicas	t IPv6 Multica	ast	
												Update
Routing	Table	Config	ure Route	s								
• Basic	;		Route Ty	pe	Network	Address	Subnet M	isk	Next H	op IP Address	Preference	Description
 Advanced 	6	<	Default		*				10.10.1	10.2		
Route Config	uration											
*Route Prefer	ences											
		Learne	ed Routes									
		Ne	etwork Add	Iress	Subnet Mas	Protoco	Route Type	Next Hop	Interface I	Next Hop IP Ad	dress Preference	a Metric

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

This creates the default route entry in the routing table.

Add a Static Route

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

CLI: Add a Static Route

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

(FSM7328S)	#show ip route			
Total Numbe	r of Routes			1
Network	Subnet		Next Hop	Next Hop
Address	Mask	Protocol	Intf	IP Address
10.10.10.0	255.255.255.0	Local	1/0/3	10.10.10.1

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

Web Interface: Add a Static Route

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

A screen similar to the following displays.

System	Switching		Routing		QoS	Security	/ Monitor	ng	Maintenanc	e Help	Index		
	IP IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discover	VRRF	Multicast	IPv6 Multic	ast		
													Update
Routing	Table	Config	jure Route	s									
• Basic	~		Route Ty	pe	Netwo	rk Address	Subnet N	ask	Next Ho	p IP Address	Preference	Description	
 Advanced 	^		Static		✓ 10.10	20.0	255.255.2	55.0	192.168	3.1.1			
Route Config	juration		Default		0.0.0.0)	0.0.0.0		10.10.10	0.2	1		
*Route Prefer	ences												
		Learn	ed Routes										
		N	etwork Add	dress	Subnet Ma	sk Protoc	col Route Type	Next Hop	Interface N	lext Hop IP Ad	dress Preference	e 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.

VLAN Routing

VLAN routing for a VLAN and for the switch

6

This chapter includes the following sections:

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

VLAN Routing Concepts

You can configure the 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 more segmentation or security is required.

The next section shows you how to configure the 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 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 that you use to configure the managed switch to provide the VLAN routing support shown in the diagram.

Managed Switches



Figure 11. 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.

Syste		Swite	ching		Routing	QoS	Security	Monito	ing	Maintenance	Help	Index
VLAN	Auto-Vo	IP iš	SCSI	STP	Multicast	MVR	Address Table	Ports LAC	i A	VILAG		
	VLAN		R	leset								
• Basic			^	Rese	t Configurat	ion						
• VLAN	l Configur	ation										
• Advance	ed		~									
			Ir	nternal	VLAN Cont	iguration						
				Interr	al VLAN AI	location Ba	ase 4	093				
				Interr	al VLAN AI	location Po	olicy	Ascending 💿	Desc	cending		
			V	LAN (Configuration	1						
						/I AN Nam		Make Static	7			
				-	10		e vizni i ype					
					10	VLAN 10	-	Disable Y				
					1 0	letault	Default	Disable				

- 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.

Syste	em	Sv	witching		Routing	QoS	Security	Monitorir	ng M	aintenance	Help	Index
VLAN	Auto-	VolP	iSCSI	STP	Multicast	MVR	Address Table	Ports LAG	MLAG			
	VLA	N		Reset								
• Basic			~	Res	et Configurat	ion						
• VLAN	I Config	uration	i)									
• Advanc	ed		~									
				Interna	al VLAN Con	figuration						
				Inter	mal VLAN A	location B	ase 40	93				
				Inter	mal VLAN A	location P	olicy 🔘	Ascending 💿 D	escending			
				VLAN	Configuratio	1						
					VLAN ID	/LAN Nam	e VLAN Type	Make Static				
					20	VLAN20		Disable 👻				
					1 0	default	Default	Disable				
					10 '	VLAN10	Static	Disable				

- 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.

Syst	em	Sw	ritching		Routing	QoS	Securi	у	Monitorin	ig 🛛	Maintenance	Help	Index
	Auto-V	olP	iSCSI	STP	Multicast	MVR	Address Tab	e Ports	LAG	MLAG			
	VLAN			VLAN I	Vembership								
 Basic 			~	VLAN	ID						10	*	
* Advanc	ed		^	Group	Operation						Lints		
- VLAM	V Configu	ration		VLAN	Name						VI AN	10	-
• VLAI	V Membe	rship		VLAN	Туре						Static		
- VLAM	V Status			-									
• Port Confi	PVID ouration			Ports	nit 1 1 3 4	i 7 9	11 13	5 17 1	9 21 2	3			
• MAC	Based V	/LAN		1 onto	T								
• Proto Grou	ocol Base p Configu	ed VLA tration	AN		2 4 E	8 1	0 12 14	6 18 2	0 22 2	24			

- 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.

System	S	witching	1	Routing	QoS	Security		Monitorin	g	Maintenance	Help	Index
VLAN A	ito-VolP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAG			
ν	LAN		VLAN I	Membership								
• Basic		~	VLAN	ID						20	*	
 Advanced 		^	Group	Operation						Unta	a All 🗸	
• VLAN Co	nfiguratio	n	VLAN	Name						VLAN	20	1.
VLAN M	embership)	VLAN	Туре						Static		
• VLAN St	atus			nit 1								
Port PVII Configura) tion		Ports	1 3	5 7	9 11 13 15	17 1	9 21 2	3			
•MAC Ba	ed VLAN			Т								
• Protocol Group Co	Based VL Infiguratio	AN		2 4	3 8 1	10 12 14 16	18 2	0 22 2	4			

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

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

- j. Click Apply.
- **3.** Assign PVID to VLAN10 and VLAN20.
 - a. Select Switching > VLAN > Advanced > Port PVID Configuration.

System S	witching	810	Routing	9	S Security	Monitoring	Maintenance Help	Index		
VEAN Auto-VolP	ises	STF	Multica	st MV	R Address Table	Ports LAG ML	AG			
VLAN		PVID	Configurati	on						
Basic	*	1.2	3 LAGS A	10					Go To Interface	Go
Advanced VLAN Configuration	1		Interface	PVID	VLAN Member	VLAN Tag	Acceptable Frame Types	Configured Ingress Filtering	Current Ingress Filtering	Port Priority (0 to 7)
• VLAN Membership				10	1		×	*		
+VLAN Status			1/0/1	1	1,10	10	Admit All	Disable	Disable	0
Part PVID		2	1/0/2	1	1,10	10	Admit All	Disable	Disable	0
Configuration			1/0/3	1	1,20	20	Admit All	Disable	Disable	0
MAC Based VLAN			1/0/4	1	1	None	Admit All	Disable	Disable	0

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

Basic	÷	12	3 LAGS A	JI.					Go To Interface	Go
Advanced • VLAN Configuration	2		Interface	PVID	VLAN Member	VLAN Tag	Acceptable Frame Types	Configured Ingress Filtering	Current Ingress Filtering	Port Priority (0 to 7)
*VLAN Membership			1/0/3	20	1.20	20	Admit All v	Disable v	Disable	0
VLAN Status		18	1/0/1	10	1,10	10	Admit All	Disable	Disable	0
Port PVID			1/0/2	10	1,10	10	Admit All	Disable	Disable	0
Configuration		1	1/0/3	1	1.20	20	Admit All	Disable	Disable	0
+MAC Based VLAN		B	1/0/4	1	1	None	Admit All	Disable	Disable	0

- 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.

System	Switchi	ng	Routing		QoS	Secu	rity	Monitorin	g	Maintenance	Help	Index
Routing Table	IP IPv6	VLAM	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP	Multicast	IPv6 Multicast	
VLA	N.	VLA	Routing (Configu	ation							
VLAN Routing	Wizard		VLAN ID	Port	MAC A	ddress IF	Addres	s	Subnet	Mask		
 VLAN Routing 			10 ~				192.150.3	.1	255.255	5.255.0		
								gao.				

- 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.

System	Sv	vitching		Routing		QoS	Security	Monitoring	ĥ (Maintenance	Help	Index
Routing Table	IP	IPv6		ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast	
VLA	N		VLAN	Routing C	onfigura	ation						
VLAN Routing	Wizaro	ł		VLAN ID	Port	MAC A	Address	IP Address	S	ubnet Mask	÷	
 VLAN Routing 				20 ~				192.150.4.1	2	255.255.255.0		
				10	0/4/1	20:0C:	C8:4D:95:99	192.150.3.1	2	55.255.255.0		

- 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.

RIP

Routing Information Protocol

This chapter includes the following sections:

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

Note: RIP is available on M5300 and M6100 series switches only. However, the following M5300 series switches require a license to support RIP: M5300-28G, M5300-52G, M5300-28G-POE+, and M5300-52G-POE+.

7

Routing Information Protocol Concepts

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

There are two versions of RIP (the 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 12. Network with RIP on ports 1/0/2 and 1/0/3

Enable Routing for the Switch

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

CLI: Enable Routing for the Switch

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

Web Interface: Enable Routing for the Switch

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

System	Switching	;	Routing		QoS	Securit	у	Monitoring		Maintenance	Help	Index
Routing Table	IP IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast	
IP	<u>.</u>	IP Con	figuration									
• Basic	^	Defa	ult Time	to Live				64				
• IP Configurat	tion	Rout	ting Mode	e				Enable	e 🔘 Disa	able		
 Statistics 		ICM	P Echo F	eplies				Enable	e 🔘 Disa	able		
 Advanced 	~	ICM	P Redired	cts				Enable	e 🖲 Disa	able		
		ICM	P Rate Li	mit Int	erval			1000		(0 to 21	147483647 ms)	
		ICM	P Rate Li	mit Bu	irst Size			100		(1 to 20	00)	
		Max	imum Ne	xt Hop	IS			16				
		Max	imum Ro	utes				12288				
		Sele	ct to con	figure	Global Det	fault Gatewa	У					
		Glob	al Defaul	t Gate	way			0.0.0.0				

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

Enable Routing for Ports

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

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

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

Web Interface: Enable Routing for the Ports

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

System	Swi	tching		Routing	1	QoS	Security	/ Monitoring	f	Maintenance	Help	Index		
Routing Table	膨	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast			
IP			IP Inte	erface Co	nfigurat	ion								
Basic		~	12	VLANS	All									
IP Configuration	n	^		Port	Descri	ption	VLAN ID	IP Address Config Method	uration	IP Address	Subnet Mask	Ro Mo	uting de	Administrative Mode
 Statistics 				1/0/2	1			Manual 🗸		192.150.2.1	255.255.	255.0 E	nable 🗸	Enable 👻
IP Interface Configuration				1/0/1				None		0.0.0.0	0.0.0.0	Dis	able	Enable
 Secondary IP 				1/0/2 1/0/3 1/0/4				None None None		0.0.0.0	0.0.0.0	Dis Dis Dis	able able able	Enable Enable Enable
				1/0/5				None		0.0.0.0	0.0.0.0	UIS	able	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 Configuration Method field, select Manual.
 - In the IP Address field, enter 192.150.2.1.

- In the Subnet Mask field, enter 255.255.255.0.
- In the Routing Mode field, select Enable.
- d. Click Apply to save the settings.
- 2. Assign IP address 192.150.3.1/24 to interface 1/0/3.
 - a. Select Routing > Advanced >IP Interface Configuration.

System	Sv	vitching		Routing	E .	QoS	Securit	y Monitoring	š - 1	Maintenance	Help	Index		
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicas			
IP			IP Inte	erface Co	nfigurati	on								
• Basic		~	1 2	All		- lai								
Advanced IP Configurat	ion	^		Port	Descri	ption	VLAN ID	IP Address Config Method	uration	IP Address	Subnet Mask	Ro Ma	uting de	Administrative Mode
 Statistics 				1/0/3				Manual 👻		192.150.3.1	255.25	5.255.0 E	nable 🛩	Enable Y
IP Interface Configuration				1/0/1				None		0.0.0.0	0.0.0.0	Dis	sable able	Enable
 Secondary IF 	þ			1/0/3				None		0.0.0.0	0.0.0.0	Dis	sable	Enable
				1/0/4				None		0.0.0.0	0.0.0.0	Dis	able	Enable
				1/0/5				None		0.0.0	0.0.0.0	Dis	sable	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 Configuration Method field, select Manual.

- In the IP Address field, enter 192.150.3.1.
- In the Subnet Mask field, enter 255.255.255.0.
- In the Routing Mode field, select Enable.
- d. Click Apply to save the settings.

Enable RIP on the Switch

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

CLI: Enable RIP on the Switch

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

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

Web Interface: Enable RIP on the Switch

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

System	SI	witching		Routing		QoS	Securit	у	Monitorir	ig 🛛	Maintenance	F	lelp	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Mu	Ilticast	
RI	þ		RIP Co	onfiguratio	on j									
• Basic		^	RIP	Admin M	ode	0	Disable 💿	Enable						
RIP Configur	ation													
 Advanced 		~												

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

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

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

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

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

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

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

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

A screen similar to the following displays.

System	Sv	vitching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RP OSPF	OSPFv3 Rout	er Discovery	VRRP Multicast	IPv6 Multicast	
RIF	5		RIP In	terface Co	nfiguration					
•Basic		~	12	All						
Advanced BIP Configure	ation	^		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication H	Key Authentication Key ID
Intorface Cor	Fourat	ion			~	~	Enable 👻	×		
interface our	inguita	ion :		1/0/1	RIP-2	Both	Disable	None		0
 Route Redist 	tributio	n		1/0/2	RIP-2	Both	Disable	None		0
				1/0/3	RIP-2	Both	Disable	None		0
1										

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

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

Configure VLAN Routing with RIP Support

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



Figure 13. VLAN routing RIP configuration example

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

CLI: Configure VLAN Routing with RIP Support

1. Configure VLAN routing with RIP support on the 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 nonvirtual router port.

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

4. Enable RIP for the VLAN router ports.

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

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

Web Interface: Configure VLAN Routing with RIP Support

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

A screen similar to the following displays.

System	Sw	itching		Routing		QoS	8	Secu	rity		Mor	nitorin	ıg		Mai	ntena	ance	2	F	lelp		Inc	lex		
Routing Table	IP	IPv6		ARP	RIP	OSPI	F 0	SPFv3	R	outer	Disc	overy	N	/RRP	- N	lultic	ast	IPv	6 Mu	lticas	st				
VLA	١N		VLAN	Routing	Wizard																				
 VLAN Routing 	Wizard	l	Vlar	ı ID													10								
VLAN Routing			IP A	ddress													192	2 150	3.1						
			Netv	vork Mas	sk												255	6.255	.255.1	D					
				Linit 1																					
			Port	c 1	3 5	7	0 1	1 13	15	17	10	21	23	25	27	20	21	33	35	37	30	41	13	45	47
			r on				<u>,</u>																		
				Т					2								, *								
				2	4 6	8	10 1	2 14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48

- **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.

System	S۱	vitching		Routing		QoS	S	ecurity		Mo	nitorin	ıg		Mainte	nance		ł	lelp		Inc	lex		
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSP	Fv3	Route	er Disc	overy	V	RRP	Mul	ticast	IP	v6 Mi	ultica	st				
VLA	IN		VLAN	Routing	Wizard																		
VLAN Routing	Wizar	d	Vla	n ID											20								
VLAN Routing			IP /	Address											19	2.150	.4.1						
			Net	work Mas	sk										25	5.255	.255.	0					
				Unit 1																			
			Po	ts 1	3 5	79	11	13	15 17	19	21	23	25	27 2	9 31	33	35	37	39	41	43	45	47
					<u>т</u>																_		
				2	4 6	8 10	12	14	6 18	20	22	24	26	28 3	32	34	36	38	40	42	44	46	48

- **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.

System	S۱	vitching		Routing		QoS	Securit	у	Monitoring		Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP		OSPF	OSPFv3	Rout	er Discovery	VRRP	Multicast	IPv6 Multicast	
RIF	,		RIP Co	onfiguratio	n								
• Basic		^	RIP	Admin M	ode	0	Disable 🖲	Enable					
RIP Configur	ation												
 Advanced 		~											

- 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.

System Swite	ching		Routing	QoS	Security	Monitoring	Maintenance	Help Inc	lex			ia I
Routing Table IP IP	16	VLAN	ARP	RP OSPF	OSPEv3 Rout	er Discovery	VRRP Multicast	IPv6 Multicast				
RIP		RIP Int	terface Co	nfiguration							Update Cancel	Apply
Basic	*	12	VLANS A	1						Go To k	iterface	Go
Advanced PIP Configuration	^		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Key	Authentication Key ID	Bad Packets Received	Bad Routes Received	Lipdate
Interlace Configuration					*	Enable ~						
Route Redistribution			vlan 20 vlan 10	RIP-2 RIP-2	Both Both	Disable Disable	None None		0			
		12	VLANS A							Go To In	terface	Go

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

- c. Scroll down and select the interface vlan10 and vlan 20 check boxes.
- d. Enter the following information:For RIP Mode, select the **Enable** radio button.
- e. Click Apply to save the settings.

OSPF

Open Shortest Path First

This chapter includes the following sections:

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

Note: OSPF is available on M5300 and M6100 series switches only. However, the following M5300 series switches require a license to support OSPF: M5300-28G, M5300-52G, M5300-28G-POE+, and M5300-52G-POE+.

Open Shortest Path First Concepts

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

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

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

The 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 the 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 the 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.

Managed Switches





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) (Interface 1/0/3)#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)#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.

System	S۱	witching		Routing		QoS	Securit	у	Monitorin	g	Mainte	nance	Help	Index	
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	er Discovery	VRR	P Mul	ticast	IPv6 Multic	ast	
IP	2		IP Conf	figuration											
•Basic		^	Defa	ult Time	to Live	1			64						
 IP Configurat 	ion		Rout	ing Mode					Enal	ole 🔘 D	isable				
 Statistics 			ICMF	P Echo R	eplies				Enal	ble 🔘 D	isable				
 Advanced 		~	ICMF	P Redired	ts				Enal	ole 💿 D	isable				
			ICMF	P Rate Li	mit Int	erval			1000			(0 to 21	147483647 m	s)	
			ICMF	P Rate Li	mit Bu	irst Size			100			(1 to 20	00)		
			Maxi	mum Ne	xt Hop	IS			16						
			Maxi	mum Ro	utes				12288						
			Sele	ct to con	figure	Global De	fault Gatewa	у							
			Glob	al Defaul	t Gate	way			0.0.0.0						

- **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.

System	Sv	vitching		Routing	g i	QoS	Securit	y Monitoring	0	Maintenance	Help	Index		
Routing Table	(P	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast	5 <u>.</u>		
			ID Inte	uface Cr	nfigurat	ion								
	<u>.</u>	-	ir inte	mace of	oningurai	1011								
• Basic		~	12	All										
 Advanced 		^						IP Address Configur	noite		Subnot	Re	uting	Administrativo
 IP Configurat 	ion			Port	Descr	iption	VLAN ID	Method	ation	IP Address	Mask	Mo	ode	Mode
 Statistics 				1/0/2				Manual ~		192.150.2.1	255.255.	255.0 E	inable 🗸	Enable 🛩
• IP Interface				1/0/1				None		0.0.0.0	0.0.0.0	Di	sable	Enable
Configuration	Ľ			1/0/2				None		0.0.0.0	0.0.0.0	Di	sable	Enable
 Secondary IF 	0			1/0/3				None		0.0.0.0	0.0.0.0	Di	sable	Enable
				1/0/4				None		0.0.0.0	0.0.0.0	Di	sable	Enable
				1/0/5				None		0.0.0.0	0.0.0.0	Di	sable	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 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.

System	Switch	hing		Routing		QoS	Security	Monitoring	Maintenance	Help	Index		
Routing Table	P IP	v6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery VR	RP Multicast	IPv6 Multicast			
P	2		IP Inte	erface Co	infigurat	tion							
 Basic 		~	12	All									
 Advanced 		~			1		1			202300		- Appendi	and output of the second
• IP Configurati	on			Port	Descr	iption	VLAN ID	IP Address Configuration Method	on IP Address	Subnet Mask	Ro	uting ode	Administrative Mode
 Statistics 				1/0/3				Manual 🗸	192.150.3.1	255.255	255.0 E	nable 🗸	Enable ~
• IP Interface				1/0/1				None	0.0.0.0	0.0.0.0	Di	sable	Enable
Configuration				1/0/2				Manual	192.150.2.1	255.255.2	255.0 Er	able	Enable
 Secondary IP 				1/0/3				None	0.0.0.0	0.0.0.0	Di	sable	Enable
				1/0/4				None	0.0.0.0	0.0.0.0	Di	sable	Enable
				1/0/5				None	0.0.0.0	0.0.0.0	Di	sable	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	display	/s.
--	---	--------	---------	----	-----	-----------	---------	-----

ojotom	Switching	ă.	Routing		QoS	Secur	ity	Monitori	ng	Main	tenance	He	lp	Index
Routing Table	IP IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discover	/ VRRI	D Mi	ulticast	IPv6 Mult	icast	
OSPE		Default	t Route A	dvortise	Configu	ration								
Basic		Dofa	ult Inform	ation (riginato	(ation	Dicable	- Enabla						
Advanced		Ahve		auon c	inginate		True	Falso						
OSPE Configu	ration	Met	ric.				inde @	1 0130	10 40 1	677794	4			
Common Area		Metr	ric Type			0	Extern	al Type 1 🖲	Externa	Type 2	<i>4)</i> 2			
Stub Area Con	figuration													
NSSA Area Configuration	1544	OSPE	Configura	ation										
Configuration			0	_										
• Area Range		Rout	ter ID				192.15	9.9.9						
Area Range Configuration	auration	Rout	ter ID nin Mode				192.15 Enabl	9.9.9 e ¥						
Area Range Configuration Interface Config	guration	Rout Adm ASE	ter ID hin Mode 3R Mode				192.15 Enabl	9.9.9 e ×						
Area Range Configuration Interface Config Interface Statis	guration	Rout Adm ASE RFC	ter ID hin Mode 3R Mode : 1583 Co	mpatib	lity		192.15 Enabl Disabl	9.9.9 e × e						
Area Range Configuration Interface Config Interface Statis Neighbor Table	guration stics	Rout Adm ASE RFC ABF	ter ID hin Mode 3R Mode 3 1583 Co 3 Status	mpatib	lity		192.15 Enabl Disabl Disab	9.9.9 e × e						
Area Range Configuration Interface Configuration Interface Statis Neighbor Table Link State Dat	guration stics abase	Rout Adm ASE RFC ABF Opa	ter ID hin Mode BR Mode 1583 Co Status que LSA	mpatibi Status	lity		192.15 Enabl Disabl Disab	9.9.9 e • e • e •						
Area Range Configuration Interface Config Interface Statis Neighbor Table Link State Dat Virtual Link Configuration	guration stics abase	Rout Adm ASE RFC ABF Opa Exit	ter ID nin Mode R Mode 1583 Co Status que LSA Overflow	mpatibi Status Interval	lity (secs)		192.15 Enabl Disabl Disab Enabl	9.9.9 e • e • e •	(0 t	o 2147-	483647)			
Area Range Configuration Interface Configuration Interface Configuration Interface Statis Neighbor Table Link State Dat Virtual Link Configuration Route Redistril	guration stics abase bution	Rout Adm ASE RFC ABF Opa Exit SPF	ter ID ain Mode 3R Mode 1583 Co 1583 Co Status que LSA Overflow E Delay Ti	mpatibi Status Interval me(sec	lity (secs) s)		192.15 Enabl Disabl Disabl Enabl 0	9.9.9 e ~ e ~ e ~	(0 t (0 t	o 21474	483647) 5)			

- **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.

System	Switching	ŝ,	Routing	QoS	Security	Mo	onitoring	Mainter	алсе	Help	Index	
Routing Table	IP IPv6	VLAN	ARP	RIP OSPF	OSPFv3 R	louter Dis	covery VRRI	P Multi	cast IPv6 N	Aulticast		
OSF	PF	OSPF	Interface	Configuration								
Basic	*											
Dasic	10.4	12	All									
 Advanced 	~	-			Subnet		Admin	Router	Retransmit	Hello	Dead	Iftransit Delav
OSPF Config	guration		Interface	IP Address	Mask	Area ID	Mode	Priority	Interval	Interval	Interval	Interval
Common Ar	ea		1/0/2	192.150.2.1	255.255.255.0	0.0.0.2	Enable v	128	5	10	40	1
Configuration	1		1/0/1	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Stub Area C 	onfiguration		1/0/2	192.150.2.1	255.255.255.0	0	Disable	1	5	10	40	1
• NSSA Area			1/0/3	192.150.3.1	255.255.255.0	0	Disable	1	5	10	40	1
Configuration	1		1/0/4	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
• Area Range			1/0/5	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
Configuration	1		1/0/6	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
 Interface Cor 	nfiguration		1/0/7	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
 Interface Sta 	itistics		1/0/8	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1

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

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

- In the OSPF Area ID field, enter 0.0.0.2.
- In the OSPF Admin Mode field, select Enable.
- In the **Priority** field, enter **128**.
- In the Metric Cost field, enter 32.
- c. Click Apply to save the settings.
- 6. Enable OSPF on port 1/0/3.
 - a. Select Routing > OSPF > Advanced > Interface Configuration.

A screen similar to the following displays.

and the second s	Switching		Routing	QoS	Security	Mo	onitoring	Mainter	nance	Help	Index	
Routing Table	IP IPv6	VLAN	ARP	RIP OSPF	OSPFv3 R	louter Dis	covery VRR	⊃ Multi	cast IPv6 N	Aulticast		
	_											
OSP	P	OSPE	- Interface	Configuration								
Basic	~	12	All									
 Advanced 	~	1			2424-020 XX	1	Nonvos		10 M. 10			140 0000000
• OSPE Config	uration		Interface	IP Address	Subnet	Area ID	Admin	Router	Retransmit	Hello	Dead	Iftransit Delay
CONT COMING	uration				Midok		wode	Filonty	mervai	mervar	mervar	menvai
Common Are Configuration	а		1/0/3	192.150.3.1	255.255.255.0	0.0.0.3	Disable 🛩	255	5	10	40	1
Configuration			1/0/1	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Stub Area Co 	nfiguration		1/0/2	192.150.2.1	255.255.255.0	0.0.0.2	Enable	128	5	10	40	1
 NSSA Area 			1/0/3	192.150.3.1	255.255.255.0	0	Disable	1	5	10	40	1
Configuration			1/0/4	0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Area Range			1/0/5	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
Configuration			1/0/6	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
 Interface Con 	figuration		1/0/7	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
 Interface Stat 	istics		1/0/8	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
		-										

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

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

- In the OSPF Area ID field, enter 0.0.0.3.
- In the OSPF Admin Mode field, select Enable.
- In the **Priority** field, enter **255**.
- In the Metric Cost field, enter 64.
- c. Click Apply to save the settings.

OSPF on a Border Router

The example is shown as CLI commands and as a web interface procedure. For an OSPF sample network, see *Figure 14* on page 134.

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) (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.

System	Sw	<i>i</i> tching		Routing		QoS	Secur	ity	Monitorin	g	Maintenance	Help	Index
Routing Table	P	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP	Multicast	IPv6 Multicast	
IP			IP Con	figuratior	1								
• Basic		^	Defa	ult Time	to Live				64				
 IP Configurat 	ion		Rout	ting Mod	е				Enal	ole 🔘 Dis	able		
 Statistics 			ICM	P Echo F	Replies				Enal	ole 🔘 Dis	able		
 Advanced 		~	ICM	P Redire	cts				Enal	ole 🖲 Dis	able		
			ICM	P Rate L	imit Inf	terval			1000		(0 to 21	47483647 ms)	
			ICM	P Rate L	imit Bu	urst Size			100		(1 to 20	00)	
			Max	imum Ne	ext Hop	os			16				
			Max	imum Ro	outes				12288				
			Sele	ect to con	figure	Global De	efault Gatew	ay					
			Glob	oal Defau	t Gate	way			0.0.0.0				
L													

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.

System	Sw	itching		Routing		QoS	Security	/ Monit	oring	Maintenance	Help	Index		
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discov	ery VRR	P Multicast	IPv6 Multicast			
									2					
P			IP Inte	rface Co	infigurat	ion								
•Basic		~	12	All										
 Advanced 		~						THE STREET	2 35 22A		Tax in m	1.00	1/1252	There are access
• IP Configuration	on			Port	Descri	ption	VLAN ID	IP Address (Method	Configuration	IP Address	Subnet Mask	Ro Mo	uting de	Administrative Mode
 Statistics 				1/0/2				Manual 👻		192.150.2.2	255.255	255.0 E	nable 👻	Enable ~
IP Interface				1/0/1				None		0.0.0.0	0.0.0.0	Dis	able	Enable
Configuration				1/0/2				None		0.0.0	0.0.0.0	Dis	able	Enable
 Secondary IP 				1/0/3				None		0.0.0	0.0.0.0	Dis	able	Enable
			C	1/0/4				None		0.0.0.0	0.0.0.0	Dis	able	Enable
				1/0/5				None		0.0.0.0	0.0.0.0	Dis	able	Enable
1														

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

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

- **c.** Enter the following information:
 - In the IP Address Configuration Method field, select Manual.
 - In the IP Address field, enter 192.150.2.2.
 - In the Network Mask field, enter 255.255.255.0.
 - In the Admin Mode field, select Enable.
- d. Click Apply to save the settings.
- 3. Assign IP address 192.130.3.1 to port 1/0/3:
 - a. Select Routing > IP > Advanced > IP Interface Configuration.

System	Sw	itching	ŝ.	Routing		QoS	Securit	y Monitoring		Maintenance	Help	Index		
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast			
P	1		IP Inte	erface Co	onfiguratio	on								
•Basic		×	1 2	All										
 Advanced IP Configuration 	on	^		Port	Descrip	tion	VLAN ID	IP Address Config Method	uration	IP Address	Subnet Mask	Ro Mo	uting idé	Administrative Mode
 Statistics 				1/0/3				Manual 👻		192.130.3.1	255.255	.255.0 E	nable 🗸	Enable 🗸
IP Interface Configuration				1/0/1				None Manual		0.0.0.0	0.0.0.0	255.0 En	able able	Enable Enable
 Secondary IF 	í.			1/0/3				None		0.0.0.0	0.0.0.0	Dis	able	Enable
				1/0/4				None		0.0.0	0.0.0.0	Dis	able	Enable
				1/0/5				None		0.0.0.0	0.0.0.0	Dis	able	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 Configuration Method field, select Manual.
 - In the IP Address field, enter 192.130.3.1.
 - In the Network Mask field, enter 255.255.255.0.
 - In the Admin Mode field, select Enable.
- d. Click Apply to save the settings.
- 4. Assign IP address 192.64.4.1 to port 1/0/4.
 - a. Select Routing > IP > Advanced > IP Interface Configuration.

System	Sv	vitching		Routing		QoS	Security	y Moni	toring	Maintenance	Help	Index		
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Disco	very VRR	P Multicast	IPv6 Multicast			
P	5		IP Inte	erface Co	onfigurat	ion								
• Basic		~	12	All										
 Advanced IP Configurat 	ion	^		Port	Descri	ption	VLAN ID	IP Address Method	Configuratio	n IP Address	Subnet Mask	Rou Mo	iting de	Administrative Mode
 Statistics 				1/0/4				Manual ~		192.64.4.1	255.255.2	255.0 Er	nable 🛩	Enable ~
IP Interface	5 - P			1/0/1	ſ			None		0.0.0.0	0.0.0	Dis	able	Enable
Configuration	}			1/0/2				Manual		192.150.2.2	255.255.2	255.0 Ena	able	Enable
 Secondary IF 	2			1/0/3				Manual		192.130.3.1	255.255.2	255.0 Ena	able	Enable
				1/0/4				None		0.0.0.0	0.0.0.0	Dis	able	Enable
				1/0/5				None		0.0.0.0	0.0.0	Dis	able	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 Configuration Method field, select Manual.
 - In the IP Address field, enter 192.64.4.1.
 - In the Network Mask field, enter 255.255.255.0.
 - In the Admin Mode field, select Enable.
- d. Click Apply to save the settings.
- 5. Specify the router ID, and enable OSPF for the switch.
 - a. Select Routing > OSPF > Advanced > OSPF Configuration.

System Sw	vitching		Routing		QoS	Secur	ity	Monitorin	g	Maintenance	Help	Index
Routing Table IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Route	r Discovery	VRRP	Multicast	IPv6 Multicast	i i
OSPF		Default	Route A	dvertis	e Configu	ration						
• Basic	~	Defa	ult Inform	nation (Driginate	۲	Disable	Enable				
 Advanced 	^	Alwa	ys			0	True 🖲	False				
OSPF Configuration	1	Metr	ic			0			(0 to 16)	777214)		
 Common Area Configuration 		Metr	ic Type			0	Externa	l Type 1 🖲 l	External 1	ype 2		
 Stub Area Configuration 												
 NSSA Area Configuration 		OSPF	Configur	ation								
• Area Range		Rout	er ID				192.13	0.1.1				
Configuration		Adm	in Mode				Enable	• •				
 Interface Configuration 	ion	ASB	R Mode				Disable					
 Interface Statistics 		RFC	1583 Co	mpatib	ility		Disab	e ¥				
 Neighbor Table 		ABR	Status									
 Link State Databas 	e	Opa	que LSA	Status			Enable	• •				
Virtual Link Configuration		Exit	Overflow	Interva	l (secs)		0	1	(0 to	2147 <mark>48364</mark> 7)		

- **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.

System	Swi	itching		Routing	QoS	Security	Mc	nitoring	Mainter	ance	Help	Index	
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 R	Router Dise	overy VRR	P Multi	cast IPv6 N	lulticast		
■ Advanced		^	OSPF	Interface	Configuration								
OSPF Config Common Are	guration		1 2	All	23-								
Configuration	1			Interface	IP Address	Subnet Mask	Area ID	Admin Mode	Router Priority	Retransmit Interval	Hello Interval	Dead Interval	Iftransit Delay Interval
Configuration	1			1/0/2	192.150.2.2	255.255.255.0	0.0.0.2	Enable ×	128	5	10	40	1
 NSSA Area Configuration 	1			1/0/1	0.0.0.0	0.0.0.0	0	Disable	128	5	10	40	1
Aroa Pango				1/0/2	192.150.2.2	255.255.255.0	0	Enable	1	5	10	40	1
Configuration	1			1/0/3	192.130.3.1	255.255.255.0	0	Disable	1	5	10	40	1
Interface Cor	nfiguratio	on.		1/0/4	192.64.4.1	255.255.255.0	0	Disable	1	5	10	40	1
alataria a Ota	1.1.1.1.1			1/0/5	0.0.0	0.0.0	0	Disable	1	5	10	40	1
 Intenace Sta 	usucs			1/0/6	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1

- 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.

System	Switching		Routing	QoS	Security	Mo	nitoring	Mainter	iance	Help	Index	
Routing Table	IP IPv6	VLAN	ARP	RIP OSPF	OSPFv3 R	outer Disc	overy VRR	P Multi	cast IPv6 N	lulticast		
 Advanced OSPF Config Common Area 	guration	OSPF 1 2	Interface	Configuration								
Configuration Stub Area	1		Interface	IP Address	Subnet Mask	Area ID	Admin Mode	Router Priority	Retransmit Interval	Hello Interval	Dead Interval	lftransit Delay Interval
Configuration	1		1/0/3	192.130.3.1	255.255.255.0	0.0.0.3	Enable v	255	5	10	40	1
 NSSA Area Configuration 	1		1/0/1	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
- Assa Daaraa			1/0/2	192.150.2.2	255.255.255.0	0.0.0.2	Enable	128	5	10	40	1
Configuration	1		1/0/3	192.130.3.1	255.255.255.0	0	Disable	1	5	10	40	1
 Interface Cor 	figuration		1/0/4	192.64.4.1	255.255.255.0	0	Disable	1	5	10	40	1
a lata da a Cta	tinting.		1/0/5	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
• Intenace Sta	usues		1/0/6	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1

- 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.

System	Switching		Routing	QoS	Security	Mo	nitoring	Mainter	nance	Help	Index	
Routing Table I	P IPv6	VLAN	ARP	RIP OSPF	OSPFv3 F	Router Dis	covery VRRI	⊃ Multi	cast IPv6 M	Aulticast		
• Advanced	^	OSPF	Interface	Configuration								
OSPF Configuration Common Area	ation	1 2	All									
Configuration • Stub Area			Interface	IP Address	Subnet Mask	Area ID	Admin Mode	Router Priority	Retransmit Interval	Hello Interval	Dead Interval	lftransit Delay Interval
Configuration			1/0/4	192.64.4.1	255.255.255.0	0.0.0.2	Enable v	255	5	10	40	1
 NSSA Area Configuration 			1/0/1	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
• Area Range			1/0/2	192.150.2.2	255.255.255.0	0.0.0.2	Enable	128	5	10	40	1
Configuration			1/0/3	192.130.3.1	255.255.255.0	0.0.0.3	Enable	255	5	10	40	1
 Interface Config 	uration		1/0/4	192.64.4.1	255.255.255.0	0	Disable	1	5	10	40	1
			1/0/5	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Intenace Statist 	lics		1/0/6	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1

- 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 15. 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 inter	face all	
Router ID	IP Address	Neighbor Inte	erface	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 Ho	p 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.

System	Sv	vitching		Routing		QoS	Securit	у	Monitoring		Maintenance	Help	Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast	
IP	2 0.		IP Con	figuration									
Basic		^	Defa	ult Time t	o Live				64				
 IP Configurat 	tion		Rout	ting Mode					Enable	le 🔘 Dis	able		
 Statistics 			ICM	P Echo R	eplies				Enable	e 🔘 Disa	able		
 Advanced 		~	ICM	P Redirec	ts				Enable	le 🖲 Dis	able		
			ICM	P Rate Li	mit Inte	erval			1000		(0 to 21	47483647 ms)	
			ICM	P Rate Li	mit Bu	rst Size			100		(1 to 20	10)	
			Max	imum Ne	xt Hop	s			16				
			Max	imum Ro	utes				12288				
			Sele	ect to con	figure (Global De	fault Gatewa	У					
			Glob	al Defaul	Gate	way			0.0.0.0				

- **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.

System	Switching	Ř.	Routing	j Q	loS Sec	urity Monit	oring Maintena	ance Help	Index	
Routing Table	P IPv6	VLAN	ARP	RIP (OSPF OSPFv	3 Router Discov	ery VRRP Multic	ast IPv6 Multicast		
IP		IP Int	erface Co	onfiguration						
•Basic	~	1 2	All							
Advanced	^	1					angennegen b	1.000		
• IP Configuration	1		Port	Description	on VLAM	I ID Method	IP Addr	ess Subnet Mask	Routii Mode	ng Administrative Mode
 Statistics 			2/0/11			Manual ~	192.16	8.10.1 255.255	.255.0 Enal	ble 👻 Enable 👻
• IP Interface			2/0/1			None	0.0.0.0	0.0.0.0	Disab	le Enable
Configuration			2/0/2			None	0.0.0.0	0.0.0.0	Disab	le Enable
 Secondary IP 			2/0/3			None	0.0.0.0	0.0.0.0	Disab	le Enable
			2/0/4			None	0.0.0.0	0.0.0.0	Disab	le Enable
			2/0/5			None	0.0.0.0	0.0.0.0	Disab	le Enable
			2/0/6			None	0.0.0.0	0.0.0.0	Disab	le Enable
			2/0/7			None	0.0.0.0	0.0.0.0	Disab	le Enable
			2/0/8			None	0.0.0.0	0.0.0.0	Disab	le Enable
			2/0/9			None	0.0.0.0	0.0.0.0	Disab	le Enable
			2/0/10			None	0.0.0.0	0.0.0.0	Disab	le Enable
			2/0/11			None	0.0.0.0	0.0.0.0	Disab	le 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 Configuration Method field, select Manual.
 - In the IP Address field, enter 192.168.10.1.

- In the Network Mask field, enter 255.255.255.0.
- In the Admin Mode field, select Enable.
- d. Click Apply to save the settings.
- 3. Assign IP address 192.168.20.1 to port 2/0/19:
 - a. Select Routing > IP > Advanced > IP Interface Configuration.

System	Sw	itching		Routing	QoS	Security	Monitoring	Maintenance	Help In	dex	
Routing Table		IPv6	VLAN	ARP	RIP OSPF	OSPFv3	Router Discovery VRRF	P Multicast	IPv6 Multicast		
IP			IP Inte	erface Co	nfiguration						
• Basic		~	1 2	All							
 Advanced 		~	1	1							l'anne anne anne anne anne anne anne anne
• IP Configuration	on			Port	Description	VLAN ID	Method	IP Address	Mask	Mode	Administrative Mode
 Statistics 				2/0/19			Manual 👻	192.168.20.1	255.255.255.0	Enable ~	Enable v
• IP Interface				2/0/1			None	0.0.0	0.0.0	Disable	Enable
Configuration				2/0/2			None	0.0.0.0	0.0.0	Disable	Enable
 Secondary IP 				2/0/3			None	0.0.0.0	0.0.0	Disable	Enable
				2/0/4			None	0.0.0.0	0.0.0	Disable	Enable
				2/0/5			None	0.0.0.0	0.0.0	Disable	Enable
				2/0/6			None	0.0.0.0	0.0.0	Disable	Enable
				2/0/7			None	0.0.0.0	0.0.0.0	Disable	Enable
				2/0/8			None	0.0.0	0.0.0	Disable	Enable
				2/0/9			None	0.0.0.0	0.0.0	Disable	Enable
				2/0/10			None	0.0.0.0	0.0.0	Disable	Enable
				2/0/11			Manual	192.168.10.1	255.255.255.0	Enable	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 Configuration Method field, select Manual.
 - In the IP Address field, enter 192.168.20.1.
 - In the Network Mask field, enter 255.255.255.0.
 - In the Admin Mode field, select Enable.
- d. Click Apply to save the settings.
- 4. Specify the router ID, and enable OSPF for the switch.
 - a. Select Routing > OSPF > Basic > OSPF Configuration.

System	S۱	witching		Routing		QoS	Securit	y Mo	nitoring	Ma	aintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Disc	overy VI	RRP	Multicast	IPv6 Multicast	
OSF	۶F		OSPF	Configur	ation								
•Basic		^	Adm	in Mode		Disa	able 💿 Enat	ole					
OSPF Config	guratio	n	Rout	er ID		1.1.1.1							
 Advanced 		×											

- 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.

System	Switch	ing		Routing	QoS	Security	Mor	itoring	Maintena	ance I	leip	Index	
Routing Table	IP IPv	6 V	LAN	ARP	RIP OSPF	OSPFv3 Ro	uter Disci	overy VRRI	 Multic 	ast IPv6 M	ulticast		
OSPI		C	SPF	Interface (Configuration								
• Basic			12	All									
 Advanced 		×				Subnot		Admin	Doutor	Potranemit	Hollo	Dead	Iffrancit Dolou
 OSPF Config 	juration			Interface	IP Address	Mask	Area ID	Mode	Priority	Interval	Interval	Interval	Interval
Common Are	a			2/0/11	192.168.10.1	255.255.255.0	0.0.0.0	Enable 🗸	1	5	10	40	1
Conliguration				2/0/1	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
 Stub Area Configuration 				2/0/2	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
Configuration				2/0/3	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
 NSSA Area Configuration 				2/0/4	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
Configuration				2/0/5	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Area Range Configuration 	6			2/0/6	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
Configuration	-	6		2/0/7	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Interface Cor 	inguration	12		2/0/8	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
 Interface State 	tistics			2/0/9	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
• Neighbor Tab	ole			2/0/10	0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
•Link State D	atabaso			2/0/11	192.168.10.1	255.255.255.0	0	Disable	1	5	10	40	1
Link Otate Di	atabase			2/0/12	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1

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

System	Switchin	g	Routing	QoS	Security	Mor	iitoring	Maintena	ince l	lelp	Index	
Routing Table	IP IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Ro	outer Disco	overy VRRP	Multic	ast IPv6 M	ulticast		
(
OSPF		OSP	F Interface	Configuration								
• Basic	~	12	2 All									
 Advanced 	~						hansen an	-	The second second	1	1	
OSPF Configu	ration		Interface	IP Address	Subnet Mask	Area ID	Admin Mode	Router Priority	Retransmit Interval	Hello Interval	Dead Interval	Iftransit Delay Interval
Common Area			2/0/19	192.168.20.1	255.255.255.0	0.0.0.1	Enable ~	1	5	10	40	1
Configuration	OSPF asic Vanced OSPF Configuration Configuration Stub Area Configuration VSSA Area Configuration		2/0/1	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Stub Area			2/0/2	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Configuration			2/0/3	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 NSSA Area 			2/0/4	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Conngulation			2/0/5	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Area Range Configuration 			2/0/6	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Configuration			2/0/7	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Interface Confi 	guration		2/0/8	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Interface Statis 	stics		2/0/9	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Neighbor Table	9		2/0/10	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
- Link State Dat	abaco		2/0/11	192.168.10.1	255.255.255.0	0	Enable	1	5	10	40	1
Link State Dat	00036		2/0/12	0000	0000	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 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.

System	S	witching		Routing		QoS	Securi	ty Monitoring		Maintenance	Help	Index	
Routing Table	IP	IPv6	VLAN	ARP	RIP		OSPFv3	Router Discovery	VRRF	Multicast	IPv6 Multicast		
OSPI			OSPF	Stub Are	a Conf	iguration							
• Basic		~		Area ID			SPF Runs	Area Border Router	Count	Area LSA Coun	t Area LSA CI	necksum	Import Summary LSAs
 Advanced 		~		0.0.0.1									Disable ~
OSPF Config	uratio	n	-	-			-				-	_	
Common Are Configuration	a												
 Stub Area Configuration 													

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

CLI: Configure Area 1 as a Stub Area on A2

1. Enable routing on the switch.

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

2. Set the router ID to 2.2.2.2.

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

3. Configure area 0.0.0.1 as a stub area.

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

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

```
(Netgear Switch) (Config-router)#exit
(Netgear Switch) (Config-router)#exit
(Netgear Switch) (Config)#interface 1/0/15
(Netgear Switch) (Interface 1/0/15) #routing
(Netgear Switch) (Interface 1/0/15)#ip address 192.168.20.2 255.255.255.0
(Netgear Switch) (Interface 1/0/15)#ip ospf
(Netgear Switch) (Interface 1/0/15)#ip ospf areaid 0.0.0.1
(Netgear Switch) (Interface 1/0/15)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #show ip route
Total Number of Routes..... 2
                                    Next Hop Next Hop
  Network
               Subnet
                                     Intf
  Address
                Mask
                          Protocol
                                                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.

System	S	witching		Routing		QoS	Securit		Monitoring		Maintenanc		Help	Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRF	P Multicast	IF	Pv6 Multicast	
IP	i.		IP Con	figuration										
• Basic		^	Defa	ult Time t	to Live	1. R			64					
 IP Configurat 	tion		Rout	ting Mode	8				Enable	le 🔘 Dis	able			
 Statistics 			ICM	P Echo R	eplies				Enable	le 🔘 Dis	sable			
 Advanced 		~	ICM	P Redirec	ts				Enable	le 🖲 Dis	able			
			ICM	P Rate Li	mit Int	erval			1000		(0 to	2147	483647 ms)	
			ICM	P Rate Li	mit Bu	rst Size			100		(1 to .	200)		
			Max	imum Ne	xt Hop	s			16					
			Max	imum Ro	utes				12288					
			Sele	ct to con	figure	Global De	fault Gatewa	у						
			Glob	al Defaul	t Gate	way			0.0.0.0					

- **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.

System	S	witching	jį į	Rou	ting		QoS	Securit	y M	onitoring]	Maintenan	ce	Help	Inde:	×			
Routing Table		IPv6	VLA	N AI	٩P	RIP	OSPF	OSPFv3	Router Dis	covery	VRRP	Multicas	st I	Pv6 Multicast					
P	į		IP I	nterface	Co	nfigurat	ion												
• Basic		~	1	2 All															
 Advanced 		~							ID Addres	. Confi	aurotion			Cubrat		Douting		Administrativ	
 IP Configurat 	ion		0	Por		Descri	ption	VLAN ID	Method	is conin	guration	IP Addres	s	Mask		Mode		Mode	ve
 Statistics 				1/0/	15				Manual	~		192.168.2	20.2	255.255.	255.0	Enable	~	Enable ~	
IP Interface			ĺ	1/0/	1				None			0.0.0.0		0.0.0.0		Disable		Enable	
Conliguration	2		ા	1/0/	2				None			0.0.0.0		0.0.0.0		Disable		Enable	
 Secondary IF 	2		1	1/0/	3				None			0.0.0.0		0.0.0		Disable		Enable	
			1	1/0/	4				None			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 Configuration Method field, select Manual.
 - In the IP Address field, enter 192.168.20.2.

- In the Network Mask field, enter 255.255.255.0.
- In the Admin Mode field, select Enable.
- d. Click Apply to save the settings.
- 3. Specify the router ID, and enable OSPF for the switch.
 - a. Select Routing > OSPF > Basic > OSPF Configuration.

System	S	witching		Routing		QoS	Securit	y	Monitoring		Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP		OSPFv3	Rou	iter Discovery	VRRP	Multicast	IPv6 Multicast	
OSF	PF		OSPF	Configura	ation								
• Basic		^	Adm	nin Mode		O Disa	able 💿 Enat	ble					
OSPF Config	guratio	n	Rout	ter ID		2.2.2.2							
 Advanced 		~											

- 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.

System	Switch	ning		Routing	QoS	Security	Mor	iitoring	Maintena	ance l	lelp	Index	
Routing Table	IP IP	6	VLAN	ARP	RIP OSPF	OSPFv3 Ro	uter Disco	overy VRRP	Multic	ast IPv6 M	ulticast		
OSPF			OSPF	Interface (Configuration								
•Basic		~	12	All									
 Advanced 		~		-		Qubmat		Admin	Dautar	Detropopit	Lalla	Dood	Itranait Dalau
OSPF Configu	ration			Interface	IP Address	Mask	Area ID	Mode	Priority	Interval	Interval	Interval	Interval
Common Area	i.			1/0/15	192.168.20.2	255.255.255.0	0.0.0.1	Enable ~	1	5	10	40	1
Configuration				1/0/1	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Stub Area Configuration				1/0/2	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Configuration				1/0/3	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 NSSA Area Configuration 				1/0/4	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
Configuration				1/0/5	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
 Area Range Configuration 				1/0/6	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Configuration				1/0/7	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Interface Confi 	guration			1/0/8	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
		110-1											

- 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.

System	Switch	ing		Routing	6	QoS	Securi	iy N	lanitoring		Maintenance		Help	Index				
Routing Table IP	IPv	6	VLAN	ARP	RIP	OSPE	OSPFv3	Router Di	covery	VRRP	Multicast	IPv6 N	luiticast					
OSPF		ġ	OSPF	Stub Ar	iéa Cor	figuration											Add	Delete Cancel
Basic		÷		Area 10	N:		SPF Runs	Area Borde	r Router (Count	Area LSA Co	ont Are	ILSA C	hecksum	Import Summary LSAs	Default Cost	9	Type of Service
 Advanced OSPF Configura 	tion	^		0.0.0 1											Disable ~			
* Common Area Configuration																		
Stub Area Configuration																		

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

NSSA Areas



Figure 16. 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)#inter	face 2/0/11		
(Netgear Switch)) (Interface 2/0	/11)#routing		
(Netgear Switch)) (Interface 2/0	/11)#ip addres	s 192.168.1	0.1 255.255.255.0
(Netgear Switch)) (Interface 2/0	/11)#ip ospf		
(Netgear Switch)) (Interface 2/0	/11)#exit		
(Netgear Switch)) (Config)#inter	face 2/0/19		
(Netgear Switch)) (Interface 2/0	/19)#routing		
(Netgear Switch)) (Interface 2/0	/19)#ip addres	s 192.168.2	0.1 255.255.255.0
(Netgear Switch)) (Interface 2/0	/19)#ip ospf		
(Netgear Switch)) (Interface 2/0	/19)#ip ospf a	reaid 0.0.0	.1
(Netgear Switch)) (Interface 2/0	/19)#exit		
(Netgear Switch)) (Config)#exit			
(Netgear Switch)) #show ip route			
Total Number of	Routes		2	
Network	Subnet		Next Hop	Next Hop
Address	Mask	Protocol	Intf	IP Address
14.1.1.0	255.255.255.0	OSPF Inter	2/0/11	192.168.10.2
14.1.2.0	255.255.255.0	OSPF Inter	2/0/11	192.168.10.2
192.168.10.0	255.255.255.0	Local	2/0/11	192.168.10.1
192.168.20.0	255.255.255.0	Local	2/0/19	192.168.20.1
192.168.40.0	255.255.255.0	OSPF NSSA T2	2/0/19	192.168.20.2
192.168.41.0	255.255.255.0	OSPF NSSA T2	2/0/19	192.168.20.2
192.168.42.0	255.255.255.0	OSPF NSSA T2	2/0/19	192.168.20.2

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

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

A screen similar to the following displays.

System	S	witching		Routing		QoS	Securit		Monitoring	9	Maintenance	Help	Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	er Discovery	VRRP	Multicast	IPv6 Multicast	
IP	i.		IP Con	figuration									
• Basic		^	Defa	ult Time	to Live				64				
 IP Configurat 	ion		Rout	ing Mode	e				Enab	le 🔘 Dis	able		
 Statistics 			ICMF	P Echo F	Replies				Enable	le 🔘 Dis	able		
 Advanced 		~	ICMF	P Redired	cts				Enab	le 🖲 Dis	able		
			ICMF	P Rate Li	imit Int	erval			1000		(0 to 2	147483647 ms)	
			ICMF	P Rate Li	imit Bu	rst Size			100		(1 to 20	00)	
			Maxi	imum Ne	xt Hop	IS			16				
			Maxi	imum Ro	utes				12288				
			Sele	ct to con	figure	Global De	fault Gatewa	у					
			Glob	al Defaul	t Gate	way			0.0.0.0				

- **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.

System	Sv	/itching		Routing	hi 🚺	QoS	Security	Monitoring		Maintenance	Help	Index		
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast			
IP	5 5		IP Inte	erface Co	nfigurati	on								
•Basic		~	12	All										
 Advanced 		^	1						Section .		0.1.1	0	-	A 1
•IP Configurat	ion			Port	Descri	ption	VLAN ID	Method	Iration	IP Address	Mask	Ro Mo	uting ide	Mode
 Statistics 				2/0/11				Manual 🗸		192.168.10.1	255.255	.255.0 E	nable 🗸	Enable 👻
• IP Interface				2/0/1				None		0.0.0	0.0.0.0	Dis	able	Enable
Configuration	Ľ.			2/0/2				None		0.0.0.0	0.0.0.0	Dis	able	Enable
 Secondary IF 	2			2/0/3				None		0.0.0.0	0.0.0.0	Dis	able	Enable
				2/0/4				None		0.0.0.0	0.0.0.0	Dis	able	Enable
				2/0/5				None		0.0.0.0	0.0.0.0	Dis	able	Enable
				2/0/6				None		0.0.0	0.0.0	Dis	able	Enable
				2/0/7				None		0.0.0.0	0.0.0	Dis	able	Enable
				2/0/8				None		0.0.0	0.0.0	Dis	able	Enable
				2/0/9				None		0.0.0	0.0.0	Dis	able	Enable
				2/0/10				None		0.0.0.0	0.0.0.0	Dis	able	Enable
				2/0/11				None		0.0.0.0	0.0.0.0	Dis	able	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.

System	Sw	itching		Routing		QoS	Securit	y Moni	toring	Maintenance	Help	Index		
Routing Table	P.	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Disco	very VRRI	P Multicast	IPv6 Multicast			
P			IP Inte	erface Co	nfigurati	on								
•Basic		~	1 2	All										
 Advanced 		~	1	tanina.	9			line e la com		44	0.1	-	244.52	
• IP Configuration	on			Port	Descrip	tion	VLAN ID	Method	Configuration	IP Address	Subnet Mask	Ro Mo	uting de	Administrative Mode
• Statistics				2/0/19				Manual ~		192.168.20.1	1 255.255	.255.0 E	nable 🗸	Enable v
• IP Interface				2/0/1				None		0.0.0.0	0.0.0.0	Dis	able	Enable
Configuration		-	C	2/0/2				None		0.0.0.0	0.0.0.0	Dis	able	Enable
 Secondary IP 	ŝn.			2/0/3				None		0.0.0.0	0.0.0	Dis	able	Enable
				2/0/4				None		0.0.0	0.0.0.0	Dis	able	Enable
				2/0/5				None		0.0.0.0	0.0.0	Dis	able	Enable
			C	2/0/6				None		0.0.0.0	0.0.0	Dis	able	Enable
				2/0/7				None		0.0.0.0	0.0.0.0	Dis	able	Enable
				2/0/8				None		0.0.0.0	0.0.0.0	Dis	able	Enable
				2/0/9				None		0.0.0	0.0.0	Dis	able	Enable
				2/0/10				None		0.0.0.0	0.0.0	Dis	able	Enable
				2/0/11				Manual		192.168.10.1	1 255.255	.255.0 En	able	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.

System	Sv	witching		Routing		QoS	Securit	у	Monitoring		Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	iter Discovery	VRRP	Multicast	IPv6 Multicast	
OSF	PF		OSPF	Configur	ation								
• Basic		^	Adm	in Mode		O Disa	able 💿 Enat	ole					
OSPF Config	guratio	n	Rout	er ID		2.2.2.2							
 Advanced 		~											

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.

System	Switching		Routing	QoS	Security	Mor	itoring	Maintena	nce H	lelp	Index	
Routing Table	IP IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Ro	uter Disc	overy VRRP	Multica	ast IPv6 Mi	ulticast		
OSPF		OSPF	Interface	Configuration								
• Basic	~	1 2	All									
 Advanced 	~				Outrast		A MARKA	Dester	Determents	11202	Deed	Margarette Distance
OSPF Configu	ration		Interface	IP Address	Mask	Area ID	Mode	Priority	Interval	Interval	Interval	Interval
Common Area			2/0/11	192.168.10.1	255.255.255.0	0.0.0.0	Enable ~	1	5	10	40	1
Conliguration			2/0/1	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Stub Area Configuration 			2/0/2	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Configuration			2/0/3	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 NSSA Area Configuration 			2/0/4	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Comgulation			2/0/5	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Area Range Configuration 			2/0/6	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
			2/0/7	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Interface Contig 	guration		2/0/8	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Interface Statis 	stics		2/0/9	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Neighbor Table	9		2/0/10	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
I ink State Dat	ahaco		2/0/11	192.168.10.1	255.255.255.0	0	Disable	1	5	10	40	1
Linit Otate Dat			2/0/12	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1

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.

System Swite	ching		Routing	QoS	Security	Mon	itoring	Maintena	ance H	lelp	Index	
Routing Table IP IF	۷6 ۱	VLAN	ARP	RIP OSPF	OSPFv3 Ro	uter Disco	wery VRRP	Multic	ast IPv6 M	ulticast		
OSPF		OSPF	Interface	Configuration								
•Basic	*	12	All									
Advanced	~				Output		Autoria	Deules	Detromonia	blalla	Dead	Based Delay
OSPF Configuration			Interface	IP Address	Mask	Area ID	Mode	Priority	Interval	Interval	Interval	Interval
Common Area			2/0/19	192,168,20,1	255.255.255.0	0.0.0.1	Enable ~	1	5	10	40	1
Coniguration			2/0/1	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
 Stub Area Configuration 			2/0/2	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Comgulation			2/0/3	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 NSSA Area Configuration 			2/0/4	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Comgulation			2/0/5	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Area Range Configuration			2/0/6	0.0.0.0	0.0.0	0	Disable	1	5	10	40	1
Configuration	_		2/0/7	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Interface Configuration 	1		2/0/8	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Interface Statistics 			2/0/9	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Neighbor Table 			2/0/10	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Link State Database			2/0/11	192.168.10.1	255.255.255.0	0	Enable	1	5	10	40	1
- LIIIK State Database			2/0/12	0.0.0.0	0.0.0.0	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 an NSSA area.
 - a. Select Routing > OSPF > Advanced > NSSA Area Configuration.

*Advanced * Area ID SPF Area Border Area LSA Area LSA Checkson USAs	t Summary Admin Mode Metric Value Metric Type Translator Role
*Common Area Configuration	
* Stub Area Configuration	
- NSSA Area Configuration	

- **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)#inter	face 1/0/11		
(Netgear Switch)	(Interface 1/0	/11)#routing		
(Netgear Switch)	(Interface 1/0	/11)#ip addre	ss 192.168.3	0.1 255.255.255.0
(Netgear Switch)	(Interface 1/0	/11)#ip rip		
(Netgear Switch)	(Interface 1/0	/11)#exit		
(Netgear Switch)	(Config)#inter	face 1/0/15		
(Netgear Switch)	(Interface 1/0	/15)#routing		
(Netgear Switch)	(Interface 1/0	/15)#ip addre	ss 192.168.2	0.2 255.255.255.0
(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		б	
Network	Subnet		Next Hop	Next Hop
Address	Mask	Protocol	Intf	IP Address
0.0.0.0	0.0.0.0	OSPF Inter	1/0/15	192.168.20.1
192.168.20.0	255.255.255.0	Local	1/0/15	192.168.20.2
192.168.30.0	255.255.255.0	Local	1/0/11	192.168.30.1
192.168.40.0	255.255.255.0	RIP	1/0/11	192.168.30.2
192.168.41.0	255.255.255.0	RIP	1/0/11	192.168.30.2
192.168.42.0	255.255.255.0	RIP	1/0/11	192.168.30.2

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

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

A screen similar to the following displays.

System	Sv	vitching		Routing		QoS	Securi		Monitoring]	Maintenance	Help	Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP	Multicast	IPv6 Multicast	
IP	2 10		IP Con	figuration									
Basic		^	Defa	ult Time I	o Live				64				
 IP Configurat 	tion		Rout	ing Mode					Enable	le 🔘 Disa	able		
 Statistics 			ICM	P Echo R	eplies				Enable	le 🔘 Disa	able		
 Advanced 		~	ICM	P Redired	ts				Enab	le 🖲 Disa	able		
			ICM	P Rate Li	mit Inte	rval			1000		(0 to 21	147483647 ms)	
			ICM	P Rate Li	mit Bu	st Size			100		(1 to 20	00)	
			Max	imum Ne	xt Hop:	6			16				
			Max	imum Ro	utes				12288				
			Sele	ct to con	figure (Global Def	fault Gatewa	y					
			Glob	al Defaul	Gatev	vay			0.0.0.0				

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

A screen similar to the following displays.

System	Sv	witching		Routing		QoS	Security	/ Monitoring	Ĩ	Maintenance	Help	Index		
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast			
IP	έ.		IP Inte	erface Co	onfigurat	ion								
• Basic		~	12	All										
 Advanced IP Configuration 	tion	^		Port	Descri	iption	VLAN ID	IP Address Config Method	uration	IP Address	Subnet Mask	Ron Mo	uting de	Administrative Mode
* Statistics				1/0/11				Manual 👻		192.168.30.1	255.255.2	255.0 E	nable 🗸	Enable v
IP Interface Configuration	ĩ			1/0/1				None		0.0.0.0	0.0.0.0	Dis	able	Enable
 Secondary If 	2			1/0/2				None		0.0.0.0	0.0.0.0	Dis	able	Enable
				1/0/4				None		0.0.0.0	0.0.0.0	Dis	able able	Enable
				1/0/6 1/0/7				None None		0.0.0.0	0.0.0.0	Dis	able able	Enable Enable
				1/0/8				None		0.0.0.0	0.0.0.0	Dis	able	Enable
				1/0/9				None		0.0.0.0	0.0.0.0	Dis	able	Enable
				1/0/10				None		0.0.0.0	0.0.0.0	Dis	able	Enable
			1	1/0/11				None		0000	0000	Dis	able	Enable

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

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

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

- In the Network Mask field, enter 255.255.255.0.
- In the Routing Mode field, select Enable.
- d. Click Apply to save the settings.
- 3. Assign IP address 192.168.20.2 to port 1/0/15.
 - a. Select Routing > IP > Advanced > IP Interface Configuration.

System	Sv	vitching		Routing	<u>k</u>	QoS	Security	y Moni	toring	Maintenance	Help	Index		
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Disco	very VRR	P Multicast	IPv6 Multicast			
IP			IP Inte	erface Co	nfigurat	ion								
• Basic		~	12	All										
 Advanced IP Configuration 	on	^	-	Port	Descri	ption	VLAN ID	IP Address Method	Configuration	IP Address	Subnet Mask	Rou Moo	iting Je	Administrative Mode
 Statistics 				1/0/15				Manual ~		192.168.20.	2 255.255.	255.0 Er	iable 🗸	Enable 🗸
IP Interface Configuration				1/0/1				None		0.0.0.0	0.0.0.0	Dis	able	Enable
 Secondary IP 				1/0/2				None None		0.0.0.0	0.0.0.0	Disi	able able	Enable

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

System	Sw	itching		Routing		QoS	Securit	y Mon	itoring	Mainter	nance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Disco	wery VR	RP Mult	icast l	Pv6 Multicast	
OSP	۴		OSPF	Configur	ation								
Basic		^	Adm	iin Mode		Disa	able 🖲 Enat	ole					
OSPF Config	uration		Rout	er ID		2.2.2.2							
• Advanced		~											

- 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.

System	Switch	ing		Routing	QoS	Security	Monitoring		Maintenance	Help	Index	
Routing Table	IP IPv	6 VL	AN.	ARP	RIP OSPF	OSPFv3 Rout	er Discovery	VRRP	Multicast	IPv6 Multicast		
RIP		RI	P Int	terface Co	nfiguration							
•Basic		~	12	All								
 Advanced 		^	٥	Interface	Send Version	Receive Version	RIP Mode	Auther	ntication Type	Authentication I	Key Aut	nentication Key ID
 RIP Configura 	ition	_		1/0/11	RIP-2 ×	Both ×	Enable ×	None	×		0	
 Interface Cont 	figuration		'n	1/0/1	DID 2	Both	Dicablo	Nono			0	
 Route Redistr 	ribution			1/0/2	RIP-2	Both	Disable	None			0	
				1/0/3	RIP-2	Both	Disable	None			0	
				1/0/4	RIP-2	Both	Disable	None			0	
				1/0/5	RIP-2	Both	Disable	None			0	
				1/0/6	RIP-2	Both	Disable	None			0	
				1/0/7	RIP-2	Both	Disable	None			0	
				1/0/8	RIP-2	Both	Disable	None			0	
				1/0/9	RIP-2	Both	Disable	None			0	
				1/0/10	RIP-2	Both	Disable	None			0	
				1/0/11	RIP-2	Both	Disable	None			0	

- **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.

System	Switchi	ng	Routing	Q₀S	Security	Mor	nitoring	Maintena	ance H	lelp	Index	
Routing Table	IP IPv6	i VLA	N ARP	RIP OSPF	OSPFv3 R	outer Disc	overy VRRP	Multic	ast IPv6 M	ulticast		
OSPF		OSF	F Interface	Configuration								
• Basic	*	1	2 All									
 Advanced 	^				Subnot	1	Admin	Doutor	Potranemit	Hollo	Doad	Itrancit Dolov
 OSPF Configu 	iration		Interface	IP Address	Mask	Area ID	Mode	Priority	Interval	Interval	Interval	Interval
Common Area	E.		1/0/15	192.168.20.2	255.255.255.0	0.0.0.1	Disable 👻	1	5	10	40	1
Configuration			1/0/1	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Stub Area Configuration 			1/0/2	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Configuration		0	1/0/3	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 NSSA Area Configuration 			1/0/4	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Configuration		0	1/0/5	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Area Range Configuration 			1/0/6	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
Configuration		0	1/0/7	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1
 Interface Confi 	guration		1/0/8	0.0.0.0	0.0.0.0	0	Disable	1	5	10	40	1

- **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.

System Switch	hing		Routing	QoS	Security	Monitoring	Maint	enance Hel	p Index				
Routing Table IP IP	6	VLAN	ARP RIP	OSPI OS	PFV3 Router1	Discovery	VRRP Mu	lticast IPv6 Multi	cast		Add	Delete Cancel	Apply
OSPF		OSPF	NSSA Area C	onfiguration									÷
• Basic	ž				1					Default Inform	stion Originate		
 Advanced OSPF Configuration 	^		Area 1D	SPF Rum	Area Border Router Count	Area LSA Count	Area LSA Checksum	Import Summary LSAs	Admin Mode	Metric Value	Metric Type	Translator Role	Translat Interval
*Common Area Configuration			0.0.0.1					Disable ~	*				•
Stub Area Configuration													
NSSA Area Configuration													

- 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.

System	Sw	itching		Routing	QoS	Security	/ Monito	ring	Maintena	ince Help	Index	
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3	Router Discove	ry VRRP	Multic	ast IPv6 Multicas	t	
Advanced		^	OSPF	Route Red	istribution							
Common Area	anation			Source	Redistribute	Metric	Λ	Netric Type		Tag	Subnets	Distribute List
Configuration	a			RIP	Enable ~				~		~	
 Stub Area Configuration 				Connected	d Disable							
NSSA Area				RIP	Disable							
Configuration Area Range				OSPF	Disable							
Configuration				BGP	Disable							
 Interface Conf 	figurati	on										
Interface Stat	istics											
 Neignbor Tabi Link State Da 	le stabacc	<i></i>										
 Virtual Link Configuration 		**										
Route Redistr	ribution	10										

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

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

c. Enter the following information:

In the Redistribute field, select Enable.

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

VLAN Routing OSPF

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

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

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

The 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 11, Layer 3 switch configured for port routing* on page 114.

1. Configure the 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)#ip ospf
```

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.

System Switching	Routing QoS Security Monitoring Maintenance Help Index
Routing Table IP IPv6	VLAN ARP RIP OSPF OSPFn3 RouterDiscovery VRRP Multicast IPv6 Multicast
VLAN	VLAN Routing Wizard
VLAN Routing Wizard	Vian ID
VLAN Routing	IP Address 192.150.3.1
	Network Mask 255.255.255.0
	Unit 1
	Ports 1 2 5 7 9 11 12 15 17 19 21 22 25 27 29 31 23 25 27 30 41 43 45 47 2 4 6 8 10 12 14 16 18 20 22 24 26 20 30 32 34 35 38 40 42 44 45 44

- **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.

System Switch	ng Routing QoS Security Monitoring Maintenance Help Index
Routing Table IP IPv6	VLAN ARP RIP OSPF OSPFv3 Router Discovery VRRP Multicast IPv6 Multicast
VLAN	VLAN Routing Wizard
VLAN Routing Wizard	Vian ID 20
VLAN Routing	IP Address 192 150 4.1 Network Mask 255 255 0
	Ports 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 2 4 6 8 19 12 14 16 18 20 22 24 25 28 30 32 34 36 38 49 42 44 46 43

- **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.

System	Sw	vitching		Routing		QoS	Securit	ý	Monitorin	g	Maintenance	He	lp	Index	- 10
Routing Table	IP	IPv6	VLAN	ARP	RIP		OSPFv3	Rou	iter Discovery	VRRP	Multicast	IPv6 Mult	icast		
															-
OSF	PF		OSPF	Configura	ation										
• Basic		^	Adm	nin Mode		O Disa	able 💿 Enat	ole							
OSPF Config	guration	1	Rout	ter ID		192.15	50.9.9								
 Advanced 		~													

- 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.

System Switching Routing Table IP IPv6	VLAN	ARP	QoS RIP OSPE	OSPFv3 R	outer Disc	onitoring covery VRF	Mainte 89 Mult	icast IPv6.1	Help Noticest	Index					Cancel A
OSPF	OSPI	Interface (Configuration												
•Basic ~	1.2	VLANS A	E										Go	To Interface	
Advanced OSPF Configuration		Interface	IP Address	Subnet Mask	Area ID	Admin Mode	Router Priority	Retransmit Interval	Hello Interval	Dead Interval	Iffransit Deby Interval	LSA Ack Interval	MTU Igoore	Passive Mode	Network Type
Common Area		Man 10	192 150 3 1	255 255 255 0	0.0.0.2	Enable Y	128	5	10	40	1	1	Disable v	Disable ~	Broadcast
Computation	2	vian 10	192.150.3.1	255.255.255.0	0	Disable	1	5	10	40	1	1	Disable	Disable	Broadcast
Stub Area Configuration	8	vian 20	192.150.4.1	255.255.255.0	0	Disable	1	5	10	40	1	1	Disable	Disable	Broadcast
NSSA Area Configuration	1.2	VLANS A	1										Go	To Interface	G
Area Range Configuration															
Interface Configuration															

- **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.

Routing Table IP IF	36	VLAN	ARP	RIP 0.995	OSPEV3 R	outer Disc	covery VRR	P Multi	cast IPv6 h	luticast						Cancel	Apply
OSPF		OSPF	Interface (Configuration													
Basic		12	VLANS A	1										Go	To Interface		Go
•OSPF Configuration	1		Interface	IP Address	Suboet Mask	Area ID	Admin Mode	Router Priority	Retransmit Interval	Hello Interval	Dead Interval	Ittransit Delay Interval	LSA Ack Interval	MTU Ignore	Passive Mode	Network Type	
Common Area Configuration			utan 20	192 150 4 1	255:255:255 0	0.0.0.3	Enable v	255	5	10	40	1	1	Disable v	Disable 👻	Broadcast	v
Stub Area Configuration			vlan 10 vlan 20	192.150.3.1 192.150.4.1	255.255.255.0 255.255.255.0	0.0.0.2 0	Enable Disable	128 1	5 5	10 10	40 40	1	1	Disable Disable	Disable Disable	Broadcast Broadcast	
NSSA Area Configuration		12	VLANS A	1										Ge 1	o Interface		Go
Area Range Configuration																	
Interface Configuration	•																

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

OSPFv3

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





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
                                                       DeadTime
                                           State
_____ ____
                    _____
                             _____
                                        _____
                                                       _____
2.2.2.2
                      13
                               1/0/1
                                       Full/BACKUP-DR
                                                         34
            1
```

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
_____
        _____ ___
                         _____
                                               ____
                                    _____
                                   Full/ DR
1.1.1.1
           1
                  1
                         1/0/13
                                                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.

System	S۱	vitching		Routing		QoS	Securit	у	Monitori	ng	Maintenance	Help	Index				
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery VRRP Multic				ast IPv6 Multicast					
IPv	6		IPv6 G	lobal Cor	figurati	on											
• Basic		^	IPv6	Unicast	Routing			Disa	ble 🖲 Ena	ble							
Global Config	guratio	n	Hop	Limit					64 (1 to 255)								
•Route Table			ICM	Pv6 Rate	Limit E	rror Interv	al	1000		(0 to	2147483647	msecs)					
 Advanced 		~	ICM	Pv6 Rate	Limit E	urst Size		100 ((1 to 200)						

- **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.

System	Sı	witching		Routing		QoS	Securit	y	Monitoring	9	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP	Multicast	IPv6 Multicast	
OSPI	Fv3		OSPF	v3 Config	uration								
Basic		^	Adm	nin Mode		O Disa	able 💿 Enal	ble					
OSPFv3 Cor	ifigurat	tion	Rout	ter ID		1.1.1.1							
Advanced		~											

- **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.

System Switching	,	Routing QoS	Security	Monitoring	Maintenance	Help	Index	1			
Routing Table IP IPAG	VLAN	ARP RIP OSPF	OSPEV3 Router D	iscovery VRRP	Multicast	IPi6 Mulbcast					
											Add
PV6	IPv61	sterface Selection									
'Basic ~	Inte	dace 1/0/1	3								
Advanced •											
Global Configuration											
*Interface Configuration	IP\61	sterface Configuration									
Prefix Configuration		Names of	Topo so Marina	T SOMEON	Mobil Edu	Deale	in the second second	Charles I.		Automation	Countried
Statistics	1	Ipv6 Prefor	Prefix Length	EUI64	Time	Life	Time	Flag		Flag	State
Neighbour Table		2001:1	64						÷		
Static Route Configuration		fe80: 220c c8# fe4d 959	64	Disable						1	[ACTIVE]
Route Table											

- b. Under IPv6 Prefix Selection, in the Interface list, select 1/0/1.
- c. Under IPv6 Interface Configuration, enter the following information:
 - In the IPv6 Prefix field, enter 2001::1.
 - In the Length field, enter 64.
 - In the EUI64 field, select Disable.
 - In the **Onlink Flag** field, select **Disable**.
 - In the Autonomous Flag field, select Disable.

- **d.** Click **Add** to save the settings.
- 5. Enable OSPFv3 on port 1/0/1.
 - a. Select Routing > OSPFv3 > Advanced > Interface Configuration.

System	5	Switching	3	Routing	Qo:	G Secu	rity	Monitoring	М	aintenance	Help	1	Index		
Routing Table	IP	IPv6	VLAN	ARP	RIP 05	PF OSPFv3	Router	Discovery	VRRP	Multicast	IPv6 Multic	ast			
OSPF	- v3		OSPF	v3 Interfac	e Configura	ition									
•Basic		~	1 2	VLANS A	II										
 Advanced OSPFv3 Cor 	nfigura	ation		Interface	IPv6 Address	Area ID		Admin Mode	Router Priority	Retransmit Interval	Hello Interval	Dead Interval	LSA Ack Interval	lftransit Delay Interval	MTU Ignore
Common Are	ea			1/0/1		0.0.00		Enable ~	1	5	10	40	1	1	Disable 🛩
Configuration	n			1/0/1		0.0.0.0		Disable	1	5	10	40	1	1	Disable
 Stub Area Configuration 				1/0/2		0.0.0		Disable	1	5	10	40	1	1	Disable
Configuration				1/0/3		0.0.0.0		Disable	1	5	10	40	1	1	Disable
 NSSA Area Configuration 				1/0/4		0.0.0.0		Disable	1	5	10	40	1	1	Disable
Comgutation				1/0/5		0.0.0.0		Disable	1	5	10	40	1	1	Disable
 Area Range Configuration 	1			1/0/6		0.0.0		Disable	1	5	10	40	1	1	Disable
loturfunc Out		ates -		1/0/7		0.0.0		Disable	1	5	10	40	1	1	Disable
• Intenace Col	niigun	atton		1/0/8		0.0.0.0		Disable	1	5	10	40	1	1	Disable

- **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.

Switching	Routir	ıg	QoS	Securi	ty	Monitorir	ıg	Maintenance	Help		ndex
IP IPv6	VLAN ARF	P RIP	OSPF		Router	Discovery	VRRP	Multicast	IPv6 Multic	ast	
figuration	OSPFv3 Neig	hbor Tabl	e								
a								S	earch Interfac	e	Go
L.	Interface	Interface Identifier	Router ID	Area ID	Options	Router Priority	State		Dead Time(secs)	Events	Retransmission Queue length
E .	1/0/1	105	2.2.2.2	0.0.0.0	19	1	Loading/I	BACKUP-DR	39	4	0
figuration											
tistics											
ole											
	Switching IP IPv6	Switching Routin IP IPv6 VLAN ARF diguration a diffuguration	Switching IP IPv6 VLAN ARP RIP figuration a figuration figurat	Switching Routing QoS IP IPv6 VLAN ARP RIP OSPF figuration OSPFv3 Neighbor Table Interface Interface Router in Interface Interface Interface Router infiguration 1/0/1 105 2.2.2.2	Switching Routing QoS Security IP IPv6 VLAN ARP RIP OSPF OSPFv3 figuration OSPFv3 Neighbor Interface Interface Router Area Interface Interface Interface Router Area ID Infiguration 1/0/1 105 2.2.2.2 0.0.00	Switching Routing QoS Security IP IPv6 VLAN ARP RIP OSPF OSPF OSPFv3 Router figuration a Interface Interface Router Area Options inguration 1/0/1 105 2.2.2.2 0.0.0.0 19	Switching Routing QoS Security Monitorin IP IPv6 VLAN ARP RIP OSPF OSPFv3 Router Discovery figuration OSPFv3 Neighbor Table Interface Interface Router Area Options Router Interface Interface Router Interface Router Interface Priority Infiguration Interface Interface Router Interface Router Priority infiguration Interface Interface Router Area Options Router infiguration Interface Interface Router Area Interface Interface infiguration Interface Interface Router Area Interface Interface istics Interface Interface Router Interface Int	Switching Routing QoS Security Monitoring IP IP-K6 VLAN ARP RIP OSPF OSPFV3 Router Discovery VRP figuration OSPFv3 Neighbor Table Interface Interface Router Interface Area Options Router State infiguration Interface Interface Router Interface Area Interface Interface <td>Switching Routing QoS Security Monitoring Maintenance IP IP-K6 VLAN ARP RIP OSPF OSPFV3 Router Discovery VRP Multicast figuration Cost Area D D Options Router State infiguration Interface Interface Router Area D Options Router State infiguration 1/0/1 105 2.2.2.2 0.0.0.0 19 1 Loading/BACKUP-DR</td> <td>Switching Routing QoS Security Monitoring Maintenance Help IP IPx6 VLAN ARP RIP OSPF OSPFv3 Router Discovery VRP Multicast IPx6 Multic figuration OSPFv3 Neighbor Table Search Interface Interface Router ID Options Router State Dead Interface Interface Router ID Options Router State Dead Infiguration Interface Interface Router Area Options Router State Dead Infiguration Infiguration Interface Router Area Options Router State Dead Infiguration In</td> <td>Switching Routing QoS Security Monitoring Maintenance Help I IP IPv6 VLAN ARP RIP OSPF OSPFv3 Router Discovery VRP Multicast IPv6 Multicast figuration OSPFv3 Neighbor Table Search Interface Interface Router ID Options Router State Dead Time(secs) Events infiguration 1/0/1 105 2.2.2.2 0.0.0.0 19 1 Loading/BACKUP-DR 39 4</td>	Switching Routing QoS Security Monitoring Maintenance IP IP-K6 VLAN ARP RIP OSPF OSPFV3 Router Discovery VRP Multicast figuration Cost Area D D Options Router State infiguration Interface Interface Router Area D Options Router State infiguration 1/0/1 105 2.2.2.2 0.0.0.0 19 1 Loading/BACKUP-DR	Switching Routing QoS Security Monitoring Maintenance Help IP IPx6 VLAN ARP RIP OSPF OSPFv3 Router Discovery VRP Multicast IPx6 Multic figuration OSPFv3 Neighbor Table Search Interface Interface Router ID Options Router State Dead Interface Interface Router ID Options Router State Dead Infiguration Interface Interface Router Area Options Router State Dead Infiguration Infiguration Interface Router Area Options Router State Dead Infiguration In	Switching Routing QoS Security Monitoring Maintenance Help I IP IPv6 VLAN ARP RIP OSPF OSPFv3 Router Discovery VRP Multicast IPv6 Multicast figuration OSPFv3 Neighbor Table Search Interface Interface Router ID Options Router State Dead Time(secs) Events infiguration 1/0/1 105 2.2.2.2 0.0.0.0 19 1 Loading/BACKUP-DR 39 4

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

BGP

Border Gateway Protocol

This chapter includes the following sections:

- Border Gateway Protocol Concepts
- Example1: Configure BGP on Switches A, B, and C in the Same AS

- Example 2: Create eBGP on Switches A and D
- Example 3: Create an iBGP Connection with a Loopback Interface
- Example 4: Configure Reflection for iBGP
- Example 5: Filter Routes with NLRI
- Example 6: Filter Routes with AS_PATH
- Example 7: Filter Routes with Route Maps
- Example 8: Exchange IPv6 Routes over an IPv4 BGP

Note: BGP is available on the M6100 series switches only.

Border Gateway Protocol Concepts

Border Gateway Protocol (BGP) is an exterior routing protocol that was developed for use in TCP/IP networks. The primary function of BGP is to allow different autonomous systems (ASs) to exchange network reachability information.

An AS is a set of routers that are under a single technical administration. This set of routers uses a different routing protocol, for example, Open Shortest Path First (OSPF), for intra-AS routing. One or more routers in the AS are configured to be border routers, exchanging information with other border routers (in different ASs) on behalf of all of the intrarouters.

Although the primary function of BGP is to exchange routing information between ASs, it can be used with an AS. Once it is used in an AS, it is called internal BGP or iBGP. In contrast, the BGP used between ASs is called external BGP or eBGP.

Note: The NETGEAR ProSafe Managed Switch does not support any version of BGP other than version 4.

Note: BGP can be configured through the CLI only.

Note:	SNMP support is limited to the standard MIB, which provides primarily
	status reporting.

Note: The only optional parameter recognized in an Open message is the Capabilities option (RFC 5492). RFC 4271 deprecates the Authentication option. If a neighbor includes the deprecated authentication parameter in its Open message, NETGEAR BGP rejects the Open message and does not form an adjacency.

Note: NETGEAR eBGP doesn't support multihop (RFC 4271 section 5.1.3).

Example1: Configure BGP on Switches A, B, and C in the Same AS

iBGP is an internal BGP connection between peers in the same AS. Because AS_PATH does not change in the same AS, iBGP cannot prevent loops as EBGP does. To protect against loops between iBGPs, iBGP does not advertise the routes learned from an iBGP peer to another iBGP peer, which is why iBGP must be fully meshed.

This example shows how to configure iBGP in the AS100 switch. Switches A, B, and C are all in the same AS100 switch and connected to each other. Each switch has various subnets configured in multiple VLANs.



Figure 18. Topology

Configure BGP on Switch A

1. Create VLANs 100, 200, and 300 and assign IP addresses.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan) #vlan 200,300
(Netgear Switch) (Vlan) #vlan routing 200
(Netgear Switch) (Vlan) #vlan routing 300
(Netgear Switch) (Vlan) #exit
(Netgear Switch) #configure
(Netgear Switch)(config) # interface 1/0/2
(Netgear Switch) (Interface 1/0/2) #vlan pvid 200
(Netgear Switch) (Interface 1/0/2) #vlan participation include 200
(Netgear Switch) (Interface 1/0/2) #interface 1/0/3
(Netgear Switch) (Interface 1/0/3) #vlan pvid 300
(Netgear Switch) (Interface 1/0/3) #vlan participation include 300
(Netgear Switch) (Interface 1/0/3) #interface vlan 200
(Netgear Switch) (Interface vlan 100) # interface vlan 200
(Netgear Switch) (Interface vlan 200) # ip address 192.168.1.1 /24
(Netgear Switch) (Interface vlan 200) # interface vlan 300
(Netgear Switch) (Interface vlan 300) # ip address 192.168.3.2 /24
```

2. Configure the local BGP AS as 100 and the BGP peer as 100.

An iBGP session is created.

```
(Netgear Switch) #configure
(Netgear Switch) (Config) #ip routing
(Netgear Switch) (Config) #router bgp 100
(Netgear Switch) (Config-router) # bgp router-id 192.168.1.1
(Netgear Switch) (Config-router) # network 192.168.1.0 mask 255.255.255.0
(Netgear Switch) (Config-router) # network 192.168.3.0 mask 255.255.255.0
(Netgear Switch) (Config-router) # neighbor 192.168.1.2 remote-as 100
(Netgear Switch) (Config-router) # neighbor 192.168.3.1 remote-as 100
(Netgear Switch) (Config-router) # neighbor 192.168.3.1 remote-as 100
```
Configure BGP on Switch B

1. Create VLANs 300 and 400 and assign IP addresses.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan) #vlan 300,400
(Netgear Switch) (Vlan) #vlan routing 300
(Netgear Switch) (Vlan) #vlan routing 400
(Netgear Switch) (Vlan) #exit
(Netgear Switch) #configure
(Netgear Switch)(config) # interface 1/0/1
(Netgear Switch) (Interface 1/0/1) #vlan pvid 400
(Netgear Switch) (Interface 1/0/1) #vlan participation include 400
(Netgear Switch) (Interface 1/0/1) #interface 1/0/2
(Netgear Switch) (Interface 1/0/2) #vlan pvid 300
(Netgear Switch) (Interface 1/0/2) #vlan participation include 300
(Netgear Switch) (Interface 1/0/2) #interface vlan 300
(Netgear Switch) (Interface vlan 300) # ip address 192.168.3.1 /24
(Netgear Switch) (Interface vlan 300) # interface vlan 400
(Netgear Switch) (Interface vlan 400) # ip address 192.168.2.2 /24
```

 Configure the local BGP AS as 100 and the BGP peer as 100. An iBGP session is created.

(Netgear	Switch)	#configure
(Netgear	Switch)	(Config) #ip routing
(Netgear	Switch)	(Config) #router bgp 100
(Netgear	Switch)	(Config-router) # bgp router-id 192.168.2.2
(Netgear	Switch)	(Config-router) # network 192.168.2.0 mask 255.255.255.0
(Netgear	Switch)	(Config-router) # network 192.168.3.0 mask 255.255.255.0
(Netgear	Switch)	(Config-router) # neighbor 192.168.2.1 remote-as 100
(Netgear	Switch)	(Config-router) # neighbor 192.168.3.2 remote-as 100
(Netgear	Switch)	(Config-router) #exit

Configure BGP on Switch C

1. Create VLANs 200 and 400 and assign IP addresses.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan) #vlan 200,400
(Netgear Switch) (Vlan) #vlan routing 200
(Netgear Switch) (Vlan) #vlan routing 300
(Netgear Switch) (Vlan) #exit
(Netgear Switch)#configure
(Netgear Switch)(config) # interface 1/0/1
(Netgear Switch) (Interface 1/0/1) #vlan pvid 200
(Netgear Switch) (Interface 1/0/1) #vlan participation include 200
(Netgear Switch) (Interface 1/0/1) #interface 1/0/2
(Netgear Switch) (Interface 1/0/2) #vlan pvid 400
(Netgear Switch) (Interface 1/0/2) #vlan participation include 400
(Netgear Switch) (Interface 1/0/2) #interface vlan 200
(Netgear Switch) (Interface vlan 200) # ip address 192.168.1.2 /24
(Netgear Switch) (Interface vlan 200) # interface vlan 400
(Netgear Switch) (Interface vlan 400) # ip address 192.168.2.1 /24
```

2. Configure the local BGP AS as 100 and the BGP peer as 100.

An iBGP session is created.

```
(Netgear Switch) #configure
(Netgear Switch) (Config) #ip routing
(Netgear Switch) (Config) #router bgp 100
(Netgear Switch) (Config-router) # bgp router-id 192.168.1.2
(Netgear Switch) (Config-router) # network 192.168.1.0 mask 255.255.255.0
(Netgear Switch) (Config-router) # network 192.168.2.0 mask 255.255.255.0
(Netgear Switch) (Config-router) # neighbor 192.168.1.1 remote-as 100
(Netgear Switch) (Config-router) # neighbor 192.168.2.2 remote-as 100
(Netgear Switch) (Config-router) # neighbor 192.168.2.2 remote-as 100
```

Check the BGP Neighbor Status

Check the BGP neighbor on Switch A to see if the BGP neighbor is established. Use the same command to check it on Switches B and C.

(Netgear Switch) #show	in han neight	ors 192 168	1 2		
Remote Address	The sale merain		192 168 1 2		
Remote AS	••••••••••		100		
Deer ID			192 168 1 2		
Deer Admin Status			172.100.1.2 97197		
Deer State			FGTARLIGHED		
Logal Interface Address	· • • • • • • • • • • • • • • • • • • •		102 168 1 1		
Logal Dort			192.100.1.1		
Domete Dert	••••••		47156		
Compaction Detroit Thtom		• • • • • • • • • • • •	1/9		
Neighber Grachilitier	al		2 sec		
Neighbor Capabilities .	•••••		MP RF		
IPv4 Unicast Support	•••••		Both		
IPv6 Unicast Support	•••••		None		
Template Name	•••••		None		
Update Source	•••••	••••	loopback 0		
Configured Hold Time		••••	None		
Configured Keep Alive 7	ime		None		
Negotiated Hold Time	•••••		90 sec		
Negotiated Keep Alive 7	ime		30 sec		
MD5 Password	••••••		None		
Last Error (Sent)	••••••		Hold Timer E	Expired	
Last SubError	•••••		None		
Time Since Last Error .	••••••••••		0 days 05	hrs 35 mins	s 48 secs
Established Transitions	3		3		
Established Time			0 days 00	hrs 00 mins	s 19 secs
Time Since Last Update			0 days 00	hrs 00 mins	s 18 secs
IPv4 Outbound Update Gr	oup		0		
IPv6 Outbound Update Gr			None		
Open Up	odate Keepa	live Not	ification	Refresh	Total
Msgs Sent 43	7	2600	1	0	2651
Msgs Rcvd 3	3	2259	1	0	2266
Received UPDATE Queue S	Size: 0 bytes.	High: 4 Li	imit: 392192	Drops: 0	
IPv4 Prefix Statistics:					
	Inbound	Outbour	nd		
Prefixes Advertised	0	207	7		
Prefixes Withdrawn	0	101	1		
Prefixes Current	0	-0-	2		
Prefixes Accepted	0	N / 2	4		
Prefixes Rejected	0	N / 2	-		
Max NLRI per Update	0	101	-)		
Min NIPI per Undate	0	TOC	1		
MINI MURI PEL OPUALE	U	-	L		

Or use show ip bgp summary to display a summary of all neighbors.

```
(Netgear Switch) #show ip bgp summary
IPv4 Routing ..... Enable
BGP Admin Mode ..... Enable
BGP Router ID ..... 192.168.1.1
Local AS Number ..... 100
Number of Network Entries ..... 2
Number of AS Paths ..... 0
Neighbor
          ASN MsgRcvd MsgSent
                               State
                                       Up/Down Time Pfx Rcvd
_____
                                         _____
         _____
                      -----
172.126.1.2
                       875
                                                     0
           200
                 368
                               ESTABLISHED 0:21:11:24
192.168.1.2
                                                     0
           100
                 2262
                       2648
                               ESTABLISHED 0:03:22:45
192.168.3.1
           100
                 22
                        26
                               ESTABLISHED 0:02:11:15
                                                     0
```

Example 2: Create eBGP on Switches A and D

This example shows how to configure external BGP among switches in different ASs. In *Figure 18, Topology* on page 179, Switches A and D are in different ASs. Switch A is in AS 100 and Switch D in AS 200. This example shows how to establish the eBGP session between Switch A and Switch D.

Configure eBGP on Switch A

1. Create VLAN 100 and assign IP address 172.126.1.1.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan) #vlan 100
(Netgear Switch) (Vlan) #vlan routing 100
(Netgear Switch) (Vlan) #exit
(Netgear Switch) #
(Netgear Switch) (Config) #interface 1/0/1
(Netgear Switch) (Interface 1/0/1) #interface 1/0/1
(Netgear Switch) (Interface 1/0/1) #vlan pvid 100
(Netgear Switch) (Interface 1/0/1) #vlan participation include 100
(Netgear Switch) (Interface 1/0/1) #interface vlan 100
(Netgear Switch) (Interface vlan 100) #ip address 172.126.1.1 /24
```

2. Configure the local AS as 100 and the peer AS as 200 to create an eBGP session with peer 172.126.1.2 (Switch D).

(Netgear Switch) #configure (Netgear Switch) (Config) #ip routing (Netgear Switch) (Config) #router bgp 100 (Netgear Switch) (Config-router) # bgp router-id 172.126.1.1 (Netgear Switch) (Config-router) # network 172.126.1.0 mask 255.255.255.0 (Netgear Switch) (Config-router) # neighbor 172.126.1.2 remote-as 200 (Netgear Switch) (Config-router) #exit

Configure eBGP on Switch D

1. Create VLAN 100 on Switch D with IP address 172.126.1.2.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan) #vlan 100
(Netgear Switch) (Vlan) #vlan routing 100
(Netgear Switch) (Vlan) #exit
(Netgear Switch) #config
(Netgear Switch) (Config) #interface 1/0/1
(Netgear Switch) (Interface 1/0/1) #vlan participation include 100
(Netgear Switch) (Interface 1/0/1) #vlan pvid 100
(Netgear Switch) (Interface 1/0/1) #interface 1/0/1
(Netgear Switch) (Interface 1/0/1) #interface 1/0/1
(Netgear Switch) (Interface 1/0/1) #interface vlan 100
(Netgear Switch) (Interface vlan 100) #ip address 172.126.1.2 /24
(Netgear Switch) (Interface vlan 100) #exit
(Netgear Switch) (Config) #exit
```

2. Enable BGP on VLAN 200 on Switch D and using Switch A as an eBGP partner.

```
(Netgear Switch) (Config) #router bgp 200
(Netgear Switch) (Config-router) #bgp router-id 172.126.1.2
(Netgear Switch) (Config-router) #network 172.126.1.0 mask 255.255.255.0
(Netgear Switch) (Config-router) #neighbor 172.126.1.1 remote-as 100
(Netgear Switch) (Config-router) #exit
```

Check the eBGP Neighbor Status

Check the BGP neighbor on Switch A to see if the BGP neighbor is established. Use the same command to check it on Switch D.

(Netgear Switch) #show ip bgp neighbors 172.126.1.2	
Remote Address	
Remote AS 200	
Peer ID 172.126.1.2	
Peer Admin Status START	
Peer State	
Local Interface Address 172.126.1.1	
Local Port 47038	
Remote Port	
Connection Retry Interval 2 sec	
Neighbor Capabilities MP RF	
IPv4 Unicast Support Both	
IPv6 Unicast Support Received	
Template Name	
Update Source	
Configured Hold Time None	
Configured Keep Alive Time None	
MD5 Password	
Last Error (Sent)	
Last SubError	
Time Since Last Error S days 00 hrs 43 mins 22 secs	
Established Transitions 2	
Established Time 0 days 00 hrs 43 mins 22 secs	
Time Since Last Update 0 days 02 hrs 12 mins 43 secs	
IPv4 Outbound Update Group None	
IPv6 Outbound Update Group None	
Open Update Keepalive Notification Refresh Total	
Msgs Sent 454 6 414 1 0 875	
Msgs Rcvd 2 2 364 0 0 368	
Received UPDATE Queue Size: 0 bytes. High: 422 Limit: 392192 Drops: 0	
IPv4 Prefix Statistics:	
Inbound Outbound	
Prefixes Advertised 200 206	
Prefixes Withdrawn 0 1	
Prefixes Current 0 0	
Prefixes Accepted 0 N/A	
Prefixes Rejected 0 N/A	
Max NLRI per Update 100 100	
Min NLRI per Update 100 1	

Or

(Netgear Switch) #show ip bgp summary									
IPv4 Routing				Enable					
BGP Admin Mod	e			Enable					
BGP Router ID				172.126.1	.1				
Local AS Numb	er			100					
Number of Net	work Entri	es		2					
Number of AS	Paths			0					
Neighbor	ASN MsgR	cvd MsgS	ent	State	Up/Down Time	Pfx Rcvd			
172.126.1.2	200	368	875	ESTABLISHED	0:21:11:24	0			
192.168.1.2	100	2262	2648	ESTABLISHED	0:03:22:45	0			
192.168.3.1	100	22	26	ESTABLISHED	0:02:11:15	0			

Example 3: Create an iBGP Connection with a Loopback Interface

Loopback interface is often used as a BGP connection because it is always up on the network, unlike a physical port, for which the link might be down. This example shows how to set up an iBGP connection with loopback interface between Switches D and E. You create static routes or use an IGP protocol such as OSPF or RIP to configure the switch to reach the IP address of loopback interface.

Since NETGEAR BGP does not support multihop eBGP, eBGP cannot be established with loopback interface.

Configure iBGP on Switch D

1. Create VLAN 200 with IP address 172.126.2.1.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan) #vlan 200
(Netgear Switch) (Vlan) #vlan routing 200
(Netgear Switch) (Vlan) #exit
(Netgear Switch) #
(Netgear Switch) (Config) #interface 1/0/2
(Netgear Switch) (Interface 1/0/2) #vlan participation include 200
(Netgear Switch) (Interface 1/0/2) #interface vlan 200
(Netgear Switch) (Interface vlan 200) #ip address 172.126.2.1 /24
```

2. Create loopback 0.

(Netgear Switch) (Config) #interface loopback 0
(Netgear Switch) (Interface loopback 0) #ip address 10.1.1.1 /32
(Netgear Switch) (Interface loopback 0) #exit

3. Create a static route to the loopback interface 0 (10.1.2.1).

(Netgear Switch) (Config) #ip route 10.1.2.1 255.255.255.255 172.126.2.2

 Create a BGP neighbor with loopback interface (10.1.2.1) in Switch E (configured in the next session).

(Netgear Switch) (Config) #router bgp 200 (Netgear Switch) (Config-router) # bgp router-id 10.1.1.1 (Netgear Switch) (Config-router) # neighbor 10.1.2.1 remote-as 200 (Netgear Switch) (Config-router) #neighbor 10.1.2.1 update-source loopback 0

Configure eBGP on Switch E

1. Create VLAN 200 with IP address 172.126.2.2.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan) #vlan 200
(Netgear Switch) (Vlan) #vlan routing 200
(Netgear Switch) (Vlan) #exit
(Netgear Switch) #config t
(Netgear Switch) (Config) #interface 1/0/1
(Netgear Switch) (Interface 1/0/1) #vlan participation include 200
(Netgear Switch) (Interface 1/0/1) #interface vlan 200
(Netgear Switch) (Interface vlan 200) #ip address 172.126.2.2 /24
```

2. Create loopback 0 on Switch E with IP address 10.1.2.1.

(Netgear Switch) (Config) #interface loopback 0
(Netgear Switch) (Interface loopback 0) #ip address 10.1.2.1 /32
(Netgear Switch) (Interface loopback 0) #exit

3. Create a static route to the loopback interface 0 (10.1.1.1) on Switch D.

(Netgear Switch) (Config) #ip route 10.1.1.1 255.255.255.255 172.126.2.1

4. Create a BGP neighbor with loopback interface on Switch E,

(Netgear Switch) (Config) #router bgp 200 (Netgear Switch) (Config-router) # bgp router-id 10.1.2.1 (Netgear Switch) (Config-router) # neighbor 10.1.1.1 remote-as 200 (Netgear Switch) (Config-router) #neighbor 10.1.1.1 update-source loopback 0

Check the iBGP Status

Check the iBGP status on Switch D and on Switch E with the same command.

(Netgear Switch) #show ip bgp summary										
IPv4 Routing Enable										
BGP Admin Mode										
BGP Router ID	BGP Router ID									
Local AS Number				200						
Number of Network	Entri	es		1						
Number of AS Paths				0						
Neighbor	ASN	MsgRcvd	MsgSent	State	Up/Down Time	Pfx Rcvd				
10.1.2.1	200	11	13	ESTABLISHED	0:00:04:20	0				
172.126.1.1	100	75	164	ESTABLISHED	0:00:35:40	0				

Example 4: Configure Reflection for iBGP



Figure 19. iBGP Topology

iBGP must be fully meshed because an iBGP speaker does not advertise the routes learned from another iBGP speaker to a third iBGP speaker. As a result, the total number of iBGP sessions among n iBGP routers is n(n-1)/2 sessions, and each router contains (n-1) sessions. To reduce the iBGP sessions, we can enable route refection (RR) for iBGP. In this example, we configure Switch A as the route reflector and Switches B and C as clients so that A, B, and C do not need to be fully meshed. This example shows only how to configure reflection. For the an example how to configure iBGP, see *Example 3: Create an iBGP Connection with a Loopback Interface* on page 187.

Configure RR on Switch A

Configure RR on Switch A. Switches B and C are considered reflection clients.

(Netgear Switch) (Config) #router bgp 100 (Netgear Switch) (Config-router) #bgp router-id 192.168.1.1 (Netgear Switch) (Config-router) #neighbor 172.126.3.1 remote-as 100 (Netgear Switch) (Config-router) #neighbor 172.12.3.1 route-reflector-client (Netgear Switch) (Config-router) #neighbor 192.168.1.2 remote-as 100 (Netgear Switch) (Config-router) #neighbor 192.168.1.2 route-reflector-client (Netgear Switch) (Config-router) #neighbor 192.168.1.2 route-reflector-client (Netgear Switch) (Config-router) #neighbor 192.168.1.2 route-reflector-client

Configure the cluster ID on Switches A, B, and C. A routing information loop can occur if a cluster contains more than one RR. In this case, we configure the cluster ID to avoid the loop. You must configure all RRs in the same cluster with a 4-byte cluster ID so that an RR can recognize updates from RRs in the same cluster.

```
(Netgear Switch) (Config)#router bgp 100
(Netgear Switch) (Config-router)# bgp cluster-id 192.168.1.1
(Netgear Switch) (Config-router)#
```

Configure RR on Switch B and C

Configure the same cluster ID on Switches B and C.

```
(Netgear Switch) (Config)#router bgp 100
(Netgear Switch) (Config-router)# bgp cluster-id 192.168.1.1
(Netgear Switch) (Config-router)#
```

Example 5: Filter Routes with NLRI

Route control is the basic functionality of BGP. BGP provides many ways to control this BGP update message to send or receive the specific routes. The easier way to perform this is by using the prefix list.

To filter BGP routes with prefix lists, create the prefix lists and bind them to a BGP speaker. This filters the BGP routes exchanged with the neighbors.

To create a prefix list, use the command ip prefix-list in global configuration mode. To bind it to a BGP speaker, use the command desribute prefix or neighbor <ip address> prefix-list in BGP router configuration mode.

The following example shows how to configure the prefix list on Switch A. Assume that some routes are learned by BGP on Switches B and C, but Switch A is interested in 136.1.1.0/24 only.

This example does not include the steps for how to create an iBGP session. See *Example 3: Create an iBGP Connection with a Loopback Interface* on page 187 for iBGP session configuration.

The following is the route table when no prefix list is configured.

```
(Netgear Switch) (Config-router)#show ip route
Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
      B - BGP Derived, IA - OSPF Inter Area
      E1 - OSPF External Type 1, E2 - OSPF External Type 2
      N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
С
      192.168.1.0/24 [0/1] directly connected, 1/0/2
В
      136.1.1.0/24 [200/0] via 192.168.1.2, 00h:00m:08s, 1/0/2
В
      136.1.2.0/24 [200/0] via 192.168.1.2, 00h:00m:08s, 1/0/2
В
      136.1.3.0/24 [200/0] via 192.168.1.2, 00h:00m:08s, 1/0/2
В
      172.222.1.0/24 [200/0] via 192.168.3.1, 00h:00m:08s, 1/0/3
В
      172.222.2.0/24 [200/0] via 192.168.3.1, 00h:00m:08s, 1/0/3
С
      192.168.3.0/24 [0/1] directly connected, 1/0/3
```

Create a prefix list and apply it to BGP to permit 136.1.1.0/24 only and deny all other routes from any iBGP neighbor.

(Netgear Switch) (Config)#ip prefix-list prefix1 permit 136.1.1.0/24 (Netgear Switch) (Config)#router bgp 100 (Netgear Switch) (Config-router)# distribute-list prefix prefix1 in

The following is the IP route table after prefix1 is configured in BGP. Only 136.1.1.0/24 appears in the table and all of the other routes that were exchanged from Switches B and C are removed.

```
(Netgear Switch) (Config-router)#show ip route
Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
B - BGP Derived, IA - OSPF Inter Area
E1 - OSPF External Type 1, E2 - OSPF External Type 2
N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
C 192.168.1.0/24 [0/1] directly connected, 1/0/2
B 136.1.1.0/24 [200/0] via 192.168.1.2, 00h:00m:08s, 1/0/2
C 192.168.3.0/24 [0/1] directly connected, 1/0/3
```

If you want to filter routes from a specific neighbor, use the following command:

(Netgear Switch) (Config-router)#neighbor 36.1.1.2 prefix-list prefix1 in

If you want to filter routes that will be sent out to a neighbor, use the option <out>:

```
(Netgear Switch) (Config-router)#distribute-list prefix-list prefix1 out
Or
(Netgear Switch) (Config-router)#neighbor 36.1.1.2 prefix-list prefix1 out
```

Example 6: Filter Routes with AS_PATH

Although filtering by prefix list is easy and fast, it is not practical to filter routes in the case of a large number of routes. In this case, BGP provides the AS_PATH filter to control routes based on AS_PATH instead of each specific address in a prefix list. It allows users to create an AS-PATH list using regular expressions. Regular expressions use special characters to find matches in the given texts.

The following special characters are supported in AS_PATH regular expressions.

Special Character	Symbol	Behavior	example
asterisk	*	Matches zero or more sequences of the pattern.	1* matches any occurrence of the number 1 including none 12* matches the characters 12 and any characters that follow 12.
brackets	[]	Designates a range of single-character patterns.	[0123a-z] matches 0, 1, and w, but not 4, 8, or K
caret	^	Matches the beginning of the input string.	^123 matches 1234, but not 01234
dollar sign	\$	Matches the end of the input string.	123\$ matches 0123, but not 1234
hyphen	-	Separates the end points of a range.	[a-z] matches any character between a and z.
period		Matches any single character, including white space.	0.0 matches 0x0 and 020 tt matches strings such as test, text, and tart
plus sign	+	Matches 1 or more sequences of the pattern.	2+ requires there to be at least one number 2 in the string to be matched

Table 1. Special characters supported in AS_PATH regular expressions

question mark	?	Matches 0 or 1 occurrences of the pattern. (Press Ctrl-V prior to pressing question mark to prevent it from being interpreted as a help command.)	a?c matches ac and abc
underscore	_	Matches a comma (,), left brace ({), right brace (}), left parenthesis, right parenthesis, the beginning of the input string, the end of the input string, or a space.	The characters _1300_ can match any of the following strings: ^1300\$ ^1300space space1300 {1300, ,1300, {1300}, ,1300,

Table 1.	Special character	s supported in AS	PATH regular	expressions	(continued)
----------	-------------------	-------------------	--------------	-------------	-------------

This example does not include the steps for how to create an eBGP session. See *Example 2: Create eBGP on Switches A and D* on page 184 for the eBGP session configuration.

Switch A is denied to all of the routes in which AS_PATH contains only 200 and permits others.

```
(Netgear Switch)(Config) #ip as-path access-list 1 deny ^200$
(Netgear Switch)(Config) #ip as-path access-list 1 permit .*
(Netgear Switch) (Config-router) #neighbor 172.126.1.2 filter-list 1 in
```

Example 7: Filter Routes with Route Maps

You can implement route filters with BGP route maps. BGP route maps are separated by PBR route maps. BGP route maps support the following filter list:

- as-path
- community
- ip address prefix-list
- ipv6 address prefix-list

This example shows how to filter BGP routes with AS-PATH list.

This example does not include the steps for how to create an eBGP session. See *Example 2: Create eBGP on Switches A and D* on page 184 for the eBGP session configuration.

1. Create route-map 1.

(Netgear Switch) #config (Netgear Switch) (Config)#ip as-path access-list 1 deny '^200\$' (Netgear Switch) (Config)#ip as-path access-list 1 permit '^*' (Netgear Switch) (Config)#route-map route-map1 (Netgear Switch) (route-map)#match as-path 1

Before we apply route-map1 to BGP, the route table is as follows:

```
(Netgear Switch) (Config-router) #show ip route
Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
С
       172.126.1.0/24 [0/1] directly connected,
                                                 1/0/1
В
       172.126.2.0/24 [20/0] via 172.126.1.2,
                                               00h:02m:01s, 1/0/1
В
       172.126.3.0/24 [20/0] via 172.126.1.2, 00h:02m:01s, 1/0/1
С
       192.168.1.0/24 [0/1] directly connected, 1/0/2
В
       192.168.2.0/24 [200/0] via 192.168.1.2, 00h:10m:13s, 1/0/2
С
       192.168.3.0/24 [0/1] directly connected, 1/0/3
```

2. Apply route-map1 to the BGP neighbor.

(Netgear Switch) (Config) #router bgp 100 (Netgear Switch) (Config-router) #neighbor 172.126.1.2 route-map route-map1

After you apply route-map1 to BGP, the output of route table is as follows. The routes 172.126.2.0/24 and 172.126.3.0/24 are removed from the route table.

```
(Netgear Switch) (Config-router) #show ip route
Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
С
       172.126.1.0/24 [0/1] directly connected,
                                                 1/0/1
С
       192.168.1.0/24 [0/1] directly connected,
                                                  1/0/2
В
      192.168.2.0/24 [200/0] via 192.168.1.2, 00h:10m:25s, 1/0/2
С
       192.168.3.0/24 [0/1] directly connected,
                                                 1/0/3
```

Example 8: Exchange IPv6 Routes over an IPv4 BGP

IPv6 BGP configuration is similar to IPv4 BGP. The following example shows how to set up an IPv6 BGP session. In this example, we set up an IPv6 BGP session between Switches A and C.

Configure IPv6 BGP on Switch A

1. Enable IPv6 unicast globally.

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

Configure the IPv6 address on port 1/0/2.

```
(Netgear Switch) (Config) #interface 1/0/2
(Netgear Switch) (Interface 1/0/2) #routing
(Netgear Switch) (Interface 1/0/2) #ipv6 enable
(Netgear Switch) (Interface 1/0/2)#ipv6 address 2001:1:1::1/64
```

3. Configure IPv6 BGP.

```
(Netgear Switch) (Config) #router bgp 100
(Netgear Switch) (Config-router) #neighbor 2001:1:1::2 remote-as 100
(Netgear Switch) (Config-router) #address-family ipv6
(Netgear Switch) (config-router-af) #neighbor 2001:1:1::2 activate
```

Configure IPv6 BGP on Switch B

1. Enable IPv6 unicast globally.

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

Configure the IPv6 address on port 1/0/1.

```
(Netgear Switch) (Config) #interface 1/0/1
(Netgear Switch) (Interface 1/0/2) #routing
(Netgear Switch) (Interface 1/0/2) #ipv6 enable
(Netgear Switch) (Interface 1/0/2) #ipv6 address 2001:1:1::2/64
```

3. Configure IPv6 BGP.

(Netgear Switch) (Config) #router bgp 100 (Netgear Switch) (Config-router) #neighbor 2001:1:1:1:1 remote-as 100 (Netgear Switch) (Config-router) #address-family ipv6 (Netgear Switch) (config-router-af) #neighbor 2001:1:1:1 activate

PBR

Policy-based routing

This chapter includes the following sections:

- Policy-Based Routing Concept
- Route-Map Statements
- PBR Processing Logic
- PBR Configurations
- PBR Example

Note: PBR is available on the M6100 series switches only.

10

Policy-Based Routing Concept

Normally, switches make forwarding decisions based on routing tables, which get populated by information given by dynamic routing protocols or static routing, to forward packets to destination addresses. Policy-based routing (PBR) is a feature that enables network administrators to define forwarding behavior based on packet contents. PBR is used to override traditional destination-based routing behavior.

Configuring PBR involves configuring a route map with the match and set commands and then applying the corresponding route map to the inbound traffic on routing interfaces. One interface can contain only one route-map tag, but administrators can create multiple route-map entries with different sequence numbers. These entries are evaluated in sequence-number order until the first match is found. If no match is found, packets are routed as usual.

Route-Map Statements

A route-map statement that is used for PBR is configured as permit or deny. If the statement is marked as deny, traditional destination-based routing is performed on the packet that meet the match criteria:

- If users specify any match/set statements in a route-map statement that are marked as deny, they will not be effective because traditional destination-based routing is performed on packets meeting the specified match criteria.
- If the statement is marked as permit, and if the packet meets all the match criteria, then the set commands in the route-map statement are applied.

If no match is found in the route map, the packet is not dropped. Packets are forwarded using the routing decision that is made by performing destination-based routing.

If network administrators do not want to revert to normal forwarding, but instead want to drop a packet that does not match the specified criteria, a set statement needs to be configured to route the packets to interface null 0 as the last entry in the route map.

Packets that are generated by the switch itself are not normally policy routed. But a provision in other industry standard products applies a policy through a local PBR. All packets originating on the switch are then subject to the local PBR. However, this feature is not supported in NETGEAR Software Version 10.2.

Starting with Software Version 10.2, the NETGEAR switch supports the route-map infrastructure for BGP. Match parameters defined in this chapter for policy-based routing operate in isolation with BGP. These options do not interfere with BGP protocol processing or policy propagation in any way.

For example, if a match clause is placed in a route-map statement based on the length of the packet, BGP does not honor that clause. As stated earlier, these statements apply for L3 routed traffic (mainly data traffic) to override a routing decision.

The following packet entities are supported in NETGEAR Software Version 10.2 to classify L3 routed traffic:

- The size of the packet
- Protocol of the payload (Protocol ID field in IP header)
- Source MAC address
- Source IP address
- Destination IP address
- Priority (802.1P priority)

NETGEAR's policy-based routing feature overrides routing decisions taken by the switch and makes the packet follow different actions specified in the following order to define forwarding criteria:

- List of next hop IP addresses. The IP address can specify the adjacent next hop router in the path toward the destination to which the packets should be forwarded. The first IP address associated with a currently active ARP entry is used to route the packets.
- List of default next hop IP addresses. This list indicates the list of next-hop routers to which a packet must be routed if no explicit route exists for the packet's destination address in the routing table. A default route in the routing table is not considered an explicit route for an unknown destination address.
- IP precedence. A numeric value can be specified to set the precedence in the IP packets being forwarded. IP precedence value implies 3 IP precedence bits in the IP packet header. With 3 bits, network administrators have 8 possible values for the IP precedence. This value will be set in IPV4 header of packets when configured.

PBR Processing Logic

The processing logic used by policy-based routing is as follows when a packet is received on an interface configured with a route map, the forwarding logic processes each route-map statement according to the sequence number.

The route map with a permit statement uses the following logic:

- The incoming packet is matched against the criteria in the match term specified in the route map. This match command can refer to an IP/MAC access list. An ACL that is used in the match term itself includes one or more permit or deny rules. Now, the incoming packet is matched against the rules in the AC, and a permit or deny decision is reached.
- If the decision reached in the previous step is permit, then policy-based routing executes the action specified in set terms of the route-map statement over an incoming packet.
- If the decision reached in the earlier step is deny, then policy-based routing does not apply any action that is specified in set terms in the route-map statement. In this situation, the counter for this match statement is not incremented and the processing logic moves to next route-map statement in the sequence. If no next route-map statement exists, the processing logic terminates and the packet goes through standard destination-based routing logic.

The route map with a deny statement uses the following logic:

- The incoming packet is matched against the criteria in the match term specified in the route map. This match command can refer to an IP/MAC access list. An ACL that is used in the match term itself has one or more permit or deny rules. Now, the incoming packet is matched against the rules in the ACL, and a permit or deny decision is reached.
- If the decision reached in the previous step is permit, then policy-based routing processing logic terminates and the packet goes through standard destination-based routing logic.
- If the decision reached in the earlier step is deny, the counter for this match statement is not incremented and the processing logic moves to next route-map statement in the sequence. If no next route-map statement exists, the processing logic terminates and the packet goes through standard destination-based routing logic.

The following table specifies the desired actions:

ACL	Match	Outcome	Route Map	Action
Permit	Yes	Permit	Permit	Set
Permit	No	Deny	Permit	Next
Permit	Yes	Permit	Deny	Route
Permit	No	Deny	Deny	Next
Deny	Yes	Deny	Permit	Next
Deny	No	Deny	Permit	Next
Deny	Yes	Deny	Deny	Next
Deny	No	Deny	Deny	Next

Table 2. Desired actions

The following actions are taken:

- **Next**. Fall through to the next route map, and if no further route maps exist, route using the default routing table.
- Set. Route according to the action in the set clause.
- **Route** (alone). Route using the default routing table.

PBR Configurations

PBR is configurable on the following types of eligible routing interfaces:

- Physical ports
- VLAN interfaces

On VLAN interfaces, when an ACL is applied, it implies that when any packet arrives with a corresponding VLAN ID on any port, it is matched and a corresponding action is taken.

The same phenomenon applies to ACLs specified in the match clause of PBR. That is, if a PBR route map is applied on a VLAN interface, any packet coming with a corresponding VLAN ID on any port is matched against PBR rules corresponding to the match ACL clause and the corresponding set actions are taken into effect. To perform policy-based routing based on VLAN ID as the matching criteria for incoming packets, apply an ACL rule on the VLAN interface, but do not configure a rule with the VLAN ID as the match condition.

PBR supports the preconfiguration of the route map on routing interfaces. If routing is not enabled on an interface, the route map can still be applied on that particular interface. When routing is not enabled on an interface, route-map configuration is not pushed into hardware. Rather, it is maintained only in configuration. As soon as routing is enabled on that particular interface, configuration is applied to hardware.

PBR Example

Network administrators can use PBR when load sharing must be done for the incoming traffic across multiple paths based on packet entities in the incoming traffic.

Normally, to optimally utilize the data networks of the organization, the bulk traffic associated with the company activity must use a higher-bandwidth, high-cost (price of link) link while the basic connectivity continues over a lower bandwidth, low-cost link for interactive traffic. For such applications, policy-based routing is the right fit.

Consider the network that is composed of two groups with different IP address ranges. If group1 addresses must be routed through ISP1 and group2 addresses must be routed through ISP2, the switch that is connected with different groups must be policy routed. Configure a match in the route map on the IP address range of different groups. This way, an equal access as well as source IP address-sensitive routing is achieved through PBR.



Figure 20. PBR topology

1. Create an IP ACL 1 to match 10.1.0.0/16.

(Netgear Switch) (Config) #access-list 1 permit 10.1.0.0 0.0.255.255

2. Create an IP ACL 2 to match 10.2.0.0/16.

(Netgear Switch) (Config)#access-list 2 permit 10.2.0.0 0.0.255.255

3. Create a route map pbr_1 with sequence number 10 to match ip ACL 1.

```
(Netgear Switch) (Config) #route-map pbr_1 permit 10
(Netgear Switch) (route-map) #match ip address 1
(Netgear Switch) (route-map) #set ip next-hop 20.1.1.2
(Netgear Switch) (route-map) #exit
```

4. Create a route map pbr_1 with sequence number 11 to match ip ACL 2.

```
(Netgear Switch) (Config) # route-map pbr_1 permit 11
(Netgear Switch) (route-map) #match ip address 2
(Netgear Switch) (route-map) #set ip next-hop 20.2.1.2
(Netgear Switch) (route-map) #exit
```

Create VLAN 30 and put interface 1/0/1 and 1/0/2 into it.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan) #vlan 30
(Netgear Switch) (Vlan) #vlan routing 30
(Netgear Switch) (Vlan) #exit
(Netgear Switch) (Config) #interface 1/0/1-1/0/2
(Netgear Switch) (Interface 1/0/1-1/0/2) #vlan participation include 30
(Netgear Switch) (Interface 1/0/1-1/0/2) #vlan pvid 30
(Netgear Switch) (Interface 1/0/1-1/0/2) #exit
(Netgear Switch) (Config) #interface vlan 30
(Netgear Switch) (Interface vlan 30) #routing
(Netgear Switch) (Interface vlan 30) #ip address 10.1.1.1 255.0.0.0
(Netgear Switch) (Interface vlan 30) #exit
```

6. Enable PBR on VLAN 30.

```
(Netgear Switch) (Config) #interface vlan 30
(Netgear Switch) (Interface vlan 30) #routing
(Netgear Switch) (Interface vlan 30) #ip policy route-map pbr_1
(Netgear Switch) (Interface vlan 30) #exit
```

7. Configure IP address 20.1.1.1 on interface 1/0/3.

```
(Netgear Switch) (Config) #interface 1/0/3
(Netgear Switch) (Interface 1/0/3) #routing
(Netgear Switch) (Interface 1/0/3) #ip add 20.1.1.1 /16
```

8. Configure IP address 20.2.1.1 on interface 1/0/4.

```
Netgear Switch) (Config) #interface 1/0/4
(Netgear Switch) (Interface 1/0/4) #routing
(Netgear Switch) (Interface 1/0/4) #ip add 20.2.1.1 /16
```

ARP

Proxy Address Resolution Protocol

11

This chapter includes the following sections:

- Proxy ARP Concepts
- Proxy ARP Examples

Proxy ARP Concepts

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

Proxy ARP Examples

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

CLI: show ip interface

(Netgear Switch) #show ip interface ?									
<slot port=""> brief</slot>	Enter an interface in a Display summary informa settings for all ports	slot/port format. ation about IP configuration							
(Netgear Switch) #show i	p interface 0/24								
Routing Mode		Disable							
Administrative Mode		Enable							
Forward Net Directed Bro	oadcasts	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></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.

System	Sw	ritching		Routing	0	20S 8	ecurity	Monitorir	ıg l	Maintenance		Help	Index	
Routing Table		IPv6	VLAN	ARP	RIP	OSPF OSF	PFv3 Ro	uter Discovery	VRRP	Multicast	IPv6 IV	lulticast		
P			IP Inte	rface Cor	nfiguratior	1								
• Basic		~	12	VLANS /	All									
 Advanced IP Configurat 	ion	^	Fo	rward Ne badcasts	t Directed	d Active Sta	te MAC /	Address	Encapsula Type	ation Proxy	Arp	Local Proxy Arp	Bandwic	ICMP Destination Unreachables
 Statistics 			D	isable 🗸		Inactive	20:0C	C8:4D:95:98	Ethernet	✓ Enal	ole 🗸	Disable	✓ 100000	Enable 🗸
IP Interface Configuration			Di	sable sable		Active	20:0C	C8:4D:95:98	Ethernet Ethernet	Enabl	e e	Disable Disable	1000000) Enable
 Secondary IF 	>		Di	sable		Inactive	20:0C	C8:4D:95:98	Ethernet	Enabl	e	Disable	100000	Enable

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

VRRP

Virtual Router Redundancy Protocol

This chapter includes the following sections:

- Virtual Router Redundancy Protocol Concepts
- VRRP on a Master Router
- VRRP on a Backup Router

Note: VRRP is available on the M5300, M6100, and M7100 series switches. However, the following M5300 series switches require a license to support VRRP: M5300-28G, M5300-52G, M5300-28G-POE+, and M5300-52G-POE+.

12

Virtual Router Redundancy Protocol Concepts

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



Figure 21. VRRP

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

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.

System	Switching		Routing			QoS	Securit		Monitoring		Maintenance	Help	Index				
Routing Table	IP I	Pv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	er Discovery	VRRP	Multicast	IPv6 Multicast					
IP			IP Cont	figuration													
- Basic		~	Defau	lt Time t	o Live				64								
• IP Configurat	ion		Routin	ng Mode					Enable	Enable Disable							
 Statistics 			ICMP	Echo R	eplies				Enable O Disable								
 Advanced 		~	ICMP	Redirec	s				Enable	e 🖲 Disal	ble						
			ICMP	Rate Lir	nit Inte	erval			1000		47483647 ms)						
			ICMP	Rate Lir	nit Bu	rst Size			100		(1 to 20						
		Maxir	num Nex	t Hop	S			4 8160									
		Maxin	num Rou	ites													
			Selec	t to conf	gure (Global Defa	ault Gateway	6									
			Globa	l Default	Gatev	vay			192.168.	10.1							

- **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.

System Switching			Routing			QoS	Securit	/ Monito	oring	Maintenance	Help	Index			
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discove	ry VRRF	P Multicast	IPv6 Multica	ist			
IP			IP Int	erface C	onfigurat	ion									
• Basic		×	13	VLANS	All										
 Advanced IP Configurat 	ion	^		Port	Descrip	otion	VLAN ID	IP Address Co Method	nfiguration	IP Address	Subne Mask	t Ro Mo	outing ode	Administra Mode	tive
 Statistics 				1/0/2				Manual 🛩		192.150.2.1	255.2	55.255.0 E	nable 🗸	Enable	~
• IP Interface	NA			1/0/1				None		0.0.0.0	0.0.0.0) Di	sable	Enable	
Conliguration		3	☑ 1/0/2			None		0.0.0.0	0.0.0.0) Di:	Disable				
 Secondary IF 	,		0	1/0/3				None		0.0.0	0.0.0.0) Di:	sable	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.

System	System Switching		Routing			QoS Security		ty Monitoring		Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery		Multicast	IPv6 Multicast	
VRF	P		Global	Configur	ation							
•Basic		~	Admi	in Mode) Disa	ible 🔵 Enab	,le				
VRRP Config	guratio	n										
 Advanced 		~										
			Table (Configura	tion							
				VRID (1	to 255)	j	Interface	Interface IP Address	Prima	ry IP Address	Mode	State
				20			1/0/2 ×		192.1	50.2.1	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.

System	Sw	vitching		Routing		QoS	Securi	ty	Monitoring	g i	Maintenance	Help	Index			
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast				
IP			IP Con	figuration	<u>í – – – – – – – – – – – – – – – – – – –</u>											
Basic		~	Defau	ult Time t	o Live				64							
• IP Configurati	ion		Routi	ng Mode					Enable	e 🔘 Disat	ole					
 Statistics 			ICMP	Echo Re	eplies				Enable	e 🔘 Disab	ble					
 Advanced 		~	ICMP	Redirect	ts				Enable	e 🖲 Disab	ble					
			ICMP	Rate Lin	nit Inte	arval			1000							
			ICMP	Rate Lin	nit Bu	rst Size			100		(1 to 20	(1 to 200)				
			Maxir	mum Nex	d Hop	S			4							
			Maxir	mum Rou	ites				8160							
			Selec	t to confi	igure (Global Def:	ault Gatewa	V								
			Globa	al Default	Gatev	way			192 168	192 168 10 1						

- **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.

System	Switching		Routing		3	QoS	Security	/ Monitoring	Maintenance	Help	Index	
Routing Table	P	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery VRRP	Multicast	IPv6 Multicast		
IP			IP Inte	rface Co	onfigurat	ion						
Basic		~	13	All								
 Advanced IP Configuration 	on	٩		Port	Descri	iption	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Routing Mode	Administrative Mode
 Statistics 				1/0/4				Manual 🛩	192.150.4.1	255.255.0	.0 Enable 🛩	Enable ~
IP Interface Configuration				1/0/1				None	0.0.0.0	0.0.0.0	Disable	Enable
 Secondary IP 				1/0/2				None	0.0.0.0	0.0.0.0	Disable	Enable
				1/0/4				None	0.0.0.0	0.0.0	Disable	Enable
				1/0/5				None	0.0.0.0	0.0.0.0	Disable	Enable
				1/0/6				None	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.

System	Sm	tching		Routing		QoS	Securit	/	Monitoring		Maintenance	Help	Index						-
Routing Table	IP.	IP16	VLAN	ARP	RIP	OSPF	OSPFv3	Router	Discovery		Multicast	IPv6 Multicast							
																	Add De	iete Cancel	Αρριγ
VRR	P	1	Global	Configural	ion														C
Basic		+	Adm	sin Mode		😔 Disab	le 🖲 Enab	le											
•Advanced		*																	
VRRP Config	guration																		
VRRP Secon Address Conf	ndary IP figuratio	an	Table	Configurati	on														Ø
 VRRP Trackin Configuration 	ing		Ú.	VRID (1 t	255)	Interface	Pre-e Mode	mpl	Accept Mod	(11	nfigured Priority o 254)	Operational Priority	Advertisement (1 to 255)	Interval.	Interface IP Address	Owner	VMAC Address	Primary IP Address	Auth
VRRP Statist	tics			1		1/0/4	4	×	-	25	4		1					192.150.2.1	

- **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.

ACLs

Access Control Lists

This chapter includes the following sections:

- Access Control List Concepts
- MAC ACLs
- Set Up an IP ACL with Two Rules
- One-Way Access Using a TCP Flag in an ACL
- Use ACLs to Configure Isolated VLANs on a Layer 3 Switch

13

- Set up a MAC ACL with Two Rules
- ACL Mirroring
- ACL Redirect
- Configure a Management ACL
- Configure IPv6 ACLs

Access Control List Concepts

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

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

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

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

MAC ACLs

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

- Source MAC address with mask.
- Destination MAC address with mask.
- VLAN ID (or range of IDs).
- Class of Service (CoS) (802.1p).
- EtherType:
 - Secondary CoS (802.1p).
 - Secondary VLAN (or range of IDs).
- L2 ACLs can apply to one or more interfaces.
- Multiple access lists can be applied to a single interface: the sequence number determines the order of execution.
- You can assign packets to queues using the assign queue option.
- You can redirect packets using the redirect option.
IP ACLs

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

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

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

ACL Configuration

To configure ACLs:

- 1. Create an ACL by specifying a name (MAC ACL or named IP ACL) or a number (IP ACL).
- 2. Add new rules to the ACL.
- 3. Configure the match criteria for the rules.
- 4. Apply the ACL to one or more interfaces.

Set Up an IP ACL with Two Rules

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



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

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
```

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

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

Web Interface: Set Up an IP ACL with Two Rules

- 1. Create IP ACL 101 on the switch.
 - a. Select Security > ACL > IP ACL.

A screen similar to the following displays.

System	Switc	hing	Routing	QoS	Securit	y 👘	Monitoring	Maintenance	Help	Index
Management S	Security	Acces	s Port Authenti	cation Tra	ffic Control	Control				
AC	L	IF	ACL Configuration	on						
 ACL Wizard 			Current Number	of ACL	0					
Basic		~	Maximum ACL		100					
 Advanced 		^								
• IP ACL										
• IP Rules		IF	ACL Table							
 IP Extended 	Rules	-			20	23				
• IPv6 ACL			IP ACL ID		Rules	Туре				
• IPv6 Rules			101							
• IP Binding C	onfiguratio	on								
 Binding Tabl 	е									
• VLAN Bindin	ig Table									

- b. In the IP ACL ID field, enter 101.
- c. Click Add to create ACL 101.
- 2. Create a new rule associated with ACL 101.
 - a. Select Security > ACL > IP ACL > IP Extended Rules.

A screen similar to the following displays.

System Switching	,	Routin	9	QoS	Securit	/	fonitoring	M	aintenance	Hel	p Inde	x						Í
Management Security Act	cess	Port Aut	thenticatio	on Traff	ic Control	Control	ARL											
																- 1	dd Deli	ete Cancel
ACL	IP Rul	les																0
 ACL Wizard 	ACI	. ID/Nar	ne	101	-													
-Basic -																		
Advanced																		
· IP ACL	Exten	ded ACI	L Rule Ta	ble														2.6
• IP Rules	-		1	1		_	-		n	_		here and				191	-	-
• IP Extended Rules		Rule	Action	Looging	Assign	Mirror	Redirect	Match	Protocol	TCP Flag	Established	Source	Source	Source 14	Source	Source 14	Source	Destination
· IPv6 ACL		ID :			Queue ID	Interface	Interface	Every	Type			Address	Mask	Port Action	Port	Start Port	End Port	Address
• IPv6 Rules	No	rules	have b	een con	figured	for this	ACL											
•IP Binding Configuration																		
Binding Table																		
VLAN Binding Table																		
1.000																		

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

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

System Switching	Routing QoS	Security Monitoring	Maintenance Help	Index	
Management Security Ac	cess Port Authentication 1	raffic Control Control ASI			
ACL	Extended ACL Rule Configura	ation(100-199)			
ACL Wizard	ACL ID/Name	101			
Basic ~	Rule ID	22			
Advanced •	Action	ermit	Egress Queue	~ (0-6)	
IP ACL IP Rules	Logging	Deny Disable	Enable		
IP Extended Rules IP/6 ACL	Interface Match Every	Mirror Redirect	•		
IPv6 Rules IP Binding Configuration	Protocol Type	UDP ~	(0 to 255)		
Binding Table	TCP Flag	URG RST	lignore ~	ACK. SYN	Ignore - PSH Ignore - FIN
VLAN Binding Table	Src	IP Address	192 168 77.0	0.0.0.255	
	Src L4	Host Port	Other 🖌	Equal ×	(0 to 65535)
		Range	Start Port	Other *	(0 to 65535) End Port
	Dst	IP Address	192.178.77.0	0.0.0.255	

- **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.

System Switching	Routing QoS	Security Monitoring	Maintenance Help	Index				
Management Security Acc	ess Port Authentication T	raffic Control Control ACL	NA STATES	6				
ACI.	Extended ACL Rule Configura	tion(100-199)						
ACL Wizard	ACL ID/Name	101						
Basic 👻	Rule ID	1						
Advanced ~	Action	ermit	Egress Queue	× (0-6)				
• IP ACL	Logging	② Deny ∞ Disable	C Enable	10 M				
IP Extended Pulas	Interface	(Mirror	+					
• IPv6 ACL • IPv6 Rules	Match Every	G Redirect	v					
IP Binding Configuration Binding Table	TCP Flag	URG est	Ignore v	ACK	Ignore v PSH			
VLAN Binding Table	Src	IP Address	192.168.77.0	0.0.0.255	Ignore ·			
	Src L4	Host Port	Other ~	Equal 👻	(0 to 65535)			
	Dst	 Range IP Address 	192 178 77 0	Other ~ 0.0.0.255	(0 to 65535) End Port			

- **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.

ACL		IP Bin	ding C	onfigu	ration	(
ACL Wizard Basic Advanced IP ACL) (ACL Direc Sequ	D tion ence f	Numb	er										10 Inb 1	l ~	Ŷ	(1 to	4294	96729	95)					 	
*IP Rules			Jnit 1																								 -
IP Extended Rules IP(6 ACL		Ports	1		ģ		11	13	15	17	19	21	23	25	27	29 3	1 3	Ţ	5 37	39	41	43	45	47			
+IPv6 Rules			2	4	8	8 1	0 12	14	16	18	20	22	24	26	28	30 3	12 3	4 3	6 38	40	42	44	46	48			
• IP Binding Configuration	on -	-	Jnit 2																								~
Binding Table VLAN Binding Table		Ports	1	3	5			13	15	17	19	21	23	25	27	29 3			5 37	39	41	43					

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

One-Way Access Using a TCP Flag in an ACL

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



Figure 23. One-Way Web access using a TCP flag in an ACL

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

This is a two-step process:

- Step 1: Configure the VLAN and IP addresses on Switch A on page 223
- Step 2: Configure on Switch B on page 225

Step 1: Configure the VLAN and IP addresses on Switch A

(See Figure 23, 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)#vlan participation include 200
(Netgear Switch) (Interface 0/44)#exit
(Netgear Switch) (Interface vlan 200
(Netgear Switch) (Interface-vlan 200)#routing
(Netgear Switch) (Interface-vlan 200)#ip address 192.168.200.1 255.255.255.0
(Netgear Switch) (Interface-vlan 200)#exit
```

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

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

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

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

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

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

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

(Netgear	Switch)	(Config)#ir	nterface ()/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)#exi	it			

Step 2: Configure on Switch B

(See Figure 23, One-Way Web access using a TCP flag in an ACL on page 222.)

1. Create VLAN 40 with port 1/0/24 and assign IP address 192.168.40.1/24.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 40
(Netgear Switch) (Vlan)#vlan routing 40
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan pvid 40
(Netgear Switch) (Interface 1/0/24)#vlan participation include 40
(Netgear Switch) (Interface 1/0/24)#exit
(Netgear Switch) (Config)#interface vlan 40
(Netgear Switch) (Interface-vlan 40)#routing
(Netgear Switch) (Interface-vlan 40)#ip address 192.168.40.1 255.255.255.0
(Netgear Switch) (Interface-vlan 40)#exit
```

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

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

3. Create VLAN 200 with port 1/0/48 and assign IP address 192.168.200.1/24.

(Netgear	Switch)	#vlan database
(Netgear	Switch)	(Vlan)#vlan 200
(Netgear	Switch)	(Vlan)#vlan routing 200
(Netgear	Switch)	(Config)#interface 1/0/48
(Netgear	Switch)	(Interface 1/0/48)#vlan pvid 200
(Netgear	Switch)	(Interface 1/0/48)#vlan participation include 200
(Netgear	Switch)	(Interface 1/0/48)#exit
(Netgear	Switch)	#interface vlan 200
(Netgear	Switch)	(Interface-vlan 200)#routing
(Netgear	Switch)	(Interface-vlan 200)#ip address 192.168.200.2 255.255.255.0
(Netgear	Switch)	(Interface-vlan 200)#exit

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

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

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

This is a two-part process:

- Configuring VLAN and IP addresses on switch A on page 226
- Configuring the Switch B on page 234

Configuring VLAN and IP addresses on switch A

- 1. Create VLAN 30 with IP address 192.168.30.1/24.
 - a. Select Routing > VLAN > VLAN Routing Wizard.

System Switching	Routing QoS Security Monitoring Maintenance Help Index
Routing Table IP IPv6	VLAN ARP RIP OSPF OSPFv3 Router Discovery VRRP Multicast IPv6 Multicast
VLAN	VLAN Routing Wizard
VLAN Routing Wizard VLAN Routing	Vian ID 30 IP Address (922168.30.1
	Network Mask 255.255.255.0
	Ports 1 2 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 25 27 39 41 43 45 47
	2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 Unit 2
	Pote 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 2 4 6 8 10 12 14 15 16 20 22 24 25 27 29 31 33 35 37 39 41 43 2 4 6 8 10 12 14 15 16 20 22 24 25 29 30 32 24 35 38 40 42 44

- **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.

System	Switching	Routing	QoS	Secur	ty Monitoring	Maintenance	Help	Index	
Routing Table	IP IPv6	VILAN ARP	RIP OSE	F OSPEVA	Router Discovery	VRRP Multicast	IPv6 Multicast		
VLA		VLAN Routing	Wizard						
VLAN Routing	Wizard	Vlan ID				100)		
VLAN Routing		IP Address				192	2 168 100 1		
		Network Mar	sk			255	255 255 0		
		Unit 1							*
		Ports 1	3 5 7	0 11 13	15 17 19 21 2	3 25 27 29 31	33 35 37 3	9 41 43 45	47
		2	4 5 8	10 12 14	15 18 20 22 24	4 26 28 30 32	34 36 38	10 42 44 45	48
		Unit 2							
		Ports 1	3 5 7	9 11 13	15 17 19 21 2	3 25 27 29 31	33 35 37 3	9 41 43	
								. ا ا	
		2	4 0 8	10 12 14	10 18 20 22 24	4 xo xo 30 32	34 36 38 4	10 4Z 44	

- **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.

System Switchin	g Routing QoS Security Monitoring Maintenance Help Index
Routing Table IP IPv6	VLAN ARP RIP OSPF OSPFA Router Discovery VRRP Multicast IPv6 Multicast
VLAN	VLAN Routing Wizard
VLAN Routing Wizard	Vian ID 300
VLAN Routing	IP Address 192 168 200 1
	Network Mask 255 255 255 0
	Unit 1
	Perts 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47
	z 4 0 0 10 12 14 10 18 20 22 24 20 28 30 32 34 30 30 40 42 44 40 40
	Ports 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43
	2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44

- **b.** Enter the following information:
 - In the Vian 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.

System	Sv	vitching		Routing		QoS	Securit	y	Monitoring	g	Maintenance	Hel	lp Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	er Discovery	VRRP	Multicast	IPv6 Multi	icast
IP	Ú.		IP Cont	figuratior									
• Basic		~	Defa	ult Time	to Live	5			64				
 IP Configurat 	tion		Rout	ing Mod	9				Enab	le 🖲 Dis	able		
 Statistics 			ICMF	^o Echo F	eplies				Enable	le 🔘 Dis	able		
 Advanced 		~	ICMF	P Redire	sts				Enab	le 🖲 Dis	able		
			ICMF	P Rate L	mit Inf	erval			1000		(0 to 2	147483647 r	ms)
			ICMF	P Rate L	mit Bu	ırst Size			100		(1 to 2	00)	
			Maxi	imum Ne	xt Hop	os			4				
			Maxi	imum Ro	utes				12288				
			Sele	ct to cor	figure	Global De	fault Gatewa	y					
			Glob	al Defau	t Gate	way			0.0.0.0				
1													

- 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.

0		and the second		Pineter .		0 0	100	100000			and the second	No.	19.8		
System	Swi	tching		Routing	q	05 54	ecunty	Monitorir	1g Mi	antenance	Help	Index			
Housing Table	IP 1	P90	VLAN	PAPEP	HOP- C	JOHN COM	PAR ROL	ARE DISCOVERY	VHORP	MUNICAN	IEV6 MURICA	194			Pris and
															Update
Routing	Table		Config	jure Route:	5										
Basic		^	1	Route Ty	pe	Network Ad	dress	Subnet Ma	isk.	Next Hop	Address	Preference	Des	cription	
 Route Config 	paration			Static	Ŷ	192.168.40	0	255 255 25	55.0	192.168.2	200.2				
• Advanced		×				-	6	al Reconstruction		and the second se			and the second second		
			Learn	ed Routes											
			-		-							00.000000000000000000000000000000000000	IN STREET, INC.		
			76	etwork Add	mas Si	ibnet Mask	Protocol	Route Type	Next Hop Int	erface Ne	nd Hop Addres	s Preference	Metric		

- **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.

System Switching	g Routing	QoS Security	Monitoring	Maintenance Hel	p Index			
Noting Table IP IPv6	VLAN ARP RIP	OSPF OSPFV3 R	auter Discovery VRR	P Multicast IPv6 Multi	cast			
						0	odate Add Delete	Cancel Apply
Routing Table	Configure Routes							0
•Basic	Route Type	Network Address	Subnet Mask	Next Hop Address	Preference	Description		
Route Configuration	Static	~ 192 168 50.0	255 255 255.0	192.168.200.2				
• Advanced	Static	192.168.40.0	255 255 255.0	192 168 200 2	1	1		
	Learned Routes							9
	Network Address	Subnet Mask Protocol	Route Type Next Ho	p Interface Next Hop Add	ress Preference M	fetric		

- **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.

System	Switc	hing	Routing	QoS	Security	6	Monitoring	Maintenance	Help	Index
Management S	Security	Access	Port Authenti	cation Traf	fic Control	Control	ACL			
AC	L	IP /	ACL Configuratio	n						
ACL Wizard		C	urrent Number	of ACL	0					
Basic		~ N	Aaximum ACL		100					
 Advanced 		^								
• IP ACL										
• IP Rules		IP /	ACL Table							
 IP Extended 	Rules				D (1)	-				
 IPv6 ACL 			I IP ACL ID		Rules	туре	- 2			
IPv6 Rules			101							
• IP Binding C	onfiguratio	on								
 Binding Tabl 	e									
VLAN Bindin	ng Table									

- 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.

System	Swite	ching	Routing	QoS	Securit	y M	onitoring	Maintenance	Help	Index
Management S	Security	Access	Port Authenti	ication Traff	ic Control	Control				
AC	L	IP	ACL Configuration	on						
ACL Wizard			Current Number	of ACL	1					
 Basic 		~ I	Maximum ACL		100					
 Advanced 		^								
• IP ACL										
• IP Rules		IP	ACL Table							
 IP Extended 	Rules	-								
• IPv6 ACL			IP ACL ID	F	Rules Typ	e				
• IPv6 Rules			102							
• IP Binding C	onfigurati	on	<u>101</u>	() Exte	ended IP AC	L			
 Binding Table 	е									
• VLAN Bindin	ng Table									

- 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.

ACL Witzard Basic Advanced	ACL	IP Ru	les														-		
P Rules Portanded	ACL Wizard Basic Advanced •IP ACL	ACI	L ID/Nam	ie Dute Te	101	v													
PPA ACL PPA Action Port Start Port End Port PPA Rules No rules have been configured for this ACL	P Rules IP Extended Rules	Exten	Rule	Action	Logging	Assign	Murror	Redirect	Match	Protocol	TCP Flag	Established	Source IP	Source IP	Source	Source L4	Source L4	Source L4	Destinatio
	IPv6 ACL IPv6 Rules	No	rules	have b	een con	figured f	for this	ACL	Comy	13.04		Conservation of the	Addmss	Mask	Part Action	Port	Start Port	End Port	Address
P Binding Configuration	•IP Binding Configuration																		

b. Under IP Extended Rules, in the ACL ID list, select 101.

c. Click Add.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index	
Management Secu	urity Acce	ss Port Authenti	ication Traff	ic Control Cor	trol ACL			46. XV	
ACI		Extended ACL Rule	e Configuration	n(100-199)					
ACL Wizard		ACL ID/Name		101					
 Basic 	~	Rule ID		1					
 Advanced 	^	Action		Per	nit	Egress	Queue	~ (0-6)	
IP ACL IP Rules IP Extended Ru IPv6 ACL IPv6 Rules IP Binding Confi Binding Table Vi AN Binding Table	les guration	Logging Interface Match Every Protocol Type TCP Flag		 Den Disa Mirr Red False TCP URG RST 	y bble or irect	Enab Ignore Ignore	le * (0 to 255) * *	ACK SYN	Clear ∽ Set ∽
	1	Src		● IP A	ddress				

- **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	od Delo	to Ca
ACL	IP Rul	85																
CL Wizard	ACL	ID/Nam	6	102	-1													
asic	*																	
dvanced	~																	
IP ACL	Exten	fed ACL	Rule Ta	ble														
IP Rules					_					1			-	100000	-			
IP Extended Rules	-	Rule	Action	Logana	Assign.	Mirror	Redirect	Match	Protocol	TCP Flag	Established	Source	Source	Source	Source	Source	Source	Destina
IPv6 ACL		ID :		~~35/~3	Queue ID	Interlace	Interface	Every	Type	i en i na		Address	Mask	Port Action	Port	Start Port	End Port	Address
Pv6 Rules	No	rules	have b	een con	figured f	for this	ACL											
P Binding Configuration																		
Binding Table																		

- b. Under IP Extended Rules, in the ACL ID list, select 102.
- c. Click Add.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index	
Management Secur	rity Acces	s Port Authent	ication Tra	ffic Control Con	trol ACL				
	-								
ACL	E	xtended ACL Rul	e Configuratio	on(100-199)					
 ACL Wizard 		ACL ID/Name		102					
• Basic	~	Rule ID		1					
 Advanced 	^	Action		err	nit	Egress	Queue	✓ (0-6)	
• IP ACL				🔘 Den	У			X	
• IP Rules		Logging		💌 Disa	ible	Enab	e		
• IP Extended Rule	es	Interface		Mirr	or		~		
• IPv6 ACL		305 6725		Red	irect		~		
• IPv6 Rules		Match Every		False	*				
• IP Binding Config	uration	Protocol Type		IP	~		(0 to 255)		
 Binding Table 		TCP Flag		URG		Ignore	~	ACK	Ignore 🛩
• VI AN Binding Ta	ible			RST		Ignore	Ý	SYN	Ignore 😽
		Src		O IP A	ddress				

- **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.

ACL		IP Binding Configuration	
ACL Wizard		ACLID 101 -	
Basic	~	Direction	d v
- Advanced		Sequence Number	(1 to 4294967296)
- IP ACL		Contract and a	(110 4604001600)
- IP Rules		Unit 1	
• IP Extended Rules		Ports 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29	31 33 35 37 39 41 43 45 47
· IPV6 ACL			
AID C Dular			
-11-10 140163		2 4 6 8 10 12 14 16 18 20 22 24 26 28 30	32 34 36 38 40 42 44 46 48
P Binding Configurate	an:	Unit 2	
 Binding Table 		Ports 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29	31 33 35 37 39 41 43
 VLAN Binding Table 			
			i w i w i w i w i w i w i w i w i w i w
		2 4 6 8 10 12 14 16 18 20 22 24 26 28 30	32 34 36 38 40 42 44

- **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.

System Swite	g Routing QoS Security Monitorin	g Maintenance Help Index
Management Security	cess Port Authentication Traffic Control Control	
ACL	IP Binding Configuration	
ACL Wizard Basic Advanced IP ACL	ACL ID Direction Sequence Number	102 V Inboand V 2 (1 to 4294967295)
 IP Rules IP Extended Rules IPv6 ACL IPv6 Rules 	Unit 1 Ports 1 3 5 7 9 11 13 15 17 19 21 2 2 4 6 8 10 12 14 16 18 20 22 2	3. 25 27 29 31 33 35 37 39 41 43 45 47
IP Binding Configuration Binding Table VLAN Binding Table	Unit 2 Ports 1 3 5 7 9 11 13 15 17 19 21 2 2 4 9 8 10 12 14 18 18 22 22 2	3 25 27 29 31 33 35 37 30 41 43 4 2 28 30 32 35 37 30 41 43 4 2 28 30 32 35 38 40 42 44

- **b.** Under Binding Configuration, make the following selection and enter the following information:
 - In the ACL ID list, select 102.
 - In the Sequence Number field, enter 2.
- c. Click Unit 1. The ports display.
- d. Click the gray box under port 44.

A check mark displays in the box.

e. Click Apply to save the settings.

Configuring the Switch B

- 1. Create VLAN 40 with IP address 192.168.40.1/24.
 - a. Select Routing > VLAN > VLAN Routing Wizard.

A screen similar to the following displays.

System Switchin	g Routing QoS Security Monitoring Maintenance Help Index
Routing Table IP IPv6	VLAN ARP RIP OSPF OSPFN3 Router Discovery VRRP Multicest IPV6 Multicest
VLAN	VLAN Routing Wizard
VLAN Routing Wizard	Vian ID 40
• VLAW Robing	IP Address 192.168.40.1 Network Mask Designed on A
	L0012012000
	Ports 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47
	Unit 2
	Ports 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43
U	a 7 9 9 10 10 11 11 12 12 12 12 12 12 12 12 12 12 12

- **b.** Enter the following information:
 - In the Vian 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.

System Switching	Routing QoS Security Monitoring Maintenance Help Index
Routing Table IP IPv6	VEWI ARP RIP OSPF OSPFv3 Router Discovery VRRP Multicast IFV6 Multicast
VLAN	VLAN Routing Wizard
VLAN Routing Wizard	Vian ID 60
VLAN Routing	IP Address 192,168,50,1 Network Mask 096,945,950,0
	Unit 1
	Ports 1 2 5 7 9 11 12 15 17 19 21 22 25 27 29 21 33 25 37 39 41 43 45 47
	2 4 6 8 10 12 14 16 18 20 22 24 25 28 30 32 34 36 38 40 42 44 45 48 Unt 2
	Pots 1 2 5 7 9 11 13 15 17 19 21 23 25 27 29 31 23 25 37 39 41 43
	2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44

- **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 ${\bf 25}$ twice until ${\bf U}$ 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.

System Switching	Routing QoS Security Monitoring Maintenance Help Index
Routing Table IP IPv6	VLAN ARP RIP OSPF OSPFV3 Router Discovery VRRP Multicast IPv6 Multicast
VLAN	VLAN Routing Wizard
VLAN Routing Wizard	Vian ID 200
VLAN Routing	IP Address 192.168.200.2
	Network Mask 255 255 2
	Unit 1
	Ports 1 3 5 7 0 11 13 15 17 10 21 23 25 27 29 31 33 35 37 30 41 43 45 47
	Ports 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43
	2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 38 38 40 42 44

- **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.

System	Switching		Routing		QoS	Security	y	Monitorin	9	Mainte	nance	Ho	łp 📗	Index			
Routing Table	IP IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Route	r Discovery	VRR	P. Mult	ticast	IPv6 Mult	icast			_	
Routing	Table	Config	gure Route	9												Lipdale Ac	d
Basic	^		Route Ty	pe	Netw	rork Address		Subnet Mar	śk)	Ne	xt Hop	Address	Pre	ference	Description		
Route Config	uration		Static		- 192	168.100.0		255 255 25	5.0	19	2.168.2	00.1					

- **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.

System Switchin	9	Routing	QoS	Se	ecurity	Monitorii	ng Mainten	nce	Help	Index	1		
touring Table IP IPv6	VLA	ARP P	IP OSP	F OSP	Fv3 Ro	iter Discovery	VRRP Multic	ast IPv6 M	Multicast				
													Update
Routing Table	Cont	igure Routes											
asic .		Route Typ	i N	letwork Ad	deess	Subnet Ma	ank Next	Hop Addres	a P	aference		Description	
Route Configuration		Static	~ 1	02 168 10	1	255 255 2	55.0 102	168 200 2					-
dvanced -		Static	1	92 168 100	0.0	255 255 25	55.0 192	68 200 2	1		-		
					e								
	100	- Chanc			e 19								
		r chanc											
	Lear	ned Routes											
	Lean	ned Routes	ss Subri	at Mask	Protocol	Route Type	Next Hop Interfac	Next Hop	Address	Preference	Metric	1	
	Lear	ned Routes Network Addro 192.168.100.0	ss Subri 255.2	at Mask 55.255.0	Protocol Static	Route Type Static	Next Hop Interfact vlan 200	Next Hop 192 168 2	Address	Preference	Metric 0	1	
	Lear	ned Routes Setwork Addre 92.168.100.0 92.168.200.0	ss Subri 255.2 255.2	at Mask 55.255.0 55.255.0	Protocol Static Local	Route Type Static Connected	Next Hop Interface vian 200 vian 200	Next Hop 192 168 2 192 168 2	Address 200.2 200.1	Preference 1 0	Metric 0 1		
	Lear	ned Routes Network Addr 92 168 100 0 92 168 200 0	55 Subra 255.2 255.2	et Mask 55.255.0 55.255.0	Protocol Static Local	Route Type Static Connected	Next Hop Interfact vlan 200 vlan 200	Next Hop 192 168 2 192 168 2	Address 200.2 200.1	Preference 1 0	Metric 0 1		
	Lear	ned Routes Interfect Addre 92 168 200 0	5 Subri 255.2 255.2	at Mask 55.255.0 55.255.0	Protocol Static Local	Route Type Static Connected	Next Hop Interfact vian 200 vian 200	Next Hop 192 168 2 192 168 2	Address 200.2 200.1	Preference 1 0	Metric 0 1		

- **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 24. 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) (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) (Interface-vlan 24)#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) (Interface-vlan 48)#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)#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.

System	Switching	Routing	QoS Secu	rity Monitoring	Maintenance	Help Index	
Routing Table	IP IP/6	VIAN ARP RIP	OSPF OSPFV3	Router Discovery	/RRP Multicast IP	v6 Multicast	
VLA	N	VLAN Routing Wizan	d				
VLAN Routing	Woxard	Vlan ID			-		
VLAN Routing		IP Address			192.168	3.24.1	
		Network Mask			265.255	5,255.0	
		Unit 1					
		Ports 1 3	5 7 9 11 13	15 17 19 21 23	25 27 29 31 33	35 37 39 41 43 45	47
				ininini m			
		2 4 8	5 8 10 12 14	16 18 20 22 24	26 28 30 32 34	36 38 40 42 44 46	48
		Unit 2					~
		Ports 1 3 5	5 7 9 11 13	15 17 19 21 23	25 27 29 31 33	35 37 39 41 43	
		لبلبا					

- **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.

System Switch	ng Routing QoS Security Monitoring Maintenance Help Index
Routing Table IP IPv	5 VLAN ARP RIP OSPF-OSPF-3 Router Discovery VRRP Multicast IPv6 Multicast
VLAN	VLAN Routing Wizard
VLAN Routing Wizard	Vian ID
VLAN Routing	P Address 400 400 40 4
	Network Mask 255,255,0
	Unit 1
	Ports 1 2 5 7 9 11 13 15 17 19 21 22 25 27 29 31 23 35 37 39 41 43 45 47
	2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48
	Unit 2
	Ports 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 23 35 37 29 41 43
	2 4 6 8 10 12 14 16 18 20 22 24 28 38 30 32 34 36 38 40 42 44

- **b.** Enter the following information:
 - In the VIan 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.

System	Sv	vitching		Routing		QoS	Securit	y 🛛	Monitoring)	Maintenance	Help	Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router (Discovery	VRRP	Multicast	IPv6 Multicast	
IP			IP Con	figuration									
• Basic		^	Defa	ult Time	to Live				64				
 IP Configurat 	ion		Rout	ing Mode	9				Enable	le 🔘 Disa	able		
 Statistics 			ICMF	P Echo F	eplies				Enable	le 🔘 Disa	able		
 Advanced 		~	ICMF	P Redired	ts				Enable	le 🖲 Disa	able		
			ICMF	P Rate Li	mit Int	erval			1000		(0 to 21	147483647 ms)	
			ICMF	P Rate Li	mit Bu	rst Size			100		(1 to 20	00)	
			Maxi	imum Ne	xt Hop	s			4				
			Maxi	imum Ro	utes				12288				
			Sele	ct to con	figure	Global De	fault Gatewa	у					
			Glob	al Defaul	t Gate	way			0.0.0.0				

- **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.

System	Switching	Routing	QoS	Security	Mo	nitoring	Maintenance	Help	Index
Management S	Security Acc	ess Port Authentie	cation Traf	fic Control C	ontrol /	ACL			
AC	۶L	IP ACL Configuratio	n						
ACL Wizard		Current Number of	of ACL	0					
Basic	*	Maximum ACL		100					
 Advanced 	~								
• IP ACL									
• IP Rules		IP ACL Table							
 IP Extended 	Rules			Pulae T	ine.				
- IPv6 ACL		101		rules ()	pe				
 IPv6 Rules 		101							
IP Binding C	Configuration								
 Binding Tab 	le								
VLAN Bindi	ng Table								

- 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.

System	Swite	ching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	ecurity	Access	Port Authent	ication Traffic Co	ontrol Control	ACL			
AC	L	IP /	ACL Configuration	on					
ACL Wizard		(Current Number	of ACL					
Basic		× N	Aaximum ACL	1	00				
 Advanced 		~							
• IP ACL									
• IP Rules		IP /	ACL Table						
 IP Extended 	Rules			2.1					
• IPv6 ACL			IP ACL ID	Rules	s Type				
 IPv6 Rules 			102	0	Estandad ID	ACL			
• IP Binding C	onfigurati	on	U <u>101</u>	U	L'Atendeu IF	AUL			
 Binding Table 	e								
• VLAN Bindin	ig Table								

- 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.

System Switching		Routing	QoS S	Security	Monitoring	Maintenance	Help	Index
Management Security Acc	ess	Port Authentic	cation Traffic Co	introl Control				
ACL	IP AC	L Configuratio	n					
ACL Wizard	Cur	rent Number o	f ACL					
Basic v	Max	kimum ACL	1					
Advanced ^								
• IP ACL								
• IP Rules	IP AC	L Table						
• IP Extended Rules	_			W.	_			
· IPv6 ACL		IP ACL ID	Rules	Туре				
IPv6 Rules		103						
IP Binding Configuration		<u>101</u>	0	Extended IP	ACL			
Binding Table		102	0	Extended IP /	ACL			
• VI AN Binding Table								
vicinity rable								

- 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.

oystem on	itching	Routing	g QoS	Security	Monitoria	9 N	aintenance	Hel	p Inde	K			
Management Security	Access	Port Aut	hentication Traf	fic Control	Control AG				10	10			
ACL	p	Rules											
ACL Wizard		ACL ID/Nam	ne 101										
Basic	4		101										
Advanced	-												
+IP ACL	Ev	tandad ACI	Dvia Tabla										
•IP Rules	-	rended Aou	. Hore Table					_	_	_			_
		Rule	Action Looping	Assign	Mirror Redire	ct Match	Protocol	TOP Fina	Established	Source	Source	Source	Sourc
• IP Extended Rules				Queue ID	Interface Interfa	te Every	Туре	area a read	Latanana	Address	Mask	Port Action	Port
IP Extended Rules IPv6 ACL		- 10											
IP Extended Rules IPv6 ACL IPv6 Rules	1	No rules	have been cor	figured f	or this ACL					A MARINE MARK		Provide States	C. MIL
PLExtended Rules IPv6 ACL IPv6 Rules IP Binding Configura	ation	No rules	have been cor	ifigured f	or this ACL					- Martin Grade	10000		Come.
P Extended Rules PV6 ACL IPv6 Rules IP Binding Configura Binding Table	tion	No rules	have been cor	ufigured f	or this ACL					T Sala Cal		Contraction of	C. Carlo

- b. Under IP Extended Rules, in the ACL ID field, select 101.
- c. Click Add.

System Switching Management Security Ac	Routing QoS cess Port Authentication Tr	Security Manitoring	Maintenance Help	Index	
ACL.	Extended ACL Rule Configurat	tion(100-199)			
ACL Wizard	ACL ID/Name	101			
Basic ~	Rule ID	1			
Advanced •	Action	Permit	Egress Queue	- (0-8)	
IP ACL IP Pole	Logging	 Deny Disable 	Enable	1	
IP Extended Rules	Interface	 Mirror Redirect 			
IPv6 Rules	Match Every Protocol Type	False ~	(0 to 255)		
IP Binding Configuration Binding Table	TCP Flag	URG	tgnore ~	ACK SYN	Ignore - PSH FIN
VLAN Binding Table	Src	IP Address Address	spices s		
	Src L4	Port	Other ~	Equal ~	(0 to 65535)
	Dst	 IP Address 	192.168.24.0	Other 4 0.0.0.255	(0 to 65535) End Port

- **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.

ACL	IP Rul	03														17		347
ACL Wizard	ACL	D/Nam	ie .	102	•													
Basic ·																		
•IP ACL	Exten	ded ACL	. Rule Tai	ble														
IP Rules IP Extended Rules IP(6.AC)		Rule ID	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Match Every	Protocol Type	TCP Flag	Established	Source IP Address	Source IP Mask	Source L4 Port Action	Source L4 Port	Source L4 Start Port	Source L4 End Port	Destinat IP Address
• IPv6 Rules	No	rules	have b	een con	figured f	for this	ACL			-	_	ACCULATION OF	190392901	ALCONTRACTOR OF	CONTRACT OF	Designment of the second s	ANN SCANTAL	0000104094
IP Binding Configuration																		
Binding Table																		

- b. Under IP Extended Rules, in the ACL ID field, select 102.
- c. Click Add.

A screen similar to the following displays.

System Switching	Routing QoS	Security Monitoring	Maintenance Help	Index	
ACL	Extended ACL Rule Configura	tion(100-199)			
ACL Wizard	ACL ID/Name	102			
- Basic -	Rule ID	1			
Advanced	Action	@ Permit	Egress Queue	< (0-6)	
•IP ACL	Logging	 Deny Disable 	O Enable	1	
P Extended Rules	Interface	Mirror Redirect			
•IPv6 Rules	Match Every Protocol Type	False *	(0 to 255)		
IP Binding Configuration Binding Table	TCP Flag	URG	Ignore +	ACK	Ignore - PSH
VLAN Binding Table	Src	IP Address	Ignore *		ignoro ·
	Stc L4	 Host Port 	Other +	Equal *	(0 to 65535)
		Range	Start Port	Other ~	(0 to 65535) End Port
	Dst	IP Address	192 168 48 0	0.0.0.255	MPCPGGGGGG

- **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.

																Ad	dd Dele	te Can
ACL	IP Rule	65																
ACL Wizard	ACL	D/Nam	ie.	103	v													
Basic 👻																		
Advanced A																		
IP ACL	Extent	ded ACL	Rule Tal	ble														
· IP Rules	_			-	_			-				_		-			-	
· IP Extended Rules		Rule	Action	Looping	Assign	Mirror	Redirect	Match	Protocol	TCP Flan	Established	Source	Source	Source	Source	Source	Source	Destination
· IPv6 ACL		ID	0.000		Queue ID	Interface	Interface	Every	Туре	10.1103	CTATION.	Address	Mask	Port Action	Port	Start Port	End Port	Address
·IPv6 Rules	No	rules	have b	een con	figured t	for this	ACL.											
·IP Binding Configuration																		
Binding Table																		

- b. Under IP Extended Rules, in the ACL ID field, select 103.
- c. Click Add.

A screen similar to the following displays.

Management Security A	ccess Port Authentication	Traffic Control Control Am	T	N	
ACL.	Extended ACL Rule Configura	ation(100-199)			
ACL Wizard	ACL ID/Name	103			
Basic	 Rule ID 	1			
Advanced	- Action	ermit	Egress Queue	× (0-6)	
• IP ACL	Logging	 Deny Disable 	Enable		
IP Extended Rules IP/6 ACL	Interface	Mirror Redirect	+ +		
IPv6 Rules IP Binding Configuration	Protocol Type	False ~	(0 to 255)	2.7417	neu
Binding Table M AM Binding Table	TCP Flag	RST	Ignore ~	SYN	Ignore V FIN
- vorw circling table	Sirc	 IP Address Host 			
	Src L4	 Port Range 	Other ~ Start Port	Equal •	(0 to 65535) (0 to 65535) End Pol
	Dst	IP Address		Control -	1. 1. 44444

- **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.

		IP Binding Configuration	
ACL Wizard		ACLID 400 c	
Basic	٠	Direction	
Advanced	+	Sequence Number	
·IP ACL		1 (1 to 4294967295)	
•IP Rules		Unit 1	
·IP Extended Rules		Porta 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47	
HP/6 ACL			
AID C Dulas			
- IP-VO POINTS		2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48	
• IP Binding Configuratio	•	Unit 2	
 Binding Table 		Date 1 3 5 7 9 41 13 16 17 19 21 23 26 27 29 31 33 35 37 39 41 43	

- **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.

System Switching Management Security Acc	Routing QoS Security Monitoring Maintenance Help Index
ACL	IP Binding Configuration
ACL Wizard Basic Advanced IP ACL IP Rules	ACL ID 10 10 10 10 10 10 10 10 10 10 10 10 10
IP Extended Rules IP/6 ACL IP/6 Rules IP 6 Rules	Ports 1 3 5 7 9 11 13 15 17 19 21 25 25 27 29 11 33 35 37 39 41 43 45 47 2 4 6 9 10 12 14 18 18 20 22 24 28 28 29 20 22 34 35 30 40 42 44 45 48
Binding Table VLAN Binding Table	Unit Z Ports 1 3 5 7 0 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 2 4 6 8 10 12 14 15 10 20 22 24 25 20 30 32 34 35 38 40 42 44

- **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.

System Sw	itching	F	touting	QoS	Security	Monitoring	Maintenance	Help Index	
Management Security	Acc	ess Po	et Authon	tication T	affic Control	Control AGL			
ACL		IP Bindie	an Confin	ration					
ACL Wizard		ACLE	-y comp	and the second			(and the second		
Basic		Directio					103 4		
Advanced		Camina	ana Musada				Inbound +		
· IP ACL		Sedner	ice nume				2	(1 to 4294967295)	
*IP Rules		💼 Ur	it t						
•IP Extended Rules		Ports	1 3	5 7 9	11 13 15	17 19 21 23	25 27 29 31 3	3 35 37 39 41 43 45 4	7
+ IPv6 ACL									
· IPv6 Rules			ЧU					<u>,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,</u>	
·IP Binding Configura	tion	-	2 4	0 8 1	12 14 10	18 20 22 24	26 28 30 32 3	4 30 38 40 42 44 46 4	
Binding Table		U	11.2						
AM AN Diedes Table		Ports	1 3	5 7 9	11 13 15	17 19 21 23	25 27 29 31 3	3 35 37 39 41 43	
- view cinding race							┉┉	┥╾┥╾┥╾┥╾	
		U 2	-62 B.	0 0 3	1 16 14 10	10 60 22 24	20 20 30 32 3	a 30 30 au 42 44	

- **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.

System	Switch	ing	Routing	QoS	Seci	irity	Monitoring	Maintenance	Help	Index
Management S	ecurity /	Access	Port Authenti	cation Tra	ffic Contro	l Control				
AC	Ē	MA	C ACL							
• ACL Wizard		С	urrent Number	of ACL	0					
 Basic 		^ N	laximum ACL		100					
• MAC ACL										
•MAC Rules										
 MAC Binding Configuration 	9	MA	C ACL Table	70						
Binding Table	e	(Name	1	Rules	Direction				
 Advanced 		~	acl_bpdu							
				40						

- b. In the Name field, enter acl_bpdu.
- c. Click Add to create ACL acl_bpdu.
- 2. Create a new rule that is associated with the ACL acl_bpdu.
 - a. Select Security > ACL > MAC ACL > MAC Rules.

	0	_	35				2				<u></u>			_		5
System	Swite	ching		Routing	Qo	S	Secu	ity	M	onitoring	Ma	intena	ance	Help	Index	
Management S	ecurity	Acce	iss	Port Authe	entication	Tra	affic Control	Contro								
AC	t _{ra}		Rules													
ACL Wizard			ACL	Name	-	cl bo	du x									
• Basic		~			a	"_ob	uu -									
• MAC ACL																
MAC Rules			Rule T	able												
 MAC Binding Configuration 					1. July 1. Jul		Assian	Mirror		Redirect	Match			a	 No. 2012 	Destination MAC
Binding Table	e			ID	Action		Queue Id	Interface		Interface	Every		CoS	Destinati	on MAC	Mask
Advanced		~		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 another rule that is associated with the ACL acl_bpdu.
 - a. Select Security > ACL > MAC ACL > MAC Rules.

System	Swite	ching		Routing	QoS	Secu	rity 🚺 🕅	lonitoring	Maint	enance	Help	Index	
Management S	ecurity	Acce	985	Port Auther	tication Tra	affic Control	Control						
ACI	<u>k</u> e	4	Rules										
ACL Wizard			ACI	Name	acl br	du 👻							
 Basic 		^			1.000=0								
• MAC ACL													
MAC Rules			Rule	Table									
 MAC Binding Configuration 	3			ID	Action	Assign	Mirror	Redirect	Match	CoS	Destinati	on MAC	Destination MAC
Binding Table	Э			10	/ Action	Queue Id	Interface	Interface	Every	000	Destinati		Mask
 Advanced 		~		2	Permit 👻		×	¥		×			
				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 Permit.

- **c.** Click the **Add** button.
- **4.** Apply the ACL acl_bpdu to port 2.
 - a. Select Security > ACL > MAC ACL > MAC Binding Configuration.

ACL Wizard ACL ID acL bods ~ Image: ACL ID acL bods ~ Image: Image: Im	ACL	MAC Binding Configuration		
MAC ALL Sequence Number 1 (1 to 4294967295) MAC Bules Unit 1 Ports 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 23 35 37 39 41 43 Ports 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 23 35 37 39 41 43 Ports 1 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2	VCL Wizard Basic	ACL ID Direction	acl_bpdu ❤ Inbound ❤	
Construction Ports 1 5 7 9 11 15 17 19 21 23 25 27 29 31 33 35 37 34 43 Binding Table Image: Table </td <td>MAC ACL</td> <td>Sequence Number</td> <td>1 (1 to 4294967295)</td> <td></td>	MAC ACL	Sequence Number	1 (1 to 4294967295)	
	MAC binding Configuration Binding Table	Ports 1 3 5 7 9 11 13 15 17	19 21 23 25 27 29 31 33 35 37 39 41 43	

- **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.

Managed Switches



Figure 25. 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
            Rules Direction
ACL ID/Name
                         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
 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.

System	Switch	ing	Routing	QoS	Securit	y I	Aonitoring	Maintenance	Help	Index
Management S	Security A	Access	Port Authenti	cation Trat	ffic Control	Control				
AC	L	IP A	CL Configuratio	in						
ACL Wizard		Ci	urrent Number o	of ACL	1					
•Basic		~ M	aximum ACL		100					
 Advanced 		~								
• IP ACL										
• IP Rules		IP A	CL Table							
• IP Extended	Rules		-			_	ň			
IPv6 ACL		L	J IP ACL ID		Rules	Туре				
IPv6 Rules			monitorHos	t						
• IP Binding C	onfiguration									
 Binding Tabl 	e									
• VLAN Bindir	ng Table									

- b. In the IP ACL ID field, enter monitorHost.
- c. Click Add to create ACL monitorHost.

System	Switch	ing	Routing	QoS	Securi	y	Monitoring	Maint	enance	Help	Index
Management S	ecurity a	Access	Port Authenti	cation Traf	fic Control	Control					
ACI	L.	IP A	CL Configuratio	n							
ACL Wizard		Cu	rrent Number o	of ACL	2		17 H				
Basic		∽ Ma	aximum ACL		100						
 Advanced 		^									
• IP ACL											
• IP Rules		IP A	CL Table								
 IP Extended 	Rules										
· IPv6 ACL			I IP ACL ID		Rules Typ	e					
 IPv6 Rules 			l		D Dies						
• IP Binding C	onfiguration	1	monitornost		J	IEU IF ACI					
Binding Table	е										
• VLAN Bindin	g Table										

- 2. Create a rule to match host 10.0.0.1 in the ACL monitorHost.
 - a. Select Security > ACL > Advanced > IP Extended Rules.

System	Switcl	ning	Routing	g G	loS	Security	y i	Monitoring	M	aintenance	Hel	o Inde:	<]		
Management Se	curity	Access	s Port Aut	hentication	Traffi	c Control	Control	ACL.							
ACL		IF	Rules												
ACL Wizard			ACL ID/Nan	ne	monit	orHost ~									
Basic		~													
 Advanced 		^													
• IP ACL		E	xtended ACI	Rule Tabl	e										
• IP Rules			1		2						(8	120	12
• IP Extended I	Rules		Rule	Action I	_ogging	Assign	Mirror	Redirect	Match	Protocol	TCP Flag	Established	Source IP	Source	Source L4
• IPv6 ACL						Queue ID	птепасе	Internace	Every	туре	5 -		Address	Mask	Port Action
IPv6 Rules			No rules	have be	en con	figured	for thi:	5 ACL							
• IP Binding Co	nfiguratio	n													
 Binding Table 															
• VLAN Binding	y Table														

b. Click **Add**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index	
Management S	Security Access	Port Authenti	cation Tra	ffic Control Cont	rol ACL				
AC	L Ex	tended ACL Rule	e Configuratio	on(100-199)					
ACL Wizard	1	ACL ID/Name		monitor	Host				
 Basic 	~ [Rule ID		1					
 Advanced 	~ /	Action		Pern	nit	Egress	Queue	× (0-6	6)
• IP ACL				O Den	/	_			<i>.</i>
• IP Rules	I	_ogging		Olsa	ble	🔘 Enab	le		
 IP Extended 	I Rules	nterface		Mirro	NF	1/0/19	*		
• IPv6 ACL				Redi	rect		~		
• IPv6 Rules	1	Match Every		False	¥				
• IP Binding C	Configuration	Protocol Type		IP	~		(0 to 255)		
Binding Tab	lo	FCP Flag		URG		Ignore	~	ACK	
	T.U.			RST		Ignore	*	SYN	
• VLAN BINDI	ng lable	Src		IP A	ddress	10.0.0.1		0.0.0.0	
				 Host 					
VLAN Bindir	ng Table s	Src		 IP A Host 	ddress	lgnore 10.0.0.1	<u> </u>	0.0.0.0	

- 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.

	IP	Rule	3													
ACL Wizard Basic Advanced IP ACL	- -	ACL	ID/Nam	ne . Rule Tat	monit	orHost ~										
IP Rules IP Extended Rules IP/6 ACL			Rule ID	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Match Every	Protocol Type	TCP Flag	Established	Source IP Address	Source IP Mask	Source L4 Port Action	Source L4 Port
IPv6 Rules IP Binding Configuration Binding Table			1	Permit			1/0/19		False	4 (IP)			10.0.0.1	0.0.0.0		

b. Click Add.

A screen similar to the following displays.

System	Swite	hing	Routing	QoS	Security	Monitoring	Maintenance	Help	Index	
Management S	Security	Acces	Port Authent	ication Tra	ffic Control Con	itrol ACL			19. AR	
AC	ïL.	E	xtended ACL Rul	e Configuratio	on(100-199)					
ACL Wizard			ACL ID/Name		monito	rHost				
Advanced		^	Action		2	mit	Egress	Queue	✓ (0-6)	
IP ACL IP Rules			Logging		⊚ Den ⊚ Disa	y able	😑 Enab	le		
• IP Extended	l Rules		Interface		💿 Mirr 🔘 Red	or irect		* *		
IPv6 ACL IPv6 Rules			Match Every		True	~				
IP Binding C Binding Tab	Configuratio	on	TCP Flag		URG	×	Ignore	(U to 255) ~	ACK	Ignore ~
• VLAN Bindi	ng Table		Src		RST	ddress	Ignore	×	SYN	Ignore 🜱
					🕔 Hos	t				

- 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.

System	Switching	9	-	Routing		QoS	Security	/ Th	Nonitoring	M	aintenance	Hel	nde	s			
Management Secu	inty Ac	cess	P	Port Aut	henticati	on Traff	ic Control	Control	ACL			- 22					
ACL		IP	Rule	15													
ACL Wizard		1	ACL	ID/Nan	ne	monit	orHost ~										
Basic		•															
 Advanced 	-	4															
*IP ACL		E	tend	led ACI	. Rule Ta	ble											
*IP Rules			_	-	-	-				_	-	1		-		1	-
•IP Extended Rule	les:			Rule	Action	Logana	Assign	Minor	Redirect	Match	Protocol	TCP Flag	Established	Source	Source P.	Source L4	Source L4
· IPv6 ACL				10			Cicene IC.	anteriac, e	middingen	coury	1.ypa			Address	Mask	Port Action	Port
IPv6 Rules				1	Permit			1/0/19		False	4 (IP)			10.0.0.1	0.0.0.0		
+IP Binding Config	guration			2	Permit					True							
*Binding Table																	
+VLAN Binding Ta	able																

- 4. Bind the ACL with interface 1/0/1.
 - a. Select Security > ACL > Advanced > IP Binding Configuration.

ACL		P Bindi	ng Co	nligura	tion																				
ACL Wizard Basic Advanced IP ACL	• •	ACL IE Directi Seque	on nce N	umber										mo Inb 1	nitorHc aund	st ~	1 to 4	2949	57295	i.			 	 	_
IP Rules IP Extended Rules IPv6 ACL IPv6 Rules		Ports	nit 1	3 5	7	9	11	13 14	5 1	7 19	21	23	25	27	29 3'	33	36	37	39		45	47			
P Binding Configuration Binding Table VLAN Binding Table	P .	Ports	nit 2 1	3 5	7	9	11	13	5 1	7 19	21	23	25	27	29 31	33	35	37	39	(1 4)					
			2	4 0	JL	10	12	14	6 1	8 20	22	24	26	28	30 33	34	36	38	40	42 44					

- 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.

ACL Redirect

This feature redirects a specified traffic stream to a specified interface.



Figure 26. 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
                                  VLAN(s)
                        Interface(s)
_____ _____
                inbound
           2
redirectHTTP
                        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
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.

System	Swite	hing	Routing	QoS	Securit	у	Monitoring	Maintenance	Help	Index
Management S	Security	Access	Port Authenti	cation Tra	ffic Control	Control				
AC	Ĺ	IP /	ACL Configuratio	on						
ACL Wizard		0	Current Number	of ACL	1					
 Basic 		~ N	laximum ACL		100					
 Advanced 		^								
• IP ACL										
• IP Rules		IP ,	ACL Table							
 IP Extended 	Rules						1			
• IPv6 ACL				-1	Rules	Type	-8			
• IPv6 Rules			redirectHTT	P						
• IP Binding C	onfiguratio	on								
 Binding Tabl 	е									
VLAN Bindin	ng Table									

- b. In the IP ACL field, enter redirectHTTP.
- c. Click Add to create the IP ACL redirectHTTP.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	ecurity Access	Port Authenti	cation Traffic	Control Con	trol ACL			
ACI	L IP	ACL Configuration	on					
ACL Wizard		Current Number	of ACL	2				
 Basic 	~	Maximum ACL		100				
 Advanced 	~							
• IP ACL								
• IP Rules	IP	ACL Table						
• IP Extended	Rules				_			
• IPv6 ACL		IP ACL ID	Ri	iles Type				
 IPv6 Rules 				News d ID	ACI			
• IP Binding Co	onfiguration		E V	Named IP	AUL			
Binding Table	9							
• VLAN Bindin	g Table							

- 2. Create a rule to redirect HTTP traffic.
 - a. Select Security > ACL > Advanced > IP Extended Rules.

System Switc	hing	Rout	ing	QoS	Securit	y 1	Monitoring	M	aintenance	Hel	p Inde	x		
Management Security	Acces	s Port A	uthenticati	on Traff	ic Control	Control	ACL							
<u>.</u>														
ACL	IF	P Rules												
ACL Wizard		ACL ID/N	ame	redire	ctHTTP ¥									
• Basic	~													
Advanced	~													
• IP ACL	E	xtended A	CL Rule Ta	ble										
• IP Rules		-					1	1	1			last the second		- 55
IP Extended Rules		Rul	e Action	Logging	Assign	Mirror	Redirect	Match	Protocol	TCP Flag	Established	Source	Source	Source L4
• IPv6 ACL		- ID		35 - 3	Queue ID	Interface	Interface	Every	Туре	3		Address	Mask	Port Action
• IPv6 Rules		No rule	s have b	een con	figured	for this	ACL							
• IP Binding Configuration	on													
 Binding Table 														
 VLAN Binding Table 														

b. Click **Add**.

System Switch	ing Routing	QoS Security	Monitoring	Maintenance	Help	Index		
Management Security	Access Port Authent	tication Traffic Control C	ontrol AG					
ACL.	Extended ACL Ru	le Configuration(100-199)						
ACL Wizard	ACL ID/Name	redir	ectHTTP					
Basic	 Rule ID 	1						
Advanced	 Action 	* P	ermit	Egress	Queue	~ (0-6)		
IP ACL IP Rules IP Extended Rules IPv6 ACL IPv6 ACL IPv6 Rules IP Binding Configuration Binding Table VLAN Binding Table	Logging Interface Match Every Protocol Type TCP Flag Sac	D D T D T D T T T T T C R R R R R R R R	eny isable edirect se - S S F Address	Enabl 1/0/19 Ignore Ignore	le v (0 to 255) v v	ACK SYN	Ignore Ignore	▼ PSM ▼ FIN
	Src L4 Dst	● H ● P ● R ● F	ost ont ange * Address	Other Start P	~] fort	Equal Other ~	•]	(0 to 65535) (0 to 65535) End Port

- c. In the Rule ID field, enter 1.
- d. In the protocol field, select www-http.
- e. For Action, select the Permit radio button.
- f. In the Redirect Interface list, select 1/0/19.
- g. In the Dst L4 Port list, select http.
- **h.** Click **Apply**. The Extended ACL Rules screen displays, as described in the next step in this procedure.
- 3. Create a rule to match every other traffic.
 - a. Select Security > ACL > Advanced > IP Extended Rules.

ACL	IP I	Rule	2													
ACL Wizard Basic Advanced •IP ACL	- Ext	CL I	ID/Nam	ie . Rule Tal	redire	ctHTTP ¥										
IP Rules IP Extended Rules IP/6 ACL		•	Rule ID	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Match Every	Protocol Type	TCP Flag	Established	Source IP Address	Source IP Mask	Source L4 Port Action	Source L4 Port
•IPv6 Rules			1	Permit				1/0/19	False	6 (TCP)		False				

b. Click **Add**.

A screen similar to the following displays.

System Switch	hing	Routing	QoS	Security	Monitoring	Maintenance	Help	index			
Management Security	Acc	rss Port Authentic	ation Traff	ic Control Cor	trol AlaL						
ACL		Extended ACL Rule	Configuration	n(100-199)							
ACL Wizard		ACL ID/Name		redirec	TTP						
Basic	×	Rule ID		2							
Advanced	^	Action		(e) Per	mit	Egres	s Queue	~ (0.6)			
- IP ACL				O Der	y.						
• IP Rules		Logging		- Dis	sble	Enal	ale				
• IP Extended Rules		Interface		() Min	57		*				
· IPv6 ACL				Rec	inect						
• IPv6 Rules		Match Every		True	*						
•IP Binding Configuratio	n	Protocol Type		P			(0 to 255)	(1) (A) (1)			
Binding Table		TCP Hag		URG		lignore		ACK	Ignore -		PSH
VLAN Binding Table		1.00		RST		lignare	*	SYN	lgnore 🛩		FIN
		Stc		11 IP 4	ddress						
		Sec.1.4		Pios Dec	1						
		OIC L4		- P'00		Other	~	Equal 4		(0 to 65535)	-
				Rar	ge	Start F	110*	Other ~		(0 to 65535)	End Port

- 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.

ACL	ip Rul	63													
ACL Wizard	ACL	ID/Nan	ne	redire	ctHTTP ~										
Basic	*														
Advanced	•														
*IP ACL	Exten	4.4 AP1	Dute Tel	bla.											
•IP Roles	Exten	Sec Aug	- Poper sat	uie.								_			
• IP Extended Rules		Rule	Action	Lansing	Assign	Mirror	Redirect	Match	Protocol	TCP Film	Established	Source	Source	Source	Source
+IPv6 ACL		ID .	Chamber -	e-Minula	Queue ID	Interface	Interface	Every	Туре	inter i find		Address	Mask	Port Action	Port
	1	1	Permit			1	1/0/19	False	6 (TCP)	-	False				
IPv6 Rules			Dermit					True							
IPv6 Rules IP Binding Configuration	8	2	1. Givint												
IPv6 Rules IP Binding Configuration		2	1. Giver												

- 4. Bind the ACL with interface 1/0/1.
 - a. Select Security > ACL > Advanced > IP Binding Configuration.

System Swite	ching		Routing	E I	QoS		Secu	ŧγ	M	onitori	ng	N	lainten	ance		Holp		Ind	ex	1-			
Management Security	Acc	ess P	ort Auti	hentica	tion	Traffic	Control	Con	trol	ACB.													
A/1																							
ALL	14	IP Bind	ng Con	ngurat	ion																		
ACL Wizard		ACL IE	Ĵ.									1	direct	HTTP	÷								
Basic	*	Directi	on										hound										
Advanced	÷	Seque	nce Nu	mber								1	ibouile.		15.00	12010	67206	17					
· IP ACL												1.5			11.14	42.04		2					
• IP Rules		U 💼	nit t																				
• IP Extended Rules		Ports.	1	3 5	7	9 11	13	15 17	19	21	23 25	27	29	31 3	3 3	5 37	39	41	43 4	5.4	7		
+IPv6 ACL			L)[1				1	JL.			
ID-C Dulas				л.,																JL.			
Sinve Roles	1	-	2	4 6	8	10 12	14	16 18	20	22	24 26	28	30	32 3	14 3	6 38	40	42	44 4	6 4	8		
• IP binding Conliguration	on	U 💼	nit 2																				
 Binding Table 		Ports	1 :	3 5	7	9 11	13	15 17	19	21	23 25	27	29	31 3	3 3	5 37	39	41	43				
 VLAN Binding Table 																							
												1			Т								
			2 1	\$ 6	8	10 12	14	16 18	20	22	24 28	28	30	32 3	14 3	6 38	40	42	44				

- 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.

Configure a Management ACL

A management ACL lets you control access to the switch. You can permit specific hosts to access the switch and deny access to all other hosts. You can also specify a specific access method for a permitted host. For example, you can specify that a host can access the switch over a Telnet connection only

The following example shows how to configure a management ACL.

Example 1: Permit Any Host to Access the Switch Through Telnet or HTTP:

Permit any host to access the managed VLAN IP address of 169.254.100.100 through a Telnet or HTTP connection:

(Netgear	Switch)	(Config)#ip access-list acl_for_cpu
(Netgear	Switch)	(Config-ipv4-acl)#permit tcp any 169.254.100.100 0.0.0.0 eq telnet
(Netgear	Switch)	(Config-ipv4-acl)#deny tcp any any eq http
(Netgear	Switch)	(Config-ipv4-acl)#permit tcp any 169.254.100.100 0.0.0.0 eq http
(Netgear	Switch)	(Config-ipv4-acl)#deny tcp any any eq http
(Netgear	Switch)	(Config-ipv4-acl)#deny every
(Netgear	Switch)	(Config-ipv4-acl)#exit
(Netgear	Switch)	(Config)#ip access-group acl_for_cpu control-plane

Example 2: Permit a Specific Host to Access the Switch Through SSH Only

Permit a specific host access the switch over an SSH connection only.

```
(Netgear Switch) (Config)#ip access-list acl_for_cpu
(Netgear Switch) (Config-ipv4-acl)#permit tcp 10.100.5.13 0.0.0.0 any eq ssh
(Netgear Switch) (Config-ipv4-acl)#deny tcp any any eq ssh
(Netgear Switch) (Config-ipv4-acl)#permit every
(Netgear Switch) (Config-ipv4-acl)#exit
(Netgear Switch) (Config)#ip access-group acl_for_cpu control-plane
```

Configure IPv6 ACLs

This feature extends the existing IPv4 ACL by providing support for IPv6 packet classification. Each ACL is a set of up to 12 rules applied to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and can apply to one or more of the following fields within a packet:

- Source IPv6 prefix
- Destination IPv6 prefix
- Protocol number
- Source Layer 4 port
- Destination Layer 4 port
- DSCP value
- Flow label

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

Managed Switches



Figure 27. IPv6 ACLs

The script in this section shows you how to set up an IPv6 ACL with the following three rules:

- Rule-1. Permits 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:COAB:AC11::/64
2001:DB8:COAB:AC14::/64
(Netgear Switch) (Config-ipv6-acl)# permit tcp 2001:DB8:COAB:AC11::/64
2001:DB8:COAB:AC13::/64 eq telnet
(Netgear Switch) (Config-ipv6-acl)# permit tcp 2001:DB8:COAB:AC11::/64 any eq http
```

 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
Rule Number: 2
Action..... permit
Destination IP Address...... 2001:DB8:COAB:AC13::/64
Destination L4 Port Keyword..... 23(telnet)
```

Rule Number: 3Action.....Protocol.....6(tcp)Source IP Address....2001:DB8:C0AB:AC11::/64Destination 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.

System	Switching		Routing	QoS	Secu	irity	Monitoring	Maintenance	Help	Index
Management S	ecurity Ac	cess	Port Authenti	cation Traf	fic Contro	I Contro	I ACL			
AC	Ĺ.	IPv6	Configuration							
ACL Wizard		Cu	Irrent Number	of ACL	0					
 Basic 	~	Ma	aximum ACL		100					
 Advanced 	~									
• IP ACL										
• IP Rules		IPv6	ACL Table							
• IP Extended	Rules					-				
IPv6 ACL			I IPV6 ACL		Rules	Туре				
• IPv6 Rules			ipv6-acl			IPv6 ACL				
• IP Binding C	onfiguration									
Binding Table	e									
• VLAN Bindin	ig Table									

c. Click Add.

System	Switc	hing	Routing	QoS	Securi	ty	Monitoring	Maintenance	Help	Index
Management S	Security	Access	Port Authenti	cation Tra	fic Control	Control				
AC	L	IP	6 Configuration							
ACL Wizard			Current Number	of ACL	1		1/4			
Basic		~	Maximum ACL		100					
 Advanced 		^								
• IP ACL										
• IP Rules		IP	6 ACL Table							
• IP Extended	Rules						-			
• IPv6 ACL			IPv6 ACL		Rules T	ype	_			
 IPv6 Rules 					lf.	Pv6 ACL				
• IP Binding C	onfiguratio	on	Ipv6-acl		0 1	V6 ACL				
 Binding Tabl 	е									
• VLAN Bindir	ng Table									

- **2.** Define the first rule (1 of 3).
 - a. Select Security > ACL > Advanced > IPv6 Rules.

System	Switc	hing	-34	Routing		QoS	Securit	y N	Nonitoring	M	aintenance	Hel	p Inde	ĸ		
Management S	ecurity	Acces	is F	Port Aut	nenticatio	in Traff	ic Control	Control	ACL							
ACI	L _{ic}	1	Pv6 R	ules												
ACL Wizard			ACL	Name		inv6-acl	~									
• Basic		~				ipro dei										
 Advanced 		^														
• IP ACL		1	Pv6 A	CL Rule	Table											
• IP Rules		1									1			2	524	12
 IP Extended 	Rules			Rule	Action	Logging	Assign	Mirror	Redirect	Match	Protocol	TCP Flag	Established	Source IPv6	Source IPv6	Source L4
IPv6 ACL				ID.			Queue ID	Intenace	Intenace	Every	туре			Address	Prefix Length	Port Action
 IPv6 Rules 			No :	rules	have b	een con	figured	for this	ACL							
• IP Binding Co	onfiguratio	on														
Binding Table	e															
• VLAN Bindin	g Table															

- b. In the ACL Name list, select ipv6-acl.
- c. Click Add.

System Switching	Routing QoS	Security Monitoring	Maintenance Help	Index	
Management Security Acc	ess Port Authentication	Traffic Control Control Are.	h h h		
ACL	IPv6 ACL Rule Configuration				
ACL Wizard	ACL Name	ipv6-acl			
•Basic ~	Rule ID	1			
Advanced	Action	(# Permit	Egress Queue	·· (0-6)	
• IP ACL	Logging	Deny Disable	Enable		
•ID Extended Didae	Interface	Mirror			
-IP-E ACI		Redirect	4		
- ID-C D-Inc	Match Every	Oisable	O Enable		
+ID Binding Configuration	Protocol Type	IPv6 ×		(0 to 255)	
· IP Diriung Computation	TCP Flag	URG	Ignore 🛩	ACK	Ignore + PSH
· binding radie		RST	Ignore	SYN	Ignore - FIN
VLAN Binding Table	Src	IPv6 Address	2001.DB8 C0A8.AC11	64	
	Src L4	Host Port	Other +	Equal 👻	(0 to 65535)
		Range	Start Port	Other ~	(0 to 65535) End Port
	Dist	IPv6 Address	2001.DB8.C0A8.AC14	64	

- d. In the Rule ID field, enter 1.
- e. For Action, select the **Permit** radio button.
- f. In the Source Prefix field, enter 2001:DB8:C0AB:AC11:..
- g. In the Source Prefix Length field, enter 64.
- h. In the Destination Prefix field, enter 2001:DB8:C0AB:AC14:..
- i. In the Destination Prefix Length field, enter 64.
- j. Click Apply.
- 3. Add Rule 2.
 - a. Select Security > ACL > Advanced > IPv6 Rules.

• ACL Wizard • Basic		2.21																
Advanced IP ACL	2.4	ACL	Name CL Rule	Table	ip/6-acl	Ŧ												
IP Rules IP Extended Rules IPv6 ACL			Rule ID	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Match Every	Protocol Type	TCP Flag	Established	Source IPv6 Address	Source IPv6 Prefix Length	Source L4 Port Action	Source L4 Port	Source L4 Start Port	910
+IPv6 Rules		13	1	Permit					False	255 (IPv6)		False	2001.db8 c0ab ac11	64				
IP Binding Configuration Binding Table VLAN Binding Table	in																	

- b. In the ACL Name list, select ipv6-acl.
- c. Click Add.

System Switching	Routing QoS	Security Monitoring	Maintenance Help	Index	
Management Security Acc	ess Port Authentication 1	Fraffic Control Control ACL	2	14	
ACL.	IPv6 ACL Rule Configuration				
ACL Wizard	ACL Name	ip/6-acl			
•Basic v	Rule ID	2			
Advanced	Action	Permit	Egress Queue	~ (0-6)	
IP ACL IP Rules IP Rules IP Catended Rules IPA6 ACL IPA6 Rules IP Dinfling Configuration Binding Table VLAN Binding Table	Logging Interface Match Every Protocol Type TCP Flag Src	Deny Disable Mirse Redrect Disable TOP URAG RST P56 Address	Enable v Enable (0 to 255) Ignore v 2001 see crists act 11	ACK SVN 64	Ignore v PSH Ignore v FIN
	Sec L4	Host Port Range	Other + Start Port	Equal ~	(0 to 65535) (0 to 65535) End Port
	Dst	IPv6 Address	2001.db8:c0ab.ac13	64	

- d. In the Rule ID field, enter 2.
- e. For Action, select the Permit radio button.
- f. In the Protocol Type list, select TCP.
- g. In the Source Prefix field, enter 2001:DB8:C0AB:AC11::.
- h. In the Source Prefix Length field, enter 64.
- i. In the Destination Prefix field, enter 2001:DB8:C0AB:AC13:..
- j. In the Destination Prefix Length field, enter 64.
- k. In the Destination L4 Port list, select telnet.
- I. Click Apply.
- 4. Add Rule 3.
 - a. Select Security > ACL > Advanced > IPv6 Rules.

002.007	i la														Add 1	Delete C	ance
ACL	IPv6 R	ules															_
ACL Wizard	ACL	. Name		ipv6-acl	~												
Basic																	
Advanced	•																
• IP ACL	IPV6 A	CL Rule	Table														
• IP Rules		_		1				_							-		
•IP Extended Rules	-	Rule	Action	Looping	Assign	Mirror	Redirect	Match	Protocol	TOP Flag	Establebad	Source	Source	Source	Source	Source	So
+IPv6 ACL		10	Carmin	er-Minda	Queue ID	Interface	Interface	Every	Туре	and a start		Address	Prefix Length	Part Action	Port	Start Part	En
and the state of t	8	1	Permit					False	255 (IPv6)		False	2001:db8:c0ab.ac11	64				
+ IPv6 Rules		2	Permit					False	6 (TCP)		False	2001:db8:c0ab.ac11	64				
IPv6 Rules IP Binding Configuration																	
IPv6 Rules IP Binding Configuration Binding Table																	

- b. In the ACL Name list, select ipv6-acl.
- c. Click Add.

A screen similar to the following displays.

System Switching	Routing QoS	Security Monitoring	Maintenance Help	index		
Management Security Acc	ess Pod Authentication Tra	ffic Control Control ARL				
ACL	IPv6 ACL Rule Configuration					
ACL Wizard	ACL Name	ipv6-acl				
•Basic ~	Rule ID	3				
Advanced	Action	ermit	Egress Queue	· (0-6)		
IP ACL IP Rules	Logging	Deny Disable	Enable			
•IP Extended Roles	Interface	Mirror Redirect				
•IPv6 ACL	Match Every	Disable	Enable			
IPv6 Rules IP Binding Configuration	Protocol Type	TCP ~		(0 to 255)		
Binding Table	TCP Flag	URG RST	Ignore ~	ACK SYN	Ignore ~	PSH FIN
VLAN Binding Table	Src	IPv6 Address	2001 DBE COAB AC11	64	- Provine	
	Src L4	 Host Port 	Other *	Equal *	(0 to 65	(535)
		Range	Start Port	Other *	(0 to 6:	(535) End Port
	Dist	IPv6 Address				

- d. In the Rule ID field, enter 3.
- e. For Action, select the **Permit** radio button.
- f. In the Protocol Type list, select TCP.
- g. In the Source Prefix field, enter 2001:DB8:C0AB:AC11::.
- h. In the Source Prefix Length field, enter 64.
- i. In the Destination L4 Port list, select http.
- j. Click Apply.
- 5. Apply the rules to inbound traffic on port 1/0/1.

Only traffic matching the criteria will be accepted.

- a. Select Security > ACL > Advanced > IP Binding Configuration.
- b. In the ACL ID list, select ipv6-acl.
- c. In the Sequence Number list, select 1.
- d. Click Unit 1.
- e. Select Port 1.

System Swite	thing		Routi	ng		QoS		Sec	nity		Mo	mitor	ing.		Ma	inter	ance			telp		In	dex					
Management Security	Acc	165 3	Port A	athen	ticatio	00	Intic	Contro	d (Contri	ol	NG1												an.				
A/9		10.0																										
AUL	i.	IP Bin	aing C	ontigu	nación																			_				
• AUL Wizard		ACL	D												ip	6-acl	*											
• Basic	*	Direc	tion												In	-												
 Advanced 	*	Sequ	ence l	Numb	er										-							22						
+ IP ACL															1			10	10 42	3436	1149	27						
• IP Rules		1	Jnit 1																									
·IP Extended Rules		Ports	1	3	5	2	9 11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47			
ID-6 ACI			\mathbf{P}																									
- ID C Dulas																												
• IPv6 Rules	-		2	4	6	8	10 12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48			
 IP Binding Configurate 	00		Jnit 2																									
Binding Table		Ports	+	3	5	7	9 11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43					
+VLAN Elinding Table							1	1																				
				Hì	Ξì	۳ř		F	H	H		T		Ξ	H	F	T		Tì	۲ì		F						
			2	4	6	2	10 12	14	16	18	20	22	24	-26	28	30	32	34	36	38	40	42	44					

- f. Click the Apply button.
- 6. View the binding table.

Select Security > ACL > Advanced > Binding Table.

System	Switching		Routing	QoS	Sec	urity Mo	onitoring	Maintenance	Help	Index
Management S	ecurity Acc	ess F	ort Authen	tication	Traffic Contr	ol Control				
AC	1	IP ACL	. Binding Ta	ible						
ACL Wizard			Interface	Direction	ACL Type	ACL ID/Name	Sequence N	lumber		
Basic	~		1/0/1	In Bound	IPV6 ACL	inv6-acl	1			
 Advanced 	^			in bound	I VOVIOL	ipro dei	1983			
• IP ACL										
• IP Rules										
• IP Extended	Rules									
- IPv6 ACL										
IPv6 Rules										
• IP Binding C	onfiguration									
Binding Table	9									
• VLAN Bindin	g Table									

CoS Queuing

14

Class of Service Queuing

This chapter describes Class of Service (CoS) queue mapping, CoS Configuration, and traffic shaping features. The chapter includes the following sections:

- CoS Queuing Concepts
- Show classofservice Trust
- Set classofservice Trust Mode
- Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode
- Set CoS Trust Mode for an Interface
- Configure Traffic Shaping

CoS Queuing Concepts

Each port has one or more queues for packet transmission. During configuration, you can determine the mapping and configuration of these queues.

Based on the service rate and other criteria you configure, queues provide preference to specified packets. If a delay is necessary, the system holds packets until the scheduler authorizes transmission. As queues become full, packets are dropped. Packet drop precedence indicates the packet's sensitivity to being dropped during queue congestion.

You can CoS on a per-interface basis:

- You can configure CoS mapping.
- Queue parameters and queue management are configurable per interface.
- Some hardware implementations allow queue depth management using tail dropping or weighted random early discard (WRED).
- Some hardware implementations allow queue depth management using tail dropping.
- The operation of CoS queuing involves queue mapping and queue configuration.

CoS Queue Mapping

CoS queue mapping uses trusted and untrusted ports.

Trusted Ports

- The system takes at face value certain priority designations for arriving packets.
- Trust applies only to packets that have that trust information.
- There can be only one trust field at a time per port.
 - 802.1p user priority (This is the default trust mode and is managed through switching configuration.)
 - IP precedence
 - IP DiffServ Code Point (DSCP)

The system can assign the service level based upon the 802.1p priority field of the L2 header. You configure this by mapping the 802.1p priorities to one of three traffic class queues. These queues are:

- **Queue 2**. Minimum of 50 percent of available bandwidth
- Queue 1. Minimum of 33 percent of available bandwidth
- **Queue 0**. Lowest priority, minimum of 17 percent of available bandwidth

For untagged traffic, you can specify the default 802.1p priority on a per-port basis.

Untrusted Ports

- No incoming packet priority designation is trusted; therefore, the default priority value for the port is used.
- All ingress packets from untrusted ports, where the packet is classified by an ACL or a DiffServ policy, are directed to specific CoS queues on the appropriate egress port. That specific CoS queue is determined by either the default priority of the port or a DiffServ or ACL-assigned queue attribute.
- Used when trusted port mapping is unable to be honored for instance, when a non-IP DSCP packet arrives at a port configured to trust IP DSCP.

CoS Queue Configuration

CoS queue configuration involves port egress queue configuration and drop precedence configuration (per queue). The design of these on a per-queue, per-drop precedence basis allows you to create the service characteristics that you want for different types of traffic.

Port egress queue configuration:

- Scheduler type, strict vs. weighted
- Minimum guaranteed bandwidth
- Maximum allowed bandwidth per-queue shaping
- Queue management type, tail drop vs. WRED

Drop precedence configuration (per queue):

- WRED parameters
 - Minimum threshold
 - Maximum threshold
 - Drop probability
 - Scale factor
- Tail drop parameters, threshold

Per-interface basis:

• Queue management type, rail Drop vs. WRED

Only if per-queue configuration is not supported

- WRED decay exponent
- Traffic shaping for an entire interface

Show classofservice Trust

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

CLI: Show classofservice Trust

To use the CLI to show CoS trust mode, use these commands:

```
(Netgear Switch) #show classofservice trust?
<cr> Press Enter to execute the command.
(Netgear Switch) #show classofservice trust
Class of Service Trust Mode: Dot1P
```

Web Interface: Show classofservice Trust

Select QoS > CoS > Basic > CoS Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index	
CoS DiffServ		2				(s		2 - 11 - 10 - 10 - 10 - 10 - 10 - 10 - 1	
CoS	Co	S Configuration							
•Basic	^ (Global 	All Y			Global Trust N	Node	trust dot1p	~
CoS Configurat Advanced	ion ~) Interface	1/0/1			Interface Trust	t Mode	trust dot1p	~

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 dotlp 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></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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index	
CoS DiffServ								· · · ·	
CoS	s <u>c</u>	oS Configuration							
•Basic	^	Global	All v			Global Trust N	lode	trust dot1	o v
CoS Configur	ration	o. L	i come co					177 - 177 - 178 -	
 Advanced 	~	Interrace	1/0/1	×		Interface Trust	: Mode	trust dot1	p Y

- 2. Select the Global radio button.
- 3. In the Global Trust Mode list, select trust dot1p.
- 4. Click **Apply** to save the settings.

Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode

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

CLI: Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode

(Netgear Switch)	(Config)#cos-queue min-bandwidth?
<bw-0></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>.</bw-7></bw-0>
(Netgear Switch)	(Config)#cos-queue min-bandwidth 15 25 10 5 5 20 10 10
(Netgear Switch)	(Config)#cos-queue strict?
<queue-id></queue-id>	Enter a Queue Id from 0 to 7.
(Netgear Switch)	(Config)#cos-queue strict 1?
<cr></cr>	Press Enter to execute the command.
<queue-id></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.
--	---	--------	---------	----	-----	-----------	-----------

System	Switching		Routing	Qo	S Security	Monitoring	Maintenance He
CoS DiffServ						· · · ·	
			0	0.5			
CoS		Interra	ce Queue	Configura	tion		
•Basic	~	12	3 LAG All			Go To Inter	ace Go
 Advanced 	~	-		Queue	Minimum		
CoS Configuratio	n	-	Interface	ID	Bandwidth	Scheduler Type	Queue Management Type
• 802 1n to Oueue			1/0/2	0 ~	15	Weighted ~	TailDrop 🖌
Mapping			1/0/1	0	0	Weighted	TailDrop
• IP DSCP Queue			1/0/2	0	0	Weighted	TailDrop
Mapping			1/0/3	0	0	Weighted	TailDrop
 CoS Interface 			1/0/4	0	0	Weighted	TailDrop
Configuration			1/0/5	0	0	Weighted	TailDrop
Interface Queue			1/0/6	0	0	Weighted	TailDrop
Configuration			1/0/7	0	0	Weighted	TailDrop
• CoS Queue Drop	0		1/0/8	0	0	Weighted	TailDrop
Configuration			1/0/9	0	0	Weighted	TailDrop
3			1/0/10	0	0	Weighted	TailDrop
			1/0/11	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.

System	Switching	10	Routing	Qo	S Security	Monitoring	Maintenance	Help	Index
CoS DiffServ		<i></i>							
CoS		Interfa	ce Queue	Configura	tion				
• Basic	~	1 2	3 LAG All			Go To Interf	ace 🥂 🥵	io -	
Advanced	^		Interface	Queue	Minimum	Scheduler Type	Queue Management T	VDe	
 CoS Configuration 	m		intendee.	ID	Bandwidth	o officiation () po	daede management i	100	
* 802.1p to Queue			1/0/2	1 ~	25	Strict 🛩	TailDrop 👻		
Mapping			1/0/1	0	0	Weighted	TailDrop		
• IP DSCP Queue			1/0/2	0	0	Weighted	TailDrop		
Mapping			1/0/3	0	0	Weighted	TailDrop		
 CoS Interface 			1/0/4	0	0	Weighted	TailDrop		
Configuration			1/0/5	0	0	Weighted	TailDrop		
Interface Queue			1/0/6	0	0	Weighted	TailDrop		
Configuration			1/0/7	0	0	Weighted	TailDrop		
CoS Queue Drop)		1/0/8	0	0	Weighted	TailDrop		
Precedence			1/0/9	0	0	Weighted	TailDrop		
guluon			1/0/10	0	0	Weighted	TailDrop		
			1/0/11	0	0	Weighted	TailDrop		

- 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></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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index	
CoS DiffServ			· · · · ·						
CoS	Co	S Configuration							
• Basic	× (Global	All 🗸			Global Trust N	Node	untrusted	~
 Advanced CoS Configuration 	^ (Interface	1/0/3 ,	·		Interface Trust	Mode	trust dot1p	~

- 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 $\langle b_W \rangle$ 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></bw>		Enter the shaping bandwidth percentage from 0 to 100
		in increments of 5.
(Netgear	Switch)	(Config)#traffic-shape 70?
<cr></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.

System	Switching		Routing	QoS S	ecurity M	onitoring	Maintenance	Help	Index
CoS DiffServ									
CoS		CoS	Interface C	onfiguration					
Basic	×	13	LAG All	Go To Interface	e. 📃	Go			
 Advanced 	^		Interface	Interface Trust Mode	Interface Shapin	n Rate			
CoS Configuratio	n	-	1/0/3	802.1p	70	, ruce			
*802.1p to Queue			1/0/1	Untrusted	0				
			1/0/2	Untrusted	0				
Mapping			1/0/3	Untrusted	0				
CoS Interface			1/0/4	Untrusted	0				
Configuration			1/0/5	Untrusted	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.

DiffServ

Differentiated Services

This chapter includes the following sections:

- Differentiated Services Concepts
- DiffServ
- DiffServ for VoIP
- Auto VoIP
- DiffServ for IPv6
- Color Conform Policy

15

Differentiated Services Concepts

Differentiated services (DiffServ) is one technique for implementing Quality of Service (QoS) policies. Using DiffServ in your network allows you to directly configure the relevant parameters on the switches and routers rather than using a resource reservation protocol. This section explains how to configure the 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 managed switch, DiffServ allows you to control what traffic is accepted and what traffic is discarded.

How you configure DiffServ support on the 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 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 28. 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 srcip 172.16.20.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit
(Netgear Switch) (Config class-map)#exit
(Netgear Switch) (Config class-map)#exit
(Netgear Switch) (Config class-map)#match srcip 172.16.30.0 255.255.255.0
(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)#exit
(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-class-map)#assign-queue 4
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-class-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)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/3)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/3)#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.

System	Switching	Routing	o <mark>S</mark> Secu	rity	Monitoring	Maintenance	Help	Index
CoS DiffSen	/					- <u> </u>		\$1
DiffS	erv Di	ffServ Configuration						
Diffserv Wizard	1	DiffServ Admin Mode	Oisable	e 💿 Enable				
• Basic	~							
DiffServ Cont	figuration							
 Advanced 	~ SI	atus						
		MIB Table	Current Size	Max Size	е			
		Class Table	0	32				
		Class Rule table	0	416				
		Policy table	0	64				
		Policy Instance table	0	1792				
		Policy Attributes table	0	5376				
		Service table	0	208				

- 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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
DiffS	erv C	lass Name						
Diffserv Wizard	i)	Class Name		Class	Type			
Basic	¥	finance dent		All	~			
 Advanced 	^	intance_dept		701				
DiffServ Conf	iguration							
Class Config	uration							

- **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.

DiffServ	Class Information						
Diffserv Wizard Basic Advanced DiffServ Configuration	Class Name Class Type	finance _o dept Alt					
Class Configuration	DiffServ Class Configurat	100					
 IPv6 Class Configuration 	Match Every	An	0.00				
Policy Configuration	Reference Class	7					
Service Interface Configuration	Class Of Service	0					
Service Statistics	© VLAN		(1 to 409.	3)			
	Secondary Class of	Service 0	*				
	Secondary VLAN		(1 to 409	3)			
	Ethernet Type	Ab	detalic			(600 to ##	hex)
	Source MAC	Ad	iress			Mask	
	Destination MAC	Ad	fress			Mask	
	Protocol Type	ICA	IP v		(0 to	» 255)	
	Source IP	Add	fress	172 16 10 0		Mask	255 255 255 0

- 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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
DiffServ	32	Class Name						
Diffserv Wizard		Class Name	э	Class	Type			
Basic	~	Marketing (tent	All	~			
 Advanced 	^	finance der	vt.	ΔII				
DiffServ Configu	ration	- interior	<u>A</u>	1.750				
Class Configura	tion							

- **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.

System Switching	Routing	S Security M	Monitoring Maintenance	Help Index	
DiffServ	Class Information				
Diffserv Wizard Basic Advanced DiffServ Configuration Offser Configuration	Class Name Int Class Type AD DiffServ Class Configuratio	arhiebog_dest -			
IPv6 Class Configuration Policy Configuration Senice Interface Configuration Senice Statistics	Match Every Reference Class Class Of Service VLAN Secondary Class of S Secondary VLAN Ethernet Type Source MAC Protocol Type Source IP	Any U finance_de 0 U (1 to Appletalik Address Address Address	et = 4093) * 1722.16.20.0	(0 to 255)	(600 to ## hex) Mask Mask Mask

- 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.

System	Switching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ					50- 		άς		à
D:#0		0							
Dinserv	K.	Class	sivame						
 Diffserv Wizard 			Class Name	1	Clas	s Type			
Basic	~		-						
Advanced	~		Test_dept		All	~			
, taranood			finance_dept		All				
 DiffServ Configur 	ration		Marketing_de	ept	All				
Class Configurat	tion								

- **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	g Routing	QoS	Security	Monitoring	Maintenan	ce Help	Index		
CoS Preserve		-	9				⁷⁷⁴		
	-								
DiffServ	Class Information								
Diffserv Wizard	Class Name	Test_de	pt.						
Basic v	Class Type	(All -							
Advanced .									
DiffServ Configuration									
Class Configuration	DiffServ Class Config	guration							
IPv6 Class Configuration	 Match Every 		Any	*					
Policy Configuration	Reference Class	5	financ	e dept -					
Service Interface Configuration	Class Of Service	6	0 ~						
Service Statistics	© VLAN			(1 to 4093)					
Contro Character	Secondary Class	is of Service	0. ~						
	Secondary VLA	N		(1 to 4093)					
	Ethernet Type			talk 👻				(600 to fff	hex)
	Source MAC		Addre	35				Mask	
	Destination MA	с	Addre	0.5				Mask	
	Protocol Type						(0 to 255)		
	Source IP		Addre	\$5 172.1	16.30.0			Mask	255,255,255.0

- 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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ				- 0				o 11 14
DiffServ		Class Name						
Diffserv Wizard		Class Nam	e	Clas	з Туре			
Basic	~	Developme	ent	All	*			
 Advanced 	~	finance_de	<u>ot</u>	All				
DiffServ Configur	ration	Marketing	dept	All				
Class Configuration	tion	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.

System Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index		
CoS (1994)					20			i.	
DdlServ	Class Information								
Diffserv Wizard	Class Name	Develop	ement						
Basic 👻	Class Type	All							
Advanced ^									
DiffServ Configuration									
Class Configuration	DiffServ Class Config	guration							
IPv6 Class Configuration	Ø Match Every		Any	-					
Policy Configuration	Reference Class	5	finance	e dept (*)					
Service Interface Configuration	Class Of Service	e	0						
Coningenation	O VLAN			(1 to 4093)					
· Seroce Statistics	Secondary Class	is of Service	0.~						
	Secondary VLA	14		(1 to 4093)					
	G Ethernet Type		Applet	alic: V				(600 to ffff	hex)
	Source MAC		Addres	55				Mask	
	Destination MA	C	Addres	55				Mask	
	Protocol Type		ICMP				(0 to 255)		
	Source IP		Addres	ss 172	15.40.0			Mask	255.255.255.0

- 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.

System	Switching		Routing	QoS	Securit	y Monito	ring	Maintenance	Help	Index
CoS DiffServ	-	.07		8						
DiffServ		Polic	y Configuration	1						
Diffserv Wizard			Policy Name		Policy Type	Member Class				
Basic	~		internet acce	ISS	~	finance dent	~			
Advanced	^		-			Toologie - activ	-			
DiffServ Configura	ation									
Class Configurati	on									
• IPv6 Class Config	guration									
Policy Configurat	ion									

- **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.
| System | Switchir | ıg | Routing | QoS | Securi | ty Monitoring | Maintenance | Help | Index |
|------------------------------------|------------|----|-----------------|------|-------------|------------------|-------------|-------------------------|-------|
| CoS DiffServ | | | | | | | | (C <mark>.</mark> 1777) | |
| DiffSen | V | Po | licy Configurat | ion | | | | | |
| Diffserv Wizard | | | Policy Nar | ne | Policy Type | Member Class | | | |
| Basic | | ř | internet_ad | cess | In 👻 | Marketing_dept 👻 | | | |
| DiffServ Config | uration | | internet_ac | cess | In | finance_dept | | | |
| Class Configur | ation | | | | | | | | |
| IPv6 Class Cor | figuration | | | | | | | | |
| Policy Configur | ration | | | | | | | | |

- **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.

System	Switching		Routing	QoS	Securi	y Monitoring	Maintenance	Help	Index
CoS DiffServ									
DiffServ		Polic	y Configuration						
Diffserv Wizard			Policy Name	F	Policy Type	Member Class			
Basic	*		internet energy		In an	Manhading dank an			
 Advanced 	^		Internet_access	s	in ×	Warketing_dept *			
DiffServ Configur	ation		internet access	s li	n	Marketing dept			
Class Configurat	ion								
• IPv6 Class Confi	guration								
Policy Configura	tion								

- **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.

System Swit	ching		Routing Q	Securit	y Monitoring	Maintenance	Help Index
CoS DiffServ							
DiffServ		Polic	y Configuration				
Diffserv Wizard			Policy Name	Policy Type	Member Class		
- Basic	~		internet access	In X	Development x		
 Advanced 	^		internet_access	lin	finance dent		
DiffServ Configuration			internet access	In	Marketing dept		
 Class Configuration 			internet_access	In	Test_dept		
• IPv6 Class Configurat	ion						
Policy Configuration							
 Service Interface Configuration 							
 Service Statistics 							

- **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.

System	Switchin	g	Routing	QoS	Securit	y Monitorin	g	Maintenance	Help	Index
CoS DiffServ										
DiffSe	N	Polic	y Configuration							
Diffserv Wizard			Policy Name	Pol	icy Type	Member Class				
Basic	1	*	T oney runne		cy type	includer oldes				
Advanced					~		~			
D.100 0 5	1		internet_access	<u>a</u> In		finance_dept				
 DiffServ Config 	guration		internet_access	<u>a</u> In		Marketing_dept				
 Class Configu 	iration		internet_access	in In		Test_dept				
• IPv6 Class Co	onfiguration		internet_access	<u>s</u> In		<u>Development</u>				
Policy Configu	uration									
 Service Interfa Configuration 	ice									
 Service Statis 	tics									

b. Click the **internet_access** check box for the member class finance_dept.

System Sw	itching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
DiffServ		Class Information						
Diffserv Wizard Basic Advanced DiffServ Configuratio Class Configuration	• •	Policy Name Policy Type Member Class Nar Policy Attribute	ne	internet_access In finance_dept				
IPv6 Class Configura Policy Configuration Service Interface Configuration Service Statistics	ition	Policy Attribute		Assign Queue Drop Mark VLAN CoS Mark CoS As Sec Mark IP Preceder Mirror Redirect Mark IP DSCP Simple Policy	condary CoS icce	1 • 0 • 0 • af11 • Color Mode		Color Blind

- 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.

System	Switchir	ng	Routing	QoS	Securit	y Monitoring	Maintenance	Help	Index
CoS DiffServ	0			λ					
DiffS	erv	Polic	y Configuration						
Diffserv Wizard			Policy Name	F	Policy Type	Member Class			
• Basic		*	I oney roune		onoj tijpo				
 Advanced 						Ŷ	1		
D:00 0 0			internet_acce	ess li	n	finance_dept			
* DiliSelv Com	iguration		internet_acce	ess l	n	Marketing_dept			
 Class Config 	uration		internet_acce	ess l	n	Test_dept			
• IPv6 Class C	onfiguration		internet_acce	iss I	n	Development			
Policy Config	juration								
 Service Interf Configuration 	ace								
• Service Stati	stics								

b. Click the **internet_access** check box for marketing_dept.

received and the relieving displayed	A	screen	similar	to	the	following	displays
--------------------------------------	---	--------	---------	----	-----	-----------	----------

System Swi	itching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ					3) (t) (t)		A	×
2								
DiffServ		Class Information						
Diffserv Wizard		Policy Name		internet_access				
• Basic	~	Policy Type		In				
 Advanced 	^	Member Class Nar	ne	Marketing_dept				
 DiffServ Configuration 	n							
 Class Configuration 								
IPv6 Class Configura	ation	Policy Attribute		We 10 14		400-000-0-0		
Policy Configuration	£	Policy Attribute	۲	Assign Queue		2 *		
Service Interface Configuration			0	Drop				
Senice Statistics			0	Mark VLAN CoS		0 ~		
- Service Statistics			0	Mark CoS As Sec	ondary CoS			
			0	Mark IP Preceden	ce	0 ~		
			0	Mirror		*		
			0	Redirect		×		
			0	Mark IP DSCP		af11 ~		
			0	Simple Policy				
						Color Mode		Color Blind

- 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.

System	Switching		Routing	QoS	Securit	y Monitoring	Maintenance	Help	Index
CoS DiffServ									
DiffServ		Polic	y Configuration						
Diffserv Wizard			Policy Name	Po	licy Type	Member Class	P.		
Basic	~	-	i oney riante		koj tjpo				
Advanced	~	-			~	× ·			
DiffServ Configuration	ation		internet_access	in In		tinance_dept Marketing_dept			
Class Configurat	ion		internet access	in in		Test dent			
• IPv6 Class Configurat	guration		internet_access	In		Development			
Policy Configurat	tion								
 Service Interface Configuration 									
 Service Statistic: 	s								

b. Click the **internet_access** check mark for test_dept.

System Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ							
DiffServ	Class Information						
Diffserv Wizard	Policy Name		internet access				
•Basic 🗸	Policy Type		In				
Advanced	Member Class Name		Test_dept				
 DiffServ Configuration 							
 Class Configuration 							
 IPv6 Class Configuration 	Policy Attribute						
Policy Configuration	Policy Attribute	، ھ	Assign Queue		3 🕶		
Service Interface Configuration		0	Drop				
Conliguration		0	Mark VLAN CoS		0 ~		
- Service Statistics			Mark CoS As Sec	condary CoS			
		0	Mark IP Preceder	ice	0 ~		
		0	Mirror		~		
		0	Redirect		~		
		0	Mark IP DSCP		af11 ×		
		0	Simple Policy		L'ANGLES COM		
					Color Mode		Color Blind

- 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.

System Swite	hing	80	Routing	QoS	Securit	y Monitorine	Mainte	nance	Help	Index
CoS DiffServ										
DiffServ		Polic	y Configuration							
Diffserv Wizard			Policy Name	-	Policy Type	Member Class				
Basic	~	-								
Advanced	~		-		Ť		~			
DiffCont Configuration			internet_acces	is I	n	finance_dept				
- Dinserv Conniguration			internet_acces	<u>is</u>	n	Marketing_dept				
 Class Configuration 			internet_acces	is I	n	Test_dept				
IPv6 Class Configurati	on		internet_acces	is I	n	<u>Development</u>				
Policy Configuration										
 Service Interface Configuration 										
 Service Statistics 										

b. Click the **internet_access** check mark for development_dept.

A	screen	similar	to th	ne fo	llowing	displays.
---	--------	---------	-------	-------	---------	-----------

System Switchir	ng Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ							
DiffServ	Class Information						
Diffserv Wizard	Policy Name		internet_access				
• Basic	 Policy Type 		In				
Advanced	 Member Class Nam 	le	Development				
 DiffServ Configuration 							
Class Configuration							
IPv6 Class Configuration	Policy Attribute						
Policy Configuration	Policy Attribute	۲	Assign Queue		4 ~		
Service Interface		0	Drop				
Configuration		0	Mark VLAN CoS		0 ~		
* Service Statistics		0	Mark CoS As Sec	ondary CoS			
		0	Mark IP Preceden	ce	0 ~		
		0	Mirror		~		
		0	Redirect				
		0	Mark IP DSCP		and d		
		0	Simple Policy		airi		
			pier eneg		Color Mode		Color Plind

- 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.

System S	Switching		Routing	QoS	Security	Monitoring	Mai	ntenance	Help
CoS DiffSery									
DiffServ		Servi	ce Interface Co	onfiguration					
Diffserv Wizard		13	LAG All			Go To li	nterface		Go
 Basic 	¥							() ()	
 Advanced 	~		Interface		Policy In Name	Policy Out Name	Direction	Operational 3	Status
DiffServ Configura	ition				internet_access ~	~			
Class Configuration	on		1/0/1						
• IPv6 Class Config	uration		1/0/2						
• Daliou Configurati	0.0		1/0/3						
- Folicy Conliguiati	ION		1/0/4						
 Service Interface Configuration 	1		1/0/5						
- Caralan Otablatian			1/0/6						
· Service Statistics			1/0/7						

- 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.

System	Switching		Routing	C	oS Securit	y Monitoring	Maintenance	Help	Index
CoS DiffServ									÷.
CoS		Interf	ace Queue	Configura	ation				
Basic	~	1 3	LAG AII		Go To	Interface	Go		
Advanced	^				No.				
 CoS Configuratio 	m		Interface	D	Bandwidth	Queue Manageme	nt Type		
* 802.1p to Queue			1/0/5	1 ~	25	TailDrop 🗸			
mapping			1/0/1	0	0	TailDrop			
IP DSCP Queue Mapping			1/0/2	0	0	TailDrop			
Mapping			1/0/3	0	0	TailDrop			
 CoS Interface Configuration 			1/0/4	0	0	TailDrop			
Conniguration			1/0/5	0	0	TailDrop			
 Interface Queue Configuration 			1/0/6	0	0	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.

System	Switching		Routing	C	toS Sec	urity I	Monitoring	Maintenance	Help	Index
CoS DiffServ										
CoS	\$	Interf	ace Queue	Configura	ation					
• Basic	×	13	LAG All		Go	To Interface		Go		
 Advanced 	^		1	Ourse	N.M. Salaharana					
 CoS Configur 	ation		Interface	ID	Bandwidth	Qu	eue Manager	nent Type		
* 802.1p to Qu	eue		1/0/5	2 🗸	25	Τε	ailDrop 🗸			
wapping			1/0/1	1	0	Tai	Drop			
 IP DSCP Que Mapping 	eue		1/0/2	1	0	Tai	Drop			
wapping			1/0/3	1	0	Tai	Drop			
 CoS Interface Configuration 	9		1/0/4	1	0	Tai	Drop			
Comiguration			1/0/5	1	25	Tai	Drop			
 Interface Que Configuration 			1/0/6	1	0	Tai	Drop			

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.

System S	witching		Routing	Qo	S Security	Monitoring	Maintenance Help	Inc
CoS DiffServ								
0-0		Interfa		Configura	tion			
05		interne	de queue	oomiguru				
Basic	~	12	3 LAG All			Go To Interf	Go	
Advanced	^			Queue	Minimum			
CoS Configuration	1	-	Interface	ID	Bandwidth	Scheduler Type	Queue Management Type	
• 802 1n to Queue			1/0/5	3 ¥	25	Weighted 🛩	TailDrop 🖌	
Mapping			1/0/1	2	0	Weighted	TailDrop	
• IP DSCP Queue			1/0/2	2	0	Weighted	TailDrop	
Mapping			1/0/3	2	0	Weighted	TailDrop	
CoS Interface			1/0/4	2	0	Weighted	TailDrop	
Configuration			1/0/5	2	25	Weighted	TailDrop	
Interface Queue			1/0/6	2	0	Weighted	TailDrop	
Configuration			1/0/7	2	0	Weighted	TailDrop	
CoS Queue Drop			1/0/8	2	0	Weighted	TailDrop	
Configuration			1/0/9	2	0	Weighted	TailDrop	
			1/0/10	2	0	Weighted	TailDrop	
			1/0/11	2	0	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 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.

System	Switching		Routing	Qo	S Security	Monitoring	Maintenance	Help
CoS DiffServ								
CoS		Interfa	ice Queue	Configura	tion			
Basic	v	1 2	3 LAG All			Go To Interf	ace	o
 Advanced 	^	-	Interface	Queue	Minimum	Sabadular Tura	Quaue Management To	100
CoS Configurat	ion	-	Intenace	ID	Bandwidth	Scheduler Type	Queue Management Ty	pe
• 802 1p to Que	10		1/0/5	4 ~	25	Weighted 🛩	TailDrop 👻	
Mapping			1/0/1	3	0	Weighted	TailDrop	
• IP DSCP Queu	e		1/0/2	3	0	Weighted	TailDrop	
Mapping			1/0/3	3	0	Weighted	TailDrop	
CoS Interface			1/0/4	3	0	Weighted	TailDrop	
Configuration			1/0/5	3	25	Weighted	TailDrop	
Interface Queu	e		1/0/6	3	0	Weighted	TailDrop	
Configuration			1/0/7	3	0	Weighted	TailDrop	
CoS Queue Dr	op		1/0/8	3	0	Weighted	TailDrop	
Configuration			1/0/9	3	0	Weighted	TailDrop	
3			1/0/10	3	0	Weighted	TailDrop	
			1/0/11	3	0	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 4.
- d. In the Minimum Bandwidth field, enter 25.
- e. Click Apply.

DiffServ for VolP

One of the most valuable uses of DiffServ is to support Voice over IP (VoIP). VoIP traffic is inherently time sensitive: For a network to provide acceptable service, a guaranteed transmission rate is vital. This example shows one way to provide the necessary quality of service: how to set up a class for UDP traffic, have that traffic marked on the inbound side, and then expedite the traffic on the outbound side. The configuration script is for Router 1 in the accompanying diagram: A similar script should be applied to Router 2.



Figure 29. Diffserv for VoIP in Router 1

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

CLI: Configure DiffServ for VolP

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)#assign-queue 5
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-class-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.

System	Switching	100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100	Routing	Qos	S Security	Monitoring	Maintenance	Help	Index
CoS DiffServ									
Co	S	Interfa	ce Queue	Configurat	tion				
•Basic	×	12	3 LAG All			Go To Interf	ace	Go	
 Advanced CoS Configu 	^ ration		Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Managemer	nt Type	
■ 802 1p to O	10110		1/0/2	5 ¥	0	Strict 🗸	TailDrop 🖌		
Mapping	ieue		1/0/1	0	0	Weighted	TailDrop		
• IP DSCP Qu	ieue		1/0/2	0	0	Weighted	TailDrop		
Mapping			1/0/3	0	0	Weighted	TailDrop		
 CoS Interfac 	e		1/0/4	0	0	Weighted	TailDrop		
Configuration	1		1/0/5	0	0	Weighted	TailDrop		
Interface Qu	eue		1/0/6	0	0	Weighted	TailDrop		
Configuration	1		1/0/7	0	0	Weighted	TailDrop		
CoS Queue	Drop		1/0/8	0	0	Weighted	TailDrop		
Configuration	1		1/0/9	0	0	Weighted	TailDrop		
			1/0/10	0	0	Weighted	TailDrop		
			1/0/11	0	0	Weighted	TailDrop		

- **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.



- **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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffSen								
DiffS	ierv Cla	ass Name						
Diffserv Wizard	1	Class Name		Clas	s Type			
Basic	×	class voin		A11	v Jpc			
Advanced	~	Class_voip		All				
DiffServ Conf	figuration							
Class Config	juration							
• IPv6 Class C	Configuration							
Policy Config	guration							
 Service Inter Configuration 	face 1							
	ictics							

- 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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffSen								
DiffS	ierv	Class Information						
Diffserv Wizard	đ	Class Name	class_v	/oip				
Basic	v	Class Type	All					
 Advanced 	^							
DiffServ Cont	figuration							
Class Config	juration	DiffServ Class Conf	guration					
• IPv6 Class C	Configuration	Match Every		Any	~			
 Policy Config 	guration	Reference Class	IS	×				
Service Inter	face	Class Of Service	e	0 ~				
Conliguration		VLAN			(1 to 4093)			
· Service Stati	isues	Secondary Cla	ss of Service	0 ~				
		Secondary VL/	AN		(1 to 4093)			
		Ethernet Type		Apple	talk Y			
		Source MAC		Addre	ss			
		O Destination MA	٨C	Addre	SS			
		Protocol Type		UDP	v			(0 to 255)
		Source IP		Addre	SS			

- 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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
DiffSe	erv C	lass Name						
Diffserv Wizard	6	Class Name	i.	Clas	es Type			
• Basic	~		•.		is type			
 Advanced 	~			All	*			
DiffServ Confi	guration			All				
Class Configu	uration							
• IPv6 Class Co	onfiguration							
 Policy Config 	uration							
 Service Interfa Configuration 	ace							
 Service Statis 	stics							

- 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.

System Switching	Routing QoS	Security Monitoring	Maintenance	Help	Index	
CoS OdiStere						
DiffServ	Reference Class	class voip *				
Diffserv Wizard	Class Of Senice	0 -				
•Basic v	() VLAN	(1 to 4093)				
Advanced A	G Secondary Class of Service	0 ~				
DiffServ Configuration	Secondary VLAN	(1 to 3093)				
- Class Configuration	 Ethemet Type 	Appletalk ~				(600 to 1111 hex)
IPv6 Class Configuration	Source MAC	Address				Mask
Policy Configuration	Destination MAC	Address				Mask
Service Interface Configuration	Protocol Type	ICMP ×			(0 to 255)	
Service Statistics	Source IP	Address				Mask
	Source L4 Port	domain ~			(0 to 6553	5)
	② Destination IP	Address				Mask
	Obstination L4 Port	domain 🛩			(0 to 6553	5)
	· IP DSCP	EF *				(0 to 63)
	Precedence Value	0 - (0 to 7)				
	@ IP ToS	Bit Value				Bit Mask

- 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.

System	Switching	2	Routing	QoS	Securit	y Monitorir	ng	Maintenance	Help	Index
CoS DiffServ		- 532				10	3)			
DiffServ		Polic	y Configuration							
 Diffserv Wizard 			Policy Name		Policy Type	Member Class				
- Basic	~	-	nel usin		r oney rype					
- Advanced	~		pol_volp		Ŷ	class_volp *				
DiffServ Configu	ration									
Class Configura	ation									
• IPv6 Class Con	figuration									
Policy Configur	ation									

- **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.

System Sw	vitching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
DiffServ		Class Information						
Diffserv Wizard		Policy Name		pol_voip				
•Basic	*	Policy Type		In				
Advanced	^	Member Class Na	me	class_voip				
 DiffServ Configuration 	on							
 Class Configuration 								
 IPv6 Class Configur 	ation	Policy Attribute						
Policy Configuration	t:	Policy Attribute	0	Assign Queue		5 ~		
Service Interface Configuration			0	Drop				
Senice Statistics			0	Mark VLAN CoS		0 ~		
Genice Granatica			0	Mark CoS As Se	condary CoS			
			0	Mark IP Preceder	nce	0 ~		
			0	Mirror		×		
			0	Redirect		~		
			۲	Mark IP DSCP		EF 👻		
			0	Simple Policy				

- 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.

System : CoS DiffServ	Switching		Routing	QoS	Securit	y Monitoring	Maintenance	Help	Index
DiffServ		Polic	y Configuration						
Diffserv Wizard Basic Advanced DiffServ Configura Class Configurati IPv6 Class Config	× ation on guration		Policy Name pol_voip pol_voip		Policy Type In ✓	Member Class class_ef ~ class_voip			
Policy Configurat Service Interface Configuration Service Statistics	ion								

- 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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
DiffServ	e (Class Information						
• Diffserv Wizard		Policy Name		pol_voip				
Basic	~	Policy Type		In				
 Advanced 	^	Member Class N	ame	class_ef				
DiffServ Configu	iration							
Class Configura	ation							
• IPv6 Class Con	figuration p	Policy Attribute						
Policy Configuration	ation	Policy Attribute	0	Assign Queue		E ×		
 Service Interfac Configuration 	e		0	Drop		3		
Service Statistic	cs		0	Mark VLAN Cos	3	0 ~		
			0	Mark CoS As S	econdary CoS			
			0	Mark IP Precede	ence	0 ~		
			0	Mirror		~		
			0	Redirect		~		
			۲	Mark IP DSCP		FF Y		
			0	Simple Policy				

- 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.

System	Switching	3	Routing	QoS Securi	ty Mor	nitoring	Maintenance	Help	Index
CoS DiffServ									
DiffServ		Servi	ce Interface Cor	nfiguration					
Diffserv Wizard		13	LAG All		Go To I	nterface	Go		
Basic	~				10	L			
 Advanced 	^		Interface	Policy In Name	Policy Out Name	Direction	Operational Status		
DiffServ Configura	ation		1/0/2	pol voip ~	×				
Class Configurati	ion	0	1/0/1						
 IPv6 Class Config 	guration		1/0/2						
Policy Configurat	ion		1/0/3						
r oney ooningaraa	aon -		1/0/4						
 Service Interface Configuration 	2		1/0/5						
			1/0/6						

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 VolP

The Auto VoIP feature makes it easy to set up voice over IP (VoIP) for IP phones on a switch. From software release 10.0.0 on, the switch supports both protocol-based and OUI-based Auto-VoIP configurations.

Protocol-Based Auto VolP

In a VoIP system, various signaling protocols are used to establish the connection between two VoIP devices. Protocol-based Auto VoIP provides a better class of service (CoS) to data and signaling VoIP streams than to other traffic. The supported signaling protocols are Session Initiation Protocol (SIP), H.323, and Skinny Call Control Protocol (SCCP). Depending on your configuration, after VoIP packets are identified, the switch takes the following actions:

- If you enable remarking, the switch remarks the voice traffic 802.1p priority with the configured priority at the ingress port to ensure that voice traffic always receives the highest priority throughout the network. You must enable egress tagging on the appropriate uplink port to let the switch carry the remarked priority to the egress port.
- If you assign a queue, make sure that you allocate sufficient bandwidth to the queue to fullfil the priority treatment for VoIP traffic.

Note: Queue assignment and remark 802.1p priority are mutually exclusive configurations. You can configure each configuration on a per-port basis.

After a call session completes and the call is disconnected, the QoS rules are removed.

The ports on which you configure protocol-based Auto VoIP are made members of the voice VLAN automatically. By default, no VLAN is used for the voice VLAN. You must create a voice VLAN first.

OUI-Based Auto VoIP

OUI-based Auto VoIP prioritizes VoIP packets based on the bytes of the organizationally unique identifiers (OUIs) in the source MAC address. The switch is preconfigured with a default list of OUIs. You can also add OUIs that need prioritization. The switch can support up to 128 OUIs, including the default OUIs.

By default, the switch uses the highest available priority for all frames that match OUIs on the OUI list. You can override the default priority and configure a different priority. You need to map the priority to a traffic class to achieve the desired egress queuing for VoIP traffic.

The switch assigns all VoIP traffic that matches a known OUI list to the VoIP VLAN. If you modify the VoIP VLAN, all existing MAC VLAN entries are removed. The MAC entries are deleted from the forwarding database and relearned with the new VLAN as the devices transmit packets. The port VLAN membership also changes.

The switch assigns untagged VoIP traffic only to the VoIP VLAN and uses the associated priority for egress queuing.

If you enable port mirroring on a port that is configured for Auto VoIP, the port remains nonoperational.

Managed Switches



Example 1: Enable Protocol-Based Auto VoIP

This example is provided as CLI commands and as a web interface procedure.

CLI: Protocol-Based Auto VolP

This script in this section shows how to set up Auto VoIP per port.

1. Enable protocol-based Auto VoIP on a specific port of the switch.

```
(Netgear Switch)(Configure)#interface 2/0/1
(Netgear Switch)(Interface 2/0/1)#auto-voip protocol-based
```

2. Display the Auto VoIP information.

Web Interface: Configure Protocol-Based Auto VoIP

- 1. Enable protocol-based Auto VoIP on a specific port of the switch:
 - a. Select Switching > Auto-VoIP > Protocol-based > Port Settings.

A screen similar to the following displays.

Syst	em	Sw	vitching		Routing	QoS	Security	· 1	Monitorin	ig	Maintenance	Help	Index
VLAN			iSCSI	STP	Multicas	t MVR	Address Table	Ports	LAG	MLAC	3		
	Auto-\	VolP		Protoc	ol Based G	lobal Settin	igs						
• Protoco	ol-based	d	~	Prio	ritization Ty	pe	Traffic Class	*					
• Port	Setting	s		Clas	ss Value		6 ×						
• OUI-ba	sed		~										
• Auto-V	olP Sta	tus											
				Protoc	ol Based P	ort Settings							
									-				
				12	LAG All G	o To Interfa	ice	Go					
					Interface	Auto VolP	Mode Operation	nal Status	5				
					2/0/1	Enable N	- Down						
					2/0/1	Disable	Down						
					2/0/2	Disable	Down						
					2/0/3	Disable	Down						
					2/0/4	Disable	Down						

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

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

- c. From the Auto VoIP Mode mode, select Enable.
- d. Click Apply.

Example 2: Change the Queue of Protocol-Based Auto VoIP

This example is provided as CLI commands and as a web interface procedure.

CLI: Change the Queue of Protocol-Based Auto VoIP

Protocol-based VoIP classifies and prioritizes packets and places them in the higher-priority queue. By default, the packets are placed in egress queue 6. However, you can override the egress queue setting. The following example shows how to assign the protocol-based Auto VoIP to egress queue 4.

1. Change the egress queue of protocol-based Auto VoIP.

(Netgear Switch) (Config)#auto-voip protocol-based traffic-class 4

2. Display the Auto VoIP information.

Web Interface: Configure Protocol-Based Auto VoIP

- 1. Change the queue of protocol-based Auto VoIP.
 - a. Select Switching > Auto-VoIP > Protocol-based > Port Settings.

Syste	em	Sv	vitching		Routing	QoS	Security	1	Nonitorin	g	Maintenance	Help	Index
VLAN			iSCSI	STP	Multicas	st MVR	Address Table	Ports	LAG	MLAG			
	Auto-V	olP		Protoc	ol Based C	Global Settin	gs						
• Protoco	ol- <mark>based</mark>		^	Prio	ritization Ty	ype	Traffic Class	~					
• Port	Settings			Clas	s Value		4 ~						
• OUI-bas	sed		~										
• Auto-Vo	oIP State	us											
				Protoc	ol Based F	ort Settings							
				1 2	lag <mark>al</mark> i (Go To Interfa	ce	Go					
					Interface	Auto VolP	Mode Operation	hal Status	5				
							*						
					2/0/1	Enable	Up						
					2/0/2	Disable	Down						
					2/0/3	Disable	Down						
					2/0/4	Disable	Down						

- b. From the Class Value menu, select 4.
- c. Click Apply.

Example 3: Create an Auto VoIP VLAN

This example is provided as CLI commands and as a web interface procedure.

CLI: Create an Auto VoIP VLAN

Since no default VoIP VLAN is specified, you must create a VLAN first to use auto VoIP.

1. Create VLAN 5.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 5
(Netgear Switch) (Vlan)#exit
```

2. Assign the VoIP traffic to VLAN 5, which becomes the VoIP VLAN.

(Netgear Switch) (Config)#auto-voip vlan 5

3. Display the protocol-based Auto VoIP information.

4. Display the OUI-based Auto VoIP information.



Web Interface: Change the Auto VoIP VLAN

- 1. Create a VLAN 5:
 - a. Select Switching > VLAN > Basic > Vlan Configuration.

A screen similar to the following displays.

Syste	em 📃	Swit	tching		Routing	QoS	Security	Monitori	ng	Maintenance	Help	Index
VLAN	Auto-Vol	P i	iscsi	STP	Multicast	MVR	Address Table	Ports LAG	MLAG	G		
	VLAN			Reset								
• Basic			~	Reset	t Configuration	on						
• VLAN	I Configura	ation										
• Advance	ed		~									
				Interna	VLAN Cont	iguration						
				Intern	al VLAN All	ocation Ba	ase 40	93				
				Intern	al VLAN All	ocation Po	olicy 🔘	Ascending 🖲 D	escendir	1g		
				VLAN	Configuration	1						
					VLAN ID V	LAN Nam	e VLAN Type	Make Static				
					5			Disable 👻				
					1 d	efault	Default	Disable				

- **b.** In the VLAN ID field, enter **5**.
- c. Click Add.
- 2. Assign the VoIP traffic to VLAN 5.
 - a. Select Switching > Auto-VoIP > Protocol-based > Port Settings.

Syst	em S	witching		Routing	QoS	Security		Aonitorin	g	Maintenance	Help	Index
VLAN	Auto-VolP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAC	3		
	Auto-VolP		OUI Ba	sed Properti	es							
• Protoco	ol-based	~	Auto-	OIP VLAN I	D	5		(1 to 40	93)			
• OUI-ba	sed	^	OUI-b	ased priority		7 ~						
• Prop	erties											
• Port	Settings											
• OUI 1	Fable											
- Auto-V	olP Status											

- b. From the VoIP VLAN Id menu, select 5.
- c. Click Apply.

DiffServ for IPv6

This feature extends the existing QoS ACL and DiffServ functionality by providing support for IPv6 packet classification.



Figure 31. 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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ	0			ar e) 		8	
DiffSe	erv IP	/6 Class Name						
Diffserv Wizard		Class Name		Clas	Тупе			
• Basic	~							
 Advanced 	~ -				•			
DiffServ Confi	iguration							
Class Config	uration							
IPv6 Class C	onfiguration							

- b. In the Class Name field, enter classicmpv6.
- c. In the Class Type list, select All.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
DiffSe	erv IPv	6 Class Name						
Diffserv Wizard		Class Name	1	Class	з Туре			
 Basic 	¥	classicmpu6		All	~			
Advanced	~	classicilipio		All				
DiffServ Confi	guration							
 Class Configu 	uration							
IPv6 Class Co	onfiguration							

d. Click Add to create the IPv6 class.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
DiffSe	erv IP	v6 Class Name						
 Diffserv Wizard 		Class Name		Clas	s Tuna			
• Basic	¥	Coluss Hame		0103	s type			
 Advanced 	~	classismaß		All				
 DiffServ Confi 	iguration			Aii				
Class Configu	uration							
• IPv6 Class Co	onfiguration							
 Policy Config 	juration							

- 2. Define matching criteria as protocol ICMPv6.
 - a. Select QoS > DiffServ > Advanced > IPv6 Class Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								N
DiffServ		IPv6 Class Name						
• Diffserv Wizard		Class Name		Class	Type			
• Basic	*	1		0.000	.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			
 Advanced 	^				*			
DiffServ Configuration	ation			All				
Class Configurati	on							
 IPv6 Class Config 	guration							

b. Click the class **classicmpv6**.

System Switch	ing	Routing	QoS	Security	Monito	ing Maintenan	ce Help	Index
CoS DiffServ				8				
DiffServ		IPv6 Class Information	on					
Diffserv Wizard Basic Advanced DiffServ Configuration Class Configuration	× ^	Class Name Class Type IPv6 DiffServ Class (Classico All Configuratio	mpv6				
IPv6 Class Configuratio Policy Configuration Service Interface Configuration Service Statistics		Match Every Reference Class Protocol Type Source Prefix/Le Source L4 Port Destination Pref Destination L4 F For Flow Label IP DSCP	s ength fix/Length Port	Any - class_e ICMPv6 domain domain		(0 to 1048575)		(0 to 255) (0 to 65535) (0 to 65535) (0 to 65535)

c. Select the Protocol Type radio button, select Other, and enter 58.

System Switch	ing	Routing	QoS	Security	Monitorin	g Maintenance	Help	Index	
CoS DiffServ									
DiffServ		IPv6 Class Informatio	on						
Diffserv Wizard		Class Name	classic	mpv6					
Basic	~	Class Type	All						
Advanced	^								
DiffServ Configuration									
 Class Configuration 		IPv6 DiffServ Class C	Configuratio	n					
IPv6 Class Configuratio	n	Match Every		Any ×					
Policy Configuration		Reference Class	s	class_e	f v				
 Service Interface Configuration 		Protocol Type		Other	~			(0 to 25	55)
Conliguiation		Source Prefix/Le	ength						
Genice Statistics		Source L4 Port		domain				(0 to 65535)	
		Oestination Pref	fix/Length						
		Oestination L4 F	Port	domain	×			(0 to 65535)	
		Flow Label				(0 to 1048575)			
		IP DSCP		af11	×			(0) to 63)

d. Click the Apply button.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
DiffSer	v	IPv6 Class Informat	ion					
 Diffserv Wizard 		Class Name	classic	npv6				
 Basic 	~	Class Type	All					
 Advanced 	^							
• DiffServ Configu	uration ation	IPv6 DiffServ Class	Configuration					
• IPv6 Class Cor	nfiguration	Match Every		Any ×				
Policy Configure	ration	Reference Class	S	class_e	f ~			
 Service Interfaction 	ce	Protocol Type		ICMPv6	*			(0 to 255)
 Service Statist 	ics	Source Prefix/L	ength					
		Source L4 Port		domain	v			(0 to 65535)
		Oestination President	efix/Length					
		Oestination L4	Port	domain	v			(0 to 65535)
		Flow Label			(0	to 1048575)		
		IP DSCP		af11	×			(0 to 63)

- 3. Create the policy policyicmpv6, and associate the previously created class classicmpv6.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffSer	1					k	!	
DiffS	erv Po	olicy Configuration	1					
Diffserv Wizard		Policy Name		Dolicy Type Mr	ambar Class			
Basic	~	L T OICY Warne		тонсу туре тие	ember Glass			
 Advanced 	~			~	~			
DiffServ Cont	iguration							
Class Config	uration							
• IPv6 Class C	onfiguration							
Policy Config	guration							
 Service Inter Configuration 	face 1							
 Service Stati 	stics							

- b. In the Policy Name field, enter policyicmpv6.
- c. In the Policy Type list, select In.
- d. In the Member Class list, select classicmpv6.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
DiffSe	rv	Policy Configuration	ı					
Diffserv Wizard		Policy Name		Policy Type	Member Class			
Basic	~	noliguismpuß		In a	alassiamm C. y			
 Advanced 	^	policyicinpvo		in ×	classicmpvo *			
DiffServ Config	guration							
Class Configu	ration							
• IPv6 Class Co	infiguration							
Policy Configu	iration							
 Service Interfa Configuration 	ice							
 Service Statis 	tics							

- e. Click Add.
- 4. Set the attribute as assign queue 6.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.

System Switch	ing	Routing	QoS	Securit	y Monitoring	Maintenance	Help	Index
CoS DiffServ								
DiffServ	Poli	cy Configuration						
Diffserv Wizard		Policy Name		Policy Type	Member Class			
• Basic	×	, i unoy riskino		• • • • • •	×			
Advanced OffServ Configuration Class Configuration IPv6 Class Configuration Policy Configuration Service Interface Configuration Service Statistics		policyicmpv6		In	classicmpv6			

- **b.** Click the policy **policyicmpv6**.
- c. In the Assign Queue list, select 6.

A screen similar to the	following displays.
-------------------------	---------------------

System Switching	Routing	20S Security	Monitoring	Maintenance	Help Index	
CoS DiffServ						
DiffServ	Class Information					
Diffserv Wizard	Policy Name	policyicmpv6				
•Basic ~	Policy Type	In				
Advanced	Member Class Name	classicmpv6				
 DiffServ Configuration 						
 Class Configuration 						
IPv6 Class Configuration	Policy Attribute					
 Policy Configuration 	Policy Attribute	Assign Queue		6 ¥		
Service Interface Configuration		Drop				
Sonigo Statistics		Mark VLAN CoS		0. ~		
- Service Statistics		Mark CoS As Sec	condary CoS			
		Mark IP Preceder	ice	0.~		
		Mirror		~		
		Redirect		~		
		Mark IP DSCP		af11 ×		
		Simple Policy				
				Color Mode	Color Bline	d

- 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.

System	Switching		Routing	QoS	Security	Monitorin	ig N	Naintenance	Help	Index
CoS DiffServ					\$	Y				
DiffSe	erv	Servir	ce Interface Co	onfiguration						
Diffserv Wizard	1	13	LAG All			Go To Ir	nterface	Go		
• Basic	~			-						
 Advanced 	~		Interface	F	Policy In Jame	Policy Out Name	Direction	Operational Stat	JS	
DiffServ Config	guration				~	~				
 Class Configu 	uration		1/0/1							
• IPv6 Class Cc	onfiguration		1/0/2							
Policy Config	uration		1/0/3							
T Olicy Conlige	Gracion		1/0/4							
 Service Interfa Configuration 	ace		1/0/5							
- Crasica Chatia			1/0/6							
 Service Staus 	atics		1/0/7							
1			1/0/8							

- b. In the Policy Name list, select policyicmpv6.
- c. Select the Interface 1/0/1, 1/0/2, and 1/0/3 check boxes.

System Switch	ing	Routing	QoS	Security	Monitoring	g M	aintenance
CoS DiffServ							
DiffServ	Servio	ce Interface C	onfiguration				
iffserv Wizard	1 2	LAG All	1.11		Go To li	nterface	G
Basic	× _	100000000000			1000		
Advanced	~ 🗖	Interface		Policy In Name	Policy Out Name	Direction	Operational Stat
 DiffServ Configuration 				policyicmpv6 🗸	~		
 Class Configuration 	1	1/0/1					
 IPv6 Class Configuratio 	n 💌	1/0/2					
Policy Configuration		1/0/3					
r oncy configuration		1/0/4					
Service Interface Configuration		1/0/5					
		1/0/6					
Service Statistics		1/0/7					

d. Click Apply.

A screen similar to the following displays.

System Swi	tching	8	Routing	QoS	Security	Monitorir	ig N	Maintenance	Help	Index
CoS DiffServ		172						*		17
DiffServ		Servi	ce Interface C	onfiguration						
Diffserv Wizard		13	LAG AII			Go To I	nterface	G	o	
• Basic	~		a national and							
Advanced	^		Interface		Policy In Name	Policy Out Name	Direction	Operational Sta	tus	
 DiffServ Configuration 	i	1			×	×				
 Class Configuration 			1/0/1		policyicmpv6		In	Down		
• IPv6 Class Configura	tion		1/0/2		policyicmpv6		In	Down		
Policy Configuration			1/0/3	1	policyicmpv6		In	Down		
T oney configuration	-		1/0/4							
 Service Interface Configuration 			1/0/5							
Contraction of the second s		-	41010							

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) (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)#vlan tagging 5
(Netgear Switch) (Interface 1/0/25)#vlan tagging 5
```

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 transmit	Switch) violate-	(Config-policy-classmap)#police-simple 1000 64 conform-action 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.

Syste	m Sv	witching		Routing	QoS	Security	Monitori	ng	Maintenance	Help	Index
	Auto-VolP	iscsi	STP	Multicast	MVR	Address Table	Ports LAG	MLAG)		
	VLAN		Reset								
Basic		^	Rese	t Configuratio	n						
• VLAN	Configuration	n									
• Advance	bed	~									
			Interna	I VLAN Confi	guration						
			Intern	al VLAN Allo	cation Ba	ise 40	93				
			Intern	al VLAN Allo	cation Po	licy 🔘	Ascending 🖲 D	escendin	g		
			VI AND	Configuration							
			VLAN	conliguration	<u> </u>						
				VLAN ID VL	AN Name	VLAN Type	Make Static				
				5			Disable 👻				
				1 de	fault	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.

Syst	em Si	witching		Routing		QoS		See	curity		М	onito	ring		Ма	ainter	ance			Help		1	ndex		
VLAN	Auto-VolP	iSCSI	STP	Multi	cast	MVR	Ad	dress 1	Table	Po	rts	LAG	6 1	MLAC	3										
	VLAN		VLAN I	Vembei	rship																				
Basic		~	VLAN	ID													1	5 v	1						
• Advanc	ed	~	Group	Operat	tion												1	Unta	a All						
• VLAM	Configuration	1	VLAN	Name													V	LAN	0005						
• VLAI	N Membership		VLAN	Type													S	static							
• VLAM	V Status			nit 1																					
• Port Confi	PVID guration		Ports		3 5	7	9	11 13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
•MAC	Based VLAN								╞																
• Proto Grou	ncol Based VL	AN		2	4 6	8	10	12 14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48

- 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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffSer								
DiffS	erv Cl	ass Name						
Diffserv Wizard	I.	Class Name	i.	Clas	s Type			
 Basic 	~			- Olds				
 Advanced 	^	class_vian		All	~			
DiffServ Con	iguration							
Class Config	uration							
• IPv6 Class C	onfiguration							
 Policy Config 	guration							
 Service Inter Configuration 	face 1							
 Service Stat 	stics							

- **b.** Enter the following information:
 - In the Class Name field, enter class_vlan.
 - In the Class Type list, select All.
- c. Click Add to create a new class class_vlan.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
DiffSe	erv Cla	ass Name						
Diffserv Wizard		Class Name		Class	s Type			
• Basic	~							
 Advanced 	~			All.	·			
DiffServ Confi	guration			240				
Class Configu	uration							

d. Click class_vlan to configure this class.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffSen	(×
DiffS	erv	Class Information						
Diffserv Wizard	ł	Class Name	class_V	LAN				
 Basic 	×	Class Type	All					
 Advanced 	^							
DiffServ Cont	figuration							
Class Config	uration	DiffServ Class Confi	iguration					
• IPv6 Class C	Configuration	Match Every		Any	~			
Policy Config	guration	Reference Class	S I	~				
Service Inter	face	Class Of Service	ce	0 ~				
Conliguration	1	VLAN		5	(1 to 4093)			
• Service Stati	ISTICS	Secondary Cla	ss of Service	0 ~				
		Secondary VLA	AN		(1 to 4093)			

- 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.

System	Switching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ					Ŵ.T				
DiffSon		Class	Name						
- Diffeent Witterd		Ciasa			36				
 Diliserv vvizaru 			Class Name		Clas	s Type			
Basic	~		class color			~			
Advanced	^		elass VI AN		All	E			
DiffServ Configur	ation	9	01033_112/114		7.01				
Class Configurat	tion								
IPv6 Class Confi	guration								
Policy Configura	tion								

- **b.** Enter the following information:
 - In the Class Name field, enter class_color.
 - In the Class Type list, select All.
- c. Click Add to create a new class class_color.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
DiffServ		Class Name						
Diffserv Wizard		Class Name		Clas	s Type			
Basic	*				×			
 Advanced 	~	Class VI AN		All				
DiffServ Configur	ation	<pre>class_color</pre>		All				
Class Configurat	tion							

d. Click class_color to configure this class.

System Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ							
DiffServ	Class Information						
Diffserv Wizard	Class Name	class_co	lor				
•Basic 🗸	Class Type	All					
Advanced							
DiffServ Configuration							
Class Configuration	DiffServ Class Config	uration					
 IPv6 Class Configuration 	Match Every		Any	*			
 Policy Configuration 	Reference Class	3	class	VLAN ×			
Service Interface Configuration	Class Of Service	e	0 ~				
Coniga Statistics	VLAN			(1 to 4093)			
Office Otalistics	Secondary Class	s of Service	0 ~				
	Secondary VLA	N		(1 to 4093)			
	Ethernet Type		Apple	talk 🗸			
	Source MAC		Addre	ss			
	Destination MAG	2	Addre	SS			

- 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.

- 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.

Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
erv	Policy Configuration	1					
	Doliou Nam		Paliou Tuna	Member Class			
~	Believ view		Folicy type 1	Member Class			
^	policy_vian		ln Y	class_vlan Y			
iguration	policy_vian		In				
uration							
onfiguration							
juration							
ace							
stics							
	Switching average of the second secon	switching Routing	switching Routing QoS	Switching Routing QoS Security Policy Configuration Policy Name Policy Type policy_vlan In ~ guration policy_vlan In ~ acce stics stics	switching Routing QaS Security Monitoring	Switching Routing QoS Security Monitoring Maintenance av Policy Configuration Image: Class of the second	Switching Routing QoS Security Monitoring Maintenance Help av Policy Configuration In Class_Vlan In <

- **b.** Under Policy Configuration, scroll down and select the **policy_vlan** check box.
- c. In the Member Class field, enter class_vlan.
- d. Click Apply.
- 7. Configure policy_vlan.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.
 - **b.** Click **policy_vlan**.

Quetum Quetching	Pauling	0.0 Sacanity Mendaning	Maintananca Hade	Index		
CoS Dillion	Routing	Goo Security Monitoring	- Maintenance Prei			
						Cancel Apply
DiffServ	Policy Attribute	④ Assign Queue	0 ~			
Diffserv Wizard		Drop				
•Basic v		Mark VLAN CoS	0 ~			
Advanced A		Mark CoS As Secondary CoS				
DiffServ Configuration		Mark IP Precedence	0 ~			
Class Configuration		Mirror				
IPv6 Class Configuration		Redirect	*			
Policy Configuration		Mark IP DSCP	2011			
Service Interface Configuration		Simple Policy				
Service Statistics			Color Conform Class	class_color ~	Color Mode	Color Aware 👻
			Comitted Rate	1000		
			Comitted Burst Size	64		
			Conform Action	Send		
				() Drop		
				Mark CoS	0 -	
				Mark CoS As Secondary CoS	- Marinell	

- c. Select the Simple Policy radio button.
- d. In the Color Mode list, select Color Aware.
- e. In the Color Conform Class list, select class_color.
- f. In the Committed Rates field, enter 1000.
- g. In the Committed Burst Size field, enter 64.
- h. For Conform Action, select the Send radio button.
- i. For Violate Action, select the Drop radio button.
- j. Click Apply.
- 8. Apply policy_vlan to interface 1/0/13.
 - a. Select QoS > DiffServ > Advanced > Service Interface Configuration.

System	Switching		Routing	QoS	Security	Monitori	ng	Maintenance	Help	Index
CoS DiffServ										
DiffSer	v	Servic	e Interface Co	nfiguration						
Diffserv Wizard		12	LAG AII			Go To li	nterface	Go		
Basic	×	-								
 Advanced 	^		Interface		Policy In Name	Policy Out Name	Direction	Operational Status		
 DiffServ Config 	juration		1/0/13		policy_vlan 👻	~				
Class Configure	ration		1/0/1							
IPv6 Class Co	nfiguration		1/0/2							
Policy Configu	ration		1/0/3							
• Sonico Intorfa	CO		1/0/4							
Configuration	ue .		1/0/5							
 Service Statist 	tics		1/0/6							
			1/0/7							
			1/0/8							
			1/0/9							
			1/0/10							
			1/0/11							
			1/0/12							
			1/0/13							

- **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.

IGMP Snooping and Querier

Internet Group Management Protocol features

16

This chapter includes the following sections:

- Internet Group Management Protocol Concepts
- IGMP Snooping
- Show igmpsnooping
- Show mac-address-table igmpsnooping
- External Multicast Router
- Multicast Router Using VLAN
- IGMP Querier Concepts
- Enable IGMP Querier
- Show IGMP Querier Status

Internet Group Management Protocol Concepts

NETGEAR implements Internet Group Management Protocol (IGMP) in the following way:

- IGMP uses version 1, version 2, or version 3.
- IGMP includes snooping.
- You can enable IGMP snooping on a per-VLAN basis.

IGMP Snooping

The following are examples of the commands used in the IGMP snooping feature.

CLI: Enable IGMP Snooping

The following example shows how to enable IGMP snooping.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#set igmp
(Netgear Switch) (Config)#exit
```

Web Interface: Enable IGMP Snooping

Configure IGMP snooping:

1. Select Switching > Multicast > IGMP Snooping Configuration.

Syste	em S	Switching		Routing	QoS	Security	N	Aonitoring		Maintenance	Help	Index	
VLAN	Auto-VolP	iSCSI	STP		MVR	Address Table	Ports	LAG	MLAG	;			
	Multicast		IGMP S	nooping Con	figuration	-							
• MFDB		v	Admin	Mode			🔘 Di	sable 🛞 E	nable				
IGMP S	Snooping	~	Multica	ast Control F	rame Co	unt	0						
• Config	guration		Valida	te IGMP IP h	ieader		🔘 Di	sable 🖲 E	nable				
• Interfa	ace Configura	ation	Interfa	ces Enabled	for IGMF	9 Snooping							
• IGMF Config	VLAN guration		Proxy	Querier Mod	e		🔘 Di	sable 🖲 E	nable				
• Multic Confi	cast Router guration		10.01.0		IOMP								
• Multic Config	cast Router \ guration	VLAN	VLAN IL	JS Enabled ti	or IGIVIP	Shooping							
• Queri	er Configurat	ion											
• Queri Confi	er VLAN guration												
• MLD Sr	nooping	×											

- 2. For Admin Mode select the Enable radio button.
- 3. For Unknown Multicast Filtering, select the Enable radio button.
- 4. Click Apply.

Show igmpsnooping

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

CLI: Show igmpsnooping

(Netgear Switch) #show igmpsnooping Admin Mode..... Disable Multicast Control Frame Count..... 0 Interfaces Enabled for IGMP Snooping..... None VLANs enabled for IGMP snooping..... None

Web Interface: Show igmpsnooping

Select **Switching > Multicast > IGMP Snooping Configuration**. A screen similar to the following displays.

System	S	witching		Routing	QoS	Security		Monitorin	g	Maintenance	Help	Index
VLAN Auto	-VolP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAG			
	240											
Multi	icast		IGMP S	Snooping Co	nfiguration							
 MFDB 		~	Admir	Mode			O D	sable 💿	Enable			
 IGMP Snoopir 	ng	~	Multic	ast Control I	rame Co	unt	0					
Configuratio	n		Valida	te IGMP IP	neader		O D	sable 💿	Enable			
 Interface Co 	onfigurat	ion	Interfa	ces Enablec	for IGMP	Snooping						
 IGMP VLAN Configuratio 	l In		Proxy	Querier Moo	le		O D	sable 💿	Enable			
 Multicast Re Configuration 	outer m		10 411			0						
 Multicast Re Configuratio 	outer VI in	LAN	VLANT	Us Enabled	or IGIVIP :	Shooping						
Querier Con	figuratio	on										
 Querier VLA Configuratio 	AN m											
• MLD Snooping	g	~										

Show mac-address-table igmpsnooping

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

CLI for IGMPv1 and IGMPv2: Show mac-address-table igmpsnooping

(Netgear Switch) #show mac	-address-ta	able igmpsnooping ?	
<cr></cr>	ress Enter	to execute the com	mand.
(Netgear Switch) #show mac	-address-ta	able igmpsnooping	
	Туре	Description	Interfaces
00:01:01:00:5E:00:01:16	Dynamic	Network Assist	Fwd: 1/0/47
00:01:01:00:5E:00:01:18	Dynamic	Network Assist	Fwd: 1/0/47
00:01:01:00:5E:37:96:D0	Dynamic	Network Assist	Fwd: 1/0/47
00:01:01:00:5E:7F:FF:FA	Dynamic	Network Assist	Fwd: 1/0/47
00:01:01:00:5E:7F:FF:FE	Dynamic	Network Assist	Fwd: 1/0/47

CLI for IGMPv3: show igmpsnooping ssm entries

(Net	gear Switch) #show igmp:	snooping ssm entries		
VLAN			Source	
ID	Group	Source Ip	Filter Mode	Interfaces
1000	224.1.1.1	1.1.1.1	include	1/0/2

Web Interface: Show mac-address-table igmpsnooping

Select Switching > Multicast > IGMP Snooping Table.

A screen similar to the following displays.

Syst	em 🗾	Switching	Routing	QoS	Security	/ Monit	oring	Maintenance	Help	Index
VLAN	Auto-VolF	iscsi	STP Multica	at MVR	Address Table	Ports LA	G ML	AG	· · · ·	×
	Multicast		MFDB Table							
• MFDB		^			Search M	AC Address		Go		
• MFD	B Table				Contentin			21-12		
• MFD	B Statistics		MAC Address	VLAN ID	Component 1	ype Description	on For	warding Interfaces		
IGMP S	Snooping	*								
• MLD S	nooping	v								

External Multicast Router

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

CLI: Configure the Switch with an External Multicast Router

This example configures the interface as the one the multicast router is attached to. All IGMP packets that are snooped by the switch are forwarded to the multicast router that is reachable from this interface.

(Netgear Switch)(Interface 1/0/3)# set igmp mrouter interface

Web Interface: Configure the Switch with an External Multicast Router

1. Select Switching > Multicast > Multicast Router Configuration.

Syst	em Sv	vitching		Routing	QoS	Security	Monitoring M	laintenance	Help	Index
VLAN	Auto-VolP	iSCSI	STF	Multic:	ast MVR	Address Table Po	ts LAG MLAG			10
	100000-000 - 100									
	Multicast		IGMF	Snooping	Interface Conf	iguration				
• MFDB		~	12	3 LAG AII				Go To In	terface	Go
•IGMP \$	Snooping	^		Interface	Admin Mode	Membership Interva	I Max Response Time	Expiration Time	Fast Leave	Proxy Querier
* Confi	guration			1/0/2	Enable y	260	110	0	Disable	Enable at
 Interf 	ace Configurat	ion		1/0/5	Enable *	200	10	0	Disable •	Enable *
LOLAT	2.2.11			1/0/1	Disable	260	10	0	Disable	Enable
• IGIVIE	² VLAN			1/0/2	Disable	260	10	0	Disable	Enable
Oom	guration			1/0/3	Disable	260	10	0	Disable	Enable
 Multi Confi 	cast Router			1/0/4	Disable	260	10	0	Disable	Enable

- 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.

Syste	m	Switching		Routing	QoS	Security	N	lonitoring	3	Maintenance	Help	Index
VLAN	Auto-VolP	iscsi	STP		MVR	Address Table	Ports	LAG	MLAG			
	Multicast		Multica	st Router V	LAN Conf	iguration						
• MFDB		~	Interfa	се	1/0/3	~						
IGMP S	nooping	^										
• Confi	guration											
• Interfa	ace Configu	ration	Multica	st Router V	LAN Conf	iguration						
 IGMF Confid 	VLAN		• •	/LAN ID	Multicast	t Router						
• Multic Confi	ast Router guration			2	Enable	×						
• Multic Confi	ast Router guration	VLAN										

- 2. Under Multicast Router VLAN Configuration, scroll down and select the Interface 1/0/3 check box.
- 3. Enter the following information in the Multicast Router VLAN Configuration.
 - In the VLAN ID field, enter 2.
 - In the Multicast Router field, select Enable.
- 4. Click Apply.

IGMP Querier Concepts

When the switch is used in network applications where video services such as IPTV, video streaming, and gaming are deployed, the video traffic is normally flooded to all connected ports because such traffic packets usually have multicast Ethernet addresses. IGMP snooping can be enabled to create a multicast group to direct that traffic only to those users that require it.

However, the IGMP snooping operation usually requires an extra network device—usually a router—that can generate an IGMP membership query and solicit interested nodes to respond. With the built-in IGMP querier feature inside the switch, such an external device is no longer needed.



Figure 32. 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)#set igmp querier
```

Web Interface: Enable IGMP Querier

1. Select Switching > Multicast > IGMP VLAN Configuration.

Syst	em Sv	vitching		Routing	QoS	Security		Monitorin	ıg	Maintenance	Help	Index
VLAN	Auto-VolP	iscsi	STP	Multicast	MVR	Address Table	Ports	LAG	MLA	3	йШ.н	
	Multicast		IGMP S	Snooping Co	nfiguration	8						
• MFDB		*	Admir	Mode) Di	sable 🔘	Enable	9		
• IGMP \$	Snooping	~	Multic	ast Control	rame Cou	int	0					
• Confi	guration		Valida	te IGMP IP	header) Di	sable 🔘	Enable	3		
• Interf	ace Configurat	ion	Interfa	ces Enabled	for IGMP	Snooping						
• IGMF Confi	P VLAN guration		Proxy	Querier Mo	de) Di	sable 🖲	Enable	9		
• Multi Confi	cast Router guration		1/I AN II									
• Multi	cast Router VI	_AN	VLAN	US ENADIED	IUT IGIVIP 5	snooping						

- 2. Enable IGMP snooping on VLAN 1.
 - a. Select Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration.

Syste	em	Swi	tching	Routing		QoS	Security	Monitoring	Maintenance	Help Index		
VLAN	Auto-Vo	olP	iscsi	STF) Multica	st MVR A	Address Table	Ports LAG MI	AG			
1	Multione	at	_	ICME	MAN Cor	fouration						
<i>u</i> :	wuncas	st		IGIVIP	VLAN CO	inguration						
• MFDB • IGMP S	Snooping		×	•	VLAN ID	Admin Mode	Fast Leave	Membership Interval	Maximum Response Time	e Multicast Router Expiry Time	Report Suppression	Proxy Querier
• Config	guration				1	Enable 👻	×.				×	×
• Interfa	ace Con <mark>f</mark> ig	guratio	on									
IGMF Confi	P VLAN guration											

- **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.

System Switching	Routing	QoS	Security	Monitori	ng	Maintenance	Help	Index
VLAN Auto-VolP iSCSI	STP Multicast	MVR A	ddress Table	Ports LAG	MLAG			
Multicast	Querier Configuratio	n						
•MFDB ~	Querier Admin Mo	de	🔘 Disa	ible 💿 Enable				
IGMP Snooping A	Snooping Querier	Address	10.10.1	10.1				
Configuration	IGMP Version		2		(1 to 2)			
 Interface Configuration 	Query Interval(sec:	s)	60		(1 to 18	00)		
 IGMP VLAN Configuration 	Querier Expiry Inte	rval(secs)	60		(60 to 3	00)		
 Multicast Router Configuration 								
 Multicast Router VLAN Configuration 	VLAN IDS Enabled I	or IGIVIP Sh	ooping Querier					
Querier Configuration								

- **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.

System	n Sw	itching		Routing	QoS	Security	Monitoring	Mainter	iance H	lelp Ind	ex
VLAN .	Auto-VolP	iscsi	STP	Multica	iai MVR Ad	dress Table P	orts LAG N	ЛLAG			
1	Multicast		IGMP	Snooping	Querier VLAN Co	nfiguration					
• MFDB • IGMP Sn	looping	~		VLAN ID	Querier Election Participate Mod	Querier VLAf Address	N Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Max Response Time
• Configu	uration			1	~						
• Interfac	e Configurati	on									
 IGMP \ Configu 	VLAN uration										
• Multica Configu	ast Router uration										
 Multica Configu 	ast Router VL uration	AN									
• Querier	r Configuratio	n									
Querier Configu	r VLAN tration										

- 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.

The command shows that the IGMP admin mode is Active. The mode is controlled by the set igmp command. If the mode is inactive, no query packet is sent.

Web Interface: Show IGMP Querier Status

1. Select Switching > Multicast > IGMP Snooping > Querier Configuration.

A screen similar to the following displays.

Syst	em	Switching		Routing	QoS	Security		Monitorin	g	Maintenance	Help	Index
VLAN	Auto-VolF	iscsi	STP		MVR	Address Table	Ports	LAG	ML	AG		
	Multicast		Querier	Configuratio	n							
• MFDB		~	Quer	ier Admin M	ode	Dis	able 🔘	Enable				
· IGMP \$	Snooping	^	Snoo	ping Querier	Address	0.0.0.	0					
• Confi	guration		IGMF	Version		2			(1 to	o 2)		
• Interf	ace Configu	ration	Quer	y Interval(see	s)	60			(1 to	o 1800)		
• IGMF Confi	VLAN guration		Quer	ier Expiry Int	erval(secs)	125			(60	to 300)		
• Multi Confi	cast Router guration											
• Multi Confi	cast Router guration	VLAN	VLAN I	Ds Enabled	for IGMP S	nooping Querier						
• Quer	ier Configura	ation										
• Quer Confi	ier VLAN guration											
• MLD S	nooping	~										

2. Click Refresh.

MVR

Multicast VLAN Registration

17

This chapter includes the following sections:

- Multicast VLAN Registration
- Configure MVR in Compatible Mode
- Configure MVR in Dynamic Mode

Multicast VLAN Registration

The IGMP Layer 3 protocol is widely used for IPv4 network multicasting. In Layer 2 networks, the IGMP protocol uses resources inefficiently. For example, a Layer 2 switch multicast traffic to all ports even if there are receivers connected to only a few ports.

To fix this problem, the IGMP snooping protocol was developed. But the problem reappears when receivers are in different VLANs. Multicast VLAN registration (MVR) is intended to solve the problem of receivers in different VLANs. It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.

MVR, like the IGMP Snooping protocol, allows a Layer 2 switch to snoop on the IGMP control protocol. Both protocols operate independently of each other. Both protocols can be enabled on the switch interfaces at the same time. In such a case, MVR listens to the join and report messages only for groups configured statically. All other groups are managed by IGMP snooping.

There are two types of MVR ports: source and receiver.

- The source port is the port to which the multicast traffic flows using the multicast VLAN.
- The receiver port is the port where a listening host is connected to the switch. It can
 utilize any (or no) VLAN, except the multicast VLAN. This implies that the MVR switch
 performs VLAN tag substitution from the multicast VLAN source port to the VLAN tag
 used by the receiver port.

The multicast VLAN is the VLAN that you configure in the specific network for MVR purposes. The multicast VLAN is used to transfer multicast traffic over the network to avoid duplication of multicast streams for clients in different VLANs. The operator must configure the multicast VLAN manually for all source ports in the network. A diagram of a network configured for MVR is shown in the following illustration. SP is the source port and RP is the receiver port.

Managed Switches



Figure 33. 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.

Managed Switches

```
(Netgear Switch) (Config)#interface 0/1
(Netgear Switch) (Interface 0/1) #vlan participation include 1001
(Netgear Switch) (Interface 0/1) #vlan pvid 1001
(Netgear Switch) (Interface 0/1)#vlan participation exclude 1
(Netgear Switch) (Interface 0/1)#mvr
(Netgear Switch) (Interface 0/1)#mvr type receiver
(Netgear Switch) (Interface 0/1)#mvr vlan 999 group 224.1.2.3
(Netgear Switch) (Interface 0/1)#exit
(Netgear Switch) (Config)#interface 0/5
(Netgear Switch) (Interface 0/5)#vlan participation include 1002
(Netgear Switch) (Interface 0/5) #vlan pvid 1002
(Netgear Switch) (Interface 0/5) #vlan participation exclude 1
(Netgear Switch) (Interface 0/5)#mvr
(Netgear Switch) (Interface 0/5)#mvr stype receiver
(Netgear Switch) (Interface 0/5)#mvr vlan 999 group 224.1.2.3
(Netgear Switch) (Interface 0/5)#exit
(Netgear Switch) (Config)#interface 0/7
(Netgear Switch) (Interface 0/7) #vlan participation include1003
(Netgear Switch) (Interface 0/7) #vlan pvid 1003
(Netgear Switch) (Interface 0/7) #vlan participation exclude 1
(Netgear Switch) (Interface 0/7)#mvr
(Netgear Switch) (Interface 0/7)#mvr type receiver
(Netgear Switch) (Interface 0/7)#mvr vlan 999 group 224.1.2.3
(Netgear Switch) (Interface 0/7)#exit
```

5. Display the MVR status.

(Netgear Swit	cch) #show mvr										
MVR Running.		TRUE									
MVR multicast	ULAN	999									
MVR Max Mult:	icast Groups	256									
MVR Current r	multicast groups	1									
MVR Global qu	ery response time.	5 (tenths of sec)									
MVR Mode		compatible									
(Netgear Sw:	itch) #show mvr inte	erface									
Port	Туре	Status	Immediate Leave								
0/1	RECEIVER	ACTIVE/InVLAN	DISABLED								
0/5	/5 RECEIVER ACTIVE/InVLAN DISABLED										
0/7	/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.

Syst	em	Switching		Routing	QoS	Security	Monitorir	ng	Maintenance	Help	Index
VLAN	Auto-Voll	iscsi	STF	Multicas	t MVR	Address Table	Ports LAG	MLAG	G		
	VLAN		Reset								
• Basic		^	Res	et Configurat	ion						
• VLA	N Configura	tion									
• Advanc	ed.	~									
			Intern	al VLAN Cor	figuration						
			Inter	nal VLAN Al	location Bas	se 40	93				
			Inter	nal VLAN Al	location Pol	icy 🔘	Ascending 🖲 De	escendir	ng		
			VLAN	Configuratio	n						
				VLAN ID	/LAN Name	VLAN Type	Make Static				
				999	mVlan		Disable 🛩				
				1 (lefault	Default	Disable				
				3 1	/LAN0003	Static	Disable				
				10 \	/LAN0010	Static	Disable				

- 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.

Syst	em Si	witching		Routing	QoS		Securi	y	N	lonitori	ng	1	Mainte	nance	•		Help		lr	ndex		
VLAN	Auto-VolP	iscsi	STP	Multicast	MVR	Addre	ess Tabl	e F	orts	LAG	ML	AG										
	VLAN			/lembership																		
• Basic		~	VLAN	ID											999	~						
• Advanc	ed	~	Group	Operation											Unta	ig All	~					
- VLAN	Configuration	ń.	VLAN	Name										T	nVlar	n			0			
• VLAN	N Membership		VLAN	Туре											Static							
• VLAN	V Status			nit 1																		
• Port I Confi • MAC	PVID guration Based VLAN		Ports		5 7	9 11 T	13	5 17	19	21	23 2	5 27	29	31	33	35	37	39	41	43	45	47
• Proto Grou	col Based VL p Configuration	AN n		2 4	6 8	10 12	14 1	6 18	20	22	24 2	6 28	30	32	34	36	38	40	42	44	46	48

- 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.

Syste	em	Sw	vitching	F	Routing	QoS	Security	N	Aonitorin	g	Maintenance	Help	Index
VLAN	Auto-V	olP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAG	5		
	MVR			MVR C	onfiguration								
 Basic 			^	MVR	Running			Oisable	le 🔘 Ena	able			
• MVR	Configura	ation		MVR	Multicast VI	an		999		(1 to 40	93)		
* Advanc	ed		~	MVR	Max Multica	ast Group	S	256					
				MVR	Current Mult	ticast Gro	oups	0					
				MVR	Global quer	y respons	se time	5		(1 to 10	0)		
				MVR	Mode			compare	atible 🔘	dynamic	C		

- **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.

Syst	em	Sv	vitching		Routing	QoS	Security	Monit	oring	Mainten	ance	Help	Index
VLAN	Auto-	VolP	iSCSI	STP	Multicast	MVR	Address Table	Ports LA	G ML	AG			
	MV	R		MVR G	roup Configu	iration							
•Basic			~		MVR Group	IP			Status	Members	Count		
• Advanc	ed		~		224.1.2.3								
• MVR	Configu	uration								14.6			
• MVR Confi	Group guration												
• MVR Confi	Interfac guratior	ce 1											
• MVR	Group	Membe	ership										
• MVR	Statist	ics											

- b. In the MVR Group IP field, enter 224.1.2.3.
- c. Click Add.
- 5. Configure a receiver on interface 0/1, 0/5, and 0/7.
 - a. Select Switching > MVR > Basic > MVR Interface Configuration.

System Sw	itching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VLAN Auto-VolP	iSCSI	STR	o Multic	ast MVR	Address Table	Ports LAG	MLAG		<i>.</i>)
MVR		MVR	Interface (Configuration					
Basic	~	12	3 All		Go	To Interface	Go		
Advanced	^		Interface	Admin Mode	Type	Immediate Leave	Status		
 MVR Configuration 				~	×	~	and the second s		
 MVR Group Configuration 			1/0/1	Disable	none	Disable	Active/InVLAN		
• MVR Interface			1/0/2	Disable	none	Disable	Inactive/InVLAN		
Configuration			1/0/3	Disable	none	Disable	Inactive/InVLAN		
• MVR Group Membe	rship		1/0/4	Disable	none	Disable	Inactive/InVLAN		
	1		1/0/5	Disable	none	Disable	Inactive/InVLAN		
• WIVE Statistics			1/0/6	Disable	none	Disable	Inactive/InVLAN		
			1/0/7	Disable	none	Disable	Inactive/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.

System Switchi	ng	Routing	QoS	Security	Monitoring	g Maintenance	Help	Index
VLAN Auto-VolP iSC	SI S	TP Multic	ast MVR	Address Table	Ports LAG	MLAG		
MVR				s 1-				
		Interface	Admin Mode	Туре	Immediate Leave	Status		
* Basic	~	1/0/9	Disable ×	source ×	Disable ~	Inactive/InVI AN		
 Advanced 	^	1/0/1	Dicable	0000	Dicabla	Activo/In//LAN		
 MVR Configuration 	6	1/0/1	Disable	none	Disable	Inactive/InVLAN		
• MV/P Group	1	1/0/2	Disable	none	Disable	Inactive/InVLAN		
Configuration	1	1/0/4	Disable	none	Disable	Inactive/InVLAN		
MVR Interface	(] 1/0/5	Disable	none	Disable	Inactive/InVLAN		
Configuration		1/0/6	Disable	none	Disable	Inactive/InVLAN		
• MVR Group Membership	p (1/0/7	Disable	none	Disable	Inactive/InVLAN		
 MVR Statistics 	0	1/0/8	Disable	none	Disable	Inactive/InVLAN		
	6	1/0/9	Disable	none	Disable	Inactive/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.
- 7. Configure MVR Group Membership.
 - a. Select Switching > MVR > Advanced > MVR Membership.

Syste	em	Switching		Routing	QoS	;	Security	li,	Monite	oring	M	laintenance		Help	l	ndex
VLAN	Auto-VolP	iscsi	STP	Multicast	MVR	Addre	ess Table	Port	s LA	G N	/ILAG					
	MVR		MVR G	iroup Memb	ership											
Basic Advance	ed	*	Group	IP nit 1						22	4.1.2.3	*				
• MVR • MVR Config • MVR Config	Configuration Group guration Interface guration	n	Ports	1 3	5 7 2 2 6 8	9 11 9 11 10 12	13 15 13 15 14 16	17 17 18	19 21 19 21 20 22	23	25 27 26 28	29 31 29 1 29 31 30 32	33 35 1 1 1 1 1 1 1 1	37 1000	39 41 40 42	43
• MVR • MVR	Group Men Statistics	nbership	Ports	nit 2	5 7	9 11	13 15	17	19 21	23						
				2 4	6 8	10 12	14 16	18	20 22	24						

- 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)#vlan name 1003 Vlan3 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.

Managed Switches

```
(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 Swit	cch) #show mvr		
MVR Running.		TRUE	
MVR multicast	z VLAN	999	
MVR Max Mult:	icast Groups	256	
MVR Current n	multicast groups	1	
MVR Global qu	aery response time.	5 (tenths of sec)	
MVR Mode		compatible	
(Netgear Sw:	itch) #show mvr inte	erface	
Port	Туре	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.

Syste	em 🤤	Switching		Routing	QoS	Security	Monito	ring	Maintenance	Help	Index
VLAN	Auto-VolP	iSCSI	STF	Multicas	MVR	Address Table	Ports LAG	G MLAG	3		
	VLAN		Reset								
 Basic 		¥	Res	et Configurat	ion	0					
• Advanc	ed	^									
• VLAN	I Configuration	on									
• VLAN	l Membershi	р	Intern	al VLAN Cor	figuration						
• VLAN	l Status		Inter	nal VLAN Al	location Bas	e 40	93				
• Port I Confi	⊃VID guration		Inter	nal VLAN AI	location Poli	су 🔘	Ascending 🖲	Descendir	ıg		
• MAC	Based VLA	N									
• Proto Group	col Based V p Configuration	LAN on	VLAN	Configuratio	n	-22					
• Proto	col Based V	LAN		VLAN ID	/LAN Name	VLAN Type	Make Static				
Grou	p Membershi	p		999	mVlan	Static	Disable 🛩				
IP SU VLAN	ibnet Based ↓			1 0	lefault	Default	Disable				

- 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.

Syste	em S	Switching		Routing	QoS		Security	3	Мо	nitoring]	Ma	intenar	ice	8	Help		li	ıdex
	Auto-VolP	iSCSI	STP	Multicast	MVR	Addre	ss Table	Por	ts	LAG	MLAC	3							
	VLAN		VLAN I	Vembership															
• Basic		~	VLAN	ID										999	~				
 Advanc 	ed	^	Group	Operation										Unt	ag All	v			
• VLAN	I Configuratio	n	VLAN	Name										mVIa	an			1	
• VLAN	l Membershi	p	VLAN	Туре										Stati	с				
- VLAN	l Status		-	lucia d															
 Port F Config 	PVID guration		Ports	1 3	5 7	9 11	13 15	17	19	21 23	3 25	27	29 3	1 33	35	37	39	41	43
-MAC	Based VLAN	1				T							ا ک						
• Proto	col Based VI	LAN				10 12	14 16	18	20	22 2	1 26	28	30 3	2 34	36	38	40	42	44
Group	ooninguruure				0	10 12	14 10	10	20		20	20	00 0.		00	00			44

- 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.

Syst	em	Sw	ritching		Routing	QoS	Security	Mo	nitoring	Maintenance	Help	Index
VLAN	Auto-V	olP	iSCSI	STP	Multicast	MVR	Address Table	Ports I	LAG MI	LAG		
	MVR	e.		MVR C	onfiguration							
• Basic			^	MVR	Running			Disable (Enable			
• MVR	Configur	ation		MVR	Multicast V	lan		999	(1 to	o 4093)		
• Advanc	ed		~	MVR	Max Multic	ast Groups		256				
				MVR	Current Mu	ticast Grou	ips	1				
				MVR	Global quer	y response	time	5	(1 to	o 100)		
				MVR	Mode			compatit	ole 🔘 dyna	amic		

- 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.

em	Switch	ing	F	Routing	QoS	Security		Monitori	ng	Mainten	апсе	Help	Index
Auto-Vol	P iSC	SI S	TP	Multicast	MVR	Address Table	Ports	LAG	MLA	AG			
MVR		MV	/R Gr	oup Configu	iration								
		~		AVR Group	IP				Status	Members	Count		
ed		^	1	224.1.2.3									
Configurati	on	_						10					
Group guration													
Interface guration													
Group Mer	nbershi	р											
Statistics													
	MVR Auto-Volf MVR ed Configurati Group guration Interface guration Group Mer Statistics	m Switch Auto-VolP iSC MVR ed Configuration Group juration Group Membershi Statistics	Switching Auto-VolP iSCSI S MVR MV ed ~ Configuration	Switching F Auto-VolP iSCSI STP MVR MVR MVR ed ^ Image: Configuration Group Juration Image: Configuration Group Membership Statistics	Switching Routing Auto-VolP iSCSI STP Multicast MVR MVR Group Configuration MVR Group 224,12,3 Group guration Interface guration STP MVR Group Group guration Statistics Statistics Statistics	Switching Routing QoS Auto-VolP iSCSI STP Multicast MVR MVR MVR Group Configuration MVR Group IP 224,12,3 ed ^ 224,12,3 . Group puration Interface . . Statistics . . .	Switching Routing QoS Security Auto-VolP iSCSI STP Multicast MVR Address Table MVR MVR Group Configuration	switching Routing QoS Security I Auto-VoIP ISCSI STP Multicast MVR Address Table Ports MVR MVR Group Configuration MVR Group IP Image: Configuration Image:	Switching Routing QoS Security Monitori Auto-VolP ISCSI STP Multicast MVR Address Table Ports LAG MVR MVR Group Configuration	Switching Routing QoS Security Monitoring Auto-VoIP ISCSI STP Multicast MVR Address Table Ports LAG MLA MVR MVR Group Configuration	Switching Routing QoS Security Monitoring Mainten Auto-VolP ISCSI STP Multicast MVR Address Table Ports LAG MLAG MVR MVR Group Configuration MVR Group IP Status Members ed ^ Image: Configuration Status Members Group guration Image: Configuration Status Members Group guration For particular and particular an	Switching Routing QoS Security Monitoring Maintenance Auto-VolP ISCSI STP Multicast MVR Address Table Ports LAG MLAG MVR MVR Group Configuration MVR Group IP Status Members Count ed ^ 224,12.3	Switching Routing QoS Security Monitoring Maintenance Help Auto-VoIP ISCSI STP Multicast MVR Address Table Ports LAG MLAG MVR MVR Group Configuration MVR Group IP Status Members Count ed

- **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.

System Swit	tching		Routing	QoS	Security	Monitoring	Maintenan	ce Help	Index
VLAN Auto-VolP	iSCSI	STF	^o Multica	ast MVR	Address Table	Ports LAG	MLAG		
MVR	-	MVR	Interface C	Configuration					
• Basic	~	1 2	3 All		Go	To Interface	Go		
 Advanced MVR Configuration 	^		Interface	Admin Mode	Туре	Immediate Leave	Status		
• MVR Conliguration				~	~	~			
Configuration			1/0/1	Disable	none	Disable	Active/InVLAN		
MVP Interface			1/0/2	Disable	none	Disable	Inactive/InVLAN		
Configuration			1/0/3	Disable	none	Disable	Inactive/InVLAN		
• MVR Group Member	ship		1/0/4	Disable	none	Disable	Inactive/InVLAN		
the manual states			1/0/5	Disable	none	Disable	Inactive/InVLAN		
 MVR Statistics 			1/0/6	Disable	none	Disable	Inactive/InVLAN		
			1/0/7	Disable	none	Disable	Inactive/InVLAN		

- 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.

System	Switching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VLAN Auto-VolP	iSCSI	STP	Multica	st MVR A	Address Table	Ports LAG	MLAG		
MVR		MVR	nterface C	onfiguration					
Basic	~	1.0	A.II.			Co To Interface	00		
		1 Z	All			Go to intenace	60		
Advanced	^		Interface	Admin Mode	Type	Immediate Leave	Status		
 MVR Configuratio 	n		4/0/0	Tault a		Discritica	The second state and		
• MVR Group			1/0/9	Enable *	source *	Disable *	Inactive/InvLAIN		
Configuration			1/0/1	Enable	receiver	Disable	Inactive/InVLAN		
• MVR Interface			1/0/2	Disable	none	Disable	Inactive/InVLAN		
Configuration			1/0/3	Disable	none	Disable	Inactive/InVLAN		
• MVR Group Mem	bership		1/0/4	Disable	none	Disable	Inactive/NotInVLAN		
more oroup more	boromp		1/0/5	Enable	receiver	Disable	Inactive/InVLAN		
• MVR Statistics			1/0/6	Disable	none	Disable	Inactive/InVLAN		
			1/0/7	Enable	receiver	Disable	Inactive/InVLAN		
			1/0/8	Disable	none	Disable	Inactive/InVLAN		
			1/0/9	Enable	none	Disable	Inactive/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.

Syst	em	Sw	ritching		Routing	ň	Qo	5		Secu	irity		М	onito	ring		Ma	aintena	псе		Help	Х.	Ir	ıdex
VLAN	Auto-	VolP	iSCSI	STP	Multi	cast	MVR	A	ddres	ss Ta	ble	Po	rts	LAG	6 1	MLAG	3							
	MV	R		MVR G	roup M	ember	ship																	
• Basic			~	Group	IP										2	24.1	23 .	,						
• Advanc	ed		^	-											24									
• MVR	Configu	iration		U	nit 1			100	1007			100		- 20		0.0047							100	
• MVR	Group			Ports		3 5		9	11	13	15	1/	19	21	23	25	27	29	31 33	35	37	39	41	43
• MV/D	Interfac	1																						
Confi	guration	1			2	4 6	8	10	12	14	16	18	20	22	24	26	28	30	32 34	36	38	40	42	44
• MVR	Group	Membe	ership	U	nit 2																			
• MVR	Statisti	ics		Ports	1	3 5	7	9	11	13	15	17	19	21	23									
					2	4 6		10	12	14	16	18	20	22	24									
					2			10	12	14	10	10	20	LL	24									

Security Management

Port security features

This chapter includes the following sections:

- Port Security Concepts
- Set the Dynamic and Static Limit on Port 1/0/1
- Convert the Dynamic Address Learned from 1/0/1 to a Static Address

18

- Create a Static Address
- Protected Ports
- 802.1x Port Security
- Create a Guest VLAN
- Assign VLANs Using RADIUS
- Dynamic ARP Inspection
- Static Mapping
- DHCP Snooping
- Find a Rogue DHCP Server
- Enter Static Binding into the Binding Database
- Maximum Rate of DHCP Messages
- IP Source Guard
- Authorization
- Accounting
- Use the Authentication Manager to Set Up an Authentication Method List

Port Security Concepts

Port security helps to secure the network by preventing unknown devices from forwarding packets. When a link goes down, all dynamically locked addresses are freed. The port security feature offers the following benefits:

- You can limit the number of MAC addresses on a given port. Packets that have a matching MAC address (secure packets) are forwarded; all other packets (unsecure packets) are restricted.
- You can enable port security on a per port basis.

Port security implements two traffic filtering methods, dynamic locking and static locking. These methods can be used concurrently.

• **Dynamic locking**. You can specify the maximum number of MAC addresses that can be learned on a port. The maximum number of MAC addresses is platform-dependent and is listed in the software release notes. After the limit is reached, additional MAC addresses are not learned. Only frames with allowable source MAC addresses are forwarded.

Note: If you want to set a specific MAC address for a port, set the dynamic entries to 0, then allow only packets with a MAC address matching the MAC address in the static list.

Dynamically locked addresses can be converted to statically locked addresses. Dynamically locked MAC addresses are aged out if another packet with that address is not seen within the age-out time. You can set the time-out value. Dynamically locked MAC addresses are eligible to be learned by another port. Static MAC addresses are not eligible for aging.

• **Static locking**. You can manually specify a list of static MAC addresses for a port. Dynamically locked addresses can be converted to statically locked addresses.

Set the Dynamic and Static Limit on Port 1/0/1

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

CLI: Set the Dynamic and Static Limit on Port 1/0/1

(Netgear Switch)	(Netgear Switch) (Config) #port-security											
Enable port-secu	urity globally											
(Netgear Switch)) (Config)#interface 1/	0/1										
(Netgear Switch)) (Interface 1/0/1)#por	t-security										
Enable port-secu	urity 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 l	Set the static limit to 3											
(Netgear Switch)) (Interface 1/0/1)#ex											
(Netgear Switch)) (Config)#ex											
(Netgear Switch)) #show port-security 1	/0/1										
Admin	Dynamic	Static	Violation									
Intf Mode Limit Limit Trap Mode												
1/0/1 Disabl	led 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.

System	Swite	ching	R	outing	QoS	Secu	ity	Monitoring	Maintena	nce	Help	Index
Management S	Security	Acc	ess Po	rt Authentio	cation 1		Control	ACL				
Traffic C	Control		Port Sec	urity Settin	igs							
 MAC Filter 		~	Port Se	curity Mod	е	O Disable	Enable					
Port Security		~										
Port Adminis	stration											
Interface Cor	nfiguration	1	Port Sec	urity Violat	ions							
• Dynamic MA • Static MAC .	AC Addres Address	55	Port	Last Vio	lation MA	KC V	'LAN ID					

- **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.

System Sv	vitching		Routin	g QoS	Security Monito	oring Maintenance	Help li
Management Security	Acce	ess	Port Au	thentication T	affic Control Control ACI		
Traffic Control		Interf	ace Cont	figuration			
MAC Filter	~	12	3 LAG	All		Go To Port	Go
Port Security	^		Deat	O a succión a Marsia	May Long MAC Address	Mary Challe MAC Address	Violation Tran
Port Administration		-	Pon	Security Mode	Wax Learned WAC Address	Max Static MAC Address	violation Trap
Interface Configurat	ioni		1/0/1	Enable Y	10	3	Disable 🛩
- intenace conligurat	1011		1/0/1	Disable	4096	48	Disable
 Dynamic MAC Add 	ress		1/0/2	Disable	4096	48	Disable
 Static MAC Addres 	s		1/0/3	Disable	4096	48	Disable
Private Group	~		1/0/4	Disable	4096	48	Disable
			1/0/5	Disable	4096	48	Disable
Protected Port			1/0/6	Disable	4096	48	Disable
Private Vlan	~		1/0/7	Disable	4096	48	Disable
Storm Control	~		1/0/8	Disable	4096	48	Disable
			1/0/9	Disable	4096	48	Disable
			1/0/10	Disable	4096	48	Disable

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

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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	ecurity Acce	ss Port Authen	tication Tra	, fic Control Cor	ntrol ACL			
Traffic C	Control	Port Security Sett	ings					
• MAC Filter	×	Convert Dynamic	c Address to S	itatic				
Port Security	^	Number Of Dyna	imic MAC Add	resses Learned:	0			
Port Adminis	stration							
Interface Cor	nfiguration							
Dynamic MA	C Address	Dynamic MAC Ac	Idress Table					
• Static MAC .	Address	Port List	1/0/1 🗸					
Private Group	~	VLAN ID	MAC A	ddress				
Protected Port		-						
Private Vlan	~							
Storm Control	~							

- 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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	ecurity Access	Port Authentica	ation Traf	ic Control Cor	ntrol ACL			
Traffic C	Control Po	rt List						
• MAC Filter	∼ In	terface	1/0/1 ~					
Port Security	^							
Port Adminis	stration		011174.000					
 Interface Cor 	figuration	atic MAC Address	Table					
• Dynamic MA	C Address	Static MAC Ad	ldress V	'LAN ID				
Static MAC	Address	00:13:00:01:02	::03	3 🗸				
Private Group	×							
Protected Port								
Private Vlan	~							
• Storm Control	×							

- 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.



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 192.168.1.254 255.255.25.0
(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)#vlan participation include 202
(Netgear Switch) (Interface 1/0/48)#vlan 202
(Netgear Switch) (Interface 1/0/48)#exit
(Netgear Switch) (Interface-vlan 202)#routing
(Netgear Switch) (Interface-vlan 202)ip address 10.100.5.34 255.255.05
(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 511.

a. Select System > Services > DHCP Server > DHCP Server Configuration.

System	Switching	Routing	QoS	Securi	ity	Monitor	ing	Maintenance	Help	Index
Management De	evice View	Services Chass	is SNMP	LLDP	ISDP	Timer Sc	hedule			
Services		DHCP Pool Configu	ration							
DHCP Server	^	Pool Name		Cre	ate 🛩					
DHCP Server Configuration		Pool Name		pool	I_a		(1 to 31	alphanumeric chara	acters)	
DHCP Rool		Type of Binding		Dyn	namic	~				
Configuration		Network Address		192.	168.1.0					
DHCP Pool Opti	ions	Network Mask		255.	255.255.	0				
DHCP Server St	tatistics	Network Prefix Le	ngth				(0 to 32	9		
DHCP Bindings		Client Name								
Information		Hardware Addres	S		0:00:00:0	0:00				
 DHCP Conflicts Information 		Hardware Address	s Type	Eth	ernet ~					
DHCP Relay		Client ID								
DHCP L2 Relay	~	Host Number		0.0.0	0.0					
• UDP Relay	~	Host Mask			0.0					
DHCPv6 Server	~	Host Prefix Lengt	h				(1-32)			
DHCPv6 Relay		Lease Time		Infin	nite	~				
		Days		0			(0 to 59	U		
		Hours		0			(0 to 23	9		

- **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.

System	S	witching		Routing		QoS		Secur	ity		Monito	ring	81	Mai	ntena	ince	*	J	Help		In	dex		
Routing Table	IP	IPv6		ARP	RIP	OSPF	05	SPFv3	Ro	uter ()iscove	ry	VRRF	P N	Aultic:	ast	IP\	/6 Mi	ultica	ist				
VLA	N		VLAN	Routing '	Wizard																			
 VLAN Routing 	Wiza	rd	Vlan	ID											3	192					3			
 VLAN Routing 			IP Ac	Idress												192.	168.	1.254	4					
			Netw	ork Mas	k											255.	255.	255.0	D					
			1	Jnit 1																				
			Ports	1	3 5	7	9 11	13	15	17	19 21	23	25	27	29	31	33	35	37	39	41	43	45	47
												U					Mar.							
											- A Mary	U									-			
				2	46	8 1	0 12	14	16	18	20 22	24	26	28	30	32	34	36	38	40	42	44	46	48

- **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.

System	S	witching		Routing		QoS		Secu	urity	1	M	onitori	ng		Ma	inten	ance		1	Help		In	ıdex	1	
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSF	F	DSPFv	3 F	Route	r Dis	cover	K 1	VRRF		Multio	cast	IP	v6 M	ultica	ast			46	
V/I A	M		VIANE	Pouting	Wizard																				
VL/-		140	VLANT	touting	VVIZaru																				
VLAN Routing	Wiza	rd	Vlan	ID													202	2							
VLAN Routing			IP Ad	dress													10.	100.5	5.34						
			Netwo	ork Mas	k												255	5.255	.255.	0					
			1	J <mark>nit 1</mark>																					
			Ports	1	3 5	7	9 1	1 13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
																								-	U
				2	4 6	8	10 1	2 14	16	18	20	22	24	26	28	30	32	34	36	3.8	40	12	44	46	45

- **b.** Enter the following information:
 - In the Vian 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.

System	SI	witching		Routing		QoS	Secur	tý	Monitoring	g I	Maintenance	Help	Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast	
IP			IP Con	figuratior	1								
• Basic		~	Defau	ilt Time t	o Live				64				
 IP Configurat 	ion		Routi	ng Mode					Enable	e 💿 Disat	ble		
 Statistics 			ICMP	Echo R	eplies				Enable	e 🖲 Disat	ble		
 Advanced 		~	ICMP	Redirec	ts				Enable	e 🖲 Disat	ole		
			ICMP	Rate Li	mit <mark>In</mark> te	rval			1000		(0 to 214	17483647 ms)	
			ICMP	Rate Lir	nit Bur	st Size			100		(1 to 200)))	
			Maxir	num Nex	d Hops	;			4				
			Maxir	num Rou	utes				8160				

- **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.

System	S	witching	8 I	Routing	t m	QoS	Security	Monitor	ing	Maintenanc	e Help	Index	
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discover	y VRRP	Multicast	IPv6 Multicast		
Routing	Table	ŝ.	Confi	gure Route	s								
• Basic		^		Route Ty	ре	Network	Address	Subnet Ma	isk	Next Hop	Address P	reference	
 Route Config 	uratio	n		Static		✓ 192.168	3.40.0	255.255.2	55.0	192.168.	200.2		1
* Advanced		~		Default		0.0.0.0		0.0.0.0		192.168.	10.1 2	53	
			Learn Ne 0. 19	ed Routes etwork Add 0.0.0 2.168.10.0	Iress	Subnet Mas 0.0.0.0 255.255.255	k Protoc Default 5.0 Local	ol Route Type Static Connected	Next Hop vlan 1 vlan 1	Interface N 1	lext Hop Address 92.168.10.1 92.168.10.138	Preference 253 0	Metric 0 1

- **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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Sec	urity Access	Port Authentica	ition Traffi	c Control Co	ontrol ACL			
Traffic Con	trol Pro	tected Ports Cont	iguration					
MAC Filter Port Security Private Group	¥ G ¥ G	roup ID roup Name			1 ~			
Protected Port		Unit 1						
Private Vlan Storm Control	v Pi	2 4 6	7 9 8 10	11 13 15 11 13 15 12 14 16	17 19 21 23 2 10 10 10 10 10 10 10 10 10 10 10 10 10 1	25 27 29 31 33 1 1 1 1 1 1 1 1 1 1 26 28 30 32 34	35 37 39 36 38 40	41 43 42 44
	P	orts 1 3 5	7 9	11 13 15 11 13 15 12 14 16	17 19 21 23 10 10 10 10 18 20 22 24			

- **b.** Under Protected Ports Configuration, click **Unit 1**. The ports display.
 - Click the gray box under port 23. A check mark displays in the box.
 - Click the gray box under port 24. A check mark displays in the box.
- c. Click Apply to activate ports 23 and 24 as protected ports.

802.1x Port Security

This section describes how to configure the 802.1x port security feature on a switch port. IEEE 802.1x authentication prevents unauthorized clients from connecting to a VLAN unless these clients are authorized by the server. 802.1x port security prevents unauthorized clients from connecting to a VLAN. It can be configured on a per-port basis.



Figure 35. 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 10.100.5.33 255.255.0
(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.

System	Sv	vitching		Routing		QoS	Securi	ty	Monitoring	, I	Maintenance	Help	Index
Routing Table	P	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Route	Discovery	VRRP	Multicast	IPv6 Multicast	
IP			IP Con	figuration									
• Basic		^	Defau	It Time to	o Live				64				
 IP Configurati 	on		Routi	ng Mode					Enable	e 🖲 Disab	le		
 Statistics 			ICMP	Echo Re	eplies				Enable	e 🖲 Disab	le		
 Advanced 		~	ICMP	Redirect	ts				Enable	e 🖲 Disab	le		
			ICMP	Rate Lin	nit Inter	val			1000		(0 to 21	47483647 ms)	
			ICMP	Rate Lin	nit Burs	st Size			100		(1 to 20	0)	
			Maxir	num Nex	t Hops				4				

- **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.

System	Sv	vitching		Routin	g	QoS	Securit	y Monitoring		Maintenance	Help	Index		
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast			
IP			IP Int	erface C	onfigurati	on								
•Basic		~	12	3 VLAN	S All									
 Advanced IP Configuration 	ion	^		Port	Descrip	tion	VLAN ID	IP Address Configura Method	ation	IP Address	Subnet Mask	Rou Mod	ting le	Administrative Mode
 Statistics 				1/0/1	-			Manual ~		192.168.1.1	255.255.2	55.0 En	able 🗸	Enable ¥
• IP Interface	20			1/0/1				None		0.0.0.0	0.0.0.0	Dis	able	Enable
Configuration				1/0/2				None		0.0.0.0	0.0.0.0	Dis	able	Enable

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.

System	S١	witching		Routin	g	QoS	Security	y Monitoring	N	Aaintenance	Help	Index		
Routing Table	IP.	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery V	/RRP	Multicast	IPv6 Multicast			
IP	Ū		IP Int	erface C	onfigurat	ion								
•Basic		~	12	3 VLAN	S All									
 Advanced IP Configuration 	on	^		Port	Descrip	tion	VLAN ID	IP Address Configurat Method	tion	P Address	Subnet Mask	Roi Mo	uting de	Administrative Mode
 Statistics 				1/0/19				Manual 👻		10.100.5.33	255.255.2	55.0 Er	nable 🛩	Enable V
• IP Interface				1/0/1				None	(0.0.0	0.0.0	Dis	able	Enable
Configuration		-		1/0/2				None	0	0.0.0.0	0.0.0.0	Dis	able	Enable
 Secondary IP 				1/0/3				None	10	0.0.0.0	0.0.0.0	Dis	able	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.

System	Switching	ľ	Routing	QoS	Securit	у	Mon	itoring		Mainten	ance		lelp	Inc	dex
Management Sec	urity Acce	ss	Port Authenti	cation Tra	ffic Control	Contro	ol A(CL.							
Management S	Security	Login	Authenticatio	in List											
• Local User	~		List Name		1	2		3		4		5		6	
Enable Password	1		dot1xList		Radius 👻	N/A	*	N/A	~	N/A	~	N/A	~	N/A	~
 Line Password 			defaultList		ocal	N/A		N/A		N/A		N/A		N/A	
• RADIUS	~		networkList		ocal	N/A		N/A		N/A		N/A		N/A	
 TACACS 	~														
Authentication Li	st 🔺														
Login Authentic	cation List														

- **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.

System	Switcl	hing		Routin	g QoS	Se	curity	Monitoring	Maintena	nce	Help	Index	1
Management S	lecurity	Acc	ess		hentication Traffic	Cont	rol Control	ACL					
Port Authe	ntication		Port	Authentic	ation								
• Basic		~	12	3 All									
 Advanced 		~			ė.		1	0.0	T 3	0.1	0		
• 802.1X Confi	guration			Port	Control Mode		MAB	Period	Period	VLAN I	D VI	LAN Period	VLAN ID
Port Authent	ication			1/0/19	Force Authorized	~	Disable 👻	60	30	0	9	0	0
Port Summa	ry			1/0/1	Auto		Disable	60	30	0	90)	0
Client Summ	nary			1/0/2	Auto		Disable	60	30	0	90)	0

- **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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	Security Ac	cess Port Authent	ication Traf	fic Control Cor	itrol ACL			
Port Authe	entication	802.1X Configuration	on					
Basic	^	Administrative Mo	de	🔘 Disa	ible 🖲 Enable			
• 802.1X Confi	iguration	VLAN Assignmer	nt Mode	💿 Disa	able 🔘 Enable			
 Advanced 	~	EAPOL Flood Mo	de	Oisa	ible 🔘 Enable			
		Dynamic VLAN C	reation Mode	Disab	le 🖌			
		Monitor Mode		Disab	le 🛩			
		Users		Non-c	onfigured user 💌			
		Login		defaul	tList 👻			
		Authentication Lis	st	dot1xL	ist			

- **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.

System Switching	9	Routing QoS	Security	Monitoring		Maintenance	Help	a In	dex				
Management Security	Sr	rver Configuration	Contract Section							A00	Deleto	iear counter	s Update
Local User Enable Password	1	Radius Server IP Address	Radius Server Name	Cu	crent: F	Port	Secret Sonfigured	Secret		Primary Server	Message Authentica	tor Type	
Line Password		10.100.5.17	1			1812	Yes 👻	*****		Yes ~	Enable	4	~
·RADIUS	6												
 Radius Configuration 	St	atistics											
Server Configuration	-	tistres.		_	_	_		_			-	_	_
*Accounting Server Configuration		Radius Round Access Server Trip Time Request	Access Retransmissions	Access Accepts	Access Reject	s Access s Challenges	Malforme Response	d Access Is	Bad Authenticators	Pending Requests	Timeouts	Unknown Types	Packets Dropped

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.

System Switc	hing	1	Routing	QoS	Sec	urity Moniti	oring N	taintenance He	lp Index			
Management Security	Acce	19.8	Port Autho	entication	Traffic Contro	d Control ACL						
										Add	Delete Ck	air counters
Management Security		Acco	ounting Serv	er Configura	ation							
Local User	*		Accountin	in Server IP	10	12 - 13 - 14 - 14 - 14 - 14 - 14 - 14 - 14	1.820	i konserv	w 12 3		R - 1892	22-2
Enable Password		2	Accounting Server IP A		Accountin	g Server Name	Port	Secret Configur	ed Secret		Accounting	Mode
Line Password			10,100,5	17			1813	Yes *	******		Enable ·	
RADIUS												
Radius Configuration		Frat	ation									
* Server Configuration		Clati	ISUCS									
Accounting Server Configuration		AS	ecounting erver	Round Trip Time	Accounting Requests	Accounting Retransmissions	Accounting Responses	Malformed Accounting Responses	g Bad Authenticators	Peoding Requests Timeout	s Unknown Types	Packets Dropped

- 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.

Management Securi	Y .	Accounting Se	rver Configura	ation					27		2004		n r	
cal User able Password	*	G Accour Addres	ting Server IF s	Accountin	g Server Name	Port	Secret Configured	i Secret			Accounting	Mode		
e Password		10,100	5.17				Yes *				Enable ~			
DIUS	~			100			The second second							
adius Configuration														
erver Configuration		Statistics												
ccounting Server		Accounting	Round	Accounting	Accounting	Accounting	Malformed Accounting	Bad	Pending	limeouts	Unknown	Packets		
CACS	×	- Deriver	rup may	condinana	- contractivities and	responses	rvesponses -	entreprised of the	scodnageo	TTP- MARK	Types	caropped		
thentication List	~													

- 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 36. Guest VLAN

If a port is in port-based mode, and a client that does not support 802.1X is connected to an unauthorized port that has 802.1X enabled, the client does not respond to the 802.1X requests from the switch. The port remains in the unauthorized state, and the client is not granted access to the network. If the guest VLAN is configured for that port, then the port is placed in the configured guest VLAN and the port is moved to the authorized state, allowing access to the client after a certain amount of time (determined by the guest VLAN period). If the client attached is 802.1x aware, then this allows the client to respond to 802.1X requests from the switch.

For a port in MAC-based mode, if a guest VLAN has been configured on the port and if traffic from an unauthenticated client is detected on the port, the guest VLAN timer is started for that client. If the client is 802.1x unaware and does not respond to any 802.1x requests, when the guest VLAN timer expires, the client is authenticated and associated with the guest VLAN. This ensures that traffic from the client is accepted and switched through the guest VLAN.

In this example, dot1x is enabled on all the ports so that all the hosts that are authorized are assigned to VLAN 1. On ports 1/0/1 and 1/0/24, guest VLAN is enabled. If guests connect to the port, they are assigned to VLAN 2000, so that guests cannot access the internal VLAN, but can access each other in the guest VLAN.

CLI: Create a Guest VLAN

1. Enter the following commands:

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

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)#dot1x port-control force-authorized
```

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)
Transmit Period (secs)
Guest VLAN ID 2000
Guest VLAN Period (secs)
Supplicant Timeout (secs)
Server Timeout (secs) 30
Maximum Requests 2
VLAN Id 2000
VLAN Assigned Reason Guest
Reauthentication Period (secs)
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.

Syste	em	Swit	tching		Routing	QoS	Security	Monitorir	ng Maintenance	Help	Index
VLAN	Auto-Vo	olP	iSCSI	STF	Multicas	MVR /	Address Table	Ports LAG	MLAG		A
	VLAN	l.		Reset							
•Basic			~	Res	et Configurat	ion					
• VLAN	I Configu	ration									
• Advanc	ed		~								
				Intern	al VLAN Cor	figuration					
				Inter	nal VLAN Al	location Base	e 40	93			
				Inter	nal VLAN AI	location Polic	y 🔘	Ascending 🖲 De	escending		
				VLAN	Configuratio	n					
					VLAN ID	/LAN Name	VLAN Type	Make Static			
					2000			Enable 🛩			
					1 0	lefault	Default	Disable			
					3 \	/LAN0003	Static	Disable			

- 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.

Syste	em	Sv	vitching		Routing	QoS	;	Securi	ty	N	lonitor	ing		Mainte	enanc	e		Help	-	Ir	ıdex		
VLAN	Auto-\	VolP	iSCSI	STP	Multicast	MVR	Addr	ress Tabl	le F	orts	LAG	N	ILAG										
	VLAN	1		VLAN I	Membership	2																	_
 Basic 			~	VLAN	ID											2000) ~						
• Advanc	ed		~	Group	Operation											Unta	ag All	~					
• VLAN	V Config	uration	1	VLAN	Name											VLAN	12000)					
• VLAN	1 Memb	ership		VLAN	Туре											Static	3						
• VLAN	V Status	5		1	Init 1																		
Port F Config	PVID guration			Ports	1 3	5 7	9 11	1 13	15 1	7 19	21	23	25	27 29	31	33	35	37	39	41	43	45	47
• MAC	Based	VLAN																					
• Proto Group	col Bas p Config	ed VL	AN 1		2 4	6 8	10 12	2 14	16 1	8 20	22	24	26	28 30	32	34	36	38	40	42	44	46	48

- 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.

System Swit	ching		Routin	ng QoS S	iecurity		Monitoring	Maintena	nce He	lp Index				
Management Security	Acc	cess		abantisation Traffic Co	ntrol	Control	ACL							
												Ca	nicel Appl	y Initiatize
Port Authentication	Ŕ.	Port	Authenti	cation										
Basic	-	12	J AJI										Go	To Port
Advanced +802.1X Configuration	2		Port	Control Mode	MAE	1	Quiet Period	Transmit Period	Guest VLAN ID	Guest VLAN Period	Unauthenticated VLAN ID	Supplicant Timeout	Server Timeout	Maximum Requests
Port Authentication			1/0/6	Force Authorized	Dis	able ¥	60	30	0	90	0	30	30	2
Port Summary	-		1/0/1	Auto	Disa	ble	60	30	0	90	0	30	30	2
* Client Summary		0	1/0/2	Auto	Disa	ible	60	30	0	90	0	30	30	2
			1/0/3	Auto	Disa	ible	60	30	0	90	0	30	30	2
		8	1/0/4	Auto	Disa	ble	60	30	0	90	0	30	30	2
		13	1/0/5	Auto	Disa	ible.	60	30	0	90	0	30	30	2
		1	1/0/6	Auto	Disa	ble	60	30	0	90	0	30	30	2

- 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.

System	Switching	Routing QoS	Security	Monitoring	Maintenance	Help	Index
Management Se	curity Acce	ess Port Authentication	Traffic Control Cont	rol ACL			
Port Author	tication	802 1V Configuration					
	incanon			200 - 201 Sec. 2003			
Basic	^	Administrative Mode	O Disal	ble 💿 Enable			
• 802.1X Config	uration	VLAN Assignment Mode	Oisal	ble 🔵 Enable			
 Advanced 	~	EAPOL Flood Mode	Oisal	ble 🔘 Enable			
		Dynamic VLAN Creation N	Aode Disable	e ¥			
1		Monitor Mode	Disable	e ~			
		Users	admin	~			
		Login	default	List ~			
		Authentication List	dot1xL is	st			

- **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.

System	Swite	ching	Į,	Routing	QoS	Securi	ty	Mon	itoring		Maintena	ance	ŀ	lelp	Inc	lex
Management Seci	unty	Acce	ss	Port Authenticat	ion Traf	fic Control	Control	A	CL							
Management S	ecunty	y .	ogin	Authentication L	ist									_		
 Local User 		~		List Name	1	á	2		3		4		5	1	6	
Enable Password				ale fer till int		Dealine	-		ALLA		biz A		NUA		AL/A	
Line Password				detaultList		Radius Y	N/A	~	N/A	~	N/A	~	N/A	· · · · ·	N/A	~
Line r assword				defaultList	L	ocal	N/A		N/A		N/A		N/A		N/A	
RADIUS		~		networkList	L	ocal	N/A		N/A		N/A		N/A		N/A	
• TACACS		~														
Authentication Lis	t	^														
Login Authentic	ation l	List														

- 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.

System Switch Management Security	hing Acce	53	Routing Port Authenticati	QoS on Traffic	Security Control Control	ACL	ing	Maintenance	i Hel	p li	ndex				
Management Security		Serve	r Configuration									Add	Delete	lear counte	s Update
Local User Enable Password	×		Radius Server IP	Address	Radius Server Nam	a	Current	Port	Secret Configured	Secret		Primary Server	Message Authenticat	Servi Type	м
Line Password			192.168.0.1	- 2					Yes v	*******		×			
+RADIUS	•														
Radius Configuration		Statio	tion												
Server Configuration		Genera				_									
Accounting Server Configuration		Ra Se	dius Round ner Trip Time	Access Requests	Access Retransmissions	Acces Acces	ta Rejet	rss Access cts Challenge	Malforme Respons	d Access es	Bad Authenticators	Pending Requests	Timeouts	Unknown Types	Packets Dropped
 TACACS 	*											S			

- 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.

System	Switch	ning	Routir	ng QoS	Se	curity	Monitoring	Maintenar	nce Hei	lp Index	
Management Se	curity	Acces	s Port Au	uthentication Traf	fic Cont	rol Control	ACL				18
Port Authen	tication	P	ort Authent	ication							
•Basic		~	1 2 3 All								
* Advanced		~					0.00	Transmission	1000	Current	The second construction of
• 802.1X Configu	uration		Port	Control Mode		MAB	Period	Period	VLAN ID	VLAN Period	VLAN ID
Port Authentic	ation		1/0/1	Auto	×	Disable ~	60	30	2000	90	0
Port Summary	/		☑ 1/0/1	Auto		Disable	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 37. 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.

System	Switching	Routing	g QoS	Secu	irity	Moni	itoring	Maintenance	Help	Index
Management	Device View	Services C	Chassis PoE	SNMP	LLDP	ISDP	Timer So	chedule		
Manage	ement	IPv4 Network I	nterface Configur	ation						
 System Inform 	ation	IP Address				192.168	.0.5			
 System CPU S 	Status 🗸 🗸	Subnet Mask	<			255.255	.255.0			
 Switch Statisti 	CS	Default Gater	way			0.0.0.0				
 USB Device In 	formation	Burned In MA	AC Address			20:0C:C	8:4D:95:72	2		
 Loopback Inter 	face	Locally Admi	inistered MAC Ac	Idress		00:00:00				
Network Interfa	ice ^	MAC Addres	s Type			Burne	ed In 🔘 Lo	cally Administered		
IPv4 Network Configuration	<	Current Netw	ork Configuration	Protocol		None	Bootp	OHCP		
		DHCP Vendo	or Class Identifier			Disat	ole 🔘 Enal	ble		
Configuration	1	DHCP Vendo	or Class Identifier	String						
• IPv6 Network	< Neighbor	Management	VLAN ID			1		(1 to 4093)		
 IPv4 Service 	Port	Interface Sta	tus			Up				

- 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.

Syste	em	Sw	vitching		Routing	QoS	Security	Monite	oring	Maintenance	Help	Index
VLAN	Auto-Voll	Ρ	iscsl	STP	Multicast	MVR	Address Table	Ports LA	g Ml	.AG		
	VLAN			Reset								
•Basic			^	Rese	t Configuratio	on						
• VLAN	I Configura	ition	8									
• Advanc	ed		~									
				Interna	I VLAN Conf	iguration						
				Interr	nal VLAN Alle	cation Ba	se 40	93				
				Interr	al VLAN Allo	cation Po	licy 🔘	Ascending 💿	Descen	ding		
				VLAN	Configuration							
					VLAN ID V	_AN Name	VLAN Type	Make Static				
					2000			~				
					1 de	fault	Default	Disable	2			

- 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.

System Sw	ritching	<u>[]</u>	Routin	ig QoS Se	curity [Monitoring	Maintena	nce F	lelp Index	2
Management Security	Acc	ess	Port Au	thentication Traffic Cont	rol Control	ACL			<i></i>	
Port Authenticatio	m	Port	Authenti	cation						
Basic	~	12	3 All							
 Advanced 802.1X Configuratio 	^ 1	۲	Port	Control Mode	MAB	Quiet Period	Transmit Period	Guest VLAN ID	Guest VLAN Period	Unauthenticated VLAN ID
Port Authentication	1		1/0/6	Force Authorized 🗸	Disable 🛩	60	30	2000	90	0
Port Summary		0	1/0/1	Auto	Disable	60	30	0	90	0
Client Summary			1/0/2	Auto	Disable	60	30	0	90	0
			1/0/3	Auto	Disable	60	30	0	90	0
			1/0/4	Auto	Disable	60	30	0	90	0
			1/0/5	Auto	Disable	60	30	0	90	0
			1/0/6	Auto	Disable	60	30	0	90	0

- **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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	Security Acc	ess Port Authenti	cation Traf	ffic Control Contr	ol ACL			
Port Authe	entication	802.1X Configuratio	n					
 Basic 	^	Administrative Mo	de	🔘 Disab	le 🖲 Enable			
• 802.1X Confi	iguration	VLAN Assignmen	t Mode	O Disab	le 🖲 Enable			
 Advanced 	~	EAPOL Flood Mo	de	Oisab	le 🔘 Enable			
		Dynamic VLAN C	reation Mode	Disable	~			
		Monitor Mode		Disable	~			
		Users		admin	~			
		Login		default	ist ×			
		Authentication Lis	st	dot1xLis	t			

- **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.

System	Switch	ing		Routing	QoS	Seci	urity	Mon	itoring		Maintena	nce	t i	lelp	In	dex
Management Secu	rity 7	Acces	s	Port Authenti	cation	Traffic Contro	l Cont	rol A	CL.							
Management Se	curity	L	ogin	Authenticatio	n List											
• Local User		~		List Name		1	2		3		4		5		6	-
 Enable Password 				defaultList		Radius	✓ N/A	~	N/A	~	N/A	~	N/A	~	N/A	~
Line Password				defaultList		Local	N/A		N/A	-	N/A		N/A		N/A	
RADIUS		~		networkList		Local	N/A		N/A		N/A		N/A		N/A	
TACACS		~														
 Authentication List 		~														
Login Authentica	tion Lis	st														

- **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.

System	Switching	Rou	ting	QoS	Security	Monitori	ng	Maintenance	Hel	p Ir	ndex
Management S	ecurity Acces	ss Port	Authenticati	on Traffic	Control Contro	ACL					8
Management	t Security	Server Con	figuration								
 Local User 	~		0 10		5 r 6 N				Secret	0	
 Enable Passwo 	ord	B Radi	us Server IP	Address	Radius Server Nar	ne C	urrent F	'οπ (onfigured	Secret	
 Line Password 		192.	168.0.1						Yes 🗸		
• RADIUS	~										
 Radius Config 	guration										
 Server Config 	uration	statistics				10			-72		y
 Accounting S Configuration 	Gerver	Radius Server	Round Trip Time	Access Requests	Access Retransmissions	Access Accept	Access Rejects	Access Challenges	Malforme Respons	ed Access ies	Bad Authenticators
• TACACS	~										

- 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 38. 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 a DHCP snooping entry exists. However, ARP packets from the static client are dropped. For information about how to prevent ARP packets from static clients to be dropped, see *Static Mapping* on page 386.

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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Se	ecurity Acce	ess Port Authent	cation Traf	fic Control Con	tro) ACL			
Contr	ol	DHCP Snooping G	lobal Configur	ation				
• DHCP Snooping	g ^	DHCP Snooping I	Node	🖲 Disable 🔵	Enable			
Global Config	uration	MAC Address Va	lidation	🔘 Disable 🖲	Enable			
Interface Cont	iguration							
• Binding Confi • Persistent Co	guration nfiguration	VLAN Configuration	1					
 Statistics 		VLAN ID	E	HCP Snooping N	lode			
• IP Source Guar	d v			~				
Dynamic ARP I	nspection 👻	New York Control of Co	C) 10.					

- **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.

System	Switchir	g	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	Security A	cess	Port Authenti	cation Tra	fic Control Con	trol ACL			
Cont	trol	DH	CP Snooping G	obal Configu	ration				
DHCP Snoopir	ng	< Dł	ICP Snooping N	Node	🔘 Disable 🖲	Enable			
Global Config	guration	M.	AC Address Va	lidation	🔘 Disable 🖲	Enable			
Interface Cor	nfiguration								
 Binding Cont 	figuration								
• Persistent C	onfiguration	VLA	N Configuration	1					
 Statistics 		8	VLAN ID	[HCP Snooping N	lode			
 IP Source Gua 	ırd	×			*				
Dynamic ARP	Inspection								

- b. In the VLAN ID field, enter 1.
- c. In the DHCP Snooping Mode field, select Enable.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	ecurity Acces	s Port Authent	ication Tra	ffic Control Cont	rol ACL			
Contr	ol D	HCP Snooping G	lobal Configu	ration				
DHCP Snoopin	g ^	DHCP Snooping	Mode	🔘 Disable 💿	Enable			
Global Config	uration	MAC Address Va	lidation	🔘 Disable 💿	Enable			
• Interface Con	figuration							
 Binding Confi 	guration							
• Persistent Co	onfiguration	LAN Configuratio	n					
 Statistics 		VLAN ID	[OHCP Snooping M	ode			
•IP Source Guar	rd 🗸	1		Enable V				
Dynamic ARP I	nspection 🐱		and pro-					
Captive Portal	v							

- 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.

System	Switching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Secu	urity Acc	ess	Port Auth	entication T	raffic Control	ontrol ACL			
Control		DHC	D Spaaning	Intorfaco Con	fouration				
DHCP Snooping	~	1.0		g intenace con	inguration .	No To Navado a - F			
Global Configura	ation	12	J LAG AII		En la companya de la		00		
 Interface Configuration 	uration		Interface	Trust Mode	Invalid Packets	Rate Limit(pps)	Burst Interval(secs)		
Binding Configu	ration			¥	~				
			1/0/1	Disable	Disable	None	N/A		

- 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.



- 5. Enable ARP Inspection in VLAN 1.
 - a. Select Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration.

System Swi	tching		Routin	g QoS	Security	Monitoring	Maintenance	Help	Index
Management Security	Acce	SS	Port Au	thentication	Traffic Control	Control ACL			
Control	1		V Configu	ration					
PLIOP O			r ooninge			1			
•DHCP Shooping	~		VLAN	Admin Modo	Invalid Dackote	APP ACL Mama	Static		
 IP Source Guard 	~		ID	Administrode	invalid Fackets	AN AGE Mame	Flag		
Dynamic ARP Inspect	on 🔺			*	~		~		
DAI Configuration			1	Disable	Enable		Disable		
DALVI AN Configura	tion		3	Disable	Enable		Disable		
En a vera vooringena	uon		2000	Disable	Enable		Disable		
 DAI Interface Configuration 									

- b. In the VLAN ID field, enter 1.
- c. In the Dynamic ARP Inspection field, select Enable.

A screen similar to the following displays.

System Switch	ning		Routin	g QoS	Security	Monitoring	Maintenance	Help	Index
Management Security	Acce	ess	Port Au	thentication	Traffic Control	Control ACL			
Te									
Control		VLA	V Configu	uration					
DHCP Snooping	~		VE AN			THE CONTRACTOR	Static		
IP Source Guard	~		ID	Admin Mode	Invalid Packets	ARP ACL Name	Flag		
Dynamic ARP Inspection	^		1	Enable ~	~		Disable 👻		
DAI Configuration			1	Disable	Enable		Disable		
• DALVLAN Configuration			3	Disable	Enable		Disable		
			2000	Disable	Enable		Disable		
 DAI Interface Configuration 									

d. Click Apply.

A screen similar to the following displays.

System Switch	ing	Routin	g QoS	Security	Monitoring	Maintenance	Help	Index
Management Security	Access	s Port Au	thentication	Traffic Control	Control ACL			
Control	V	LAN Configu	iration					
DHCP Snooping	~			1	in the second second	Static		
IP Source Guard	~	ID	Admin Mode	Invalid Packets	ARP ACL Name	Flag		
Dynamic ARP Inspection	^	1	Enable 👻	Enable 👻		Disable 🛩		
 DAI Configuration 	_	1	Disable	Enable		Disable		
DALVLAN Configuration	r.	3	Disable	Enable		Disable		
DALLY		2000	Disable	Enable		Disable		
Configuration								

Now all the ARP packets received on the ports that are member of the VLAN are copied to the CPU for ARP inspection. If there are trusted ports, you can configure them as trusted in the next step. ARP packets received on the trusted ports are not copied to the CPU.

Note: Make sure that the administrator computer has a DHCP snooping entry or can access the device through the trusted port for ARP. Otherwise, you might get disconnected from the device.

- 6. Configure port 1/0/1 as trusted.
 - a. Select Security > Control > Dynamic ARP Inspection > DAI Interface Configuration.
 - b. Select the Interface 1/0/1 check box.
 - c. For the Trust Mode, select Enable.
 - d. Click Apply.

System S	witching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Securit	ay Acc	cess	Port Auth	entication T	raffic Control 🛛 🔅	ontrol ACL			,
Control		DAL	nterface C	onfiguration					
 DHCP Snooping 	~	13	LAG AII		Go To Interface	Go			
 IP Source Guard 	*		Interface	Trust Made	Data Limit/nno)	Puret Internal/accel			
Dynamic ARP Inspe	ction ^	-	Intenace	Trust wode	Rate Limit(pps)	Durst interval(secs)			
• DAL Configuration				Y					
DAr Conigeration			1/0/1	Disable	15	1			
DAI VLAN Configu	iration		1/0/2	Disable	15	1			
DAI Interface Configuration			1/0/3	Disable	15	1			
			1/0/4	Disable	15	1			
DAI ACL Configura	ation		1/0/5	Disable	15	1			

Now ARP packets from the DHCP client will go through; however ARP packets from the static client are dropped, since it does have a DHCP snooping entry. It can be overcome by static configuration as described in the following section, *Static Mapping* on page 386.

Static Mapping

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

CLI: Configure Static Mapping

1. Create an ARP ACL.

(Netgear Switch) (Config)# arp access-list ArpFilter

2. Configure the rule to allow the static client.

```
(Netgear Switch) (Config-arp-access-list)# permit ip host 192.168.10.2
  mac host 00:11:85:ee:54:e9
```

3. Configure ARP ACL used for VLAN 1.

(Netgear Switch) (Config)# ip arp inspection filter ArpFilter vlan 1

Now the ARP packets from the static client go through because the client has an entry in the ARP table. ACL ARP packets from the DHCP client go also through because the client has a DHCP snooping entry.

This command can include the optional static keyword. If the static keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings. In this example, ARP packets from the DHCP client are dropped since it does not have a matching rule, though it has a DHCP snooping entry.

Web Interface: Configure Static Mapping

- 1. Create an ARP ACL.
 - a. Select Security > Control > Dynamic ARP Inspection > DAI ACL Configuration.
 - b. In the Name field, enter ArpFilter.
 - c. Click Add.

A screen similar to the following displays.

System S	witching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Securit	y Access	Port Authenti	cation Tra	ffic Control Cor	ntrol ACL			
Control	DA	d ACL Configurat	ion					
DHCP Snooping IP Source Guard	ž	Name	_	-				
Dynamic ARP Inspe- DAI Configuration	ction 🔺	ArpFilter						
 DAI VLAN Configu DAI Interface Configuration 	ration							
DAI ACL Configura DAI ACL Rule Configuration	ation							

- 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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Sec	curity Access	Port Authenti	cation Traf	fic Control Cont	el ACL			
Contro	Ru	les						
DHCP Snooping	~ A	CL Name	ArpFilter	*				
• IP Source Guard	~							
• Dynamic ARP In	spection 🔺							
DAI Configurati	on DA	I Rule Table						
DAI VLAN Con	figuration	Source IP A	ddress S	ource MAC Addre	ss			
• DAI Interface								
Configuration		192.168.10.2	2 0	0:11:85:EE:54:E9				
DALACL Config	guration							
Configuration								

- 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.

System Switc	hing	Routin	g QoS	Security	Monitoring	Maintenance	Help	Index
Management Security	Access	s Port Au	thentication	Traffic Control	Control ACL			
Control	V	LAN Configu	iration					
DHCP Snooping	~	- VI AN				Static		
• IP Source Guard	×	ID ID	Admin Mode	Invalid Packets	ARP ACL Name	Flag		
Dynamic ARP Inspection	~		Enable 👻	~		~		
 DAI Configuration 		1	Disable	Enable		Disable		
DAI VLAN Configuration	n e							

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.





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 i	(GSM7328S) #show ip dhcp snooping binding									
Total number of bi	ndings: 1									
MAC Address	IP Address	VLAN	Interface	Туре	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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	ecurity Acc	ess Port Authenti	cation Traf	fic Control Car	trol ACL			W.
Cont	rol	DHCP Snooping G	lobal Configur	ation				
DHCP Snoopir	ig ^	DHCP Snooping	Mode	💿 Disable 🔘	Enable			
Global Config	guration	MAC Address Va	lidation	🔘 Disable 🖲	Enable			
Interface Cor	figuration							
 Binding Cont 	iguration							
• Persistent C	onfiguration	VLAN Configuration						
 Statistics 		VLAN ID	C	HCP Snooping N	lode			
 IP Source Gua 	rd 🗸			~				
Dynamic ARP	Inspection ~							
 Captive Portal 	Y							

- **b.** For DHCP Snooping Mode, select **Enable**.
- c. Click Apply.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Secu	irity Acces	ss Port Authentical	tion Traff	fic Control Con	trol ACL			S
Control		OHCP Snooping Glob	al Configura	ation				
DHCP Snooping	~	DHCP Snooping Mo	de	💿 Disable 🔘) Enable			
· Global Configura	ation	MAC Address Valida	ation	🔘 Disable 🖲	Enable			
 Interface Configu 	uration							
Binding Configure	ation							
Persistent Confi	guration	/LAN Configuration						
 Statistics 		ULAN ID	D	HCP Snooping N	lode			
•IP Source Guard	~			~				
Dynamic ARP Ins	pection 🗸							
Captive Portal	~							

- 2. Enable DHCP snooping in a VLAN.
 - a. Select Security > Control > DHCP Snooping Global Configuration.

A screen similar to the following displays.

System Swi	tching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Security	Acces	s Port Authentio	cation Traf	ic Control Cor	ttol ACL			
Control		HCP Snooping Gl	obal Configur	ation				
DHCP Snooping	~	DHCP Snooping N	lode	💿 Disable 🔘	Enable			
Global Configuration		MAC Address Val	idation	🔘 Disable 🖲	Enable			
Interface Configuration	on							
 Binding Configuration 	1							
• Persistent Configura	tion	/LAN Configuration						
 Statistics 		U VLAN ID	D	HCP Snooping N	lode			
• IP Source Guard	~			~				
Dynamic ARP Inspect	ion 🗸	Desc.						
Captive Portal	~							

- b. In the VLAN ID list, select 1.
- c. For DHCP Snooping Mode, select the **Enable** radio button.

System	Switchin	9	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	ecurity Ac	cess	Port Authenti	cation Traff	ic Control Con	rol ACL			
Cont	rol	DHC	P Snooping Gl	lobal Configura	ation				
DHCP Snoopin	ig 🦯	DH	CP Snooping N	Mode	🖲 Disable 🔘	Enable			
 Global Config 	guration	MA	C Address Va	lidation	🔘 Disable 🖲	Enable			
 Interface Cor 	nfiguration								
 Binding Conf 	iguration								
• Persistent C	onfiguration	VLA	V Configuration	1					
 Statistics 			VLAN ID	D	HCP Snooping M	ode			
IP Source Gua	rd 🔊				*				
Dynamic ARP	Inspection 🔻		1	E	nable				
Captive Portal	`								

- d. Click Apply.
- 3. Configure the port through which DHCP server is reached as trusted.
 - a. Select Security > Control > DHCP Snooping Interface Configuration.

System	Switchi	ng	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	ecurity A	ccess	Port Auth	entication T	raffic Control 🛛 🤅	ontrol ACL			ö
Cont	rol	DHC	P Snooping) Interface Con	figuration				
DHCP Snoopin	ig	^ 13	B LAG All		C	Go To Interface	Go		
Global Configuration		Interface	Trust Mode	Invalid Packets	Rate Limit(pps)	Burst Interval(secs)			
Interface Configuration Binding Configuration			×	~					
	0	1/0/1	Enable	Disable	None	N/A			

- **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.

System	Switching	ş. I	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Se	curity Acc	ess	Port Auth	entication Ti	affic Control 0	ontrol ACL			
Contro	ol	DHC	⊃ Snooping) Interface Con	figuration				
DHCP Snooping	^	1 3	LAG All		c	Go To Interface	Go		
Global Configu Interface Confi	iration iguration		Interface	Trust Mode	Invalid Packets	Rate Limit(pps)	Burst Interval(secs)		
Binding Config	uration			~	×				
Persistent Cor	nfiguration		1/0/1 1/0/2	Enable Disable	Disable Disable	None None	N/A N/A		

4. Select Security > Control > DHCP Snooping Binding Configuration.



Find a Rogue DHCP Server

If you enable DHCP snooping, you can find a rogue DHCP server in the network.

CLI: Find a Rogue DHCP server

1. Check the statistics on the untrusted ports.

(NETGEAR) #sh	ow ip dhcp snooping sta	tistics	
Interface	MAC Verify	Client Ifc	DHCP Server
	Failures	Mismatch	Msgs Rec'd
1/0/1	0	0	0
1/0/2	0	0	0
1/0/3	0	0	0
1/0/4	0	0	0
1/0/5	0	0	0
1/0/6	0	0	0
1/0/7	0	0	0
1/0/8	0	0	0
1/0/9	0	0	0
1/0/10	0	0	0
1/0/11	0	0	0
1/0/12	0	0	0
1/0/13	0	0	0
1/0/14	0	0	0
1/0/15	0	0	0
1/0/16	0	0	0
1/0/17	0	0	0
1/0/18	0	0	0
1/0/19	0	0	0
1/0/20	0	0	0
1/0/21	0	0	0
1/0/22	0	0	0
1/0/23	0	0	0
1/0/24	0	0	0
1/0/25	0	0	0
1/0/26	0	0	0
1/0/27	3704	0	4634

In the previous command output, the messages in the DHCP Server Msgs Rec'd column for port 1/0/27 increased, indicating that the port is connected to a rogue DHCP server.

2. Control the logging DHCP messages filtration by the DHCP Snooping application for port 1/0/27.

(Netgear Switch) (Interface 1/0/27)#ip dhcp snooping log-invalid

3. Display the buffered logging output and search for "DHCP packet; op Reply" so you can determine the IP address and MAC address of the rogue DHCP server.

```
(Netgear Switch) #show logging buffered
<12> Jan 1 05:45:02 172.26.2.129-1 DHCP_SNP[108612668]: ds_util.c(1777) 1112 %%
DHCP packet: op Reply, htype 1, hlen 6, hops 0, xid 3478478447, secs 0, ciaddr
0.0.0.0, yiaddr 10.100.4.14, server 10.100.5.253, giaddr 0.0.0.0, chaddr
6C:B0:CE:19:AE:3D.
<12> Jan 1 05:45:02 172.26.2.129-1 DHCP_SNP[108612668]: ds_util.c(1735) 1111 %% IP
packet: ver/hlen 0x45, tos 0, len 299, id 0, flags/offset 00, ttl 64, proto 17,
src 10.100.5.253, dst 255.255.255.
<12> Jan 1 05:45:02 172.26.2.129-1 DHCP_SNP[108612668]: ds_util.c(1702) 1110 %%
Ethernet header: dest FF:FF:FF:FF:FF:FF, src 00:26:F2:F6:B3:6C, type/len 0x8100.
<12> Jan 1 05:45:02 172.26.2.129-1 DHCP_SNP[108612668]: ds_main.c(2596) 1109 %%
DHCP snooping dropping DHCP server message received on untrusted interface 1/0/27 on
vlan 1. This message appears when DHCP Snoping untrusted port drops the DHCP Server
message.
```

In the previous example, the IP address of the DHCP server is 10.100.5.253 and the MAC address is 00:26:F2:F6:B3:6C.

Web Interface: Find a Rogue DHCP server

- 1. Check the statistics on the untrusted ports:
 - a. Select Security > Control > DHCP Snooping > Statistics.

System	Switching	Rout	ing QoS	S Security	Monitoring	Maintenance	Help	Index
Management S	Security Acces	s Port A	uthentic ation	Traffic Control Co	ntrol ACL			
Cont	trol	1/0/15	0	0	0			
DHCP Snoopi	ng 🔨	1/0/16	0	0	0			
Global Confi	iguration	1/0/17	0	0	0			
Global Configuration		1/0/18	0	0	0			
 Interface Co 	onfiguration	1/0/19	0	0	0			
 Binding Configuration 		1/0/20	0	0	0			
• Persistent C	onfiguration	1/0/21	0	0	0			
	oningeration	1/0/22	0	0	0			
 Statistics 		1/0/23	0	0	0			
IP Source Gua	ard 🗸	1/0/24	0	0	0			
• IPv6 Source G	Guard v	1/0/25	0	0	0			
Durantic ADD lasestica		1/0/26	0	0	0			
- Dynamic ARF	mapee don v	1/0/27	3532	0	4418			
Captive Portal	×	1/0/28	0	0	0			

- **b.** Determine if messages in the DHCP Server Msgs Rec'd column increase for any port.
- **a.** The previous figure shows that the messages increased for port 1/0/27, indicating that the port is connected to a rogue DHCP server.

- 2. Enable the logging of invalid packets for port 1/0/27.
 - a. Select Security > Control > DHCP Snooping > Interface Configuration.

System	Switching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	Security Acce	ess	Port Auther	itication Tra	affic Control Co	ntrol ACL			
0		DHC	Snooping	Interface Cont	figuration				
Cont	trol	Diffe	Shooping	Intenace Con	Ingulation				
DHCP Snoopi	ng ^	12	LAG All		Go	To Interface	Go		
Global Confi	guration		Interface	Trust Mode	Invalid Packets	Rate Limit(nns)	Rurst Interval/secs)		
- Interface Co	nfiguration	-	1/0/27	Disable	Enable	Nono	N/A		
Binding Cont	figuration		1/0/2/	Disable *	Disable V	None	N/A		
Descistant C			1/0/1	Disable	Disable	None	N/A		
• Persistent C	onfiguration		1/0/2	Disable	Disable	None	N/A		
 Statistics 		-	1/0/3	Disable	Disable	None	N/A		
• IP Source Gua	ard 🗸		1/0/4	Disable	Disable	None	N/A		
IDUG Source C	lund		1/0/5	Disable	Disable	None	N/A		
- IF vo Source C	Juaru 🗸		1/0/6	Disable	Disable	None	N/A		
Dynamic ARP	Inspection ~		1/0/7	Disable	Disable	None	N/A		
Captive Portal	~		1/0/8	Disable	Disable	None	N/A		
			1/0/9	Disable	Disable	None	N/A		
			1/0/10	Disable	Disable	None	N/A		
			1/0/11	Disable	Disable	None	N/A		
			1/0/12	Disable	Disable	None	N/A		
			1/0/13	Disable	Disable	None	N/A		
			1/0/14	Disable	Disable	None	N/A		
			1/0/15	Disable	Disable	None	N/A		
			1/0/16	Disable	Disable	None	N/A		
			1/0/17	Disable	Disable	None	N/A		
			1/0/18	Disable	Disable	None	N/A		
			1/0/19	Disable	Disable	None	N/A		
			1/0/20	Disable	Disable	None	N/A		
			1/0/21	Disable	Disable	None	N/A		
			1/0/22	Disable	Disable	None	N/A		
			1/0/23	Disable	Disable	None	N/A		
			1/0/24	Disable	Disable	None	N/A		
			1/0/25	Disable	Disable	None	N/A		
			1/0/26	Disable	Disable	None	N/A		
			1/0/27	Disable	Disable	None	N/A		

- b. Select the 1/0/27 check box.
- c. In the Invalid Packets field, select Enable.
- d. Click Apply.
- 3. Determine the IP address and MAC address for the rogue DHCP server:
 - a. Select Monitoring > Logs > Logs > Buffered logs.

A screen similar to the following displays.



b. Search for "DHCP packet; op Reply".

In the previous figure, the IP address of the DHCP server is 10.100.5.253 and the MAC address is 00:26:F2:F6:B3:6C.

Enter Static Binding into the Binding Database

You can also enter the static binding into the binding database.

CLI: Enter Static Binding into the Binding Database

1. Enter the DHCP snooping static binding.

```
(Netgear Switch) (Config)# ip dhcp snooping binding 00:11:11:11:11:11:11 vlan 1 192.168.10 .1 interface 1/0/2
```

2. Check to make sure that the binding database has the static entry.

(GSM7328S) #show ip dhcp snooping binding									
Total number of bi	Total number of bindings: 2								
MAC Address	IP Address	VLAN	Interface	Туре	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.

System	Switching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Secu	rity Acc	ess	Port Authen	tication Traffic	: Control Contro	I ACL			
Control		Stati	c Binding Co	nfiguration					
 DHCP Snooping 	^		Interface	MAC Address	VLAN I	D IP Address			
 Global Configura 	tion		1/0/2 ~	00:11:11:11:1	1:11 1 👻	192.168.10.1			
Interface Configu Binding Configur	iration		1/0/2	00:18:8B:56:F	D:35 1	192.168.10.94	1		

- 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.

System	Switching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Se	ecurity Acc	ess	Port Autheni	tication Traffi	ic Control Cont	rol ACL			
Contr	ol	Statio	: Binding Cor	nfiguration					
DHCP Snooping	9 ^		Interface	MAC Address	s VLAN	ID IP Address			
 Global Config 	uration		1/0/2 ~	00:11:11:11:1	1:11 1 ~	192.168.10.1			
 Interface Con Binding Confi 	figuration ouration		1/0/2	00:18:8B:56:F	FD:35 1	192.168.10.94	4		

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 snc	oping interfaces	s 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.

System Switchin	g	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Security A	cess	Port Auth	entication T	raffic Control 🛛 🔘	ontrol ACL			
Control	DHC	P Snooping	g Interface Con	figuration				
DHCP Snooping	^ 13	LAG AII		(Go To Interface	Go		
 Global Configuration 		Interface	Trust Mode	Invalid Packets	Rate Limit(pps)	Burst Interval(secs)		
 Interface Configuration 								
 Binding Configuration 	-							
- Development Conferentian		1/0/1	Disable	Disable	None	N/A		
- reisistent Conliguration		1/0/2	Disable	Disable	None	N/A		
 Statistics 		1/0/3	Disable	Disable	None	N/A		

2. Select the interface, fill in the Rate Limit (pps) field, and then click Apply.

System Swit	ching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Security	Access	Port Auth	entication T	raffic Control	ontrol ACL			
Control	DHO	CP Snooping	g Interface Cor	figuration				
DHCP Snooping	^ 1 3	3 LAG All		(Go To Interface	Go		
Global Configuration		1 toxatoo	Taxas Mada	Jacobil Phasebooks	Prote 1 (contractory)	Deniet lister collections)		
 Interface Configuration 	n (menace	Trust Mode	Invalid Packets	Rate Limit(pps)	Durst interval(secs)		
Binding Configuration			×	×				
		1/0/1	Disable	Disable	None	N/A		
Persistent Configurati	on 📃	1/0/2	Disable	Disable	None	N/A		
 Statistics 		1/0/3	Disable	Disable	None	N/A		

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.





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 bi	ndings: 1							
MAC Address	IP Address	VLAN	Interface	Туре	Lease (Secs)			
 00:16:76:A7:88:CC	192.168.10.86	 1	1/0/2	DYNAMIC	86400			

If the entry does not exist in the DHCP Snooping Binding table, you can add the entry manually through the ip verify binding <mac-address> vlan <vlan id> <ip address> interface <interface id> command in global configuration mode.

5. Enable IP Source Guard in interface 1/0/2.

```
(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.

System	Switchir	ıg	Routing QoS		Security	Monitoring	Maintenance	Help	Index
Management S	nt Security Access		Port Authenti	cation Traf	fic Control Cor	urði ACL			
Cont	trol	DH	CP Snooping GI	obal Configur	ation				
DHCP Snoopir	ng	^ D	HCP Snooping N	Node	🖲 Disable 🥥) Enable			
Global Config	guration	N	AC Address Val	idation	🔘 Disable 🖲) Enable			
 Interface Cor Binding Cont 	nfiguration figuration	VL.	AN Configuration	r;					
Statistics IP Source Gua	ird	~	VLAN ID		HCP Snooping N	Node			

- **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.

System	Switchir	ig	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	Security A	ccess	Port Authenti	ication Tra	ffic Control Con	trol ACL			
Cont	rol	DH	CP Snooping G	lobal Configu	ration				
• DHCP Snoopin	ng	^ DI	HCP Snooping I	Mode	🔘 Disable 🖲	Enable			
Global Config	guration	M	AC Address Va	ilidation	🔵 Disable 🖲	Enable			
• Interface Cor	nfiguration								
 Binding Cont 	figuration								
• Persistent C	onfiguration	VL/	N Configuration	0					
 Statistics 		6	VLAN ID	I	OHCP Snooping M	ode			
• IP Source Gua	ird	~			~				

- **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.

System	Switchin	g	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Sec	curity Ac	cess	Port Authenti	cation Tra	iffic Control Cont	rol ACL			
Contro	I)	DHC	P Snooping G	obal Configu	ration				
DHCP Snooping		DH	CP Snooping	Node	🔘 Disable 🖲	Enable			
Global Configu	ration	MA	C Address Va	lidation	🔘 Disable 🖲	Enable			
Interface Config	guration								
• Binding Config • Persistent Con	uration figuration	VLA	N Configuration	<u>.</u>					
 Statistics 			VLAN ID		DHCP Snooping M	ode			
•IP Source Guard	spection 、		1	1	Enable 🔻				

d. Click Apply.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Se	ecurity Acces	s Port Authentic	ation Tra	ffic Control Cor	trol ACL			
Contr	ol	HCP Snooping Glo	bal Configu	ration				
• DHCP Snooping	g ^	DHCP Snooping M	ode	🔘 Disable 🖲	Enable			
Global Config	uration	MAC Address Vali	dation	🔘 Disable 🖲	Enable			
 Interface Cont Binding Confi Persistent Co 	figuration guration	/LAN Configuration						
 Statistics IP Source Guar 	d v	VLAN ID	Ĩ	OHCP Snooping N	lode			

- **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.

System	Switching		Routing QoS		Security	Monitoring	Maintenance	Help	Index
Management S	ecurity Acc	ess	Port Author	entication Tr	affic Control	ontrol ACL			
Contr	rol	DHC	P Snooping	Interface Con	figuration				
DHCP Snoopin	HCP Snooping		LAG AII		(Go To Interface	Go		
Global Config	juration		Interface	Trust Mode	Invalid Packets	Rate Limit(pps)	Burst Interval(secs)		
Interface Con	nguration		1/0/1	Enable Y	Disable 🗸	None	N/A		
Binding Confi	guration		1/0/1	Disable	Disable	None	N/A		
Statistics	unguration		1/0/2 1/0/3	Disable Disable	Disable Disable	None None	N/A N/A		

- b. Select Interface 1/0/1 check box.
- c. For interface 1/0/1, in the Trust Mode field, select Enable.
- d. Click Apply.
- a. Select Security > Control > DHCP Snooping Interface Configuration.

A screen similar to the following displays.

System S	Switching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Securi	ty Acc	ess	Port Author	entication Tr	affic Control	ontrol ACL			
Control		DHC	P Snooping	j Interface Con	figuration				
DHCP Snooping		1 3	LAG All		C	Go To Interface	Go		
Global Configuration	on		Interface	Trust Mode	Invalid Packets	Rate Limit(pps)	Burst Interval(secs)		
 Interface Configura 	ation					and the second prove			
Binding Configurat	tion		1/0/1	Enable Y	Disable 👻	None	N/A		
Dinding comgarat	Dinding Conliguration		1/0/1	Disable	Disable	None	N/A		
 Persistent Configuration 			1/0/2	Disable	Disable	None	N/A		
 Statistics 			1/0/3	Disable	Disable	None	N/A		

4. View the DHCP Snooping Binding table.

Select Security > Control > DHCP Snooping Binding Configuration.

A screen similar to the following displays.

System	Switchi	ing		Routing	QoS	Security	Λ	Ionitoring	Mainten	ance	Help	Index
Management Sec	curity A	Acce	ss	Port Authent	ication Tra	ffic Control C		ACL				
Control		Ĩ	Statio	: Binding Cor	figuration							
DHCP Snooping		^		Interface	MAC Addres	ss VL	AN ID	IP Address				
 Global Configur 	ration			~			~					
 Interface Config 	guration	_		1/0/2	00:18:8B:56	:FD:35 1		192.168.10.9	4			
Binding Configu	uration											
Persistent Con Statistics	figuration	E.	Dyna	mic Binding (Configuration							
• IP Source Guard		~	Int	erface MAC	Address VI	AN ID IP Add	Iress L	ease Time				

- 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.

System S	witching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Securit	y Acc	ess	Port Authority	entication Tra	ffic Control Cor	trol ACL			
Control		IP So	ource Guar	d Interface Confi	guration				
DHCP Snooping	~	13	LAG All	Go To Interface		Go			
IP Source Guard	^		Interface	IPSG Mode	IPSG Port Secu	ritaz			
 Interface Configura 	tion	-	intenace	II OO MIDDE	IT OUT OIL ORCU	incy			
Binding Configurati	ion			×	¥				
	17.02		1/0/1	Disable	Disable				
Dynamic ARP Inspection >		1/0/2	Disable	Disable					

- 6. Set up IP source guard static binding.
 - a. Select Security > Control > IP Source Guard > Binding Configuration.
 - **b.** Select the Interface **1/0/2** check box.
 - c. In the MAC Address field, enter 00:05:05:05:05:05.
 - d. In the VLAN ID field, enter 1.
 - e. In the IP Address field, enter 192.168.10.80.
 - f. Click Add.

A screen similar to the following displays.

System	Switch	ning	Rou	ting	QoS	Se	curity	Monitoring	Maintenance	Help	Index
Management S	ecurity	Acce	ess Port	Authen	tication	Traffic Cont	trol Control	ACL			
Contr	rol		Static Bind	ing Co	nfiguration						
DHCP Snoopin	g	v	🔲 Inter	face	MAC Ac	Idress	VLAN ID	IP Address	Filter Typ	e	
• IP Source Guar	rd	^	1/0	/2 ~	00:05:05	5:05:05:05	1 -	192.168.10.80)		
 Interface Con 	figuration			_							
- Binding Confi	guration										
Dynamic ARP I	Inspection	¥	Dynamic E	inding	Configurat	ion					
• Captive Portal		×	Interfac	MAG	C Address	VLAN ID	IP Address	Filter Type			
			1/0/2			1	192.168.10.9	4 ip			

Authorization

Authorization determines if a user is authorized to perform certain activities, including user EXEC command authorization and privileged EXEC command authorization.

Command Authorization

TACACS+ servers support command authorization. The RADIUS protocol does not support command authorization but you can use a vendor-specific attribute (VSA) with attribute value (AV) pair 26 to download a list of commands that are permitted or denied for a user. This list of commands is downloaded from the RADIUS server. When a user executes a command, the command is validated against the downloaded command list for the user. Any change in a user command authorization access list takes effect after a user has logged on and logged in again.

The vendor-specific attribute netgear-cmdAuth is defined as follows:

VENDOR netgear 4526 ATTRIBUTE netgear-cmdAuth 1 string netgear

Specify the command in the following format.

netgear-cmdAuth = "deny:spanning-tree;interface *",

Note: The maximum length of the command string in the vendor attribute cannot be longer than 64 bytes. RADIUS- based command authorization supports a maximum of 50 commands.

Note: You can use both a TACACS+ server and a RADIUS server for command authorization. If the first method of command authorization returns an error, the second method is used for command authorization.

CLI: Configure Command Authorization by a TACACS+ Server

```
(Netgear Switch)(Config)#aaa authorization commands commandlist tacacs
(Netgear Switch)(Config)#tacacs-server host 10.100.5.13
(Netgear Switch)(Config)#exit
(Netgear Switch)(Config)#tacacs-server key 12345678
(Netgear Switch)(Config)#line telnet
(Netgear Switch)(Config-telnet)#authorization commands default
(Netgear Switch)#show authorization methods
show authorization methods : Command Is Not Authorized
(Netgear Switch) #show authorization methods
Command Authorization Method Lists
_____
dfltCmdAuthList
                        •
                              none
commandlist
                       :
                             tacacs
Line Command Method List
_____
Console dfltCmdAuthList
Telnet commandlist
SSH
        dfltCmdAuthList
Exec Authorization Method Lists
_____
dfltExecAuthList
                         •
                              none
Line Exec Method List
_____
Console dfltExecAuthList
Telnet dfltExecAuthList
SSH dfltExecAuthList
```

Exec Authorization

When user command authentication succeeds, the user receives access to the user EXEC mode. You can also provide a user direct access to the privileged EXEC mode by using the EXEC authorization method.

If the EXEC authorization method uses a TACACS+ authorization server, a separate session is established with the TACACS+ server to return the authorization attributes.

If the EXEC authorization method uses a RADIUS authorization server, service-type attribute 6 or Cisco vendor-specific attribute (VSA) "shell:priv-lvl" is used. If the service-type attribute value is returned as administrator or the Cisco VSA "shell:priv-lvl" is at least FD_USER_MGR_ADMIN_ACCESS_LEVEL(15), the user receives access to the privileged EXEC mode.

Because the RADIUS protocol does not support authorization, the privilege level attribute must be returned with the authentication response. If the service-type attribute is already

present in RADIUS response packet as administrator, the Cisco VSA "shell:priv-lvl" is ignored.

CLI: Configure Exec Command Authorization by a TACACS+ Server

(Netgear Sv	(Netgear Switch)(Config)#aaa authorization exec execList tacacs							
(Netgear Sv	witch)(Config)#tacac	s-serve	r host 10.100.5.13					
(Netgear Sv	witch)(Config)#tacac	s-serve	r host 10.100.5.13					
(Netgear Sv	witch)(Config)#tacac	s-serve	r key 12345678					
(Netgear Switch)(Config)#line telnet								
(Netgear Sv	witch)(Config-telnet)#autho	rization commands execList					
(M7100-242	() #show authorizati	on meth	ods					
Command Aut	chorization Method L	ists						
dfltCmdAuth	nList	:	none					
commandlist	<u>.</u>	:	tacacs					
Line	Command Method List							
Console	dfltCmdAuthList							
Telnet	execList							
SSH	dfltCmdAuthList							
Exec Author	rization Method List	s						
dfltExecAut	thList	:	none					
execList		:	tacacs					
Line	Exec Method List							
Console	dfltExecAuthList							
Telnet	execList							
SSH	dfltExecAuthList							

Accounting

The accounting process records what a user does or has done on the switch. You can configure a TACACS+ accounting server or RADIUS accounting server to account for the following actions:

- Account for services that were used, such as in a billing environment. You can use this type of accounting as an auditing tool for security services.
- Account when a user logs in and logs out of a user EXEC session.

CLI: Configure Telnet Command Accounting by a TACACS+ Server

Note: TACACS+ accounting supports both user EXEC command authorization and privileged EXEC command authorization.

```
(Netgear Switch)(Config)#tacacs-server host 10.100.5.13
(Netgear Switch)(Tacacs)#key 12345678
(Netgear Switch)(Tacacs)#exit
(Netgear Switch)(Config)#
(Netgear Switch)(Config)#aaa accounting commands default stop-only tacacs
(Netgear Switch)(Config)#line telnet
(Netgear Switch)(Config-telnet)#accounting commands default
(Netgear Switch)(Config-telnet)#exit
(Netgear Switch) #show accounting methods
AcctType MethodName MethodType
                                 Method1 Method2
Exec dfltExecList start-stop radius
Commands dfltCmdList stop-only tacacs
      EXEC Method List Command Method List
Line
----- ------
Console none
                          none
Telnet dfltExecList
                        dfltCmdList
SSH
      none
                         none
HTTPS none
                          none
HTTP none
                          none
```

Configure Telnet EXEC Accounting by RADIUS Server

RADIUS accounting supports EXEC mode but does not support command mode.

```
(Netgear Switch)(Config) #radius server host acct 10.100.5.13
(Netgear Switch)(Config) #radius server key acct 10.100.5.13
Enter secret (64 characters max):12345678
Re-enter secret:12345678
(Netgear Switch)(Config) #radius accounting mode
(Netgear Switch)(Config)#aaa accounting exec default stop-only radius
(Netgear Switch) #show radius
Number of Configured Authentication Servers.... 0
Number of Configured Accounting Servers..... 1
Number of Named Authentication Server Groups... 0
Number of Named Accounting Server Groups..... 1
Number of Retransmits..... 4
Timeout Duration..... 5
RADIUS Accounting Mode..... Enable
RADIUS Attribute 4 Mode..... Disable
RADIUS Attribute 4 Value..... 0.0.0.0
(Netgear Switch) #show accounting methods
AcctType MethodName MethodType Method1 Method2
_____ ____
      dfltExecList
                                radius
Exec
                     stop-only
Commands dfltCmdList
                     stop-only
                                tacacs
Line
      EXEC Method List
                       Command Method List
_____ ____
Console none
                        none
Telnet dfltExecList
                       dfltCmdList
SSH
     none
                        none
HTTPS
      none
                        none
HTTP
      none
                        none
```

Use the Authentication Manager to Set Up an Authentication Method List

Note: The authentication manager is available on the M6100 series switches only.

The authentication manager lets you configure an authentication method list, which you can apply on a per-port basis. If authentication is disabled, no authentication method is applied and the port provides open access. By default, authentication is disabled for all ports.

The authentication manager lets you configure the following authentication methods in an authentication method list:

- dot1x
- MAB
- captive portal (that is, web authentication)

The default authentication method list applies these authentication methods in the order dot1x, MAB, and captive portal as the default methods for all ports.

You cannot configure another authentication method after the captive portal method, that is, the captive portal method must be the last method in an authentication method list.

When a client connects to a port, the switch attempts to authenticate the client through the port-based authentication method list. If an authentication method times out (or an error occurs), the switch attempts to authenticate with the next authentication method in the list. If all authentication methods time out, the switch starts a timer for which the value is equal to the authentication restart timer. At the expiration of the timer, the authentication manager restarts the authentication process for the first method in the list. If the client connection goes down and comes up again, the authentication manager restarts the authentication sequence.

Note: The authentication manager controls only the order in which the switch executes the authentication methods. The authentication manager does not configure or change the authentication methods. You need to ensure that the switch is configured correctly so that the switch can execute the authentication methods as presented in the authentication method list.

The priority of an authentication method is determined by its position in authentication method list. If you do not configure authentication method priorities, the relative priorities (that is, the highest first) are in the same order as that of the port-based authentication list.

Authentication priority allows a higher-priority method to interrupt an authentication process that is in progress with a lower-priority method. Alternatively, if a client is already authenticated, an interrupt from a higher priority method can cause a client that is already authenticated through a lower-priority method to be reauthenticated through the higher-priority method.

Configure a Dot1x-MAB Authentication Method List with Dot1x-MAB Priority

Note: This section describes how to configure the authentication order and priority. For information about configuring the dot1x authentication method, which is also referred to as 802.1x port security, see *802.1x Port Security* on page 364.

In this example, the authentication manager first selects dot1x as the authentication method. If dot1x authentication is successful, the client is authenticated. If the client is not enabled, dot1x and dot1x authentication time out, and the authentication manager selects MAB as the next authentication method. If MAB authentication is successful, the client is authenticated. If MAB authentication fails, the port is placed in the unauthorized state and the authentication manager starts a timer. When the timer expires, the authentication manager restarts the authentication process with dot1x authentication.



Figure 41. Dot1x, MAB, and captive portal authentication method list with default priority

The CLI command to enable authentication is as follows.

(Netgear Switch)#configure (Netgear Switch)(Config)#authentication enable

Configure a Dot1x-MAB Authentication Method List with MAB-Dot1x Priority

Note: This section describes how to configure the authentication order and priority. For information about configuring the MAB authentication method, see *Configure MAC Authentication Bypass on a Switch* on page 414.

If the switch authenticated a client by using MAB but the client is enabled for dot1x after it is authenticated, the EAPOL start frames that the client sends to the authentication manager causes the port to be placed in the unauthorized state and the switch then attempts to authenticate the client by using dot1x. This situation occurs because the default priority for dot1x authentication is higher than the default priority for MAB authentication.

To prevent the port from being placed in the unauthorized state, assign MAB authentication a higher priority than dot1x authentication. In that situation, if the client sends EAPOL start frames to the authentication manager, the authentication manager selects the first configured authentication method in the list, that is, dot1x, and compares the priority of the current authenticated method (that is, MAB) with the newly selected method (that is, dot1x). Because the priority for MAB authentication is higher than the priority for dot1x authentication, the authentication manager does not start dot1x authentication.

The CLI command to enable authentication is as follows.

(Netgear Switch)#configure (Netgear Switch)(Config)#authentication enable

Configure a Dot1x, MAB, and Captive Portal Authentication Method List with Default Priority

Note: This section describes how to configure the authentication order and priority. For information about configuring the captive portal authentication method, see *Chapter 37, Captive Portal*.



Figure 42. Dot1x, MAB, and captive portal authentication method list with default priority

In this example, a visiting client attempts to connect to a corporate network in which the authentication manager is enabled. In such a situation, configure the authentication method list in the order dot1x, followed by MAB, and followed by captive portal.

If the client is enabled for dot1x but fails to authenticate using dot1x, the authentication manager places the port in the unauthorized state and stops the process. If the client is not enabled for dot1x, the dot1x authentication process times out, and the authentication manager selects the next configured authentication method in the list, which is MAB. Because the client's MAC address is unknown in the corporate network, the MAB authentication process also times out.

The authentication manager selects the third configured authentication method in the list, which is captive portal. If the client can provide valid credentials for web authentication, the client is admitted to the network. If the client cannot provide valid credentials, the authentication manager starts a timer for reauthentication because no other authentication method is available in the list. At the expiration of the timer, the authentication manager restarts the authentication process for the first method in the list.

The CLI command to enable authentication is as follows.

(Netgear Switch)#configure
(Netgear Switch)(Config)#authentication enable

MAB

19

MAC Authentication Bypass

This chapter includes the following sections:

- MAC Authentication Bypass Concepts
- Configure MAC Authentication Bypass on a Switch
- Configure a Network Policy Server on a Microsoft Windows Server 2008 R2 or Later Server
- Configure an Active Directory on a Microsoft Windows Server 2008 R2 or Later Server
- Reduce the MAB Authentication Time

MAC Authentication Bypass Concepts

MAC Authentication Bypass (MAB) provides 802.1X-unaware clients controlled access to the network by using the MAC address of the client device as the identifier.

MAB has the following requirements:

- You must preconfigure the known and allowable MAC addresses and corresponding access rights in the authentication server.
- The port control mode of the port must be MAC-based.

You can configure MAB on a per-port basis. If you configure MAB on a port and the port receives a packet from an unknown MAC address, the following sequence of events can occur:

- 1. The authenticator sends an EAPOL Request ID packet to the supplicant and the switch starts a timer that is based on the guest VLAN period for the supplicant.
- **2.** If the client does not respond when the timer expires, the switch treats the client as an 802.1X-unaware client.
- **3.** The authenticator sends a request to the authentication server with the MAC address of the client in hhhhhhhhhh (nondotted decimal MAC format) format as the user name and the MD5 hash of the MAC address as the password.
- 4. The authentication server checks its preconfigured database for the authorized MAC addresses and returns either an Access-Accept or Access-Reject message, depending on whether the server can find the MAC address in its database.

The switch can place the 802.1X-unaware client in a VLAN that is assigned by the RADIUS server or apply a specific filter ID to the client traffic.

MAB initiates only after the 802.1X guest VLAN period times out. If the client responds to any of the EAPOL identity requests, MAB does not initiate for that client. MAB and guest VLANs are mutually exclusive. If you configure a guest VLAN instead of MAB on a port and the 802.1X guest VLAN period times out, the switch places the client in the guest VLAN. If you do not configure a guest VLAN or MAB on a port and the 802.1X guest VLAN period times out, the switch below the switch denies the client access.

The following figure illustrates MAB operation.



Figure 43. MAB operation

The following figure shows a switch that has MAB configured on port 1/0/1. The IP phone that is connected to this port can access the network after being authenticated successfully by the Microsoft network policy server.



Figure 44. MAB topology with a switch, IP phone, and Microsoft server

Configure MAC Authentication Bypass on a Switch

This section provides an example of how to configure MAC Authentication Bypass (MAB) on a switch. The example is shown as CLI commands and as a web interface procedure.

CLI: Configure the Switch to Perform MAB with a Microsoft Network Policy Server

1. Enable 802.1X authentication on the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#dot1x system-auth-control
```

2. Configure RADIUS to authenticate 802.1X users.

(Netgear Switch) (Config) #aaa authentication dot1x default radius

3. Configure the switch to communicate with the Microsoft network policy server.

In this example, the Microsoft network policy server IP address is 10.1.10.46. The shared key on the switch and the RADIUS server must match.

```
(Netgear Switch) (Config)#radius server host auth 10.1.10.46
(Netgear Switch) (Config)#radius server key auth 10.1.10.46
Enter secret (64 characters max):*****
Re-enter secret:*****
(Netgear Switch) (Config)#radius server primary 10.1.10.46
```

 Configure force-authorization on the port that connects to the Microsoft network policy server (port 1/0/1 in this example).

(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#dot1x port-control force-authorized
(Netgear Switch) (Interface 1/0/1)#exit

5. Configure MAB on the port that connects to the IP phone (port 1/0/10 in this example).

(Netgear	Switch)	#config
(Netgear	Switch)	(Config)#interface 1/0/10
(Netgear	Switch)	(Interface 1/0/10)#dot1x port-control mac-based
(Netgear	Switch)	(Interface 1/0/10)#dot1x mac-auth-bypass
(Netgear	Switch)	(Interface 1/0/10)#exit
(Netgear	Switch)	(config)#exit

6. To reduce the MAB authentication time, decrease the time of guest VLAN period.

(Netgear Switch) #config (Netgear Switch) (Config)#interface 1/0/10 (Netgear Switch) (Interface 1/0/10)#dot1x timeout guest-vlan-period 1

Web Interface: Configure the Switch to Perform MAB with a Microsoft Network Policy Server

- 1. Enable 802.1X authentication on the switch:
 - a. Select Security > Port Authentication > Basic > 802.1X Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monit	oring	Maintenance	Help	Index
Management Sec	curity Acc	ess Port Authent	ication Tra	fic Control Contr	ol ACI	-			
Port Authenti	ication	802.1X Configuration	n						
• Basic	^	Administrative Mo	ode	🔘 Disab	e 🖲 Ena	able			
• 802.1X Configu	iration	VLAN Assignmer	nt Mode	Disab	e 🔘 Ena	able			
 Advanced 	×	EAPOL Flood Mo	ide	💿 Disab	e 🔘 Ena	able			
		Dynamic VLAN C	reation Mode	Disable	~				
		Monitor Mode		Disable	~				
		Users		admin		×			
		Login		defaultL	ist 🗸				
		Authentication Lis	st	dot1xList					

- **b.** Under 802.1X Configuration, next to Administrative Mode, select the **Enable** radio button.
- c. Click Apply.
- 2. Configure RADIUS to authenticate 802.1X users:
 - a. Select Security > Management Security > Authentication List > Dot1x Authentication List.

A screen similar to the following displays.

System	Switchi	ng	Routing	QoS	Security	N	Ionitoring	Maintenance	Help	Index
Management S	ecurity A	ccess	Port Authenti	cation Tra	ffic Control C	Control	ACL			
Managemen	t Security	Dot	1x Authenticati	on List						
Local User		~	List Na	ime	1					
 Enable Passweight 	ord		dot1xL	ist	Radius Y					
Line Password										
• RADIUS		~								
• TACACS		~								
 Authentication 	List	^								
Login Auther	ntication Lis	tsi i								
Enable Authorities	entication									
Dot1x Authe List	ntication									

- **b.** Select the **dot1xList** check box.
- c. From the 1 menu, select Radius.
- d. Click Apply.

3. Configure the switch to communicate with the Microsoft network policy server.

In this example, the IP address of the Microsoft network policy server is 10.1.10.46. The shared key between the switch and the server must match.

a. Select Security > Management Security > RADIUS > Server Configuration.

A screen similar to the following displays.

lystem S	Switching		Routing	QoS	Security	Monitorin	9	Maintenance	Hel		ndex				
ogennett Social	ay Acc	ess	Port Authentic	ation Traffi	c Control Control	ACL									
(a												Add	Delete	Clear counte	rs Update
Management Sec	unty	Serve	r Configuration	(
.cal User nable Password	2		Radius Server	IP Address	Radius Server Nam	e G	arrent P	Port	Secret Configured	Secret		Primary Server	Message Authentic	ator Type	or
ine Password			10.1.10.46		Microsoft-NPS		1	1812	Yes ·			Yes 👻	Enable	- Su	indard 🛩
DIUS		-													
Radius Configurati	ion	Ctati													
Server Configuration	80	Stati	SUC B												
Accounting Server Configuration		Ri	idius Round Inver Trip Tin	Access Requests	Access Retransmissions	Access Accepts	Access Rejects	Access Challenge	Malforma Respons	d Access	Bad Authenticators	Pending Requests	Timeouts	Unknown Types	Packets Dropped
ACACS															
uthentication List	~														
Anin Sassians															

- **b.** Configure the following settings:
 - In the RADIUS Server IP Address field, enter 10.1.10.46.
 - In the RADIUS Server Name field, enter Microsoft-NPS.
 - In the Port field, enter **1812.**
 - From the Secret Configured menu, select Yes.
 - In the Secret field, enter the secret key.
 - From the **Primary Server** menu, select **Yes**.
 - From the Message Authenticator menu, select **Enable**.
 - From the Server Type menu, select **Standard**.
- c. Click Add.
- **4.** Configure the port that connects to the Microsoft network policy server (in this example, port 1/0/1) to be force-authorized:
 - a. Select Security > Port Authentication > Advance > Port Authentication.

A screen similar to the following displays.

						100.0					C	ncel Appl	y Initialize	Reauthentical
Port Authentica	tion	Port	Authenti	cation										0
*Basic	~	12	3 All									Go	To Port	Go
 Advanced 802.1X Configurat 	on		Port	Control Mode	MAB	Quiet Period	Transmit Period	Guest VLAN ID	Guest VLAN Period	Unauthenticated VLAN ID	Supplicant Timeout	Server Timeout	Maximum Requests	PAE Capabilities
Port Authenticate	n (1/0/1	Force Authorized	Disable 👻	60	30	0	90	0)	30	30	2	Authentical
· Port Summary		×	1/0/1	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato
· Client Summary		13	1/0/2	Auto	Disable	60	30	0	90	0	30	30	2	Authenticate
		8	1/0/3	Auto	Disable	60	30	0	90	0	30	30	2	Authenticate
		13	1/0/4	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato
		0	1/0/5	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato
		0	1/0/6	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato
		1	1/0/7	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato
			1/0/8	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato
			1/0/9	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato
	_	0	1/0/10	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato

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

The table heading displays the information for port 0/1.

- **c.** Configure the following settings:
 - From the Control Mode menu, select Force Authorized.
 - From the MAB menu, select **Disable**.

Leave all other settings on the screen at their default value.

- d. Click Apply.
- 5. Configure the port that connects to the IP phone (in this example, port 1/0/10) for MAB:
 - a. Select Security > Port Authentication > Advance > Port Authentication.

A screen similar to the following displays.

System S	Switching		Routin	g QoS	Security	Monitoring	Maintenary	ce He	lp Index					
Management Securit	ty Acce	195		trentoution Traffic	Control Control	ACL								
											Ca	ncri Appl	y Initializo	Reauthenticale
Port Authentical	tion	Port	Authentic	ation										0
• Basic	*	12	3 All									Go	To Port	Go
Advanced 802 1X Configurati	ion	•	Port.	Control Mode	MAB	Quiet Period	Transmit Period	Guest VLAN ID	Guest VLAN Penod	Unauthenticated VLAN ID	Supplicant Timeout	Server Timeout	Maximum Requests	PAE Capabilities
Port Authenticatio	n		1/0/10	MAC Based	· Disable ·	60	30	0	90	0	30	30	2	Authenticat
*Port Summary			1/0/1	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato
Client Summary		13	1/0/2	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato
		- 63	1/0/3	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato
			1/0/4	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato
		10	1/0/5	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato
		10	1/0/6	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato
		B	1/0/7	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato
		E	1/0/8	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato
			1/0/9	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato
		2	1/0/10	Auto	Disable	60	30	0	90	0	30	30	2	Authenticato

b. Select the check box that corresponds to port 0/10.

The table heading displays the information for port 0/10.

- c. Configure the following settings:
 - From the Control Mode menu, select **MAC Based**.
 - From the MAB menu, select Enable.

Leave all other settings on the screen at their default value.

d. Click Apply.

Note: For information about how to reduce the MAB authentication time, see *Reduce the MAB Authentication Time* on page 427.

Configure a Network Policy Server on a Microsoft Windows Server 2008 R2 or Later Server

1. Enable EAP-MD5 support.



WARNING:

Serious problems can occur if you modify the registry incorrectly by using the Registry Editor or by using another method. These problems might require that you reinstall your Microsoft operating system. Modify the registry at your own risk.

To reenable EAP-MD5 support in Microsoft Windows Vista, add the following registry entries:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\4
```

```
Value name: RolesSupported
Value type: REG_DWORD
Value data: 000000a
Value name: FriendlyName
Value type: REG_SZ
Value data: MD5-Challenge
Value name: Path
Value type: REG_EXPAND_SZ
Value data: %SystemRoot%\System32\Raschap.dll
Value type: REG_DWORD
Value data: 0000001
Value type: REG_DWORD
Value data: 0000001
```

2. If your Windows server 2008 R2 does not have service pack 1 installed, download and install Microsoft hot fix KB981190 from the following Microsoft website:

http://support.microsoft.com/kb/981190.

- 3. On the Windows server 2008 R2, configure the RADIUS client:
 - a. Click Network Policy and Access Services > NPS > RADIUS Clients and Servers > RADIUS Clients.

The server manager starts.



- **b.** Configure the following settings:
 - In the Friendly name field, enter the switch name (in this example, enter **M4100-D12G**).
 - In the Address (IP or DNS) field, enter the IP address of the switch that connects to the network policy server (in this example, enter **10.1.10.50**.
 - In the Shared secret field and Confirm shared secret field, enter the secret key.

The shared key between the switch and the server must match.

- 4. Configure the connection request policies for the network policy server:
 - a. Click Network Policy and Access Services > NPS > Policies > Connection Request Policies.
 - b. Double-click Secured Wired (Ethernet) Connections.

The Secure Wired (Ethernet) Connections Properties pop-up screen displays with the Overview tab selected:

🖡 Server Manager			_ 6 >
File Action View Help			
Server Hanager Ration Vew Hep Server Manager Ven Hep Server Manager Ven Hep Active Directory Certificate Services DNS Server DNS Server DNS Server DNS Server RADUS Clents and Servers RADUS Clents RADUS Clent	Connection Request Policies Connection request policies allow forwards to remote RADIUS se connection request policy. Policy Name Secure Wired (Ethernet) Con- Connections Policy Name Policy Name Policy Name Policy Name Policy Nate Forabled. NPS evaluates I Policy Nate Forabled. NPS evaluates Policy State Forabled. NPS evaluates Policy State Forabled. NPS evaluates Policy State Forabled. Policy Policy Policy Policy State Forabled. Policy State Forabled. Policy State Forabled. Policy State Forabled. Policy State Forabled. Policy State Forabled. Policy State Forabled. Policy State Forabled. Policy State Forabled. Policy Po	w you to designate whether connection requests are processed locally or wrem. For NAP VPN or 802 1X, you must configure PEAP authentication in Ratus Processing Order Source Frubled 1 Unspecified nacctions Properties Secure Wired (Ethemet) Connection Secure Wired (Ethemet) Connection d consecure to NPS, You can select et the policy while processing connection request to NPS. You can select et the trebler is required. If your network access server is an 802 1X authenticate as server:	Actions Connection Request Policies New Expertist Wex Exertist Wex Exertist Wex Exertist Exer
B Gonfguration B E Storage	Setta Set Ad Cor NA Set Set Set Set Set Set Set Set Set Set	access server that sends the connection request to NPS. You can select at Inether is required. If your network access server is an 302 1X authentication is server:	her the network access server ng switch or windess access point,
			X Cancel Apply

- c. Select the Policy enabled check box.
- d. From the Type of network access server menu, select Unspecified.Leave the Vendor specific radio button cleared.
- e. Click the Apply button.
- f. Click the Conditions tab.

server Manager (WIN-#MLUUQM513P)	Connection Request Policies			Actions
Roles	Connection request polici	es allow you to designate	whether connection requests are processed locally or	Connection Request Policies
Active Directory Domain Services Server	forwarded to remote RAD connection request policy	IUS servers, For NAP VP /.	N or 802 1X, you must configure PEAP authentication in	New
Network Policy and Access Services	Policy Name	Status Pr	ocessing Order Source	
RADIUS Clients and Servers	Secure Wired (Bhemet) Conne	ections Enabled 1	Unspecified	View
RADIUS Clients	Secure Wired (Etherne	et) Connections Prop	erties	×
Remote RADIUS Server Groups	Ourselaw Conditions	Cattions		
Connection Request Policies	Overview	l serraide l		Innectio
Network Policies	Configure the condition	ns for this network policy.		
Health Policies	If conditions match the	connection request, NP	S uses this policy to authorize the connection request. If condition	ns do not match the
Network Access Protection Accounting	connection request, N	PS skips this policy and e	evaluates other policies, il additional policies are configured.	
E 📕 Templates Management			NAS Port Type	×
Routing and Remote Access	S Condition	Value	Specify the access media types required to match this policy	
Features	S NAS Port Type	Ethernet	Common dial-up and VPN tunnel types	
Diagnostics	Conc		Async (Modem)	
Storage	Cor		ISDN Sync	
	NA		Virtual (VPN)	
			Common 802 1X connection tunnel types	
			Ethemet	
			D FDDI	
			Token Ring	
			Wreless - IEEE 802.11	
			Others	
			ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase	e Modulation
			Async (Modem)	-
	Setti		Cable	
	Set Condition description:			
	Aut The NAS Port Type co	ondition specifies the type 5 802 11 wireless and Di	or	Cancel 1
	Ed	- vol. 11 mileress, drid El	UN	
	At			
	Ove		Add	Edit Remove

- **g.** Configure the NAS Port Type field as Ethernet.
- h. Click the Apply button.
- i. Click the Settings tab.



- j. Select the Override Network policy authentication settings check box.
- **k.** Under the EAP Types field, click the **Add** button.
- I. From the menu, select MD5-Challenge.
- m. Click the OK button.

MD5-Challenge is added to the EAP Types field.

- n. From the EAP Types field, select MD5-Challenge.
- o. Click the Apply button.
- 5. Configure the network policies for the network policy server:
 - a. Click Network Policy and Access Services > NPS > Policies > Network Policies.
 - b. Double-click Secured Wired (Ethernet) Connections.

The Secure Wired (Ethernet) Connections Properties pop-up screen displays with the Overview tab selected:



- c. Select the Policy enabled check box.
- d. Select the Grant access radio button.
- e. From the Type of network access server menu, select **Unspecified**. Leave the Vendor specific radio button cleared.
- f. Click the Apply button.
- g. Click the Conditions tab.



- **h.** Configure the NAS Port Type field as Ethernet.
- i. Click the Apply button.
- j. Click the Constraints tab.



- **k.** Under the EAP Types field, click the **Add** button.
- I. From the menu, select MD5-Challenge.
- m. Click the OK button.

MD5-Challenge is added to the EAP Types field.

- n. From the EAP Types field, select MD5-Challenge.
- o. Click the Apply button.
- p. Click the Settings tab.



- **q.** Select all four encryption check boxes, including the **No encryption** check box.
- **r.** Click the **Apply** button.

Configure an Active Directory on a Microsoft Windows Server 2008 R2 or Later Server

- 1. Create a user account with the following settings:
 - **Logon name**. The MAC address of the device for which you want to allow a connection.
 - **Password**. Any temporary password.
- 2. Right-click the new user account name and select Properties.



- 3. Select the **Password never expires** check box.
- 4. Select the Store password using reversible encryption check box.
- 5. Click the Apply button.
- 6. Create a Password Settings Object (PSO) as described at the following Microsoft website:

http://technet.microsoft.com/en-us/library/cc754461(v=ws.10).aspx.

Use the default setting for all the attributes except for the following setting: msDS-PasswordComplexityEnabled = FALSE.

7. Apply PSO to the user account that you created in *Step 1*, as described at the following Microsoft website:

http://technet.microsoft.com/en-us/library/cc731589(v=ws.10).aspx#BKMK_1.

8. Change the password for the user account that you created in Step 1.

For the password, use the MAC address of the device for which you want to allow a connection, and use uppercase letters only.

Reduce the MAB Authentication Time

MAB waits for the expiration of the guest VLAN period before MAB sends a request to the authentication server with the MAC address as the user name and the MD5 hash as the password. To reduce the MAB authentication time, decrease the guest VLAN period. The default period for the guest VLAN period is 90 seconds.

CLI: Reduce the Authentication Time for MAB

Change the guest VLAN period timer to 10 seconds using the CLI:

```
(Netgear Switch) #config
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#dot1x timeout guest-vlan-period 10
```

Web Interface: Reduce the Authentication Time for MAB

Change the guest VLAN period timer to 10 seconds using the web interface:

1. Select Security > Port Authentication > Advanced > Port Authentication.

A screen similar to the following displays.

System Sw	vitching.	1 1	Routin	g QoS S	ecurity	Monitoring	Maintena	nce He	slp Index				
Management Security	Acc	855		mentiousine Traffic Co	ntroi Control	ACL							
Port Authenticatio	an i	Port	Authenti	cation							9	incel Appl	y Initialize
•Basic	~	12	3 All									Go	To Port
Advanced 802.1X Configuration	î		Port	Control Mode	MAB	Quiet Period	Transmit Period	Guest VLAN ID	Guest VLAN Period	Unauthenticated VLAN ID	Supplicant Timeout	Server Timeout	Maximum Requests
Port Authentication			1/0/1	MAC Based	Enable Y	60	30	0	10	0	30	30	2
Port Summary			1/0/1	Auto	Disable	60	30	0	90	0	30	30	2
Client Summary			1/0/2	Auto	Disable	60	30	0	90	0	30	30	2
200			1/0/3	Auto	Disable	60	30	0	90	0	30	30	2
		1	1/0/4	Auto	Disable	60	30	0	90	0	30	30	2
		10	1/0/5	Auto	Disable	60	30	0	90	0	30	30	2
		. 83	1/0/6	Auto	Disable	60	30	0	90	0	30	-30	2
			1/0/7	Auto	Disable	60	30	0	90	0	30	30	2
		- 🖂	1/0/8	Auto	Disable	60	30	0	90	0	30	30	2
		- 63	1/0/9	Auto	Disable	60	30	0	90	0	30	30	2
		8	1/0/10	Auto	Disable	60	30	0	90	0	30	30	2

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

The table heading displays the information for port 0/1.

3. In the Guest VLAN Period field, enter 10

Leave the other settings on the screen at the default value.

4. Click Apply.

SNTP

Simple Network Time Protocol

This chapter includes the following sections:

- Simple Network Time Protocol Concepts
- Show SNTP (CLI Only)
- Configure SNTP
- Set the Time Zone (CLI Only)
- Set the Named SNTP Server



Simple Network Time Protocol Concepts

Simple Network Time Protocol (SNTP) offers the following benefits:

- It can be used to synchronize network resources and for adaptation of NTP.
- SNTP provides synchronized network timestamp.
- It can be used in broadcast or unicast mode.
- It supports SNTP client implemented over UDP, which listens on port 123.

Show SNTP (CLI Only)

The following are examples of the commands used in the SNTP feature.

show sntp

```
(Netgear Switch) #show sntp?
<cr> Press Enter to execute the command.
client Display SNTP Client Information.
server Display SNTP Server Information.
```

show sntp client

(Netgear Switch) #show snt	o client
Client Supported Modes:	unicast broadcast
SNTP Version:	4
Port:	123
Client Mode:	unicast
Unicast Poll Interval:	б
Poll Timeout (seconds):	5
Poll Retry:	1

show sntp server

(Netgear Switch) #show snt	p server
Server IP Address:	81.169.155.234
Server Type:	ipv4
Server Stratum:	3
Server Reference Id:	NTP Srv: 212.186.110.32
Server Mode:	Server
Server Maximum Entries:	3
Server Current Entries:	1
SNTP Servers	
IP Address:	81.169.155.234
Address Type:	IPV4
Priority:	1
Version:	4
Port:	123
Last Update Time:	MAY 18 04:59:13 2005
Last Attempt Time:	MAY 18 11:59:33 2005
Last Update Status:	Other
Total Unicast Requests:	1111
Failed Unicast Requests:	361

Configure SNTP

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

CLI: Configure SNTP

NETGEAR switches do not have a built-in real-time clock. However, it is possible to use SNTP to get the time from a public SNTP/NTP server over the Internet. You may need permission from those public time servers. The following steps configure SNTP on the switch:

1. Configure the SNTP server IP address.

The IP address can be either from the public NTP server or your own. You can search the Internet to locate the public server. The servers available could be listed in domain-name format instead of address format. In that case, use the ping command on the PC to find the server's IP address. The following example configures the SNTP server IP address to 208.14.208.19.

(Netgear Switch) (Config)#sntp server 208.14.208.19

2. After configuring the IP address, enable SNTP client mode.

The client mode can be either broadcast mode or unicast mode. If the NTP server is not your own, you must use unicast mode.

(Netgear Switch) (Config)#sntp client mode unicast

When the SNTP client mode is enabled, the client waits for the polling interval to send the query to the server. The default value is approximately 1 minute.

3. After this period, issue the show command to confirm that the time was received.

The time will be used in all logging messages.

```
(Netgear Switch) #show sntp server
Server IP Address:
                                  208.14.208.19
Server Type:
                                 ipv4
Server Stratum:
                                  4
Server Reference Id:
                                NTP Srv: 208.14.208.3
Server Mode:
                                 Server
Server Maximum Entries:
                                 3
                                 1
Server Current Entries:
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.

System	Switch	ning		Routing	QoS	Secur	rity	Monitori	ng	Maintenance	Help	Index		
Management	Device V	iew	Serv	ices Chass	is PoE	SNMP	LLDP IS	DP Ti	mer Sc	hedule				
Manag	ement		SNTP	Server Config	uration									
 System Inform 	ation			Server Type	Address					Port		Priority	Ve	rsion
System CPU :	Status	~		IPv4 ¥	208.14.20	8.19				123		1	4	1
 Switch Statist 	ics			DNS	time-d.net	gear.com				123		1	4	
USB Device In	formation													
 Loopback Inte 	face													
Network Interfa	ace	~	SNTP	Server Statu										
• Time		^	Ad	dress	Last L	Jpdate Time		Las	st Atter	npt Time	Last Atte	mpt Status	Requests	Failed Requests
• Time Config	uration		tin	ie-d.netgear.c	om Jan 1	00:00:00 19	70 (UTC+0	.00) Jan	n 1 00:0	0:00 1970 (UTC+0:00)	Other		0	0
 SNTP Serve Configuration 	r n													
 Summer Tin Configuration 	1e 1													

- **b.** Enter the following information:
 - In the Server Type field, select IPV4.
 - In the Address field, enter 208.14.208.19.
 - In the **Port** field, enter **123**.
 - In the **Priority** field, enter **1**.
 - In the Version field, enter 4.
- c. Click Add.
- 2. Configure SNTP globally.
 - a. Select System > Management > Time > SNTP Global Configuration.

A screen similar to the following displays.

System	Switching	Rout	ing	QoS	Secu	irity	Moni	toring	Maintenance	Help	Index
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer S	chedule		
Manage	ement	Time Config	uration								
 System Inform 	ation	Clock Sou	rce	O Loc	al 💿 SNTI	P					
• System CPU S	Status 🗸 🗸										
 Switch Statisti 	cs										
• USB Device In	formation	SNTP Globa	al Configura	tion							
Loopback Inter	face	Client Mod	le		Oisal	ble 💿 U	nicast 🔘	Broadcas	st		
 Network Interfa 	ice 🗸	Port			123	(1	23 or 102	25 to 6553	35) Default:123		
• Time	^	Unicast Po	oll Interval		6	(6	to 10)				
 Time Configu 	uration	Broadcast	Poll Interva	d.	6	(6	to 10)				
• SNTP Server	r	Unicast Po	oll Timeout		5	(1	to 30)				
Configuration	1	Unicast Po	oll Retry		1	(0	to 10)				
Configuration	1e 1	Time Zone	Name		PST						
• DNS	~	Offset Hou	rs		-8	(-	12 to 13)				
 SDM Template 	Preference	Offset Min	utes		0	(0	to 59)				
• Green Etherne	t v										
- **b.** Enter the following information:
 - For Client Mode, Select the **Unicast** radio button.
 - In the Time Zone Name field, enter PST.
 - In the Offset Hours field, enter -8.
- c. Click Apply.

Set the Time Zone (CLI Only)

The SNTP/NTP server is set to Coordinated Universal Time (UTC) by default. The following example shows how to set the time zone to Pacific Standard Time (PST), which is 8 hours behind GMT/UTC.

```
(Netgear switch)(config)#clock timezone PST -8
```

Set the Named SNTP Server

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

CLI: Set the Named SNTP Server

NETGEAR provides SNTP servers accessible by NETGEAR devices. Because NETGEAR might change IP addresses assigned to its time servers, it is best to access an SNTP server by DNS name instead of using a hard-coded IP address. The public time servers available are time-a, time-b, and time-c.

Enable a DNS name server and access a time server with the following commands:

```
(Netgear switch) (config)#ip domain-lookup
(Netgear switch) (config)#ip name-server 192.168.1.1
(Netgear switch) (config)#sntp server time-a.netgear.com
```

where 192.168.1.1 is the public network gateway IP address for your device.

This method of setting DNS name look-up can be used for any other applications that require a public IP address, for example, a RADIUS server.

Web Interface: Set the Named SNTP Server

- **1.** Configure the SNTP server.
 - a. Select System > Management > Time > SNTP Server Configuration.

A screen similar to the following displays.

System	Switch	ing		Routi	ng	QoS	Sec	urity	Mon	itoring	Ma	aintenance	Help	Index		
Management	Device Vi	ew	Serv	ices	Chassis	PoE	SNMP	LLDP	ISDP	Timer S	chedule					
Manag	ement		SNTF	Server	Configu	ration										
 System Inform 	ation			Server	Type	Adrees						Port		Priority	Me	reion
• System CPU :	Status	~	5.00	Conver	Type	-1001033						T ON		ritomy	, v e	Talon .
 Switch Statist 	cs			DNS	~	time-f.netg	ear.com					123		1	4	
USB Dovice In	formation			IPv4	4	208.14.208	8.19					123		1	4	
- COD Device III	ionnation			DNS	1	ime-d.net	gear.com					123		1	4	
 Loopback Intel 	rtace															
Network Interfa	ace	~	ONTE		01-1											
• Time		~	SINTE	Server	Status											
• Time Config	uration		Ad	Idress		Last U	pdate Tin	пе		Last Atte	empt Tir	ne	Last Att	empt Status	Requests	Failed Requests
SNTP Serve			20	8.14.20	8.19	Jan 1	00:00:00	1970 (UTC	C+0:00)	Jan 1 00	00:00 1	1970 (UTC+0:00)	Other		0	0
Configuration	0		tin	ne-d.net	tgear.co	n Jul 14	19:49 <mark>:28</mark>	2014 (UT	C+0:00)	Jul 14 19	9:50:40	2014 (UTC+0:00)	Succes	S	4	0
 Summer Tin Configuration 	าe า															
• DNS		~														
SDM Template	Preference	э														
Green Etherne	t.	×														

- **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.

System	Switching	Ro	uting	QoS	Sec	urity	Moni	toring	Maintenance	Help	Index
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer Sc	:hedule		
Manage	ement	DNS Confi	guration								
 System Inform 	ation	DNS Sta	tus		0	Disable () Enable				
System CPU 8	Status 🗸 🗸	DNS Def	ault Name					(1 to 25	5 alphanumeric cha	aracters)	
 Switch Statisti 	cs	Retry Nu	mber		2			(0 to 10)	0)		
USB Device In	formation	Respons	e Timeout (secs)	3			(0 to 36)	00 secs)		
 Loopback Inter 	face										
 Network Interfa 	ice v										
• Time	*	DNS Serve	er Configura	tion							
• DNS	^	🗐 Seri	al No DN	S Server		Prefere	nce				
DNS Configu	iration		192	2.168.1.1							
 Host Configu 	iration	1	219	.141.140.	10	1					
 SDM Template 	Preference	2	12.1	7.210.170		0					
• Green Etherne	t v										

- **b.** Enter the following information:
 - For DNS Status, select the **Enable** radio button
 - In the DNS Server field, enter 192.168.1.1.
- c. Click Add.

Tools

21

Tools to manage, monitor, and personalize the switch and network

This chapter includes the following sections:

- Traceroute
- Configuration Scripting
- Pre-Login Banner
- Port Mirroring
- Remote SPAN
- Dual Image
- Outbound Telnet
- Full Memory Dump

Traceroute

This section describes the traceroute feature. Use traceroute to discover routes that packets take when traveling on a hop-by-hop basis to their destination through the network.

- Traceroute maps network routes by sending packets with small time-to-live (TTL) values and watches the ICMP time-out announcements.
- The traceroute command displays all L3 devices.
- It can be used to detect issues on the network.
- Traceroute tracks up to 20 hops.
- The default UPD port is used 33343 unless you specify otherwise in the traceroute command.

The following shows an example of using the traceroute command to determine how many hops there are to the destination. The command output shows each IP address that the packet passes through and how long it takes for the packet to reach its destination. In this example, the packet takes 16 hops to reach its destination.

CLI: Traceroute

(Net	gear Switch) #tra	aceroute?			
<ipa< td=""><td>addr> Enter</td><td>IP address.</td><td></td><td></td><td></td></ipa<>	addr> Enter	IP address.			
(Net	gear Switch) #tra	aceroute 21	6.109.118.74	1 ?	
<cr></cr>	> Press Enter	to execute	the command		
<poi< td=""><td>et> Enter j</td><td>port no.</td><td></td><td></td><td></td></poi<>	et> Enter j	port no.			
(Net	gear Switch) #tra	aceroute 21	6.109.118.74	ł	
trad	cing 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	
б	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.

System	Swi	tching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Save Config	Reset	Upload	Download	File Managem	ent Troublesho	oling			a. 10
Trouble	shooting	Tra	aceRoute IPv₄	1					
• Ping IPv4		IF	^o Address/Ho	stname	216.109.118.74	(Max 255 c	characters/x.x.x.x)		
Ping IPv6		F	Probes Per Ho	р	3	(1 to 10)			
Traceroute IF	Pv4	N	Nax TTL		30	(1 to 255)			
 Traceroute IF 	°∨6	lr	nit TTL		1	(1 to 255)			
		N	/laxFail		5	(1 to 255)			
		łr	nterval(secs)		3	(1 to 60)			
		F	ort		33434	(1 to 6553	5)		
		5	lize		0	(0 to 3993)	6)		
		5	Source		None ~				

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 Command
- script list Command and script delete Command
- script apply running-config.scr Command
- Create a Configuration Script
- Upload a Configuration Script

Configuration scripting:

- Allows you to generate text-formatted files.
- Provides scripts that can be uploaded and downloaded to the system.
- Provides flexibility to create command configuration scripts.
- Can be applied to several switches.
- Can save up to 10 scripts or 500 K of memory.
- Provides script format of one CLI command per line.

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 Command

(Netgear S	witch) #script ?
apply	Applies configuration script to the switch.
delete	Deletes a configuration script file from the switch.
list	Lists all configuration script files present on the switch.
show	Displays the contents of configuration script.
validate	Validate the commands of configuration script.

script list Command and script delete Command

script apply running-config.scr Command

(Netgear Switch) #script apply running-config.scr Are you sure you want to apply the configuration script? (y/n) y The system has unsaved changes. Would you like to save them now? (y/n) y Configuration Saved!

Create a Configuration Script

(Netgear Switch) #show running-c	onfig running-config.scr
Config script created successful	ly.
(Netgear Switch)	#script list
Configuration Script Name	Size(Bytes)
running-config.scr	3201
<pre>1 configuration script(s) found. 1020799 bytes free.</pre>	

Upload a Configuration Script

```
(Netgear Switch) #copy nvram: script running-config.scr
tftp://192.168.77.52/running-config.scr
Mode....
                             TFTP
Set TFTP Server IP.....
                            192.168.77.52
TFTP Path....
                             ./
TFTP Filename.....
                             running-config.scr
Data Type.....
                            Config Script
Source Filename.....
                            running-config.scr
Are you sure you want to start? (y/n) y
File transfer operation completed successfully.
```

Pre-Login Banner

Pre-login banner:

- Allows you to create message screens that display when a user logs in to the CLI.
- By default, no banner file exists.
- You can upload or download.
- File size cannot be larger than 2 K.

The Pre-Login Banner feature is only for the CLI interface.

Create a Pre-Login Banner

This command is provided for the CLI only.

1. On your computer, use Notepad to create a banner.txt file that contains the banner to be displayed.

Login Banner - Unauthorized access is punishable by law.

2. Transfer the file from the PC to the switch using TFTP.

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 S	Switch)#config			
(Netgear S	Switch)(Config)#monito	r session 1	mode	
Enable min	rror			
(Netgear S	Switch)(Config)#monito	r session 1	source interface 1/0/2	
Specify th	ne source interface.			
(Netgear S	Switch)(Config)#monito	r session 1	destination interface	1/0/3
Specify th	ne destination interfa	ce.		
(Netgear S	Switch)(Config)#exit			
(Netgear S	Switch)#show monitor s	ession 1		
Session II	D Admin Mode Pr	obe Port	Mirrored Port	
1	En	able	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.

System	Switching	9	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Ports Logs		sFlow							
Mirro	oring	Mirrori	ng Global Co	onfiguration					
Multiple Port I	Mirroring	Desti Sess Status	nation Interfa ion Mode Table	ice	1/0/3 ↔	Enable			
		123	CPU LAGS	All			Go T <mark>o</mark> Ir	nterface	Go
			Source Po	rt	E	Direction	Status		
			1/0/2		1	Γx and Rx 👻	Mirror		
			1/0/1			5.6 K			
			1/0/2 1/0/3		Т	x and Rx	Mirror		

- 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.

Remote SPAN

Mirroring lets you monitor traffic to and from a port by copying the traffic to a probe port for analysis. Mirroring is usually limited to on one switch. With a remote switched port analyzer (RSPAN), you can extend mirroring to all participating switches.





In the previous figure, Switch 1 is the source switch, Switch 2 and Switch 3 are intermediate switches, and Switch 4 is the destination switch.

You must configure the ports that are connected to the destination switch with tagging, with the VLAN ID as the RSPAN VLAN. You must also configure the ports on the intermediate switches that are connected to the source switch and destination switch with the RSPAN VLAN. Only one RSPAN VLAN is supported.

On the source switch, the traffic that is received on and transmitted from source port (1/0/1) is tagged with the RSPAN VLAN and transmitted on the configured reflector port. The reflector port (1/0/2) is the physical interface that carries the mirrored traffic to the destination switch.

The intermediate switches forward the incoming tagged traffic to the destination switch. Enable RSPAN VLAN egress tagging on the ports of the intermediate switches that are connected to the destination switch.

The destination switch accepts all the packets that are tagged with the RSPAN VLAN and mirrors the packets on the destination port to which you must connect a traffic analyzer.

The original tag is retained at the destination switch. Mirrored traffic has double tagging: The inner tag is the original VLAN ID and the outer tag is the RSPAN VLAN ID.

CLI: Enable RSPAN on a Switch

- 1. On the source switch (Switch 1), configure the following settings:
 - Source ports (the ports for which the traffic must be mirrored)
 - RSPAN VLAN (the destination for the mirrored traffic)
 - Reflector port (the port that is connected, through the intermediate switches, to the destination switch)
 - Tx/Rx (both egress and ingress traffic must be mirrored)

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 5
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#vlan 5
(Netgear Switch) (Config)(Vlan 5)#remote-span
(Netgear Switch) (Config)(Vlan 5)#exit
(Netgear Switch) (Config) #monitor session 1 mode
(Netgear Switch) (Config) #monitor session 1 source interface 1/0/1
(Netgear Switch) (Config)#monitor session 1 destination remote vlan 5 reflector-port
1/0/2
(Netgear Switch) (Config)#exit
(Netgear Switch) #show monitor session 1
Session Admin Probe Src Mirrored Ref. Src Dst Type IP
                                                          MAC
ID Mode Port VLAN Port Port RVLAN RVLAN
                                                    ACL
                                                           ACL
 _____ _____
1
                       1/0/1 1/0/2
                                          5 Rx,Tx
      Enable
```

2. On the intermediate switches (Switch 2 and Switch 3), configure the ports that are connected to the source and destination switches as tagged members of the VLAN.

Note: You do not need to configure RSPAN on the intermediate switches.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 5
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/23
(Netgear Switch) (Interface 1/0/23)#vlan participation include 5
(Netgear Switch) (Interface 1/0/23)#vlan tagging 5
(Netgear Switch) (Interface 1/0/23)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan participation include 5
(Netgear Switch) (Interface 1/0/24)#vlan tagging 5
(Netgear Switch) (Interface 1/0/24)#vlan tagging 5
(Netgear Switch) (Interface 1/0/24)#vlan tagging 5
```

- 3. On the destination switch (Switch 4), configure the following settings:
 - RSPAN VLAN (the source of the mirrored traffic)
 - The probe port (the port that is connected, through the intermediate switches, to the source switch)

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 5
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#vlan 5
(Netgear Switch) (Config)(Vlan 5) #remote-span
(Netgear Switch) (Config)(Vlan 5)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#vlan participation include 5
(Netgear Switch) (Interface 1/0/3)#vlan tagging 5
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config) #monitor session 1 mode
(Netgear Switch) (Config) #monitor session 1 source remote vlan 5
(Netgear Switch) (Config)#monitor session 1 destination interface 1/0/4
(Netgear Switch) #show monitor session 1
Session Admin Probe Src Mirrored Ref. Src Dst Type IP
                                                               MAC
TD
      Mode
            Port
                   VLAN Port
                                Port RVLAN RVLAN
                                                       ACL
                                                               ACL
_____ _____
1
    Enable 1/0/4
                                       5
```

Dual Image

Traditionally switches contain a single image in the permanent storage. This image is loaded into memory every time there is a reboot. The dual image feature allows switches to have two images in permanent storage. You can denote one of these images as an active image that will be loaded in subsequent reboots and the other image as a backup image. This feature provides for reduced down time for the switches, when the firmware is being upgraded or downgraded.

The images are stored in the file system with the file names *image1* and *image2*. These names are used in the CLI, Web, and SNMP interfaces. Each of the images can be associated with a textual description. The switch provides commands to associate and retrieve the text description for an image. A switch also provides commands to activate the backup image such that it is loaded in subsequent reboots. This activation command makes the current active image as the backup image for subsequent reboots.

On three successive errors executing the **active-image**, the switch attempts to execute the **backup-image**. If there are errors executing the **backup-image** as well, the bootloader will invoke the boot menu.

The Dual Image feature works seamlessly with the stacking feature. All members in the stack must be uniform in their support for the dual Image feature. The Dual Image feature works in the following way in a stack.

- When an image is activated, the management node notifies all the participating nodes. All nodes activate the specified image.
- When any node is unable to execute the **active-image** successfully, it attempts to execute the **backup-image**. Such cases will require user intervention to correct the problem, by using appropriate stacking commands.

CLI: Download a Backup Image and Make It Active

```
(Netgear Switch) #copy tftp://192.168.0.1/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
    imagel
             image2
                    current-active
                                   next-active
_____
            8.0.0.2
    5.11.2.51
                       image1
1
                                    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
_____
    5.11.2.51 8.0.0.2
1
                       imagel
                                    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.

System	Swi	tching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Save Config	Reset	Upload		File Managem	ent Troublesho	oting			(.).
Down	load	Fil	e Download						
File Download		F	ile Type		Archive		~		
HTTP File Dov	vnload	Ir	mage Name		image2 ×				
USB File Dow	nload	Т	ransfer Mode		TFTP Y				
		S	Server Address	з Туре	IPv4 ×				
		5	erver Address	8	10.100.5.7				
		F	Remote File Pa	ath	1				
		F	Remote File Na	ame	Gsm73xxse-r8v0	m0b3.			
1									

- 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.

System	Switchin	g	Rou	ting Qa	S Sec	urity Monitor	ing Maintena	nce Help
Save Config	Reset Up	load l	Downlo	ad File Man	agement Tro	oubleshooting		
File Man	agement	Dual	Image	Configuration				
• Copy		1		10 I I 20		lean or or or	No	
• Dual Imaga C	opfouration		Unit	Image Name	Active Image	Next Active Image	Image Description	Version
- Duai mage o	uniguration		1	image2	False	True 🛩		6.11.15.11
			1	image1	True	True		10.2.0.5
			1	image2	False	False		6.11.15.11

- **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
- CLI: transport output telnet
- Web Interface: Configure Telnet
- CLI: Configure the Session Limit and Session Time-out
- Web Interface: Configure the Session Time-out

Outbound Telnet:

- Establishes an outbound Telnet connection between a device and a remote host.
- A Telnet connection is initiated, each side of the connection is assumed to originate and terminate at a network virtual terminal (NVT).
- Server and user hosts do not maintain information about the characteristics of each other's terminals and terminal handling conventions.
- Must use a valid IP address.

CLI: show network

```
(Netgear Switch) >telnet 192.168.77.151
Trying 192.168.77.151...
(Netgear Switch)
User:admin
Password:
(Netgear Switch)
             >en
Password:
(Netgear Switch)
             #show network
IP Address..... 192.168.77.151
Subnet Mask..... 255.255.255.0
Default Gateway...... 192.168.77.127
Locally Administered MAC Address..... 00:00:00:00:00:00
MAC Address Type..... Burned In
Network Configuration Protocol Current... DHCP
Management VLAN ID..... 1
Web Mode..... Enable
Java Mode ..... Disable
```

CLI: show telnet

(Netgear Switch)#show telnet Outbound Telnet Login Timeout (minutes)..... 5 Maximum Number of Outbound Telnet Sessions.... 5 Allow New Outbound Telnet Sessions...... Yes

CLI: transport output telnet

```
(Netgear Switch) (Config)#lineconfig ?
<cr>
                         Press Enter to execute the command.
(Netgear Switch) (Config)#lineconfig
(Netgear Switch) (Line)#transport ?
input
                         Displays the protocols to use to connect to a
                         specific line of the router.
output
                         Displays the protocols to use for outgoing
                         connections from a line.
(Netgear Switch) (Line)#transport output ?
telnet
                        Allow or disallow new telnet sessions.
(Netgear Switch) (Line)#transport output telnet ?
                         Press Enter to execute the command.
<cr>
(Netgear Switch) (Line)#transport output telnet
(Netgear Switch) (Line)#
```

Web Interface: Configure Telnet

1. Select Security > Access > Telnet.

System	Switching	Routing QoS	Security	Monitoring	Maintenance	Help	Index
Management See	curity Access	s Port Authentication Traffi	ic Control Cor	itrol ACL		ż	
Access • HTTP • HTTPS • SSH	s I	Enable Authentication List	enableList	v			
Telnet Console Port Denial of Service Configuration Access Control	~	Telnet Server Admin Mode Allow new telnet sessions Session Timeout (Minutes) Maximum Number of Sessions Current Number of Sessions utbound Telnet	Dis Dis 5 0	able Enable (1 (C	to 160) to 5)		
	1	Allow new telnet sessions Session Timeout (Minutes) Maximum Number of Sessions Current Number of Sessions	 Dis 5 0 	able Enable (1 (6)	to 160)) to 5)		

- 2. Under Outbound Telnet, for Admin Mode, select the Enable radio button.
- 3. Click Apply.

CLI: Configure the Session Limit and Session Time-out

```
(Netgear Switch) (Line)#session-limit ?
<0-5> Configure the maximum number of outbound telnet sessions
allowed.
(Netgear Switch) (Line)#session-limit 5
(Netgear Switch) (Line)#session-timeout ?
<1-160> Enter time in minutes.
(Netgear Switch) (Line)#session-timeout 15
```

Web Interface: Configure the Session Time-out

1. Select Security > Access > Telnet.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	ecurity Acces	s Port Authent	ication Traf	fic Control Cor	trol ACL			×
Acce	SS	Enable Authentic	ation List	enableList	×			
• HTTP • HTTPS • SSH	ž I	nbound Telnet						
- Telnet		Telnet Server Adr	min Mode	O Disa	able e Enable			
Console Port		Allow new telnet	sessions	O Disa	able 🖲 Enable			
Denial of Service	e	Session Timeout	(Minutes)	5		(1 to 160)		
Access Contro	· ·	Maximum Numbe	er of Sessions	5	((0 to 5)		
,		Current Number o	of Sessions	0				
	<u>-</u>	Outbound Telnet						
		Allow new telnet	sessions	O Disa	able 🖲 Enable			
		Session Timeout	(Minutes)	15	((1 to 160)		
		Maximum Numbe	er of Sessions	5] ((0 to 5)		
		Current Number of	of Sessions	0				

- 2. Enter the following information:
 - In the Session Timeout field, enter 15.
 - In the Maximum number of sessions field, enter 5.
- **3.** Click **Apply**.

Full Memory Dump

The full memory dump feature provides the ability to retrieve the state of a crashed system and load it into a debugger to recreate the crashed state. This capability is useful when the switch encounters a crash. The following example shows how to enable this feature and dump the information from a switch.

1. Select the way to transfer the exception dump.

You can select NFS, TFTP, or USB. If you select NFS, you need an NFS share mount point on the network. Similarly, for TFTP mode, you need a TFTP server on the network. For USB mode, you need a USB sticker plugged into the USB slot on the front panel.

(Netgear Switch) (Config) #exception protocol tftp

2. Configure the IP address for the NFS or TFTP server.

(Netgear Switch) (Config) #exception dump tftp-server 172.26.2.100

3. Change the name of the dump file.

The file name is formed as follows:

- If hostname is selected: file-name-prefix_hostname_Time_Stamp.bin
- If hostname is not selected: file-name-prefix_MAC_Address_Time_Stamp.bin

By default, the file name is core, but you can change it with the following command:

(Netgear Switch) (Config) #exception core-file mydump

4. (Optional) Enable the switch-chip-register.

This dumps the register value in the chipset.

(Netgear Switch) (Config) #exception switch-chip-register enable

Syslog

System logging

This chapter includes the following sections:

- Syslog Concepts
- Show Logging
- Show Logging Buffered
- Show Logging Traplogs
- Show Logging Hosts
- Configure Logging for a Port
- Email Alerting



Syslog Concepts

The syslog feature:

- Allows you to store system messages and errors.
- Can store to local files on the switch or a remote server running a syslog daemon.
- Provides a method of collecting message logs from many systems.

The following illustration explains how to interpret log files.



Figure 46. Log Files

Show Logging

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

CLI: Show Logging

(Netgear Switch) #show logging	Netgear Switch) #show logging						
Lenging Glient Legel Dout		F14					
Logging Client Local Port	•	514					
CLI Command Logging	:	disabled					
Console Logging	:	disabled					
Console Logging Severity Filter	:	alert					
Buffered Logging	:	enabled					
Syslog Logging	:	enabled					
plane postud		chabica					
Log Messages Received	:	66					
Log Messages Dropped	:	0					
Log Messages Relayed	:	0					
Log Messages Ignored	:	0					

Web Interface: Show Logging

- 1. Configure the syslog.
 - a. From the main menu, select **Monitoring > Logs > Sys Log Configuration**.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Mo	nitoring	Maintenance	Help	Index
Ports Logs	Mirroring s	Flow							
Logs		Syslog Configuration							
Buffered Logs		Admin Status		🔘 Disable 🖲 Er	able				
Command Log Configuration		Local UDP Port		514	(1	to 65535)			
Console Log Co	nfiguration	Messages Receive	d	919					
Syslog Configur	ation	Messages Relayed		0					
• Trap Logs		Messages Ignored		0					
 Event Logs 									
Persistent Logs		Host Configuration							
		IP Address Ty	pe Host	Address	Status	Port	Sev	erity Filter	
			×					×	

- **b.** In the Syslog Configuration, next to the Admin Status, select the **Enable** radio button.
- c. Click Apply.
- **2.** Configure the command log.
 - a. Select Monitoring > Logs > Command Log.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Ports Logs	Mirroring sF	low				14. V		0
Logs		Command Log Con	figuration					
 Buffered Logs 		Admin Status	Oisa	able 🔘 Enable				
Command Log Configuration								
Console Log Cor	nfiguration							

- **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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Ports Logs I	Mirroring sFlo	W						
Logs	Co	nsole Log Config	uration					
 Buffered Logs 	A	dmin Status	🔘 Disa	ible 🖲 Enable				
 Command Log Configuration 	S	everity Filter	Alert	~				
Console Log Con	figuration							
 Syslog Configurat 	tion							
 Trap Logs 								
 Event Logs 								
Persistent Logs								

- **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.

System Switchin	ig Routing	QoS	Security	Monitoring	Maintenance	Help	Index	
Ports Logs Mirroring	sFlow							
Logs	Buffered Logs							
Buffered Logs	Admin Status	Oisable	Enable					
Command Log Configuration	Behavior	Wrap	*					
Console Log Configuration								
 Syslog Configuration 	Message Log							
 Trap Logs 	Total number of M	20000	102					
 Event Logs 	Total Humber of M	cooligeo	102					
Persistent Logs	Description							
	<14> Jan 1 02:0	9:23 192.168.10.	138-1 UNITM	IGR[127337108]: un	iitmgr.c(6895) 921 %%	Copy of run	ning configurati	on to <mark>b</mark> ackup unit complete
	<14> Jan 1 02:0	6:55 192.168.10	138-1 CLI_W	'EB[127641740]: en	nweb_common_custo	n.c(119) 919	%% HTTP Sea	ssion 11 ended for user adn
	<14> Jan 1 01:5	3:0 <mark>3</mark> 192.168.10	138-1 Genera	al[127641740]: mair	1_login.c(214) 918 %%	HTTP Sessi	on 13 initiated	for user admin connected fr
	<14> Jan 1 01:5	3:03 192.168.10.	138-1 CLI_W	'EB[127641740]: en	nweb_common_custo	n.c(162) 917	%% HTTP See	ssion 13 started for user ad
	<14> Jan 1 01:5	1:57 192.168.10.	138-1 UNITM	IGR[127337108]: un	itmgr.c(6895) 916 %%	Copy of run	ning configurati	on to backup unit complete
	<14> Jan 1 01:4	9:57 192.168.10	138-1 UNITM	IGR[127337108]: ur	iitmgr.c(6895) 914 %%	Copy of run	ning configurati	on to backup unit complete
	<14> Jan 1 01:4	6: <mark>4</mark> 4 192.168.10	138-1 UNITM	IGR[127337108]: un	itmgr.c(6895) 912 %%	Copy of run	ning configurati	on to backup unit complete
	<14> Jan 1 01:4	2:36 192.168.10.	138-1 UNITM	IGR[127337108]: un	itmgr.c(6895) 910 %%	Copy of run	ning configurati	on to backup unit complete

- **b.** Under Buffer Logs, for Admin Status, select the **Enable** radio button.
- c. Click Apply.

Show Logging Buffered

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

CLI: Show Logging Buffered

```
(Netgear Switch) #show logging buffered ?
        Press Enter to execute the command.
<cr>
(Netgear Switch) #show logging buffered
Buffered (In-Memory) Logging
                                    : enabled
Buffered Logging Wrapping Behavior : On
                                    : 3949
Buffered Log Count
<14> Jan 13 00:42:58 172.26.2.129-1 CLI_WEB[101123540]: emweb_common_custom.c(119)
6497 %% HTTP Session 11 ended for user admin connected from 10.120.5.28
<14> Jan 13 00:36:21 172.26.2.129-1 UNITMGR[102633148]: unitmgr.c(6898) 6496 %% Copy
of running configuration to backup unit complete
<14> Jan 13 00:34:21 172.26.2.129-1 UNITMGR[102633148]: unitmgr.c(6898) 6494 %% Copy
of running configuration to backup unit complete
<13> Jan 13 00:33:45 172.26.2.129-1 TRAPMGR[102518604]: traputil.c(701) 6492 %% Link
Up: tunnel0
<13> Jan 13 00:33:44 172.26.2.129-1 TRAPMGR[102518604]: traputil.c(701) 6491 %% Link
Down: tunnel0
<13> Jan 13 00:33:44 172.26.2.129-1 TRAPMGR[102518604]: traputil.c(701) 6490 %% Link
Up: tunnel0
```

The priority (that is, the number that is stated in angle brackets before each logging message, for example, <14> in the previous example) is calculated by multiplying the facility number by 8 and adding the numerical value of the severity. If you know the priority, you can determine the facility and severity in the following ways:

- Facility = Priority divided by 8. The whole number is the facility. For example, if the priority is 14, divide 14 by 8. The result is 1.75. The whole number is 1, which is the facility.
- Severity = Priority minus 8. For example, if the priority is 14, subtract 8 from 14. The result is 6, which is the severity.

Web Interface: Show Logging Buffered

Select **Monitoring > Logs > Buffer Logs**. A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index	
Ports Logs	Mirroring sl	Flow							
Logs		Buffered Logs							
Buffered Logs		Admin Status	🔘 Disa	ble 🖲 Enable					
 Command Log Configuration 		Behavior	Wrap	~					
Console Log Con	figuration								
 Syslog Configura 	ition	Message Log							
 Trap Logs 		Tatal averbas of M		400					
Event Logs		Total number of iv	lessages	102					
Persistent Logs		Description							
		<14> Jan 1 02:0	9:23 192.168.	10.138-1 UNITM	/IGR[127337108]: un	itmgr.c(6895) 921 %9	6 Copy of runi	ning configurat	ion to backup unit complete
		<14> Jan 1 02:0	6:55 192.168.	10.138-1 CLI_V	VEB[127641740]: en	nweb_common_custo	m.c(119) 919	%% HTTP Se	ssion 11 ended for user admi
		<14> Jan 1 01:5	3:03 <mark>1</mark> 92.168.	10.138-1 Gener	ral[127641740]: mair	login.c(214) 918 %%	6 HTTP Sessi	on 13 initiated	for user admin connected fro
		<14> Jan 1 01:5	3:03 192.168.	10.138-1 CLI_V	VEB[127641740]: en	nweb_common_custo	m.c(162) 917	%% HTTP Se	ssion 13 started for user adm
		<14> Jan 1 01:5	1:57 192.168	10.138-1 UNITM	//GR[127337108]: un	itmgr.c(6895) 916 %%	6 Copy of runi	ning configurat	ion to backup unit complete
		<14> Jan 1 01:4	9:57 192.168.	10.138-1 UNIT	MGR[127337108]: un	itmgr.c(6895) 914 %%	6 Copy of runi	ning configurat	ion to backup unit complete
		<14> Jan 1 01:4	6:44 192.168.	10.138-1 UNITM	/IGR[127337108]: un	itmgr.c(6895) 912 %%	6 Copy of runi	ning configurat	ion to backup unit complete
		<14> Jan 1 01:4	2:36 192.168.	10.138-1 UNITM	/IGR[127337108]: un	itmgr.c(6895) 910 %%	6 Copy of runi	ning configurat	ion to backup unit complete

Show Logging Traplogs

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

CLI: Show Logging Traplogs

(Netgear Switch)	#show logging traplogs ?							
<pre><cr> Press Enter to execute the command.</cr></pre>								
(Netgear Switch)	#show logging traplogs							
Number of Traps Since Last	Reset 6							
Trap Log Capacity								
Number of Traps Since Log	Last Viewed 6							
Log System Up Time	Тгар							
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: \setminus							
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.

System	Switching	Roi	uting QoS	Security	Monitoring	Maintenance	Help	Index
Ports Logs	Mirroring sFlor	N						
Log	s Tra	p Logs						
Buffered Logs	N	umber d	of Traps Since Last	Reset	34			
Command Log	Tr	ap Log	Capacity		256			
Console Log Co	onfiguration	umber d	of Traps Since Log I	_ast Viewed	34			
 Syslog Configu 	iration							
Trap Logs	Тга	n Logs						
• Event Logs		p nogo					-	
Persistent Logs	s 🧧	.og S	ystem Up Time	Тгар				
200) Ja	an 1 00:02:15 1970	Cold Start: Unit: I				
		1 Ja	an 1 00:01:47 1970	Link Up: vlan 1				
		2 Ja	an 1 00:01:39 1970	Spanning Tree To	pology Change Initia	ated: 0, Interface: 2/0/3	3	
	3	3 Ja	an 1 00:01:39 1970	Spanning Tree To	pology Change: 0, l	Unit: 1		
	14	4 Ja	an 1 00:01:39 1970	Link Up: 2/0/3				
		5 Ja	an 1 00:01:36 1970	Power On Start h	as completed on un	iit 1.		
	1	6 Ja	an 1 00:01:26 1970	SFP inserted in 2	/0/41			
		7 Ja	an 1 00:01:23 1970	Entity Database:	Configuration Chang	ged		
		3 Ja	an 1 00:01:18 1970	SFP inserted in 3	/0/1	800		

Show Logging Hosts

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

CLI: Show Logging Hosts



Web Interface: Show Logging Hosts

Select **Monitoring > Logs > Sys Log Configuration**. A screen similar to the following displays.

System Switch	ing Routing	J QoS	Security	Mo	nitoring	Maintenance	Help
Ports Logs Mirroring	sFlow			- 44		A	· · · ·
Logs	Syslog Config	uration					
Buffered Logs	Admin Statu	s	🔘 Disable 🖲 E	Enable			
Command Log Configuration	Local UDP F	ort	514	()	to 65535)		
Console Log Configuration	Messages R	eceived	923				
 Syslog Configuration 	Messages R	elayed	0				
• Trap Logs	Messages Ig	nored	0				
 Event Logs 							
Persistent Logs	Host Configura	ation					
	Those Conligue						
	IP Addr	ess Type Hos	t Address	Status	Port	Severi	ty Filter
		~					~
	IPv4	192	168.21.253	Active	514	Critica	1

Configure Logging for a Port

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

CLI: Configure Logging for the Port

(Netgear Switch)	#config
(Netgear Switch)	(Config)#logging ?
buffered	Buffered (In-Memory) Logging Configuration.
cli-command	CLI Command Logging Configuration.
console	Console Logging Configuration.
host	Enter IP Address for Logging Host
syslog	Syslog Configuration.
(Netgear Switch)	(Config)#logging host ?
<hostaddress></hostaddress>	Enter Logging Host IP Address
reconfigure	Logging Host Reconfiguration
remove	Logging Host Removal
(Netgear Switch)	(Config)#logging host 192.168.21.253 ?
<cr></cr>	Press Enter to execute the command.
<port></port>	Enter Port Id

```
(Netgear Switch) (Config)#logging host 192.168.21.253 4 ?
               Press Enter to execute the command.
<cr>
<severitylevel> Enter Logging Severity Level (emergency|0, alert|1, critical|2,
error 3, warning 4, notice 5, info 6, debug 7).
(Netgear Switch) (Config) #logging host 192.168.21.253 4 1 ?
<cr>
              Press Enter to execute the command.
(Netgear Switch) (Config)#logging host 192.168.21.253 4 1
(Netgear Switch) #show logging hosts
Index IP Address
                       Severity Port Status
----- ----- ----- -----
     192.168.21.253 alert
1
                                   4
                                        Active
```

Web Interface: Configure Logging for the Port

1. Select Monitoring > Logs > Sys Log Configuration.

System	Switching	Routing	QoS Security	Mo	nitoring	Maintenance	Help	Index	
Ports Logs M	irroring sFlow	y							
	0.5	les Que ferreites							
Logs	Sysi	log Configuration							
 Buffered Logs 	Ad	imin Status	🔘 Disable 🖲) Enable					
 Command Log Configuration 	Loc	cal UDP Port	514	(1	to 65535)				
Console Log Config	guration Me	ssages Received	925						
 Syslog Configuration 	on	issages Relayed	U						
• Trap Logs	Me	ssages Ignored	0						
 Event Logs 									
Persistent Logs	Hos	t Configuration							
		IP Address Type	Host Address	Status	Port	Severil	ty Filter		
		~					~		
		J IPv4	192.168.21.253	Active	4	Alert			

- 2. Enter the following information:
 - In the Host Address field, enter your host address 192.168.21.253.
 - In the **Port** field, enter **4**.
 - In the Severity Filter list, select Alert.
- 3. Click Add.

Email Alerting

Email alerting is an extension of the logging system. The logging system allows you to configure a set of destinations for log messages. This feature adds the email configuration, through which the log messages are sent to a configured SMTP server such that an administrator can receive the log in an email account of their choice.

This feature is enabled globally. When email alerting is enabled, selected log messages are sent to an SMTP server. Log messages are divided into three groups by severity level: urgent, nonurgent, and never.



Figure 47. Log message severity levels

The network administrator can adjust the urgent and non-urgent severity levels. These levels are global and apply to all destination email addresses. Log messages in the urgent group are sent immediately to the SMTP server with each log message in a separate mail. After a delay period that you can configure, log messages in the nonurgent group are placed in a batch in a single email message.

Email alerting also provides a configuration option that allows the network administrator to specify the severity level at which SNMP traps are logged. Using this option, the administrator can put traps in the urgent group, the non-urgent group, or the never group for emailing. Traps are not emailed by default. For traps to be emailed, the network administrator has to either increase the severity at which traps are logged, or lower the severity level of log messages that are emailed.

The network administrator can configure multiple destination email addresses, and for each email address, specify whether to deliver urgent log messages, nonurgent log messages, or both.

When the log buffer is full, an exception occurs to how messages are sent to the SMTP server. When the log buffer is full before the periodic timer expires, the periodic timer is ignored and all log messages that were not sent previously are immediately forwarded to the SMTP server.

CLI: Send Log Messages to admin@switch.com Using Account aaaa@netgear.com

1. Configure an SMTP server, for example, smtp.netgear.com. Before you configure the SMTP server, you need to have an account on SMTP server.

```
(Netgear Switch) (Config)#mail-server "smtp.netgear.com" port 465
(Netgear Switch) (Mail-Server)#security tlsv1
(Netgear Switch) (Mail-Server)# username aaaa
(Netgear Switch) (Mail-Server)# password xxxxxx
(Netgear Switch) (Mail-Server)#exit
```

2. Configure logging mail. The from-addr is the source address of the email and the to-addr is the destination address of the email.

```
(Netgear Switch) (Config)#logging email
(Netgear Switch) (Config)#logging email from-addr aaaa@netgear.com
(Netgear Switch) (Config)#logging email message-type urgent to-addr
admin@switch.com
(Netgear Switch) (Config)#logging email message-type non-urgent to-addr
admin@switch.com
```

3. Increase the severity of traps to 3 (error). By default, it is 6 (informational).

```
(Netgear Switch) (Config)#logging traps 3
```

Chassis Switch Management



Configure system and interface features

This chapter includes the following sections:

- Chassis Switch Management and Connectivity
- Supervisor and Chassis Members
- Chassis Firmware
- Add, Remove, or Replace a Chassis Member
- Chassis Switch Configuration Files
- Preconfigure a Switch
- Move the Supervisor to a Different Blade

Note: Chassis switch management is available on the M6100 series switches only.

Chassis Switch Management and Connectivity

You can manage the chassis switch through the supervisor. To access the supervisor, use either a serial connection to the chassis supervisor's console port or a Telnet connection to the IP address of service port (out-of-baud) or normal ports on the front panel.

You can use any of the following methods to manage the chassis:

- Web management interface
- CLI (over a serial connection, Telnet, or SSH)
- A network management application through SNMP

Supervisor and Chassis Members

A chassis switch is a set of up to three blade boards. The blades connect to each other through the chassis backplane. The blade that controls the operation of the chassis is the supervisor. The other blade boards in the chassis are chassis members. Layer 2 and Layer 3 protocols present the entire chassis as a single entity to the network.

Supervisor

The supervisor is the single point of chassis management. From the supervisor, you configure the following features:

- System-level (global) features that apply to all chassis members
- Interface-level features for all interfaces on any chassis member

A chassis is identified in the network by its network IP address. The network IP address is assigned according to the MAC address of the supervisor. Every chassis member is uniquely identified by slot number.

The supervisor contains the saved and running configuration files for the members. The configuration files include the system-level settings for the chassis switch and the interface-level settings for all chassis members. Each chassis member retains a copy of the saved file for backup purposes. If the supervisor is removed from the chassis, another member is elected supervisor and then runs from that saved configuration.

Only a member in slot 1 or 2 is eligible to be chassis supervisor. If the chassis supervisor becomes unavailable, the member in standby is elected as supervisor. A set of factors determine which switch is elected the supervisor. The supervisor is elected or reelected based on one of the following factors and in the order listed:

- 1. The blade that is currently the supervisor.
- 2. The blade in slot 1 has a higher priority value than the blade in slot 2.
- 3. Only the blade in slot 1 or slot 2 can be elected supervisor.

A supervisor retains its role unless one of these events occurs:

- The supervisor is removed from the chassis.
- The supervisor is reset or powered off.
- The supervisor fails.

If a supervisor reelection occurs, the new supervisor becomes available after a few seconds. In the meantime, the chassis uses the forwarding tables in memory to minimize network disruption. The physical interfaces on the other available chassis members are not affected while a new supervisor is elected. If a new supervisor is elected and the previous supervisor becomes available, the previous supervisor does not resume its role as supervisor.

Chassis Members

A chassis has up to three blades connected through the backplane. A chassis always includes one supervisor; the other blades are members. The operation of the chassis continues uninterrupted during membership changes unless you remove the supervisor.

A slot number (1 to 3) identifies each member in the chassis. The slot number also determines the interface-level configuration that a chassis member uses. You can display the slot member number by using the show chassis command. The slot number is fixed per slot and not changed.

Chassis Firmware

All chassis members must run the same firmware version. This helps ensure full compatibility in the chassis protocol version among the chassis members.

If a chassis member is running a different firmware version than the supervisor, that chassis member is not allowed to join the chassis. Use the show chassis command to list the chassis members and firmware versions. For more information, see *Code Mismatch* on page 469.

You can upgrade a member that is running an incompatible firmware image by using the following command: copy [image1 |image2] unit://<1-3>/[image1|image2]

This command copies the firmware image from a supervisor to the one with incompatible firmware. You must reload the member to join the chassis as a fully functioning member.

Code Mismatch

If a member is added to a chassis and it does not use the same version of code as that of the supervisor, the following occurs:

- Ports on the added member remain in the detached state.
- A message displays on the CLI indicating a code mismatch with the newly added member.
- To cause the newly added member to merge normally with the chassis switch, use the copy command to load the correct code from the supervisor to the newly added member. Then reset the newly added member. It reboots normally and joins the chassis switch.
Configuration Mismatch

If a member is added to a chassis and the member is of a different model type than that of a preconfigured member, the following occurs:

- Ports on that member remain in the detached state.
- A message displays in the log indicating a code mismatch with that member.
- To cause the member to merge normally with the chassis, use the no member commend to reset the model type.

Upgrade the Firmware

All chassis members must run the same firmware version. Ports on chassis members that do not match the supervisor's firmware version do not come up, and the show chassis command shows a code mismatch error.

- 1. NETGEAR recommends that you schedule the firmware upgrade when no excessive network traffic (such as a broadcast event) is occurring.
- 2. Download new firmware to the supervisor using TFTP or HTTP and the copy command.

Once the firmware is successfully loaded on the supervisor, it automatically propagates to the other members in the chassis.

CAUTION: To avoid errors during code propagation, do not remove supervisor or members.

- 3. If an error occurs during code propagation, first check to make sure that the supervisor is running the correct firmware. Then issue the copy command to make another attempt to copy the firmware to the members that were not updated.
- 4. After code is loaded to all members of the chassis, 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, use the following procedure:

- 1. Save the current configuration by uploading it from the chassis, using the copy command from the CLI.
- 2. Load new code into the chassis supervisor. Reboot the chassis.
- 3. After the chassis boots, issue the clear configure command to erase the current configuration.
- 4. Download the saved configuration back to the master. This configuration is then automatically propagated to all members of the chassis switch.

Add, Remove, or Replace a Chassis Member

You can add, remove, or replace a chassis member.

Add a Blade to an Operating Chassis

- 1. Preconfigure the new member, if desired.
- 2. Remove the blank front panel from the chassis slot.
- 3. Slide the blade slightly into the open slot.
- 4. Keep the injector/ejector handles in the open position as you slide the blade into the chassis slot.
- 5. Use both hands to push both handles toward the center of the blade.
- 6. Finger tighten or use a screwdriver to turn the front pane screws on each injector/ejector handle clockwise and completely down.
- 7. Verify, by monitoring the supervisor console port, that the new blade joins the chassis by issuing the show chassis command. The new blade should join as a member (never as supervisor; the existing supervisor of the chassis should not change).
- 8. If the firmware version of the newly added member is not the same as the existing supervisor, update the firmware as described in *Upgrade the Firmware* on page 470.

Remove a Blade from the Chassis

- 1. Finger loosen or use a screwdriver to turn the screws on each injector/ejector handle counterclockwise and completely up.
- 2. Use both hands to pull up both handles from the center of the blade.
- 3. Pull out the blade slightly and then completely out.
- 4. Install the blank front panel to the open slot.
- 5. To remove the member from the chassis configuration, issue the no member <unit-id> command.

Replace a Chassis Member

- 1. Finger loosen or use a screwdriver to turn the screws on each injector/ejector handle counterclockwise and completely up.
- 2. Use both hands to pull up both handles from the center of the blade.
- 3. Pull out the blade slightly and then completely out.
- 4. If you will be installing a blade that is a different model, remove the blade from the configuration by issuing the no member <unit-id> command.
- 5. Install the new blade in the chassis.

You can put it either in the same position as the previous blade or in another open slot.

6. If you are installing a blade that is the same model, put it in the same position in the chassis as the one that you just removed.

- 7. Verify, by monitoring the supervisor console port, that the new member successfully joins the chassis by issuing the show chassis command. The new blade should join as a member (never as supervisor; the existing supervisor of the chassis should not change).
- 8. If the code version of the newly added member is not the same as the existing chassis, update the code as described in *Upgrade the Firmware* on page 470.

Chassis Switch Configuration Files

The configuration files record the settings for all global and interface-specific settings that define the operation of the chassis and individual members. Once a save config command is issued, all chassis members store a copy of the configuration settings. If a supervisor becomes unavailable, any chassis member that assumes the role of supervisor will operate from the saved configuration files.

Note: The supervisor does not store the copy of configuration settings to the newly added member until you issue the save or write memory command. If you add a new member to the chassis, make sure to issue the save or write memory command after the new member join the chassis successfully.

Preconfigure a Switch

You can preconfigure (supply a configuration to) a new blade before it joins the chassis. You can specify the chassis member number, the blade type, and the interfaces associated with a blade that is not currently part of the chassis.

Note: If you are replacing a member with the same model in the same position in the chassis, you do not need to preconfigure it. The new member assumes the same configuration as the previous member.

- 1. Issue the member <unit-id> <switchindex> command. To view the supported unit types, use the show supported switchtype command.
- **2.** Configure the member that you just defined with configuration commands, just as if the member 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 member type for a specific slot number, attaching a blade with a different blade type for this slot number causes the chassis to report an error. The show chassis command indicates a configuration mismatch for the new member and the ports on that slot do not come up. To resolve this situation, you can change the slot number of the mismatched unit or delete the preconfigured blade type using the no member <unit-id> command.

When you add a new blade to the chassis, the chassis applies either the preconfigured configuration or the default configuration. The following table lists the events that occur when the chassis compares the preconfigured configuration with the new member.

Same Blade Type	Same Slot	Result
Yes	Yes	The chassis applies the configuration to the preconfigured new blade and adds the blade to the chassis.
Yes	No	The chassis applies the default configuration to the new blade and adds the blade to the chassis.
No	Yes	The chassis considers it a configuration mismatch. All of its ports retain detached mode and no configuration applies to the member.
No	No	The chassis applies the default configuration to the new blade and adds the blade to the chassis.

 Table 3. Preconfigured blade compared to chassis configuration

Move the Supervisor to a Different Blade

Only one blade can be the supervisor in one chassis. But you can move the supervisor to another blade if you must do so. In the chassis, only the blades in slot 1 or slot 2 can be used as the supervisor, so two blades are required and they are in slot 1 and slot 2.

This example is provided as CLI commands and a web interface procedure.

CLI: Move the Supervisor to a Different Blade

- 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 configuration. The command is movemanagement <fromunit-id> <tounit-id>.
- 2. Make sure that you can log in on the console attached to the new supervisor. Use the show switch command to verify that all blades rejoined the chassis.
- 3. NETGEAR recommends that you reset the chassis with the reload command after moving the supervisor.

Web Interface: Move the Supervisor to a Different Blade

1. Select System > Chassis > Basic > Chassis Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS Security	/ Monitoring	Maintenance He	lip Index	
Management	Device View	Senices Channe	PoE SNMP L	DP ISOP Timer Sch	iédule		
Char	ssis	Chassis Sample Mod	0				
Basic	-	Sample Mode	Commutation . w				_
+ Chassis Co	alguration.	Max samples	0				
Advanced							
•NSP	1						
		Chassis Configuration	6				
		Unit ID Swite	th Type	Hardware Manager	nent Preference	Management Status	
		2 - XCA	18944F 🗸	Unassigned		Management +	
		1 XCM	1948-uPoE	Unassigned		Marcon Marcon Co	
		2 XCM	1944F	Unassigned		Management	
						StandBy	

2. Under Chassis Configuration, scroll down and select the **Unit ID 2** check box.

Now 2 appears in the Unit ID field at the top.

- 3. In the Management Status drop-down list, select Management.
- 4. Click the Apply button.
 - **Note:** If you move the management from the supervisor to standby, you can lose the connection to the chassis because the IP address could change if the switch gets its IP address using DHCP.

Switch Stacks



Manage switch stacks

This chapter describes the concepts and recommended operating procedures to manage NETGEAR stackable managed switches that are running release 11.0 or a newer release.

This chapter includes the following sections:

- Switch Stack Management and Connectivity
- Stack Master and Stack Members
- Install and Power-up a Stack
- Switch Firmware and Firmware Mismatch
- Stack Switches Using Ethernet Ports and a Stack Cable
- Stack Switches Using 10G Fiber
- Add, Remove, or Replace a Stack Member
- Switch Stack Configuration Files
- Preconfigure a Switch
- Renumber Stack Members
- Move the Stack Master to a Different Unit

Note: Switch stacking is available on the M5300 series switches only.

Switch Stack Management and Connectivity

You manage the switch stack through the stack master. You cannot manage stack members on an individual basis. To access the stack master, use either a serial connection to the switch master's console port or a Telnet connection to the IP address of the stack.

You can use these methods to manage switch stacks:

- Web management interface.
- CLI (over a serial connection).
- A network management application through SNMP.

Stack Master and Stack Members

A switch stack is a set of up to eight switches that are connected through their stack ports. The switch that controls the operation of the stack is the stack master. The stack master and the other switches in the stack are stack members. Stack members use stacking technology to behave and work together as a unified system. Layer 2 and Layer 3 protocols present the entire switch stack as a single entity to the network.

The following figure shows an example of switches that are interconnected to form a stack.



Figure 48. Stacked switches

Stack Master

The stack master is the single point of stack-wide management. From the stack master, you can configure:

- System-level (global) features that apply to all stack members
- Interface-level features for all interfaces on any stack member

A switch stack is identified in the network by its network IP address. The network IP address is assigned according to the MAC address of the stack master. Every stack member is uniquely identified by its own stack member number.

The stack master contains the saved and running configuration files for the switch stack. The configuration files include the system-level settings for the switch stack and the interface-level settings for all stack members. Each stack member retains a copy of the saved file for backup purposes. If the master is removed from the stack, another member is elected master, and then runs from that saved configuration.

All stack members are eligible stack masters. If the stack master becomes unavailable, the remaining stack members participate in electing a new stack master. A set of factors determine which switch is elected the stack master. The stack master is elected or re-elected based on one of these factors and in the order listed:

- 1. The switch that is currently the stack master
- 2. The switch with the highest stack member priority value

Note: NETGEAR recommends assigning the highest priority value to the switch that you prefer to be the stack master. This ensures that the switch is re-elected as stack master if a re-election occurs.

3. The switch with the higher MAC address

A stack master retains its role unless one of these events occurs:

- The stack master is removed from the switch stack.
- The stack master is reset or powered off.
- The stack master fails.
- The switch stack membership is increased by adding powered-on standalone switches or switch stacks.

In the case of a master re-election, the new stack master becomes available after a few seconds. In the meantime, the switch stack uses the forwarding tables in memory to minimize network disruption. The physical interfaces on the other available stack members are not affected while a new stack master is elected. If a new stack master is elected and the previous stack master becomes available, the previous stack master does not resume its role as stack master.

Stack Members

A switch stack can include up to eight stack members connected through their stack ports. A switch stack always includes one stack master.

A standalone switch is a switch stack with one stack member that also operates as the stack master. You can connect one standalone switch to another to create a switch stack containing two stack members, with one of them being the stack master. You can connect standalone switches to an existing switch stack to increase the stack membership.

The operation of the switch stack continues uninterrupted during membership changes unless you remove the stack master or you add powered-on standalone switches or switch stacks.

Stack Member Numbers

A stack member number (1 to 8) identifies each member in the switch stack. The member number also determines the interface-level configuration that a stack member uses. You can display the stack member number by issuing the **show switch user** EXEC command.

A new, out-of-the-box switch (one that did not join a switch stack or was not manually assigned a stack member number) ships with a default stack member number of 1. When the switch joins a switch stack, the default stack member number of the switch changes to the lowest available member number in the stack.

Stack members in the same switch stack cannot be assigned the same stack member number. Every stack member, including a standalone switch, retains its member number until you manually change the number or unless the number is already being used by another member in the stack. Fore more information, see *Renumber Stack Members* on page 494.

Stack Member Priority Values

You can change a stack member priority. This is useful if you want to change the master of the stack. To change the stack member priority, issue the **switch unit priority value** command in the global config mode.

Install and Power-up a Stack

Many switch models include a *Hardware Installation Guide* with information about rack mounting and stack cabling.

Compatible Switch Models

NETGEAR stackable managed switches include the following models:

- M5300-28G
- M5300-52G

- M5300-28G3
- M5300-52G3
- M5300-28GF3
- M5300-28G-POE+
- M5300-52G-POE+

Install a Switch Stack

> To install a switch stack:

- **1.** Install the switches in a rack.
- 2. Install all stacking cables, including the redundant stack link.

NETGEAR highly recommends that you install a redundant link between the switches.

- 3. Identify the switch to be the master and power it up.
- 4. Monitor the console port.

Allow the master switch to come up to the login prompt. If the switch has the default configuration, it should come up as unit #1, and automatically become a master switch. If not, renumber the units.

5. If you want to configure switches offline, preconfigure the other switches to be added to the stack.

For more information, see *Preconfigure a Switch* on page 492.

6. Power on a second switch, making sure it is adjacent (that is, the next physical switch in the stack) to the switch already powered up.

This ensures that the second switch comes up as a member of the stack, and not a master of a separate stack.

7. Monitor the master switch to make sure that the second switch joins the stack.

You can issue the **show switch** command to determine when the switch joins the stack. It will be assigned a unit number (unit #2, if it has the default configuration).

8. As an option, renumber this stack member.

For more information, see *Renumber Stack Members* on page 494.

9. To add more members to the stack, repeat steps Step 6 through Step 8.

Always power on a switch adjacent to the switches already in the stack.

Switch Firmware and Firmware Mismatch

All stack members must run the same firmware version to ensure full compatibility in the stack protocol version among the stack members.

If a stack member is running a different firmware version than the stack master, that stack member is not allowed to join the stack. To list the stack members and firmware versions, issue the **show switch** command.

If a switch is added to a stack and it does not run the same firmware version as the master, the following occurs:

- The new unit boots up and becomes a member of the stack.
- Ports on the added unit remain in the detached state.
- A message displays on the CLI indicating a code (firmware) mismatch with the newly added unit.

To enable the newly added unit to merge normally with the stack, issue the copy xmodem | ymodem | zmodem | tftp://ip/filepath/filename command. This command copies the firmware image from a stack member to the one with incompatible firmware. That switch automatically reloads and joins the stack as a fully functioning member.

Upgrade the Firmware

All stack members must run the same firmware version. Ports on stack members that do not match the master switch firmware version do not come up. In that situation, the output of the **show switch** command shows a code (firmware) mismatch error.

Note: NETGEAR recommends that you schedule the firmware upgrade when there is no excessive network traffic (such as a broadcast event).

- > To download new firmware to the master switch and other switches in the stack:
 - 1. Using TFTP or xmodem, issue the copy command on the master switch.

After the firmware is successfully loaded onto the master switch, the firmware automatically propagates to the other units in the stack.



CAUTION:

To avoid errors during firmware propagation, do not move stack cables or reconfigure units.

- 2. If an error occurs during firmware propagation, do the following:
 - **a.** Check to make sure the master switch is running the correct firmware.

- **b.** Attempt again to copy the firmware to the units that did not get updated by issuing the copy command in stack configuration mode.
- 3. After the firmware is loaded to all members of the stack, reset all the switches

The new firmware takes effect.

Migrate Configuration with a Firmware Upgrade

In some cases, a configuration might not be carried forward in a firmware update.

- If a configuration is not carried forward in a firmware update, to download new firmware to the master switch and other switches in the stack:
 - 1. Save the current configuration by uploading it from the stack, using the copy command from the CLI.
 - 2. Load new firmware onto the stack manager.
 - 3. Reboot the stack.
 - 4. Upon reboot, enter the boot menu and erase the configuration (that is, restore is to factory default settings).
 - 5. Continue with the boot of the operational firmware.
 - 6. After the stack is up, download the saved configuration to the master.

This saved configuration is automatically propagated to all members of the stack.

Web Interface: Copy Master Firmware to a Stack Member

1. Select Maintenance > File Management > Copy.

A screen similar to the following displays.



- 2. In the Stack Member menu, select 2.
- **3.** Click **Apply**.

Stack Switches Using Ethernet Ports and a Stack Cable

This example shows how to stack two switches at close range.



Figure 49. Using a stack cable to connect switches through their Ethernet ports

> To set up a stack between two switches:

- 1. Insert AX742 modules into both switches.
- 2. Connect the AX 742 modules with a stack cable.
- 3. Configure the Switch A and Switch B as described in one of the following sections:
 - CLI: Configure the Stack Ports as Ethernet Ports on page 482
 - Web Interface: Copy Master Firmware to a Stack Member on page 481

CLI: Configure the Stack Ports as Ethernet Ports

1. On Switch A, configure the stack port and reboot the switch.

(Netgear Switch) #show stack-port										
	C	onfigured	Running		Link					
		Stack	Stack	Link	Speed					
Unit Intf SlotId T	Type XFP Adapter	Mode	Mode	Status	(Gb/s)					
2 0/27	None	Stack	Stack	Link Down	0					
2 0/28	AX742 (stack)	Stack	Stack	Link Down	12					
(Netgear Switch) #c	config									
(Netgear Switch) (C	Config)#stack									
(Netgear Switch) (C	Config-stack)#stack-p	ort 2/0/28	ethernet							
(Netgear Switch) (C	Config-stack)#exit									
(Netgear Switch) (C	Config)#exit									
(Netgear Switch) #r	reload									
Are you sure you wa	ant to reload the sta	ck? (y/n)	У							

2. After Switch A reboots, check the stack port configuration.

(Netge	(Netgear Switch) #show port 2/0/28											
		Admin	Physical	Physical	Link	Link	LACP	Actor				
Intf	Туре	Mode	Mode	Status	Status	Trap	Mode	Timeout				
2/0/28		Enable	10G Full	10G Full	Up	Enable	Enable	long				

3. On Switch B, configure the stack port and reboot the switch.

(Netgear Switch)	#				
(Netgear Switch)	#show stack-port				
		Configured	Running		Link
		Stack	Stack	Link	Speed
Unit Intf SlotId	d Type XFP Adapter	Mode	Mode	Status	(Gb/s)
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 1/0/5	1 ethernet		
(Netgear Switch)	(Config-stack)#exit				
(Netgear Switch)	(Config)#exit				
(Netgear Switch)	#reload				
Are you sure you	want to reload the s	stack? (y/n)	У		

4. After Switch B reboots, check the stack port configuration.

(Netgea	(Netgear Switch) #show port 2/0/28											
		Admin	Physical	Physical	Link	Link	LACP	Actor				
Intf	Туре	Mode	Mode	Status	Status	Trap	Mode	Timeout				
1/0/51	Enable	10G Ful	l 10G Full	Up	Enable	Enable	long					

Web Interface: Configure the Stack Ports as Ethernet Ports

- 1. On Switch A, configure a stack port as an Ethernet port.
 - a. Select System > Stacking > Advanced > Stack Port Configuration.

A screen similar to the following displays.

System Swit	tching		Routing		QoS	Security	Monitoring	Maintenance	Help	ndex		
Management Device	View	Licen	ise Se	rvices		king PoE S	INMP LLDP ISDP	Timer Schedule				
												Update Cancel Apply
Stacking		Stack-	ort Confi	iguratio	n							Ø
Basic	~	12	All									
Advanced	^		Unit ID	Port	Type	Product name	Configured Stack Mode	Running Stack Mode	Link Status	Link Speed (Gbps)	Transmit Data Rate (Mbps)	Transmit Error Rate (Errors/s)
Stack Configuration			2	0/28			Ethernet ~	Stack	Up	12	0	0
Stack Status			2	0/25			Ethernet	Ethernet	Down	10	0	0
- Stack-port Configural	tion		2	0/26			Ethernet	Ethernet	Down	10	0	0
Stack-port Diagnostic	ne.		2	0/27			Stack	Stack	Down	12	0	0
oner por bingroom	100	8	2	0/28			Stack	Stack	Up	12	0	0
Stack Firmware Synchronization												
•NSF	2	12	All									
0.000												

- b. Scroll down and select the 2/0/28 check box.
- c. In the Configured Stack Mode menu, select Ethernet.
- d. Click Apply to save the settings.
- 2. Reboot the switch.
 - a. Select Maintenance > Reset > Device Reboot.

A screen similar to the following displays.

System Switching	Routing Q	S Security	Monitoring	Maintenance	Help	Index	
Save Config Reset Up	load Download File Ma	nagement Troubleshi	oting				
							Cancel Apply
Reset	Device Reboot						e
Device Reboot	Reboot Unit No.	2 ~					
Factory Default	Save prior to reboot						
Password Reset	Don't save prior to	reboot					
-							

- b. In the Reboot Unit No. menu, select 2.
- c. Click Apply.
- 3. On Switch B, configure a stack port as an Ethernet port.
 - a. Select System > Stacking > Advanced > Stack Port Configuration.

A screen similar to the following displays.

System	Switching		Routing		QoS	Security	Monitoring	Maintenance	Help	ndex		
Management	Device View	Licer	ise Se	rvices		king PoE s	SNMP LLDP ISDP	Timer Schedule				
												Update Cancel Apply
Stack	king	Stack-	port Conf	iguratio	n							C
Basic	~	12	All									
Advanced	^		Unit ID	Port	Type	Product name	Configured Stack Mode	Running Stack Mode	Link Status	Link Speed (Gbps)	Transmit Data Rate (Mbps)	Transmit Error Rate (Errors/s)
Stack Config	guration		1	0/51			Ethernet 👻	Stack	Down	12	0	0
Stack Status	s		1	0/49			Ethernet	Ethernet	Down	10	0	0
- Stack-port C	Configuration		1	0/50			Ethernet	Ethernet	Down	10	0	0
• Stack-port D	liagnostics		1	0/51			Stack	Stack	Down	12	0	0
Stack Firmw Synchronizat	vare		1	0/52			Stack	Stack	Up	12	0	0
•NSF	~	12	All									
	48											

- **b.** Scroll down and select the **1/0/51** check box.
- c. In the Configured Stack Mode menu, 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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index	
Save Config	Reset Up	load Download	File Manageme	int Troublesh	ooting				
									Cancel Apply
Re	iset	Device Reboot							Ø
Device Rebo	ot	Reboot Unit N	la.	1 -					
Factory Defa	ult	 Save prior 	to reboot						
Password Re	eset	Oon't save	prior to reboot						

- b. In the Reboot Unit No. menu, select 1.
- c. Click Apply.

The switch reboots.

Stack Switches Using 10G Fiber

This example shows how to stack two switches in different buildings at long distance using 10G fiber.



Figure 50. Using 10G fiber to stack switches in different buildings

- > To set up a stack between two switches in different buildings at long distance:
 - 1. Insert AX741 modules into both switches.
 - 2. Connect the AX741 modules with a fiber cable.
 - 3. Configure the Switch A and Switch B as described in one of the following sections:
 - CLI: Stack Switches Using 10G Fiber on page 486
 - Web Interface: Stack Switches Using 10G Fiber on page 488

CLI: Stack Switches Using 10G Fiber

1. On Switch A, display the stack port information.

(Netg	(Netgear Switch) #show stack-port												
	Configured Running Link												
					Stack	Stack	Link	Speed					
Unit	Intf	SlotId	Туре	XFP Adapter	Mode	Mode	Status	(Gb/s)					
1	0/51			None	Ethernet	Ethernet	Link Down	12					
1	0/52			AX741	Stack	Stack	Link Down	0					

Because port 1/0/52 is already configured as a stack port, no action is required.

2. On Switch B, display the stack port information.

(Neto	(Netgear Switch) #show stack-port												
	Configured Running Link												
					Stack	Stack	Link	Speed					
Unit	Intf	SlotId	Туре	XFP Adapter	Mode	Mode	Status	(Gb/s)					
2	0/27			None	Stack	Stack	Link Dow	n 0					
2	0/28			AX741	Ethernet	Ethernet	Link Dow	n 12					

3. Because port 2/0/28 functions in Ethernet mode, change it 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.
```

5. On Switch A, display the switch information.

(Ne	tgear Switch) #show swi	tch			
	Management	Standby	Preconfig	Plugged-in	Switch	Code
SW	Switch	Status	Model ID	Model ID	Status	Version
1	Mgmt Sw		M5300-28G3	M5300-28G3	OK	11.0.0.3
2	Stack Mbr	Oper Stby	M5300-28G3	M5300-28G3	OK	11.0.0.3

Web Interface: Stack Switches Using 10G Fiber

- 1. On Switch A, display the stack port information.
 - a. Select System > Stacking > Advanced > Stack Port Configuration.

A screen similar to the following displays.

System Switch	hing		Routing		QoS	Security	Monitoring	Maintenance	Help	Index		
Management Device V	fiew.:	Licer	ise Se	rvices		ing PoE S	NMP LLDP ISDP	Timer Schedule				
												Update Cancel Apply
Stacking		Stack-	ort Confi	iguratio	n							0
Basic	~	12	All									
Advanced	•		Unit ID	Port	Type	Product name	Configured Stack Mode	Running Stack Mode	Link Status	Link Speed (Gbps)	Transmit Data Rate (Mbps)	Transmit Error Rate (Errors/s)
Stack Configuration							*					
Stack Status			1	0/49			Ethernet	Ethernet	Down	10	0	0
Stack-port Configuration	1		1	0/50			Ethernet	Ethernet	Down	10	0	0
Stack-port Diagnostics			1	0/51			Ethernet	Stack	Down	12	0	0
Stack Firmware Synchronization			1	0/52			Stack	Stack	Up	12	0	0
•NSF	4	12	All									
	~~											

Because port 1/0/52 is already configured as a stack port, no action is required.

- 2. On Switch B, configure port 2/0/28 as a stack port.
 - a. Select System > Stacking > Advanced > Stack Port Configuration.

A screen similar to the following displays.

System Sw	itching		Routing		QoS	Security	Mor	nitoring	Maintenance	Help	Index		
Management Device	e View	Licen	ise Se	rvices		king PoE S	INMP LL	DP ISDP	Timer Schedule				
													Update Cancel Apply
Stacking		Stack-p	ort Confi	iguratio	n								d
Basic		12	All										
Advanced	~		Unit ID	Port	Туре	Product name	Configured	i Stack Mode	Running Stack Mode	Link Status	Link Speed (Gbps)	Transmit Data Rate (Mbps)	Transmit Error Rate (Errors/s)
Stack Configuration			2	0/28			Stack	*	Stack	Up	12	0	0
Stack Status			2	0/25			Ethernet		Ethernet	Down	10	0	0
Stack-port Configura	ation	۲	2	0/26			Ethernet		Ethemet	Down	10	0	0
Stack-port Diagnost	ies	0	2	0/27			Stack		Stack	Down	12	0	0
Stack Firmware Synchronization			2	0/28			Ethernet		Stack	Up	12	0	0
•NSF	¥	12	PAIL										

- b. Scroll down and select the 2/0/28 check box.
- c. In the Configured Stack Mode menu, select Stack.
- d. Click Apply to save the settings.
- **3.** Reboot the switch.
 - a. Select Maintenance > Reset > Device Reboot.

A screen similar to the following displays.

System Swite	hing Routing QoS	Security Monitoring	Maintenance	Help Index	
Save Config Reset	Upload Download File Managem	ent Troubleshooting			
					Cancel Apply
Reset	Device Reboot				e
Device Reboot	Reboot Unit No.	2 -			
Factory Default	Save prior to reboot				
Password Reset	On't save prior to reboot				

- b. In the Reboot Unit No. menu, select 2.
- c. Click Apply.

The switch reboots.

Add, Remove, or Replace a Stack Member

You can manage an operating stack.

Add Switches to an Operating Stack

> To add new switches to an operating stack:

- Make sure that the redundant stack connection is functional. All stack members must be connected in a logical ring.
- 2. Preconfigure any new switches.
- 3. Power off all new switches that must join the stack.



CAUTION:

If you cable one or more powered-on switches to the stack, the existing stack and the new switches assume that two stacks are merging. They elect a single, new stack master, and you cannot specify which switch becomes the new master. All stack members assume the configuration that is based on the new stack master. Stack members change their stack member numbers to the lowest available numbers.

4. Install the new switches in the rack.

This procedure assumes installation below the bottom-most switch, or above the top-most switch.

5. Disconnect the redundant stack cable that connects the last switch in the stack to the first switch in the stack at the position in the ring where you intend to insert the new switch.

Note: If you want to merge an operational stack into the this stack, add the switches as a group by unplugging one stacking cable in the operational stack and physically connecting all unpowered units at that point.

- 6. Connect this cable to the new switch, following the established order of stack-up to stack-down connections.
- 7. Power up the new switches one by one.
- 8. Verify, by monitoring the master switch console port, that the new switch joins the stack by issuing the **show** switch command. The new switch joins as a member (never as master; the existing master of the stack must not change).
- **9.** If the firmware version of the newly added member is not the same as the existing stack, update the firmware (see *Upgrade the Firmware* on page 480.).

Remove a Switch from a Stack

> To remove a switch from a stack:

1. Make sure that the redundant stack connection is functional.

All stack members must be connected in a logical ring.

2. Power down the switch that you want to remove.



CAUTION:

If the switch stack is not cabled correctly, removing powered-on stack members might cause the switch stack to divide (that is, partition) into two or more switch stacks, each with the same configuration. Make sure that the switch stack is cabled correctly.

- 3. Disconnect the stack cables.
- 4. If you do not intend to replace the switch, reconnect the stack cable from the stack member above to the stack member below the switch that you intend to remove.
- 5. Remove the switch from the rack.
- 6. To remove the switch not only from the stack but also from the stack configuration, issue the **no member** *unit-id* command.
 - **Note:** If the switch stack divides, and you want the switch stacks to remain separate, change the IP address or addresses of the newly created switch stacks.

- 7. If the switch stack divides but you do not intend to partition the switch stack, do the following:
 - **a.** Power off the newly created switch stacks.
 - **b.** Reconnect them to the original switch stack through their stack ports.
 - c. Power on the switches.

Replace a Stack Member

> To replace a stack member:

1. Make sure that the redundant stack connection is functional.

All stack members must be connected in a logical ring.

- 2. Power down the switch that you intend to remove and disconnect its stack cables.
- 3. Remove the switch from the rack.
- 4. If you intend to install a different model switch, remove the unit from the configuration by issue the no member unit-id command.
- 5. Install the new switch in the rack:
 - If you are installing the same model switch, place the switch in the same position in the stack as the switch that you just removed.
 - If you are installing a different model switch, either place the switch in the same position as the previous switch, or at the bottom of the stack.
- 6. Cable the new switch, following the established order of stacking cables.
- 7. Power up the new switch.

Verify, by monitoring the master switch console port, that the new switch successfully joins the stack by issuing the **show** switch command. The new switch must join as a member (not as master; the existing master of the stack must not change).

8. If the firmware version of the newly added member is not the same as the existing stack, update the firmware (see *Upgrade the Firmware* on page 480).

Switch Stack Configuration Files

The configuration files include all global and interface-specific settings that define the operation of the stack and its individual members. If you issue the **save config** command, all stack members store a copy of the configuration settings. If a stack master becomes unavailable, the stack member that assumes the role of stack master operates from the saved configuration files.

When a new, out-of-box switch joins a switch stack, the switch uses the system-level settings of that switch stack. However, if you want the store to store this system level configuration, you must issue the **save config** command.

You can back up and restore the stack configuration by using the **copy** command in the same way as you back up and restore a standalone switch configuration.

The following table provides switch stack configuration scenarios. Most of the scenarios assume that at least two switches are connected through their stack ports.

Table 4. Switch stack master scenarios	Table 4.	Switch	stack	master	scenarios
--	----------	--------	-------	--------	-----------

Scenario	Action	Result
Stack master election specifically determined by existing stack masters.	Connect two powered-on switch stacks through the stack ports.	Only one of the stack masters becomes the new stack master. No other stack members become the stack master.
recommend this scenario.		
Stack master election specifically determined by the stack member priority value.	 Connect two switches through their stack ports. To set a stack member to a higher member priority value, issue the switch stack-member-number priority new-priority-number global configuration command. Restart both stack members at the same time. 	The stack member with the higher-priority value is elected stack master.
Stack master election specifically determined by the MAC address.	Assuming that both stack members have the same priority value and firmware image, restart both stack members at the same time.	The stack member with the higher MAC address is elected stack master.
Add a stack member.	 Power off the new switch Through their stack ports, connect the new switch to a powered-on switch stack. Power on the new switch. 	The stack master is retained. The new switch is added to the switch stack.
Stack master failure.	Remove (or power off) the stack master.	One of the remaining stack members becomes the new stack master. All other members in the stack remain stack members and do not reboot.

Preconfigure a Switch

You can preconfigure (that is, supply a configuration to) a new switch before it joins the switch stack. You can specify the stack member number, the switch type, and the interfaces that are associated with a switch that is not currently part of the stack.

Note: If you are replacing a switch with the same model in the same position in the stack, you do not need to preconfigure it. The new switch assumes the same configuration as the previous switch.

> To preconfigure a switch:

- 1. Issue the member unit-id switchindex command.
- 2. To view the supported unit types, use the show supported switchtype command.
- 3. Configure the unit that you defined in *Step 1*, just as if the unit were physically present.

Ports for the preconfigured unit come up in a detached state.

4. To see the ports, use the **show port all** command.

Now you can configure the detached ports for VLAN membership and any other port-specific configuration.

After you preconfigure a unit type for a specific unit number, attaching a unit with a different unit type for this unit number causes the switch to report an error. In this situation, the output of the **show switch** command indicates a configuration mismatch for the new unit and the ports on that unit do not come up. To resolve this situation, you can change the unit number of the mismatched unit or delete the preconfigured unit type by issuing the **no member** unit-id command.

When you add a preconfigured switch to the switch stack, the stack applies either the preconfigured configuration or the default configuration. The following table lists the events that can occur when the switch stack compares the preconfigured configuration with the new switch.

Switch Type Is the Same	Stack Member Number	Result
Yes	Is the same	The switch stack applies the configuration to the preconfigured new switch and adds it to the stack.
Yes	Does not match	 The switch stack applies its default stack member number to the preconfigured switch and adds it to the stack. The stack member number configuration in the preconfigured switch changes to reflect the new information.
	Is not found in the stack configuration	 The switch stack applies the default configuration to the new switch and adds it to the stack. The preconfigured information is changed to reflect the new information.
	Is not found in the preconfigured switch	The switch stack applies the default configuration to the preconfigured switch and adds it to the stack.

Table 5.	Preconfigured	switches	compared	to stack	configuration
		•			•••·····

Renumber Stack Members

This example is provided as CLI commands and a web interface procedure.

CLI: Renumber Stack Members

- Note: When you issue a command such as move management or renumber, NETGEAR recommends that you wait until the command fully executes before issuing the next command. For example, after you issue a reset command for a stack member, issue the show port command to verify that the switch remerged with the stack and that all ports joined before you issue a next command.
- If specific numbering is required, NETGEAR recommends that you assign stack members their numbers when they are first installed and configured in the stack.
- If the stack unit number for a switch is unused, you can renumber the unit by issuing the switch <oldunit-id> renumber <newunit-id> global config mode command.
- If you preconfigured the new unit ID, you might need to remove the new unit ID from the configuration before renumbering the unit.
- If you need to reassign multiple existing stack unit numbers, the configuration could become mismatched. To avoid this situation, NETGEAR recommends that you power down all switches except the master, and then add them back one at a time (see *Add Switches to an Operating Stack* on page 489).

To renumber stack members, issue the following CLI command:

```
(Netgear Switch) (Config)#switch 3 renumber 2
All the switches in the stack will be reset to perform Manager unit renumbering and
the configuration of Manager switch interfaces will be cleared.
Are you sure you want to renumber? (y/n) y
```

Web Interface: Renumber Stack Members

- 1. Renumber the stacking member's ID from 3 to 2.
 - a. Select System > Management > Basic > Stack Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring		Private Processing Pro-Co	нер				
Management	Device View	License Servi	ces Slacking	POE SNMP	P LLDP I	ISDP	Timer Schedule					
										Add	Delete Update	Gancel A
Stacki	úng	Management Unit	Selection									
Basic	^	Management U	Init Selected:	1 -								
Stack Config	guration	-										
Advanced	*											
NSF	×	Stack Sample Mode	Cummu	latve v								
NSF	·	Stack Sample Mode Sample Mode Stack Configuratio	Cummu n	lative 👻								
NSF	×	Stack Sample Mode Sample Mode Stack Configuratio	Cummu n Change Switch ID	lative +	tch Type		Hardware Manager	nent Preference	Switch Priority	Management Status	Standby Status	Switch Statu
NSF	×	Stack Sample Mode Sample Mode Stack Configuratio	Cummu n 2hange Switch ID 2	to Swit	tch Type 300-28G3	~	Hardware Managen Unassigned	nent Preference	Switch Priority Unassigned ~	Management Status StackMember v	Standby Status Opr Standby	Switch Statut
NSF	*	Stack Sample Mode Sample Mode Stack Configuratio	Cummu n Change Switch ID 2	to Swit	tch Type 300-28G3 00-52G-POE+	*	Hardware Managen Unassigned Unassigned	nent Proference	Switch Priority Unassigned ~ Unassigned	Management Status StackMember ~ Management	Standby Status Opr Standby None	Switch Status OK OK

- **b.** Scroll down and select the **3** check box.
- c. In the Change Switch ID to field, enter 2.
- d. Click Apply to save the settings.

Now, the unit ID of the stacking member is 2.

System	Switching		Routing	QoS	Security	Monitorin	9	Maintenance	Help	Index					
Management	Device View	Licer	se Service	s Stacking	PoE SNM	P LLDP	ISDP	Timer Schedule							
													Add	Delete Update	Cancel Apply
Stack	king	Manag	ment Unit Se	ection											
Basic	~	Mar	nagement Uni	t Selected:	1 *										
Stack Config	iguration														
Advanced	~														
•NSF	~	Stack S	Sample Mode	64											94
		Sar Stack (ple Mode	Cumm	ulative 👻										
			Unit ID Ch	ange Switch I	D to Sw	tch Type		Hardware Manag	ement Prefer	ence Sw	itch Priority	Manageme	ent Status	Standby Status	Switch Status
							v				÷				
			1		M5	300-52G-PO	E+	Unassigned		Un	assigned	Managem	ent	None	OK
			2		M5	300-28G3		Unassigned		Un	assigned	StackMen	nber	None	OK
			3		M5	300-28G3		Unassigned		Un	assigned	StackMen	nber	None	Not present

Move the Stack Master to a Different Unit

This example is provided as CLI commands and a Web interface procedure.

CLI: Move the Stack Master to a Different Unit

1. To mover the stack master to a different unit number, issue the movemanagement <fromunit-id> <tounit-id> command.

The operation takes between 30 seconds and 3 minutes, depending on the stack size and configuration.

- 2. Make sure that you can log in on the console that is attached to the new master.
- 3. To verify that all units rejoined the stack, issue the **show** switch command.
- 4. Reset the stack by issuing the **reload** command.

To mover the stack master to a different unit number, issue the following CLI command:

```
(Netgear Switch) (Config)#stack
(Netgear Switch) (Config-stack)#movemanagement 1 2
```

Web Interface: Move the Stack Master to a Different Unit

1. Select System > Management > Basic > Stack Configuration.

A screen similar to the following displays.

2. In the Management Unit Selected menu, select 2.

A warning window displays.

Management	Device View	License Serv	nces Stacking		ISDP Timer Schedule					
								Add	Delete Update	Cancel Appl
Stac	king	Management Unit	L Selection							
Basic	^	Management I	Unit Selected	2.1						
	guration			Confirm dialog			×			
Advanced	*			Moving stack m all interfaces. A	anagement will unconfigure re you sure you want to mo	e entire stack inclu ove stack	ding			
NSF		Stack Sample Mo	ode	management? (0	OK/Cancel)					
		Sample Mode	Cummula	ative -						
						OK Can	cel			
		Stack Configuratio	on			OK Can	cel .			
		Stack Configuratio	ion Change Switch ID t	o Switch Type	Hardware Manage	OK Can	Switch Priority	Management Status	Standby Status	
		Stack Configuratio	on Change Switch ID t	o Switch Type	Hardware Manage	OK Can	Switch Priority	Management Status	Standby Status	Switch Statum
		Stack Configuration	ion Change Switch ID t	o Switch Type M5300-526-POE	Hardware Manage Vinassigned	OK Can	Switch Priority	Management Status	Standby:Status None	Switch Status OK
		Stack Configuration	on Charge Switch ID t	Switch Type M5300-52G-POE M5300-52G-POE M5300-28G3	+ Unassigned Unassigned	OK Can	Switch Pnonty Unassigned Unassigned	Management Status	Standby Status None None	Switch Status OK OK

- 3. Click the OK button.
- 4. Click **Apply** to save the settings.

Note: If the master receives its IP address from a DHCP server and you move the master to a different unit, its IP address might change and you could lose the connection to the switch.

SNMP

Simple Network Management Protocol

25

This chapter includes the following sections:

- Add a New Community
- Enable SNMP Trap
- SNMP Version 3
- sFlow
- Time-Based Sampling of Counters with sFlow

Add a New Community

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

CLI: Add a New Community

```
(Netgear switch) #config
(Netgear switch) (Config)#snmp-server community rw public@4
```

Web Interface: Add a New Community

1. Select System > SNMP > SNMP V1/V2 > Community Configuration.

A screen similar to the following displays.

System	Switching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management	Device View	Ser	ices Chass	is PoE	SNMP LLDP	ISDP Timer Se	chedule	10 (A)	
SNM	P	Com	munity Configu	ration					
SNMP V1/V2	^		Community N	lame	Client Address	Client IP Ma	sk Access Mode	Status	
Community Configuration		f	public@4		0.0.0.0	0.0.0.0	Read-Write	✓ Enable	• •
• Trap Configur	ration		public		0.0.0.0	0.0.0.0	Read-Only	Enable	
• Trap Flags			private		0.0.0.0	0.0.0.0	Read-Write	Enable	
Supported MI	IBS								
SNMP V3	~								

- 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.

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.

System	Switching	R	outing	QoS	Secur	rity	Mon	itoring	Maintenance	Hel	p Index
Management	Device View	Service	s Chassis	s PoE	SNMP	LLDP	ISDP	Timer Scl	nedule		
SNN	MР	Trap Cor	figuration								
SNMP V1/V2	~	🗆 Ca	immunity Na	ime	Version	f	Protocol	Address	St	atus	
 Community Configuration 	n	p	Iblic		SNMP V1	~	IPv4 ×	10.100.5.1	7 E	Enable 🗸	
Trap Configu	Iration										
 Trap Flags 											
 Supported N 	IIBS										
SNMP V3	×										

- 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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index	
Management	Device View	Services Char	asis PoE	SNMP LLDP	ISDP Timer S	chedule		,	
SNM	P	Trap Flags							
SNMP V1/V2	^	Authentication		🔘 Disab	ele 💿 Ena <mark>bl</mark> e				
Community		Link Up/Down		🔘 Disat	le 💿 Enable				
Configuration		Multiple Users		🔘 Disab					
 Trap Configur 	ration	Spanning Tree		Disable Enable					
Trap Flags		ACL		Oisab	le 🔘 Enable				
 Supported MI 	IBS	Captive Portal		💿 Disab					
SNMP V3	~	DVMRP		 ● Disable ○ Enable ● Disable ○ Enable 					
		PIM							
		PoE		🔘 Disab	le 💿 Enable				
		OSPEv2 Trans							

- **b.** For Link Up/Down, select the **Enable** radio button.
- c. Click Apply.

SNMP Version 3

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

CLI: Configure SNMPv3

```
(Netgear Switch) #config
(Netgear Switch) (Config)#users passwd admin
Enter old password:
Enter new password:12345678
Confirm new password:12345678
Password Changed!
change the password to "12345678"
(Netgear Switch) (Config)#users snmpv3 authentication admin md5
Set the authentication mode to md5
(Netgear Switch) (Config)#users snmpv3 encryption admin des 12345678
Set the encryption mode to des and the key is "12345678"
```

Web Interface: Configure SNMPv3

1. Change the user password.

If you set the authentication mode to MD5, you must make the length of password longer than 8 characters.

a. Select Security > Management Security > User Configuration > User Management.

A screen similar to the following displays.

System	Switching		Routing	QoS	Security	Monitoring	Maintenance	Help	o Index
Management Se	eurity Acce	ess	Port Authenti	cation Traffic C	ontrol Cont	rol ACL			
Management	Security	Mana	ige Users						
• Local User	~			and the second		Confirm	Access	Lockout	Daceword
• User Manager	nent		User Name	Edit Password	Password	Password	Mode	Status	Expiration Date
•User Passwor	d		admin	Disable 👻			READ_WRITE Y	FALSE	
Configuration			admin	Disable	******	******	READ_WRITE	FALSE	
 Enable Passwor 	ď		guest	Disable	******	******	READ_ONLY	FALSE	
Line Password									
• RADIUS	~								
• TACACS	*								
 Authentication L 	ist 🗸 🗸								
Login Sessions									

- **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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management	Device View	Services Chass	sis PoE	SNMP LLDP	ISDP Timer S	chedule		
SNM	1P	User Names						
• SNMP V1/V2	~	User Name	admin	*				
 SNMP V3 	^							
User Configu	iration	User Configuration						
		SNMP V3 Access Authentication Pro Encryption Protoc Encryption Key	s Mode otocol col	Read/Write None None E	▼ MD5 © SHA DES 8 to 64 l	hexadecimal character	rs	

- 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 51. 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	Owner	Time out	Max Datagram	Port	IP Address		
Index	String		Size				
1	NetMonit	31535988	1400	6343	192.168.10.2		
2		0	1400	6343	0.0.0		
3		0	1400	6343	0.0.0		
4		0	1400	6343	0.0.0		
5		0	1400	6343	0.0.0		
6		0	1400	6343	0.0.0		
7		0	1400	6343	0.0.0		
8		0	1400	6343	0.0.0		
(GSM7328	s) #						

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)# i	Interface	e 1/0/1	L		
(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	Receiver	Packet	Max Header
Data Source	Index	Sampling Rate	Size
1/0/1	1	1024	64

Web Interface: Configure Statistical Packet-based Sampling with sFlow

- 1. Configure the sFlow receiver IP address.
 - a. Select Monitoring > sFlow > Advanced > sFlow Receiver Configuration.
 - **b.** Select the **1** check box.
 - c. In the Receiver Owner field, enter NetMonitor.
 - d. In the Receiver Timeout field, enter 31536000.
 - e. In the Receiver Address field, enter 192.168.10.2.

A screen similar to the following displays.

System Switch	mg		Routing	QoS	Security Monit	toring Mainte	mance Help	Index		
Ports Logs Mirroring	sP	low								
sFlow		sFlov	v Receiver (Configuration						
•Basic •Advanced	~		Receiver Index	Receiver Owner	Receiver Timeout	No Timeout	Maximum Datagram Size	Receiver Address	Receiver Port	Datagram Version
• sFlow Agent Information	8		1	netMonitor	31536000	False +	1400	192.168 10.2	6343	5
sFlow Receiver		3 1			0	False	1400	0.0.0.0	6343	5
Configuration			2		0	False	1400	0.0.0.0	6343	5
sFlow Interface Configuration		8	3		0	False	1400	0.0.0	6343	5
		100	4		0	Faire	1400	0000	6343	

f. Click Apply.

A screen similar to the following displays.

System	Switching	9	Routing	QoS	Security	Monitoring Mainte	enance Help	Index		
Ports Logs	Mirroring	sHo								
sFlo	w	sFl	ow Receiver	Configuration						
•Basic •Advanced			Receiver Index	Receiver Owner	Receiver Timeout	No Timeout	Maximum Datagram Size	Receiver Address	Receiver Port	Datagram Version
•sFlow Agent	Information		1	netMonitor	31536000	False +	1400	192.168.10.2	6343	5
• sFlow Recen	er	1	6 1		0	False	1400	0.0.0.0	6343	5
Configuration		1	2		0	False	1400	0.0.0.0	6343	5
. sFlow Interfa	ce.	1	1 3		0	False	1400	0.0.0	6343	5
Configuration	6	1.12	11 A			Ealers	4488		12.12	

- 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.

System	Switching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Ports Logs Mi	rroring s	Flow			14				
sFlow		sFlov	v Interface (Configuration					
Basic	ic 🔺 123 All						Go To	Interface Go	
 Advanced 	~		-		Poller			Sample	(
 sFlow Agent Infor 	mation		Interface	Receiver Index	Poller Inter	val R	eceiver Index	Sampling Rate	Maximum Header Size
 sFlow Receiver Configuration 			1/0/1	0	0	1		1024	64
• sElow Interface	-		1/0/1	0	0	0		0	128
Configuration			1/0/2	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.

System	Switching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index	
Ports Logs	Mirroring a									3
sFlo	w	sFlov	v Interface	Configuration						
• Basic	12	3 All					Go T	To Interface	Go	
 Advanced 	^		Poller				Sampler			
 sFlow Agent 	Information		Interface	Receiver Index	Poller Ir	nterval R	eceiver Index	Sampling Ra	ite N	laximum Header Size
 sFlow Receir Configuration 	ver 1									
 sFlow Interfa 	ce		1/0/1	0	0	1		1024	6	4
Configuration			1/0/2	0	0	0		0	1	28

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

Configure the sampling ports sFlow receiver index, and polling interval:

- 1. Select Monitoring > sFlow > Advanced > sFlow Interface Configuration.
- 2. Select the Interface 1/0/1 check box.
- 3. In the Poller Interval field, enter 300.

A screen similar to the following displays.

System	Switching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index	
Ports Logs N	Airroring s									
sFlow		sFlov	v Interface	Configuration						
•Basic	~	12	3 All					Go 1	o Interface	Go
Advanced	^	0			Poller			Samp	ler	
 sFlow Agent Infe 	ormation		Interface	Receiver Index	Poller I	nterval F	Receiver Index	Sampling Ra	te I	Maximum Header Size
 sFlow Receiver Configuration 										
 sFlow Interface 	8		1/0/1	1	300			1024		54
Configuration			1/0/2	0	0	0)	0		128

4. Click Apply.

DNS

26

Domain Name System

This chapter includes the following sections:

- Domain Name System Concepts
- Specify Two DNS Servers
- Manually Add a Host Name and an IP Address

Domain Name System Concepts

The Domain Name System (DNS) protocol maps a host name to an IP address, allowing you to replace the IP address with the host name for IP commands such as a ping and a traceroute, and for features such as RADIUS, DHCP relay, SNTP, SNMP, TFTP, SYSLOG, and UDP relay.

You can obtain the DNS server IP address from your ISP or public DNS server list. DNS is used to resolve the host's IP address. It enables a static host name entry to be used to resolve the IP address. The following are examples of how the DNS feature is used.

Specify Two DNS Servers

The following example shows how to specify two DNS servers (that is, two IP addresses for DNS servers) and to resolve an IP address using the DNS server. The example is shown as CLI commands and as a web interface procedure.

CLI: Specify Two DNS Servers

```
(Netgear Switch)#config
(Netgear Switch) (Config)#ip name-server 12.7.210.170 219.141.140.10
(Netgear Switch) (Config)#ip domain-lookup
(Netgear Switch) (Config)#exit
(Netgear Switch)#ping www.netgear.com
Send count=3, Receive count=3 from 206.82.202.46
```

Web Interface: Specify Two DNS Servers

1. Select System > Management > DNS > DNS Configuration.

System	Switching	Ro	uting	QoS	Sec	urity	Mon	itoring	Maintenance	Help	Index
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer S	chedule		
Manage	ement	DNS Cont	iguration								
 System Inform 	ation	DNS Sta	itus		0	Disable 🖲	Enable				
• System CPU S	Status 🗸	DNS De	ault Name					(1 to 2	55 alphanumeric chara	cters)	
 Switch Statisti 	cs	Retry Nu	mber		2			(0 to 10	00)		
 USB Device In 	formation	Respons	e Timeout (secs)	3			(0 to 30	500 secs)		
 Loopback Inter 	face										
 Network Interfa 	ice 🗸										
• Time	~	DNS Serv	er Configura	tion							
- DNS	~	Ser	ial No DN	S Server		Prefere	nce				
DNS Configu	iration										
• Host Configu	iration	■ 1	219	.141.140.	10	1					
 SDM Template 	Preference	2	12.	7.210.170		0					
Green Etherne	t v										

- 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.

System	stem Switching		iting	QoS	Sec	urity	Moni	itoring	Maintenance	Help	Index
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer S	chedule		
Manage	ement	DNS Host	Configurati	on							
 System Inform 	ation	Host	Name (1 t	o 255 chai	racters)	IP Addre	ISS				
 System CPU S 	Status 🗸 🗸			-							
 Switch Statisti 	cs	i www	netgear.co	om		206 92 2	02.46				
USB Device Int	formation		gearer								
 Loopback Inter 	face										
Network Interfa	ice v	Dynamic H	lost Mappir	ng							
• Time	~	Host	Total El	apsed	Type	Addresse	s				
• DNS	~	3. A.									
DNS Configu	iration										
- Heat Configu	10000										

- 2. Under DNS Host Configuration, enter the following information:
 - In the Host Name field, enter www.netgear.com.
 - In the IP Address field, enter 206.82.202.46.
- 3. Click Add.

The host name and IP address now show in the DNS Host Configuration table.

DHCP Server



Dynamic Host Configuration Protocol Server

This chapter includes the following sections:

- Dynamic Host Configuration Protocol Concepts
- Configure a DHCP Server in Dynamic Mode
- Configure a DHCP Server that Assigns a Fixed IP Address

Note: The DHCP server is available on M5300 and M6100 series switches only. However, the following M5300 series switches require a license to support the DHCP server: M5300-28G, M5300-52G, M5300-28G-POE+, and M5300-52G-POE+.

Dynamic Host Configuration Protocol Concepts

When a client sends a request to a Dynamic Host Configuration Protocol (DHCP) server, the DHCP server assigns the IP address from address pools that are specified on the switch. The network in the DHCP pool must belong to the same subnet.

A DHCP server allows the switch to dynamically assign an IP address to a DHCP client that is attached to the switch. It also enables the IP address to be assigned based on the client's MAC address. The following are examples of how the DHCP Server feature is used.

Configure a DHCP Server in Dynamic Mode

The following example shows how to create a DHCP server with a dynamic pool. The example is shown as CLI commands and as a web interface procedure.

CLI: Configure a DHCP Server in Dynamic Mode

(Netgear	Switch)	#vlan database
(Netgear	Switch)	(Vlan)#vlan 200
(Netgear	Switch)	(Vlan)#vlan routing 200
(Netgear	Switch)	(Vlan)#exit
(Netgear	Switch)	(Config)#interface 1/0/1
(Netgear	Switch)	(Interface 1/0/1)#vlan participation include 200
(Netgear	Switch)	(Interface 1/0/1)#vlan pvid 200
(Netgear	Switch)	(Interface 1/0/1)#exit
(Netgear	Switch)	(Config)#interface vlan 200
(Netgear	Switch)	(Interface-vlan 200)#routing
(Netgear	Switch)	(Interface-vlan 200)#ip address 192.168.100.1 255.255.255.0
(Netgear	Switch)	#config
(Netgear	Switch)	(Config)#service dhcp
(Netgear	Switch)	(Config)#ip dhcp pool pool_dynamic
(Netgear	Switch)	(Config)#network 192.168.100.0 255.255.255.0

Note: If there is no DHCP L3 relay between client PC and DHCP server, there must be an active route whose subnet is the same as the DHCP dynamic pool's subnet.

Web Interface: Configure a DHCP Server in Dynamic Mode

- 1. Create VLAN 200.
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

A screen similar to the following displays.

System	Sw	<i>i</i> tching		Routing	QoS	Security	Moni	oring	Maintenance	Help	Index
VLAN Auto	VolP	iSCSI	STP	Multicast	MVR	Address Table	Ports LA	AG MI	LAG		ан са С
VL	AN		Reset								
•Basic		^	Reset	Configuratio	n						
VLAN Confi	guration										
 Advanced 		~	Internal	VLAN Confi	guration						
			Intern Intern	al VLAN Allo al VLAN Allo	cation Ba cation Po	se 40 licy O	93 Ascending 🖲	Descer	nding		
			VLAN (Configuration							
				/LAN ID VI.	AN Name	VLAN Type	Make Statio	2			
				200			Disable 🗸				
				de	fault	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.

Syste	em Sv	vitching	ſ	Routing		QoS		Sec	urity		М	onitor	ing		Ma	inten	ance	2	1	Help		lr	ıdex		
VLAN	Auto-VolP	iSCSI	STP	Multica	st	MVR	Add	ress Ta	able	Por	ts	LAG	1	MLAG	à										
	VLAN		VLAN N	/lembersh	iip																				
• Basic • Advanco • VLAN	ed I Configuratior	~	VLAN Group VLAN	ID Operatio Name	n												2 L V	200 Jntaj LAN(✓ g All 0200	~	•				
• VLAN • VLAN	l Membership I Status		VLAN	Type													S	tatic							
• Port F Config • MAC	PVID guration Based VLAN		Ports		5	7	9 1	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
Proto Grour	col Based VL Configuration	AN		2 4	6	8	10 1:	2 14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48

- 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.

System	n Sa	vitching		Routing	Qo	S Security	Monitoring	Maintenance Help	Index		
VLAN.	Auto-VolP	iscsi	ST	 Multic 	ast MVF	Address Table	Ports LAG MLAG	<i>b</i>			
-	VLAN		PVID	Configura	tion						
Basic			12	3 LAGS A	NI.					Go To Interface	Go
• Advanced	đ				1						Part Delugit
·VLAN (Configuration		-	Interface	PVID	VLAN Member	VLAN Tag	Acceptable Frame Types	Configured Ingress Filtering	Current Ingress Filtering	(0 to 7)
·VLAN !	Membership			1/0/1	200	1	None	Admit Ali 🗸	Disable -	Disable	0
·VLAN S	Status		×	1/0/1	1	1	None	Admit All	Disable	Disable	0
· Port PA	VID			1/0/2	1	1	None	Admit All	Disable	Disable	0
Configu	mation		8	1/0/3	1	1	None	Admit All	Disable	Disable	0
·MAC B	ased VLAN			1/0/4	1	1	None	Admit All	Disable	Disable	0

- **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.

System	Switching	Rout	ing	QoS	Sec	urity	Mon	itoring	Maintenance	Help	Index
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer So	chedule		
Servi	ces	DHCP Serve	er Configura	ation							
• DHCP Server	^	Admin Mo	de		🔘 Dis	able 💿 E	nable				
DHCP Serve Configuration	rr 1	Ping Pack	et Count		2			(0, 2 to 10	9		
 DHCP Pool Configuration 	1	Bootp Auto	gging Mod omatic Mo	e de	 Dis Dis 	able 💿 E able 🔘 E	nable nable				
• DHCP Pool	Options										
DHCP Serve	r Statistics	Excluded A	ddress								
DHCP Bindin Information DHCP Confli Information	igs cts	🔲 IP Ra	nge From		IP Range	То					

- **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.

System	Switching	Routing	QoS	Securi	ty	Monitoring	Maintenance	Help	Index
Management	Device View	Services Chass	is PoE	SNMP L	LDP IS	DP Timer	Schedule		
Service	es	DHCP Pool Configu	ration						
DHCP Server	^	Pool Name		Crea	te 🛩				
• DHCP Server		Pool Name		PooL	Dynamic	(1 to	31 alphan <mark>umeric charac</mark>	cters)	
• DHCP Pool		Type of Binding		Dyna	imic ~				
Configuration		Network Address		192.1	68.100.0				
DHCP Pool O	ptions	Network Mask		255.2	55.255.0				
• DHCP Server	Statistics	Network Prefix Ler	gth			(0 to	32)		
DHCP Binding	gs	Client Name							
Information		Hardware Address				0			
 DHCP Conflict Information 	ts	Hardware Address	Туре	Ethe	rnet 🖌				
DHCP Relay		Client ID							
• DHCP L2 Relay	~	Host Number		0.0.0.					
• UDP Relay	~	Host Mask			0				
DHCPv6 Server	~	Host Prefix Length				(1-32,			

- e. Under DHCP Pool Configuration, enter the following information:
 - In the **Pool Name** list, select **Create**.
 - In the **Pool Name** field, enter **pool_dynamic**.
 - In the Type of Binding list, select Dynamic.
 - In the Network Number field, enter 192.168.100.0.
 - In the Network Mask field, enter 255.255.255.0. As an alternate, you can enter 24 in the Network Prefix Length field. Do not fill in both the Network Mask field and Network Prefix Length fields.
 - In the **Days** field, enter **1**.
- f. Click Add.

The pool_dynamic name is now added to the Pool Name drop-down list.

Configure a DHCP Server that Assigns a Fixed IP Address

The following example shows how to set up a DHCP server with an IP address pool and let the DHCP server assign a fixed IP address based on a MAC address. The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure a DHCP Server that Assigns a Fixed IP Address

(Netgear	Switch)‡	config
(Netgear	Switch)	(Config)#service dhcp
(Netgear	Switch)	(Config)#ip dhcp pool pool_manual
(Netgear	Switch)	(Config)#client-name dhcpclient
(Netgear	Switch)	(Config)#hardware-address 00:01:02:03:04:05
(Netgear	Switch)	(Config)#host 192.168.200.1 255.255.255.0
(Netgear	Switch)	(Config)#client-identifier 01:00:01:02:03:04:05

Note: The unique identifier is a concatenation of the media type and MAC addresses. For example, the Microsoft client identifier for Ethernet address c8:19:24:88:f1:77 is 01:c8:19:24:88:f1:77, where 01 represents the Ethernet media type. For more information, see the "Address Resolution Protocol Parameters" section of RFC 1700.

Web Interface: Configure a DHCP Server that Assigns a Fixed IP Address

1. Select System > Services > DHCP Server > DHCP Server Configuration.

A screen similar to the following displays.

System	Switching	Rout	ing	QoS	Sec	urity	Mon	itoring	Maintenance	Help	Index
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer S	chedule		
Servio	ces	DHCP Serve	er Configur	ation							
DHCP Server	^	Admin Mo	de		O Dis	able 💿 E	Inable				
DHCP Serve Configuration DHCP Pool Configuration DHCP Pool	r 1 Options	Ping Pack Conflict Lo Bootp Aut	et Count Igging Mod omatic Mo	e de	2 © Dis • Dis	able 💿 E able 🔘 E	nable nable	(0, 2 to 10	0)		
DHCP Serve DHCP Bindir Information DHCP Confli Information	r Statistics ngs cts	Excluded A	ddress Inge From		IP Range	To					

- 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.

System	Switching	Routing	QoS	Sec	urity	Mon	itoring	Maintenance	Help	Index
Management	Device View	Services Cha	ssis PoE	SNMP	LLDP	ISDP	Timer S	chedule		
Servi	ces	DHCP Pool Confi	guration							
• DHCP Server	^	Pool Name		C	reate 🛩					
• DHCP Serve	er	Pool Name		po	ol_manua	al	(1 to 3	1 alphanumeric chara	cters)	
DHCR Real	1	Type of Binding		N	lanual	~				
Configuratio	n	Network Addres	S	0.0	0.0.0					
DHCP Pool	Options	Network Mask		0.0	0.0.0					
• DHCP Serve	er Statistics	Network Prefix L	ength				(0 to 32	2)		
DHCP Bindi	ngs	Client Name								
Information		Hardware Addre	SS	00	:01:02:03	04:05				
 DHCP Confl Information 	icts	Hardware Addre	ss Type	E	thernet	*				
DHCP Relay		Client ID								
• DHCP L2 Rela	y v	Host Number		19	2.168 <mark>.</mark> 200).1				
• UDP Relay	~	Host Mask		25	5.255.255	5.0				
DHCPv6 Serve	er v	Host Prefix Leng	<u>gth</u>	24			(1-32)			
		Lease Time		In	finite		*			
		Days		0			(0 to 59	9)		
		Hours		0			(0 to 23	3)		
		Minutes		0			(0 to 59	9)		

- 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 **255.255.0**. 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.

DHCPv6 Server



Dynamic Host Configuration Protocol version 6 Server

This chapter includes the following sections:

- Dynamic Host Configuration Protocol Version 6 Concepts
- CLI: Configure DHCPv6 Prefix Delegation
- Web Interface: Configure DHCPv6 Prefix Delegation
- Configure a Stateless DHCPv6 Server
- Configure a Stateful DHCPv6 Server

Note: The DHCPv6 server is available on M5300 and M6100 series switches only. However, the following M5300 series switches require a license to support the DHCPv6 server: M5300-28G, M5300-52G, M5300-28G-POE+, and M5300-52G-POE+.

Dynamic Host Configuration Protocol Version 6 Concepts

Dynamic Host Configuration Protocol version 6 (DHCPv6) for IPv6 is used to assign IPv6 addresses statefully and distribute other configuration information such as domain name or DNS server.

DHCPv6 supports stateful address allocation, prefix delegation, and stateless services. This chapter describes how to configure the prefix delegation mode using a DHCPv6 pool. When you create a DHCPv6 pool, you need to assign a prefix to the client DHCP unique identifier (DUID).

DUID is used to identify the client's unique DUID value. The format is xx:xx:xx:xx:xx:xx: RFC3315 defines three types:

- Link-layer address plus time:
 - 00:01:hardware type:time:link-layer address
 - Hardware type 16 bit hardware type reserved by IANA. 1 means an Ethernet device.
 - Time: 32-bit unsigned integer. The time in seconds when this DUID was generated since 00:00:00 1/1/2000.
 - Link-layer address The link layer address of a device generating the DUID.
- Vendor-assigned unique ID based on Enterprise Number:
 - 00:02:enterprise-number:identifier
 - Enterprise-number 32-bit integer reserved by IANA.
 - Identifier Variable length data for each vendor
- Link-layer address:
 - 00:03:hardware type:link-layer address
 - Hardware type 16 bit hardware type reserved by IANA. 1 means an Ethernet device.
 - Link-layer address The link layer address of a device generating the DUID.

In the following case, the CPE router requests prefix from the PE router. The PE router chooses prefix (2001:1::/64) for delegation, and responds with the prefix to the requesting CPE router. The CPE router subnets the prefix and assigns the longer prefixes to links in the user's network. The CPE router is then responsible to assign the 2001:1:1::/96 to one user's network and 2001:1:2::/96 to another user's network.

Managed Switches



Figure 52. DHCPv6 stateful IPv6 address assignment

CLI: Configure DHCPv6 Prefix Delegation

1. Enable IPv6 routing.

```
(Netgear Switch) #configure
(NETGEAR SWITCH) (Config)#ip routing
(NETGEAR SWITCH) (Config)#ipv6 unicast routing
```

2. Create a DHCPv6 pool and enable DHCP service.

```
(NETGEAR SWITCH) (Config)#service dhcpv6
(NETGEAR SWITCH) (Config)#ipv6 dhcp pool pool1
(NETGEAR SWITCH) (Config dhcp6 pool)#domain name netgear.com
(NETGEAR SWITCH) (Config dhcp6s pool)#prefix delegation 2001:1::/64
00:01:00:01:15:40:14:4f:00:00:00:4d:aa:d0
(NETGEAR SWITCH) (Config dhcp6s pool)#exit
```

3. Enable DHCPv6 service on port 1/0/9.

```
(NETGEAR SWITCH) (Config)#interface 1/0/9
(NETGEAR SWITCH) (Interface 1/0/9)#routing
(NETGEAR SWITCH) (Interface 1/0/9)#ipv6 address 2001:1::1/64
(NETGEAR SWITCH) (Interface 1/0/9)#ipv6 enable
(NETGEAR SWITCH) (Interface 1/0/9)#ipv6 dhcp server pool1 preference 20
(NETGEAR SWITCH) (Interface 1/0/9)#exit
```

4. Show DHCPv6 binding.

(NETGEAR SWITCH) #show ipv6 dhcp binding
Client Address
Client Interface 1/0/9
Client DUID 00:01:00:01:15:40:14:4f:00:00:00:4d:aa:d0
Identity Association ID
Binding Prefix Address/Length 2001:1::/64
Binding Prefix Type IA_PD
Binding Expiration (secs)
Binding Prefix Valid Lifetime (secs) infinite
Binding Prefix Preferred Lifetime (secs) infinite

Web Interface: Configure DHCPv6 Prefix Delegation

- **1.** Enable IP routing globally.
 - a. Select Routing > IP > Basic > IP Configuration.

System	SI	vitching		Routing		QoS	Secu	ity	Monitoring	3	Maintenance	Help	Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	iter Discovery	VRRP	Multicast	IPv6 Multicast	· · · · · · · · · · · · · · · · · · ·
IP			IP Con	figuratior	1								
• Basic		^	Defau	lt Time t	o Live				64				
 IP Configurat 	ion		Routi	ng Mode					Enable	e 🔘 Disal	ble		
 Statistics 			ICMP	Echo R	eplies				Enable	e 🔘 Dis <mark>a</mark> l	ble		
 Advanced 		×	ICMP	Redirec	ts				Enable	e 🖲 Disa	ble		
			ICMP	Rate Lir	nit Inte	rval			1000		(0 to 214	17483647 ms)	
			ICMP	Rate Lir	nit <mark>B</mark> ur	st Size			100		(1 to 200	2)	
			Maxir	num Nex	d Hops	ł.			4				
			Maxir	num Rou	ites				8160				

- b. For Routing Mode, select the Enable radio button.
- c. Click Apply to save the settings.
- 2. Enable IPv6 unicast globally.
 - a. Select Routing > IPv6 > Basic > Global Configuration.

witching		Routing		QoS	Securit	y Monitoring		Maintenance	Help	Index	
IPv6	VLAN	LAN ARP RIP OSPF OSPFv3 Router Discovery VRRP Multicast IPv6 Multicas									
	IPv6 G	lobal Cor	nfigurat	ion							
~	IPv6 I	Jnicast F	Routing			Disable Enable					
on	Hop l	imit				64	(1 to 2	?55)			
	ICMP	v6 Rate	Limit E	rror Interv	al	1000	(0 to 2	2147483647 m	isecs)		
v	ICMP	v6 Rate	Limit B	urst Size		100	(1 to 2	2001			
	Switching IPv6 A on.	IPv6 VLAN IPv6 VLAN IPv6 G IPv6 I IPv6 I IPv6 I ICMP ICMP	Switching Routing IPv6 VLAN ARP IPv6 Global Col PV6 Uncast f IPv6 Uncast f ID Limit ICMPv6 Rate ICMPv6 Rate	Switching Routing IPv6 VLAN ARP RIP IPv6 Global Configuration IPv6 Unicast Routing on IPv6 Unicast Routing Hop Limit ICMPv6 Rate Limit E ICMPv6 Rate Limit E ICMPv6 Rate Limit B	Routing QoS IPv6 VLAN ARP RIP OSPF IPv6 Global Configuration A IPv6 Unicast Routing ON HPv6 Unicast Routing VIAN ARP Ripv6 Unicast Routing ON HOp Limit ICMPv6 Rate Limit Error Interv	Routing QoS Securit IPv6 VLAN ARP RIP OSPF OSPFv3 IPv6 Global Configuration	Routing Routing QoS Security Monitoring IPv6 VLAN ARP RIP OSPF OSPFv3 Router Discovery IPv6 Global Configuration	Routing Routing QoS Security Monitoring IPv6 VLAN ARP RIP OSPF OSPFv3 Router Discovery VRRP IPv6 Global Configuration	Routing QoS Security Monitoring Maintenance IPv6 VLAN ARP RIP OSPF OSPFv3 Router Discovery VRP Multicast IPv6 Global Configuration IPv6 Unicast Routing Disable © Enable on Hop Limit 64 (1 to 255) ICMPv6 Rate Limit Error Interval 1000 (0 to 2147483647 n) v ICMPv6 Rate Limit Burst Size 1000 (1 to 200)	Routing QoS Security Monitoring Maintenance Help IPv6 VLAN ARP RIP OSPF OSPFv3 Router Discovery VRP Multicast IPv6 Multicast IPv6 Global Configuration IPv6 Unicast Routing © Disable © Enable on Hop Limit 64 (1 to 255)	

- **b.** For IPv6 Unicast Routing, select the **Enable** radio button.
- c. Click Apply to save the settings.
- 3. Enable IPv6 address on interface 1/0/9.
 - a. Select Routing > IPv6 > Advanced > Interface Configuration.

A screen similar to the following displays.

System	Switching		Routing	QoS	Security	y Monitoring	Mainter	nance	Help	Index		
Routing Table	IP IPv6	VLAN	I ARP	RIP OSPF	OSPFv3	Router Discovery	VRRP Multi	icast IPv6 M	lulticast			
IPvē	;	IPv6	Interface C	onfiguration								
• Basic	~	12	3 VLANS	All								
Advanced	~				DUCDUC	Statalaga Address	Douting	Admin	Onerationa	P.	Duplicate Address	Life Times
Global Config	uration		Interface	IPv6 Mode	Client Mode	AutoConfig Mode	Mode	Mode	Mode	MTU	Detection Transmits	Interval
Interface Con	figuration		1/0/9	Disable 🗸	Disable 🛩	Disable ~	Disable 🛩	Enable 🗸	Disable	1500	1	1800
Prefix Configu	uration		1/0/1	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800
Statistics			1/0/2	Disable	Disable	Disable	Disable	Enable	Disable	1500	81	1800
• Maighhour Ta	blo		1/0/3	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800
Treighbour Ta	Die		1/0/4	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800
Static Route Configuration			1/0/5	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800
Conliguration			1/0/6	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800
 Route Table 			1/0/7	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800
• Route Prefere	ence		1/0/8	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800
• Tunnel Confic	uration		1/0/9	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800

b. Scroll down and select the interface **1/0/9** check box to the left of the Interface column.

1/0/9 displays in the Interface field of the table heading.

- c. Enter the following information:
 - In the IPv6 Mode field, select Enable.
 - In the Routing Mode field, select Enable.
- d. Click Apply to apply the settings.
- 4. Configure the prefix on interface 1/0/9.
 - a. Select Routing > IPv6 > Advanced > Prefix Configuration.

System	Switching		Routing	QoS	Security	/ Monito	ring	Maintenance	Help	Index	
Routing Table IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3	Router Discove	ry VRF	RP Multicast	IPv6 Multicast		
IPv6		IPv6 I	nterface Se	election							
Basic	×	Inter	face	1/0/9 ~							
Advanced	^										
 Global Configura Interface Configura 	tion ration	IPv6 I	nterface Co	onfiguration							
Prefix Configurat	ion		In C Drafin		Drafiy Longth	ELIK	4	Valid Life	Preferred		Onlink
 Statistics 			ipvo mieno		Frenx Lengui	EOR	4	Time	Life Time		Flag
• Neighbour Table			2001:1:1:	1	64		~				

- b. In the Interface list, select interface 1/0/9.
- c. In the Ipv6 Prefix field, enter 2001:1::1.
- d. In the Prefix Length field, select 64.
- e. Click Add.

The IPv6 prefix for interface 1/0/9 is created.

- 5. Enable the DHCPv6 server configuration.
 - a. Select System > Services > DHCPv6 Server > DHCPv6 Server Configuration.

System	Switching	Rout	ing	QoS	Sec	urity	Moni	toring	Maintenance	Help	Index
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer S	chedule		
Servio	ces	DHCPv6 Se	rver Configu	iration							
DHCP Server	~	Admin Mo	de		O Disab	ole 💿 En	able				
DHCP Relay		DHCPv6 S	erver DUID								
DHCP L2 Rela	y ~										
• UDP Relay	*										
DHCPv6 Serve	r^										
DHCPv6 Ser Configuration	ver										
DHCPv6 Poo Configuration	d.										
DHCPv6 Prei Delegation C	fix onfiguration										

- **b.** For Admin Mode, select the **Enable** radio button.
- c. Click Apply to save the settings.
- 6. Create a DHCPv6 pool named pool1.
 - a. Select System > Services > DHCP Server > DHCPv6 Pool Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management	Device View	Services Cha	ssis SNMP	LLDP ISDP	Timer Schedule			
Servio	ces	DHCPv6 Pool Cor	figuration					
DHCP Server DHCP Relay DHCP L2 Rela UDP Relay DHCPv6 Serve OHCPv6 Serve OHCPv6 Serve OHCPv6 Serve OHCPv6 Serve Configuration	y v v r ^ ver	Pool Name Pool Name Default Router A Domain Name	ddresses <u>v</u>	reate v				

- b. In the Pool Name list, select Create.
- c. In the Pool Name field, enter pool1.
- d. Click Apply to save the settings.
- 7. Configure the prefix in the pool1.
 - a. Select System > Services > DHCPv6 Server > DHCPv6 Pool Configuration.

System Switc	hing	Routing	QoS	Secunty	Monitoring	Maintenance	Help Index	3	
Management Device V	5ew	Services Chars	aia SNMP	LLDP ISD	P Timer Schedule	•			
Services		DHCPv6 Prefix De	legation Config	guration					Add
DHCP Server	*	Pool Name	Prefix	P	efix Longth	DUID	Glient-Name	Valid Lifetime	Prefer Lifetime
DHCP Relay		pool1 ~	2001:1:	6	4	00:01:00:01:15:40:14:4	191311021002105-C		
DHCP L2 Relay	*								
DUP Relay	Č.								
DHCPv6 Server Configuration									
DHCPv6 Pool Configuration									
DHCPv6 Prefix	20								

- b. In the Pool Name field, select pool1.
- c. In the Prefix field, enter 2001:1::.
- d. In the Prefix Length field, enter 64.
- e. Click Apply to save the settings.
- 8. Configure DHCPv6 on interface 1/0/9.
 - a. Select System > Services > DHCPv6 Server > DHCPv6 Interface Configuration.

System	Switching		Routing	QoS	Securit	y Monito	ring Ma	intenance	Help	Index
Management	Device View	Se	vices Cł	nassis PoE	SNMP L	LDP ISDP	Timer Schedule			
Servic	°65	рнс	Pv6 Interfac	ce Configuration	16					
DHCP Server	~	1 2	3 All	o o o nigaration		Go To Interface	6	Go		
DHCP Relay			Interface	Admin mode	Pool Name	Rapid Commit	Preference			
DHCP L2 Relay	y ~		1/0/9	Enable 👻	*	~				
DHCPv6 Server	· ·		1/0/1	Disable						
•DHCPv6 Serv	/er		1/0/2	Disable						
Configuration			1/0/4	Disable						
 DHCPv6 Poo Configuration 			1/0/5	Disable						
DHCPv6 Pref	ix		1/0/7	Disable						
DHCPv6 Inter	oninguration face		1/0/8	Disable						
Configuration	1.1.20		11019	UISAUle						

b. Scroll down and select the interface **1/0/9** check box to the left of the Interface column.

1/0/9 displays in the Interface field of the table heading.

- c. In the Admin mode field, select Enable.
- d. In the Pool Name field, select pool1.
- e. Click Apply to save the settings.

Configure a Stateless DHCPv6 Server

This example show how you can use a DHCPv6 server to pass on information about a DNS server to clients that receive an IPv6 address in autoconfiguration mode or manual mode. The configured DHCP pool does not contain a prefix pool but contains information about the DNS server. The ipv6 nd other-config-flag command must be enabled on the IPv6 interface.

The following sections show how to configure a DNS server for clients with a stateless IPv6 address using a DHCPv6 server.

CLI: Configure a Stateless DHCPv6 Server

1. Enable IPv6 routing.

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

2. Create an IPv6 pool with a DNS server and enable the DHCPv6 service.

```
(Netgear Switch) (Config)#ipv6 dhcp pool ipv6_server
(Netgear Switch) (Config-dhcp6s-pool)#dns-server 2011:9:18::1
(Netgear Switch) (Config-dhcp6s-pool)#exit
(Netgear Switch) (Config)#service dhcpv6
```

3. Enable the IPv6 DHCP server on interface 2/0/21.

Note: In this case, you must configure the **ipv6 nd other-config-flag** command on the interface, otherwise the host cannot update the DNS server.

(Netgear	Switch)	(Config)#ir	nterface 2/0/2	21
(Netgear	Switch)	(Interface	2/0/21)#routi	ng
(Netgear	Switch)	(Interface	2/0/21)#ipv6	address 2003:1000::1/64
(Netgear	Switch)	(Interface	2/0/21)#ipv6	enable
(Netgear	Switch)	(Interface	2/0/21)#ipv6	nd other-config-flag
(Netgear	Switch)	(Interface	2/0/21)#ipv6	dhcp server ipv6_server
(Netgear	Switch)	(Interface	2/0/21)#exit	

Web Interface: Configure a Stateless DHCPv6 Server

- 1. Enable ipv6 routing.
 - a. Select Routing > IPv6 > Basic > Global Configuration.

System	S	witching		Routing		QoS	Securit	у	Monitoring		Maintenance	Help	Index
Routing Table	IP		VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP	Multicast	IPv6 Multicast	
IPv	6		IPv6 G	lobal Cor	figurat	ion							
• Basic		~	IPv6 l	Jnicast F	Routing) Disa	ble 💿 Enable	e			
Global Config	guratio	n	Hop L	.imit				64		(1 to 2	255)		
• Route Table			ICMP	v6 Rate	imit E	rror Interv	al	1000		(0 to 2	2147483647 m	isecs)	
 Advanced 		~	ICMP	v6 Rate	.imit B	urst Size		100		(1 to 2	200)		

- **b.** For IPv6 Unicast Routing, select the **Enable** radio button.
- c. Click Apply to save the settings.
- 2. Enable IPv6 routing on interface 2/0/21.
 - a. Select Routing > IPv6 > Advanced > Interface Configuration.

System	Sv	vitching		Routing	QoS	Security	Monitoring	Mainten	ance F	lelp In	dex	
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3	Router Discovery	VRRP Multic	ast IPv6 Mi	ılticast		
		_										
IPv	ŏ		IPv6 I	nterface Co	onfiguration							
Basic		~	12	All								
Advanced		^				DUOD A		H ALLAND		-		-
Global Config	uratio	n		Interface	IPv6 Mode	Client Mode	AutoConfig Mode	Mode	Mode	Mode	MTU	Duplicate Address Detection Transmit
Interface Cor	figurat	ion		2/0/21	Enable Y	Disable 🗸	Disable ~	Enable ~	Enable Y	Disable	1500	1
 Prefix Config 	Iration			2/0/1	Disable	Disable	Disable	Disable	Enable	Disable	1500	1
 Statistics 				2/0/2	Disable	Disable	Disable	Disable	Enable	Disable	1500	1
• Naighbour Tr	blo			2/0/3	Disable	Disable	Disable	Disable	Enable	Disable	1500	1
- Neighbour 12	DIE			2/0/4	Disable	Disable	Disable	Disable	Enable	Disable	1500	1
 Static Route 				2/0/5	Disable	Disable	Disable	Disable	Enable	Disable	1500	1
Configuration				2/0/6	Disable	Disable	Disable	Disable	Enable	Disable	1500	1
 Route Table 				2/0/7	Disable	Disable	Disable	Disable	Enable	Disable	1500	1
 Route Prefer 	ence			2/0/8	Disable	Disable	Disable	Disable	Enable	Disable	1500	1
• Tunnel Confi	wratio	n		2/0/9	Disable	Disable	Disable	Disable	Enable	Disable	1500	1
ranner oonn	, and the			2/0/10	Disable	Disable	Disable	Disable	Enable	Disable	1500	1

- b. Scroll down and select the 2/0/21 check box to the left of the Interface column.
 2/0/21 displays in the Interface field of the table heading.
- c. In the IPv6 Mode field, select Enable.
- d. In the Routing Mode field, select Enable.
- e. Click Apply to save the settings.
- 3. Configure IPv6 address on interface 2/0/21.
 - a. Select Routing > IPv6 > Advanced > Prefix Configuration.

Rousing Table IP EV6 VLAN ARP PIP OSPF4 Rouser Discovery VRRP Multicast IPv6 Multicast IPv6 Interface Selection - - - - - Value - 20/21 ~ - - - - • Oliobal Configuration - Interface Configuration - - - • Prefix Configuration - - - - - • Statistics - - - - - • Configuration - - - - -	Add D	Delete Cancel Acc
IPA6 IPA6 Interface Selection *Basic Interface *Advanced 2/0/21 * *Olobal Configuration 2/0/21 * *Interface Configuration 2/0/21 * *Interface Configuration 1 *Statistics Ip6 Prefix *Neighbour Table 2003 1000:1 *Statis Route Configuration 64	Add D	Delete Cancel Acc
ENG ENG Environmentation Environme	annua Ourant	
Basic Interface 20/21 • Advanced + *Global Configuration + *Interface Configuration + *Interface Configuration + *Statistica * *Neighbour Table 2003.1000.1 *Statistica 1040.56400 ceff s191 se40 *Statistica 1040.56400 ceff s191 se40	annuar Cumant	
Advanced Advanced *Global/Configuration *Interface Configuration *Interface Configuration PVs Interface Configuration *Dirtish Configuration *Interface Configuration *Dirtish Configuration *Interface Configuration *Statistics *Interface Configuration *Neighbour Table 2003 1000:1 *Statistics *100 Geb0 ceff 1619 se40 *Statistic *100 Geb0 ceff 1619 se40	Currant	
- Obala Configuration *Interface Configuration -Prefax Configurati	annution Dismant-	
Vite/face Configuration IPV6 Interface Configuration •Prefix Configuration Ipv6 Prefix Prefix Length Valid Lafe Preferred Lafe Time Onlinix Flag •Statistics 2003 1000:1 64 ✓ Onlinix ✓ •Statistics 1680:5660 celf fs19:ae40 64 Oisable ✓ ✓	Parant-	
Prefix Configuration Statistics Ipr6 Prefix Prefi	Parant	
Statistics Ip6 Prefix Prefix Length PLI64 Valid Unit Prefix Length Plag Plag Plag		
*Neighbour Table 2003.1000.1 84 v v v v v v v v v v v v v v v v v v	State	
Static Route Configuration fe80: 6eb0 ceff fe19:ae40: 64 Disable	*	
	[TENT]	
Route Table		
*Route Preference		
*Tunnel Configuration		

- b. In the Interface list, select 1/0/21.
- c. In the IPv6 Prefix field, enter 2003:1000::1.
- d. In the Prefix Length field, enter 64.
- e. In the EUI64 field, select Disable.
- f. Click Add.
- 4. Enable DHCPv6 service.
 - a. Select System > Services > DHCPv6 Server > DHCPv6 Server Configuration.

System	Switching	Routing	g (QoS	Secu	rity	Monitoring	Maintenance	Help	Index
Management	Device View	Services (Chassis	SNMP	LLDP	ISDP	Timer Schedule			
Servi	ces	DHCPv6 Serve	er Configur	ation						
DHCP Server	~	Admin Mode	e		O Disab	le 🖲 En	able			
DHCP Relay		DHCPv6 Se	erver DUID							
DHCP L2 Rela	у ~									
UDP Relay	~									
DHCPv6 Serve	r ^									
DHCPv6 Ser Configuration	ver 1									
1										

- **b.** For Admin Mode, select the **Enable** radio button.
- c. Click Apply to save the settings.
- 5. Create a DHCPv6 pool.
 - a. Select System > Services > DHCP Server > DHCPv6 Pool Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management	Device View	Services Cl	nassis SNMP	LLDP ISDP	Timer Schedule			
Servi	ces	DHCPv6 Pool C	Configuration					
DHCP Server	¥	Pool Name	C	reate y				
DHCP Relay		Pool Name	ipv	6 server				
DHCP L2 Rela	ay v	DNS Server Ad	dresses ^	-				
 UDP Relay 	~		00	14.0.0.4				
DHCPv6 Serve	er ^		20	11:9:8::1				
 DHCPv6 Ser Configuration 	rver n							
DHCPv6 Poo Configuration	ol n							
DHCPv6 Pre Delegation C	afix Configuration							
DHCPv6 Inte Configuration	erface n							
DHCPv6 Bin Information	idings	Domain Name	v					
 DHCPv6 Ser Statistics 	rver							

- b. From the Pool Name list, select Create.
- c. In the Pool Name field, enter ipv6_server.
- d. In the DNS Server Addresses fields, enter 20011:9:18::1 (which is the IPv6 address of the DNS server).
- e. Click Apply to save the settings.
- 6. Enable DHCPv6 pool on interface 2/0/21.
 - a. Select System > Services > DHCPv6 Server > DHCPv6 Interface Configuration.

System	witching		Routing	QoS	Security	Monitori	ing Maintenance	Help	Index
Management Dev	ice View	Servi	ces Ch	assis SNMP	LLDP IS	SDP Timer Sc	hedule		
Services		DHCP	v6 Interfac	e Configuration					
DHCP Server	~	12	All			Go To Interface	Go		
DHCP Relay			Interface	Admin mode	Pool Name	Rapid Commit	Preference		
DHCP L2 Relay	~		2/0/21	Enable ×	inv6 st y	Disable Y	20		
UDP Relay	~		2/0/21	Disable	ipvo_st	Disable	20		
DHCPv6 Server	^		2/0/1	Disable					
DHCPv6 Server Configuration			2/0/3	Disable					
DHCPv6 Pool Configuration			2/0/5	Disable					
DHCPv6 Prefix			2/0/6 2/0/7	Disable					
Delegation Config	uration		2/0/8	Disable					
DHCPv6 Interface Configuration			2/0/9	Disable					
Sonngaration			2/0/10	Disable					

- b. Select the 2/0/21 check box to the left of the Interface column.
 2/0/21 displays in the Interface field of the table heading.
- c. In the Admin mode field, select Enable.
- d. In the Pool Name field, select ipv6_server.
- e. Click Apply to save the settings.

Configure a Stateful DHCPv6 Server

This example shows how you can use a DHCPv6 server to assign an IPv6 address directly to a client in the same way that an IPv4 DHCPv4 server assigns an IPv4 address to an IPv4 client. A stateful DHCPv6 server assigns the IPv6 address to a client based on the configured IPv6 prefix in the DHCPv6 pool.

The following sections show how to configure a DHCPv6 server that functions in stateful mode.

CLI: Configure a Stateful DHCPv6 Server

1. Enable IPv6 routing.

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

2. Create an IPv6 pool with a DNS server and enable the DHCPv6 service.

(Netgear Switch) (Config)#ipv6 dhcp pool ipv6_server (Netgear Switch) (Config-dhcp6s-pool)#address prefix 2001:1:2::/64 (Netgear Switch) (Config-dhcp6s-pool)#exit (Netgear Switch) (Config)#service dhcpv6 3. Enable the IPv6 DHCP server on interface 1/0/1.

(Netgear	Switch)	(Config)#interface 1/0/1	
(Netgear	Switch)	(Interface 1/0/1) #routing	
(Netgear	Switch)	(Interface 1/0/1)#ipv6 address 2001:1:2::1/64	
(Netgear	Switch)	(Interface 1/0/1)#ipv6 enable	
(Netgear	Switch)	(Interface 1/0/1)#ipv6 dhcp server ipv6_server	
(Netgear	Switch)	(Interface 1/0/1)#exit	

Web Interface: Configure a Stateful DHCPv6 Server

- 1. Enable ipv6 routing.
 - a. Select Routing > IPv6 > Basic > Global Configuration.

System	S	witching	F	Routing		QoS	Security	Monitoring	Ma	aintenance	Help	Index
Routing Table	IP		VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast	
IPvi	6		IPv6 Gl	obal Cont	figurati	on						
Basic		^	IPv6	Unicast	Routin	ng		Disable Enable	le			
Global Config	guratio	on	Hop	Limit				64	(1	to 255)		
Route Table			ICM	Pv6 Rate	Limit	Error Inte	rval	1000	(0	to 214748364	47 msecs)	
 Advanced 		~	ICM	Pv6 Rate	Limit	Burst Siz	e	100	(1	to 200)		
			5									

- **b.** For IPv6 Unicast Routing, select the **Enable** radio button.
- c. Click Apply to save the settings.
- 2. Enable IPv6 routing on interface 1/0/1.
 - a. Select Routing > IPv6 > Advanced > Interface Configuration.

System Swite	hing		Routing	QoS	Security	Monitoring	Maintena	ince	Help In	dex				
Routing Table IP		VLAN	ARP	RIP OSPF	OSPFv3	Router Discovery	VRRP Mul	ticast IP	6 Multicast					
														Cancel Appl
IPv6		IPv6 In	terface Co	nfiguration										
Basic	*	12	3 VLANS	All								Go T	o Interface	Go
Advanced Global Configuration	•	-	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	Adv Reachable
Interface Configuration	n		1/0/1	Enable 👻	Disable ~	Disable ~	Enable ~	Enable	- Enable	1500	1	1800	0	0
Prefix Configuration			1/0/1	Enable	Disable	Disable	Enable	Enable	Enable	1500	1	1800	0	0
			1/0/2	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
Statistics		0	1/0/3	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
Neighbour Table		0	1/0/4	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
Static Route			1/0/5	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
Configuration			1/0/6	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
Route Table		0	1/0/7	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
• Routo Profesence			1/0/8	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
- novie r idielence			1/0/9	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
Tunnel Configuration			1/0/10	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0

b. Select the 1/0/1 check box to the left of the Interface column.

1/0/1 displays in the Interface field of the table heading.

- c. In the IPv6 Mode field, select Enable.
- d. In the Routing Mode field, select Enable.
- e. Click Apply to save the settings.
- 3. Configure the IPv6 address on interface 1/0/1.
 - a. Select Routing > IPv6 > Advanced > Prefix Configuration.

System Switching		Routing	QoS	Security	Monitoring) M.	aintenance	Help	Index				
Routing Table IP IPV6	VLAN	ARP	RIP OSPF	OSPFv3	Router Discover	y VRRP	Multicast	IPv6 Multicas	£.	1			
												Add	Delete Cancel Apply
IPv6	IPv6 In	nterface Se	ection										Ø
•Basic ~	Inte	erface	1/0/1 ~										
Advanced													
Global Configuration													
Interface Configuration	IPv6 I	nterface Co	onfiguration										Ø
Prefix Configuration							Valid Life		Preferred		Onlink	Autonomous	Current
Statistics		I Ipv6 Pret	iX.	Prefix Len	gth	E0164	Time		Life Time		Flag	Flag	State
Neighbour Table		2001:1:2	8 4)	64			1]			1.1	v v	
Static Route Configuration		fe80::6et	0.ceff;fef9.f6e3	64		Disable							[ACTIVE]
Route Table													
Route Preference													
Tunnel Configuration													

- b. In the Interface list, select 1/0/1.
- c. In the IPv6 Prefix field, enter 2001:1:2::1.
- d. In the Length field, enter 64.
- e. In the EUI64 field, select Disable.
- f. Click Add.
- **4.** Enable the DHCPv6 service.
 - a. Select System > Services > DHCPv6 Server > DHCPv6 Server Configuration.

System	witching	ing Rou	ting QoS	Security	Monitoring	Maintenance	Help	Index	
Management De	ice View	iew Services	Chassis PoE	SNMP LLDP	ISDP Timer	Schedule			
									Cancel Apply
Services		DHCPv6 S	erver Configuration	8					
DHCP Relay	- 0	Admin N	Node	🕞 Disable 🖲	Enable				
DHCP L2 Relay		DHCPV	6 Server DUID	00.01:00:06:4	b:3e:3a:1d:6c:b0	ce:19:16:e0			
• UDP Relay	~	e							
DHCPv6 Server	•								
DHCPv6 Server Configuration									
DHCPv6 Pool Configuration									
DHCPv6 Prefix Delegation Configuration									
DHCPv6 Interfac Configuration	e l								
DHCPv6 Binding Information	5								
DHCPv6 Server Statistics									
Delegation Configuration • DHCPv6 Interfac Configuration • DHCPv6 Binding Information • DHCPv6 Server Statistic s	0 5								

- **b.** For Admin Mode, select the **Enable** radio button.
- c. Click Apply to save the settings.
- 5. Create the DHCPv6 pool.
 - a. Select System > Services > DHCP Server > DHCPv6 Pool Configuration.

System	Switching	Routing QoS	Security	Monitoring Maintenance	Help	Index		
Management De	vice View	Services Chassis PoE	SNMP LLDP IS	SDP Timer Schedule	-94 - 19-	19 19		
Constant		DHCPv6 Pool Configuration					elete Cancel	Apply
- DHCD Balay			10000					
DHCP Relay		Pool Name	Create ~					
UDP Palm	Ŷ	Pool Name	ipv6_server					
DHCRUS Septer		Divisi Server Addresses						
DHCPv6 Server	<u> </u>	Domain Name						
Configuration								
DHCPv6 Pool Configuration								
DHCPv6 Prefix Delegation Configuration								
DHCPv6 Interfa Configuration	e							
DHCPv6 Bindin Information	j5							
DHCPv6 Server Statistics								

- b. In the Pool Name list, select Create.
- c. In the Pool Name field, enter ipv6_server.
- d. Click Apply to save the settings.
- 6. Configure the prefix for the DHCPv6 pool.
 - a. Select System > Services > DHCPv6 Prefix Delegation Configuration > DHCPv6 Prefix Delegation Configuration.

System	Switching		Routing	QoS Se	scurity Monitoring	Maintenance	Help Index		
Management D	wice View	DHCE	ices Chast	anation Configuration	P LLDP ISDP TimerS	Schedule			Add Delete Cancel Apply
DHCP Relay			Pool Name	Prefix	Prefix Length	DUID	Client Name	Valid Lifetime	Prefer Lifetime
DHCP L2 Relay	~		ipv6_sr v	2001:1:2::	64	ab.cd.ef	1	4294967295	4294967295
+UDP Relay	*								
DHCPv6 Server	~								
DHCPv6 Serve Configuration									
DHCPv6 Pool Configuration									
DHCPv6 Prefix Delegation Configuration									
DHCPv6 Interfa Configuration	ce								
DHCPv6 Bindin Information	75								
DHCPv6 Serve Statistics									

- b. In Pool Name list, select ipv6_server.
- c. In the Prefix field, enter 2001:1:2::.
- d. In the Prefix Length field, enter 64.
- e. Click Add.
- 7. Enable the DHCPv6 pool on interface 1/0/1.
 - a. Select System > Services > DHCPv6 Server > DHCPv6 Interface Configuration.

A screen similar to the following displays.

System	Switching		Routing	QoS		Security	Monitorin	g Ma	intenance	Help	Index	
Management C	evice View		nos Chu	assis Pol		SNMP LL	DP ISDP T	imer Schedu	le:			
												Cancel
Service	5	DHCP	v6 Interfac	e Configurat	ion							
DHCP Server	*	12	3 All				Go To Interfa	:e	Go			
DHCP Relay			Interface	Admin mo	de	Pool Name	Rapid Commit	Preference				
DHCP L2 Relay	~		1/0/1	Enable	¢1	inv6 si v						
UDP Relay	*		1/0/1	Disable	-	Concernance of the second						
DHCPv6 Server			1/0/2	Disable								
·DHCPv6 Serve	br		1/0/3	Disable								
Configuration			1/0/4	Disable								
DHCPv6 Pool			1/0/5	Disable								
Configuration			1/0/6	Disable								
DHCPv6 Prefix	<		1/0/7	Disable								
Configuration			1/0/8	Disable								
- DHCD-6 Interd	-		1/0/9	Disable								
Configuration	ere 12		1/0/10	Disable								
DHCPv6 Bindi	nas		1/0/11	Disable								
Information			1/0/12	Disable								
DHCPv6 Serve	19		1/0/13	Disable								
		10	1/0/14	Disable								

b. Select the interface **1/0/1** check box to the left of the Interface column.

1/0/1 displays in the Interface field of the table heading.

- c. In the Admin mode field, select Enable.
- d. In the Pool Name field, enter ipv6_server.
- e. Click Apply to save the settings.

DVLANs and Private VLANs



Double VLANS and private VLAN groups

This chapter includes the following sections:

- Double VLANs
- Private VLAN Groups

Double VLANs

This section describes how to enable the double DVLAN feature. Double VLANs pass traffic from one customer domain to another through the metro core. Custom VLAN IDs are preserved and a provider service VLAN ID is added to the traffic so the traffic can pass the metro core in a simple and cost-effective manner. You can use VLANs to specify customer ports and a service provider port. In this example, the switches have the same configuration.



Figure 53. Double VLANS

The following example shows how to configure the NETGEAR switch shown in the preceding figure to add a double VLAN tag for traffic going from the subnet domain connected to port 1/0/24. This example assumes that a Layer 2 switch connects all these devices in your domain. The Layer 2 switch tags the packet going to the NETGEAR switch port 1/0/24. The example is shown as CLI commands and as a web interface procedure.

CLI: Enable a Double VLAN

```
Create a VLAN 200.
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#exit
Add interface 1/0/24 to VLAN 200, add pvid 200 to port.
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24) #vlan pvid 200
(Netgear Switch) (Interface 1/0/24)#vlan participation include 200
(Netgear Switch) (Interface 1/0/24)#exit
Add interface 1/0/48 to the VLAN 200 in a tagging mode.
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan participation include 200
(Netgear Switch) (Interface 1/0/48)#vlan tagging 200
(Netgear Switch) (Interface 1/0/48)#exit
Select interface 1/0/48 as the provider port.
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#mode dvlan-tunnel
(Netgear Switch) (Interface 1/0/48)#exit
```

Web Interface: Enable a Double VLAN

- 1. Create static VLAN 200:
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

Syste	em	S	witching		Routing	QoS	Security	Monitorir	ng Maintenance	Help	Index
	Auto-	VolP	iSCSI	STP	Multicas	t MVR	Address Table	Ports LAG	MLAG		
	VLA	N		Reset							
 Basic 			^	Rese	et Configural	ion					
• VLAN	I Config	juration	r (
• Advance	ed		~								
				Intern	al VLAN Co	figuration					
				Inter	nal VLAN A	location Bas	e 40	93			
				Inter	nal VLAN A	location Poli	cy 🔘	Ascending 💿 De	escending		
				VLAN	Configuratio	on					
					VLAN ID	/LAN Name	VLAN Type	Make Static			
					200	vlan200		Enable 👻			
					1 4	default	Default	Disable			

- **b.** Under VLAN Configuration, enter the following information:
 - In the VLAN ID field, enter 200.
 - In the VLAN Name field, enter vlan200.
 - In the VLAN Type field, select Static.
- c. Click Add.
- 2. Add ports 24 and 48 to VLAN 200.
 - a. Select Switching > VLAN > Advanced > VLAN Membership.

System	Sv	vitching		Routing		QoS		Seci	urity		Mo	nitori	ng		Mai	ntenar	се		Help	<u>i</u>	Ir	ıdex		
VLAN Auto	-VolP	iscsi	STP	Multio	cast	MVR	Add	ress Ta	able	Port	s	LAG	M	ILAG										
VL	٩N	Γ	VLAN	Vlember	ship																			
Basic		~	VLAN	ID													200	~						
 Advanced VLAN Conf 	iguration	^	Group VLAN	Operat Name	ion												Unt	ag All	N	•				
• VLAN Men	bership		VLAN	Type													Stati	00						
VLAN Stat Port PVID	JS			Init 1													20							
Configuratio	on		Ports	1	3 5	7	9 1	13	15	17	19	21	23	25	27	29 31	33	35	37	39	41	43	45	47
• MAC Base	d VLAN	AN											U											Т
Group Con	iouration	-MN		2	4 6	8	10 1:	2 14	16	18	20	22	24	26	28	30 32	34	36	38	40	42	44	46	48

- b. Under VLAN Membership, in the VLAN ID field, select 200.
- c. Click Unit 1. The ports display:
 - Click the gray box under port **24** twice until **U** displays. The U specifies that the egress packet is untagged for the port.
 - Click the gray box under port **48** once until **T** displays. The T specifies that the egress packet is tagged for the port.
- d. Click Apply to save the settings.
- 3. Change the port VLAN ID (PVID) of port 24 to 200:
 - a. Select Switching > VLAN > Advanced > Port PVID Configuration.

System 5	witching		Routing	6	loS Security	Monitoring	Maintenance Help	Index		
VIEW Auto-VolP	iscsi	ST	Multic	ast M	R Address Table	Ports LAG MU	AG			
VLAN	1	PVID	Configurat	tion						
Basic	~	12	I LAGS A	JI					Go To Interface	Go
Advanced • VLAN Configuration	'n		Interface	PVID	VLAN Member	VLAN Tag	Acceptable Frame Types	Configured Ingress Filtering	Current Ingress Filtering	Port Priority (0 to 7)
• VLAN Membershi	p :		1/0/24	200	1.200	None	Admit All	Disable 😁	Disable	0
+VLAN Status		10	1/0/1	4	1	None	Admit All	Disable	Disable	0
Port PVID		8	1/0/2	1	1	None	Admit All	Disable	Disable	0
Configuration		0	1/0/3	1	1	None	Admit All	Disable	Disable	0
+MAC Based VLAJ	4		1/0/4	1	1	None	Admit All	Disable	Disable	0
Protocol Basad V	AN	0	1/0/5	1	1	None	Admit All	Disable	Disable	0
Group Configuratio	on	13	1/0/6	1	1	None	Admit All	Disable	Disable	0
Protocol Based V	LAN	0	1/0/7	1	1	None	Admit All	Disable	Disable	Ū
Group Membershi	p	0	1/0/8	1	1	None	Admit All	Disable	Disable	0
*IP Subnet Based			1/0/9	1	1	None	Admit All	Disable	Disable	0
VLAN		10	1/0/10	1	1	None	Admit All	Disable	Disable	0

- **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.

Syste	em	Switch	ing		Routing	Qo	S	Security		Monitorir	ig 🛛	Maintenance	Help	Index
VLAN	Auto-Vol	P iS(CSI	STP	Multica	st MVF	R A	Address Table	Ports	LAG	MLAC			
	VLAN		(Globa	Configura	tion								
•Basic		8	~	Glob	al EtherTy	pe	8	02.1Q Tag 👻	1					
* Advanc	ed		^											
- VLAN	Configura	tion												
· VLAN	Members	hip		DVLA	N Configura	ation								
- VLAN	V Status			123	LAGS AI	I Go To In	terfac	ce	G	ю				
Port I Confi	PVID guration				Interface	Admin M	ode							
-MAC	Based VL	AN			1/0/48	Enable	~							
. Proto	col Basad	VI AN			1/0/1	Disable								
Grou	p Configura	ition			1/0/2	Disable								
• Proto	col Based	VI AN			1/0/3	Disable								
Grou	p Members	hip			1/0/4	Disable								
•IP St	ibnet Base	d			1/0/5	Disable								
VLAN	V				1/0/6	Disable								
Port I	DVLAN				1/0/7	Disable								
Confi	guration				1/0/8	Disable								

- **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 54. 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.

Syste	em S	witching		Routing	QoS	Security	Monitor	ng	Maintenance	Help	Index
VLAN	Auto-VoIP	iSCSI	STP	Multicast	MVR	Address Table	Ports LAG	MLAG	i.		
	VLAN		Reset								
 Basic 		^	Reset	Configuratio	n						
• VLAN	I Configuratio	n.									
 Advanc 	ed	~									
			Internal	VLAN Conf	iguration						
			Intern	al VLAN Allo	cation Ba	ise 40	93				
			Intern	al VLAN Allo	ocation Po	licy 💿	Ascending 💿 D	escendin	9		
			VLAN 0	Configuration							
				/LAN ID VI	_AN Name	e VLAN Type	Make Static				
				200 vi	an200		Enable 👻				
				l de	fault	Default	Disable				

- **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.

Syste	em Sv	vitching		Routing		QoS		Sec	urity		Μ	onitor	ing		M	ainte	nanco	e		Help		* 1	ndex		
VLAN	Auto-VolP	iscsi	STP	Multica	ist	MVR	Add	ress T	able	Po	rts	LAG	1	MLAG	9				9						
	VLAN		VLAN I	Vembers	hip																				
Basic		*	VLAN	ID														200	*						
Advanc	ed	^	Group	Operatic	n													Unta	ag Al		~				
• VLAN	Configuration	ı	VLAN	Name														vlan2	00						
• VLAN	I Membership		VLAN	Туре														Statio	3			6			
• VLAN	I Status			loit 1																					
Port F Confi	PVID guration		Ports	1 3	5	7	9 1	1 13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
• MAC	Based VLAN				11					U										2000 1900 - 1					
• Proto Grout	col Based VL Configuration	AN		2 4	6	8	10 1	2 14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48

- 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.

System Switchin	9	Routing	Q	S Security	Monitoring	Maintenance Help	Index		
VUM Auto-VelP ISCS	R ST	> Multic	est MV	Address Table	Ports LAG MLA	G			
VLAN	PVID	Configurat	ion						
Basic v	12	3 LAGS A	31					Go To Interface	Go
Advanced •	100								Dert Drienty
VLAN Configuration	-	Interface	PVID	VLAN Member	VLAN Tag	Acceptable Frame Types	Configured Ingress Filtering	Current Ingress Filtering	(0 to 7)
VLAN Membership			200				~		
+VLAN Status		1/0/1	1	1	None	Admit All	Disable	Disable	0
Port PVID	8	1/0/2	1	1	None	Admit All	Disable	Disable	0
Configuration	6	1/0/3	1	1	None	Admit All	Disable	Disable	0
MAC Based VLAN		1/0/4	1	1	None	Admit All	Disable	Disable	0
Protocol Elevand VI AN	0	1/0/5	1	1	None	Admit All	Disable	Disable	0
Group Configuration	2	1/0/5	1	1,200	None	Admit All	Disable	Disable	0
Destocal Racad VI AN	8	1/0/7	1	1,200	None	Admit All	Dizable	Disable	0
Group Membership	10	1/0/8	1	1	None	Admit All	Disable	Disable	0

- **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.
| System | Switching | Routing | QoS Security | Monitoring | Maintenance | Help | Index |
|---|-----------|-----------------------------------|------------------------|------------|-------------|------|-------|
| Management Secur | ity Acces | s Port Authentical | ion Traffic Control Co | ntrol ACL | | | 3 |
| Traffic Contro | ol F | ^p rivate Group Configu | ration | | | | |
| MAC Filter | ~ F | ^o rivate Group Configu | ration | | | | |
| Port Security | ~ | Group Name | Group ID | Group N | Aode | | |
| Private Group | ~ | aroun1 | 4 | commu | nity x | | |
| Private Group
Configuration | | group | | commu | inty | | |
| Private Group Membership | 10 | | | | | | |
| Protected Port | | | | | | | |

- 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.

System	Swit	ching		Routir	ıg		Qos	3		Sec	urity		N	lonito	ring	1	M	aintei	nanc	e		Help	8	Ir	ıdex	0	
Management S	Security	Acce	ss F	ort Au	ither	nticati	on					Contr	ol	ACL													
Traffic C	Control		Private	Group	o Me	mber	ship																				
MAC Filter		~	Private	Group	Me	mber	ship																				
Port Security		*	Group	D										1 ~													
Private Group		~	Grou	o Nam	e									aroup	1												
Private Grou Configuration	p 1		Grou	o Nam	е									comn	nunity												
 Private Grou Membership 	р		Ports	Init 1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
Protected Port				1 - Sa	12	1	1	1 20	12 1	1 20	12	1 20	12 1	1 - 20	12			1 da		1 20		1 da	11. 1	a in	1	1 20	
Private Vlan		~				<u>.</u>				È.		È						È.,		Ì.,		È.,					
Storm Control		~		2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48

- 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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	ecurity Access	Port Authentic	ation Tra	flic Control Cor	ntrol ACL		12	
Traffic C •MAC Filter	control Pri	vate Group Config vate G <mark>ro</mark> up Config	juration juration					
Port Security Private Group	×	Group Name		Group ID	Gro	up Mode		
Private Group Configuration	P (group2		2	isol comi	ated 👻		
 Private Group Membership 	p							

- 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.

System	Swit	ching	3	Routin	g	1	QoS	;	1	Secu	irity		М	onito	ring		М	ainte	nanc	е		Help		lr	ıdex		
Management S	Security	Acces	s P	ort Au	thent	icatio	п				0	Contr	ol	AĊL													
Traffic C	Control	P	rivate	Group	Men	nbers	hip																				
• MAC Filter		× F	Private	Group	Men	nbers	hip																				
 Port Security 		~	Group	, ID									Ē	2 ~	1												
Private Group		^	Group	Nam	е								1	2 aroup	2												
 Private Grou Configuration 	p 1		Group	Nam	е									solat	ed												
Private Grou	р		U	nit 1																							
Membership	K		Ports	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
 Protected Port 						2				20-1	1 I.	~		1 27		1 3	14 A	1 27	²⁶ []	1 20-1		1 20-1		1 20-7		1 27	
Private Vlan		~							. 1	1. "I		1	. 1	1, 1	. 1	1		1	. [ľ. "I		1	. 1	L and			
Storm Control		~		2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48

- b. In the Group ID list, select 2.
- c. Click Unit 2. The ports display.
- d. Click the gray boxes under ports 16 and 17, and a check mark displays in each box.
- e. Click Apply.

STP

Spanning Tree Protocol

This chapter includes the following sections:

- Spanning Tree Protocol Concepts
- Configure Classic STP (802.1d)
- Configure Rapid STP (802.1w)
- Configure Multiple STP (802.1s)
- Configure PVSTP and PVRSTP

30

Spanning Tree Protocol Concepts

The purpose of the Spanning Tree Protocol (STP) is to eliminate loops in the switch system. There are three STPs: Classic STP (802.1d), Rapid STP (RSTP, 802.1w), and Multiple STP (MSTP, 802.1s).

While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a few seconds. RSTP can revert back to 802.1d in order to interoperate with legacy bridges on a per-port basis. This drops the benefits it introduces.

In Multiple Spanning Tree Protocol (MSTP), each Spanning Tree instance can contain several VLANs. Each Spanning Tree instance is independent of other instances. This approach provides multiple forwarding paths for data traffic, enabling load balancing, and reducing the number of Spanning Tree instances required to support a large number of VLANs.

Configure Classic STP (802.1d)

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

CLI: Configure Classic STP (802.1d)

(Netgear Switch) (Config)# spanning-tree
(Netgear Switch) (Config)# spanning-tree mode stp
(Netgear switch) (Interface 1/0/3)# spanning-tree port mode

Web Interface: Configure Classic STP (802.1d)

- 1. Enable 802.1d on the switch.
 - a. Select Switching > STP > STP Configuration.

Syst	em	Switching	F	Routing	QoS	Security		Monitorin	ig 🛛	Maintenance	Help	Index
VLAN	Auto-VolF	P iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAC	3		
	STP		STP Co	nfiguration								
• Basic		~	Spann	ing Tree Adr	nin Mode	э	🔘 Disa	ible 💿 Er	nable			
• STP	Configuratio	m):	Force	Protocol Vei	sion		IEEE	E 802.1d	IEEE	802.1w 🔘 IEEE 8	302.1s	
* Advanc	ed	~	Config	uration Nam	e		20-0C-	C8-4D-95	i-72			
			Config	uration Revis	sion Leve		0			(0 to 65535)		
			Forwar	rd BPDU wh	ile STP [Disabled	Oisa	ible 🔘 Er	nable			
			BPDU	Guard			Oisa	ible 🛞 Er	nable			
			BPDU	Filter			Oisa	ible 🔘 Er	nable			
			Config	uration Dige:	st Key		0xac36	177 f 5028	3c <mark>d4b</mark> 8	3821d8ab26de62		
			Config	uration Form	iat Selec	tor	0					

- **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.

System Switch	ting		Routing	9	oS Se	curity	Monitoring	Maintenance	Help	Index		
VLAN Auto-VolP iSt	CSI	SI	n Multic	ast MV	R Address	Table Port	s LAG MLAG					
STP		CST	Port Confi	guration								
•Basic	+	12	3 LAGS A	MI .								Go To
*Advanced *STP Configuration	*		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	BPOU Filter	BPDU Forwarding
CST Configuration			1/0/3	128	Disable ~	0	Enabled	2	0	Enabled	Disable ~	Disable ~
CST Port Configuration		8	1/0/1	128	Disable	0	Enabled	2	0	Enabled	Disable	Disable
+CST Port Status		- 60	1/0/2	128	Disable	0	Enabled	2	0	Enabled	Disable	Disable
AUGT Configuration		X	1/0/3	128	Disable	0	Enabled	2	0	Enabled	Disable	Disable
- mor coniguration			1/0/4	128	Disable	0	Enabled	2	0	Enabled	Disable	Disable
MST Port Status		0	1/0/5	128	Disable	0	Enabled	2	0	Enabled	Disable	Disable
STP Statistics		0	1/0/6	128	Disable	0	Enabled	2	0	Enabled	Disable	Disable
		- 173	1/0/7	128	Theabla	0	Enabled	2	n	Enabled	Discable.	Dicable

- **b.** Under CST Port Configuration, scroll down and select the Interface **1/0/3** check box. Now 1/0/3 appears in the Interface field at the top.
- c. In the Port Mode field, select Enable.
- d. Click Apply.

Configure Rapid STP (802.1w)

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

CLI: Configure Rapid STP (802.1w)

(Netgear switch) (Config)# spanning-tree (Netgear switch) (Config)# spanning-tree mode rstp (Netgear switch) (Interface 1/0/3)# spanning-tree port mode

Web Interface: Configure Rapid STP (802.1w)

- 1. Enable 802.1w on the switch:
 - a. Select Switching > STP > STP Configuration.

A screen similar to the following displays.

Syste	em S	witching	Routing	QoS	Security	1	Monitorin	ıg	Maintenance	Help	Index
VLAN	Auto-VolP	iSCSI	SIP Multio	ast MVR	Address Table	Ports	LAG	MLA	G	8	2
	STP	1	STP Configurat	ion							
Basic		^	Spanning Tre	e Admin Mode		🔘 Disa	ole 💿 Er	nable			
• STP	Configuration		Force Protoco	l Version		IEEE	802.1d	IEE	E 802.1w 🔘 IEEE 8	02.1s	
Advanc	ed	~	Configuration	Name		20-0C-0	08-4D-95	5-72			
			Configuration	Revision Level		0			(0 to 65535)		
			Forward BPD	J while STP D	isabled	O Disal	ole 💿 Er	nable			
			BPDU Guard			Oisal	ole 🔘 Er	nable			
			BPDU Filter			Oisal	ole 🔘 Er	nable			
			Configuration	Digest Key		0xac361	77f5028	3cd4b8	33821d8ab26de62		
			Configuration	Format Select	or	0					

- **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.

System Swit	ching		Routing		uS Se	curity	Monitoring	Maintenance	Help	Index		
VLAN Auto-VolP i	SCSI	SI	P Multic	ast MV	R Address	Table Port	LAG MLAG					
SIP		CST	Port Config	guration								
Basic		12	3 LAGS	All								Go To
Advanced STP Configuration	a		Interface	Port Priority	Admin Edge Port	Port Path Cost	Auto Calculated Port Path Cost	Hello Timer	External Port Path Cost	Auto Calcolated External Port Path Cost	8PDU Filter	8PDU Forwarding
CST Configuration			1/0/3	128	Disable ~	0	Enabled	2	0	Enabled	Disable ~	Disable ~
+CST Port Conliguratio	n	0	1/0/1	128	Disable	0	Enabled	2	0	Enabled	Disable	Disable
CST Port Status			1/0/2	128	Disable	0	Enabled	2	0	Enabled	Disable	Disable
•MST Configuration		2	1/0/3	128	Disable	0	Enabled	2	0	Enabled	Disable	Disable
•MST Port Status			1/0/5	128	Disable	0	Enabled	2	0	Enabled	Disable	Disable
• STP Statistics		0	1/0/6	128	Disable	0	Enabled	2	0	Enabled	Disable	Disable

- b. Under CST Port Configuration, scroll down and select the Interface 1/0/3 check box.
 Now 1/0/3 appears in the Interface field at the top.
- c. In the Port Mode field, select Enable.
- d. Click Apply.

Configure Multiple STP (802.1s)

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

CLI: Configure Multiple STP (802.1s)

```
(Netgear switch) (Config) # spanning-tree
(Netgear switch) (Config) # spanning-tree mode mst
(Netgear Switch) (Config)#spanning-tree configuration name mstp_1
(Netgear Switch) (Config)#spanning-tree configuration revision 0
Configure an MSTP region name and revision for the switches in the same MSTP region.
The switches in the same MSTP region must be configured with the same region name
and revision.
Create a mst instance 1:
(Netgear switch) (Config) # spanning-tree mst instance 1
Associate the mst instance 1 with the VLAN 2 and 3:
(Netgear switch) (Config) # spanning-tree mst priority 1 4096
(Netgear switch) (Config) # spanning-tree mst vlan 1 2
(Netgear switch) (Config) # spanning-tree mst vlan 1 3
Create a mst instance 2:
(Netgear switch) (Config)# spanning-tree mst instance 2
Associate the mst instance 2 with the VLAN 11 and 12:
(Netgear switch) (Config) # spanning-tree mst priority 2 4096
(Netgear switch) (Config) # spanning-tree mst vlan 2 11
(Netgear switch) (Config) # spanning-tree mst vlan 2 12
Configure the priority and cost on port 1/0/3:
(Netgear switch) (Interface 1/0/3)# spanning-tree mst 1 port-priority 128
(Netgear switch) (Interface 1/0/3)# spanning-tree mst 1 cost 0
```

Web Interface: Configure Multiple STP (802.1s)

- 1. Enable 802.1s on the switch.
 - a. Select Switching > STP > STP Configuration.

A screen similar to the following displays.

Syste	em	Sw	vitching		Routing	QoS	Security		Aonitorin	g	Maintenance	Help	Index
VLAN	Auto-Vo	pIP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLA	AG	0	te-
	STP		ĺ	STP Co	onfiguration								
 Basic 			~	Span	ning Tree Ad	min <mark>M</mark> ode		🔘 Disa	ole 💿 Er	able			
• STP	Configura	tion		Force	Protocol Ve	rsion		IEEE	802.1d	() IEE	EE 802.1w 🖲 IEEE 80)2.1s	
• Advanc	ed		×	Config	juration Nam	e		20-0C-0	28-4D-95	-72			
				Config	juration Revi	sion Level		0			(0 to 65535)		
				Forwa	rd BPDU wh	ile STP D	lisabled	🖲 Disa	ole 🔘 Er	able			
				BPDL	l Guard			🖲 Disa	ole 🔘 Er	able			
				BPDL	J Filter			🖲 Disa	ole 🔘 Er	able			
				Config	juration Dige	st Key		0xac36	177f5028	3cd4b	83821d8ab26de62		
				Config	juration Forn	nat Select	or	0					

- **b.** Enter the following information:
 - For Spanning Tree Admin Mode, select the **Enable** radio button.
 - For Force Protocol Version, select the IEEE 802.1s radio button.
 - In the Configuration Name field, enter mstp_1.
 - In the **Configuration Revision Level** field, enter **0**.
- c. Click Apply.
- 2. Configure MST.
 - a. Select Switching > STP > MST Configuration.

System Switc	hing		Routing	QoS	Security Mo	nitoring	Maintenance Help	Index		
VLAN Auto-VolP is	CSI	SIL	Multic	ant MVR	Address Table Ports	LAG MLAG				
e.	_									Add Del
STP		MST	Configurat	ion						
Basic						AND CONTRACTOR	Time Since	Topology Change	Topology	
*Advanced	•	-	MSTID	Priority	Eindge Identifier	Vian Id	Topology Change	Count	Change	Designated Root
• STP Configuration										
CST Configuration		8	0	32768	80:00:20:0C:C8:4D:95:72	1,100,200,500	0 day 0 hr 5 min 18 sec	4	False	80:00:00:8E:F2:FF:2F:2E
+CST Dot Confouration	8	13	1	4096	10:01:20:0C:C8:4D:95:72	2-3	0 day 0 hr 2 min 23 sec	1	False	10:01:20:0C:C8:4D:95:72
- Got Port Consignation	× 1	- 69	2	4096	10:02:20:0C:C8:4D:95:72	11-12	0 day 0 hr 1 min 46 sec	1	False	10:02:20:0C:C8:4D:95:72
•CST Port Status	_									
MST Configuration										
•MST Port Status										
• STP Statistics										

- **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.

System Switc VLAN Auto-VolP iS	ting SCSI	SI	Routing Motoc	QoS ast MVR A	Security odrass Table F	Monitoring Ports LAG MUP	Mainte (G	nunce	Help Inde	×			
STP		MST	ID Selectio	an									
*Basic	+	Sel	ect MST	1 -									
Advanced	~												
STP Configuration CST Configuration		MST	Port Statu	5									
-CST Port Configuration		12	3 LAGS A	JI .									Go To Interface
CST Port Status MST Configuration			Interface	Port	Port Pr	dh Ga	to iculated	Port	Port Uptime Since	Port	Port Forwarding	Port	Designated Root
STP Statistics				- money		Co	at	10	Clear Counters	most	State	- tore	
			1/0/3	128	0	En	abled	80:03	0 day 0 hr 13 min 9 sec	Enable	Disabled	Disabled	80:01:20:0C:C8:4D:95:72
			1/0/1	128	0	En	abled	80:01	0 day 0 hr 13 min 9 sec	Enable	Disabled	Disabled	80.01.20.0C.C8.4D.95.72
			1/0/2	128	0	En	abled	80:02	0 day 0 hr 13 min 9 sec	Enable	Disabled	Disabled	80:01:20:0C:C8:4D:95:72
1		1	1/0/3	128	0	En	abled	80:03	0 day 0 hr 13 min 9 sec	Enable	Disabled	Disabled	80.01.20.0C C8 4D 95 77

- Under MST Port Configuration, scroll down and select the Interface 1/0/3 check box. Now 1/0/3 appears in the Interface field at the top.
- 5. Enter the following information:
 - In the **Port Priority** field, enter **128**.
 - In the **Port Path Cost** field, enter **0**.
- 6. Click Apply.

Configure PVSTP and PVRSTP

Per VLAN Rapid Spanning Tree Protocol (PVRSTP) is similar to Rapid Spanning Tree Protocol (RSTP) as defined by IEEE 802.1w but with one main difference: PVRSTP runs one instance per VLAN. That is, each configured VLAN runs an independent instance of PVRSTP and each instance elects a root bridge independent of another instance. A region can include as many root bridges as there are VLANs that are configured for PVRSTP. PVRSTP is equivalent to Cisco's RPVST+ and can interoperate with it.

Per VLAN Spanning Tree Protocol (PVSTP) is similar to the Spanning Tree Protocol (STP) as defined by IEEE 802.1d, but with one main difference: PVSTP runs one instance per VLAN. The protocol is equivalent to Cisco's PVST+ and can interoperate with it.

If you enable PVSTP or PVRSTP on a switch, all other spanning tree modes on the switch become disabled. The difference between Multiple Spanning Tree Protocol (MSTP) and PVSTP or PVRSTP lies primarily in the way that the protocol maps spanning tree instances to VLANs: PVSTP or PVRSTP creates a spanning tree instance for each VLAN, whereas MSTP maps one or more VLANs to each Multiple Spanning Tree (MST) instance.

If a switch that runs PVRSTP receives PVSTP Bridge Protocol Data Units (BPDUs), the switch falls back from PVRSTP to PVSTP after its migration-delay timer expires.

A switch that runs PVSTP or PVRSTP transmits IEEE spanning tree BPDUs along with Shared Spanning Tree Protocol (SSTP) BPDUs. The SSTP BPDU are transmitted as untagged packets on an access or native VLAN and transmitted as tagged packets on other VLANs. If a switch that runs PVSTP or PVRSTP receives IEEE spanning tree BPDUs, the switch include them in an access VLAN instance or native VLAN instance.

The Per VLAN Spanning Tree (PVST) behavior is as follows:

- An access port sends IEEE spanning tree BPDUs.
- A trunk port sends IEEE spanning tree BPDUs and SSTP BPDUs on the native VLAN. For other VLANs, the trunk port transmits SSTP BPDUs as tagged packets with the respective VLAN. If the trunk port receives IEEE spanning tree BPDUs, the received BPDUs are processed by the instance that is mapped to the native VLAN. The SSTP BPDUs are processed by instances to which the respective VLANs are mapped.

If a switch that is running an IEEE standard spanning tree protocol (such as STP, RSTP, or MSTP) receives SSTP BPDUs, the switch does not treat them as standard BPDUs. Instead, the incoming SSTP BPDUs are flooded to all the ports of the corresponding VLAN. As a comparison, incoming STP BPDUs are multicasted over the region.

A switch that runs an IEEE standard spanning tree protocol uses its Common and Internal Spanning Tree (CIST) to communicate with a switch that runs PVSTP or PVRSTP. On the other hand, a switch that runs PVSTP or PVRSTP uses an access VLAN instance or native VLAN instance to communicate with a switch that runs an IEEE standard spanning tree protocol.

PVRSTP embeds support for the FastUplink feature to speed up the selection of a new root and the FastBackbone feature to speed up the selection of indirect ports. You do not need to configure these features for RVRSTP. However, for PVSTP, you need to configure these features:

- **FastUplink**. This feature allows for a quick selection of a port with the lowest cost after the root port fails. That is, FastUplink reduces the converge time after a link fails. This feature is similar to Cisco's UplinkFast feature. If the primary link fails, FastUplink creates an alternate path immediately, speeding up the transition from the failed primary link to the backup link.
- **FastBackbone**. This feature allows for faster convergence time when an indirect link to the root fails. If a root port or blocked port receives an inferior BPDU from the designated switch, the switch acts as if an indirect link to the root failed. To speed up the convergence time, the switch expires the maximum age timer immediately and forces the port through the Listening and Learning states.

Note: A M6100 series switch support 32 PVSTP or PVRSTP instances. A M5300 series switch supports 5 PVSTP or PVRSTP instances.

The following diagram shows a simple PVSTP configuration.



Figure 55. PVSTP configuration

CLI: Configure PVSTP

You must configure PVSTP on Switch 1 and Switch 2. This example assumes that all switches can support PVSTP.

CLI: Configure PVSTP on Switch 1

- 1. Ensure that ports 1/0/1 and 1/0/2 are in VLAN 1002 in tagged mode because BPDU packets for PVSTP are transmitted in tagged packets.
- 2. Enable PVSTP.

(Netgear Switch) #config (Netgear Switch) (Config)#spanning-tree mode pvst

Note: After you enable PVSTP (or PVRSTP) globally, PVSTP (or PVRSTP) is applied to VLANs automatically.

3. Verify the PVSTP status.

```
(Netgear Switch) #show spanning-tree vlan 1002
VLAN 1002
 Spanning-tree enabled protocol pvst
RootID
         Priority 33770
         Address
                      6C:B0:CE:19:AE:3D
         Cost
                      20000
         Port
                      1(1/0/1)
         Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
                      33770 (priority 32768 sys-id-ext 1002)
BridgeID Priority
         Address
                      6C:B0:CE:F9:F6:E0
         Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
         Aging Time 300 sec
Interface Role
                   Sts
                                Cost
                                            Prio.Nbr
                   ----- -----
                               20000
1/0/1
        Root
                  Forwarding
                                           128.1
1/0/2 Alternate Discarding 20000
                                           128.2
```

4. Enable the FastUplink and FastBackbone features to speed up the selection of a new root and indirect ports, respectively.

```
(Netgear Switch) (Config)#spanning-tree uplinkfast
(Netgear Switch) (Config)#spanning-tree backbonefast
```

5. To enable the switch to be elected as the root in VLAN 1000, set the PVSTP priority to 0.

(Netgear Switch) (Config)#spanning-tree vlan 1000 priority 0

CLI: Configure PVSTP on Switch 2

- 1. Ensure that ports 1/0/1 and 1/0/2 are in VLAN 1002 in tagged mode because BPDU packets for PVSTP are transmitted in tagged packets.
- 2. Enable PVSTP.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#spanning-tree mode pvst
```

3. Verify the PVSTP status.

```
(Netgear Switch) #show spanning-tree vlan 1002
VLAN 1002
Spanning-tree enabled protocol pvst
        Priority 33770
RootID
        Address
                    6C:B0:CE:19:AE:3D
        Cost
                     0
                     This switch is the root
        Port
        Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
BridgeID Priority 33770 (priority 32768 sys-id-ext 1002)
        Address
                     6C:B0:CE:19:AE:3D
        Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
        Aging Time 300 sec
Interface Role
                  Sts
                          Cost
                                        Prio.Nbr
_____ _ ____
1/0/1
        Designated Forwarding
                              20000
                                         128.1
1/0/2 Designated Forwarding 20000
                                          128.
```

4. Enable the FastUplink and FastBackbone features to speed up the selection of a new root and indirect ports, respectively.

```
(Netgear Switch) (Config)#spanning-tree uplinkfast
(Netgear Switch) (Config)#spanning-tree backbonefast
```

Web Interface: Configure PVSTP

You must configure PVSTP on Switch 1 and Switch 2. This example assumes that all switches can support PVSTP.

Web Interface: Configure PVSTP on Switch 1

- 1. Ensure that ports 1/0/1 and 1/0/2 are in VLAN 1002 in tagged mode because BPDU packets for PVSTP are transmitted in tagged packets.
- 2. Enable PVSTP.
 - a. Select Switching > STP > Basic > STP Configuration.

Syste	em Si	witching	Routing	QoS	Security	M	onitoring	1	Maintenance	Help	Index
VLAN	Auto-VoIP	iSCSI	STP Multicast	MVR	Address Table	Ports	LAG	MLAG	MRP		5) (C.
	STP		STP Configuration								
Basic		^	Spanning Tree A	dmin Mo	de	O Dis	able 🖲 I	Enable			
• STP	Configuration		Force Protocol V	ersion		IEE	E 802.1	d 🔘 IEE	E 802.1w O IEEE	E 802.1s 💿 F	VST @ RPVST
· Advanc	ed	~	Configuration Na	me		6C-B0	-CE-F9-F	F6-E0			
			Configuration Re	vision Le	vel	0			(0 to 65535)		
			Forward BPDU	vhile STF	Disabled	• Dis	able 🔘	Enable			
			BPDU Guard			Dis	able 🔘 I	Enable			
			BPDU Filter			Dis	able 🔘 I	Enable			
			Configuration Dig	gest Key		Oxac3	6177f502	283cd4b	83821d8ab26de62		
			Configuration Fo	rmat Sele	ector	0					
			Fast Backbone			Dis	abled 🔘	Enable	d		
			Fast Uplink			Dis	abled 🔘	Enable	d		
			Max Update Rat	е		150			(0 to 32000 p	ackets/sec. [)efault: 150.)

A screen similar to the following displays.

- **b.** Configure the following settings:
 - For Spanning Tree Admin Mode, select the **Enable** radio button.
 - For Force Protocol Version, select the **PVST** radio button.
- c. Click Apply.

Note: After you enable PVST globally, PVST is applied to VLANs automatically.

- 3. Display the PVST status for port 1/0/1 and 1/0/2 in VLAN 1002.
 - a. Select Switching > STP > Advanced > PVST Interface.

Syst	em 📑	Switching		Routing	QoS	Security	Monitori	ng	Maintenanc	e Help	Index
VLAN	Auto-VolP	iSCSI	STP	Multicas	t MVR	Address Table	Ports LAG	MLAG	MRP		
	100560200	_	-								
	STP		PVSI/	RPVS1 Inte	erface Conf	iguration					
 Basic 		~	VLA	N ID	1002	*					
· Advanc	ed	^	12	3 LAG All							
• STP	Configuratio	n		Interface	Priority		Cost		Role	Status	
•CST	Configuratio	m									
•CST	Port Configu	uration		1/0/1	128		20000		Root	Forwarding	
•CST	Port Status			1/0/2	128		20000		Alternate	Discarding	
	o c			1/0/3	128		0				
•MS1	Configuratio	on		1/0/4	128		0				
• MST	Port Status			1/0/5	128		0				
• STP	Statistics			1/0/6	128		0				
D) (C)	TARAN			1/0/7	128		0				
•PVS	I VLAN	_		1/0/8	128		0				
• PVS	T Interface			1/0/9	128		0				
• PVS	T Statistics			1/0/10	128		0				
				1/0/11	128		0				
				1/0/12	128		0				
				1/0/13	128		0				

b. From the VLAN ID menu, select 1002.

The roles of ports 1/0/1 and 1/0/2 display.

4. To enable the switch to be elected as the root, change the PVST priority to lower value (for example, 0).

a. Select Switching > STP > Advanced > PVST VLAN.

A screen similar to the following displays.

Syst	em S	witching		Routing	QoS		Security	Monitoring	Mair	ntenance	Help	Index
VLAN	Auto-VoIP	iSCSI		Multicast	MVR	Addre	ss Table I	Ports LAG	MLAG N	IRP		
	STP		PVST/F	RPVST VLA	N Configu	ation						
Basic		~		VLAN ID	Root		Hello Time	Forward Time	Max Age	Priority		
• Advanc	ed	~		1002	None	~	2	15	20	0		
•STP	Configuration			1	None		2	15	20	32768		
•CST	Configuration			1002	None		2	15	20	32768		
•CST	Port Configur	ation										
•CST	Port Status											
•MST	Configuration	6										
•MST	Port Status											
•STP	Statistics											
• PVS	T VLAN											
•PVS	T Interface											
·PVS	T Statistics											

b. Select the 1002 check box for VLAN ID 1002.

The settings for VLAN ID 1002 display in the fields in the table heading.

- c. In the Priority field, enter 0.
- d. Click Apply.

Web Interface: Configure PVSTP on Switch 2

- 1. Ensure that ports 1/0/1 and 1/0/2 are in VLAN 1002 in tagged mode because BPDU packets for PVSTP are transmitted in tagged packets.
- 2. Enable PVSTP.
 - a. Select Switching > STP > Basic > STP Configuration.

A screen similar to the following displays.

Syst	em 🗾	Switching	Routing	QoS	Security	M	onitoring		Maintenance	Help	Index
VLAN	Auto-VolP	iscsi	STP Multicast	MVR	Address Table	Ports	LAG	MLAG	MRP		
	STP		STP Configuration								
Basic		^	Spanning Tree A	dmin Mod	le	O Dis	able 🖲 E	Enable			
• STP	Configuratio	n	Force Protocol V	ersion			E 802.10	I 🔘 IEE	E 802.1w 🔘 IEE	E 802.1s 🖲 P	VST RPVST
Advance	ed	~	Configuration Na	ame		6C-B0	-CE-19-A	E-3D			
			Configuration Re	evision Le	vel	0			(0 to 65535)		
			Forward BPDU	while STP	Disabled	Dis:	able 🔘 E	nable			
			BPDU Guard			Dis	able 🔘 E	nable			
			BPDU Filter			Dis	able 🔘 E	Inable			
			Configuration Di	gest Key		0xac36	177f502	83cd4b8	33821d8ab26de62		
			Configuration Fo	rmat Sele	ctor	0					
			Fast Backbone			Dis	abled 🔘	Enabled			
			Fast Uplink			Dis:	abled 🍥	Enabled	E.		
			Max Update Rat	e		150			(0 to 32000 p	ackets/sec. D)efault: 150.)

- **b.** Configure the following settings:
 - For Spanning Tree Admin Mode, select the **Enable** radio button.
 - For Force Protocol Version, select the **PVST** radio button.
- c. Click Apply.

Note: After you enable PVST globally, PVST is applied to VLANs automatically.

- 3. Display the PVST status for ports 1/0/1 and 1/0/2 in VLAN 1002.
 - a. Select Switching > STP > Advanced > PVST Interface.

Syst	tem 🛛	Switching		Routing	QoS	Security	M	onitoring		Maintenance	Help	Index
VLAN	Auto-VoIP	iscsi		Multicas	t MVR	Address Table	Ports	LAG	MLAG	MRP		
	STP		PVST/	RPVST Inte	erface Conf	iguration						
Basic		~	VLA	N ID	1002	*						
• Advance	ced	~	12	LAG AII								
• STP	Configuratio	n		Interface	Priority		Cost			Role	Status	
·CST	Configuratio	n										
•CST	Port Config	uration		1/0/1	128		20000			Designated	Forwarding	
•CST	Port Status			1/0/2	128		20000			Designated	Forwarding	
001	T OIT OTATUS			1/0/3	128		0					
• MS1	Configuratio	on		1/0/4	128		0					
• MST	Port Status			1/0/5	128		0					
• STP	Statistics			1/0/6	128		0					
D1 (0	T 1 // A 1			1/0/7	128		0					
•PVS	I VLAN			1/0/8	128		0					
• PVS	T Interface			1/0/9	128		0					
• PVS	T Statistics			1/0/10	128		0					
				1/0/11	128		0					
				1/0/12	128		0					
				1/0/13	128		0					

b. From the VLAN ID menu, select 1002.

The roles of ports 1/0/1 and 1/0/2 display.

Tunnels for IPv6



6in4 tunnels and 6to4 tunnels

This chapter includes the following sections:

- Tunnel Concepts
- Create a 6in4 Tunnel
- Create a 6to4 Tunnel

Note: IPv6 tunnels are available on M5300 and M6100 series switches only. However, the following M5300 series switches require a license to support IPv6 tunnels: M5300-28G, M5300-52G, M5300-28G-POE+, and M5300-52G-POE+.

Tunnel Concepts

Two methods exist for IPv6 sites to communicate with each other over the IPv4 network: 6in4 tunnel and 6to4 tunnel. The 6in4 tunnel encapsulates IPv6 traffic over an explicitly configured IPv4 destination or end port of the tunnel with the IP protocol number set to 41. The 6to4 tunnel IPv6 prefix is constructed by prepending 2002 (hexadecimal) to the global IPv4 address. For example, if the IPv4 address is 4.4.4.1, the tunnel IPv6 prefix would be 2002:404:401::/16.

The 6to4 tunnels are automatically formed IPv4 tunnels carrying IPv6 traffic. The automatic tunnel's IPv4 destination address is derived from the 6to4 IPv6 address of the tunnel's next hop. A 6to4 tunnel supports the functionality of a 6to4 border router that connects a 6to4 site to a 6to4 domain. With 6to4 tunnels, routers in a 6to4 domain, including other 6to4 border routers and 6to4 relay routers, can send and receive tunneled traffic from each other.

Create a 6in4 Tunnel

In the example, you create a 6in4 tunnel between Switch 1 and Switch 2. The tunnel carries IPv6 packets over IPv4 packets.



Figure 56. 6in4 tunnel configuration

CLI: Create a 6in4 Tunnel

You must configure Switch 1 and Switch 2.

CLI: Create a 6in4 Tunnel on Switch 1

```
(Netgear Switch) #config
(Netgear Switch) (Config) #ip routing
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1) #routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.1.1 255.255.255.0
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface tunnel 0
(Netgear Switch) (Interface tunnel 0)#ipv6 enable
(Netgear Switch) (Interface tunnel 0)#ipv6 address 2000::1/64
(Netgear Switch) (Interface tunnel 0)#tunnel mode ipv6ip
(Netgear Switch) (Interface tunnel 0)#tunnel source 192.168.1.1
(Netgear Switch) (Interface tunnel 0)#tunnel destination 192.1.168.1.2
(Netgear Switch) (Interface tunnel 0)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #show interface tunnel 0
Interface Link Status..... Up
IPv6 is enabled
IPv6 Prefix is ..... FE80::COA8:101/128
                                           2000::1/64
MTU size..... 1280 bytes
(Netgear Switch) #show interface tunnel
TunnelId Interface
                    TunnelMode
                                         SourceAddress DestinationAddress
_____
           _____
                      _____
                                         _____
                                                          _____
0
  tunnel 0
                        6 in 4 Configured 192.168.1.1
                                                           192.168.1.2
(Netgear Switch) # ping ipv6 2000::2
Send count=3, Receive count=3 from 2000::2
Average round trip time = 1.00 ms
```

CLI: Create a 6in4 Tunnel on Switch 2

```
(Netgear Switch) #config
(Netgear Switch) (Config) #ip routing
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13) #routing
(Netgear Switch) (Interface 1/0/13)#ip address 192.168.1.2 255.255.255.0
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#interface tunnel 0
(Netgear Switch) (Interface tunnel 0)#ipv6 enable
(Netgear Switch) (Interface tunnel 0)#ipv6 address 2000::2/64
(Netgear Switch) (Interface tunnel 0)#tunnel mode ipv6ip
(Netgear Switch) (Interface tunnel 0)#tunnel source 192.168.1.2
(Netgear Switch) (Interface tunnel 0)#tunnel destination 192.168.1.1
(Netgear Switch) (Interface tunnel 0)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #show interface tunnel
TunnelId Interface TunnelMode
                                      SourceAddress DestinationAddress
0 tunnel 0
                    6 in 4 Configured 192.168.1.2
                                                       192.168.1.1
```

Web Interface: Create a 6in4 Tunnel

You must configure Switch 1 and Switch 2.

Web Interface: Create a 6in4 Tunnel on Switch 1

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

System		witching		Routing		QoS	Secur	ity	Monitoring		Maintenance	Help	Index
Routing Table	P	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast	
IP			IP Con	figuratio	1								
•Basic		^	Defau	It Time	to Live				64				
• IP Configurat	tion		Routi	ng Mode	í.				Enable	e 🔘 Disat	ble		
 Statistics 			ICMP	Echo R	eplies				Enable	e 🔘 Disab	ble		
 Advanced 		Y	ICMP	Redired	ts				Enable	e 🔘 Disat	ble		
			ICMP	Rate Li	mit Inte	rval			1000		(0 to 21	47483647 ms)	
			ICMP	Rate Li	mit Bur	st Size			100		(1 to 20	10)	
			Maxir	num Ne	xt Hops	5			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.

System	Switching		Routing		QoS	Securi	y M	Monitoring	Ma	iintenance	Help	Index
Routing Table I	IP IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router D	iscovery '	VRRP	Multicast	IPv6 Multicast	
IPv6		IPv6 G	lobal Co	nfigurat	ion							
Basic	^	IPv6 I	Unicast I	Routing) Disable	Enable				
 Global Configur 	ration	Hop l	_imit				64		(1 to 255)		
*Route Table		ICMF	v6 Rate	Limit E	rror Interva	al	1000		(0 to 214	7483647 m	isecs)	
 Advanced 	×	ICMF	v6 Rate	Limit B	urst Size		100		(1 to 200	U)		

- **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.

System	S	witching		Routin		QoS	Security	y Monitorir	ig 🛛	Maintenance	Help	Index		
Routing Table	IP.	IPv6	VLAN	I ARF	RIP	OSPF	OSPFv3	Router Discovery	VRRF	P Multicast	IPv6 Multicast			
IP •Basic		~	IP Int	erface C	onfigurat	ion								
Dasic			12	3 VLAN	IS All									
 Advanced IP Configurat 	ion	~		Port	Descrip	tion	VLAN ID	IP Address Confi Method	guration	IP Address	Subnet Mask	Ro Mo	uting ide	Administrative Mode
 Statistics 				1/0/1				Manual 🗸		192.168.1.1	255.255.25	5.0 E	nable 🗸	Enable ~
• IP Interface				1/0/1				None		0.0.0.0	0.0.0.0	En	able	Enable
Configuration	9			1/0/2				None		0.0.0.0	0.0.0.0	Dis	able	Enable
 Secondary IF)			1/0/3				None		0.0.0.0	0.0.0.0	Dis	able	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.

System Switching		Routing	QoS	Security	Monitoring	Maintenance He	ip Index	0			
Routing Table IP IP/6	VLAN	ARP	RIP OSPF	OSPFv3 Route	r Discovery V	/RRP Multicast IPv6 I	Aulticast				202
IPv6	Tunne	l Configura	ation							Vod Delete Cancel	Apply
Basic Advanced		Tunnel	Mode	IPv6 Mode	IPv6 Unreachables	IPv6 Address/Prefix Leng	th EUI64	Source Address	Source Interface	Destination Address	Inte
Global Configuration		0 ~	6-in-4-configure	d 👻 Enable 👻	Enable 👻	2000::1/64	v V	192.168.1.1	· ·	✓ 192.168.1.2	
Interface Configuration Prefix Configuration Statistics Neighbour Table Static Pointe											
Configuration											
Route Table											
Koute Protetting Tunnel Configuration											

- b. In the Tunnel ID list, select 0.
- c. In the Mode field, select 6-in-4-configured.
- d. In the Source Address field, enter 192.168.1.1.
- e. In the IPv6 Mode field, select Enable.
- f. In the IPv6 Address/Prefix Length field, enter 2000::1/64.
- g. In the Destination Address field, enter 192.168.1.2.
- h. Click Apply.

Web Interface: Create a 6in4 Tunnel on Switch 2

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

System	Sv	vitching	line -	Routing		QoS	Securi	iy	Monitorin	g	Maintenance	Help	Index
Routing Table	IP .	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast	2
IP			IP Con	figuratior	1								
• Basic		^	Defau	lt Time t	o Live				64				
• IP Configuration	on		Routi	ng Mode					Enabl	e 🔘 Disa	ble		
 Statistics 			ICMP	Echo R	eplies				Enabl	e 🔘 Disa	ble		
 Advanced 		~	ICMP	Redirec	ts				Enable	e 🔘 Disa	ble		
			ICMP	Rate Li	nit Inte	rval			1000		(0 to 21	47483647 ms)	
			ICMP	Rate Li	nit Bur	st Size			100		(1 to 20	00)	
			Maxir	num Nex	kt Hops	r.			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.

System	Switching	9	Routing		QoS	Securit	y Monitoring		Maintenance	Help	Index
Routing Table	IP IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast	
IPve	5	IPv6 G	lobal Co	nfigurat	ion						
Basic	^	IPv6	Unicast I	Routing	l.	(🔵 Disable 💿 Enable				
Global Config	juration	Hop I	_imit				64	(1 to 2	55)		
 Route Table 		ICMF	V6 Rate	Limit E	rror Interv	al	1000	(0 to 2	147483647 n	isecs)	
 Advanced 	Ŷ	ICMF	V6 Rate	Limit B	urst Size		100	(1 to 2	001		

- **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.

System	S۱	witching		Routin	g	QoS	Securit	y Monitoring	Maintenance	Help	Index	
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery VR	RP Multicast	IPv6 Multicast		
IP • Basic		~	IP International IP Int	erface Ci 3 VLAN:	onfigurat S All	ion						
 Advanced IP Configuration 	on	^		Port	Descrip	tion	VLAN ID	IP Address Configuratio Method	ⁿ IP Address	Subnet Mask	Routing Mode	Administrative Mode
 Statistics 				1/0/13				Manual ~	192.168.1.2	255.255.255.	0 Enable Y	Enable Y
IP Interface Configuration				1/0/1				None	0.0.0.0	0.0.0.0	Enable	Enable
 Secondary IF 		2		1/0/2				None	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.

System Switching		Routing	Q	loS	Security		Monitoring	Main	lenance	Help	In	dex						
Routing Table IP IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router	Discovery	VRRP	Multicast:	IPv6 Mu	ticast		-X-					-
IPv6	Tunnel	Configura	tion												Add	Delete	Cancel	Apply
Basic Advanced	-	Tunnel ID	Mode		IPve	6 Mode	IPv6 Unreachables	IPv6 A	ddress/Pre	efix Length	EUI64		Source Address	Source Interface		Destination A	Address	Inte
Global Configuration		0 ~	6-in-4-	-configured	✓ Ena	abie 🛩	Enable 👻	2000	2/64	1.		¥	192.168.1.2		¥	192.168.1.1		
Prefix Configuration Statistics Neighbour Table Static Route Configuration Brute Table																		
Route Preference																		
Tunnel Configuration																		

- **b.** In the **Tunnel Id** list, select **0**.
- c. In the Mode list, select 6-in-4-configured.
- d. In the IPv6 Address/Prefix Length field, enter 2000::2/64.
- e. In the Source Address field, enter 192.168.1.2.
- f. In the Destination Address field, enter 192.168.1.1.
- g. Click Apply.

Create a 6to4 Tunnel

An IPv6 tunnel in 6to4 mode connects an isolated IPv6 domain (that is, an 6to4 island) over an IPv4 domain to remote IPv6 domains or to another 6to4 island. An IPv6 tunnel in 6to4 mode is also called an automatic 6to4 tunnel. Unlike a 6in4 tunnel, which is a point-to-point tunnel, a 6to4 tunnel is a point-to-multipoint tunnel. In a 6to4 tunnel, the IPv6 tunnel destination is determined by the IPv4 address, which is extracted from IPv6 destination address with the prefix 2002::V4ADDR::/48.

A NETGEAR switch behaves as a 6to4 border router that connects 6to4 islands (in the following figure, Switch 1 and Switch 2) to an IPv6 domain (in the following figure, Switch 3). This means the following:

The NETGEAR switch forwards traffic from an IPv6 domain (with a non-2002:: address) to a 6to4 island (with a 2002:: address) and the other way around. (In the following figure, this type of forwarding refers to the traffic between Switch 1 and Switch 3 and the traffic between Switch 2 and Switch 3).

The NETGEAR switch forwards traffic from one 6to4 island to another 6to4 island (in the following figure, the traffic between Switch 1 and Switch 2).

The NETGEAR switch does not forward traffic from one IPv6 domain (with a non-2002:: address) to other IPv6 domain (also with a non-2002:: address).



Figure 57. 6to4 tunnel configuration

Note: The following examples do not include the configuration of the IPv4 switch because the 6to4 configuration occurs only in the IPv6 island. The switch in IPv4 domain does not require any special configuration.

CLI: Create a 6to4 Tunnel

You must configure Switch1, Switch2, and Switch 3.

CLI: Create a 6to4 Tunnel on Switch 1

1. Enable routing and IPv6 routing on Switch 1.

(Netgear Switch) # config (Netgear Switch) (Config)#ipv6 unicast-routing (Netgear Switch) (Config)#ip routing

2. Configure IPv4 address on routing port 1/0/1.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 195.1.3.2 255.255.255.0
(Netgear Switch) (Interface 1/0/1)#exit
```

3. Configure the IPv6 address on the 6to4 tunnel in the format 2002:V4ADDR::Host/16, in which where V4ADDR is the source IPv4 address of the tunnel. The prefix length for the tunnel must be 16.

```
(Netgear Switch) (Config)#interface tunnel 0
(Netgear Switch) (Interface tunnel 0)#ipv6 address 2002:c301:302::1/16
(Netgear Switch) (Interface tunnel 0)#ipv6 enable
(Netgear Switch) (Interface tunnel 0)#tunnel mode ipv6ip 6to4
(Netgear Switch) (Interface tunnel 0)#tunnel source 195.1.3.2
(Netgear Switch) (Interface tunnel 0)#exit
```

4. Configure the IPv6 address for routing port 1/0/3. The IPv6 address format is 2002:V4ADDR:Subnet::Host/64, in which V4ADDR is the source IPv4 address of the tunnel and Subnet is the subnet of 2002:V4ADDR::/64.

(Netgear Switch) (Config)#interface 1/0/3 (Netgear Switch) (Interface 1/0/3)#routing (Netgear Switch) (Interface 1/0/3)#ipv6 address 2002:c301:302:1::1/64 (Netgear Switch) (Interface 1/0/3)#ipv6 enable (Netgear Switch) (Interface 1/0/3)#exit

 Create a static IPv4 route to ensure that Switch 1 can reach Switch 2 and Switch 3. You can also use a routing protocol such as RIP or OSPF to let Switch 1 learn the routes from Switch 2 and Switch 3.

(Netgear Switch) (Config)#ip route 195.1.4.0 255.255.255.0 195.1.3.1 (Netgear Switch) (Config)#ip route 195.1.5.0 255.255.255.0 195.1.3.1

6. Because Switch 1 cannot detect the route for IPv6 address 8888::/16 (of port 2/0/24 on Switch 3), create a static IPv6 route for Switch 1 with the tunnel address of Switch 3 as the next hop.

(Netgear Switch) (Config)#ipv6 route 8888::/16 2002:c301:502::1

7. Verify the configuration.

```
(Netgear Switch) #show ipv6 route
IPv6 Routing Table - 5 entries
Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
      O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
      ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2
    2002::/16 [0/0]
С
     via ::, tunnel 0
С
  2002:c301:302:1::/64 [0/0]
     via ::,
              1/0/3
6To4 2002:c301:402::/48 [1/0]
     via fe80::c301:301,
                          01h:25m:23s, tunnel 0
6To4 2002:c301:502::/48 [1/0]
     via fe80::c301:301, 00h:44m:11s, tunnel 0
    8888::/16 [1/0]
S
     via 2002:c301:502::1, tunnel 0
```

CLI: Create a 6to4 Tunnel on Switch 2

1. Enable routing and IPv6 routing on Switch 2.

(Netgear Switch) # config (Netgear Switch) (Config)#ipv6 unicast-routing (Netgear Switch) (Config)#ip routing

2. Configure the IPv4 address on routing port 2/0/1.

```
(Netgear Switch) (Config)# interface 2/0/1
(Netgear Switch) (Interface 2/0/1)#routing
(Netgear Switch) (Interface 2/0/1)#ip address 195.1.4.2 255.255.255.0
(Netgear Switch) (Interface 2/0/1)#exit
```

 Configure the IPv6 address on the 6to4 tunnel in the format 2002:V4ADDR::Host/16, in which where V4ADDR is the source IPv4 address of the tunnel. The prefix length for the tunnel must be 16.

```
(Netgear Switch) (Config)#interface tunnel 0
(Netgear Switch) (Interface tunnel 0)#ipv6 address 2002:c301:402::1/16
(Netgear Switch) (Interface tunnel 0)#ipv6 enable
(Netgear Switch) (Interface tunnel 0)#tunnel mode ipv6ip 6to4
(Netgear Switch) (Interface tunnel 0)#tunnel source 195.1.4.2
(Netgear Switch) (Interface tunnel 0)#exit
```

4. Configure the IPv6 address for routing port 2/0/3. The IPv6 address format is 2002:V4ADDR:Subnet::Host/64, in which V4ADDR is the source IPv4 address of the tunnel and Subnet is the subnet of 2002:V4ADDR::/64.

(Netgear Switch) (Config)#interface 2/0/3 (Netgear Switch) (Interface 2/0/3)#routing (Netgear Switch) (Interface 2/0/3)#ipv6 address 2002:c301:402:1::1/64 (Netgear Switch) (Interface 2/0/3)#ipv6 enable (Netgear Switch) (Interface 2/0/3)#exit

5. Create a static IPv4 route to ensure that Switch 2 can reach Switch 1. You can also use a routing protocol such as RIP or OSPF to let Switch 2 learn the route from Switch 1.

(Netgear Switch) (Config)#ip route 195.1.3.0 255.255.255.0 195.1.4.1

6. Verify the configuration.

CLI: Create a 6to4 Tunnel on Switch 3

1. Enable routing and IPv6 routing on Switch 3.

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

2. Configure IPv4 address on routing port 2/0/1.

```
(Netgear Switch) (Config)# interface 2/0/1
(Netgear Switch) (Interface 2/0/1)#routing
(Netgear Switch) (Interface 2/0/1)#ip address 195.1.5.2 255.255.0
(Netgear Switch) (Interface 2/0/1)#exit
```

3. Configure the IPv6 address on the 6to4 tunnel in the format 2002:V4ADDR::Host/16, in which where V4ADDR is the source IPv4 address of the tunnel. The prefix length for the tunnel must be 16.

```
(Netgear Switch) (Config)#interface tunnel 0
(Netgear Switch) (Interface tunnel 0)#ipv6 address 2002:c301:502::1/16
(Netgear Switch) (Interface tunnel 0)#ipv6 enable
(Netgear Switch) (Interface tunnel 0)#tunnel mode ipv6ip 6to4
(Netgear Switch) (Interface tunnel 0)#tunnel source 195.1.5.2
(Netgear Switch) (Interface tunnel 0)#exit
```

4. Configure a global IPv6 address on routing port 2/0/1.

```
(Netgear Switch) (Config)#interface 2/0/24
(Netgear Switch) (Interface 2/0/24)#routing
(Netgear Switch) (Interface 2/0/24)#ipv6 address 8888::1/64
(Netgear Switch) (Interface 2/0/24)#ipv6 enable
(Netgear Switch) (Interface 2/0/24)#exit
```

5. Create a static IPv4 route to ensure that Switch 3 can reach Switch 1. You can also use a routing protocol such as RIP or OSPF to let Switch 3 learn the route from Switch 1.

(Netgear Switch) (Config)#ip route 195.1.3.0 255.255.255.0 195.1.5.1

6. Verify the configuration.

Web Interface: Create a 6to4 Tunnel

You must configure Switch1, Switch2, and Switch 3.

Web Interface: Create a 6to4 Tunnel on Switch 1

- 1. Enable IP routing on Switch 1.
 - a. Select Routing > IP > Basic > IP Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Ma	intenance	Help	Index
Routing Table	IP IPv6	VLAN ARP	RIP OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast	
IP		IP Configuration							
Basic	^	Default Time to	Live		64				
 IP Configuration 	on	Routing Mode			Enable	Disable	e		
Statistics		ICMP Echo Re	plies		Enable	O Disable	9		
Advanced	*	ICMP Redirects	S		Enable	Disable	е		
		ICMP Rate Lim	iit Interval		1000		(0 to 2	2147483647 ms)	
		ICMP Rate Lim	iit Burst Size		100		(1 to 2	200)	
		Maximum Next	Hops		16				
		Maximum Rout	es		12288				
		Maximum Stati	c Routes		512				
		Select to config	jure Global Defa	ult Gateway					
		Global Default	Gateway		0.0.0.0				

- **b.** For Routing Mode, select the **Enable** radio button.
- c. Click Apply.
- 2. Enable IPv6 forwarding and unicast routing on Switch 1.
 - a. Select Routing > IPv6 > Basic> Global Configuration.

System	Switching	Rout	ting	QoS	Security	Monitoring	Ma	intenance	Help	Index
Routing Table	IP IPv6	VLAN A	RP RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicas	st
IPv6		IPv6 Global	Configurat	lion						
Basic	^	IPv6 Unio	ast Routin	g	(Disable Enable				
Global Configu	ration	Hop Limit	t			64	(1 to	o 255)		
Route Table		ICMPv6	Rate Limit	Error Interv	/al	1000	(0 to	214748364	7 msecs)	
Advanced	~	ICMPv6 I	Rate Limit	Burst Size		100	(1 to	o 200)		

- **b.** For IPv6 Unicast Routing, select the **Enable** radio button.
- c. Click Apply.
- 3. Create a routing interface and assign an IP address to it.

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

A screen similar to the following displays.

System	Swit	tching		Routing	9	JoS	Security	Monitoring	Maintenance	Help	Index	
Routing Table	IP I	Pv6	VLAN	ARF	RIP	OSPF	OSPFv3	Router Discovery	VRRP Multicast	IPv6 Multicast		
IP		1	IP Inte	erface Cr	onfiguratio	n						
Basic		~	12	3 All								
Advanced IP Configuration	n	^		Port	Descripti	on	VLAN ID	IP Address Configurat Method	tion IP Address	Subnet Mask	Routing Mode	Administrative Mode
Statistics				1/0/1				Manual 👻	195.1.3.2	255.255.255	5.0 Enable v	Enable 🗸
. IP Interface				1/0/1				None	0.0.0.0	0.0.0.0	Disable	Enable
Configuration				1/0/2				None	0.0.0.0	0.0.0.0	Disable	Enable
Secondary IP				1/0/3				None	0.0.0	0.0.0.0	Disable	Enable
350				1/0/4				None	0.0.0.0	0.0.0.0	Disable	Enable
				1/0/5				None	0.0.0.0	0.0.0.0	Disable	Enable
			0	1/0/5				None	0.0.0.0	0.0.0.0	Disable	Enable

b. Select the **1/0/1** check box for port 1/0/1.

The settings for port 1/0/1 display in the fields in the table heading.

- **c.** Configure the following settings:
 - In the IP Address Configuration Method field, select Manual.
 - In the IP Address field, enter 195.1.3.2.
 - In the Subnet Mask field, enter 255.255.255.0.
 - In the Routing Mode field, select Enable.
- d. Click Apply.
- 4. Create an IPv6 routing interface.
 - a. Select Routing > IPv6 > Advanced > Interface Configuration.

A screen similar to the following displays.

System S	witching		Routing	QoS	Security	Monitoring	Mainte	nance	ŀ	lelp I	ndex
Routing Table IP	IPv6	VLAN	ARP	RIP OSPI	F OSPFv3	Router Discovery	VRRP N	lulticast	IPv6	Multicast	
IPv6		IPv6 I	nterface Co	onfiguration							
Basic	Ý	12	3 All								
Advanced Global Configurati	^ on		Interface	IPv6 Mode	DHCPv6 Client Mode	Stateless Address AutoConfig Mode	Routing Mode	Admin Mode		Operational Mode	MTU
Interface Configure	ation		1/0/3	Enable 🗸	Disable 🗸	Disable 🗸	Enable 🗸	Enable	~	Disable	1500
Prefix Configuration	on		1/0/1	Disable Disable	Disable Disable	Disable Disable	Enable Disable	Enable		Disable Disable	1500
Statistics			1/0/3	Disable	Disable	Disable	Disable	Enable		Disable	1500
Neighbour Table			1/0/4	Disable	Disable	Disable	Disable	Enable		Disable	1500
Static Route			1/0/5	Disable	Disable	Disable	Disable	Enable		Disable	1500
Configuration			1/0/6	Disable	Disable	Disable	Disable	Enable		Disable	1500
Route Table			1/0/7	Disable	Disable	Disable	Disable	Enable		Disable	1500
• Route Preference			1/0/8	Disable	Disable	Disable	Disable	Enable		Disable	1500
Troute i Telefence			1/0/9	Disable	Disable	Disable	Disable	Enable		Disable	1500
Iunnel Configurati	ion		1/0/10	Disable	Disable	Disable	Disable	Enable		Disable	1500

b. Select the **1/0/3** check box for port 1/0/3.

The settings for port 1/0/3 display in the fields in the table heading.

- c. Configure the following settings:
 - In the IPv6 Mode field, select Enable.
 - In the **Routing Mode** field, select **Enable**.
- d. Click Apply.
- 5. Configure the IPv6 address for IPv6 routing interface 1/0/3.
 - a. Select Routing > IPv6 > Advanced > Prefix Configuration.

A screen similar to the following displays.

System	Switching		Routing		QoS	Security	Monitoring	M	aintenance	Help	Index
Routing Table	IP IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicas	st
IPv6		IPv6 I	nterface S	electio	<u>n</u>						
Basic	~	Inte	rface	J.	1/0/3 🗸						
Advanced	~										
Global Configure	ration										
Interface Config	guration	IPv6 I	nterface C	onfigur	ation						
Prefix Configure	ation		A KIN I				100 - 11 Mar	-	Valid Life		Proformed
Statistics		-	Ipv6 Pref	ix		Prefix Leng	gth E	UI64	Time		Life Time
Neighbour Tabl	e		2002:c30	1:302:1	21	64		Ŷ			
Static Route Configuration			fe80::6eb	0:ceff:	fe19:ae40	64	D	isable			
Route Table											
Route Preferen	ce										

b. From the **Interface** menu, select **1/0/3**.

The settings for port 1/0/3 display in the fields in the table heading.

- **c.** Configure the following settings:
 - In the Ipv6 Prefix field, enter 2002:c301:302:1::1.
 - In the **Prefix Length** field, enter 64.
 - In the EUI64 field, select Disable.
- d. Click Add.
- 6. Create a 6to4 tunnel interface.
 - a. Select Routing > IPv6 > Advanced > Tunnel Configuration.

System Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index	
Routing Table IP IPv6	VLAN ARP	RIP OSPF	OSPFv3 Route	r Discovery	/RRP Multicast II	Pv6 Multicast	t	
IPv6	Tunnel Configura	ation						
Basic Advanced	Tunnel ID	Mode	IPv6 Mode	IPv6 Unreachables	IPv6 Address/Prefix L	ength EUI6	i4 So	urce Address
Global Configuration	0 ~	6-to-4	✓ Enable ✓	v	2002:c301:302::1/16	Disa	able 👻 19	95.1.3.2
Interface Configuration Prefix Configuration Statistics Neighbour Table Static Route Configuration Route Table Route Preference Junnel Configuration								

- **b.** Configure the following tunnel settings:
 - In the **Tunnel ID** field, select **0**.
 - In the Mode field, select 6-to-4.
 - In the IPv6 Mode field, select Enable.
 - In the IPv6 Address/Prefix Length field, enter 2002:c301:302::1/16.
 - In the EUI64 field, select Disable.
 - In the **Source Address** field, enter **195.1.3.2**.
- c. Click Add.
- 7. Create a default route for nonnative IPv6 addresses.
 - a. Select Routing > IPv6 > Advanced > Static Route Configuration.

System Switch	hing	Routing	QoS	Security Monitor	ing Mainter	nance Help	Index	
Routing Table IP IP	V6 VLA	N ARP	RIP OSPF	OSPFv3 Router Discov	very VRRP M	ulticast IPv6 Multicast		
IPv6	Cont	figure Routes						
Basic Advanced	×	IPv6 Prefi	x	Prefix Length	Next Hop IPv6 Address Type	Next Hop IPv6 Address	Interface	Preference
Global Configuration		8888::		16	Global 👻	2002:c301:502::1	· · · · ·	
Interface Configuration Prefix Configuration Statistics Neighbour Table	i l							
Static Route Configuration								
Route Table								
Route Preference								
Tunnel Configuration								

- **b.** Configure the following route settings:
 - In the IPv6 Prefix field, enter 8888::.
 - In the **Prefix Length** field, enter **16**.

- In the Next Hop IPv6 Address Type field, select Global.
- In the Next Hop IPv6 Address field, enter 2002:c301:502::1.
- c. Click Add.
- 8. Create a static route for subnet 195.1.4.0/24.
 - a. Select Routing > Routing Table > Advanced > Route Configuration.

System	Sw	itching		Routing		QoS S	Security	Monitorin	g Mai	ntenance	Help	Index			
	IP	IPv6	VLAN	ARP	RIP	OSPF O	SPFv3	Router Discove	ry VRRP	Multica	st IPv6 Multicas	t			
Routing T	Table		Config	jure Routes	1										
Basic		*		Route Typ	e	Network Ar	ddress	Subnet N	lask	Nex	t Hop Address	Preferen	ice	Description	
 Advanced 		^		Static	~	195.1.4.0		255.255.3	255.0	195	1.3.1				
Route Configu	uration				_	12-4									
Route Prefere	inces														
			Learne	d Routes											
			Ne	twork Add	ess S	ubnet Mask	Protocol	Route Type	Next Hop Int	erface 1	Next Hop Address	Preference	Metric		
			19	5.1.3.0	2	55.255.255.0) Local	Connected	1/0/1	1	195.1.3.2	0	1		

- **b.** Configure the following route settings:
 - In the Network Address field, enter 195.1.4.0.
 - In the Subnet Mask field, enter 255.255.255.0.
 - In the Next Hop Address field, enter 195.1.3.1.
- c. Click Add.
- 9. Create a static route for 195.1.5.0/24.
 - a. Select Routing > Routing Table > Advanced > Route Configuration.

System	Swit	tching		Routing		QoS	Security	Monitorir	ng Maint	enance	Help	Index	Ĵ	
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discove	ary VRRP	Multicast	IPv6 Multicas	ţ.		
Routing	Table	1	Config	ure Route	\$									
Basic		~		Route Ty	pe	Network	Address	Subnet &	Mask	Next H	op Address	Preferen	1Ce	Description
Advanced		^		Static	~	195.1.5.0		255.255	255.0	195.1.3	đ			
Route Config	guration			Static		195.1.4.0	<u> </u>	255.255.	255.0	195.1.3	d	1		
Route Prefere	ences													
				1.5										
			Learne	d Routes										
			Ne	twork Add	Iress 3	Subnet Mas	k Protoco	Route Type	Next Hop Inter	face Nex	t Hop Address	Preference	Metric	
			195	5.1.3.0	3	255 255 255	0 Local	Connected	1/0/1	195	1.3.2	0	1	
			195	5140		255 255 255	0 Static	Static	1/0/1	195	1 2 1	4	0	

- **b.** Configure the following route settings:
 - In the Network Address field, enter 195.1.5.0.
 - In the Subnet Mask field, enter 255.255.255.0.
 - In the Next Hop Address field, enter 195.1.3.1.
- c. Click Add.

Web Interface: Create a 6to4 Tunnel on Switch 2

- 1. Enable IP routing on Switch 2.
 - a. Select Routing > IP > Basic > IP Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Main	itenance	Help	Index
Routing Table	IP IPv6	VLAN ARP	RIP OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicas	t
IP	,	IP Configuration							
Basic	^	Default Time to	Live		64				
IP Configura	ation	Routing Mode			Enable	Disable			
Statistics		ICMP Echo Rep	plies		Enable	Disable			
 Advanced 	~	ICMP Redirects	5		Enable	Disable			
		ICMP Rate Limi	iit Interval		1000		(0 to 2	147483647 ms)	
		ICMP Rate Limi	iit Burst Size		100		(1 to 2	00)	
		Maximum Next	Hops		16				
		Maximum Route	es		12288				
		Maximum Static	c Routes		512				
		Select to config	jure Global Defa	ault Gateway					
		Global Default C	Gateway		0.0.0.0				

- **b.** For Routing Mode, select the **Enable** radio button.
- c. Click Apply.
- 2. Enable IPv6 forwarding and unicast routing on Switch 2.
 - a. Select Routing > IPv6 > Basic> Global Configuration.

A screen similar to the following displays.

System	Switching	1	Routing		QoS	Security	Monitoring	Ma	intenance	Help	Index
Routing Table	IP IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicas	st
ID-C		IPv6 Glo	obal Cont	figuratio	n						
IPvo		IT VO OK	obar com	nguratic	-						
Basic	^	IPv6	Unicast F	Routing			Disable Enable	e			
Global Configu	ration	Hop L	_imit				64	(1 t	o 255)		
Route Table		ICMP	v6 Rate	Limit E	rror Interv	al	1000	(0 t	0 214748364	7 msecs)	
Advanced	~	ICMP	u6 Date	Limit B	uret Sizo		100	(01)	0 2001		
		IC WIP	vo Rale	Cinit D	urst Size		100	(10	0 2001		

- **b.** For IPv6 Unicast Routing, select the **Enable** radio button.
- c. Click Apply.
- 3. Create a routing interface and assign an IP address to it.
 - a. Select Routing > IP > Advanced > IP Interface Configuration.
| Routing Table | IPv6 | VLAN | ARF | RIP OSPF | OSPFv3 | Router Discovery VRR | P Multicast | IPv6 Multicast | | | | | |
|--------------------------------|------|---------|----------|--------------|---------|------------------------------------|-------------|----------------|-----------------|------------------------|----------------------|--------------------|----|
| IP | | IP Inte | erface C | onfiguration | | | | | | | Update Delet | Cancel | Ap |
| Basic | ~ | 12 | All | | | | | | | | Go To Interface | | Go |
| Advanced
• IP Configuration | • | | Port | Description | VLAN ID | IP Address Configuration
Method | IP Address | Subnet
Mask | Routing
Mode | Administrative
Mode | Link Speed Data Rate | OSPF Admin
Mode | Fo |
| Statistics | | | 2/0/1 | - | | Manual 👻 | 195.1.4.2 | 255.255.255.0 | Enable + | Enable - | 10G Full | Disable | I |
| AID Interface | | C | 2/0/1 | | | None | 0.0.0.0 | 0.0.0.0 | Enable | Enable | 10G Full | Disable | D |
| Configuration | | | 2/0/2 | | | None | 0.0.0.0 | 0.0.0.0 | Disable | Enable | Unknown | Disable | D |
| Secondary IP | | | 2/0/3 | | | None | 0.0.0.0 | 0.0.0.0 | Enable | Enable | 1000 Mbps | Disable | Di |
| | | | 2/0/4 | | | None | 0.0.0.0 | 0.0.0.0 | Disable | Enable | Unknown | Disable | D |
| | | 8 | 2/0/5 | | | None | 0.0.0.0 | 0.0.0.0 | Disable | Enable | Unknown | Disable | Di |
| | | | 2/0/6 | | | None | 0.0.0.0 | 0.0.0.0 | Disable | Enable | Unknown | Disable | D |
| | | 0 | 2/0/7 | | | None | 0.0.0.0 | 0.0.0.0 | Disable | Enable | Unknown | Disable | Di |
| | | | 2/0/8 | | | None | 0.0.0.0 | 0.0.0.0 | Disable | Enable | Unknown | Disable | Di |
| | | | 2/0/9 | | | None | 0.0.0.0 | 0.0.0.0 | Disable | Enable | Unknown | Disable | D |
| | | 0 | 2/0/10 | | | None | 0.0.0.0 | 0.0.0.0 | Disable | Enable | Unknown | Disable | D |
| | | | 2/0/11 | | | None | 0.0.0.0 | 0.0.0.0 | Disable | Enable | Unknown | Disable | Di |
| | | | 2/0/12 | | | None | 0.0.0.0 | 0.0.0.0 | Disable | Enable | Unknown | Disable | D |
| | | | 2/0/13 | | | None | 0.0.0.0 | 0.0.0.0 | Disable | Enable | Unknown | Disable | D |

- **b.** Above the table heading, Under IP Interface Configuration, click **2**.
- c. Select the 2/0/1 check box for port 2/0/1.

The settings for port 2/0/1 display in the fields in the table heading.

- d. Configure the following settings:
 - In the IP Address Configuration Method field, select Manual.
 - In the IP Address field, enter 195.1.4.2.
 - In the Subnet Mask field, enter 255.255.255.0.
 - In the Routing Mode field, select Enable.
- e. Click Apply.
- 4. Create an IPv6 routing interface.
 - a. Select Routing > IPv6 > Advanced > Interface Configuration.

A screen similar to the following displays.

System Switchi	ng	Routing	QoS	Security	Monitoring	Mainter	ance	Help I	ndex				
outing Table IP IPA	6 VLA	N ARP	RIP OSPF	OSPFv3	Router Discovery	VRRP M	ulticast IPv	6 Multicast					
													Cancel Ap
IPv6	IPv6	Interface Cr	onfiguration										
asic	× 13	3 TUNNE	LS All								Go T	o Interface	Go
dvanced Global Configuration	^	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	Adv Reachabl Interval
Interface Configuration		2/0/3	Enable 👻	Disable +	Disable 🛩	Enable +	Enable +	Disable	1500	1	1800	0	0
Prefix Configuration	1	2/0/1	Disable	Disable	Disable	Enable	Enable	Disable	1500	1	1800	0	0
Statistics	0	2/0/2	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
01000000		2/0/3	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
Neighbour Table	8	2/0/4	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
Static Route	0	2/0/5	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
Configuration	6	2/0/6	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
Route Table	6	2/0/7	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
Douta Proformera	0	2/0/8	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
TONIO T TOTOTOTICO	6	2/0/9	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
Tunnel Configuration	10	2/0/10	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0

- **b.** Above the table heading, Under IP Interface Configuration, click **2**.
- c. Select the 2/0/3 check box for port 2/0/3.

The settings for port 2/0/3 display in the fields in the table heading.

- **d.** Configure the following settings:
 - In the IPv6 Mode field, select Enable.
 - In the Routing Mode field, select Enable.
- e. Click Apply.
- **5.** Configure an IPv6 address for routing interface 2/0/3.
 - a. Select Routing > IPv6 > Advanced > Prefix Configuration.

System Switching		Routing	QoS	Security	Monitoring	Ma	intenance	Help	Index				
Routing Table IP IPo6	VLAN	ARP	RIP OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multica	st				
												Add	Delete
IPv6	IPv61	interface Se	election										
•Basic 🗸	Inte	erface	2/0/3										
•Advanced													
Global Configuration													
Interface Configuration	IPv6 I	nterface C	onfiguration										
Prefix Configuration		10 10 0 1		Sector at	12	45	Malid Life:		Deefored	Onlin	àl.	Autonomour	Cumnet
Statistics		Ipv6 Prefi	ix	Prefix Leng	gth EU	164	Time		Life Time	Flag		Flag	State
Neighbour Table		8888::1		64		~					Ý	*	
Static Route Configuration		fe80::6eb	0.ceff:fe19.ae40	64	Dis	able							[ACTIVE]
Route Table													
Route Preference													
Tunnel Configuration													
1000 CANANTAL AND CANADA CANADA (1998-1997)													

b. From the Interface menu, select 2/0/3.

The settings for port 2/0/3 display in the fields in the table heading.

- c. Configure the following settings:
 - In the Ipv6 Prefix field, enter 2002:c301:402:1::1.
 - In the Prefix Length field, enter 64.
 - In the EUI64 field, select Disable.
- d. Click Add.
- 6. Create a 6to4 tunnel interface.
 - a. Select Routing > IPv6 > Advanced > Tunnel Configuration.

System Switching		Routing	QoS	s	ecurity	Monitoring	Maintenance	lelp Ind	ex			
Routing Table IP IPv6	VLA	N ARP	RIP OSPI	F OS	PFv3 Route	r Discovery	VRRP Multicast IPv6	Multicast				
											Add Delete Canc	el Apply
IPv6	Tunne	el Configu	ration									٢
Basic Advanced		Tunnel ID	Mode		IPv6 Mode	IPv6 Unreachables	IPv6 Address/Prefix Leng	th EUI64	Source Address	Source Interface	Destination Address	Interfac
Global Configuration		0 *	6-to-4	Ŷ	Enable 👻	× .	2002:c301:402::1/16	1	195.1.4.2	v		
Interface Configuration Prefix Configuration Statistics Neighbour Table Static Route Configuration												
Route Table Route Preference												
Tunnel Configuration												

- **b.** Configure the following tunnel settings:
 - In the **Tunnel ID** field, select **0**.
 - In the **Mode** field, select **6-to-4**.
 - In the IPv6 Mode field, select Enable.
 - In the IPv6 Address/Prefix Length field, enter 2002:c301:402::1/16.
 - In the EUI64 field, select Disable.
 - In the Source Address field, enter 195.1.4.2.
- c. Click Add.
- 7. Create a static route for subnet 195.1.3.0/24.
 - a. Select Routing > Routing Table > Advanced > Route Configuration.

System	Swi	itching		Routing	(QoS	Security	Monitorin	ng Mair	tenance	Help	Index			
	IP	IPv6	VLA	N ARP	RIP	OSPF (DSPFv3 P	Router Discove	ry VRRP	Multicast	IPv6 Multicast	ti			
														Update /	ldd
Routing 1	able	Ĩ	Confi	gure Routes											
Basic		×		Route Typ	ю	Network A	Address	Subnet N	lask	Next H	lop Address	Preferen	ce	Description	
Advanced		^		Static	*	195.1.3.0		255.255.	255.0	195.1.	4,1				
Route Config	uration				_							and River			_
Route Prefere	nces														
			Learn	ed Routes											
			N	etwork Addr	ess S	Subnet Mask	Protocol	Route Type	Next Hop Inte	erface Ne	xt Hop Address	Preference	Metric		
			19	95.1.4.0	2	255.255.255.	0 Local	Connected	2/0/1	198	5.1.4.2	0	1		

- **b.** Configure the following route settings:
 - In the Network Address field, enter 195.1.3.0.
 - In the Subnet Mask field, enter 255.255.255.0.
 - In the Next Hop Address field, enter 195.1.4.1.
- c. Click Add.

Web Interface: Create a 6to4 Tunnel on Switch 3

- 1. Enable IP routing on Switch 3.
 - a. Select Routing > IP > Basic > IP Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Mai	ntenance	Help	Index
Routing Table	IP IPv6	VLAN ARP	RIP OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicas	at i
IP	,	IP Configuration							
Basic	^	Default Time to	Live		64				
IP Configura	ition	Routing Mode			Enable	Disable	e .		
Statistics		ICMP Echo Re	aplies		Enable	Disable			
 Advanced 	*	ICMP Redirect	s		Enable	Disable	•		
		ICMP Rate Lim	nit Interval		1000		(0 to 2	147483647 ms)
		ICMP Rate Lim	nit Burst Size		100		(1 to 2	00)	
		Maximum Next	t Hops		16				
		Maximum Rout	tes		12288				
		Maximum Stati	ic Routes		512				
		Select to config	gure Global Defa	ault Gateway					
		Global Default	Gateway		0.0.0.0				

- **b.** For Routing Mode, select the **Enable** radio button.
- c. Click Apply.
- 2. Enable IPv6 forwarding and unicast routing on Switch 3.
 - a. Select Routing > IPv6 > Basic> Global Configuration.

A screen similar to the following displays.

System	Switching	F	Routing		QoS	Security	Monitoring	Ma	intenance	Help	Index
Routing Table	IP IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicas	st
ID-C		IPv6 Glo	obal Cont	figuratio	n						
IPV6		IT YO OR	obai o'oni	ngunune							
Basic	^	IPv6	Unicast F	Routing			Disable Enable	e			
Global Configure	ration	Hop L	_imit				64	(1 t	o 255)		
Route Table		ICMP	v6 Rate	Limit E	rror Interv	/al	1000	10 t	0 214748364	7 msecs)	
 Advanced 	~	ICMP	v6 Rate	Limit B	urst Size		100	(1 t	o 200)		
									atomo ani		

- **b.** For IPv6 Unicast Routing, select the **Enable** radio button.
- c. Click Apply.
- 3. Create a routing interface and assign an IP address to it.
 - a. Select Routing > IP > Advanced > IP Interface Configuration.

System S	Switching	Routir	yg QoS	Security	Monitoring	Maintenance	Help Ind	ex				
Routing Table (P	IPv6	VLAN AR	P RIP OSPF	OSPFv3	Router Discovery VR	RP Multicast	IPv6 Multicast					
										Update Delet	e Cancel	Appl
IP		IP Interface 0	Configuration									C
Basic	~	1 2 All								Go To Interface		Go
Advanced •IP Configuration	^	Port	Description	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Routing Mode	Administrative Mode	Link Speed Data Rate	OSPF Admin Mode	For Bro
Statistics		2/0/1			Manual 🐱	195.1.5.2	255.255.255.0	Enable 👻	Enable 👻	10G Full	Disable	Di
+IP Interface		2/0/1			None	0.0.0.0	0.0.0.0	Disable	Enable	10G Full	Disable	Dis
Configuration		□ 2/0/2			None	0.0.0.0	0.0.0	Disable	Enable	Unknown	Disable	Dis
Secondary IP		2/0/3			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown	Disable	Dis
		2/0/4			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown	Disable	Dis
		2/0/5			None	0.0.0.0	0.0.0	Disable	Enable	Unknown	Disable	Dis
		2/0/6			None	0.0.0.0	0.0.0	Disable	Enable	Unknown	Disable	Dis
		0 2/0/7			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown	Disable	Dis
		2/0/8			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown	Disable	Dis

- b. Above the table heading, Under IP Interface Configuration, click 2.
- c. Select the 2/0/1 check box for port 2/0/1.

The settings for port 2/0/1 display in the fields in the table heading.

- **d.** Configure the following settings:
 - In the IP Address Configuration Method field, select Manual.
 - In the IP Address field, enter 195.1.5.2.
 - In the Subnet Mask field, enter 255.255.255.0.
 - In the Routing Mode field, select Enable.
- e. Click Apply.
- 4. Create an IPv6 routing interface.
 - a. Select Routing > IPv6 > Advanced > Interface Configuration.

A screen similar to the following displays.

System Switching		Routing	QoS	Security	Monitoring	Mainte	nance	Help	Index				
Routing Table IP IPv6	VLA	N ARP	RIP OSPE	OSPFv3	Router Discovery	VRRP N	fulticast If	v6 Multicast					
													Cancel Apply
IPv6	IPv6	Interface Cr	onfiguration										Ø
Basic v	12	TUNNELS	i All								Go 7	To Interface	Go
Advanced A		Interface	IPv6 Mode	DHCPv6 Client Mode	Stateless Address AutoConfig Mode	Routing Mode	Admin Mode	Operationa Mode	MTU	Duplicate Address Detection Transmits	Life Time Interval	Adv NS Interval	Adv Reachable Interval
Interface Configuration		2/0/24	Enable +	Disable +	Disable +	Enable +	Enable	- Disable	1500	1	1800	0	0
Prefix Configuration		2/0/1	Disable	Disable	Disable	Enable	Enable	Disable	1500	1	1800	0	0
• Statistice	.8	2/0/2	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
• Statisurs	0	2/0/3	Enable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
Neighbour Table	8	2/0/4	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
Static Route	0	2/0/5	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
Configuration		2/0/6	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
Route Table	0	2/0/7	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
Route Preference	8	2/0/8	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0.
Though Finderstere	8	2/0/9	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0
 Tunnel Configuration 	0	2/0/10	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0	0

- **b.** Above the table heading, Under IP Interface Configuration, click **2**.
- c. Select the 2/0/24 check box for port 2/0/24.

The settings for port 2/0/24 display in the fields in the table heading.

- d. Configure the following settings:
 - In the IPv6 Mode field, select Enable.
 - In the Routing Mode field, select Enable.
- e. Click Apply.

- 5. Configure the IPv6 address for the IPv6 routing interface 2/0/24.
 - a. Select Routing > IPv6 > Advanced > Prefix Configuration.

System Switching	9	Routing	QoS	Security	Monitoring	Mai	intenance	Help	Index				
Routing Table IP IPv6	VLA	N ARP	RIP OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicas	t				
IPv6	IPv6	Interface Se	election									Add	Delete
•Basic ~	Int	erface	2/0/24	~									
Advanced													
Global Configuration													
Interface Configuration	IPv6	Interface Cr	onfiguration										
Prefix Configuration		100 (Derive 194		n linnar ar			March 1975		Destaurat	0.00	- 12 C	A. 4	Comment
Statistics		Ipv6 Prefe	x	Prefix Len	gth EU	64	Time		Life Time	Flag	BK -	Flag	State
Neighbour Table		888821		64		×					~	~	
Static Route Configuration		fe80::6eb0	0.ceff:fe19.ae4	0 64	Dis	able							[ACTIVE]
Route Table													
Route Preference													
Tunnel Configuration													

b. From the Interface menu, select 2/0/24.

The settings for port 2/0/24 display in the fields in the table heading.

- **c.** Configure the following settings:
 - In the **Ipv6 Prefix** field, enter **8888::1**.
 - In the Prefix Length field, enter 64.
 - In the EUI64 field, select Disable.
- d. Click Add.
- 6. Create a 6to4 tunnel interface.
 - a. Select Routing > IPv6 > Advanced > Tunnel Configuration.

System Switching		1	Routing	QoS	S	ecunty	Monitoring	Maintenance Help	Index	•			
Routing Table IP IPV6	Tunn	N el C	Configur	RIP OSPF	OS	PFv3 Route	r Discovery	VRRP Multicast IPv6 Mu	ilticast.			Add Delete Cano	d Apply
•Basic ~		1	Funnel D	Mode		IPv6 Mode	IPv6 Unreachables	IPv6 Address/Prefix Length	EUI64	Source Address	Source Interface	Destination Address	Interfac
Global Configuration		1	0 ¥	6-to-4	×	Enable 👻		2002:c301:502::1		195.1.5.2	×		
Interface Configuration	0												
Prefix Configuration													
Statistics													
Neighbour Table													
Static Route Configuration													
Route Table													
Route Preference													
Tunnel Configuration													

- **b.** Configure the following tunnel settings:
 - In the **Tunnel ID** field, select **0**.
 - In the **Mode** field, select **6-to-4**.
 - In the IPv6 Mode field, select Enable.
 - In the IPv6 Address/Prefix Length field, enter 2002:c301:402::1/16.

- In the EUI64 field, select Disable.
- In the **Source Address** field, enter **195.1.4.2**.
- c. Click Add.
- d. Configure the following tunnel settings:
 - In the Tunnel ID field, select 0.
 - In the **Mode** field, select 6-to-4.
 - In the IPv6 Mode field, select Enable.
 - In the IPv6 Address/Prefix Length field, enter 2002:c301:502::1/16.
 - In the EUI64 field, select Disable.
 - In the Source Address field, enter 195.1.5.2.
- e. Click Add.
- 7. Create a static route for subnet 195.1.3.0/24.
 - a. Select Routing > Routing Table > Advanced > Route Configuration.

System	Switchi	ng	Routing		QoS S	Security	Monitorin	g Mainten	nance	Help	Index		
	IP IPv	6 1	VLAN ARP	RIP	OSPF OS	SPFv3	Router Discove	ry VRRP Mi	ulticast	IPv6 Multicast	(
													Update Ad
Routing T	Table	0	Configure Routes	5									
Basic		~	Route Typ	pe	Network Ad	ddress	Subnet M	lask	Next Hor	p Address	Preferen	ce	Description
Advanced		^	Static	¥	195.1.3.0		255.255.3	255.0	195.1.5.1				
Route Config	uration												
Route Prefere	es												
		L	earned Routes										
			Network Add	ress S	Jubnet Mask	Protocol	Route Type	Next Hop Interfa	ce Next	Hop Address	Preference	Metric	
			195150	2	55 255 255 0	Local	Connected	2/0/1	195.1	52	0	1	

- **b.** Configure the following route settings:
 - In the Network Address field, enter 195.1.3.0.
 - In the Subnet Mask field, enter 255.255.255.0.
 - In the Next Hop Address field, enter 195.1.5.1.
- c. Click Add.

IPv6 Interface Configuration



IPv6 routing and routing VLANs

This chapter includes the following sections:

- Create an IPv6 Routing Interface
- Create an IPv6 Routing VLAN
- Configure DHCPv6 Mode on the Routing Interface

Note: IPv6 interface configuration is available on M5300 and M6100 series switches only. However, the following M5300 series switches require a license to support IPv6 interface configuration: M5300-28G, M5300-52G, M5300-28G-POE+, and M5300-52G-POE+.

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) #show ipv6 interface 1/0/1	
IPv6 is enabled	
IPv6 Prefix is FE8	0::21E:2AFF:FED9:249B/128
	2000::2/64 [TENT]
Routing Mode Ena	bled
Administrative Mode Ena	bled
IPv6 Routing Operational Mode Ena	bled
Bandwidth 100	0000 kbps
Interface Maximum Transmit Unit 150	0
Router Duplicate Address Detection Transmits 1	
Router Advertisement NS Interval 0	
Router Advertisement Lifetime 180	0
Router Advertisement Reachable Time 0	
Router Advertisement Interval	
Router Advertisement Managed Config Flag Dis	abled
Router Advertisement Other Config Flag Dis	abled
Router Advertisement Suppress Flag Dis	abled
IPv6 Destination Unreachables Ena	bled
Prefix 2000::2/64	
Preferred Lifetime 604	800
Valid Lifetime 259	2000
Onlink Flag Ena	bled
Autonomous Flag Ena	bled

Web Interface: Create an IPv6 Routing Interface

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

Sv	vitching		Routing		QoS	Securi	ty	Monitoring		Maintenance	Help	Index
ΙP		VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP	Multicast	IPv6 Multicast	
		IPv6 G	lobal Cor	nfigurat	ion							
	~	IPv6	Jnicast F	Routing			Disa	able 💿 Enable	9			
ıratio	n	Hop l	.imit				64		(1 to 2	55)		
		ICMF	v6 Rate I	Limit E	rror Interv	al	1000		(0 to 2	147483647 n	nsecs)	
	¥	ICMF	v6 Rate I	imit B	urst Size		100		(1 to 2	00)		
	S\ IP	Switching IP IPv6 A aration	Switching IP IPv6 VLAN IPv6 G IPv6 G IPv6 G IPv6 I ICMP VLAN	Switching Routing IP IPv6 VLAN ARP IPv6 Global Cor IPv6 Unicast F Hop Limit ICMPv6 Rate I ICMPv6 Rate I	Switching Routing IP IPv6 VLAN ARP RIP IPv6 Global Configurat IPv6 Unicast Routing Hop Limit ICMPv6 Rate Limit B VCMPv6 Rate Limit B	Switching Routing QoS IP IPv6 VLAN ARP RIP OSPF IPv6 Global Configuration IPv6 Unicast Routing IPv6 IPv6 Unicast Routing IPv6 Unicast Routing Iration IOV6 Rate Limit Error Interval ICMPv6 Rate Limit Burst Size	Switching Routing QoS Securi IP IPv6 VLAN ARP RIP OSPF OSPFv3 IPv6 Global Configuration IPv6 Global Configuration IPv6 Unicast Routing IPv6 Unicast Routing IPv6 Unicast Routing IPv6 Unicast Routing ICMPv6 Rate Limit Error Interval ICMPv6 Rate Limit Burst Size ICMPv	Switching Routing QoS Security IP IPv6 VLAN ARP RIP OSPF OSPFv3 Routing IPv6 Global Configuration IPv6 Unicast Routing Disa ration IPv6 Unicast Routing 0 Disa VLAN ARP RIP 0 0 VIDE ICMPv6 Rate Limit Error Interval 1000 100	Switching Routing QoS Security Monitoring IP IPv6 VLAN ARP RIP OSPF OSPFv3 Router Discovery IPv6 Global Configuration IPv6 Unicast Routing Disable Disable Enable ration Hov6 Unicast Routing ICMPv6 Rate Limit Error Interval 64 1000 ICMPv6 Rate Limit Burst Size 100 Icm 100 Icm	Switching Routing QoS Security Monitoring I IP IPv6 VLAN ARP RIP OSPF OSPFv3 Router Discovery VRRP IPv6 Global Configuration IPv6 Unicast Routing Disable © Enable IPv6 Unicast Routing ICMPv6 Rate Limit Error Interval 0 Disable © Inable (1 to 2 ICMPv6 Rate Limit Burst Size 100 (1 to 2 100 (1 to 2	Switching Routing QoS Security Monitoring Maintenance IP IPv6 VLAN ARP RIP OSPF OSPFv3 Router Discovery VRRP Multicast IPv6 Global Configuration IPv6 Unicast Routing Disable @ Enable Interval IPv6 Hop Limit ICMPv6 Rate Limit Error Interval 1000 (0 to 2147483647 m) ICMPv6 Rate Limit Burst Size 100 (1 to 200) 100 (1 to 200)	Switching Routing QoS Security Monitoring Maintenance Help IP IPv6 VLAN ARP RIP OSPF OSPFv3 Router Discovery VRP Multicast IPv6 Multicast IPv6 Global Configuration Disable © Enable ration Hop Limit 64 (1 to 255) ICMPv6 Rate Limit Error Interval 1000 (0 to 2147483647 msecs)

- **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.

System Switchin	19	Routing	QoS	Security	Monitoring	Mainter	ance	Help I	ndex			
Routing Table IP IPM	VLA	N ARP	RIP OSPE	OSPEV2	Router Discovery	VRRP Multi	cast IPv6 N	hulticast				
IPv6	IPv6	Interface C	onfiguration									
Jasic	* 13	2 3 VLANS	EA.									Go To Interface
Advanced • Global Configuration		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
Interface Configuration			÷	÷	~		¥					
Prefix Configuration	18	1/0/1	Disable	Disable	Disable	Disable.	Enable	Disable.	1500	1	1800	0
Statistics	12	1/0/2	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
Meighbour Table	-6	1/0/3	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
Trangeroour Taroro	6	1/0/4	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
Static Route Configuration	6	1/0/5	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
	6	1/0/6	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
*Houte Lable	10	1/0/7	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
Route Preference	10	1/0/8	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
Trinnal Configuration	0	1/0/9	Disable	Disable	Disable	Enable	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.

System	Switchin	g .	Routing	-	QoS	Security	/ Moi	nitoring	Maintenan	ce Help	Index
Routing Table	IP IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Disc	overy VRF	RP Multicas	st IPv6 Multica	ist
IPv	6	IPv6 Ir	iterface S	Selectio	n						
•Basic	``	Inter	ace	1	1/0/1 ~						
 Advanced 											
Global Config	guration										
Interface Cor	nfiguration	IPv6 Ir	iterface C	Configu	ration						
Prefix Config	uration		Inv6 Prof	N.		Profix Long	th	ELII64	Valid Life	Pr	eferred
 Statistics 			ipvo r ter	LA		I TENA LENG		LOI04	Time	Lif	e Time
• Neighbour Ta	able		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 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.

Syst	em	Swi	tching		Routing	QoS	Security	Monitori	ng Maintenance	Help	Index
VLAN	Auto-	/olP	iSCSI	STP	Multicast	MVR	Address Table	Ports LAG	MLAG		» — · · —
	VLA	N		Reset							
• Basic			^	Reset	Configuratio	on					
• VLAI	I Config	uration									
• Advanc	ed		~								
				Interna	VLAN Conf	iguration					
				Intern	al VLAN Allo	ocation Bas	e 40!	93			
				Intern	al VLAN Allo	ocation Poli	cy 💿	Ascending 💿 De	escending		
				VLAN	Configuration						
					/LAN ID VI	_AN Name	VLAN Type	Make Static			
					500			~			
					1 de	fault	Default	Disable			

- 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.

Syste	em Sv	vitching		Routing	QoS	33	Security	2	Мо	nitoring	10	Main	tenanc	e:	ł	Help		In	ıdex	*	
	Auto-VolP	iSCSI	STP	Multicast	MVR	Addre	ess Table	Po	rts	LAG	MLAC)									
12																					
	VLAN		VLAN N	/lembership	8																
•Basic		~	VLAN	ID										500	¥						
• Advanc	ed	~	Group	Operation										Unta	a All	~					
• VLAN	Configuration	1	VLAN	Name										VLAN	0500						
• VLAN	I Membership	í i	VLAN	Туре										Static							
• VLAN	l Status																				
• Port F	⊃VID		0	nit 1										19925							
Confi	guration		Ports	1 3	5 7	9 11	13 15	17	19	21 23	25	27 2	9 31	33	35	37	39	41	43	45	47
• MAC	Based VLAN			U _																	
• Proto Group	col Based VL configuration	AN		2 4	6 8	10 12	14 16	18	20	22 24	26	28 3	0 32	34	36	38	40	42	44	46	48

- 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.

System Sw	itching		Routing	0	S Security	Monitoring	Maintenance Help	Index		
VIAN Auto-VolP	iscsi	STR	Multica	ast MV	R Address Table	Ports LAG MLAG				
VLAN		PVID	Configurat	ion						
Basic	~	12	3 LAGS A	al .					Go To Interface	Go
Advanced	~									Part Drivet
VLAN Configuration		P	Interface	PVID	VLAN Member	VLAN Tag	Acceptable Frame Types	Configured Ingress Filtering	Current Ingress Filtering	(0 to 7)
*VLAN Membership			1/0/1	500	1,500	None	Admit All 👻	Disable -	Disable	0
VLAN Status		×.	1/0/1	500	1,500	None	Admit All	Disable	Disable	0
Port PVID			1/0/2	1	1	None	Admit All	Disable	Disable	0
Configuration			1/0/3	1	1	None	Admit All	Disable	Disable	0
MAC Based VLAN		8	1/0/4	1	1	None	Admit All	Disable	Disable	0

- **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.

System	S	witching		Routing		QoS	Securi		Monitorin	ig 📗	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Route	r Discovery	VRRP	Multicast	IPv6 Multicast	
IPv	6		IPv6 G	lobal Cor	nfigurati	on							
• Basic		^	IPv6 I	Jnicast F	Routing	i	3	🔘 Disa	ble 💿 Enabl	le			
Global Config	guratio	n	Hop L	imit				64		(1 to	255)		
• Route Table			ICMP	v6 Rate I	Limit E	rror Interv	al	1000		(0 to	2147483647 n	nsecs)	
 Advanced 		~	ICMP	v6 Rate I	Limit B	urst 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.
- 5. Enable IPv6 routing on the VLAN.
 - a. Select Routing > IPv6 > Advanced > Interface Configuration.

System	Swit	ching	Vi.	Routing	QoS	Securit	y Monitoring	Mainte	nance	Help I	ndex		
Routing Table	IP I	² V6	VLAN	I ARP	RIP OSPF	OSPFv3	Router Discovery	VRRP Mult	icast IPv6 M	ulticast		k	
IPv6	i :		IPv6	Interface C	onfiguration								
•Basic		~	12	3 VLANS	All								
Advanced		^						-					
• Global Config	uration		ų,	Interface	IPv6 Mode	DHCPv6 Client Mode	Stateless Address AutoConfig Mode	Routing Mode	Admin Mode	Operational Mode	MTU	Duplicate Address Detection Transmits	Life Lime Interval
Interface Con	figuration	n		vlan 100	Enable ×	Disable 🛩	Enable ×	Enable ×	Enable 🗸	Disable	1500	1	1800
Prefix Configu	iration			vlan 1	Disable	Disable	Disable	Enable	Enable	Disable	1500	1	1800
 Statistics 				vlan 500	Disable	Disable	Disable	Enable	Enable	Disable	1500	1	1800
• Neighbour Ta	ble			vlan 100	Enable	Disable	Disable	Enable	Enable	Disable	1500	1	1800
 Static Route Configuration 			1 2	3 VLANS	All								G

- 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.

System Sv	vitching		Routing	QoS	Secur	ty Monitor	ing	Maintenance	Help	Index
Routing Table IP	IPv6	VLAN	ARP	RIP OS	PF OSPFv3	Router Discover	y VRRF	^o Multicast	IPv6 Multicast	21
IPv6		IPv6 Ir	nterface S	election						
• Basic	~	Inter	face	vlan 1)0 v					
 Advanced 	^									
 Global Configuration 	n									
Interface Configurat	ion	IPv6 Ir	nterface C	onfiguration						
Prefix Configuration			Inv6 Drof	~	Drofix Lor	iath EU	IGA	Valid Life	Prefer	red
 Statistics 			ipto i tei		T TOUX LO	igin Eo	104	Time	Life Ti	me
• Neighbour Table			2000::1		64	D	isable 🛩			
 Static Route Configuration 			fe80::220)c:c8ff.fe4d:9	575 64	Dis	able			

- b. In the Interface field, select 0/4/2.
- c. In the IPv6 Prefix field, enter 2000::1.
- d. In the Length field, enter 64.
- e. In the EUI64 field, select Disable.
- f. Click Add.

Configure DHCPv6 Mode on the Routing Interface

The routing interface supports DHCPv6 mode, which can get the IPv6 address from a DHCPv6 server (address allocation).

Note: Before you enable DHCPv6 mode, you must disable IPv6 unicast mode globally.

CLI: Configure DHCPv6 mode on routing interface

1. Enable IPv6 unicast globally.

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

2. Enable DHCPv6 on the interface 1/0/23.

```
(Netgear Switch) (Config)#interface 1/0/23
(Netgear Switch) (Interface 1/0/23)#routing
(Netgear Switch) (Interface 1/0/23)#ipv6 enable
(Netgear Switch) (Interface 1/0/23)#ipv6 address dhcp
(Netgear Switch) (Interface 1/0/23)
```

3. Show the ipv6 address assigned from 1/0/23.

(Netgear Switch) #show ipv6 interface 1/0/23
IPv6 is enabled
IPv6 Prefix is FE80::E291:F5FF:FE06:2BF6/128
2000::1D5C:7CFE:828F:8144/128 [DHCP]
Routing Mode Enabled
IPv6 Enable Mode Enabled
Administrative Mode Enabled
IPv6 Operational Mode Enabled
Bandwidth 1000000 kbps
Interface Maximum Transmit Unit 1500
Router Duplicate Address Detection Transmits 1
Address DHCP Mode Enabled
Router Advertisement NS Interval 0
Router Advertisement Lifetime 1800
Router Advertisement Reachable Time 0
Router Advertisement Interval 600
Router Advertisement Managed Config Flag Disabled
Router Advertisement Other Config Flag Disabled
Router Advertisement Router Preference medium
Router Advertisement Suppress Flag Disabled
IPv6 Destination Unreachables Enabled

Web Interface: Configure DHCPv6 mode on routing interface

- 1. Enable IPv6 unicast globally.
 - a. Select Routing > IPv6 > Basic > Global Configuration.

A screen similar to the following displays.

System	Sv	vitching	_	Routing		QoS	Securit	у	Monitoring		Maintenance	Help	Index
Routing Table	IP		VLAN	ARP	RIP	OSPF	OSPFv3	Route	r Discovery	VRRP	Multicast	IPv6 Multicast	
IPv	5		IPv6 G	lobal Cor	nfigurat	ion							
 Basic 		~	IPv6 I	Jnicast F	Routing	1)) Disat	le 🖲 Enable	ŝ.			
Global Config	guration	i j	Hop l	.imit				64		(1 to 2	255)		
• Route Table			ICMP	v6 Rate	Limit E	rror Interva	al	1000		(0 to 2	2147483647 n	nsecs)	
 Advanced 		~	ICMP	v6 Rate	Limit B	lurst Size		100		(1 to 2	200)		

- **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.

System Sv	vitching		Routing	QoS	Security	/ Monitoring	Mainter	ance	Help b	ndex			
Routing Table IP		VLAP	ARP	RIP OSPF	OSPFv3	Router Discovery	VRRP Multi	cast IPv6 M	fulticast				
IP46		IPv6	Interface C	onfiguration									
Basic	÷	12	3 VLANS	All									Go To Interface
Advanced Global Configuration	ĥ		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 Internal
Interface Configurat	ion		1/0/23	Enable +	Enable ~	Disable ~	Disable ~	Enable +	Disable	1500	1	1800	0
Prefix Configuration			1/0/1	Enable	Disable	Disable	Enable	Enable	Disable	1500	1	1800	0
Statistics		.03	1/0/2	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
* Neighbour Table			1/0/3	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
Trengenous Taken		10	1/0/4	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
 Static Route Configuration 			1/0/5	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
Configuration		0	1/0/6	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
 Route Table 		10	1/0/7	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
 Route Preference 			1/0/8	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
•Tunnel Configuration	n	.8	1/0/9	Disable	Disable	Disable	Enable	Enable	Disable	1500	1	1800	0

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.

System	Switching		Routing	QoS	Securit	/	Monitoring	į	Maintenance	Help	Index	
Routing Table	IP IPv6	VLAN	ARP	RIP OSPF	OSPFv3	Router I	Discovery	VRRF	Multicast	IPv6 Multicast	· · · · · ·	
IPv6		IPv6 In	terface S	election								
•Basic	*	Interfa	асе	1/0/23	*							
 Advanced 	^											
Global Configu	uration											
Interface Conf	figuration	IPv6 In	terface C	onfiguration								_
Prefix Configu	iration				Destro Long		FURA		Valid Life	Prefer	red	
 Statistics 			pv6 Pren	x	Prenx Leng	an/	E0104		Time	Life Ti	me	
• Neighbour Tah	ble							~				
 Static Route Configuration 			e80::220	lc:c8ff.fe4d:957	5 64		Disabl	е				

b. Scroll down and select the interface 1/0/23. You can see the IPv6 address assigned by the DHCPv6 server.

PIM

Protocol Independent Multicast

This chapter includes the following sections:

- Protocol Independent Multicast Concepts
- PIM-DM
- PIM-SM

Note: PIM is available on M5300 and M6100 series switches only. However, the following M5300 series switches require a license to support PIM: M5300-28G, M5300-52G, M5300-28G-POE+, and M5300-52G-POE+.

33

Protocol Independent Multicast Concepts

The PIM protocol can be configured to operate on IPv4 and IPv6 networks. Separate CLI commands are provided for IPv4 and IPv6 operation; however, most configuration options are common to both protocols. Therefore, this section describes only IPv4 configuration; IPv6 configuration is similar to IPv4.

Multicast protocols are used to deliver multicast packets from one source to multiple receivers. They facilitate better bandwidth utilization, and use less host and router processing, making them ideal for usage in applications such as video and audio conferencing, whiteboard tools, and stock distribution tickers. PIM is a widely used multicast routing protocol. Protocol Independent Multicast (PIM) is a standard multicast routing protocol that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. There are two types of PIM:

- PIM-Dense Mode (PIM-DM)
- PIM-Sparse Mode (PIM-SM)

PIM-DM

PIM-DM is appropriate for:

- Densely distributed receivers
- A ratio of few senders to many receivers (due to frequent flooding)
- High volume of multicast traffic
- Constant stream of traffic



Figure 58. Configuring and Using PIM-DM

PIM-DM uses the existing unicast routing table and join, prune, and graft mechanism to build a tree. PIM-DM creates source-based shortest-path distribution trees that use reverse path forwarding (RPF). PIM-DM cannot be used to build a shared distribution tree, as PIM-SM can. PIM-DM assumes that when a sender starts sending data, all downstream routers and hosts want to receive a multicast datagram. PIM-DM initially floods multicast traffic throughout the network. Routers that do not have any downstream neighbors prune back the unwanted traffic. Apart from prune messages, PIM-DM uses two other types of messages: graft messages and assert messages. Graft messages are used whenever a new host wants to join the group. Assert messages are used to shut off duplicate flows onto the same multi-access network.

To minimize the repeated flooding of datagrams and subsequent pruning associated with a particular (S,G) pair, PIM-DM uses a state refresh message. This message is sent by the routers directly connected to the source and is propagated throughout the network. When

received by a router on its RPF interface, the state refresh message causes an existing prune state to be refreshed. State refresh messages are generated periodically by the router directly attached to the source. There are two versions of PIM-DM. Version 2 does not use IGMP messages; instead, it uses a message that is encapsulated in IP packets with protocol number 103. In version 2, the Hello message is introduced in place of the query message.

CLI: Configure PIM-DM

PIM-DM on Switch A

1. Enable IP routing on the switch.

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

2. Enable pimdm on the switch.

(Netgear Switch) (Config)#ip pim dense

3. Enable IP multicast forwarding on the switch.

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

4. Enable RIP to build the unicast IP routing table.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.2.2 255.255.0
(Netgear Switch) (Interface 1/0/1)#ip rip
```

5. Enable PIM-DM on the interface.

```
(Netgear Switch) (Interface 1/0/1)#ip pim
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Interface 1/0/9)#routing
(Netgear Switch) (Interface 1/0/9)#ip address 192.168.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/9)#ip rip
(Netgear Switch) (Interface 1/0/9)#ip pim
(Netgear Switch) (Interface 1/0/9)#exit
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ip address 192.168.1.2 255.255.255.0
(Netgear Switch) (Interface 1/0/13)#ip rip
(Netgear Switch) (Interface 1/0/13)#ip pim
(Netgear Switch) (Interface 1/0/13)#ip pim
(Netgear Switch) (Interface 1/0/13)#ip pim
```

PIM-DM on Switch B

(Netgear	Switch)	#configure
(Netgear	Switch)	(Config)#ip routing
(Netgear	Switch)	(Config)#ip pim
(Netgear	Switch)	(Config)#ip multicast
(Netgear	Switch)	(Config)#interface 1/0/10
(Netgear	Switch)	(Interface 1/0/10)#routing
(Netgear	Switch)	(Interface 1/0/10)#ip address 192.168.3.2 255.255.255.0
(Netgear	Switch)	(Interface 1/0/10)#ip rip
(Netgear	Switch)	(Interface 1/0/10)#ip pim
(Netgear	Switch)	(Interface 1/0/10)#exit
(Netgear	Switch)	(Config)#interface 1/0/11
(Netgear	Switch)	(Interface 1/0/11) #routing
(Netgear	Switch)	(Interface 1/0/11)#ip address 192.168.5.1 255.255.255.0
(Netgear	Switch)	(Interface 1/0/11)#ip rip
(Netgear	Switch)	(Interface 1/0/11)#ip pim
(Netgear	Switch)	(Interface 1/0/11)#exit

PIM-DM on Switch C

(Netgear	Switch)	#configure
(Netgear	Switch)	(Config)#ip routing
(Netgear	Switch)	(Config)#ip pim dense
(Netgear	Switch)	(Config)#ip multicast
(Netgear	Switch)	(Config)#interface 1/0/21
(Netgear	Switch)	(Interface 1/0/21)#routing
(Netgear	Switch)	(Interface 1/0/21)#ip address 192.168.5.2 255.255.255.0
(Netgear	Switch)	(Interface 1/0/21)#ip rip
(Netgear	Switch)	(Interface 1/0/21)#ip pim
(Netgear	Switch)	(Interface 1/0/21)#exit
(Netgear	Switch)	(Config)#interface 1/0/22
(Netgear	Switch)	(Interface 1/0/22)#routing
(Netgear	Switch)	(Interface 1/0/22)#ip address 192.168.6.1 255.255.255.0
(Netgear	Switch)	(Interface 1/0/22)#ip rip
(Netgear	Switch)	(Interface 1/0/22)#ip pim
(Netgear	Switch)	(Interface 1/0/22)#exit

PIM-DM on Switch D

1. Enable IGMP on the switch.

(Netgear Switch) #configure (Netgear Switch) (Config)#ip routing (Netgear Switch) (Config)#ip pim dense (Netgear Switch) (Config)#ip igmp

```
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address 192.168.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/21)#ip rip
(Netgear Switch) (Interface 1/0/21)#ip pim
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) (Interface 1/0/22)#routing
(Netgear Switch) (Interface 1/0/22)#routing
(Netgear Switch) (Interface 1/0/22)#ip address 192.168.6.2 255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22)#ip pim
(Netgear Switch) (Interface 1/0/22)#exit
```

2. Enable IGMP on port 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#routing
(Netgear Switch) (Interface 1/0/24)#ip pim
(Netgear Switch) (Interface 1/0/24)#ip rip
(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
                    Protocol
Source IP
          Group IP
                              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
                              Interface
                                          Interface List
                    Protocol
          _____
                               _____
_____
                     _____
                                          _____
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.

System	S	witching		Routing	i i	QoS	Securi	ty	Monitoring	9	Maintenance	Help	Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast	
IP			IP Con	figuratior									
• Basic		^	Defau	<mark>ilt Ti</mark> me t	o Live				64				
 IP Configurati 	on		Routi	ng Mode					Enable	e 🖲 Disa	ble		
• Statistics			ICMP	Echo R	eplies				Enable	e 🖲 Disa	ble		
 Advanced 		~	ICMP	Redirec	ts				Enable	e 🖲 Disa	ble		
			ICMP	Rate Lin	nit Inte	rval			1000		(0 to 21	47483647 ms)	
			ICMP	Rate Lir	nit Bur	st Size			100		(1 to 20)	0)	

- **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.

System	Sv	vitching		Routin	ig 🛛	QoS	Securit	y Monitoring		Maintenance	Help	Index		
Routing Table		IPv6	VLAN	ARF	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast			
IP			IP Int	erface C	onfigurati	ion								
• Basic		×	12	3 VLAN	IS All	20.								
 Advanced 		^			1		1	ID Address Conferen			Outrast	Dev		Administration
• IP Configuration	n			Port	Descrip	tion	VLAN ID	Method	auon	IP Address	Mask	Mod	le le	Mode
 Statistics 				1/0/1				Manual 👻		192.168.2.2	255.255.25	i5.0 En	able 🛩	Enable 👻
• IP Interface				1/0/1				None		0.0.0.0	0.0.0.0	Disa	able	Enable
Conliguration				1/0/2				None		0.0.0.0	0.0.0.0	Dis	able	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.

System	S	witching		Routin	3	QoS	Securit	y Monitoring	Maintenance	Help	Index	
Routing Table	P	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery VR	RP Multicast	IPv6 Multicast		
IP	1		IP Int	erface Ci	onfigurat	ion						
• Basic		~	12	3 VLAN	5 All							
 Advanced IP Configurat 	ion	^		Port	Descrip	ntion	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Routing Mode	Administrative Mode
 Statistics 				1/0/9	-			Manual 🛩	192.168.3.1	255.255.25	5.0 Enable	✓ Enable ✓
IP Interface Configuration	(1/0/1				Manual	192.168.2.2	255.255.25	5.0 Enable	Enable
• Secondary IF	2			1/0/2				None	0.0.0.0	0.0.0.0	Disable	Enable
				1/0/4				None	0.0.0.0	0.0.0.0	Disable	Enable
				1/0/6 1/0/7				None None	0.0.0.0	0.0.0.0	Disable Disable	Enable Enable
				1/0/8 1/0/9				None None	0.0.0.0	0.0.0.0	Disable Disable	Enable 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.

System	Sv	vitching		Routing		QoS	Securit	y Monitoring	1	Maintenance	Help	Index			
Routing Table		IPv6	VLAN	I ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast				
IP							-								
Distant				1/0/13				Manual 🗸		192.168.1.2	255.255.255	5.0 Enable	• •	Enable ~	-
Basic		~		1/0/1				Manual		192.168.2.2	255.255.255	.0 Enable		Enable	
 Advanced 		^		1/0/2				None		0.0.0.0	0.0.0.0	Disable		Enable	
• IP Configurat	ion			1/0/3				None		0.0.0.0	0.0.0.0	Disable		Enable	
• Statistics				1/0/4				None		0.0.0.0	0.0.0.0	Disable		Enable	
Statistics		- 22		1/0/5				None		0.0.0.0	0.0.0.0	Disable		Enable	
 IP Interface Configuration 				1/0/6				None		0.0.0.0	0.0.0.0	Disable		Enable	
0	500. 			1/0/7				None		0.0.0	0.0.0.0	Disable		Enable	
 Secondary II 				1/0/8				None		0.0.0.0	0.0.0.0	Disable		Enable	
				1/0/9				None		0.0.0.0	0.0.0.0	Disable		Enable	
				1/0/10				None		0.0.0.0	0.0.0.0	Disable		Enable	
				1/0/11				None		0.0.0.0	0.0.0.0	Disable		Enable	
				1/0/12				None		0.0.0.0	0.0.0.0	Disable		Enable	
				1/0/13				None		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.

System	Swi	itching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Rou	ter Discovery	VRRP Multicast	IPv6 Multicast	
RIP			RIP Ir	nterface Co	onfiguration					
• Basic		~	12	3 VLANS	All					
 Advanced 		^		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Ke	Authentication Key ID
RIP Configurat	tion	literi (1/0/1	RIP-2 ×	RIP-2 ×	Enable ~	None Y		
• Interface Confi	iguratio	on		1/0/1	RIP-2	Both	Disable	None		0
 Route Redistri 	ibution			1/0/2	RIP-2	Both	Disable	None		0

- **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.

System	Switching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table IF	P IPv6	VLAN	I ARP	RIP OSPF	OSPFv3 Rou	ter Discovery	VRRP Multicast	IPv6 Multicast	
RIP		RIP II	nterface Co	onfiguration					
• Basic	×	12	3 VLANS	All					
• Advanced	~	0	Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Key	Authentication Key ID
RIP Configuratio Interface Configu	uration		1/0/9	RIP-2 ¥	RIP-2 ↔	Enable v	None 🗸	J	0
• Route Redistribu	ution		1/0/1 1/0/2	RIP-2 RIP-2	Both Both	Disable Disable	None None		0
			1/0/3	RIP-2	Both	Disable	None		0
			1/0/4	RIP-2	Both	Disable	None		0
			1/0/5	RIP-2	Both	Disable	None		0
			1/0/6	RIP-2	Both	Disable	None		0
			1/0/7	RIP-2	Both	Disable	None		0
			1/0/8	RIP-2	Both	Disable	None		0
			1/0/9	RIP-2	Both	Disable	None		0

- 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.

А	screen	similar	to	the	following	displays.
---	--------	---------	----	-----	-----------	-----------

System	Sw	itching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Ro	uter Discovery	VRRP Multicast	IPv6 Multicast	
RIF	5		RIP II	nte <mark>r</mark> face Ci	onfiguration					
•Basic		v	12	3 VLANS	All					
Advanced	ation	^		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Key	Authentication Key ID
- Kir Conligui	ation	22		1/0/13	RIP-2 ×	RIP-2 ×	Enable 🛩	None 🗸		0
 Interface Cor 	mgurati	on	0	1/0/1	RIP-2	Both	Disable	None		0
 Route Redist 	tribution			1/0/2	RIP-2	Both	Disable	None		0
				1/0/3	RIP-2	Both	Disable	None		0
				1/0/4	RIP-2	Both	Disable	None		0
				1/0/5	RIP-2	Both	Disable	None		0
				1/0/6	RIP-2	Both	Disable	None		0
				1/0/7	RIP-2	Both	Disable	None		0
				1/0/8	RIP-2	Both	Disable	None		0
				1/0/9	RIP-2	Both	Disable	None		0
				1/0/10	RIP-2	Both	Disable	None		0
				1/0/11	RIP-2	Both	Disable	None		0
				1/0/12	RIP-2	Both	Disable	None		0
				1/0/13	RIP-2	Both	Disable	None		0

- **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.

System	Sv	vitching		Routing		QoS	Securi	iy	Monitoring		Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP	Multicast	IPv6 Multicast	
Multica	ıst		Global	Configui	ation								
 Mroute Table 			Admi	n Mode			0	Disable	Enable				
 Global Configura 	ation		Proto	col State	Э		No	n-Opera	itional				
nterface Configuration			Table	Maximu	im Enti	y Count	204	8					
- DVMRP		×	Proto	ol			No	Protoco	ol Enabled				
IGMP		¥	Table	Entry C	ount		0						
• PIM	ame → M →												
Static Routes Configuration													
 Admin Boundary Configuration 	/												

- **b.** For Admin Mode, select the **Enable** radio button.
- c. Click Apply.
- 9. Enable PIM-DM globally.
 - a. Select Routing > Multicast > PIM > Global Configuration.

System	SI	witching		Routing		QoS	Securit	y Monit	oring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discov	ery VRR	P Multicast	IPv6 Multicast	
Multicas	st		PIM G	lobal Cor	figurati	on						
Mroute Table			Admi	n Mode		Disa	ble PIM-S	M O PIM-DM				
Global Configura	tion											
 Interface Configu 	iratio	n										
• DVMRP		~										
• IGMP		~										
• PIM		^										
Global Configu	iratio	n										

- **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.

System	Switching		Routing	QoS	Security	Monitorin	g Mai	ntenance Hel	p Inde	×		
Routing Table	IP IPv6	VLA!	ARP	RIP OSPF	OSPFV3 R	outer Discovery	VRRP	Necrosit IPv6 Multi	cast			
Multica	ist	PIM	Interface Ci	onfiguration								
Mroute Table		12	3 VLANS	All						0	to To Interface	Go
Global Configure	ation		Sector State	1200000000000000	ICCOMPANY AND IN	INCOMPANY AND			No. State Contraction	DESILOS SOLUTION	INTERNATION CONTRACTOR OF CONTRACTOR	and the second se
Interface Config	puration		interface	Admin Mode	Protocol State	IP Address	Hello Interval	Join/Prune Interval	BSR Border	DR Priority	Designated Router	Neighbor Count
• DVMRP				*					*			
+IGMP	<u></u>	1	1/0/1	Disable	Non-Operationa	192 168 2.2	30	60	Disable	1		
- Horan		12	1/0/2	Disable	Non-Operationa	0.0.0.0	30	60	Disable	1		
• PIM	÷	0	1/0/3	Disable	Non-Operationa	0.0.0.0	30	60	Disable	1		
· Global Config	guration	10	1/0/4	Disable	Non-Operationa	0.0.0.0	30	60	Disable	1		
· SSM Configu	ration	8	1/0/5	Disable	Non-Operationa	0.0.0.0	30	60	Disable	1		
Ocara Gonaga	madom	0	1/0/6	Disable	Non-Operationa	0.0.0.0	30	60	Disable	1		
 Interface Con 	figuration	0	1/0/7	Disable	Non-Operationa	0.0.0.0	30	60	Disable	1		-
· PIM Neighbo	e i		1/0/8	Disable	Non-Operationa	0.0.0.0	30	60	Disable	1		
* Candidate RF	2		1/0/9	Disable	Non-Operationa	192.168.3.1	30	60	Disable	1		
Configuration			1/0/10	Disable	Non-Operationa	0.0.0.0	30	60	Disable	1		
·BSR Candida	ite	10	1/0/11	Disable	Non-Operationa	0.0.0.0	30	60	Disable	1		
Configuration		8	1/0/12	Disable	Non-Operationa	0000	30	60	Disable	1		
Static RP		1	1/0/13	Disable	Non-Operationa	1 192 168 1 2	30	60	Disable	4		
Configuration			1/0/14	Disable	Non-Operationa	0.0.0.0	30	60	Disable	1		

- 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.

System	SI	witching		Routing		QoS	Securit	у	Monitoring]	Maintenance	Help	Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast	
IP	<u>h</u>		IP Con	figuration									
•Basic	Basic .				o Live				64				
 IP Configurat 	tion		Routi	ng Mode					Enable	e 🔘 Disat	ole		
 Statistics 			ICMP	Echo R	eplies				Enable	e 🔘 Disab	ole		
 Advanced 	•Statistics			Redirec	s				Enable	e 🔵 Disab	ole		
			ICMP	Rate Lir	nit Inte	rval			1000		(0 to 21-	47483647 ms)	
			ICMP	Rate Lir	nit Bur	st Size			100		(1 to 200	2)	

- **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.

System	S۱	witching		Routin	g	QoS	Securit	y Mor	itoring	Maintenance	Help	Index		
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Disco	very VRRF	^o Multicast	IPv6 Multicast			
IP	2		IP Int	erface C	onfigurat	ion								
• Basic		~	12	3 VI AN	S All									
Advanced		~			9. J. NI	_				0	10	-	_	10
• IP Configurat	ion		۲	Port	Descrip	ption	VLAN ID	IP Address Method	Configuration	IP Address	Subnet Mask	Rou Moi	iting de	Administrative Mode
• Statistics				1/0/10				Manual ~		192.168.3.2	255.255.2	55.0 Er	iable 🛩	Enable 🛩
• IP Interface	8			1/0/1				None		0.0.0.0	0.0.0.0	Dis	able	Enable
Configuration	1			1/0/2				None		0.0.0.0	0.0.0.0	Dis	able	Enable
 Secondary IF 	0			1/0/3				None		0.0.0.0	0.0.0.0	Dis	able	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.

System	S۱	witching		Routin	g	QoS	Security	/ Monitoring	Maintenano	ce Help	Index	ľ	
Routing Table		IPv6	VLAN	I ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP Multicas	t IPv6 Multicas	it		
IP			IP Int	erface C	onfigurati	on							
• Basic		~	1 2	3 VLAN	S All	11							
 Advanced 		~					1		an i	Colored States	D-V	2011 C	W description of the
 IP Configurat 	on			Port	Descrip	tion	VLAN ID	Method	IP Address	Mask	Mod	de	Mode
 Statistics 				1/0/11				Manual 🗸	192.168.5.	1 255.25	5.255.0 En	iable 🗸	Enable 👻
• IP Interface				1/0/1				None	0.0.0.0	0.0.0	Dis	able	Enable
Conliguration		- 28		1/0/2				None	0.0.0.0	0.0.0.0	Dis	able	Enable
 Secondary IF 				1/0/3				None	0.0.0.0	0.0.0.0	Dis	able	Enable

- 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.

System	S	witching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Rou	ter Discovery	VRRP Multicast	IPv6 Multicast	
RI	P		RIP I	nterface Co	onfiguration					
• Basic		~	12	3 VLANS	All					
• Advanced		~		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Key	Authentication Key ID
• RIP Contigui	ration			1/0/10	RIP-2 V	RIP-2 ×	Enable v	None -		0
 Interface Co 	nfigura	tion		1/0/1	RIP-2	Both	Disable	None	8	0
 Route Redis 	stributi	on		1/0/2	RIP-2	Both	Disable	None		0
				1/0/3	RIP-2	Both	Disable	None		0
				1/0/4	RIP-2	Both	Disable	None		0
				1/0/5	RIP-2	Both	Disable	None		0
				1/0/6	RIP-2	Both	Disable	None		0
				1/0/7	RIP-2	Both	Disable	None		0
				1/0/8	RIP-2	Both	Disable	None		0
				1/0/9	RIP-2	Both	Disable	None		0
				1/0/10	DID 2	Both	Dicabla	Nono		0

- 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.

System	Sv	witching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Rou	ter Discovery	VRRP Multicast	IPv6 Multicast	
RIF	þ		RIP Ir	nterface Co	onfiguration					
• Basic		*	12	3 VLANS	All					
• Advanced	ation	^		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Key	Authentication Key ID
- RiF Conligui	ation	en in 1		1/0/11	RIP-2 ¥	RIP-2 ×	Enable ~	None ~		
Interface Cor	ingurat	lion		1/0/1	RIP-2	Both	Disable	None		0
 Route Redist 	ributio	n		1/0/2	RIP-2	Both	Disable	None		0
				1/0/3	RIP-2	Both	Disable	None		0
				1/0/4	RIP-2	Both	Disable	None		0
				1/0/5	RIP-2	Both	Disable	None		0
				1/0/6	RIP-2	Both	Disable	None		0
				1/0/7	RIP-2	Both	Disable	None		0
				1/0/8	RIP-2	Both	Disable	None		0
				1/0/9	RIP-2	Both	Disable	None		0
				1/0/10	RIP-2	Both	Disable	None		0
				1/0/11	RIP-2	Both	Disable	None		0

- 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.

System		witching		Routing		QoS	Securi		Monitoring		Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router	Discovery	VRRP	Multicast	IPv6 Multicast	×
Multic	ast		Global	Configur	ation								
 Mroute Table 			Admi	n Mode			0	Disable (Enable				
 Global Configu 	ration		Proto	col State	Э		Nor	n-Operat	onal				
 Interface Config 	guratio	on	Table	Maximu	m Entr	y Count	204	18					
• DVMRP	Proto	col			No	Protocol	Enabled						
• IGMP	GMP 🗸			Entry C	ount		0						
- PIM		~											

- **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.

System	SI	witching		Routing		QoS	Securit	y Monitoring		Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast	
Multica	ast		PIM GI	obal Cor	nfigurat	ion						
Mroute Table			Admi	n Mode		Disa	ble 🔘 PIM-S	SM 💿 PIM-DM				
Global Configu	ration											
 Interface Config 	guratio	n										
• DVMRP		~										
• IGMP		~										
• PIM		~										
Global Config	guratio	n										

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.

System	Switching		Routing	QoS	Security	Monitoria	ig Mair	stenance Hel	p Inde	<		
Routing Table	P IPv6	VLA	ARP	RIP OSPF	OSPEV3 Rd	uter Discovery	VRRP	Nitoward IPv6 Multi	cast			
Multicas	6 I.	PIM	Interface C	onfiguration								
Mroute Table		12	3 VLANS	All						0	So To Interface	Go
Global Configural	ion	1		A CONTRACTOR	-	-	N 80 Y 20 Y					
Interface Configu	ration	1	Interface	Admin Mode	Protocol State	aP Address	Ptebo Interval	Join/Prune Interval	ESSR Border	DR Phority	Designated Router	Neighbor Count
- DVMRP	4			*			-		~	·		
- IGMP	0	13	1/0/1	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
- ICHIN		0	1/0/2	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
• PIM		83	1/0/3	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
· Global Configu	ration	10	1/0/4	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
+ SSM Configure	tion	10	1/0/5	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
Colin Colinguis	1001	E	1/0/6	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
 Interface Config 	puration	0	1/0/7	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
+ PIM Neighbor		0	1/0/8	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
· Candidate RP		63	1/0/9	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
Configuration			1/0/10	Disable	Non-Operational	192.168.3.2	30	60	Disable	1		
·BSR Candidate			1/0/11	Disable	Non-Operational	192.168.5.1	30	60	Disable	1		
Configuration		63	1/0/12	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.

System Switching		Routing			QoS	Securi	ty	Monitoring		Maintenance	Help	Index	
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP	Multicast	IPv6 Multicast	
IP			IP Con	figuration	1								
• Basic		~	Defau	lt Time t	o Live				64				
• IP Configuration	n		Routi	ng Mode					Enable	e 🔘 Disal	ble		
 Statistics 			ICMP	Echo R	eplies				Enable	e 🔘 Disal	ble		
 Advanced 		×	ICMP	Redirec	ts				Enable	e 🔘 Disal	ble		
			ICMP	Rate Li	mit <mark>In</mark> te	rval			1000		(0 to 21	47483647 ms)	
			ICMP	Rate Li	nit Bur	st Size			100		(1 to 20	0)	

- **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.

System	Switching		Switching Rout		Routing QoS		Securit	y Monitoring	Maintenance	Help	index		
Routing Table	IP.	IPv6	VLAN	I ARP	RIP	OSPF	OSPFv3	Router Discovery VF	RP Multicast	IPv6 Multicast			
IP			IP Int	erface C	onfigurati	on							
Basic		~	12	3 VLAN	S All								
 Advanced 		~					1		and		-		
• IP Configura	tion			Port	Descrip	tion	VLAN ID	Method	IP Address	Mask	Mode		Mode
 Statistics 				1/0/21				Manual 🛩	192,168.5.2	255.255.25	5.0 Enable	~	Enable ~
• IP Interface				1/0/1				None	0.0.0.0	0.0.0.0	Disable		Enable
Configuratio	113			1/0/2				None	0.0.0.0	0.0.0.0	Disable		Enable
 Secondary I 	P			1/0/3				None	0000	0 0 0 0	Disable		Enable

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.

System	Switching		ng Routing		ing QoS		Securit	y Monitoring	-10	Maintenance	Help	Help Index		
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	/RRP	Multicast	IPv6 Multicast			
IP			IP Int	erface C	onfigurati	on								
•Basic		~	12	3 VLAN	s All									
Advanced		^					1	ID Address OccEssion			Dokast	Dec		A destatute and a
 IP Configurat 	ion			Port	Descrip	tion	VLAN ID	Method	aton	IP Address	Mask	Mod	le le	Mode
 Statistics 				1/0/22				Manual 🗸		192.168.6.1	255.255.2	55.0 Er	able 🗸	Enable 👻
• IP Interface				1/0/1				None		0.0.0.0	0.0.0.0	Dis	able	Enable
Conliguration	1			1/0/2				None		0.0.0.0	0.0.0.0	Dis	able	Enable
 Secondary IF 	2			1/0/3				None		0.0.0.0	0.0.0	Dis	able	Enable

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.
| System | S | witching | | Routing | QoS | Security | Monitoring | Maintenance | Help | Index |
|----------------------------------|----------|----------|-------|-------------|--------------|-----------------|----------------|---------------------|--------------------|-----------------------|
| Routing Table | IP | IPv6 | VLAN | ARP | RIP OSPF | OSPFv3 Rou | iter Discovery | VRRP Multicast | IPv6 Multicast | |
| RIF | 2 | | RIP I | nterface Co | onfiguration | | | | | |
| • Basic | | ~ | 1 2 | 3 VLANS | All | | | | | |
| Advanced | | ^ | | Interface | Send Version | Receive Version | RIP Mode | Authentication Type | Authentication Key | Authentication Key ID |
| • RIP Comigur | ation | | | 1/0/21 | RIP-2 👻 | RIP-2 × | Enable 🗸 | None 👻 | | |
| • Intenace Cor | niigura | uon | | 1/0/1 | RIP-2 | Both | Disable | None | | 0 |
| Route Redist | tributio | n | | 1/0/2 | RIP-2 | Both | Disable | None | | 0 |

- 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.

System	Swit	ching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP I	Pv6	VLAN	ARP	RIP OSPF	OSPFv3 Rou	ter Discovery	VRRP Multicast	IPv6 Multicast	
RIP			RIP In	terface C	onfiguration					
Basic		~	12	3 VLANS	All					
 Advanced 		^		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Key	Authentication Key ID
• RIP Configura	ition			4(0/22			Fachle	New	Automication (Key	o a
 Interface Conf 	figuratio	n		1/0/22	RIP-2 *	RIP-2 *	Enable *	None *		0
* Douto Dodiotr	ibution		L	1/0/1	RIP-2	Both	Disable	None		0
- Route Reulsti	ibution			1/0/2	RIP-2	Both	Disable	None		0

- b. In the Interface list, select 1/0/22.
- c. For RIP Admin Mode, select the **Enable** radio button.
- d. Click Apply.
- 6. Enable mulicast globally.
 - a. Select Routing > Multicast > Global Configuration.

System	S	vitching		Routing		QoS	Securit	у	Monitoring		Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast	
Multic	ast		Global	Configur	ation								
Mroute Table			Adm	iin Mode	(0	Disab	le 🖲 Enable				
 Global Configu 	ration		Prote	ocol Stat	е		No	n-Ope	rational				
 Interface Config 	guratio	n	Table	e Maxim	um Ent	try Count	20-	48					
• DVMRP		Y	Prote	ocol			No	Proto	col Enabled				
•IGMP		~	Table	e Entry C	ount		0						
• PIM		×											
Static Routes Configuration													
Admin Bounda Configuration	гу												

- **b.** For Admin Mode, select the **Enable** radio button.
- c. Click Apply.
- 7. Enable PIM-DM globally.
 - a. Select Routing > Multicast > PIM > Global Configuration.

System	S	witching		Routing		QoS	Securit	y	Monitoring	, []	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP		IPv6 Multicast	~
Multica	ast		PIM GI	obal Cor	figurati	on							
Mroute Table		20	Admi	n Mode		O Disa	ble 🔘 PIM-S	SM 🖲	PIM-DM				
Global Configu	ration												
 Interface Config 	guratio	'n											
• DVMRP		~											
• IGMP		~											
• PIM		~											
Global Config	guratio	m											
• SSM Configu	iration												
 Interface Cor 	nfigura	tion											

- **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.

System	Switchin	9	Routing	QoS	Security	Monitoria	ng Mair	tenance Hel	p Inde			
Routing Table	IP IPv6	VI.A	N ARP	RIP OSPF	OSPFV3 Ro	uter Discovery	VRRP !	Unceall IPv6 Multi	cast			
Multica	st	PIM	Interface C	onfiguration								
Mroute Table		12	2 3 VLANS	All						(io To Interface	Go
Global Configur Interface Config	ation uration		Interface	Admin Mode	Protocol State	IP Address	Hello Interval	Join/Prune Interval	BSR Border	DR Priority	Designated Router	Neighbor Count
+DVMRP	~			Enable 👻					÷			
· IGMP	~		1/0/1	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
- DIM			1/0/2	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
		10	1/0/3	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
 Global Config 	uration	. 6	1/0/4	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
• SSM Configu	ration	6	1/0/5	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
	and the second se	0	1/0/6	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
 Interface Con 	nguration	10	1/0/7	Disable	Non-Operational	0.0.0.0	30	60	Disable	3		
 PIM Neighbor 		6	1/0/8	Disable	Non-Operational	0000	30	60	Disable	1		

- 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.

System	Sv	vitching		Routing		QoS	Securit	y	Monitoring)	Maintenance	Help	Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router I	Discovery	VRRP	Multicast	IPv6 Multicast	
IP	Ż		IP Cor	figuration									
Basic		~	Defa	ult Time to	o Live				64				
• IP Configurat	ion		Routi	ng Mode					Enable	e 🔵 Disab	le		
 Statistics 			ICMF	Echo Re	eplies				Enable	e 🔘 Disab	le		
 Advanced 		×	ICMF	Redirect	ts				Enable	e 🔘 Disab	le		
			ICMF	Rate Lir	nit Inte	rval			1000		(0 to 21	47483647 ms)	
			ICMF	^o Rate Lir	nit Bur	st Size			100		(1 to 200	D)	

- 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.

System	S	witching		Routin	g	QoS	Securit	y Monitoring		Maintenance	Help	Index		
Routing Table		IPv6	VLAN	ARF	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast			
IP			IP Int	erface C	onfigurat	ion								
•Basic		~	1 2	3 VLAN	S All									
 Advanced 		^		-				ID Address Conferen	-	and a second	Colorest	Dec		Administration
• IP Configurati	on			Port	Descrip	tion	VLAN ID	Method	ation	IP Address	Mask	Mo	de	Mode
• Statistics				1/0/21				Manual 👻		192.168.2.1	255.255.2	55.0 Er	nable 🛩	Enable 👻
• IP Interface				1/0/1				None		0.0.0.0	0.0.0	Dis	able	Enable
Configuration				1/0/2				None		0.0.0.0	0.0.0.0	Dis	able	Enable
 Secondary IP 	S.			1/0/3				None		0.0.0.0	0.0.0	Dis	able	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.

System	S	witching		Routin		QoS	Security	y Monitoring	Maintenance	Help	index		
Routing Table	IP.	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery VRR	P Multicast	IPv6 Multicast			
IP			IP Int	erface C	onfigurati	on							
Basic		~	12	3 VLAN	S All								
 Advanced IP Configuration 	ion	~		Port	Descrip	tion	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Routi Mode	ng	Administrative Mode
 Statistics 				1/0/22	1			Manual 🛩	192.168.6.2	255.255.25	5.0 Ena	ble 🛩	Enable 🗸
IP Interface Configuration	i.			1/0/1				None None	0.0.0.0	0.0.0.0	Disab Disab	le le	Enable Enable
 Secondary II 	5			1/0/3				None	0.0.0.0	0.0.0.0	Disat	le	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.

System	Switching		Routin	g	QoS	Security	y Monitoring	Maintenance	Help	Index	
Routing Table IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery VRF	RP Multicast	IPv6 Multicast		
IP • Basic	~	IP Int	erface C 3 VLAN	onfigurat S All	ion						
 Advanced IP Configuration 	~		Port	Descrip	tion	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Routing Mode	Administrative Mode
 Statistics 			1/0/24				Manual 👻	192.168.4.1	255.255.255.0	Enable 🗸	Enable ×
IP Interface Configuration			1/0/1				None	0.0.0.0	0.0.0.0	Disable Disable	Enable Enable
 Secondary IP 		0	1/0/3				None	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 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.

System	Swi	tching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP I	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Rou	iter Discovery	VRRP Multicast	IPv6 Multicast	
RIF	Ð		RIP Ir	iterface Co	onfiguration					
•Basic		~	12	3 VLANS	All					
 Advanced 		^		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Key	Authentication Key ID
 RIP Configur 	ation			1/0/21	RIP-2 ×	RIP-2 ×	Enable 👻	None Y		0
 Interface Cor 	niguratio	n	0	1/0/1	RIP-2	Both	Disable	None		0
 Route Redist 	tribution			1/0/2	RIP-2	Both	Disable	None		0
				1/0/3	RIP-2	Both	Disable	None		0

- 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.

System	S	witching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Rou	ter Discovery	VRRP Multicast	IPv6 Multicast	
RIP	19		RIP II	nterface C	onfiguration					
• Basic		~	1 2	3 VLANS	All					
Advanced		^		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Key	Authentication Key ID
• RIP Configura	ation	1		1/0/22	RIP-2 ¥	RIP-2 ×	Enable 👻	None 😽		0
• Internace Con	ngura	uon		1/0/1	RIP-2	Both	Disable	None		0
 Route Redistr 	ributic	n		1/0/2	RIP-2	Both	Disable	None		0
				1/0/3	RIP-2	Both	Disable	None		0

- 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.

System	S	witching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Rou	ter Discovery	VRRP Multicast	IPv6 Multicast	
RIF	Þ		RIP I	nterface C	onfiguration					
•Basic		Ý	12	3 VLANS	All					
 Advanced 		^		Interface	Cond Varaian	Persona Voroion	DID Mada	Authentisation Tuna	Authoritication Var	Authoptioption Key (D
* RIP Configur	ation			mtenace	Send version	Receive Version	PGF WOUE	Addrendication Type	Authentication Key	Additionation Rey 10
la constante de		11111		1/0/24	RIP-2 ¥	RIP-2 ×	Enable 🛩	None 🛩		0
 Interface Cor 	nhgura	tion	n	1/0/1	RIP-2	Both	Disable	None		0
Route Redist	tributio	n		1/0/2	RIP-2	Both	Disable	None		0
				1/0/3	RIP-2	Both	Disable	None		0

- 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.

System	Switching		Routing		QoS	Securi	ty	Monitoring		Maintenance	Help	Index
Routing Table IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Route	r Discovery	VRRP	Multicast	IPv6 Multicast	
Multicast		Global	Configu	ration								
Mroute Table		Admi	n Mode			۲	Disa <mark>bl</mark> e	Enable				
 Global Configuration 	i i	Proto	col State	е		No	n-Opera	tional				
Interface Configurati	on	Table	Maximu	m Entry	Count	204	48					
• DVMRP	~	Proto	col			No	Protoco	l Enabled				
• IGMP	×	Table	Entry C	ount		0						
• PIM	~											
Static Routes Configuration												
Admin Boundary Configuration												

- **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.

System	S	witching		Routing		QoS	Securit	ý	Monitoring	,	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Route	er Discovery	VRRP	Multicast	IPv6 Multicast	
Multica	ast		PIM G	lobal Cor	nfigurat	on							
• Mroute Table			Admi	n Mode		🔘 Disa	ble 🔘 PIM-S	SM 💿 F	PIM-DM				
Global Configu	ration												
 Interface Config 	guratio	on.											
• DVMRP		~											
IGMP		~											
- PIM		~											
Global Config	guratio	m											

- **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.

System	Sm	tching		Routing	QoS	Security	Monitoni	ig Mair	tenance Hel	p Inde	×		
Routing Table	IP	IPv6	VLA	ARP	RIP OSPF	OSPEV3 R	outer Discovery	VRRP	Moned IPv6 Multi	cast			
Multicas	ıt.		PIM	Interface C	onfiguration								
Mroute Table			12	3 VLANS	Al						0	So To Interface	Go
Global Configura	tion				Waterman	REPORTED STATISTICS	-	No. of Concession, Name		FORENESS	Records	Personal second second second	and the second se
Interface Configu	ration		1	Interface	Admin Mode	Protocol State	IP Address	Hello Interval	Join/Prune Interval	BSR Border	OR Priority	Designated Router	Neighbor Count
• DVMRP		4			Enable *						1		
. IGMP		- 6	0	1/0/1	Disable	Non-Operationa	0.0.0.0	30	60	Disable	1		
• 103mil*		1	0	1/0/2	Disable	Non-Operationa	0.0.0.0	30	60	Disable	1		
• PIM		-	- 13	1/0/3	Disable	Non-Operationa	0.0.0.0	30	60	Disable	1		
Global Configu	ration		63	1/0/4	Disable	Non-Operationa	0.0.0.0	30	60	Disable	1		
+ SSM Configur	ation		E	1/0/5	Disable	Non-Operationa	0.0.0.0	30	60	Disable	1		
Com Connigan	NUMPE	-	10	1/0/6	Disable	Non-Operationa	0.0.0.0	30	60	Disable	1		
 Interface Config 	Bruger	ors 👘	(3	1/0/7	Disable	Non-Operationa	0.0.0.0	30	60	Disable	1		
 PIM Neighbor 			0	1/0/8	Disable	Non-Operationa	0000	30	60	Disable	1		

- 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.

System	Switching			Routing		QoS	Securit	у	Monitoring		Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	iter Discovery	VRRP		IPv6 Multicast	
Multica	ast		IGMP	Global C	onfigura	ation							
Mroute Table			Admi	n Mode		O Disal	ble 🖲 Enabl	e					
Global Configu	ration												
Interface Config	guratio	n											
• DVMRP		~											
• IGMP		~											
Global Config	guratio	m											

- **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.

System	Swite	ching		Routing	QoS	Securi	ty Mor	nitoring	Maintenance	Help	Index		
Routing Table	IP IF	Pv6	VLAN	ARP	RIP OSPF	OSPFv3	Router Disc	overy VRR	P Multicast	IPv6 Multicast			
Multica	ist		IGMP	Routing Ir	nterface Config	uration							
Mroute Table			12	3 VLANS	All						Go To	Interface	Go
Global Configui	ation				1000			l'a	litest res	files and	New Cost	1	
 Interface Config 	juration			Interface	Admin Mode	Version	Robustness	Query Interval	Query Max Response Time	Startup Query Interval	Startup Query Count	Last Member Query Interval	Last Member Query Count
• DVMRP		~		1/0/24	Enable ×	V3	2	125	100	31	2	10	2
• IGMP		~		1/0/1	Disable	V3	2	125	100	31	2	10	2
Global Confid	uration			1/0/2	Disable	V3	2	125	100	31	2	10	2
Routing Inter	laco			1/0/3	Disable	V3	2	125	100	31	2	10	2
Configuration				1/0/4	Disable	V3	2	125	100	31	2	10	2

- 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 59. 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 192.168.2.2 255.255.0
(Netgear Switch) (Interface 1/0/1)#ip rip
```

```
(Netgear Switch) (Interface 1/0/1)#ip pim
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/9
(Netgear Switch) (Interface 1/0/9)#ip address 192.168.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/9)#ip rip
(Netgear Switch) (Interface 1/0/9)#ip pim
(Netgear Switch) (Interface 1/0/9)#exit
(Netgear Switch) (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 rip
(Netgear Switch) (Interface 1/0/13)#ip pim
```

PIM-SM on Switch B

 Enable the switch to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

```
(Netgear Switch)#configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim spars
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#ip pim rp-candidate interface 1/0/11 225.1.1.1
255.255.255.0
```

2. Enable the switch to announce its candidacy as a bootstrap router (BSR).

```
(Netgear Switch) (Config)#ip pim bsr-candidate interface 1/0/10 30 7
(Netgear Switch) (Config)#interface 1/0/10
(Netgear Switch) (Interface 1/0/10)#routing
(Netgear Switch) (Interface 1/0/10)#ip address 192.168.3.2 255.255.255.0
(Netgear Switch) (Interface 1/0/10)#ip pim
(Netgear Switch) (Interface 1/0/10)#ip pim
(Netgear Switch) (Interface 1/0/10)#exit
(Netgear Switch) (Interface 1/0/11)#routing
(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
```

PIM-SM on Switch C

```
(Netgear Switch)#configure
(Netgear Switch) (Config) #ip routing
(Netgear Switch) (Config) #ip pim sparse
(Netgear Switch) (Config) #ip multicast
(Netgear Switch) (Config)#ip pim rp-candidate interface 1/0/22 225.1.1.1
255.255.255.0
(Netgear Switch) (Config) #ip pim bsr-candidate interface 1/0/21 30 5
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21) #routing
(Netgear Switch) (Interface 1/0/21)#ip address 192.168.5.2 255.255.255.0
(Netgear Switch) (Interface 1/0/21) #ip rip
(Netgear Switch) (Interface 1/0/21) #ip pim
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) (Config)#interface 1/0/22
(Netgear Switch) (Interface 1/0/22) #routing
(Netgear Switch) (Interface 1/0/22)#ip address 192.168.6.1 255.255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22) #ip pim
(Netgear Switch) (Interface 1/0/22) #exit
```

PIM-SM on Switch D

```
(Netgear Switch)#configure
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config) #ip routing
(Netgear Switch) (Config) #ip igmp
(Netgear Switch) (Config) #ip pim
(Netgear Switch) (Config) #ip pim rp-candidate interface 1/0/22 225.1.1.1
255.255.255.0
(Netgear Switch) (Config) #ip pim bsr-candidate interface 1/0/22 30
                                                                       3
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21) #routing
(Netgear Switch) (Interface 1/0/21)#ip address 192.168.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/21)#ip rip
(Netgear Switch) (Interface 1/0/21) #ip pim
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) (Config)#interface 1/0/22
(Netgear Switch) (Interface 1/0/22) #routing
(Netgear Switch) (Interface 1/0/22)#ip address 192.168.6.2 255.255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22) #ip pim
(Netgear Switch) (Interface 1/0/22)#exit
```

```
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#routing
(Netgear Switch) (Interface 1/0/24)#ip address 192.168.4.1 255.255.255.0
(Netgear Switch) (Interface 1/0/24)#ip rip
(Netgear Switch) (Interface 1/0/24)#ip jmm
(Netgear Switch) (Interface 1/0/24)#ip pim
(Netgear Switch) (Interface 1/0/24)#exit
```

PIM-SM builds the multicast route table on each switch. The following tables show the routes that are built after PIM-SM switches to the source-specific tree from the shared tree.

(A) #show ip n	ncast mroute s	ummary		
	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 r	ncast mroute s	ummary	_	
	Multicas	t Route Table	e 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 n	ncast mroute s	ummary		
	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) #about in a	agat myouto a			
(D) #SHOW IP (Multicast Multicast	Douto Table	Cummona	
	MUILICAST	ROULE TADIE	Junilliary	Outgoing
	a		Incoming	outgoing
Source IP	Group IP	Protocol	Interface	Interface List
+		DIMON	1 (0 (2 2	1 /0 /04
100 100 1 1	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.

System	S	witching		Routing		QoS	Securit	y N	lonitoring	N	<i>l</i> aintenance	Help	Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Di	scovery	VRRP	Multicast	IPv6 Multicast	
IP			IP Con	figuration	l)								
 Basic 		^	Defau	ult Time t	o Live			6	54				
• IP Configurat	tion		Routi	ng Mode				6	Enable	O Disab	le		
 Statistics 			ICMF	Echo R	eplies			6	Enable	O Disab	le		
 Advanced 		×	ICMF	Redirec	ts			6	Enable	O Disab	le		
			ICMF	Rate Lin	nit Inte	rval			1000		(0 to 21.	47483647 ms)	
			ICMF	PRate Lin	nit <mark>B</mark> ur	st Size			100		(1 to 200)	

- **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.

System	Sw	ritching	i.	Routin	9	QoS	Security	y Monitoring	Mainte	enance	Help	Index		
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery V	RRP Mu	lticast	IPv6 Multicast			
IP			IP Int	erface C	onfigurat	ion								
•Basic		~	12	3 VLAN	S All									
• Advanced		1						10 x 11 x 1 x 1 x 1 x 1 x 1 x 1 x 1 x 1	023207		0.1	D -	name.	William States and States
• IP Configurati	on		U,	Port	Descrip	otion	VLAN ID	Method	IP Ad	dress	Mask	Mo	uting de	Mode
 Statistics 				1/0/1				Manual 🗸	192.1	68.2.2	255.255.25	55.0 E	nable 👻	Enable ×
• IP Interface				1/0/1				None	0.0.0.	0	0.0.0.0	Dis	able	Enable
Configuration				1/0/2				None	0.0.0.	0	0.0.0.0	Dis	sable	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.
---	--------	---------	----	-----	-----------	-----------

System	S	witching		Routin	3	QoS	Security	y Monitoring	Maintenance	Help	Index	
Routing Table	J.P.	IPv6	VLAN	I ARP	RIP	OSPF	OSPFv3	Router Discovery VRR	P Multicast	IPv6 Multicast		
IP			IP Int	erface C	onfigurat	ion						
Basic		~	1 2	3 VLAN	5 All							
Advanced • IP Configuration	on	*		Port	Descrip	otion	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Routing Mode	Administrative Mode
 Statistics 				1/0/9				Manual 🛩	192.168.3.1	255.255.25	5.0 Enable	Enable Y
IP Interface Configuration				1/0/1				None	0.0.0.0	0.0.0.0	Disable	Enable
• Secondary IP				1/0/2				None	0.0.0.0	0.0.0.0	Disable	Enable
				1/0/5				None	0.0.0.0	0.0.0.0	Disable	Enable
				1/0/0				None	0.0.0.0	0.0.0.0	Disable	Enable
				1/0/9				None	0.0.0.0	0.0.0.0	Enable	Enable

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.

System	S	witching		Routin	g	QoS	Securit	y Monitoring	Maintenance	e Help	Index	67	
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery VF	RRP Multicast	IPv6 Multicast			
IP			IP Int	erface C	onfigurati	on							
• Basic		~	1 2	3 VLAN	s All								
Advanced		^						ID ALL OLD V			D	2	
• IP Configurati	ion			Port	Descrip	tion	VLAN ID	Method	IP Address	Mask	Moc	ting le	Administrative Mode
• Statistics				1/0/13				Manual 👻	192.168.1.2	255.255.2	55.0 En	able 🛩	Enable ~
• IP Interface				1/0/1				None	0.0.0.0	0.0.0.0	Disa	able	Enable
Configuration				1/0/2				None	0.0.0.0	0.0.0.0	Disa	able	Enable
 Secondary IF 				1/0/3				None	0.0.0.0	0.0.0.0	Disa	able	Enable
				1/0/4				None	0.0.0.0	0.0.0.0	Disa	able	Enable

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.

System	Sw	itching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Rou	ter Discovery	VRRP Multicast	IPv6 Multicast	
RIP	D		RIP In	terface Co	onfiguration					
•Basic		~	12:	VLANS	All					
Advanced		^		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Key	Authentication Key ID
RIP Configuration	ation	on		1/0/1	RIP-2 ×	RIP-2 ×	Enable 👻	None Y		- 0
Interface Config	nyurau	on		1/0/1	RIP-2	Both	Disable	None		0
 Route Redist 	tributior	1		1/0/2	RIP-2	Both	Disable	None		0

- 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.

System	Swi	tching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Rou	ter Discovery	VRRP Multicast	IPv6 Multicast	
RIP).		RIP II	nterface Co	onfiguration					
•Basic		~	12	3 VLANS	All					
 Advanced 		^		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication K	ev Authentication Key ID
 RIP Configura 	ation		-	monuco	Cond Version	receive version	TAIL WOOD	a anonaconon rype		cy riddicinication ricy io
Interface Con	figuratio			1/0/9	RIP-2 ×	RIP-2 ×	Enable ~	None Y		0
- Intenace Con	nyurauo	9/IL		1/0/1	RIP-2	Both	Disable	None		0
 Route Redistr 	ribution			1/0/2	RIP-2	Both	Disable	None		0
			-	1/0/3	RIP-2	Both	Disable	None		0

- 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.

System	Swi	itching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	(P	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Rou	iter Discovery	VRRP Multicast	IPv6 Multicast	
RIF	2		RIP Ir	nterface C	onfiguration					
• Basic		~	12	3 VLANS	All					
 Advanced 		^		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Key	Authentication Key ID
• RIP Configur	ation			4/0/42			E II		, activition of the y	
 Interface Cor 	nfiguratio	on		1/0/13	RIP-Z ¥	RIP-Z Y	Enable Y	Ivone Y		U
				1/0/1	RIP-2	Both	Disable	None		0
 Route Redist 	tribution			1/0/2	RIP-2	Both	Disable	None		0
				1/0/3	RIP-2	Both	Disable	None		0

- 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.

System	S١	witching		Routing	1	QoS	Secur	ty	Monitorin	9	Maintenance	e Helj	o 👘	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP	Multicast	IPv6 Multic	ast	
Multica			Global	Configur	ation									
 Mroute Table 	- 1	Admi	n Mode			0	Disable	e 🖲 Enable						
 Global Configura 	Mroute Table Global Configuration			col State	E.		No	n-Oper	ational					
 Interface Configu 	iratio	n	Table	Maximu	m Entr	y Count	20-	48						
DVMRP		×	Proto	col			No	Protoc	ol Enabled					
• IGMP		~	Table	Entry C	ount		0							
• PIM		~												

- **b.** For Admin Mode, select the **Enable** radio button.
- c. Click Apply.
- 9. Enable PIM-SM globally.
 - a. Select Routing > Multicast > PIM > Global Configuration.

System	S	witching		Routing		QoS	Securit	y [Monitoring	j	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP	Multicast	IPv6 Multicast	
(15												
Multica	ist		PIM G	lobal Cor	figurat	ion							
• Mroute Table			Admi	n Mode		O Disa	ble 💿 PIM-S	SM O F	PIM-DM				
Global Configur	ation												
 Interface Config 	juratio	m											
• DVMRP		~											
- IGMP		~											
• PIM		~											
Global Config	juratio	n											
• SSM Configu	ration	0											

- **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.

System	Switching		Routing	QoS	Security	Monitorin	ig Mair	itenance Hel	p Inde	×		
Routing Table	IP IPv6	VLAM	ARP	RIP OSPF	OSPEV3 Ro	uter Discovery	VRRP	nteest IPv6 Mult	cast			
Multica	st	PIM	Interface C	onfiguration								
Mroute Table		12	3 VLANS	All						0	io To Interface	Go
Global Configura	ation	-	-	Sector Sector	Printing Adda	17 Addition	and the second	1000	-	00.0	(Section of the section of the secti	automa com
Interface Config	uration	12	Interface	Admin Mode	Protocol State	IP Address	Hello Interval	Join/Prune Interval	ESR Barder	DR Phonty	Designated Router	Neighbor Count
DVMRP				¥.					~			
IGMP	2		1/0/1	Disable	Non-Operational	192.168.2.2	30	60	Disable	1		
OW			1/0/2	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
1-101		0	1/0/3	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
 Global Config 	uration	- 13	1/0/4	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
• SSM Configur	ation	- 63	1/0/5	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
a state of the state	State Constitution	Ð	1/0/6	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
•Incensee Can	igulation	6	1/0/7	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
 PIM Neighbor 		0	1/0/8	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
Candidate RP		8	1/0/9	Disable	Non-Operational	192.168.3.1	30	60	Disable	1		
Configuration		0	1/0/10	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
·BSR Candidat	te		1/0/11	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
Configuration		0	1/0/12	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
Static RP		0	1/0/13	Disable	Non-Operational	192.168.1.2	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.

System	S	witching]	Routing		QoS	Securi	ty	Monitoring	9	Maintenance	Help	Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast	
IP	Ő.		IP Con	figuratior									
• Basic		~	Defau	lt Time t	o Live				64				
• IP Configurat	lion		Routi	ng Mode					Enable	e 🔘 Disal	ole		
 Statistics 			ICMP	Echo R	eplies				Enable	e 🔘 Disal	ole		
 Advanced 		~	ICMP	Redirec	ts				Enable	e 🔘 Disal	ole		
			ICMP	Rate Li	nit Inte	rval			1000		(0 to 21	47483647 ms)	
			ICMP	Rate Lin	nit Bur	st Size			100		(1 to 20	0)	

- **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.

System Switc	ching		Routing	,	QoS	Securit	y Monitoring	Maintenance	Help	Index		
Routing Table	°v6 ∖	/LAN	ARP	RIP	OSPF	OSPFv3	Router Discovery VF	RP Multicast	IPv6 Multicast			
qı		P Inte	erface Co	onfigurat	ion							
•Basic	¥	12:	3 VLAN	s ali								
 Advanced IP Configuration 	^		Port	Descrip	otion	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Rou Moc	ting le	Administrative Mode
 Statistics 			1/0/10				Manual 👻	192.168.3.2	255.255.25	5.0 En	able 🛩	Enable Y
 IP Interface Configuration 			1/0/1		_		None	0.0.0.0	0.0.0.0	Disa	ible	Enable
• Secondary IP			1/0/2 1/0/3				None None	0.0.0.0	0.0.0.0	Disa Disa	ible ible	Enable Enable

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.

System	S	witching		Routin	g	QoS	Securit	y Monitoring	Maintenance	Help	Index		
Routing Table	Р	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery VRR	P Multicast	IPv6 Multicast			
D			ID Int	orfaco C	opfiqurat	ion							
15		-	117 I.I.L	enace c	onligurat	ION							
• Basic		~	12	3 VLAN	s All								
 Advanced IP Configurat 	ion	^		Port	Descrip	tion	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Routin Mode	g	Administrative Mode
 Statistics 				1/0/11	1			Manual 👻	192.168.5.1	255.255.255	.0 Enab	ile 🗸	Enable 🛩
• IP Interface		10		1/0/1				None	0.0.0	0.0.0.0	Disabl	e	Enable
Configuration				1/0/2				None	0.0.0	0.0.0.0	Disabl	e	Enable
 Secondary IF 	2			1/0/3				None	0.0.0.0	0.0.0.0	Disabl	e	Enable

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.

System	Sv	vitching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Rou	iter Discovery	VRRP Multicast	IPv6 Multicast	
RIP	į		RIP I	nterface Co	onfiguration					
• Basic		~	12	3 VLANS	All					
 Advanced 		^	Ø	Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Key	Authentication Key ID
• RIP Configura	ation		peret	monaco		Tradition Visional	Train Tribudo	radionionion type	- Address and a start and a start and a start a	rightendouron rigy to
- Interface Con	Fourst	ion		1/0/10	RIP-2 Y	RIP-2 ×	Enable ~	None 🛩		0
- intenace con	ngurai	ion -		1/0/1	RIP-2	Both	Disable	None		0
 Route Redistr 	ributio	n		1/0/2	RIP-2	Both	Disable	None		0

- 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.

System	SI	witching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Rou	iter Discovery	VRRP Multicast	IPv6 Multicast	5.
RIF	9		RIP Ir	iterface C	onfiguration					
•Basic		~	12	3 VLANS	All					
 Advanced 		~		1.11.11.1.1.1.1	Oursel Manadara	Design Marsha	DID Mada	Avalation Trans	A about on Mary	Automotive Marcin
• RIP Configur	ation		2	intenace	Send version	Receive Version	RIP Wode	Authentication Type	Authentication Key	Authentication Key ID
in a singer		a contra de la		1/0/11	RIP-2 ×	RIP-2 ×	Enable 🗸	None 🗸		0
 Interface Cor 	ifigural	tion		1/0/1	RIP-2	Both	Disable	None		0
 Route Redist 	tributio	in		1/0/2	RIP-2	Both	Disable	None		0
				1/0/3	RIP-2	Both	Disable	None		0

- 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.

System	S۱	witching		Routing		QoS	Securi	y	Monitoring		Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	er Discovery	VRRP	Multicast	IPv6 Multicast	
Multic	ast		Global	Configur	ation								
• Mroute Table			Admi	n Mode			0	Disabl	e 🖲 Enable				
 Global Configur 	ration		Proto	col State	8		No	n-Oper	ational				
 Interface Config 	guratio	n	Table	Maximu	m Entr	y Count	204	8					
• DVMRP		~	Proto	col			No	Protoc	ol Enabled				
• IGMP		*	Table	Entry C	ount		0						
• PIM		~											
Static Routes Configuration													
 Admin Bounda Configuration 	гу												

- **b.** For Admin Mode, select the **Enable** radio button.
- c. Click Apply.
- 7. Enable PIM-SM globally.
 - a. Select Routing > Multicast > PIM > Global Configuration.

System	S	witching		Routing		QoS	Security	/	Monitoring	,	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast	
	-												
Multica	ist		PIM G	lobal Cor	nfigurat	ion							
Mroute Table			Admi	n Mode		 Disal 	ble PIM-S	M	PIM-DM				
Global Configur	ation												
Interface Config	uratio	n											
• DVMRP		~											
• IGMP		~											
• PIM		^											
Global Config	uratio	in:											
 SSM Configu 	ration												

- **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.

System	Switching		Routing	QoS	Security	Monitoria	9 Mair	stenance Hel	ip inde	×		
Routing Table	IP IPv6	VLAN	ARP	RIP OSPE	OSPEV3 Ro	uter Discovery	VRRP	Internet IPv6 Moto	cast			
Multica	ist	PIM	Interface C	onfiguration								
Mroute Table		12	3 VLANS	All							So To Interface	Go
Global Configure	ation	100	2012	Personal States		Test a la contra de		10-20-00-0			Terroristic Construction	
Interface Config	puration		Internace	Admin Mode	Protocol State	IP Address	Helio intervai	Join/Phine Interval	BSR border	DR Phonty	Designated Houter	Neighbor Count
• DVMRP	~			(¥)					8			
. 1/24.8/3			1/0/1	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
• IGMP		0	1/0/2	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
- PIM			1/0/3	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
Global Config	uration	10	1/0/4	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
+ CCM Confinit	enting	8	1/0/5	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
- aam oomgo	ration		1/0/6	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
 Interface Cont 	figuration	8	1/0/7	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
PIM Neighbor	t	8	1/0/8	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
+Candidate RF		0	1/0/9	Disable	Non-Operational	0.0.0.0	30	60	Disable	4		
Configuration			1/0/10	Disable	Non-Operational	192 168 3 2	30	60	Disable	1		
+BSR Candida	te		1/0/11	Disable	Non-Operational	192 168 5 1	30	60	Disable	1		
Configuration		0	1/0/12	Disable	Non-Operational	0.0.0.0	30	60	Disable	4		

- 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.

System	S	witching		Routing		QoS	Securi	у	Monitoring	,	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router	Discovery	VRRP	Multicast	IPv6 Multicast	
Multica	ast		PIM Ir	nterface S	electio	n							
Mroute Table			Inter	face	T.	1/0/11 ~							
Global Configur	ration												
 Interface Config 	guratio	n											
• DVMRP		~	PIM C	andidate	RP Co	nfiguration	n						
• IGMP		~		Group Ad	Idress	1	Group Mask		C-RP Ad	dvertisem	ent Interval		
• PIM		^		255.1.1.1			255.255.255	0					
 Global Config 	guratio	n	_			-16							
 SSM Configu 	iration												
 Interface Cor 	nfigura	tion											
• PIM Neighbo	r												
Candidate RI Configuration	P 												
 BSR Candida Configuration 	ate I												

- 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.

System	Switchi	ng	Routing	QoS	Securit	у	Monitoring		Maintenance	Help	Index
Routing Table	IP IPve	VLAN	ARP	RIP OSPF	OSPFv3	Router	Discovery	VRRP		IPv6 Multicast	
Multica	ast	PIM B	SR Candi	date Configurat	on						
• Mroute Table		Interfa	ace				1/0/10) ~			
Global Configur	ration	Hash	Mask Le	ngth			30		(0 to	32)	
 Interface Config 	guration	BSR	Expiry Ti	me (hh:mm:ss)							
• DVMRP	~	Priori	ty				7		(0 to	255)	
• IGMP	~	IP Ad	dress								
• PIM	^	Next	bootstrap	Message(hh:n	im:ss)						
 Global Config 	guration	Next	Candidat	e RP Advertise	nent(hh:mm:	ss)					
 SSM Configu 	iration	Adver	tisement	Interval (secs)			60		(1 to	16383)	
 Interface Con 	figuration										
• PIM Neighbo	r										
Candidate RF Configuration	5										
BSR Candida Configuration	ate										
 Static RP Configuration 	(

- 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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	Pv6	VLAN ARP	RIP OSPF	OSPFv3 Ro	outer Discovery VF	RRP Multicast I	IPv6 Multicast	
		IP Conliguration	1.00		2037			
* Basic	^	Default Time to	Live		64			
 IP Configuration 	E. C.	Routing Mode			Enable	Disable		
 Statistics 		ICMP Echo Re	plies		Enable	Disable		
Advanced	~	ICMP Redirect	S		🖲 Enable 🔘	Disable		
		ICMP Rate Lin	nit Interval		1000	(0 to 2147	483647 ms)	
		ICMP Rate Lin	nit 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.

System	Sv	vitching		Routin	g	QoS	Securit	y Monitoring	Maintenance	Help	Index	
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery V	RRP Multicast	IPv6 Multicast		
IP	j.		IP Int	erface C	onfigurati	on						
Basic		~	12	3 VLAN	S All							
 Advanced 		<u>^</u>						ID 4 11 0 5				all accession accession
• IP Configurati	on			Port	Descript	tion	VLAN ID	Method	IP Address	Mask	Mode	Mode
 Statistics 				1/0/21				Manual ~	192.168.5.2	255.255.255	.0 Enable 🗸	Enable 👻
• IP Interface				1/0/1				None	0.0.0.0	0.0.0.0	Disable	Enable
Conliguration				1/0/2				None	0.0.0.0	0.0.0.0	Disable	Enable
 Secondary IP 				1/0/3				None	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 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.

System	SI	witching		Routin	9	QoS	Securit	y Monit	oring	Maintenance	Help	Index		
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discov	ery VRR	R Multicast	IPv6 Multicast			
IP			IP Int	erface C	onfiguratio	on								
• Basic		~	12	3 VLAN	s All									
 Advanced 		^						ID Addeses C	anfinitation	ell.	Quinnat	Dev	tin a	Administrativa
 IP Configurati 	on			Port	Descript	tion	VLAN ID	Method	orniguration	IP Address	Mask	Mod	le le	Mode
 Statistics 				1/0/22				Manual 🛩		192.168.6.1	255.255.2	55.0 Er	able 🗸	Enable 🗸
IP Interface				1/0/1	7			None		0.0.0.0	0.0.0	Dis	able	Enable
Conliguration	8			1/0/2				None		0.0.0.0	0.0.0	Dis	able	Enable
 Secondary IF 				1/0/3				None		0.0.0.0	0.0.0.0	Dis	able	Enable

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.

System	Sw	itching	_	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Rou	uter Discovery	VRRP Multicast	IPv6 Multicast	
RIF	D		RIP II	nterface Co	onfiguration					
•Basic		~	1 2	3 VLANS	All					
 Advanced 		^		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Key	Authentication Key ID
 RIP Configur 	ation			1/0/21	RIP-2 ×	RIP-2 ×	Enable 🗸	None 🗸		0
 Interface Cor 	ifigurati	on		1/0/1	RIP-2	Both	Disable	None		0
 Route Redis 	ribution	1		1/0/2	RIP-2	Both	Disable	None		0

- 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.

System	S	witching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Rou	ter Discovery	VRRP Multicast	IPv6 Multicast	
RIF	D		RIP I	nterface Co	onfiguration					
Basic		~	12	3 VLANS	All					
Advanced		^		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Key	Authentication Key ID
• RIP Configur	ation	tion		1/0/22	RIP-2 ×	RIP-2 ×	Enable 🗸	None 👻		
• Route Redist	tributio	on		1/0/1 1/0/2	RIP-2 RIP-2	Both Both	Disable Disable	None None		0 0

- **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.

System	S	witching		Routing		QoS	Securi	y	Monitoring	,	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP		IPv6 Multicast	
Multic	ast		Global	Configur	ation								
Mroute Table			Admi	n Mode			01	Disabl	e 🖲 Enable				
Global Configu	ration	k.	Proto	col State	9		Nor	n-Oper	ational				
 Interface Config 	guratio	n	Table	Maximu	m Entr	y Count	204	8					
DVMRP		~	Proto	col			No	Protoc	col Ena <mark>b</mark> led				
• IGMP		~	Table	Entry C	ount		0						
• PIM		×											
 Static Routes Configuration 													
 Admin Bounda Configuration 	ry												

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

- 7. Enable PIM-SM globally.
 - a. Select Routing > Multicast > PIM > Global Configuration.

System	S۱	vitching		Routing		QoS	Securit	y	Monitoring	, ľ	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP		IPv6 Multicast	
Multica	ast		PIM GI	obal Cor	figurat	ion							
Mroute Table			Adm	in Mode	1	Disa	able 💿 PIM-	SM 🔘	PIM-DM				
Global Configu	ration												
 Interface Config 	guratio	n											
• DVMRP		~											
 IGMP 		~											
• PIM		^											
Global Config	guratio	n											
 SSM Configu 	uration												
 Interface Cor 	nfigurat	ion											
• PIM Neighbo	DIF:												
 Candidate RI Configuration 	P 1												
 BSR Candida Configuration 	ate 1												
 Static RP Configuration 	1												

- **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.

System Se	ntching		Routing	QoS	Security	Monitoria	ng Main	itenance Hel	p Inde	x		
Routing Table IP	IPv6	VLA	N ARP	RIP OSPF	OSPPi3 R	outer Discovery	VRRP	olocast I IPv6 Mult	cast-			
Multicast		PIM	Interface C	onfiguration								
- Mroute Table		12	3 VLANS	All						c	So To Interface	Go
Global Configuration			Interface	Admin Mode	Protocol State	IP Address	Hello Interval	Join/Prune Interval	BSR Border	DR Priority	Designated Router	Neighbor Count
+DVMRP	۰. ₂			Enable Y			1			1		
-1/2440		0	1/0/1	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
- IOME		. 0	1/0/2	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
• PIM	<u>^</u>		1/0/3	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
 Global Configuration 		12	1/0/4	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
•SSM Configuration		10	1/0/5	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
Contractor of Contractor	-	10	1/0/6	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
Interface Configurat	on	8	1/0/7	Disable.	Non-Operational	0.0.0.0	30	60	Disable	1		
PIM Neighbor	_	0	1/0/8	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		

- 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.

System	S	witching		Routing		QoS	Securi	ty	Monitorin	9	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Route	r Discovery	VRRP	Multicast	IPv6 Multicast	с.
Multica	ast		PIM In	terface S	electio	n							
Mroute Table			Inter	ace		1/0/22 ~							
 Global Configur 	ration												
 Interface Config 	guratio	n											
• DVMRP		~	PIM C	andidate	RP Co	onfiguration	1						
• IGMP		~		Group Ad	dress	(Group Mask		C-RP A	dvertisern	ient Interval		
• PIM		^		225.1.1.	1		255.255.255	.0					
 Global Config 	guratio	n											
 SSM Configu 	iration												
 Interface Con 	figura	tion											
• PIM Neighbo	r												
Candidate Rf Configuration	P												

- 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.

System	Swi	itching		Routing		QoS	Security	/ M	lonitoring	1	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Dis	scovery	VRRP	Multicast	IPv6 Multicast	
Multica	ast		PIM BS	SR Cand	idate Co	nfiguratio	on						
 Mroute Table 			Interfa	ice					1/0/21	~			
 Global Configu 	ration		Hash	Mask Le	ength				30		(0 to	32)	
 Interface Config 	guration		BSR I	Expiry T	me (hh:r	mm:ss)							
• DVMRP		~	Priorit	У					5		(0 to	255)	
• IGMP		~	IP Ad	dress									
• PIM		^	Next	bootstra	o Messa	ge(hh:m	m:ss)						
 Global Config 	guration		Next (Candidat	e RP Ac	lvertiserr	ent(hh:mm:	ss)					
 SSM Configu 	iration		Adver	tisement	Interval	(secs)			60		(1 to	16383)	
Interface Cor	figuratio	on											
• PIM Neighbo	r												
 Candidate RI Configuration 													
 BSR Candida Configuration 	ate I												

- 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.

System	SI	witching		Routing		QoS	Securit	y 🛛	Monitoring	3	Maintenance	Help	Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP	Multicast	IPv6 Multicast)
IP			IP Con	figuration									
 Basic 		^	Defau	lt Time t	o Live				64				
• IP Configurat	ion		Routi	ng Mode					Enable	e 🔘 Disa	ible		
• Statistics			ICMP	Echo R	eplies				Enable	e 🔘 Disa	ible		
 Advanced 		×	ICMP	Redirec	ts				Enable	e 🔘 Disa	ible		
			ICMP	Rate Lir	nit Inte	rval			1000		(0 to 21	47483647 ms)	
			ICMP	Rate Lir	nit Bur	st Size			100		(1 to 20)	0)	

- **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.

System S	Switching		Routin	g	QoS	Security	y Monitoring	Maintenance	Help	Index	
Routing Table	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery V	RRP Multicast	IPv6 Multicast		
IP		IP Int	erface C	onfiguratio	'n						
• Basic	~	12	3 VLAN	S All							
Advanced	^						ID A LL COMPANY		0.1		a survey and
• IP Configuration			Port	Descripti	ion	VLAN ID	Method	IP Address	Mask	Mode	Mode
 Statistics 			1/0/21				Manual 👻	192.168.2.1	255.255.255	.0 Enable •	r Enable Y
IP Interface			1/0/1				None	0.0.0.0	0.0.0	Disable	Enable
Configuration			1/0/2				None	0.0.0.0	0.0.0.0	Disable	Enable
 Secondary IP 			1/0/3				None	0000	0000	Disable	Enable

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.

System	S	witching		Routin		QoS	Security	/ Monitoring		Maintenance	Help	Index	
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRF	P Multicast	IPv6 Multicast		
IP			IP Int	erface C	onfigurati	ion							
•Basic		~	12	3 VLAN	S All								
 Advanced IP Configurat 	ion	^		Port	Descrip	ition	VLAN ID	IP Address Configu Method	iration	IP Address	Subnet Mask	Routing Mode	Administrative Mode
 Statistics 				1/0/22				Manual 🗸		192.168.6.2	255.255.255	.0 Enable	✓ Enable ✓
• IP Interface				1/0/1	6			None		0.0.0.0	0.0.0.0	Disable	Enable
Configuration	2			1/0/2				None		0.0.0.0	0.0.0.0	Disable	Enable
 Secondary IF 	2			1/0/3				None		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 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.

System	Sw	vitching		Routin	g 👘	QoS	Securit	y Monitoring	Maintenanc	e Help	Index		
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery VI	RRP Multicas	t IPv6 Multicast			
IP Paoin	80 T		IP Inte	erface C	onfigurat	ion							
• Dasic		Ť	12	3 VLAN	s all								
 Advanced IP Configurat 	ion	^		Port	Descrip	otion	VLAN ID	IP Address Configurati Method	ion IP Address	Subnet Mask	Rout Mode	ing e	Administrative Mode
 Statistics 				1/0/24	1			Manual ~	192.168.4.	1 255.255.2	55.0 Ena	able 👻	Enable ~
• IP Interface				1/0/1				None	0.0.0.0	0.0.0.0	Disa	ble	Enable
Computation	Н			1/0/2				None	0.0.0.0	0.0.0.0	Disa	ble	Enable
 Secondary IF 	þ			1/0/3				None	0.0.0.0	0.0.0.0	Disa	ble	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.

System	Sw	itching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Rou	ter Discovery	VRRP Multicast	IPv6 Multicast	A.
RIF	ס		RIP II	nterface C	onfiguration					
•Basic		~	12	3 VLANS	All					
 Advanced 		^		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Key	Authentication Key ID
 RIP Configur 	ation	-		1/0/21	RIP-2 ×	RIP-2 ×	Enable 👻	None -		
 Interface Cor 	nfigurati	оп		1/0/1	RIP-2	Both	Disable	None		0
 Route Redis 	tribution			1/0/2	RIP-2	Both	Disable	None		0

- 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.

System	S	witching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Rou	iter Discovery	VRRP Multicast	IPv6 Multicast	
RIP	D		RIP II	nterface Co	onfiguration					
• Basic		×	12	3 VLANS	All					
 Advanced 		^		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication K	Kev Authentication Key ID
 RIP Configura 	ation			1(0(22		DID 2 y	Engble av	Nana y		6
Interface Con	ifigura			1/0/22		NIF-2	Linable *	INDRE .*	1	0
Route Redist	ributic	n		1/0/1	RIP-2	Both	Disable	None		0
				1/0/2	RIP-2	Both	Disable	None		U
				1/0/3	RIP-2	Both	Disable	None		0

- 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.

System	Swit	ching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP II	⊃v6	VLAN	ARP	RP OSPF	OSPFv3 Rou	iter Discovery	VRRP Multicast	IPv6 Multicast	
2014-02-0										
RIP			RIP In	nterface Co	onfiguration					
• Basic		~	12	3 VLANS	All					
 Advanced 		^		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Key	Authentication Key ID
 RIP Configura 	ition			1/0/24	RIP.2 ×	RIP-2 ×	Enable ×	None x		0
 Interface Conf 	figuratio	n)		1/0/24		100-2	Enable	NUT		
*Route Redistr	ibution			1/0/1	RIP-2	Both	Disable	None		U
- Route Redistr	ibution			1/0/2	RIP-2	Both	Disable	None		0
			8	1/0/3	RIP-2	Both	Disable	None		0

- 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.

System	Sw	vitching		Routing		QoS	Securi	ty	Monitoring		Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast	
Multica	ast		Global	Configur	ation								
Mroute Table			Admi	n Mode			0	Disabl	e 🖲 Enable				
 Global Configura 	ation		Proto	col State	9		Op	eratior	al				
Interface Configu	uratior	1	Table	Maximu	m Ent	ry Count	20	18					
• DVMRP		~	Proto	col			No	Proto	col Enabled				
•IGMP		~	Table	Entry C	ount		0						
- PIM		~											
 Static Routes Configuration 													
Admin Boundary Configuration	У												

- **b.** For Admin Mode, select the **Enable** radio button.
- c. Click Apply.
- 9. Enable PIM-SM globally.
 - a. Select Routing > Multicast > PIM > Global Configuration.

System	S	witching		Routing		QoS	Securit	у	Monitoring		Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP		IPv6 Multicast	
Multica	ast		PIM G	lobal Con	figurati	on							
Mroute Table			Adm	nin Mode		O Disa	able 🔘 PIM-	SM 🖲	PIM-DM				
Global Configu	ration												
Interface Config	guratio	n											
• DVMRP		v											
• IGMP		~											
• PIM		~											
Global Config	guratio	n											
 SSM Configu 	iration												
 Interface Cor 	nfigurat	ion											
• PIM Neighbo	r												
 Candidate RI Configuration 	P 1												
 BSR Candida Configuration 	ate 1												
 Static RP Configuration 	1												

- **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.

System S	witchin	19	Routing	QoS	Security	Monitoria	ng Mair	tenance Hel	p Inde	×		
Routing Table IP	IP\6	VLA	N ARP	RIP OSPF	OSPEv3 R	outer Discovery	VRRP	Minnel IPv6 Multi	cast.			
Multicast		PIM	Interface C	onfiguration								
Mroute Table		312	2 3 VLANS	All						ं	3o To Interface	Go
Global Configuration			-	North States			The second second			1000 company	12000000000000000	The second second
Interface Configurati	on	1 2	Intertace	Admin Mode	Protocol State	IP Address	Hello Interval	Join/Prune Interval	BSK Border	UR Priority	Designated Router	Reighbor Count
• DVMRP	ų,			*						1		
IGMP			1/0/1	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
-		10	1/0/2	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
• PIM	<u>^</u>		1/0/3	Disable	Non-Operational	0.00.0	30	60	Disable	1		
Global Configurati	on:	6	1/0/4	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
*SSM Configuration	n	- 6	1/0/5	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
		10	1/0/6	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
 Interface Configur 	tion	6	1/0/7	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		
PIM Neighbor		0	1/0/8	Disable	Non-Operational	0.0.0.0	30	60	Disable	1		

- 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.

System	S	witching		Routing		QoS	Secur	ity	Monitori	ıg	Maintenance	e Help
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast
Montes Mroute Table Global Configur Interface Config DVMRP	asi ration guratio	on Y	PIM In Inter	iterface S face andidate	Selectio	n 1/0/22 ~ nfiguratior	1					
PIM		~		Group A	ddress		Group Mask	¢	C-RP	Advertisen	nent Interval	
 Global Config 	juratio	n		225.1.1.	1		255.255.255	5.0				
 SSM Configu Interface Con PIM Neighbo 	iration ifigura r	tion										
Candidate RF	D											

- 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.

System	em Switchir		Switching		g Routing			QoS	Securit	y Mo	nitoring		Maintenance	Help In	dex	
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Dise	covery	VRRP	Multicast	IPv6 Multicast				
Munuca	สรเ		DIM D													
Mroute Table			PIND	SR Cano	idate C	onligurati	on									
Global Configu	ration		Interfa	ace					1/0/22	~						
Interface Config	Interface Configuration				ength				30		(0 to	(0 to 32)				
DVMRP		~	BSR	Expiry T	ime (hł	n:mm:ss)										
IGMP		~	Priori	ty					0			(0 to 255)				
PIM		~	IP Ad	dress												
Global Confid	ouratio	n	Next	bootstra	p Mess	age(hh:m	m:ss)									
• COM Canfor	garation		Next	Candida	te RP /	Advertisen	nent(hh:mm:	ss)								
- SSIVI Conligu	ration		Adver	tisemen	t Interva	al (secs)			60			(1 to 16383)				
 Interface Cor 	ntigura	tion														
• PIM Neighbo	r															
 Candidate RF Configuration 	P															
BSR Candida Configuration	ate 1															
(1)																

- 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.

System	S	witching		Routing		QoS	Securit	у	Monitoring		Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP		IPv6 Multicast	
Multica	ast		IGMP (Global C	onfigur	ation							
Mroute Table			Admir	n Mode) Disa	ble 🖲 Enabl	le					
Global Configu	ration												
 Interface Config 	guratio	in											
• DVMRP		~											
• IGMP		~											
Global Config	guratio	m											

- **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.

System Switchi		3	Routing	QoS	Secu	rīty Mo	nitoring	Maintenance	Help	Index		
Routing Table IP	IPv6	VLAN	I ARP	RIP OSPI	OSPFv3	Router Disc	overy VRF	RP Multicast	IPv6 Multicast			
Multicast		IGMF	P Routing I	nterface Config	uration							
Mroute Table		12	3 VLANS	All						Go To I	nterface	Go
 Global Configuration 				New W		24	Less.	1				
Interface Configuratio	n		Interface	Admin Mode	Version	Robustness	Query Interval	Query Max Response Time	Startup Query Interval	Startup Query Count	Last Member Query Interval	Last Member Query Count
• DVMRP	~		1/0/24	Enable v	V3	2	125	100	31	2	10	2
• IGMP	~		1/0/1	Disable	V3	2	125	100	31	2	10	2
 Global Configuratio 	n		1/0/2	Disable	V3	2	125	100	31	2	10	2
Routing Interface			1/0/3	Disable	V3	2	125	100	31	2	10	2
Configuration			1/0/4	Disable	V3	2	125	100	31	2	10	2

- **b.** Under IGMP Routing Interface Configuration, scroll down and select the Interface **1/0/24** check box.
- c. In the Admin Mode field, select Enable.
- d. Click Apply to save the settings.

DHCP L2 Relay and L3 Relay



Dynamic Host Configuration Protocol Relays

This chapter includes the following sections:

- DHCP L2 Relay
- DHCP L3 Relay
- Configure a DHCP L3 Switch

DHCP L2 Relay

DHCP relay agents eliminate the need to have a DHCP server on each physical network. Relay agents populate the giaddr field and also append the Relay Agent Information option to the DHCP messages. DHCP servers use this option for IP addresses and other parameter assignment policies. These DHCP relay agents are typically IP routing-aware devices and are referred to as Layer 3 relay agents.

In some network configurations, Layer 2 devices can append the relay agent Information option as they are closer to the end hosts.



Figure 60. DHCP L2 Relay

These Layer 2 devices typically operate only as bridges for the network and might not have an IPv4 address on the network. Lacking a valid IPv4 source address, they cannot relay packets directly to a DHCP server on another network. These Layer 2 devices append the Relay agent information option and broadcast the DHCP message. This section provides information about where a Layer 2 relay agent fits in and how it is used.

CLI: Enable DHCP L2 Relay

1. Enter the following commands:

```
(Netgear Switch)#vlan database
(Netgear Switch)(Vlan)#vlan 200
(Netgear Switch)(Vlan)#exit
```

2. Enable the DHCP L2 relay on the switch.

```
(Netgear Switch) (Config)#dhcp l2relay
(Netgear Switch) (Config)#dhcp l2relay vlan 200
```

3. Enable the Option 82 Circuit ID field.

(Netgear Switch) (Config)#dhcp l2relay circuit-id vlan 200

4. Enable the Option 82 Remote ID field.

(Netgear Switch) (Config)#dhcp l2relay remote-id rem_id vlan 200

5. Enable DHCP L2 relay on port 1/0/4.

(Netgear Switch) (Config)#interface 1/0/4 (Netgear Switch) (Interface 1/0/4)# dhcp l2relay

```
(Netgear Switch) (Interface 1/0/4)# vlan pvid 200
(Netgear Switch) (Interface 1/0/4)# vlan participation include 200
(Netgear Switch) (Interface 1/0/4)# exit
```

6. Enable DHCP L2 relay on port 1/0/5.

```
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)# dhcp l2relay
(Netgear Switch) (Interface 1/0/5)# vlan pvid 200
(Netgear Switch) (Interface 1/0/5)# vlan participation include 200
(Netgear Switch) (Interface 1/0/5)# exit
```

7. Enable DHCP L2 relay on port 1/0/6.

```
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)# dhcp l2relay
```

8. Trust packets with option 82 received on port 1/0/6.

```
(Netgear Switch) (Interface 1/0/6)# dhcp l2relay trust
(Netgear Switch) (Interface 1/0/6)# vlan pvid 200
(Netgear Switch) (Interface 1/0/6)# vlan participation include 200
(Netgear Switch) (Interface 1/0/6)# exit
```

Web Interface: Enable DHCP L2 Relay

- 1. Create VLAN 200.
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

A screen similar to the following displays.

Syste	em	Switching		g Routing		QoS	Security	Monitorin	ng	Maintenance	Help	Index
	Auto-	VolP	iscsi	STP	Multicast	MVR	Address Table	Ports LAG	MLAG	3		10
	VLA	N		Reset								
 Basic 			^	Reset	Configuratio	n						
• VLAN	I Config	uratior	i									
• Advance	ed		~									
				Interna	VLAN Confi	guration						
				Intern	al VLAN Allo	cation Bas	e 40	93				
				Intern	al VLAN Allo	cation Poli	icy 🔘	Ascending 💿 De	escendir	19		
				VLAND	Configuration							
				VLAN	Sonnguration		- (2 2					
					VLAN ID VI	AN Name	VLAN Type	Make Static				
					200			Disable 🗸				
					1 de	fault	Default	Disable				

- 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.

System	System Switching		Routin	ig 🛛	QoS		Securi	y 🛛	M	onitor	ng		Mainte	nance		Н	elp		Index		
VLAN Auto	-VolP iSCS	SI STP	Mul	ticast	MVR	Addr	ess Tabl	e P	orts	LAG	Μ	LAG								0	
VLA	AN	VLAN	Memb	ership																	
• Basic	~	VLA	N ID											2	00	~					
 Advanced 	^	Grou	p Oper	ation										1	Intag	All	~				
• VLAN Conf	iguration	VLA	V Name	9										V	LANO	200					
- VLAN Mem	nbership	VLA	∖ Туре											S	tatic						
VLAN State	us		Unit 1																		
Port PVID Configuration	on	Port	s 1	3 5	7	9 11	13	5 17	19	21	23	25 21	29	31	33	35 3	7 3	9 41	43	45	47
• MAC Base	d VLAN			U_U																	1000
 Protocol Ba Group Conf 	ased VLAN figuration		2	4 6	8	10 12	14	6 18	20	22	24	26 28	30	32	34	36 3	8 4	0 42	44	46	48

- 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.
| System Switchi | ng | Routing | | QoS Security | Monitoring | Maintenance Help | Index |
|---|-------|----------------|--------|-------------------|----------------|------------------------|------------------------------|
| VLAN Auto-VolP iSC | SI ST | P Multic | ast N | IVR Address Table | Ports LAG MLAG | | |
| VLAN | PVI | Configurat | ion | | | | |
| •Basic 🗸 | 12 | 3 LAGS A | JI | | | | |
| • Advanced ^ | | Interface | PVID | VLAN Member | VLAN Tag | Acceptable Frame Types | Configured Ingress Filtering |
| • VLAN Membership | | | 200 | | | × | ~ |
| VLAN Status | 6 | 1/0/1 | 1 | 1 | None | Admit All | Disable |
| Port PVID | 6 | 1/0/2 | 1 | 1 | None | Admit All | Disable |
| Configuration | 6 | 1/0/3 | 1 | 1 | None | Admit All | Disable |
| • MAC Based VLAN | | 1/0/4 | 1 | 1 | None | Admit All | Disable |
| Protocol Based VLAN
Group Configuration | | 1/0/5
1/0/6 | 1
1 | 1 | None
None | Admit All
Admit All | Disable
Disable |

- 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.

System	Switching	9	Routing	QoS	Security	Monite	oring	Maintenance	Help	Index
Management	Device View	/ Sei	vices Ch	assis PoE	SNMP LLD	PISDP	Timer S	chedule		
Servic	ces	DHC	P L2 Relay	Global Configu	ration					
DHCP Server	~	Adr	min Mode	O Dis:	able 💿 Enable					
DHCP Relay										
DHCP L2 Relay	y ^									
DHCP L2 Re	lay Global	DHC	P L2 Relay	VLAN Configur	ation					
• DHCP I 2 Re	lav		VLAN ID	Admin Mode	Circuit ID Mode	Remote ID) String			
Interface Cor	figuration		200	Disable 👻	Disable 🛩					
DHCP L2 Re	lay		1	Disable	Disable					
Intenace Sta	usuus		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.

System	Switchin	g	Rout	ng	QoS	Seci	urity	Mon	toring	Maintenance	Help	Index
Management De	evice Viev	v s	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer S	chedule		
Services		Dł	HCP L2 R	elay Config	guration							
DHCP Server		- 1	2 3 LAG	S All Go	To Interfac	ce	1	Go				
DHCP Relay			Interfa	ice Admi	in Mode	82 Optic	on Trust I	Mode				
DHCP L2 Relay DHCP L2 Relay Configuration	Global	Ì	1/0/1	Dical	¥	Disable	*					
DHCP L2 Relay	iration		1/0/1	Disal	ble	Disable						
DHCP L2 Relay Interface Statistic	cs		 1/0/3 1/0/4 1/0/5 	Disal	ble	Disable						
• UDP Relay		.	 1/0/5 1/0/6 	Disal	ble	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.

System	Switch	ing		Routing		QoS	Secu	urity	Mon	itoring	Maintenance	Help	Index
Management	Device Vi	ew	Ser	vices Cl	nassis	PoE	SNMP	LLDP	ISDP	Timer Se	chedule	0	
Servie	ces		DHCI	^D L2 Relay	Config	uration							
• DHCP Server		~	12	3 LAGS A	All Go T	o Interfac	e		Go				
DHCP Relay							-						
• DHCP L2 Rela	iy	^	-	Interface	Admir	n Mode	82 Optio	n Trust	Mode				
• DHCP 12 Re	elav Global					~		~					
Configuration	1			1/0/1	Disab	le	Disable						
• DHCP 12 Re	elav			1/0/2	Disab	le	Disable						
Interface Cor	nfiguration			1/0/3	Disab	le	Disable						
• DHCP L2 Re	elav			1/0/4	Disab	le	Disable						
Interface Sta	atistics			1/0/5	Disab	le	Disable						
• UDP Relay		v		1/0/6	Disab	le	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 61. 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.

System	Swi	tching		Routing		QoS	Securi	ly	Monitoring	9	Maintenance	e Help	Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRR	Multicast	IPv6 Multicast	
IP			IP Con	figuration									
• Basic		^	Defau	lt Time t	o Live				64				
• IP Configurati	on		Routi	ng Mode					Enable	e 🔵 Dis	able		
 Statistics 			ICMP	Echo R	eplies				Enable	e 🔵 Dis	able		
 Advanced 		~	ICMP	Redirec	ts				Enable	e 🔵 Dis	able		
			ICMP	Rate Lir	nit Inte	rval			1000		(0 to 2	147483647 ms)	
			ICMP	Rate Lir	nit Bu <mark>r</mark>	st Size			100		(1 to 2	00)	
			Maxin	num Ne>	t Hops	3			4				

- **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.

System	Swite	ching		Routing	1	QoS	Securit	y Monitoring		Maintenance	Help	Index	
Routing Table	P IF	Pv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast		
IP			IP Int	erface Co	onfigurati	ion							
Dasic			12	3 VLANS	S All								
 Advanced IP Configuration 	1	^		Port	Descrip	tion	VLAN ID	IP Address Config Method	uration	IP Address	Subnet Mask	Rou Moo	iting de
 Statistics 								Manual 🛩		10.100.1.1	255.255.2	:55.0	~
• IP Interface				1/0/1				None		0.0.0.0	0.0.0.0	Disa	able
Configuration				1/0/2				None		0.0.0.0	0.0.0.0	Disa	able
 Secondary IP 				1/0/3				None		0.0.0.0	0.0.0.0	Disa	able

- 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.

System	Sw	itching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Rou	uter Discovery	VRRP Multicast	IPv6 Multicast	
RIP	ì		RIP II	nterface C	onfiguration					
• Basic		~	1 2	3 VLANS	All					
Advanced PIR Configura	ation	^		Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Ke	y Authentication Key ID
- RiP Conligura	ation Second		8	1/0/3	RIP-2 ¥	RIP-2 ¥	Enable v	None 🗸		Q
- Intenace com	ngurau	011		1/0/1	RIP-2	Both	Disable	None		0
 Route Redistr 	ribution	ų.		1/0/2	RIP-2	Both	Disable	None		0
				1/0/3	RIP-2	Both	Disable	None		0

- 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	display	/S.
--	---	--------	---------	----	-----	-----------	---------	-----

System	Switching	Rout	ing	QoS	Sec	urity	Mor	nitoring	Maintenance	Help	Index
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer Sc	hedule		
Servio	ces	DHCP Serve	er Configura	ition							
DHCP Server	~	Admin Mo	de) Dis	able 💿 E	nable				
DHCP Server Configuration	r V	Ping Pack	et Count		2	NSR 112372		(0, 2 to 10			
DHCP Pool Configuration	1	Conflict Lo Bootp Auto	gging Mod omatic Mod	e le	DisDis	able 💿 E able 🔘 E	nable Inable				
DHCP Pool (Options										
DHCP Server	r Statistics	<u></u>									
DHCP Bindin Information	ngs	Excluded A	ddress								
DHCP Conflic Information	cts	10.20	nge From 10.1.1		IP Range 10.200.1.1	10					

- **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.

System	Switching	R	outing	QoS	Sec	urity	Mon	itoring	Maintenance	Help	Index
Management	Device View		Chassis	PoE	SNMP	LLDP	ISDP	Timer So	shedule		
Servic	es	DHCP Se	rver Configu	ation							
DHCP Server	^	Admin I	/lode		Dis	able 💿 E	nable				
DHCP Server Configuration		Ping Pa	cket Count		2			(0, 2 to 10)		
• DHCP Pool		Conflict	Logging Mod	le	Dis	able 💿 E	nable				
Configuration		Bootp A	utomatic Mc	de	Dis	able 🔘 E	nable				
• DHCP Pool (Options										
DHCP Server	Statistics										
DHCP Bindin	igs	Excluded	Address				0				
Duop o		🔲 IP	Range From		IP Range	То					
Information	CLS	10	.200.2.1		10.200.2.	1					
• DHCP Relay		10	200.1.1		10.200.1.	1					

- 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.

System	Switching	Rou	ting	QoS	Sec	curity	Mon	itoring	Maintenance	Help	Index
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer S	chedule		
Servi	ices	DHCP Pool	Configurat	ion							
DHCP Server	~	Pool Nam	e		C	reate	~				
DHCP Serve Configuration	er	Pool Nam	e		dh	cp_serve		(1 to 3	1 alphanumeric chara	cters)	
• DHCP Pool		Type of Bi	inding		D	ynamic	~				
Configuratio	n)	Network A	ddress		10	.200.1.1					
• DHCP Pool	Options	Network N	/lask		25	5.255.258	i.0				
• DHCP Serve	er Statistics	Network F	Prefix Lengt	h				(0 to 3	2)		
• DHCP Bindi	ings	Client Nar	ne								
Information		Hardware	Address								
 DHCP Confl Information 	licts	Hardware	Address T	уре	E	thernet	~				
DHCP Relay		Client ID									
DHCP L2 Rela	ay 🗸	Host Num	ber								
UDP Relay	· •	Host Mas	k								
DHCPV6 Serve	or v	Host Prefi	x Length					(1-32)			

- **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 **255.255.0**. 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.

System	Switching	Routing	QoS	Seci	urity	Moni	toring	Maintenance	Help	Index
Management	Device View	Services Cl	hassis PoE	SNMP	LLDP	ISDP	Timer S	chedule	· · · · ·	
Servi	ices	DHCP Pool Co	nfiguration							
DHCP Server	^	Pool Name		Cr	eate 🛩					
DHCP Serve Configuration	ər n	Pool Name		dho	p_server	_second	(1 to 3	1 alphanumeric chara	cters)	
DHCP Pool		Type of Bindir	ig	Dy	namic	~				
Configuration	n	Network Addr	ess	10.	200.2.0					
DHCP Pool	Options	Network Mask	<	255	5.255.255	.0				
• DHCP Serve	er Statistics	Network Prefix	k Length				(0 to 3.	2)		
• DHCP Bindi	ngs	Client Name								
Information		Hardware Add	Iress							
 DHCP Confl Information 	icts	Hardware Add	lress Type	Et	hernet	-				
DHCP Relay		Client ID								
• DHCP L2 Rela	ay v	Host Number		0.0	0.0					
	6 5 0	Hoot Mook		1000	70.52		-			

- **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 **255.255.0**. 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 10.200.2.1 255.255.0
(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.

System	SI	witching		Routing		QoS	Secur	ty	Monitoring	, I	Maintenance	Help	Index
Routing Table	P	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP	Multicast	IPv6 Multicast	
			1										
IP			IP Con	figuration	1								
• Basic		^	Defau	lt Time t	o Live				64				
 IP Configurat 	ion		Routi	ng Mode					Enable	e 🔘 Disab	le		
 Statistics 			ICMP	Echo R	eplies				Enable	e 🔘 Disab	le		
 Advanced 		~	ICMP	Redirec	ts				Enable	e 🔘 Disab	le		
			ICMP	Rate Li	mit Inte	rval			1000		(0 to 21-	47483647 ms)	
			ICMP	Rate Li	mit Bur	st Size			100		(1 to 20	0)	
			Maxir	num Ne:	kt Hops				4				

- **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.

System	Sv	witching		Routing		QoS	Securit	y Monitorin	g	Maintenance	Heip	Index	
Routing Table	P	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast	1.	
5													
P	1		-	1/0/4				Manual 👻		10.100.1.2	255.255.25	5.0 Enable	✓ Enable ✓
•Basic		~		1/0/1				None		0.0.0.0	0.0.0.0	Disable	Enable
 Advanced 		^		1/0/2				None		0.0.0.0	0.0.0.0	Disable	Enable
• IP Configurati	on			1/0/3				None		0.0.0.0	0.0.0	Disable	Enable
• Statistics				1/0/4				None		0.0.0.0	0.0.0	Disable	Enable
Statistics		-		1/0/5				None		0.0.0.0	0.0.0	Disable	Enable
 IP Interface Configuration 				1/0/6				None		0.0.0.0	0.0.0.0	Disable	Enable

- **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.

System	Swite	ching		Routing	QoS	Security	Monitoring	Maintenance	Help	ndex
Routing Table	IP IF	Pv6	VLAN	ARP	RIP OSPF	OSPEv3 Rou	ter Discovery	VRRP Multicast	IPv6 Multicast	
RIP			RIP II	nterface Co	onfiguration					
• Basic		~	12	3 VLANS	All					
 Advanced 		~		Interface	Sand Varsion	Receive Version	RIP Mode	Authentication Type	Authentication Key	Authentication Key ID
• RIP Configura	ation			intendoe	Certa Version	Treceive version	Tur Would	Addition type	Addrendeddon rycy	Huttentication regy is
Interface Con	figuration			1/0/4	RIP-2 ¥	RIP-2 ×	Enable ~	None ~		
sintenace com	nguration	•		1/0/1	RIP-2	Both	Disable	None		0
 Route Redistr 	ribution			1/0/2	RIP-2	Both	Disable	None		0
				1/0/3	RIP-2	Both	Disable	None		0
				1/0/4	RIP-2	Both	Disable	None		0

- 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.

System	S	witching]	Routir	g	QoS	Securit	y Monitoring	Maintena	ince Help	Index	
Routing Table	P	IPv6	VLAN	I ARF	RIP	OSPF	OSPFv3	Router Discovery	VRRP Multic	ast IPv6 Multicast		
IP	j.		IP Int	erface C	onfigurat	ion						
• Basic		¥	12	3 VLAN	IS All							
 Advanced IP Configurat 	ion	^		Port	Descrip	tion	VLAN ID	IP Address Configura Method	ition IP Addre	ss Subnet Mask	Routing Mode	g Administrative Mode
 Statistics 								Manual 👻	10.200.1	.1 255.255.2	55.0 Enabl	e 👻 Enable 👻
IP Interface Configuration	į			1/0/1 1/0/2				None None	0.0.0.0	0.0.0.0	Disable	e Enable Enable
• Secondary IF	0			1/0/3				None	0.0.0.0	0.0.0.0	Disable	e Enable
				1/0/5				None	0.0.0.0	0.0.0.0	Disable	e Enable
				1/0/6 1/0/7				None None	0.0.0.0	0.0.0.0	Disable	e Enable e Enable
				1/0/8				None	0.0.0.0	0.0.0.0	Disable	e Enable

- 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.

System	SI	witching		Routin	g	QoS	Securit	y Monitoring	Maintenance	Help	Index	
Routing Table	P	IPv6	VLAN	I ARP	RIP	OSPF	OSPFv3	Router Discovery VRR	⊃ Multicast	IPv6 Multicast		
IP			IP Int	erface C	onfigurat	ion						
• Basic		~	12	3 VLAN	S All							
 Advanced IP Configuration 	on	^		Port	Descrip	tion	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Routing Mode	Administrative Mode
 Statistics 							1	Manual 🗸	10.200.2.1	255.255.255	0 Enable 🛩	Enable ×
IP Interface Configuration				1/0/1				None	0.0.0.0	0.0.0.0	Disable	Enable
 Secondary IP 				1/0/2 1/0/3 1/0/4				None	0.0.0.0	0.0.0.0	Disable	Enable
				1/0/5				None	0.0.0.0	0.0.0.0	Disable	Enable
				1/0/6				None	0.0.0.0	0.0.0.0	Disable	Enable
				1/0/7				None	0.0.0.0	0.0.0.0	Disable	Enable
				1/0/8				None	0.0.0	0.0.0.0	Disable	Enable

- **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.

System	S	witching		Routing		QoS	Secu	ity	Monitoring		Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP		OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast	
RIF	5	1	Config	iration									
T MI	11		Coning	aración									
• Basic		×	Sourc	ce			Connected	~					
 Advanced 		^	Redis	stribute N	lode	1	Enable 🗸						
• RIP Configura	ation		Metri	с		0			(0 to 15, 0	to uncor	ifigure)		
Interface Cor	nfigura	tion	Distri	bute List		0			(0 to 199,	0 to unco	nfigure)		
Route Redist	tributio	n				10							

- 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.

System	Switching	Routing	QoS	Sec	urity	Monit	oring	Maintenance	Help	Index
Management	Device View	Services Chass	is PoE	SNMP	LLDP	ISDP	Timer So	chedule		
Servic	es	DHCP Relay								
DHCP Server	~	Maximum Hop Co	unt	4			(1 to 1	16)		
DHCP Relay		Admin Mode		C	Disable	Enable				
DHCP L2 Relay	y ~	Minimum Wait Tin	ne (secs)	0			(0 to 1	100)		
 UDP Relay 	v	Circuit ID Option N	1ode	۲	Disable	Enable				
DHCPv6 Server	· ·									
		DHCP Relay Statist	ics							
		Requests Receive	d	0						
		Requests Relayed		0						
		Packets Discarded	ł	0						

- **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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Inde>
Management I	Device View	Services Chas	sis PoE	SNMP LLDP	ISDP Timer Sch	nedule		0
Service	s	UDP Relay Configu	ration					
DHCP Server	~	Admin Mode	O Dis	able 💿 Enable				
DHCP Relay								
DHCP L2 Relay	×							
UDP Relay	~	UDP Relay Global	Configuratio	n				
UDP Relay Glo Configuration	obal	Server Addre	SS	UDP Port	UDP Port Other Va	lue Hit Count		
 UDP Relay Int Configuration 	erface	10:100:1.1		dhcp 🗸	67			
DHCPv6 Server	~							

- 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

35

This chapter includes the following sections:

- Multicast Listener Discovery Concepts
- Configure MLD
- MLD Snooping

Note: MLD is available on M5300 and M6100 series switches only. However, the following M5300 series switches require a license to support MLD: M5300-28G, M5300-52G, M5300-28G-POE+, and M5300-52G-POE+.

Multicast Listener Discovery Concepts

Multicast Listener Discovery (MLD) protocol enables IPv6 routers to discover multicast listeners, the nodes that are configured to receive multicast data packets, on its directly attached interfaces. The protocol specifically discovers which multicast addresses are of interest to its neighboring nodes and provides this information to the active multicast routing protocol that determines the flow of multicast data packets.

Periodically, the multicast router sends general queries requesting multicast address listener information from systems on an attached network. These queries are used to build and refresh the multicast address listener state on the attached networks. In response to the queries, multicast listeners reply with membership reports. These membership reports specify their multicast addresses listener state and their desired set of sources with current-state multicast address records.

The multicast router also processes unsolicited filter- mode-change records and source-list-change records from systems that want to indicate interest in receiving or not receiving traffic from particular sources.

Configure MLD

In this case, PIM-DM is enabled on Switch A and Switch B, and MLD is enabled on Switch B's port 1/0/24 to discover the multicast listeners.



Figure 62. Configure MLD

CLI: Configure MLD

MLD on Switch A

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

```
(Netgear Switch) (Config) #ipv6 unicast-routing
(Netgear Switch) (Config)#ipv6 pim dense
(Netgear Switch) (Config) #ip routing
(Netgear Switch) (Config) #ip multicast
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1) #routing
(Netgear Switch) (Interface 1/0/1)#ipv6 address 2001:1::1/64
(Netgear Switch) (Interface 1/0/1)#ipv6 enable
(Netgear Switch) (Interface 1/0/1)#ipv6 pim
(Netgear Switch) (Interface 1/0/1)#ipv6 ospf
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13) #routing
(Netgear Switch) (Interface 1/0/13)#ipv6 address 2001:2::1/64
(Netgear Switch) (Interface 1/0/13)#ipv6 enable
(Netgear Switch) (Interface 1/0/13) #ipv6 pim
(Netgear Switch) (Interface 1/0/13)#ipv6 ospf
(Netgear Switch) (Interface 1/0/13)#exit
```

MLD on Switch B

1. Enable OSPFv3 to build a unicast route table.

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

2. Enable IPV6 unicast routing on the switch.

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

3. Enable IPV6 MLD on the switch.

(Netgear Switch) (Config)#ipv6 mld router

4. Enable IPV6 PIM-DM on the switch.

(Netgear Switch) (Config)#ipv6 pim dense

5. Enable IP multicast forwarding on the switch.

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

6. Enable MLD on interface 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21) #routing
(Netgear Switch) (Interface 1/0/21)#ipv6 address 2001:1::2/64
(Netgear Switch) (Interface 1/0/21)#ipv6 enable
(Netgear Switch) (Interface 1/0/21)#ipv6 pim
(Netgear Switch) (Interface 1/0/21)#ipv6 ospf
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24) #routing
(Netgear Switch) (Interface 1/0/24)#ipv6 address 2001:3::1/64
(Netgear Switch) (Interface 1/0/24)#ipv6 enable
(Netgear Switch) (Interface 1/0/24) #ipv6 mld router
(Netgear Switch) (Interface 1/0/24)#ipv6 pim
(Netgear Switch) (Interface 1/0/24) #exit
The MLD group information on switch B:
(B) #show ipv6 mld groups ff32::1
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.

System	S	witching	5	Routing		QoS	Securi	ty	Monitoring	3	Maintenance	Help	Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP	Multicast	IPv6 Multicast	
IP			IP Con	figuration									
• Basic		~	Defau	lt Time t	o Live				64				
• IP Configurat	tion		Routi	n <mark>g Mod</mark> e					Enable	e 💿 Disat	ple		
 Statistics 			ICMP	Echo R	eplies				Enable	e 🖲 Disat	ole		
 Advanced 		v	ICMP	Redirec	ts				Enable	e 🖲 Disat	ble		
			ICMP	Rate Lir	nit Inter	val			1000		(0 to 21-	47483647 ms)	
			ICMP	Rate Lir	nit Bur	st Size			100		(1 to 20	0)	
			Maxi	num Ne>	t Hops				4		4.000	4.85	

- **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.

System	S	witching		Routing	-	QoS	Securit	y Monitoring	J	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast	
IPve	i		IPv6 G	lobal Co	nfigurat	ion						
Basic		^	IPv6 l	Jnicast I	Routing	i.	(🔵 Disable 💿 Enable)			
Global Config	juratio	m	Hop L	.imit				64	(1 to :	255)		
Route Table			ICMP	v6 Rate	Limit E	rror Interv	al	1000	(0 to :	2147483647 m	isecs)	
 Advanced 		Y	ICMP	v6 Rate	Limit B	urst Size		100	(1 to :	200)		

- **b.** For IPv6 Unicast Routing, select the **Enabl**e 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.

System Switchin	9	Routing	QoS	Security	Monitoring	Mainter	ance	Help k	ndex			
Routing Table IP IP-10	VLA	N ARP	RIP OSPE	OSPFv3	Router Discovery	VRRP Multi	cast IPv6 M	hilticast				
IPv6	IPv6	Interface C	onfiguration									
Basic	* 12	3 VLANS	As									Go
Advanced Global Configuration	•	Interface	IPv6 Mode	DHCPv6 Client Mode	Stateless Address AutoConfig Mode	Routing Mode	Admin Mode	Operational Mode	мто	Duplicate Address Detection Transmits	Life Time Interval	Adv NS Interval
Interface Configuration		1/0/1	Enable *	Disable	Disable ~	Enable +	Enable ×	Disuble	1500	1	1800	0
Prefix Configuration		1/0/1	Enable	Disable	Disable	Enable	Enable	Disable	1500	1	1800	0
Statistics	B	1/0/2	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
*Neighbour Table	0	1/0/3	Disable	Disable	Disable	Enable	Enable	Disable	1500	1	1800	0
Static Route Configuration	8	1/0/5	Disable	Disable	Disable	Disable	Enable	Disable	1500	i	1800	0
Route Table	8	1/0/6	Disable Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
Route Preference	E	1/0/8	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800	0
•Tunnel Configuration	0	1/0/9	Disable Disable	Disable Disable	Disable	Disable Disable	Enable	Disable Disable	1500 1500	1	1800	0

- 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.

System	Switching	2	Routing	QoS	Security	Monitoring		Maintenance	Help	Index				
Routing Table II	P IIN6	VLAN	ARP	RIP OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast					
IPv6		IPv6	interface Se	election										
• Basic		Inte	rface	1/0/1 ~										
Advanced	~			Franker and										
• Global Configura	noite													
Interface Config	uration	IPv6	interface Co	sofiguration										
Prefix Configura	tion		INE DWEN	li -	Drafty Land	ek ELUGA		Valid Life	Pref	erred	Onlink		Autonomous	Current
Statistics			ibio i ress		Filmer could			Time	Life	Time	Flag		Flag	State
•Neighbour Table	0				1		~	-				4	~	
Static Route			2001:1:1:	1	64	Disabl	e	2592000	6048	00	Enable		Enable	[TENT]
Configuration		10	fe80::220d	: c8#fe4d 9575	64	Disabl	0							[TENT]
 Route Table 														
*Route Preference	10													
	Second													

- **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.

System	Switching	g	Routing	QoS	S Securi	ty	Monitoring		Maintenance	Help	Index
Routing Table	IP IPv6	VLAN	ARP	RIP OS	PF OSPFv3	Router	Discovery	VRRF	P Multicast	IPv6 Multicast	
IPvē	;	IPv6 I	nterface S	election							
Basic	~	Inter	face	1/0/13	×						
Advanced	-	1		110110							
Global Config	juration										
• Interface Con	figuration	IPv6 I	nterface C	onfiguration							
Prefix Configu	uration		Inv6 Droft		Drofiy Lor	ath	ELIIGA		Valid Life	Prefer	red
 Statistics 			ipvo i reil	^	I TENA LEI	gui	20104		Time	Life Ti	me
• Neighbour Ta	ble							~			
Static Route			2001:2::1		64		Disable	е	2592000	60480	10
Configuration			fe80::220	c:c8ff.fe4d:9	575 64		Disable	e			
• Route Table											
• Route Prefere	ence										

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.



- **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.

System	Sw	itching		Routing	Qo	S Se	curity	Monitoring	M	aintenance	Hel)	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP O	SPF OSPI	v3 Route	r Discovery	VRRP	Multicast	IPv6 Multic	ast	
OSPF	Fv3		OSPF	v3 Interfac	ce Configur	ation							
• Basic		~	12	3 VLANS	All								
 Advanced 		^			10.0	n			-	-	1		
• OSPFv3 Con	figurati	on		Interface	Address	Area ID		Admin Mode	Priority	Interval	Interval	Dead Interval	LSA Ack Interval
Common Are	a			1/0/1		0.0.0.0		Enable 🗸	1	5	10	40	1
Configuration				1/0/1		0.0.0.0		Enable	1	5	10	40	1
 Stub Area Co 	onfigura	tion		1/0/2		0.0.0		Disable	1	5	10	40	1
 NSSA Area 				1/0/3		0.0.0		Disable	1	5	10	40	1
Configuration				1/0/4		0.0.0		Disable	1	5	10	40	1
Area Range				1/0/5		0.0.0		Disable	1	5	10	40	1
Configuration				1/0/6		0.0.0		Disable	1	5	10	40	1
 Interface Con 	ifigurati	on		1/0/7		0.0.0.0		Disable	1	5	10	40	1

- 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.

System	S۱	vitching		Routing		QoS	Securi	ty	Monitoring		Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP		IPv6 Multicast	
Multic	ast		Global	Configur	ation								
Mroute Table			Admi	n Mode			0	Disable	💿 Enable				
Global Configur	ation		Proto	col State	9		No	n-Opera	ational				
 Interface Config 	uratio	n	Table	Maximu	m Entr	y Count	204	8					
- DVMRP		~	Proto	col			No	Protoc	ol Enabled				
• IGMP		~	Table	Entry C	ount		0						
• PIM		~											
 Static Routes Configuration 													
 Admin Boundar Configuration 	У												

- **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.

System	Sw	vitching		Routing		QoS	Securit	y Mo	onitoring	I	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Dise	covery	VRRP	Multicast	IPv6 Multicast	π
IPv6 Mu	lticast		PIM G	lobal Cor	figurati	on							
 Mroute Table 			Admi	n Mode		O Disal	ble 💿 PIM-S	M PIM-D	M				
- IPv6 PIM		^											
Global Config	guration	15											
 SSM Configu 	uration												
 Interface Cor 	nfigurati	ion											
• PIM Neighbo	or												
 Candidate RI Configuration 	P 1												
 BSR Candida Configuration 	ate 1												
 Static RP Co 	onfigura	ition											
• MLD		~											
 Static Routes Configuration 													

- **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.

System	Switching		Routing	QoS	Security	Monitoring	Maintenan	ce Help	Index		
Routing Table	IP IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Ro	uter Discovery VI	RRP Multicas	t IPv6 Multicast			
IPv6 Mul	ticast	PIM	Interface C	onfiguration							
Mroute Table		12	3 VLANS	All						G	o To Interface
- IPv6 PIM	~	Terry			lan an a		The second s	Norman and a state of the second s			
 Global Confid 	uration		Interface	Admin Mode	Protocol State	IPv6 Prefix/Length	Hello Interval	Join/Prune Interval	BSR Border	DR Priority	Designated Route
• SSM Configu	ration		1/0/1	Enable 🛩	Non-Operational		30	60	Disable 🛩	1	
- SSIVI Conligu	ration		1/0/1	Disable	Non-Operational		30	60	Disable	1	
 Interface Cor 	figuration		1/0/2	Disable	Non-Operational		30	60	Disable	1	
• PIM Neighbo			1/0/3	Disable	Non-Operational		30	60	Disable	1	
Candidate RI	0		1/0/4	Disable	Non-Operational		30	60	Disable	1	
Configuration			1/0/5	Disable	Non-Operational		30	60	Disable	1	
 BSR Candida 	ite		1/0/6	Disable	Non-Operational		30	60	Disable	1	
Configuration			1/0/7	Disable	Non-Operational		30	60	Disable	1	
 Static RP Co 	nfiguration		1/0/8	Disable	Non-Operational		30	60	Disable	1	
• MLD	×		1/0/9	Disable	Non-Operational		30	60	Disable	1	
- Statia Doutoo			1/0/10	Disable	Non-Operational		30	60	Disable	1	
Configuration			1/0/11	Disable	Non-Operational		30	60	Disable	1	

- 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.

System	Sw	itching		Routing		QoS	Securi	ty	Monitoring	3	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP	Multicast	IPv6 Multicast	
ID			ID Card										
IF			IP Con	iguration	1								
 Basic 		^	Defau	lt Time t	o Live				64				
 IP Configurati 	on		Routir	ng Mode					Enable	e 🔘 Disab	le		
 Statistics 			ICMP	Echo R	eplies				Enable	e 🔘 Disab	le		
 Advanced 		~	ICMP	Redirec	ts				Enable	e 🖲 Disab	le		
			ICMP	Rate Lin	mit Inte	rval			1000		(0 to 214	47483647 ms)	
			ICMP	Rate Li	nit Bur	st Size			100		(1 to 200	0)	
			Maxir	num Nex	d Hops				4				

- **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.

System	Sv	witching		Routing		QoS	Securi	y Monito	ring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discove	ry VRRP	Multicast	IPv6 Multicast	
IPve	į		IPv6 G	lobal Co	nfigurat	ion						
Basic		^	IPv6 I	Jnicast I	Routing	É.	9	🖲 Disable 🔘 En	able			
Global Config	uratio	n	Hop L	.imit				64	(1 to	255)		
 Route Table 			ICMP	v6 Rate	Limit E	rror Interv	al	1000	(0 to	2147483647 r	nsecs)	
Advancod		~	ICMP	v6 Rate	Limit B	urst Size		100	(1 to	200)		

- **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.

System	Switching		Routing	QoS	Security	/ Monitoring	Mainte	enance	Help	Index		
Routing Table	IP IPv6	VLAN	ARP	RIP OSPF	OSPFv3	Router Discovery	VRRP Mul	ticast IPv6 M	ulticast			
IPvé		IPv6 I	nterface C	onfiguration								
• Basic	¥	12	3 VLANS	All								12
 Advanced Global Config 	vration	U	Interface	IPv6 Mode	DHCPv6 Client Mode	Stateless Address AutoConfig Mode	Routing Mode	Admin Mode	Operationa Mode	MTU	Duplicate Address Detection Transmits	Life Time Interval
Interface Con	figuration		1/0/21	Enable 🗸	Enable 👻	Enable Y	Disable 🗸	Enable Y	Disable	1500	1	1800
Prefix Config	uration		1/0/1	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800
Statistics			1/0/2	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800
• Neighbour Ta	hlo		1/0/3	Disable	Disable	Disable	Disable	Enable	Disable	<mark>1500</mark>	1	1800
Neighbour ra	bie		1/0/4	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800
 Static Route Configuration 			1/0/5	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800
Configuration			1/0/6	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800
• Route Table			1/0/7	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800
• Route Prefere	ence		1/0/8	Disable	Disable	Disable	Disable	Enable	Disable	1500	1	1800
 Tunnel Config 	juration		1/0/9	Disable	Disable	Disable	Disable	Enable	Disa <mark>b</mark> le	1500	1	<mark>1</mark> 800

- 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.

System	Switch	ning		Routing		QoS	Securit		Monitoring		Maintenance	Help	Index
Routing Table	IP IP	√6 \\	'LAN	ARP	RIP	OSPF	OSPFv3	Route	er Discovery	VRRP	Multicast	IPv6 Multicast	
IPv6	ļ.		Pv6 Inte	erface S	electio	on							
•Basic		~	Interfa	се	F	1/0/21 ~							
 Advanced 		~											
 Global Config 	uration												
Interface Con'	figuration	1	Pv6 Inte	arface C	onfigu	ration							
Prefix Configu	uration		÷.							Va	lid Life	Preferred	
 Statistics 			L) Ip	w6 Pretic	x	H	refix Length		EU164	Tir	né	Life Time	
• Neighbour Ta	ble		2	2000:1::2	!	6	i4			~			
Static Route Configuration													

- **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.

System Swite	hing		Routing	QoS	Security	y N	lonitoring	Mainte	nance	Help Index	
Routing Table IP		VLAN	ARP	RIP OSP	F OSPFv3	Router Di	scovery V	RRP Mult	icast IPv6 N	Aulticast	
IPv6		IPv6 In	terface S	election							
•Basic	~	Interfa	ace	1/0/24	~						
 Advanced 	~										
 Global Configuration 											
 Interface Configuration 		IPv6 In	terface C	onfiguration							_
Prefix Configuration			nu C Drofo		Deafur Lanath		ELIICA	Valid Life		Preferred	
Statistics			pvo mielo	¢.	Prelix Length		E0104	Time		Life Time	
 Neighbour Table 			2000:5::1	(64		~				

- 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.



- 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.

System	Swit	ching		Routing	Qo	S	Security	Monitorin	g N	laintenance	Hel	p	Index
Routing Table	IP I	Pv6	VLAN	ARP	RIP O	SPF 0	SPEV3 Ro	uter Discovery	VRRP	Multicast	IPv6 Multi	cast	
OSPF	=v3		OSPF	v3 Interfac	ce Configur	ation							
• Basic		~	12:	3 VLANS	All								
 Advanced 		~		o townsheet	in c				1	-	(hannes)	1 PROVIDED	1000
• OSPFv3 Con	figuratio	n		Interface	Address	Area ID		Mode	Priority	Interval	Interval	Interval	Interval
Common Are	a								~	1			1
Configuration	15 - 1962 - 197			1/0/1		0.0.0.0		Disable	1	5	10	40	1
 Stub Area Co 	onfigurat	ion		1/0/2		0.0.0.0		Disable	1	5	10	40	1
•NSSA Area				1/0/3		0.0.0.0		Disable	1	5	10	40	1
Configuration	S.			1/0/4		0.0.0.0		Disable	1	5	10	40	1
 Area Range 				1/0/5		0.0.0.0		Disable	1	5	10	40	1
Configuration	l)			1/0/6		0.0.0.0		Disable	1	5	10	40	1
 Interface Cor 	figuratio	n		1/0/7		0.0.0.0		Disable	1	5	10	40	1
+ Interface Cto	tiotico			1/0/8		0000		Dicable	4	E	10	40	4

- **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.

System	Switc	hing		Routing		QoS	Securi	ty	Monitoring	g	Maintenance	Help	Index
Routing Table	IP IP	v6 \	LAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRR	P Multicast	IPv6 Multica	st
Multic	ast		Global	Configur	ation								
Mroute Table			Admi	n Mode			۲	Disabl	e 🔘 Enable				
 Global Configur 	ation		Proto	col State	9		No	n-Opei	ational				
 Interface Config 	uration		Table	Maximu	m Ent	ry Count	204	18					
 DVMRP 		~	Proto	col			No	Proto	ol Enabled				
• IGMP		~	Table	Entry Co	ount		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.

System	S	witching		Routing		QoS	Securit	y Monitoring		Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast	
IPv6 Mu	lticast		PIM GI	obal Co	nfigurati	on						
• Mroute Table • IPv6 PIM		^	Admi	n Mode		O Disa	ble 🖲 PIM-S	SM 🔘 PIM-DM				
Global Config	guratio	on.										
• SSM Configu	iration	i.										

- **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.

System	Switching		Routing	QoS	Security	Monitoring	Maintenan	ce Help	Index		
Routing Table	IP IPv6	VLAN	I ARP	RIP OSPF	OSPFv3 Ro	uter Discovery VF	RP Multicas	t IPv6 Multicast	· · · · · ·		
ID C MA	1	DIM		- F							
	llicast	Pilvi	ntenace C	onliguration							
Mroute Table		12	3 VLANS	All						G	io To Interface
IPv6 PIM	^	1 mail					Transmont		Tarana arrista	-	Contractor and the second
Global Confid	uration		interface	Admin Mode	Protocol State	IPv6 Prefix/Length	Hello Interval	Join/Prune Interval	BSR Border	DR Priority	Designated Router
10011 Carta				~					~		
- SSIM Conligu	iration		1/0/1	Disable	Non-Operational		30	60	Disable	1	
 Interface Cor 	ifiguration		1/0/2	Disable	Non-Operational		30	60	Disable	1	
• PIM Neighbo	r		1/0/3	Disable	Non-Operational		30	60	Disable	1	
Candidate RI	Þ		1/0/4	Disable	Non-Operational		30	60	Disable	1	
Configuration	Í.		1/0/5	Disable	Non-Operational		30	60	Disable	1	

- **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.

System	Sv	witching		Routing		QoS	Securit	y Monitorin	g	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRF	P Multicast	IPv6 Multicast	
IPv6 Mu	lticast		MLD G	ilobal Co	nfigurat	ion						
 Mroute Table 			Admi	n Mode		🔘 Disa	ble 🖲 Enabl	e				
IPv6 PIM		¥										
• MLD		^										
Global Config	guratio	n.										
 Routing Inter Configuration 	face 1											
 Routing Inter Statistics 	face											
• MLD Groups												
• MLD Traffic												
Proxy Interfa Configuration	ce 1											
 Proxy Interfa Statistics 	се											
• Proxy Memb	ership											
 Static Routes Configuration 												

- **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.

System	Sv	vitching		Routing	QoS	Security	Monitorin	g Mai	ntenance	Help	Index	
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Ro	uter Discovery	VRRP N	Iulticast IPV6			
IPv6 Mu	ticast		MLD	Routing In	terface Configu	ration						
• Mroute Table			12	3 VLANS	All							
• IPv6 PIM		~						1				
- MLD		^	ų	Interface	Admin Mode	Operational Mod	e Version	Robustness	Query Interval	Query Ma	ix Response Time	Startup Query Interval
• Global Confi	uratio	1		1/0/24	Enable 👻	Not In Service	V2	2	125	10000		31
		8. 		1/0/1	Disable	Not In Service	V2	2	125	10000		31
Configuration	ace			1/0/2	Disable	Not In Service	V2	2	125	10000		31
 Routing Inter 	face			1/0/3	Disable	Not In Service	V2	2	125	10000		31
Statistics	2225			1/0/4	Disable	Not In Service	V2	2	125	10000		31

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.

Syste	em	Sv	vitching		Routing	QoS	Security	Monit	oring	Maintenance	Help	Index
	Auto-V	/olP	iSCSI	STP	Multicast	MVR	Address Table	Ports LA	g MLA	AG		
	VLA	N		Reset								
 Basic 			^	Reset	Configuratio	n						
• VLAN	I Config	uration	15									
• Advance	ed		~									
				Internal	VLAN Confi	guration						
				Interna	al VLAN Allo	cation Bas	e 40	93				
				Intern	al VLAN Allo	cation Poli	cy 🔘	Ascending 💿	Descend	ing		
				VLAN (Configuration							
					/LAN ID VL	AN Name	VLAN Type	Make Static				
					300			Disable 👻				
					de	fault	Default	Disable			12	

- 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.

Syste	m	Switching		Routing		QoS		Seci	urity		М	onito	ring		Ma	ainter	ance	•	1	Help	2	lı	ıdex		
VLAN	Auto-VolP	iscsi	STP	Multica	st	MVR	Add	ress Ta	able	Por	ts	LAG	3 1	MLAG	3										
	VLAN		VLAN	Vemberst	nip																				
• Basic		~	VLAN	ID														300	~						
* Advance	ed	^	Group	Operatio	n													Unta	q All	~	-				
• VLAN	Configurat	ion	VLAN	Name													1	/LAN	0300						
• VLAN	Membersh	nip	VLAN	Type														Static							
• VLAN	Status		100	nit 1																					
Port F Config	VID juration		Ports		5	7	9 1	1 13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
Protoc Group	based VLA col Based \ Configurat	VLAN ion		2 4	6	8	10 1	2 14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48

- 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.

Syste	em S	Switching		Routing	Q	oS Security	Monitorin	g Maintenance	Help	Index
VLAN	Auto-VolP	iSCSI	STF	P Multica	ast MV	R Address Table	Ports LAG	MLAG		
ġ.	VLAN		PVID	Configurat	ion					
• Basic		~	12	3 LAGS A	JI					
• Advanc • VLAN	ed I Configuratio	^ on		Interface	PVID	VLAN Member	VLAN Tag	Acceptable	Frame Types	Configured Ing
• VLAN	I Membership	р		1/0/1	300	1	None	Admit All	~	Disable 🗸
. VLAN	I Status			1/0/1	1	1	None	Admit All		Disable
• Port I	PVID			1/0/2	1	1	None	Admit All		Disable
Confi	guration	-		1/0/3	1	1	None	Admit All		Disable

- 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.

em S	witching	Rou	uting C	loS	Security		Monitoring		Maintenance	Help	Index
Auto-VolP	iSCSI	STP M	Aulticast MN	R A	ddress Table	Ports	LAG	MLAC	3		
Multicast		MLD Snoo	ping Configura	tion							
	~	MLD Sno	oping Admin N	Aode) Di	sable 💿 Ei	nable			
Snooping	~	Multicast	Control Frame	Count		0					
nooping	^	Interfaces	s Enabled for N	ILD Sno	ooping						
guration		Proxy Qu	uerier Mode) Di	sable 🖲 Ei	nable			
ace Configura	ation										
	em S Auto-VolP Multicast Snooping guration ace Configura	am Switching Auto-VoIP iSCSI Multicast × Snooping × guration ace Configuration	Switching Rot Auto-VoIP iSCSI STP I Multicast MLD Snoc MLD Snoc MLD Snoc snooping Multicast Interface guration Proxy Qu Proxy Qu	em Switching Routing Q Auto-VoIP iSCSI STP Multicast MV Multicast MLD Snooping Configura MLD Snooping Admin M Multicast Control Frame Interfaces Enabled for M Proxy Querier Mode	em Switching Routing QoS Auto-VoIP iSCSI STP Multicast MVR Au Multicast MLD Snooping Configuration MLD Snooping Admin Mode Multicast Control Frame Count Interfaces Enabled for MLD Sno guration Proxy Querier Mode	em Switching Routing QoS Security Auto-VoIP iSCSI STP Multicast MVR Address Table Multicast Multicast MLD Snooping Configuration MLD Snooping Admin Mode Multicast Control Frame Count Interfaces Enabled for MLD Snooping guration Proxy Querier Mode	switching Routing QoS Security I Auto-VoIP iSCSI STP Multicast MVR Address Table Ports Multicast MLD Snooping Configuration MLD Snooping Admin Mode Image: Configuration Image: Configuration <td>Switching Routing QoS Security Monitoring Auto-VolP iSCSI STP Multicast MVR Address Table Ports LAG Multicast MLD Snooping Configuration Disable © E Snooping MLD Snooping Admin Mode © Disable © E Nooping Multicast Control Frame Count 0 nooping Interfaces Enabled for MLD Snooping © Disable © E guration Proxy Querier Mode © Disable © E</td> <th>Switching Routing QoS Security Monitoring Auto-VoIP iSCSI STP Multiceast MVR Address Table Ports LAG MLAC Multiceast MLD Snooping Configuration Image: Configuration</th> <td>Switching Routing QoS Security Monitoring Maintenance Auto-VoIP iSCSI STP Multicast MVR Address Table Ports LAG MLA Multicast MLD Snooping Configuration O Disable © Enable Multicast MLD Snooping Admin Mode © Disable © Enable Monitoring Multicast Control Frame Count 0 Interfaces Enabled for MLD Snooping Interfaces Enabled for MLD Snooping Proxy Querier Mode © Disable © Enable</td> <td>Switching Routing QoS Security Monitoring Maintenance Help Auto-VoIP iSCSI STP Multicast MVR Address Table Ports LAG MLA Multicast MLD Snooping Configuration MLD Snooping Control Frame Count 0 Interfaces Enabled for MLD Snooping Proxy Querier Mode © © Disable © Enable </td>	Switching Routing QoS Security Monitoring Auto-VolP iSCSI STP Multicast MVR Address Table Ports LAG Multicast MLD Snooping Configuration Disable © E Snooping MLD Snooping Admin Mode © Disable © E Nooping Multicast Control Frame Count 0 nooping Interfaces Enabled for MLD Snooping © Disable © E guration Proxy Querier Mode © Disable © E	Switching Routing QoS Security Monitoring Auto-VoIP iSCSI STP Multiceast MVR Address Table Ports LAG MLAC Multiceast MLD Snooping Configuration Image: Configuration	Switching Routing QoS Security Monitoring Maintenance Auto-VoIP iSCSI STP Multicast MVR Address Table Ports LAG MLA Multicast MLD Snooping Configuration O Disable © Enable Multicast MLD Snooping Admin Mode © Disable © Enable Monitoring Multicast Control Frame Count 0 Interfaces Enabled for MLD Snooping Interfaces Enabled for MLD Snooping Proxy Querier Mode © Disable © Enable	Switching Routing QoS Security Monitoring Maintenance Help Auto-VoIP iSCSI STP Multicast MVR Address Table Ports LAG MLA Multicast MLD Snooping Configuration MLD Snooping Control Frame Count 0 Interfaces Enabled for MLD Snooping Proxy Querier Mode © © Disable © Enable

- **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.

System	S	witching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VLAN Au	ito-VolP	iSCSI	STF	Multica	ist MVR	Address Table Por	ts LAG MLAG	3		
Mu	ulticast		MLD	VLAN Conf	iguration					
MFDB IGMP Snoo	ping	*		VLAN ID	Fast Leave	Membership Interva	Maximum Response Time	Multicast Router Expiry Time	Proxy Querier Mode	
MLD Snoop	ping	~		300	×				~	
Configurat	tion									
• Interface (Configura	ation								
MLD VLA Configurat	N tion									

- **b.** Enter the following information:
 - In the VLAN ID field, enter 300.
 - In the Admin Mode field, select Enable.
- 6. Click Add.

DVMRP



Distance Vector Multicast Routing Protocol

This chapter includes the following sections:

- Distance Vector Multicast Routing Protocol Concepts
- CLI: Configure DVMRP
- Web Interface: Configure DVMRP

Note: DVMRP is available on M5300 and M6100 series switches only. However, the following M5300 series switches require a license to support DVMRP: M5300-28G, M5300-52G, M5300-28G-POE+, and M5300-52G-POE+.

Distance Vector Multicast Routing Protocol Concepts

The Distance Vector Multicast Routing Protocol (DVMRP) is used for multicasting over IP networks without routing protocols to support multicast. The DVMRP is based on the RIP protocol but more complicated than RIP. DVRMP maintains a link-state database to keep track of the return paths to the source of multicast packages.

The DVMRP operates as follows:

- The first message for any source-group pair is forwarded to the entire multicast network, with respect to the time-to-live (TTL) of the packet.
- TTL restricts the area to be flooded by the message.
- All the leaf routers that do not have members on directly attached subnetworks send back prune messages to the upstream router.
- The branch that transmitted a prune message is deleted from the delivery tree.
- The delivery tree, which is spanning to all the members in the multicast group, is constructed.

In this example, DVMRP is running on switches A, B, and C. IGMP is also running on Switch C, which is connected to the host directly. After the host sends an IGMP report to switch C, multicast streams are sent from the multicast resource to the host along the path built by DVMRP.



Figure 63. DVMRP

CLI: Configure DVMRP

DVRMP on Switch A

1. Create routing interfaces 1/0/1, 1/0/13, and 1/0/21.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.1.1 255.255.255.0
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ip address 192.168.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (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)#routing
(Netgear Switch) (Interface 1/0/21)#ip address 192.168.3.2 255.255.0
(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 Summar	У							
			Incoming	Outgoing						
Source IP	Group IP	Protocol	Interface	Interface List						
192.168.1.2	225.0.0.1	DVMRP	1/0/1	1/0/21						

DVRMP on Switch B

1. Create routing ports 1/0/13 and 1/0/20.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ip address 192.168.2.2 255.255.255.0
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (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) (Interface 1/0/20)#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 s	ummary
Multicast Route Table Summary	
Incom	ing Outgoing
Source IP Group IP Protocol Inter	face 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) (Interface 1/0/3)#interface 1/0/3
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.168.4.2 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#routing
(Netgear Switch) (Interface 1/0/24)#ip address 192.168.5.1 255.255.255.0
(Netgear Switch) (Interface 1/0/24)#exit
```

2. Enable IP multicast forwarding on the switch.

(Netgear Switch) (Config)#ip multicast

3. Enable IP DVMRP protocol on the switch.

(Netgear Switch) (Config) #ip dvmrp

4. Enable DVMRP mode on interfaces 1/0/3, 1/0/11, and 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip dvmrp
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#interface 1/0/11
(Netgear Switch) (Interface 1/0/11)#ip dvmrp
(Netgear Switch) (Interface 1/0/11)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#ip dvrmp
(Netgear Switch) (Interface 1/0/24)#ip dvrmp
```

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	n) #show ip dvmr	p neighbor		
Interface			1/0/11	
Neighbor IP Add	lress		192.168	.3.2
State			Active	
Up Time (hh:mm:	ss)		00:01:0	3
Expiry Time (hł	1:mm:ss)		00:00:2	4
Generation ID .			88099	
Major Version .			3	
Minor Version .			255	
Capabilities			Prune G	enID Missing 11441
Received Routes	3		0	
Received Bad Pa	ackets		0	
Received Bad Ro	outes		0	
Interface			1/0/3	
Neighbor IP Add	lress		192.168	.4.1
State			Active	
Up Time (hh:mm:	ss)		00:01:1	7
Expiry Time (hł	1:mm:ss)		00:00:2	3
Generation ID .			1116347	728
Major Version .			3	
Minor Version .			255	
More Entries or	quit(q)			
Capabilities			Prune G	enID Missing 11441
Received Routes	3		0	
Received Bad Pa	ackets		0	
Received Bad Ro	outes		0	
(Netgear Switch	n) #show ip mcas	st mroute deta	il summary	
	Multicast Ro	oute Table Sum	mary	
			Incoming	Outgoing
Source IP	Group IP	Protocol	Interface	Interface List
192.168.1.2	225.0.0.1	DVMRP	1/0/11	1/0/24

Web Interface: Configure DVMRP

DVMRP on Switch A

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

A screen similar to the following displays.

System	SI	witching		Routing		QoS	Securi	ty	Monitoring	g 🛛 🛚 🔊	laintenance	Help	Index
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast	
IP			IP Con	figuration	1								
Basic		^	Defau	lt Time t	o Live				64				
• IP Configurat	tion		Routi	ng Mode					Enable	e 💿 Disabl	e		
 Statistics 			ICMP	Echo R	eplies				Enable	e 🖲 Disabl	е		
Advanced		~	ICMP	Redirec	ts				Enable	e 🖲 Disabl	e		
			ICMP	Rate Lin	mit Inte	rval			1000		(0 to 21	47483647 ms)	
			ICMP	Rate Lin	mit Bur	st Size			100		(1 to 200	0)	
			Maxi	num Nex	d Hops	5			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.

System		witching		Routin		QoS	Securit		Monitorin		Maintenance	Help	Index	
Routing Table	P	IPv6	VLAN	I ARP	RIP	OSPF	OSPFv3	Route	er Discovery	VRRF	P Multicast	IPv6 Multicast		
IP			IP Inf	erface C	onfigurat	ion								
• Basic		~	12	3 VLAN	S All									
 Advanced IP Configuration 	on	^		Port	Descrip	otion	VLAN ID	IP Ac Meth	ldress Config od	juration	IP Address	Subnet Mask	Ro Mo	uting ode
 Statistics 				1/0/1				Man	iual 🛩		192.168.1.1	255.255.2	55.0 E	nable 🗸
• IP Interface			2	1/0/1				Manu	al		192.168.1.1	255.255.25	55.0 En	able

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.

System		witching		Routin		QoS	Securit	y Monitoring		Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast	
IP		Ť	IP Int	erface C	onfigurat	ion						
• Basic		~	1 2	3 VLAN	s all							
 Advanced IP Configurat 	ion	^		Port	Descrip	otion	VLAN ID	IP Address Config Method	uration	IP Address	Subnet Mask	Routing Mode
 Statistics 				1/0/13				Manual 🗸		192.168.2.1	255.255.25	5.0 Enable
• IP Interface				1/0/1				Manual		192,168,1,1	255.255.255	5.0 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.

System	Switch	hing		Routing	3	QoS	Securit	y	Monitoring	3	Maintenance	Help	Index	
Routing Table	IP IP	v6	VLAN	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP	Multicast	IPv6 Multicast		
IP		į,	IP Inte	erface Co	onfigurat	ion								
• Basic		~	12	3 VLAN	s ali									
 Advanced 		^						10.4	dalara a Maraka			Deckarat	Dec	
• IP Configuration	on			Port	Descrip	otion	VLAN ID	Meth	nod	uration	IP Address	Mask	Mo	de
 Statistics 				1/0/21				Ma	nual 🗸		192.168.3.2	255.255.2	255.0 Ei	nable 🗸
IP Interface				1/0/1				Man	ual		192.168.1.1	255.255.2	255.0 En:	able

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.

System Swite	hing		Routing		QoS	Securi	ty	Monitoring		Maintenance	Help	Index
Routing Table IP IF	v6	VLAN	ARP	RIP	OSPF	OSPFv3	Router	Discovery	VRRP	Multicast	IPv6 Multicast	
Multicast		Global	Configur	ation								
Mroute Table		Admir	n Mode			۲	Disable 🔘	Enable				
Global Configuration		Proto	col State	9		No	n-Operatio	nal				
 Interface Configuration 		Table	Maximu	im Entr	y Count	204	18					
DVMRP	~	Proto	col			No	Protocol I	Enabled				
IGMP	*	Table	Entry C	ount		0						
PIM	~											
 Static Routes Configuration 												
 Admin Boundary Configuration 												

- **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.

System	Swi	itching		Routing		QoS	Securit	y Monitoring		Maintenance	Help	Index
Routing Table I	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP		IPv6 Multicast	N
Multicas	st		DVMR	P Global	Config	uration						
 Mroute Table 			Admi	n Mode			Oisab	le 💿 Enable				
Global Configurat	tion		Versi	on			3					
Interface Configur	ration		Total	Number	of Rout	es	0					
• DVMRP		^	Reac	hable Ro	utes		0					
Global Configur	ration	ţ.										
 Interface Config 	guratio	on										
DVMRP Neight	bor											
• DVMRP Next H	Hop											
DVMRP Prune												
• DVMRP Route												
•IGMP		~										

- 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.

	Switchin	9	Routing	QoS	Security	Monitoring	Maintenan	ce Help	Index		
Routing Table	IP IPv6	VLA	N ARP	RIP OSPF	OSPEv3 Ra	uter Discovery	VRRP Mailinea	IPv6 Multica	ast		
Multicar	ate:	DVN	ARP Interfa	ce Configuration							
Mroute Table		1	2 3 VLANS	All						Go To Interface	Go
Global Configuration	tion				Interface	Parameters			Interface	Statistics	
Intenace Comgu Intenace	ration		Interface	Interface Mode	Protocol State	Local Address	Interface Metric	Generation ID	Received Bad Packets	Received Bad Routes	Sent Routes
Global Configu	ration		1/0/1	Enable -	Not In Service	192,168 1.1	1		0	0	0
Interface Confi	auration	2	1/0/1	Enable	Not In Service	192.168.1.1	1		0	0	0
Third de course	and the second second	100	i i a le le	With a file	Alast In Providence					10	

- 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.

System	Swite	hing:	Routing		QoS	Securit	y	Monitoring	,	Maintenance	Help	Index
Routing Table	IP IF	W6 VI	AN ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast	
		IF	Configuration	1								
• Basic		~	Default Time t	o Live				64				
Advanced		~ 1	Routing Mode					Enable	e 🔘 Disab	ole		
 IP Configuration 	ion		CMP Echo R	eplies				Enable	e 🔘 Disab	ole		
 Statistics 		1	CMP Redirec	ts				Enable	e 🖲 Disab	ble		
• IP Interface)	CMP Rate Li	nit Inte	rval			1000		(0 to 21	47483647 ms)	
Configuration		1	CMP Rate Li	nit Bur	st Size			100		(1 to 200	0)	
 Secondary IF)	1	Maximum Ne:	kt Hops				4				

- 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.

System	Sv	vitching		Routin	g	QoS	Securit	y Monitoring	Maintenance	Help	Index	
Routing Table	IP	IPv6	VLAN	I ARP	RIP	OSPF	OSPFv3	Router Discovery VF	RP Multicast	IPv6 Multicast		
IP			IP Int	erface C	onfigurat	ion						
• Basic		~	12	3 VLAN	S All							
• Advanced • IP Configurati	on	^		Port	Descrip	otion	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Routing Mode	Administrative Mode
 Statistics 				1/0/13	1			Manual 🛩	192.168.2.2	255.255.255.	0 Enable	✓ Enable ✓
IP Interface Configuration				1/0/1				Manual	192.168.1.1	255.255.255. 0 0 0 0	0 Enable Disable	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 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.

System	S	witching		Routin	g	QoS	Securit	y Monitoring	Maintenance	Help	Index	
Routing Table	IP	IPv6	VLAN	I ARP	RIP	OSPF	OSPFv3	Router Discovery VI	RRP Multicast	IPv6 Multicast		
P			IP Int	erface C	onfigurati	on						
•Basic		*	12	3 VLAN	S All							
 Advanced IP Configurat 	ion	^		Port	Descrip	tion	VLAN ID	IP Address Configurati Method	on IP Address	Subnet Mask	Routing Mode	Administrative Mode
 Statistics 				1/0/20				Manual 👻	192.168.4.1	255.255.255	5.0 Enable	✓ Enable ✓
• IP Interface				1/0/1				Manual	192.168.1.1	255.255.255	i.0 Enable	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.

System	S	witching		Routing		QoS	Securi	ty	Monitoring	,	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Route	r Discovery	VRRP	Multicast	IPv6 Multicast	
Multic	ast		Global	Configur	ation								
Mroute Table			Admi	n Mode			۲	Disable	Enable				
 Global Configur 	ration		Proto	col State	Э		No	n-Operat	ional				
 Interface Config 	guratio	n	Table	Maximu	im Entr	y Count	204	18					
- DVMRP		~	Proto	col			No	Protoco	Enabled				
• IGMP		×	Table	Entry C	ount		0						
• PIM		~											
 Static Routes Configuration 													
Admin Bounda Configuration	гу												

- **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.

System	Sv	vitching		Routing		QoS	Securi	ty Monitoring		Maintenance	Help	Index
Routing Table IF	P	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP		IPv6 Multicast	
Multicast	t		DVMR	P Global	Config	uration						
Mroute Table			Admin	n Mode			Oisat	e 🖲 Ena <mark>b</mark> le				
 Global Configurati 	on		Versi	on			3					
Interface Configura	ation	n	Total	Number	of Rou	tes	0					
• DVMRP		^	Reac	hable Ro	utes		0					
Global Configura	atio	nt										
Interface Config	urat	ion										
DVMRP Neighb	or											
• DVMRP Next H	lop											
DVMRP Prune												
DVMRP Route												

- **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.

System	Switching		Routing	QoS	Security	Monitoring	Maintenan	ice Help	Index		
Routing Table IF	P IPv6	VLA	N ARP	RIP OSPF	OSPFv3 R	outer Discovery	VRRP Malicea	el IPv6 Multic	ast		
Multicast	C I	DVN	NRP Interfac	ce Configuration							
Mroute Table		12	3 VLANS	All					(So To Interface	Go
Global Configuration	on				Interface	Parameters			Interface	Statistics	
DVMRP			Interface	Interface Mode	Protocol State	Local Address	Interface Metric	Generation ID	Received Bad Packets	Received Bad Routes	Sent Routes
Global Configura	tion			Enable 🗵			· · · · · ·				
-Interface Config	mation	0	1/0/1	Enable	Not In Service	192.168.1.1	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

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

System	Switching	R	outing		JoS	Securi		Monitoring		Maintenance	Help	Index
Routing Table	IP IPv6	VLAN .	ARP	RIP	OSPF	OSPFv3	Rout	er Discovery	VRRP	Multicast	IPv6 Multicast	
IP		IP Config	uration									
• Basic	~	Default	Time to	Live				64				
• IP Configurati	ion	Routing	Mode					Enable	e 🖲 Disat	ble		
Statistics		ICMP E	cho Rej	plies				Enable	e 💿 Disat	ole		
 Advanced 	*	ICMP R	edirects	S				Enable	e 🖲 Disat	ble		
		ICMP R	ate Lim	nit Interva	al			1000		(0 to 214	17483647 ms)	
		ICMP R	ate Lim	nit Burst	Size			100		(1 to 200))	
		Maximu	m Next	t Hops				4				

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

- 2. Configure 1/0/11 as a routing port and assign an IP address to it.
 - a. Select Routing > IP > Advanced > IP Interface Configuration.

System	S	witching		Routin	g	QoS	Security	y Monitor	ing	Maintenance	Help	Index		
Routing Table		IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discover	y VRRF	P Multicast	IPv6 Multicast			
IP	8		IP Int	erface C	onfigurat	ion								
• Basic		Ŷ	12	3 VLAN	S All									
 Advanced 		~						ID Address Car	Foundation		Culturat	Dec	ato a	Administration
• IP Configurat	on			Port	Descrip	otion	VLAN ID	Method	niguration	IP Address	Mask	Mo	de	Mode
 Statistics 				1/0/11	1			Manual 🛩		192.168.3.1	255.255.2	5.0 Er	iable 👻	Enable ~
IP Interface Configuration		2		1/0/1				None		0.0.0.0	0.0.0.0	Ena	ble	Enable

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.

System	Sv	vitching		Routin	g	QoS	Securit	y Monitoring	Maintenance	Help	Index		
Routing Table		IPv6	VLAN	I ARF	RIP	OSPF	OSPFv3	Router Discovery VRR	P Multicast	IPv6 Multicast			
IP	že Že		IP Int	erface C	onfigurat	ion							
•Basic		×	12	3 VLAN	S All								
 Advanced IP Configurat 	ion	^		Port	Descrip	xion	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Rou Mor	iting de	Administrative Mode
 Statistics 				1/0/3	1	_		Manual 👻	192.168.4.2	255.255.2	55.0 Er	iable 👻	Enable 🗸
IP Interface Configuration	i)			1/0/1				None None	0.0.0.0	0.0.0.0	Ena	ible able	Enable Enable
 Secondary If 	>		2	1/0/3				Manual	192.168.4.2	255.255.2	55.0 Ena	ible	Enable

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.

System	S	witching		Routin	g 📗	QoS	Security	y Monitoring		Maintenance	Help	Index		
Routing Table	P	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast		de .	
IP			IP Int	erface C	onfigurat	ion								
• Basic		~	12	3 VLAN	S All									
 Advanced IP Configurat 	ion	^		Port	Descrip	otion	VLAN ID	IP Address Configura Method	ation	IP Address	Subnet Mask	Rou Mor	iting de	Administrative Mode
 Statistics 				1/0/24	C			Manual ~		192.168.5.1	255.255.25	55.0 Er	iable 🗸	Enable 👻
• IP Interface				1/0/1				None		0.0.0.0	0.0.0.0	Dis	able	Enable
Configuration	2		0	1/0/2				None		0.0.0.0	0.0.0.0	Dis	able	Enable
 Secondary If 	2			1/0/3				None		0.0.0.0	0.0.0.0	Dis	able	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.

System	Sv	vitching		Routing		QoS	Securi	ty	Monitoring	g 📗	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast	
Multic	ast		Global	Configur	ation								
Mroute Table			Admir	n Mode			0	Disabl	e 🖲 Enable				
 Global Configur 	ration		Proto	col State	Э		No	n-Ope	ational				
Interface Config	guratio	n	Table	Maximu	im Entr	y Count	204	18					
• DVMRP		×	Proto	col			No	Proto	col Enabled				
•IGMP		×	Table	Entry C	ount		0						
• PIM		~											
 Static Routes Configuration 													
Admin Bounda	гу												

- **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.

System	Sv	vitching		Routing	10	QoS	Securit	y Monitoring	9	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP		IPv6 Multicast	X
Multica	ast		DVMR	P Global	Config	uration						
 Mroute Table 			Admi	n Mode			Oisab	le 🖲 Enable				
Global Configura	ation		Versi	on			3					
 Interface Configu 	uratio	n	Total	Number	of Rout	es	0					
• DVMRP		~	Reac	hable Ro	utes		0					
Global Configu	uratio	n i										
 Interface Confi 	igurat	ion										
DVMRP Neigh	hbor											
• DVMRP Next	Hop											
• DVMRP Prune	е											
• DVMRP Route	е											

- **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.

	Sw	tching		Routing	QoS	Secunty	Monitoring	Maintenan	ce Help	Index		
Routing Table	IP	IPv6	VLAN	ARP	RIP OSPF	OSPFv3 Ro	uter Discovery	VRRP Million	iPv6 Multic	aste		
Multica	ist		DVM	RP Interfac	e Configuration							
Mroute Table			12	3 VLANS	All					G	So To Interface	Go
Global Configura	ation					Interface	Parameters			Interface 3	Statistics	
number comig: NVMPP	uration			interface	Interface Mode	Protocol State	Local Address	Interface Metric	Generation ID	Received Bad Packets	Received Bad Routes	Sent Routes
Global Confin	ration				Enable ~							
Interface Confi	iourati	m	8	1/0/1	Enable	Not In Service	0.0.0.0	1		0	0	0
				1/0/2	Disable	Not In Service		1		0	0	0

- 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.

System	S	witching		Routing		QoS	Securi	y	Monitoring	3	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Rou	ter Discovery	VRRP	Multicast	IPv6 Multicast	
Multic	ast		IGMP	Global C	onfigur	ation							
• Mroute Table			Admi	n Mode	Gingan) Disa	ble 💿 Enab	le					
Global Configu	ration												
 Interface Config 	guratio	HT .											
• DVMRP		~											
• IGMP		^											
Global Config	guratic	m											

- **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.

System	Swite	hing		Routing	QoS	Secur	ity Mo	nitoring	Maintenance	Help	Index		
Routing Table	IP IF	'v6	VLAN	ARP	RIP OSP	F OSPFv3	Router Disc	overy VF	RRP Multicast	IPv6 Multicast			
Multic	act		IGME	Routing I	aterface Confi	auration							
Mroute Table			1 2	3 VLANS	All	Jananon					Go To I	nterface	Go
Global Configur Interface Config	ation uration			Interface	Admin Mode	Version	Robustness	Query Interval	Query Max Response Time	Startup Query Interval	Startup Query Count	Last Member Query Interval	Last Member Query Count
DVMRP		×		1/0/24	Enable Y	V3	2	125	100	31	2	10	2
• IGMP		~		1/0/1	Disable	V3	2	125	100	31	2	10	2
Global Config	uration			1/0/2	Disable	V3	2	125	100	31	2	10	2
 Routing Interf 	ace			1/0/3	Disable	V3	2	125	100	31	2	10	2
Configuration				1/0/4	Disable	V3	2	125	100	31	2	10	2

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.



_____ **37**

Captive portals and client authentication

This chapter includes the following sections:

- Captive Portal Concepts
- Captive Portal Configuration Concepts
- Enable a Captive Portal
- Client Access, Authentication, and Control
- Block a Captive Portal Instance
- Local Authorization, Create Users and Groups
- Remote Authorization (RADIUS) User Configuration
- SSL Certificates

Captive Portal Concepts

The captive portal feature is a software implementation that blocks clients from accessing the network until user verification has been established. You can set up verification to allow access for both guests and authenticated users. Authenticated users must be validated against a database of authorized captive portal users before access is granted.

The authentication server supports both HTTP and HTTPS web connections. In addition, you can configure a captive portal to use an optional HTTP port (in support of HTTP proxy networks). If configured, this additional port is then used exclusively by the captive portal. This optional port is in addition to the standard HTTP port 80, which is being used for all other web traffic.

The captive portal for wired interfaces allows the clients directly connected to the switch to be authenticated using a captive portal mechanism before the client is given access to the network. When you enable the captive portal feature on a wired physical port, the port is set in captive-portal- enabled state such that all the traffic coming to the port from the unauthenticated clients is dropped except for the ARP, DHCP, DNS, and NETBIOS packets. The switch forwards these packets so that unauthenticated clients can get an IP address and resolve the hostname or domain names. Data traffic from authenticated clients goes through, and the rules do not apply to these packets.

All the HTTP/HTTPS packets from unauthenticated clients are directed to the CPU on the switch for all the ports for which you enabled the captive portal feature. When an unauthenticated client opens a web browser and tries to connect to network, the captive portal redirects all the HTTP/HTTPS traffic from unauthenticated clients to the authenticating server on the switch. A captive portal web page is sent back to the unauthenticated client. The client can authenticate. If the client successfully authenticates, the client is given access to port.

You can enable the captive portal feature on all the physical ports on the switch. It is not supported for VLAN interfaces, loopback interfaces, or logical interfaces. The captive portal feature uses MAC-address based authentication and not port-based authentication. This means that all the clients connected to the captive portal interface must be authenticated before they can get access to the network.

Clients connecting to the captive portal interface have three states; unknown, unauthenticated, and authenticated.

- **Unknown**. In the unknown state, the captive portal does not redirect HTTP/S traffic to the switch, but instead asks the switch whether the client is authenticated or unauthenticated.
- **Unauthenticated**. The captive portal directs the HTTP/S traffic to the switch so that the client can authenticate with the switch.
- **Authenticated**. After successful authentication, the client is placed in authenticated state. In this state, all the traffic emerging from the client is forwarded through the switch.

Captive Portal Configuration Concepts

This chapter introduces the objects that make up the captive portal and describes the interaction between the captive portal and the network administrator. It explains what configurations are visible to the network administrator and enumerates the events.

All the configurations included in this section are managed using the CLI, the web interface, and SNMP, with one exception; to customize the captive portal web page, you must use the web interface.

The captive portal configuration provides the network administrator control over verification and authentication, assignment to interfaces, client sessions, and web page customization.

You can create multiple captive portal configuration instances. Each captive portal configuration contains various flags and definitions used to control client access and content to customize the user verification web page. A captive portal configuration can be applied to one or more interfaces. An interface can only be a physical port on the switch. Software release 8.0 and newer versions can contain up to 10 captive portal configurations.

Enable a Captive Portal

CLI: Enable a Captive Portal

1. Enable captive portal on the switch.

```
(Netgear Switch) (config)#captive-portal
(Netgear Switch) (Config-CP)#enable
```

2. Enable captive portal instance 1.

```
(Netgear Switch) (Config-CP)#configuration 1
(Netgear Switch) (Config-CP 1)#enable
```

3. Enable captive portal instance 1 on port 1/0/1.

```
(Netgear Switch) (Config-CP 1)#interface 1/0/1
```

Web Interface: Enable a Captive Portal

- 1. Enable captive portal on the switch.
 - a. Select Security > Control > Captive Portal > CP Global Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management	Security Acc	cess Port Authenti	ication Tra	ffic Control Co	introl ACL			
DHCP Snoop	ing 🗸 🗸	Captive Portal Glob	bal Configurat	tion				
• IP Source Gu	ard v	Admin Mode		Disa	ble 💿 Enable			
Dynamic ARP	Inspection Y	Operational Statu	S	Disableo	i			
Captive Porta	al ^	Disabled Reason		Adminis	trator Disabled			
• CP Global C	Configuration	CP IP Address		0.0.0.0				
• CP Configure	ation	Additional HTTP I	Port	0	(0	to 65535)		
• CP Binding		Additional HTTP S	Secure Port	0	(0	to 65535)		
Configuration	n	Authentication Tir	neout	300	(60	0 to 600)		
• CP Binding	Table	Supported Captiv	e Portais	10				
• CP Group C	onfiguration	Configured Captiv	e Portals	1				
CP User Cor	nfiguration	Active Captive Po	rtals	0				
• CP Trap Flag	gs	System Supported	d Users	1024				
CP Client		Local Supported	Users	128				
		Configured Local	Users	0				
		Authenticated Use	ers	0				

- 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.

System S	witching	Routing	QoS	Security	Monitoring	Maint	enance	Help	Index	
Management Secur	ity Acces	s Port Auther	tication Tra	ffic Control Co	ntrol ACL					
DHCP Snooping	~ <u>C</u>	aptive Portal Co	nfiguration							
IP Source Guard	~				1201 5					
Dynamic ARP Inspe	ection 🖌	CP ID	CP Name		Admin Mode	Protocol	Verification	Block		Group
Captive Portal	^	1 👻	Default		Disable 💌	http 💌	Guest	Disable	. 💌	
CP Global Configu	iration	☑ 1	Default		Disable	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.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Se	curity Acces	s Port Authen	ication Tra	ffic Control	ontrol ACL			
DHCP Snooping	· · · C	aptive Portal Bin	ding Configur	ation				
• IP Source Guard	· ۲ د	aptive Portal Bin	ding Configur	ation				
Dynamic ARP In	spection v	Options				CP ID 1 CP Nar	ne Default	
Captive Portal	^	- Constant						
•CP Global Con	figuration	Unit 1	55 7 1 100	and the product of				
• CP Configuration	on	Ports 1 3	5 7 9	11 13 15 1	7 19 21 23 2	25 27 29 31 33	35 37 39	41 43 45 47
CP Binding Configuration								
Configuration		2 4	6 8 10	12 14 16 1	3 20 22 24 3	26 28 30 32 34	36 38 40	42 44 46 48

- 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.

System	Switching		Routing	QoS	Security	Monitoring	Mainte	enance	Help	Index	k
Management S	Security Acce	ISS	Port Authenti	ication Tra	ffic Control Co	ntrol ACL					
DHCP Snoopi	ng ~	Capt	ive Portal Con	figuration							
IP Source Gua Dynamic ARP	ard × Inspection ×		CP ID	CP Name		Admin Mode	Protocol	Verification	Block		Group
Captive Portal CP Global Ci	^		1	Default		Enable 💌	http 💌	Guest 💌	Enable	•	-
CP Configura	ition	V		Default		Enable	http	Guest	Blocked		0

- 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.

System	Switching		Routing	QoS	Security	M	lonitoring	Maintenance	Help	Index
Management S	Security Ac	cess	Port Authen	tication Tra	ffic Control C		ACL			
DHCP Snoopin	ng ~	CP	Group Configu	ration						
•IP Source Gua	ird 🗸		Group ID (Group Name						
Dynamic ARP	Inspection ¥		2 🔻	Group2						
Captive Portal	^		1 [Default						
• CP Global Co	onfiguration									
• CP Configura	ition									
CP Binding Configuration										
•CP Binding T	able									
CP Group Co	onfiguration									

- **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.

System Switch	hing		Routing	QoS	Securit	y Monito	ing Mair	itenance	Help	li	ndex
Management Security	Acc	ess	Port Authent	ication Tra	ffic Control	Centrel ACL					
DHCP Snooping	*	CPI	Js <mark>er</mark> Configura	tion		1900					
Dynamic ARP Inspection	n y		User ID	User N	lame	Edit Password	Password	Confirm Password	G	Group	Session Timeout
CP Global Configuratio	'n		2	user1		Disable 💌	******		-	1 ~	[
CP Configuration CP Binding Configuration			1								
CP Binding Table											
CP Group Configuratio CP User Configuration	n										

- **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).

RADIUS Attribute	No.	Description	Range	Usage	Default
User-Name	1	User name to be authorized.	1–32 characters	Required	None
User-Password	2	User password.	8–64 characters	Required	None
Session-Timeout	27	Logout once session timeout is reached (seconds). If the attribute is 0 or not present, use the value configured for the captive portal.	Integer (seconds)	Optional	0
Idle-Timeout	28	Log out once idle timeout is reached (seconds). If the attribute is 0 or not present, use the value configured for the captive portal.	Integer (seconds)	Optional	0
WISPr-Max-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, 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, use the value configured for the captive portal.	Integer	Optional	0

 Table 6. RADIUS Attributes for Configuring Captive Portal Users

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.

System	Switching		Routing	QoS	Security	Monitoring	Mainte	enance	Help Inde	ĸ
Management S	Security Acces	ss	Port Authent	ication Trat	fic Control Co	ontrol ACL				
DHCP Snoopi	ng 🗸	Capt	ive Portal Cor	figuration						
IP Source Gua Dynamic ARP	ard × Inspection ×		CP ID	CP Name		Admin Mode	Protocol	Verification	Block	Group
Captive Portal	^		1 💌	Default		Enable 💌	http 💌	RADIUS 💌	Not Blocked	1 💌
CP Global Cl CP Configura	ation	V	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.

iSCSI



Internal Small Computer System Interface

This chapter includes the following sections:

- iSCSI Concepts
- Enable iSCSI Awareness with VLAN Priority Tag
- Enable iSCSI Awareness with DSCP
- Set the iSCSI Target Port
- Show iSCSI Sessions

iSCSI Concepts

The Internal Small Computer System Interface (iSCSI) feature is used in networks containing iSCSI initiators and targets where the administrator desires to protect the iSCSI traffic from interruption by giving the traffic preferential QoS treatment. The dynamically generated classifier rules are used to direct the iSCSI data traffic to queues that can be given the desired preference characteristics over other data transiting the switch. This can avoid session interruptions during times of congestion that would otherwise cause iSCSI packets to be dropped.

The administrator can select VLAN priority tag (VPT) or DSCP mapping for the QoS preferential treatment. iSCSI flows are assigned by default to the highest VPT/DSCP queue not used for chassis management or voice VLAN. The administrator should also take care of configuring the relevant Class of Service parameters for the queue chosen in order to complete the setting.

The following figure shows an example of iSCSI implementation.



Clients with iSCSI initiators connected to switch

Figure 64. Sample iSCSI implementation

Enable iSCSI Awareness with VLAN Priority Tag

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

CLI: Enable iSCSI Awareness with VLAN Priority Tag

Use the following commands to enable iSCSI awareness, select VPT, and set VLAN number and aging time.

```
(Netgear Switch) #config
(Netgear Switch) (Config) #iscsi enable
(Netgear Switch) (Config) #iscsi cos vpt 5
(Netgear Switch) (Config) #iscsi aging time 10
(Netgear Switch) (Config) #exit
```

Web Interface: Enable iSCSI Awareness with VLAN Priority Tag

- 1. Enable iSCSI awareness, select VPT, and set VLAN number and aging time.
 - a. Select Switching > iSCSI > Basic.

Syste	em	Sw	vitching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VLAN	Auto-	VolP		STP	Multicast	MVR A	ddress Table	Ports LAG N	ILAG		
Basic			^	ISCSI G	lobal Config	uration					
• Globa	l Config	uration	n i i	iscsi :	Status	C	Disable 💿 E	nable			
• Sessio	ons			QoS P	rofile	0	VLAN Priority	Tag 🔘 DSCP			
• Advanc	ed		~	VLAN	Priority Tag	5	•				
				DSCP		4	6 -				
				Remar	k	C	Disable 💿 E	nable			
				iscsi	Aging Time	1(1	(1 to 43200	minutes)		

- **b.** Enter the following information:
 - Next to iSCSI Status, select the **Enable** radio button.
 - Next to QoS Profile, select the VLAN Priority Tag radio button.
 - From the VLAN Priority Tag menu, select 5 (the default value).
 - Next to Remark, select the **Enable** radio button (the default value).
 - In the iSCSI Aging Time field, enter **10** (the default value).
- c. Click Apply to save the settings.

Enable iSCSI Awareness with DSCP

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

CLI: Enable iSCSI Awareness with DSCP

Use the following commands to enable iSCSI awareness, select DSCP, and set DSCP queue number and aging time.

```
(Netgear Switch) #config
(Netgear Switch) (Config) #iscsi enable
(Netgear Switch) (Config) #iscsi cos dscp 46
(Netgear Switch) (Config) #iscsi aging time 10
(Netgear Switch) (Config) #exit
```

Web Interface: Enable iSCSI Awareness with DSCP

- 1. Enable iSCSI awareness, select DSCP, and set the DSCP queue number and aging time.
 - a. Select Switching > iSCSI > Basic.

Systen	n Sw	itching	Routing		QoS	Security	Monitoring	Maintenance	Help	Index
VLAN	Auto-VoIP		STP	Multicast	MVR A	Address Table	Ports LAG M	LAG		
 Basic 		^	ISCSI G	lobal Config	uration					
• Global (Configuration	r	ISCSI S	Status	C) Disable 💿 E	Enable			
 Session 	ns		QoS Pr	rofile	C	VLAN Priority	/ Tag 💿 DSCP			
Advance	d	~	VLAN F	Priority Tag	E					
			DSCP		4	6				
			Remark	k	C) Disable 🇿 E	Enable			
			iSCSI /	Aging Time	1	D	(1 to 43200 n	ninutes)		

- **b.** Enter the following information:
 - Next to iSCSI Status, select the **Enable** radio button.
 - Next to QoS Profile, select the **DSCP** radio button.
 - From the DSCP menu, select **46** (the default value).
 - Next to Remark, select the **Enable** radio button (the default value).
 - In the iSCSI Aging Time field, enter **10** (the default value).
- 2. Click Apply to save the settings.

Set the iSCSI Target Port

When working with iSCSI that does not use the standard IANA assigned iSCSI ports (3260/860), NETGEAR recommends that you specify the target IP address. Then, the switch snoops frames only if the TCP destination port is one of the configured TCP ports and the destination IP address is the target IP address. This configuration improves the performance of the switch by preventing the CPU from processing non-iSCSI flows.

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

CLI: Set iSCSI Target Port

Use the following commands to set iSCSI target port to 49154 at IP address 172.16.1.20.

```
(Netgear Switch) #config
(Netgear Switch) (Config) #iscsi target port 49154 address 172.16.1.20
(Netgear Switch) (Config) #exit
```

Web Interface: Set iSCSI Target Port

- 1. Configure the iSCSI target port.
 - a. Select Switching > iSCSI > Advanced > iSCSI Targets.

System	Sw	itching		Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VLAN Auto	-VolP	iscsi	STR	P Multicast	MVR A	Address Table	Ports LAG MI	AG		2 - 75
Basic		~	ISCSI	Targets Confi	iguration					
Advanced Global Confi	iguration	Â		TCP Port		IP Address	Target Nan (0 to 223)	ne		
• iSCSI Targe	ets	-		49154		172.16.1.20				
Sessions Sessions De	etailed			860 3260		0.0.0.0 0.0.0.0				

- **b.** Enter the following information:
 - In the TCP Port field, enter 49154.
 - In the IP Address field, enter 172.16.1.20.
- c. Click Apply to save the settings.

Show iSCSI Sessions

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

CLI: Show iSCSI Sessions

Use the following commands to show iSCSI sessions and session details:

```
(Netgear Switch) #show iscsi sessions
Session 0:
_____
Target: iqn.2012-08.com.example:storage.lun1
Initiator: iqn.1991-05.com.microsoft:netgear-think
ISID: 400001370000
(Netgear Switch) #show iscsi sessions detailed
Session 0:
_____
Target: iqn.2012-08.com.example:storage.lun1
Initiator: iqn.1991-05.com.microsoft:netgear-think
Up Time: 00:00:04:11 (DD:HH:MM:SS)
Time for aging out: 382 secs
ISID: 400001370000
               Initiator Target
TCP Port IP Address
Initiator
                                               Target
IP Address
                             IP Address
                                              TCP Port
_____ ____
                                                _____

        192.168.10.107
        57965
        192.168.10.116
        3260

(Netgear Switch) #
```

The command shows that there is an active iSCSI session. The initiator is at IP address 192.168.10.107 and the Target is at IP address 192.168.10.116

Web Interface: Show iSCSI Sessions

- 1. Show iSCSI sessions.
 - a. Select Switching > iSCSI > Advanced > Sessions.

A screen similar to the following displays.

Syste	em	Sv	vitching		Routing	QoS	Securit	/	Monitorin	g	Maintenance	Help	Index
VLAN	Auto-	VolP		STP	Multicast	MVR	Address Table	Ports	LAG	MLAC	3		
	iSC	SI		iscsi s	Sessions								
•Basic			~	Targ	et Name		Ini	tiator Nam	e			ISID (Init	iator Session ID)
 Advanc Globa iSCS 	ed al Config I Target	guratio s	n	iqn.2	2012-12.loca	l.mynet:sto	rage.lun1 iq	n. 1991-05.	com.mic	rosoft:jil	tran-t430.netgear.cc	m 4000013	70000
• Sess • Sess	ions ions De	atailed											

- 2. Click Refresh.
- **3.** Show the iSCSI session details.
 - a. Select Switching > iSCSI > Advanced > Sessions detailed.

A screen similar to the following displays.

System Swite	hing	Routing	QoS S	Security	Monitoring	Maintenance	Help Ind
VLAN Auto-VolP 1	SCSI	STP Multicast M	/IVR Addres	s Table – F	Ports LAG	MLAG	
iSCSI		iSCSI Sessions Detaile	ed				
Basic	~	Session Index		0 ~			
• Advanced	^	Target Name		iqn.20	iqn.2012-12.local.mynet:storage.lun1		
Global Configuration		Initiator Name		iqn.19	iqn.1991-05.com.microsoft:jitran-t430.netgear.com		
• iSCSI Targets		Up Time		00:00:	00:00:06:35 (DD:HH:MM:SS)		
 Sessions 		Time for aging out (in Seconds)		206	206		
Sessions Detailed		ISID (Initiator Session ID)		400001370000			
		Initiator IP address	Initiator TC	P Port	Target IP Addre	ss Target TCP Port	
		192.168.10.201	52060	1	192,168,10,170	3260	

4. Click Refresh.

Override Factory Defaults

Use another factory default configuration file



This chapter includes one section:

Override the Factory Default Configuration File

Override the Factory Default Configuration File

NETGEAR managed switches support a single set of default configurations and scaling parameters, which are hard-coded in the factory default configuration file. To enable you to use a different set of default configurations and scaling parameters, you can override the factory default configuration file and specify that another file in the file system must be regarded as the factory defaults. After you issue the clear config privileged EXEC command, the switch uses the new factory defaults.

CLI: Install Another Factory Defaults Configuration File

1. Create a new factory default configuration file.

The file format must be the same as the format of the startup configuration file.

2. Disable STP and LLDP MED on all interfaces.

If the switch is not configured for STP and LLDP MED, you can skip this step.

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#no spanning-tree
(Netgear Switch) (Config)#no lldp med all
```

- 3. Save the new factory default configuration file as a text file named factory_default.txt.
- **4.** Download the factory_default.txt file to the switch.

CLI: Erase the Old Factory Default Configuration File

1. Erase the old factory default configuration file from the switch.

(Netgear Switch) #erase factory-default

2. Reload the switch.

The new factory default configuration file (that is, the factory_default.txt. file) takes effect.

NETGEAR SFP

Small form-factor pluggable

This chapter includes one section: Connect with NETGEAR SFP AGM731F



Connect with NETGEAR SFP AGM731F

Cisco provides a way to support third-party small form-factor pluggables (SFPs). For example, you can get the NETGEAR SFP AGM731F to work between a Cisco switch and a NETGEAR switch.

1. Before connecting the NETGEAR switch to the Cisco switch, configure the following command on the Cisco switch.

```
service unsupported-transceiver
no errdisable detect cause gbic-invalid
```

2. Make sure that the autonegotiation mode is the same on both sides.

The following supported AN mode can be configured on the NETGEAR switch and the Cisco switch.

XCM8944+AGM731F	CISCO+AGM731F	Result
Autonegotiate	No speed nonegotiate	Link is up
No Autonegotiate	speed nonegotiate	Link is up

Index

Numerics

10G fiber connection, switch stacks 6in4 tunnels 6to4 tunnels 802.1d (classic STP) 802.1s (MSTP) 802.1w (RSTP) 802.1x (port security)

Α

access ports 63 accounting for commands 404 ACL mirroring 251 ACL redirection 257 ACLs (access control lists) 216 active directory (AD), MAB 426 ARP (Address Resolution Protocol) dynamic inspection 381 proxy feature 205 authentication manager 407 authentication, captive portal 701 authorization privileged EXEC commands 403 user EXEC commands 402 auto VoIP 305

B

backup router, VRRP 212 banner, pre-login 443 bindings, static 395 bootstrap router (BSR) 621 border gateway protocol (BGP) 178 border routers, OSPF 140 BSR (bootstrap router) 621 buffered logs, syslog 460

С

captive portals 698 chassis switch management 468 class, DiffServ 281 classic STP 545 client access, captive portal 701 color conform policies, DiffServ 319 command accounting 404 command authorization 402 compatibility, switch stack firmware 491 compatible mode, MVR 340 configuration files, switch stacks 491 configuration scripting 440 CoS (Class of Service) queuing 272

D

DAI (Dynamic ARP inspection) 381 DCPDP (Dual Control Plane Detection Protocol) 94 default configuration file, overriding 715 default routes, port routing 108 dense mode, PIM 598 DHCP L2 relay 647 DHCP L3 relay 652 DHCP messages, maximum rate 396 DHCP reservation, configuring 514 DHCP servers configuring 511 rogue, finding 392 DHCP snooping 388 DHCPv6 routing interface 593 DHCPv6 servers 518 Differentiated services Code Point (DSCP) CoS queuing 272 DiffServ 281 iSCSI 708 DiffServ (Differentiated Services) 281 Distance Vector Multicast Routing Protocol ((DVMRP) 680 DNS (domain name system) 508 double VLANs (DVLANs) 534 DSCP (Differentiated services Code Point) CoS queuing 272 DiffServ 281 iSCSI 708

Dual Control Plane Detection Protocol (DCPDP) 94 dual images 448 DVLANs (double VLANs) 534 DVMRP (Distance Vector Multicast Routing Protocol) 680 Dynamic ARP inspection (DAI) 381 dynamic mode DHCP server 511 MVR 346 dynamic port locking 354

E

edge device, DiffServ **281** email alerting, syslog **465** EXEC command authorization **403**

F

factory defaults, overriding **715** firmware and firmware mismatch, switch stacks **480**

G

GARP (Generic Attribute Registration Protocol) groups, captive portal guest VLANs GVRP (GARP VLAN Registration Protocol)

Η

host name, DNS **509** hosts, logging **462**

IGMP (Internet Group Management Protocol) snooping and querying 328 installing, switch stacks 478 inter-area routers IPv4 133 IPv6 520 interior node, DiffServ 281 IP ACLs 217 IP source quard 397 IPv6 ACLs 263 configuring interfaces 585 DHCPv6 servers 518 DiffServ 312 inter-area routers 520 tunnels 560

iSCSI initiators and targets **708** isolated ports **54**, **361** isolated VLANs **54**, **237**

L

LAGs (link aggregation groups) 70 levels of severity, syslog 465 limits, dynamic and static MAC addresses 355 locking ports 354

Μ

MAB (MAC Authentication Bypass) 412 MAC ACLs 216 MAC addresses, static 357 MAC Authentication Bypass (MAB) 412 MAC-based VLANs 29 management ACLs 262 managing, switch stacks 489 mapping CoS queues 272 static 386 master router, VRRP 210 master switch and member switches, switch stacks 476 migrating configuration, switch stacks 481 mirroring ACLs 251 ports 444 MLAG (multichassis link aggregation group) 73 MLD (multicast listener discovery) 663 monitoring, sFLow 502 moving, stack master 496 MSTP (multiple STP) 548 multicast routers 331 multicast VLAN registration (MVR) 339 multichassis link aggregation group (MLAG) 73 MVR (multicast VLAN registration) 339

Ν

network policy server, MAB **418** NSSA areas, OSPF **155**

0

organizationally unique identifier (OUI) 306 OSPF (Open Shortest Path First) 133 OUI-based auto VoIP 306 outbound Telnet 451

Ρ

Per VLAN (Rapid) Spanning Tree Protocol (PV(R)STP) 550 PIM (Protocol Independent Multicast) 598 policy based routing (PBR) 199 policy server, MAB 418 policy, DiffServ 281 port analyzer 445 port mirroring 444 port routing 103 port security 354 preconfiguring, switch stack members 492 primary VLANs 54 priority values, switch stack members 478 private VLAN groups 538 private VLANs 54 promiscuous ports 54 protected ports 358 Protocol Independent Multicast (PIM) 598 protocol-based auto VoIP 305 protocol-based VLANs 33 PV(R)STP (Per VLAN (Rapid) Spanning Tree Protocol) 550

Q

queriers, IGMP 333 queues, CoS 273

R

RADIUS accounting server 406 assigning VLANs 375 captive portal authorization 704 redirection, ACLs 257 relays, DHCP L2 and DHCP L3 646 remote switched port analyzer (RSPAN) 445 renumbering, switch stack members 494 reverse path forwarding (RPF) 599 RIP (Routing Information Protocol) 120 rogue DHCP servers 392 route-map statement 199 routing interface, configuring for IPv6 586 routing, VLANs 113 RPF (reverse path forwarding) 599 RSPAN (remote switched port analyzer) 445 RSTP (rapid STP) 546 rules. ACLs 216

S

sampling, sFlow 505 SCCP (Skinny Call Control Protocol) 305 scheduler mode, strict priority 275 scripting, configuration 440 security, ports 354 service, DiffServ 281 Session Initiation Protocol (SIP) 305 session limit and time-out, Telnet 454 severity levels, syslog 465 sFlow monitoring 502 shaping traffic, CoS 278 Simple Network Time Protocol (SNTP) 430 SIP (Session Initiation Protocol) 305 Skinny Call Control Protocol (SCCP) 305 small form-factor pluggable (SFP) 718 SNMP (Simple Network Management Protocol) 497 snooping DHCP 388 IGMP 328 MLD 675 SNTP (Simple Network Time Protocol) 430 Spanning Tree Protocol (STP) 545 sparse mode, PIM 621 SSL certificates 706 stacking switches 475 stateful address assignment, IPv6 518 stateless DHCPv6 server 524, 528 static bindings 395 static MAC addresses 357 static mapping 386 static port locking 354 static routes, port routing 109 static routing, MLAG interfaces 83 STP (Spanning Tree Protocol) 545 strict priority schedule mode, CoS 275 stub areas, OSPF 146 subnet-based VLANs 37 switch port modes 63 switch stacks 475 system logging (syslog), logging, syslog 457

T

TACACS+ accounting server target port, iSCSI TCP flags, ACLs Telnet, outbound
time zone, SNTP server traceroute **438**, **439**, traffic shaping, CoS traplogs, syslog traps, SNMP trunk ports trust mode global, configuring interface, configuring for trusted ports, CoS tunnels, IPv6

U

Unidirectional Link Detection (UDLD) 77 untrusted ports, CoS 273 upgrading firmware, switch stacks 480 users, captive portal 702

V

Virtual Private Cloud (VPC) 74 Virtual Router Redundancy Protocol (VRRP) concepts and configuring 209 multichassis link aggregation group (MLAG) 76 virtual VLANs 37 VLAN groups, private 538 VLAN priority tag (VPT) 708 VLAN routing concepts and configuring 113 IPv6 589 OSPF 166 RIP 127 VLANs concepts and configuring 21 double VLANs 534 guest VLANs 370 voice 40 voice VLANs 40 VoIP (voice over IP) auto 305 DiffServ 298 VPC (Virtual Private Cloud) 74 VPTs (VLAN priority tag) 708 VRRP (Virtual Router Redundancy Protocol) concepts and configuring 209 multichassis link aggregation group (MLAG) 76

W

WRED (weighted random early discard) 272