ProSafe Managed Switch
Software Administration Manual

9.0.2 for
GSM5212P
GSM7212F
GSM7212P
GSM7224P
©2011 NETGEAR, Inc. All rights reserved.

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

**Technical Support**

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

Phone (US & Canada only): 1-888-NETGEAR
Phone (Other Countries): See Support information card.

**Trademarks**

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

**Statement of Conditions**

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

**Revision History**

<table>
<thead>
<tr>
<th>Publication Part Number</th>
<th>Version</th>
<th>Publish Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>202-10515-06</td>
<td>v1.0</td>
<td>October 2011</td>
<td>Add MVR feature.</td>
</tr>
<tr>
<td>202-10515-05</td>
<td>v1.0</td>
<td>July 2011</td>
<td>Add DHCPv6 and DHCPv6 mode features.</td>
</tr>
<tr>
<td>202-10515-04</td>
<td>v1.0</td>
<td>November 2010</td>
<td>New document template.</td>
</tr>
<tr>
<td>202-10515-03</td>
<td>v 1.0</td>
<td>June 2010</td>
<td>Move some content to the <em>Software Setup Guide</em>.</td>
</tr>
<tr>
<td>202-10515-02</td>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>202-10515-01</td>
<td></td>
<td></td>
<td>Original publication.</td>
</tr>
</tbody>
</table>
Table of Contents

Chapter 1  Documentation Resources

Chapter 2  VLANs
  Create Two VLANs .............................................................. 10
  Assign Ports to VLAN2 ........................................................ 12
  Assign Ports to VLAN3 ........................................................ 13
  Assign VLAN3 as the Default VLAN for Port 1/0/2 ...................... 15
  Create a MAC-Based VLAN ................................................. 16
  Create a Protocol-Based VLAN ............................................ 19
  Virtual VLANs: Create an IP Subnet–Based VLAN .................... 21
  Voice VLANs ..................................................................... 24

Chapter 3  LAGs
  Create Two LAGs ................................................................. 35
  Add Ports to LAGs ............................................................... 36
  Enable Both LAGs ............................................................... 38

Chapter 4  Port Routing
  Port Routing Configuration ................................................... 40
  Enable Routing for the Switch .............................................. 41
  Enable Routing for Ports on the Switch ................................... 41
  Add a Default Route .......................................................... 44
  Add a Static Route .............................................................. 45

Chapter 5  VLAN Routing
  Create Two VLANs .............................................................. 47
  Set Up VLAN Routing for the VLANs and the Switch ................. 52

Chapter 6  RIP
  Routing for the Switch ......................................................... 55
  Routing for Ports ................................................................. 56
  RIP for the Switch ............................................................... 57
  RIP for Ports 1/0/2 and 1/0/3 ................................................ 58
  VLAN Routing with RIP ...................................................... 60

Chapter 7  OSPF
  Inter-area Router ............................................................... 65
OSPF on a Border Router .............................................. 70
Stub Areas ..................................................................... 75
nssa Areas ................................................................... 84
VLAN Routing OSPF ...................................................... 93
OSPFv3 ....................................................................... 98

Chapter 8  ARP
Proxy ARP Examples ..................................................... 103

Chapter 9  VRRP
VRRP on a Master Router ............................................ 106
VRRP on a Backup Router ............................................ 108

Chapter 10  ACLs
Set Up an IP ACL with Two Rules ............................... 113
One-Way Access Using a TCP Flag in an ACL .......... 117
Use ACLs to Configure Isolated VLANs on a Layer 3 Switch .... 132
Set up a MAC ACL with Two Rules ....................... 144
ACL Mirroring ............................................................. 147
ACL Redirect ............................................................. 152
Configure IPv6 ACLs ................................................. 157

Chapter 11  CoS Queuing
CoS Queue Mapping .................................................. 165
CoS Queue Configuration .......................................... 166
Show classofservice Trust ......................................... 166
Set classofservice Trust Mode ................................. 167
Show classofservice IP-Precedence Mapping ............ 168
Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode .............................. 169
Set CoS Trust Mode for an Interface ....................... 170
Configure Traffic Shaping ............................................ 171

Chapter 12  DiffServ
DiffServ ................................................................. 174
DiffServ for VoIP ......................................................... 190
Auto VoIP ................................................................. 197
DiffServ for IPv6 ........................................................ 201
Color Conform Policy ............................................... 208

Chapter 13  IGMP Snooping and Querier
IGMP Snooping .......................................................... 216
Show igmpsnooping .................................................. 217
Show mac-address-table igmpsnooping ................. 218
External Multicast Router ......................................... 219
Multicast Router Using VLAN ............................... 220
Chapter 14  MVR (Multicast VLAN Registration)
  Configure MVR in Compatible Mode ........................................... 227
  Configure MVR in Dynamic Mode ............................................. 234

Chapter 15  Security Management
  Port Security ................................................................. 240
  Set the Dynamic and Static Limit on Port 1/0/1 ......................... 241
  Convert the Dynamic Address Learned from 1/0/1 to a Static Address .. 243
  Create a Static Address .................................................... 244
  Protected Ports ............................................................. 244
  802.1x Port Security .......................................................... 251
  Create a Guest VLAN ....................................................... 257
  Assign VLANs Using RADIUS .............................................. 262
  Dynamic ARP Inspection .................................................... 268
  Static Mapping ............................................................... 274
  DHCP Snooping ............................................................... 276
  Enter Static Binding into the Binding Database ......................... 279
  Maximum Rate of DHCP Messages ....................................... 280
  IP Source Guard ............................................................. 282

Chapter 16  SNTP
  Show SNTP (CLI Only). .................................................... 287
  Configure SNTP ............................................................. 289
  Set the Time Zone (CLI Only). ............................................ 291
  Set the Named SNTP Server ................................................. 291

Chapter 17  Tools
  Traceroute ................................................................. 294
  Configuration Scripting ..................................................... 296
  Pre-Login Banner .......................................................... 299
  Port Mirroring ............................................................... 300
  Dual Image ................................................................. 301
  Outbound Telnet ............................................................ 304

Chapter 18  Syslog
  Show Logging ............................................................... 309
  Show Logging Buffered .................................................... 311
  Show Logging Traplogs ..................................................... 312
  Show Logging Hosts ....................................................... 313
  Configure Logging for a Port ............................................. 314
Chapter 19  Switch Stacks

Switch Stack Management and Connectivity .......................... 318
The Stack Master and Stack Members ............................... 319
Install and Power-up a Stack ........................................ 321
Switch Firmware ...................................................... 322
Configure a Stacking Port as an Ethernet Port ..................... 324
Stack Switches Using 10G Fiber .................................... 327
Add, Remove, or Replace a Stack Member ......................... 330
Switch Stack Configuration Files .................................... 332
Preconfigure a Switch ................................................ 333
Renumber Stack Members .............................................. 334
Move the Stack Master to a Different Unit ....................... 336

Chapter 20  SNMP

Add a New Community ................................................ 337
Enable SNMP Trap .................................................... 338
SNMP V3 .............................................................. 339
sFlow ................................................................. 341
Time-Based Sampling of Counters with sFlow ..................... 345

Chapter 21  DNS

Specify Two DNS Servers ............................................. 346
Manually Add a Host Name and an IP Address .................... 347

Chapter 22  DHCP Server

Configure a DHCP Server in Dynamic Mode ....................... 349
Configure a DHCP Reservation ..................................... 352

Chapter 23  DHCPv6 Server

CLI: Configure DHCPv6 .............................................. 357
Web Interface: Configure an Inter-area Router ................. 358
Configure Stateless DHCPv6 Server ............................... 362

Chapter 24  Double VLANs and Private VLAN Groups

Double VLANs ...................................................... 366
Private VLAN Groups ............................................... 370

Chapter 25  Spanning Tree Protocol

Configure Classic STP (802.1d) ................................... 376
Configure Rapid STP (802.1w) ...................................... 378
Configure Multiple STP (802.1s) .................................. 379
Chapter 26  Tunnel

CLI: Create a Tunnel ................................. 383
Web Interface: Create a Tunnel ..................... 385

Chapter 27  IPv6 Interface Configuration

Create an IPv6 Routing Interface .................. 390
Create an IPv6 Network Interface ................. 393
Create an IPv6 Routing VLAN .................... 395
Configure DHCPv6 Mode on the Routing Interface . 400

Chapter 28  PIM

PIM-DM .................................................. 403
PIM-SM .................................................. 427

Chapter 29  DHCP L2 Relay and L3 Relay

DHCP L2 Relay ....................................... 454
DHCP L3 Relay ....................................... 460

Chapter 30  MLD

Configure MLD ........................................ 471
MLD Snooping ........................................ 484

Chapter 31  DVMRP

CLI: Configure DVMRP ............................... 490
Web Interface: Configure DVMRP .................. 496

Chapter 32  Captive Portal

Captive Portal Configuration ........................ 508
Enable Captive Portal ................................ 508
Client Access, Authentication, and Control ...... 510
Block a Captive Portal Instance .................... 511
Local Authorization, Create Users and Groups .... 511
Remote Authorization (RADIUS) User Configuration .... 513
SSL Certificates ..................................... 515

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

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

- **Create Two VLANs** on page 10
- **Assign Ports to VLAN2** on page 12
- **Assign Ports to VLAN3** on page 13
- **Assign VLAN3 as the Default VLAN for Port 1/0/2** on page 15
- **Create a MAC-Based VLAN** on page 16
- **Create a Protocol-Based VLAN** on page 19
- **Virtual VLANs: Create an IP Subnet–Based VLAN** on page 21
- **Voice VLANs** on page 24

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.

![Diagram of a switch with VLAN configurations]

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

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

**Create Two VLANs**

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

**CLI: Create Two VLANS**

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

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

**Web Interface: Create Two VLANS**

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

![VLAN Configuration Screen](image)

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.

![VLAN Configuration Screen](image)

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

c. Click **Add**.
Assign Ports to VLAN2

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

CLI: Assign Ports to VLAN2

```bash
(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 vланonly
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan pvid 2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#exit
(Netgear Switch) (Config)#vlan port tagging all 2
(Netgear Switch) (Config)#
```

Web Interface: Assign Ports to VLAN2

1. Assign ports to VLAN2.
   a. Select Switching > VLAN > Advanced > VLAN Membership. A screen similar to the following displays.
   
   ![VLAN Membership Screen](image)

   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.
ProSafe Managed Switch

Chapter 2. VLANs

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

![Port VLAN Id Configuration](image)

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.

**Assign Ports to VLAN3**

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

**CLI: Assign Ports to VLAN3**

```
(Netgear Switch) (Config)#interface range 1/0/2-1/0/4
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#vlan participation include 3
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#exit
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#vlan acceptframe all
(Netgear Switch) (Interface 1/0/4)#exit
(Netgear Switch) (Config)#exit
```
Web Interface: Assign Ports to VLAN3

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

   ![VLAN Membership Screen](image)

   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.

   ![Port PVID Configuration Screen](image)

   b. Scroll down and select the Interface 1/0/4 check box. Now 1/0/4 appears in the Interface field at the top.
   c. In the **Acceptable Frame Types** list, select **Admit All**.
   d. Click **Apply** to save the settings.
Assign VLAN3 as the Default VLAN for Port 1/0/2

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

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

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

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

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

   ![Port VLAN 1d Configuration](image)

   b. Under PVID Configuration, scroll down and select the Interface 1/0/2 check box. Now 1/0/2 appears in the Interface field at the top.

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

   d. Click Apply to save the settings.
Create a MAC-Based VLAN

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

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

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

CLI: Create a MAC-Based VLAN

1. Create VLAN3.

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

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

```
(Netgear Switch)#config
(Netgear Switch)(Config)#interface 1/0/23
(Netgear Switch)(Interface 1/0/23)#vlan participation include 3
(Netgear Switch)(Interface 1/0/23)#vlan pvid 3
(Netgear Switch)(Interface 1/0/23)#exit
```
3. Map MAC 00:00:0A:00:00:02 to VLAN3.

   ```
   (Netgear Switch)(Config)#exit
   (Netgear Switch)#vlan data
   (Netgear Switch)(Vlan)#vlan association mac 00:00:0A: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.

   ![VLAN Configuration](image)

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

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

![VLAN Membership Screen]

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.

![Port VLAN Id Configuration Screen]

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

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

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

4. **Map the specific MAC to VLAN3.**

a. Select **Switching > VLAN > Advanced > MAC based VLAN**. A screen similar to the following displays.

![MAC Based VLAN Configuration Screen]
b. Enter the following information:
   • In the MAC Address field, enter 00:00:0A:00:00:02.
   • In the PVID (1 to 4093) field, enter 3.

c. Click Add.

Create a Protocol-Based VLAN

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

CLI: Create a Protocol-Based VLAN

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

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

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

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

3. Assign VLAN protocol group 1 to VLAN 4.

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

4. Assign VLAN protocol group 2 to VLAN 5.

   (Netgear Switch)(Vlan)#protocol group 2 5
5. Enable protocol VLAN group 1 and 2 on the interface.

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

Web Interface: Create a Protocol-Based VLAN

1. Create the protocol-based VLAN group vlan_ipx.
   a. Select Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration. A screen similar to the following displays.

   ![Protocol Based VLAN Group Configuration](image)

   Enter the following information:
   - In the Group Name field, enter `vlan_ipx`.
   - In the Protocol list, select IPX.
   - In the VLAN ID field, enter 4.
   b. Click Add.

2. Create the protocol-based VLAN group vlan_ip.
   a. Select Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration. A screen similar to the following displays.

   ![Protocol Based VLAN Group Configuration](image)

   b. Enter the following information:
      - In the Group Name field, enter `vlan_ip`.
      - In the Protocol list, select IP and ARP while holding down the Ctrl key.
In the VLAN field, enter 5.

c. Click Add.

3. Add port 11 to the group vlan_ipx.

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

b. In the Group ID list, select 1.

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

d. Click the Apply button.

4. Add port 11 to the group vlan_ip.

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

b. In the Group ID list, select 2.

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

d. Click Apply.

Virtual VLANs: Create an IP Subnet–Based VLAN

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

![Diagram](image)

**Figure 2. IP subnet–based VLAN**

**CLI: Create an IP Subnet–Based VLAN**

```plaintext
(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.

```plaintext
(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.

```plaintext
(Netgear Switch) #show mac-addr-table vlan 2000
MAC Address       Interface     Status
-----------------  ---------  ------------
00:00:24:58:F5:56  1/0/1      Learned
00:00:24:59:00:62  1/0/24     Learned
```
Web Interface: Create an IP Subnet–Based VLAN

   a. Select Switching > VLAN > Basic > VLAN Configuration. A screen similar to the following displays.
      b. Enter the following information:
         • In the VLAN ID field, enter 2000.
         • In the VLAN Type list, select Static.
      c. Click Add.

2. Assign all the ports to VLAN 2000.
   a. Select Switching > VLAN > Advanced > VLAN Membership. A screen similar to the following displays.
      b. In the VLAN ID list, select 2000.
      c. Click Unit 1. The ports display.
      d. Click the gray box before Unit 1 until U displays.
      e. Click Apply.

3. Associate the IP subnet with VLAN 2000.
a. Select **Switching > VLAN > Advanced > IP Subnet Based VLAN.** A screen similar to the following displays.

![IP Subnet Based VLAN Configuration](image)

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.

![Diagram of network setup](image)

**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**


```
(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

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

   ![VLAN Configuration Screen](image.png)

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

   ![VLAN Configuration Screen](image.png)

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

   ![VLAN Membership Screen](image.png)

   b. In the VLAN Membership table, in the **VLAN ID** list, select 10.
c. Select Port 1 and Port 2 as tagged. A screen similar to the following displays.

![Screen display of VLAN Membership](image)

\[\text{Screen display of VLAN Membership}\]

d. Click Apply.

3. Configure Voice VLAN globally.

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

![Screen display of Voice VLAN Configuration](image)

\[\text{Screen display of Voice VLAN Configuration}\]

b. For Admin Mode, select the Enable radio button.
c. Click **Apply**. A screen similar to the following displays.

![Voice VLAN Configuration](image)

   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.

![Voice VLAN Configuration](image)

e. Click **Apply**.

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

![DiffServ Class Configuration](image)

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

![Class Configuration](image)

**ProSafe Managed Switch**

**Chapter 2. VLANs**

6. Configure matching criteria for the class as **VLAN 10**.
   a. Select **QoS > DiffServ > Advanced > Class Configuration**. A screen similar to the following displays.

![Class Configuration](image)

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

![Class Configuration](image)

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

![DiffServ Configuration](image)

7. Create the DiffServ policy **PolicyVoiceVLAN**.
   a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.

![Policy Configuration](image)

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

![Policy Configuration](image)

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

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

![Policy Configuration Screen](image1.png)

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

![Policy Class Configuration Screen](image2.png)

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

![Policy Class Configuration Screen](image3.png)

d. Click Apply.

9. Assign it to interfaces 1/0/1 and 1/0/2.
a. Select QoS > DiffServ > Advanced > Service Interface Configuration. A screen similar to the following displays.

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

c. Set the Policy Name field as PolicyVoiceVLAN. A screen similar to the following displays.

d. Click Apply. A screen similar to the following displays.
LAGs

Link Aggregation Groups

This chapter provides the following examples:

- Create Two LAGs on page 35
- Add Ports to LAGs on page 36
- Enable Both LAGs on page 38

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

Figure 4. Example network with two LAGs

LAGs offers the following benefits:

- Increased reliability and availability. If one of the physical links in the LAG goes down, traffic is dynamically and transparently reassigned to one of the other physical links.
ProSafe Managed Switch

- Better use of physical resources. Traffic can be load-balanced across the physical links.
- Increased bandwidth. The aggregated physical links deliver higher bandwidth than each individual link.
- Incremental increase in bandwidth. A physical upgrade could produce a tenfold increase in bandwidth; LAG produces a two- or fivelfold increase, useful if only a small increase is needed.

Create Two LAGs

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

CLI: Create Two LAGs

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

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

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

<p>| Port-Link | Log. | Channel | Adm. | Trap | STP | Mbr | Port Type Ports Speed Active |
|-----------|------|---------|------|------|-----|-----|--------|-------------------|</p>
<table>
<thead>
<tr>
<th>Intf</th>
<th>Name</th>
<th>Link</th>
<th>Mode</th>
<th>Mode</th>
<th>Mode</th>
<th>Type</th>
<th>Ports</th>
<th>Speed</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>lag_10</td>
<td>Down</td>
<td>En.</td>
<td>En.</td>
<td>Dis.</td>
<td>Dynamic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/2</td>
<td>lag_20</td>
<td>Down</td>
<td>En.</td>
<td>En.</td>
<td>Dis.</td>
<td>Dynamic</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Web Interface: Create Two LAGs

1. Create LAG lag_10.
   a. Select **Switching > LAG > LAG Configuration**. A screen similar to the following displays.
b. In the **Lag Name** field, enter *lag_10*.

c. Click **Add**.

2. **Create LAG lag_20**.

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

   ![LAG Configuration Screen]

   b. In the **Lag Name** field, enter *lag_20*.

   c. Click **Add**.

**Add Ports to LAGs**

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

**CLI: Add Ports to the LAGs**

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 0/2
(Netgear Switch) (Interface 0/2)#addport 1/1
(Netgear Switch) (Interface 0/2)#exit
(Netgear Switch) (Config)#interface 0/3
(Netgear Switch) (Interface 0/3)#addport 1/1
(Netgear Switch) (Interface 0/3)#exit
(Netgear Switch) (Config)#interface 0/8
(Netgear Switch) (Interface 0/8)#addport 1/2
(Netgear Switch) (Interface 0/8)#exit
(Netgear Switch) (Config)#interface 0/9
(Netgear Switch) (Interface 0/9)#addport 1/2
(Netgear Switch) (Interface 0/9)#exit
(Netgear Switch) (Config)#exit
```
Web Interface: Add Ports to LAGs

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

   ![LAG Membership Screen](image)

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

2. Add ports to lag_20.
   a. Select **Switching > LAG > LAG Membership**. A screen similar to the following displays.

   ![LAG Membership Screen](image)

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

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

**CLI: Enable Both LAGs**

By default, the system enables link trap notification.

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

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

**Web Interface: Enable Both LAGs**

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

   ![LAG Configuration Screen](image)

2. Select the top check box and the check boxes for lag_10 and lag_20 are selected.
3. In the **Admin Mode** field, select **Enable**.
4. Click **Apply** to save the settings.
This chapter provides the following sections:

- *Port Routing Configuration* on page 40
- *Enable Routing for the Switch* on page 41
- *Enable Routing for Ports on the Switch* on page 41
- *Add a Default Route* on page 44
- *Add a Static Route* on page 45

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

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

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

The router’s IP address is often statically configured in the end station, although the 7000 Series Managed Switch supports protocols such as DHCP that allow the address to be assigned dynamically. Likewise, you can assign some of the entries in the routing tables used by the router statically, but protocols such as RIP and OSPF allow the tables to be created and updated dynamically as the network configuration changes.
Port Routing Configuration

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

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

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

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

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

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

![Layer 3 switch configured for port routing](image)

Figure 5. Layer 3 switch configured for port routing
Enable Routing for the Switch

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

CLI: Enable Routing for the Switch

The following script shows the commands you would use to configure a 7000 Series Managed Switch to provide the port routing support shown in *Figure 5, Layer 3 switch configured for port routing* on page 40.

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

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

Web Interface: Enable Routing for the Switch

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

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

Enable Routing for Ports on the Switch

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

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

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

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

Web Interface: Enable Routing for Ports on the Switch

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

   ![IP Interface Configuration Screen](image)

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

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

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

   ![Configuration Interface Table]

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

3. Assign IP address 192.150.5.1/24 to interface 1/0/5.
   a. Select Routing > IP > Advanced > IP Interface Configuration. A screen similar to the following displays.

   ![Configuration Interface Table]

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

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

### Add a Default Route

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

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

### CLI: Add a Default Route

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

Note that IP subnet 10.10.10.0 should be configured using either port routing (*Enable Routing for Ports on the Switch* on page 41) or VLAN routing (see *Set Up VLAN Routing for the VLANs and the Switch* on page 52).

### Web Interface: Add a Default Route

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

2. In the **Route Type** list, select **DefaultRoute**.

3. In the **Next Hop IP Address** field, enter one of the routing interface’s IP addresses.
   - The **Network Address** and **Subnet Mask** fields will not accept input as they are not needed.
The Preference field is optional. A value of 1 (highest) will be assigned by default if not specified.

4. Click the Add button on the bottom of the screen. This creates the default route entry in the routing table.

Add a Static Route

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

CLI: Add a Static Route

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

```
(FSM7328S) #show ip route

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

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

To delete the static route, simply add “no” keyword in the front of the “ip route” command.
Web Interface: Add a Static Route

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

2. In the **Route Type** list, select **Static**.

3. Fill in the **Network Address** field. Note that this field should have a network IP address, not a host IP address. Do not enter something like 10.100.100.1. The last number should always be 0 (zero).

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

5. The **Preference** field is optional. A value of 1 is entered by default if you do not enter a number.

6. Click the **Add** button on the bottom of the screen. The screen is updated with the static route shown in the routing table.

7. To remove a route entry, either static or default, select the check box to the left of the entry, and click the **Delete** button on the bottom of the screen.
This chapter provides the following examples:

- *Create Two VLANs* on page 47
- *Set Up VLAN Routing for the VLANs and the Switch* on page 52

You can configure the 7000 Series Managed Switch with some ports supporting VLANs and some supporting routing. You can also configure it to allow traffic on a VLAN to be treated as if the VLAN were a router port.

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

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

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

### Create Two VLANs

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

The diagram in this section shows a Layer 3 switch configured for port routing. It connects two VLANs, with two ports participating in one VLAN, and one port in the other. The script
shows the commands you would use to configure a 7000 Series Managed Switch to provide the VLAN routing support shown in the diagram.

Figure 6. 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.

   ![VLAN Configuration Screen](image)

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

   ![VLAN Configuration Screen](image)

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

2. Add ports to the VLAN10 and VLAN20.
a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays.

![VLAN Membership Screen](image)

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.

![VLAN Membership Screen](image)

g. In the **VLAN ID** list, select 20.

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

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

j. Click **Apply**.

3. Assign PVID to VLAN10 and VLAN20.
a. Select **Switching > VLAN > Advanced > Port PVID Configuration**. A screen similar to the following displays.

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

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

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

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

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

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

h. Click **Apply** to save the settings.
Set Up VLAN Routing for the VLANs and the Switch

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

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

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

   ```plaintext
   (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.

   ```plaintext
   (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.

   ```plaintext
   (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.

<table>
<thead>
<tr>
<th>VLAN ID (1 to 4093)</th>
<th>Port</th>
<th>MAC Address</th>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td></td>
<td></td>
<td>192.150.3.1</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

2. Enter the following information:
   - In the **VLAN ID (1 to 4093)** list, select 10.
   - In the **IP Address** field, enter 192.150.3.1.
   - In the **Subnet Mask** field, enter 255.255.255.0.

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

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

<table>
<thead>
<tr>
<th>VLAN ID (1 to 4093)</th>
<th>Port</th>
<th>MAC Address</th>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>4/3/1</td>
<td>00:14:6c:6a:7e:25</td>
<td>192.150.4.1</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

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.
Chapter 6. RIP

Routing Information Protocol

This chapter provides the following examples:

- Routing for the Switch on page 55
- Routing for Ports on page 56
- RIP for the Switch on page 57
- RIP for Ports 1/0/2 and 1/0/3 on page 58
- VLAN Routing with RIP on page 60

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.
Routing for the Switch

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

**CLI: Enable Routing for the Switch**

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

**Web Interface: Enable Routing for the Switch**

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

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

3. Click **Apply** to save the settings.
Routing for Ports

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

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

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

### Web Interface: Enable Routing for the Ports

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

   ![Configuration Screen](image)

   - 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.

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

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

   d. Click Apply to save the settings.
2. Assign IP address 192.150.3.1/24 to interface 1/0/3.

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

   b. Scroll down and select the interface 1/0/3 check box. Now 1/0/3 appears in the Interface field at the top.

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

   d. Click Apply to save the settings.

**RIP for the Switch**

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

**CLI: Enable RIP on the Switch**

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

```
(Netgear Switch) #config
(Netgear Switch) (Config)#router rip
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#exit
(Netgear Switch) (Config)#exit
```
Web Interface: Enable RIP on the Switch

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

![RIP Configuration Screen]

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

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

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

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

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

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip rip
(Netgear Switch) (Interface 1/0/2)#ip rip receive version both
(Netgear Switch) (Interface 1/0/2)#ip rip send version rip2
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip rip
(Netgear Switch) (Interface 1/0/3)#ip rip receive version both
(Netgear Switch) (Interface 1/0/3)#ip rip send version rip2
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#exit
```
Web Interface: Enable RIP for Ports 1/0/2 and 1/0/3

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

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

3. Click Apply to save the settings.

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

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

## VLAN Routing with RIP

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

![Figure 8. VLAN routing RIP configuration example](image)

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 a 7000 Series Managed Switch.

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

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

3. Configure the IP address and subnet mask for a non-virtual router port.

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

4. Enable RIP for the VLAN router ports. Authentication defaults to none, and no default route entry is created.

```
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip rip
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip rip
(Netgear Switch) (Interface vlan 20)#exit
(Netgear Switch) (Config)#exit
```
Web Interface: Configure VLAN Routing with RIP Support

1. Configure a VLAN and include ports 1/0/2 in the VLAN:
   a. Select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.
   
   ![VLAN Routing Wizard](image)

   b. Enter the following information:
      - In the Vlan ID field, enter 10.
      - In the IP Address field, enter 192.150.3.1.
      - In the Network Mask field, enter 255.255.255.0.
   c. Click Unit 1. The ports display.
   d. Click the gray box under port 2 until T displays. The T specifies that the egress packet is tagged for the port.
   e. Click Apply to save the VLAN that includes ports 2.

2. Configure a VLAN, and include port 1/0/3 in the VLAN:
   a. Select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.
   
   ![VLAN Routing Wizard](image)

   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.

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

   - Enter the following information:
     - In the **Interface** list, select 0/2/1.
     - For RIP Admin Mode, select the **Enable** radio button.
   - Click **Apply** to save the settings.
Chapter 7. OSPF

Open Shortest Path First

This chapter provides the following examples:

- **Inter-area Router** on page 65
- **OSPF on a Border Router** on page 70
- **Stub Areas** on page 75
- **nssa Areas** on page 84
- **VLAN Routing OSPF** on page 93
- **OSPFv3** on page 98

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

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

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

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

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

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

The following figure shows a network segment with an inter-area router connecting areas 0.0.0.2 and 0.0.0.3. The sample script shows the commands used to configure a 7000 Series Managed Switch as the inter-area router in the diagram by enabling OSPF on port 1/0/2 in area 0.0.0.2 and port 1/0/3 in area 0.0.0.3.

Figure 9. Network segment with an inter-area router connecting areas 0.0.0.2 and 0.0.0.3

CLI: Configure an Inter-area Router

1. Enable routing for the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```
### 2. Assign IP addresses to ports.

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

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

```bash
(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.

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

(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip ospf
(Netgear Switch) (Interface 1/0/3)#ip ospf areaid 0.0.0.3
(Netgear Switch) (Interface 1/0/3)#ip ospf priority 255
(Netgear Switch) (Interface 1/0/3)#ip ospf cost 64
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#exit
```
Web Interface: Configure an Inter-area Router

1. Enable IP routing on the switch.
   a. Select Routing > IP > Basic > IP Configuration. A screen similar to the following displays.
   
   ![IP Configuration screenshot]
   
   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.
   
   ![IP Interface Configuration screenshot]
   
   b. Scroll down and select the interface 1/0/2 check box. Now 1/0/2 appears in the Interface field at the top.
   c. Enter the following information:
      • In the IP Address field, enter 192.150.2.1.
      • In the Subnet Mask field, enter 255.255.255.0.
      • In the Administrative Mode field, select Enable.
   d. Click Apply to save the settings.

3. Assign IP address 192.150.3.1 to port 1/0/3:
a. Select Routing > IP > Advanced > IP Interface Configuration. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>VLAN ID</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Routing Mode</th>
<th>Administrative Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/3</td>
<td></td>
<td></td>
<td>192.150.3.1</td>
<td>255.255.255.0</td>
<td>Enable</td>
<td>Enable</td>
</tr>
<tr>
<td>1/0/1</td>
<td></td>
<td></td>
<td>192.150.2.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Enable</td>
</tr>
<tr>
<td>1/0/2</td>
<td></td>
<td></td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>Enable</td>
</tr>
<tr>
<td>1/0/3</td>
<td></td>
<td></td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>Enable</td>
</tr>
<tr>
<td>1/0/4</td>
<td></td>
<td></td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>Enable</td>
</tr>
</tbody>
</table>

b. Scroll down and select the interface 1/0/3 check box. Now 1/0/3 appears in the Interface field at the top.

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

d. Click Apply to save the settings.

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

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

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

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

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

   ![Interface Configuration Screen](image)

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

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

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

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

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

   ![Interface Configuration Screen](image)

   b. Scroll down and select the interface **1/0/3** check box. Now 1/0/3 appears in the Interface field at the top.

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

In the **Metric Cost** field, enter **64**.

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

## OSPF on a Border Router

The example is shown as CLI commands and as a Web interface procedure. For an OSPF sample network, see *Figure 9* on page 65.

### CLI: Configure OSPF on a Border Router

1. Enable routing for the switch.

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

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

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

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

   ```
   (Netgear Switch) (Config)#router ospf
   (Netgear Switch) (Config router)#enable
   (Netgear Switch) (Config router)#router-id 192.130.1.1
   (Netgear Switch) (Config router)#no 1583compatibility
   (Netgear Switch) (Config router)#exit
   (Netgear Switch) (Config)#exit
   ```
4. Enable OSPF for the ports, and set the OSPF priority and cost for the ports.

```plaintext
(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.

   ![IP Configuration Screen](image)

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

2. Assign IP address 192.150.2.2 to port 1/0/2.
a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

![IP Interface Configuration Screen](image)

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

c. Enter the following information:
   - In the **IP Address** field, enter **192.150.2.2**.
   - In the **Network Mask** field, enter **255.255.255.0**.
   - In the **Admin Mode** field, select **Enable**.

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

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

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

   ![IP Interface Configuration Screen](image)

   b. Scroll down and select the interface `1/0/3` check box. Now `1/0/3` appears in the Interface field at the top.

   c. Enter the following information:
      - In the **IP Address** field, enter **192.130.3.1**.
      - In the **Network Mask** field, enter **255.255.255.0**.
      - In the **Admin Mode** field, select **Enable**.

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

4. Assign IP address 192.64.4.1 to port 1/0/4.
a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

![IP Interface Configuration](image)

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

c. Enter the following information:
   - In the **IP Address** field, enter **192.64.4.1**.
   - In the **Network Mask** field, enter **255.255.255.0**.
   - In the **Admin Mode** field, select **Enable**.

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

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

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

![OSPF Configuration](image)

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

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

7. Enable OSPF on port 1/0/3.
   a. Select **Routing > OSPF > Advanced > Interface Configuration**. A screen similar to the following displays.
   ![Interface Configuration Screen](image.png)
   
   b. Under Interface Configuration, scroll down and select the interface 1/0/3 check box. Now 1/0/3 appears in the Interface field at the top.
   - In the **OSPF Area ID** field, enter 0.0.0.3.
   - In the **OSPF Admin Mode** field, select **Enable**.
• In the **Priority** field, enter 255.
• In the **Metric Cost** field, enter 64.

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

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

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>OSPF Area ID</th>
<th>OSPF Admin Mode</th>
<th>Router Priority (0 to 255)</th>
<th>Retransmit Interval (0 to 3600)</th>
<th>Hello Interval (1 to 65535)</th>
<th>Dead Interval (1 to 2147483647)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/4</td>
<td>0.0.0.2</td>
<td>Enable</td>
<td>255</td>
<td>5</td>
<td>30</td>
<td>48</td>
</tr>
<tr>
<td>1/0/1</td>
<td>0.0.0.1</td>
<td>Disable</td>
<td>1</td>
<td>10</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>1/0/2</td>
<td>0.0.0.2</td>
<td>Enable</td>
<td>255</td>
<td>5</td>
<td>10</td>
<td>40</td>
</tr>
<tr>
<td>1/0/3</td>
<td>0.0.0.3</td>
<td>Enable</td>
<td>255</td>
<td>5</td>
<td>10</td>
<td>40</td>
</tr>
<tr>
<td>1/0/4</td>
<td>0.0.0.4</td>
<td>Enable</td>
<td>255</td>
<td>5</td>
<td>10</td>
<td>40</td>
</tr>
</tbody>
</table>

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 10. Area 1 is a stub area](image)
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 IDd 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
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.

   ![Screen capture of IP Configuration](image)

   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.

   ![Screen capture of IP Interface Configuration](image)
b. Scroll down and select the interface 2/0/11 check box. Now 2/0/11 appears in the Interface field at the top.

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

d. Click Apply to save the settings.

3. Assign IP address 192.168.20.1 to port 2/0/19:
   a. Select Routing > IP > Advanced > IP Interface Configuration. A screen similar to the following displays.

   ![Screen Capture]

   b. Scroll down and select the interface 2/0/19 check box. Now 2/0/19 appears in the Interface field at the top.

   c. Enter the following information:
      • In the IP Address field, enter 192.168.20.1.
      • In the Network Mask field, enter 255.255.255.0.
      • In the 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.

   ![Screen Capture]

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

   c. Click Apply to save the settings.

5. Enable OSPF on the port 2/0/11.
a. Select Routing > OSPF > Advanced > Interface Configuration. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>Interface</th>
<th>OSPF Area ID</th>
<th>Admin Mode</th>
<th>Priority (0 to 255)</th>
<th>Hello Interval (1 to 65535)</th>
<th>Dead Interval (1 to 65536)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/0/11</td>
<td>0.0.0.0</td>
<td>Enable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/2</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/3</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/4</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/5</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/6</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/7</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/8</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/9</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/10</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
</tbody>
</table>

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

c. Click Apply to save the settings.

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

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>OSPF Area ID</th>
<th>Admin Mode</th>
<th>Priority (0 to 255)</th>
<th>Hello Interval (1 to 65535)</th>
<th>Dead Interval (1 to 65536)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/0/19</td>
<td>0.0.0.1</td>
<td>Enable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/2</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/3</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/4</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/5</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/6</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/7</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/8</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/9</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
<tr>
<td>2/0/10</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>19</td>
<td>40</td>
</tr>
</tbody>
</table>

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

c. Click Apply to save the settings.

7. Configure area 0.0.0.1 as a stub area.
a. Select **Routing > OSPF > Advanced > Stub Area Configuration**. A screen similar to the following displays.

![Stub Area Configuration](image)

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
```

<table>
<thead>
<tr>
<th>Network Address</th>
<th>Subnet Mask</th>
<th>Protocol</th>
<th>Intf</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>OSPF Inter</td>
<td>1/0/15</td>
<td>192.168.20.1</td>
</tr>
<tr>
<td>192.168.20.0</td>
<td>255.255.255.0</td>
<td>Local</td>
<td>1/0/15</td>
<td>192.168.20.2</td>
</tr>
</tbody>
</table>

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.

   ![IP Configuration](image)

   - For Routing Mode, select the Enable radio button.
   - 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.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>VLAN ID</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Routing Mode</th>
<th>Admin Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/15</td>
<td></td>
<td></td>
<td>192.168.20.2</td>
<td>255.255.255.0</td>
<td>Enable</td>
<td>Enable</td>
</tr>
<tr>
<td>1/0/1</td>
<td></td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>Enable</td>
<td>Enable</td>
<td></td>
</tr>
<tr>
<td>1/0/2</td>
<td></td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>Enable</td>
<td>Enable</td>
<td></td>
</tr>
</tbody>
</table>

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

c. Enter the following information:
- In the **IP Address** field, enter **192.168.20.2**.
- In the **Network Mask** field, enter **255.255.255.0**.
- In the **Admin Mode** field, select **Enable**.

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

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

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

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

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

4. Enable OSPF on port 1/0/15.
a. Select Routing > OSPF > Advanced > Interface Configuration. A screen similar to the following displays.

b. Under Interface Configuration, scroll down and select the interface 1/0/15 check box.
   • In the OSPF Area ID field, enter 0.0.0.1.
   • In the OSPF Admin Mode field, select Enable.

c. Click Apply to save the settings.

5. Configure area 0.0.0.1 as a stub area.

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

b. In the Area ID field, enter 0.0.0.1.

c. Click Add to save the settings.
nssa Areas

Figure 11. 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.

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

```plaintext
(Netgear Switch) (Interface 2/0/19)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #show ip route
```

<table>
<thead>
<tr>
<th>Network</th>
<th>Subnet</th>
<th>Protocol</th>
<th>Intf</th>
<th>Next Hop</th>
<th>Next Hop IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1.1.0</td>
<td>255.255.255.0</td>
<td>OSPF Inter</td>
<td>2/0/11</td>
<td>192.168.10.2</td>
<td></td>
</tr>
<tr>
<td>14.1.2.0</td>
<td>255.255.255.0</td>
<td>OSPF Inter</td>
<td>2/0/11</td>
<td>192.168.10.2</td>
<td></td>
</tr>
<tr>
<td>192.168.10.0</td>
<td>255.255.255.0</td>
<td>Local</td>
<td>2/0/11</td>
<td>192.168.10.1</td>
<td></td>
</tr>
<tr>
<td>192.168.20.0</td>
<td>255.255.255.0</td>
<td>Local</td>
<td>2/0/19</td>
<td>192.168.20.1</td>
<td></td>
</tr>
<tr>
<td>192.168.40.0</td>
<td>255.255.255.0</td>
<td>OSPF NSSA T2</td>
<td>2/0/19</td>
<td>192.168.20.2</td>
<td></td>
</tr>
<tr>
<td>192.168.41.0</td>
<td>255.255.255.0</td>
<td>OSPF NSSA T2</td>
<td>2/0/19</td>
<td>192.168.20.2</td>
<td></td>
</tr>
<tr>
<td>192.168.42.0</td>
<td>255.255.255.0</td>
<td>OSPF NSSA T2</td>
<td>2/0/19</td>
<td>192.168.20.2</td>
<td></td>
</tr>
</tbody>
</table>

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.
      ![IP Configuration Screen](image)
   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.
   
   ![IP Interface Configuration Screen]

   b. Scroll down and select the interface 2/0/11 check box. Now 2/0/11 appears in the Interface field at the top.
   c. Enter the following information:
      • In the IP Address field, enter 192.168.10.1.
      • In the Network Mask field, enter 255.255.255.0.
      • In the Admin Mode field, select Enable.
   d. Click Apply to save the settings.

3. Assign IP address 192.168.20.1 to port 2/0/19.
   a. Select Routing > IP > Advanced > IP Interface Configuration. A screen similar to the following displays.
   
   ![IP Interface Configuration Screen]

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>OSPF Area ID</th>
<th>OSPF Admin Mode</th>
<th>Router Priority (0 to 255)</th>
<th>Retransmit Interval (0 to 3600)</th>
<th>Hello Interval (1 to 65535)</th>
<th>Dead Interval (1 to 2147483647)</th>
<th>Etransmit Delay Interval (1 to 3600)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/0/19</td>
<td>0.0.0.1</td>
<td>Enable</td>
<td>1</td>
<td>1</td>
<td>10</td>
<td>40</td>
<td>1</td>
</tr>
<tr>
<td>2/0/1</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>9</td>
<td>10</td>
<td>40</td>
<td>1</td>
</tr>
<tr>
<td>2/0/2</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>5</td>
<td>10</td>
<td>40</td>
<td>1</td>
</tr>
<tr>
<td>2/0/3</td>
<td>0.0.0.0</td>
<td>Disable</td>
<td>1</td>
<td>5</td>
<td>10</td>
<td>40</td>
<td>1</td>
</tr>
</tbody>
</table>

b. Scroll down and select the interface 2/0/19 check box. 2/0/19 now appears in the Interface field at the top.

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

d. Click Apply to save the settings.

7. Configure area 0.0.0.1 as a nssa area.

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

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

c. Click Add to save the settings.

**CLI: Configure Area 1 as an nssa Area on A2**

1. Enable routing on the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#router ospf
```
2. Set the router ID to 2.2.2.2.

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

3. Configure the area 0.0.0.1 as an nssa area.

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

4. Redistribute the RIP routes into the OSPF.

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

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

!(Netgear Switch) (Config-router)#exit
!(Netgear Switch) (Config)#interface 1/0/11
!(Netgear Switch) (Interface 1/0/11)#routing
!(Netgear Switch) (Interface 1/0/11)#ip address 192.168.30.1 255.255.255.0
!(Netgear Switch) (Interface 1/0/11)#ip rip
!(Netgear Switch) (Interface 1/0/11)#exit
!(Netgear Switch) (Config)#interface 1/0/15
!(Netgear Switch) (Interface 1/0/15)#routing
!(Netgear Switch) (Interface 1/0/15)#ip address 192.168.20.2 255.255.255.0
!(Netgear Switch) (Interface 1/0/15)#ip ospf
!(Netgear Switch) (Interface 1/0/15)#ip ospf areaid 0.0.0.1
!(Netgear Switch) (Interface 1/0/15)#exit
!(Netgear Switch) (Config)#exit
!(Netgear Switch) #show ip route

<table>
<thead>
<tr>
<th>Network Address</th>
<th>Subnet Mask</th>
<th>Protocol</th>
<th>Next Hop</th>
<th>Next Hop IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>OSPF Inter</td>
<td>1/0/15</td>
<td>192.168.20.1</td>
</tr>
<tr>
<td>192.168.20.0</td>
<td>255.255.255.0</td>
<td>Local</td>
<td>1/0/15</td>
<td>192.168.20.2</td>
</tr>
<tr>
<td>192.168.30.0</td>
<td>255.255.255.0</td>
<td>Local</td>
<td>1/0/11</td>
<td>192.168.30.1</td>
</tr>
<tr>
<td>192.168.40.0</td>
<td>255.255.255.0</td>
<td>RIP</td>
<td>1/0/11</td>
<td>192.168.30.2</td>
</tr>
<tr>
<td>192.168.41.0</td>
<td>255.255.255.0</td>
<td>RIP</td>
<td>1/0/11</td>
<td>192.168.30.2</td>
</tr>
<tr>
<td>192.168.42.0</td>
<td>255.255.255.0</td>
<td>RIP</td>
<td>1/0/11</td>
<td>192.168.30.2</td>
</tr>
</tbody>
</table>
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.
   
<table>
<thead>
<tr>
<th>System</th>
<th>Switching</th>
<th>Routing</th>
<th>QoS</th>
<th>Security</th>
<th>Monitoring</th>
<th>Maintenance</th>
<th>Help</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Table</td>
<td>IP</td>
<td>VLAN</td>
<td>ARP</td>
<td>RIP</td>
<td>OSPF</td>
<td>Router Discovery</td>
<td>VRRP</td>
<td></td>
</tr>
</tbody>
</table>

   - For Routing Mode, select the Enable radio button.
   - 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.
   
<table>
<thead>
<tr>
<th>System</th>
<th>Switching</th>
<th>Routing</th>
<th>QoS</th>
<th>Security</th>
<th>Monitoring</th>
<th>Maintenance</th>
<th>Help</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Table</td>
<td>IP</td>
<td>VLAN</td>
<td>ARP</td>
<td>RIP</td>
<td>OSPF</td>
<td>Router Discovery</td>
<td>VRRP</td>
<td></td>
</tr>
</tbody>
</table>

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

3. Assign IP address 192.168.20.2 to port 1/0/15.
a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

![IP Interface Configuration](image)

b. Under Configuration, scroll down and select the interface 1/0/15 check box. Now 1/0/15 appears in the Interface field at the top.

c. Enter the following information:
   - In the **IP Address** field, enter 192.168.20.2.
   - In the **Network Mask** field, enter 255.255.255.0.
   - In the **Routing Mode** field, select **Enable**.

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

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

![OSPF Configuration](image)

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

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

5. Enable RIP on port 1/0/11.
   a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

![Interface Configuration](image)
b. Enter the following information:
   • In the Interface field, select 1/0/11.
   • For RIP Admin Mode, select the Enable radio button.

c. Click Apply to save the settings.

6. Enable OSPF on port 1/0/15.
   a. Select Routing > OSPF > Advanced > Interface Configuration. A screen similar to the following displays.

   ![Interface Configuration Table]

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

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

d. Click Apply to save the settings.

7. Configure area 0.0.0.1 as an nssa area.
   a. Select Routing > OSPF > Advanced > NSSA Area Configuration. A screen similar to the following displays.

   ![NSSA Area Configuration Table]

   b. In the Area ID field, enter 0.0.0.1.

c. Click Add to save the settings.

8. Redistribute the RIP routes into the OSPF area.
a. Select **Routing > OSPF > Advanced > Route Redistribution**. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>Basic</th>
<th>Advanced</th>
<th>OSPF</th>
<th>Configuration</th>
<th>Common Area</th>
<th>Stub Area</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RIP</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

### VLAN Routing OSPF

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

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

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

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

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

This example adds support for OSPF to the configuration created in the base VLAN routing example in Figure 6, Layer 3 switch configured for port routing on page 48.

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

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

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

```
(Netgear Switch) (Config)#router ospf
(Netgear Switch) (Config router)#router-id 192.150.9.9
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#exit
```
3. Enable OSPF for the VLAN and physical router ports.

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

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

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

Web Interface: Configure VLAN Routing OSPF

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

   ![VLAN Routing Wizard](image)

   b. Enter the following information:
      - In the Vlan ID field, enter **10**.
      - In the IP Address field, enter **192.150.3.1**.
      - In the Network Mask field, enter **255.255.255.0**.
   c. Click Unit 1. The ports display:
Click the gray box under port 2 until T displays. The T specifies that the egress packet is tagged for the port.

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

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

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

   
   ![VLAN Routing Wizard Screen]

   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.

   
   ![OSPF Configuration Screen]

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

   c. In the Router ID field, enter 192.150.9.9.

   d. Click Apply to save the setting.

4. Enable OSPF on VLAN 10.
a. Select **Routing > OSPF > Advanced > Interface Configuration**. A screen similar to the following displays.

![Interface Configuration Screen](image)

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

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

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

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

5. Enable OSPF on VLAN 20.

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

   ![Interface Configuration Screen](image)

   b. Under Interface Configuration, click **VLANS** to show all the VLAN interfaces.
c. Scroll down and select the interface 0/2/2 check box. Now 0/2/2 appears in the Interface field at the top.

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

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

**OSPFv3**

OSPFv3 is the Open Shortest Path First routing protocol for IPv6. It is similar to OSPFv2 in its concept of a link state database, intra- and inter-area, and AS external routes and virtual links. It differs from its IPv4 counterpoint in a number of respects, including the following:

- Peering is done through link-local addresses; the protocol is link based rather than network based;
- and addressing semantics have been moved to leaf LSAs, which eventually allow its use for both IPv4 and IPv6.
- Point-to-point links are also supported in order to enable operation over tunnels. It is possible to enable OSPF and OSPFv3 at the same time. OSPF works with IPv4, and OSPFv3 works with IPv6. The following example shows how to configure OSPFv3 on a IPv6 network.

![Figure 12. OSPFv3 Protocol for IPv6](image)

**CLI: Configure OSPFv3**


```
(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

<table>
<thead>
<tr>
<th>Router ID</th>
<th>Priority</th>
<th>Intf ID</th>
<th>Interface</th>
<th>State</th>
<th>DeadTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.2</td>
<td>1</td>
<td>13</td>
<td>1/0/1</td>
<td>Full/BACKUP-DR</td>
<td>34</td>
</tr>
</tbody>
</table>
```

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
```

```
+--------+-------+-------+----------+--------+
<table>
<thead>
<tr>
<th>Router ID</th>
<th>Priority</th>
<th>IntfID</th>
<th>Interface</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>1</td>
<td>1</td>
<td>1/0/13</td>
<td>Full/ DR</td>
</tr>
</tbody>
</table>
+--------+-------+-------+----------+--------+
```

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.

   ![IPv6 Global Configuration](image)

   b. For IPv6 Unicast Routing Mode, select the Enable radio button.
   c. Click Apply to save the settings.

2. Specify the router ID, and enable OSPFv3 for the switch.
   a. Select Routing > OSPFv3 > Basic > OSPFv3 Configuration. A screen similar to the following displays.

   ![OSPF Configuration](image)

   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.
ProSafe Managed Switch

Chapter 7.  OSPF    |    101

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

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

c. Enter the following information:
   • In the IPv6 Mode field, select Enable.
   • In the Routing Mode field, select Enable.

d. Click Apply to save the settings.

4. Assign the IP address 2001::1 to port 1/0/1.

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

b. Under IPv6 Prefix Selection, in the Interface list, select 1/0/1.

c. Under IPv6 Interface Configuration, enter the following information:
   • In the IPv6 Prefix field, enter 2001::1.
   • In the Length field, enter 64.
   • In the EUI64 field, select Disable.
   • In the the Onlink Flag field, select Disable.
   • In the Autonomous Flag field, select Disable.

d. Click Add to save the settings.

5. Enable OSPFv3 on port 1/0/1.
a. Select **Routing > OSPFv3 > Advanced > Interface Configuration**. A screen similar to the following displays.

![IPv6 Prefix Configuration](image)

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

b. Under IP Interface Configuration, scroll down and select the interface `1/0/1` checkbox. 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.

![OSPF Neighbor Table](image)

To use the Web interface to configure OSPF on switch A2, repeat this process for switch A2.
Proxy ARP allows a router to answer ARP requests when the target IP address is not that of the router itself but a destination that the router can reach. If a host does not know the default gateway, proxy ARP can learn the first hop. Machines in one physical network appear to be part of another logical network. Without proxy ARP, a router responds to an ARP request only if the target IP address is an address configured on the interface where the ARP request arrived.

**Proxy ARP Examples**

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

**CLI: show ip interface**

```
(Netgear Switch) #show ip interface ?
<slot/port> Enter an interface in slot/port format.
brie Display summary information about IP configuration
settings for all ports.

(Netgear Switch) #show ip interface 0/24
Routing Mode................................. Disable
Administrative Mode......................... Enable
Forward Net Directed Broadcasts........... Disable
Proxy ARP................................. Disable
Active State............................... Inactive
Link Speed Data Rate....................... Inactive
MAC Address............................. 08:00:17:05:05:02
Encapsulation Type....................... Ethernet
IP MTU.................................. 1500
```
CLI: ip proxy-arp

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

<cr> Press Enter to execute the command.

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

Web Interface: Configure Proxy ARP on a Port

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

2. Under Configuration, scroll down and select the Interface 1/0/3 check box. Now 1/0/3 appears in the Interface field at the top.

3. In the Proxy Arp field, select Enable.

4. Click Apply to save the settings.
This chapter provides the following examples:

- **VRRP on a Master Router** on page 106
- **VRRP on a Backup Router** on page 108

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.

![Diagram of VRRP configuration](image)

**Figure 13. VRRP**

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

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

CLI: Configure VRRP on a Master Router

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

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

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

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

3. Enable VRRP for the switch.

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

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

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

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

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

6. Enable VRRP on the port.

```
(Netgear Switch) (Interface 1/0/2)#ip vrrp 20 mode
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```
Web Interface: Configure VRRP on a Master Router

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

   ![IP Configuration Screen](image)

   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.

   ![IP Interface Configuration Screen](image)

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

3. Enable VRRP on port 1/0/2.
a. Select Routing > VRRP > Advanced > VRRP Configuration. A screen similar to the following displays.

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

c. Enter the following information in the VRRP Configuration:
   - In the VRID (1 to 255) field, enter 20.
   - In the Interface field, select 1/0/2.
   - In the Primary IP Address field, enter 192.151.2.1.
   - 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.

   ```bash
   (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.

   ```bash
   (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.

   ![IP Configuration](image)

   **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.

```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>VLAN ID</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Routing Mode</th>
<th>Administrative Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/4</td>
<td></td>
<td></td>
<td>192.150.4.1</td>
<td>255.255.0.0</td>
<td>Enable</td>
<td>Enable</td>
</tr>
<tr>
<td>1/0/2</td>
<td></td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>Enable</td>
<td>Enable</td>
<td></td>
</tr>
<tr>
<td>1/0/3</td>
<td></td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>Enable</td>
<td>Enable</td>
<td></td>
</tr>
<tr>
<td>1/0/4</td>
<td></td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>Enable</td>
<td>Enable</td>
<td></td>
</tr>
<tr>
<td>1/0/5</td>
<td></td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>Enable</td>
<td>Enable</td>
<td></td>
</tr>
</tbody>
</table>
```

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.

```
<table>
<thead>
<tr>
<th>VRID (1 to 255)</th>
<th>Interface</th>
<th>Pre-emupt Mode</th>
<th>Priority (1 to 255)</th>
<th>Advertisment Interval (sec) (1 to 255)</th>
<th>Interface IP Address</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>1/0/4</td>
<td>Enable</td>
<td>254</td>
<td>1</td>
<td>192.150.2.1</td>
<td></td>
</tr>
</tbody>
</table>
```

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

- **MAC ACLs** on page 112
- **Set Up an IP ACL with Two Rules** on page 113
- **One-Way Access Using a TCP Flag in an ACL** on page 117
- **Use ACLs to Configure Isolated VLANs on a Layer 3 Switch** on page 132
- **Set up a MAC ACL with Two Rules** on page 144
- **ACL Mirroring** on page 147
- **ACL Redirect** on page 152
- **Configure IPv6 ACLs** on page 157

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

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

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

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

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

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

IP ACLs

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

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

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

ACL Configuration

To configure ACLs:

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

## Set Up an IP ACL with Two Rules

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

![Diagram showing a network setup with IP addresses and ACL rules](image)

**Figure 14. 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:

```bash
(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
```

---

ProSafe Managed Switch

Chapter 10. ACLs | 113
2. Define the second rule for ACL 101 to set conditions for UDP traffic similar to those for TCP traffic.

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

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

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

**Web Interface: Set Up an IP ACL with Two Rules**

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

   ![IP ACL screen](image)

   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.

   ![IP Extended Rules screen](image)

   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.

   ![Extended ACL Rule Configuration](image)

   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.

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.

b. Click Apply to save the settings.

5. Apply ACL 101 to port 2.

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

b. Under IP Binding Configuration, enter the following information:
In the **ACL ID** list, select **10**.
In the **Sequence Number** field, enter **1**.

c. Click **Unit 1**. The ports display.
d. Click the gray box under port **2**. A check mark displays in the box.
e. Click **Apply** to save the settings.

### One-Way Access Using a TCP Flag in an ACL

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

![Figure 15. One-Way Web access using a TCP flag in an ACL](image)

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

This is a two-step process:

- **Step 1: Configure the Switch** on page 117
- **Step 2: Configure the GSM7352S** on page 119

**Step 1: Configure the Switch**

(See **Figure 15. One-Way Web access using a TCP flag in an ACL.**)
1. Create VLAN 30 with port 0/35 and assign IP address 192.168.30.1/24.

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

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

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 100
(Netgear Switch) (Vlan)#vlan routing 100
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 0/13
(Netgear Switch) (Interface 0/13)#vlan pvid 100
(Netgear Switch) (Interface 0/13)#vlan participation include 100
(Netgear Switch) (Interface 0/13)#exit
(Netgear Switch) (Config)#interface vlan 100
(Netgear Switch) (Interface-vlan 100)#routing
(Netgear Switch) (Interface-vlan 100)#ip address 192.168.100.1 255.255.255.0
(Netgear Switch) (Interface-vlan 100)#exit
(Netgear Switch) (Config)#exit
```
3. Create VLAN 200 with port 0/44 and assign IP address 192.168.200.1/24.

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

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

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

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

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

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

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

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

**Step 2: Configure the GSM7352S**

(See Figure 15, One-Way Web access using a TCP flag in an ACL on page 117.)

1. Enter the following commands.

```
(Netgear Switch) (Config)#interface 0/44
(Netgear Switch) (Interface 0/44)#ip access-group 101 in 1
(Netgear Switch) (Interface 0/44)#ip access-group 102 in 2
(Netgear Switch) (Interface 0/44)#exit
```
2. Create VLAN 40 with port 1/0/24 and assign IP address 192.168.40.1/24.

   (Netgear Switch) #vlan database
   (Netgear Switch) (Vlan)#vlan 40
   (Netgear Switch) (Vlan)#vlan routing 40
   (Netgear Switch) #configure
   (Netgear Switch) (Config)#interface 1/0/24
   (Netgear Switch) (Interface 1/0/24)#vlan pvid 40
   (Netgear Switch) (Interface 1/0/24)#vlan participation include 40
   (Netgear Switch) (Interface 1/0/24)#exit
   (Netgear Switch) (Config)#interface vlan 40
   (Netgear Switch) (Interface-vlan 40)#routing
   (Netgear Switch) (Interface-vlan 40)#ip address 192.168.40.1 255.255.255.0
   (Netgear Switch) (Interface-vlan 40)#exit

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

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

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#vlan routing 200
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan pvid 200
(Netgear Switch) (Interface 1/0/48)#vlan participation include 200
(Netgear Switch) (Interface 1/0/48)#exit
(Netgear Switch) #interface vlan 200
(Netgear Switch) (Interface-vlan 200)#routing
(Netgear Switch) (Interface-vlan 200)#ip address 192.168.200.2 255.255.255.0
(Netgear Switch) (Interface-vlan 200)#exit
```

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

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

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

This is a two-part process:

- **Configuring the Switch** on page 121
- **Configuring the GSM7342S Switch** on page 129

**Configuring the Switch**

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

b. In the VLAN Routing Wizard, enter the following information:
   - In the **Vlan ID** field, enter **30**.
   - In the **IP Address** field, enter **192.168.30.1**.
   - In the **Network Mask** field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.
d. Click the gray box under port **35** twice until **U** displays. The **U** specifies that the egress packet is untagged for the port.
e. Click **Apply** to save VLAN 30.

2. Create VLAN 100 with IP address 192.168.100.1/24.

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

b. Enter the following information:
   - In the **Vlan ID** field, enter **100**.
• In the **IP Address** field, enter *192.168.100.1*.
• In the **Network Mask** field, enter *255.255.255.0*.

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

d. Click the gray box under port 13 twice until **U** displays. The **U** specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 100.


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

![VLAN Routing Wizard](image)

b. Enter the following information:
   • In the **Vlan ID** field, enter **200**.
   • In the **IP Address** field, enter *192.168.200.1*.
   • In the **Network Mask** field, enter *255.255.255.0*.

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

d. Click the gray box under port 44 twice until **U** displays. The **U** specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 200.

4. Enable IP routing.
a. Select Routing > IP > Basic > IP Configuration. A screen similar to the following displays.

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

c. Click Apply to enable IP routing.

5. Add a static route with IP address 192.268.40.0/24:
   a. Select Routing > Routing Table > Basic > Route Configuration. A screen similar to the following displays.

b. Under Configure Routes, make the following selection and enter the following information:
   - In the Route Type list, select Static.
   - In the Network Address field, enter 192.168.40.0.
   - In the Subnet Mask field, enter 255.255.255.0.
   - In the Next Hop IP Address field, enter 192.168.200.2.

c. Click Add.

6. Create a static route with IP address 192.168.50.0/24:
a. Select **Routing > Routing Table > Basic > Route Configuration**. A screen similar to the following displays.

![Route Configuration Screen](image)

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

c. Click **Add**.

7. **Create an ACL with ID 101.**

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

![IP ACL Screen](image)

   b. In the IP ACL Table, in the **IP ACL ID** field, enter **101**.
   
   c. Click **Add**.

8. **Create an ACL with ID 102.**
a. Select **Security > ACL > Advanced > IP ACL**. A screen similar to the following displays.

![IP ACL Table](image)

b. In the IP ACL Table, in the **IP ACL ID** field, enter 102.

c. Click **Add**.

9. Add and configure an IP extended rule that is associated with ACL 101.

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

![IP Extended Rules](image)

b. Under IP Extended Rules, in the **ACL ID** list, select 10.
c. Click **Add**. The Extended ACL Rule Configuration screen displays.

![Extended ACL Rule Configuration](image)

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

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

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

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

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

![IP Extended Rules](image)

b. Under IP Extended Rules, in the **ACL ID** list, select **102**.
c. Click **Add**. The Extended ACL Rule Configuration screen displays.

![Extended ACL Rule Configuration](image)

d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:
   - In the **Rule ID** field, enter 1.
   - For Action, select the **Permit** radio button.
   - In the **Match Every** field, select **False**.
   - In the **Protocol Type** list, select **IP**.

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

11. Apply ACL 101 to port 44.
   a. Select **Security > ACL > Advanced > IP Binding Configuration**. A screen similar to the following displays.

![IP Binding Configuration](image)

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.

![IP Binding Configuration](image)

b. Under Binding Configuration, make the following selection and enter the following information:
   - In the **ACL ID** list, select **102**.
   - In the **Sequence Number** field, enter **2**.

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

d. Click the gray box under port **44**. A check mark displays in the box.

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

**Configuring the GSM7342S Switch**


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

![VLAN Routing Wizard](image)

b. Enter the following information:
   - In the **Vlan ID** field, enter **40**.
• In the **IP Address** field, enter **192.168.40.1**.
• In the **Network Mask** field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.
d. Click the gray box under port **24** twice until **U** displays. The U specifies that the egress packet is untagged for the port.
e. Click **Apply** to save VLAN 40.

2. Create VLAN 50 with IP address 192.168.50.1/24:
   
a. Select **Routing > VLAN > VLAN Routing Wizard**. A screen similar to the following displays.
   
   ![VLAN Routing Wizard](image)

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

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

b. Enter the following information:
   - In the Vlan ID field, enter 200.
   - In the IP Address field, enter 192.168.200.2.
   - In the Network Mask field, enter 255.255.255.0.

c. Click Unit 1. The ports display.
d. Click the gray box under port 48 twice until U displays. The U specifies that the egress packet is untagged for the port.
e. Click Apply to save VLAN 200.

4. Create a static route with IP address 192.168.100.0/24:
   a. Select Routing > Routing Table > Basic > Route Configuration. A screen similar to the following displays.

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

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

   ![Route Configuration Screen]

   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.

![Diagram](image)

**Figure 16. Using ACLs to isolate VLANs on a Layer 3 switch**

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

1. Enter the following CLI commands.

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

   (Netgear Switch) (Config)#interface vlan 24
   (Netgear Switch) (Interface-vlan 24)#routing
   (Netgear Switch) (Interface-vlan 24)#ip address 192.168.24.1 255.255.255.0
   (Netgear Switch) (Interface-vlan 24)#exit
   (Netgear Switch) (Config)#exit
   ```
2. Create VLAN 48, add port 1/0/48 to it, and assign IP address 192.168.48.1 to it.

   ```
   (Netgear Switch) #vlan database
   (Netgear Switch) (Vlan)#vlan 48
   (Netgear Switch) (Vlan)#vlan routing 48
   (Netgear Switch) (Vlan)#exit
   (Netgear Switch) #config
   (Netgear Switch) (Config)#interface 1/0/48
   (Netgear Switch) (Interface 1/0/48)#vlan participation include 48
   (Netgear Switch) (Interface 1/0/48)#vlan pvid 48
   (Netgear Switch) (Interface 1/0/48)#exit
   (Netgear Switch) (Config)#vlan interface vlan 48
   (Netgear Switch) (Interface-vlan 48)#routing
   (Netgear Switch) (Interface-vlan 48)#ip address 192.168.48.1 255.255.255.0
   (Netgear Switch) (Interface-vlan 48)#exit
   ```

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

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

4. Enable IP routing on the switch.

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

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

   ```
   (Netgear Switch) (Config)#ip route default 10.100.5.252
   ```
6. Create ACL 101 to deny all traffic that has the destination IP address 192.168.24.0/24.

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

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

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

8. Create ACL 103 to permit all other traffic.

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

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

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

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

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

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

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

![VLAN Routing Wizard]

b. Enter the following information:
   - In the Vlan ID field, enter 24.
   - In the IP Address field, enter 192.168.24.1.
   - In the Network Mask field, enter 255.255.255.0.

c. Click Unit 1. The ports display.
d. Click the gray box under port 24 twice until U displays. The U specifies that the egress packet is untagged for the port.
e. Click Apply to save VLAN 24.

2. Create VLAN 48 with IP address 192.168.48.1.

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

![VLAN Routing Wizard]

b. Enter the following information:
   - In the Vlan ID field, enter 48.
   - In the IP Address field, enter 192.168.48.1.
   - In the Network Mask field, enter 255.255.255.0.
c. Click **Unit 1**. The ports display.

d. Click the gray box under port 48 twice until **U** displays. The **U** specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 48.

3. Create VLAN 38 with IP address 10.100.5.34.
   a. Select **Routing > VLAN > VLAN Routing Wizard**. A screen similar to the following displays.

   ![VLAN Routing Wizard Image]

   b. Enter the following information in the VLAN Routing Wizard:
      - In the **Vlan ID** field, enter **38**.
      - In the **IP Address** field, enter **10.100.5.34**.
      - In the **Network Mask** field, enter **255.255.255.0**.

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

   d. Click the gray box under port 38 twice until **U** displays. The **U** specifies that the egress packet is untagged for the port.

   e. Click **Apply** to save VLAN 38.

4. Enable IP routing:
   a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.

   ![IP Configuration Image]

   b. Under IP Configuration, make the following selections:
      - For Routing Mode, select the **Enable** radio button.
      - For IP Forwarding Mode, select the **Enable** radio button.
c. Click **Apply** to enable IP routing.

5. Create an ACL with ID 101.
   a. Select **Security > ACL > Advanced > IP ACL**. A screen similar to the following displays.

   ![IP ACL Screen](image)

   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.

   ![IP ACL Screen](image)

   b. In the IP ACL Table, in the **IP ACL ID** field, enter 102.
   c. Click **Add**.

7. Create an ACL with ID 103.
a. Select Security > ACL > Advanced > IP ACL. A screen similar to the following displays.

b. In the IP ACL ID field of the IP ACL Table, enter 103.

c. Click Add.

8. Add and configure an IP extended rule that is associated with ACL 101:

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

b. Under IP Extended Rules, in the ACL ID field, select 101.
c. Click Add. The Extended ACL Rule Configuration screen displays.

![Extended ACL Rule Configuration](image)

- In the **Rule ID** field, enter **1**.
- Under **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**.

Click **Apply** to save the settings.

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

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

![IP Extended Rules](image)

b. Under IP Extended Rules, in the **ACL ID** field, select **102**.
c. Click **Add**. The Extended ACL Rule Configuration screen displays.

![Extended ACL Rule Configuration](image)

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

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

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

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

![IP Extended Rules](image)

b. Under IP Extended Rules, in the **ACL ID** field, select **103**.
c. Click Add. The Extended ACL Rule Configuration screen displays.

d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:
   - In the Rule ID field, enter 1.
   - For Action mode, select the Permit radio button.
   - In the Match Every field, select False.
   - In the Protocol Type field, select IP.

e. Click Apply to save the settings.

11. Apply ACL 102 to port 24:
   a. Select Security > ACL > Advanced > IP Binding Configuration. A screen similar to the following displays.

   b. Under Binding Configuration, make the following selection and enter the following information:
      - In the ACL ID field, select 102.
In the **Sequence Number** field, enter 1.

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

d. Click the gray box under port 24. A check mark displays in the box.

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

**12.** Apply ACL 101 to port 48:

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

```
<table>
<thead>
<tr>
<th>System</th>
<th>Switching</th>
<th>Routing</th>
<th>QoS</th>
<th>Security</th>
<th>Monitoring</th>
<th>Maintenance</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Security</td>
<td>Access</td>
<td>Port Authentication</td>
<td>Traffic Control</td>
<td>ACL</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

MAC ACL
IP ACL
IP Rules
IP Extended Rules
IP Binding
Configuration
Binding Table

IP Binding Configuration

<table>
<thead>
<tr>
<th>Binding Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL ID</td>
</tr>
<tr>
<td>101</td>
</tr>
</tbody>
</table>

Port Selection Table

<table>
<thead>
<tr>
<th>Port</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>23</th>
<th>24</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```

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.

![IP Binding Configuration Screen]

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.

```plaintext
(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.

```plaintext
(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.

```bash
(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.

```bash
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#mac access-group acl_bpdu in
```

### Web Interface: Set up a MAC ACL with Two Rules

1. Create MAC ACL 101 on the switch.
   a. Select **Security > ACL > MAC ACL**. A screen similar to the following displays.

   ![MAC ACL screen](image1.png)

   b. In the **Name** field, enter *acl_bpdu*.
   c. Click **Add** to create ACL acl_bpdu.

2. Create a new rule associated with the ACL acl_bpdu.
   a. Select **Security > ACL > MAC ACL > MAC Rules**. A screen similar to the following displays.

   ![MAC Rules screen](image2.png)

   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 associated with the ACL acl_bpdu.
   a. Select Security > ACL > MAC ACL > MAC Rules. A screen similar to the following displays.

   a. Select acl_bpdu in the ACL Name field.
   b. Enter the following information in the Rule Table.
      • In the ID field, enter 2.
      • In the Action field, select the Permit.
   c. Click the Add button.

4. Apply the ACL acl_bpdu to port 2.
   a. Select Security > ACL > MAC ACL > MAC Binding Configuration. A screen similar to the following displays.

   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.

![ACL Mirroring Diagram](image)

**Figure 17. ACL mirroring**

**CLI: Configure ACL Mirroring**

The script in this section shows how to mirror the traffic stream received from a host in an interface. These examples mirror the traffic from the host 10.0.0.1 connected to the interface 1/0/1.
1. Create an IP access control list with the name monitorHost.

```
(Netgear Switch) (Config)# ip access-list monitorHost
```

2. Define the rules to match host 10.0.0.1 and to permit all others.

```
(Netgear Switch) (Config-ipv4-acl)# permit ip 10.0.0.1 0.0.0.0 any mirror 1/0/19
(Netgear Switch) (Config-ipv4-acl)# permit every
```

3. Bind the ACL with interface 1/0/1.

```
(Netgear Switch) (Interface 1/0/1)#ip access-group monitorHost in 1
```

4. View the configuration.

```
(Netgear Switch) # show ip access-lists
Current number of ACLs: 1  Maximum number of ACLs: 100

ACL ID/Name           Rules Direction Interface(s) VLAN(s)
---------------------- ----- ------------ ------------------ ---------------
monitorHost           2    inbound     1/0/1

(Netgear Switch) # show ip access-lists monitorHost

ACL Name: monitorHost
Inbound Interface(s): 1/0/1

Rule Number: 1
Action......................................... permit
Match All...................................... FALSE
Protocol....................................... 255(ip)
Source IP Address................. 10.0.0.1
Source IP Mask......................... 0.0.0.0
Mirror Interface...................... 1/0/19

Rule Number: 2
Action......................................... permit
Match All...................................... TRUE

Web Interface: Configure ACL Mirroring

1. Create an IP access control list with the name monitorHost on the switch.
a. Select Security > ACL > Advanced > IP ACL. A screen similar to the following displays.

![IP ACL screen](image)

b. In the IP ACL ID field, enter monitorHost.

c. Click Add to create ACL monitorHost, and the following screen displays:

![ ACL monitorHost screen](image)

2. Create a rule to match host 10.0.0.1 in the ACL monitorHost.

   a. Select Security > ACL > Advanced > IP Extended Rules. A screen similar to the following displays.
b. Click **Add**, and the Extended ACL Rule Configuration screen displays.

![Extended ACL Rule Configuration](image)

- **Step 1**: In the **Rule ID** field, enter 1.
- **Step 2**: For **Action**, select the **Permit** radio button.
- **Step 3**: In the **Mirror Interface** list, select **1/0/19**.
- **Step 4**: In the **Src IP Address** field, enter **10.0.0.1**.
- **Step 5**: In the **Src IP Mask** field, enter **0.0.0.0**.
- **Step 6**: Click **Apply**.

3. Create a rule to match every other traffic.
   
a. Select **Security > ACL > Advanced > IP Extended Rules**. A screen similar to the following displays.
b. Click **Add**, and a screen similar to the following displays.

![Extended ACL Rule Configuration](image)

- **Rule ID** field, enter **2**.
- Select the **Permit** radio button.
- In the **Match Every** field, select **True**.
- Click **Apply**. At the end of this configuration a screen similar to the following displays.

![Extended ACL Rule Table](image)

4. Bind the ACL with interface 1/0/1.
   a. Select **Security > ACL > Advanced > IP Binding Configuration**. A screen similar to the following displays.

![IP Binding Configuration](image)

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.
ACL Redirect

This feature redirects a specified traffic stream to a specified interface.

CLI: Redirect a Traffic Stream

The script in this section shows how to redirect an HTTP traffic stream received in an interface to the specified interface. This example redirects the HTTP traffic stream received in port 1/0/1 to port 1/0/19.
1. Create an IP access control list with the name redirectHTTP.

   (Netgear Switch) (Config)#ip access-list redirectHTTP

2. Define a rule to match the HTTP stream and define a rule to permit all others.

   (Netgear Switch) (Config-ipv4-acl)# permit tcp any any eq http redirect 1/0/19
   (Netgear Switch) (Config-ipv4-acl)# permit every

3. Bind the ACL with interface 1/0/1.

   (Netgear Switch) (Interface 1/0/1)#ip access-group redirectHTTP in 1

4. View the configuration.

   (Netgear Switch) # show ip access-lists
   Current number of ACLs: 1  Maximum number of ACLs: 100

   ACL ID/Name    Rules Direction Interface(s)         VLAN(s)
   ------------------------- ----- ---------- -------------------  ------------
   redirectHTTP                 2      inbound     1/0/1

   (Netgear Switch) # show ip access-lists redirectHTTP

   ACL Name: redirectHTTP
   Inbound Interface(s): 1/0/1

   Rule Number: 1
   Action......................................... permit
   Match All...................................... FALSE
   Protocol....................................... 6(tcp)
   Destination L4 Port Keyword.............. 80(www/http)
   Redirect Interface......................... 1/0/19

   Rule Number: 2
   Action......................................... permit
   Match All...................................... TRUE

Web Interface: Redirect a Traffic Stream

This example redirects the HTTP traffic stream received in port 1/0/1 to port 1/0/19.

1. Create an IP access control list with the name redirectHTTP.
a. Select **Security > ACL > Advanced > IP ACL**. A screen similar to the following displays.

![ProSafe Managed Switch](image)

b. In the **IP ACL** field, enter **redirectHTTP**.

c. Click **Add** to create the IP ACL redirectHTTP. A screen similar to the following displays.

![ProSafe Managed Switch](image)

2. Create a rule to redirect HTTP traffic.

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

![ProSafe Managed Switch](image)
b. Click **Add**, and the Extended ACL Rule Configuration screen displays.

c. In the **Rule ID** field, enter **1**.
d. For **Action**, select the **Permit** radio button.
e. In the **Redirect Interface** list, select **1/0/19**.
f. In the **Dst L4 Port** list, select **http**.
g. Click **Apply**. The Extended ACL Rules screen displays, as described in the next step in this procedure.

3. Create a rule to match every other traffic.
   a. Select **Security > ACL > Advanced > IP Extended Rules**. A screen similar to the following displays.
b. Click Add, and the Extended ACL Rule Configuration screen displays.

c. In the Rule ID field, enter 2.
d. For Action, select the Permit radio button.
e. In the Match Every field, select True.
f. Click Apply. A screen similar to the following displays.

4. Bind the ACL with interface 1/0/1.
   a. Select Security > ACL > Advanced > IP Binding Configuration. A screen similar to the following displays.

   b. In the Sequence Number field, enter 1.
   c. In the Port Selection Table, click Unit 1 to display all the ports.
d. Select the check box below Port 1.
e. Click Apply. At the end of this configuration a screen similar to the following displays.

Configure IPv6 ACLs

This feature extends the existing IPv4 ACL by providing support for IPv6 packet classification. Each ACL is a set of up to 12 rules applied to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and can apply to one or more of the following fields within a packet:

- Source IPv6 prefix
- Destination IPv6 prefix
- Protocol number
- Source Layer 4 port
- Destination Layer 4 port
- DSCP value
- Flow label
Note that the order of the rules is important: When a packet matches multiple rules, the first rule takes precedence. Also, once you define an ACL for a given port, all traffic not specifically permitted by the ACL is denied access.

The script in this section shows you how to set up an IPv6 ACL with the following three rules:

- **Rule-1.** Permits every traffic to the destination network 2001:DB8:C0AB:AC14::/64.
- **Rule-2.** Permits IPv6 TELNET traffic to the destination network 2001:DB8:C0AB:AC13::/64.
- **Rule-3.** Permits IPv6 HTTP traffic to any destination.

**CLI: Configure an IPv6 ACL**

1. Create the access control list with the name ipv6-acl.

```
(Netgear Switch) (Config)# ipv6 access-list ipv6-acl
```

2. Define three rules to:
   - Permit any IPv6 traffic to the destination network 2001:DB8:C0AB:AC14::/64 from the source network 2001:DB8:C0AB:AC11::/64.
• Permit IPv6 Telnet traffic to the destination network 2001:DB8:C0AB:AC13::/64 from the source network 2001:DB8:C0AB:AC11::/64.
• Permit IPv6 HTTP traffic to any destination network from the source network 2001:DB8:C0AB:AC11::/64.

(Netgear Switch) (Config-ipv6-acl)# permit ipv6 2001:DB8:C0AB:AC11::/64 2001:DB8:C0AB:AC14::/64
(Netgear Switch) (Config-ipv6-acl)# permit tcp 2001:DB8:C0AB:AC11::/64 2001:DB8:C0AB:AC13::/64 eq telnet
(Netgear Switch) (Config-ipv6-acl)# permit tcp 2001:DB8:C0AB:AC11::/64 any eq http

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

(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ipv6 traffic-filter ipv6-acl in
(Netgear Switch) (Interface 1/0/1)# exit
(Netgear Switch) (Config)#exit

4. View the configuration.

(Netgear Switch) #show ipv6 access-lists
Current number of all ACLs: 1  Maximum number of all ACLs: 100
IPv6 ACL Name        Rules Direction Interface(s) VLAN(s)
--------------------- ----- -------- ------------- -------------------
ipv6-acl             3  inbound  1/0/1

ACL Name: ipv6-acl
Inbound Interface(s): 1/0/1

Rule Number: 1
Action................................. permit
Protocol................................. 255(ipv6)
Source IP Address................. 2001:DB8:C0AB:AC11::/64
Destination IP Address............ 2001:DB8:C0AB:AC14::/64

Rule Number: 2
Action................................. permit
Protocol................................. 6(tcp)
Source IP Address................. 2001:DB8:C0AB:AC11::/64
Destination IP Address............ 2001:DB8:C0AB:AC13::/64
Destination L4 Port Keyword........ 23(telnet)
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.
   
   ![IPv6 ACL Table](image1)

   c. Click Add. A screen similar to the following displays.
   
   ![IPv6 ACL Rules](image2)

2. Define the first rule (1 of 3).
   a. Select Security > ACL > Advanced > IPv6 Rules. A screen similar to the following displays.
   
   ![IPv6 Rules](image3)

   b. In the ACL Name list, select ipv6-acl.
c. Click **Add**.

d. In the **Rule ID** field, enter 1.

e. For Action, select the **Permit** radio button.

f. In the **Source Prefix** field, enter 2001:DB8:C0AB:AC11::.

g. In the **Source Prefix Length** field, enter 64.

h. In the **Destination Prefix** field, enter 2001:DB8:C0AB:AC14::.

i. In the **Destination Prefix Length** field, enter 64. A screen similar to the following displays.

![IPv6 ACL Rule Configuration](image)

j. Click **Apply**.

3. **Add Rule 2.**

   a. In the **Rule ID** field, enter 2.

   b. For Action, select the **Permit** radio button.

   c. In the **Protocol Type** list, select TCP.

   d. In the **Source Prefix** field, enter 2001:DB8:C0AB:AC11::.

   e. In the **Source Prefix Length** field, enter 64.

   f. In the **Destination Prefix** field, enter 2001:DB8:C0AB:AC13::.

   g. In the **Destination Prefix Length** field, enter 64.
h. In the **Destination L4 Port** list, select **telnet**. A screen similar to the following displays.

![IPv6 ACL Rule Configuration](image)

i. Click **Apply**.

4. **Add Rule 3.**
   a. In the **Rule ID** field, enter **3**.
   b. For Action, select the **Permit** radio button.
   c. In the **Protocol Type** list, select **TCP**.
   d. In the **Source Prefix** field, enter **2001:DB8:C0AB:AC11::**.
   e. In the **Source Prefix Length** field, enter **64**.
   f. In the **Destination L4 Port** list, select **http**. A screen similar to the following displays.

![IPv6 ACL Rule Configuration](image)

g. Click **Apply**.

5. **Apply the rules to inbound traffic on port 1/0/1. Only traffic matching the criteria will be accepted.**
   a. Select **Security > ACL > Advanced > IP Binding Configuration.**
b. In the **ACL ID** list, select **ipv6-acl**.

c. In the **Sequence Number** list, select **1**.

d. Click **Unit 1**.

e. Select **Port 1**. A screen similar to the following displays.

![IP Binding Configuration](image1.png)

f. Click **Apply**. A screen similar to the following displays.

![IP Binding Configuration](image2.png)

6. View the binding table.

Select **Security > ACL > Advanced > Binding Table**. A screen similar to the following displays.

![IP ACL Binding Table](image3.png)
This chapter describes Class of Service (CoS) queue mapping, CoS Configuration, and traffic shaping features. This chapter provides the following examples:

- Show classofservice Trust on page 166
- Set classofservice Trust Mode on page 167
- Show classofservice IP-Precedence Mapping on page 168
- Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode on page 169
- Set CoS Trust Mode for an Interface on page 170
- Configure Traffic Shaping on page 171

Each port has one or more queues for packet transmission. During configuration, you can determine the mapping and configuration of these queues.

Based on the service rate and other criteria you configure, queues provide preference to specified packets. If a delay is necessary, the system holds packets until the scheduler authorizes transmission. As queues become full, packets are dropped. Packet drop precedence indicates the packet's sensitivity to being dropped during queue congestion.

Select per interface configuration scheme:

You can configure CoS mapping, queue parameters, and queue management are configurable per interface.

Queue management is configurable per interface.

Some hardware implementations allow queue depth management using tail dropping or weighted random early discard (WRED).

Some hardware implementations allow queue depth management using tail dropping.

The operation of CoS queuing involves queue mapping and queue configuration.
CoS Queue Mapping

CoS queue mapping uses trusted and untrusted ports.

Trusted Ports

- The system takes at face value certain priority designations for arriving packets.
- Trust applies only to packets that have that trust information.
- There can be only one trust field at a time - per port.
  - 802.1p user priority (This is the default trust mode and is managed through switching configuration.)
  - IP precedence
  - IP DiffServ Code Point (DSCP)

The system can assign the service level based upon the 802.1p priority field of the L2 header. You configure this by mapping the 802.1p priorities to one of three traffic class queues. These queues are:

- **Queue 2.** Minimum of 50 percent of available bandwidth
- **Queue 1.** Minimum of 33 percent of available bandwidth
- **Queue 0.** Lowest priority, minimum of 17 percent of available bandwidth

For untagged traffic, you can specify the default 802.1p priority on a per-port basis.

Untrusted Ports

- No incoming packet priority designation is trusted; therefore, the default priority value for the port is used.
- All ingress packets from untrusted ports, where the packet is classified by an ACL or a DiffServ policy, are directed to specific CoS queues on the appropriate egress port. That specific CoS queue is determined by either the default priority of the port or a DiffServ or ACL-assigned queue attribute.
- Used when trusted port mapping is unable to be honored - for instance, when a non-IP DSCP packet arrives at a port configured to trust IP DSCP.
CoS Queue Configuration

CoS queue configuration involves port egress queue configuration and drop precedence configuration (per queue). The design of these on a per-queue, per-drop precedence basis allows you to create the service characteristics that you want for different types of traffic.

Port egress queue configuration:
- Scheduler type, strict vs. weighted
- Minimum guaranteed bandwidth
- Maximum allowed bandwidth per-queue shaping
- Queue management type, tail drop vs. WRED

Drop precedence configuration (per queue):
- WRED parameters
  - Minimum threshold
  - Maximum threshold
  - Drop probability
  - Scale factor
- Tail drop parameters, threshold

Per-interface basis:
- Queue management type, tail Drop vs. WRED

Only if per-queue configuration is not supported
- WRED decay exponent
- Traffic shaping for an entire interface

Show classofservice Trust

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

CLI: Show classofservice Trust

To use the CLI to show CoS trust mode, use these commands:

```
(Netgear Switch) #show classofservice trust?
<cr> Press Enter to execute the command.
(Netgear Switch) #show classofservice trust
Class of Service Trust Mode: Dot1P
```
Web Interface: Show classofservice Trust

Select QoS > CoS > Basic > CoS Configuration. A screen similar to the following displays.

![CoS Configuration](image)

Set classofservice Trust Mode

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

CLI: Set classofservice Trust Mode

```
(Netgear Switch) (Config)#classofservice?
dot1p-mapping                      Configure dot1p priority mapping.
ip-dscp-mapping                    Maps an IP DSCP value to an internal traffic class.
trust                              Sets the Class of Service Trust Mode of an Interface.
(Netgear Switch) (Config)#classofservice trust?
dot1p                              Sets the Class of Service Trust Mode of an Interface
to 802.1p.
ip-dscp                            Sets the Class of Service Trust Mode of an Interface
to IP DSCP.
(Netgear Switch) (Config)#classofservice trust dot1p?
<cr>                                Press Enter to execute the command.
(Netgear Switch) (Config)#classofservice trust dot1p
```

Web Interface: Set classofservice Trust Mode

1. Select QoS > CoS > Basic > CoS Configuration. A screen similar to the following displays.

![CoS Configuration](image)
2. Select the **Global** radio button.
3. In the **Global Trust Mode** list, select **trust dot1p**.
4. Click **Apply** to save the settings.

### Show classofservice IP-Precedence Mapping

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

#### CLI: Show classofservice IP-Precedence Mapping

```
(Netgear Switch) #show classofservice ip-precedence-mapping

<table>
<thead>
<tr>
<th>IP Precedence</th>
<th>Traffic Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
</tr>
</tbody>
</table>
```

#### Web Interface: Show classofservice ip-precedence Mapping

1. Select **QoS > CoS > Advanced > IP Precedence Queue Mapping**. A screen similar to the following displays.

2. In the Interface list, select **All**.
   The global IP precedence to queue mapping is displayed.

3. In the **Interface** list, select the specific interface (such as 1/0/1).
The IP precedence to queue mapping of the interface is displayed.

**Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode**

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

**CLI: Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode**

```
(Netgear Switch) (Config)#cos-queue min-bandwidth?
<bw-0>                   Enter the minimum bandwidth percentage for Queue 0.
(Netgear Switch) (Config)#cos-queue min-bandwidth 15
Incorrect input! Use 'cos-queue min-bandwidth <bw-0>..<bw-7>.
(Netgear Switch) (Config)#cos-queue min-bandwidth 15 25 10 5 5 20 10 10
(Netgear Switch) (Config)#cos-queue strict?
<queue-id>               Enter a Queue Id from 0 to 7.
(Netgear Switch) (Config)#cos-queue strict 1?
<cr>                     Press Enter to execute the command.
<queue-id>               Enter an additional Queue Id from 0 to 7.
(Netgear Switch) (Config)#cos-queue strict 1
```

**Web Interface: Configure CoS-queue Min-bandwidth and Strict Priority Scheduler Mode**

1. For Interface 1/0/2, set the minimum bandwidth to 15 for queue 0.
   a. **Select QoS > CoS > Advanced > Interface Queue Configuration.** A screen similar to the following displays.

```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Queue ID</th>
<th>Minimum Bandwidth</th>
<th>Scheduler Type</th>
<th>Queue Management Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/2</td>
<td>0</td>
<td>15</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
<tr>
<td>1/0/1</td>
<td>0</td>
<td>0</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
<tr>
<td>1/0/2</td>
<td>0</td>
<td>25</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
<tr>
<td>1/0/3</td>
<td>0</td>
<td>10</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
<tr>
<td>1/0/4</td>
<td>0</td>
<td>5</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
<tr>
<td>1/0/5</td>
<td>0</td>
<td>20</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
</tbody>
</table>
```

b. In the **Queue ID** list, select **0**.
c. Under Interface Queue Configuration, scroll down and select the interface 1/0/2 check box. Now 1/0/2 appears in the Interface field at the top.

d. Enter the following information:
   - In the **Minimum Bandwidth** field, enter 15.
   - In the **Scheduler Type** list, select **Weighted**.

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

2. For interface 1/0/2, set the minimum bandwidth 25 for queue 1, and set the scheduler type to strict.

a. Select **QoS > CoS > Advanced > Interface Queue Configuration**. A screen similar to the following displays.

   - In the **Queue ID** list, select 1.
   - 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.
   - Enter the following information:
     - In the **Minimum Bandwidth** field, enter 25.
     - In the **Scheduler Type** list, select **Strict**.
   - Click **Apply** to save the settings.

### Set CoS Trust Mode for an Interface

The example is shown as CLI commands and as a Web interface procedure.
CLI: Set CoS Trust Mode for an Interface

```
(Netgear Switch) (Interface 1/0/3)#classofservice trust?
  dot1p        Sets the Class of Service Trust Mode of an Interface
to 802.1p.
  ip-dscp     Sets the Class of Service Trust Mode of an Interface
to IP DSCP.
(Netgear Switch) (Interface 1/0/3)#classofservice trust dot1p?
  <cr>        Press Enter to execute the command.
(Netgear Switch) (Interface 1/0/3)#classofservice trust dot1p
```

**Note:** The traffic class value range is 0—6 instead of 0—7 because queue 7 is reserved in a stacking build for stack control, and therefore you cannot configure it.

Web Interface: Set CoS Trust Mode for an Interface

1. Select QoS > CoS > Advanced > CoS Configuration. A screen similar to the following displays.

   ![Web Interface Screen]

2. Under CoS Configuration, select the Interface radio button.
3. In the Interface list, select 1/0/3.
4. In the Interface Trust Mode list, select trust dot1p.
5. Click Apply to save the settings.

Configure Traffic Shaping

Traffic shaping controls the amount and volume of traffic transmitted through a network. This has the effect of smoothing temporary traffic bursts over time. Use the traffic-shape
command to enable traffic shaping by specifying the maximum transmission bandwidth limit for all interfaces (Global Config) or for a single interface (Interface Config).

The <bw> value is a percentage that ranges from 0 to 100 in increments of 5. The default bandwidth value is 0, meaning no upper limit is enforced, which allows the interface to transmit up to its maximum line rate.

The bw value is independent of any per-queue maximum bandwidth values in effect for the interface and should be considered as a second-level transmission rate control mechanism that regulates the output of the entire interface regardless of which queues originate the outbound traffic.

CLI: Configure traffic-shape

```
(Netgear Switch) (Config)#traffic-shape?
<bw>                     Enter the shaping bandwidth percentage from 0 to 100
                         in increments of 5.
(Netgear Switch) (Config)#traffic-shape 70?
<cr>                     Press Enter to execute the command.
(Netgear Switch) (Config)#traffic-shape 70
(Netgear Switch) (Config)#
```

Web Interface: Configure Traffic Shaping

1. Set the shaping bandwidth percentage to 70 percent.
   a. Select QoS > CoS > Advanced > CoS Interface Configuration. A screen similar to the following displays.

   ![CoS Interface Configuration Screen](image)

   b. Under CoS Interface Configuration, scroll down and select the interface 1/0/3 check box. Now 1/0/3 appears in the Interface field at the top.

   c. In the Interface Shaping Rate (0 to 100) field, enter 70.

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

This chapter provides the following examples:

- **DiffServ** on page 174
- **DiffServ for VoIP** on page 190
- **Auto VoIP** on page 197
- **DiffServ for IPv6** on page 201
- **Color Conform Policy** on page 208

Differentiated services (DiffServ) is one technique for implementing Quality of Service (QoS) policies. Using DiffServ in your network allows you to directly configure the relevant parameters on the switches and routers rather than using a resource reservation protocol. This section explains how to configure the 7000 Series Managed Switch to identify which traffic class a packet belongs to, and how it should be handled to provide the quality of service you want. As implemented on the 7000 Series Managed Switch, DiffServ allows you to control what traffic is accepted and what traffic is discarded.

How you configure DiffServ support on a 7000 Series Managed Switch varies depending on the role of the switch in your network:

- **Edge device.** An edge device handles ingress traffic, flowing toward the core of the network, and egress traffic, flowing away from the core. An edge device segregates inbound traffic into a small set of traffic classes, and is responsible for determining a packet’s classification. Classification is based primarily on the contents of the Layer 3 and Layer 4 headers, and is recorded in the Differentiated Services Code Point (DSCP) added to a packet’s IP header.

- **Interior node.** A switch in the core of the network is responsible for forwarding packets, rather than for classifying them. It decodes the DSCP code point in an incoming packet, and provides buffering and forwarding services using the appropriate queue management algorithms.

Before configuring DiffServ on a particular 7000 Series Managed Switch, you must determine the QoS requirements for the network as a whole. The requirements are expressed in terms of rules, which are used to classify inbound traffic on a particular interface. The switch software does not support DiffServ in the outbound direction.

Rules are defined in terms of classes, policies, and services:
• **Class.** A class consists of a set of rules that identify which packets belong to the class. Inbound traffic is separated into traffic classes based on Layer 3 and Layer 4 header data and the VLAN ID, and marked with a corresponding DSCP value. One type of class is supported: All, which specifies that every match criterion defined for the class must be true for a match to occur.

• **Policy.** Defines the QoS attributes for one or more traffic classes. An example of an attribute is the ability to mark a packet at ingress. The 7000 Series Managed Switch supports a traffic conditions policy. This type of policy is associated with an inbound traffic class and specifies the actions to be performed on packets meeting the class rules:
  - Marking the packet with a given DSCP code point, IP precedence, or CoS
  - Policing packets by dropping or re-marking those that exceed the class’s assigned data rate
  - Counting the traffic within the class

• **Service.** Assigns a policy to an interface for inbound traffic.

---

**DiffServ**

This example shows how a network administrator can provide equal access to the Internet (or other external network) to different departments within a company. Each of four departments has its own Class B subnet that is allocated 25 percent of the available bandwidth on the port accessing the Internet.

![Diagram](image)

**Figure 20. Class B subnet with differentiated services**

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

1. Ensure that the DiffServ operation is enabled for the switch.

   ```
   (Netgear Switch) #config
   (Netgear Switch) (Config)#diffserv
   ```

2. Create a DiffServ class of type all for each of the departments, and name them. Define the match criteria of source IP address for the new classes.

   ```
   (Netgear Switch) (Config)#class-map match-all finance_dept
   (Netgear Switch) (Config class-map)#match srcip 172.16.10.0 255.255.255.0
   (Netgear Switch) (Config class-map)#exit

   (Netgear Switch) (Config)#class-map match-all marketing_dept
   (Netgear Switch) (Config class-map)#match srcip 172.16.20.0 255.255.255.0
   (Netgear Switch) (Config class-map)#exit

   (Netgear Switch) (Config)#class-map match-all test_dept
   (Netgear Switch) (Config class-map)#match srcip 172.16.30.0 255.255.255.0
   (Netgear Switch) (Config class-map)#exit

   (Netgear Switch) (Config)#class-map match-all development_dept
   (Netgear Switch) (Config class-map)#match srcip 172.16.40.0 255.255.255.0
   (Netgear Switch) (Config class-map)#exit
   ```

3. Create a DiffServ policy for inbound traffic named 'internet_access', adding the previously created department classes as instances within this policy.
This policy uses the assign-queue attribute to put each department’s traffic on a different egress queue. This is how the DiffServ inbound policy connects to the CoS queue settings established in the following example.

```
(Netgear Switch) (Config)#policy-map internet_access in
(Netgear Switch) (Config policy-map)#class finance_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 1
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class marketing_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 2
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class test_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 3
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class development_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 4
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#exit
```

4. Attach the defined policy to interfaces 1/0/1 through 1/0/4 in the inbound direction.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/1)#exit

(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/2)#exit

(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/3)#exit

(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/4)#exit
```

5. Set the CoS queue configuration for the (presumed) egress interface 1/0/5 such that each of queues 1, 2, 3, and 4 gets a minimum guaranteed bandwidth of 25 percent. All queues for this interface use weighted round robin scheduling by default. The DiffServ inbound policy designates that these queues are to be used for the departmental traffic through the
assign-queue attribute. It is presumed that the switch will forward this traffic to interface 1/0/5 based on a normal destination address lookup for Internet traffic.

(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#cos-queue min-bandwidth 0 25 25 25 25 0 0 0
(Netgear Switch) (Interface 1/0/5)#exit
(Netgear Switch) (Config)#exit

Web Interface: Configure DiffServ

1. Enable DiffServ.
   a. Select QoS > DiffServ > Basic > DiffServ Configuration. A screen similar to the following displays.

   ![DiffServ Configuration Screen]

   b. For DiffServ Admin Mode, select the Enable radio button.
   c. Click Apply to save the settings.

2. Create the class finance_dept.
   a. Select QoS > DiffServ > Advanced > Class Configuration. A screen similar to the following displays.

   ![Class Configuration Screen]

   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.

![](image1.png)

e. Under Diffserv Class Configuration, enter the following information:
   - In the Source IP Address field, enter 172.16.10.0.
   - In the Source Mask field, enter 255.255.255.0.

f. Click Apply.

3. Create the class marketing_dept:

   a. Select QoS > Diffserv > Advanced > Class Configuration. A screen similar to the following displays.

   ![Screen Shot](image2.png)

   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.

![DiffServ Class Configuration](image)

- In the **Source IP Address** field, enter **172.16.20.0**.
- In the **Source Mask** field, enter **255.255.255.0**.

f. Click **Apply**.

4. Create the class **test_dept**:

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

![Class Configuration](image)

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.

![ProSafe Managed Switch](image)

- **Click test_dept to configure this class.**

  - 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**.
  - **Click Apply.**

5. Create class **development_dept**.

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

![ProSafe Managed Switch](image)

- **Enter the following information:**
  - In the **Class Name** field, enter **development_dept**.
  - In the **Class Type** list, select **All**.
- **Click the Add to create a new class development_dept.**
d. Click development_dept to configure this class.

![DiffServ Configuration Screen]

- In the Source IP Address field, enter 172.16.40.0.
- In the Source Mask field, enter 255.255.255.0.

f. Click Apply.

6. Create a policy named internet_access and add the class finance_dept to it.

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

![Policy Configuration Screen]

b. Enter the following information:
- In the Policy Selector field, enter internet_access.
- In the Member Class list, select the finance_dept.

c. Click Add to create a new policy internet_access.

7. Add the class marketing_dept into the policy internet_access.
a. Select QoS > DiffServ > Advanced > Policy Configuration. A screen similar to the following displays.

![Policy Configuration Screen](image)

b. Under Policy Configuration, scroll down and select the **internet_access** check box. **internet_access** now appears in the Policy Selector field at the top.

c. In the **Member Class** list, select **marketing_dept**.

d. Click **Apply** to add the class **marketing_dept** to the policy **internet_access**.

8. Add the class **test_dept** into the policy **internet_access**.

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

![Policy Configuration Screen](image)

b. Under Policy Configuration, scroll down and select the **internet_access** check box. **Internet_access** now appears in the Policy Selector field at the top.

c. In the **Member Class** list, select **test_dept**.

d. Click **Apply** to add the class **test_dept** to the policy **internet_access**.

9. Add the class **development_dept** into the policy **internet_access**.
a. Select QoS > DiffServ > Advanced > Policy Configuration. A screen similar to the following displays.

![Policy Configuration Screen](image1)

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.

![Policy Configuration Screen](image2)
b. Click the **internet_access** check box for the member class finance_dept. A screen similar to the following displays.

![DiffServ Configuration Screen](image)

b. In the **Assign Queue** list, select 1.

c. Click **Apply**.

d. **Assign queue 2 to marketing_dept.**

11. **Assign queue 2 to marketing_dept.**

a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.
b. Click the **internet_access** check box for marketing_dept. A screen similar to the following displays.

![Policy Class Configuration](image)

![Assign Queue list](image)

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.

![Policy Configuration](image)
b. Click the `internet_access` check mark for `test_dept`. A screen similar to the following displays.

c. In the **Assign Queue** list, select 3.

d. Click **Apply**.

13. Assign queue 4 to `development_dept`.

a. Select **QoS > DiffServ > Advanced > Policy Configuration**. A screen similar to the following displays.
b. Click the **internet_access** check mark for development_dept. A screen similar to the following displays.

![DiffServ screen](image)

c. In the **Assign Queue** list, select 4.

d. Click **Apply**.

14. Attach the defined policy to interfaces 1/0/1 through 1/0/4 in the inbound direction.

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

![DiffServ Service Configuration](image)

b. Scroll down and select the check boxes for interfaces 1/0/1, 1/0/2, 1/0/3, and 1/0/4.

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

d. Click **Apply**.

15. Set the CoS queue 1 configuration for interface 1/0/5.
a. Select QoS > CoS > Advanced > Interface Queue Configuration. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Queue ID</th>
<th>Minimum Bandwidth</th>
<th>Scheduler Type</th>
<th>Queue Management Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/5</td>
<td>1</td>
<td>25</td>
<td>Weighted</td>
<td>taildrop</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Queue ID</th>
<th>Minimum Bandwidth</th>
<th>Scheduler Type</th>
<th>Queue Management Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/5</td>
<td>2</td>
<td>25</td>
<td>Weighted</td>
<td>taildrop</td>
</tr>
</tbody>
</table>

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.
1. Select **QoS > CoS > Advanced > Interface Queue Configuration**. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Queue ID</th>
<th>Minimum Bandwidth</th>
<th>Scheduler Type</th>
<th>Queue Management Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/5</td>
<td>3</td>
<td>25</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
<tr>
<td>1/0/2</td>
<td>3</td>
<td>25</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
<tr>
<td>1/0/6</td>
<td>2</td>
<td>25</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
<tr>
<td>1/0/7</td>
<td>2</td>
<td>25</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Queue ID</th>
<th>Minimum Bandwidth</th>
<th>Scheduler Type</th>
<th>Queue Management Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/5</td>
<td>4</td>
<td>25</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
<tr>
<td>1/0/1</td>
<td>3</td>
<td>25</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
<tr>
<td>1/0/2</td>
<td>3</td>
<td>25</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
<tr>
<td>1/0/3</td>
<td>3</td>
<td>25</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
<tr>
<td>1/0/4</td>
<td>3</td>
<td>25</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
<tr>
<td>1/0/5</td>
<td>3</td>
<td>25</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
<tr>
<td>1/0/6</td>
<td>3</td>
<td>25</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
<tr>
<td>1/0/7</td>
<td>3</td>
<td>25</td>
<td>weighted</td>
<td>taildrop</td>
</tr>
</tbody>
</table>

b. Under Interface Queue Configuration, scroll down and select the Interface 1/0/5 check box. Now 1/0/5 appears in the Interface field at the top.

c. In the **Queue ID** list, select 4.

d. In the **Minimum Bandwidth** field, enter 25.

e. Click **Apply**.
DiffServ for VoIP

One of the most valuable uses of DiffServ is to support Voice over IP (VoIP). VoIP traffic is inherently time sensitive: For a network to provide acceptable service, a guaranteed transmission rate is vital. This example shows one way to provide the necessary quality of service: how to set up a class for UDP traffic, have that traffic marked on the inbound side, and then expedite the traffic on the outbound side. The configuration script is for Router 1 in the accompanying diagram: A similar script should be applied to Router 2.

Figure 21. Diffserv for VoIP in Router 1

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

CLI: Configure DiffServ for VoIP

1. Enter Global configuration mode. Set queue 5 on all ports to use strict priority mode. This queue will be used for all VoIP packets. Activate DiffServ for the switch.

{(Netgear Switch) #config
(Netgear Switch) (Config)#cos-queue strict 5
(Netgear Switch) (Config)#diffserv}
2. Create a DiffServ classifier named `class_voip` and define a single match criterion to detect UDP packets. The class type `match-all` indicates that all match criteria defined for the class must be satisfied in order for a packet to be considered a match.

```
(Netgear Switch) (Config)#class-map match-all class_voip
(Netgear Switch) (Config class-map)#match protocol udp
(Netgear Switch) (Config class-map)#exit
```

3. Create a second DiffServ classifier named `class_ef` and define a single match criterion to detect a DiffServ code point (DSCP) of `EF` (expedited forwarding). This handles incoming traffic that was previously marked as expedited somewhere in the network.

```
(Netgear Switch) (Config)#class-map match-all class_ef
(Netgear Switch) (Config class-map)#match ip dscp ef
(Netgear Switch) (Config class-map)#exit
```

4. Create a DiffServ policy for inbound traffic named `pol_voip`, then add the previously created classes `class_ef` and `class_voip` as instances within this policy.

This policy handles incoming packets already marked with a DSCP value of `EF` (according to the `class_ef` definition), or marks UDP packets according to the `class_voip` definition) with a DSCP value of `EF`. In each case, the matching packets are assigned internally to use queue 5 of the egress port to which they are forwarded.

```
(Netgear Switch) (Config)#policy-map pol_voip in
(Netgear Switch) (Config policy-map)#class class_ef
(Netgear Switch) (Config policy-class-map)#assign-queue 5
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class class_voip
(Netgear Switch) (Config policy-class-map)#mark ip-dscp ef
(Netgear Switch) (Config policy-class-map)#assign-queue 5
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#exit
```

5. Attach the defined policy to an inbound service interface.

```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#service-policy in pol_voip
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```
Web Interface: Diffserv for VoIP

1. Set queue 5 on all interfaces to use strict mode.
   a. Select QoS > CoS > Advanced > CoS Interface Configuration. A screen similar to the following displays.
   
   ![Interface Queue Configuration](image)
   
   b. Under Interface Queue Configuration, select all the interfaces.
   c. In the Queue ID list, select 5.
   d. In the Scheduler Type list, select Strict.
   e. Click Apply to save the settings.

2. Enable DiffServ.
   a. Select QoS > DiffServ > Basic > DiffServ Configuration. A screen similar to the following displays.
   
   ![DiffServ configuration](image)
   
   b. For Diffserv Admin Mode, select the Enable radio button.
   c. Click Apply to save the settings.

3. Create a class class_voip.
a. Select QoS > DiffServ > Advanced > DiffServ Configuration. A screen similar to the following displays.

b. In the Class Name field, enter class_voip.

c. In the Class Type list, select All.

d. Click Add to create a new class.

e. Click class_voip. A screen similar to the following displays:

f. In the Protocol Type list, select UDP.

g. Click Apply to create a new class.

4. Create a class class_ef:
a. Select QoS > DiffServ > Advanced > DiffServ Configuration. A screen similar to the following displays.

![DiffServ Configuration Screen](image)

b. In the Class Name field, enter class_ef.

c. In the Class Type list, select All.

d. Click Add to create a new class.

e. Click class_ef. Another screen similar to the following displays:

![DiffServ Class Configuration Screen](image)

f. In the IP DSCP list, select ef.

g. Click Apply to create a new class.

5. Create a policy pol_voip. and add class_voip to this policy.
a. Select QoS > DiffServ > Advanced > Policy Configuration. A screen similar to the following displays.

b. In the Policy Selector field, enter pol_voip.

c. In the Member Class list, select class_voip.

d. Click Add to create a new policy.

e. Click the pol_voip whose class member is class_voip. A screen similar to the following displays.

f. In the Assign Queue list, select 5.

g. For Policy Attribute, select the Mark IP DSCP radio button, and select ef.

h. Click Apply to create a new policy.

6. Add class_ef to the policy pol_voip.
a. Select QoS > DiffServ > Advanced > Policy Configuration. A screen similar to the following displays.

![Policy Configuration Screen]

b. Under Policy Configuration, scroll down and select the pol_voip check box. Pol_voip now appears in the Policy Selector field at the top.

c. In the Member Class list, select class_ef in.

d. Click Apply to add the class class_ef to the policy pol_voip.

e. Click the pol_voip whose class member is class_ef, and a screen similar to the following displays.

![Policy Class Configuration Screen]

f. In the Assign Queue list, select 5.

g. Click Apply to create a new policy.

7. Attach the defined policy to interface 1/0/2 in the inbound direction.
a. Select QoS > DiffServ > Advanced > Service Configuration. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>System</th>
<th>Switching</th>
<th>Routing</th>
<th>QoS</th>
<th>Security</th>
<th>Monitoring</th>
<th>Maintenance</th>
<th>Help</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DiffServ Service Configuration

<table>
<thead>
<tr>
<th>Interface</th>
<th>Policy In</th>
<th>Direction</th>
<th>Operational Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

c. In the Policy In list, select pol_voip.

d. Click Apply to create a new policy.

Auto VoIP

The Auto-VoIP feature makes it easy to set up VoIP for IP phones on a switch. This functionality copies VoIP signaling packets to the CPU to get the source and destination IP address and Layer 4 port of the current session. Based on these parameters a filter is
installed to assign the highest priority to VOIP data packets. As soon as the call ends, the filters are removed.

Figure 22. Auto VoIP

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

**CLI: Configure Auto VoIP**

This script in this section shows how to set up auto VoIP system-wide.

1. Enable auto VoIP on all the interfaces in the device.

   ```
   (Netgear Switch) (Config)# auto-voip all
   ```
2. View the auto VoIP information:

```
(Netgear Switch) # show auto-voip interface all

<table>
<thead>
<tr>
<th>Interface</th>
<th>Auto VoIP Mode</th>
<th>Traffic Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/1</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/2</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/3</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/4</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/5</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/6</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/7</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/8</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/9</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/10</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/11</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/12</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/13</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/14</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/15</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/16</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/17</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/18</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/19</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/20</td>
<td>Enabled</td>
<td>6</td>
</tr>
</tbody>
</table>

--More-- or (q)uit

<table>
<thead>
<tr>
<th>Interface</th>
<th>Auto VoIP Mode</th>
<th>Traffic Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/21</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/22</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/23</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/24</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/25</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/26</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/27</td>
<td>Enabled</td>
<td>6</td>
</tr>
<tr>
<td>1/0/28</td>
<td>Enabled</td>
<td>6</td>
</tr>
</tbody>
</table>
```

Auto VoIP classifies and prioritizes the packets and places only the packets in the higher-priority queue. In the previous example, they are placed in queue 6. You can override the egress queue setting using the commands `cos-queue strict` or `cos-queue min-bandwidth` if you want.
Web Interface: Configure Auto-VoIP

1. Enable auto VoIP for all the interfaces in the device.
   a. Select QoS > DiffServ > Auto VoIP. A screen similar to the following displays.

   ![Auto VoIP Configuration](image)

   b. Select the check box in the first row to select all the interfaces.
   c. In the Auto VoIP Mode field, select Enable. A screen similar to the following displays.

   ![Auto VoIP Configuration](image)

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

   ![Auto VoIP Configuration](image)
DiffServ for IPv6

This feature extends the existing QoS ACL and DiffServ functionality by providing support for IPv6 packet classification.

Figure 23. 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 policyicmpv6 to interfaces 1/0/1, 1/0/2 and 1/0/3:

(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# service-policy in policyicmpv6
(Netgear Switch) (Interface 1/0/1)# exit

(Netgear Switch) (Config)# interface 1/0/2
(Netgear Switch) (Interface 1/0/2)# service-policy in policyicmpv6
(Netgear Switch) (Interface 1/0/2)# exit

(Netgear Switch) (Config)# interface 1/0/3
(Netgear Switch) (Interface 1/0/3)# service-policy in policyicmpv6
(Netgear Switch) (Interface 1/0/3)# exit

Web Interface: Configure DiffServ for IPv6

1. Create the IPv6 class classicmpv6.
a. Select QoS > DiffServ > Advanced > IPv6 Class Configuration. A screen similar to the following displays.

b. In the Class Name field, enter classicmpv6.

c. In the Class Type list, select All. A screen similar to the following displays.

d. Click Add to create the IPv6 class. A screen similar to the following displays.

2. Define matching criteria as protocol ICMPv6.
   a. Select QoS > DiffServ > Advanced > IPv6 Class Configuration. A screen similar to the following displays.
b. Click the class `classicmpv6`. A screen similar to the following displays.

![DiffServ Configuration Screen](image1)

- Click the class `classicmpv6`. A screen similar to the following displays.
- Select the Protocol Type radio button, select Other, and enter 58. A screen similar to the following displays.

![Protocol Type Configuration Screen](image2)

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

![Apply Configuration Screen](image3)

3. Create the policy `policyicmpv6`, and associate the previously created class `classicmpv6`. 

---

204 | Chapter 12. DiffServ
a. Select QoS > DiffServ > Advanced > Policy Configuration. A screen similar to the following displays.

![DiffServ Policy Configuration Screen]

b. In the Policy Name field, enter policyicmpv6.
c. In the Policy Type list, select In.
d. In the Member Class list, select classicmpv6. A screen similar to the following displays.

![DiffServ Policy Configuration Screen with classicmpv6 selected]
e. Click Add.

4. Set the attribute as assign queue 6.

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

![DiffServ Policy Configuration Screen with assign queue 6]

Chapter 12. DiffServ | 205
b. Click the policy `policyicmpv6`. A screen similar to the following displays.

![Policy Configuration](image)

In the **Assign Queue** list, select 6.

![Policy Class Configuration](image)

d. Click **Apply**.

5. Attach the policy `policyicmpv6` to interfaces 1/0/1, 1/0/2, and 1/0/3.
a. Select **QoS > DiffServ > Advanced > Service Interface Configuration**. A screen similar to the following displays.

b. In the **Policy Name** list, select **policyicmpv6**.

c. Select the Interface 1/0/1, 1/0/2, and 1/0/3 check boxes. A screen similar to the following displays.

d. Click **Apply**. A screen similar to the following displays.
Color Conform Policy

This example shows how to create a policy to police the traffic to a committed rate. The packets with IP precedence value of 7 are colored green to ensure that these packets are the last to be dropped when there is congestion. The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure a Color Conform Policy

1. Create a VLAN 5 and configure ports 1/0/13 and 1/0/25 as its members.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 5
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#vlan participation include 5
(Netgear Switch) (Interface 1/0/13)#vlan tagging 5
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#interface 1/0/25
(Netgear Switch) (Interface 1/0/25)#vlan participation include 5
(Netgear Switch) (Interface 1/0/25)#vlan tagging 5
(Netgear Switch) (Interface 1/0/25)#exit
```

2. Create classes class_vlan and class_color.

   **Note:** DiffServ service is enabled by default.

```
(Netgear Switch) (Config)#class-map match-all class_vlan
(Netgear Switch) (Config-classmap)#match vlan 5
(Netgear Switch) (Config-classmap)#exit
(Netgear Switch) (Config)#class-map match-all class_color
(Netgear Switch) (Config-classmap)#match ip precedence 7
(Netgear Switch) (Config-classmap)#exit
```

3. Create a policy to police the traffic to a rate of 1000 kbps with an allowed burst size of 64 KB. Furthermore, the packets with IP precedence value of 7 will be colored green. That
means these packets will be the last packets to be dropped in the event of congestion beyond the policed rate.

(Netgear Switch) (Config)#policy-map policy_vlan in
(Netgear Switch) (Config-policy-map)#class class_vlan
(Netgear Switch) (Config-policy-classmap)#police-simple 1000 64 conform-action transmit violate-action drop
(Netgear Switch) (Config-policy-classmap)#conform-color class_color
(Netgear Switch) (Config-policy-classmap)#exit
(Netgear Switch) (Config-policy-map)#exit

4. Apply this policy to port 1/0/13.

(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#service-policy in policy_vlan
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#exit

Web Interface: Configure a Color Conform Policy

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

   ![VLAN Configuration Screen](image)

   b. In the **VLAN ID** field, enter **5**.
   c. Click **Add**.

2. Add ports 1/0/13 and 1/0/25 to VLAN 5.
a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays.

![VLAN Membership Screen]

b. In the **VLAN ID** list, select 5.

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

d. Click the gray boxes under ports 13 and 25 until T displays. The T specifies that the egress packet is tagged for the port.

e. Click **Apply**.

3. Create a class class_vlan:

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

![Class Configuration Screen]

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**.

![DiffServ Wizard](image1)

- **Class Name**
  - **Class Name**: class_vlan
  - **Class Type**: All

- **DiffServ Class Configuration**
  - VLAN: 5

- Click **Apply**.

4. Create a class **class_color**.
   a. Select **QoS > DiffServ > Advanced > Class Configuration**. A screen similar to the following displays.

![DiffServ Wizard](image2)

- **Class Name**
  - **Class Name**: class_color
  - **Class Type**: All
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.

   ![DiffServ Class Configuration Image]

   d. Click class_color to configure this class. A screen similar to the following displays:

   ![DiffServ Class Configuration Image]

   e. Under Diffserv Class Configuration, in the Precedence Value list, select 7.

   f. Click Apply.

5. Create a policy policy_vlan.
a. Select QoS > DiffServ > Advanced > Policy Configuration. A screen similar to the following displays.

b. In the Policy Name field, enter policy_vlan.

c. In the Policy Type list, select In.

d. Click Add.

6. Associate policy_vlan with class_vlan.

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

b. Under Policy Configuration, scroll down and select the policy_vlan check box.

c. In the Member Class field, enter class_vlan.

d. Click Apply.

7. Configure policy_vlan.
a. Select QoS > DiffServ > Advanced > Policy Configuration. Click policy_vlan. A screen similar to the following displays.

b. Select the Simple Policy radio button.

c. In the Color Mode list, select Color Aware.

d. In the Color Conform Class list, select class_color.

e. In the Committed Rates field, enter 1000.

f. In the Committed Burst Size field, enter 64.

g. For Conform Action, select the Send radio button.

h. For Violate Action, select the Drop radio button.

i. Click Apply.

8. Apply policy_vlan to interface 1/0/13.
a. Select **QoS > DiffServ > Advanced > Service Interface Configuration**. A screen similar to the following displays.

```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Policy Name</th>
<th>Direction</th>
<th>Operational Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/13</td>
<td>policy_vlan</td>
<td>In</td>
<td></td>
</tr>
<tr>
<td>1/0/2</td>
<td></td>
<td>In</td>
<td></td>
</tr>
<tr>
<td>1/0/3</td>
<td></td>
<td>In</td>
<td></td>
</tr>
<tr>
<td>1/0/4</td>
<td></td>
<td>In</td>
<td></td>
</tr>
<tr>
<td>1/0/5</td>
<td></td>
<td>In</td>
<td></td>
</tr>
<tr>
<td>1/0/6</td>
<td></td>
<td>In</td>
<td></td>
</tr>
<tr>
<td>1/0/7</td>
<td></td>
<td>In</td>
<td></td>
</tr>
<tr>
<td>1/0/8</td>
<td></td>
<td>In</td>
<td></td>
</tr>
<tr>
<td>1/0/9</td>
<td></td>
<td>In</td>
<td></td>
</tr>
<tr>
<td>1/0/10</td>
<td></td>
<td>In</td>
<td></td>
</tr>
<tr>
<td>1/0/11</td>
<td></td>
<td>In</td>
<td></td>
</tr>
<tr>
<td>1/0/12</td>
<td></td>
<td>In</td>
<td></td>
</tr>
<tr>
<td>1/0/13</td>
<td></td>
<td>In</td>
<td></td>
</tr>
</tbody>
</table>
```

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.
This chapter provides the following examples:

- **IGMP Snooping**
- *Show igmpsnooping* on page 217
- *Show mac-address-table igmpsnooping* on page 218
- **External Multicast Router** on page 219
- **Multicast Router Using VLAN** on page 220
- **IGMP Querier** on page 221
- **Enable IGMP Querier** on page 222
- *Show IGMP Querier Status* on page 225

**IGMP**:

- Uses version 3 of IGMP.
- Includes snooping.
- Snooping can be enabled per VLAN.

**IGMP Snooping**

The following are examples of the commands used in the IGMP snooping feature.

**CLI: Enable IGMP Snooping**

The following example shows how to enable IGMP snooping.

```plaintext
(Netgear Switch) #config
(Netgear Switch) (Config)#set igmp
(Netgear Switch) (Config)# set igmp unknown-multicast filter
(Netgear Switch) (Config)#exit
```
Web Interface: Enable IGMP Snooping

1. Configure IGMP snooping:
   a. Select **Switching > Multicast > IGMP Snooping Configuration**. A screen similar to the following displays.

   ![IGMP Snooping Configuration Screen]

   b. For Admin Mode select the **Enable** radio button.
   c. For Unknown Multicast Filtering, select the **Enable** radio button.
   d. Click **Apply**.

Show igmpsnooping

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

CLI: Show igmpsnooping

```
(Netgear Switch) #show igmpsnooping
Admin Mode................................. Disable
Unknown Multicast Filtering.............. Disable
Multicast Control Frame Count............ 0
Interfaces Enabled for IGMP Snooping..... None
VLANs enabled for IGMP snooping......... None
```
Web Interface: Show igmpsnooping

Select **Switching > Multicast > IGMP Snooping Configuration**. A screen similar to the following displays.

```
Show mac-address-table igmpsnooping

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

**CLI: Show mac-address-table igmpsnooping**

```
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:01:01:00:5E:00:01:16</td>
<td>Dynamic Network Assist</td>
<td>Fwd: 1/0/47</td>
</tr>
<tr>
<td>00:01:01:00:5E:00:01:18</td>
<td>Dynamic Network Assist</td>
<td>Fwd: 1/0/47</td>
</tr>
<tr>
<td>00:01:01:00:5E:37:96:D0</td>
<td>Dynamic Network Assist</td>
<td>Fwd: 1/0/47</td>
</tr>
<tr>
<td>00:01:01:00:5E:7F:FF:FA</td>
<td>Dynamic Network Assist</td>
<td>Fwd: 1/0/47</td>
</tr>
<tr>
<td>00:01:01:00:5E:7F:FF:FE</td>
<td>Dynamic Network Assist</td>
<td>Fwd: 1/0/47</td>
</tr>
</tbody>
</table>
Web Interface: Show mac-address-table igmpsnooping

Select Switching > Multicast > IGMP Snooping Table. A screen similar to the following displays.

External Multicast Router

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

CLI: Configure the Switch with an External Multicast Router

This example configures the interface as the one the multicast router is attached to. All IGMP packets snooped by the switch is forwarded to the multicast router reachable from this interface.

(Netgear Switch)(Interface 1/0/3)# set igmp mrouter interface
Web Interface: Configure the Switch with an External Multicast Router

1. Select Switching > Multicast > Multicast Router Configuration. A screen similar to the following displays.

   ![IGMP Snooping Interface Configuration]

2. Under Multicast Router Configuration, scroll down and select the Interface 1/0/3 check box. Now 1/0/3 appears in the Interface field at the top.

3. In the Admin Mode field, select Enable.

4. Click Apply.

Multicast Router Using VLAN

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

CLI: Configure the Switch with a Multicast Router Using VLAN

This example configures the interface to forward only the snooped IGMP packets that come from VLAN ID (<VLAN Id>) to the multicast router attached to this interface.

```
(Netgear Switch)(Interface 1/0/3)# set igmp mrouter 2
```
Web Interface: Configure the Switch with a Multicast Router Using VLAN

1. Select Switching > Multicast > Multicast Router VLAN Configuration. A screen similar to the following displays.

```
Multicast Router VLAN Configuration

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Multicast Router</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Enable</td>
</tr>
</tbody>
</table>
```

2. Under Multicast Router VLAN Configuration, scroll down and select the Interface 1/0/3 check box.

3. Enter the following information in the Multicast Router VLAN Configuration.
   - In the VLAN ID field, enter 2.
   - In the Multicast Router field, select Enable.

4. Click Apply.

IGMP Querier

When the switch is used in network applications where video services such as IPTV, video streaming, and gaming are deployed, the video traffic is normally flooded to all connected ports because such traffic packets usually have multicast Ethernet addresses. IGMP snooping can be enabled to create a multicast group to direct that traffic only to those users that require it.

However, the IGMP snooping operation usually requires an extra network device—usually a router—that can generate an IGMP membership query and solicit interested nodes to
respond. With the built-in IGMP querier feature inside the switch, such an external device is no longer needed.

**Figure 24. 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.

```plaintext
(Netgear switch) #vlan database
(Netgear switch) (vlan)#set igmp 1
(Netgear switch) (vlan)#set igmp querier 1
(Netgear switch) (vlan)#exit
(Netgear switch) #config
(Netgear switch) (config)#set igmp querier
(Netgear switch) (config)#set igmp querier address 10.10.10.1
(Netgear switch) (config)#exit
```

**Web Interface: Enable IGMP Querier**

1. Select **Switching > Multicast > IGMP VLAN Configuration**. A screen similar to the following displays.

2. Enable IGMP snooping on VLAN 1.
   a. Select **Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration**. A screen similar to the following displays.

   b. Enter the following information:
   - In the **VLAN ID** field, enter *1*.
   - In the **Admin Mode** field, select **Enable**.
c. Click Add.

3. Enable the IGMP snooping querier globally.
   a. Select Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration. A screen similar to the following displays.
   
   ![IGMP Snooping Querier Configuration Screen]
   
   b. Enter the following information:
      - For Querier Admin Mode, select the Enable radio button.
      - In the Querier IP Address field, enter 10.10.10.1.
   
   c. Click Apply.

4. Enable the IGMP snooping querier on VLAN 1.
   a. Select Switching > Multicast > IGMP Snooping Querier VLAN Configuration. A screen similar to the following displays.
   
   ![IGMP Snooping Querier VLAN Configuration Screen]
   
   b. In the VLAN ID field, enter 1.

5. Click Add.
Show IGMP Querier Status

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

CLI: Show IGMP Querier Status

To see the IGMP querier status, use the following command.

```
(Netgear Switch) #show igmpsnooping querier vlan 1
VLAN 1 : IGMP Snooping querier status
----------------------------------------------
IGMP Snooping Querier VLAN Mode............ Enable
Querier Election Participate Mode.......... Disable
Querier VLAN Address....................... 0.0.0.0
Operational State........................... Disabled
Operational version......................... 2
```

The command shows that the IGMP admin mode is Active. The mode is controlled by the set igmp command. If the mode is inactive, no query packet is sent.

Web Interface: Show IGMP Querier Status

1. Select Switching > Multicast > IGMP Snooping Configuration. A screen similar to the following displays.

2. Click Refresh.
This chapter provides the following examples:

- Configure MVR in Compatible Mode
- Configure MVR in Dynamic Mode

The IGMP Layer 3 protocol is widely used for IPv4 network multicasting. In Layer 2 networks, the IGMP protocol uses resources inefficiently. For example, a Layer 2 switch multicasts traffic to all ports even if there are receivers connected to only a few ports.

To fix this problem, the IGMP Snooping protocol was developed. But the problem reappears when receivers are in different VLANs. Multicast VLAN Registration (MVR) is intended to solve the problem of receivers in different VLANs. It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.

MVR, like the IGMP Snooping protocol, allows a Layer 2 switch to snoop on the IGMP control protocol. Both protocols operate independently of each other. Both protocols can be enabled on the switch interfaces at the same time. In such a case, MVR listens to the join and report messages only for groups configured statically. All other groups are managed by IGMP snooping.

There are two types of MVR ports: source and receiver.

- The source port is the port to which the multicast traffic flows using the multicast VLAN.
- The receiver port is the port where a listening host is connected to the switch. It can utilize any (or no) VLAN, except the multicast VLAN. This implies that the MVR switch performs VLAN tag substitution from the multicast VLAN source port to the VLAN tag used by the receiver port.

The Multicast VLAN is the VLAN that is configured in the specific network for MVR purposes. It has to be manually specified by the operator for all source ports in the network. It is a VLAN that is used to transfer multicast traffic over the network to avoid duplication of
multicast streams for clients in different VLANs. A diagram of a network configured for MVR is shown in the following illustration. SP is the source port and RP is the receiver port.

![Diagram of a network configured for MVR](image)

**Figure 25. Network configured for MVR**

**Note:** The following examples show how to configure the MVR on the MVR switch (GSM7212P in this case).

**Configure MVR in Compatible Mode**

In compatible mode, the MVR switch does not learn multicast groups; the groups have to be configured by the operator as the MVR does not forward IGMP reports from the hosts (RP port) to the IGMP router (SP port). To operate in this mode, the IGMP router has to be statically configured to transmit all required multicast streams to the MVR switch.
CLI: Configure MVR in Compatible Mode

1. Create MVlan, VLAN1, VLAN2, and VLAN3.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 999,1001, 1002, 1003
(Netgear Switch) (Vlan)#vlan name 999 mVlan
(Netgear Switch) (Vlan)#vlan name 1001 Vlan1
(Netgear Switch) (Vlan)#vlan name 1002 Vlan2
(Netgear Switch) (Vlan)#vlan name 1003 Vlan3
(Netgear Switch) (Vlan)#exit
```

2. Enable MVR, configure VLAN 999 as a multicast VLAN, and add group 224.1.2.3 to MVR.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#mvr
(Netgear Switch) (Config)#mvr vlan 999
(Netgear Switch) (Config)#mvr group 224.1.2.3
```

3. Configure multicast VLAN on the source port.

```
(Netgear Switch) (Config)#interface 0/9
(Netgear Switch) (Interface 0/9)#vlan participation include 999
(Netgear Switch) (Interface 0/9)#vlan tagging 999
(Netgear Switch) (Interface 0/9)#mvr
(Netgear Switch) (Interface 0/9)#mvr type source
(Netgear Switch) (Interface 0/9)#exit
```

4. Configure the receive ports.
Note: The receive port can participate in only one VLAN.

(Netgear Switch) (Config)#interface 0/1
(Netgear Switch) (Interface 0/1)#vlan participation include 1001
(Netgear Switch) (Interface 0/1)#vlan pvid 1001
(Netgear Switch) (Interface 0/1)#vlan participation exclude 1
(Netgear Switch) (Interface 0/1)#mvr
(Netgear Switch) (Interface 0/1)#mvr type receiver
(Netgear Switch) (Interface 0/1)#mvr vlan 999 group 224.1.2.3
(Netgear Switch) (Interface 0/1)#exit

(Netgear Switch) (Config)#interface 0/5
(Netgear Switch) (Interface 0/5)#vlan participation include 1002
(Netgear Switch) (Interface 0/5)#vlan pvid 1002
(Netgear Switch) (Interface 0/5)#vlan participation exclude 1
(Netgear Switch) (Interface 0/5)#mvr
(Netgear Switch) (Interface 0/5)#mvr type 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 include 1003
(Netgear Switch) (Interface 0/7)#vlan pvid 1003
(Netgear Switch) (Interface 0/7)#vlan participation exclude 1
(Netgear Switch) (Interface 0/7)#mvr
(Netgear Switch) (Interface 0/7)#mvr type receiver
(Netgear Switch) (Interface 0/7)#mvr vlan 999 group 224.1.2.3
(Netgear Switch) (Interface 0/7)#exit
5. Show mvr status.

(Netgear Switch) #show mvr
MVR Running........................ TRUE
MVR multicast VLAN............... 999
MVR Max Multicast Groups........ 256
MVR Current multicast groups.... 1
MVR Global query response time... 5 (tenths of sec)
MVR Mode.......................... compatible

(Netgear Switch) #show mvr interface

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Status</th>
<th>Immediate Leave</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>RECEIVER</td>
<td>ACTIVE/InVLAN</td>
<td>DISABLED</td>
</tr>
<tr>
<td>0/5</td>
<td>RECEIVER</td>
<td>ACTIVE/InVLAN</td>
<td>DISABLED</td>
</tr>
<tr>
<td>0/7</td>
<td>RECEIVER</td>
<td>ACTIVE/InVLAN</td>
<td>DISABLED</td>
</tr>
<tr>
<td>0/9</td>
<td>SOURCE</td>
<td>ACTIVE/InVLAN</td>
<td>DISABLED</td>
</tr>
</tbody>
</table>

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:

   ![VLAN Configuration Screen]

   b. In the VLAN ID field, enter 999, and in the VLAN Name field, enter mVlan.
   c. Click Add.
   d. Repeat step b and c to create VLAN1 1001, VLAN2 1002, and VLAN3 1003.
2. Add port 9 into MVLAN 999 with tagged mode.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays:

   b. In the VLAN ID list, select **999**.
   c. Click **Unit 1**. The ports display.
   d. Click the gray box under port 9 until **T** displays. The **T** specifies that the egress packet is tagged for the ports.
   e. Click **Apply** to save the settings.
   f. Repeat steps from **b** to **e**, add port 0/1 to VLAN1 1001, add port 0/5 to VLAN2 1002, and add port 0/7 to VLAN3 1003.

3. Enable MVR and multicast VLAN
   a. Select **Switching > MVR > Basic > MVR Configuration**. A screen similar to the following displays:

   b. For MVR Running, select **Enable**.
   c. In the MVR Multicast VLAN field, enter **999**.
   d. Click **Apply**.
4. Add multicast group 224.1.2.3 to MVR. 
   a. Select **Switching > MVR > Basic > MVR Group Configuration**. A screen similar to the following displays:

   ![MVR Group Configuration](image1)

   b. In the MVR Group IP field, enter **224.1.2.3**.
   c. Click **Add**.

5. Configure a receiver on interface 0/1, 0/5, and 0/7.
   a. Select **Switching > MVR > Basic > MVR Interface Configuration**. A screen similar to the following displays:

   ![MVR Interface Configuration](image2)

   b. Under MVR Interface Configuration, scroll down and select the Interface 0/1, 0/5 and 0/7 check boxes.
   c. Enter the following information:
      - In the Admin Mode list, select **Enable**.
      - In the Type list, select **Receiver**.
   d. Click **Apply** to save the settings.
6. Configure source interface.
   a. Select Switching > MVR > Basic > MVR Interface Configuration. A screen similar to the following displays:

   ![MVR Interface Configuration](image)

   b. Under MVR Interface Configuration, scroll down and select the Interface 0/9 check box.
   c. Enter the following information:
      - In the Admin Mode list, select **Enable**.
      - In the Type list, select **source**.
   d. Click **Apply** to save the settings.

7. Configure MVR Group Membership.
   a. Select Switching > VLAN > Advanced > VLAN Membership. A screen similar to the following displays:

   ![MVR Group Membership](image)

   b. In the Group IP list, select **224.1.2.3**.
   c. Click **Unit 1**. The ports display.
   d. Click the gray boxes under ports 1, 5, and 7. (Port 9 is already in MVR group 224.1.2.3 because it is configured as the source port.)
   e. Click **Apply** to save the settings.
Configure MVR in Dynamic Mode

**CLI: Configure MVR in Dynamic Mode**

In dynamic mode, the MVR switch learns existing multicast groups by snooping the IGMP queries from router on source ports and forwarding the IGMP reports from the hosts to the IGMP router on the Multicast VLAN (with appropriate translation of the VLAN ID).

1. Create MVLAN, VLAN1, VLAN2, and VLAN3.

    (Netgear Switch) #vlan database
    (Netgear Switch) (Vlan)#vlan 999,1001, 1002, 1003
    (Netgear Switch) (Vlan)#vlan name 999 mVlan
    (Netgear Switch) (Vlan)#vlan name 1001 Vlan1
    (Netgear Switch) (Vlan)#vlan name 1002 Vlan2
    (Netgear Switch) (Vlan)#vlan name 1003 Vlan3
    (Netgear Switch) (Vlan)#exit

2. Enable MVR, configure VLAN 999 as a multicast VLAN, and add group 224.1.2.3 to MVR.

    (Netgear Switch) #config
    (Netgear Switch) (Config)#mvr
    (Netgear Switch) (Config)#mvr vlan 999
    (Netgear Switch) (Config)#mvr group 224.1.2.3

3. Configure MVR in dynamic mode.

    (Netgear Switch) (Config)#mvr mode dynamic

4. Configure multicast VLAN on the source port.

    (Netgear Switch) (Config)#interface 0/9
    (Netgear Switch) (Interface 0/9)#vlan participation include 999
    (Netgear Switch) (Interface 0/9)#vlan tagging 999
    (Netgear Switch) (Interface 0/9)#mvr
    (Netgear Switch) (Interface 0/9)#mvr type source
    (Netgear Switch) (Interface 0/9)#exit
5. Configure the receive ports.

**Note:** A receive port can participate in only one VLAN.

```plaintext
(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 include 1003
(Netgear Switch) (Interface 0/7)#vlan pvid 1003
(Netgear Switch) (Interface 0/7)#vlan participation exclude 1
(Netgear Switch) (Interface 0/7)#mvr
(Netgear Switch) (Interface 0/7)#mvr type receiver
(Netgear Switch) (Interface 0/7)#exit
```
6. Show the MVR status.

(Netgear Switch) #show mvr
MVR Running....................... TRUE
MVR multicast VLAN.............. 999
MVR Max Multicast Groups........ 256
MVR Current multicast groups.... 1
MVR Global query response time.. 5 (tenths of sec)
MVR Mode......................... compatible

(Netgear Switch) #show mvr interface

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Status</th>
<th>Immediate Leave</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>RECEIVER</td>
<td>ACTIVE/InVLAN</td>
<td>DISABLED</td>
</tr>
<tr>
<td>0/5</td>
<td>RECEIVER</td>
<td>ACTIVE/InVLAN</td>
<td>DISABLED</td>
</tr>
<tr>
<td>0/7</td>
<td>RECEIVER</td>
<td>ACTIVE/InVLAN</td>
<td>DISABLED</td>
</tr>
<tr>
<td>0/9</td>
<td>SOURCE</td>
<td>ACTIVE/InVLAN</td>
<td>DISABLED</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>MVR Group IP</th>
<th>Status</th>
<th>Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.1.2.3</td>
<td>ACTIVE</td>
<td>0/1(d)</td>
</tr>
</tbody>
</table>

Web Interface: Configure MVR in Dynamic Mode

1. Create MVLAN 999, VLAN1 1001, VLAN2 1002, and VLAN3 1003.
   a. Select Switching > VLAN > Basic > VLAN Configuration. A screen similar to the following displays:

   b. In the VLAN ID field, enter 999, and in the VLAN Name field, enter mVlan.
   c. Click Add.
   d. Repeat step b and c to create VLAN1 1001, VLAN2 1002, and VLAN3 1003.
   e. Add port 9 into MVLAN 999 with tagged mode.
f. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays:

<table>
<thead>
<tr>
<th>System</th>
<th>Switching</th>
<th>Routing</th>
<th>QoS</th>
<th>Security</th>
<th>Monitoring</th>
<th>Maintenance</th>
<th>Help</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>STP</td>
<td>Multicast</td>
<td>VLAN</td>
<td>Address Table</td>
<td>Ports</td>
<td>LAG</td>
<td>VLAN Membership</td>
<td>VLAN ID</td>
</tr>
<tr>
<td>Basic</td>
<td>Advanced</td>
<td>VLAN Configuration</td>
<td>VLAN Membership</td>
<td>VLAN Status</td>
<td>Port VLAN Configuration</td>
<td>MAC Based VLAN</td>
<td>Protocol Based VLAN</td>
<td>Group Configuration</td>
</tr>
<tr>
<td>VLAN Membership</td>
<td>VLAN ID</td>
<td>Group Operation</td>
<td>Untag All</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN ID</td>
<td>999</td>
<td>Group Operation</td>
<td>Untag All</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN Name</td>
<td>multiple</td>
<td>Untag All</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN Type</td>
<td>Static</td>
<td>Untag All</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN Tagging</td>
<td>Untag All</td>
<td>Untag All</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN Port Tagging</td>
<td>Untag All</td>
<td>Untag All</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port 1 2 3 4 5 6 7 8 9 10 11 12</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAG</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- In the VLAN ID list, select **999**.
- Click **Unit 1**. The ports display.
- Click the gray boxes under port 9 until T displays. The T specifies that the egress packet is tagged for the ports.
- Click **Apply** to save the settings.
- Repeat steps from b to e, add port 0/1 to VLAN1 1001, add port 0/5 to VLAN2 1002, and add port 0/7 to VLAN3 1003.

2. **Enable MVR and multicast VLAN.**

a. Select **Switching > MVR > Basic > MVR Configuration**. A screen similar to the following displays:

<table>
<thead>
<tr>
<th>System</th>
<th>Switching</th>
<th>Routing</th>
<th>QoS</th>
<th>Security</th>
<th>Monitoring</th>
<th>Maintenance</th>
<th>Help</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>STP</td>
<td>Multicast</td>
<td>VLAN</td>
<td>Address Table</td>
<td>Ports</td>
<td>LAG</td>
<td>MVR Configuration</td>
<td>MVR Running</td>
</tr>
<tr>
<td>Basic</td>
<td>Advanced</td>
<td>MVR Configuration</td>
<td>MVR Group Configuration</td>
<td>MVR Interface Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVR Configuration</td>
<td>MVR Running</td>
<td>MVR Multicast Vlan</td>
<td>MVR Max Multicast Groups</td>
<td>MVR Current Multicast Groups</td>
<td>MVR Global query response time</td>
<td>MVR Mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVR Running</td>
<td>Enable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVR Multicast Vlan</td>
<td>999</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVR Max Multicast Groups</td>
<td>256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVR Current Multicast Groups</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVR Global query response time</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVR Mode</td>
<td>Dynamic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- From the MVR Running list, select **Enable**.
- In the MVR Multicast Vlan field, enter **999**.
- From the MVR mode list, select **dynamic**.
- Click **Apply**.

3. **Add multicast group 224.1.2.3 to the MVR.**

a. Select **Switching > MVR > Basic > MVR Group Configuration**. A screen similar to the following displays:

<table>
<thead>
<tr>
<th>System</th>
<th>Switching</th>
<th>Routing</th>
<th>QoS</th>
<th>Security</th>
<th>Monitoring</th>
<th>Maintenance</th>
<th>Help</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>STP</td>
<td>Multicast</td>
<td>VLAN</td>
<td>Address Table</td>
<td>Ports</td>
<td>LAG</td>
<td>MVR Group Configuration</td>
<td>MVR Group IP</td>
</tr>
<tr>
<td>Basic</td>
<td>Advanced</td>
<td>MVR Configuration</td>
<td>MVR Group Configuration</td>
<td>MVR Interface Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVR Group Configuration</td>
<td>MVR Group IP</td>
<td>Status</td>
<td>Members</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVR Group IP</td>
<td>224.1.2.3</td>
<td>Status</td>
<td>Members</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
b. In the MVR Group IP field, enter 224.1.2.3.
c. Click Add.

4. Configure a receiver on interface 0/1, 0/5 and 0/7.
   a. Select Switching > MVR > Basic > MVR Interface Configuration. A screen similar to the following displays:
   
   ![MVR Interface Configuration Screen](image)

   b. Under MVR Interface Configuration, scroll down and select the Interface 0/1, 0/5 and 0/7 check boxes
   
   c. Enter the following information:
      - In the Admin Mode list, select Enable.
      - In the Type list, select Receiver.
   
   d. Click Apply to save the settings.

5. Configure a source interface.
   a. Select Switching > MVR > Basic > MVR Interface Configuration. A screen similar to the following displays:
   
   ![MVR Interface Configuration Screen](image)
b. Under MVR Interface Configuration, scroll down and select the Interface 0/9 check box.

c. Enter the following information:
   - In the Admin Mode list, select Enable.
   - In the Type list, select source.

d. Click Apply to save the settings.

6. After port 1 receives an IGMP report for multicast group 224.1.2.3, it is added into MVR group 224.1.2.3.

a. Select Switching > MVR > Advanced > MVR Group Membership. A screen similar to the following displays:
In this chapter, examples are provided for the following topics:

- Port Security
- Set the Dynamic and Static Limit on Port 1/0/1 on page 241
- Convert the Dynamic Address Learned from 1/0/1 to a Static Address on page 243
- Create a Static Address on page 244
- Protected Ports on page 244
- 802.1x Port Security on page 251
- Create a Guest VLAN on page 257
- Assign VLANs Using RADIUS on page 262
- Dynamic ARP Inspection on page 268
- Static Mapping on page 274
- DHCP Snooping on page 276
- Enter Static Binding into the Binding Database on page 279
- Maximum Rate of DHCP Messages on page 280
- IP Source Guard on page 282

Port Security

Port Security helps secure the network by preventing unknown devices from forwarding packets. When a link goes down, all dynamically locked addresses are freed. The port security feature offers the following benefits:

- You can limit the number of MAC addresses on a given port. Packets that have a matching MAC address (secure packets) are forwarded; all other packets (unsecure packets) are restricted.
- You can enable port security on a per port basis.

Port security implements two traffic filtering methods, dynamic locking and static locking. These methods can be used concurrently.

- **Dynamic locking.** You can specify the maximum number of MAC addresses that can be learned on a port. The maximum number of MAC addresses is platform dependent and is
given in the software Release Notes. After the limit is reached, additional MAC addresses are not learned. Only frames with an allowable source MAC addresses are forwarded.

**Note:** If you want to set a specific MAC address for a port, set the dynamic entries to 0, then allow only packets with a MAC address matching the MAC address in the static list.

Dynamically locked addresses can be converted to statically locked addresses. Dynamically locked MAC addresses are aged out if another packet with that address is not seen within the age-out time. You can set the time out value. Dynamically locked MAC addresses are eligible to be learned by another port. Static MAC addresses are not eligible for aging.

- **Static locking.** You can manually specify a list of static MAC addresses for a port. Dynamically locked addresses can be converted to statically locked addresses.

### Set the Dynamic and Static Limit on Port 1/0/1

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

**CLI: Set the Dynamic and Static Limit on Port 1/0/1**

```plaintext
(Netgear Switch) (Config)#port-security
Enable port-security globally
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#port-security
Enable port-security on port 1/0/1
(Netgear Switch) (Interface 1/0/1)#port-security max-dynamic 10
Set the dynamic limit to 10
(Netgear Switch) (Interface 1/0/1)#port-security max-static 3
Set the static limit to 3
(Netgear Switch) (Interface 1/0/1)#ex
(Netgear Switch) (Config)#ex
(Netgear Switch) #show port-security 1/0/1
```

<table>
<thead>
<tr>
<th>Intf</th>
<th>Admin</th>
<th>Dynamic Limit</th>
<th>Static Limit</th>
<th>Violation Trap Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/1</td>
<td>Disabled</td>
<td>10</td>
<td>3</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Web Interface: Set the Dynamic and Static Limit on Port 1/0/1

1. Select **Security > Traffic Control > Port Security > Port Administrator.** A screen similar to the following displays.

   ![Port Security Configuration](image)

   - Under Port Security Configuration, next to Port Security Mode, select the **Enable** radio button.
   - Click **Apply** to save the settings.

2. Set the dynamic and static limit on the port 1/0/1:
   a. Select **Security > Traffic Control > Port Security > Interface Configuration.** A screen similar to the following displays.

   ![Port Security Interface Configuration](image)

   - Scroll down and select the Interface 1/0/1 check box. Now 1/0/1 appears in the Interface field at the top.
   - 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**.
   - Click **Apply** to save the settings.
Convert the Dynamic Address Learned from 1/0/1 to a Static Address

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

**CLI: Convert the Dynamic Address Learned from 1/0/1 to the Static Address**

```
(Netgear Switch)(Interface 1/0/1)#port-security mac-address move
Convert the dynamic address learned from 1/0/1 to the static address
(Netgear Switch)(Interface 1/0/1)#exit
(Netgear Switch)(Config)#exit
(Netgear Switch)#show port-security static 1/0/1
Number of static MAC addresses configured: 3
Statically configured MAC Address VLAN ID
---------------------------------------------
00:0E:45:30:15:F3  1
00:13:46:EC:2F:62  1
00:14:6C:E8:81:23  1
```

**Web Interface: Convert the Dynamic Address Learned from 1/0/1 to the Static Address**

1. Select **Security > Traffic Control > Port Security > Dynamic MAC Address**. A screen similar to the following displays.

2. Under Port Security Configuration, in the **Port List** field, select 1/0/1.
3. Select the **Convert Dynamic Address to Static** check box.
4. Click **Apply** to save the settings.
Create a Static Address

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

CLI: Create a Static Address

```
(Netgear Switch) (Interface 1/0/1)#port-security mac-address 00:13:00:01:02:03
```

Web Interface: Create a Static Address

1. Select Security > Traffic Control > Port Security > Static MAC address. A screen similar to the following displays.

2. Under Port List, in the Interface list, select 1/0/1.

3. In the Static MAC Address section of the screen, enter the following information:
   - In the Static MAC Address field, enter 00:13:00:01:02:03.
   - In the Vlan ID list, select 3.

4. Click Add.

Protected Ports

This section describes how to set up protected ports on the switch. Some situations might require that traffic is prevented from being forwarded between any ports at Layer 2 so that one user cannot see the traffic of another user on the same switch. Protected ports can:

- Prevent traffic from being forwarded between protected ports.
- Allow traffic to be forwarded between a protected port and a non-protected port.
In following example, PC 1 and PC 2 can access the Internet as usual, but PC 1 cannot see the traffic that is generated by PC 2, that is, no traffic is forwarded between PC 1 and PC 2.

![Diagram showing a Layer 2 switch, PC 1, Internet, and PC 2 with IP addresses 192.168.1.192 and 192.168.1.252 respectively, and traffic flow from 10.100.5.34 to PC 1 and from PC 2 to 192.168.1.252.]

**Figure 26. Protected ports**

**CLI: Configure a Protected Port to Isolate Ports on the Switch**

1. Create one VLAN 192 including PC 1 and PC 2.

```
(Netgear Switch) #vlan database
(Netgear Switch) #vlan 192
(Netgear Switch) #vlan routing 192
(Netgear Switch) #exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/23
(Netgear Switch) (Interface 1/0/23)#vlan pvid 192
(Netgear Switch) (Interface 1/0/23)#vlan participation include 192
(Netgear Switch) (Interface 1/0/23)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan pvid 192
(Netgear Switch) (Interface 1/0/24)#vlan participation include 192
(Netgear Switch) (Interface 1/0/24)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface-vlan 192)#interface vlan 192
(Netgear Switch) (Interface-vlan 192)#routing
(Netgear Switch) (Interface-vlan 192)#ip address 192.168.1.254 255.255.255.0
(Netgear Switch) (Interface-vlan 192)#exit
```
2. Create one VLAN 202 connected to the Internet.

   (Netgear Switch) #vlan database
   (Netgear Switch) (Vlan)#vlan 202
   (Netgear Switch) (Vlan)#vlan routing 202
   (Netgear Switch) (Vlan)#exit
   (Netgear Switch) #configure
   (Netgear Switch) (Config)#interface 1/0/48
   (Netgear Switch) (Interface 1/0/48)#vlan pvid 202
   (Netgear Switch) (Interface 1/0/48)#vlan participation include 202
   (Netgear Switch) (Interface 1/0/48)#exit
   (Netgear Switch) (Config)#interface vlan 202
   (Netgear Switch) (Interface-vlan 202)#routing
   (Netgear Switch) (Interface-vlan 202)#ip address 10.100.5.34 255.255.255.0
   (Netgear Switch) (Interface-vlan 202)#exit

3. Create a DHCP pool to allocated IP addresses to PCs.

   (Netgear Switch) (config)#service dhcp
   (Netgear Switch) (config)#ip dhcp pool pool-a
   (Netgear Switch) (Config-dhcp-pool)#dns-server 12.7.210.170
   (Netgear Switch) (Config-dhcp-pool)#default-router 192.168.1.254
   (Netgear Switch) (Config-dhcp-pool)#network 192.168.1.0 255.255.255.0
   (Netgear Switch) (Config-dhcp-pool)#exit

4. Enable IP routing and configure a default route.

   (Netgear Switch)(config)#ip routing
   (Netgear Switch)(config)#ip route 0.0.0.0 0.0.0.0 10.100.5.252

5. Enable a protected port on 1/0/23 and 1/0/24.

   (Netgear Switch) (Config)#interface 1/0/23
   (Netgear Switch) (Interface 1/0/23)#switchport protected
   (Netgear Switch) (Interface 1/0/23)#exit
   (Netgear Switch) (Config)#interface 1/0/24
   (Netgear Switch) (Interface 1/0/24)#switchport protected
   (Netgear Switch) (Interface 1/0/24)#exit
Web Interface: Configure a Protected Port to Isolate Ports on the Switch

1. Create a DHCP pool:

   **Note:** This example assumes that the DHCP service is enabled. For information about how to enable the DHCP service, see the Web interface procedure in *Configure a DHCP Server in Dynamic Mode* on page 349.

   a. Select **System > Services > DHCP Server > DHCP Server Configuration**. A screen similar to the following displays.

   b. Under DHCP Pool Configuration, enter the following information:
      - In the **Pool Name** field, select **Create**.
      - In the **Pool Name** field, enter **pool-a**.
      - In the **Type of Binding** field, select **Dynamic**.
• In the Network Number field, enter 192.168.1.0.
• In the Network Mask field, enter 255.255.255.0.
• In the Days field, enter 1.
• Click Default Router Addresses. The DNS server address fields display. In the first Router Address field, enter 192.168.1.254.
• Click DNS Server Addresses. The router address fields display. In the first DNS Server Address field, enter 12.7.210.170.

c. Click Add.

2. Configure a VLAN and include ports 1/0/23 and 1/0/24 in the VLAN:
   a. Select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.

   ![VLAN Routing Wizard](image)

   b. Enter the following information:
      • In the Vlan ID field, enter 192.
      • In the IP Address field, enter 192.168.1.254.
      • In the Network Mask field, enter 255.255.255.0.
   c. Click Unit 1. The ports display:
      • Click the gray box under port 23 twice until U displays.
      • Click the gray box under port 24 twice until U displays.
      The U specifies that the egress packet is untagged for the port.
   d. Click Apply to save the VLAN that includes ports 23 and 24.

3. Configure a VLAN and include port 1/0/48 in the VLAN:
a. Select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.

![VLAN Routing Wizard Screen]

b. Enter the following information:
   • In the Vlan ID field, enter 202.
   • In the IP Address field, enter 10.100.5.34.
   • In the Network Mask field, enter 255.255.255.0.

c. Click Unit 1. The ports display:

d. Click the gray box under port 48 twice until U displays. The U specifies that the egress packet is untagged for the port.

e. Click Apply to save the VLAN that includes port 48.

4. Enable IP routing:

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

![IP Configuration Screen]

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

c. Click Apply to enable IP routing.

5. Configure default route for VLAN 202:
a. Select **Routing > Routing Table > Basic > Route Configuration**. A screen similar to the following displays.

![Routing Configuration Screen](image)

b. Under Configure Routes, in the **Route Type** list, select **Default Route**.

c. In the **Next Hop IP Address** field, enter **10.100.5.252**.

d. Click **Add** to add the route that is associated to VLAN 202 to the Learned Routes table.

6. Configure port 23 and port 24 as protected ports:

a. Select **Security > Traffic Control > Protected Port**. A screen similar to the following displays.

![Protected Ports Membership Screen](image)

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 27. Using 802.1x port security

The following example shows how to authenticate the dot1x users by a RADIUS server. The management IP address is 10.100.5.33/24. The example is shown as CLI commands and as a Web interface procedure.

**CLI: Authenticating dot1x Users by a RADIUS Server**

1. Assign an IP address to 1/0/19, and set force authorized mode to this port, and create a user name list dot1xList.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.1.1 255.255.255.0
(Netgear Switch) (Config)#dot1x system-auth-control
(Netgear Switch) (Config)#interface 1/0/19
(Netgear Switch) (Interface 1/0/19)#routing
(Netgear Switch) (Interface 1/0/19)#ip address 10.100.5.33 255.255.255.0
(Netgear Switch) (Interface 1/0/19)#dot1x port-control force-authorized
```
2. Use RADIUS to authenticate the dot1x users.

   (Netgear Switch) (Config)#aaa authentication dot1x default radius

3. Configure a RADIUS authentication server.

   (Netgear Switch) (Config)#radius server host auth 10.100.5.17

4. Configure the shared secret between the RADIUS client and the server.

   Netgear Switch) (Config)#radius server key auth 10.100.5.17
   Enter secret (16 characters max):123456
   Re-enter secret:123456

5. Set the RADIUS server as a primary server.

   (Netgear Switch) (Config)#radius server msgauth 10.100.5.17
   (Netgear Switch) (Config)#radius server primary 10.100.5.17


   (Netgear Switch) (Config)#radius accounting mode
   (Netgear Switch) (Config)#radius server host acct 10.100.5.17

7. Configure the shared secret between the accounting server and the client.

   (Netgear Switch) (Config)#radius server key acct 10.100.5.17
   Enter secret (16 characters max):123456
   Re-enter secret:123456

Web Interface: Authenticating dot1x Users by a RADIUS Server

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

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

c. Click Apply to save the settings.

2. Assign IP address 192.168.1.1/24 to the interface 1/0/1.

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

b. Under IP Interface Configuration, scroll down and select the Interface 1/0/1 check box. Now 1/0/1 appears in the Interface field at the top.

c. Enter the following information:
   - In the IP Address field, enter 192.168.1.1.
   - In the Subnet Mask field, enter 255.255.255.0.
   - In the Routing Mode field, select Enable.

d. Click Apply to save the settings.

3. Assign IP address 10.100.5.33/24 to interface 1/0/19:
a. Select **Routing > Advanced > IP Interface Configuration**. A screen similar to the following displays.

![IP Interface Configuration Screen](image)

b. Scroll down and select the interface **1/0/19** check box. Now 1/0/19 appears in the Interface field at the top.

c. Enter the following information:
   - In the **IP Address** field, enter **10.100.5.33**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Routing Mode** field, select **Enable**.

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

4. Create an authentication name list.
   a. Select **Security > Management Security > Login > Authentication List**. A screen similar to the following displays.

![Authentication List Screen](image)

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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Control Mode</th>
<th>Quiet Period (s)</th>
<th>Transient Period (s)</th>
<th>Supplicant Timeout (s)</th>
<th>Server Timeout (s)</th>
<th>Maximum Requests</th>
<th>Periodic Reauthentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/1</td>
<td>Force Authorized</td>
<td>50</td>
<td>30</td>
<td>30</td>
<td>30</td>
<td>2</td>
<td>Disable</td>
</tr>
<tr>
<td>1/0/2</td>
<td>Auto</td>
<td>60</td>
<td>30</td>
<td>30</td>
<td>30</td>
<td>2</td>
<td>Enable</td>
</tr>
</tbody>
</table>

b. Scroll down and select the Interface 1/0/19 check box. Now 1/0/19 appears in the Interface field at the top.

c. In the Control Mode list, select Force Authorized.

d. Click Apply to save the settings.

6. Enable dot1x on the switch.

a. Select Security > Port Authentication > Server Configuration. A screen similar to the following displays.

b. For Administrative Mode, select the Enable radio button.

c. In the Login list, select dot1xList.

d. Click Apply to save settings.

7. Configure the RADIUS authentication server.

a. Select Security > Management Security > Server Configuration. A screen similar to the following displays.

b. In the Server Address field, enter 10.100.5.17.
c. In the **Secret Configured** field, select **Yes**.

d. In the **Secret** field, enter **123456**.

e. In the **Primary Server** field, select **Yes**.

f. In the **Message Authenticator** field, select **Enable**.

g. Click **Add**.


   a. Select **Security > Management Security > RADIUS > Radius Configuration**. A screen similar to the following displays.

   ![Radius Configuration Screen](image)

   b. In the **Server Address** field, enter **10.100.5.17**.

   c. In the **Accounting Mode** field, select **Enable**.

   d. Click **Apply**.

9. Configure the accounting server.

   a. Select **Security > Management Security > RADIUS > Radius Accounting Server Configuration**. A screen similar to the following displays.

   ![Accounting Server Configuration Screen](image)

   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.

If a port is in port-based mode, and a client that does not support 802.1X is connected to an unauthorized port that has 802.1X enabled, the client does not respond to the 802.1X requests from the switch. The port remains in the unauthorized state, and the client is not granted access to the network. If the guest VLAN is configured for that port, then the port is placed in the configured guest VLAN and the port is moved to the authorized state, allowing access to the client after a certain amount of time (determined by the guest VLAN period). If the client attached is 802.1x aware, then this allows the client to respond to 802.1X requests from the switch.

For a port in MAC-based mode, if traffic from a unauthenticated client is noticed on a port then, if guest VLAN has been configured on the port, the guest VLAN timer is started for that client. If the client is 802.1x unaware and does not respond to any 802.1x requests, when the guest VLAN timer expires, the client is authenticated and associated with the guest VLAN. This ensures that traffic from the client is accepted and switched through the guest VLAN.

In this example, dot1x is enabled on all the ports so that all the hosts that are authorized are assigned to VLAN 1. On ports 1/0/1 and 1/0/24, guest VLAN is enabled. If guests connect to the port, they are assigned to VLAN 2000, so that guests cannot access the internal VLAN, but can access each other in the guest VLAN.
CLI: Create a Guest VLAN

1. Enter the following commands:

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

2. Create VLAN 2000, and have 1/0/1 and 1/0/24 as members of VLAN 2000.

   ```
   (Netgear Switch) (Config)#aaa authentication dot1x default radius
   (Netgear Switch) (Config)#dot1x system-auth-control
   (Netgear Switch) (Config)#radius server host auth 192.168.0.1
   (Netgear Switch) (Config)#radius server key auth 192.168.0.1
   Enter secret (16 characters max):12345
   Re-enter secret:12345
   (Netgear Switch) (Config)#interface 1/0/6
   (Netgear Switch) (Interface 1/0/6)#dot1x port-control force-authorized
   (Netgear Switch) (Interface 1/0/6)#exit
   (Netgear Switch) (Config)#interface 1/0/12
   (Netgear Switch) (Interface 1/0/12)#dot1x port-control force-authorized
   (Netgear Switch) (Interface 1/0/12)#exit
   ```

3. Enable dot1x and RADIUS on the switch.

   ```
   (Netgear Switch) (Config)#interface 1/0/1
   (Netgear Switch) (Interface 1/0/1)#dot1x guest-vlan 2000
   (Netgear Switch) (Interface 1/0/1)#exit
   (Netgear Switch) (Config)#interface 1/0/24
   (Netgear Switch) (Interface 1/0/24)#dot1x guest-vlan 2000
   (Netgear Switch) (Interface 1/0/24)#exit
   ```
4. Enable the guest VLAN on ports 1/0/1 and 1/0/24.

(Netgear Switch) #show dot1x detail 1/0/1
Protocol Version............................... 1
PAE Capabilities............................... Authenticator
Control Mode................................... auto
Authenticator PAE State....................... Authenticated
Backend Authentication State.............. Idle
Quiet Period (secs)............................ 60
Transmit Period (secs)......................... 30
Guest VLAN ID................................. 2000
Guest VLAN Period (secs)..................... 90
Supplicant Timeout (secs).................... 30
Server Timeout (secs).......................... 30
Maximum Requests............................. 2
VLAN Id........................................ 2000
VLAN Assigned Reason....................... Guest
Reauthentication Period (secs).............. 3600
Reauthentication Enabled..................... FALSE
Key Transmission Enabled..................... FALSE
Control Direction............................ both
Maximum Users................................ 16
Unauthenticated VLAN ID..................... 0
Session Timeout............................... 0
Session Termination Action.................. Default

Web Interface: Create a Guest VLAN

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

   b. In the VLAN ID field, enter 2000.
c. In the **VLAN Type** field, select **Static**.

d. Click **Add**.


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

   ![VLAN Membership Screen](image)

   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.

   ![Port Authentication Screen](image)

   b. Scroll down and select the Interface **1/0/6** and **1/0/12**, check boxes.
   
   c. In the **Control Mode** list, select **Force Authorized**.
   
   d. Click **Apply** to save settings.

4. Enable dot1x on the switch.
Make sure that 1/0/12 and 1/0/6 are configured as force authorized before you do this step; otherwise you cannot access the switch through the Web Interface.

a. Select Security > Port Authentication > Basic > 802.1x Configuration. A screen similar to the following displays.

![802.1X Configuration Screen](image)

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.

![Dot1x Authentication List](image)

b. Select the defaultList check box.

c. In the 1 list, select RADIUS.

d. Click Add.

6. Configure the RADIUS authentication server.
a. Select **Security > Management Security > Radius > Server Configuration**. A screen similar to the following displays.

b. In the **Radius Server IP Address** field, enter **192.168.0.1**.

c. In the **Secret Configured** field, select **Yes**.

d. In the **Secret** field, enter **12345**.

e. Click **Add**.

7. Configure the guest VLAN.

a. Select **Security > Port Authentication > Advanced > Port Authentication**. A screen similar to the following displays.

b. Scroll down and select the port 1/0/1 and 1/0/24 check boxes.

c. In the **Guest VLAN ID** field, enter **2000**.

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

### Assign VLANs Using RADIUS

This feature allows the client to connect from any port and be assigned to the appropriate VLAN assigned by the RADIUS server. This gives flexibility for the clients to move around the network without requiring the administrator to do static VLAN configuration. When multiple hosts are connected to the switch on the same port, only one host uses authentication. If any VLAN information is applied on the port based on the authenticated host, the VLAN applies that information to all the hosts that are connected to that port.
• After a port is in an authorized state, if any client initiates dot1x authentication, the port clears authenticated clients’ states, and in the process clears the VLAN assigned to the port (if any). Then the port continues with the new client authentication and authorization process.

• When a client authenticates itself initially on the network, the switch acts as the authenticator to the clients on the network and forwards the authentication request to the RADIUS server in the network.

For use in VLAN assignment, the following tunnel attributes are used:

• Tunnel-Type = VLAN (13)
• Tunnel-Medium-Type = 802
• Tunnel-Private-Group-ID = VLANID where VLANID is 12 bits, with a value between 1 and 4094.

![Figure 29. VLAN assignment using RADIUS](image)

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**


```
(Netgear Switch) #network protocol none
Changing protocol mode will reset ip configuration.
Are you sure you want to continue? (y/n) y
(Netgear Switch) #network parms 192.168.0.5 255.255.255.0
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 2000
(Netgear Switch) #exit
```
2. Enable dot1x authentication on the switch

   (Netgear Switch) (Config)#dot1x system-auth-control

3. Use the RADIUS as the authenticator.

   (Netgear Switch) (Config)#aaa authentication dot1x default radius

4. Enable the switch to accept VLAN assignment by the RADIUS server.

   (Netgear Switch) (Config)#authorization network radius

5. Set the RADIUS server IP address.

   (Netgear Switch) (Config)#radius server host auth 192.168.0.1

6. Set the NAS-IP address for the RADIUS server.

   (Netgear Switch) (Config)#radius server key auth 192.168.0.1
   Enter secret (16 characters max):12345
   Re-enter secret:12345
   Set the radius server key.
   (Netgear Switch) (Config)#radius server attribute 4 192.168.0.1

7. Force 1/0/6 to be authorized for it to connect to the RADIUS server.

   (Netgear Switch) (Config)#interface 1/0/6
   (Netgear Switch) (Interface 1/0/6)#dot1x port-control force-authorized
   (Netgear Switch) (Interface 1/0/6)#exit
8. Show the dot1x detail for 1/0/5.

```
(Netgear Switch) #show dot1x detail 1/0/5
Port........................................... 1/0/5
Protocol Version............................... 1
PAE Capabilities............................... Authenticator
Control Mode................................... auto
Authenticator PAE State....................... Authenticated
Backend Authentication State................... Idle
Quiet Period (secs)............................ 60
Transmit Period (secs)......................... 30
Guest VLAN ID................................ 0
Guest VLAN Period (secs)...................... 90
Supplicant Timeout (secs).................... 30
Server Timeout (secs)......................... 30
Maximum Requests............................ 2
VLAN Id........................................ 2000
VLAN Assigned Reason......................... RADIUS
Reauthentication Period (secs)................. 3600
Reauthentication Enabled.................... FALSE
Key Transmission Enabled.................... FALSE
Control Direction........................... both
Maximum Users................................ 16
Unauthenticated VLAN ID..................... 0
Session Timeout............................. 0
Session Termination Action................... Default
```

Web Interface: Assign VLANS Using RADIUS

1. Assign the IP address for the Web Management Interface.
   a. Select System > Management > Network Interface > IPv4 Network Configuration. A screen similar to the following displays.
b. For Current Network Configuration Protocol, select the None radio button.

c. In the IP Address field, enter 192.168.0.5.

d. In the Subnet Mask field, enter 255.255.255.0.

e. Click Apply.


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

   b. In the VLAN ID field, enter 2000.

   c. In the VLAN Type field, select Static.

   d. Click Add.

3. Set force authorized mode on ports 1/0/6 and 1/0/12.

   a. Select Security > Port Authentication > Advanced > Port Authentication. A screen similar to the following displays.

   b. Under Port Authentication, scroll down and select the 1/0/6 and 1/0/12 check boxes.

   c. In the Control Mode list, select Force Authorized.

   d. Click Apply to save settings.
4. Enable dot1x on the switch.

Make sure that 1/0/12 and 1/0/6 are configured as force authorized before you do this step; otherwise, you cannot access the switch through the Web Management Interface.

a. Select Security > Port Authentication > Basic > 802.1x Configuration. A screen similar to the following displays.

b. For Administrative Mode, select the Enable radio button.

c. For VLAN Assignment Mode, select the Enable radio button.

d. Click Apply to save settings.

5. Configure the dot1x authentication list.

a. Select Security > Management Security > Authentication List > Dot1x Authentication List. A screen similar to the following displays.

b. Select the defaultList check box.

c. In the 1 list, select RADIUS.

d. Click Add.

6. Configure the RADIUS authentication server.
a. Select **Security > Management Security > Radius > Server Configuration**. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>Radius Server IP Address</th>
<th>Radius Server Name</th>
<th>Current Port</th>
<th>Secret Configured</th>
<th>Secret</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.1</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

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 30. 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

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>VLAN</th>
<th>Interface</th>
<th>Type</th>
<th>Lease (Secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:16:76:A7:88:CC</td>
<td>192.168.10.86</td>
<td>1</td>
<td>1/0/2</td>
<td>DYNAMIC</td>
<td>86400</td>
</tr>
</tbody>
</table>
```

5. Enable ARP inspection in VLAN 1.

```
(Netgear Switch) (Config)# ip arp inspection vlan 1
```

Now all ARP packets received on ports that are members of the VLAN are copied to the CPU for ARP inspection. If there are trusted ports, you can configure them as trusted in the next step. ARP packets received on trusted ports are not copied to the CPU.

6. Configure port 1/0/1 as trusted.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip arp inspection trust
```

Now ARP packets from the DHCP client go through because there is a DHCP snooping entry; however ARP packets from the static client are dropped. It can be overcome by static configuration as described in Static Mapping on page 274.

**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.
      
```
[Image: DHCP Snooping Global Configuration]
```

   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.

![DHCP Snooping Global Configuration Screen](image)

b. In the **VLAN ID** field, enter 1.

c. In the **DHCP Snooping Mode** field, select **Enable**. A screen similar to the following displays.

![DHCP Snooping Global Configuration Screen](image)

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.

![DHCP Snooping Interface Configuration Screen](image)

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.

![DHCP Snooping Interface Configuration](image1.png)

4. **View the DHCP Snooping Binding table.**
   a. Select **Security > Control > DHCP Snooping Binding Configuration**. A screen similar to the following displays.

![DHCP Snooping Binding Configuration](image2.png)

5. **Enable ARP Inspection in VLAN 1.**
   a. Select **Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration**. A screen similar to the following displays.

![Dynamic ARP Inspection Configuration](image3.png)

   b. In the **VLAN ID** field, enter 1.
c. In the **Dynamic ARP Inspection** field, select **Enable**. A screen similar to the following displays.

![Dynamic ARP Inspection Configuration](image)

Now all the ARP packets received on the ports that are member of the VLAN are copied to the CPU for ARP inspection. If there are trusted ports, you can configure them as trusted in the next step. ARP packets received on the trusted ports are not copied to the CPU.

**Note:** Make sure the administrator PC has a DHCP snooping entry or can access the device through the trusted port for ARP. Otherwise, you might get disconnected from the device.

6. Configure port 1/0/1 as trusted.
   a. Select **Security > Control > Dynamic ARP Inspection > DAI Interface Configuration**.
   b. Select the Interface 1/0/1 check box.
   c. For the **Trust Mode**, select **Enable**.
d. Click **Apply**. A screen similar to the following displays.

Now ARP packets from the DHCP client will go through; however ARP packets from the static client are dropped, since it does not have a DHCP snooping entry. It can be overcome by static configuration as described in the following section, *Static Mapping* on page 274.

**Static Mapping**

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

**CLI: Configure Static Mapping**

1. Create an ARP ACL.

   ```
   (Netgear Switch) (Config)# arp access-list ArpFilter
   ```

2. Configure the rule to allow the static client.

   ```
   (Netgear Switch) (Config-arp-access-list)# permit ip host 192.168.10.2
   mac host 00:11:85:ee:54:e9
   ```

3. Configure ARP ACL used for VLAN 1.

   ```
   (Netgear Switch) (Config)# ip arp inspection filter ArpFilter vlan 1
   ```

4. Now the ARP packets from the static client will go through since it has an entry in the ARP ACL ARP packets from the DHCP client is also through since it has a DHCP snooping entry.

   This command can include the optional static keyword. If the **static** keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings. In this example, ARP packets from the DHCP client are dropped since it does not have a matching rule, though it has a DHCP snooping entry.
Web Interface: Configure Static Mapping

1. Create an ARP ACL.
   a. Select Security > Control > Dynamic ARP Inspection > DAI ACL Configuration.
   b. In the Name field, enter ArpFilter.
   c. Click Add. A screen similar to the following displays.

2. Configure a rule to allow the static client.
   b. In the ACL Name list, select ArpFilter.
   c. In the Source IP Address field, enter 192.168.10.2.
   d. In the Source MAC Address field, enter 00:11:85:EE:54:E9.
   e. Click Add. A screen similar to the following displays.

3. Configure the ARP ACL used for VLAN 1.
   a. Select Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration.
   b. In the ARP ACL Name field, enter ArpFilter.
DHCP Snooping

DHCP snooping is a security feature that monitors DHCP messages between a DHCP client and DHCP server to filter harmful DHCP messages 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.

![DHCP Snooping Diagram](image)

**Figure 31. DHCP Snooping**

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

**CLI: Configure DHCP Snooping**

1. Enable DHCP snooping globally.

   ```plaintext
   (Netgear Switch) (Config)# ip dhcp snooping
   ```
2. Enable DHCP snooping in a VLAN.

   (Netgear Switch) (Config)# ip dhcp snooping vlan 1

3. Configure the port through which the DHCP server is reached as trusted.

   (Netgear Switch) (Config)# interface 1/0/1
   (Netgear Switch) (Interface 1/0/1)# ip dhcp snooping trust

4. View the DHCP Snooping Binding table.

   (GSM7328S) #show ip dhcp snooping binding

   Total number of bindings: 1

   MAC Address       IP Address     VLAN   Interface    Type    Lease (Secs)
   -----------------  ---------------  ----  -----------  -------  -----------
   00:16:76:A7:88:CC    192.168.10.89     1        1/0/2  DYNAMIC        86400

Web Interface: Configure DHCP Snooping

1. Enable DHCP snooping globally:
   a. Select Security > Control > DHCP Snooping Global Configuration. A screen similar to the following displays.

   ![DHCP Snooping Global Configuration](image)

   b. For DHCP Snooping Mode, select Enable.
   c. Click Apply. A screen similar to the following displays:

   ![DHCP Snooping Mode](image)

2. Enable DHCP snooping in a VLAN.
a. Select Security > Control > DHCP Snooping Global Configuration. A screen similar to the following displays.

```
DHCP Snooping Global Configuration

DHCP Snooping Mode: [Disable, Enable]
MAC Address Validation: [Disable, Enable]

VLAN Configuration

VLAN ID  DHCP Snooping Mode
1  Enable
```

b. In the VLAN ID list, select 1.

c. For DHCP Snooping Mode, select the Enable radio button. A screen similar to the following displays.

```
DHCP Snooping Global Configuration

DHCP Snooping Mode: [Disable, Enable]
MAC Address Validation: [Disable, Enable]

VLAN Configuration

VLAN ID  DHCP Snooping Mode
1  Enable
```

d. Click Apply.

3. Configure the port through which DHCP server is reached as trusted.

a. Select Security > Control > DHCP Snooping Interface Configuration. A screen similar to the following displays.

```
DHCP Snooping Interface Configuration

Interface  Trust Mode  Looping Invalid Packets  Rate Limit(s)  Burst Interval(msec)
1/0/1  Enable  Disable  15  1
```

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

c. For Interface 1/0/1, in the Trust Mode field, select Enable.
d. Click **Apply**. A screen similar to the following displays.

![DHCP Snooping Interface Configuration](image)

4. View the DHCP Snooping Binding configuration.

Select **Security > Control > DHCP Snooping Binding Configuration**. A screen similar to the following displays.

![DHCP Snooping Binding Configuration](image)

**Enter Static Binding into the Binding Database**

You can also enter the static binding into the binding database.

**CLI: Enter Static Binding into the Binding Database**

1. Enter the DHCP snooping static binding.

```
(Netgear Switch) (Config)# ip dhcp snooping binding 00:11:11:11:11:11
vlan 1 192.168.10 .1 interface 1/0/2
```
2. Check to make sure the binding database has the static entry.

```
(GSM7328S) #show ip dhcp snooping binding
Total number of bindings:  2

MAC Address         IP Address     VLAN   Interface    Type    Lease (Secs)
------------------------     ---------------     --------  -----------  -------
00:11:11:11:11:11    192.168.10.1      1        1/0/2      STATIC
00:16:76:A7:88:CC  192.168.10.89    1        1/0/2      DYNAMIC        86348
```

Web Interface: Enter Static Binding into the Binding Database

1. Select **Security > Control > DHCP Snooping > Binding Configuration.**
2. Fill in the fields for the static binding and click **Apply.**
3. Check to make sure that the binding database shows the entry in the Static Binding Configuration table.

Maximum Rate of DHCP Messages

To prevent DHCP packets being used as DoS attachments when DHCP snooping is enabled, the snooping application enforces a rate limit for DHCP packets received on untrusted interfaces. DHCP snooping monitors the receive rate on each interface separately. If the receive rate exceeds the configured limit, DHCP snooping brings down the interface. The user must specify “no shutdown” on this interface to further work with that port.
CLI: Configure the Maximum Rate of DHCP Messages

1. Control the maximum rate of DHCP messages.

   (Netgear Switch) (Interface 1/0/2)# ip dhcp snooping limit rate 5

2. View the rate configured.

   (GSM7328S) #show ip dhcp snooping interfaces 1/0/2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust State</th>
<th>Rate Limit (pps)</th>
<th>Burst Interval (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/2</td>
<td>No</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

Web Interface: Configure the Maximum Rate of DHCP Messages

1. Select Security > Control > DHCP Snooping > Interface Configuration. A screen similar to the following displays:

2. Select the interface, fill in the Rate Limit (pps) field, and then click Apply.

   The screen shows the new rate limit for the interface.
IP Source Guard

IP Source Guard uses the DHCP snooping bindings database. When IP Source Guard is enabled, the switch drops incoming packets that do not match a binding in the bindings database. IP Source Guard can be configured to enforce just the source IP address or both the source IP address and source MAC address.

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

CLI: Configure Dynamic ARP Inspection

1. Enable DHCP snooping globally.

```
(Netgear Switch) (Config)# ip dhcp snooping
```
2. Enable DHCP snooping in a VLAN.

   (Netgear Switch) (Config)# ip dhcp snooping vlan 1

3. Configure the port through which the DHCP server is reached as trusted.

   (Netgear Switch) (Config)# interface 1/0/1
   (Netgear Switch) (Interface 1/0/1)# ip dhcp snooping trust

4. View the DHCP Snooping Binding table.

   (GSM7328S) #show ip dhcp snooping binding

   Total number of bindings: 1

   +-----------------+------------+----+----------+-------+------------+
   | MAC Address     | IP Address | VLAN| Interface | Type  | Lease (Secs) |
   +-----------------+------------+----+----------+-------+------------+
   | 00:16:76:A7:88:CC | 192.168.10.86 | 1  | 1/0/2    | DYNAMIC | 86400       |

   If the entry does not exist in the DHCP Snooping Binding table, it can statically added through the command `ip verify binding <mac-address> vlan <vlan id> <ip address> interface <interface id>` in global configuration mode.

5. Enable IP Source Guard in interface 1/0/2.

   (GSM7352Sv2) (Interface 1/0/2)#ip verify source port-security

   With this configuration, the device verifies both the source IP address and the source MAC address. If the port-security option is skipped, the device verifies only the source IP address.

Web Interface: Configure Dynamic ARP Inspection

1. Enable DHCP snooping globally.
   a. Select Security > Control > DHCP Snooping Global Configuration. A screen similar to the following displays.
b. For DHCP Snooping Mode, select the **Enable** radio button.

c. Click **Apply**.

2. Enable DHCP snooping in a VLAN.

a. Select **Security > Control > DHCP Snooping Global Configuration**. A screen similar to the following displays.

![DHCP Snooping Global Configuration](image)

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.

![VLAN Configuration](image)

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

![VLAN Configuration](image)

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.

![DHCP Snooping Interface Configuration](image1)

b. Select Interface 1/0/1 check box.
c. For interface 1/0/1, in the Trust Mode field, select Enable.
d. Click Apply. A screen similar to the following displays.

![DHCP Snooping Interface Configuration](image2)

4. View the DHCP Snooping Binding table.
   Select Security > Control > DHCP Snooping Binding Configuration. A screen similar to the following displays.

![DHCP Snooping Binding Configuration](image3)

5. Enable IP source guard in the interface 1/0/2.
   a. Select Security > Control > IP Source Guard > Interface Configuration.
   b. Select the Interface 1/0/2 check box.
   c. For the IPSG mode, select Enable.
d. Click **Apply**. A screen similar to the following displays.

6. Set up IP source guard static binding.
   a. Select **Security > Control > IP Source Guard > Binding Configuration**.
   b. Select the Interface 1/0/2 check box.
   c. In the **MAC Address** field, enter **00:05:05:05:05:05**.
   d. In the **VLAN ID** field, enter **1**.
   e. In the **IP Address** field, enter **192.168.10.80**.
   f. Click **Add**. A screen similar to the following displays.
SNTP

Simple Network Time Protocol

This chapter provides the following examples:

- Show SNTP (CLI Only)
- Configure SNTP on page 289
- Set the Time Zone (CLI Only) on page 291
- Set the Named SNTP Server on page 291

The SNTP feature offers these benefits:

- It can be used to synchronize network resources and for adaptation of NTP.
- SNTP provides synchronized network timestamp.
- It can be used in broadcast or unicast mode.
- It supports SNTP client implemented over UDP, which listens on port 123.

Show SNTP (CLI Only)

The following are examples of the commands used in the SNTP feature.

```
show sntp
```

(Netgear Switch Routing) #show sntp?

<cr> Press Enter to execute the command.
client Display SNTP Client Information.
server Display SNTP Server Information.
show sntp client

(client) #show sntp client

Client Supported Modes:  unicast broadcast
SNTP Version:  4
Port:  123
Client Mode:  unicast
Unicast Poll Interval:  6
Poll Timeout (seconds):  5
Poll Retry:  1

show sntp server

(client) #show sntp server

Server IP Address:  81.169.155.234
Server Type:  ipv4
Server Stratum:  3
Server Reference Id:  NTP Srv: 212.186.110.32
Server Mode:  Server
Server Maximum Entries:  3
Server Current Entries:  1

SNTP Servers
----------

IP Address:  81.169.155.234
Address Type:  IPV4
Priority:  1
Version:  4
Port:  123
Last Update Time:  MAY 18 04:59:13 2005
Last Attempt Time:  MAY 18 11:59:33 2005
Last Update Status:  Other
Total Unicast Requests:  1111
Failed Unicast Requests:  361
Configure SNTP

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

CLI: Configure SNTP

NETGEAR switches do not have a built-in real-time clock. However, it is possible to use SNTP to get the time from a public SNTP/NTP server over the Internet. You may need permission from those public time servers. The following steps configure SNTP on the switch:

1. Configure the SNTP server IP address. The IP address can be either from the public NTP server or your own. You can search the Internet to locate the public server. The servers available could be listed in domain-name format instead of address format. In that case, use the ping command on the PC to find the server’s IP address. The following example configures the SNTP server IP address to 208.14.208.19.

   (Netgear Switch) (Config)#sntp server 208.14.208.19

2. After configuring the IP address, enable SNTP client mode. The client mode can be either broadcast mode or unicast mode. If the NTP server is not your own, you must use unicast mode.

   (Netgear Switch) (Config)#sntp client mode unicast

3. Once SNTP client mode is enabled, the client waits for the polling interval to send the query to the server. The default value is approximately 1 minute. After this period, issue the show
command to confirm that the time has been received. The time will be used in all logging messages.

(Netgear Switch) #show sntp server
Server IP Address:                 208.14.208.19
Server Type:                       ipv4
Server Stratum:                    4
Server Reference Id:               NTP Srv: 208.14.208.3
Server Mode:                       Server
Server Maximum Entries:            3
Server Current Entries:            1
SNTP Servers
-----------
IP Address: 208.14.208.19
Address Type: IPV4
Priority: 1
Version: 4
Port: 123
Last Update Time: Mar 26 03:36:09 2006
Last Attempt Time: Mar 26 03:36:09 2006
Last Update Status: Success
Total Unicast Requests: 2
Failed Unicast Requests: 0

Web Interface: Configure SNTP

1. Configure the SNTP server.
   a. Select System > Management >Time > SNTP Server Configuration. A screen similar to the following displays.

   b. Enter the following information:
ProSafe Managed Switch

- In the **Server Type** field, select **IPV4**.
- In the **Address** field, enter **208.14.208.19**.
- In the **Port** field, enter **123**.
- In the **Priority** field, enter **1**.
- In the **Version** field, enter **4**.

c. Click **Add**.

2. Configure SNTP globally.
   
a. Select **System > Management > Time > SNTP Global Configuration**. A screen similar to the following displays.

b. Enter the following information:
   - For Client Mode, Select the **Unicast** radio button.
   - In the **Time Zone Name** field, enter **PST**.
   - In the **Offset Hours** field, enter **-8**.

c. Click **Apply**.

**Set the Time Zone (CLI Only)**

The SNTP/NTP server is set to Coordinated Universal Time (UTC) by default. The following example shows how to set the time zone to Pacific Standard Time (PST), which is 8 hours behind GMT/UTC.

```
(Netgear switch)(config)#clock timezone PST -8
```

**Set the Named SNTP Server**

The example is shown as CLI commands and as a Web interface procedure.
CLI: Set the Named SNTP Server

NETGEAR provides SNTP servers accessible by NETGEAR devices. Because NETGEAR might change IP addresses assigned to its time servers, it is best to access an SNTP server by DNS name instead of using a hard-coded IP address. The public time servers available are time-a, time-b, and time-c.

Enable a DNS name server and access a time server with the following commands:

```
(Netgear switch) (config)#ip domain-lookup
(Netgear switch) (config)#ip name-server 192.168.1.1
(Netgear switch) (config)#sntp server time-a.netgear.com
```

where 192.168.1.1 is the public network gateway IP address for your device.

This method of setting DNS name look-up can be used for any other applications that require a public IP address, for example, a RADIUS server.

Web Interface: Set the Named SNTP Server

1. Configure the SNTP server.
   a. Select System > Management > Time > SNTP Server Configuration. A screen similar to the following displays.

   ![SNTP Server Configuration Screen](image)

   b. Enter the following information:
      - In the Server Type list, select DNS.
      - In the Address field, enter time-f.netgear.com
      - In the Port field, enter 123.
      - In the Priority field, enter 1.
      - In the Version field, enter 4.
   c. Click Add.

2. Configure the DNS server.
a. Select System > Management > DNS > DNS Configuration. A screen similar to the following displays.

b. Enter the following information:
   - For DNS Status, select the Enable radio button
   - In the DNS Server field, enter 192.168.1.1.

c. Click Add.
This chapter provides the following examples:

- Traceroute
- Configuration Scripting on page 296
- Pre-Login Banner on page 299
- Port Mirroring on page 300
- Dual Image on page 301
- Outbound Telnet on page 304

**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 the packet passes through and how long it takes to get there. In this example, the packet takes 16 hops to reach its destination.
## CLI: Traceroute

```plaintext
(Netgear Switch) #traceroute?
<ipaddr>      Enter IP address.

(Netgear Switch) #traceroute 216.109.118.74 ?
<cr>    Press Enter to execute the command.
<port>        Enter port no.

(Netgear Switch) #traceroute 216.109.118.74

racing route over a maximum of 20 hops

<table>
<thead>
<tr>
<th>Hop</th>
<th>IP Address</th>
<th>RTT</th>
<th>Delay</th>
<th>Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.254.24.1</td>
<td>40 ms</td>
<td>9 ms</td>
<td>10 ms</td>
</tr>
<tr>
<td>2</td>
<td>10.254.253.1</td>
<td>30 ms</td>
<td>49 ms</td>
<td>21 ms</td>
</tr>
<tr>
<td>3</td>
<td>63.237.23.33</td>
<td>29 ms</td>
<td>10 ms</td>
<td>10 ms</td>
</tr>
<tr>
<td>4</td>
<td>63.144.4.1</td>
<td>39 ms</td>
<td>63 ms</td>
<td>67 ms</td>
</tr>
<tr>
<td>5</td>
<td>63.144.1.141</td>
<td>70 ms</td>
<td>50 ms</td>
<td>50 ms</td>
</tr>
<tr>
<td>6</td>
<td>205.171.21.89</td>
<td>39 ms</td>
<td>70 ms</td>
<td>50 ms</td>
</tr>
<tr>
<td>7</td>
<td>205.171.8.154</td>
<td>70 ms</td>
<td>50 ms</td>
<td>70 ms</td>
</tr>
<tr>
<td>8</td>
<td>205.171.8.222</td>
<td>70 ms</td>
<td>50 ms</td>
<td>80 ms</td>
</tr>
<tr>
<td>9</td>
<td>205.171.251.34</td>
<td>60 ms</td>
<td>90 ms</td>
<td>50 ms</td>
</tr>
<tr>
<td>10</td>
<td>209.244.219.181</td>
<td>60 ms</td>
<td>70 ms</td>
<td>70 ms</td>
</tr>
<tr>
<td>11</td>
<td>209.244.11.9</td>
<td>60 ms</td>
<td>60 ms</td>
<td>50 ms</td>
</tr>
<tr>
<td>12</td>
<td>4.68.121.146</td>
<td>50 ms</td>
<td>70 ms</td>
<td>60 ms</td>
</tr>
<tr>
<td>13</td>
<td>4.79.228.2</td>
<td>60 ms</td>
<td>60 ms</td>
<td>60 ms</td>
</tr>
<tr>
<td>14</td>
<td>216.115.96.185</td>
<td>110 ms</td>
<td>59 ms</td>
<td>70 ms</td>
</tr>
<tr>
<td>15</td>
<td>216.109.120.203</td>
<td>70 ms</td>
<td>66 ms</td>
<td>95 ms</td>
</tr>
<tr>
<td>16</td>
<td>216.109.118.74</td>
<td>78 ms</td>
<td>121 ms</td>
<td>69 ms</td>
</tr>
</tbody>
</table>
```
Web Interface: Traceroute

1. Select Maintenance > Troubleshooting > Traceroute. A screen similar to the following displays.

Use this screen to tell the switch to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. Once you click the Apply button, the switch will send three traceroute packets each hop, and the results will be displayed in the result table.

2. In the IP Address field, enter 216.109.118.74.

3. Click Apply.

Configuration Scripting

This section provides the following examples:

- script on page 297
- script list and script delete on page 297
- script apply running-config.scr on page 298
- Create a Configuration Script on page 298
- Upload a Configuration Script on page 298

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

```bash
(Netgear Switch) #script ?

apply       Applies configuration script to the switch.
delete      Deletes a configuration script file from the switch.
list        Lists all configuration script files present on the switch.
show        Displays the contents of configuration script.
validate    Validate the commands of configuration script.
```

### script list and script delete

```bash
(Netgear Switch) #script list

<table>
<thead>
<tr>
<th>Configuration Script Name</th>
<th>Size(Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic.scr</td>
<td>93</td>
</tr>
<tr>
<td>running-config.scr</td>
<td>3201</td>
</tr>
</tbody>
</table>

2 configuration script(s) found.
1020706 bytes free.

(Netgear Switch) #script delete basic.scr

Are you sure you want to delete the configuration script(s)? (y/n) y

1 configuration script(s) deleted.
```
script apply running-config.scr

(Netgear Switch) #script apply running-config.scr
Are you sure you want to apply the configuration script? (y/n) y
The system has unsaved changes.
Would you like to save them now? (y/n) y
Configuration Saved!

Create a Configuration Script

(Netgear Switch) #show running-config running-config.scr
Config script created successfully.

(Netgear Switch) #script list

<table>
<thead>
<tr>
<th>Configuration Script Name</th>
<th>Size(Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>running-config.scr</td>
<td>3201</td>
</tr>
</tbody>
</table>

1 configuration script(s) found.
1020799 bytes free.

Upload a Configuration Script

(Netgear Switch) #copy nvram: script running-config.scr
tftp://192.168.77.52/running-config.scr
Mode......................... TFTP
Set TFTP Server IP......... 192.168.77.52
TFTP Path.................... ./
TFTP Filename................. running-config.scr
Data Type..................... Config Script
Source Filename............... running-config.scr

Are you sure you want to start? (y/n) y
File transfer operation completed successfully.
Pre-Login Banner

Pre-login banner:

- Allows you to create message screens that display when a user logs in to the CLI.
- By default, no banner file exists.
- You can upload or download.
- File size cannot be larger than 2 K.

The Pre-Login Banner feature is only for the CLI interface.

Create a Pre-Login Banner (CLI Only)

1. On your PC, using Notepad create a banner.txt file that contains the banner to be displayed.

```
Login Banner - Unauthorized access is punishable by law.
```

2. Transfer the file from the PC to the switch using TFTP.

```
(Netgear Switch Routing) #copy tftp://192.168.77.52/banner.txt nvram:clibanner
Mode........................................... TFTP
Set TFTP Server IP............................. 192.168.77.52
TFTP Path...................................... ./
TFTP Filename.................................. banner.txt
Data Type...................................... Cli Banner

Are you sure you want to start? (y/n) y

CLI Banner file transfer operation completed successfully!

(Netgear Switch Routing)#exit

(Netgear Switch Routing) >logout

Login Banner - Unauthorized access is punishable by law.
User:
```

**Note:** The `no clibanner` command removes the banner from the switch.
Port Mirroring

The port mirroring feature:

- Allows you to monitor network traffic with an external network analyzer.
- Forwards a copy of each incoming and outgoing packet to a specific port.
- Is used as a diagnostic tool, debugging feature, or means of fending off attacks.
- Assigns a specific port to copy all packets to.
- Allows inbound or outbound packets to switch to their destination and to be copied to the mirrored port.

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

**CLI: Specify the Source (Mirrored) Ports and Destination (Probe)**

```
(Netgear Switch)#config
(Netgear Switch)(Config)#monitor session 1 mode
    Enable mirror
(Netgear Switch)(Config)#monitor session 1 source interface 1/0/2
    Specify the source interface.
(Netgear Switch)(Config)#monitor session 1 destination interface 1/0/3
    Specify the destination interface.
(Netgear Switch)(Config)#exit
(Netgear Switch)#show monitor session 1
    Session ID Admin Mode Probe Port Mirrored Port
    -------------- ------------- ------------- -------------
    1                Enable  1/0/3           1/0/2
```
Web Interface: Specify the Source (Mirrored) Ports and Destination (Probe)

1. Select **Monitoring > Mirroring > Port Mirroring**. A screen similar to the following displays.

2. Scroll down and select the Source Port 1/0/2 check box. The value 1/0/2 now appears in the Interface field at the top.

3. Enter the following information:
   - In the **Destination Port** field, enter 1/0/3.
   - In the **Session Mode** field, select **Enable**.

4. Click **Apply**.

Dual Image

Traditionally switches contain a single image in the permanent storage. This image is loaded into memory every time there is a reboot. The dual image feature allows switches to have two images in permanent storage. You can denote one of these images as an active image that will be loaded in subsequent reboots and the other image as a backup image. This feature provides for reduced down time for the switches, when the firmware is being upgraded or downgraded.

The images are stored in the file system with the file names `image1` and `image2`. These names are used in the CLI, Web, and SNMP interfaces. Each of the images can be associated with a textual description. The switch provides commands to associate and retrieve the text description for an image. A switch also provides commands to activate the backup image such that it is loaded in subsequent reboots. This activation command makes the current active image as the backup image for subsequent reboots.

On three successive errors executing the **active-image**, the switch attempts to execute the **backup-image**. If there are errors executing the **backup-image** as well, the bootloader will invoke the boot menu.

The Dual Image feature works seamlessly with the stacking feature. All members in the stack must be uniform in their support for the dual image feature. The Dual Image feature works in the following way in a Stack.
• When an image is activated, the Management node notifies all the participating nodes. All nodes activate the specified image.
• When any node is unable to execute the active-image successfully, it attempts to execute the backup-image, as mentioned in the section above. Such cases will require user intervention to correct the problem, by using appropriate stacking commands.

**CLI: Download a Backup Image and Make It Active**

```bash
(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 bytes 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...7277776 bytes transferred...7443392 bytes transferred...7609496 bytes transferred...7775600 bytes transferred...7941704 bytes transferred...8107808 bytes transferred...8274016 bytes transferred...8440224 bytes transferred...8606432 bytes transferred...8772640 bytes transferred...8938848 bytes transferred...9105056 bytes transferred...9271264 bytes transferred...9437472 bytes transferred...9603680 bytes transferred...9769888 bytes transferred...9936104 bytes transferred...10102312 bytes transferred...10268528 bytes transferred...10434736 bytes transferred...10601048 bytes transferred...10767264 bytes transferred...10933480 bytes transferred...11099792 bytes transferred...11266008 bytes transferred...11432320 bytes transferred...11598632 bytes transferred...11764944 bytes transferred...11931256 bytes transferred...12097568 bytes transferred...12263880 bytes transferred...12430192 bytes transferred...12596504 bytes transferred...12762816 bytes transferred...12929128 bytes transferred...13095440 bytes transferred...13261752 bytes transferred...13428064 bytes transferred...13594376 bytes transferred...13760688 bytes transferred...13926992 bytes transferred...14093304 bytes transferred...14259616 bytes transferred...14425928 bytes transferred...14592240 bytes transferred...14758552 bytes transferred...14924864 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
 imagel : default image
 image2 :
 Images currently available on Flash
```
Web Interface: Download a Backup Image and Make It Active

1. Download a backup image using tftp.

   a. Select Maintenance > Download > File Download. A screen similar to the following displays.

   ![File Download Screen]

   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.

![Dual Image Configuration screen](image)

b. Under Dual Image Configuration, scroll down and select the **Image 2** check box. The image2 now appears in the Image name field at the top.

c. In the **Active Image** field, select **TRUE**.

d. Click **Apply**.

**Outbound Telnet**

In this section, the following examples are provided:

- **CLI: show network** on page 305
- **CLI: transport output telnet** on page 306
- **Web Interface: Configure Telnet** on page 306
- **CLI: Configure the session-limit and session-timeout** on page 307
- **Web Interface: Configure the Session Timeout** on page 307

**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.
ProSafe Managed Switch

CLI: show network

<table>
<thead>
<tr>
<th>(Netgear Switch Routing) &gt;telnet 192.168.77.151</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trying 192.168.77.151...</td>
</tr>
<tr>
<td>(Netgear Switch Routing)</td>
</tr>
<tr>
<td>User:admin</td>
</tr>
<tr>
<td>Password:</td>
</tr>
<tr>
<td>(Netgear Switch Routing) &gt;en</td>
</tr>
<tr>
<td>Password:</td>
</tr>
<tr>
<td>(Netgear Switch Routing) #show network</td>
</tr>
<tr>
<td>IP Address.................................... 192.168.77.151</td>
</tr>
<tr>
<td>Subnet Mask.................................... 255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway............................... 192.168.77.127</td>
</tr>
<tr>
<td>Burned In MAC Address......................... 00:10:18.82.04:E9</td>
</tr>
<tr>
<td>Locally Administered MAC Address............... 00:00:00:00:00:00</td>
</tr>
<tr>
<td>MAC Address Type............................. Burned In</td>
</tr>
<tr>
<td>Network Configuration Protocol Current...     DHCP</td>
</tr>
<tr>
<td>Management VLAN ID............................ 1</td>
</tr>
<tr>
<td>Web Mode...................................... Enable</td>
</tr>
<tr>
<td>Java Mode ..................................... Disable</td>
</tr>
</tbody>
</table>

CLI: show telnet

<table>
<thead>
<tr>
<th>(Netgear Switch Routing)#show telnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound Telnet Login Timeout (minutes)....... 5</td>
</tr>
<tr>
<td>Maximum Number of Outbound Telnet Sessions.... 5</td>
</tr>
<tr>
<td>Allow New Outbound Telnet Sessions............. Yes</td>
</tr>
</tbody>
</table>
### CLI: transport output telnet

```lua
(Netgear Switch Routing) (Config)#lineconfig ?

<cr> Press Enter to execute the command.

(Netgear Switch Routing) (Config)#lineconfig

(Netgear Switch Routing) (Line)#transport ?

input Displays the protocols to use to connect to a specific line of the router.

output Displays the protocols to use for outgoing connections from a line.

(Netgear Switch Routing) (Line)#transport output ?

telnet Allow or disallow new telnet sessions.

(Netgear Switch Routing) (Line)#transport output telnet ?

<cr> Press Enter to execute the command.

(Netgear Switch Routing) (Line)#transport output telnet

(Netgear Switch Routing) (Line)#
```

### Web Interface: Configure Telnet

1. Select **Security > Access > Telnet**. A screen similar to the following displays.
2. Under Outbound Telnet, for Admin Mode, select the **Enable** radio button.
3. Click **Apply**.

### CLI: Configure the session-limit and session-timeout

```bash
(Netgear Switch Routing) (Line)#session-limit ?
<0-5> Configure the maximum number of outbound telnet sessions allowed.

(Netgear Switch Routing) (Line)#session-limit 5

(Netgear Switch Routing) (Line)#session-timeout ?
<1-160> Enter time in minutes.

(Netgear Switch Routing) (Line)#session-timeout 15
```

### Web Interface: Configure the Session Timeout

1. Select **Security > Access > Telnet**. A screen similar to the following displays.

2. Enter the following information:
   - In the **Session Timeout** field, enter **15**.
   - In the **Maximum number of sessions** field, enter **5**.
3. Click **Apply**.
This chapter provides the following examples:

- *Show Logging* on page 309
- *Show Logging Buffered* on page 311
- *Show Logging Traplogs* on page 312
- *Show Logging Hosts* on page 313
- *Configure Logging for a Port* on page 314
- *Email Alerting* on page 316

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 33. Log Files](image-url)
Show Logging

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

CLI: Show Logging

(Netgear Switch Routing) #show logging

<table>
<thead>
<tr>
<th>Logging Client Local Port</th>
<th>514</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI Command Logging</td>
<td>disabled</td>
</tr>
<tr>
<td>Console Logging</td>
<td>disabled</td>
</tr>
<tr>
<td>Console Logging Severity Filter</td>
<td>alert</td>
</tr>
<tr>
<td>Buffered Logging</td>
<td>enabled</td>
</tr>
<tr>
<td>Syslog Logging</td>
<td>enabled</td>
</tr>
<tr>
<td>Log Messages Received</td>
<td>66</td>
</tr>
<tr>
<td>Log Messages Dropped</td>
<td>0</td>
</tr>
<tr>
<td>Log Messages Relayed</td>
<td>0</td>
</tr>
<tr>
<td>Log Messages Ignored</td>
<td>0</td>
</tr>
</tbody>
</table>

Web Interface: Show Logging

1. Configure the syslog.
   a. From the main menu, select Monitoring > Logs > Sys Log Configuration.

   ![Syslog Configuration](image)

   b. In the Syslog Configuration, next to the Admin Status, select the **Enable** radio button.
   c. Click **Apply**.

2. Configure the command log.
a. Select Monitoring > Logs > Command Log.

b. Under Command Log, for Admin Status, select the Disable radio button.

c. Click Apply.

3. Configure the console log.

a. Select Monitoring > Logs > Console Log.

b. Under Console Log Configuration, for Admin Status, select the Disable radio button.

c. Click Apply.

4. Configure the buffer logs.
a. Select **Monitoring > Logs > Buffer Logs**. A screen similar to the following displays.

b. Under Buffer Logs, for Admin Status, select the **Enable** radio button.

c. Click **Apply**.

**Show Logging Buffered**

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

**CLI: Show Logging Buffered**

```
(Netgear Switch Routing) #show logging buffered ?
<cr> Press Enter to execute the command.

(Netgear Switch Routing) #show logging buffered

Buffered (In-Memory) Logging : enabled
Buffered Logging Wrapping Behavior : On
Buffered Log Count : 66

<1> JAN 01 00:00:02 0.0.0.0-0 UNKN[268434944]: usmdb_sim.c(1205) 1 % Error 0 (0x0)
<2> JAN 01 00:00:09 0.0.0.0-1 UNKN[268434944]: bootos.c(487) 2 % Event (0xaaaaaaaa)
<6> JAN 01 00:00:09 0.0.0.0-1 UNKN[268434944]: bootos.c(531) 3 % Starting code...
<6> JAN 01 00:00:16 0.0.0.0-3 UNKN[251627904]: cda_cnfgr.c(383) 4 % CDA: Creating new STK file.
<6> JAN 01 00:00:39 0.0.0.0-3 UNKN[233025712]: edb.c(360) 5 % EDB Callback: Unit Join: 3.
<6> JAN 01 00:00:40 0.0.0.0-3 UNKN[251627904]: sysapi.c(1864) 6 % File user_mgr_cfg: same version (6) but the sizes (2312->7988) differ
```
Web Interface: Show Logging Buffered

Select Monitoring > Logs > Buffer Logs. A screen similar to the following displays.

![Buffered Logs Screen]

Show Logging Traplogs

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

**CLI: Show Logging Traplogs**

```
(Netgear Switch Routing)   #show logging traplogs
?                          
<cr>  Press Enter to execute the command.
(Netgear Switch Routing)   #show logging traplogs
Number of Traps Since Last Reset.......... 6
Trap Log Capacity......................256
Number of Traps Since Log Last Viewed...... 6

Log System Up Time   Trap
--- --------------      ----------------------------------------------
0  0 days 00:00:46    Link Up: Unit: 3 Slot: 0 Port: 2
1  0 days 00:01:01    Cold Start: Unit: 0
2  0 days 00:21:33    Failed User Login: Unit: 1 User ID: admin
3  0 days 18:33:31    Failed User Login: Unit: 1 User ID: 
4  0 days 19:27:05    Multiple Users: Unit: 0 Slot: 3 Port: 1
5  0 days 19:29:57    Multiple Users: Unit: 0 Slot: 3 Port: 1
```

Web Interface: Show Logging Trap Logs
Select Monitoring > Logs > Trap Logs. A screen similar to the following displays.

![Trap Logs Screen](image)

Show Logging Hosts

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

**CLI: Show Logging Hosts**

```
(Netgear Switch Routing) #show logging hosts ?
<cr> Press Enter to execute the command.

(Netgear Switch Routing) #show logging hosts
```

<table>
<thead>
<tr>
<th>Index</th>
<th>IP Address</th>
<th>Severity</th>
<th>Port</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.21.253</td>
<td>critical</td>
<td>514</td>
<td>Active</td>
</tr>
</tbody>
</table>
Web Interface: Show Logging Hosts

Select Monitoring > Logs > Sys Log Configuration. A screen similar to the following displays.

![Syslog Configuration Screen]

Configure Logging for a Port

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

**CLI: Configure Logging for the Port**

```
(Netgear Switch Routing) #config

(Netgear Switch Routing) (Config)#logging ?

buffered                   Buffered (In-Memory) Logging Configuration.
cli-command             CLI Command Logging Configuration.
console                Console Logging Configuration.
host                    Enter IP Address for Logging Host
syslog             Syslog Configuration.

(Netgear Switch Routing) (Config)#logging host ?

<hostaddress>             Enter Logging Host IP Address
reconfigure               Logging Host Reconfiguration
remove                Logging Host Removal

(Netgear Switch Routing) (Config)#logging host 192.168.21.253 ?

<cr>             Press Enter to execute the command.
<port>           Enter Port Id
```
Web Interface: Configure Logging for the Port

1. Select Monitoring > Logs > Sys Log Configuration. A screen similar to the following displays.

2. Enter the following information:
   - In the Host Address field, enter your host address 192.168.21.253.
   - In the Port field, enter 4.
   - In the Severity Filter list, select Alert.

3. Click Add.
Email Alerting

Email Alerting is an extension of the logging system. The logging system allows you to configure a set of destinations for log messages. This feature adds the email configuration, through which the log messages are sent to a configured SMTP server such that an administrator may receive the log in an email account of their choice.

This feature is enabled globally. When email alerting is enabled, selected log messages are sent to an SMTP server. Log messages are divided into three groups by severity level: urgent, non-urgent, and never.

The network administrator can adjust the urgent and non-urgent severity levels. These levels are global and apply to all destination email addresses. Log messages in the urgent group are sent immediately to the SMTP server with each log message in a separate mail. Log messages in the non-urgent group are batched into a single email message and after a configurable delay.

Email alerting also provides a configuration option that allows the network administrator to specify the severity level at which SNMP traps are logged. Using this option, the administrator can put traps in the urgent group, the non-urgent group, or the never group for emailing. Traps are not emailed by default. For traps to be emailed, the network administrator has to either increase the severity at which traps are logged, or lower the severity level of log messages that are emailed.

The network administrator can configure multiple destination email addresses, and for each email address, specify whether to deliver urgent log messages, non-urgent log messages, or both.

There is an exception to the sending of the messages periodically to the SMTP server. When the log buffer is completely full before the expiry of the periodic timer sending of the log messages to the SMTP server does not until the expiry of the timer. When the log buffer is full, a connection is opened immediately with the SMTP server, and all the messages that have not previously been emailed are sent to it.
CLI: Send Log Messages to admin@switch.com Using Account aaaa@netgear.com

1. Configure an SMTP server, for example, smtp.netgear.com. Before you configure the smtp server, you need to have an account on SMTP server.

```
(Netgear Switch) (Config)#mail-server "smtp.netgear.com" port 465
(Netgear Switch) (Mail-Server)#security tlsv1
(Netgear Switch) (Mail-Server)# username aaaa
(Netgear Switch) (Mail-Server)# password xxxxxx
(Netgear Switch) (Mail-Server)#exit
```

2. Configure logging mail. From-addr is the source address of email and to-addr is the destination address of email.

```
(Netgear Switch) (Config)#logging email
(Netgear Switch) (Config)#logging email from-addr aaaa@netgear.com
(Netgear Switch) (Config)#logging email message-type urgent to-addr admin@switch.com
(Netgear Switch) (Config)#logging email message-type non-urgent to-addr admin@switch.com
```

3. Increase the severity of traps to 3 (error). By default, it is 6 (infor).

```
(Netgear Switch) (Config)#logging traps 3
```
This chapter describes the concepts and recommended operating procedures to manage NETGEAR stackable managed switches running release 4.x.x.x or newer.

This chapter includes the following topics:

- **Switch Stack Management and Connectivity**
- **The Stack Master and Stack Members** on page 319
- **Install and Power-up a Stack** on page 321
- **Switch Firmware** on page 322
- **Configure a Stacking Port as an Ethernet Port** on page 324
- **Stack Switches Using 10G Fiber** on page 327
- **Add, Remove, or Replace a Stack Member** on page 330
- **Switch Stack Configuration Files** on page 332
- **Preconfigure a Switch** on page 333
- **Renumber Stack Members** on page 334
- **Move the Stack Master to a Different Unit** on page 336

## Switch Stack Management and Connectivity

You manage the switch stack through the stack master. You cannot manage stack members on an individual basis. To access the stack master, use either a serial connection to the switch master’s console port, or a Telnet connection to the IP address of the stack.

You can use these methods to manage switch stacks:

- Web Management Interface.
- CLI (over a serial connection).
- A network management application through SNMP.
The Stack Master and Stack Members

A switch stack is a set of up to 8 switches connected through their stacking ports. The switch that controls the operation of the stack is the stack master. The stack master and the other switches in the stack are stack members. Stack members use stacking technology to behave and work together as a unified system. Layer 2 and Layer 3 protocols present the entire switch stack as a single entity to the network. The following figure shows an example of switches that are interconnected to form a stack.

![Connecting AX742 modules with stacking cable](image)

Figure 35. Stacked switches

Stack Master

The stack master is the single point of stack-wide management. From the stack master, you configure:

- System-level (global) features that apply to all stack members.
- Interface-level features for all interfaces on any stack member.

A switch stack is identified in the network by its network IP address. The network IP address is assigned according to the MAC address of the stack master. Every stack member is uniquely identified by its own stack member number.

The stack master contains the saved and running configuration files for the switch stack. The configuration files include the system-level settings for the switch stack and the interface-level settings for all stack members. Each stack member retains a copy of the saved file for backup purposes. If the master is removed from the stack, another member is elected master, and then runs from that saved configuration.

All stack members are eligible stack masters. If the stack master becomes unavailable, the remaining stack members participate in electing a new stack master. A set of factors determine which switch is elected the stack master. The stack master is elected or re-elected based on one of these factors and in the order listed:
1. The switch that is currently the stack master.
2. The switch with the highest stack member priority value.

**Note:** NETGEAR recommends assigning the highest priority value to the switch that you prefer to be the stack master. This ensures that the switch is re-elected as stack master if a re-election occurs.

3. The switch with the higher MAC address.

A stack master retains its role unless one of these events occurs:

- The stack master is removed from the switch stack
- The stack master is reset or powered off
- The stack master has failed
- The switch stack membership is increased by adding powered-on standalone switches or switch stacks

In the case of a master re-election, the new stack master becomes available after a few seconds. In the meantime, the switch stack uses the forwarding tables in memory to minimize network disruption. The physical interfaces on the other available stack members are not affected while a new stack master is elected. If a new stack master is elected and the previous stack master becomes available, the previous stack master does not resume its role as stack master.

## Stack Members

A switch stack has up to 8 stack members connected through their stacking ports. A switch stack always has one stack master.

A standalone switch is a switch stack with one stack member that also operates as the stack master. You can connect one standalone switch to another to create a switch stack containing two stack members, with one of them being the stack master. You can connect standalone switches to an existing switch stack to increase the stack membership.

The operation of the switch stack continues uninterrupted during membership changes unless you remove the stack master or you add powered-on standalone switches or switch stacks.

## Stack Member Numbers

A stack member number (1 to 8) identifies each member in the switch stack. The member number also determines the interface-level configuration that a stack member uses. You can display the stack member number by using the `show switch user` EXEC command.

A new, out-of-the-box switch (one that has not joined a switch stack or has not been manually assigned a stack member number) ships with a default stack member number of 1. When it
joins a switch stack, its default stack member number changes to the lowest available member number in the stack.

Stack members in the same switch stack cannot have the same stack member number. Every stack member, including a standalone switch, retains its member number until you manually change the number or unless the number is already being used by another member in the stack.

See Renumber Stack Members on page 334.

Stack Member Priority Values

You can change a stack member priority. This is useful if you want to change the master of the stack. Use the following command (in the global config mode):

switch unit priority value

Install and Power-up a Stack

Note: Many switch models such as the GSM7200PS and GSM7300S series have a Hardware Installation Guide that includes additional information about rack mounting and stack cabling.

Compatible Switch Models

NETGEAR stackable managed switches include the following models:

- FSM7226RS
- FSM7250RS
- FSM7328S
- FSM7328PS
- FSM7352S
- FSM7352PS
- GSM7328S
- GSM7352S
- GSM7328FS
- GSM7228PS
- GSM7252PS

The FSM family, GSM family, and XSM72224S cannot be stacked together at this point.
Install a Switch Stack

Note: Many models of switches have a Hardware Installation Guide that includes additional information about rack mounting and switch stack cabling.

1. Install the switches in a rack.
2. Install all stacking cables, including the redundant stack link. It is highly recommended that a redundant link be installed.
3. Identify the switch to be the master. Power up this switch first.
4. Monitor the console port. Allow this switch to come up to the login prompt. If the switch has the default configuration, it should come up as unit #1, and automatically become a master switch. If not, renumber the units.
5. If you want to configure switches offline, preconfigure the other switches to be added to the stack. See Preconfigure a Switch on page 333.
6. Power on a second switch, making sure it is adjacent (the next physical switch in the stack) to the switch already powered up. This ensures that the second switch comes up as a member of the stack, and not a master of a separate stack.
7. Monitor the master switch to see that the second switch joins the stack. Use the show switch command to determine when the switch joins the stack. It will be assigned a unit number (unit #2, if it has the default configuration).
8. Renumber this stack member, if you want. See Renumber Stack Members on page 334 for recommendations for renumbering stack members.

Repeat steps 6 through 8 to add members to the stack. Always power on a switch adjacent to the switches already in the stack.

Switch Firmware

All stack members must run the same firmware version. This helps ensure full compatibility in the stack protocol version among the stack members.

If a stack member is running a different firmware version than the stack master, that stack member is not allowed to join the stack. Use the show switch command to list the stack members and firmware versions. See the following section Code Mismatch.

You can upgrade a switch that has an incompatible firmware image by using the command copy xmodem | ymodem | zmodem | tftp://ip/filepath/filename. This command copies the firmware image from a stack member to the one with incompatible firmware. That switch automatically reloads and joins the stack as a fully functioning member.
Code Mismatch

If a switch is added to a stack and it does not have the same version of code as that of the master, the following occurs:

- The new unit boots up and becomes a member of the stack.
- Ports on the added unit remain in the detached state.
- A message displays on the CLI indicating a code mismatch with the newly added unit.
- To have the newly added unit to merge normally with the stack, use the copy command to load the correct code from the master to the newly added unit. Then reset the newly added member. It should reboot normally and join the stack.

Upgrade the Firmware

All stack members must run the same firmware version. Ports on stack members that don’t match the master switch firmware version don’t come up and the `show switch` command shows a code mismatch error.

1. NETGEAR recommends that you schedule the firmware upgrade when there is no excessive network traffic (such as a broadcast event).
2. Download new firmware using TFTP or xmodem to the master switch using the `copy` command.
   - Once the firmware is successfully loaded on the master switch, it automatically propagates to the other units in the stack.

   **CAUTION:**
   - To avoid errors during code propagation, do not move stack cables or reconfigure units.

3. If an error occurs during code propagation, first check to make sure the master switch is running the correct firmware. Then issue the `copy` command (in stack configuration mode) to make another attempt to copy the firmware to the units that did not get updated.
4. Once code is loaded to all members of the stack, reset all the switches so that the new firmware starts running.

Migrate Configuration with a Firmware Upgrade

In some cases, a configuration might not be carried forward in a code update. For updates where this issue is to be expected, the following procedure should be followed:

1. Save the current configuration by uploading it from the stack, using the `copy` command from the CLI.
2. Load new code into the stack manager. Reboot the stack.
3. Upon reboot, go into the boot menu and erase the configuration (restore to factory defaults)
4. Continue with the boot of operational code.
5. Once the stack is up, download the saved configuration back to the master. This configuration should then be automatically propagated to all members of the stack.

Copy Master Firmware to a Stack Member (Web Interface)

1. Select System > Management > Basic > Stack Configuration. A screen similar to the following displays.

   ![Screenshot of system configuration interface]

2. In the Copy Master Firmware to Unit list, select 2.
3. Click Apply.

Configure a Stacking Port as an Ethernet Port

Figure 36. Configuring a stacking port as an Ethernet port

Follow these steps to set up the topology:

1. Insert the AX742 into the I/O module on the switch.
2. Configure the switch A and B as described in the following instructions.
3. Connect the AX 742 with stack cable.
4. Reboot Switch A and Switch B.
CLI: Configure a Stacking Port as an Ethernet Port

1. On Switch A, Configure the Stack Port and Reboot

   (Netgear Switch) #show stack-port
   Configured Running Link
   Stack Stack Link Speed
   Unit Intf SlotId 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) #config
   (Netgear Switch) (Config)#stack
   (Netgear Switch) (Config-stack)#stack-port 2/0/28 ethernet
   (Netgear Switch) (Config-stack)#exit
   (Netgear Switch) (Config)#exit
   (Netgear Switch) #reload
   Are you sure you want to reload the stack? (y/n) y

   After Switch A reboots:

   (Netgear Switch) #show port 2/0/28
   Admin    Physical   Physical  Link   Link     LACP     Actor
   Intf   Type    Mode     Mode     Status    Status  Trap     Mode     Timeout
   ------ -----  -------  --------  ---------  ------  -------  -------  -----
   2/0/28   Enable   10G Full  10G Full    Up     Enable   Enable   long

2. On Switch B, Configure the stack port and reboot.

   (Netgear Switch) #
   (Netgear Switch) #show stack-port
   Configured Running Link
   Stack Stack Link Speed
   Unit Intf SlotId 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 1/0/51 ethernet
   (Netgear Switch) (Config-stack)#exit
   (Netgear Switch) (Config)#exit
   (Netgear Switch) #reload
   Are you sure you want to reload the stack? (y/n) y
After Switch B reboots:

<table>
<thead>
<tr>
<th>Intf</th>
<th>Type</th>
<th>Mode</th>
<th>Mode</th>
<th>Status</th>
<th>Status</th>
<th>Trap</th>
<th>Mode</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/51</td>
<td>Enable</td>
<td>10G Full</td>
<td>10G Full</td>
<td>Up</td>
<td>Enable</td>
<td>Enable</td>
<td>long</td>
<td></td>
</tr>
</tbody>
</table>

### Web Interface: Configure a Stacking Port as an Ethernet Port

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.
   ![Web Interface Screenshot](image)
   b. Under Stack Port Configuration, scroll down and select the 2/0/28 check box.
   c. In the Configured Stack Mode list, 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.
   ![Web Interface Screenshot](image)
   b. In the Reboot Unit No. list, 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.

![Stack Port Configuration](image)

b. Under Stack Port Configuration, scroll down and select the **1/0/51** check box.

c. In the Configured Stack Mode list, select **Ethernet**.

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

4. Reboot the switch.

a. Select **Maintenance > Reset > Device Reboot**. A screen similar to the following displays.

![Device Reboot](image)

b. In the **Reboot Unit No.** list, select **1**.

c. Click **Apply**.

### Stack Switches Using 10G Fiber

This example shows how to stack two switches in different buildings at long distance using 10G fiber. First insert AX741 to I/O slot on Switch A, and insert AX741 to I/O slot on Switch B. Then connect the two AX741 with fiber.

![Stack Switches Using 10G Fiber](image)

**Figure 37. Using 10G fiber to stack switches in different buildings**
CLI: Stack Switches Using 10G Fiber

1. On Switch A, show the port information.

```
(Netgear Switch) #show stack-port
Configured  Running       Link
    Stack    Stack    Link     Speed
Unit Intf SlotId Type   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
```

In this case, port 1/0/52 has been configured as stack, so no action is needed.

2. On Switch B, show the stack port information.

```
(Netgear Switch) #show stack-port
Configured  Running       Link
    Stack    Stack    Link     Speed
Unit Intf SlotId Type   XFP Adapter Mode   Mode      Status    (Gb/s)
---- ------ ------- -----  -----------  --------  --------  --------  --------
2     0/27     None    Stack    Stack      Link Down    0
2     0/28    AX741    Ethernet Ethernet Link Down   12
```

3. Since 2/0/28 is in Ethernet mode, it must be changed to stack mode.

```
(Netgear Switch) (Config)#stack
(Netgear Switch) (Config-stack)#stack-port 2/0/28 stack
(Netgear Switch) (Config-stack)#exit
(Netgear Switch) (Config)
```

4. Reboot Switch B.

```
(Netgear Switch) #reload
Management switch has unsaved changes.
Would you like to save them now? (y/n) n
Configuration Not Saved!
Are you sure you want to reload the stack? (y/n) y
Reloading all switches.
```
On Switch A, you see the following:

```
(Netgear Switch) #show switch

<table>
<thead>
<tr>
<th>Management</th>
<th>Standby</th>
<th>Preconfig</th>
<th>Plugged-in</th>
<th>Switch</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW Switch</td>
<td>Status</td>
<td>Model ID</td>
<td>Model ID</td>
<td>Status</td>
<td>Version</td>
</tr>
<tr>
<td>---</td>
<td>--------</td>
<td>---------</td>
<td>----------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>1 Mgmt Sw</td>
<td>GSM7352Sv2</td>
<td>GSM7352Sv2</td>
<td>OK</td>
<td>8.0.1.2</td>
<td></td>
</tr>
<tr>
<td>2 Stack Mbr</td>
<td>Oper Stby</td>
<td>GSM7328Sv2</td>
<td>GSM7328Sv2</td>
<td>OK</td>
<td>8.0.1.2</td>
</tr>
</tbody>
</table>
```

Web Interface: Stack Switches Using 10G Fiber

1. On Switch A, show the Port Information.
   a. Select **System > Stacking > Advanced > Stack Port Configuration**. A screen similar to the following displays.

```
<table>
<thead>
<tr>
<th>System</th>
<th>Switching</th>
<th>Routing</th>
<th>GoS</th>
<th>Security</th>
<th>Monitoring</th>
<th>Maintenance</th>
<th>Help</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>Advanced</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Config</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Config</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

b. Since the port 1/0/52 is stack mode already, nothing needs to be done.

2. On Switch B, configure port 2/0/28 as stacking port.
   a. Select **System > Stacking > Advanced > Stack Port Configuration**. A screen similar to the following displays.

```
<table>
<thead>
<tr>
<th>System</th>
<th>Switching</th>
<th>Routing</th>
<th>GoS</th>
<th>Security</th>
<th>Monitoring</th>
<th>Maintenance</th>
<th>Help</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>Advanced</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Config</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Config</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

b. Scroll down and select the **2/0/28** check box.
   c. In the **Configured Stack Mode** list, select **Stack**.
   d. Click **Apply** to save the settings.

3. Reboot the switch.
a. Select **Maintenance > Reset > Device Reboot**. A screen similar to the following displays.

![Device Reboot Screen]

b. In the **Reboot Unit No.** list, select 2.

c. Click **Apply**.

### Add, Remove, or Replace a Stack Member

#### Add Switches to an Operating Stack

1. Make sure the redundant stack connection is in place and functional. All stack members should be connected in a logical ring.
2. Preconfigure the new switches, if desired.
3. Power off all new switches that will be joining the stack.

**CAUTION:**

If you cable one or more powered-on switches to the stack, the existing stack and the new switches assume two stacks are merging. They elect a single, new stack master, and you cannot specify which switch becomes the new master. All stack members assume configuration based on the new stack master. Stack members change their stack member numbers to the lowest available numbers.

4. Install the new switches in the rack. This procedure assumes installation below the bottom-most switch, or above the top-most switch.
5. Disconnect the redundant stack cable that connects the last switch in the stack back up to the first switch in the stack at the position in the ring where the new switch is to be inserted.

**Note:** If you want to merge an operational stack into the this stack, add the switches as a group by unplugging one stacking cable in the operational stack and physically connecting all unpowered units at that point.
6. Connect this cable to the new switch, following the established order of stack-up to stack-down connections.

7. Power up the new switches one by one. Verify, by monitoring the master switch console port, that the new switch joins the stack by issuing the `show switch` command. The new switch should join as a member (never as master; the existing master of the stack should not change).

8. If the firmware version of the newly added member is not the same as the existing stack, update the firmware as described in *Upgrade the Firmware* on page 323.

Remove a Switch from the Stack

1. Make sure the redundant stack connection is in place and functional. All stack members should be connected in a logical ring.

2. Power down the switch to be removed.

    **Note:** Removing powered-on stack members can cause the switch stack to divide (partition) into two or more switch stacks, each with the same configuration. However, if cabled correctly, the switch stack should not divide.

3. Disconnect the stack cables.

4. If the switch is not to be replaced, reconnect the stack cable from the stack member above to the stack member below the switch being removed.

5. Remove the switch from the rack.

6. If you want to remove the switch from the stack configuration, issue the command:
   ```
   no member <unit-id>
   ```

   If the switch stack divides, and you want the switch stacks to remain separate, change the IP address or addresses of the newly created switch stacks.

   If you did not intend to partition the switch stack:

   1. Power off the newly created switch stacks.
   2. Reconnect them to the original switch stack through their stacking ports.
   3. Power on the switches.

Replace a Stack Member

1. Make sure the redundant stack connection is in place and functional. All stack members should be connected in a logical ring.

2. Power down the switch to be removed and disconnect its stack cables.

3. Remove the switch from the rack.

4. If you will be installing a different model switch, remove the unit from the configuration by issuing the command `no member <unit-id>`.
5. Install the new switch in the rack:
   • If you are installing the same model switch, put it in the same position in the stack as
     the one that you just removed.
   • If you are installing a different model switch you can either put it in the same position
     as the previous switch, or at the bottom of the stack.

6. Cable the new switch, following the established order of stacking cables.

7. Power up the new switch. Verify, by monitoring the master switch console port, that the new
   switch successfully joins the stack by issuing the `show switch` command. The new switch
   should join as a member (never as master; the existing master of the stack should not
   change).

8. If the code version of the newly added member is not the same as the existing stack, update
   the code as described in Upgrade the Firmware on page 323.

Switch Stack Configuration Files

The configuration files record settings for all global and interface-specific settings that define
the operation of the stack and individual members. Once a `save config` command is
issued, all stack members store a copy of the configuration settings. If a stack master
becomes unavailable, any stack member assuming the role of stack master will operate from
the saved configuration files.

When a new, out-of-box switch joins a switch stack, it uses the system-level settings of that
switch stack. However, if you want it to store this system level configuration, you must issue a
`save config` command.

You back up and restore the stack configuration using the copy command the same way that
you would for standalone switch configuration.

The following table provides switch stack configuration scenarios. Most of the scenarios
assume at least two switches are connected through their stacking ports.

Table 1. Switch Stack Master Scenarios

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack master election specifically determined by existing stack masters. Note: This is not recommended.</td>
<td>Connect two powered-on switch stacks through the stacking ports.</td>
<td>Only one of the stack masters becomes the new stack master. No other stack members become the stack master.</td>
</tr>
</tbody>
</table>
| Stack master election specifically determined by the stack member priority value. | • Connect two switches through their stacking ports.  
   • Use the global configuration command `switch
     stack-member-number priority new-priority-number` to set a
     stack member to a higher member priority value.  
   • Restart both stack members at the same time. | The stack member with the higher-priority value is elected stack master.      |
You can preconfigure (supply a configuration to) a new switch before it joins the switch stack. You can specify the stack member number, the switch type, and the interfaces associated with a switch that is not currently part of the stack.

**Note:** If you are replacing a switch with the same model in the same position in the stack, you do not need to preconfigure it. The new switch assumes the same configuration as the previous switch.

1. Issue the `member <unit-id> <switchindex>` command. To view the supported unit types, use the `show supported switchtype` command.
2. Next, configure the unit you just defined with configuration commands, just as if the unit were physically present.
   Ports for the preconfigured unit come up in a detached state.
3. To see the ports, use the `show port all` command. Now you can configure the detached ports for VLAN membership and any other port-specific configuration.

After you preconfigure a unit type for a specific unit number, attaching a unit with different unit type for this unit number causes the switch to report an error. The `show switch` command indicates config mismatch for the new unit and the ports on that unit don’t come up. To resolve this situation, you can change the unit number of the mismatched unit or delete the preconfigured unit type using the `no member <unit-id>` command.

When you add a preconfigured switch to the switch stack, the stack applies either the preconfigured configuration or the default configuration. The following table lists the events:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack master election specifically determined by the MAC address.</td>
<td>Assuming that both stack members have the same priority value and firmware image, restart both stack members at the same time.</td>
<td>The stack member with the higher MAC address is elected stack master.</td>
</tr>
</tbody>
</table>
| Add a stack member. | • Power off the new switch  
   • Through their stacking ports, connect the new switch to a powered-on switch stack.  
   • Power on the new switch. | The stack master is retained. The new switch is added to the switch stack. |
| Stack master failure. | Remove (or power off) the stack master. | One of the remaining stack members becomes the new stack master. All other members in the stack remain stack members and do not reboot. |
that occur when the switch stack compares the preconfigured configuration with the new switch.

Table 2. Preconfigured Switches Compared to Stack Configuration

<table>
<thead>
<tr>
<th>Switch Type Is the Same</th>
<th>Stack Member Number</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Is the same.</td>
<td>The switch stack applies configuration to the preconfigured new switch and adds it to the stack.</td>
</tr>
</tbody>
</table>
| Yes                     | Does not match.     | • The switch stack applies its default stack member number to the preconfigured switch and adds it to the stack.  
  • The stack member number configuration in the preconfigured switch changes to reflect the new information. |
| Is not found in the stack configuration. | | • The switch stack applies the default configuration to the new switch and adds it to the stack.  
  • The preconfigured information is changed to reflect the new information. |
| Is not found in the preconfigured switch. | | The switch stack applies the default configuration to the preconfigured switch and adds it to the stack. |

Renumber Stack Members

This example is provided as CLI commands and a Web interface procedure.

CLI: Renumber Stack Members

**Note:** When issuing a command (such as move management, or renumber), NETGEAR recommends that you wait until the command has fully executed before issuing the next command. For example, if a reset is issued to a stack member, use the `show port` command to verify that the switch has re-merged with the stack, and all ports are joined before issuing the next command.

- If specific numbering is required, NETGEAR recommends that you assign stack members their numbers when they are first installed and configured in the stack, if possible.
- If the stack unit number for a switch is unused, you can renumber the unit by using the `switch <oldunit-id> renumber <newunit-id>` CLI command. This command is found in global config mode.
- If the newunit-id has been preconfigured, you might need to remove the newunit-id from the configuration before renumbering the unit.
If you need to reassign multiple existing stack unit numbers, the configuration could become mismatched. To avoid this situation, NETGEAR recommends that you power down all switches except the master, and then add them back one at a time using the procedure in Section Add Switches to an Operating Stack on page 330.

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.
   
   ![Stack Configuration Screen](image)

   b. Under Stack Configuration, scroll down and select the Unit ID 3 check box.
   c. In the Unit ID list, select 2.
   d. Click Apply.
   e. Now the unit ID of the stacking member is 2.
Move the Stack Master to a Different Unit

This example is provided as CLI commands and a Web interface procedure.

**CLI: Move the Stack Master to a Different Unit**

1. Using the `movemanagement` command, move the master to a different unit number. The operation takes between 30 seconds and 3 minutes depending on the stack size and configuration. The command is `movemanagement <fromunit-id> <tounit-id>`.
2. Make sure that you can log in on the console attached to the new master. Use the `show switch` command to verify that all units rejoined the stack.
3. NETGEAR recommends that you rest the stack with the `reload` command after moving the master.

**Web Interface: Move the Stack Master to a Different Unit**

1. Select System > Management > Basic > Stack Configuration. A screen similar to the following displays.

![Web Interface Screenshot]

2. In the Management Unit Selected list, select 2.
   
   A warning window displays.
3. Click the OK button.
4. Click Apply.

**Note:** If you move a master to a different unit, you might lose the connection to the switch because the IP address could change if the switch gets its IP address using DHCP.
This chapter provides the following examples:

- **Add a New Community**
- **Enable SNMP Trap** on page 338
- **SNMP V3** on page 339
- **sFlow** on page 341
- **Time-Based Sampling of Counters with sFlow** on page 345

**Add a New Community**

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

**CLI: Add a New Community**

```
(Netgear switch) #config
(Netgear switch) (Config)#snmp-server community rw public@4
```
Web Interface: Add a New Community

1. Select System > SNMP > SNMP V1/V2 > Community Configuration. A screen similar to the following displays.

2. In the Community Name field, enter public@4.
3. In the Client Address field, enter 0.0.0.0.
4. In the Client IP Mask field, enter 0.0.0.0.
5. In the Access Mode field, select Read/Write.
6. In the Status field, select Enable.
7. Click Add.

Enable SNMP Trap

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

**CLI: Enable SNMP Trap**

This example shows how to send SNMP trap to the SNMP server.

```
(Netgear switch) #config
(Netgear switch) (Config)# snmptrap public 10.100.5.17
   Enable send trap to SNMP server 10.100.5.17
(Netgear switch) (Config)#snmp-server traps linkmode
   Enable send link status to the SNMP server when
   link status changes.
```
Web Interface: Enable SNMP Trap

1. Enable SNMP trap for the server 10.100.5.17.
   a. Select System > SNMP > SNMP V1/V2 > Trap Configuration. A screen similar to the following displays.

   ![Screen shot of Trap Configuration]

   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.

   ![Screen shot of Trap Flags]

   b. For Link Up/Down, select the Enable radio button.
   c. Click Apply.

SNMP V3

The example is shown as CLI commands and as a Web interface procedure.
CLI: Configure SNMP V3

(Netgear Switch) #config
(Netgear Switch) (Config)#users passwd admin
Enter old password: 
Enter new password:12345678
Confirm new password:12345678
Password Changed!
change the password to “12345678”
(Netgear Switch) (Config)#users snmpv3 authentication admin md5
Set the authentication mode to md5
(Netgear Switch) (Config)#users snmpv3 encryption admin des 12345678
Set the encryption mode to des and the key is “12345678”

Web Interface: Configure SNMP V3

1. Change the user password.
   If you set the authentication mode to MD5, you must make the length of password longer than 8 characters.
   a. Select **Security > Management Security > User Configuration > User Management**. A screen similar to the following displays.

   ![User Management Screen](image)

   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.

```
<table>
<thead>
<tr>
<th>System</th>
<th>Switching</th>
<th>Routing</th>
<th>QoS</th>
<th>Security</th>
<th>Monitoring</th>
<th>Maintenance</th>
<th>Help</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

```
SNMP V3 User Configuration

User

User Name: admin

User Configuration

SNMP v3 Access Mode: Read/Write
Authentication Protocol: None, MD5, SHA
Encryption Protocol: None, DES
Encryption Key: ********
```

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.

![Diagram of network setup with PC, Interface 1/0/2, Interface 1/0/1, Interface 1/0/3, GSM73xxS, Uplink interface 1/0/24, and Switch/Router connected to sFlow collector with IP address 192.168.10.2]

**Figure 38. 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 satagram size is 1400. It can be modified to a value between 200 and 9116 using the command `sflow receiver 1 maxdatagram <size>`.

<table>
<thead>
<tr>
<th>Receiver Owner</th>
<th>Time out</th>
<th>Max Datagram Port</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>String</td>
<td>Size</td>
<td>Size</td>
</tr>
<tr>
<td>----</td>
<td>--------</td>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>1</td>
<td>NetMonit</td>
<td>31535988</td>
<td>1400</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>1400</td>
<td>6343 192.168.10.2</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>1400</td>
<td>6343 0.0.0.0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>1400</td>
<td>6343 0.0.0.0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>1400</td>
<td>6343 0.0.0.0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>1400</td>
<td>6343 0.0.0.0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>1400</td>
<td>6343 0.0.0.0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>1400</td>
<td>6343 0.0.0.0</td>
</tr>
</tbody>
</table>

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.

5. View the sampling port configurations.

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.

![Screen display](image1)

f. Click Apply. A screen similar to the following displays.

![Screen display](image2)

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.

![Screen display](image3)

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.

![Screen display](image4)
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
   Data Source   Receiver  Poller                  Interval
   ------------  ----------   -------------        -------
   1/0/1        1            1                      300
   ```

Web Interface: Configure Time-Based Sampling of Counters with sFlow

1. Configure the sampling ports sFlow receiver index, and polling interval.
   a. Select Monitoring > sFlow > Advanced > sFlow Interface Configuration.
   b. Select the Interface 1/0/1 check box.
   c. In the Poller Interval field, enter 300. A screen similar to the following displays.

   ![sFlow Interface Configuration](image)

   d. Click Apply.
Domain Name System

This chapter provides the following examples:

- Specify Two DNS Servers
- Manually Add a Host Name and an IP Address on page 347

This section describes the Domain Name System (DNS) feature. The DNS protocol maps a host name to an IP address, allowing you to replace the IP address with the host name for IP commands such as a ping and a traceroute, and for features such as RADIUS, DHCP relay, SNTP, SNMP, TFTP, SYSLOG, and UDP relay.

You can obtain the DNS server IP address from your ISP or public DNS server list. DNS is used to resolve the host’s IP address. It enables a static host name entry to be used to resolve the IP address. The following are examples of how the DNS feature is used.

Specify Two DNS Servers

The following example shows how to specify two DNS servers (that is, two IP addresses for DNS servers) and to resolve an IP address using the DNS server. The example is shown as CLI commands and as a Web interface procedure.

**CLI: Specify Two DNS Servers**

```
(Netgear Switch)#config
(Netgear Switch) (Config)#ip name-server 12.7.210.170 219.141.140.10
(Netgear Switch) (Config)#ip domain-lookup
(Netgear Switch) (Config)#exit
(Netgear Switch)#ping www.netgear.com

Send count=3, Receive count=3 from 206.82.202.46
```
Web Interface: Specify Two DNS Servers

1. Select System > Management > DNS > DNS Configuration. A screen similar to the following displays.

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.

![Image of DNS Host Configuration screen]

2. Under DNS Host Configuration, enter the following information:
   - In the **Host Name** field, enter **www.netgear.com**.
   - In the **IP Address** field, enter **206.82.202.46**.

3. Click **Add**.

The host name and IP address now show in the DNS Host Configuration table.
This chapter provides the following examples:

- **Figure** on page 349
- **Configure a DHCP Reservation** on page 352

When a client sends a request to a DHCP server, the DHCP server assigns the IP address from address pools that are specified on the switch. The network in the DHCP pool must belong to the same subnet.

DHCP server allows the switch to dynamically assign an IP address to a DHCP client that is attached to the switch. It also enables the IP address to be assigned based on the client’s MAC address. The following are examples of how the DHCP Server feature is used.

## Configure a DHCP Server in Dynamic Mode

The following example shows how to create a DHCP server with a dynamic pool. The example is shown as CLI commands and as a Web interface procedure.

### CLI: Configure a DHCP Server in Dynamic Mode

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#vlan routing 200
(Netgear Switch) (Vlan)#exit
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#vlan participation include 200
(Netgear Switch) (Interface 1/0/1)#vlan pvid 200
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface vlan 200
(Netgear Switch) (Interface-vlan 200)#routing
(Netgear Switch) (Interface-vlan 200)#ip address 192.168.100.1 255.255.255.0
(Netgear Switch) #config
(Netgear Switch) (Config)#service dhcp
(Netgear Switch) (Config)#ip dhcp pool pool_dynamic
(Netgear Switch) (Config)#network 192.168.100.0 255.255.255.0
```
Note: If there is no DHCP L3 relay between client PC and DHCP server, there must be an active route whose subnet is the same as the DHCP dynamic pool's subnet.

Web Interface: Configure a DHCP Server in Dynamic Mode

1. Create VLAN 200.
   a. Select Switching > VLAN > Basic > VLAN Configuration. A screen similar to the following displays.

   ![VLAN Configuration Screen]

   b. Under VLAN Configuration, in the VLAN ID field, enter 200.
   c. Click Add.

2. Add port 1/0/1 to VLAN 200.
   a. Select Switching > VLAN > Advanced > VLAN Membership. A screen similar to the following displays.

   ![VLAN Membership Screen]

   b. In the VLAN ID field, select 200.
   c. Click Unit 1. The ports display.
d. Click the gray boxes under ports 1 and 24 until U displays. The U specifies that the egress packet is untagged for the port.

e. Click Apply.

3. Assign PVID to the VLAN 200.
   a. Select Switching > VLAN> Advanced > Port PVID Configuration. A screen similar to the following displays.

   ![Port PVID Configuration](image)

   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.

   ![DHCP Server Configuration](image)

   b. For Admin Mode, select the **Enable** radio button.
   c. Click Apply to enable the DHCP service.
d. Select System > Services > DHCP Server > DHCP Pool Configuration. A screen similar to the following displays.

![DHCP Pool Configuration](image)

e. Under DHCP Pool Configuration, enter the following information:
   - In the Pool Name list, select Create.
   - In the Pool Name field, enter pool_dynamic.
   - In the Type of Binding list, select Dynamic.
   - In the Network Number field, enter 192.168.100.0.
   - In the Network Mask field, enter 255.255.255.0. As an alternate, you can enter 24 in the Network Prefix Length field. Do not fill in both the Network Mask field and Network Prefix Length fields.
   - In the Days field, enter 1.

f. Click Add.

The pool_dynamic name is now added to the Pool Name drop-down list.

**Configure a DHCP Reservation**

The following example shows how to create a DHCP server with an IP address pool that is makes fixed IP to MAC address assignments. The example is shown as CLI commands and as a Web interface procedure.
CLI: Configure a DHCP Reservation

{(Netgear Switch)#config
  (Netgear Switch) (Config)#service dhcp
  (Netgear Switch) (Config)#ip dhcp pool pool_manual
  (Netgear Switch) (Config)#client-name 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 Reservation

1. Select System > Services > DHCP Server > DHCP Server Configuration. A screen similar to the following displays.

2. For Admin Mode, select the Enable radio button.
3. Click Apply to enable the DHCP service.
4. Select **System > Services > DHCP Server > DHCP Pool Configuration**. A screen similar to the following displays.

![DHCP Pool Configuration](image)

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 **Host Mask** field, enter **255.255.255.0**. As an alternate, you can enter **24** in the **Network Prefix Length** field.
   - In the **Days** field, enter **1**.

6. Click **Add**. The pool_manual name is now added to the Pool Name drop-down list.
This chapter provides the following examples:

- **CLI: Configure DHCPv6** on page 357
- **Web Interface: Configure an Inter-area Router** on page 358
- **Configure Stateless DHCPv6 Server** on page 362

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is used to assign IPv6 addresses statefully and distribute other configuration information such as domain name or DNS server.

Although DHCPv6 supports stateful address allocation, prefix delegation and stateless services, only prefix delegation mode and stateless service are supported on managed switches. This chapter shows how to configure prefix delegation mode using DHCPv6 pool. When create a DHCPv6 pool, user needs to assign a prefix to client DUID.

DUID is used to identify the client's unique duid value. The format is xx:xx:xx:xx:xx:xx. RFC3315 defines three types:

**a. Link-layer address plus time:**
- 00:01:hardware type:time:link-layer address
- Hardware type - 16 bit hardware type reserved by IANA. 1 means an Ethernet device.
- Time: 32-bit unsigned integer. The time in seconds when this DUID was generated since 00:00:00 1/1/2000.
- Link-layer address - The link layer address of a device generating the DUID.

**b. Vendor-assigned unique ID based on Enterprise Number:**
- 00:02:enterprise-number:identifier
  - Enterprise-number - 32-bit integer reserved by IANA.
  - Identifier - Variable length data for each vendor

**c. Link-layer address:**
- 00:03:hardware type:link-layer address
  - Hardware type - 16 bit hardware type reserved by IANA. 1 means an Ethernet device.
  - Link-layer address - The link layer address of a device generating the DUID.
In the following case, the CPE router requests prefix from the PE router. The PE router chooses prefix (2001:1::/64) for delegation, and responds with the prefix to the requesting CPE router. The CPE router subnets the prefix and assigns the longer prefixes to links in the user’s network. The CPE router is then responsible to assign the 2001:1:1::/96 to one user’s network and 2001:1:2::/96 to another user’s network.

Figure 39. DHCPv6 stateful IPv6 address assignment
CLI: Configure DHCPv6

1. Enable IPv6 routing.

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ipv6 unicast routing
```

2. Create a DHCPv6 pool and enable DHCP service.

```
(Netgear Switch) (Config)#service dhcpv6
(Netgear Switch) (Config)#ipv6 dhcp pool pool1
(Netgear Switch) (Config dhcp6 pool)#domain name netgear.com
(Netgear Switch) (Config dhcp6 pool)#prefix delegation 2001:1::/64
  00:01:00:01:15:40:14:4f:00:00:00:4d:aa:d0
(Netgear Switch) (Config dhcp6 pool)#exit
```

3. Enable DHCPv6 service on port 1/0/9.

```
(Netgear Switch) (Config)#interface 1/0/9
(Netgear Switch) (Interface 1/0/9)#routing
(Netgear Switch) (Interface 1/0/9)#ipv6 address 2001:1::1/64
(Netgear Switch) (Interface 1/0/9)#ipv6 enable
(Netgear Switch) (Interface 1/0/9)#ipv6 dhcp server pool1 preference 20
(Netgear Switch) (Interface 1/0/9)#exit
```

4. Show DHCPv6 binding.

```
(Netgear Switch) #show ipv6 dhcp binding
Client Address................................. FE80::200:FF:FE4D:AAD0
Client Interface............................... 1/0/9
Client DUID.................................... 00:01:00:01:15:40:14:4f:00:00:00:4d:aa:d0
Identity Association ID....................... 5090000
Binding Prefix Address/Length............... 2001:1::/64
Binding Prefix Type ......................... IA_PD
Binding Expiration (secs).................... 4294967284
Binding Prefix Valid Lifetime (secs)........ infinite
Binding Prefix Preferred Lifetime (secs).... infinite
```
Web Interface: Configure an Inter-area Router

1. Enable IP routing globally
   a. Select Routing > IP > Basic > IP Configuration. A screen similar to the following displays.

   ![IP Configuration Screen](image)

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

2. Enable IPv6 unicast globally
   a. Select Routing > IPv6 > Basic > Global Configuration. A screen similar to the following displays.

   ![IPv6 Global Configuration Screen](image)

   b. For IPv6 Unicast Routing, select the Enable radio button.
   c. Click Apply to apply the setting.

3. Enable IPv6 address on interface 1/0/9.
a. Select **Routing > IPv6 > Advanced > Interface Configuration**. A screen similar to the following displays.

![IPv6 Interface Configuration Screen](image)

b. Scroll down and select the interface **1/0/9** check box. Now **1/0/9** appears in the Interface field at the top.

c. Enter the following information:
   - In the IPv6 Mode field, select **Enable**.
   - In the Routing Mode field, select **Enable**.

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

4. Configure prefix on interface **1/0/9**.

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

![IPv6 Prefix Configuration Screen](image)

b. Scroll down and select interface **1/0/9**.

c. Enter the following information:
   - In the IPv6 Prefix field, enter **2001:1::1**.
   - In the Prefix Length field, select **64**.

d. Click **Add** to create IPv6 prefix to interface **1/0/9**.

5. Enable DHCPv6 Server Configuration
a. Select System > Services > DHCPv6 Server > DHCPv6 Server Configuration. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>System</th>
<th>Switching</th>
<th>Routing</th>
<th>QoS</th>
<th>Security</th>
<th>Monitoring</th>
<th>Maintenance</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6 Server</td>
<td>DHCP Relay</td>
<td>DHCP L2 Relay</td>
<td>UDP Relay</td>
<td>DHCPv6 Server Configuration</td>
<td>DHCPv6 Pool Configuration</td>
<td>DHCPv6 Prefix Delegation Configuration</td>
<td>DHCPv6 Interface Configuration</td>
</tr>
</tbody>
</table>

b. For Admin Mode, Select the Enable radio button.

c. Click Apply to apply the setting.

6. Create a DHCPv6 pool named pool1.

a. Select System > Services > DHCPv6 Server > DHCPv6 Pool Configuration. A screen similar to the following displays.

b. From the Pool Name drop-down list, select Create.

c. In the Pool Name field, enter pool1.

d. Click Apply to apply the setting.

7. Configure prefix in the pool1

a. Select System > Services > DHCPv6 Server > DHCPv6 Pool Configuration. A screen similar to the following displays.

b. From the Pool Name drop-down list, select Pool1.
c. Enter 2001:1:: in the Prefix field.
d. In the Prefix Length field, enter 64.
e. In the Prefix field, enter 00:01:00:01:15:40:14:4f:00:00:00:4d:aa:d0.
f. Click Apply to apply the setting.

   a. Select System > Services > DHCPv6 Server > DHCPv6 Interface Configuration.
      A screen similar to the following displays.

      ![DHCPv6 Interface Configuration Screen]

      b. Scroll down and select the interface 1/0/9 check box. Now 1/0/9 appears in the Interface field at the top.
   
   c. Enter the following information:
      - In the Admin mode field, select Enable.
      - In the Pool Name field, enter pool1.
      - In the Administrative Mode field, select Enable.
   
   d. Click Apply to apply the settings.

9. Show DHCPv6 binding.
Select System > Services > DHCPv6 Server > DHCPv6 Binding Information. A screen similar to the following displays.

Configure Stateless DHCPv6 Server

This example uses the DHCPv6 server to configure the information about DNS server to those clients which get IPv6 in autoconfig mode or manual mode. The configured DHCP pool doesn’t contain a prefix pool but contains DNS server to be passed to clients. The IPv6 interface must have the ‘ipv6 nd other-config-flag’ command enabled.

CLI: Configure Stateless DNS Server

This example shows how to configure a DNS server to clients with stateless IPv6 address using DHCPv6 server.

1. Enable ipv6 routing.

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

2. Create an IPv6 pool with DNS server and enable dhcpv6 service.

   (Netgear Switch) (Config)#ipv6 dhcp pool ipv6_server
   (Netgear Switch) (Config-dhcp6s-pool)#dns-server 2011:9:18::1
   (Netgear Switch) (Config-dhcp6s-pool)#exit
   (Netgear Switch) (Config)#service dhcpv6

Note: In this case, you have to configure the command `ipv6 nd other-config-flag` on the interface, otherwise, the host cannot update the DNS with it.

```
(Netgear Switch) (Config)#interface 2/0/21
(Netgear Switch) (Interface 2/0/21)#routing
(Netgear Switch) (Interface 2/0/21)#ipv6 address 2003:1000::1/64
(Netgear Switch) (Interface 2/0/21)#ipv6 enable
(Netgear Switch) (Interface 2/0/21)#ipv6 nd other-config-flag
(Netgear Switch) (Interface 2/0/21)#ipv6 dhcp server ipv6_server
(Netgear Switch) (Interface 2/0/21)#exit
```

Web Interface: Configure Stateless DHCPv6 Server

1. Enable ipv6 routing.
   a. Select **Routing > IPv6 > Basic > Global Configuration**. A screen similar to the following displays:

   ![IPv6 Global Configuration](image)

   b. For IPv6 Unicast Routing, select the **Enable** radio button.
   c. Click **Apply**.

2. Enable ipv6 routing on the interface 2/0/21.
   a. Select **Routing > IPv6 > Advanced > Interface Configuration**. A screen similar to the following displays:

   ![IPv6 Interface Configuration](image)

   b. Under IPv6 Interface Configuration, scroll down and select the Interface **2/0/21** check box. Now 2/0/21 appears in the Interface field at the top.
   c. In the **IPv6 Mode** field, select **Enable**.
   d. In the **Routing Mode** field, select **Enable**.
   e. In the **Adv Other Config Flag** field, select **Enable**.
f. Click **Apply** to save the settings.

3. **Configure IPv6 address on the interface 2/0/21.**
   a. Select **Routing > IPv6 > Advanced > Prefix Configuration**. A screen similar to the following displays:
   ![IPv6 Prefix Configuration Screen](image)
   b. In the Interface list, select **1/0/21**.
   c. In the IPv6 Prefix field, enter **2003:1000::1**.
   d. In the Length field, enter **64**.
   e. In the EUI64 field, select **Disable**.
   f. Click **Add**.

4. **Enable DHCPv6 service.**
   a. Select **System > Services > DHCPv6 Server > DHCPv6 Server Configuration**. A screen similar to the following displays:
   ![DHCPv6 Server Configuration Screen](image)
   b. For Admin Mode, Select the **Enable** radio button.
   c. Click **Apply**.
5. Create DHCPv6 pool.
   a. Select System > Services > DHCP Server > DHCPv6 Pool Configuration. A screen similar to the following displays:
   b. From the Pool Name drop-down list, select Create.
   c. In the Pool Name field, enter ipv6_server.
   d. In the DNS Server Addresses fields, enter 2001:9:18::1 (the DNS server IPv6 address).
   e. Click Apply.

   a. Select System > Services > DHCPv6 Server > DHCPv6 Interface Configuration. A screen similar to the following displays:
   b. Scroll down and select the interface 2/0/21 check box. Now 2/0/21 appears in the Interface field at the top.
   c. Enter the following information:
      • In the Admin mode field, select Enable.
      • In the Pool Name field, enter ipv6_server.
   d. Click Apply.
Double VLANs and Private VLAN Groups

This chapter includes the following examples:
- Double VLANs
- Private VLAN Groups on page 370

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.

![Diagram of Double VLANs](image_url)
The following example shows how to configure the NETGEAR switch shown in the preceding figure to add a double VLAN tag for traffic going from the subnet domain connected to port 1/0/24. This example assumes there is a Layer 2 switch connecting all these devices in your domain. The Layer 2 switch tags the packet going to the NETGEAR switch port 1/0/24. The example is shown as CLI commands and as a Web interface procedure.

**CLI: Enable a Double VLAN**

Create a VLAN 200.

```
(Netgear Switch)#vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#exit
```

Add interface 1/0/24 to VLAN 200, add pvid 200 to port.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan pvid 200
(Netgear Switch) (Interface 1/0/24)#vlan participation include 200
(Netgear Switch) (Interface 1/0/24)#exit
```

Add interface 1/0/48 to the VLAN 200 in a tagging mode.

```
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan participation include 200
(Netgear Switch) (Interface 1/0/48)#vlan tagging 200
(Netgear Switch) (Interface 1/0/48)#exit
```

Select interface 1/0/48 as the provider port.

```
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#mode dvlan-tunnel
(Netgear Switch) (Interface 1/0/48)#exit
```

**Web Interface: Enable a Double VLAN**

1. Create static VLAN 200:
a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays.

![VLAN Configuration](image)

b. Under VLAN Configuration, enter the following information:
   - In the **VLAN ID** field, enter 200.
   - In the **VLAN Name** field, enter vlan200.
   - In the **VLAN Type** field, select Static.

c. Click **Add**.

2. Add ports 24 and 48 to VLAN 200.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays.

![VLAN Membership](image)

b. Under VLAN Membership, in the **VLAN ID** field, select 200.

c. Click **Unit 1**. The ports display:
   - Click the gray box under port 24 twice until U displays. The U specifies that the egress packet is untagged for the port.
• Click the gray box under port 48 once until T displays. The T specifies that the egress packet is tagged for the port.

d. Click Apply to save the settings.

3. Change the port VLAN ID (PVID) of port 24 to 200:
   a. Select Switching > VLAN > Advanced > Port PVID Configuration. A screen similar to the following displays.

   ![Port PVID Configuration Screen](image)
   
   b. Scroll down and select the Interface 1/0/24 check box. Now 1/0/24 appears in the Interface field at the top.
   
   c. In the PVID (1 to 4093) field, enter 200.
   
   d. Click Apply to save the settings.

4. Configure port 48 as the provider service port:
   a. Select Switching > VLAN > Advanced > Port DVLAN Configuration. A screen similar to the following displays.

   ![Port DVLAN Configuration Screen](image)
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 shows 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 41. Private VLAN groups in community mode and isolated mode](image-url)
ProSafe Managed Switch

Chapter 24. Double VLANs and Private VLAN Groups |

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.

```bash
(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.

```bash
(Netgear Switch) (conf-if-range-1/0/16-1/0/17)#exit
```

Web Interface: Create a Private VLAN Group

1. Create VLAN 200.
   a. Select Switching > VLAN > Basic > VLAN Configuration. A screen similar to the following displays.

   ![VLAN Configuration Screen](image)

   b. Enter the following information:
      - In the VLAN ID field, enter 200.
      - In the VLAN Name field, enter VLAN200.
      - In the VLAN Type field, select Static.
   c. Click Add.

2. Add ports 1/0/6, 1/0/7, 1/0/16, and 1/0/17 to VLAN 200.
   a. Select Switching > VLAN > Advanced > VLAN Membership. A screen similar to the following displays.

   ![VLAN Membership Screen](image)
b. Under VLAN Membership, in the VLAN ID list, select 200.

c. Click Unit 1. The ports display.

d. Click the gray boxes under ports 6, 7, 16 and 17 until U displays. The U specifies that the egress packet is untagged for the port.

e. Click Apply.

3. Specify the PVID on ports 1/0/6, 1/0/7, 1/0/16, and 1/0/17.

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

b. Under PVID Configuration, scroll down and select the Interface 1/0/6, 1/0/7, 1/0/16, and 1/0/17 check boxes.

c. In the PVID (1 to 4093) field, enter 200.

d. In the Acceptable Frame Type list, select Admit All.

e. Click Apply to save the settings.

4. Create a private group, group1.


b. In the Group Name field, enter group1.

c. In the Group ID field, enter 1.

d. In the Group Mode list, select community.
e. Click Add.

5. Add port 6 and 7 to group1.
   a. Select Security > Traffic Control > Private Group VLAN > Private Group Membership. A screen similar to the following displays.

   ![Screen display of Private Group Membership]

   b. In the Group ID list, select 1.
   c. Click Unit 1. The ports display.
   d. Click the gray boxes under ports 6 and 7. A check mark displays in each box.
   e. Click Apply.

6. Create a private group, group2.
   a. Select Security > Traffic Control > Private Group VLAN > Private Group Configuration. A screen similar to the following displays.

   ![Screen display of Private Group Configuration]

   b. In the Group Name field, enter group2.
   c. In the Group ID field, enter 2.
   d. In the Group Mode field, select isolated.
   e. Click Add.

7. Add ports 16 and 17 to group2.
a. Select **Security > Traffic Control > Private Group VLAN > Private Group VLAN > Private Group Membership**. A screen similar to the following displays.

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

c. Click **Unit 2**. The ports display.

d. Click the gray boxes under ports 16 and 17, and a check mark displays in each box.

e. Click **Apply**.
This chapter provides the following examples:

- **Configure Classic STP (802.1d)**
- **Configure Rapid STP (802.1w)** on page 378
- **Configure Multiple STP (802.1s)** on page 379

The purpose of Spanning Tree is to eliminate loops in the switch system. There are three STPs: Classic STP (802.1d), Rapid STP (RSTP, 802.1w), and Multiple STP (MSTP, 802.1s).

While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a few seconds. RSTP can revert back to 802.1d in order to interoperate with legacy bridges on a per-port basis. This drops the benefits it introduces.

In Multiple Spanning Tree Protocol (MSTP), each Spanning Tree instance can contain several VLANs. Each Spanning Tree instance is independent of other instances. This approach provides multiple forwarding paths for data traffic, enabling load balancing, and reducing the number of Spanning Tree instances required to support a large number of VLANs.

### Configure Classic STP (802.1d)

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

#### CLI: Configure Classic STP (802.1d)

```bash
(Netgear Switch) (Config)# spanning-tree
(Netgear Switch) (Config)# spanning-tree forceversion 802.1d
(Netgear switch) (Interface 1/0/3)# spanning-tree port mode
```
Web Interface: Configure Classic STP (802.1d)

1. Enable 802.1d on the switch.
   a. Select Switching > STP > STP Configuration. A screen similar to the following displays.
      - 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.
   b. Click Apply.

2. Configure the CST port.
   a. Select Switching > STP > CST Port Configuration. A screen similar to the following displays.
      - 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.
   b. In the Port Mode field, select Enable.
   d. Click Apply.
Configure Rapid STP (802.1w)

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

**CLI: Configure Rapid STP (802.1w)**

```
(Netgear switch) (Config)# spanning-tree
(Netgear switch) (Config)# spanning-tree forceversion 802.1w
(Netgear switch) (Interface 1/0/3)# spanning-tree port mode
```

**Web Interface: Configure Rapid STP (802.1w)**

1. Enable 802.1w on the switch:
   a. Select *Switching > STP > STP Configuration*. A screen similar to the following displays.

   ![STP Configuration Screen](image)

   b. Enter the following information:
      - For Spanning Tree Admin Mode, select the **Enable** radio button.
      - For Force Protocol Version, select the **IEEE 802.1w** radio button.
   c. Click **Apply**.

2. Configure the CST port.
a. Select **Switching > STP > CST Port Configuration**. A screen similar to the following displays.

![CST Port Configuration](image)

b. Under CST Port Configuration, scroll down and select the Interface 1/0/3 check box. Now 1/0/3 appears in the Interface field at the top.

c. In the **Port Mode** field, select **Enable**.

d. Click **Apply**.

**Configure Multiple STP (802.1s)**

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

**CLI: Configure Multiple STP (802.1s)**

```
(Netgear switch) (Config)# spanning-tree
(Netgear switch) (Config)# spanning-tree forceversion 802.1s
(Netgear switch) (Config)# spanning-tree mst instance 1
Create a mst instance 1
(Netgear switch) (Config)# spanning-tree mst priority 1 4096
(Netgear switch) (Config)# spanning-tree mst vlan 1 2
(Netgear switch) (Config)# spanning-tree mst vlan 1 3
Associate the mst instance 1 with the VLAN 2 and 3
(Netgear switch) (Config)# spanning-tree mst instance 2
Create a mst instance 2
(Netgear switch) (Config)# spanning-tree mst priority 2 4096
(Netgear switch) (Config)# spanning-tree mst vlan 2 11
(Netgear switch) (Config)# spanning-tree mst vlan 2 12
Associate the mst instance 2 with the VLAN 11 and 12
(Netgear switch) (Interface 1/0/3)# spanning-tree mst 1 port-priority 128
(Netgear switch) (Interface 1/0/3)# spanning-tree mst 1 cost 0
```
Web Interface: Configure Multiple STP (802.1s)

1. Enable 802.1s on the switch.
   a. Select Switching > STP > STP Configuration. A screen similar to the following displays.

   b. Enter the following information:
      • For Spanning Tree Admin Mode, select the Enable radio button.
      • For Force Protocol Version, select the IEEE 802.1s radio button.
   c. Click Apply.

2. Configure MST.
   a. Select Switching > STP > MST Configuration. A screen similar to the following displays.

   b. Configure MST ID 1.
      • In the MST ID field, enter 1.
      • In the Priority field, enter 4096.
• In the **VLAN Id** field, enter 2.
• Click **Add**.
• In the **VLAN Id** field, enter 3.
• Click **Apply**.

c. Configure MST ID 2.
• In the **MST ID** field, enter 2.
• In the **Priority** field, enter 4096.
• In the **VLAN Id** field, enter 11.
• Click **Add**.
• In the **VLAN Id** field, enter 12.
• Click **Apply**.

3. Configure the MST port.

   a. Select **Switching > STP > MST Port Status**. A screen similar to the following displays.

   ![MST Port Configuration Screen](image)

   4. Under MST Port Configuration, scroll down and select the Interface 1/0/3 check box. Now 1/0/3 appears in the Interface field at the top.

   5. Enter the following information:
      • In the **Port Priority** field, enter 128.
      • In the **Port Path Cost** field, enter 0.

   6. Click **Apply**.
There are two methods for IPv6 sites to communicate with each other over the IPv4 network: 6in4 tunnel and 6to4 tunnel. The 6in4 tunnel encapsulates IPv6 traffic over an explicitly configured IPv4 destination or end port of the tunnel with the IP protocol number set to 41. The 6to4 tunnel IPv6 prefix is constructed by prepending 2002 (hex) to the global IPv4 address. For example, if the IPv4 address is 4.4.4.1, the tunnel IPv6 prefix would be 2002:404:401::/16.

The 6to4 tunnels are automatically formed IPv4 tunnels carrying IPv6 traffic. The automatic tunnel’s IPv4 destination address is derived from the 6to4 IPv6 address of the tunnel’s nexthop. It supports the functionality of a 6to4 border router that connects a 6to4 site to a 6to4 domain. It sends/receives tunneled traffic from routers in a 6to4 domain that includes other 6to4 border routers and 6to4 relay routers. The example creates a 6in4 tunnel between GSM7328S_1 and GSM7328S_2. The tunnel carries IPv6 packets over IPv4 packets.

Figure 42. 6in4 tunnel between two switches
CLI: Create a Tunnel

Configure Switch GSM7328S_1

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ipv6 forwarding
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.1.1 255.255.255.0
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface tunnel 0
(Netgear Switch) (Interface tunnel 0)#ipv6 enable
(Netgear Switch) (Interface tunnel 0)#ipv6 address 2000::1/64
(Netgear Switch) (Interface tunnel 0)#tunnel mode ipv6ip
(Netgear Switch) (Interface tunnel 0)#tunnel source 192.168.1.1
(Netgear Switch) (Interface tunnel 0)#tunnel destination 192.1.168.1.2
(Netgear Switch) (Interface tunnel 0)#exit
(Netgear Switch) (Config)#exit
```

This example is using 6in4 mode. If you want to use 6to4 mode, configure each unit as below and be sure the IPv6 prefix is constructed in the format of 2002:V4ADDR::/48. (V4ADDR is the IPv4 address of the tunnel source port). In this case, IPv4 and the address is 192.168.1.1 and IPv6 prefix is 2002:c0a8:0101::

```
(Netgear Switch) (Interface tunnel 0) # ipv6 enable
(Netgear Switch) (Interface tunnel 0) # tunnel mode ipv6ip 6to4
(Netgear Switch) (Interface tunnel 0) # tunnel source 192.168.1.1
(Netgear Switch) (Interface tunnel 0) # ipv6 address 2002:c0a8:0101::1/128
(Netgear Switch) (Interface tunnel 0) # exit
(Netgear Switch) (Config) # ipv6 route 2002::/16 interface tunnel 0
```
Configure Switch GSM7328S_2

(Netgear Switch) #show interfacet tunnel 0
Interface Link Status......................... Up
IPv6 is enabled
IPv6 Prefix is .............................. FE80::C0A8:101/128
2000::1/64
MTU size..................................... 1280 bytes
#show interface tunnel
TunnelId Interface TunnelMode SourceAddress DestinationAddress
--------  ---------  ----------  -------------  ------------------
0         tunnel 0   6 in 4 Configured 192.168.1.1  192.168.1.2
(Netgear Switch) # ping ipv6 2000::2
Send count=3, Receive count=3 from 2000::2
Average round trip time = 1.00 ms

(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ipv6 forwarding
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ip address 192.168.1.2 255.255.255.0
(Netgear Switch) (Interface 1/0/13)#exit

(Netgear Switch) (Config)#interface tunnel 0
(Netgear Switch) (Interface tunnel 0)#ipv6 enable
(Netgear Switch) (Interface tunnel 0)#ipv6 address 2000::2/64
(Netgear Switch) (Interface tunnel 0)#tunnel mode ipv6ip
(Netgear Switch) (Interface tunnel 0)#tunnel source 192.168.1.2
(Netgear Switch) (Interface tunnel 0)#tunnel destination 192.168.1.1
(Netgear Switch) (Interface tunnel 0)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #show interface tunnel
TunnelId Interface TunnelMode SourceAddress DestinationAddress
--------  ---------  ----------  -------------  ------------------
0 tunnel 0       6 in 4 Configured 192.168.1.2  192.168.1.1
Web Interface: Create a Tunnel

Configure Switch GSM7328S_1

1. Enable IP routing on the switch.
   a. Select Routing > IP > Basic > IP Configuration. A screen similar to the following displays.
   
   ![IP Configuration Screen](image)
   
   b. For Routing Mode, select the Enable radio button.
   c. Click Apply.

2. Enable IPv6 forwarding and unicast routing on the switch.
   a. Select Routing > IPv6 > Basic > Global Configuration. A screen similar to the following displays.
   
   ![IPv6 Global Configuration Screen](image)
   
   b. For IPv6 Unicast Routing, select the Enable radio button.
   c. For IPv6 Forwarding, select the Enable radio button.
   d. Click Apply.

3. Create a routing interface and assign an IP address to it.
a. Select **Routing > IP > Advanced > IP Interface Configuration.** A screen similar to the following displays.

![IP Interface Configuration](image)

- **Port**
- **Description**
- **VLAN ID**
- **IP Address**
- **Subnet Mask**
- **Routing Mode**
- **Administrative Mode**

- **1/0/1**
- **192.168.1.1**
- **255.255.255.0**
- **Enable**
- **Enable**

b. Under IP Interface Configuration, scroll down and select the Port 1/0/1 check box. Now 1/0/1 appears in the Interface field at the top.
   - In the **IP Address** field, enter **192.168.1.1**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Routing Mode** field, select **Enable**.

c. Click **Apply**.

4. **Create a 6-in-4 tunnel interface.**

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

   ![Tunnel Configuration](image)

   - **Tunnel Id**
   - **IPv6 Node**
   - **IPv6 Unreachables**
   - **IPv6 Address**
   - **Prefix**
   - **Source Interface**
   - **Destination Address**
   - **Source Address**
   - **Destination Interface**
   - **Tunnel Configuration**

   - **0**
   - **Enabled**
   - **192.168.1.1**
   - **192.168.1.2**

   b. In the **Tunnel Id** list, select **0**.
   c. In the **Mode** field, select **6-in-4-configured**.
   d. In the **Source Address** field, enter **192.168.1.1**.
   e. In the **Destination Address** field, enter **192.168.1.2**.
   f. Click **Apply**.

5. **Assign an IPv6 address to the tunnel.**
a. Select **Routing > IPv6 > Advanced > Prefix Configuration**. A screen similar to the following displays.

b. In the **Interface** list, select **0/7/1**.

c. In the **IPv6 Prefix** field, enter **2000::1**.

d. In the **Length** field, enter **64**.

e. In the **EUI64** field, select **Disable**.

f. Click **Add**.

**Configure Switch GSM7328S_2**

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

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

c. Click **Apply**.

2. Enable IPv6 forwarding and unicast routing on the switch.
388 | Chapter 26. Tunnel

a. Select Routing > IPv6 > Basic > Global Configuration. A screen similar to the following displays.

b. For IPv6 Unicast Routing, select the Enable radio button.

c. For IPv6 Forwarding, select the Enable radio button.

d. Click Apply.

3. Create a routing interface and assign an IP address to it.

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

   b. Under IP Interface Configuration, scroll down and select the Port 1/0/13 check box. Now 1/0/1 appears in the Port field at the top.
      - In the IP Address field, enter 192.168.1.2.
      - In the Subnet Mask field, enter 255.255.255.0.
      - In the Routing Mode field, select Enable.

   c. Click Apply.

4. Create a 6-in-4 tunnel interface.
a. Select Routing > IPv6 > Advanced > Tunnel Configuration. A screen similar to the following displays.

b. In the Tunnel Id list, select 0.

c. In the Mode list, select 6-in-4-configured.

d. In the Source Address field, enter 192.168.1.2.

e. In the Destination Address field, enter 192.168.1.1.

f. Click Apply.

5. Assign an IPv6 address to the tunnel.

a. Select Routing > IPv6 > Advanced > Prefix Configuration. A screen similar to the following displays.

b. In the Interface list, select 0/7/1.

c. In the IPv6 Prefix field, enter 2000::2.

d. In the Length field, enter 64.

e. In the EUI64 field, select Disable.

f. Click Add.
This chapter provides the following examples:

- *Create an IPv6 Routing Interface*
- *Create an IPv6 Network Interface* on page 393
- *Create an IPv6 Routing VLAN* on page 395
- *Configure DHCPv6 Mode on the Routing Interface* on page 400

## Create an IPv6 Routing Interface

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

### CLI: Create an IPv6 Routing Interface

1. Enable IPV6 forwarding and unicast routing on the switch.

```
(Netgear Switch) (Config)#ipv6 forwarding
(Netgear Switch) (Config)#ipv6 unicast-routing
```
2. Assign an IPv6 address to interface 1/0/1.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#ipv6 enable
(Netgear Switch) (Interface 1/0/1)#ipv6 address 2000::2/64
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) #ping ipv6 2000::2
Send count=3, Receive count=3 from 2000::2
Average round trip time = 1.00 ms
(Netgear Switch) #show ipv6 brief
IPv6 Forwarding Mode........................... Enable
IPv6 Unicast Routing Mode...................... Enable
IPv6 Hop Limit................................. 0
ICMPv6 Rate Limit Error Interval............... 1000 msec
ICMPv6 Rate Limit Burst Size................... 100 messages
Maximum Routes................................. 12
```

```
(Netgear Switch) #show ipv6 interface 1/0/1
IPv6 is enabled
IPv6 Prefix is ................................ FE80::21E:2AFF:FED9:249B/128
2000::2/64 [TENT]
Routing Mode................................. Enabled
Administrative Mode............................ Enabled
IPv6 Routing Operational Mode................. Enabled
Bandwidth..................................... 1000000 kbps
Interface Maximum Transmit Unit.............. 1500
Router Duplicate Address Detection Transmits... 1
Router Advertisement NS Interval............... 0
Router Advertisement Lifetime............... 1800
Router Advertisement Reachable Time......... 0
Router Advertisement Interval............... 600
Router Advertisement Managed Config Flag...... Disabled
Router Advertisement Other Config Flag........ Disabled
Router Advertisement Suppress Flag............ Disabled
IPv6 Destination Unreachables............... Enabled
Prefix 2000::2/64
Preferred Lifetime........................... 604800
Valid Lifetime................................ 2592000
Onlink Flag.................................. Enabled
Autonomous Flag.............................. Enabled
```
Web Interface: Create an IPv6 Routing Interface

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

   ![IPv6 Global Configuration Screen]

   b. For IPv6 Unicast Routing, select the Enable radio button.
   c. For IPv6 Forwarding, select the Enable radio button.
   d. Click Apply.

2. Enable IPv6 routing on interface 1/0/1.
   a. Select Routing > IPv6 > Advanced > Interface Configuration. A screen similar to the following displays.

   ![IPv6 Interface Configuration Screen]

   b. Under IPv6 Interface Configuration, scroll down and select the Interface 1/0/1 check box. Now 1/0/1 appears in the Interface field at the top.
   c. In the IPv6 Mode field, select Enable.
   d. Click Apply to save the settings.

3. Assign an IPv6 address to the routing interface.
a. Select Routing > IPv6 > Advanced > Prefix Configuration. A screen similar to the following displays.

b. In the Interface list, select 1/0/1.

c. In the IPv6 Prefix field, enter 2000::2.

d. In the Length field, enter 64.

e. In the EUI64 field, select Disable.

f. Click Add.

Create an IPv6 Network Interface

The IPv6 network interface is the logical interface used for in-band connectivity with the switch using any of the switch’s front panel ports. The configuration parameters associated with the switch’s network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

To access the switch over an IPv6 network you must first configure it with IPv6 information (IPv6 prefix, prefix length, and default gateway).
CLI: Configure the IPv6 Network Interface

(Netgear Switch) #network ipv6 enable
(Netgear Switch) #network ipv6 address 2001:1::1/64
(Netgear Switch) #network ipv6 gateway 2001:1::2
(Netgear Switch) #show network

Interface Status............................... Always Up
IP Address..................................... 0.0.0.0
Subnet Mask.................................... 0.0.0.0
Default Gateway................................ 0.0.0.0
IPv6 Administrative Mode....................... Enabled
IPv6 Prefix is ................................ FE80::2FF:F9FF:FE70:485/64
IPv6 Prefix is ................................ 2001:1::1/64
IPv6 Default Router............................ 2001:1::2
Burned In MAC Address......................... 00:FF:F9:70:04:85
Locally Administered MAC address............. 00:00:00:00:00:00
MAC Address Type............................ Burned In
Configured IPv4 Protocol....................... None
Configured IPv6 Protocol....................... None
IPv6 AutoConfig Mode........................ Disabled
Management VLAN ID.........................1

Web Interface: Configure the IPv6 Network Interface

1. Add an IPv6 address to the network interface.
   a. Select System > Management > Network Interface > IPv6 Network Configuration. A screen similar to the following displays.

   ![IPv6 Network Interface Configuration Screen]

   b. For Admin Mode, select the Enable radio button.
   c. In the IPv6 Prefix/Prefix Length field, enter 2001:1::1/64.
   d. In the EUI64 field, select False.
   e. Click Add.
2. Add an IPv6 gateway to the network interface.
   a. Select System > Management > Network Interface > IPv6 Network Configuration. A screen similar to the following displays.

   ![IPv6 Network Interface Configuration](image)

   b. In the IPv6 Gateway field, enter 2001:1::2.
   c. Click Apply.

Create an IPv6 Routing VLAN

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

**CLI: Create an IPv6 Routing VLAN**

1. Create a routing VLAN with VLAN ID 500.

   ```
   Netgear Switch) (Vlan)#vlan 500
   (Netgear Switch) (Vlan)#vlan routing 500
   (Netgear Switch) (Vlan)#exit
   ```

2. Add interface 1/0/1 to VLAN 500.

   ```
   (Netgear Switch) #config
   (Netgear Switch) (Config)#interface 1/0/1
   (Netgear Switch) (Interface 1/0/1)#vlan participation include 500
   (Netgear Switch) (Interface 1/0/1)#vlan participation pvid 500
   (Netgear Switch) (Interface 1/0/1)#exit
   ```
3. Assign IPv6 address 2000::1/64 to VLAN 500 and enable IPv6 routing.

```
(Netgear Switch) (Config)#interface vlan 0/4/1
(Netgear Switch) (Interface 0/4/1)#routing
(Netgear Switch) (Interface 0/4/1)#ipv6 enable
(Netgear Switch) (Interface 0/4/1)#ipv6 address 2000::1/64
(Netgear Switch) (Interface 0/4/1)#exit
```

4. Enable IPV6 forwarding and unicast routing on the switch.

```
(Netgear Switch) (Config)#ipv6 forwarding
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) #ping ipv6 2000::2
Send count=3, Receive count=3 from 2000::2
Average round trip time = 1.00 ms
(Netgear Switch) #show ipv6 brief
IPv6 Forwarding Mode........................... Enable
IPv6 Unicast Routing Mode...................... Enable
IPv6 Hop Limit.................................. 0
ICMPv6 Rate Limit Error Interval............. 1000 msec
ICMPv6 Rate Limit Burst Size............... 100 messages
Maximum Routes.............................. 128
(Netgear Switch) #show ipv6 interface 0/4/1
IPv6 is enabled
IPv6 Prefix is ................................ FE80::21E:2AFF:FED9:249B/128
2000::1/64
Routing Mode.................................... Enabled
Administrative Mode............................ Enabled
IPv6 Routing Operational Mode.............. Enabled
Bandwidth..................................... 10000  kbps
Interface Maximum Transmit Unit........... 1500
Router Duplicate Address Detection Transmits 1
Router Advertisement NS Interval........... 0
Router Advertisement Lifetime.............. 1800
Router Advertisement Reachable Time....... 0
Router Advertisement Interval.............. 600
Router Advertisement Managed Config Flag.... Disabled
Router Advertisement Other Config Flag..... Disabled
Router Advertisement Suppress Flag.......... Disabled
IPv6 Destination Unreachables............... Enabled
Prefix 2000::1/64
Preferred Lifetime......................... 604800
Valid Lifetime............................... 2592000
Onlink Flag.................................. Enabled
Autonomous Flag............................. Enabled
```

396 | Chapter 27. IPv6 Interface Configuration
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.
   
   ![VLAN Configuration Screen](image1)

   b. In the VLAN ID field, enter 500.
   c. In the VLAN Type field, select Static.
   d. Click Add.

2. Add ports to VLAN 500.
   a. Select Switching > VLAN > Advanced > VLAN Membership. A screen similar to the following displays.
   
   ![VLAN Membership Screen](image2)

   b. In the VLAN ID list, select 500.
   c. Click Unit 1. The ports display.
   d. Click the gray box under port 1 until U displays, indicating that the egress packet is untagged for the port.
   e. Click Apply.

3. Specify the PVID on port 1/0/1.
a. Select **Switching > VLAN > Advanced > Port PVID Configuration**. A screen similar to the following displays.

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

c. In the **PVID (1 to 4093)** field, enter **500**.

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

4. Enable IPv6 forwarding and unicast routing on the switch.

a. Select **Routing > IPv6 > Basic > Global Configuration**. A screen similar to the following displays.

b. For IPv6 Unicast Routing, select the **Enable** radio button.

c. For IPv6 Forwarding, select the **Enable** radio button.

d. Click **Apply**.

5. Enable IPv6 routing on the VLAN.
a. Select Routing > IPv6 > Advanced > Interface Configuration. A screen similar to the following displays.

![IPv6 Interface Configuration Screen]

b. Click VLANS. The logical VLAN interface 0/4/2 displays.

c. Select the 0/4/2 check box.

d. Under IPv6 Interface Configuration, in the IPv6 Mode field, select Enable.

e. Click Apply.

6. Assign an IPv6 address to the routing VLAN.

a. Select Routing > IPv6 > Advanced > Prefix Configuration. A screen similar to the following displays.

![IPv6 Prefix Configuration Screen]

b. In the Interface field, select 0/4/2.

c. In the IPv6 Prefix field, enter 2000::1.

d. In the Length field, enter 64.

e. In the EUI64 field, select Disable.

f. Click Add.
Configure DHCPv6 Mode on the Routing Interface

The routing interface supports DHCPv6 mode, which can get the IPv6 address from a DHCPv6 server (address allocation).

**Note:** Before you enable DHCPv6 mode, you have to disable IPv6 unicast mode globally.

CLI: Configure DHCPv6 mode on routing interface

1. Enable IPv6 unicast globally.

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

2. Enable DHCPv6 on the interface 1/0/23.

   ```
   (Netgear Switch) (Config)#interface 1/0/23
   (Netgear Switch) (Interface 1/0/23)#routing
   (Netgear Switch) (Interface 1/0/23)#ipv6 enable
   (Netgear Switch) (Interface 1/0/23)#ipv6 address dhcp
   (Netgear Switch) (Interface 1/0/23)
   ```
3. Show the ipv6 address assigned from 1/0/23.

```
(Netgear Switch) #show ipv6 interface 1/0/23
IPv6 is enabled
IPv6 Prefix is ................................ FE80::E291:F5FF:FE06:2BF6/128
............................................. 2000::1D5C:7CFE:828F:8144/128 [DHCP]
Routing Mode................................... Enabled
IPv6 Enable Mode................................ Enabled
Administrative Mode............................ Enabled
IPv6 Operational Mode.......................... Enabled
Bandwidth...................................... 1000000 kbps
Interface Maximum Transmit Unit.............. 1500
Router Duplicate Address Detection Transmits... 1
Address DHCP Mode............................. Enabled
Router Advertisement NS Interval............... 0
Router Advertisement Lifetime................. 1800
Router Advertisement Reachable Time........... 0
Router Advertisement Interval.................. 600
Router Advertisement Managed Config Flag..... Disabled
Router Advertisement Other Config Flag........ Disabled
Router Advertisement Router Preference....... medium
Router Advertisement Suppress Flag............ Disabled
IPv6 Destination Unreachables................ Enabled
```

Web Interface: Configure DHCPv6 mode on routing interface

1. Enable IPv6 unicast globally.
   a. Select Routing > IPv6 > Basic > Global Configuration. A screen similar to the following displays.

   ![IPv6 Global Configuration](image)

   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.

![IPv6 Interface Configuration](client-ipv6 interface.bmp)

b. Scroll down and select the **interface 1/0/23** check box. Now 1/0/23 appears in the Interface field at the top.

c. Enter the following information:
   - In the IPv6 Mode field, select **Enable**.
   - In the Routing Mode field, select **Enable**.
   - In the DHCPv6 Client Mode field, select **Enable**.

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

3. Show the ipv6 address assigned from 1/0/23.

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

![IPv6 Prefix Configuration](client-ipv6 interface.bmp)

b. Scroll down and select the **interface 1/0/23**. You can see the IPv6 address assigned by the DHCPv6 server.
This chapter provides the following examples:

- **PIM-DM**
- **PIM-SM** on page 427

**Note:** The PIM protocol can be configured to operate on IPv4 and IPv6 networks. Separate CLI commands are provided for IPv4 and IPv6 operation; however, most configuration options are common to both protocols. Therefore, this section describes only IPv4 configuration; IPv6 configuration is similar to IPv4.

Multicast protocols are used to deliver multicast packets from one source to multiple receivers. They facilitate better bandwidth utilization, and use less host and router processing, making them ideal for usage in applications such as video and audio conferencing, whiteboard tools, stock distribution tickers, and so on. PIM is a widely used multicast routing protocol. Protocol Independent Multicast (PIM) is a standard multicast routing protocol that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. There are two types of PIM:

- PIM-Dense Mode (PIM-DM)
- PIM-Sparse Mode (PIM-SM)

**PIM-DM**

PIM-DM is appropriate for:

- Densely distributed receivers
- A ratio of few senders to many receivers (due to frequent flooding)
- High volume of multicast traffic
- Constant stream of traffic
PIM-DM uses the existing unicast routing table and join, prune, and graft mechanism to build a tree. PIM-DM creates source-based shortest-path distribution trees making use of reverse path forwarding (RPF). PIM-DM cannot be used to build a shared distribution tree, as PIM-SM can. PIM-DM assumes that when a sender starts sending data, all downstream routers and hosts want to receive a multicast datagram. PIM-DM initially floods multicast traffic throughout the network. Routers that do not have any downstream neighbors prune back the unwanted traffic. Apart from the prune messages, PIM-DM makes use of two more messages: graft and assert. Graft messages are used whenever a new host wants to join the group. Assert messages are used to shut off duplicate flows onto the same multi-access network.

To minimize the repeated flooding of datagrams and subsequent pruning associated with a particular (S,G) pair, PIM-DM uses a state refresh message. This message is sent by the routers directly connected to the source and is propagated throughout the network. When
received by a router on its RPF interface, the state refresh message causes an existing prune state to be refreshed. State refresh messages are generated periodically by the router directly attached to the source. There are two versions of PIM-DM. Version 2 does not use IGMP messages; instead, it uses a message that is encapsulated in IP packets with protocol number 103. In version 2, the Hello message is introduced in place of the query message.

**CLI: Configure PIM-DM**

**PIM-DM on Switch A**

1. Enable IP routing on the switch.

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

2. Enable pimdm on the switch.

   ```
   (Netgear Switch) (Config)#ip pim dense
   ```

3. Enable IP multicast forwarding on the switch.

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

4. Enable RIP to build the unicast IP routing table.

   ```
   (Netgear Switch) (Config)#interface 1/0/1
   (Netgear Switch) (Interface 1/0/1)#routing
   (Netgear Switch) (Interface 1/0/1)#ip address 192.168.2.2 255.255.255.0
   (Netgear Switch) (Interface 1/0/1)#ip rip
   ```
5. Enable PIM-DM on the interface.

```
(Netgear Switch) (Interface 1/0/1)#ip pim dense
(Netgear Switch) (Interface 1/0/1)#exit

(Netgear Switch) (Config)#interface 1/0/9
(Netgear Switch) (Interface 1/0/9)#routing
(Netgear Switch) (Interface 1/0/9)#ip address 192.168.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/9)#ip rip
(Netgear Switch) (Interface 1/0/9)#ip pim dense
(Netgear Switch) (Interface 1/0/9)#exit

(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ip address 192.168.1.2 255.255.255.0
(Netgear Switch) (Interface 1/0/13)#ip rip
(Netgear Switch) (Interface 1/0/13)#ip pim dense
(Netgear Switch) (Interface 1/0/13)#exit
```

**PIM-DM on Switch B**

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim dense
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#interface 1/0/10
(Netgear Switch) (Interface 1/0/10)#routing
(Netgear Switch) (Interface 1/0/10)#ip address 192.168.3.2 255.255.255.0
(Netgear Switch) (Interface 1/0/10)#ip rip
(Netgear Switch) (Interface 1/0/10)#ip pim dense
(Netgear Switch) (Interface 1/0/10)#exit
(Netgear Switch) (Config)#interface 1/0/11
(Netgear Switch) (Interface 1/0/11)#routing
(Netgear Switch) (Interface 1/0/11)#ip address 192.168.5.1 255.255.255.0
(Netgear Switch) (Interface 1/0/11)#ip rip
(Netgear Switch) (Interface 1/0/11)#ip pim dense
(Netgear Switch) (Interface 1/0/11)#exit
```
**PIM-DM on Switch C**

```bash
(Netgear Switch) #configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim dense
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address 192.168.5.2 255.255.255.0
(Netgear Switch) (Interface 1/0/21)#ip rip
(Netgear Switch) (Interface 1/0/21)#ip pim dense
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) (Config)#interface 1/0/22
(Netgear Switch) (Interface 1/0/22)#routing
(Netgear Switch) (Interface 1/0/22)#ip address 192.168.6.1 255.255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22)#ip pim dense
(Netgear Switch) (Interface 1/0/22)#exit
```

**PIM-DM on Switch D**

1. Enable IGMP on the switch.

```bash
(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 pimd dense
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) (Config)#interface 1/0/22
(Netgear Switch) (Interface 1/0/22)#routing
(Netgear Switch) (Interface 1/0/22)#ip address 192.168.6.2 255.255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22)#ip pim dense
(Netgear Switch) (Interface 1/0/22)#exit
```
2. Enable IGMP on 1/0/24.

```markdown
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#routing
(Netgear Switch) (Interface 1/0/24)#ip pim dense
(Netgear Switch) (Interface 1/0/24)#ip igmp
(Netgear Switch) (Interface 1/0/24)#ip rip
(Netgear Switch) (Interface 1/0/24)#ip address 192.168.1.1  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
<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Protocol</th>
<th>Interface</th>
<th>Interface List</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>225.1.1.1</td>
<td>PIMDM</td>
<td>1/0/13</td>
<td>1/0/1</td>
</tr>
</tbody>
</table>

(B) #show ip mcast mroute summary
Multicast Route Table Summary
<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Protocol</th>
<th>Interface</th>
<th>Interface List</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>225.1.1.1</td>
<td>PIMDM</td>
<td>1/0/10</td>
<td></td>
</tr>
</tbody>
</table>

(C) #show ip mcast mroute summary
Multicast Route Table Summary
<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Protocol</th>
<th>Interface</th>
<th>Interface List</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>225.1.1.1</td>
<td>PIMDM</td>
<td>1/0/21</td>
<td></td>
</tr>
</tbody>
</table>

(D) #show ip mcast mroute summary
Multicast Route Table Summary
<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Protocol</th>
<th>Interface</th>
<th>Interface List</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>225.1.1.1</td>
<td>PIMDM</td>
<td>7/0/21</td>
<td>7/0/24</td>
</tr>
</tbody>
</table>
```
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.

   ![IP Configuration Screen]

   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.

   ![IP Interface Configuration Screen]

   b. Under IP Interface Configuration, scroll down and select the Port 1/0/1 check box. Now 1/0/1 appears in the Port field at the top.
   c. Enter the following information:
      • In the IP Address field, enter 192.168.2.2.
      • In the Subnet Mask field, enter 255.255.255.0.
      • In the Routing Mode field, select Enable.
   d. Click Apply to save the settings.

3. Configure 1/0/9 as a routing port and assign an IP address to it.
a. Select Routing > IP > Advanced > IP Interface Configuration. A screen similar to the following displays.

b. Scroll down and select the Port 1/0/9 check box. Now 1/0/9 appears in the Port field at the top.

c. Enter the following information:
   - In the IP Address field, enter 192.168.3.1.
   - In the Subnet Mask field, enter 255.255.255.0.
   - In the Routing Mode field, select Enable.

d. Click Apply.

4. Configure 1/0/13 as a routing port and assign an IP address to it.

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

b. Under IP Interface Configuration, scroll down and select the Port 1/0/13 check box. Now 1/0/13 appears in the Port field at the top.

c. Enter the following information:
   - In the IP Address field, enter 192.168.1.2.
   - In the Subnet Mask field, enter 255.255.255.0.
5. Enable RIP on the interface 1/0/1.
   a. Select Routing > RIP > Advanced > Interface Configuration. A screen similar to the following displays.
   
   ![Interface Configuration Screen](image)

   b. In the Interface list, select 1/0/1.
   c. For RIP Admin Mode, select the Enable radio button.
   d. Click Apply.

   a. Select Routing > RIP > Advanced > Interface Configuration. A screen similar to the following displays.

   ![Interface Configuration Screen](image)

   b. In the Interface field, select 1/0/9.
   c. For RIP Admin Mode, select the Enable radio button.
   d. Click Apply.

7. Enable RIP on interface 1/0/13.
a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

![Interface Configuration Screen](image)

b. In the **Interface** list, select **1/0/13**.

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

d. Click **Apply**.

8. Enable multicast globally.

a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.

![Global Configuration Screen](image)

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

c. Click **Apply**.


a. Select **Routing > Multicast > PIM > Global Configuration**. A screen similar to the following displays.

![PIM Global Configuration Screen](image)
b. For PIM Protocol Type, select the **PIM-DM** radio button.

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

d. Click **Apply**.

10. Enable PIM-DM on interfaces 1/0/1, 1/0/9, and 1/0/13.

a. Select **Routing > Multicast > PIM > Interface Configuration**. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Mode</th>
<th>Protocol State</th>
<th>IP Address</th>
<th>Hello Interval (secs)</th>
<th>Join/Prune Interval (secs)</th>
<th>DRR Border</th>
<th>DR Priority</th>
<th>D R</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/1</td>
<td>Disable</td>
<td>Non-Operational</td>
<td>192.168.2.2</td>
<td>30</td>
<td>Disable</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/0/2</td>
<td>Disable</td>
<td>Non-Operational</td>
<td>0.0.0.0</td>
<td>30</td>
<td>60</td>
<td>Disable</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1/0/3</td>
<td>Disable</td>
<td>Non-Operational</td>
<td>0.0.0.0</td>
<td>30</td>
<td>60</td>
<td>Disable</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1/0/4</td>
<td>Disable</td>
<td>Non-Operational</td>
<td>0.0.0.0</td>
<td>30</td>
<td>60</td>
<td>Disable</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1/0/5</td>
<td>Disable</td>
<td>Non-Operational</td>
<td>0.0.0.0</td>
<td>30</td>
<td>60</td>
<td>Disable</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1/0/6</td>
<td>Disable</td>
<td>Non-Operational</td>
<td>0.0.0.0</td>
<td>30</td>
<td>60</td>
<td>Disable</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1/0/7</td>
<td>Disable</td>
<td>Non-Operational</td>
<td>0.0.0.0</td>
<td>30</td>
<td>60</td>
<td>Disable</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1/0/8</td>
<td>Disable</td>
<td>Non-Operational</td>
<td>0.0.0.0</td>
<td>30</td>
<td>60</td>
<td>Disable</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1/0/9</td>
<td>Disable</td>
<td>Non-Operational</td>
<td>192.168.2.2</td>
<td>30</td>
<td>60</td>
<td>Disable</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1/0/10</td>
<td>Disable</td>
<td>Non-Operational</td>
<td>0.0.0.0</td>
<td>30</td>
<td>60</td>
<td>Disable</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1/0/11</td>
<td>Disable</td>
<td>Non-Operational</td>
<td>0.0.0.0</td>
<td>30</td>
<td>60</td>
<td>Disable</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1/0/12</td>
<td>Disable</td>
<td>Non-Operational</td>
<td>0.0.0.0</td>
<td>30</td>
<td>60</td>
<td>Disable</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1/0/13</td>
<td>Disable</td>
<td>Non-Operational</td>
<td>192.168.1.2</td>
<td>30</td>
<td>60</td>
<td>Disable</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1/0/14</td>
<td>Disable</td>
<td>Non-Operational</td>
<td>0.0.0.0</td>
<td>30</td>
<td>60</td>
<td>Disable</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

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.

   ![Screen Shot](image1)

   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.

   ![Screen Shot](image2)

   b. Scroll down and select the Port 1/0/10 check box. Now 1/0/10 appears in the Port field at the top.
   c. Enter the following information:
      - In the IP Address field, enter 192.168.3.2.
      - In the Subnet Mask field, enter 255.255.255.0.
      - In the Routing Mode field, select Enable.
   d. Click Apply to save the settings.

3. Configure 1/0/11 as a routing port and assign an IP address to it.
a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

![IP Interface Configuration](image)

b. Under IP Interface Configuration, scroll down and select the Port 1/0/11 check box. Now 1/0/11 appears in the Port field at the top.

c. Enter the following information:
   - In the **IP Address** field, enter **192.168.5.1**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Routing Mode** field, select **Enable**.

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

4. Enable RIP on interface 1/0/10.

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

   ![Interface Configuration](image)

   b. In the **Interface** list, select **1/0/10**.

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

   d. Click **Apply**.

5. Enable RIP on interface 1/0/11.
a. Select Routing > RIP > Advanced > Interface Configuration. A screen similar to the following displays.

b. In the Interface list, select 1/0/11.
c. For RIP Admin Mode, select the Enable radio button.
d. Click Apply.

6. Enable multicast globally.

a. Select Routing > Multicast > Global Configuration. A screen similar to the following displays.

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

7. Enable PIM-DM globally.

a. Select Routing > Multicast > PIM > Global Configuration. A screen similar to the following displays.
b. For PIM Protocol Type, select the PIM-DM radio button.
c. For Admin Mode, select the Enable radio button.
d. Click Apply.

8. Enable PIM-SM on interfaces 1/0/10 and 1/0/11.

a. Select Routing > Multicast > PIM > Interface Configuration. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/10</td>
<td>Enable</td>
</tr>
<tr>
<td>1/0/11</td>
<td>Enable</td>
</tr>
</tbody>
</table>

b. Scroll down and select the Interface 1/0/10 and 1/0/11 check box.
c. In the Admin Mode field, select Enable.
d. Click Apply to save the settings.

**PIM-DM on Switch C**

1. Enable IP routing on the switch.

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

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

2. Configure 1/0/21 as a routing port and assign an IP address to it.
a. Select Routing > IP > Advanced > IP Interface Configuration. A screen similar to the following displays.

b. Scroll down select the Port 1/0/21 check box. Now 1/0/21 appears in the Interface field at the top.

c. Enter the following information:
   • In the IP Address field, enter **192.168.5.2**.
   • In the Subnet Mask field, enter **255.255.255.0**.
   • In the Routing Mode field, select Enable.

d. Click Apply to save the settings.

3. Configure 1/0/22 as a routing port and assign an IP address to it.
   a. Select Routing > IP > Advanced > IP Interface Configuration. A screen similar to the following displays.

   ![IP Interface Configuration Screen](image)

   b. Scroll down and select the Port 1/0/22 check box. Now 1/0/22 appears in the Port field at the top.

   c. Enter the following information:
      • In the IP Address field, enter **192.168.6.1**.
      • In the Subnet Mask field, enter **255.255.255.0**.
      • In the Routing Mode field, select Enable.

   d. Click Apply to save the settings.

4. Enable RIP on interface 1/0/21.
a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

![Interface Configuration Screen](image)

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.

![Interface Configuration Screen](image)

b. In the **Interface** list, select 1/0/22.

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

d. Click **Apply**.

6. Enable multicast globally.
a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.

![Global Configuration screen](image)

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.

![PIM Global Configuration screen](image)

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.
PIM on Switch A:

a. Select Routing > Multicast > PIM > Interface Configuration. A screen similar to the following displays.

b. Scroll down and select the 1/0/21 and 1/0/22 check boxes.

c. In the PIM Interface Configuration, in the Admin Mode field, select Enable.

d. Click Apply to save the settings.

PIM-DM on Switch D:

1. Enable IP routing on the switch.

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

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

c. Click Apply.

2. Configure 1/0/21 as a routing port and assign an IP address to it.
a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

```
<table>
<thead>
<tr>
<th>Part</th>
<th>Description</th>
<th>VLAN ID</th>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/21</td>
<td></td>
<td></td>
<td>192.168.2.1</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>
```

b. Scroll down and select the Port 1/0/21 check box. Now 1/0/21 appears in the Port field at the top.

c. Enter the following information in the IP Interface Configuration:
   - In the **IP Address** field, enter **192.168.2.1**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Routing Mode** field, select **Enable**.

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

3. Configure 1/0/22 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

```
<table>
<thead>
<tr>
<th>Part</th>
<th>Description</th>
<th>VLAN ID</th>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/22</td>
<td></td>
<td></td>
<td>192.168.6.2</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>
```

b. Scroll down and select the Port 1/0/22 check box. Now 1/0/22 appears in the Interface field at the top.

c. Enter the following information:
   - In the **IP Address** field, enter **192.168.6.2**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Routing Mode** field, select **Enable**.

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

4. Configure 1/0/24 as a routing port and assign an IP address to it.
a. Select Routing > IP > Advanced > IP Interface Configuration. A screen similar to the following displays.

b. Scroll down and select the Port 1/0/24 check box. Now 1/0/24 appears in the Interface field at the top.
c. Enter the following information:
   - In the IP Address field, enter 192.168.4.1.
   - In the Subnet Mask field, enter 255.255.255.0.
   - In the Routing Mode field, select Enable.
d. Click Apply to save the settings.

5. Enable RIP on interface 1/0/21.
   a. Select Routing > RIP > Advanced > Interface Configuration. A screen similar to the following displays.
   b. In the Interface list, select t 1/0/21.
   c. For RIP Admin Mode, select the Enable radio button.
   d. Click Apply.
6. Enable RIP on interface 1/0/22.
a. Select Routing > RIP > Advanced > Interface Configuration. A screen similar to the following displays.

b. In the Interface list, select 1/0/22.

c. For RIP Admin Mode, select the Enable radio button.

d. Click Apply.

7. Enable RIP on interface 1/0/24.

a. Select Routing > RIP > Advanced > Interface Configuration. A screen similar to the following displays.

b. In the Interface list, select 1/0/24.

c. For RIP Admin Mode, select the Enable radio button.

d. Click Apply.

8. Enable multicast globally.
a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.

![Global Configuration Screen](image)

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

c. Click **Apply**.


a. Select **Routing > Multicast > PIM > Global Configuration**. A screen similar to the following displays.

![PIM Global Configuration Screen](image)

b. For PIM Protocol Type, select the **PIM-SM** radio button.

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

d. Click **Apply**.

10. Enable PIM-DM on interfaces 1/0/21, 1/0/22, and 1/0/24.
a. Select **Routing > Multicast > PIM > Interface Configuration**. A screen similar to the following displays.

b. Scroll down and select the Interface 1/0/21, 1/0/22, and 1/0/24 check boxes.
c. In the **Admin Mode** field, select **Enable**.
d. Click **Apply** to save the settings.

**11.** Enable IGMP globally.

a. Select **Routing > Multicast > IGMP > Global Configuration**. A screen similar to the following displays.

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

**12.** Enable IGMP on interface 1/0/24.

a. Select **Routing > Multicast > IGMP > Interface Configuration**. A screen similar to the following displays.
b. Scroll down and select the interface 1/0/24 check box.

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

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

**PIM-SM**

Protocol-independent multicast sparse mode (PIM-SM) is used to efficiently route multicast traffic to multicast groups that can span wide area networks where bandwidth is a constraint.

---

**Figure 44. PIM-SM**

PIM-SM uses shared trees by default and implements source-based trees for efficiency; it assumes that no hosts want the multicast traffic unless they specifically ask for it. It creates a shared distribution tree centered on a defined rendezvous point (RP). Traffic from this source
is relayed to the receivers. Senders first send the multicast data to the RP, which in turn sends the data down the shared tree to the receivers. Shared trees centered on an RP do not necessarily provide the shortest, most optimal path. In such cases PIM-SM provides a means to switch to more efficient source-specific trees. A data threshold rate is defined for toggling between trees. PIM-SM uses a bootstrap router (BSR), which advertises information to other multicast routers about the RP. In a given network, a set of routers can be administratively enabled as candidate bootstrap routers. If it is not apparent which router should be the BSR, the candidates flood the domain with advertisements. The router with the highest priority is elected. If all the priorities are equal, then the candidate with the highest IP address becomes the BSR. PIM-SM is defined in RFC 4601.

The following example describes how to configure and use PIM-SM. In this case, set the switch B,C,D as RP-candidate and BSR-candidate. Switch B will become the BSR because it has the highest priority. Switch D will become the RP after RP election.

**CLI: Configure PIM-SM**

**PIM-SM on Switch A**

1. Enable IP routing on the switch.

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

2. Enable PIM-SM on the switch.

   ```
   (Netgear Switch) (Config)#ip pim sparse
   ```

3. Enable IP multicast forwarding on the switch.

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

4. Enable RIP to build a unicast IP routing table.

   ```
   (Netgear Switch) (Config)#interface 1/0/1
   (Netgear Switch) (Interface 1/0/1)#routing
   (Netgear Switch) (Interface 1/0/1)#ip address 192.168.2.2  255.255.255.0
   (Netgear Switch) (Interface 1/0/1)#ip rip
   ```
### PIM-SM on Switch B

1. Enable the switch to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

   ```
   (Netgear Switch)#configure
   (Netgear Switch) (Config)#ip routing
   (Netgear Switch) (Config)#ip pim sparse
   (Netgear Switch) (Config)#ip multicast
   (Netgear Switch) (Config)#ip pim sparse rp-candidate interface 1/0/11 225.1.1.1 255.255.255.0
   ```

2. Enable the switch to announce its candidacy as a bootstrap router (BSR).

   ```
   (Netgear Switch) (Config)#ip pim sparse bsr-candidate interface 1/0/10 30 7
   ```
PIM-SM on Switch C

(Netgear Switch)#configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim sparse
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#ip pim sparse rp-candidate interface 1/0/22 225.1.1.1 255.255.255.0
(Netgear Switch) (Config)#ip pim sparse bsr-candidate interface 1/0/21 30 5
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address 192.168.5.2 255.255.255.0
(Netgear Switch) (Interface 1/0/21)#ip rip
(Netgear Switch) (Interface 1/0/21)#ip pim sparse
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) (Config)#interface 1/0/22
(Netgear Switch) (Interface 1/0/22)#routing
(Netgear Switch) (Interface 1/0/22)#ip address 192.168.6.1 255.255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22)#ip pim sparse
(Netgear Switch) (Interface 1/0/22)#exit

PIM-SM on Switch D

(Netgear Switch)#configure
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip igmp
(Netgear Switch) (Config)#ip pim sparse
(Netgear Switch) (Config)#ip pim rp-candidate interface 1/0/22 225.1.1.1 255.255.255.0
(Netgear Switch) (Config)#ip pim bsr-candidate interface 1/0/22 30 3
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address 192.168.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/21)#ip rip
(Netgear Switch) (Interface 1/0/21)#ip pim sparse
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) (Config)#interface 1/0/22
(Netgear Switch) (Interface 1/0/22)#routing
(Netgear Switch) (Interface 1/0/22)#ip address 192.168.6.2 255.255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22)#ip pim sparse
(Netgear Switch) (Interface 1/0/22)#exit
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.

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Protocol</th>
<th>Interface</th>
<th>Interface List</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>225.1.1.1</td>
<td>PIMSM</td>
<td>1/0/13</td>
<td>1/0/1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Protocol</th>
<th>Interface</th>
<th>Interface List</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>225.1.1.1</td>
<td>PIMSM</td>
<td>1/0/10</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Protocol</th>
<th>Interface</th>
<th>Interface List</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>225.1.1.1</td>
<td>PIMSM</td>
<td>1/0/22</td>
<td></td>
</tr>
<tr>
<td>192.168.1.1</td>
<td>225.1.1.1</td>
<td>PIMSM</td>
<td>1/0/21</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Protocol</th>
<th>Interface</th>
<th>Interface List</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>225.1.1.1</td>
<td>PIMSM</td>
<td>1/0/22</td>
<td>1/0/24</td>
</tr>
<tr>
<td>192.168.1.1</td>
<td>225.1.1.1</td>
<td>PIMSM</td>
<td>1/0/21</td>
<td>1/0/24</td>
</tr>
</tbody>
</table>
Web Interface: Configure PIM-SM

PIM-SM on Switch A

1. Enable IP routing on the switch.
   a. Select Routing > IP > Basic > IP Configuration. A screen similar to the following displays.
   b. For Routing Mode, select the Enable radio button.
   c. Click Apply.

2. Configure 1/0/1 as a routing port and assign an IP address to it.
   a. Select Routing > IP > Advanced > IP Interface Configuration. A screen similar to the following displays.
   b. Scroll down and select the interface 1/0/1 check box. Now 1/0/1 appears in the Interface field at the top.
   c. Enter the following information:
      • In the IP Address field, enter 192.168.2.2.
      • In the Subnet Mask field, enter 255.255.255.0.
      • In the Routing Mode field, select Enable.
   d. Click Apply to save the settings.

3. Configure 1/0/9 as a routing port and assign an IP address to it.
a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

![ProSafe Managed Switch Interface Configuration](image)

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.

![ProSafe Managed Switch Interface Configuration](image)

b. Scroll down and select the interface 1/0/13 check box. Now 1/0/13 appears in the Interface field at the top.

c. Enter the following information:
   - In the **IP Address** field, enter **192.168.1.2**.
• In the **Subnet Mask** field, enter **255.255.255.0**.
• In the **Routing Mode** field, select **Enable**.

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

5. Enable RIP on interface 1/0/1.
   a. Select **Routing > RIP > Advanced > Interface Configuration**. A screen similar to the following displays.

   ![Interface Configuration](image)

   b. In the **Interface** field, select **1/0/1**.
   c. For RIP Admin Mode, select the **Enable** radio button.
   d. Click **Apply**.

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

   ![Interface Configuration](image)

   b. In the **Interface** field, select **1/0/9**.
   c. For RIP Admin Mode, select the **Enable** radio button.
   d. Click **Apply**.

7. Enable RIP on interface 1/0/13.
a. Select Routing > RIP > Advanced > Interface Configuration. A screen similar to the following displays.

b. Select 1/0/13 in the Interface field.

c. For RIP Admin Mode, select the Enable radio button.

d. Click Apply.

8. Enable multicast globally.

a. Select Routing > Multicast > Global Configuration. A screen similar to the following displays.

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

c. Click Apply.


a. Select Routing > Multicast > PIM > Global Configuration. A screen similar to the following displays.
b. For PIM Protocol Type, select the PIM-SM radio button.

c. For Admin Mode, select the Enable radio button.

d. Click Apply.

10. Enable PIM-SM on interfaces 1/0/1, 1/0/9, and 1/0/13.

a. Select Routing > Multicast > PIM > Interface Configuration. A screen similar to the following displays.

b. Scroll down and select the Interface 1/0/1, 1/0/9, and 1/0/13 check boxes.

c. In the Admin Mode field, select Enable.

d. Click Apply to save the settings.

**PIM-SM on Switch B:**

1. Enable IP routing on the switch.

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

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

c. Click Apply.
2. Configure 1/0/10 as a routing port and assign an IP address to it.
   a. Select Routing > IP > Advanced > IP Interface Configuration. A screen similar to the following displays.

   ![IP Interface Configuration Screen](image)

   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.

   ![IP Interface Configuration Screen](image)

   b. Scroll down and select the Port 1/0/11 check box. Now 1/0/11 appears in the Port field at the top.

   c. Enter the following information:
      - In the IP Address field, enter 192.168.5.1.
      - In the Subnet Mask field, enter 255.255.255.0.
      - In the Routing Mode field, select Enable.

   d. Click Apply to save the settings.

4. Enable RIP on interface 1/0/10.
a. Select Routing > RIP > Advanced > Interface Configuration. A screen similar to the following displays.

b. In the Interface field, select 1/0/10.

c. For RIP Admin Mode, select the Enable radio button.

d. Click Apply.

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

a. Select Routing > RIP > Advanced > Interface Configuration. A screen similar to the following displays.

b. In the Interface list, select 1/0/11.

c. For RIP Admin Mode, select the Enable radio button.

d. Click Apply.

6. Enable multicast globally.
a. Select Routing > Multicast > Global Configuration. A screen similar to the following displays.

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

c. Click Apply.

7. Enable PIM-SM globally.

a. Select Routing > Multicast > PIM > Global Configuration. A screen similar to the following displays.

b. For PIM Protocol Type, select the PIM-SM radio button.

c. For Admin Mode, select the Enable radio button.

d. Click Apply.

8. Enable PIM-SM on interfaces 1/0/10 and 1/0/11.
a. Select Routing > Multicast > PIM > Interface Configuration. A screen similar to the following displays.

b. Scroll down and select the Interface 1/0/10 and 1/0/11 check boxes.

c. In the Admin Mode field, select Enable.

d. Click Apply to save the settings.

9. Set up the candidate RP configuration.

a. Select Routing > Multicast > PIM > Candidate RP Configuration. A screen similar to the following displays.

b. In the Interface list, select 1/0/11.

c. In the Group IP field, enter 225.1.1.1.

d. In the Group Mask field, enter 255.255.255.0.

e. Click Add.

10. Set up the BSR candidate configuration.
a. Select **Routing > Multicast > PIM > BSR Candidate Configuration**. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>System</th>
<th>Switching</th>
<th>Routing</th>
<th>QoS</th>
<th>Security</th>
<th>Monitoring</th>
<th>Maintenance</th>
<th>Help</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![PIM BSR Candidate Configuration](image)

b. In the **Interface** list, select the **1/0/10**.

c. In the **Hash Mask Length** field, enter **30**.

d. In the **Priority** field, enter **7**.

e. Click **Apply**.

**PIM-SM on Switch C:**

1. Enable IP routing on the switch.

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

![IP Configuration](image)

   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.

![Image of IP Interface Configuration screen]

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.

   ![Image of IP Interface Configuration screen]

   b. Scroll down and select the 1/0/22 check box. Now 1/0/22 appears in the Interface field at the top.

   c. Enter the following information:
      - In the IP Address field, enter 192.168.6.1.
      - In the Subnet Mask field, enter 255.255.255.0.
      - In the Routing Mode field, select Enable.

   d. Click Apply to save the settings.

4. Enable RIP on the interface 1/0/21.
a. Select Routing > RIP > Advanced > Interface Configuration. A screen similar to the following displays.

![Interface Configuration Screen](image)

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.

   ![Interface Configuration Screen](image)

b. In the **Interface** list, select 1/0/22.
c. For RIP Admin Mode, select the **Enable** radio button.
d. Click **Apply**.

6. Enable multicast globally.
a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.

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

c. Click **Apply**.

7. Enable PIM-SM globally.

a. Select **Routing > Multicast > PIM > Global Configuration**. A screen similar to the following displays.

b. For PIM Protocol Type, select the **PIM-SM** radio button.

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

d. Click **Apply**.

8. Enable PIM-SM on interfaces 1/0/21 and 1/0/22.
a. Select Routing > Multicast > PIM > Interface Configuration. A screen similar to the following displays.

![PIM Interface Configuration screen](image1)

b. Scroll down and select the Interface 1/0/21 and 1/0/22 check boxes.

c. In the Admin Mode field, select Enable.

d. Click Apply to save the settings.

9. Candidate RP Configuration.

a. Select Routing > Multicast > PIM > Candidate RP Configuration. A screen similar to the following displays.

![PIM Candidate RP Configuration screen](image2)

b. In the Interface list, select 1/0/22.

c. In the Group IP field, enter 225.1.1.1.

d. In the Group Mask field, enter 255.255.255.0.

e. Click Add.

10. BSR Candidate Configuration.
a. Select Routing > Multicast > PIM > BSR Candidate Configuration. A screen similar to the following displays.

b. In the Interface list, select the 1/0/21.

c. In the Hash Mask Length field, enter 30.

d. In the Priority field, enter 5.

e. Click Apply.

**PIM-SM on Switch D**

1. Enable IP routing on the switch.

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

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

c. Click Apply.

2. Configure 1/0/21 as a routing port and assign an IP address to it.
a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

![IP Interface Configuration](image)

b. Scroll down and select the Interface 1/0/21 check box. Now 1/0/21 appears in the Interface field at the top.

c. Enter the following information:
   - In the **IP Address** field, enter **192.168.2.1**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Routing Mode** field, select **Enable**.

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

3. Configure 1/0/22 as a routing port and assign an IP address to it.

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

![IP Interface Configuration](image)

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.

![IP Interface Configuration](image)

b. Scroll down and select the Interface 1/0/24 check box. Now 1/0/24 appears in the Interface field at the top.

c. Enter the following information:
   - In the **IP Address** field, enter 192.168.4.1.
   - In the **Subnet Mask** field, enter 255.255.255.0.
   - In the **Routing Mode** field, select **Enable**.

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

5. Enable RIP on interface 1/0/21.

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

   ![Interface Configuration](image)

   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.

![Interface Configuration screen](image1)

b. In the Interface list, select 1/0/22.

c. For RIP Admin Mode, select the Enable radio button.

d. Click Apply.

7. Enable RIP on interface 1/0/24.

a. Select Routing > RIP > Advanced > Interface Configuration. A screen similar to the following displays.

![Interface Configuration screen](image2)

b. In the Interface list, select 1/0/24.

c. For RIP Admin Mode, select the Enable radio button.

d. Click Apply.

8. Enable multicast globally.
a. Select Routing > Multicast > Global Configuration. A screen similar to the following displays.

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

c. Click Apply.


a. Select Routing > Multicast > PIM > Global Configuration. A screen similar to the following displays.

b. For PIM Protocol Type, select the PIM-SM radio button.

c. For Admin Mode, select the Enable radio button.

d. Click Apply.

10. Enable PIM-SM on interfaces 1/0/21, 1/0/22, and 1/0/24.
a. Select **Routing > Multicast > PIM > Interface Configuration**. A screen similar to the following displays.

![Interface Configuration Screen](image)

b. Scroll down and select the Interface 1/0/21, 1/0/22, and 1/0/24 check boxes.

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

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

11. Set up Candidate RP configuration.

a. Select **Routing > Multicast > PIM > Candidate RP Configuration**. A screen similar to the following displays.

![Candidate RP Configuration Screen](image)

b. In the **Interface** list, select 1/0/22.

c. In the **Group IP** field, enter **225.1.1.1**.

d. In the **Group Mask** field, enter **255.255.255.0**.

e. Click **Add**.

12. Set up BSR Candidate configuration.
a. Select **Routing > Multicast > PIM > BSR Candidate Configuration**. A screen similar to the following displays.

![BSR Candidate Configuration](image)

b. In the **Interface** list, select 1/0/22.

c. In the **Hash Mask Length** field, enter 30.

d. In the **Priority** field, enter 3.

e. Click **Apply**.

13. Enable IGMP globally.

a. Select **Routing > Multicast > IGMP > Global Configuration**. A screen similar to the following displays.

![IGMP Global Configuration](image)

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

c. Click **Apply**.

a. Select **Routing > Multicast > IGMP > Interface Configuration**. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Mode</th>
<th>Version</th>
<th>Robustness</th>
<th>Query Int</th>
<th>Max Resp Time</th>
<th>Start Query Interval</th>
<th>Start Query Count</th>
<th>Last Member Query Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/24</td>
<td>Enable</td>
<td>V3</td>
<td>2</td>
<td>125</td>
<td>100</td>
<td>31</td>
<td>2</td>
<td>10</td>
</tr>
</tbody>
</table>

b. Under IGMP Routing Interface Configuration, scroll down and select the Interface 1/0/24 check box.

c. In the Admin Mode field, select Enable.

d. Click **Apply** to save the settings.
This chapter includes the following sections:

- **DHCP L2 Relay**
- **DHCP L3 Relay** on page 460
- **Configure a DHCP L3 Switch** on page 465

**DHCP L2 Relay**

DHCP relay agents eliminate the need to have a DHCP server on each physical network. Relay agents populate the `giaddr` field and also append the `Relay Agent Information` option to the DHCP messages. DHCP servers use this option for IP addresses and other parameter assignment policies. These DHCP relay agents are typically IP routing-aware devices and are referred to as Layer 3 relay agents.

In some network configurations, there is a need for Layer 2 devices to append the relay agent Information option as they are closer to the end hosts.

![Figure 45. DHCP L2 Relay](image)
These Layer 2 devices typically operate only as bridges for the network and might not have an IPv4 address on the network. Lacking a valid IPv4 source address, they cannot relay packets directly to a DHCP server located on another network. These Layer 2 devices append the Relay agent information option and broadcast the DHCP message. This section provides information about where a Layer 2 relay agent fits in and how it is used.

**CLI: Enable DHCP L2 Relay**

1. Enter the following commands:

   ```
   (Netgear Switch)#vlan database
   (Netgear Switch)(Vlan)#vlan 200
   (Netgear Switch)(Vlan)#exit
   ```

2. Enable the DHCP L2 relay on the switch.

   ```
   (Netgear Switch) (Config)#dhcp l2relay
   (Netgear Switch) (Config)#dhcp l2relay vlan 200
   ```

3. Enable the Option 82 Circuit ID field.

   ```
   (Netgear Switch) (Config)#dhcp l2relay circuit-id vlan 200
   ```

4. Enable the Option 82 Remote ID field.

   ```
   (Netgear Switch) (Config)#dhcp l2relay remote-id rem_id vlan 200
   ```

5. Enable DHCP L2 relay on port 1/0/4.

   ```
   (Netgear Switch) (Config)#interface 1/0/4
   (Netgear Switch) (Interface 1/0/4)# dhcp l2relay
   ```

   ```
   (Netgear Switch) (Interface 1/0/4)# vlan pvid 200
   (Netgear Switch) (Interface 1/0/4)# vlan participation include 200
   (Netgear Switch) (Interface 1/0/4)# exit
   ```
6. Enable DHCP L2 relay on port 1/0/5.

```
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)# dhcp l2relay
(Netgear Switch) (Interface 1/0/5)# vlan pvid 200
(Netgear Switch) (Interface 1/0/5)# vlan participation include 200
(Netgear Switch) (Interface 1/0/5)# exit
```

7. Enable DHCP L2 relay on port 1/0/6.

```
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)# dhcp l2relay
```

8. Trust packets with option 82 received on port 1/0/6.

```
(Netgear Switch) (Interface 1/0/6)# dhcp l2relay trust
(Netgear Switch) (Interface 1/0/6)# vlan pvid 200
(Netgear Switch) (Interface 1/0/6)# vlan participation include 200
(Netgear Switch) (Interface 1/0/6)# exit
```

Web Interface: Enable DHCP L2 Relay

1. Create VLAN 200.
   a. Select Switching > VLAN > Basic > VLAN Configuration. A screen similar to the following displays.

   ![VLAN Configuration Screen](image)

   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.
ProSafe Managed Switch

Chapter 29. DHCP L2 Relay and L3 Relay

29.1 DHCP L2 Relay and L3 Relay

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

![VLAN Membership Screen](image)

- **b.** In the **VLAN ID** field, select **200**.
- **c.** Click **Unit 1.** The ports display.
- **d.** Click the gray boxes under ports 4, 5, and 6 until **U** displays. The U specifies that the egress packet is untagged for the port.
- **e.** Click **Apply**.

3. Specify the PVID on ports 1/0/4, 1/0/5 and 1/0/6.

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

![Port PVID Configuration Screen](image)

- **b.** Scroll down and select the Interface 1/0/4, 1/0/5, and 1/0/6 check boxes.
- **c.** In the **PVID (1 to 4093)** field, enter **200**.
- **d.** Click **Apply** to save the settings.

4. Enable DHCP L2 relay on VLAN 200.
a. Select System > Services > DHCP L2 Relay > DHCP L2 Relay Configuration. A screen similar to the following displays.

```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Mode</th>
<th>82 Option Trust Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/1</td>
<td>Enable</td>
<td>Enable</td>
</tr>
<tr>
<td>1/0/2</td>
<td>Disable</td>
<td>Disable</td>
</tr>
<tr>
<td>1/0/3</td>
<td>Disable</td>
<td>Disable</td>
</tr>
<tr>
<td>1/0/4</td>
<td>Enable</td>
<td>Enable</td>
</tr>
<tr>
<td>1/0/5</td>
<td>Disable</td>
<td>Disable</td>
</tr>
<tr>
<td>1/0/6</td>
<td>Enable</td>
<td>Enable</td>
</tr>
</tbody>
</table>
```

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

c. Scroll down and select the VLAN ID 200 check box.

d. Enter the following information:
   - In the Admin Mode field, select Enable.
   - In the Circuit ID Mode field, select Enable.
   - In the Remote ID String field, enter rmt_id.

e. Click Apply to save the settings.

5. Enable DHCP L2 Relay on interfaces 1/0/4, 1/0/5, and 1/0/6.

a. Select System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration. A screen similar to the following displays.

```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Mode</th>
<th>82 Option Trust Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/1</td>
<td>Enable</td>
<td>Enable</td>
</tr>
<tr>
<td>1/0/2</td>
<td>Disable</td>
<td>Disable</td>
</tr>
<tr>
<td>1/0/3</td>
<td>Disable</td>
<td>Disable</td>
</tr>
<tr>
<td>1/0/4</td>
<td>Enable</td>
<td>Enable</td>
</tr>
<tr>
<td>1/0/5</td>
<td>Disable</td>
<td>Disable</td>
</tr>
<tr>
<td>1/0/6</td>
<td>Enable</td>
<td>Enable</td>
</tr>
</tbody>
</table>
```

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.

a. Select **System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration**. A screen similar to the following displays.

![DHCP L2 Relay Configuration Screen](image)

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 46. DHCP L3 relay

Configure the DHCP Server Switch

CLI: Configure a DHCP Server

1. Enable routing on the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#
```
2. Create a routing interface and enable RIP on it so that the DHCP server learns the route 10.200.1.0/24 from the DHCP L3 relay.

{(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 10.100.1.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#ip rip
(Netgear Switch) (Interface 1/0/3)#exit}

3. Create a DHCP pool.

{(Netgear Switch) (Config)#ip dhcp pool dhcp_server
(Netgear Switch) (Config-dhcp-pool)#network 10.200.1.0 255.255.255.0
(Netgear Switch) (Config-dhcp-pool)#exit
(Netgear Switch) (Config)#ip dhcp pool dhcp_server_second
(Netgear Switch) (Config-dhcp-pool)#network 10.200.2.0 255.255.255.0
(Netgear Switch) (Config-dhcp-pool)#exit
(Netgear Switch) (Config)#service dhcp
(Netgear Switch) (Config)#exit}

4. Exclude the IP address 10.200.1.1 and 10.200.2.1 from the DHCP pool because it has been used on the DHCP L3 relay.

{(Netgear Switch) (Config)#ip dhcp excluded-address 10.200.1.1
(Netgear Switch) (Config)#ip dhcp excluded-address 10.200.2.1}

Web Interface: Configure a DHCP Server

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

   ![DHCP Configuration Screen](image)

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

2. Create a routing interface and assign 10.100.1.1/24 to it.
a. Select Routing > IP > Advanced > IP Interface Configuration. A screen similar to the following displays.

![IP Interface Configuration Screen]

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

c. In the IP Address field, enter 10.100.1.1.

d. In the Subnet Mask field, enter 255.255.255.0.

e. In the Routing Mode field, select Enable.

f. Click Apply to save the settings.

3. Enable RIP on interface 1/0/3.

a. Select Routing > RIP > Advanced > Interface Configuration. A screen similar to the following displays.

![Interface Configuration Screen]

b. In the Interface field, select 1/0/3.

c. For RIP Admin Mode, select the Enable radio button.

4. Set up the DHCP global configuration.
a. Select System > Services > DHCP Server > DHCP Server Configuration. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>System</th>
<th>Switching</th>
<th>Routing</th>
<th>QoS</th>
<th>Security</th>
<th>Monitoring</th>
<th>Maintenance</th>
<th>Help</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Server</td>
<td>DHCP Server Configuration</td>
<td>DHCP Pool Configuration</td>
<td>DHCP Pool Options</td>
<td>DHCP Server Statistics</td>
<td>DHCP Bindings Information</td>
<td>DHCP Conflicts Information</td>
<td>DHCP Relay</td>
<td></td>
</tr>
</tbody>
</table>

DHCP Server Configuration

- Admin Mode
- Ping Packet Count
- Conflict Logging Mode
- Bootp Automatic Mode

Excluded Address

<table>
<thead>
<tr>
<th>IP Range From</th>
<th>IP Range To</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.200.1.1</td>
<td>10.200.1.1</td>
</tr>
</tbody>
</table>

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

c. In the IP Range From field, enter 10.200.1.1.

d. In the IP Range To field, enter 10.200.1.1.

e. Click Add.

5. Exclude 10.200.2.1 from the DHCP pool.

a. Select System > Services > DHCP Server > DHCP Server Configuration. A screen similar to the following displays:

<table>
<thead>
<tr>
<th>System</th>
<th>Switching</th>
<th>Routing</th>
<th>QoS</th>
<th>Security</th>
<th>Monitoring</th>
<th>Maintenance</th>
<th>Help</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Server</td>
<td>DHCP Server Configuration</td>
<td>DHCP Pool Configuration</td>
<td>DHCP Pool Options</td>
<td>DHCP Server Statistics</td>
<td>DHCP Bindings Information</td>
<td>DHCP Conflicts Information</td>
<td>DHCP Relay</td>
<td></td>
</tr>
</tbody>
</table>

DHCP Server Configuration

- Admin Mode
- Ping Packet Count
- Conflict Logging Mode
- Bootp Automatic Mode

Excluded Address

<table>
<thead>
<tr>
<th>IP Range From</th>
<th>IP Range To</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.200.2.1</td>
<td>10.200.2.1</td>
</tr>
</tbody>
</table>

b. In the IP Range From field, enter 10.200.2.1.

c. In the IP Range To field, enter 10.200.2.1.

d. Click Add.

6. Create a DHCP pool named dhcp_server.
a. Select **System > Services > DHCP Server > DHCP Pool Configuration**. A screen similar to the following displays.

![DHCP Pool Configuration](image)

b. Under DHCP Pool Configuration, enter the following information:
   - In the **Pool Name** list, select **Create**.
   - In the **Pool Name** field, enter **dhcp_server**.
   - In the **Type of Binding** list, select **Dynamic**.
   - In the **Network Number** field, enter **10.200.1.0**.
   - In the **Network Mask** field, enter **255.255.255.0**. As an alternate, you can enter **24** in the **Network Prefix Length** field.

**Note:** Do not fill in the Network Mask field and Network Prefix Length field at the same time.

c. Click **Add**. The pool_dynamic name is now added to the **Pool Name** drop-down list.

7. Create a DHCP pool named dhcp_server_second.
a. Select System > Services > DHCP Server > DHCP Pool Configuration. A screen similar to the following displays.

b. Under DHCP Pool Configuration, enter the following information:
   - In the Pool Name list, select Create.
   - In the Pool Name field, enter dhcp_server_second.
   - In the Type of Binding list, select Dynamic.
   - In the Network Number field, enter 10.200.2.0.
   - In the Network Mask field, enter 255.255.255.0. As an alternate, you can enter 24 in the Network Prefix Length field.
   - 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.

```bash
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#interface 1/0/16
(Netgear Switch) (Interface 1/0/16)#routing
(Netgear Switch) (Interface 1/0/16)#ip address 10.200.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/16)#exit
```

4. Configure the DHCP Server IP address and enable the DHCP L3 relay.

```bash
(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.

```bash
(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.

   ![IP Configuration screen](image)

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

2. Create a routing interface and assign 10.100.1.2/24 to it.
a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

![IP Interface Configuration](image)

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

c. In the **IP Address** field, enter **10.100.1.2**.

d. In the **Subnet Mask** field, enter **255.255.255.0**.

e. In the **Routing Mode** field, select **Enable**.

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

3. Enable RIP on interface 1/0/4.

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

![Interface Configuration](image)

b. In the **Interface** list, select **1/0/4**.

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

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

4. Create a routing interface and assign 10.200.1.1/24 to it.
a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>VLAN</th>
<th>IP Address Configuration Method</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Routing Mode</th>
<th>Administrative Mode</th>
<th>Link Speed/State/Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/1</td>
<td>Port 1/0/1</td>
<td>None</td>
<td>Manual</td>
<td>10.200.1.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Disable</td>
<td>Unknown</td>
</tr>
<tr>
<td>1/0/2</td>
<td>Port 1/0/2</td>
<td>99</td>
<td>Manual</td>
<td>10.200.2.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Enable</td>
<td>Unknown</td>
</tr>
<tr>
<td>1/0/3</td>
<td>Port 1/0/3</td>
<td>99</td>
<td>Manual</td>
<td>10.200.3.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Enable</td>
<td>Unknown</td>
</tr>
<tr>
<td>1/0/4</td>
<td>Port 1/0/4</td>
<td>99</td>
<td>Manual</td>
<td>10.200.4.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Enable</td>
<td>Unknown</td>
</tr>
<tr>
<td>1/0/5</td>
<td>Port 1/0/5</td>
<td>99</td>
<td>Manual</td>
<td>10.200.5.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Enable</td>
<td>Unknown</td>
</tr>
<tr>
<td>1/0/6</td>
<td>Port 1/0/6</td>
<td>99</td>
<td>Manual</td>
<td>10.200.6.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Enable</td>
<td>Unknown</td>
</tr>
<tr>
<td>1/0/7</td>
<td>Port 1/0/7</td>
<td>99</td>
<td>Manual</td>
<td>10.200.7.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Enable</td>
<td>Unknown</td>
</tr>
<tr>
<td>1/0/8</td>
<td>Port 1/0/8</td>
<td>99</td>
<td>Manual</td>
<td>10.200.8.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Enable</td>
<td>Unknown</td>
</tr>
<tr>
<td>1/0/9</td>
<td>Port 1/0/9</td>
<td>99</td>
<td>Manual</td>
<td>10.200.9.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Enable</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

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

c. In the **IP Address Configuration Method** field, enter **Manual**.

d. In the **IP Address** field, enter **10.200.1.1**.

e. In the **Subnet Mask** field, enter **255.255.255.0**.

f. In the **Routing Mode** field, select **Enable**.

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

5. Create a routing interface and assign 10.200.2.1/24 to it.

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>VLAN</th>
<th>IP Address Configuration Method</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Routing Mode</th>
<th>Administrative Mode</th>
<th>Link Speed/State/Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/1</td>
<td>Port 1/0/1</td>
<td>None</td>
<td>Manual</td>
<td>10.200.1.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Disable</td>
<td>Unknown</td>
</tr>
<tr>
<td>1/0/2</td>
<td>Port 1/0/2</td>
<td>99</td>
<td>Manual</td>
<td>10.200.2.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Enable</td>
<td>Unknown</td>
</tr>
<tr>
<td>1/0/3</td>
<td>Port 1/0/3</td>
<td>99</td>
<td>Manual</td>
<td>10.200.3.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Enable</td>
<td>Unknown</td>
</tr>
<tr>
<td>1/0/4</td>
<td>Port 1/0/4</td>
<td>99</td>
<td>Manual</td>
<td>10.200.4.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Enable</td>
<td>Unknown</td>
</tr>
<tr>
<td>1/0/5</td>
<td>Port 1/0/5</td>
<td>99</td>
<td>Manual</td>
<td>10.200.5.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Enable</td>
<td>Unknown</td>
</tr>
<tr>
<td>1/0/6</td>
<td>Port 1/0/6</td>
<td>99</td>
<td>Manual</td>
<td>10.200.6.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Enable</td>
<td>Unknown</td>
</tr>
<tr>
<td>1/0/7</td>
<td>Port 1/0/7</td>
<td>99</td>
<td>Manual</td>
<td>10.200.7.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Enable</td>
<td>Unknown</td>
</tr>
<tr>
<td>1/0/8</td>
<td>Port 1/0/8</td>
<td>99</td>
<td>Manual</td>
<td>10.200.8.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Enable</td>
<td>Unknown</td>
</tr>
<tr>
<td>1/0/9</td>
<td>Port 1/0/9</td>
<td>99</td>
<td>Manual</td>
<td>10.200.9.1</td>
<td>255.255.255.0</td>
<td>Disable</td>
<td>Enable</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

b. Under IP Interface Configuration, scroll down and select the Port 1/0/16 check box.

c. In the **IP Address Configuration Method** field, enter **Manual**.

d. In the **IP Address** field, enter **10.200.2.1**.

e. In the **Subnet Mask** field, enter **255.255.255.0**.

f. In the **Routing Mode** field, select **Enable**.

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

6. Redistribute the connected routes to RIP.
a. Select Routing > RIP > Advanced > Route Redistribution. A screen similar to the following displays.

b. In the Source field, select Connected.

c. In the Redistribute Mode field, select Enable.

d. Click Apply to save the settings.

7. Enable DHCP L3 relay.

a. Select System > Services > DHCP Relay. A screen similar to the following displays.

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

c. Click Apply to save the settings.

8. Configure the DHCP server IP address.

a. Select System > Services > UDP Relay. A screen similar to the following displays.

b. In the Server Address field, enter 10.100.1.1.

c. In the UDP Port field, enter dhcp.

d. Click Add to save the settings.
Multicast Listener Discovery (MLD) protocol enables IPv6 routers to discover multicast listeners, the nodes that are configured to receive multicast data packets, on its directly attached interfaces. The protocol specifically discovers which multicast addresses are of interest to its neighboring nodes and provides this information to the active multicast routing protocol that makes decisions on the flow of multicast data packets. Periodically, the multicast router sends general queries requesting multicast address listener information from systems on an attached networks. These queries are used to build and refresh the multicast address listener state on the attached networks. In response to the queries, multicast listeners reply with membership reports. These membership reports specify their multicast addresses listener state and their desired set of sources with current-state multicast address records. The multicast router also processes unsolicited filter- mode-change records and source-list-change records from systems that want to indicate interest in receiving or not receiving traffic from particular sources.
Configure MLD

In this case, PIM-DM is enabled on Switch A and Switch B, and MLD is enabled on Switch B’s port 1/0/24 to discover the multicast listeners.

IPv6 multicast source

2001:2::/65
Port 1/0/13
Switch A
2001:1::/64
Port 1/0/1
2001:3::/64
Port 1/0/21
Switch B
2001:3::/64
Host

Figure 47. 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
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


{(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ipv6 address 2001:1::2/64
(Netgear Switch) (Interface 1/0/21)#ipv6 enable
(Netgear Switch) (Interface 1/0/21)#ipv6 pim dense
(Netgear Switch) (Interface 1/0/21)#ipv6 ospf
(Netgear Switch) (Interface 1/0/21)#exit

(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#routing
(Netgear Switch) (Interface 1/0/24)#ipv6 address 2001:3::1/64
(Netgear Switch) (Interface 1/0/24)#ipv6 enable
(Netgear Switch) (Interface 1/0/24)#ipv6 mld router

(Netgear Switch) (Interface 1/0/24)#ipv6 pim dense
(Netgear Switch) (Interface 1/0/24)#exit

The MLD group information on switch B:
(B) #show ipv6 mld groups ff32::1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Group Address</th>
<th>Last Reporter</th>
<th>Up Time</th>
<th>Expiry Time</th>
<th>Filter Mode</th>
<th>Group compat mode</th>
<th>Source Address</th>
<th>ExpiryTime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FF32::1</td>
<td>FE80::200:4FF:FE8:5EFC</td>
<td>00:00:18</td>
<td>----</td>
<td>Include</td>
<td>v2</td>
<td>2001:2::2</td>
<td>00:04:02</td>
</tr>
</tbody>
</table>

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.

![IP Configuration Screen](image1)

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.

![IPv6 Global Configuration Screen](image2)

b. For IPv6 Unicast Routing, select the Enable radio button.

c. Click Apply.

3. Configure 1/0/1 and 1/0/13 as IPv6 routing ports.

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

![IPv6 Interface Configuration Screen](image3)
b. Scroll down and select the Interface 1/0/1 and 1/0/13 check boxes.

c. Enter the following information:
   • In the IPv6 Mode field, select Enable.
   • In the Routing Mode field, select Enable.
   • In the Admin Mode field, select Enable.

d. Click Apply to save the settings.

4. Assign an IPv6 address to 1/0/1.

   a. Select Routing > IPv6 > Advanced > Prefix Configuration. A screen similar to the following displays.

   b. In the Interface field, select 1/0/1.

   c. Enter the following information:
      • In the IPv6 Prefix field, enter 2001:1::1.
      • In the Prefix Length field, enter 64.
      • In the EUI64 field, select Disable.

   d. Click Add to save the settings.

5. Assign an IPv6 address to 1/0/13.
a. Select **Routing > IPv6 > Advanced > Prefix Configuration**. A screen similar to the following displays.

![IPv6 Prefix Configuration](image)

b. Select Interface 1/0/1.

c. Enter the following information:
   - In the **IPv6 Prefix** field, enter `2001:2::1`.
   - In the **Prefix Length** field, enter `64`.
   - In the **EUI64** field, select **Disable**.

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

6. Configure the router ID of OSPFv3.

a. Select **Routing > OSPFv3 > Basic > OSPFv3 Configuration**. A screen similar to the following displays.

![OSPFv3 Configuration](image)

b. In the **Router ID** field, enter `1.1.1.1`.

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

d. Click **Apply**.

7. Enable OSPFv3 on interfaces 1/0/1 and 1/0/13.
a. Select Routing > OSPFv3 > Advanced > Interface Configuration. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>Interface</th>
<th>IPv6 Address</th>
<th>Area ID</th>
<th>Admin Mode</th>
<th>Router Priority</th>
<th>Retransmit Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/1</td>
<td>0.0.0.0</td>
<td></td>
<td>Enable</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>1/0/2</td>
<td>0.0.0.0</td>
<td></td>
<td>Enable</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>1/0/3</td>
<td>0.0.0.0</td>
<td></td>
<td>Enable</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>1/0/4</td>
<td>0.0.0.0</td>
<td></td>
<td>Enable</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>

b. Scroll down and select the Interface 1/0/1 and 1/0/13 check boxes.

c. In the Admin Mode field, select Enable.

d. Click Apply to save the settings.

8. Enable multicast globally.

a. Select Routing > Multicast > Global Configuration. A screen similar to the following displays.

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

c. Click Apply.

a. Select **Routing > IPv6 Multicast > IPv6 PIM > Global Configuration**. A screen similar to the following displays.

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

c. Click **Apply**.

10. Enable PIM-DM on interfaces 1/0/1 and 1/0/13.

a. Select **Routing > IPv6 Multicast > IPv6 PIM > Interface Configuration**. A screen similar to the following displays.

b. Scroll down and select the Interface 1/0/1 and 1/0/13 check boxes.

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

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

**MLD on Switch B**

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

![IP Configuration screenshot]

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.

![IPv6 Global Configuration screenshot]

b. For IPv6 Unicast Routing, select the Enable radio button.

c. Click Apply.

3. Configure 1/0/21 and 1/0/24 as IPv6 routing ports.

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

![IPv6 Interface Configuration screenshot]
b. Scroll down and select the Interface 1/0/21 and 1/0/24 check boxes.

c. Enter the following information:
   • In the IPv6 Mode field, select Enable.
   • In the Routing Mode field, select Enable.
   • In the Admin Mode field, select Enable.

d. Click Apply to save the settings.

4. Assign an IPv6 address to 1/0/21.
   a. Select Routing > IPv6 > Advanced > Prefix Configuration. A screen similar to the following displays.
   
   ![IPv6 Prefix Configuration Screen]

   b. In the Interface field, select 1/0/21.
   c. Enter the following information:
      • In the IPv6 Prefix field, enter 2001:1::2.
      • In the Prefix Length field, enter 64.
      • In the EUI64 field, select Disable.
   d. Click Add to save the settings.

5. Assign an IPv6 address to 1/0/24.
a. Select Routing > IPv6 > Advanced > Prefix Configuration. A screen similar to the following displays.


c. Enter the following information:
   • In the IPv6 Prefix field, enter 2001:3::1.
   • In the Prefix Length field, enter 64.
   • In the EUI64 field, select Disable.

d. Click Add to save the settings.

6. Configure the router ID of OSPFv3.
   a. Select Routing > OSPFv3 > Basic > OSPFv3 Configuration. A screen similar to the following displays.

b. In the Router ID field, enter 2.2.2.2.

c. For Admin Mode, select the Enable radio button.

d. Click Apply.

7. Enable OSPFv3 on interfaces 1/0/21 and 1/0/24.
a. Select Routing > OSPFv3 > Advanced > Interface Configuration. A screen similar to the following displays.

b. Under OSPFv3 Interface Configuration, scroll down and select the Interface 1/0/21 and 1/0/24 check boxes.

c. In the OSPFv3 Interface Configuration, in the Admin Mode field, select Enable.

d. Click Apply to save the settings.

8. Enable multicast globally.
   a. Select Routing > Multicast > Global Configuration. A screen similar to the following displays.

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

   c. Click Apply.

a. Select Routing > IPv6 Multicast > IPv6 PIM > Global Configuration. A screen similar to the following displays.

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

c. Click Apply.

10. Enable PIM-DM on interfaces 1/0/21 and 1/0/24.

a. Select Routing > IPv6 Multicast > IPv6 PIM > Interface Configuration. A screen similar to the following displays.

b. Under PIM Interface Configuration, scroll down select the Interface 1/0/21 and 1/0/24 check boxes.

c. In the Admin Mode field, select Enable.

d. Click Apply to save the settings.

11. Enable MLD on the switch.
a. Select Routing > IPv6 Multicast > MLD > Global Configuration. A screen similar to the following displays.

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

c. Click Apply.

12. Enable MLD on interface 1/0/24.

a. Select Routing > IPv6 Multicast > MLD > Routing Interface Configuration. A screen similar to the following displays.

b. Under MLD Routing Interface Configuration, scroll down and select the 1/0/24 check box. Now 1/0/24 appears in the Interface field at the top.

c. In the Admin Mode field, select Enable.

d. Click Apply.

MLD Snooping

In IPv4, Layer 2 switches can use IGMP snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast address. In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.
MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes configured to receive IPv6 multicast packets) on its directly attached links and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD version 1 (MLDv1) is equivalent to IGMPv2, and MLD version 2 (MLDv2) is equivalent to IGMPv3. MLD is a subprotocol of Internet Control Message Protocol version 6 (ICMPv6), and MLD messages are a subset of ICMPv6 messages, identified in IPv6 packets by a preceding Next Header value of 58.

The switch can snoop on both MLDv1 and MLDv2 protocol packets and bridge IPv6 multicast data based on destination IPv6 multicast MAC addresses. The switch can be configured to perform MLD snooping and IGMP snooping simultaneously.

**CLI: Configure MLD Snooping**

1. Enter the following commands.

   ```
   (Netgear Switch) #vlan da
   (Netgear Switch) (Vlan)#vlan 300
   (Netgear Switch) (Vlan)#exit
   (Netgear Switch) #config
   (Netgear Switch) (Config)#interface 1/0/1
   (Netgear Switch) (Interface 1/0/1)#vlan participation include 300
   (Netgear Switch) (Interface 1/0/1)#vlan pvid 300
   (Netgear Switch) (Interface 1/0/1)#exit
   (Netgear Switch) (Config)#interface 1/0/24
   (Netgear Switch) (Interface 1/0/24)#vlan participation include 300
   (Netgear Switch) (Interface 1/0/24)#vlan pvid 300
   (Netgear Switch) (Interface 1/0/24)#exit
   (Netgear Switch) (Config)#exit
   (Netgear Switch) (Config)#set mld
   (Netgear Switch) (Config)#exit
   (Netgear Switch) #vlan database
   (Netgear Switch) (Vlan)#set mld 300
   (Netgear Switch) (Vlan)#exit
   ```

2. Enable MLD snooping on VLAN 300.

   ```
   (Netgear Switch) #show mldsnooping
   Admin Mode........................................... Enable
   Multicast Control Frame Count...................... 0
   Interfaces Enabled for MLD Snooping.............. None
   VLANs enabled for MLD snooping.................. 300
   (Netgear Switch) #
   ```
Web Interface: Configure MLD Snooping

1. Create VLAN 300.
   a. Select Switching > VLAN > Basic > VLAN Configuration. A screen similar to the following displays.
   
   ![VLAN Configuration screenshot]
   
   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.
   
   ![VLAN Membership screenshot]
   
   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.
ProSafe Managed Switch

Chapter 30. MLD | 487

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

b. Scroll down and select the interface 1/0/1 and 1/0/24 check boxes.

c. In the **PVID (1 to 4093)** field, enter 300.

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

4. Enable MLD snooping on the switch.
   a. Select **Routing > Multicast > MLD Snooping > Configuration**. A screen similar to the following displays.

5. Enable MLD snooping on the VLAN 300.
   a. Select **Routing > Multicast > MLD Snooping > MLD VLAN Configuration**. A screen similar to the following displays.
b. Enter the following information:
   • In the VLAN ID field, enter 300.
   • In the Admin Mode field, select Enable.

6. Click Add.
DVMRP

Distance Vector Multicast Routing Protocol

The DVMRP is used for multicasting over IP networks without routing protocols to support multicast. The DVMRP is based on the RIP protocol but more complicated than RIP. 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.

![Diagram of DVMRP network with IP addresses and interfaces.]  

**Figure 48. DVMRP**

**CLI: Configure DVMRP**

**DVRMP on Switch A**

1. Create routing interfaces 1/0/1, 1/0/13, and 1/0/21.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.1.1 255.255.255.0
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ip address 192.168.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address 192.168.3.2 255.255.255.0
(Netgear Switch) (Interface 1/0/21)#exit
```

2. Enable IP multicast forwarding on the switch.

```
(Netgear Switch) (Config)#ip multicast
```
3. Enable DVMRP protocol on the switch.

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

4. Enable DVMRP mode on the interfaces 1/0/1, 1/0/13, and 1/0/21.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#ip dvmrp
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#ip dvmrp
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#ip dvmrp
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) #show ip dvmrp neighbor
Interface ..................................... 1/0/13
Neighbor IP Address ........................... 192.168.2.2
State ......................................... Active
Up Time (hh:mm:ss) ......................... 00:02:40
Expiry Time (hh:mm:ss) ...................... 00:00:25
Generation ID ............................ 1116347719
Major Version ............................ 3
Minor Version ............................. 255
Capabilities ................................ Prune GenID Missing 11441
Received Routes .......................... 0
Received Bad Packets ...................... 0
Received Bad Routes ....................... 0
Interface ..................................... 1/0/21
Neighbor IP Address ........................ 192.168.3.1
State ......................................... Active
Up Time (hh:mm:ss) ......................... 00:01:44
Expiry Time (hh:mm:ss) ...................... 00:00:28
Generation ID ............................ 1116595047
Major Version ............................ 3
Minor Version ............................. 255
More Entries or quit(q)
Capabilities ................................ Prune GenID Missing 11441
Received Routes .......................... 0
Received Bad Packets ...................... 0
Received Bad Routes ....................... 0
(Netgear Switch) #show ip mcast mroute summary

Multicast Route Table Summary

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Protocol</th>
<th>Incoming</th>
<th>Outgoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.2</td>
<td>225.0.0.1</td>
<td>DVMRP</td>
<td>1/0/1</td>
<td>1/0/21</td>
</tr>
</tbody>
</table>

**DVRMP on Switch B**

1. Create routing ports 1/0/13 and 1/0/20.

   (Netgear Switch) #config
   (Netgear Switch) (Config)#ip routing
   (Netgear Switch) (Config)#interface 1/0/13
   (Netgear Switch) (Interface 1/0/13)#routing
   (Netgear Switch) (Interface 1/0/13)#ip address 192.168.2.2 255.255.255.0
   (Netgear Switch) (Interface 1/0/13)#exit
   (Netgear Switch) (Config)#interface 1/0/20
   (Netgear Switch) (Interface 1/0/20)#routing
   (Netgear Switch) (Interface 1/0/20)#ip address 192.1.168.4.1 255.255.255.0
   (Netgear Switch) (Interface 1/0/20)#exit
   (Netgear Switch) (Config)#exit

2. Enable IP multicast forwarding on the switch.

   (Netgear Switch) (Config)#ip multicast

3. Enable DVMRP protocol on the switch.

   (Netgear Switch) (Config)#ip dvmrp

4. Enable DVMRP mode on interfaces 1/0/13 and 1/0/20.

   (Netgear Switch) (Config)#interface 1/0/13
   (Netgear Switch) (Interface 1/0/13)#ip dvmrp
   (Netgear Switch) (Interface 1/0/13)#ex
   (Netgear Switch) (Config)#interface 1/0/20
   (Netgear Switch) (Interface 1/0/20)#ip dvmrp
   (Netgear Switch) (Interface 1/0/20)#exit
   (Netgear Switch) (Config)#exit
(Netgear Switch) #show ip dvrmrp neighbor
Interface .............................. 1/0/13
Neighbor IP Address ....................... 192.168.2.1
State ................................. Active
Up Time (hh:mm:ss) ....................... 00:02:26
Expiry Time (hh:mm:ss) .................... 00:00:20
Generation ID ......................... 88091
Major Version ......................... 3
Minor Version ......................... 255
Capabilities .............................. Prune GenID Missing 11441
Received Routes ....................... 0
Received Bad Packets ................. 0
Received Bad Routes ................... 0
Interface .............................. 1/0/20
Neighbor IP Address ....................... 192.168.4.2
State ................................. Active
Up Time (hh:mm:ss) ....................... 00:01:44
Expiry Time (hh:mm:ss) .................... 00:00:29
Generation ID ......................... 1116595033
Major Version ......................... 3
Minor Version ......................... 255
Capabilities .............................. Prune GenID Missing 11441
Received Routes ....................... 0
Received Bad Packets ................. 0
Received Bad Routes ................... 0

(Netgear Switch) #show ip mcast mroute detail summary

Multicast Route Table Summary

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Protocol</th>
<th>Interface</th>
<th>Interface List</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.2</td>
<td>225.0.0.1</td>
<td>DVMRP</td>
<td>1/0/13</td>
<td></td>
</tr>
</tbody>
</table>
**DVRMP on Switch C:**

1. Create routing interfaces 1/0/11, 1/0/3, and 1/0/24.

```
(Netgear Switch) #config
(Netgear Switch) (Config)# ip routing
(Netgear Switch) (Config)# ip interface 1/0/11
(Netgear Switch) (Interface 1/0/11)# ip routing
(Netgear Switch) (Interface 1/0/11)# ip address 192.168.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/11)# exit
(Netgear Switch) (Config)# interface 1/0/3
(Netgear Switch) (Interface 1/0/3)# routing
(Netgear Switch) (Interface 1/0/3)# ip address 192.168.4.2 255.255.255.0
(Netgear Switch) (Interface 1/0/3)# exit
(Netgear Switch) (Config)# interface 1/0/24
(Netgear Switch) (Interface 1/0/24)# routing
(Netgear Switch) (Interface 1/0/24)# ip address 192.168.5.1 255.255.255.0
(Netgear Switch) (Interface 1/0/24)# exit
```

2. Enable IP multicast forwarding on the switch.

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

3. Enable IP DVMRP protocol on the switch.

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

4. Enable DVMRP mode on interfaces 1/0/3, 1/0/11, and 1/0/24.

```
(Netgear Switch) (Config)# interface 1/0/3
(Netgear Switch) (Interface 1/0/3)# ip dvmrp
(Netgear Switch) (Interface 1/0/3)# exit
(Netgear Switch) (Config)# interface 1/0/11
(Netgear Switch) (Interface 1/0/11)# ip dvmrp
(Netgear Switch) (Interface 1/0/11)# exit
(Netgear Switch) (Config)# interface 1/0/24
(Netgear Switch) (Interface 1/0/24)# ip dvmrp
(Netgear Switch) (Interface 1/0/24)# exit
```

5. Enable IGMP protocol on the switch.

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

(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#ip igmp
(Netgear Switch) (Interface 1/0/24)#exit

(Netgear Switch) #show ip dvmrp neighbor
Interface ..................................... 1/0/11
Neighbor IP Address ........................... 192.168.3.2
State ......................................... Active
Up Time (hh:mm:ss) ............................ 00:01:03
Expiry Time (hh:mm:ss) ....................... 00:00:24
Generation ID ................................. 88099
Major Version ................................. 3
Minor Version ................................. 255
Capabilities .................................. Prune GenID Missing 11441
Received Routes ............................... 0
Received Bad Packets .......................... 0
Received Bad Routes ............................ 0
Interface ..................................... 1/0/3
Neighbor IP Address ........................... 192.168.4.1
State ......................................... Active
Up Time (hh:mm:ss) ............................ 00:01:17
Expiry Time (hh:mm:ss) ....................... 00:00:23
Generation ID ................................. 1116347728
Major Version ................................. 3
Minor Version ................................. 255

More Entries or quit(q)
Capabilities .................................. Prune GenID Missing 11441
Received Routes ............................... 0
Received Bad Packets .......................... 0
Received Bad Routes ............................ 0

(Netgear Switch) #show ip mcast mroute detail summary

<table>
<thead>
<tr>
<th>Multicast Route Table Summary</th>
<th>Incoming</th>
<th>Outgoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>Group IP</td>
<td>Protocol</td>
</tr>
<tr>
<td>192.168.1.2</td>
<td>225.0.0.1</td>
<td>DVMRP</td>
</tr>
</tbody>
</table>
Web Interface: Configure DVMRP

**DVMRP on Switch A**

1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**. A screen similar to the following displays.
   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply**.

2. Configure 1/0/1 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.
   b. Scroll down and select the Port 1/0/1 check box. Now 1/0/1 appears in the Port field at the top.
   c. Enter the following information:
      - In the **IP Address** field, enter **192.168.1.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** field, select **Enable**.
   d. Click **Apply** to save the settings.

3. Configure 1/0/13 as a routing port and assign an IP address to it.
a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>VLAN ID</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Routing Mode</th>
<th>Administrative Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/13</td>
<td></td>
<td></td>
<td>192.168.2.1</td>
<td>255.255.255.0</td>
<td>Enable</td>
<td>Enable</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>VLAN ID</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Routing Mode</th>
<th>Administrative Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/21</td>
<td></td>
<td></td>
<td>192.168.3.2</td>
<td>255.255.255.0</td>
<td>Enable</td>
<td>Enable</td>
</tr>
</tbody>
</table>

b. Scroll down and select the Port 1/0/13 check box. Now 1/0/13 appears in the Port field at the top.

c. Enter the following information:
   - In the **IP Address** field, enter **192.168.3.2**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Routing Mode** field, select **Enable**.

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

5. Enable IP multicast on the switch.
a. Select Routing > Multicast > Global Configuration. A screen similar to the following displays.

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

c. Click Apply.

6. Enable DVMRP on the switch.

a. Select Routing > Multicast > DVMRP > Global Configuration. A screen similar to the following displays.

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

c. Click Apply.

7. Enable DVMRP on the interface.
a. Select Routing > Multicast > DVMRP > Interface Configuration. A screen similar to the following displays.

b. Scroll down select the Interface 1/0/1, 1/0/13, and 1/0/21 check boxes.

c. In the Interface Mode field, select 300.

d. Click Apply to save the settings.

**DVMRP on Switch B**

1. Enable IP routing on the switch.

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

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

   c. Click Apply.

2. Configure 1/0/13 as a routing port and assign and IP address to it.
a. **Select Routing > IP > Advanced > IP Interface Configuration.** A screen similar to the following displays.

![IP Interface Configuration](image)

b. **Scroll down and select the Port 1/0/13 check box.** Now 1/0/13 appears in the Port field at the top.

c. **Enter the following information in the IP Interface Configuration.**
   - In the **IP Address** field, enter **192.168.2.2**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Routing Mode** field, select **Enable**.

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

3. **Configure 1/0/20 as a routing port and assign an IP address to it.**
   a. **Select Routing > IP > Advanced > IP Interface Configuration.** A screen similar to the following displays.

![IP Interface Configuration](image)

b. **Scroll and select the Port 1/0/20 check box.** Now 1/0/20 appears in the Interface field at the top.

c. **Enter the following information:**
   - In the **IP Address** field, enter **192.168.4.1**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Routing Mode** field, select **Enable**.

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

4. **Enable IP multicast on the switch.**
a. Select **Routing > Multicast > Global Configuration**. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>System</th>
<th>Switching</th>
<th>Routing</th>
<th>QoS</th>
<th>Security</th>
<th>Monitoring</th>
<th>Maintenance</th>
<th>Help</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Table</td>
<td>IP</td>
<td>IPv6</td>
<td>VLAN</td>
<td>ARP</td>
<td>RIP</td>
<td>OSPF</td>
<td>OSPFv3</td>
<td>Router Discovery</td>
</tr>
<tr>
<td>Global Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DVMRP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIM-DM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIM-SP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MLD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Static Routes Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin Boundary Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![Global Configuration screen]

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

c. Click **Apply**.

5. Enable DVMRP on the switch.

a. Select **Routing > Multicast > DVMRP > Global Configuration**. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>System</th>
<th>Switching</th>
<th>Routing</th>
<th>QoS</th>
<th>Security</th>
<th>Monitoring</th>
<th>Maintenance</th>
<th>Help</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Table</td>
<td>IP</td>
<td>IPv6</td>
<td>VLAN</td>
<td>ARP</td>
<td>RIP</td>
<td>OSPF</td>
<td>OSPFv3</td>
<td>Router Discovery</td>
</tr>
<tr>
<td>DVMRP Global Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin Mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Number of Routes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reachable Routes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![DVMRP Global Configuration screen]

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

c. Click **Apply**.

a. Select Routing > Multicast > DVMRP > Interface Configuration. A screen similar to the following displays.

![DVMRP Interface Configuration Screen]

b. Scroll down and select the Interface 1/0/13 and 1/0/20 check boxes.
c. In the Interface Mode field, select Enable.
d. Click Apply to save the settings.

**DVMRP on Switch C**

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

   ![IP Configuration Screen]

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

2. Configure 1/0/11 as a routing port and assign an IP address to it.
a. Select **Routing > IP > Advanced > IP Interface Configuration**. A screen similar to the following displays.

b. Scroll down and select the Port 1/0/11 check box. Now 1/0/11 appears in the Port field at the top.

c. Enter the following information:
   - In the **IP Address** field, enter 192.168.3.1.
   - In the **Subnet Mask** field, enter 255.255.255.0.
   - In the **Routing Mode** field, select Enable.

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

3. Configure 1/0/3 as a routing port and assign an IP address to it.

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

   b. Scroll down and select the Port 1/0/3 check box. Now 1/0/3 appears in the Port field at the top.

   c. Enter the following information:
      - In the **IP Address** field, enter 192.168.4.2.
      - In the **Subnet Mask** field, enter 255.255.255.0.
      - In the **Routing Mode** field, select Enable.

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

4. Configure 1/0/24 as a routing port and assign an IP address to it.
a. Select Routing > IP > Advanced > IP Interface Configuration. A screen similar to the following displays.

b. Scroll down and select the Port 1/0/24 check box. Now 1/0/24 appears in the Port field at the top.

c. Enter the following information:
   - In the IP Address field, enter 192.168.5.1.
   - In the Subnet Mask field, enter 255.255.255.0.
   - In the Routing Mode field, select Enable.

d. Click Apply to save the settings.

5. Enable IP multicast on the switch.
   a. Select Routing > Multicast > Global Configuration. A screen similar to the following displays.

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

c. Click Apply.

6. Enable DVMRP on the switch.
a. Select Routing > Multicast > DVMRP > Global Configuration. A screen similar to the following displays.

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

c. Click Apply.

7. Enable DVMRP on the interface.

a. Select Routing > Multicast > DVMRP > Interface Configuration. A screen similar to the following displays.

b. Scroll down and select the Interface 1/0/3, 1/0/11, and 1/0/24 check boxes.

c. Select Enable in the Interface Mode field.

d. Click Apply to save the settings.

8. Enable IGMP on the switch.
a. Select Routing > Multicast > IGMP > Global Configuration. A screen similar to the following displays.

<table>
<thead>
<tr>
<th>System</th>
<th>Switching</th>
<th>Routing</th>
<th>QoS</th>
<th>Security</th>
<th>Monitoring</th>
<th>Maintenance</th>
<th>Help</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Table</td>
<td>IP</td>
<td>IPub</td>
<td>VLAN</td>
<td>ARP</td>
<td>RIP</td>
<td>OSPF</td>
<td>OSPFv3</td>
<td>Router Discovery</td>
</tr>
</tbody>
</table>

![IGMP Global Configuration Screen]

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

c. Click Apply.

9. Enable IGMP on the interface.

a. Select Routing > Multicast > IGMP > Routing Interface Configuration. A screen similar to the following displays.

![IGMP Routing Interface Configuration Screen]

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.
Captive Portal

This chapter includes the following sections:

- Captive Portal Configuration on page 508
- Enable Captive Portal on page 508
- Client Access, Authentication, and Control on page 510
- Block a Captive Portal Instance on page 511
- Local Authorization, Create Users and Groups on page 511
- Remote Authorization (RADIUS) User Configuration on page 513
- SSL Certificates on page 515

The captive portal feature is a software implementation that blocks clients from accessing the network until user verification has been established. You can set up verification to allow access for both guests and authenticated users. Authenticated users must be validated against a database of authorized captive portal users before access is granted.

The authentication server supports both HTTP and HTTPS Web connections. In addition, you can configure captive portal to use an optional HTTP port (in support of HTTP proxy networks). If configured, this additional port is then used exclusively by captive portal. Note that this optional port is in addition to the standard HTTP port 80, which is currently being used for all other Web traffic.

Captive portal for wired interfaces allows the clients directly connected to the switch to be authenticated using a captive portal mechanism before the client is given access to the network. When a wired physical port is enabled for captive portal, the port is set in captive-portal-enabled state such that all the traffic coming to the port from the unauthenticated clients is dropped except for the ARP, DHCP, DNS and NETBIOS packets. The switch forwards these packets so that unauthenticated clients can get an IP address and resolve the hostname or domain names. Data traffic from authenticated clients goes through, and the rules do not apply to these packets.

All the HTTP/HTTPS packets from unauthenticated clients are directed to the CPU on the switch for all the ports that are enabled for captive portal. When an unauthenticated client opens a Web browser and tries to connect to network, the captive portal redirects all the HTTP/HTTPS traffic from unauthenticated clients to the authenticating server on the switch. A captive portal Web page is sent back to the unauthenticated client. The client can authenticate. If the client successfully authenticates, the client is given access to port.
You can enable captive portal on all the physical ports on the switch. It is not supported for VLAN interfaces, loopback interfaces or logical interfaces. The captive portal feature uses MAC-address based authentication and not port-based authentication. This means that all the clients connected to the captive portal interface must be authenticated before they can get access to the network.

Clients connecting to the captive portal interface have three states; unknown, unauthenticated, and authenticated.

- **Unknown.** In the unknown state, the captive portal does not redirect HTTP/S traffic to the switch, but instead asks the switch whether the client is authenticated or unauthenticated.
- **Unauthenticated.** The captive portal directs the HTTP/S traffic to the switch so that the client can authenticate with the switch.
- **Authenticated.** After successful authentication, the client is placed in authenticated state. In this state, all the traffic emerging from the client is forwarded through the switch.

### Captive Portal Configuration

This section introduces the objects that make up the captive portal and describes the interaction between the captive portal and the network administrator. It explains what configurations are visible to the network administrator and enumerates the events.

All the configurations included in this section are managed using the CLI, the Web Interface, and SNMP, with one exception; to customize the captive portal Web page, you must use the Web Interface.

The captive portal configuration provides the network administrator control over verification and authentication, assignment to interfaces, client sessions, and Web page customization.

You can create multiple captive portal configuration instances. Each captive portal configuration contains various flags and definitions used to control client access and content to customize the user verification Web page. A captive portal configuration can be applied to one or more interfaces. An interface can only be a physical port on the switch. Software release 8.0 and newer versions can contain up to 10 captive portal configurations.

### Enable Captive Portal

#### CLI: Enable Captive Portal

1. Enable captive portal on the switch.

```
(Netgear Switch) (config)#captive-portal
(Netgear Switch) (Config-CP)#enable
```
2. Enable captive portal instance 1.

```
(Netgear Switch) (Config-CP)#configuration 1
(Netgear Switch) (Config-CP 1)#enable
```

3. Enable captive portal instance 1 on port 1/0/1.

```
(Netgear Switch) (Config-CP 1)#interface 1/0/1
```

**Web Interface: Enable Captive Portal**

1. Enable captive portal on the switch.
   a. Select **Security > Control > Captive Portal > CP Global Configuration**. A screen similar to the following displays.

   ![Captive Portal Global Configuration](image)

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

2. Enable captive portal instance 1 on the switch.
a. Select Security > Control > Captive Portal > CP Configuration. A screen similar to the following displays.

b. Scroll down and select the CP 1 check box. Now CP 1 appears in the CP ID field at the top.

c. In the Admin Mode field, select Enable.

d. Click Apply to save the settings.

3. Enable CP 1 on interface 1/0/1.

a. Select Security > Controls > Captive Portal > CP Binding Configuration. A screen similar to the following displays.

b. In the CP ID list, select 1.

c. Click Unit 1. The ports display.

d. Click the gray box under port 1.

e. Click Apply.

Client Access, Authentication, and Control

User verification can be configured to allow access for guest users—users who do not have assigned user names and passwords. User verification can also be configured to allow access for authenticated users. Authenticated users are required to enter a valid user name and password that must first be validated against the local database or a RADIUS server. Network access is granted once user verification has been confirmed. The administrator can block access to a captive portal configuration. When an instance is blocked, no client traffic is allowed through any interfaces associated with that captive portal configuration. Blocking a
A captive portal instance is a temporary command executed by the administrator and not saved in the configuration.

### Block a Captive Portal Instance

#### CLI: Block a Captive Portal Instance

```
(Netgear Switch) (Config-CP 1) # block
```

#### Web Interface: Block a Captive Portal Instance

1. Select **Security > Control > Captive Portal > CP Configuration**. A screen similar to the following displays.

2. Under Captive Portal Configuration, scroll down and select the CP 1 check box. Now CP 1 appears in the CP ID field at the top.
3. In the **Block** field, select **Enable**.
4. Click **Apply** to save the settings.

### Local Authorization, Create Users and Groups

When using local authentication, the administrator provides user identities for captive portal by adding unique user names and passwords to the local user database. This configuration is global to the captive portal component and can contain up to 128 user entries (a RADIUS server should be used if more users are required). A local user can belong to one or more groups. There is one group created by default with the group name **Default** to which all new users are assigned. All new captive portal instances are also assigned to the Default group. You can create new groups and modify the user/group association to allow only a subset of users access to a specific captive portal instance. Network access is granted upon successful user name, password, and group verification.
CLI: Create Users and Groups

1. Create a group whose group ID is 2.

   (Netgear Switch) #config
   (Netgear Switch) (config)#captive-portal
   (Netgear Switch) (Config-CP)# user group 2

2. Create a user whose name is user1.

   (Netgear Switch) (Config-CP)#user 2 name user1

3. Configure the user’s password.

   (Netgear Switch) (Config-CP)#user 2 password
   Enter password (8 to 64 characters): 12345678
   Re-enter password: 12345678

4. Add the user to the group.

   (Netgear Switch) (Config-CP)#user 2 group 2

Web Interface: Create Users and Groups

1. Create a group.
   a. Select **Security > Control > Captive Portal > CP Group Configuration**. A screen similar to the following displays.

   ![Web Interface Screen]

   b. Enter the following information:
      - In the **Group ID** field, select 2.
      - In the **Group Name** field, enter **Group2**.
c. Click Add.

2. Create a user.

a. Select Security > Control > Captive Portal > CP User Configuration. A screen similar to the following displays.

b. Enter the following information:
   - In the User ID Field, enter 2.
   - In the User Name field, enter user1.
   - In the Password field, enter 12345678.
   - In the Confirm Password field, enter 12345678.
   - In the Group field, select 2.

c. Click Add.

Remote Authorization (RADIUS) User Configuration

A remote RADIUS server can be used for client authentication. In software release 8.0 (or newer), the RADIUS authentication and accounting servers are configured separate from the captive portal configuration. In order to perform authentication and accounting using RADIUS, you configure one or more RADIUS servers and then references the servers using their names in the captive portal configuration. Each captive portal instance can be assigned one RADIUS authentication server and one RADIUS accounting server.

If RADIUS is enabled for a captive portal configuration and no RADIUS servers are assigned, the captive portal activation status will indicate that the instance is disabled with an appropriate reason code.

The following table indicates the RADIUS attributes that are used to configure captive portal users. The table indicates both RADIUS attributes and vendor specific attributes (VSA) that
are used to configure captive portal. VSAs are denoted in the ID column and are comma delimited (vendor ID, attribute ID).

Table 3. RADIUS Attributes for Configuring Captive Portal Users

<table>
<thead>
<tr>
<th>RADIUS Attribute</th>
<th>No.</th>
<th>Description</th>
<th>Range</th>
<th>Usage</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-Name</td>
<td>1</td>
<td>User name to be authorized.</td>
<td>1–32 characters</td>
<td>Required</td>
<td>None</td>
</tr>
<tr>
<td>User-Password</td>
<td>2</td>
<td>User password.</td>
<td>8–64 characters</td>
<td>Required</td>
<td>None</td>
</tr>
<tr>
<td>Session-Timeout</td>
<td>27</td>
<td>Logout once session timeout is reached (seconds). If the attribute is 0 or</td>
<td>Integer (seconds)</td>
<td>Optional</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>not present then use the value configured for the captive portal.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Idle-Timeout</td>
<td>28</td>
<td>Log out once idle timeout is reached (seconds). If the attribute is 0 or</td>
<td>Integer (seconds)</td>
<td>Optional</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>not present, then use the value configured for the captive portal.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WISPr-Max-Bandwidth-Up</td>
<td>14122,7</td>
<td>Maximum client transmit rate (b/s). Limits the bandwidth at which the client</td>
<td>Integer</td>
<td>Optional</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>can send data into the network. If the attribute is 0 or not present, then</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>use the value configured for the captive portal.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WISPr-Max-Bandwidth-Down</td>
<td>14122,8</td>
<td>Maximum client receive rate (b/s). Limits the bandwidth at which the client</td>
<td>Integer</td>
<td>Optional</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>can receive data from the network. If the attribute is 0 or not present,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>then use the value configured for the captive portal.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

![Captive Portal Configuration](image)

2. Scroll down and select the CP 1 check box. Now CP 1 appears in the CP ID field at the top.

3. Enter the following information:
   - In the Verification field, select RADIUS.
   - In the Radius Auth Server field, enter the RADIUS server name Default-RADIUS-Server.

4. Click Apply.

SSL Certificates

A captive portal instance can be configured to use the HTTPS protocol during its user verification process. The connection method for HTTPS uses the Secure Sockets Layer (SSL) protocol, which requires a certificate to provide encryption. The certificate is presented to the user at connection time.

In software release 8.0 (or newer), the captive portal uses the same certificate that is used for secure HTTP connections. You can generate this certificate using a CLI command. If a captive portal instance is configured for the HTTPS protocol and there is not a valid certificate present on the system, the captive portal instance status will show Disabled with an appropriate reason code.
Index

Numerics

6to4 tunnels 382
802.1x port security 251

A

ACL mirroring 147
ACL redirect 152
ACLs 111
  IP ACL configuration 112
  IPv6 157
  isolated VLANs on a Layer 3 switch 133
  MAC ACLs 112, 144
  TCP flag 117
ARP 103
  dynamic ARP inspection 268, 269, 270
ARP, dynamic inspection 282, 283
Auto VoIP 197, 198, 200

B

banner, pre-login 299

C

captive portal 507
  configuration 508
classic STP (802.1d) 376
code mismatch (stacked switches) 323
color conform policy
  DiffServ
    color conform policy 208, 209
configuration scripting 296
CoS
  cos-queue min-bandwidth 169
  per-interface basis 166
  set classofservice trust mode 167
  setting Trust Mode 170
  show classofservice ip-precedence mapping 168
  show classofservice trust 166
  traffic shaping 171
CoS queue configuration 166
CoS queue configuratin 166
CoS queue mapping 165
CoS queueing 164

D
default VLAN 15
DHCP L2 relay 454, 455, 456
DHCP L3 relay 460, 461
DHCP messages, maximum rate 280, 281
DHCP reservation, configuring 352
DHCP server, dynamic mode 349
DHCP snooping 276, 277
DiffServ 173
  Auto VoIP 197, 198, 200
  edge device 173
  interior node 173
  IPv6 201, 202
  VoIP 190
Diffserv
  VoIP 192
distance vector multicast routing protocol (DVMRP) 489
DNS 346
  host name and IP address 347
documentation 8
dual image 301
DVMRP 489, 490, 496

E

Ethernet configuration for stacking ports 324

F

firmware
  upgrading stacked switches 323, 324
firmware for stacked switches 322

G
gaming 221
guest VLAN 257, 258, 259
IGMP querier 221, 222
enable 222, 223
status 225
IGMP snooping 217, 222
  external multicast router 219, 220
  multicast router using VLAN 220, 221
  show igmpsnooping 217
  show igmpsnooping 218
  show mac-address-table 218
  show mac-address-table igmpsnooping 218, 219
IGMPv3 216
interpreting log files 308
IP ACLs 112, 113
IP routing
  port routing 39, 40
  VLAN routing OSPF configuration 93
  VLAN routing RIP configuration 60, 62
IP source guard 282, 283
IPTV 221
IPv6 390
  network interface 393
  routing interface 390
  routing VLAN 395
LAGs
  creating 35
LAGs 34, 39
  adding ports 36, 37
  creating 35
  enabling 38
logs
  show logging hosts 313
MAC ACLs 112, 144
MLD 470, 471, 473
MLD Snooping 484
MLD snooping 484, 485, 486
multicast listener discovery (MLD) 470
NVT 304
OSPF 40, 64, 93
  border router configuration 70
  inter-area router 65
  nssa area 84
stub area configuration 75
  VLAN routing 93
OSPFv3 98
outbound Telnet 304
P
PIM 403
PIM-DM 403, 405, 409
PIM-SM 427, 428, 432
port mirroring 300, 301
  activate backup image 302
  dual image 301
port routing
  adding a default route 44
  adding a static route 45, 46
  configuration 40
  enabling routing for ports 41, 42
  enabling routing for the switch 41
port security
  802.1x 251, 252
  convert dynamic to static address 243
  static MAC address 244
private edge VLANs 9
private VLAN groups 370
protected ports 244, 245, 247
Protocol-independent multicast sparse mode 427
Protocol-Independent-Multicast 403
Proxy Address Resolution Protocol 103
QoS
  class 174
  policy 174
  service 174
R
RADIUS
  assigning VLANs 262, 263, 265
rapid STP (802.1w) 378
RIP 40, 54, 60
  VLAN routing 60, 62
Routing Information Protocol (RIP) 54
S
script 297
script delete 297
script list 297
scripting, configuration 296
security
802.1x port security 251, 252
DHCP messages, maximum rate 280, 281
DHCP snooping 276, 277
IP source guard 282
protected ports 244, 247
static binding 279, 280
static mapping 274, 275
sFlow 341, 342, 343
sFlow, time-based sampling of counters 345
show logging 309
show logging buffered 311
show logging hosts 313
show logging traplogs 312
show network 305
show SNTP (CLI only) 287
show switch 322
show telnet 305
SNMP 337
SNMP trap 338
SNTP 287
    configure 289
SNTP server 291
Spanning Tree protocol 376
stack members, renumbering 334
stacking
    moving a master to a different stack 336
stacking ports, Ethernet configuration 324
stacks
    adding switches to 330
    code mismatch 323
    compatible switch models 321
    firmware 322
    installation 322
    removing switches from 331
    upgrading firmware 323, 324
stacks, 10G fiber 327, 328, 329
static binding 279, 280
static host name 346
static mapping 274, 275
STP
    multiple STP (802.1s) 379
STPs 376
switch
    FSM family of switches 321
    GSM family of switches 321
switch priority 321
switch stack
    configuration files 332
    member numbers 320
    member priority values 321
    membership 320
    software compatibility 332
upgrading firmware 323
Syslog
    show logging 309
    show logging buffered 311
syslog 308
T
technical support 2
Telnet
    configure 306
    session-limit 307
    session-timeout 307
Telnet, outbound 304
time, set the time zone (CLI only) 291
trace route 294, 295, 296
trademarks 29, 295, 296
tunnel 382, 383, 385
V
video streaming 221
VLAN
    guest VLAN 257
    IPv6 routing VLAN 395
    private VLAN groups 370
VLAN routing 52, 53
VLANs 9
    assigning ports 12, 13, 14
    creating two VLANs 10
    default 15
    guest VLANs 257, 258, 259
    IP subnet based 21
    IP subnet-based 21, 22, 23
    MAC-based 16, 17
    private edge 9
    protocol-based 19, 20
    using RADIUS to assign 262, 263, 265
VRRP 105
    backup router 108
    master router 106
W
WRED 164