NETGEAR®

ProSAFE M4100 Managed Switches

Software Administration Manual

Software Version 10.0.1

March 2015
202-11161-02

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

After installing your device, locate the serial number on the label of your product and use it to register your product at *https://my.netgear.com*. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website. For product updates and web support, visit *http://support.netgear.com*.

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

Phone (Other Countries): Check the list of phone numbers at *http://support.netgear.com/general/contact/default.aspx*.

Contact your Internet service provider for technical support.

Compliance

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

See the regulatory compliance document before connecting the power supply.

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-11161-02	March 2015	Made the document specific to the M4100 series switches by removing sections and chapters that do not apply to the M4100 series switches.
202-11161-01	February 2013	Updated the document.
	October 2012	Added iSCSI features.
202-11153-01	August 2012	Added Private VLAN features.
202-10515-05	August 2012	Added MVR feature.
202-10515-05	July 2011	Added DHCPv6 and DHCPv6 mode features.
202-10515-04	November 2010	New document template.
202-10515-03	June 2010	Moved some content to the *Software Setup Guide*.
202-10515-02		Software release 8.0.2: new firmware with DHCP L3 Relay, color conform policy, DHCP server in dynamic mode, and configuring a stacking port as an Ethernet port.
202-10515-01		Original publication.

Table of Contents

Chapter 1 Documentation Resources

Chapter 2 VLANs

Chapter 3 LAGs

Chapter 4 Port Routing

Chapter 5 VLAN Routing

Chapter 6 Proxy ARP

Chapter 7 ACLs

Chapter 8 CoS Queuing

Chapter 9 DiffServ

Chapter 10 IGMP Snooping and Querier

Chapter 11 MVR

Chapter 12 Security Management

Chapter 13 SNTP

Chapter 14 Tools

Chapter 15 Syslog

Chapter 16 SNMP

Chapter 17 DNS

Chapter 18 DHCP Server

Chapter 19 DVLANs and Private VLANs

Chapter 20 STP

Chapter 21 DHCP L2 Relay and L3 Relay

Chapter 22 MLD Snooping

Index

1. Documentation Resources

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
- *Managed Switch Hardware Installation Guide*
- *Managed Switch Software Setup Manual*
- *ProSAFE Managed Switch Command Line Interface (CLI) User Manual*
- ProSAFE M4100 Managed Switch Web Management User Manual

VLANs

2

Virtual LANs

This chapter includes the following sections:

VLAN Concepts

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

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

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

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

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

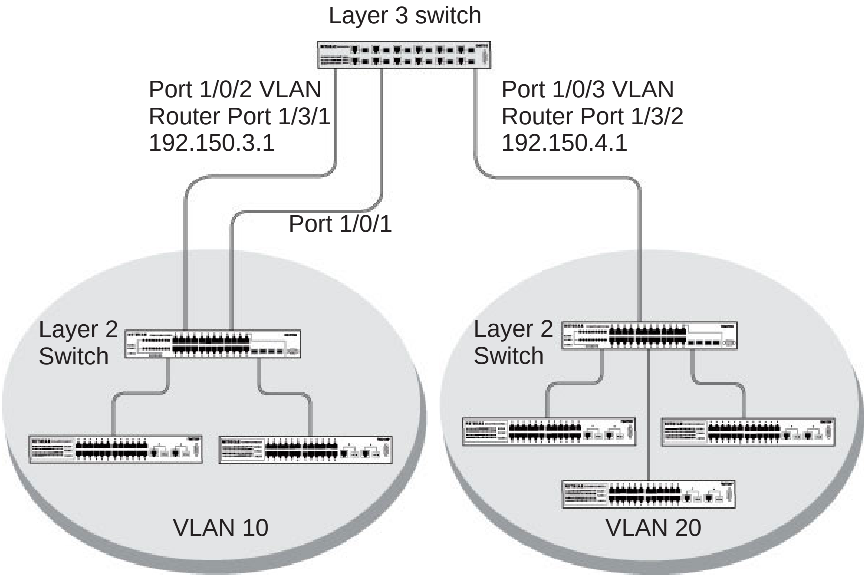


Figure 1. Switch with 4 ports configured for traffic from 2 VLANs

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

Create Two VLANs

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

CLI: Create Two VLANS

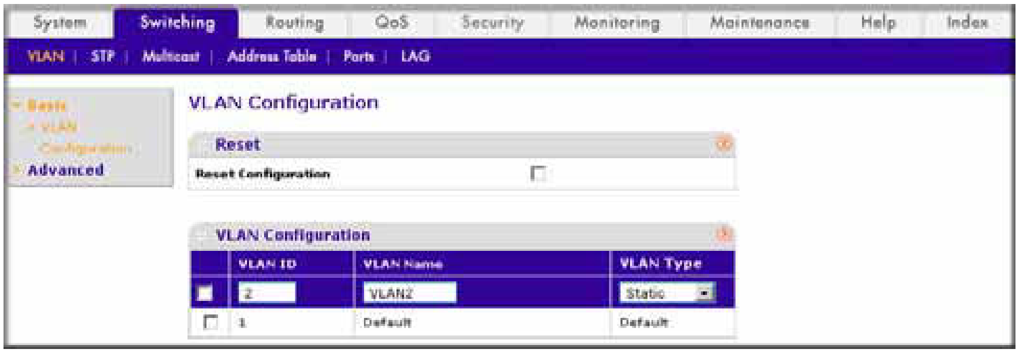
Use the following commands to create two VLANs and to assign the VLAN IDs while leaving the names blank.

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

Web Interface: Create Two VLANS

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

      A screen similar to the following displays.



VLAN Configuration

Reset

Reset Configuration □

VLAN Configuration

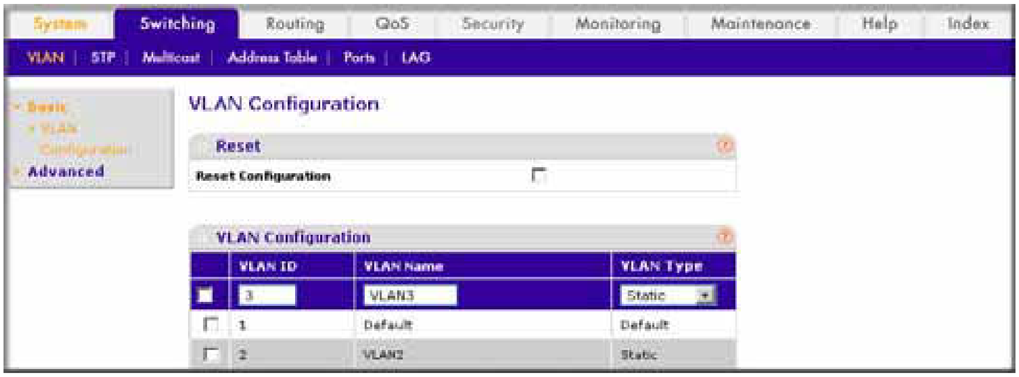
	VLAN ID	VLAN Name	VLAN Type
□	2	VLAN2	Static
□	1	Default	Default

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

   c. Click **Add.**

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

A screen similar to the following displays.



VLAN Configuration

Reset

Reset Configuration □

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type
□	3	VLAN3	Static
□	1	Default	Default
□	2	VLAN2	Static

b. Enter the following information:

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

c. Click **Add.**

Assign Ports to VLAN2

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

CLI: Assign Ports to VLAN2

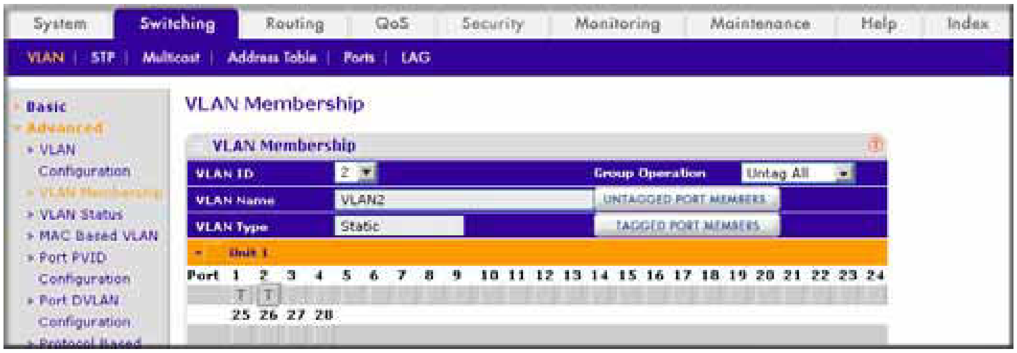
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan participation include 2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan acceptframe vlanonly
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan pvid 2
(Netgear Switch)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

Web Interface: Assign Ports to VLAN2

1. Assign ports to VLAN2.

   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

A screen similar to the following displays.



VLAN Membership

VLAN Membership

VLAN ID: 2

Group Operation: Untag All

VLAN Name: VLAN2

VLAN Type: Static

b. In the **VLAN ID** list, select **2**.

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

d. Click the gray boxes under ports **1** and **2** until **T** displays.

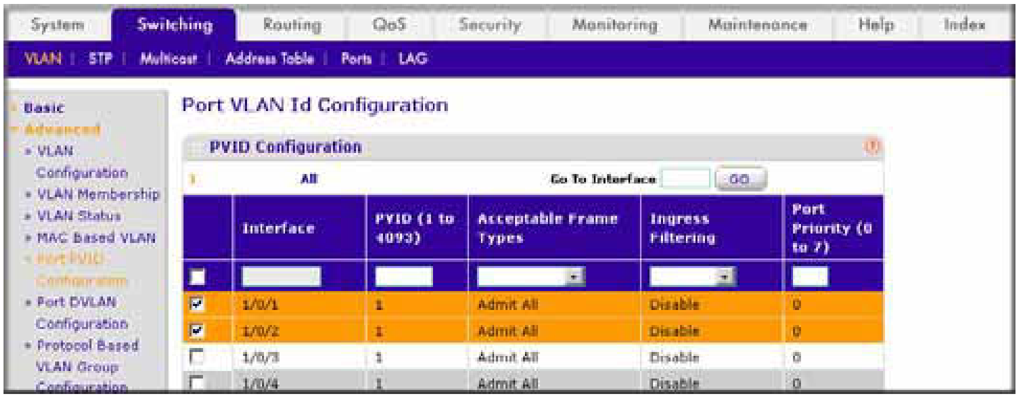
The T specifies that the egress packet is tagged for the ports.

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

2. Specify that only tagged frames will be accepted on ports 1/0/1 and 1/0/2.

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

A screen similar to the following displays.



Port VLAN Id Configuration

PVID Configuration

	Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)
□					
☑	1/0/1	1	Admit All	Disable	0
☑	1/0/2	1	Admit All	Disable	0
□	1/0/3	1	Admit All	Disable	0
□	1/0/4	1	Admit All	Disable	0

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

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

c. Enter the following information:

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

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

Create Three VLANs

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

CLI: Create Three VLANS

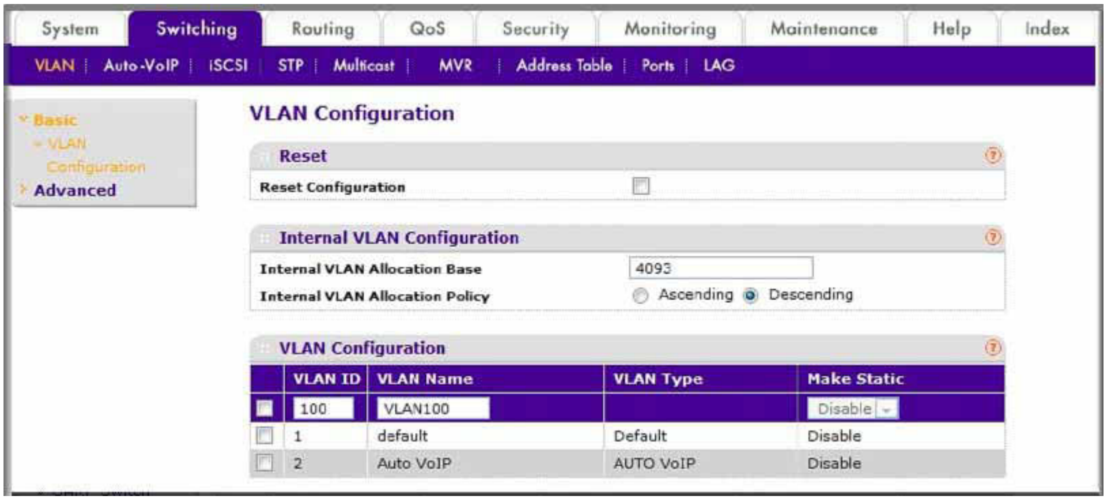
Use the following commands to create three VLANs and to assign the VLAN IDs while leaving the names blank.

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

Web Interface: Create Three VLANS

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

      A screen similar to the following displays.



VLAN Configuration

Reset

Reset Configuration □

Internal VLAN Configuration

Internal VLAN Allocation Base 4093

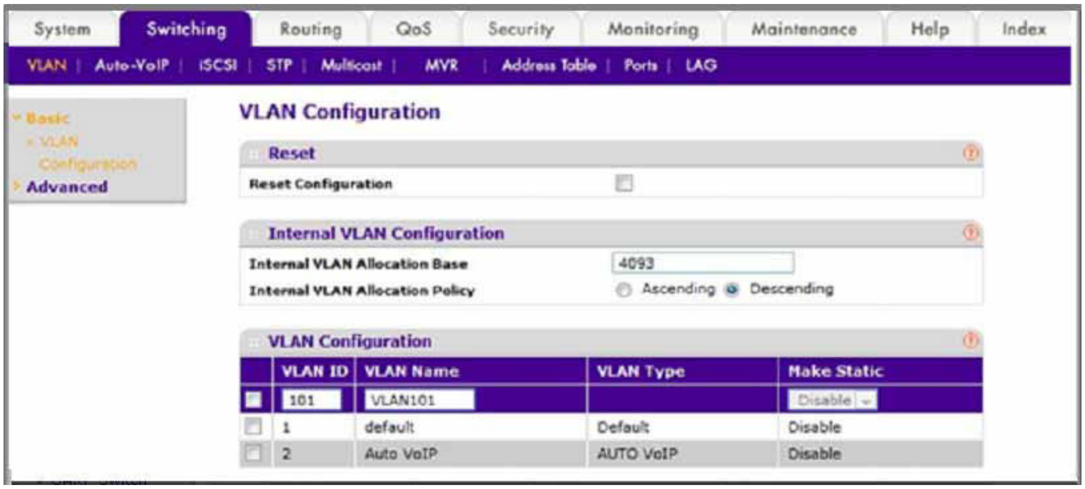
Internal VLAN Allocation Policy ○ Ascending ● Descending

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type	Make Static
□	100	VLAN100		Disable
□	1	default	Default	Disable
□	2	Auto VoIP	AUTO VoIP	Disable

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

A screen similar to the following displays.



VLAN Configuration

Reset

Reset Configuration □

Internal VLAN Configuration

Internal VLAN Allocation Base 4093

Internal VLAN Allocation Policy ○ Ascending ● Descending

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type	Make Static
□	101	VLAN101		Disable
□	1	default	Default	Disable
□	2	Auto VoIP	AUTO VoIP	Disable

b. Enter the following information:

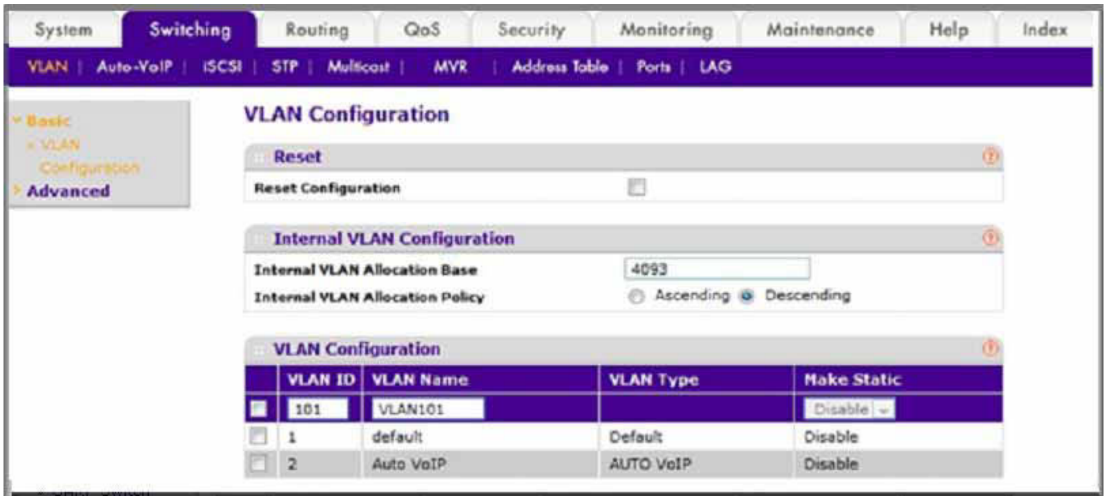
- In the **VLAN ID** field, enter **101**.
- In the **VLAN Name** field, enter **VLAN101**.

c. Click **Add.**

3. Create VLAN102.

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

A screen similar to the following displays.



VLAN Configuration

Reset

Reset Configuration □

Internal VLAN Configuration

Internal VLAN Allocation Base 4093

Internal VLAN Allocation Policy ○ Ascending ● Descending

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type	Make Static
□	101	VLAN101		Disable
□	1	default	Default	Disable
□	2	Auto VoIP	AUTO VoIP	Disable

b. Enter the following information:

- In the **VLAN ID** field, enter **102**.
- In the **VLAN Name** field, enter **VLAN102**.

c. Click **Add.**

Assign Ports to VLAN3

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

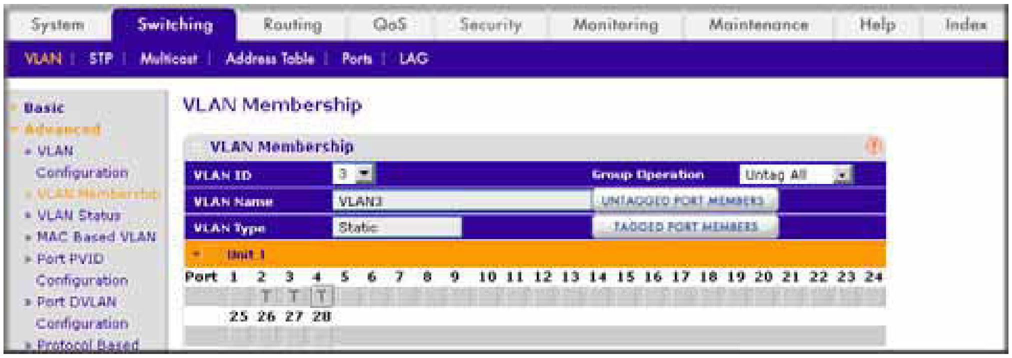
CLI: Assign Ports to VLAN3

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

Web Interface: Assign Ports to VLAN3

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

      A screen similar to the following displays.



VLAN Membership

VLAN ID: 3

Group Operation: Untag All

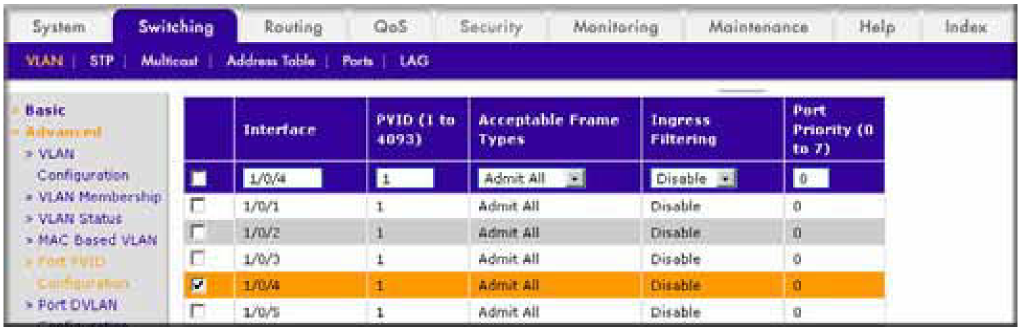
VLAN Name: VLAN3

VLAN Type: Static

   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.



	Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)
☐	1/0/4	1	Admit All	Disable	0
☐	1/0/1	1	Admit All	Disable	0
☐	1/0/2	1	Admit All	Disable	0
☐	1/0/3	1	Admit All	Disable	0
☑	1/0/4	1	Admit All	Disable	0
☐	1/0/5	1	Admit All	Disable	0

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

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

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

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

Assign 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.

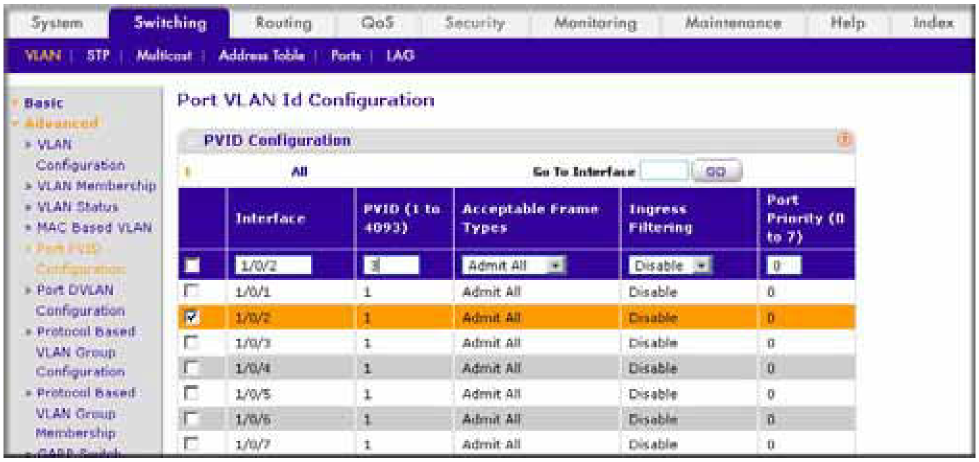
CLI: Assign VLAN3 as the Default VLAN for Port 1/0/2

```
(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. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

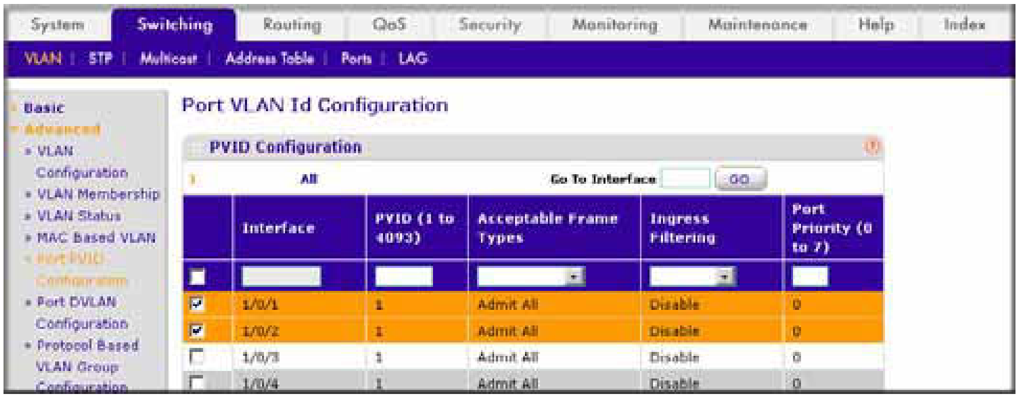
   A screen similar to the following displays.



	Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)
☐	1/0/2	3	Admit All	Disable	0
☐	1/0/1	1	Admit All	Disable	0
☑	1/0/2	1	Admit All	Disable	0
☐	1/0/3	1	Admit All	Disable	0
☐	1/0/4	1	Admit All	Disable	0
☐	1/0/5	1	Admit All	Disable	0
☐	1/0/6	1	Admit All	Disable	0
☐	1/0/7	1	Admit All	Disable	0

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

Create a MAC-Based VLAN



	Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)
☐					
☑	1/0/1	1	Admit All	Disable	0
☑	1/0/2	1	Admit All	Disable	0
☐	1/0/3	1	Admit All	Disable	0
☐	1/0/4	1	Admit All	Disable	0

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

You define a MAC to VLAN mapping by configuring an entry in the MAC to VLAN table. An entry is specified using a source MAC address and the appropriate VLAN ID. The MAC to

VLAN configurations are shared across all ports of the device (i.e., there is a system-wide table that has MAC address to VLAN ID mappings).

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

CLI: Create a MAC-Based VLAN

1. Create VLAN3.

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

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

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

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

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

4. Add all the ports to VLAN3.

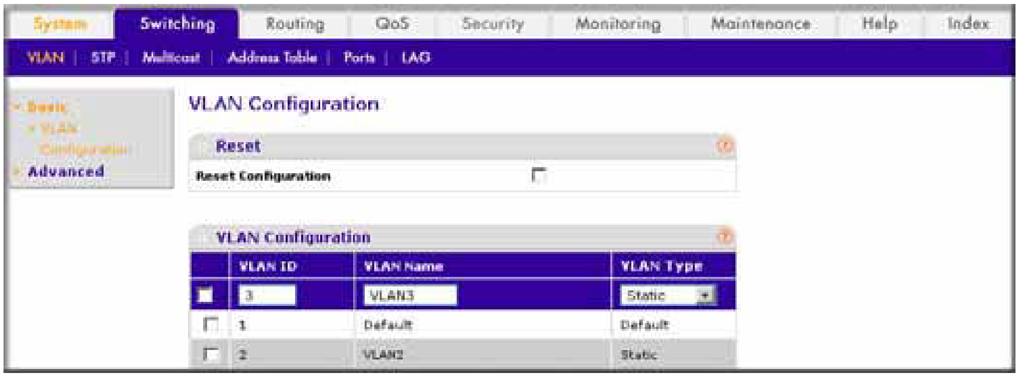
```
(Netgear Switch)#config
(Netgear Switch)(Config)#interface range 1/0/1-1/0/28
(Netgear Switch)(conf-if-range-1/0/1-1/0/28)#vlan participation include 3
(Netgear Switch)(conf-if-range-1/0/1-1/0/28)#exit
(Netgear Switch)(Config)#exit
```

Web Interface: Assign a MAC-Based VLAN

1. Create VLAN3.

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

   A screen similar to the following displays.



VLAN Configuration

Reset

Reset Configuration □

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type
□	3	VLAN3	Static
□	1	Default	Default
□	2	VLAN2	Static

   b. Enter the following information:

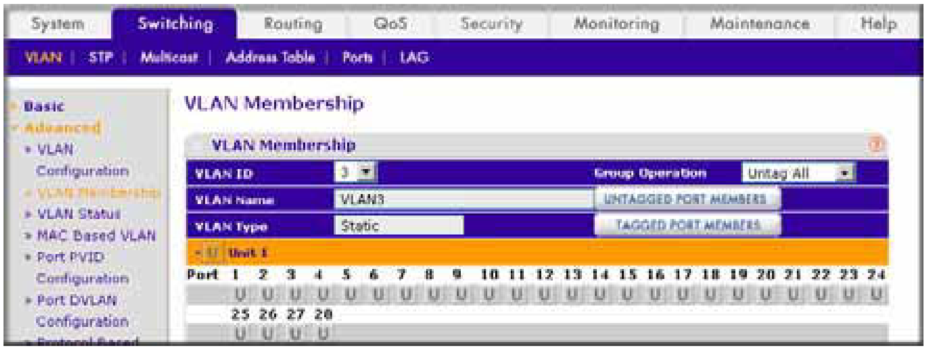
   - In the **VLAN ID** field, enter **3**.
   - In the **VLAN Nam**e field, enter **VLAN3**.
   - In the **VLAN Type** list, select **Static**.

   c. Click **Add**.

2. Assign ports to VLAN3.

   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

   A screen similar to the following displays.



VLAN Membership

VLAN Membership

VLAN ID 3 Group Operation Untag All

VLAN Name VLAN3

VLAN Type Static

U Unit 1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U
	25	26	27	28																				
	U	U	U	U																				

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

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

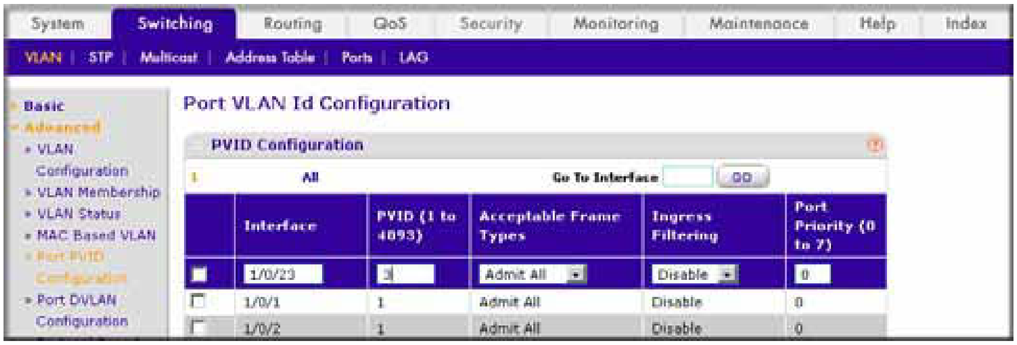
   d. Click the gray box before Unit 1 until **U** displays.

   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

PVID Configuration

1 All Go To Interface GO

	Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)
□	1/0/23	3	Admit All	Disable	0
□	1/0/1	1	Admit All	Disable	0
□	1/0/2	1	Admit All	Disable	0

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

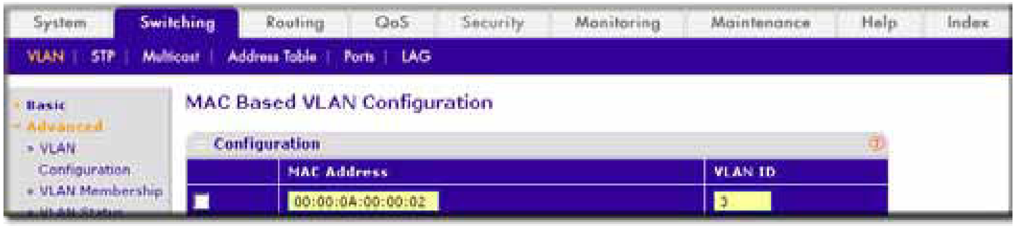
c. In the **PVID (1 to 4093)** field, enter **3**.

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

4. Map the specific MAC to VLAN3.

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

A screen similar to the following displays.



MAC Based VLAN Configuration

Configuration

	MAC Address	VLAN ID
□	00:00:0A:00:00:02	3

b. Enter the following information:

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

c. Click **Add**.

Create a Protocol-Based VLAN

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

CLI: Create a Protocol-Based VLAN

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

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

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

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

3. Assign VLAN protocol group 1 to VLAN 4.

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

4. Assign VLAN protocol group 2 to VLAN 5.

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

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

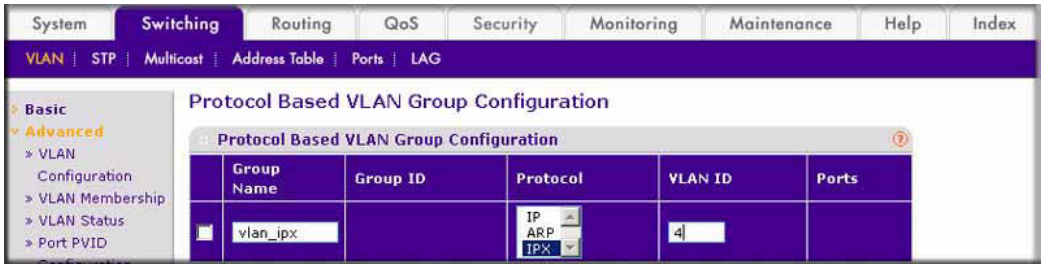
```
(Netgear Switch)(Vlan)#exit
(Netgear Switch)#config
(Netgear Switch)(Config)#interface 1/0/11
(Netgear Switch)(Interface 1/0/11)#protocol vlan group 1
(Netgear Switch)(Interface 1/0/11)#protocol vlan group 2
(Netgear Switch)(Interface 1/0/11)#exit
```

Web Interface: Create a Protocol-Based VLAN

1. Create the protocol-based VLAN group vlan_ipx.

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

   A screen similar to the following displays.



Protocol Based VLAN Group Configuration

Protocol Based VLAN Group Configuration

	Group Name	Group ID	Protocol	VLAN ID	Ports
☐	vlan_ipx		IP ARP IPX	4	

   Enter the following information:

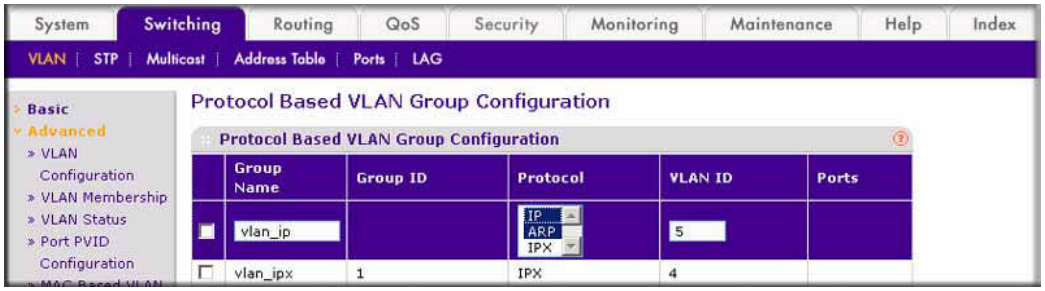
   - In the **Group Name** field, enter **vlan_ipx.**
   - In the **Protocol** list, select **IPX**.
   - In the **VLAN ID** field, enter **4.**

   b. Click **Add**.

2. Create the protocol-based VLAN group vlan_ip.

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

   A screen similar to the following displays.



Protocol Based VLAN Group Configuration

Protocol Based VLAN Group Configuration

	Group Name	Group ID	Protocol	VLAN ID	Ports
☐	vlan_ip		IP ARP IPX	5	
☐	vlan_ipx	1	IPX	4	

   b. Enter the following information:

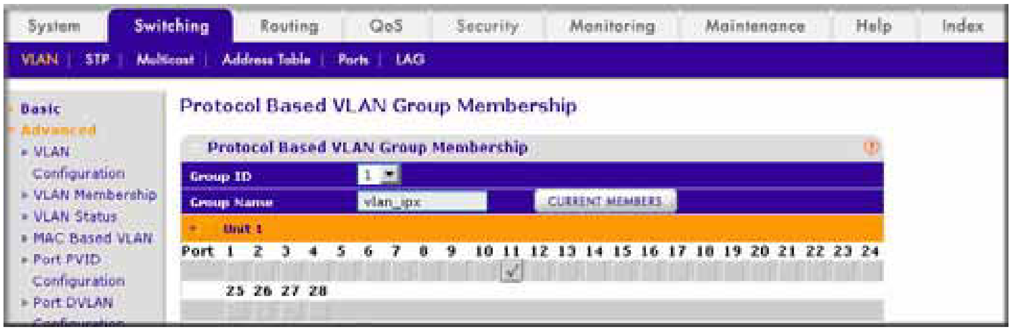
   - In the **Group Name** field, enter **vlan_ip**.
   - In the **Protocol** list, select **IP** and **ARP** while holding down the **Ctrl** key.
   - In the **VLAN** field, enter **5.**

   c. Click **Add**.

3. Add port 11 to the group vlan_ipx.

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

A screen similar to the following displays.



Protocol Based VLAN Group Membership

Group ID: 1

Group Name: vlan_ipx

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

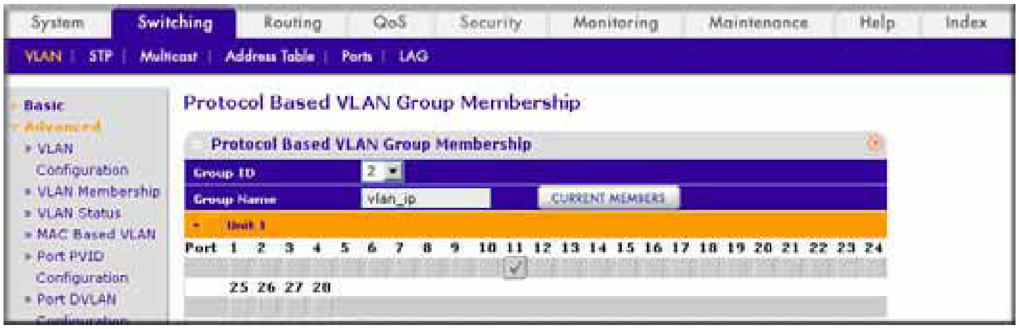
c. Click the gray box under port **11**. A check mark displays in the box.

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.



Protocol Based VLAN Group Membership

Group ID: 2

Group Name: vlan_ip

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

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

d. Click **Apply**.

Virtual VLANs: Create an IP Subnet–Based VLAN

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

VLAN is routed. The IP subnet classification feature affects only the VLAN assignment of a packet. Appropriate 802.1Q VLAN configuration must exist in order for the packet to be switched.

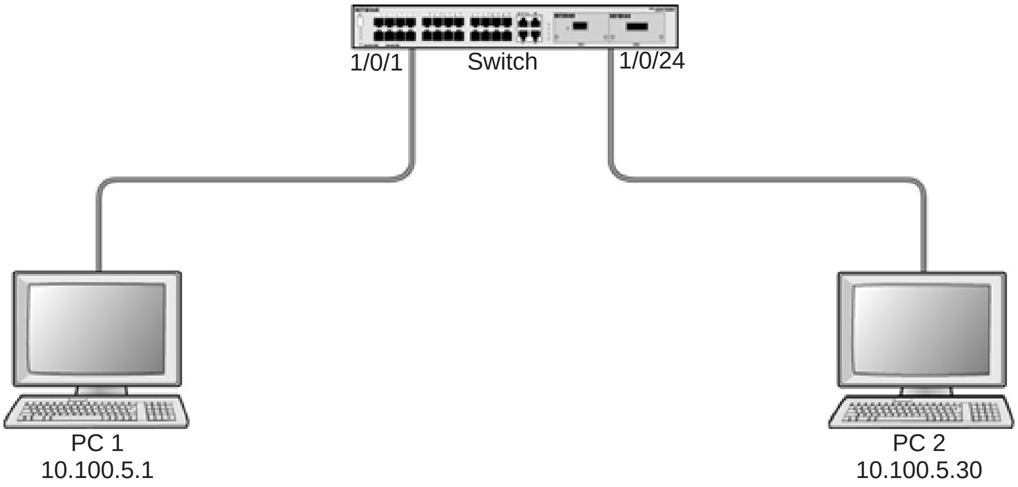


Figure 2. IP subnet–based VLAN

CLI: Create an IP Subnet–Based VLAN

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

Create an IP subnet–based VLAN 2000.

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

Assign all the ports to VLAN 2000.

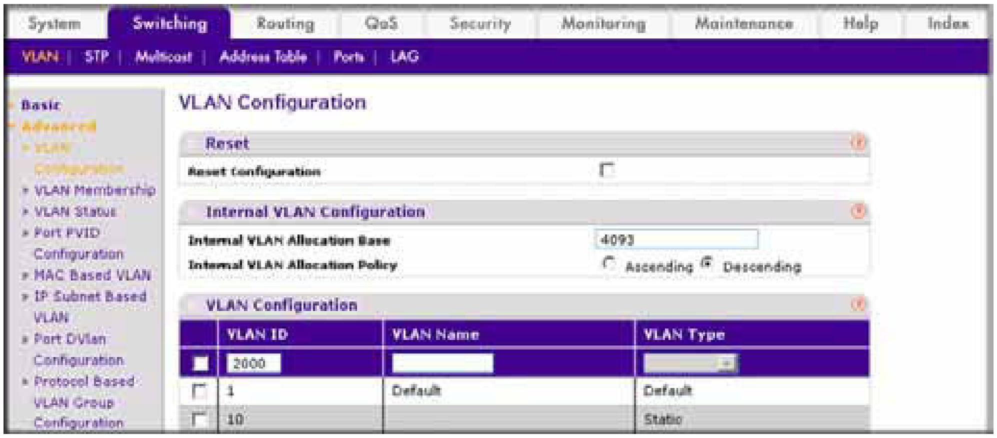
```
(Netgear Switch) #show mac-addr-table vlan 2000
MAC Address       Interface     Status
-----------------  ---------    ------------
00:00:24:58:F5:56  1/0/1        Learned
00:00:24:59:00:62  1/0/24       Learned
```

Web Interface: Create an IP Subnet–Based VLAN

1. Create VLAN 2000.

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

   A screen similar to the following displays.



VLAN Configuration

Reset

Reset configuration □

Internal VLAN Configuration

Internal VLAN Allocation Base 4093

Internal VLAN Allocation Policy ○ Ascending ● Descending

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type
□	2000		
□	1	Default	Default
□	10		Static

   b. Enter the following information:

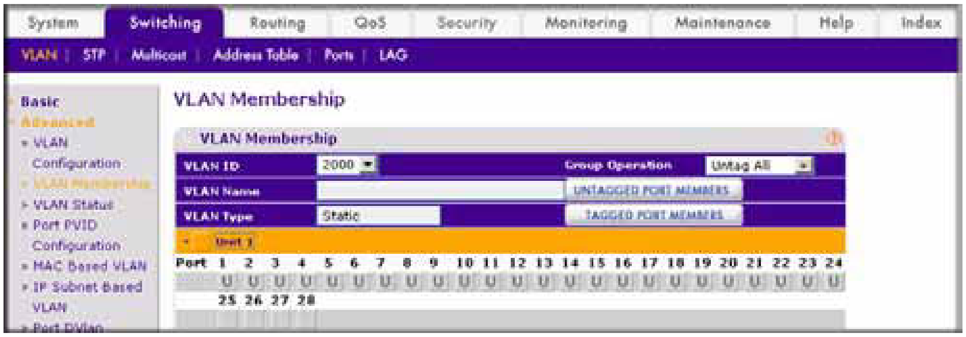
   - In the **VLAN ID** field, enter **2000**.
   - In the **VLAN Type** list, select **Static**.

   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.



VLAN Membership

VLAN Membership

VLAN ID 2000 Group Operation Untag All

VLAN Name

VLAN Type Static

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U
	25	26	27	28																				

   b. In the **VLAN ID** list, select **2000**.

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

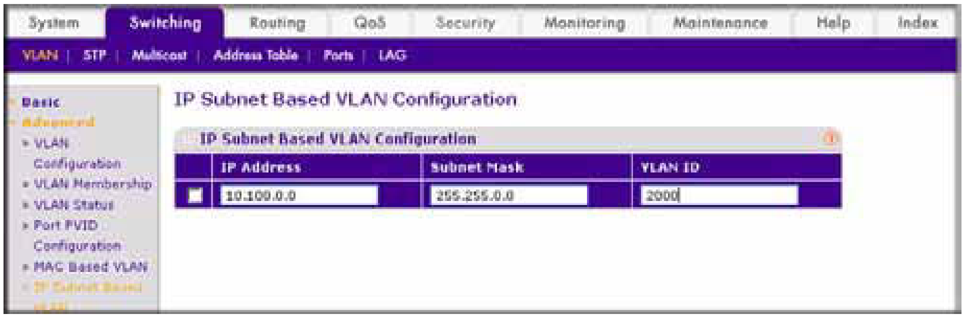
   d. Click the gray box before Unit 1 until **U** displays.

   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

IP Subnet Based VLAN Configuration

	IP Address	Subnet Mask	VLAN ID
□	10.100.0.0	255.255.0.0	2000

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.

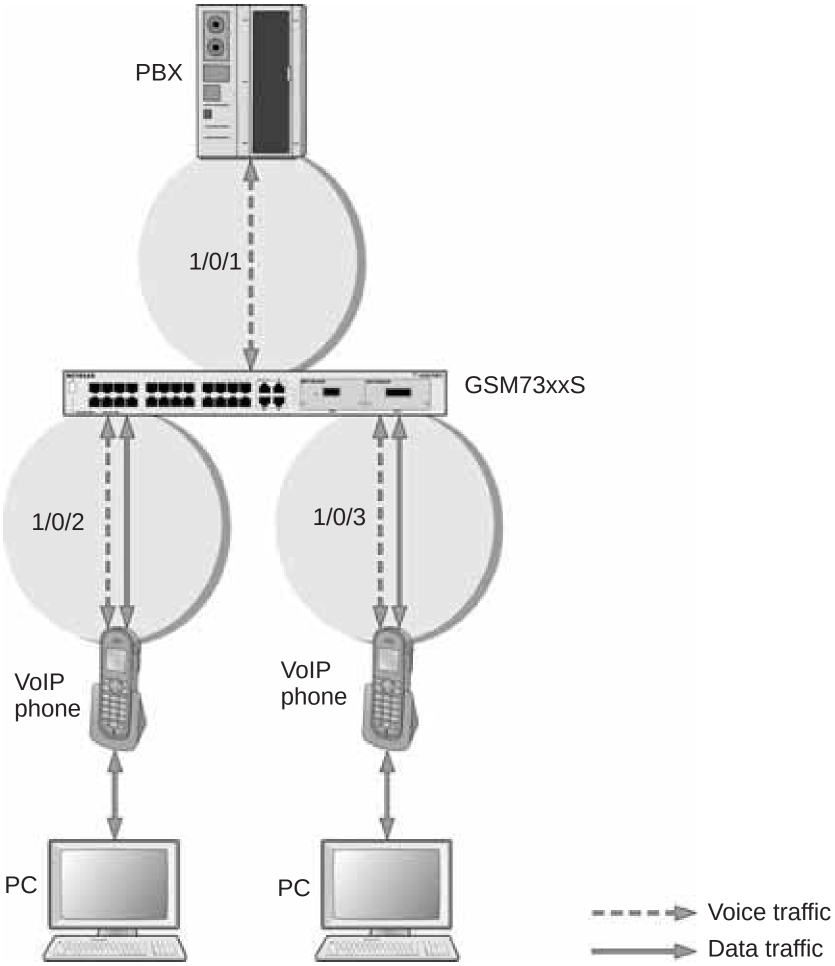


Figure 3. Voice VLAN

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

CLI: Configure Voice VLAN and Prioritize Voice Traffic

1. Create VLAN 10.

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

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

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

3. Configure Voice VLAN globally.

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

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

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

5. Create the DiffServ class ClassVoiceVLAN.

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

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

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

7. Create the DiffServ policy PolicyVoiceVLAN.

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

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

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

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

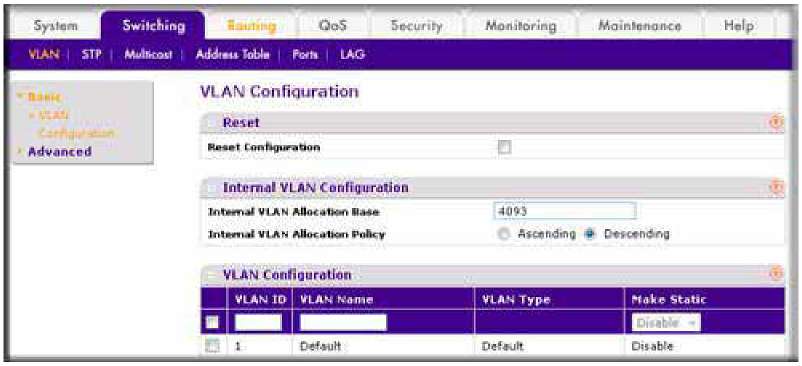
```
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)# service-policy in PolicyVoiceVLAN
```

Web Interface: Configure Voice VLAN and Prioritize Voice Traffic

1. Create VLAN 10.

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

   A screen similar to the following displays.



VLAN Configuration

Reset

Reset Configuration □

Internal VLAN Configuration

Internal VLAN Allocation Base 4093

Internal VLAN Allocation Policy ○ Ascending ● Descending

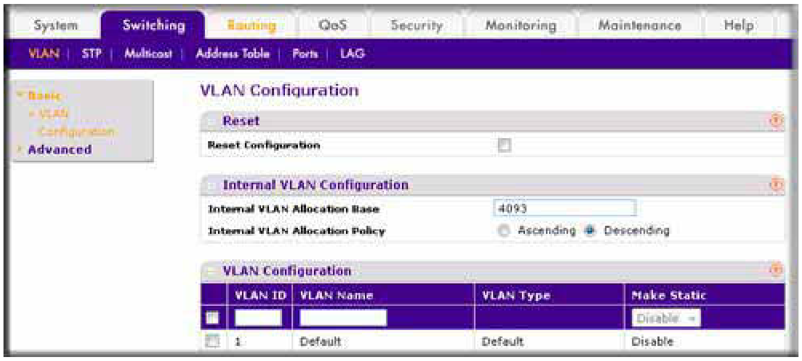
VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type	Make Static
□				Disable
□	1	Default	Default	Disable

   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

Reset

Reset Configuration □

Internal VLAN Configuration

Internal VLAN Allocation Base 4093

Internal VLAN Allocation Policy ○ Ascending ● Descending

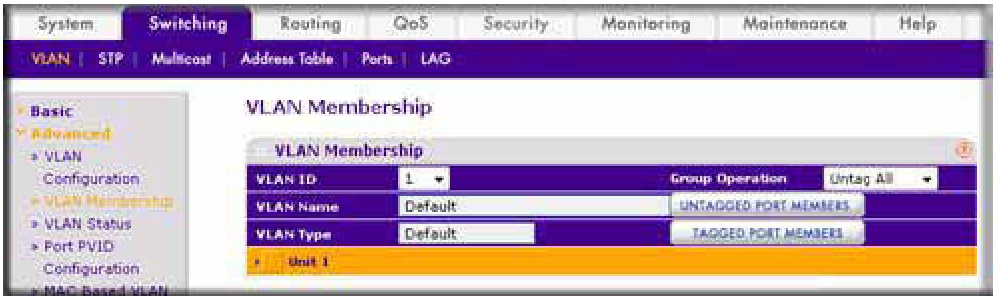
VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type	Make Static
□				Disable
□	1	Default	Default	Disable

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

   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

   A screen similar to the following displays.



VLAN Membership

VLAN Membership

VLAN ID 1 Group Operation Untag All

VLAN Name Default

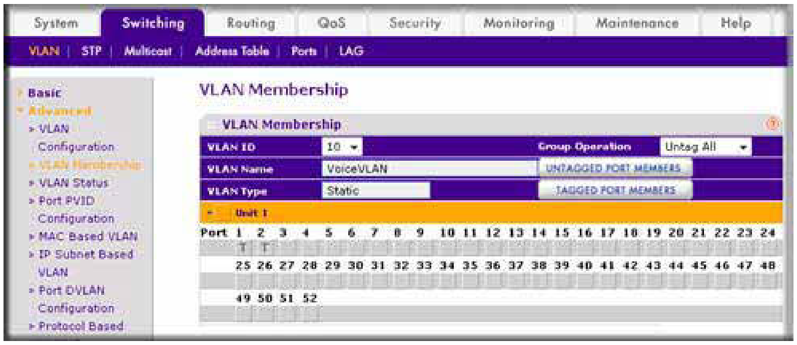
VLAN Type Default

Unit 1

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.



VLAN Membership

VLAN Membership

VLAN ID	10	Group Operation	Untag All
VLAN Name	VoiceVLAN		
VLAN Type	Static		

Unit 1

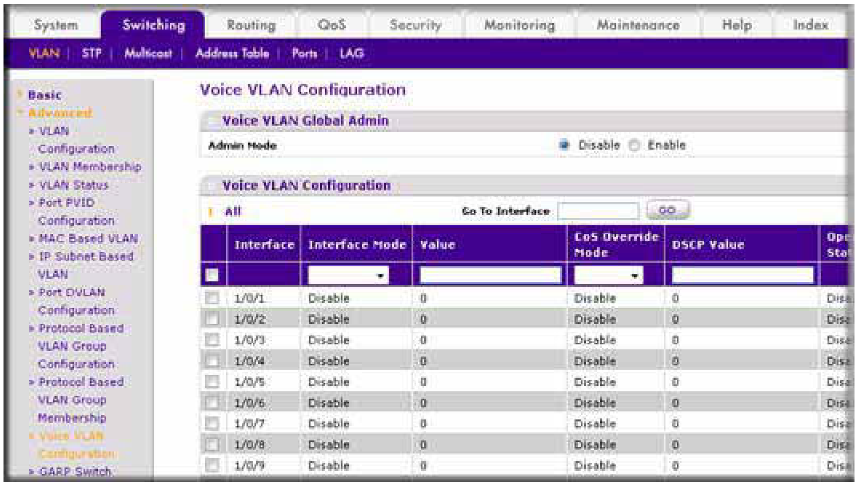
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	T	T																						
	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
	49	50	51	52																				

d. Click **Apply**.

3. Configure Voice VLAN globally.

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

A screen similar to the following displays.



Voice VLAN Configuration

Voice VLAN Global Admin

Admin Mode ● Disable ○ Enable

Voice VLAN Configuration

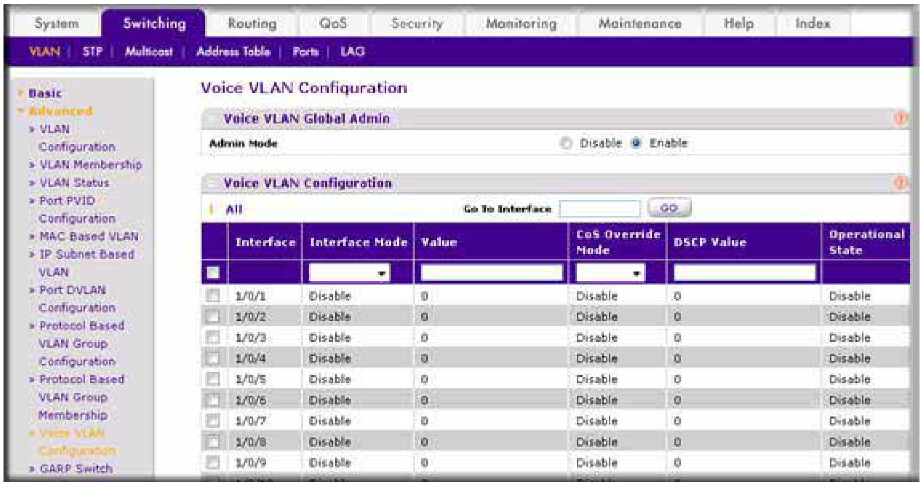
All Go To Interface

	Interface	Interface Mode	Value	CoS Override Mode	DSCP Value	Ope Sta
□						
□	1/0/1	Disable	0	Disable	0	Dis
□	1/0/2	Disable	0	Disable	0	Dis
□	1/0/3	Disable	0	Disable	0	Dis
□	1/0/4	Disable	0	Disable	0	Dis
□	1/0/5	Disable	0	Disable	0	Dis
□	1/0/6	Disable	0	Disable	0	Dis
□	1/0/7	Disable	0	Disable	0	Dis
□	1/0/8	Disable	0	Disable	0	Dis
□	1/0/9	Disable	0	Disable	0	Dis

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

c. Click **Apply**.

A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
VLAN | STP | Multicast | Address Table | Ports | LAG
Basic
Advanced
» VLAN Configuration
» VLAN Membership
» VLAN Status
» Port PVID Configuration
» MAC Based VLAN
» IP Subnet Based VLAN
» Port DVLAN Configuration
» Protocol Based VLAN Group Configuration
» Protocol Based VLAN Group Membership
» Voice VLAN Configuration
» GARP Switch
GO

Voice VLAN Configuration

Voice VLAN Global Admin

Admin Mode ○ Disable ● Enable

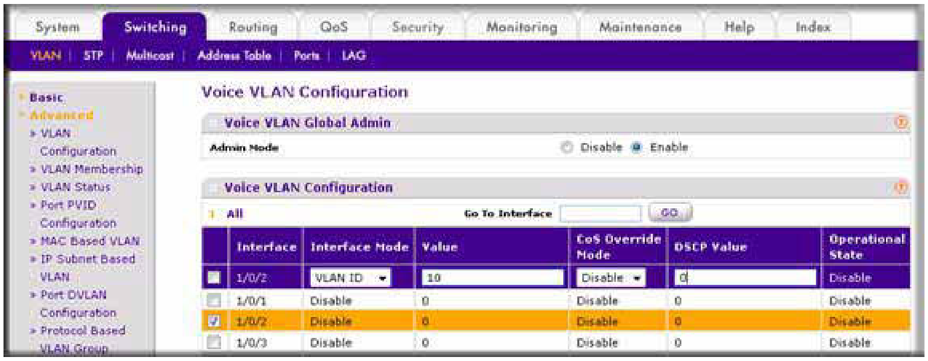
Voice VLAN Configuration

All Go To Interface

	Interface	Interface Mode	Value	CoS Override Mode	DSCP Value	Operational State
□						
□	1/0/1	Disable	0	Disable	0	Disable
□	1/0/2	Disable	0	Disable	0	Disable
□	1/0/3	Disable	0	Disable	0	Disable
□	1/0/4	Disable	0	Disable	0	Disable
□	1/0/5	Disable	0	Disable	0	Disable
□	1/0/6	Disable	0	Disable	0	Disable
□	1/0/7	Disable	0	Disable	0	Disable
□	1/0/8	Disable	0	Disable	0	Disable
□	1/0/9	Disable	0	Disable	0	Disable

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

   A screen similar to the following displays.



Voice VLAN Configuration

Voice VLAN Global Admin

Admin Mode ○ Disable ● Enable

Voice VLAN Configuration

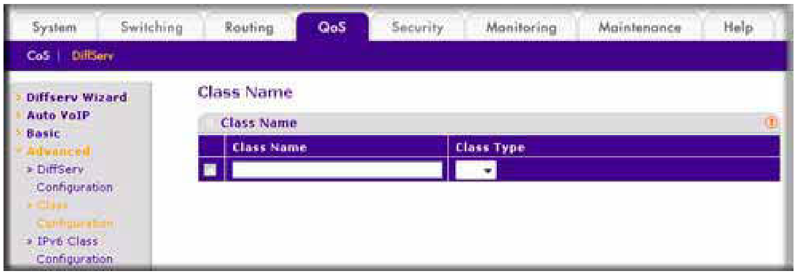
All Go To Interface

	Interface	Interface Mode	Value	CoS Override Mode	DSCP Value	Operational State
□	1/0/2	VLAN ID	10	Disable	0	Disable
□	1/0/1	Disable	0	Disable	0	Disable
☑	1/0/2	Disable	0	Disable	0	Disable
□	1/0/3	Disable	0	Disable	0	Disable

   e. Click **Apply**.

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

A screen similar to the following displays.



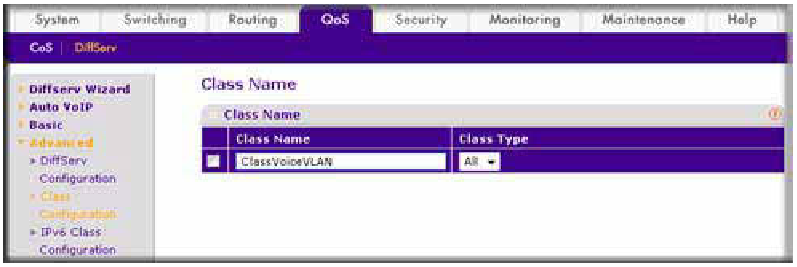
Class Name

Class Name	Class Type

b. In the **Class Name** field, enter **ClassVoiceVLAN**.

c. In the **Class Type** list, select **All**.

A screen similar to the following displays.



Class Name

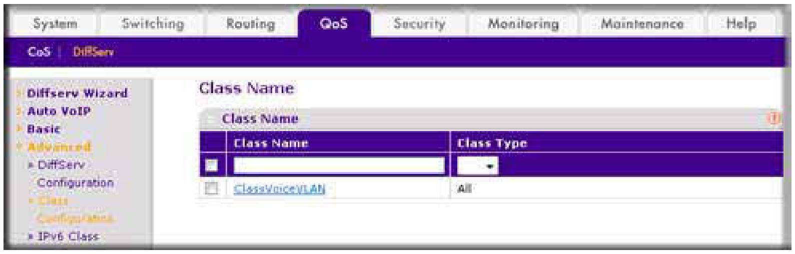
Class Name	Class Type
ClassVoiceVLAN	All

d. Click **Add**. The Class Name screen displays, as shown in the next step in this procedure.

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

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

A screen similar to the following displays.

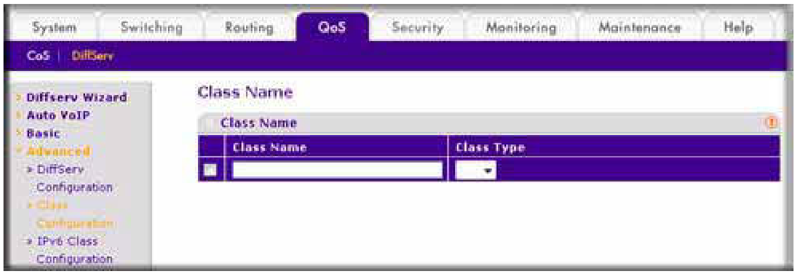


Class Name

Class Name	Class Type
ClassVoiceVLAN	All

b. Click the class **ClassVoiceVLAN**.

A screen similar to the following displays.



Class Name

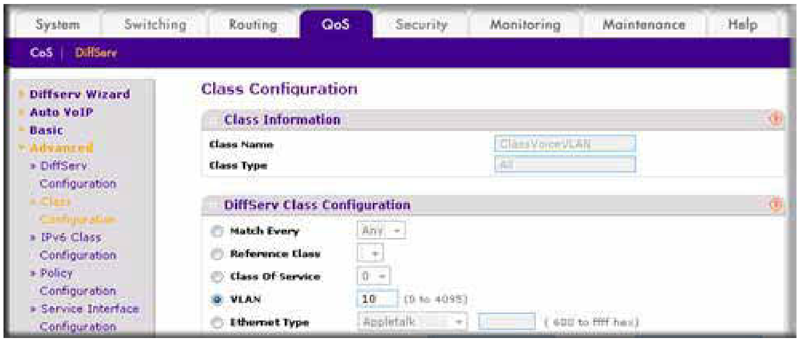
Class Name

	Class Name	Class Type
□		

c. In the DiffServ Class Configuration table, select **VLAN**.

d. In the VLAN ID field, enter 10.

A screen similar to the following displays.



Class Configuration

Class Information

Class Name ClassVoiceVLAN

Class Type All

DiffServ Class Configuration

○ Match Every Any

○ Reference Class

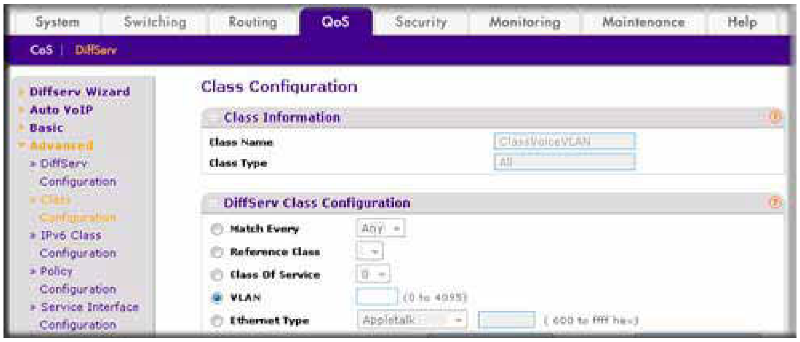
○ Class Of Service 0

● VLAN 10 (0 to 4095)

○ Ethernet Type Appletalk (600 to ffff hex)

e. Click **Apply**.

A screen similar to the following displays.



Class Configuration

Class Information

Class Name ClassVoiceVLAN

Class Type All

DiffServ Class Configuration

○ Match Every Any

○ Reference Class

○ Class Of Service 0

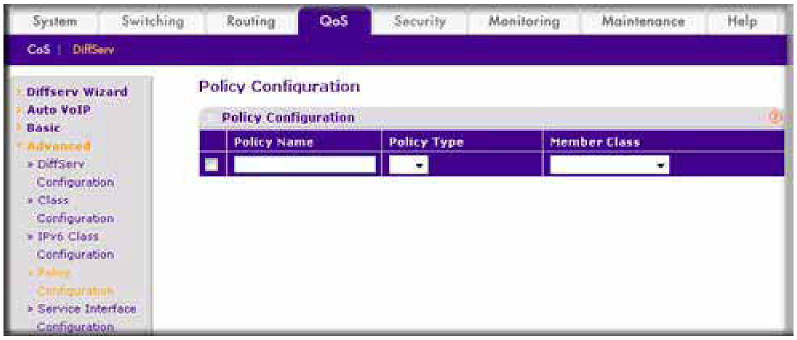
● VLAN (0 to 4095)

○ Ethernet Type Appletalk (600 to ffff hex)

7. Create the DiffServ policy PolicyVoiceVLAN.

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

A screen similar to the following displays.



Policy Configuration

Policy Configuration

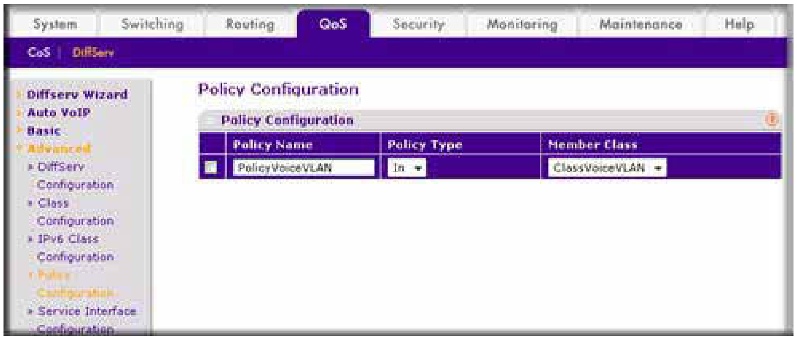
	Policy Name	Policy Type	Member Class
□			

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

Policy Configuration

	Policy Name	Policy Type	Member Class
□	PolicyVoiceVLAN	In	ClassVoiceVLAN

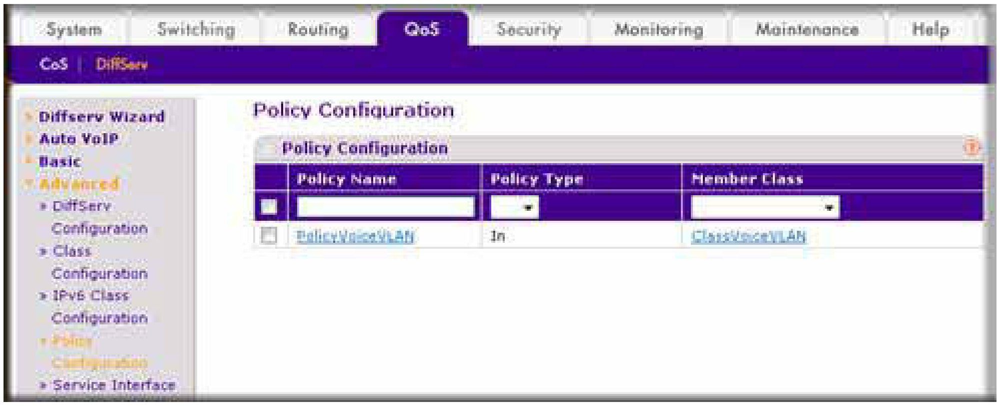
e. Click **Add**.

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

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

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

A screen similar to the following displays.



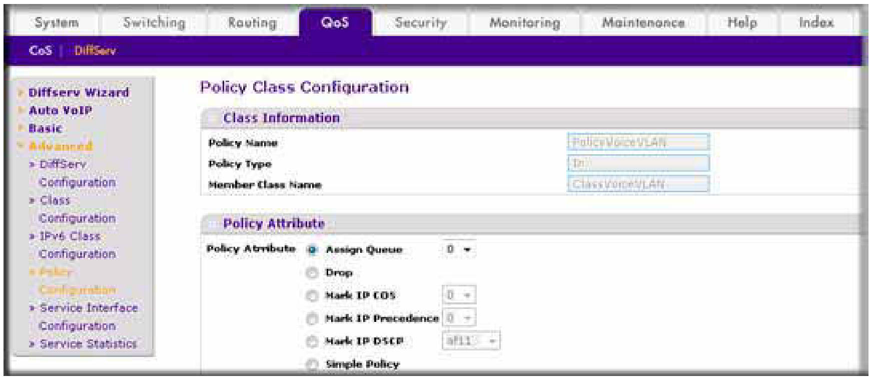
Policy Configuration

Policy Configuration

	Policy Name	Policy Type	Member Class
□			
□	PolicyVoiceVLAN	In	ClassVoiceVLAN

b. Click the **Policy PolicyVoiceVLAN**.

A screen similar to the following displays.



Policy Class Configuration

Class Information

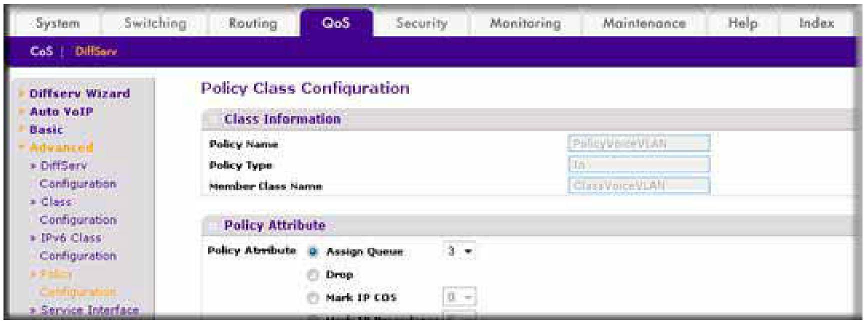
Policy Name	PolicyVoiceVLAN
Policy Type	In
Member Class Name	ClassVoiceVLAN

Policy Attribute

Policy Attribute ● Assign Queue 0
○ Drop
○ Mark IP COS 0
○ Mark IP Precedence 0
○ Mark IP DSCP af11
○ Simple Policy

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

A screen similar to the following displays.



Policy Class Configuration

Class Information

Policy Name	PolicyVoiceVLAN
Policy Type	In
Member Class Name	ClassVoiceVLAN

Policy Attribute

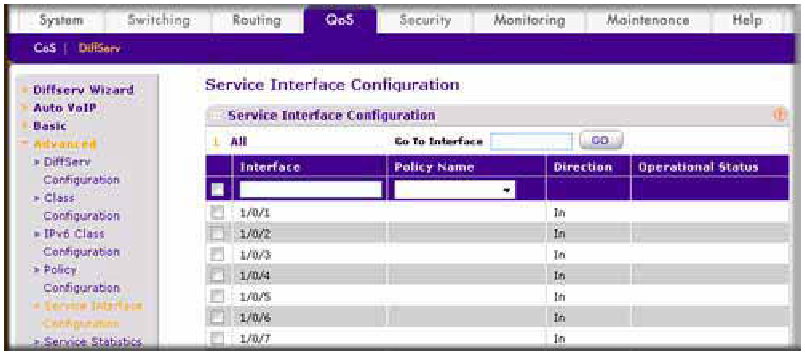
Policy Attribute ● Assign Queue 3
○ Drop
○ Mark IP COS 0

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.



Service Interface Configuration

Service Interface Configuration

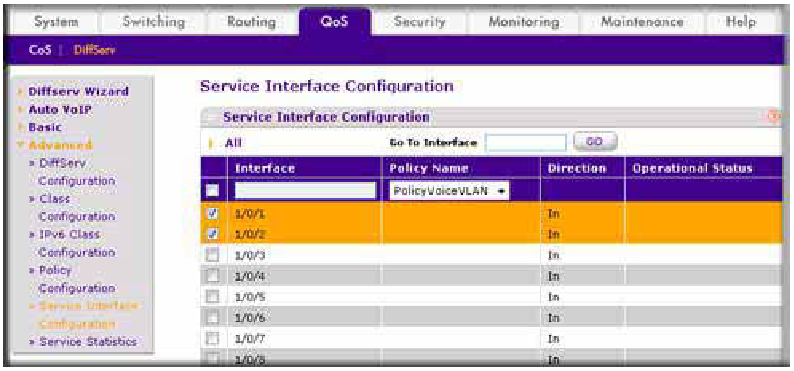
1 All   Go To Interface

	Interface	Policy Name	Direction	Operational Status
□				
□	1/0/1		In	
□	1/0/2		In	
□	1/0/3		In	
□	1/0/4		In	
□	1/0/5		In	
□	1/0/6		In	
□	1/0/7		In	

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.



Service Interface Configuration

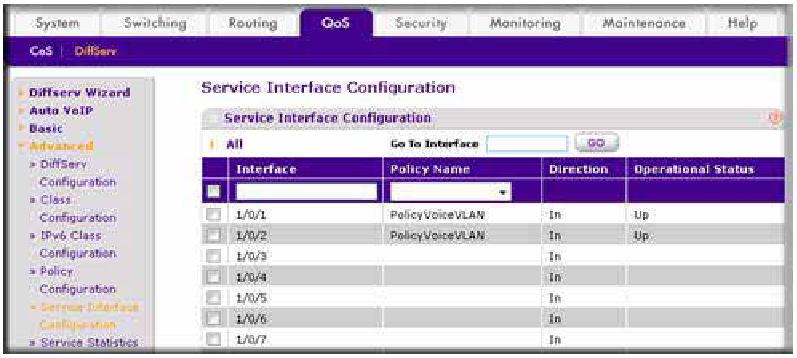
Service Interface Configuration

All   Go To Interface

	Interface	Policy Name	Direction	Operational Status
□		PolicyVoiceVLAN		
☑	1/0/1		In	
☑	1/0/2		In	
□	1/0/3		In	
□	1/0/4		In	
□	1/0/5		In	
□	1/0/6		In	
□	1/0/7		In	
□	1/0/8		In	

d. Click **Apply**.

A screen similar to the following displays.



Service Interface Configuration

Service Interface Configuration

All   Go To Interface

	Interface	Policy Name	Direction	Operational Status
□				
□	1/0/1	PolicyVoiceVLAN	In	Up
□	1/0/2	PolicyVoiceVLAN	In	Up
□	1/0/3		In	
□	1/0/4		In	
□	1/0/5		In	
□	1/0/6		In	
□	1/0/7		In	

Private VLANs

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

There are three types of VLAN within a private VLAN:

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

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

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

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

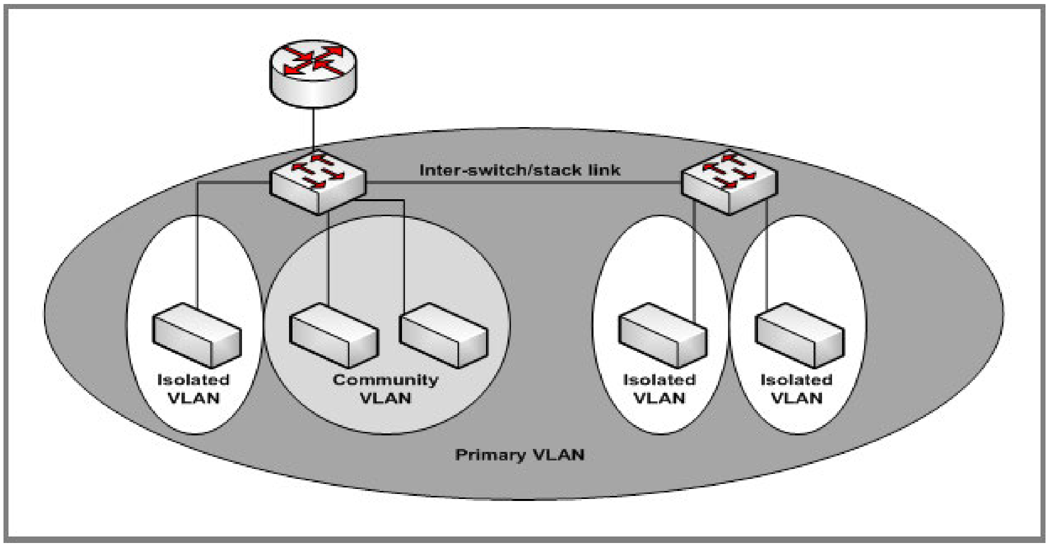


Figure 4. Private VLANs

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

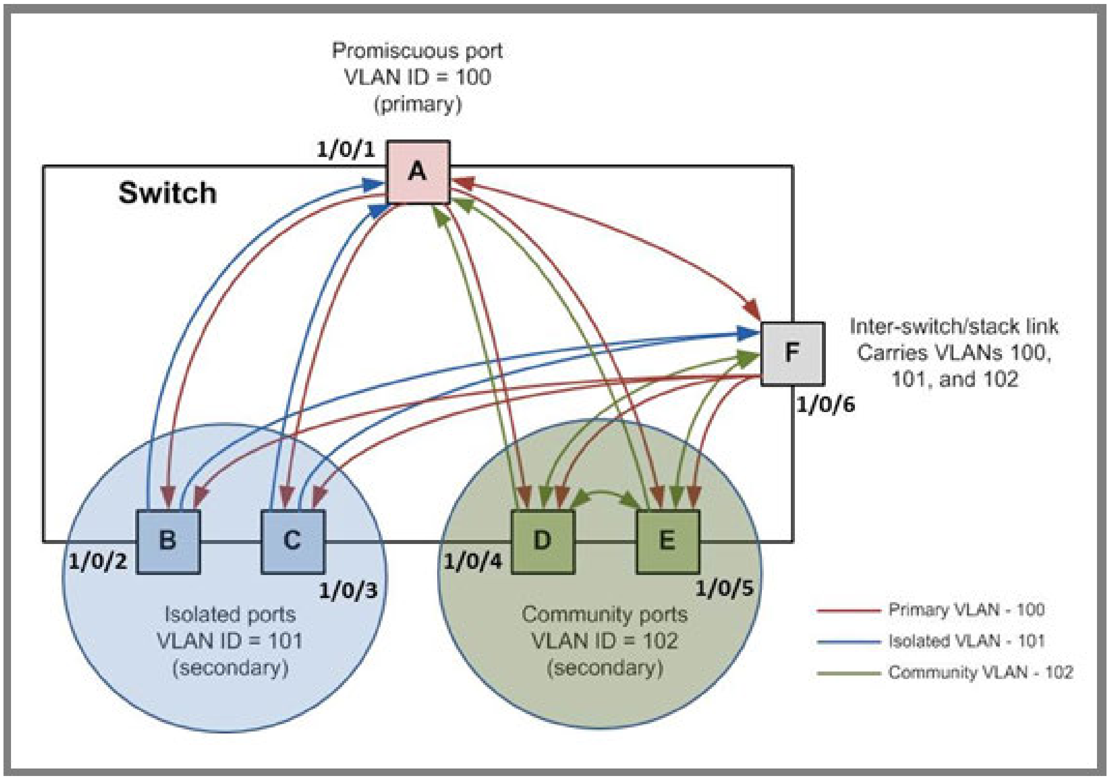


Figure 5. Packet flow within a Private VLAN domain

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

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

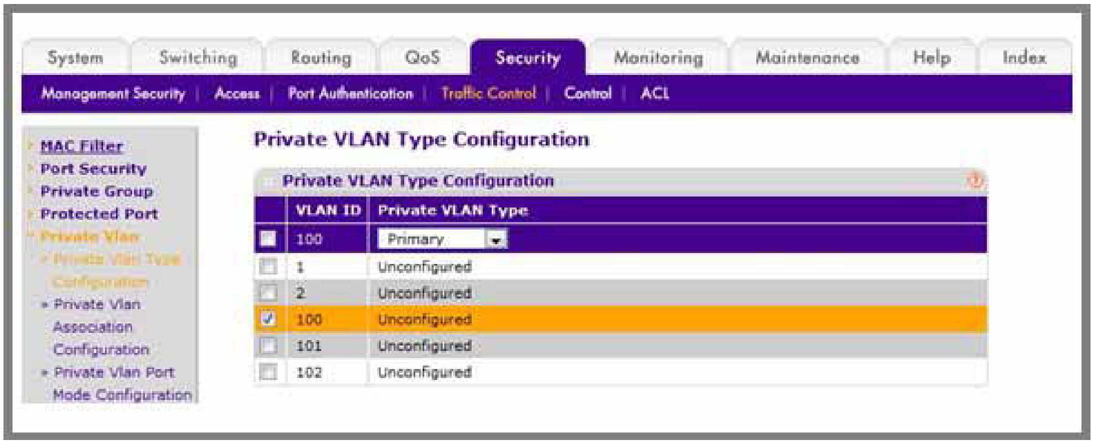
CLI: Assign Private-VLAN Type (Primary, Isolated, Community)

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

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

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

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



Private VLAN Type Configuration

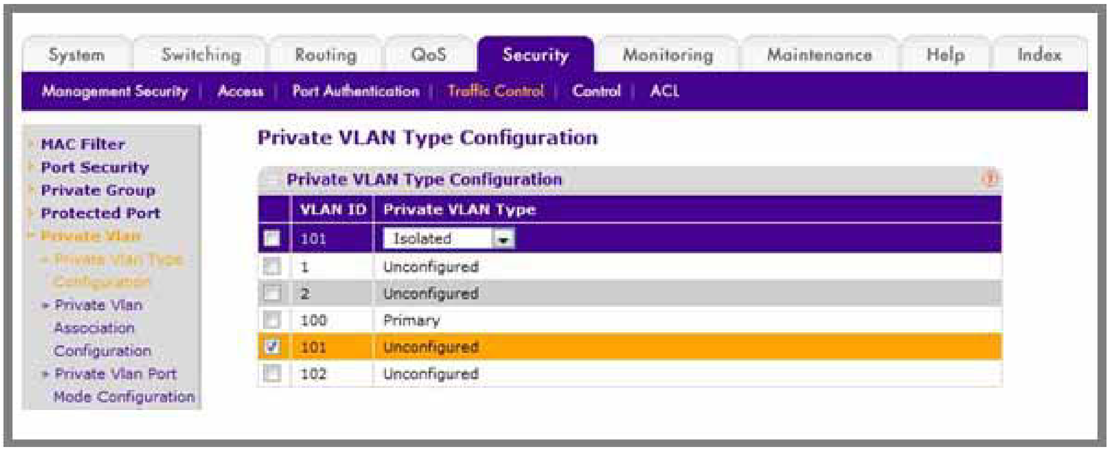
Private VLAN Type Configuration

	VLAN ID	Private VLAN Type
□	100	Primary
□	1	Unconfigured
□	2	Unconfigured
☑	100	Unconfigured
□	101	Unconfigured
□	102	Unconfigured

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

2. Assign VLAN 101 as an isolated VLAN.
   a. Select **Security** > **Traffic Control** > **Private VLAN** > **Private VLAN Type Configuration**.

   A screen similar to the following displays.



Private VLAN Type Configuration

Private VLAN Type Configuration

	VLAN ID	Private VLAN Type
□	101	Isolated
□	1	Unconfigured
□	2	Unconfigured
□	100	Primary
☑	101	Unconfigured
□	102	Unconfigured

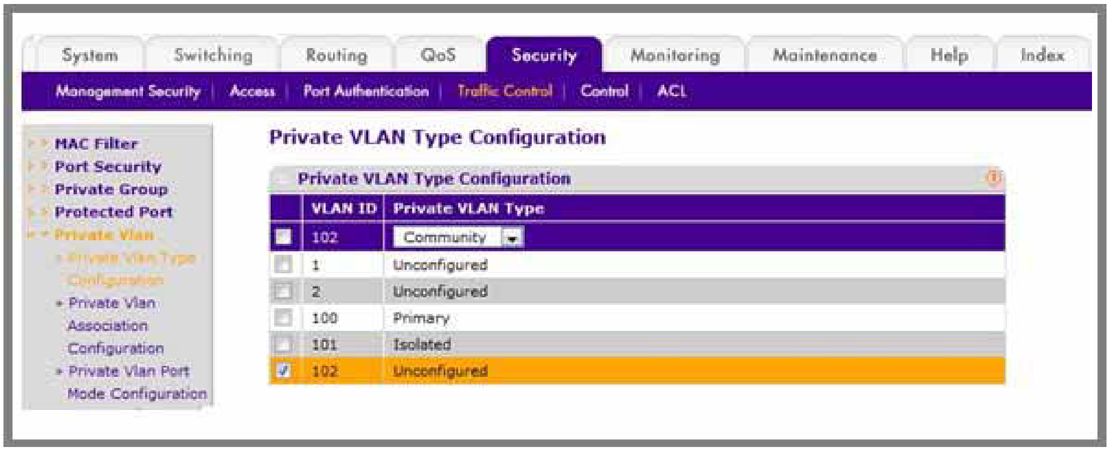
   b. Under **Private VLAN Type Configuration**, select the **VLAN ID 101** check box.

   Now 101 appears in the interface field at the top.

   c. In the **Private VLAN Type** field, select **Isolated** from the pull-down menu.
   d. Click **Apply** to save the settings

3. Assign VLAN 102 to community VLAN.
   a. Select **Security** > **Traffic Control** > **Private VLAN** > **Private VLAN Type Configuration**.

      A screen similar to the following displays.



Private VLAN Type Configuration

Private VLAN Type Configuration

	VLAN ID	Private VLAN Type
□	102	Community
□	1	Unconfigured
□	2	Unconfigured
□	100	Primary
□	101	Isolated
☑	102	Unconfigured

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

Configure Private-VLAN Association

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

CLI: Configure Private-VLAN Association

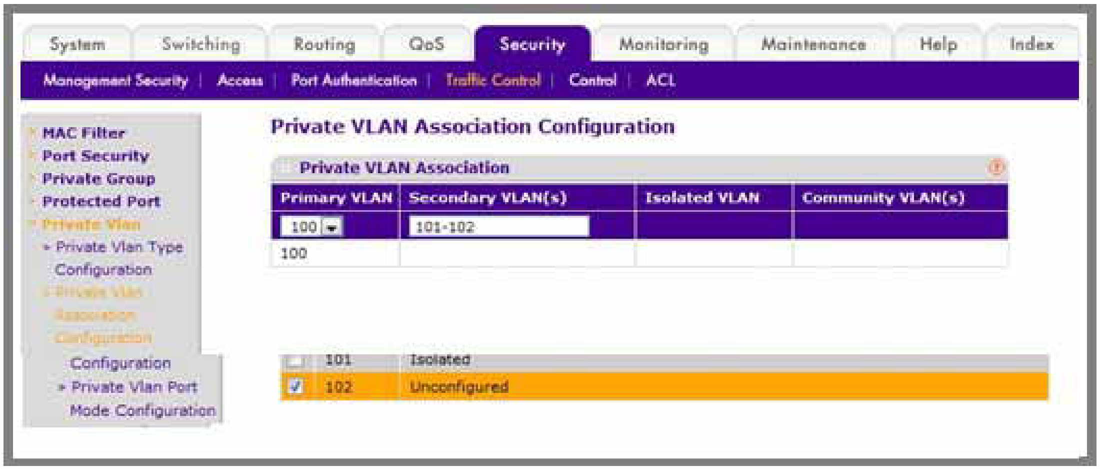
Use the following commands to associate VLAN 101-102 (secondary VLAN) to VLAN 100 (primary VLAN).

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

Web Interface: Configure Private-VLAN Association

1. Associate VLAN 101-102 (secondary VLAN) to VLAN 100 (primary VLAN).
   a. Select **Security** > **Traffic Control** > **Private VLAN** > **Private VLAN Association Configuration**.

A screen similar to the following displays.



Private VLAN Association Configuration

Private VLAN Association

Primary VLAN	Secondary VLAN(s)	Isolated VLAN	Community VLAN(s)
100	101-102		
100			

□	101	Isolated
☑	102	Unconfigured

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

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

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

Configure Private-VLAN Port Mode (Promiscuous, Host)

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

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

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

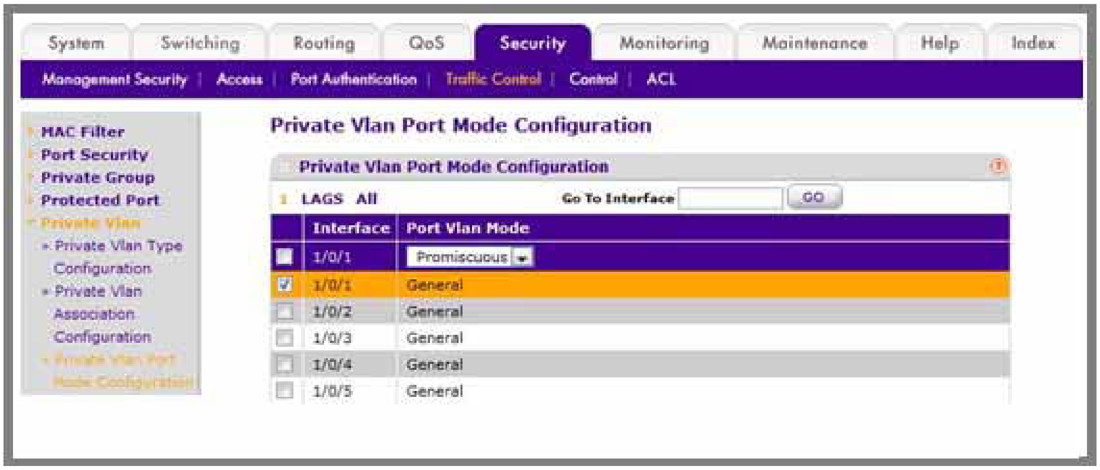
```
(Netgear Switch)  #config
(Netgear Switch)  (Config)#interface 1/0/1
(Netgear Switch)  (Interface 1/0/1)#switchport mode private-vlan promiscuous
(Netgear Switch)  (Interface 1/0/1)#exit
(Netgear Switch)  (Config)#interface 1/0/2-1/0/5
(Netgear Switch)  (Interface 1/0/2-1/0/5)#switchport mode private-vlan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

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

1. Configure port 1/0/1 to promiscuous port mode.

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

A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Management Security | Access | Port Authentication | Traffic Control | Control | ACL
MAC Filter
Port Security
Private Group
Protected Port
Private Vlan
» Private Vlan Type Configuration
» Private Vlan Association Configuration
» Private Vlan Port Mode Configuration
LAGS All
Go To Interface
GO

Private Vlan Port Mode Configuration

Private Vlan Port Mode Configuration

	Interface	Port Vlan Mode
□	1/0/1	Promiscuous
☑	1/0/1	General
□	1/0/2	General
□	1/0/3	General
□	1/0/4	General
□	1/0/5	General

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

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

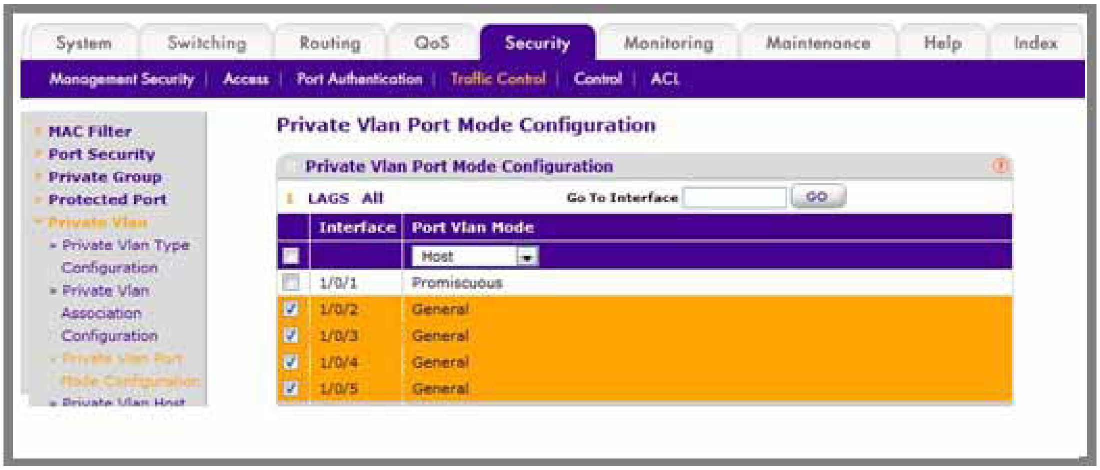
c. In the **Port VLAN Mode** field, select **Promiscuous** from the pull-down menu.

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

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

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

A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Management Security | Access | Port Authentication | Traffic Control | Control | ACL
MAC Filter
Port Security
Private Group
Protected Port
Private Vlan
» Private Vlan Type Configuration
» Private Vlan Association Configuration
» Private Vlan Port Mode Configuration
» Private Vlan Host
LAGS All
Go To Interface
GO

Private Vlan Port Mode Configuration

Private Vlan Port Mode Configuration

	Interface	Port Vlan Mode
□		Host
□	1/0/1	Promiscuous
☑	1/0/2	General
☑	1/0/3	General
☑	1/0/4	General
☑	1/0/5	General

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

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

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

Configure Private-VLAN Host Ports

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

CLI: Configure Private-VLAN Host Ports

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

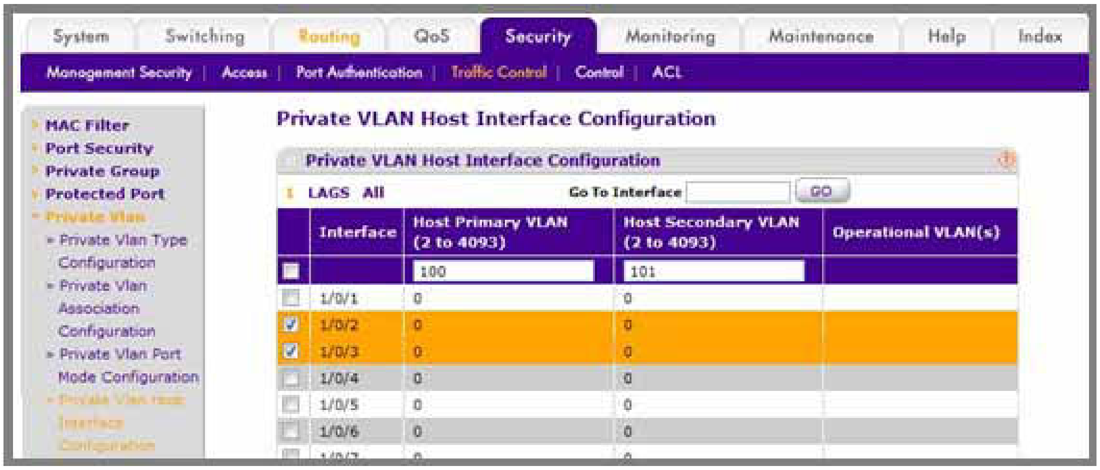
```
(Netgear Switch)  #config
(Netgear Switch)  (Config)#interface 1/0/2-1/0/3
(Netgear Switch)  (Interface 1/0/2-1/0/3)#switchport private-vlan host-association
100 101
(Netgear Switch)  (Interface 1/0/2-1/0/3)#exit
(Netgear Switch)  (Config)#interface 1/0/4-1/0/5
(Netgear Switch)  (Interface 1/0/4-1/0/5)#switchport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

Web Interface: Assign Private-VLAN Port Host Ports

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

   a. Select **Security** > **Traffic Control** > **Private VLAN** > **Private VLAN Host Interface Configuration**.

   A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Management Security | Access | Port Authentication | Traffic Control | Control | ACL
MAC Filter
Port Security
Private Group
Protected Port
Private Vlan
Private Vlan Type Configuration
Private Vlan Association Configuration
Private Vlan Port Mode Configuration
Private Vlan Host Interface Configuration
LAGS All
Go To Interface
GO

Private VLAN Host Interface Configuration

Private VLAN Host Interface Configuration

	Interface	Host Primary VLAN (2 to 4093)	Host Secondary VLAN (2 to 4093)	Operational VLAN(s)
□		100	101	
□	1/0/1	0	0	
☑	1/0/2	0	0	
☑	1/0/3	0	0	
□	1/0/4	0	0	
□	1/0/5	0	0	
□	1/0/6	0	0	
□	1/0/7	0	0	

   b. Under **Private VLAN Host Interface Configuration**, select the 1/0/2 and 1/0/3 interface check box.

   c. In the **Host Primary VLAN** field, enter 100.

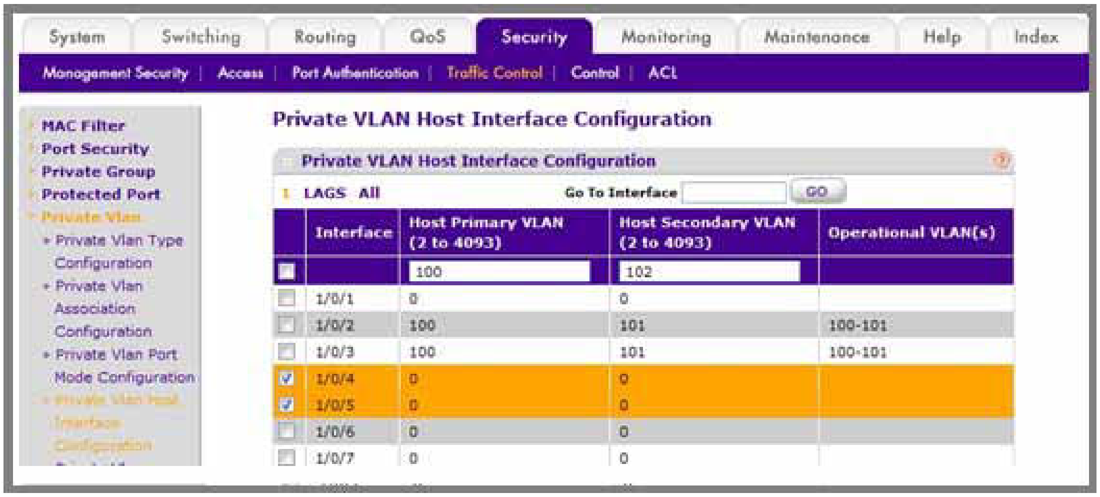
d. In the **Host Secondary VLAN** field, enter 101.

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

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

a. Select **Security** > **Traffic Control** > **Private VLAN** > **Private VLAN Host Interface Configuration**.

A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Management Security | Access | Port Authentication | Traffic Control | Control | ACL
MAC Filter
Port Security
Private Group
Protected Port
Private Vlan
» Private Vlan Type Configuration
» Private Vlan Association Configuration
» Private Vlan Port Mode Configuration
» Private Vlan Host Interface Configuration
1 LAGS All
Go To Interface
GO

Private VLAN Host Interface Configuration

Private VLAN Host Interface Configuration

	Interface	Host Primary VLAN (2 to 4093)	Host Secondary VLAN (2 to 4093)	Operational VLAN(s)
☐		100	102	
☐	1/0/1	0	0	
☐	1/0/2	100	101	100-101
☐	1/0/3	100	101	100-101
☑	1/0/4	0	0	
☑	1/0/5	0	0	
☐	1/0/6	0	0	
☐	1/0/7	0	0	

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

c. In the **Host Primary VLAN** field, enter 100.

d. In the **Host Secondary VLAN** field, enter 102.

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

Map Private-VLAN Promiscuous Port

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

CLI: Map Private-VLAN Promiscuous Port

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

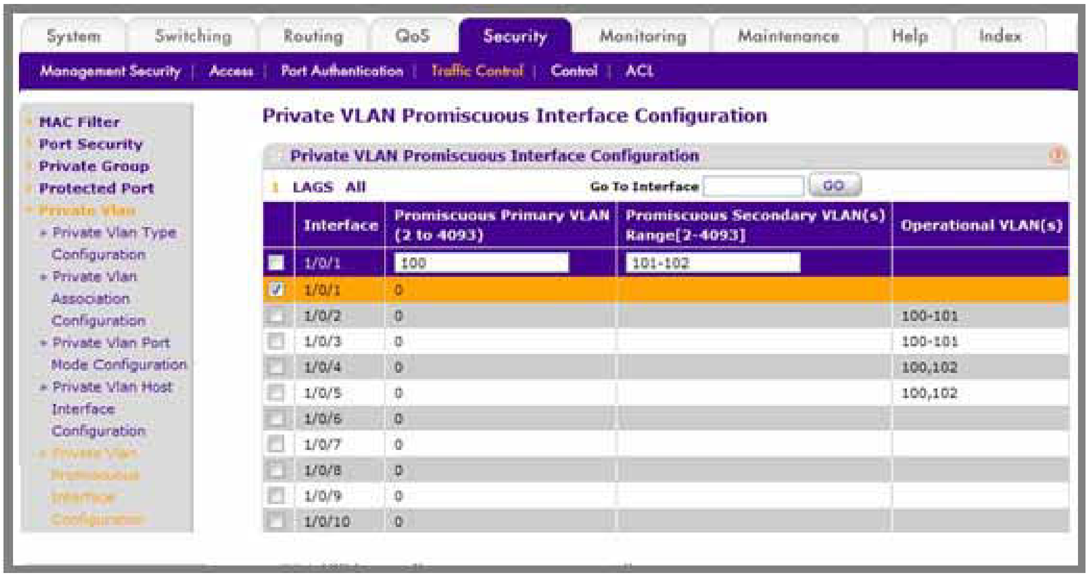
```
(Netgear Switch)  #config
(Netgear Switch)  (Config)#interface 1/0/1
(Netgear Switch)  (Interface 1/0/1)#switchport private-vlan mapping 100 101-102
(Netgear Switch)  (Interface 1/0/1)#end
```

Web Interface: Map Private-VLAN Promiscuous Port

1. Map private-VLAN promiscuous port 1/0/1 to a primary VLAN (100) and to selected secondary VLANs (101-102).

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

   A screen similar to the following displays.



Private VLAN Promiscuous Interface Configuration

Private VLAN Promiscuous Interface Configuration

1 LAGS All Go To Interface

	Interface	Promiscuous Primary VLAN (2 to 4093)	Promiscuous Secondary VLAN(s) Range[2-4093]	Operational VLAN(s)
□	1/0/1	100	101-102	
☑	1/0/1	0		
□	1/0/2	0		100-101
□	1/0/3	0		100-101
□	1/0/4	0		100,102
□	1/0/5	0		100,102
□	1/0/6	0		
□	1/0/7	0		
□	1/0/8	0		
□	1/0/9	0		
□	1/0/10	0		

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

   c. In the **Promiscuous Primary VLAN** field, enter 100.

   d. In the **Promiscuous Secondary VLAN** field, enter 101-102.

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

3. LAGs

Link Aggregation Groups

3

This chapter includes the following sections:

- *LAG Concepts*
- *Create Two LAGs*
- *Add Ports to LAGs*
- *Enable Both LAGs*

LAG Concepts

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

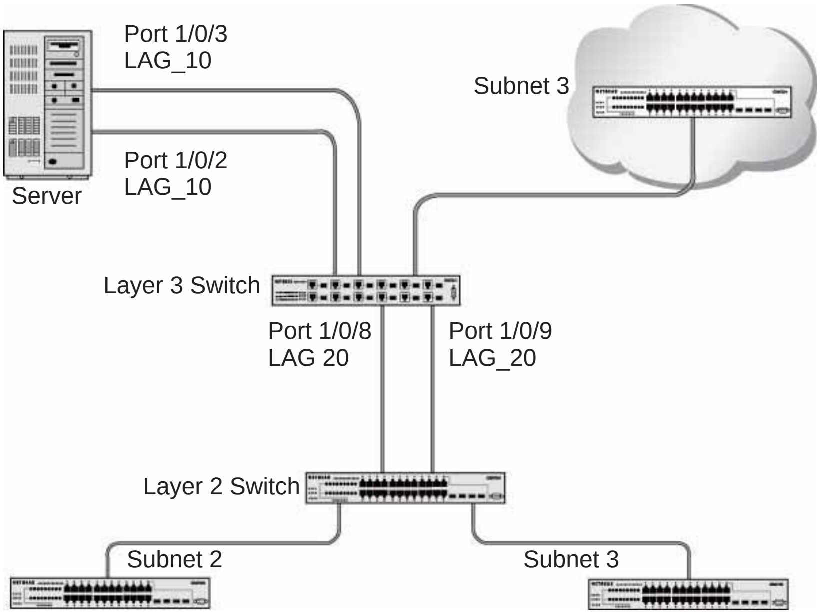


Figure 6. Example network with two LAGs

LAGs offer the following benefits:

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

Create Two LAGs

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

CLI: Create Two LAGs

```
(Netgear Switch) #config
(Netgear Switch) (Config)#port-channel name lag 1 lag_10
(Netgear Switch) (Config)#port-channel name lag 1 lag_20
(Netgear Switch) (Config)#exit
```

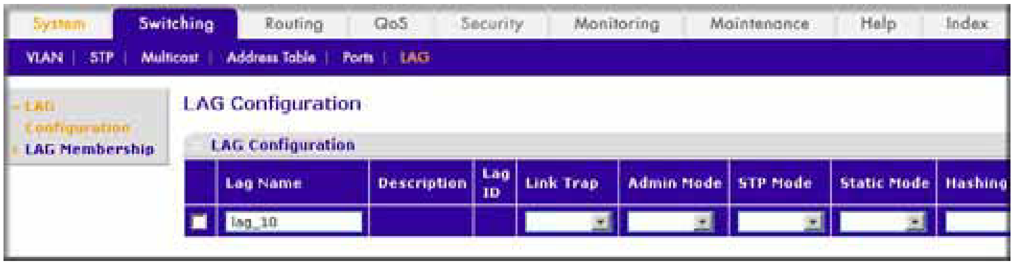
Use the show port-channel all command to show the logical interface IDs you will use to identify the LAGs in subsequent commands. Assume that lag_10 is assigned ID 1/1, and lag_20 is assigned ID 1/2.

```
(Console) #show port-channel all
            Port-                   Link
Log.       Channel            Adm. Trap  STP          Mbr      Port     Port
Intf        Name        Link  Mode Mode  Mode   Type   Ports    Speed    Active
------ -------------- ------ ---- ---- ------ ------- ------ --------- ------
1/1    lag_10         Down   En.  En.  Dis.   Dynamic
1/2    lag_20         Down   En.  En.  Dis.   Dynamic
```

Web Interface: Create Two LAGs

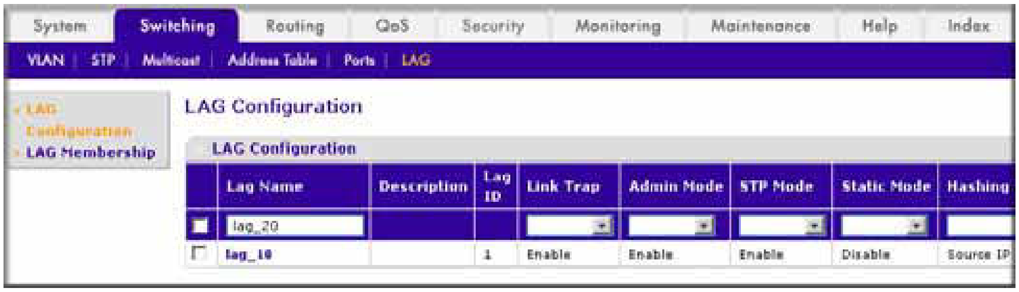
1. Create LAG lag_10.
   a. Select **Switching > LAG > LAG Configuration**.

      A screen similar to the following displays.



   b. In the **Lag Name** field, enter **lag_10**.
   c. Click **Add**.
2. Create LAG lag_20.

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



LAG Configuration

LAG Configuration

	Lag Name	Description	Lag ID	Link Trap	Admin Mode	STP Mode	Static Mode	Hashing
□	lag_20							
□	lag_10		1	Enable	Enable	Enable	Disable	Source IP

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

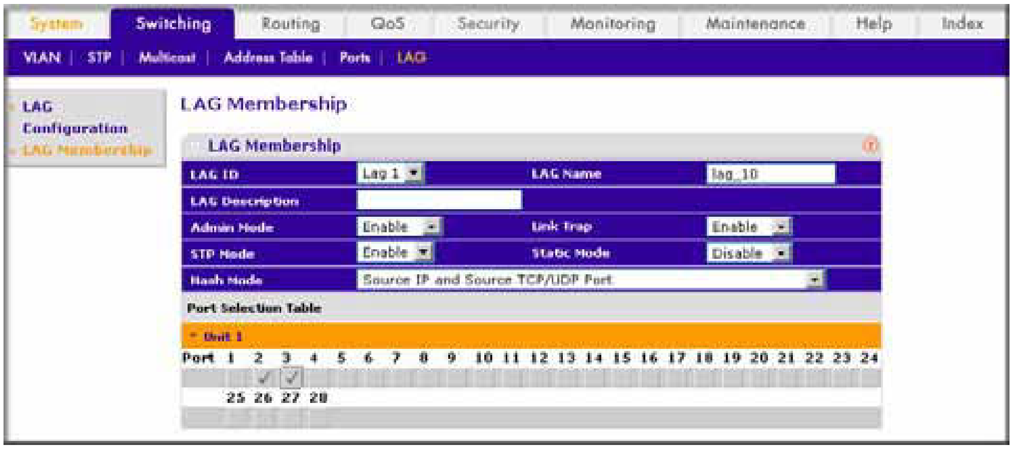
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 0/2
(Netgear Switch) (Interface 0/2)#addport 1/1
(Netgear Switch) (Interface 0/2)#exit
(Netgear Switch) (Config)#interface 0/3
(Netgear Switch) (Interface 0/3)#addport 1/1
(Netgear Switch) (Interface 0/3)#exit
(Netgear Switch) (Config)#interface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

LAG Membership

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

Port Selection Table

Unit 1

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

25	26	27	28

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**.

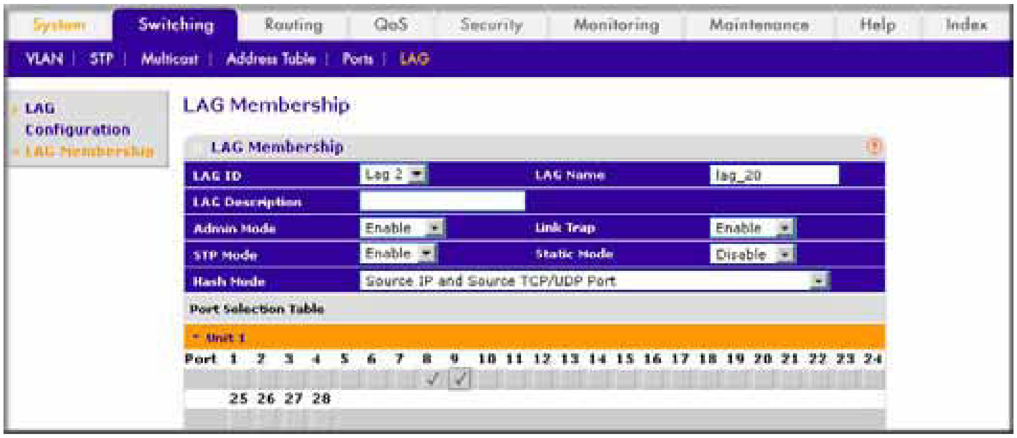
Two check marks display in the box.

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

LAG Membership

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

Port Selection Table

Unit 1

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

25	26	27	28

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

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

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

Two check marks display in the boxes.

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

Enable Both LAGs

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

CLI: Enable Both LAGs

By default, the system enables link trap notification.

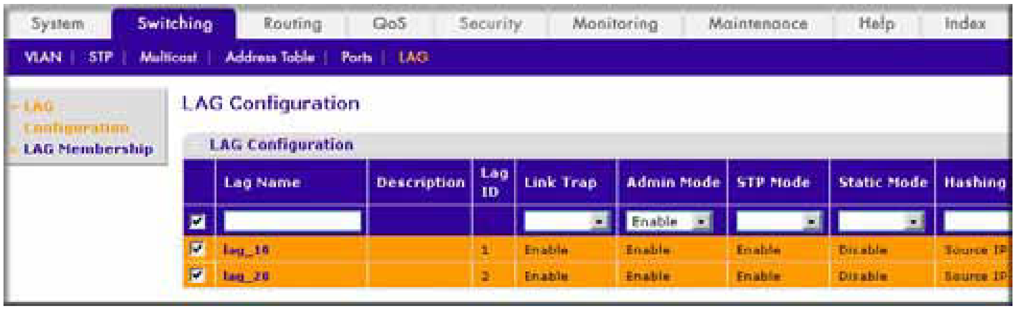
```
(Console) #config
(Console) (Config)#port-channel adminmode all
(Console) (Config)#exit
```

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

Web Interface: Enable Both LAGs

a. Select **Switching > LAG > LAG Configuration**.

A screen similar to the following displays.



LAG Configuration

LAG Configuration

	Lag Name	Description	Lag ID	Link Trap	Admin Mode	STP Mode	Static Mode	Hashing
☑					Enable			
☑	lag_10		1	Enable	Enable	Enable	Disable	Source IP
☑	lag_20		2	Enable	Enable	Enable	Disable	Source IP

b. Select the top check box and the check boxes for **lag_10** and **lag_20** are selected.

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

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

4 Port Routing

Port routing, default routes, and static routes

This chapter includes the following sections:

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

Port Routing Concepts

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

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

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

The router's IP address is often statically configured in the end station, although the M4100 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 M4100 Managed Switch always supports Layer 2 bridging, but Layer 3 routing must be explicitly enabled, first for the M4100 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 M4100 Managed Switch's management IP address, or to that of any active router interface if the management address is not configured.

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

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

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

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

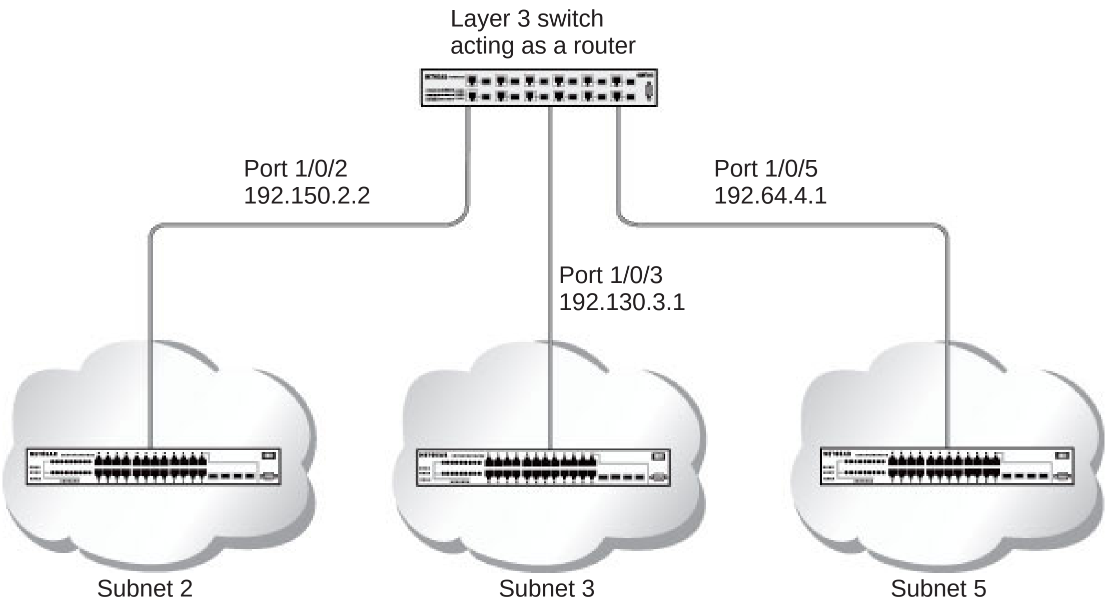


Figure 7. Layer 3 switch configured for port routing

Enable Routing for the Switch

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

CLI: Enable Routing for the Switch

The following script shows the commands that you would use to configure a M4100 Managed Switch to provide the port routing support shown in *Figure 7, Layer 3 switch configured for port routing* on page 59.

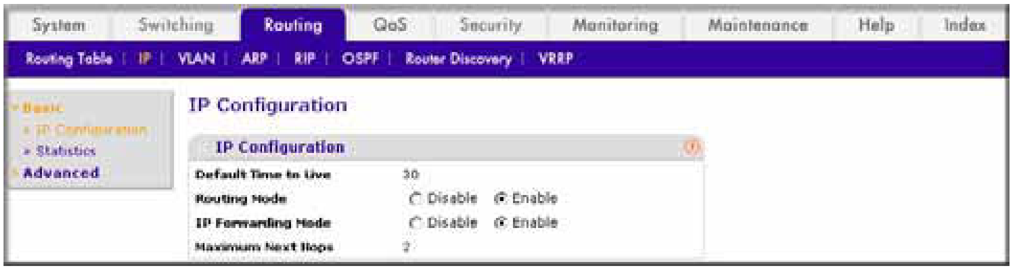
Use the following command to enable routing for the switch. Execution of the command enables IP forwarding by default.

```
(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.



IP Configuration

IP Configuration

Default Time to Live	30
Routing Mode	○ Disable ● Enable
IP Forwarding Mode	○ Disable ● Enable
Maximum Next Hops	2

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

Enable Routing for Ports on the Switch

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

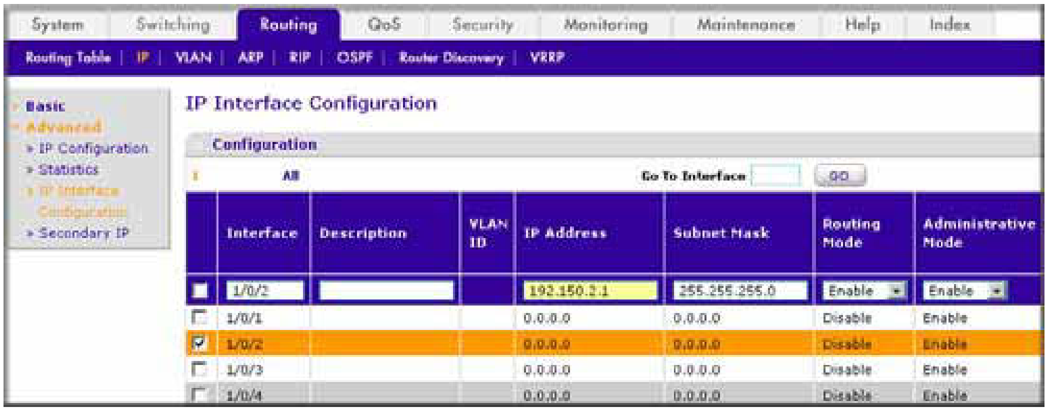
CLI: Enable Routing for Ports on the Switch

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

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

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

Web Interface: Enable Routing for Ports on the Switch

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

      A screen similar to the following displays.



	Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
□	1/0/2			192.150.2.1	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable
☑	1/0/2			0.0.0.0	0.0.0.0	Disable	Enable
□	1/0/3			0.0.0.0	0.0.0.0	Disable	Enable
□	1/0/4			0.0.0.0	0.0.0.0	Disable	Enable

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

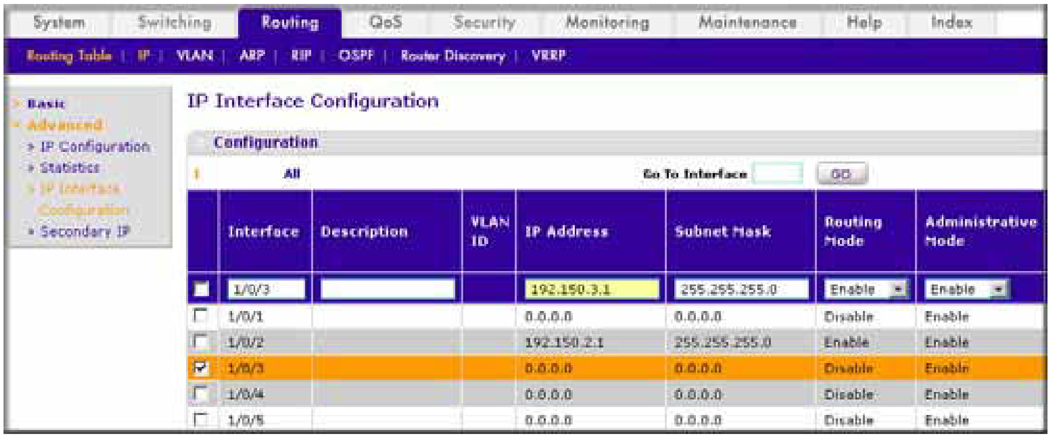
      Now 1/0/2 appears in the Interface field at the top.

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

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

2. Assign IP address 192.150.3.1/24 to interface 1/0/3.
   a. Select **Routing > IP> Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



	Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
□	1/0/3			192.150.3.1	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable
□	1/0/2			192.150.2.1	255.255.255.0	Enable	Enable
☑	1/0/3			0.0.0.0	0.0.0.0	Disable	Enable
□	1/0/4			0.0.0.0	0.0.0.0	Disable	Enable
□	1/0/5			0.0.0.0	0.0.0.0	Disable	Enable

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

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

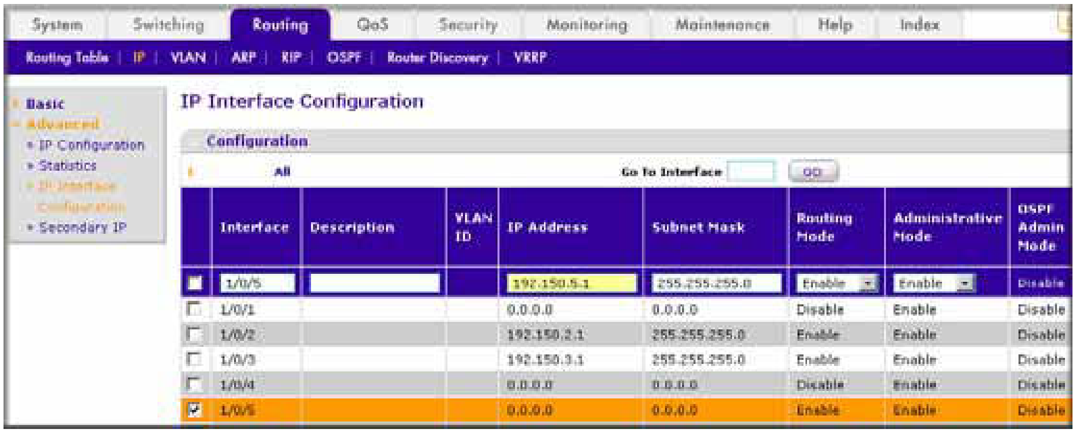
c. Enter the following information:
   - In the **IP Address** field, enter **192.150.3.1**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Routing Mode** field, select **Enable**.

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

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.



IP Interface Configuration

Configuration

All   Go To Interface

	Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode	OSPF Admin Mode
□	1/0/5			192.150.5.1	255.255.255.0	Enable	Enable	Disable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable	Disable
□	1/0/2			192.150.2.1	255.255.255.0	Enable	Enable	Disable
□	1/0/3			192.150.3.1	255.255.255.0	Enable	Enable	Disable
□	1/0/4			0.0.0.0	0.0.0.0	Disable	Enable	Disable
☑	1/0/5			0.0.0.0	0.0.0.0	Enable	Enable	Disable

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

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

c. Enter the following information:
   - In the **IP Address** field, enter **192.150.5.1**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Routing Mode** field, select **Enable**.

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

Add a Default Route

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

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

CLI: Add a Default Route

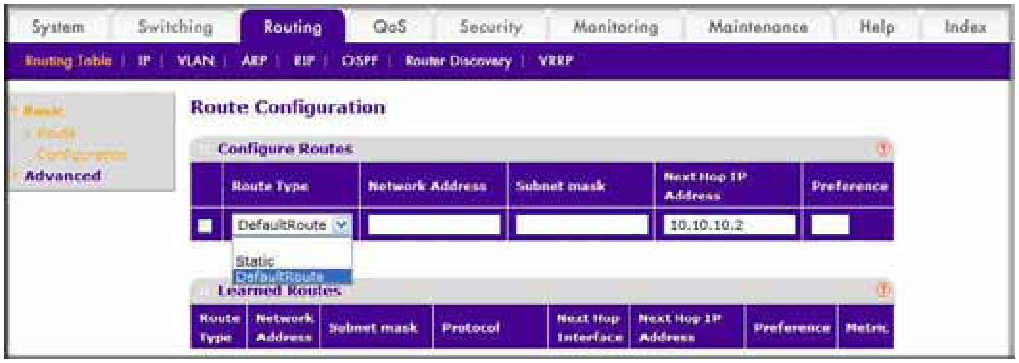
```
(FSM7338S) (Config) #ip route default?
<nexthopip> Enter the IP Address of the next router.
(FSM7328S) (Config)#ip route default 10.10.10.2
```

Note: IP subnet 10.10.10.0 should be configured using either port routing (see *Enable Routing for Ports on the Switch* on page 60) or VLAN routing (see *Set Up VLAN Routing for the VLANs and the Switch* on page 72).

Web Interface: Add a Default Route

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

   The Route Configuration screen displays.



Route Configuration

Configure Routes

	Route Type	Network Address	Subnet mask	Next Hop IP Address	Preference
□	DefaultRoute			10.10.10.2	

Learned Routes

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

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

   This creates the default route entry in the routing table.

Add a Static Route

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

CLI: Add a Static Route

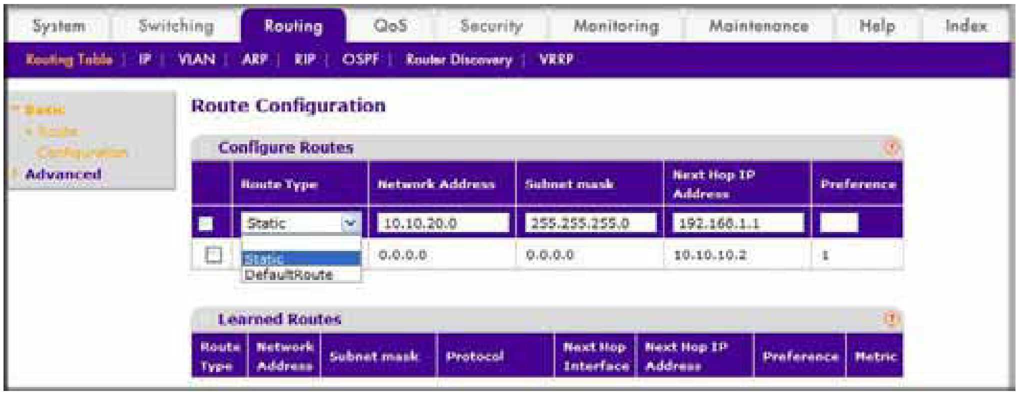
The following commands assume that the switch already has a defined a routing interface with a network address of 10.10.10.0, and is configured so that all packets destined for network 10.10.100.0 take the path of routing port.

```
(FSM7328S) #show ip route

Total 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.



Route Configuration

Configure Routes

	Route Type	Network Address	Subnet mask	Next Hop IP Address	Preference
□	Static	10.10.20.0	255.255.255.0	192.168.1.1	
□		0.0.0.0	0.0.0.0	10.10.10.2	1

Learned Routes

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

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

   Note that this field should have a network IP address, not a host IP address. Do not enter something like *10,100.100.1*. The last number should always be 0 (zero).

4. In the **Subnet Mask** field, enter a value that matches the subnet range that you want to use.
5. The **Preference** field is optional. A value of 1 is entered by default if you do not enter a number.
6. Click the **Add** button on the bottom of the screen. The screen is updated with the static route shown in the routing table.
7. To remove a route entry, either static or default, select the check box to the left of the entry, and click the **Delete** button on the bottom of the screen.

5. VLAN Routing

5

VLAN routing for a VLAN and for the switch

This chapter includes the following sections:

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

VLAN Routing Concepts

You can configure the ProSAFE M4100 Managed Switches with some ports supporting VLANs and some supporting routing. You can also configure it to allow traffic on a VLAN to be treated as if the VLAN were a router port.

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

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

The next section shows you how to configure the ProSAFE M4100 Managed Switches 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 M4100 Managed Switch to support VLAN routing. The configuration of the VLAN router port is similar to that of a physical port. The main difference is that, after the VLAN has been created, you must use the *show ip vlan* command to determine the VLAN’s interface ID so that you can use it in the router configuration commands.

The diagram in this section shows a Layer 3 switch configured for port routing. It connects two VLANs, with two ports participating in one VLAN, and one port in the other. The script shows the commands that you would use to configure a M4100 Managed Switch to provide the VLAN routing support shown in the diagram.

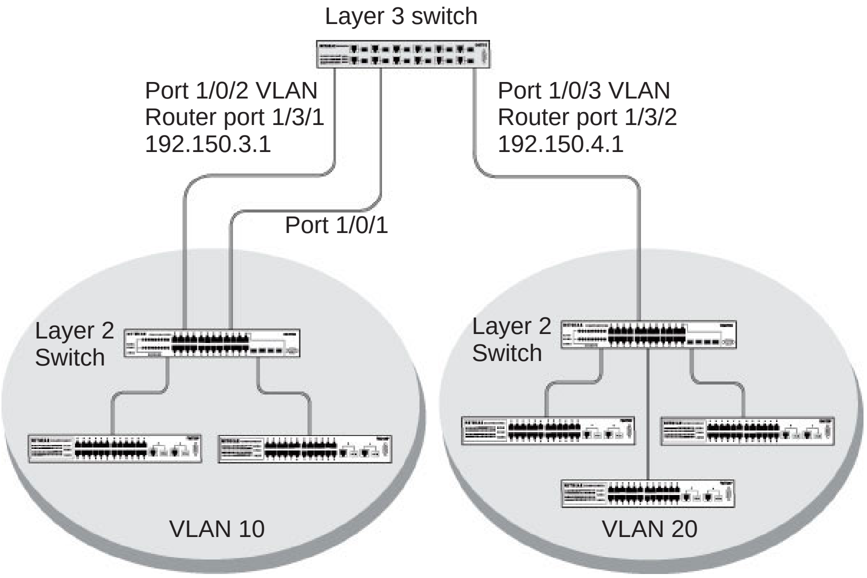


Figure 8. Layer 3 switch configured for port routing

CLI: Create Two VLANs

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

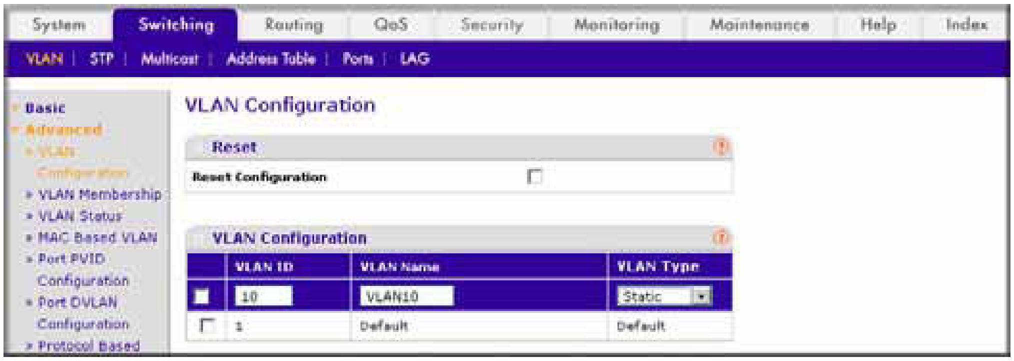
```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 10
(Netgear Switch) (Vlan)#vlan 20
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #conf
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan participation include 10
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan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

Web Interface: Create Two VLANs

1. Create VLAN 10 and VLAN20.

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

   A screen similar to the following displays.



VLAN Configuration

Reset

Reset Configuration □

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type
☑	10	VLAN10	Static
□	1	Default	Default

   b. In the **VLAN ID** field, enter **10**.

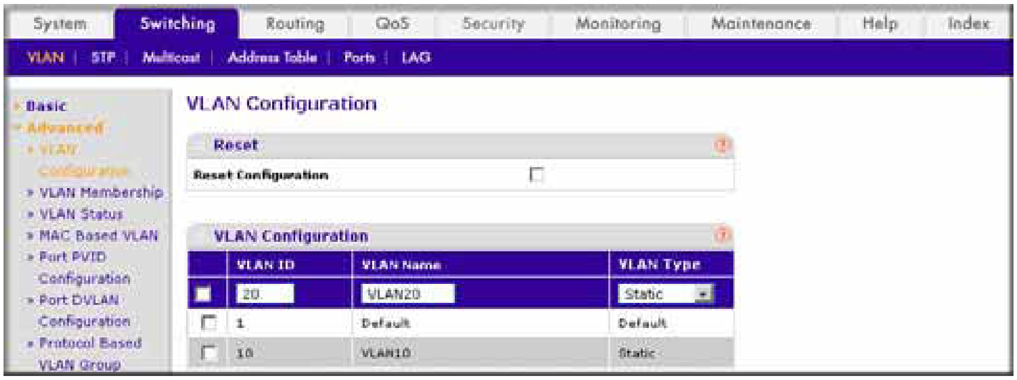
   c. In the **VLAN Name** field, enter **VLAN10**.

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

   e. Click **Add**.

   f. Select **Switching > VLAN > Advanced > VLAN Configuration**.

   A screen similar to the following displays.



VLAN Configuration

Reset

Reset Configuration □

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type
☑	20	VLAN20	Static
□	1	Default	Default
□	10	VLAN10	Static

   g. In the **VLAN ID** field, enter **20**.

   h. In the **VLAN Name** field, enter **VLAN20**.

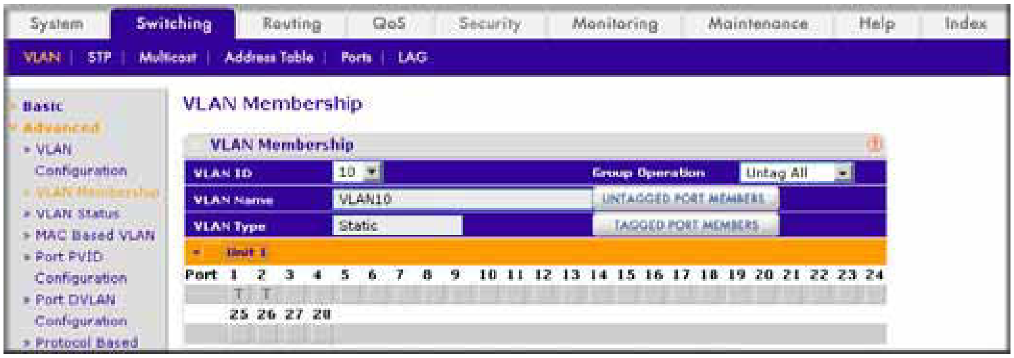
   i. In the **VLAN Type** list, select **Static**.

   j. Click **Add**.

2. Add ports to the VLAN10 and VLAN20.

   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

A screen similar to the following displays.



VLAN Membership

VLAN Membership

VLAN ID: 10

Group Operation: Untag All

VLAN Name: VLAN10

VLAN Type: Static

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	T	T																						
	25	26	27	28																				

b. In the **VLAN ID** field, select **10**.

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

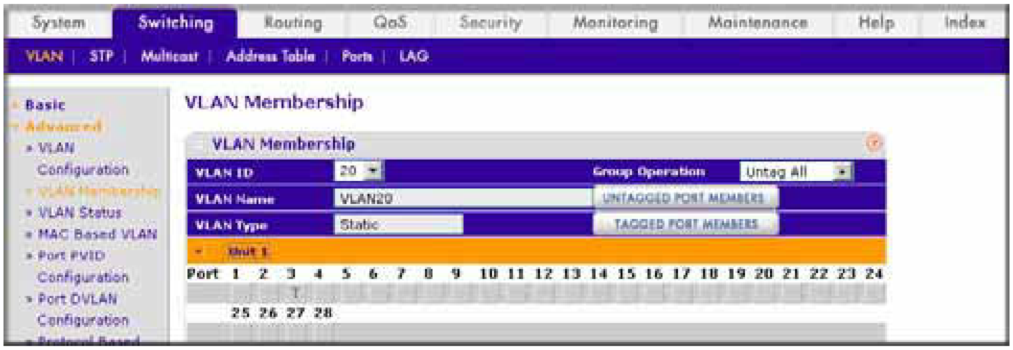
d. Click the gray boxes under ports **1** and **2** until **T** displays.

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

VLAN Membership

VLAN ID: 20

Group Operation: Untag All

VLAN Name: VLAN20

VLAN Type: Static

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
			T																					
	25	26	27	28																				

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.

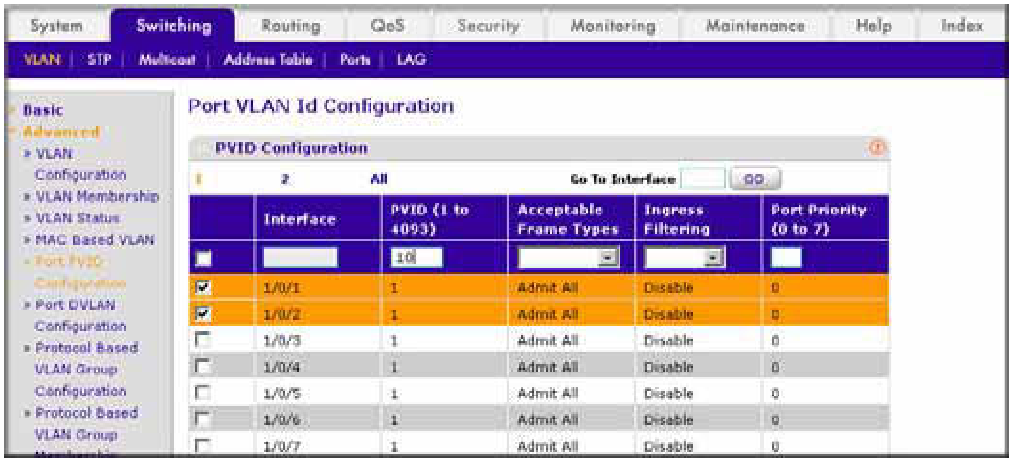
The T specifies that the egress packet is tagged for the port.

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.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
VLAN | STP | Multicast | Address Table | Ports | LAG
Basic
Advanced
» VLAN Configuration
» VLAN Membership
» VLAN Status
» MAC Based VLAN
» Port PVID Configuration
» Port DVLAN Configuration
» Protocol Based VLAN Group Configuration
» Protocol Based VLAN Group Membership
1
2
All
Go To Interface
GO

Port VLAN Id Configuration

PVID Configuration

	Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)
□		10			
☑	1/0/1	1	Admit All	Disable	0
☑	1/0/2	1	Admit All	Disable	0
□	1/0/3	1	Admit All	Disable	0
□	1/0/4	1	Admit All	Disable	0
□	1/0/5	1	Admit All	Disable	0
□	1/0/6	1	Admit All	Disable	0
□	1/0/7	1	Admit All	Disable	0

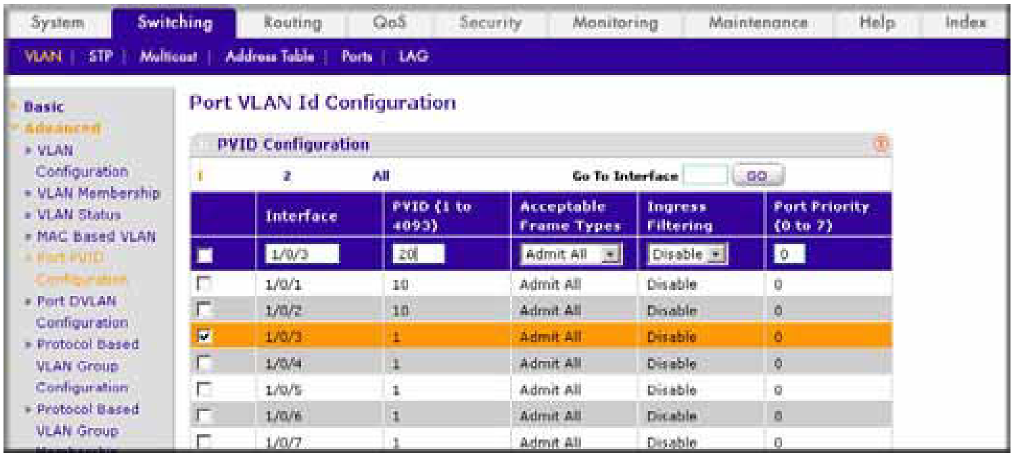
b. Scroll down and select **1/0/1 and 1/0/2 check boxes**.

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

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

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

A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
VLAN | STP | Multicast | Address Table | Ports | LAG
Basic
Advanced
» VLAN Configuration
» VLAN Membership
» VLAN Status
» MAC Based VLAN
» Port PVID Configuration
» Port DVLAN Configuration
» Protocol Based VLAN Group Configuration
» Protocol Based VLAN Group Membership
1
2
All
Go To Interface
GO

Port VLAN Id Configuration

PVID Configuration

	Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)
□	1/0/3	20	Admit All	Disable	0
□	1/0/1	10	Admit All	Disable	0
□	1/0/2	10	Admit All	Disable	0
☑	1/0/3	1	Admit All	Disable	0
□	1/0/4	1	Admit All	Disable	0
□	1/0/5	1	Admit All	Disable	0
□	1/0/6	1	Admit All	Disable	0
□	1/0/7	1	Admit All	Disable	0

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

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

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

Set Up VLAN Routing for the VLANs and the Switch

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

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

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

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

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

2. Enable routing for the switch.

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

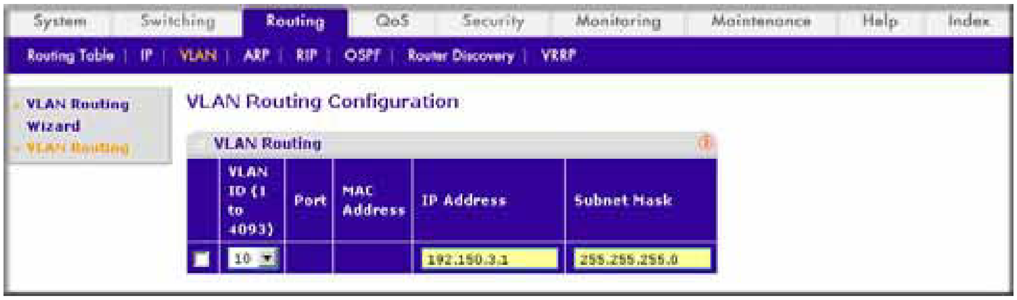
3. The next sequence shows an example of configuring the IP addresses and subnet masks for the virtual router ports.

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

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

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

   A screen similar to the following displays.

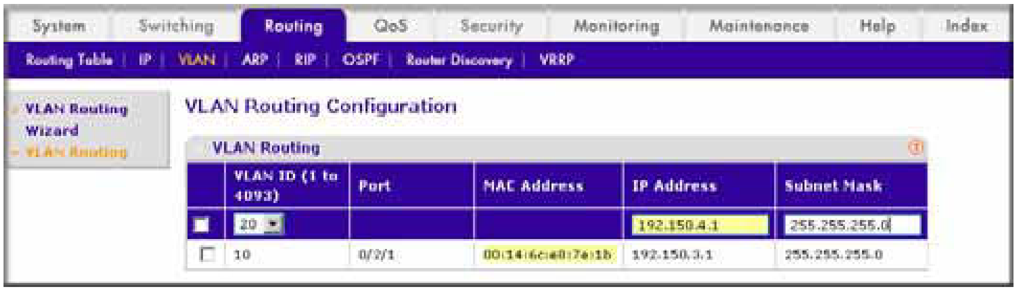


VLAN Routing Configuration

VLAN Routing

	VLAN ID (1 to 4093)	Port	MAC Address	IP Address	Subnet Mask
□	10			192.150.3.1	255.255.255.0

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



VLAN Routing Configuration

VLAN Routing

	VLAN ID (1 to 4093)	Port	MAC Address	IP Address	Subnet Mask
□	20			192.150.4.1	255.255.255.0
□	10	0/2/1	00:14:6c:e0:7e:1b	192.150.3.1	255.255.255.0

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

6. Proxy ARP

Proxy Address Resolution Protocol

6

This chapter includes the following sections:

- *Proxy ARP Concepts*
- *Proxy ARP Examples*

Proxy ARP Concepts

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

Proxy ARP Examples

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

CLI: show ip interface

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

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

(Netgear Switch) #show ip interface 0/24

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

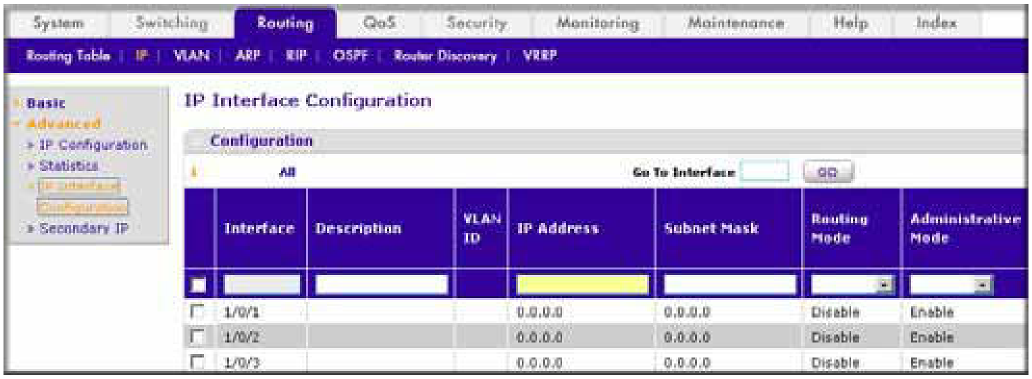
CLI: ip proxy-arp

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

<cr>                     Press Enter to execute the command.

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

Web Interface: Configure Proxy ARP on a Port

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

   A screen similar to the following displays.



IP Interface Configuration

Configuration

All

	Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable
□	1/0/2			0.0.0.0	0.0.0.0	Disable	Enable
□	1/0/3			0.0.0.0	0.0.0.0	Disable	Enable

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

ACLs

7

Access Control Lists

This chapter includes the following sections:

ACL Concepts

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

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

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

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

MAC ACLs

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

- Source MAC address with mask.
- Destination MAC address with mask.
- VLAN ID (or range of IDs).
- Class of Service (CoS) (802.1p).
- EtherType:
    - Secondary CoS (802.1p).
    - Secondary VLAN (or range of IDs).
- L2 ACLs can apply to one or more interfaces.
- Multiple access lists can be applied to a single interface: the sequence number determines the order of execution.
- You 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 M4100 Managed Switch only if the source and destination stations have IP addresses within the defined sets.

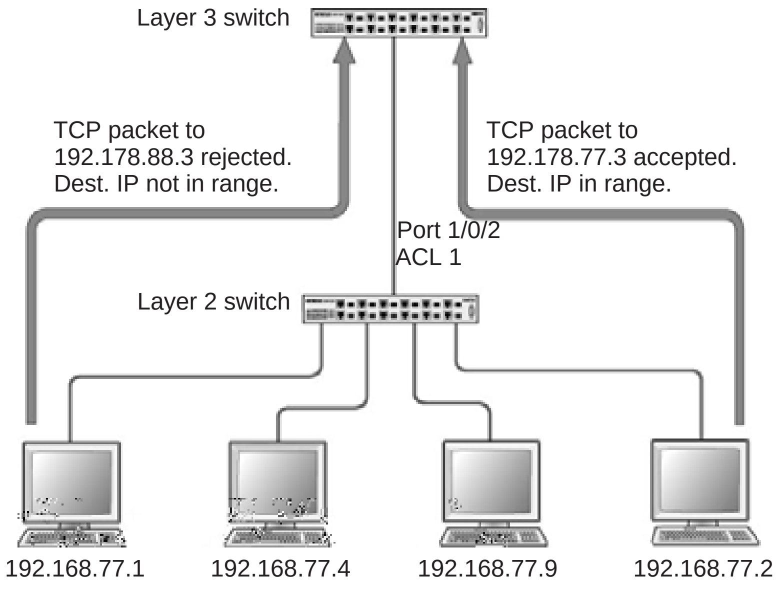


Figure 9. IP ACL with rules for TCP traffic and UDP traffic

CLI: Set Up an IP ACL with Two Rules

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

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

1. Enter these commands:

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

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

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

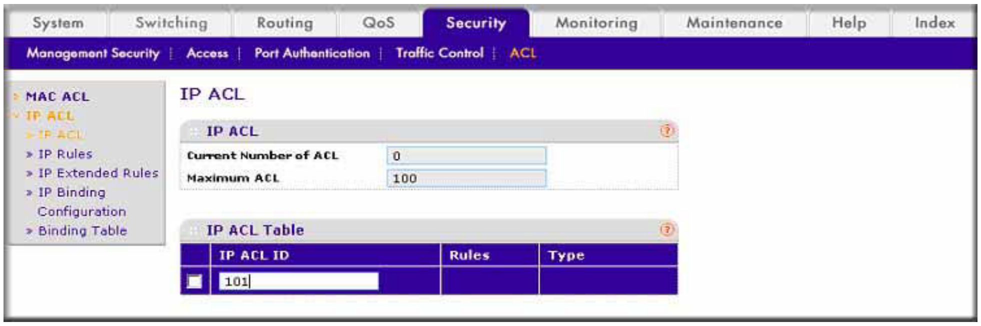
3. Apply the rule to inbound traffic on port 1/0/2. Only traffic matching the criteria will be accepted.

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

Web Interface: Set Up an IP ACL with Two Rules

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

      A screen similar to the following displays.



IP ACL

IP ACL

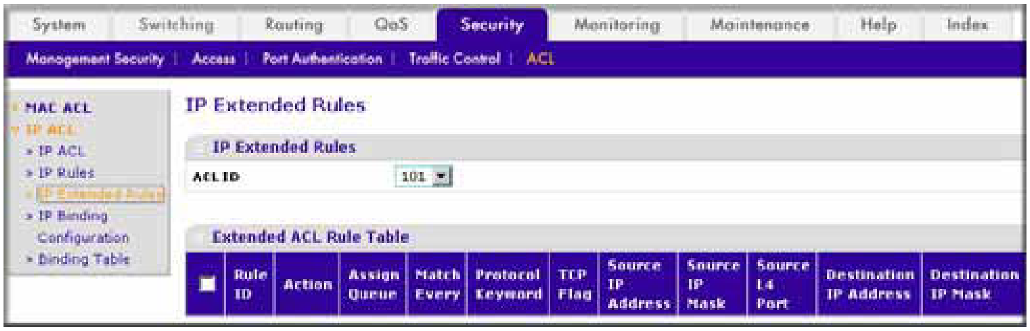
Current Number of ACL	0
Maximum ACL	100

IP ACL Table

	IP ACL ID	Rules	Type
□	101		

   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

IP Extended Rules

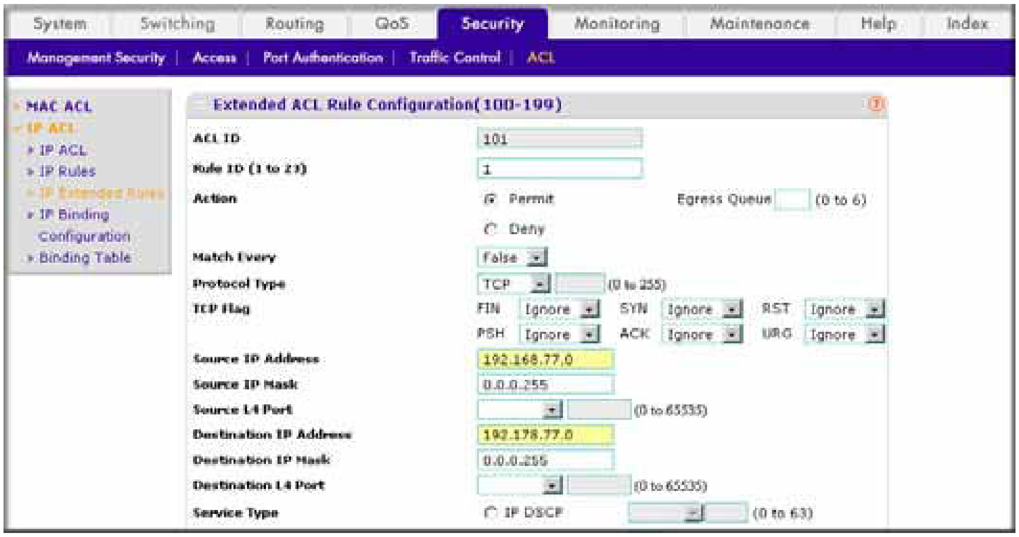
ACL ID	101

Extended ACL Rule Table

□	Rule ID	Action	Assign Queue	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source IP Mask	Source L4 Port	Destination IP Address	Destination IP Mask

   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(100-199)

ACL ID 101

Rule ID (1 to 23) 1

Action ● Permit ○ Deny Egress Queue (0 to 6)

Match Every False

Protocol Type TCP (0 to 255)

TCP Flag FIN Ignore SYN Ignore RST Ignore PSH Ignore ACK Ignore URG Ignore

Source IP Address 192.168.77.0

Source IP Mask 0.0.0.255

Source L4 Port (0 to 65535)

Destination IP Address 192.178.77.0

Destination IP Mask 0.0.0.255

Destination L4 Port (0 to 65535)

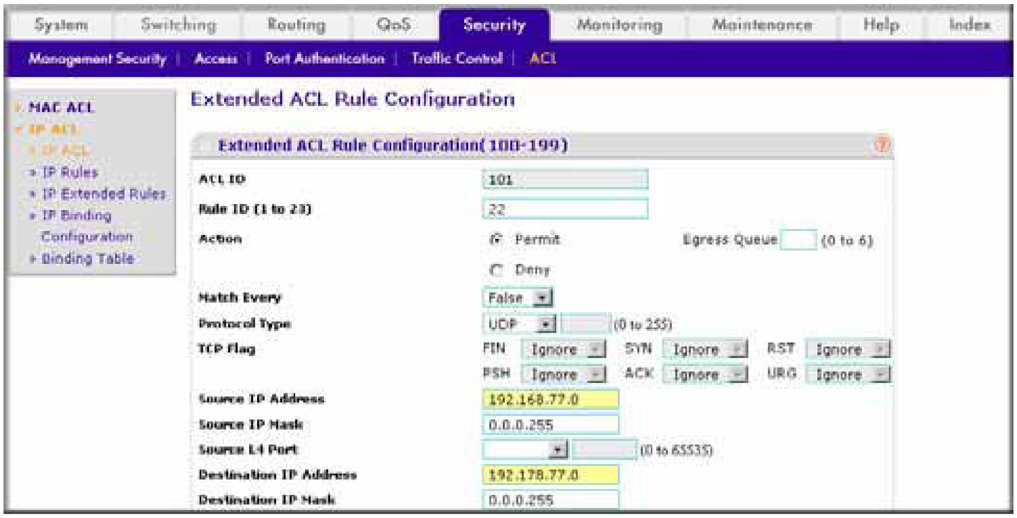
Service Type ○ IP DSCP (0 to 63)

a. In the Extended ACL Rule Configuration, enter the following information:
   - In the **Rule ID (1 to 23)** field, enter **1**.
   - For Action, select the **Permit** radio button.
   - In the **Protocol Type** list, select **TCP**.
   - In the **Source IP Address** field, enter **192.168.77.0**.
   - In the **Source IP Mask** field, enter **0.0.0.255**.
   - In the **Destination IP Address** field, enter **192.178.77.0**.
   - In the **Destination IP Mask** field, enter **0.0.0.255**.

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

4. Create another ACL rule and add it to the ACL 101.

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



Extended ACL Rule Configuration

Extended ACL Rule Configuration(100-199)

ACL ID 101

Rule ID (1 to 23) 22

Action ● Permit ○ Deny Egress Queue (0 to 6)

Match Every False

Protocol Type UDP (0 to 255)

TCP Flag FIN Ignore SYN Ignore RST Ignore PSH Ignore ACK Ignore URG Ignore

Source IP Address 192.168.77.0

Source IP Mask 0.0.0.255

Source L4 Port (0 to 65535)

Destination IP Address 192.178.77.0

Destination IP Mask 0.0.0.255

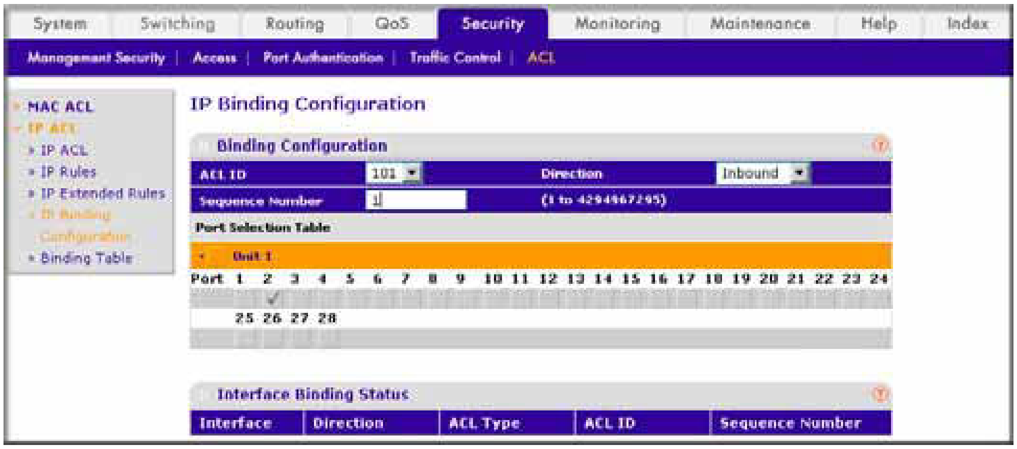
b. Under Extended ACL Rule Configuration, enter the following information:
   - In the **Rule ID (1 to 23)** field, enter **22**.
   - For Action, select the **Permit** radio button.
   - In the **Protocol Type** list, select **UDP**.
   - In the **Source IP Address** field, enter **192.168.77.0**.
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

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

5. Apply ACL 101 to port 2.

a. Select **Security > ACL > IP ACL > IP Binding Configuration**.

A screen similar to the following displays.



IP Binding Configuration

Binding Configuration

ACL ID	101	Direction	Inbound
Sequence Number	1	(1 to 4294967295)	

Port Selection Table

Unit 1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
		✓																						
	25	26	27	28																				

Interface Binding Status

Interface	Direction	ACL Type	ACL ID	Sequence Number

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.

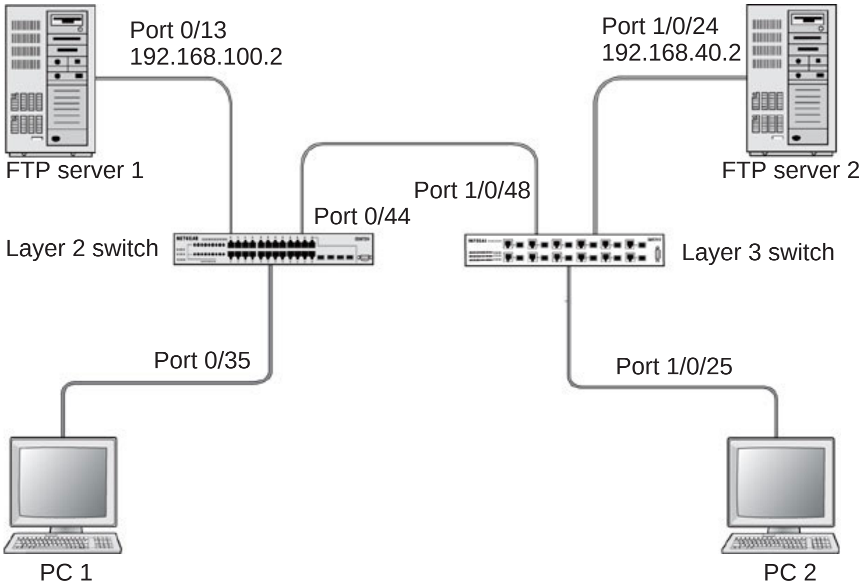


Figure 10. One-Way Web access using a TCP flag in an ACL

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

This configuration consists of two step:

- *Step 1: Configure the Switch* on page 85
- *Step 2: Configure the GSM7352S* on page 86

Step 1: Configure the Switch

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

1. Enter the following commands.

```
(Netgear Switch) (Config)#interface 0/44
(Netgear Switch) (Interface 0/44)#ip access-group 101 in 1
(Netgear Switch) (Interface 0/44)#ip access-group 102 in 2
(Netgear Switch) (Interface 0/44)#exit
```

2. Create VLAN 40 with port 1/0/24 and assign IP address 192.168.40.1/24.

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

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

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

4. Create VLAN 200 with port 1/0/48 and assign IP address 192.168.200.1/24.

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

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

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

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

This configuration consists of two steps:

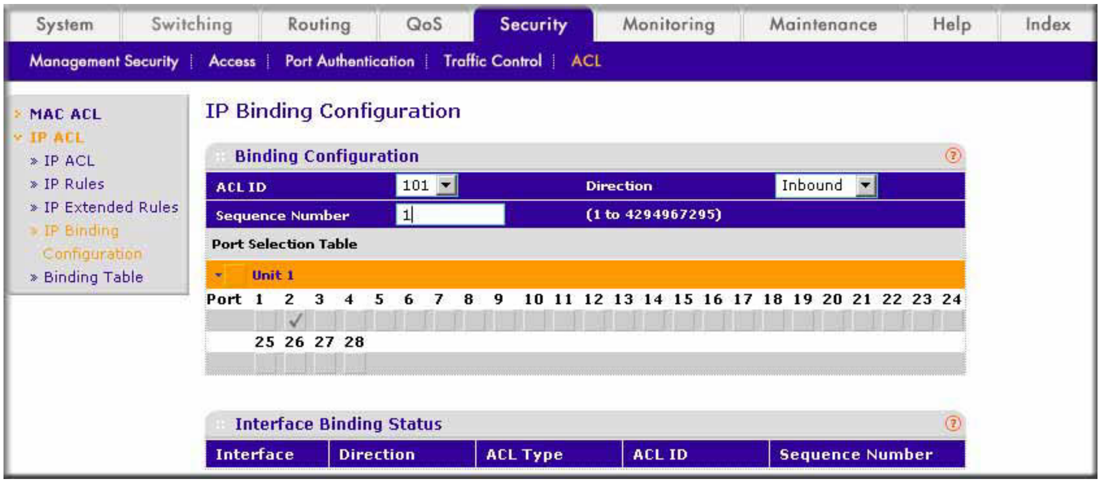
- *Configure the Switch* on page 88
- *Configure the GSM7342S Switch* on page 96

Configure the Switch

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

   a. Select **Routing > VLAN > VLAN Routing Wizard**.

A screen similar to the following displays.n the VLAN Routing Wizard,



IP Binding Configuration

Binding Configuration

ACL ID	101	Direction	Inbound
Sequence Number	1	(1 to 4294967295)	

Port Selection Table

Unit 1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
		✓																						
	25	26	27	28																				

Interface Binding Status

Interface	Direction	ACL Type	ACL ID	Sequence Number

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.

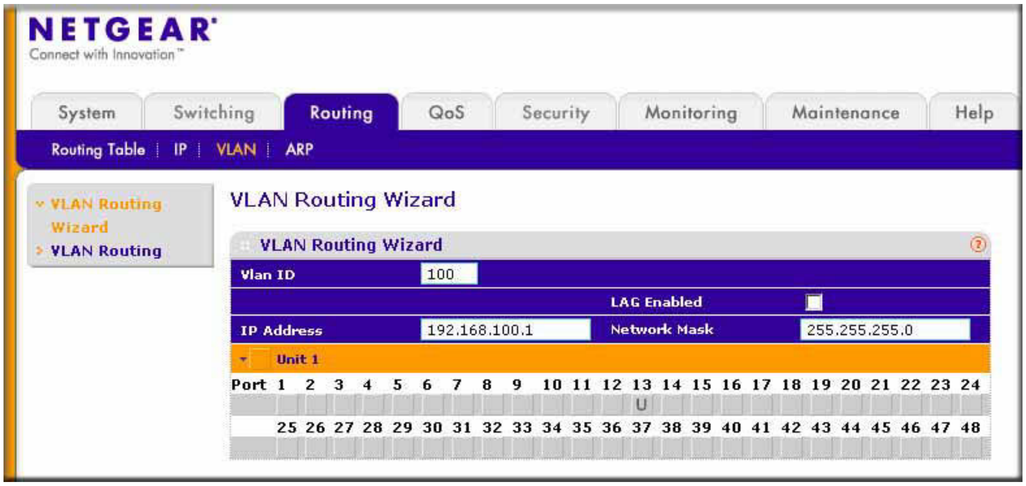
The U specifies that the egress packet is untagged for the port.

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.



VLAN Routing Wizard

VLAN Routing Wizard

Vlan ID	100		
		LAG Enabled	□
IP Address	192.168.100.1	Network Mask	255.255.255.0

Unit 1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
													U											
	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48

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

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

d. Click the gray box under port **13** twice until **U** displays.

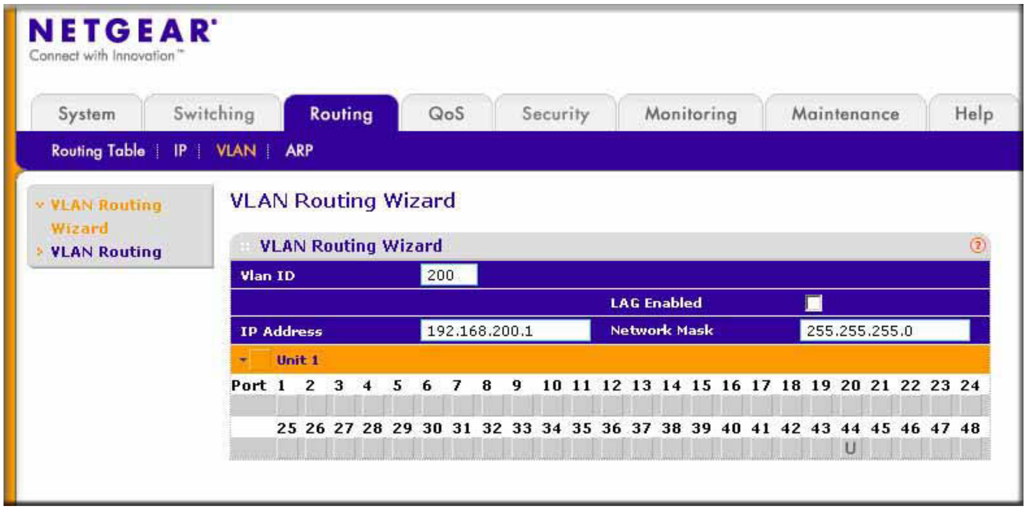
   The U specifies that the egress packet is untagged for the port.

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

3. Create VLAN 200 with IP address 192.168.200.1/24.

   a. Select **Routing > VLAN > VLAN Routing Wizard**.

   A screen similar to the following displays.



VLAN Routing Wizard

VLAN Routing Wizard

Vlan ID 200

LAG Enabled □

IP Address 192.168.200.1 Network Mask 255.255.255.0

Unit 1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
																				U				

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.

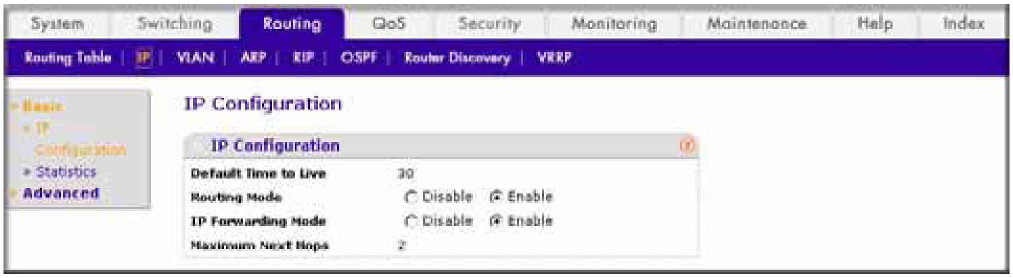
   The U specifies that the egress packet is untagged for the port.

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.



IP Configuration

IP Configuration

Default Time to Live	30
Routing Mode	○ Disable ● Enable
IP Forwarding Mode	○ Disable ● Enable
Maximum Next Hops	2

b. Under IP Configuration, make the following selections:

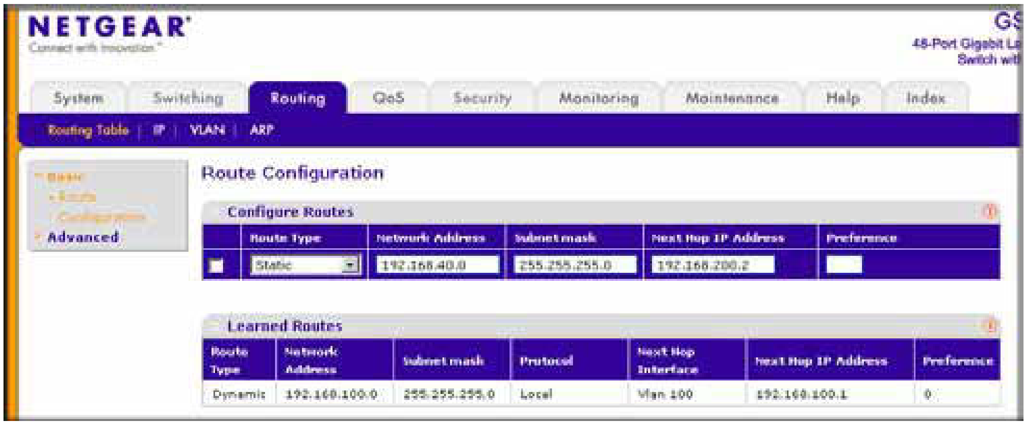
- For Routing Mode, select the **Enable** radio button.
- For IP Forwarding Mode, select the **Enable** radio button.

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.



Route Configuration

Configure Routes

	Route Type	Network Address	Subnet mask	Next Hop IP Address	Preference
□	Static	192.168.40.0	255.255.255.0	192.168.200.2	

Learned Routes

Route Type	Network Address	Subnet mask	Protocol	Next Hop Interface	Next Hop IP Address	Preference
Dynamic	192.168.100.0	255.255.255.0	Local	Vlan 100	192.168.100.1	0

b. Under Configure Routes, make the following selection and enter the following information:

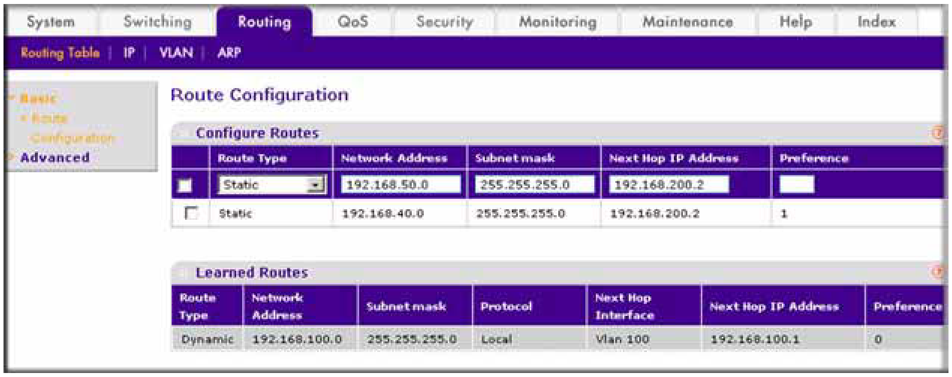
- In the Route Type list, select **Static**.
- In the **Network Address** field, enter **192.168.40.0**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Next Hop IP Address** field, enter **192.168.200.2**.

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

Configure Routes

	Route Type	Network Address	Subnet mask	Next Hop IP Address	Preference
□	Static	192.168.50.0	255.255.255.0	192.168.200.2	
□	Static	192.168.40.0	255.255.255.0	192.168.200.2	1

Learned Routes

Route Type	Network Address	Subnet mask	Protocol	Next Hop Interface	Next Hop IP Address	Preference
Dynamic	192.168.100.0	255.255.255.0	Local	Vlan 100	192.168.100.1	0

b. Under Configure Routes, make the following selection and enter the following information:

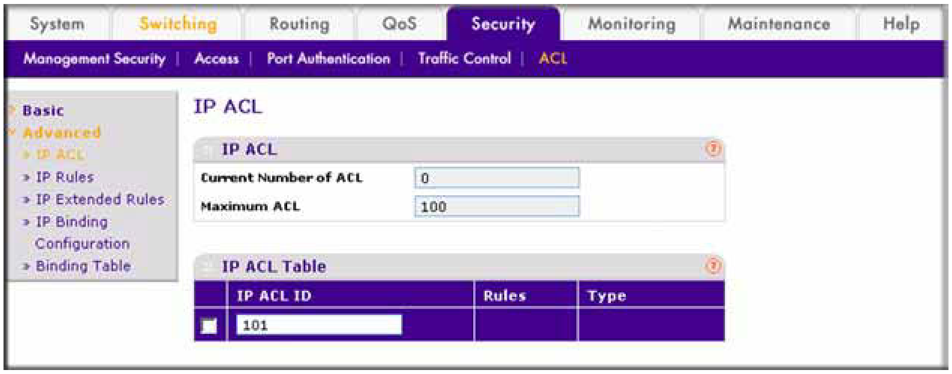
- In the **Route Type** list, select **Static**.
- In the **Network Address** field, enter **192.168.50.0**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Next Hop IP Address** field, enter **192.168.200.2**.

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

IP ACL

Current Number of ACL: 0

Maximum ACL: 100

IP ACL Table

	IP ACL ID	Rules	Type
□	101		

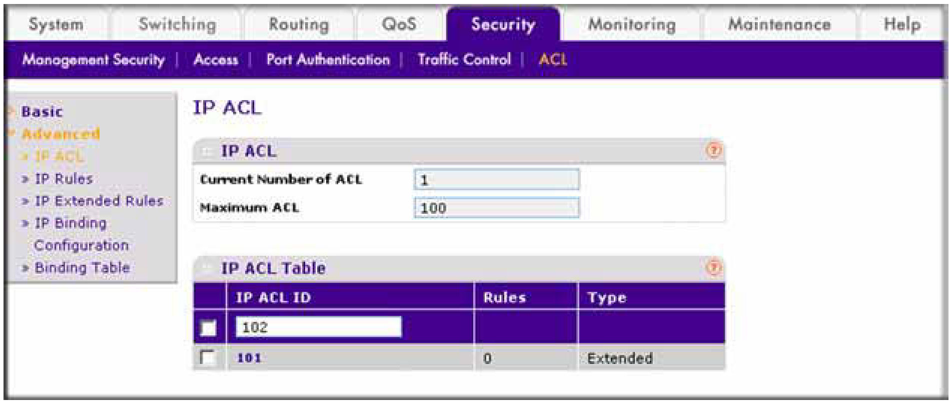
b. In the IP ACL Table, in the **IP ACL ID** field, enter **101**.

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

IP ACL

Current Number of ACL	1
Maximum ACL	100

IP ACL Table

	IP ACL ID	Rules	Type
☐	102		
☐	101	0	Extended

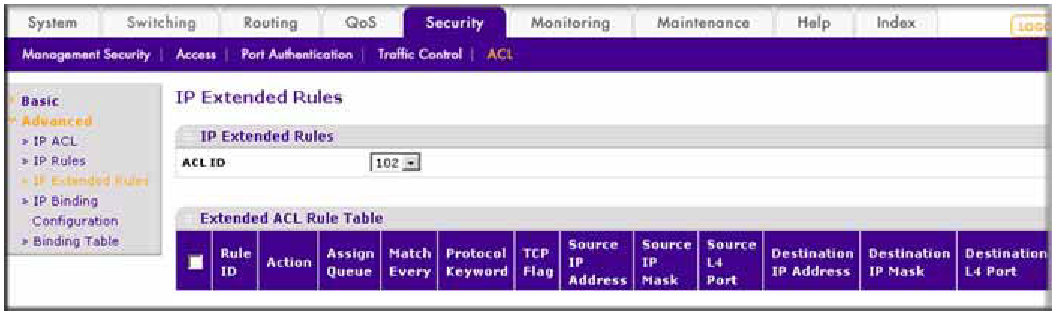
b. In the IP ACL Table, in the **IP ACL ID** field, enter **102**.

c. Click **Add**.

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

IP Extended Rules

ACL ID	102

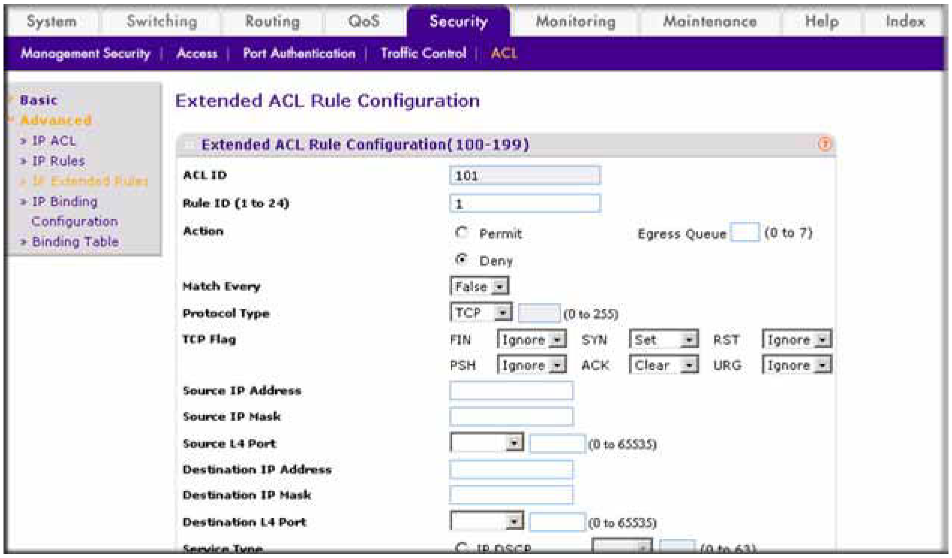
Extended ACL Rule Table

☐	Rule ID	Action	Assign Queue	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source IP Mask	Source L4 Port	Destination IP Address	Destination IP Mask	Destination L4 Port

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

Extended ACL Rule Configuration(100-199)

ACL ID	101		
Rule ID (1 to 24)	1		
Action	○ Permit ● Deny	Egress Queue	(0 to 7)
Match Every	False		
Protocol Type	TCP (0 to 255)		
TCP Flag	FIN Ignore PSH Ignore	SYN Set ACK Clear	RST Ignore URG Ignore
Source IP Address			
Source IP Mask			
Source L4 Port	(0 to 65535)		
Destination IP Address			
Destination IP Mask			
Destination L4 Port	(0 to 65535)		
Service Type	○ IP DSCP (0 to 63)		

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

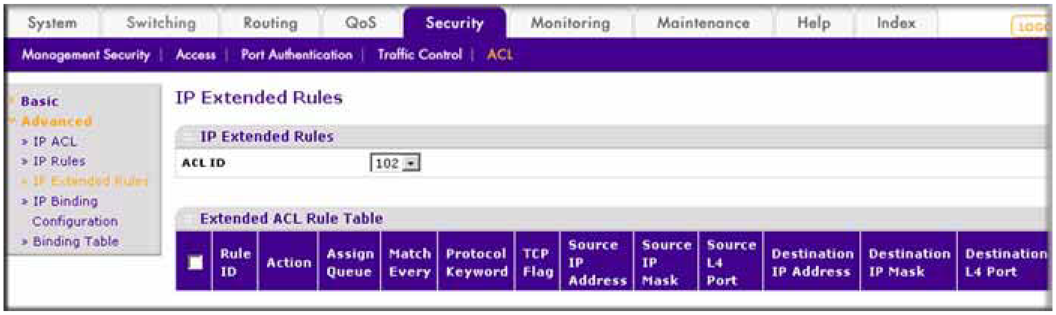
- In the **Rule ID** field, enter **1**.
- For Action mode, select the **Deny** radio button.
- In the **Match Every** field, select **False**.
- In the **Protocol Type** list, select **TCP**.
- For TCP Flag, in the **SYN** field, select **Set**, and in the **ACK** field, select **Clear**.

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

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

a. Select **Security > ACL > Advanced > IP Extended Rules**.

A screen similar to the following displays.



IP Extended Rules

IP Extended Rules

ACL ID 102

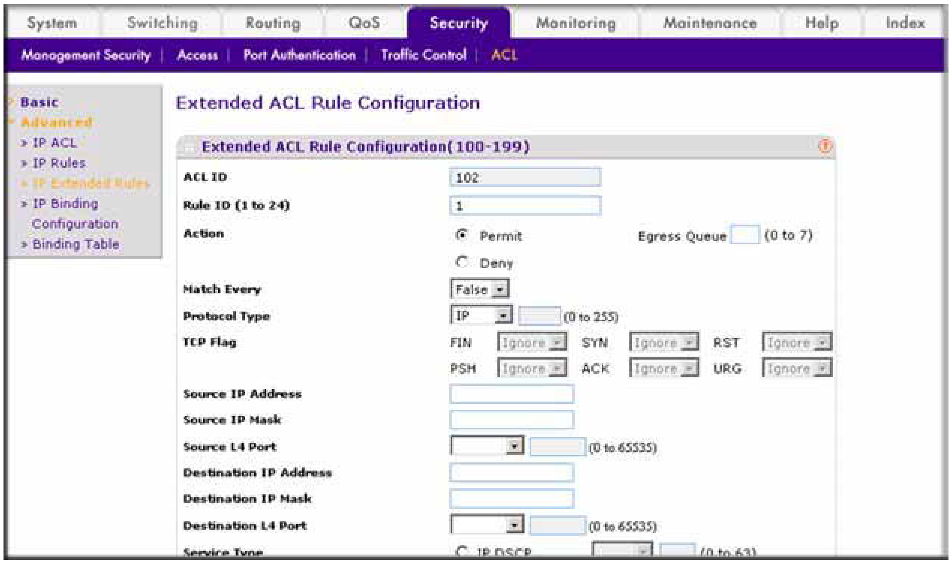
Extended ACL Rule Table

□	Rule ID	Action	Assign Queue	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source IP Mask	Source L4 Port	Destination IP Address	Destination IP Mask	Destination L4 Port

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

Extended ACL Rule Configuration(100-199)

ACL ID: 102

Rule ID (1 to 24): 1

Action: ● Permit ○ Deny — Egress Queue (0 to 7)

Match Every: False

Protocol Type: IP (0 to 255)

TCP Flag: FIN Ignore, SYN Ignore, RST Ignore, PSH Ignore, ACK Ignore, URG Ignore

Source IP Address

Source IP Mask

Source L4 Port (0 to 65535)

Destination IP Address

Destination IP Mask

Destination L4 Port (0 to 65535)

Service Type: ○ IP DSCP (0 to 63)

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

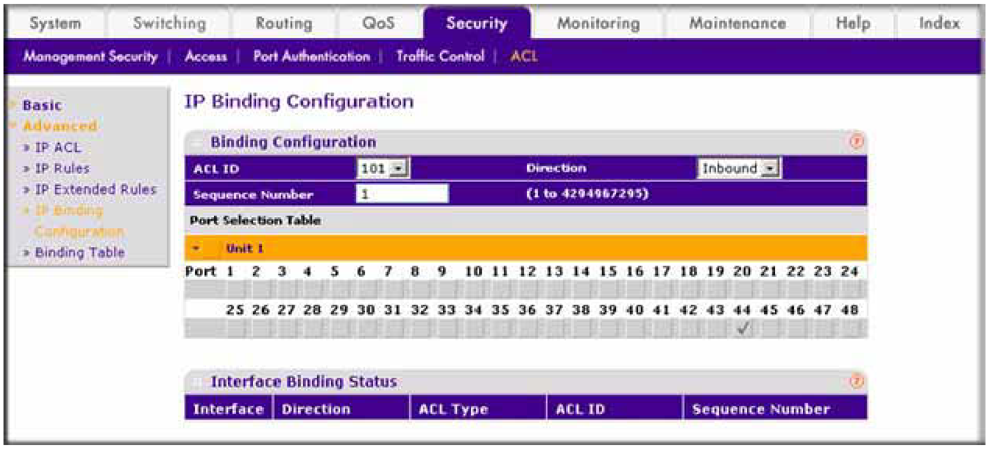
- In the **Rule ID** field, enter **1**.
- For Action, select the **Permit** radio button.
- In the **Match Every** field, select **False**.
- In the **Protocol Type** list, select **IP**.

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

Binding Configuration

ACL ID: 101 — Direction: Inbound

Sequence Number: 1 (1 to 4294967295)

Port Selection Table

Unit 1

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

25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48

Port 44: ✓

Interface Binding Status

Interface	Direction	ACL Type	ACL ID	Sequence Number

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.

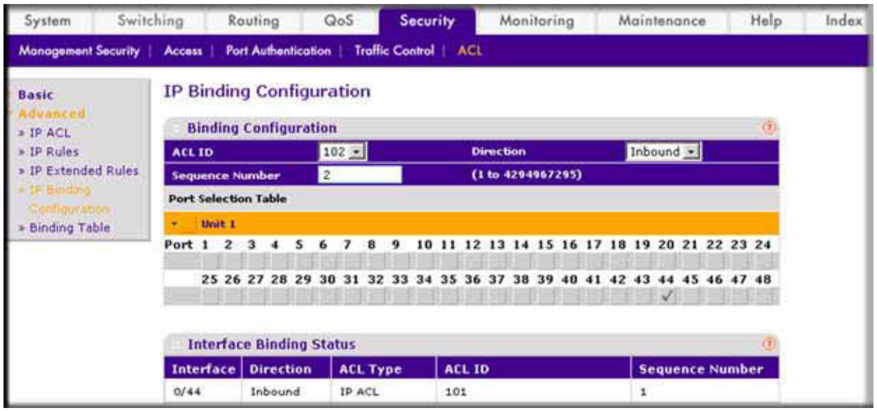
d. Click the gray box under port **44**. A check mark displays in the box.

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

Binding Configuration

ACL ID	102	Direction	Inbound
Sequence Number	2	(1 to 4294967295)	

Interface Binding Status

Interface	Direction	ACL Type	ACL ID	Sequence Number
0/44	Inbound	IP ACL	101	1

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.

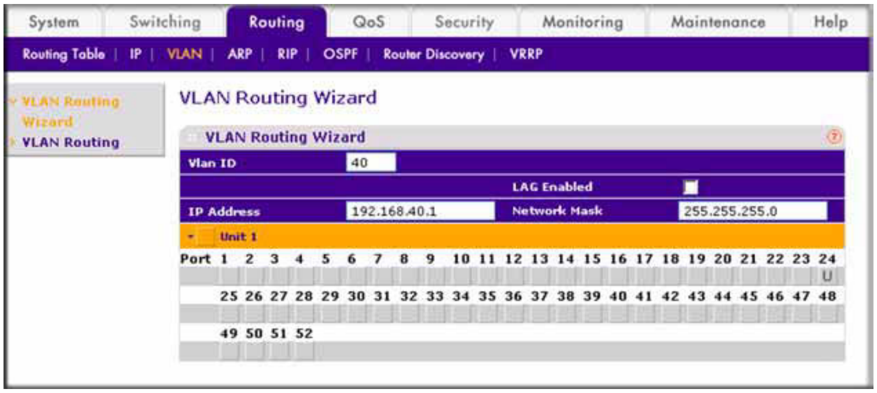
e. Click **Apply** to save the settings.

Configure the GSM7342S Switch

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

a. Select **Routing > VLAN > VLAN Routing Wizard**.

A screen similar to the following displays.



VLAN Routing Wizard

Vlan ID 40

LAG Enabled □

IP Address 192.168.40.1 Network Mask 255.255.255.0

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.

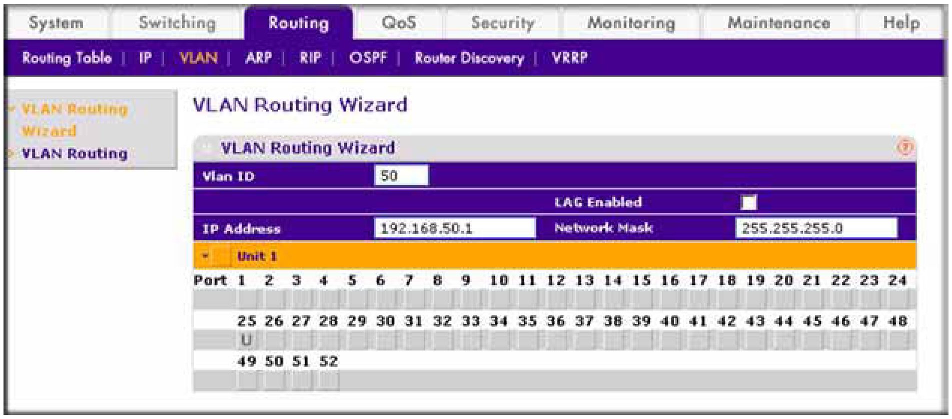
The U specifies that the egress packet is untagged for the port.

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

Vlan ID 50

LAG Enabled □

IP Address 192.168.50.1 Network Mask 255.255.255.0

b. Enter the following information:

- In the **Vlan ID** field, enter **50**.
- In the **IP Address** field, enter **192.168.50.1**.
- In the **Network Mask** field, enter **255.255.255.0**.

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

- d. Click the gray box under port **25** twice until **U** displays.

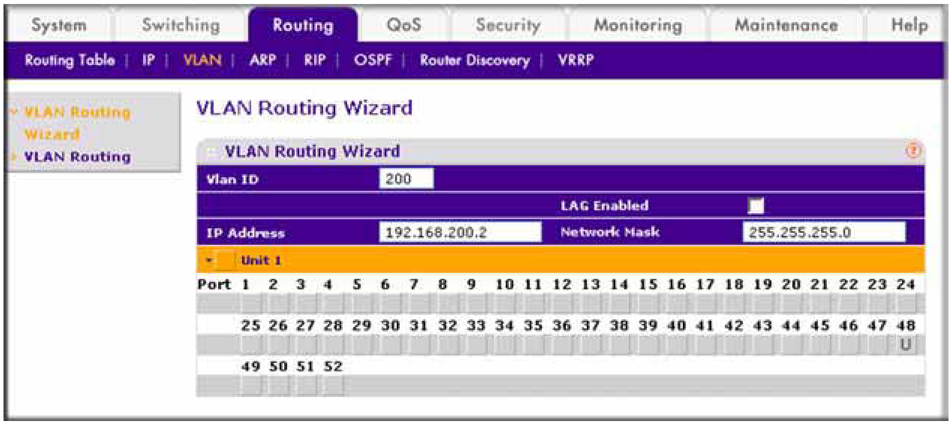
  The U specifies that the egress packet is untagged for the port.

- e. Click **Apply** to save VLAN 50.

3. Create VLAN 200 with IP address 192.168.200.2/24.

- a. Select **Routing > VLAN > VLAN Routing Wizard**.

  A screen similar to the following displays.



VLAN Routing Wizard

VLAN Routing Wizard

Vlan ID 200

LAG Enabled □

IP Address 192.168.200.2 Network Mask 255.255.255.0

Unit 1

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

25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 U

49 50 51 52

- 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.

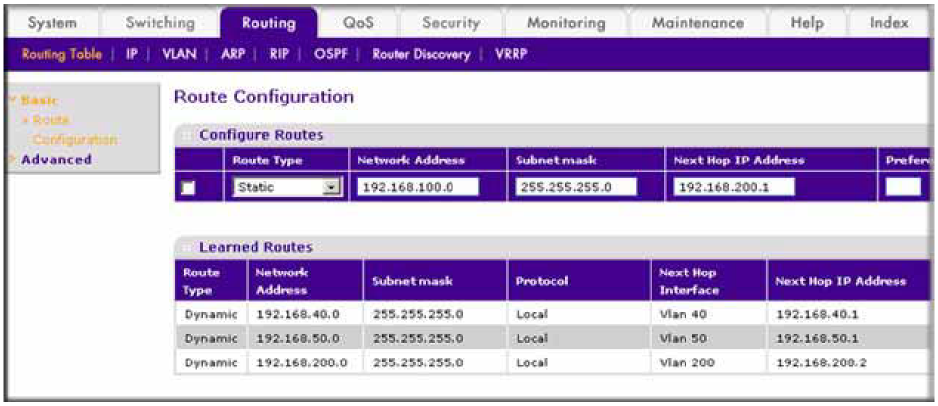
  The U specifies that the egress packet is untagged for the port.

- 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.



Route Configuration

Configure Routes

	Route Type	Network Address	Subnet mask	Next Hop IP Address	Prefere
□	Static	192.168.100.0	255.255.255.0	192.168.200.1	

Learned Routes

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

b. Under Configure Routes, make the following selections and enter the following information:

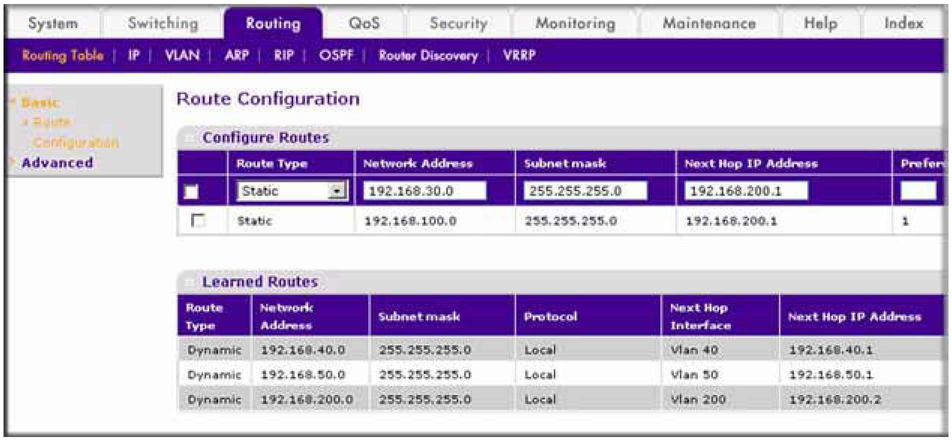
- Select **Static** in the **Route Type** field.
- In the **Network Address** field, enter **192.168.100.0**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Next Hop IP Address** field, enter **192.168.200.1**.

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

Configure Routes

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

Learned Routes

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

b. Under Configure Routes, make the following selection and enter the following information:

- In the **Route Type** field, select **Static**.
- In the **Network Address** field, enter **192.168.30.0**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Next Hop IP Address** field, enter **192.168.200.1**.

c. Click **Add**.

Use ACLs to Configure Isolated VLANs on a Layer 3 Switch

This example shows how to isolate VLANs on a Layer 3 switch by using ACLs. In this example, PC 1 is in VLAN 24, PC 2 is in VLAN 48, and the server is in VLAN 38. PC 1 and PC 2 are isolated by an ACL but can both access the server. The example is shown as CLI commands and as a Web interface procedure.

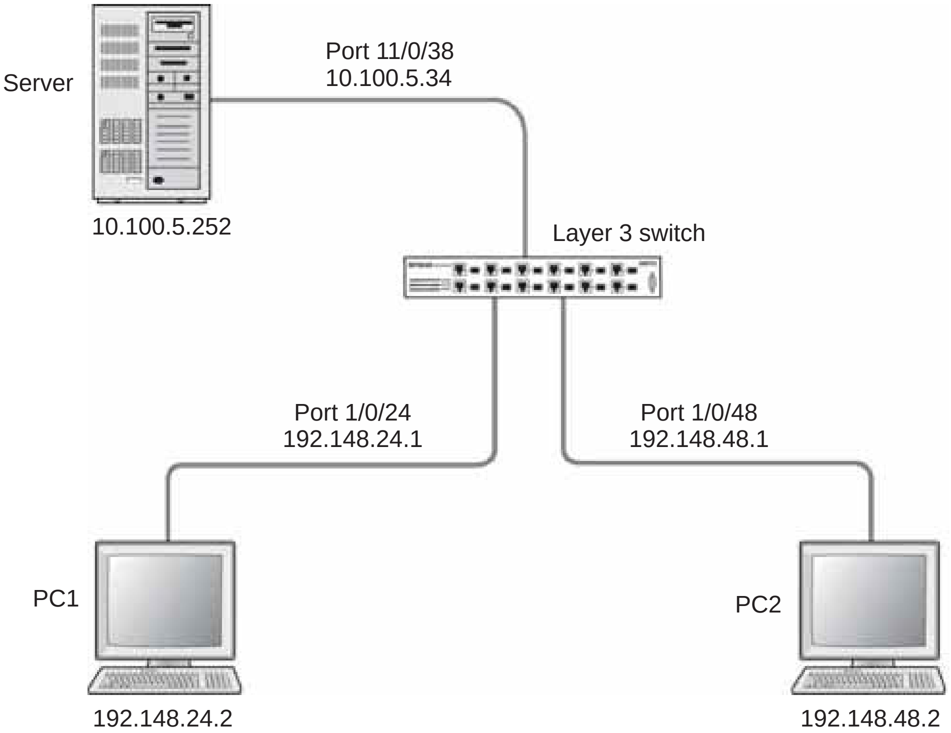


Figure 11. Using ACLs to isolate VLANs on a Layer 3 switch

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

1. Enter the following CLI commands.

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

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

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

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

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

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

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

4. Enable IP routing on the switch.

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

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

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

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

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

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

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

8. Create ACL 103 to permit all other traffic.

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

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

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

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

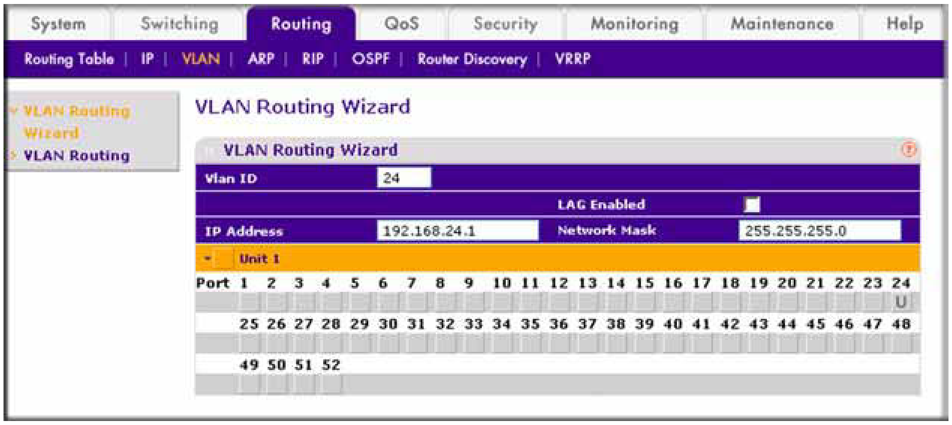
```
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#ip access-group 101 in 1
(Netgear Switch) (Interface 1/0/48)#ip access-group 103 in 2
(Netgear Switch) (Interface 1/0/48)#exit
```

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

1. Create VLAN 24 with IP address 192.168.24.1.

   a. Select **Routing > VLAN > VLAN Routing Wizard**.

   A screen similar to the following displays.



Vlan ID 24

LAG Enabled □

IP Address 192.168.24.1

Network Mask 255.255.255.0

   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.

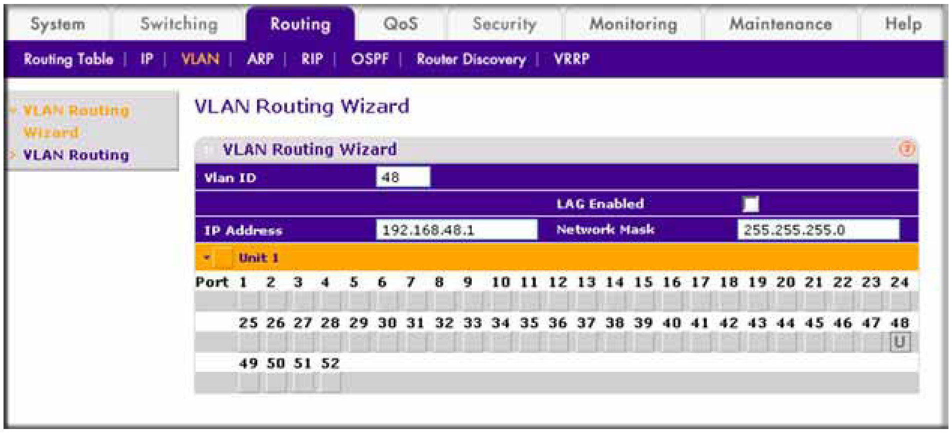
   The U specifies that the egress packet is untagged for the port.

   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

Vlan ID	48		
		LAG Enabled	□
IP Address	192.168.48.1	Network Mask	255.255.255.0

Unit 1

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

25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 — port 48: U

49 50 51 52

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.

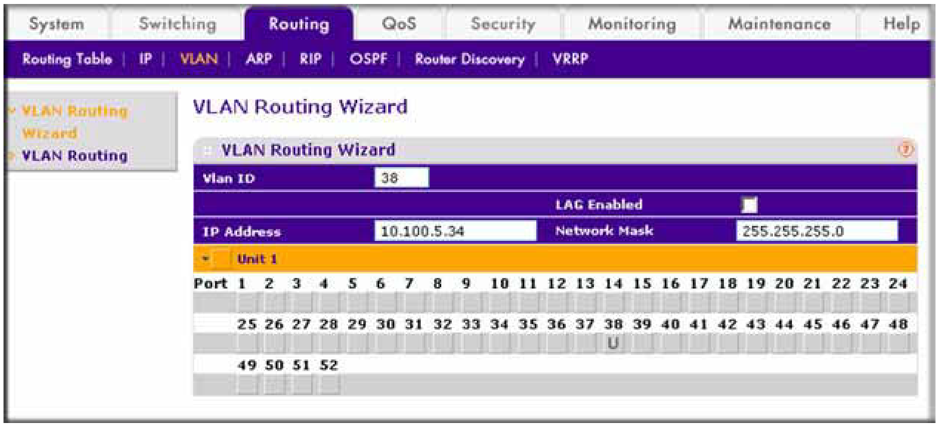
The U specifies that the egress packet is untagged for the port.

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

Vlan ID	38		
		LAG Enabled	□
IP Address	10.100.5.34	Network Mask	255.255.255.0

Unit 1

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

25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 — port 38: U

49 50 51 52

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.

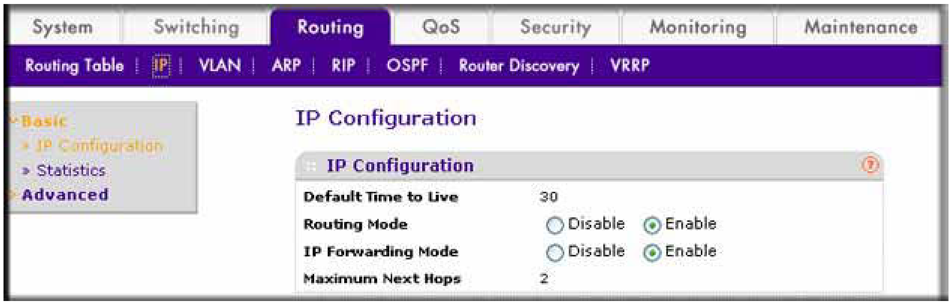
The U specifies that the egress packet is untagged for the port.

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

IP Configuration

Default Time to Live	30
Routing Mode	○ Disable ● Enable
IP Forwarding Mode	○ Disable ● Enable
Maximum Next Hops	2

b. Under IP Configuration, make the following selections:

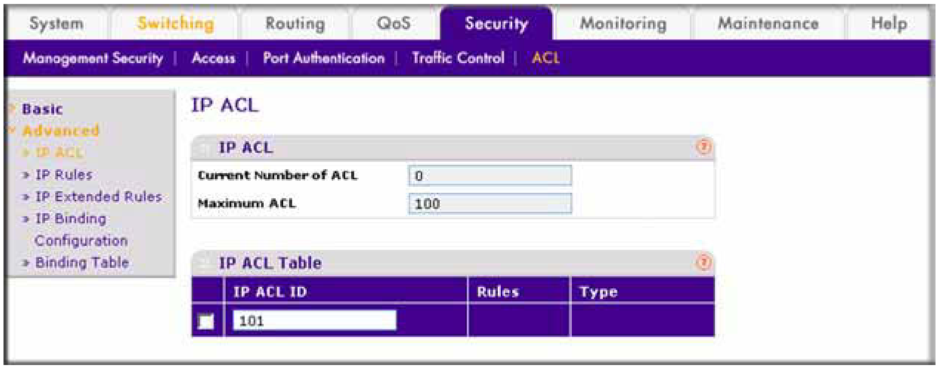
- For Routing Mode, select the **Enable** radio button.
- For IP Forwarding Mode, select the **Enable** radio button.

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

IP ACL

Current Number of ACL	0
Maximum ACL	100

IP ACL Table

	IP ACL ID	Rules	Type
□	101		

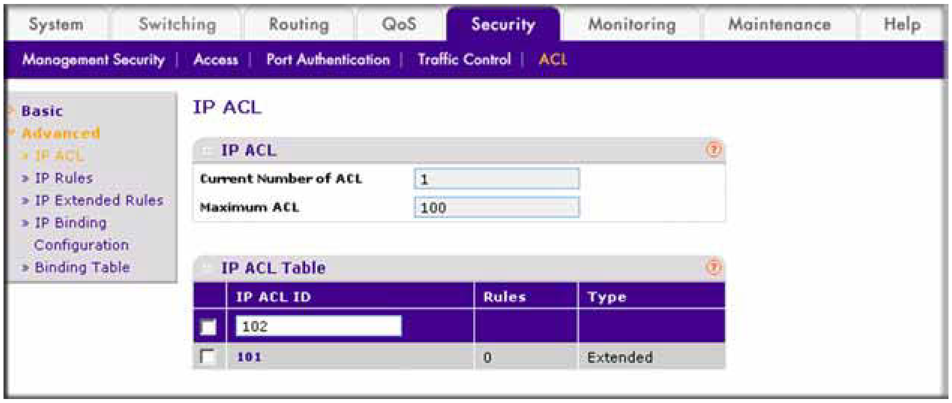
b. In the IP ACL Table, in the **IP ACL ID** field, enter **101**.

c. Click **Add**.

6. Create an ACL with ID 102.

a. Select **Security > ACL > Advanced > IP ACL**.

A screen similar to the following displays.



IP ACL

IP ACL

Current Number of ACL	1
Maximum ACL	100

IP ACL Table

	IP ACL ID	Rules	Type
☐	102		
☐	101	0	Extended

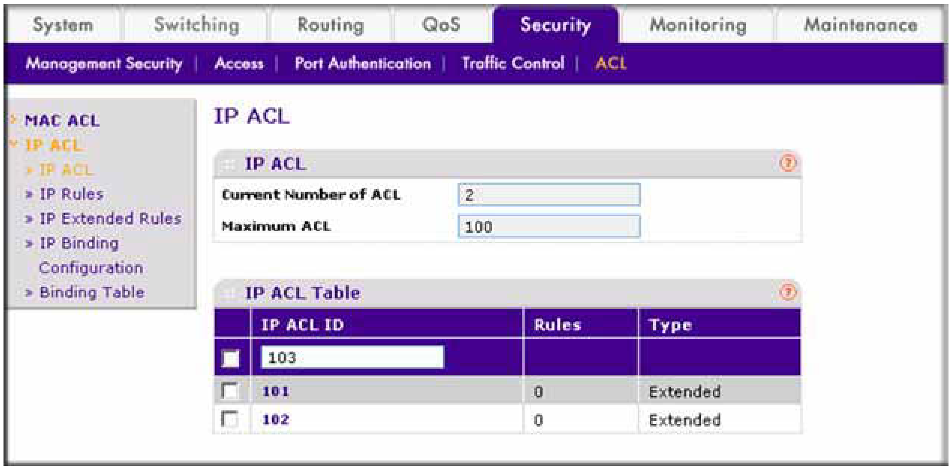
b. In the IP ACL Table, in the **IP ACL ID** field, enter **102**.

c. Click **Add**.

7. Create an ACL with ID 103.

a. Select **Security > ACL > Advanced > IP ACL**.

A screen similar to the following displays.



IP ACL

IP ACL

Current Number of ACL	2
Maximum ACL	100

IP ACL Table

	IP ACL ID	Rules	Type
☐	103		
☐	101	0	Extended
☐	102	0	Extended

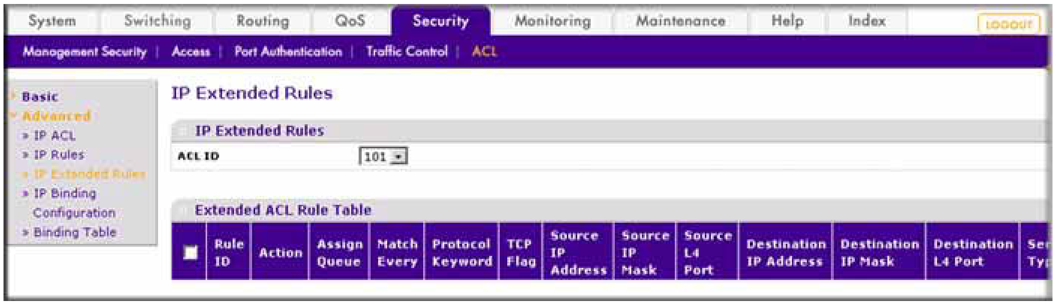
b. In the **IP ACL ID** field of the IP ACL Table, enter **103**.

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.



IP Extended Rules

IP Extended Rules

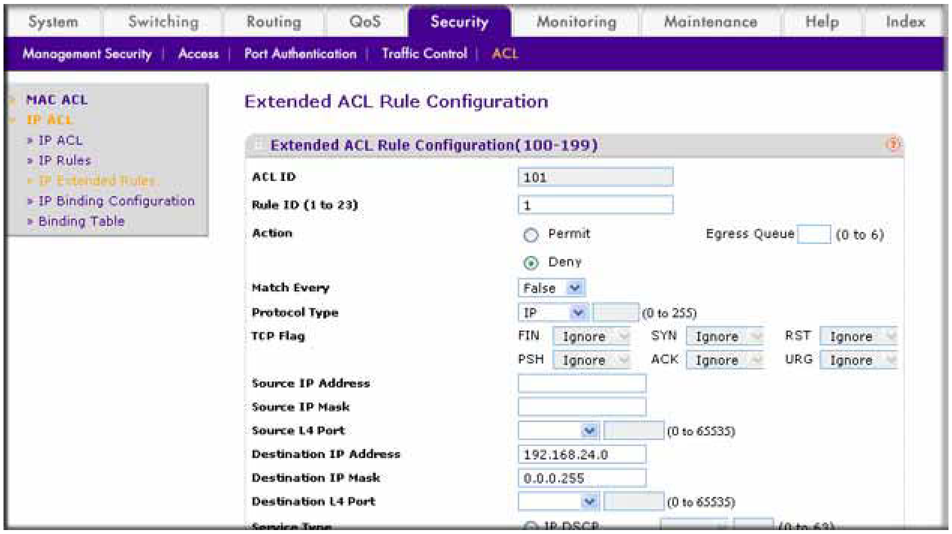
ACL ID: 101

Extended ACL Rule Table

□	Rule ID	Action	Assign Queue	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source IP Mask	Source L4 Port	Destination IP Address	Destination IP Mask	Destination L4 Port	Se Ty

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

Extended ACL Rule Configuration(100-199)

ACL ID	101
Rule ID (1 to 23)	1
Action	○ Permit Egress Queue (0 to 6) ● Deny
Match Every	False
Protocol Type	IP (0 to 255)
TCP Flag	FIN Ignore SYN Ignore RST Ignore PSH Ignore ACK Ignore URG Ignore
Source IP Address	
Source IP Mask	
Source L4 Port	(0 to 65535)
Destination IP Address	192.168.24.0
Destination IP Mask	0.0.0.255
Destination L4 Port	(0 to 65535)
Service Type	○ IP DSCP (0 to 63)

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

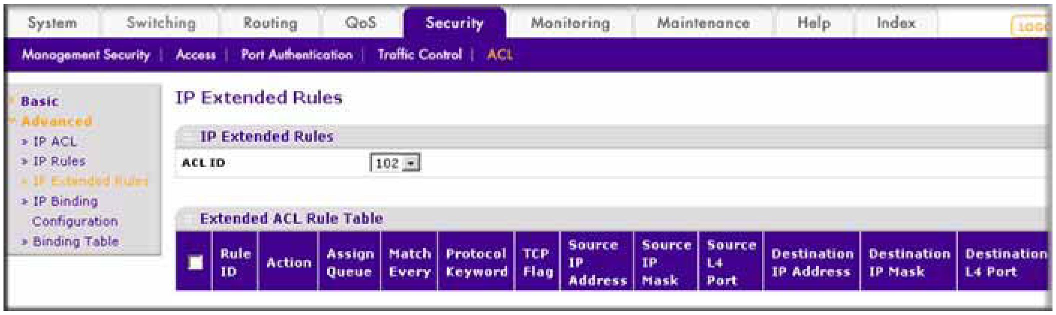
- In the **Rule ID** field, enter **1**.
- For Action, select the **Deny** radio button.
- In the **Match Every** field, select **False**.
- In the **Destination IP Address** field, enter **192.168.24.0**.
- In the **Destination IP Mask** field, enter **0.0.0.255**.

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

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

a. Select **Security > ACL > Advanced > IP Extended Rules**.

A screen similar to the following displays.



IP Extended Rules

IP Extended Rules

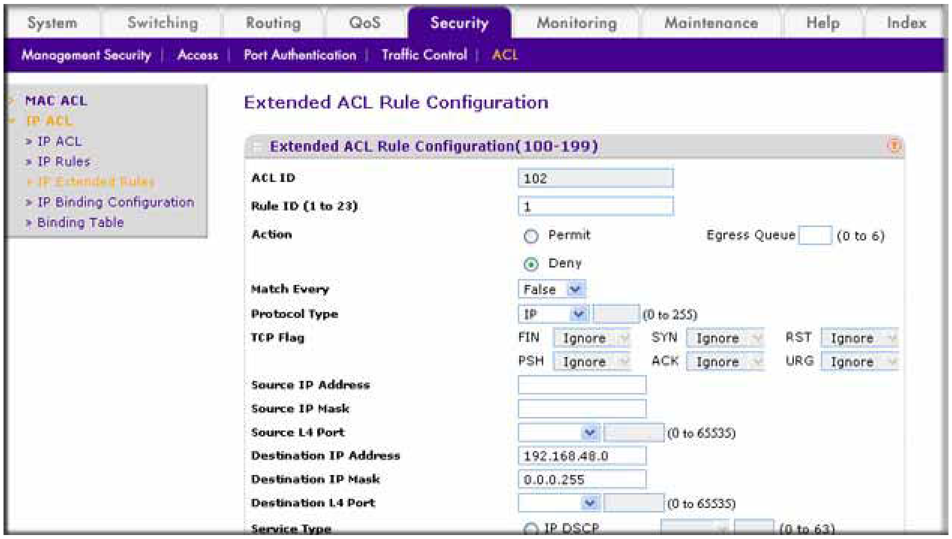
ACL ID 102

Extended ACL Rule Table

□	Rule ID	Action	Assign Queue	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source IP Mask	Source L4 Port	Destination IP Address	Destination IP Mask	Destination L4 Port

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

Extended ACL Rule Configuration(100-199)

ACL ID	102
Rule ID (1 to 23)	1
Action	○ Permit Egress Queue (0 to 6) ● Deny
Match Every	False
Protocol Type	IP (0 to 255)
TCP Flag	FIN Ignore SYN Ignore RST Ignore PSH Ignore ACK Ignore URG Ignore
Source IP Address	
Source IP Mask	
Source L4 Port	(0 to 65535)
Destination IP Address	192.168.48.0
Destination IP Mask	0.0.0.255
Destination L4 Port	(0 to 65535)
Service Type	○ IP DSCP (0 to 63)

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

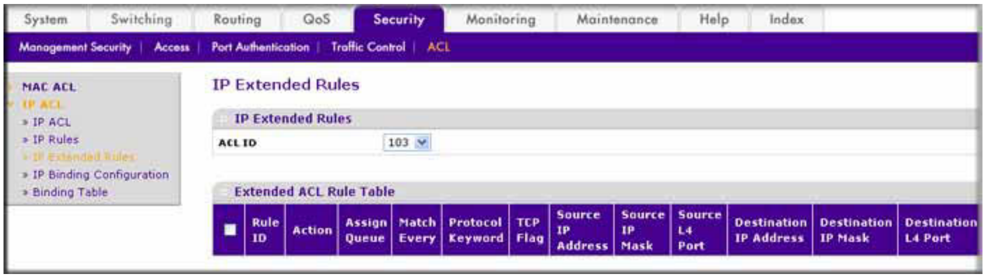
- In the **Rule ID** field, enter **1**.
- For Action mode, select the **Deny** radio button.
- In the **Match Every** field, select **False**.
- In the **Destination IP Address** field, enter **192.168.48.0**.
- In the **Destination IP Mask** field, enter **0.0.0.255**.

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

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

a. Select **Security > ACL > Advanced > IP Extended Rules**.

A screen similar to the following displays.



IP Extended Rules

IP Extended Rules

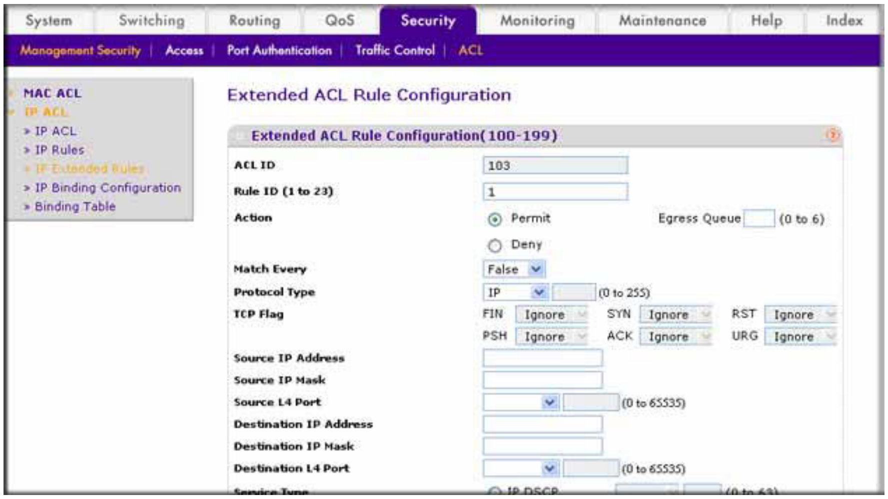
ACL ID 103

Extended ACL Rule Table

□	Rule ID	Action	Assign Queue	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source IP Mask	Source L4 Port	Destination IP Address	Destination IP Mask	Destination L4 Port

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

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



Extended ACL Rule Configuration

Extended ACL Rule Configuration(100-199)

ACL ID	103		
Rule ID (1 to 23)	1		
Action	● Permit	Egress Queue	(0 to 6)
	○ Deny		
Match Every	False		
Protocol Type	IP (0 to 255)		
TCP Flag	FIN Ignore	SYN Ignore	RST Ignore
	PSH Ignore	ACK Ignore	URG Ignore
Source IP Address			
Source IP Mask			
Source L4 Port	(0 to 65535)		
Destination IP Address			
Destination IP Mask			
Destination L4 Port	(0 to 65535)		
Service Type	○ IP DSCP (0 to 63)		

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

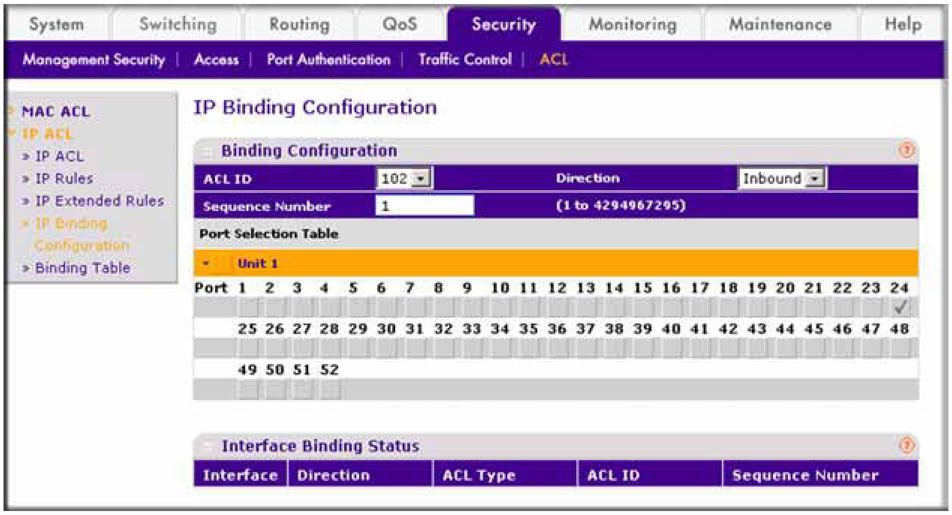
- In the **Rule ID** field, enter **1**.
- For Action mode, select the **Permit** radio button.
- In the **Match Every** field, select **False**.
- In the **Protocol Type** field, select **IP**.

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.



IP Binding Configuration

Binding Configuration

ACL ID	102	Direction	Inbound
Sequence Number	1	(1 to 4294967295)	

Port 24: ✓

Interface Binding Status

Interface	Direction	ACL Type	ACL ID	Sequence Number

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**.

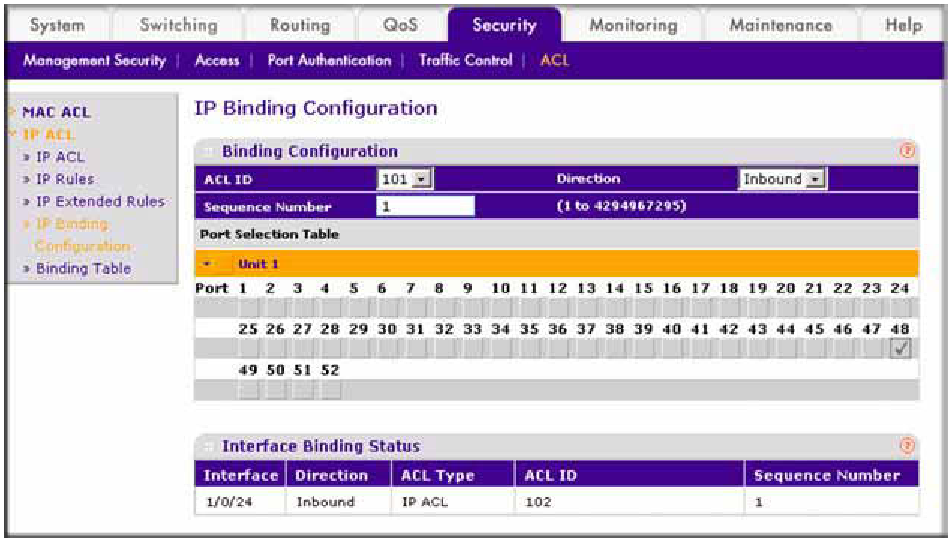
A check mark displays in the box.

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.



IP Binding Configuration

Binding Configuration

ACL ID	101	Direction	Inbound
Sequence Number	1	(1 to 4294967295)	

Port 48: ✓

Interface Binding Status

Interface	Direction	ACL Type	ACL ID	Sequence Number
1/0/24	Inbound	IP ACL	102	1

b. Under Binding Configuration, make the following selection and enter the following information:
   - In he **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**.

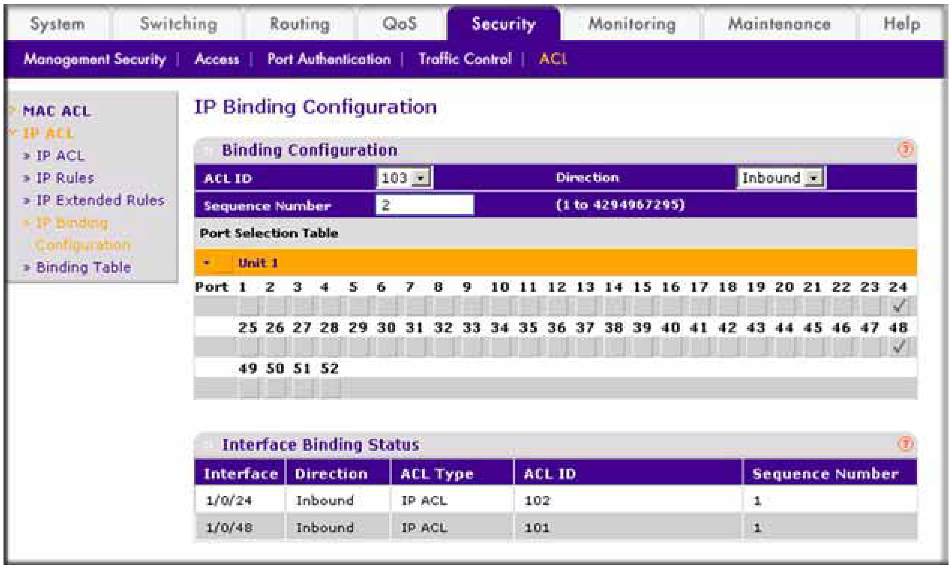
   A check mark displays in the box.

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

Binding Configuration

ACL ID: 103

Direction: Inbound

Sequence Number: 2 (1 to 4294967295)

Port Selection Table

Unit 1

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

25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 ✓

49 50 51 52

Interface Binding Status

Interface	Direction	ACL Type	ACL ID	Sequence Number
1/0/24	Inbound	IP ACL	102	1
1/0/48	Inbound	IP ACL	101	1

b. Under Binding Configuration, make the following selection and enter the following information:
   - In the **ACL ID** field, select **103**.
   - In the **Sequence Number** field, enter **2**.

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

   Configure the following ports:
   - Click the gray box under port **24**. A check mark displays in the box.
   - Click the gray box under port **48**. A check mark displays in the box.

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

Set up a MAC ACL with Two Rules

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

CLI: Set up a MAC ACL with Two Rules

1. Create a new MAC ACL acl_bpdu.

```
(Netgear Switch) #
(Netgear Switch) #config
(Netgear Switch) (Config)#mac access-list extended acl_bpdu
```

2. Deny all the traffic that has destination MAC 01:80:c2:xx:xx:xx.

```
(Netgear Switch) (Config-mac-access-list)#deny any 01:80:c2:00:00:00
00:00:00:ff:ff:ff
```

3. Permit all the other traffic.

```
(Netgear Switch) (Config-mac-access-list)#permit any
(Netgear Switch) (Config-mac-access-list)#exit
```

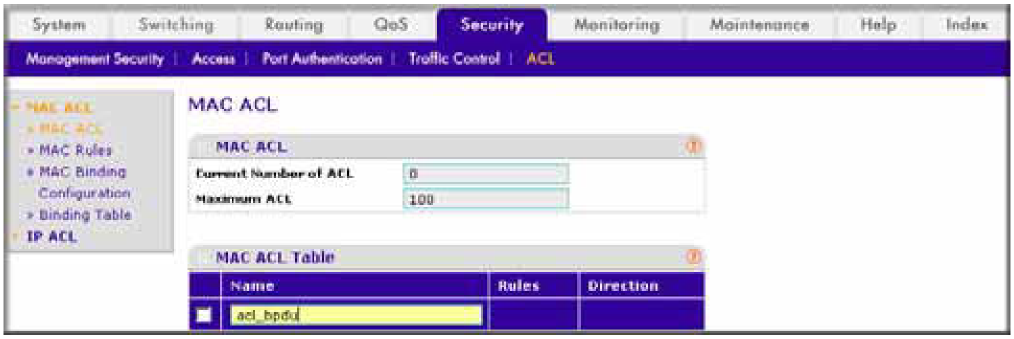
4. Apply the MAC ACL acl_bpdu to port 1/0/2.

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

Web Interface: Set up a MAC ACL with Two Rules

1. Create MAC ACL 101 on the switch.
   a. Select **Security > ACL > MAC ACL**.

A screen similar to the following displays.



MAC ACL

MAC ACL

Current Number of ACL	0
Maximum ACL	100

MAC ACL Table

	Name	Rules	Direction
□	acl_bpdu		

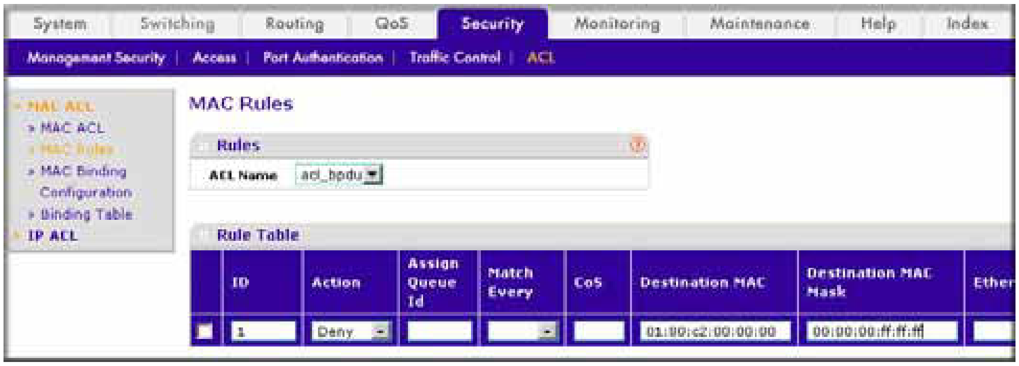
b. In the **Name** field, enter **acl_bpdu**.

c. Click **Add** to create ACL acl_bpdu.

2. Create a new rule associated with the ACL acl_bpdu.

a. Select **Security > ACL > MAC ACL > MAC Rules**.

A screen similar to the following displays.



MAC Rules

Rules

ACL Name: acl_bpdu

Rule Table

	ID	Action	Assign Queue Id	Match Every	CoS	Destination MAC	Destination MAC Mask	Ether
□	1	Deny				01:80:c2:00:00:00	00:00:00:ff:ff:ff	

a. In the **ACL Name** field, select **acl_bpdu**.

b. In the **Action** field, select **Deny**.

c. Enter the following information in the Rule Table.

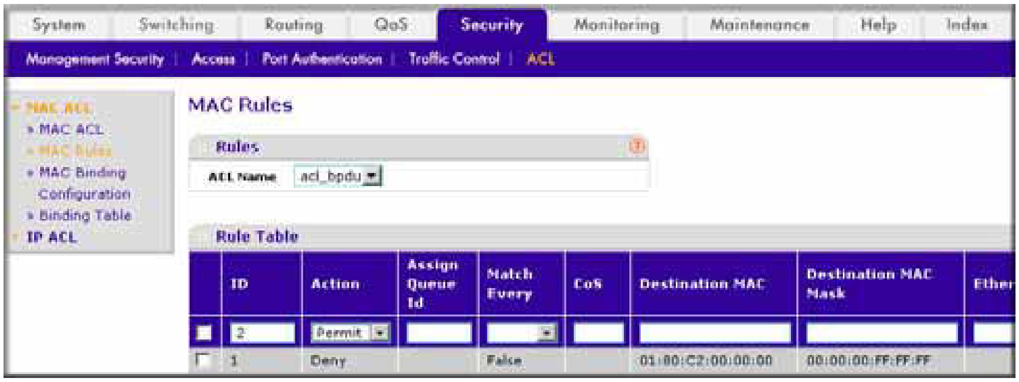
- In the **ID** field, enter **1**.
- In the **Destination MAC** field, enter **01:80:c2:00:00:00**.
- In the **Destination MAC Mask** field, enter **00:00:00:ff:ff:ff**.

d. Click the **Add** button.

3. Create a another rule associated with the ACL acl_bpdu.

a. Select **Security > ACL > MAC ACL > MAC Rules**.

A screen similar to the following displays.



MAC Rules

Rules

ACL Name acl_bpdu

Rule Table

	ID	Action	Assign Queue Id	Match Every	CoS	Destination MAC	Destination MAC Mask	Ether
□	2	Permit						
□	1	Deny		False		01:80:C2:00:00:00	00:00:00:FF:FF:FF	

a. Select **acl_bpdu** in the **ACL Name** field.

b. Enter the following information in the Rule Table.

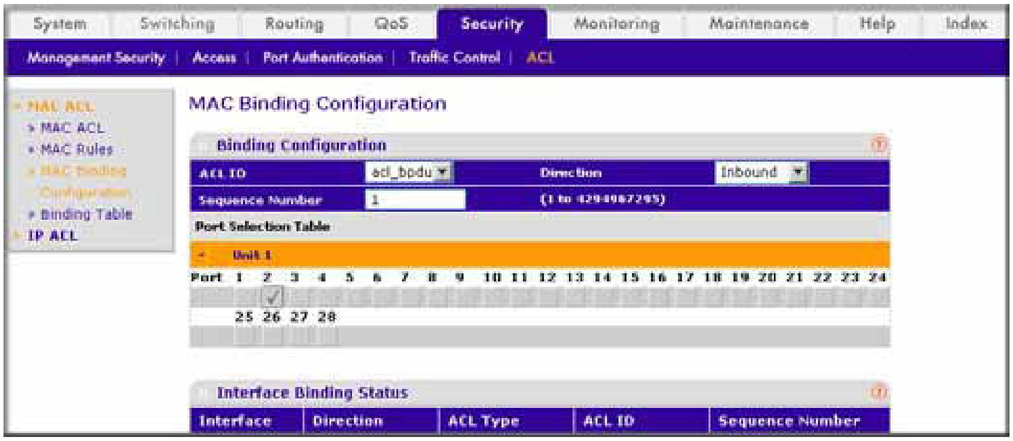
- In the **ID** field, enter **2**.
- In he **Action** field, select the **Permit**.

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.



MAC Binding Configuration

Binding Configuration

ACL ID	acl_bpdu	Direction	Inbound
Sequence Number	1	(1 to 4294967295)	

Port Selection Table

Unit 1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
		✓																						
	25	26	27	28																				

Interface Binding Status

Interface	Direction	ACL Type	ACL ID	Sequence Number

b. Enter the following information in the MAC Binding Configuration.

- IN the **ACL ID** field, select **acl_bpdu**.
- In the **Sequence Number** field, enter **1**.

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

d. Click the gray box under port **2**. A check mark displays in the box.

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

ACL Mirroring

This feature extends the existing port mirroring functionality by allowing you to mirror a designated traffic stream in an interface using ACL rules. Define an ACL rule matching the desired traffic with the option mirror to an interface. Any traffic matching this rule will be copied to the specified mirrored interface.

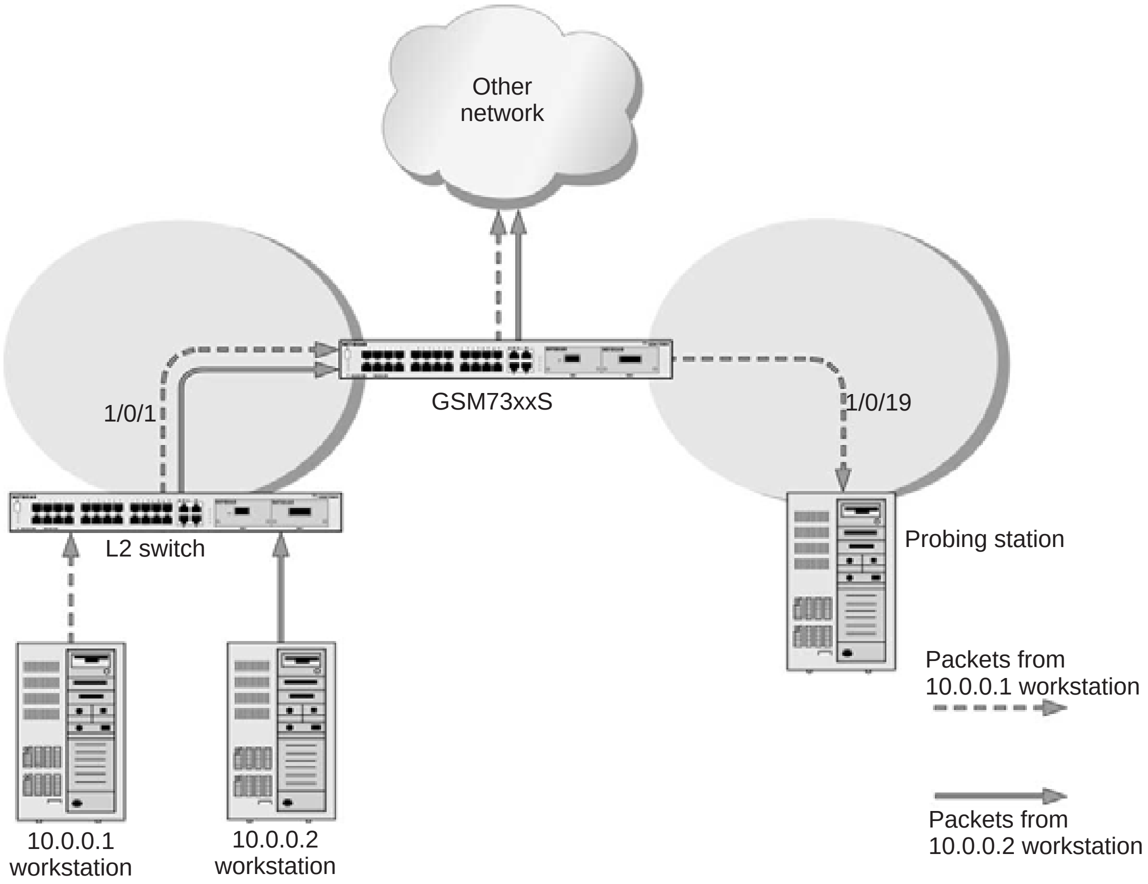


Figure 12. ACL mirroring

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.

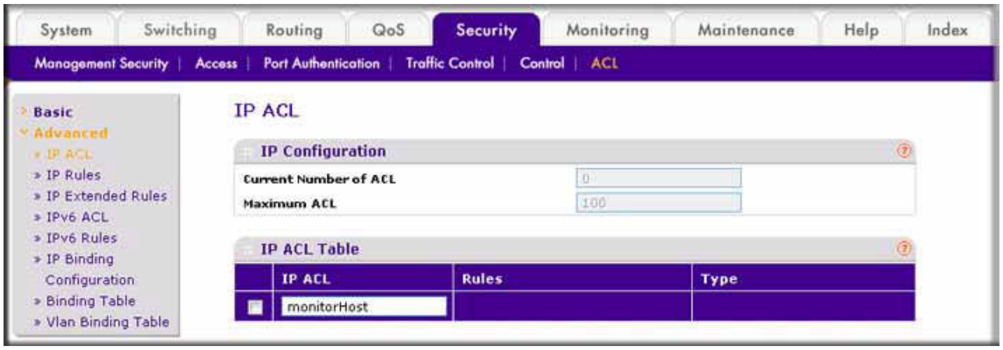
```
(Netgear Switch) # show ip access-lists
Current number of ACLs: 1  Maximum number of ACLs: 100

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

IP Configuration

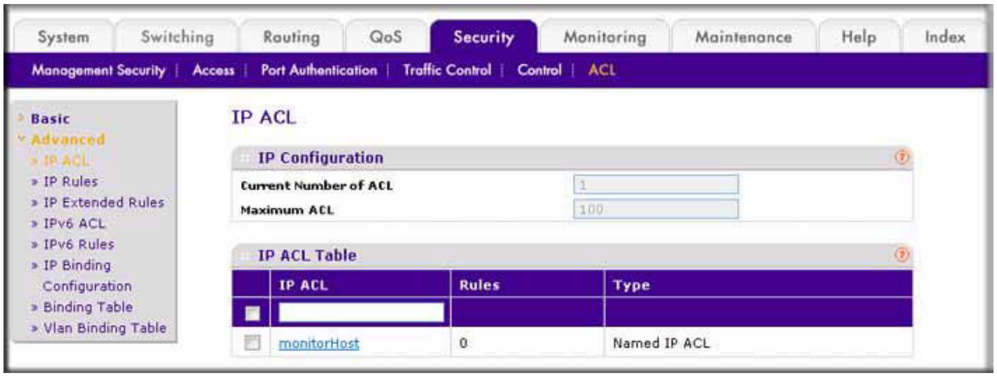
Current Number of ACL	0
Maximum ACL	100

IP ACL Table

	IP ACL	Rules	Type
□	monitorHost		

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

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



IP ACL

IP Configuration

Current Number of ACL	1
Maximum ACL	100

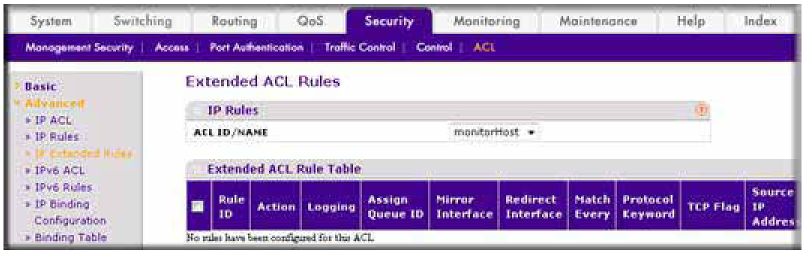
IP ACL Table

	IP ACL	Rules	Type
□			
□	monitorHost	0	Named IP ACL

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.



Extended ACL Rules

IP Rules

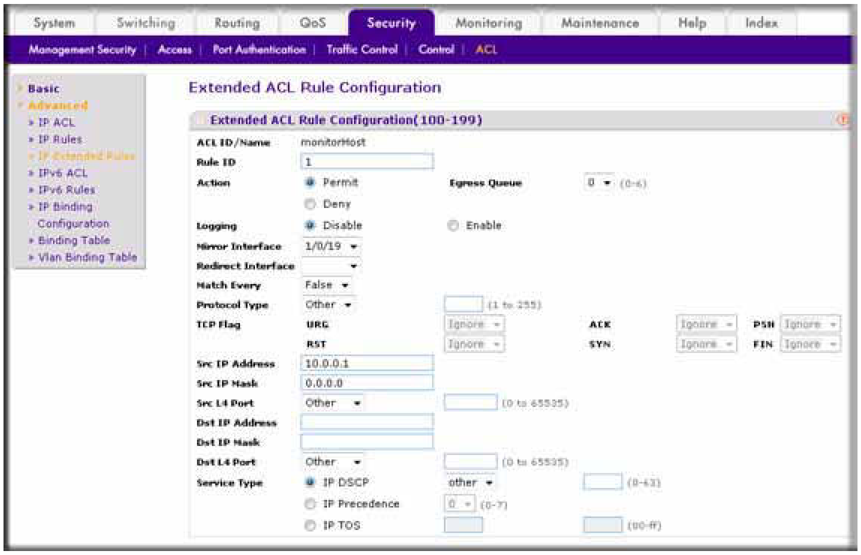
ACL ID/NAME	monitorHost

Extended ACL Rule Table

□	Rule ID	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Match Every	Protocol Keyword	TCP Flag	Source IP Addres

No rules have been configured for this ACL.

b. Click **Add**, and the Extended ACL Rule Configuration screen displays.



Extended ACL Rule Configuration

Extended ACL Rule Configuration(100-199)

ACL ID/Name	monitorHost					
Rule ID	1					
Action	● Permit	Egress Queue	0 (0-6)			
	○ Deny					
Logging	● Disable	○ Enable				
Mirror Interface	1/0/19					
Redirect Interface						
Match Every	False					
Protocol Type	Other	(1 to 255)				
TCP Flag	URG	Ignore	ACK	Ignore	PSH	Ignore
	RST	Ignore	SYN	Ignore	FIN	Ignore
Src IP Address	10.0.0.1					
Src IP Mask	0.0.0.0					
Src L4 Port	Other	(0 to 65535)				
Dst IP Address						
Dst IP Mask						
Dst L4 Port	Other	(0 to 65535)				
Service Type	● IP DSCP	other	(0-63)			
	○ IP Precedence	0 (0-7)				
	○ IP TOS		(00-ff)			

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

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

e. In the **Mirror Interface** list, select **1/0/19**.

f. In the **Src IP Address** field, enter **10.0.0.1**.

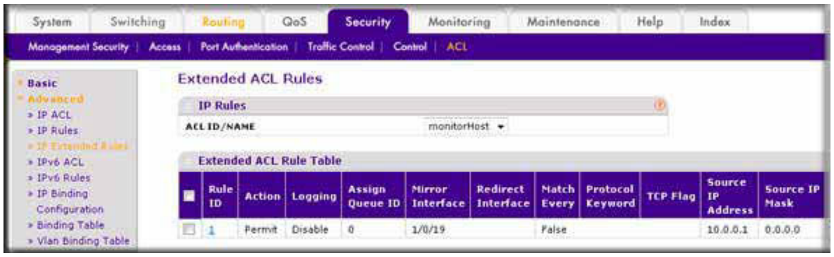
g. In the **Src IP Mask** field, enter **0.0.0.0**.

h. Click **Apply**.

3. Create a rule to match every other traffic.

a. Select **Security > ACL > Advanced > IP Extended Rules**.

A screen similar to the following displays.



Extended ACL Rules

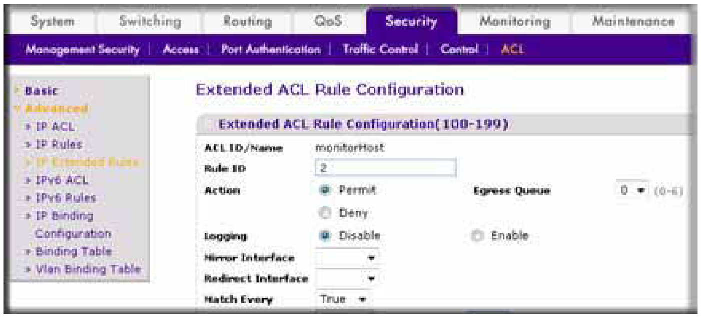
IP Rules

ACL ID/NAME: monitorHost

Extended ACL Rule Table

□	Rule ID	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source IP Mask
□	1	Permit	Disable	0	1/0/19		False			10.0.0.1	0.0.0.0

b. Click **Add**, and a screen similar to the following displays.



Extended ACL Rule Configuration

Extended ACL Rule Configuration(100-199)

ACL ID/Name	monitorHost		
Rule ID	2		
Action	● Permit	Egress Queue	0 (0-6)
	○ Deny		
Logging	● Disable	○ Enable	
Mirror Interface			
Redirect Interface			
Match Every	True		

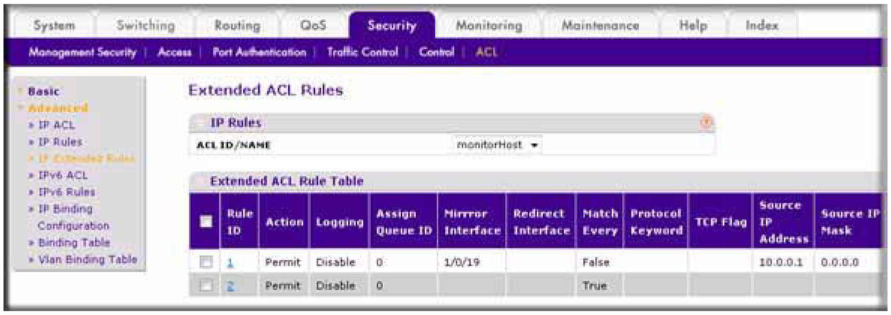
c. In the **Rule ID** field, enter **2**.

d. Select the **Permit** radio button.

e. In the **Match Every** field, select **True**.

f. Click **Apply**.

At the end of this configuration a screen similar to the following displays.



Extended ACL Rules

IP Rules

ACL ID/NAME: monitorHost

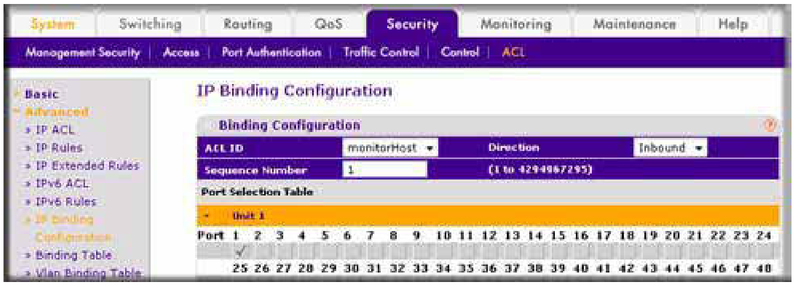
Extended ACL Rule Table

□	Rule ID	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source IP Mask
□	1	Permit	Disable	0	1/0/19		False			10.0.0.1	0.0.0.0
□	2	Permit	Disable	0			True				

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

Binding Configuration

ACL ID	monitorHost	Direction	Inbound
Sequence Number	1	(1 to 4294967295)	

Port Selection Table

Unit 1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	✓																							
	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48

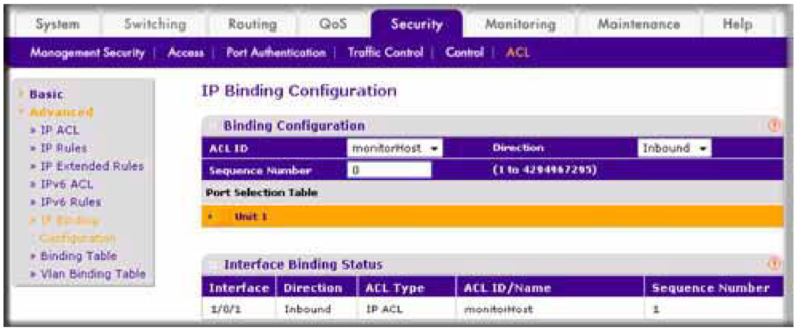
b. In the **Sequence Number** field, enter **1**.

c. In the Port Selection Table, click **Unit 1** to display all the ports for the device.

d. Select the **Port 1** check box.

e. Click **Apply**.

A screen similar to the following displays.



IP Binding Configuration

Binding Configuration

ACL ID	monitorHost	Direction	Inbound
Sequence Number	0	(1 to 4294967295)	

Port Selection Table

Unit 1

Interface Binding Status

Interface	Direction	ACL Type	ACL ID/Name	Sequence Number
1/0/1	Inbound	IP ACL	monitorHost	1

ACL Redirection

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

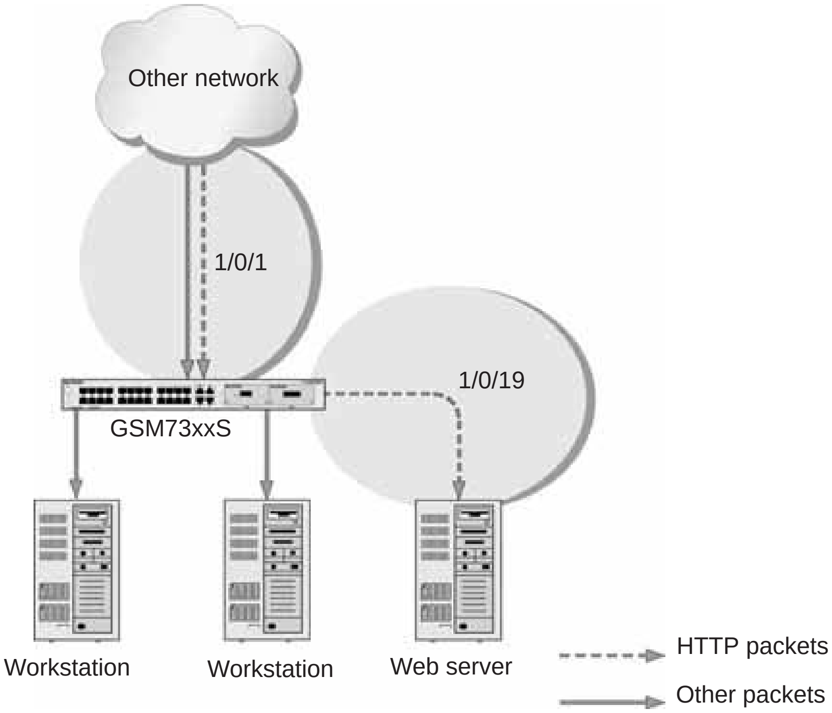


Figure 13. ACL Redirect

CLI: Redirect a Traffic Stream

The script in this section shows how to redirect an HTTP traffic stream received in an interface to the specified interface. This example redirects the HTTP traffic stream received in port 1/0/1 to port 1/0/19.

1. Create an IP access control list with the name redirectHTTP.

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

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

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

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

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

4. View the configuration.

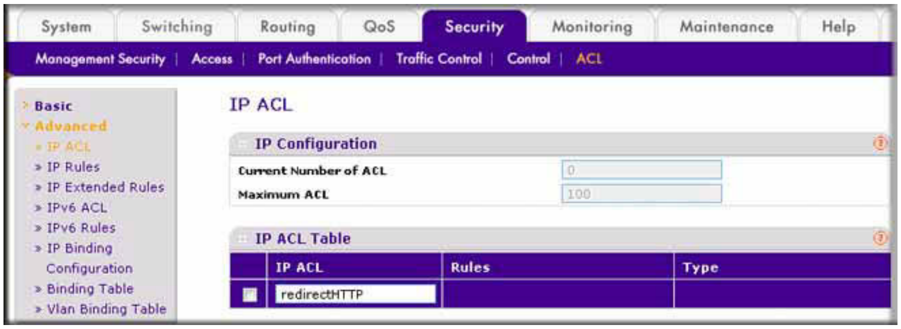
```
(Netgear Switch) # show ip access-lists
Current number of ACLs: 1  Maximum number of ACLs: 100

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

(Netgear Switch)  #show ip access-lists redirectHTTP

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

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

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

Web Interface: Redirect a Traffic Stream

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

1. Create an IP access control list with the name redirectHTTP.
   a. Select **Security > ACL > Advanced > IP ACL**.

      A screen similar to the following displays.



IP ACL

IP Configuration

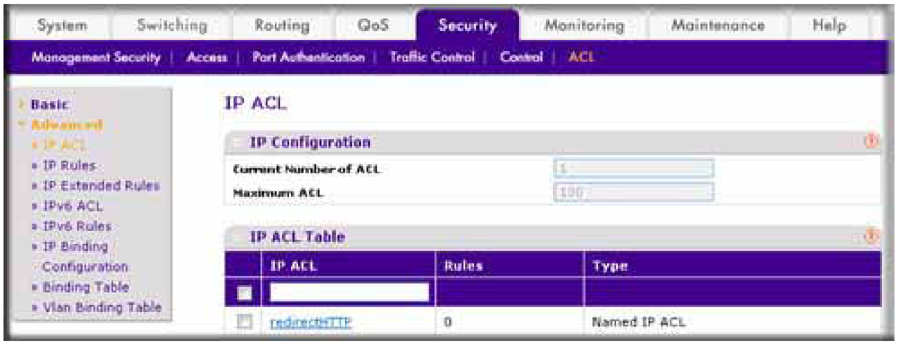
Current Number of ACL	0
Maximum ACL	100

IP ACL Table

	IP ACL	Rules	Type
□	redirectHTTP		

   b. In the **IP ACL** field, enter **redirectHTTP**.
   c. Click **Add** to create the IP ACL redirectHTTP.

      A screen similar to the following displays.



IP ACL

IP Configuration

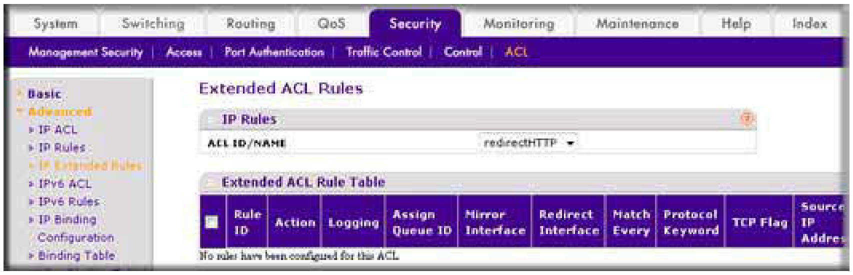
Current Number of ACL	1
Maximum ACL	100

IP ACL Table

	IP ACL	Rules	Type
□			
□	redirectHTTP	0	Named IP ACL

2. Create a rule to redirect HTTP traffic.
   a. Select **Security > ACL > Advanced > IP Extended Rules**.

      A screen similar to the following displays.



Extended ACL Rules

IP Rules

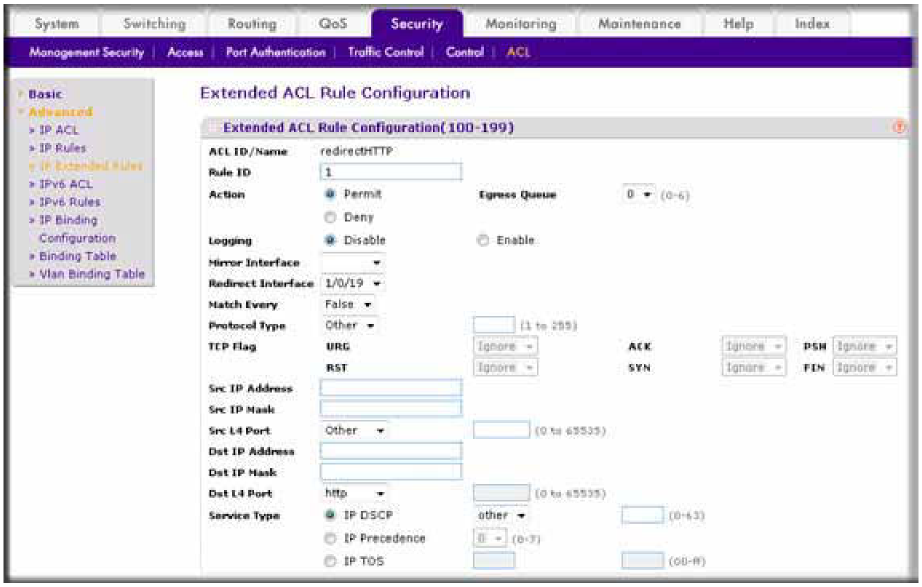
ACL ID/NAME	redirectHTTP

Extended ACL Rule Table

□	Rule ID	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Match Every	Protocol Keyword	TCP Flag	Source IP Addres

No rules have been configured for this ACL.

b. Click **Add**, and the Extended ACL Rule Configuration screen displays.



Extended ACL Rule Configuration

Extended ACL Rule Configuration(100-199)

ACL ID/Name	redirectHTTP					
Rule ID	1					
Action	● Permit	Egress Queue	0 (0-6)			
	○ Deny					
Logging	● Disable	○ Enable				
Mirror Interface						
Redirect Interface	1/0/19					
Match Every	False					
Protocol Type	Other	(1 to 255)				
TCP Flag	URG	Ignore	ACK	Ignore	PSH	Ignore
	RST	Ignore	SYN	Ignore	FIN	Ignore
Src IP Address						
Src IP Mask						
Src L4 Port	Other	(0 to 65535)				
Dst IP Address						
Dst IP Mask						
Dst L4 Port	http	(0 to 65535)				
Service Type	● IP DSCP	other	(0-63)			
	○ IP Precedence	0 (0-7)				
	○ IP TOS		(00-ff)			

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**.

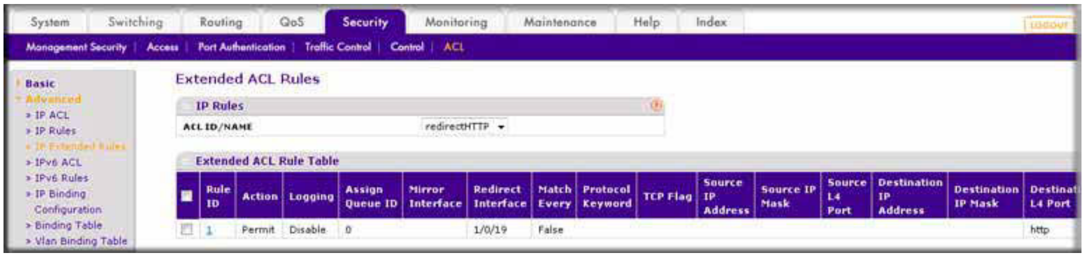
f. In the **Dst L4 Por**t list, select **http**.

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.



Extended ACL Rules

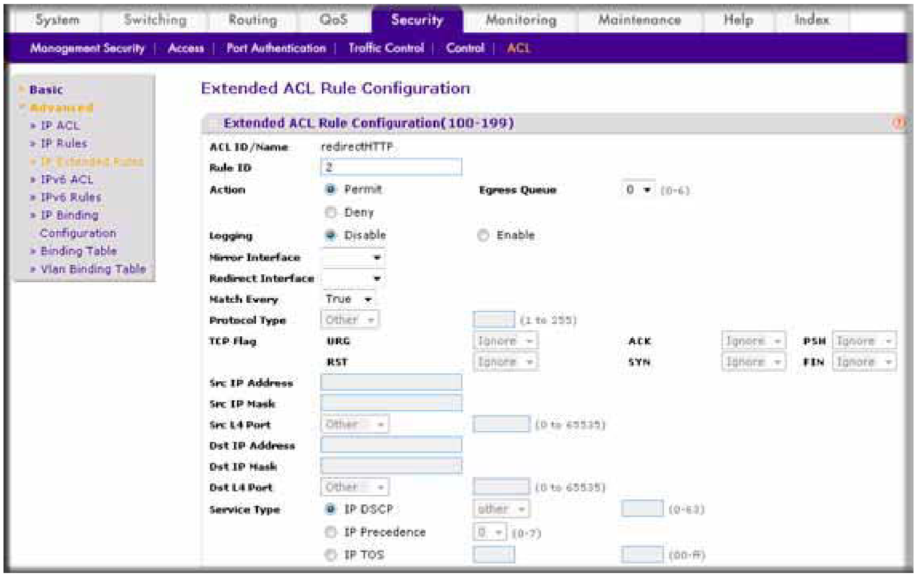
IP Rules

ACL ID/NAME redirectHTTP

Extended ACL Rule Table

□	Rule ID	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source IP Mask	Source L4 Port	Destination IP Address	Destination IP Mask	Destinat L4 Port
□	1	Permit	Disable	0		1/0/19	False								http

b. Click **Add**, and the Extended ACL Rule Configuration screen displays.



Extended ACL Rule Configuration

Extended ACL Rule Configuration(100-199)

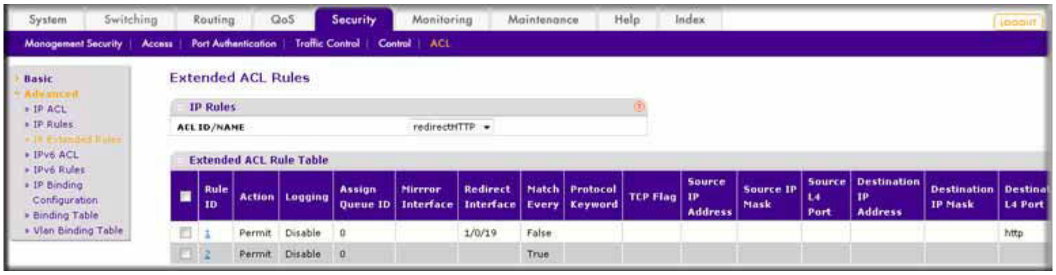
ACL ID/Name	redirectHTTP					
Rule ID	2					
Action	● Permit	Egress Queue	0 (0-6)			
	○ Deny					
Logging	● Disable	○ Enable				
Mirror Interface						
Redirect Interface						
Match Every	True					
Protocol Type	Other	(1 to 255)				
TCP Flag	URG	Ignore	ACK	Ignore	PSH	Ignore
	RST	Ignore	SYN	Ignore	FIN	Ignore
Src IP Address						
Src IP Mask						
Src L4 Port	Other	(0 to 65535)				
Dst IP Address						
Dst IP Mask						
Dst L4 Port	Other	(0 to 65535)				
Service Type	● IP DSCP	other	(0-63)			
	○ IP Precedence	0 (0-7)				
	○ IP TOS		(00-ff)			

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.



Extended ACL Rules

IP Rules

ACL ID/NAME: redirectHTTP

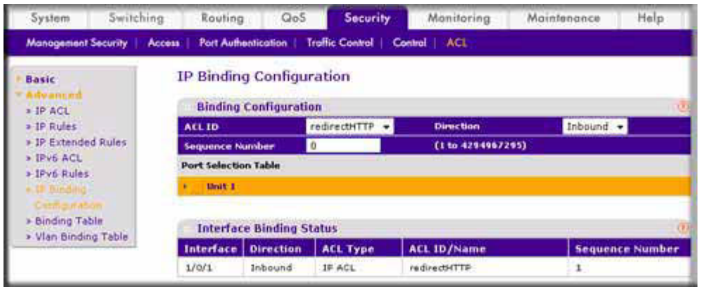
Extended ACL Rule Table

□	Rule ID	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source IP Mask	Source L4 Port	Destination IP Address	Destination IP Mask	Destina L4 Port
□	1	Permit	Disable	0		1/0/19	False								http
□	2	Permit	Disable	0			True								

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

Binding Configuration

ACL ID	redirectHTTP	Direction	Inbound
Sequence Number	0	(1 to 4294967295)	

Port Selection Table

Unit 1

Interface Binding Status

Interface	Direction	ACL Type	ACL ID/Name	Sequence Number
1/0/1	Inbound	IP ACL	redirectHTTP	1

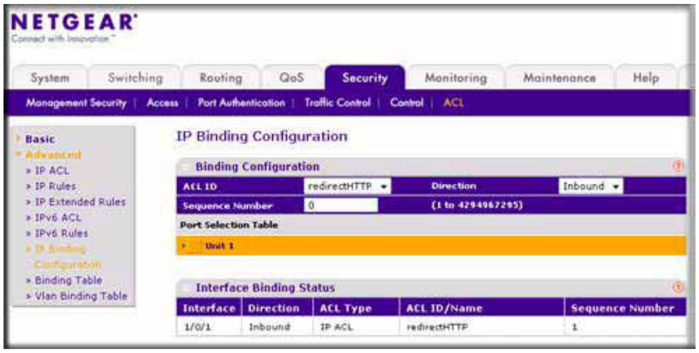
b. In the **Sequence Number** field, enter **1**.

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.



IP Binding Configuration

Binding Configuration

ACL ID: redirectHTTP
Direction: Inbound
Sequence Number: 0 (1 to 4294967295)

Port Selection Table

Unit 1

Interface Binding Status

Interface	Direction	ACL Type	ACL ID/Name	Sequence Number
1/0/1	Inbound	IP ACL	redirectHTTP	1

Configure IPv6 ACLs

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

- Source IPv6 prefix
- Destination IPv6 prefix
- Protocol number
- Source Layer 4 port
- Destination Layer 4 port
- DSCP value
- Flow label

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

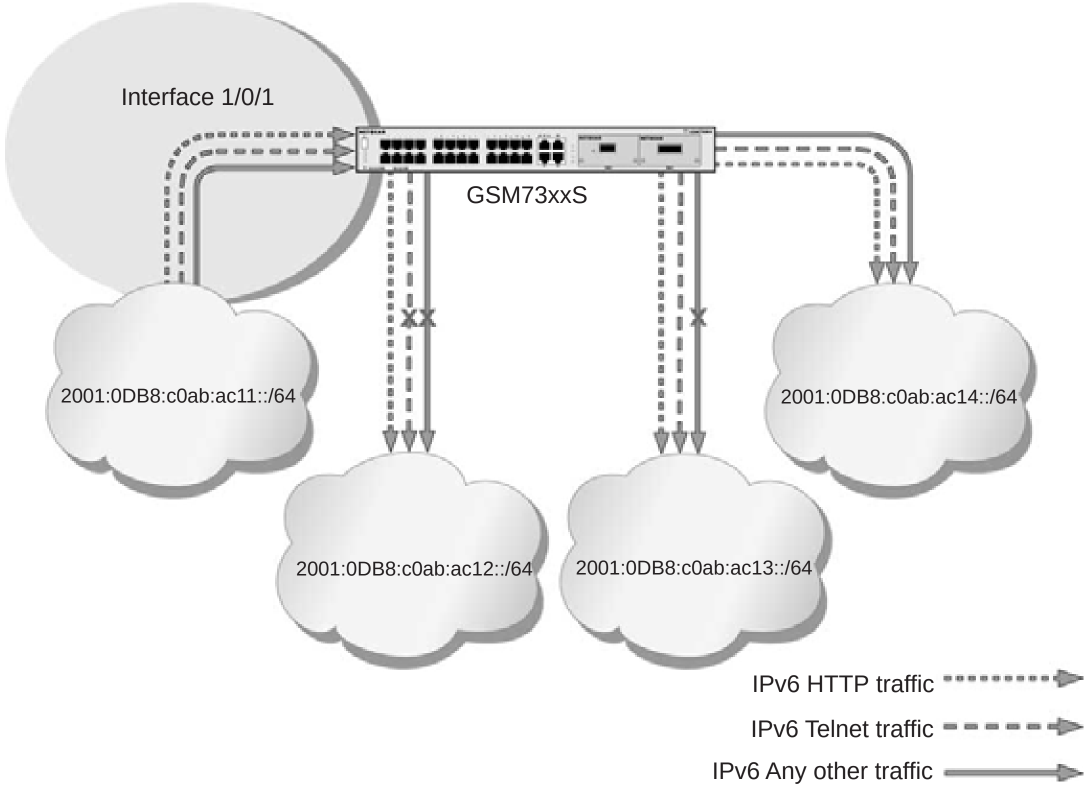


Figure 14. IPv6 ACLs

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

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

CLI: Configure an IPv6 ACL

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

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

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

- Permit IPv6 HTTP traffic to *any* destination network from the source network 2001:DB8:C0AB:AC11::/64.

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

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

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

4. View the configuration.

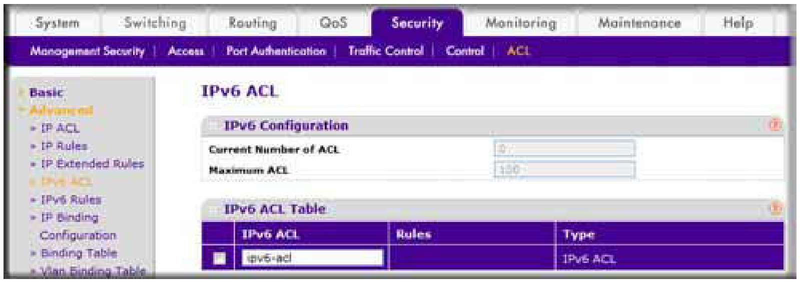
```
(Netgear Switch) #show ipv6 access-lists
Current number of all ACLs: 1  Maximum number of all ACLs: 100
IPv6 ACL Name          Rules   Direction     Interface(s)     VLAN(s)

---------------------  -----  ---------     -------------   -------------------
ipv6-acl                 3     inbound        1/0/1
(Netgear Switch) #show ipv6 access-lists ipv6-acl

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

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

Rule Number: 2
Action......................................... permit
Protocol....................................... 6(tcp)
Source IP Address.............................. 2001:DB8:C0AB:AC11::/64
Destination IP Address......................... 2001:DB8:C0AB:AC13::/64
Destination L4 Port Keyword.................... 23(telnet)
```

```
Rule Number: 3
Action....................................... permit
Protocol..................................... 6(tcp)
Source IP Address............................ 2001:DB8:C0AB:AC11::/64
Destination L4 Port Keyword.................. 80(www/http)
```

Web Interface: Configure an IPv6 ACL

1. Create the access control list with the name ipv6-acl
   a. Select **Security > ACL > Advanced > IPv6 ACL**.
   b. In the IPv6 ACL Table, in the **IPv6 ACL** field, enter **ipv6-acl**.

   A screen similar to the following displays.



IPv6 ACL

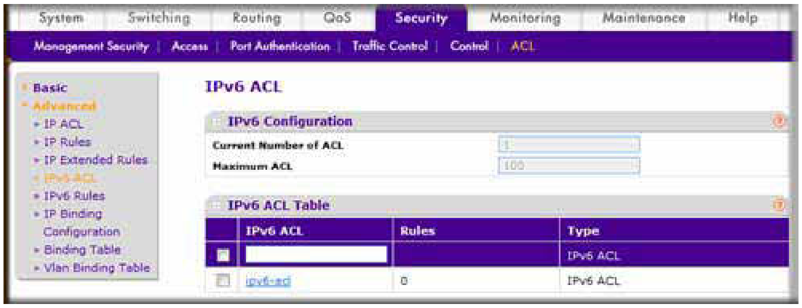
IPv6 Configuration

Current Number of ACL	0
Maximum ACL	100

IPv6 ACL Table

	IPv6 ACL	Rules	Type
■	ipv6-acl		IPv6 ACL

   c. Click **Add**. A screen similar to the following displays.



IPv6 ACL

IPv6 Configuration

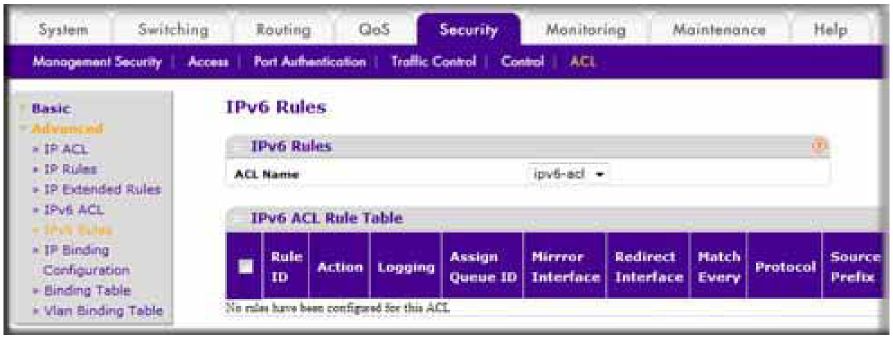
Current Number of ACL	1
Maximum ACL	100

IPv6 ACL Table

	IPv6 ACL	Rules	Type
■			IPv6 ACL
□	ipv6-acl	0	IPv6 ACL

2. Define the first rule (1 of 3).
   a. Select **Security > ACL > Advanced > IPv6 Rules**.

   A screen similar to the following displays.



IPv6 Rules

IPv6 Rules

ACL Name	ipv6-acl ▾

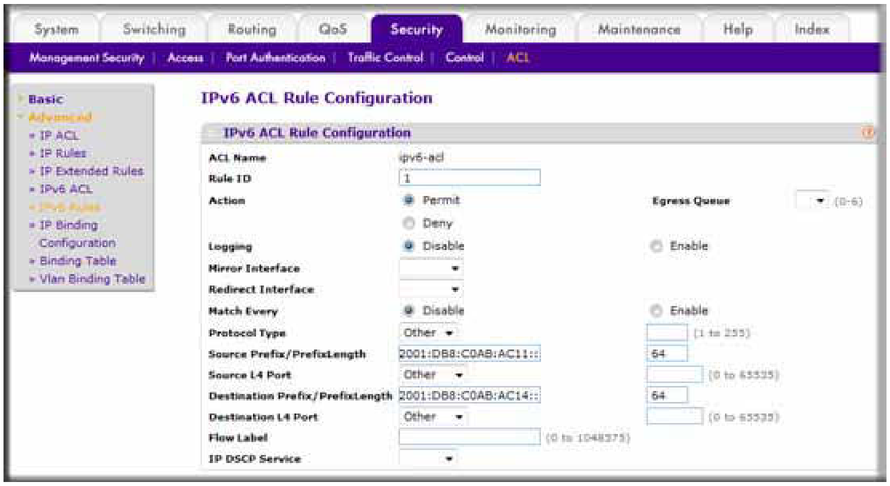
IPv6 ACL Rule Table

■	Rule ID	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Match Every	Protocol	Source Prefix

No rules have been configured for this ACL.

- **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

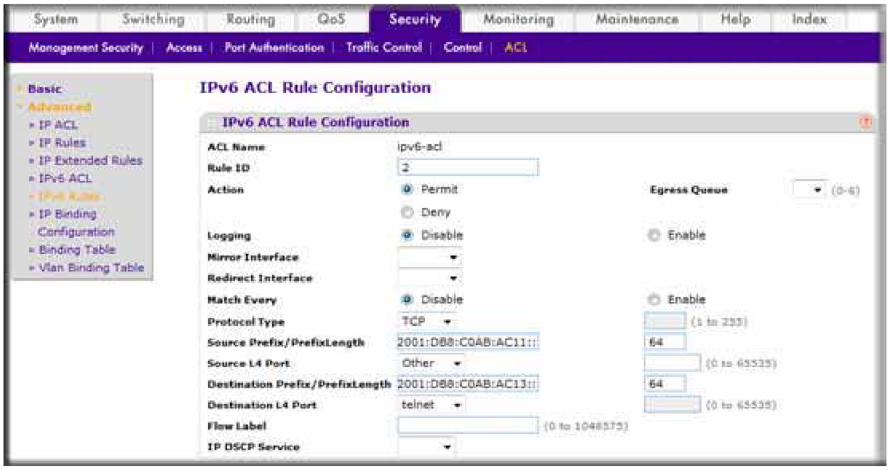
IPv6 ACL Rule Configuration

ACL Name ipv6-acl
Rule ID 1
Action ● Permit ○ Deny
Egress Queue (0-6)
Logging ● Disable ○ Enable
Mirror Interface
Redirect Interface
Match Every ● Disable ○ Enable
Protocol Type Other (1 to 255)
Source Prefix/PrefixLength 2001:DB8:C0AB:AC11:: 64
Source L4 Port Other (0 to 65535)
Destination Prefix/PrefixLength 2001:DB8:C0AB:AC14:: 64
Destination L4 Port Other (0 to 65535)
Flow Label (0 to 1048575)
IP DSCP Service

- **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

IPv6 ACL Rule Configuration

ACL Name	ipv6-acl		
Rule ID	2		
Action	● Permit ○ Deny	Egress Queue	(0-6)
Logging	● Disable	○ Enable	
Mirror Interface			
Redirect Interface			
Match Every	● Disable	○ Enable	
Protocol Type	TCP	(1 to 255)	
Source Prefix/PrefixLength	2001:DB8:C0AB:AC11::	64	
Source L4 Port	Other	(0 to 65535)	
Destination Prefix/PrefixLength	2001:DB8:C0AB:AC13::	64	
Destination L4 Port	telnet	(0 to 65535)	
Flow Label	(0 to 1048575)		
IP DSCP Service			

i. Click **Apply**.

4. Add Rule 3.

a. In the **Rule ID** field, enter **3**.

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

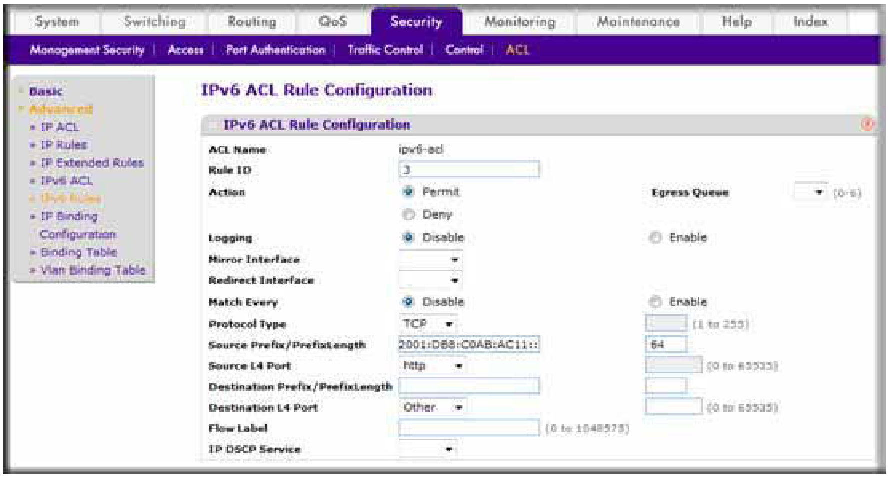
c. In the **Protocol Type** list, select **TCP**.

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

IPv6 ACL Rule Configuration

ACL Name	ipv6-acl		
Rule ID	3		
Action	● Permit ○ Deny	Egress Queue	(0-6)
Logging	● Disable	○ Enable	
Mirror Interface			
Redirect Interface			
Match Every	● Disable	○ Enable	
Protocol Type	TCP	(1 to 255)	
Source Prefix/PrefixLength	2001:DB8:C0AB:AC11::	64	
Source L4 Port	http	(0 to 65535)	
Destination Prefix/PrefixLength			
Destination L4 Port	Other	(0 to 65535)	
Flow Label	(0 to 1048575)		
IP DSCP Service			

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**.

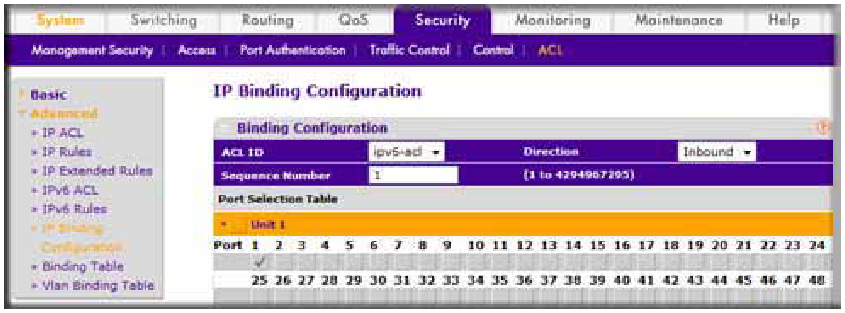
b. In the **ACL ID** list, select **ipv6-acl**.

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

Binding Configuration

ACL ID: ipv6-acl
Direction: Inbound
Sequence Number: 1 (1 to 4294967295)

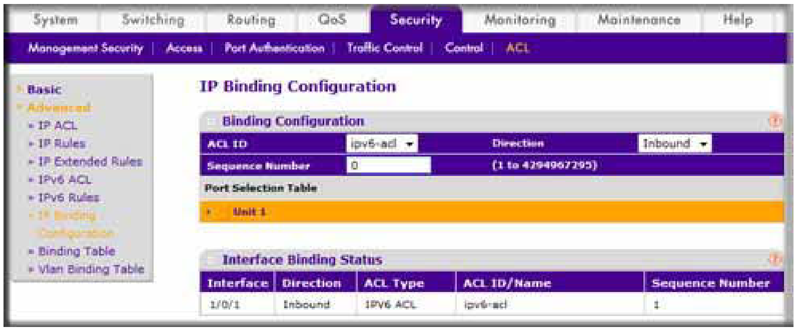
Port Selection Table

Unit 1

Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
✓
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48

f. Click **Apply**.

A screen similar to the following displays.



IP Binding Configuration

Binding Configuration

ACL ID: ipv6-acl
Direction: Inbound
Sequence Number: 0 (1 to 4294967295)

Port Selection Table

Unit 1

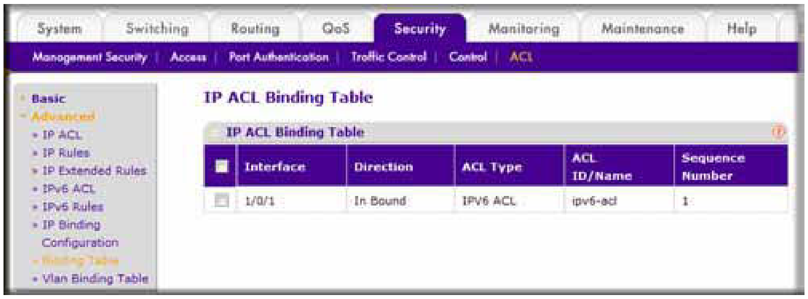
Interface Binding Status

Interface	Direction	ACL Type	ACL ID/Name	Sequence Number
1/0/1	Inbound	IPV6 ACL	ipv6-acl	1

6. View the binding table.

Select **Security > ACL > Advanced > Binding Table**.

A screen similar to the following displays.



IP ACL Binding Table

IP ACL Binding Table

■	Interface	Direction	ACL Type	ACL ID/Name	Sequence Number
□	1/0/1	In Bound	IPV6 ACL	ipv6-acl	1

CoS Queuing

8

Class of Service Queuing

This chapter includes the following sections:

- *QoS Queuing Concepts*
- *Show classofservice Trust*
- *Set classofservice Trust Mode*
- *Show classofservice IP-Precedence Mapping*
- *Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode*
- *Set CoS Trust Mode for an Interface*
- *Configure Traffic Shaping*

QoS Queuing Concepts

This chapter describes Class of Service (CoS) queue mapping, CoS Configuration, and traffic shaping features. 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, rail Drop vs. WRED

Only if per-queue configuration is not supported

- WRED decay exponent
- Traffic shaping for an entire interface

Show classofservice Trust

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

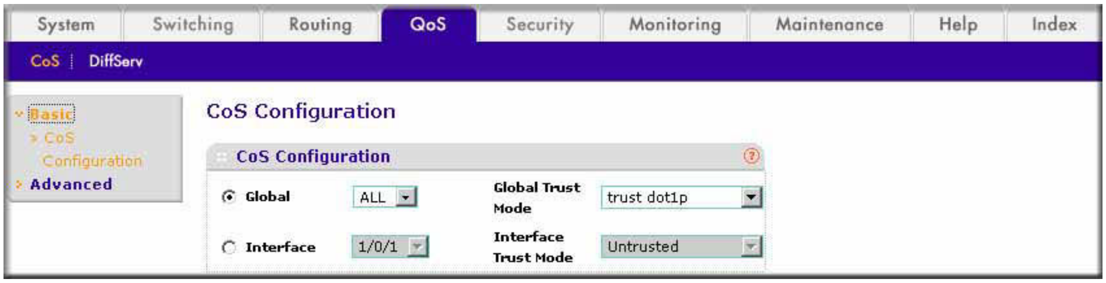
CLI: Show classofservice Trust

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

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

Web Interface: Show classofservice Trust

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



CoS Configuration

CoS Configuration

● Global ALL — Global Trust Mode: trust dot1p

○ Interface 1/0/1 — Interface Trust Mode: Untrusted

Set classofservice Trust Mode

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

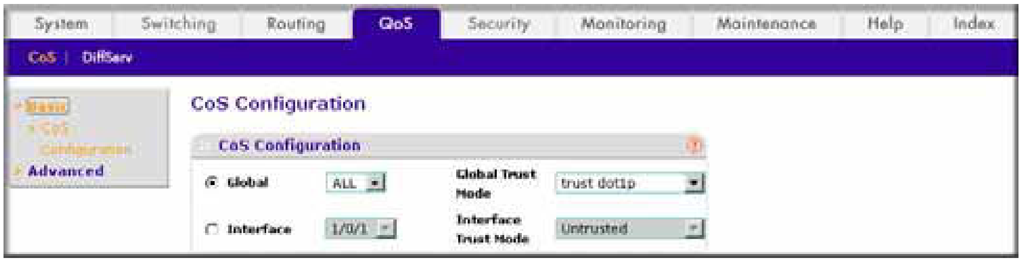
CLI: Set classofservice Trust Mode

```
(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

CoS Configuration

● Global ALL | Global Trust Mode trust dot1p

○ Interface 1/0/1 | Interface Trust Mode Untrusted

2. Select the **Global** radio button.
3. In the **Global Trust Mode** list, select **trust dot1p**.
4. Click **Apply** to save the settings.

Show classofservice IP-Precedence Mapping

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

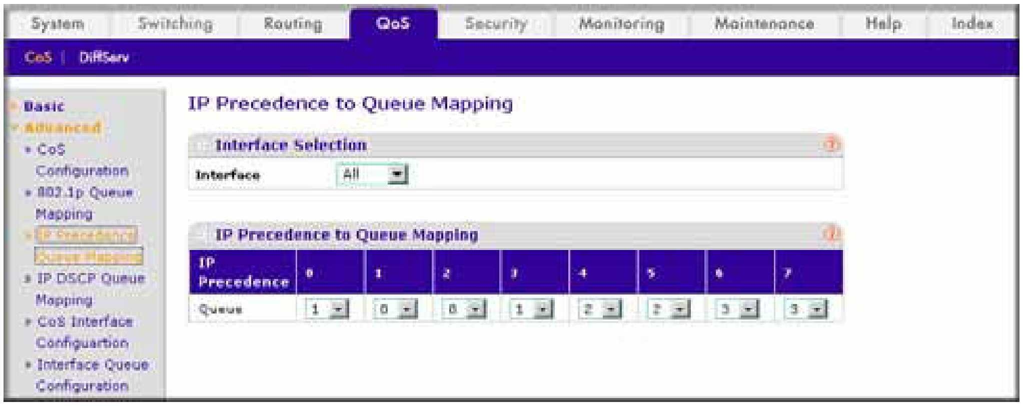
CLI: Show classofservice IP-Precedence Mapping

```
(Netgear Switch) #show classofservice ip-precedence-mapping
IP Precedence     Traffic Class
-------------     -------------
    0                 1
    1                 0
    2                 0
    3                 1
    4                 2
    5                 2
    6                 3
    7                 3
```

Web Interface: Show classofservice ip-precedence Mapping

1. Select **QoS > CoS > Advanced > IP Precedence Queue Mapping**.

A screen similar to the following displays.



IP Precedence to Queue Mapping

Interface Selection

Interface: All

IP Precedence to Queue Mapping

IP Precedence	0	1	2	3	4	5	6	7
Queue	1	0	0	1	2	2	3	3

2. In the Interface list, select **All**.

   The global IP precedence to queue mapping is displayed.

3. In the **Interface** list, select the specific interface (such as **1/0/1**).

   The IP precedence to queue mapping of the interface is displayed.

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

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

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

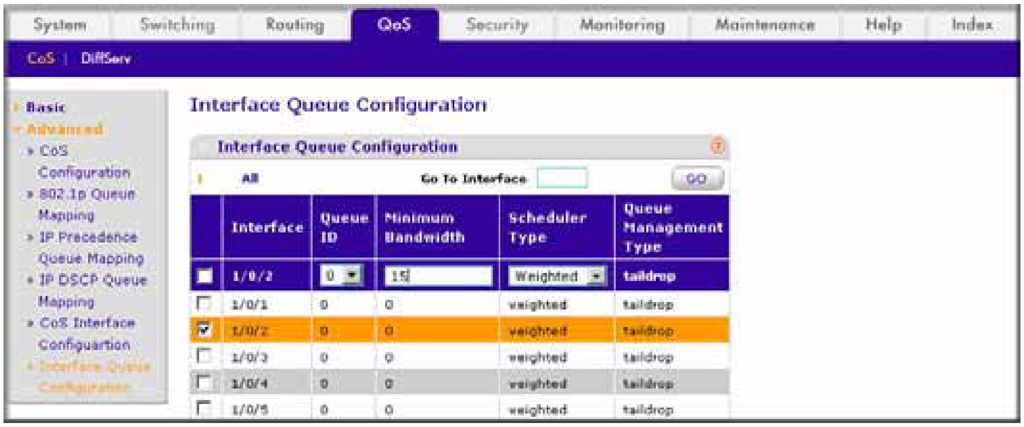
```
(Netgear Switch) (Config)#cos-queue min-bandwidth?
<bw-0>                    Enter the minimum bandwidth percentage for Queue 0.
(Netgear Switch) (Config)#cos-queue min-bandwidth 15
Incorrect input! Use 'cos-queue min-bandwidth <bw-0>..<bw-7>.
(Netgear Switch) (Config)#cos-queue min-bandwidth 15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

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

1. For Interface 1/0/2, set the minimum bandwidth to 15 for queue 0.

   a. Select **QoS > CoS > Advanced > Interface Queue Configuration**.

   A screen similar to the following displays.



Interface Queue Configuration

Interface Queue Configuration

All   Go To Interface

	Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
☐	1/0/2	0	15	Weighted	taildrop
☐	1/0/1	0	0	weighted	taildrop
☑	1/0/2	0	0	weighted	taildrop
☐	1/0/3	0	0	weighted	taildrop
☐	1/0/4	0	0	weighted	taildrop
☐	1/0/5	0	0	weighted	taildrop

   b. In the **Queue ID** list, select **0**.

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

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

   d. Enter the following information:

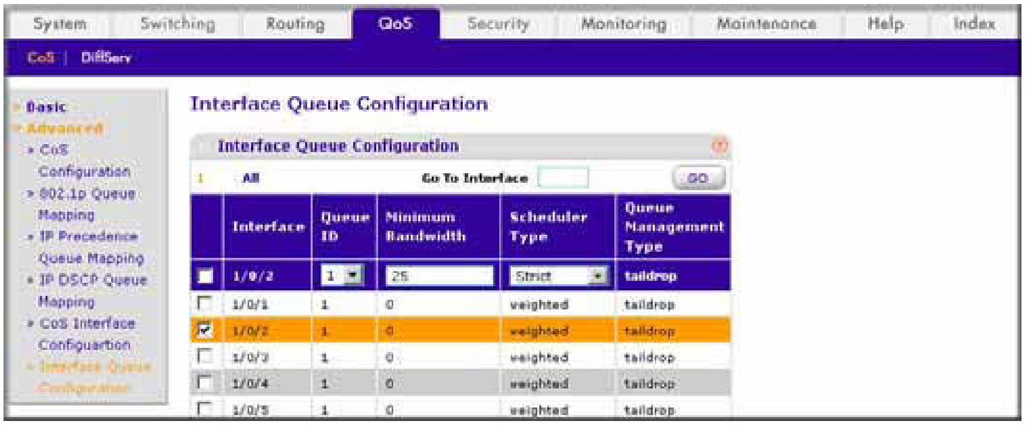
   - In the **Minimum Bandwidth** field, enter **15**.
   - In the **Scheduler Type** list, select **Weighted**.

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

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

   a. Select **QoS > CoS > Advanced > Interface Queue Configuration**.

A screen similar to the following displays.



Interface Queue Configuration

Interface Queue Configuration

1 All Go To Interface

	Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
□	1/0/2	1	25	Strict	taildrop
□	1/0/1	1	0	weighted	taildrop
☑	1/0/2	1	0	weighted	taildrop
□	1/0/3	1	0	weighted	taildrop
□	1/0/4	1	0	weighted	taildrop
□	1/0/5	1	0	weighted	taildrop

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

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

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

d. Enter the following information:

   - In the **Minimum Bandwidth** field, enter **25**.
   - In the **Scheduler Type** list, select **Strict**.

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

Set CoS Trust Mode for an Interface

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

CLI: Set CoS Trust Mode for an Interface

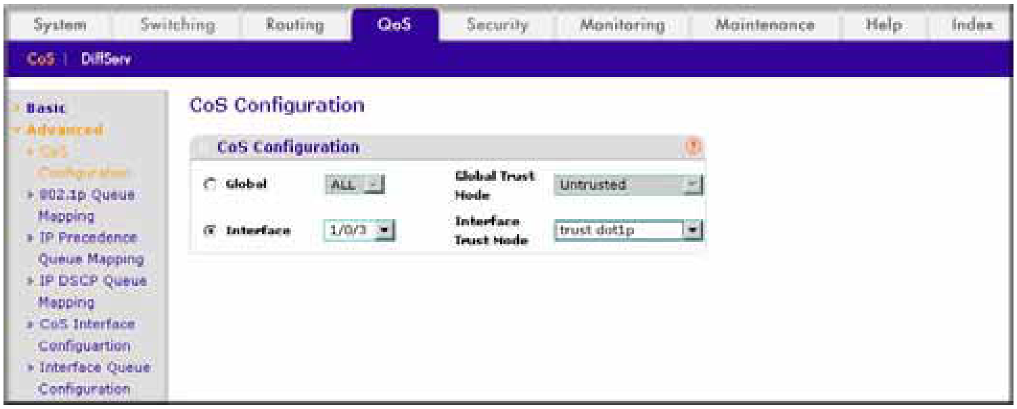
```
(Netgear Switch) (Interface 1/0/3)#classofservice trust?
dot1p                     Sets the Class of Service Trust Mode of an Interface
                          to 802.1p.
ip-dscp                   Sets the Class of Service Trust Mode of an Interface
                          to IP DSCP.
(Netgear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



CoS Configuration

CoS Configuration

○ Global ALL | Global Trust Mode Untrusted

● Interface 1/0/3 | Interface Trust Mode trust dot1p

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

Configure Traffic Shaping

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

The <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

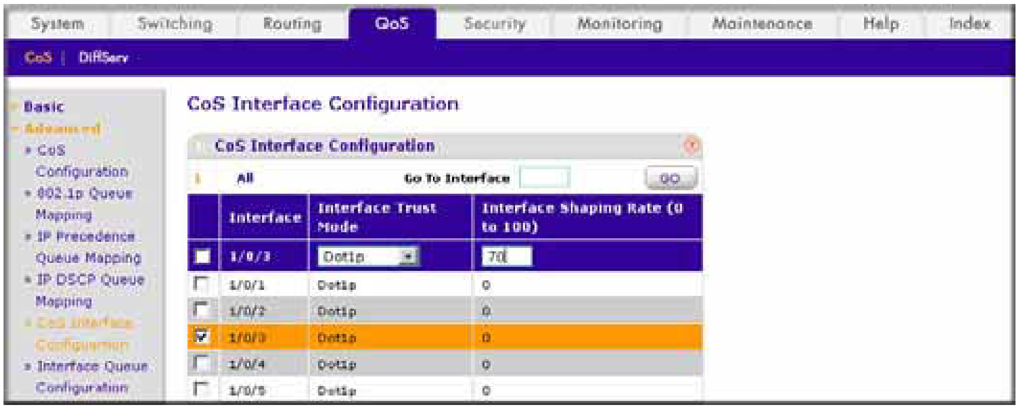
```
(Netgear Switch) (Config)#traffic-shape?
<bw>                     Enter the shaping bandwidth percentage from 0 to 100
                         in increments of 5.
(Netgear Switch) (Config)#traffic-shape 70?
<cr>                     Press Enter to execute the command.
(Netgear Switch) (Config)#traffic-shape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



	Interface	Interface Trust Mode	Interface Shaping Rate (0 to 100)
□	1/0/3	Dot1p	70
□	1/0/1	Dot1p	0
□	1/0/2	Dot1p	0
☑	1/0/3	Dot1p	0
□	1/0/4	Dot1p	0
□	1/0/5	Dot1p	0

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

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

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

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

9. DiffServ

9

Differentiated Services

This chapter includes the following sections:

- *DiffServ Concepts*
- *Configure DiffServ*
- *DiffServ for VoIP*
- *Auto VoIP*
- *DiffServ for IPv6*
- *Color Conform Policy*

DiffServ Concepts

Differentiated services (DiffServ) is one technique for implementing Quality of Service (QoS) policies. Using DiffServ in your network allows you to directly configure the relevant parameters on the switches and routers rather than using a resource reservation protocol.This section explains how to configure the ProSAFE M4100 Managed Switches 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 M4100 Managed Switch, DiffServ allows you to control what traffic is accepted and what traffic is discarded.

How you configure DiffServ support on a M4100 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 M4100 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.

Configure DiffServ

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

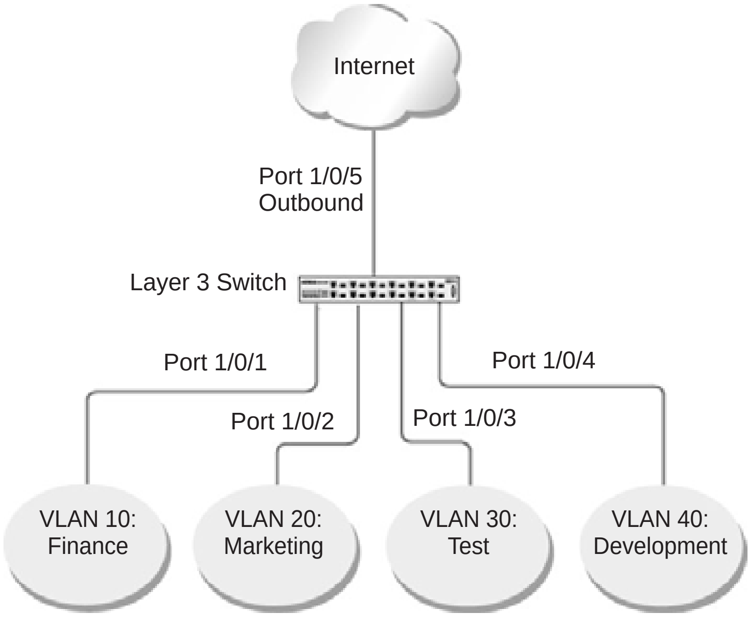


Figure 15. Class B subnet with differentiated services

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.

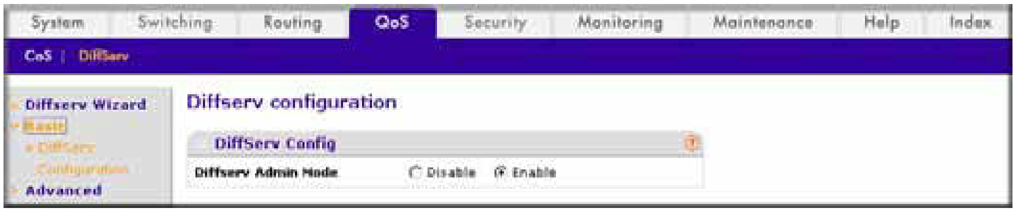
```
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#cos-queue min-bandwidth 0 25 25 25 25 0 0 0
(Netgear Switch) (Interface 1/0/5)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Configure DiffServ

1. Enable Diffserv.

   a. Select **QoS > DiffServ > Basic > DiffServ Configuration**.

   A screen similar to the following displays.



Diffserv Admin Mode ○ Disable ● Enable

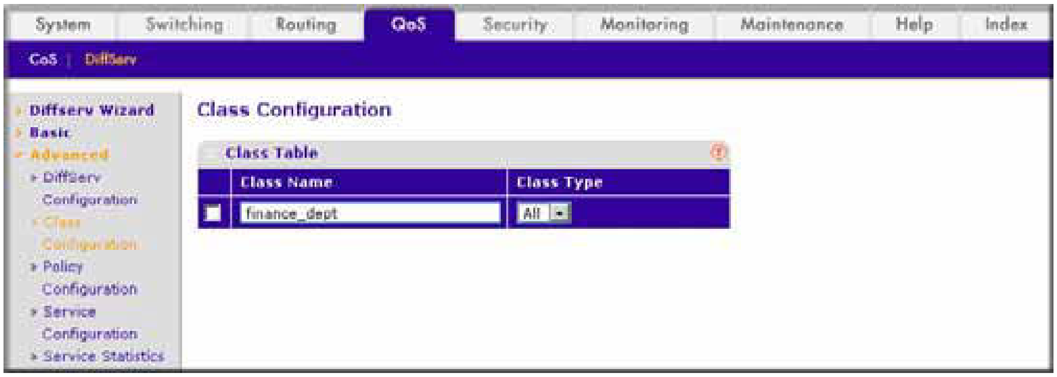
   b. For Diffserv Admin Mode, select the **Enable** radio button.

   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

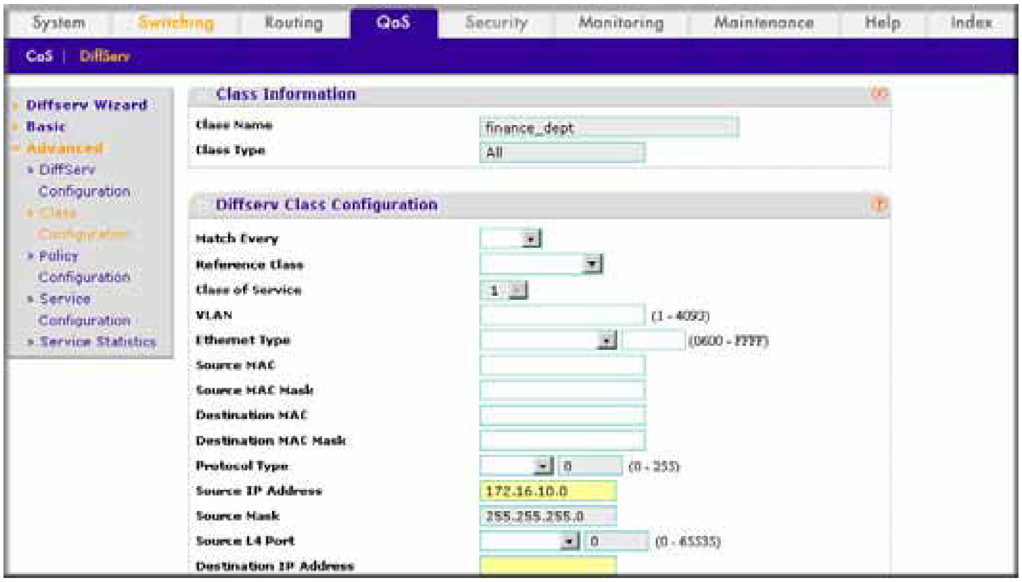
Class Table

	Class Name	Class Type
□	finance_dept	All

   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.



Class Information

Class Name	finance_dept	
Class Type	All	

Diffserv Class Configuration

Match Every		
Reference Class		
Class of Service	1	
VLAN		(1 - 4093)
Ethernet Type		(0600 - FFFF)
Source MAC		
Source MAC Mask		
Destination MAC		
Destination MAC Mask		
Protocol Type	0	(0 - 255)
Source IP Address	172.16.10.0	
Source Mask	255.255.255.0	
Source L4 Port	0	(0 - 65535)
Destination IP Address		

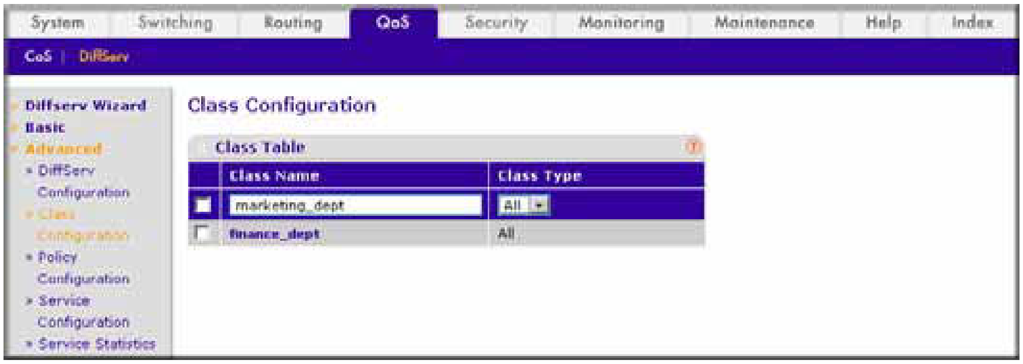
   e. Under Diffserv Class Configuration, enter the following information:
      - In the **Source IP Address** field, enter **172.16.10.0**.
      - In the **Source Mask** field, enter **255.255.255.0**.

   f. Click **Apply**.

3. Create the class marketing_dept:

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

A screen similar to the following displays.



Class Configuration

Class Table

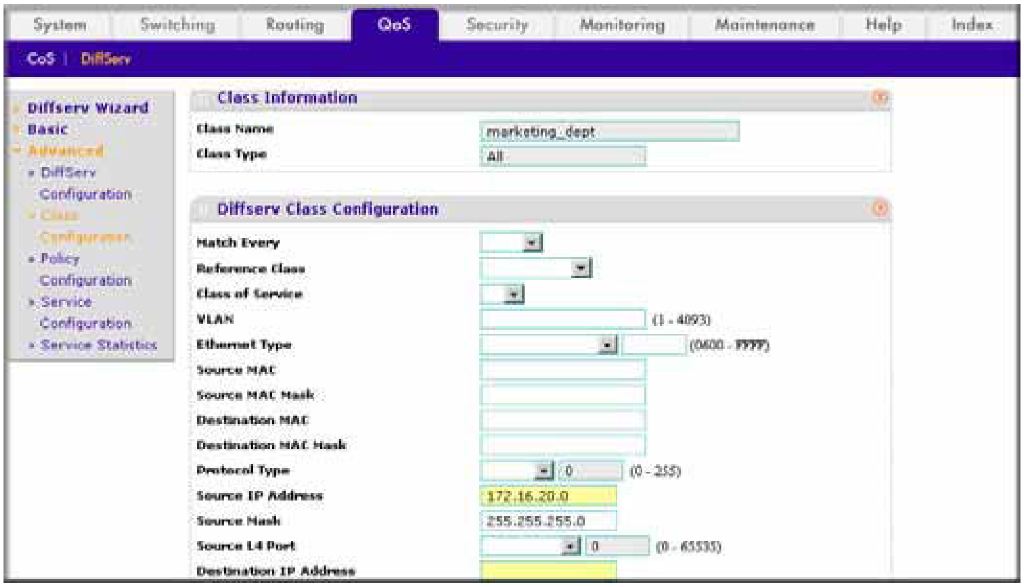
	Class Name	Class Type
☐	marketing_dept	All
☐	finance_dept	All

b. Enter the following information:

- In the **Class Name** field, enter **marketing_dept**.
- In the **Class Type** list, select **All**.

c. Click **Add** to create a new class marketing_dept.

d. Click **marketing_dept** to configure this class.



Class Information

Class Name	marketing_dept
Class Type	All

Diffserv Class Configuration

Match Every		
Reference Class		
Class of Service		
VLAN		(1 - 4093)
Ethernet Type		(0600 - FFFF)
Source MAC		
Source MAC Mask		
Destination MAC		
Destination MAC Mask		
Protocol Type	0	(0 - 255)
Source IP Address	172.16.20.0	
Source Mask	255.255.255.0	
Source L4 Port	0	(0 - 65535)
Destination IP Address		

e. Under Diffserv Class Configuration, enter the following information:

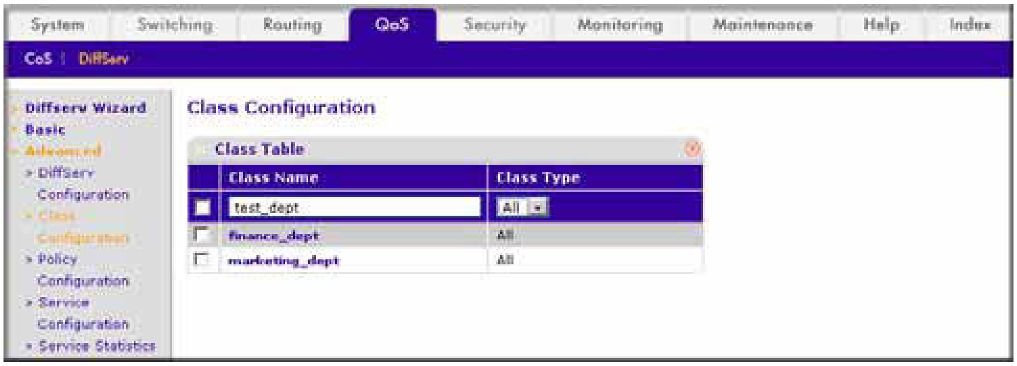
- In the **Source IP Address** field, enter **172.16.20.0**.
- In the **Source Mask** field, enter **255.255.255.0**.

f. Click **Apply**.

4. Create the class test_dept:

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

A screen similar to the following displays.



Class Configuration

Class Table

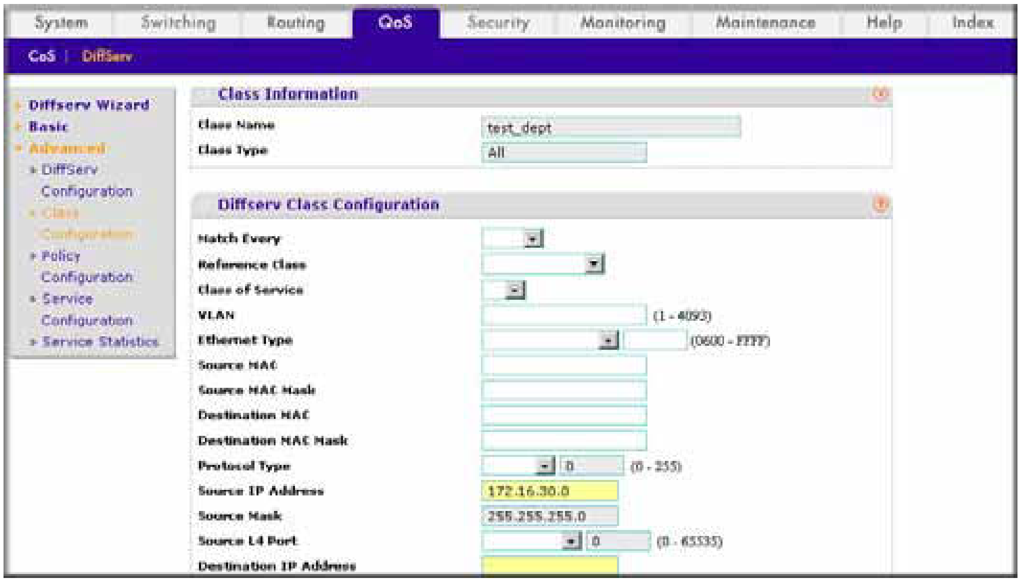
	Class Name	Class Type
□	test_dept	All
□	finance_dept	All
□	marketing_dept	All

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.



Class Information

Class Name	test_dept
Class Type	All

Diffserv Class Configuration

Match Every	
Reference Class	
Class of Service	
VLAN	(1 - 4093)
Ethernet Type	(0600 - FFFF)
Source MAC	
Source MAC Mask	
Destination MAC	
Destination MAC Mask	
Protocol Type	0 (0 - 255)
Source IP Address	172.16.30.0
Source Mask	255.255.255.0
Source L4 Port	0 (0 - 65535)
Destination IP Address	

e. Under Diffserv Class Configuration, enter the following information:

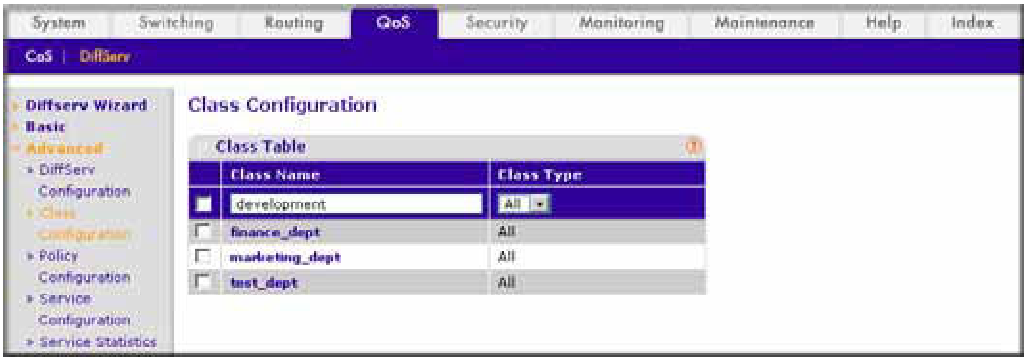
- In the **Source IP Address** field, enter **172.16.30.0**.
- In the **Source Mask** field, enter **255.255.255.0**.

f. Click **Apply**.

5. Create class development_dept.

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

A screen similar to the following displays.



Class Configuration

Class Table

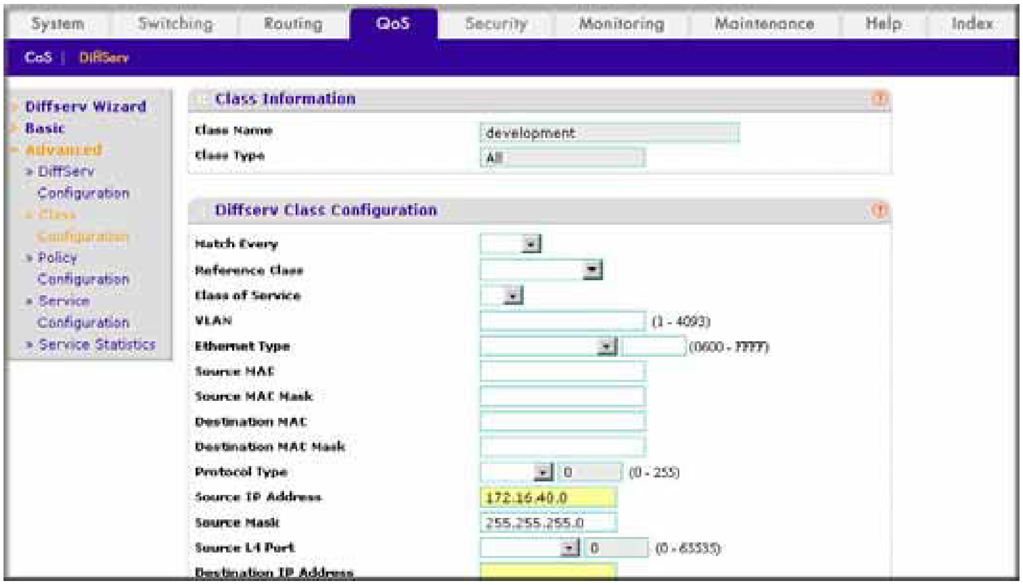
	Class Name	Class Type
□	development	All
□	finance_dept	All
□	marketing_dept	All
□	test_dept	All

b. Enter the following information:

- In the **Class Name** field, enter **development_dept**.
- In the **Class Type** list, select **All**.

c. Click the **Add** to create a new class development_dept.

d. Click **development_dept** to configure this class.



Class Information

Class Name	development
Class Type	All

Diffserv Class Configuration

Match Every		
Reference Class		
Class of Service		
VLAN		(1 - 4093)
Ethernet Type		(0600 - FFFF)
Source MAC		
Source MAC Mask		
Destination MAC		
Destination MAC Mask		
Protocol Type	0	(0 - 255)
Source IP Address	172.16.40.0	
Source Mask	255.255.255.0	
Source L4 Port	0	(0 - 65535)
Destination IP Address		

e. Under Diffserv Class Configuration, enter the following information:

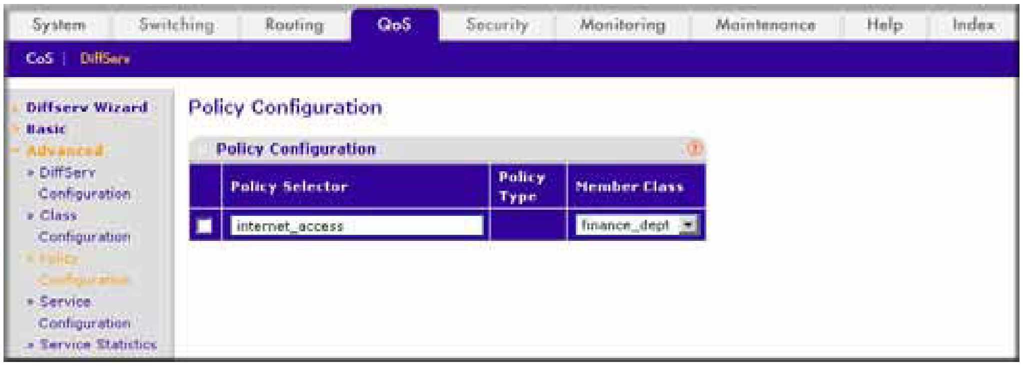
- In the **Source IP Address** field, enter **172.16.40.0**.
- In the **Source Mask** field, enter **255.255.255.0**.

f. Click **Apply**.

6. Create a policy named internet_access and add the class finance_dept to it.

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

A screen similar to the following displays.



Policy Configuration

Policy Configuration

	Policy Selector	Policy Type	Member Class
□	internet_access		finance_dept

b. Enter the following information:

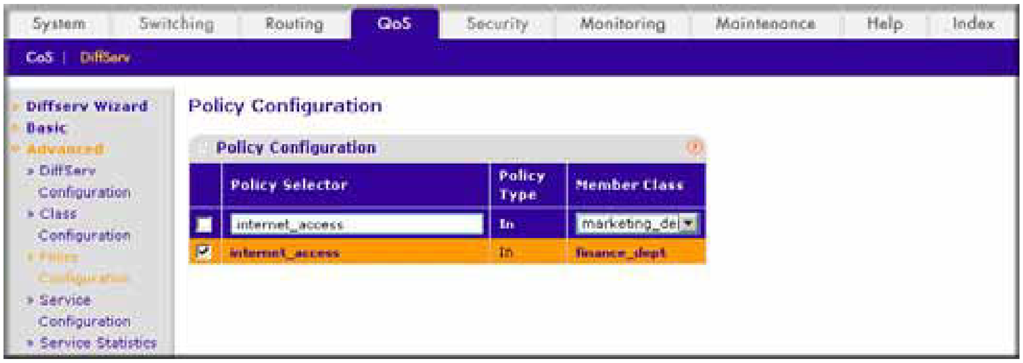
- In the **Policy Selector** field, enter **internet_access**.
- In the **Member Class** list, select the **finance_dept**.

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

Policy Configuration

	Policy Selector	Policy Type	Member Class
□	internet_access	In	marketing_de
☑	internet_access	In	finance_dept

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.

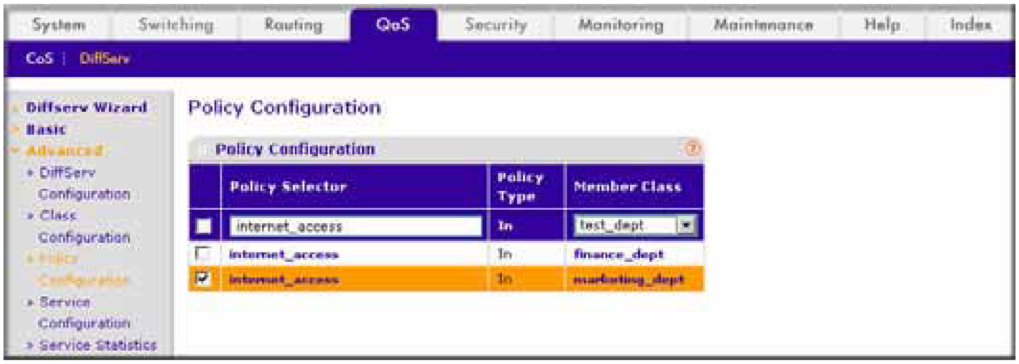
c. In the **Member Class** list, select **marketing_dept**.

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

Policy Configuration

	Policy Selector	Policy Type	Member Class
☐	internet_access	In	test_dept
☐	internet_access	In	finance_dept
☑	internet_access	In	marketing_dept

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.

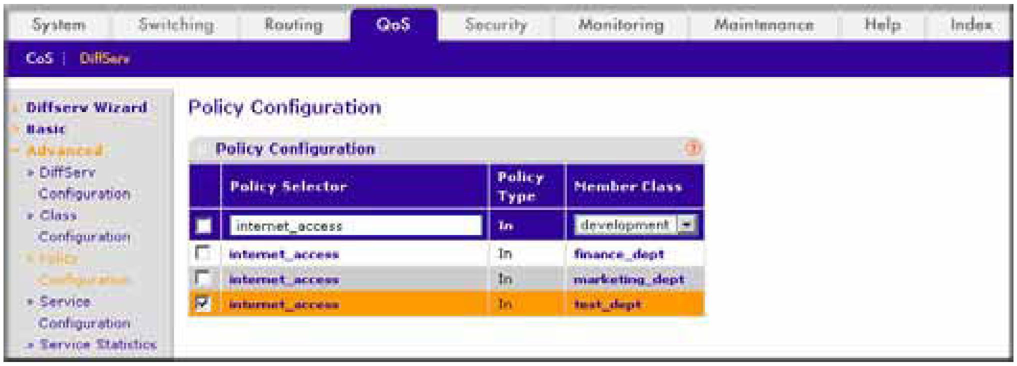
c. In the **Member Class** list, select **test_dept**.

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

Policy Configuration

	Policy Selector	Policy Type	Member Class
☐	internet_access	In	development
☐	internet_access	In	finance_dept
☐	internet_access	In	marketing_dept
☑	internet_access	In	test_dept

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.

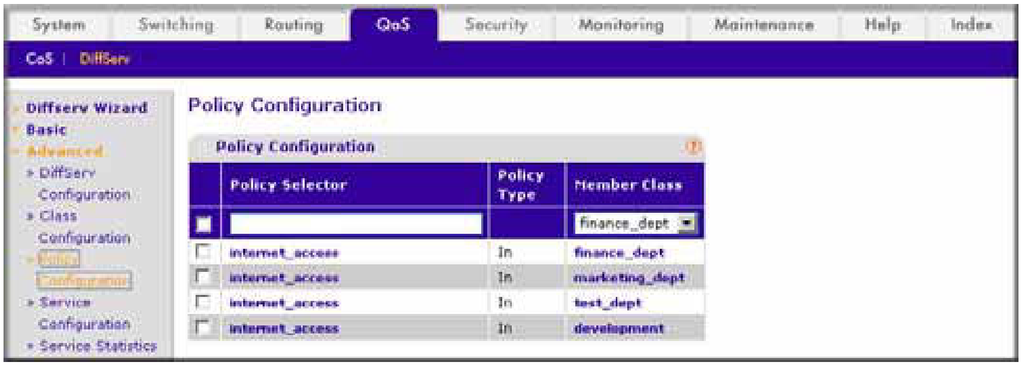
c. In the **Member Class** list, select **development_dept**.

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.



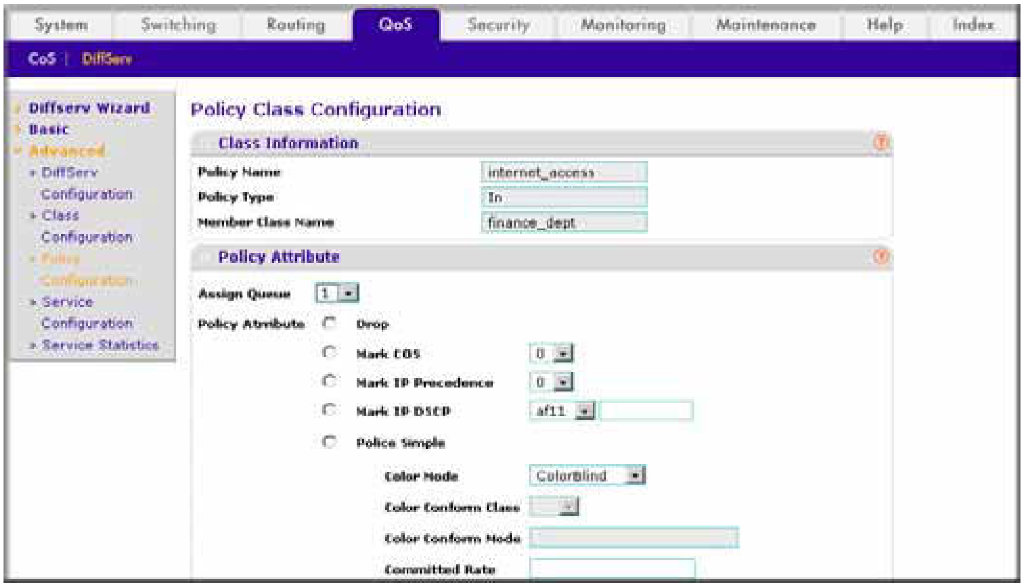
Policy Configuration

Policy Configuration

	Policy Selector	Policy Type	Member Class
☐			finance_dept
☐	internet_access	In	finance_dept
☐	internet_access	In	marketing_dept
☐	internet_access	In	test_dept
☐	internet_access	In	development

b. Click the **internet_access** check box for the member class finance_dept.

A screen similar to the following displays.



Policy Class Configuration

Class Information

Policy Name: internet_access
Policy Type: In
Member Class Name: finance_dept

Policy Attribute

Assign Queue: 1
Policy Attribute: ○ Drop
○ Mark COS 0
○ Mark IP Precedence 0
○ Mark IP DSCP af11
○ Police Simple
Color Mode: Colorblind
Color Conform Class:
Color Conform Mode:
Committed Rate:

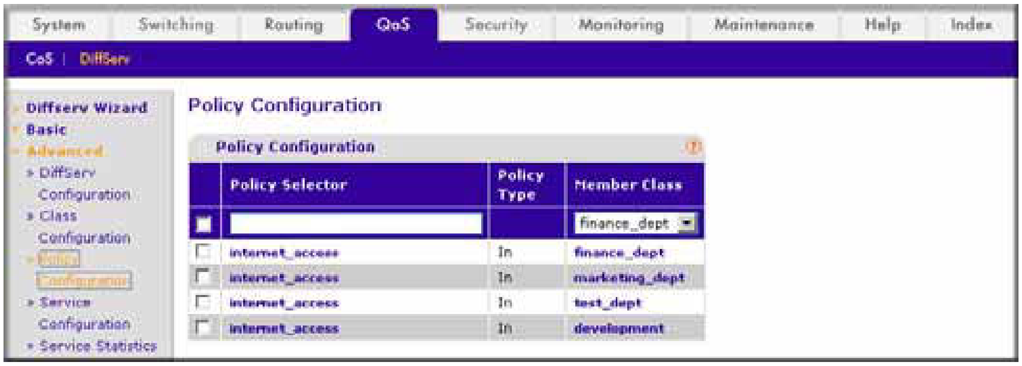
c. In the **Assign Queue** list, select **1**.

d. Click **Apply**.

11. Assign queue 2 to marketing_dept.

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

A screen similar to the following displays.



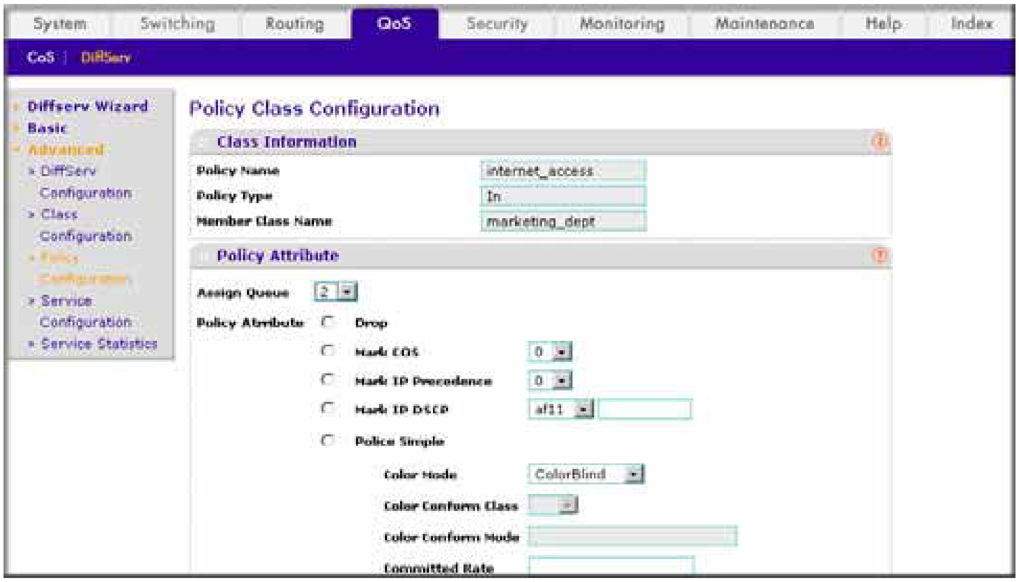
Policy Configuration

Policy Configuration

	Policy Selector	Policy Type	Member Class
☐			finance_dept
☐	internet_access	In	finance_dept
☐	internet_access	In	marketing_dept
☐	internet_access	In	test_dept
☐	internet_access	In	development

b. Click the **internet_access** check box for marketing_dept.

A screen similar to the following displays.



Policy Class Configuration

Class Information

Policy Name	internet_access
Policy Type	In
Member Class Name	marketing_dept

Policy Attribute

Assign Queue: 2

Policy Attribute:
- ○ Drop
- ○ Mark COS: 0
- ○ Mark IP Precedence: 0
- ○ Mark IP DSCP: af11
- ○ Police Simple
  - Color Mode: ColorBlind
  - Color Conform Class:
  - Color Conform Mode:
  - Committed Rate:

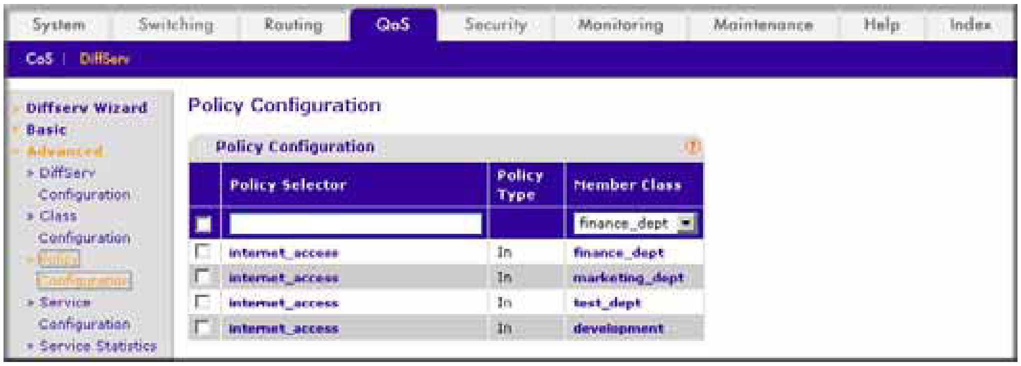
c. In the **Assign Queue** list, select **2**.

d. Click **Apply**.

12. Assign queue 3 to test_dept.

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

A screen similar to the following displays.



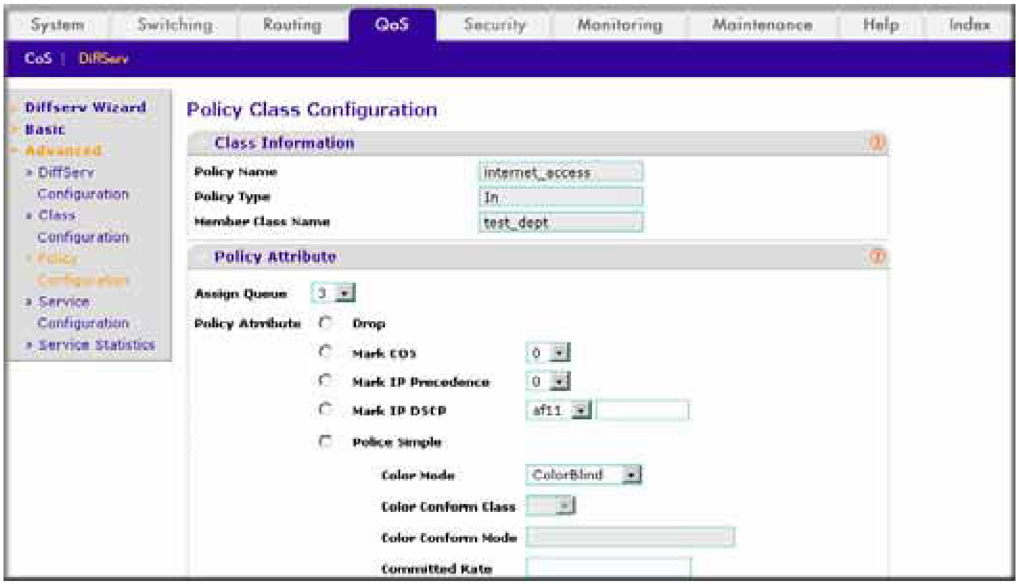
Policy Configuration

Policy Configuration

	Policy Selector	Policy Type	Member Class
□			finance_dept
□	internet_access	In	finance_dept
□	internet_access	In	marketing_dept
□	internet_access	In	test_dept
□	internet_access	In	development

b. Click the **internet_access** check mark for test_dept.

A screen similar to the following displays.



Policy Class Configuration

Class Information

Policy Name	internet_access
Policy Type	In
Member Class Name	test_dept

Policy Attribute

Assign Queue: 3

Policy Attribute:
- ○ Drop
- ○ Mark COS: 0
- ○ Mark IP Precedence: 0
- ○ Mark IP DSCP: af11
- ○ Police Simple
  - Color Mode: ColorBlind
  - Color Conform Class
  - Color Conform Mode
  - Committed Rate

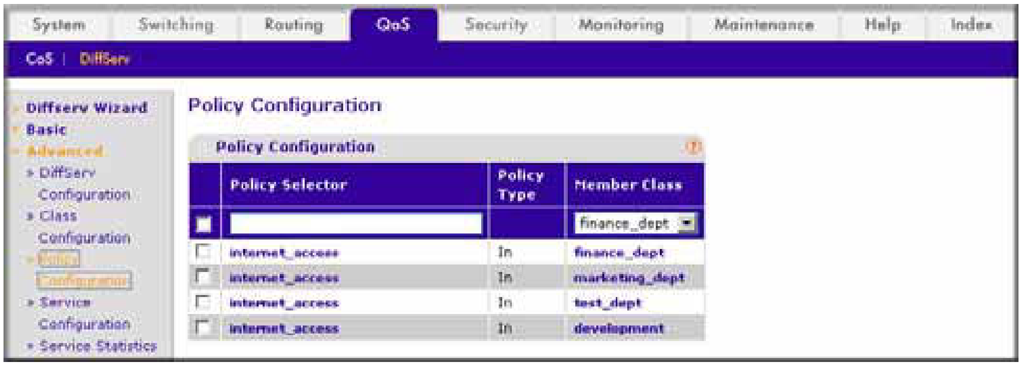
c. In the **Assign Queue** list, select **3**.

d. Click **Apply**.

13. Assign queue 4 to development_dept.

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

A screen similar to the following displays.



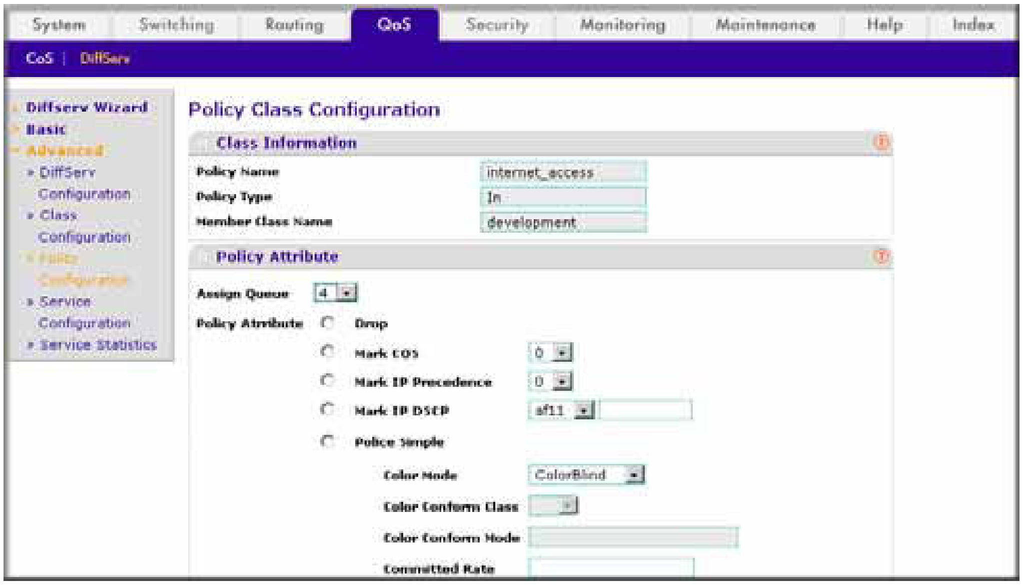
Policy Configuration

Policy Configuration

	Policy Selector	Policy Type	Member Class
☑			finance_dept
□	internet_access	In	finance_dept
□	internet_access	In	marketing_dept
□	internet_access	In	test_dept
□	internet_access	In	development

b. Click the **internet_access** check mark for development_dept.

A screen similar to the following displays.



Policy Class Configuration

Class Information

Policy Name	internet_access
Policy Type	In
Member Class Name	development

Policy Attribute

Assign Queue: 4

Policy Attribute:
○ Drop
○ Mark COS: 0
○ Mark IP Precedence: 0
○ Mark IP DSCP: af11
○ Police Simple
Color Mode: ColorBlind
Color Conform Class
Color Conform Mode
Committed Rate

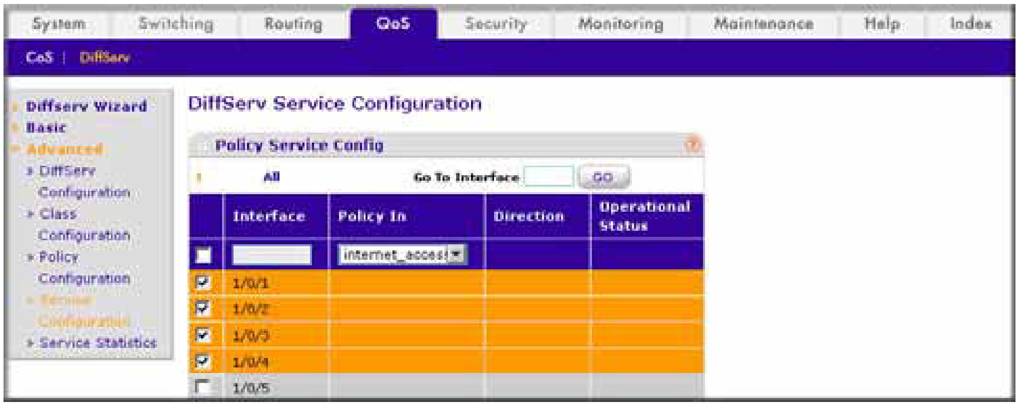
c. In the **Assign Queue** list, select **4**.

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

Policy Service Config

	Interface	Policy In	Direction	Operational Status
□		internet_access		
☑	1/0/1			
☑	1/0/2			
☑	1/0/3			
☑	1/0/4			
□	1/0/5			

b. Scroll down and select the check boxes for interfaces **1/0/1**, **1/0/2**, **1/0/3**, and **1/0/4**.

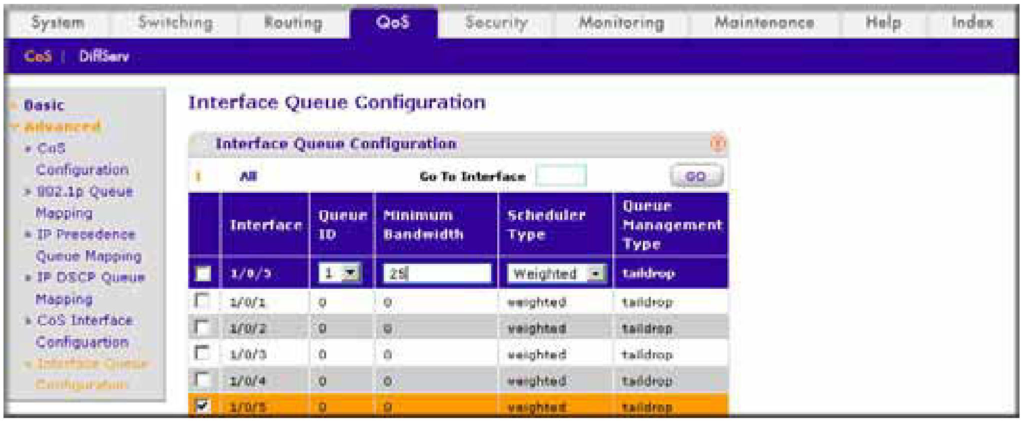
c. In the **Policy In** list, select **internet_access**.

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.



Interface Queue Configuration

Interface Queue Configuration

	Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
□	1/0/5	1	25	Weighted	taildrop
□	1/0/1	0	0	weighted	taildrop
□	1/0/2	0	0	weighted	taildrop
□	1/0/3	0	0	weighted	taildrop
□	1/0/4	0	0	weighted	taildrop
☑	1/0/5	0	0	weighted	taildrop

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

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

c. In the **Queue ID** list, select **1**.

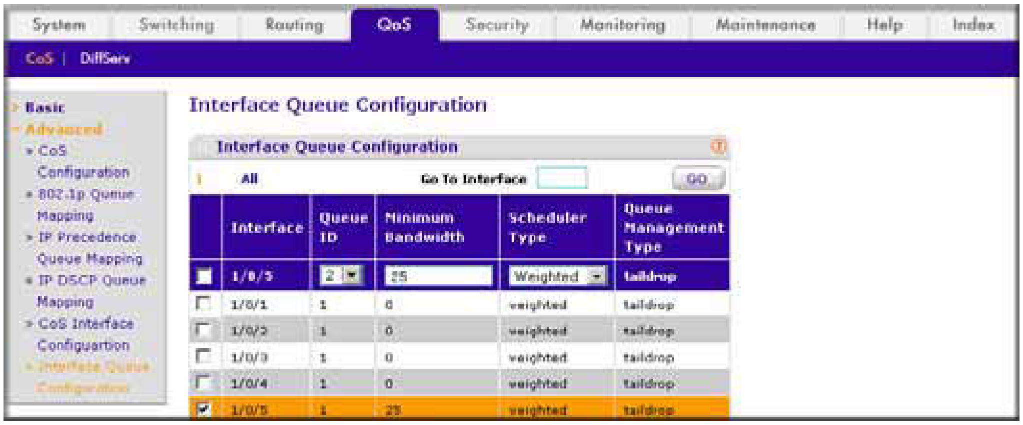
d. In the **Minimum Bandwidth** field, enter **25**.

e. Click **Apply**.

16. Set the CoS queue 2 configuration for interface 1/0/5.

a. Select **QoS > CoS > Advanced > Interface Queue Configuration**.

A screen similar to the following displays.



Interface Queue Configuration

Interface Queue Configuration

All   Go To Interface

	Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
□	1/0/5	2	25	Weighted	taildrop
□	1/0/1	1	0	weighted	taildrop
□	1/0/2	1	0	weighted	taildrop
□	1/0/3	1	0	weighted	taildrop
□	1/0/4	1	0	weighted	taildrop
☑	1/0/5	1	25	weighted	taildrop

b. Under Interface Queue Configuration, scroll down and select the interface **1/0/5** check box.

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

c. In the **Queue ID** list, select **2**.

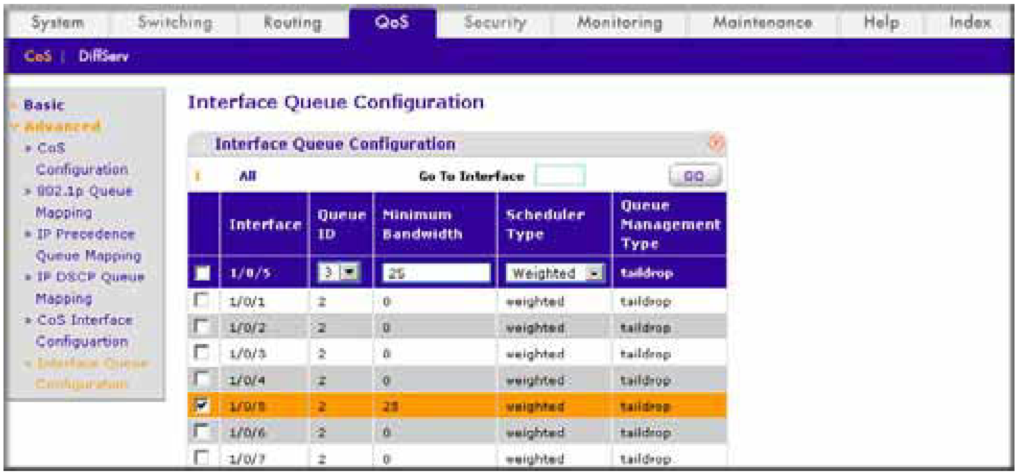
d. In the **Minimum Bandwidth** field, enter **25**.

e. Click **Apply**.

17. Set the CoS queue 3 configuration for interface 1/0/5.

a. Select **QoS > CoS > Advanced > Interface Queue Configuration**.

A screen similar to the following displays.



Interface Queue Configuration

Interface Queue Configuration

All   Go To Interface

	Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
□	1/0/5	3	25	Weighted	taildrop
□	1/0/1	2	0	weighted	taildrop
□	1/0/2	2	0	weighted	taildrop
□	1/0/3	2	0	weighted	taildrop
□	1/0/4	2	0	weighted	taildrop
☑	1/0/5	2	25	weighted	taildrop
□	1/0/6	2	0	weighted	taildrop
□	1/0/7	2	0	weighted	taildrop

b. Under Interface Queue Configuration, scroll down and select the interface **1/0/5** check box.

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

c. In the **Queue ID** list, select **3**.

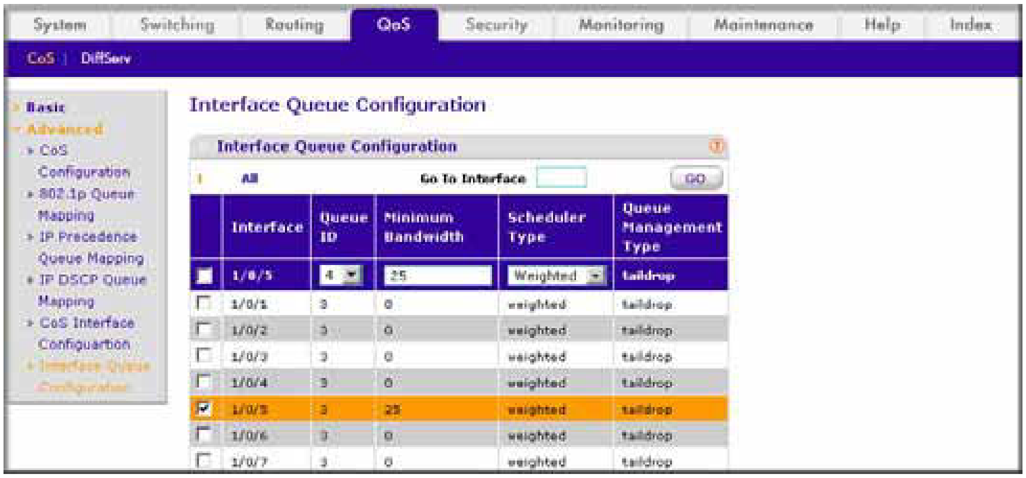
d. In the **Minimum Bandwidth** field, enter **25**.

e. Click **Apply**.

18. Set the CoS queue 4 configuration for interface 1/0/5.

a. Select **QoS > CoS > Advanced > Interface Queue Configuration**.

A screen similar to the following displays.



Interface Queue Configuration

Interface Queue Configuration

All   Go To Interface

	Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
☐	1/0/5	4	25	Weighted	taildrop
☐	1/0/1	3	0	weighted	taildrop
☐	1/0/2	3	0	weighted	taildrop
☐	1/0/3	3	0	weighted	taildrop
☐	1/0/4	3	0	weighted	taildrop
☑	1/0/5	3	25	weighted	taildrop
☐	1/0/6	3	0	weighted	taildrop
☐	1/0/7	3	0	weighted	taildrop

b. Under Interface Queue Configuration, scroll down and select the Interface **1/0/5** check box.

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

c. In the **Queue ID** list, select **4**.

d. In the **Minimum Bandwidth** field, enter **25**.

e. Click **Apply**.

DiffServ for 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.

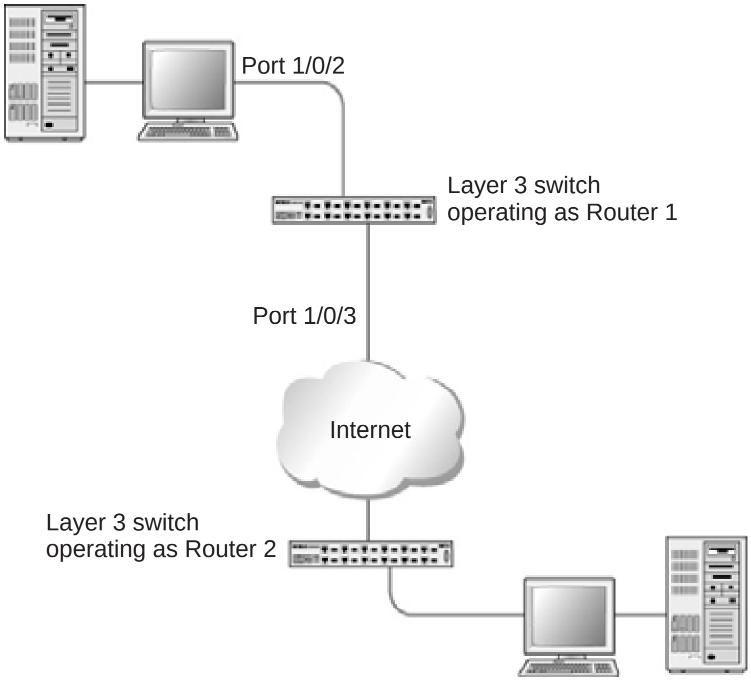


Figure 16. Diffserv for VoIP in Router 1

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
```

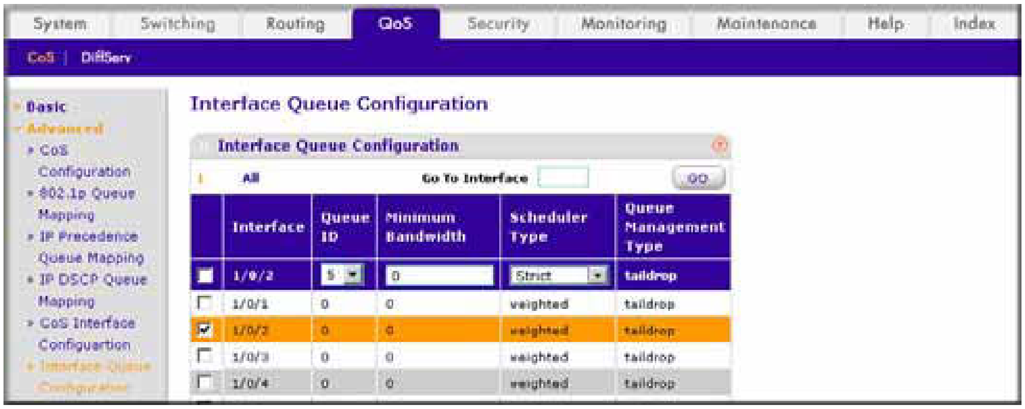
5. Attach the defined policy to an inbound service interface.

```
(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

Interface Queue Configuration

	Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
□	1/0/2	5	0	Strict	taildrop
□	1/0/1	0	0	weighted	taildrop
☑	1/0/2	0	0	weighted	taildrop
□	1/0/3	0	0	weighted	taildrop
□	1/0/4	0	0	weighted	taildrop

b. Under Interface Queue Configuration, select all the interfaces.

c. In the **Queue ID** list, select **5**.

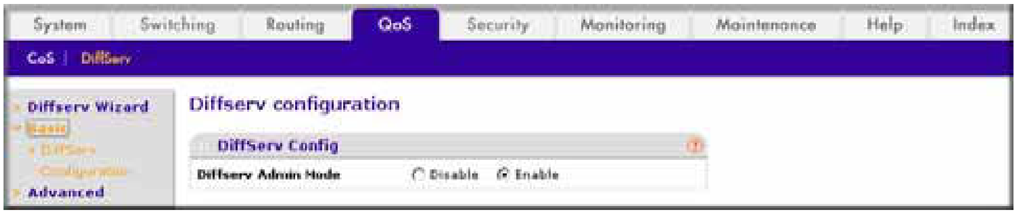
d. In the **Scheduler Type** list, select **Strict**.

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

2. Enable DiffServ.

a. Select **QoS > DiffServ > Basic > DiffServ Configuration**.

A screen similar to the following displays.



Diffserv configuration

DiffServ Config

Diffserv Admin Mode ○ Disable ● Enable

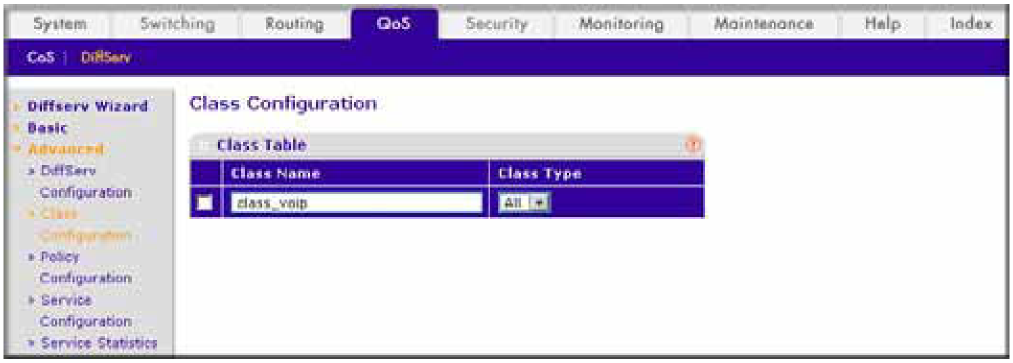
b. For Diffserv Admin Mode, select the **Enable** radio button.

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.



Class Configuration

Class Table

	Class Name	Class Type
□	class_voip	All

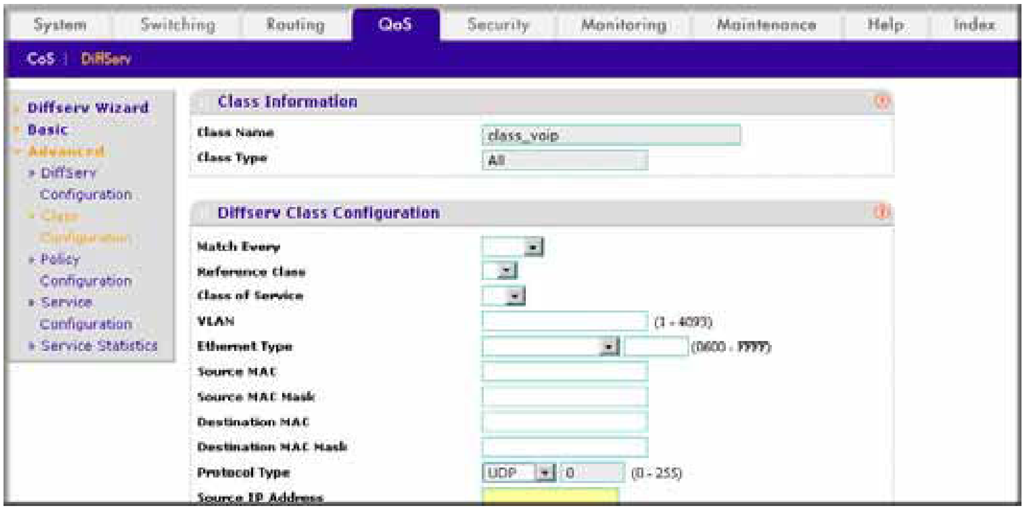
b. In the **Class Name** field, enter **class_voip**.

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:



Class Information

Class Name	class_voip
Class Type	All

Diffserv Class Configuration

Match Every	
Reference Class	
Class of Service	
VLAN	(1 - 4093)
Ethernet Type	(0600 - FFFF)
Source MAC	
Source MAC Mask	
Destination MAC	
Destination MAC Mask	
Protocol Type	UDP 0 (0 - 255)
Source IP Address	

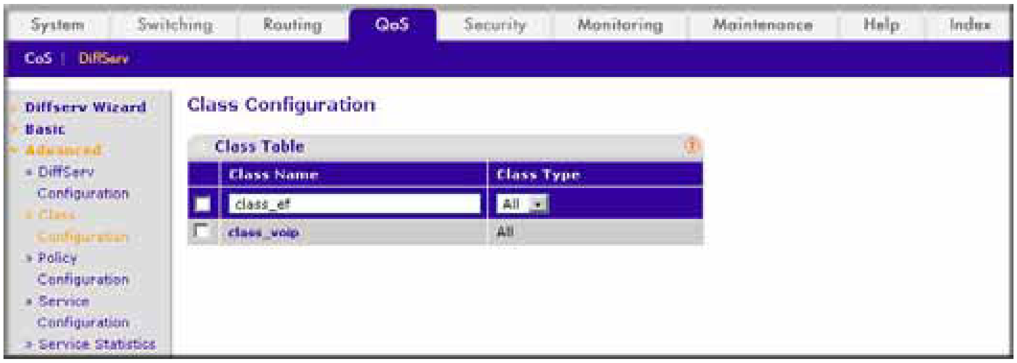
f. In the **Protocol Type** list, select **UDP**.

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.



Class Configuration

Class Table

	Class Name	Class Type
☐	class_ef	All
☐	class_voip	All

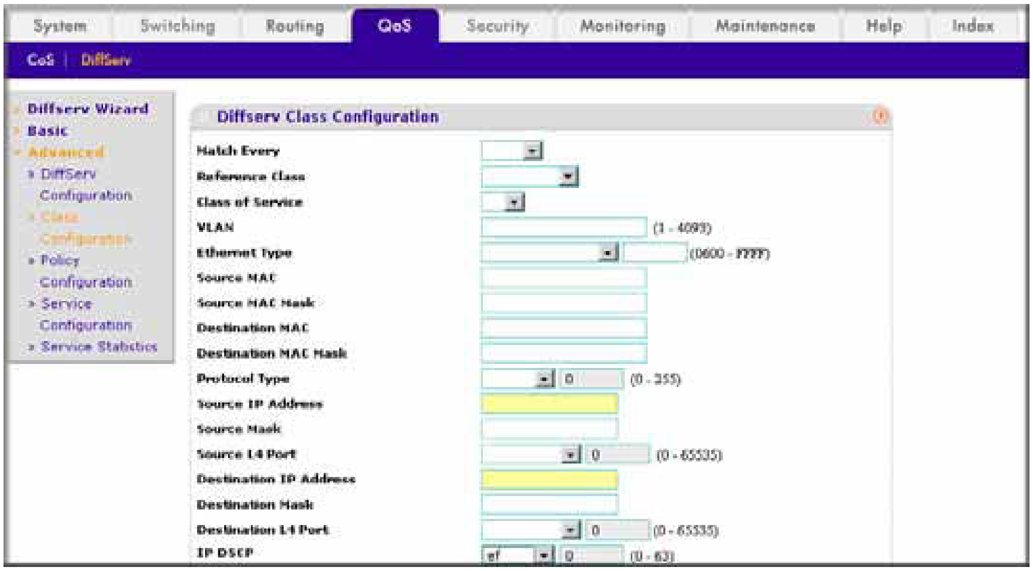
b. In the **Class Name** field, enter **class_ef**.

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

Match Every
Reference Class
Class of Service
VLAN (1 - 4093)
Ethernet Type (0600 - FFFF)
Source MAC
Source MAC Mask
Destination MAC
Destination MAC Mask
Protocol Type 0 (0 - 255)
Source IP Address
Source Mask
Source L4 Port 0 (0 - 65535)
Destination IP Address
Destination Mask
Destination L4 Port 0 (0 - 65535)
IP DSCP ef 0 (0 - 63)

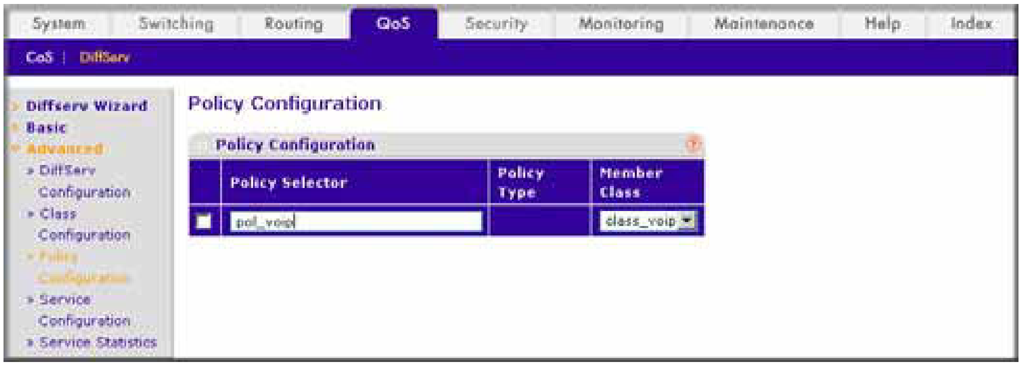
f. In the **IP DSCP** list, select **ef**.

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.



Policy Configuration

Policy Configuration

	Policy Selector	Policy Type	Member Class
□	pol_voip		class_voip

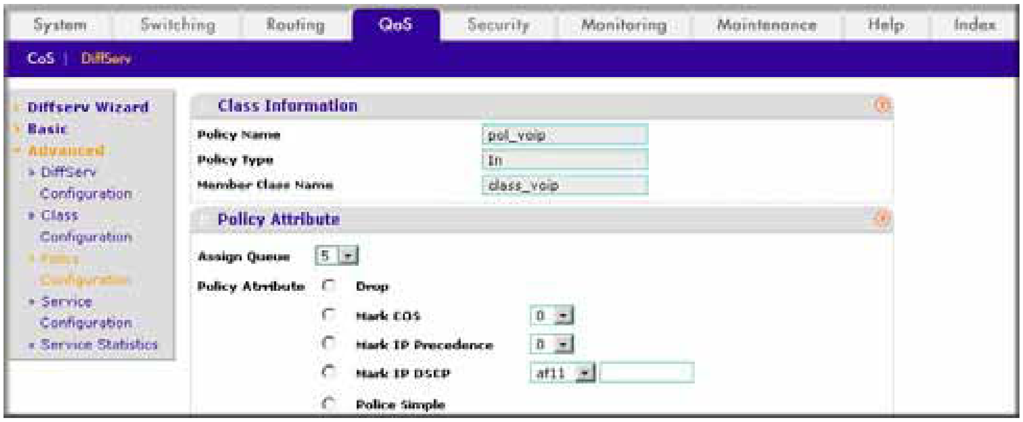
   b. In the **Policy Selector** field, enter **pol_voip**.

   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.



Class Information

Policy Name	pol_voip
Policy Type	In
Member Class Name	class_voip

Policy Attribute

Assign Queue 5

Policy Attribute
○ Drop
○ Mark COS 0
○ Mark IP Precedence 0
○ Mark IP DSCP af11
○ Police Simple

f. In the **Assign Queue** list, select **5**.

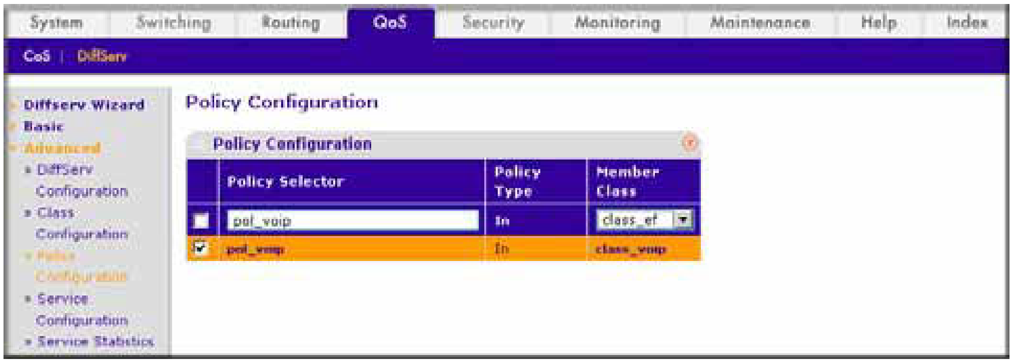
g. For Policy Attribute, select the **Mark IP DSCP** radio button, and select **ef**.

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

Policy Configuration

	Policy Selector	Policy Type	Member Class
□	pol_voip	In	class_ef
☑	pol_voip	In	class_voip

b. Under Policy Configuration, scroll down and select the **pol_voip** check box.

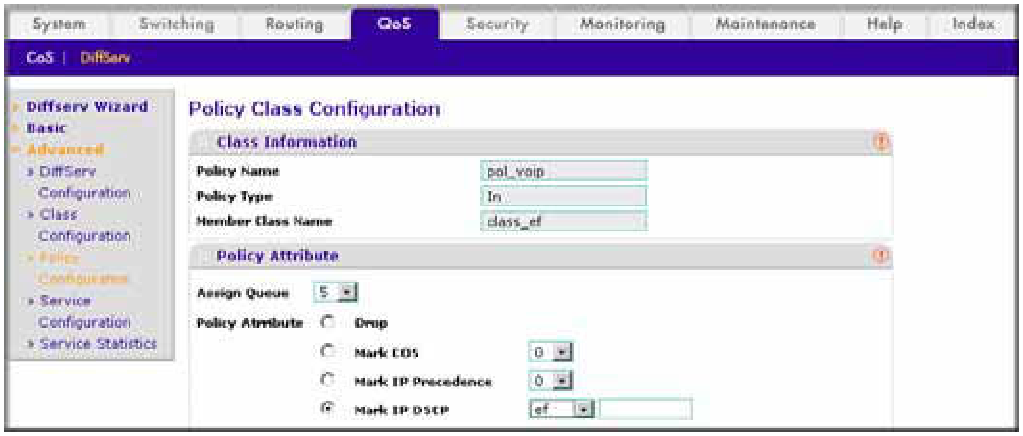
Pol_voip now appears in the Policy Selector field at the top.

c. In the **Member Class** list, select **class_ef** in.

d. Click **Apply** to add the class class_ef to the policy pol_voip.

e. Click the **pol_voip** whose class member is class_ef.

A screen similar to the following displays.



Policy Class Configuration

Class Information

Policy Name	pol_voip
Policy Type	In
Member Class Name	class_ef

Policy Attribute

Assign Queue	5		
Policy Attribute	○	Drop	
	○	Mark COS	0
	○	Mark IP Precedence	0
	●	Mark IP DSCP	ef

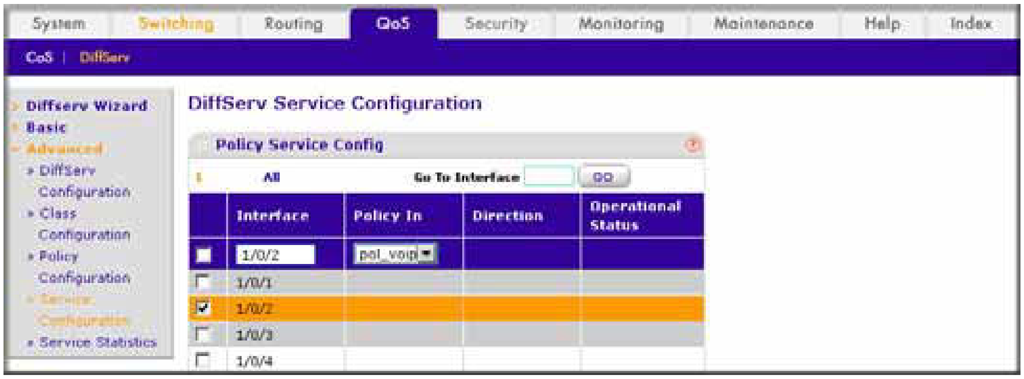
f. In the **Assign Queue** list, select **5**.

g. Click **Apply** to create a new policy.

7. Attach the defined policy to interface 1/0/2 in the inbound direction.

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

A screen similar to the following displays.



DiffServ Service Configuration

Policy Service Config

	Interface	Policy In	Direction	Operational Status
□	1/0/2	pol_voip		
□	1/0/1			
☑	1/0/2			
□	1/0/3			
□	1/0/4			

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.

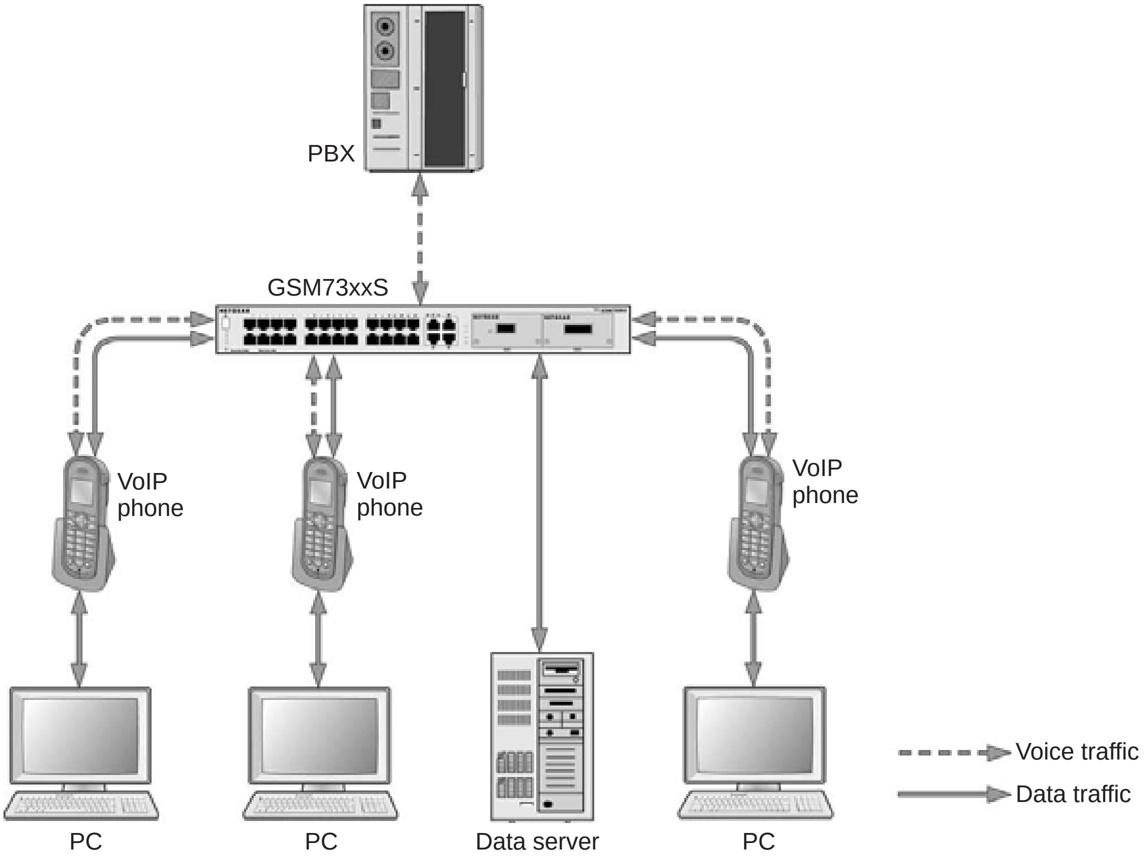


Figure 17. Auto VoIP

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

CLI: Configure Auto VoIP

This script in this section shows how to set up auto VoIP system-wide.

1. Enable auto VoIP on all the interfaces in the device.

```
(Netgear Switch) (Config)# auto-voip all
```

2. View the auto VoIP information:

```
(Netgear Switch) # show auto-voip interface all

        Interface  Auto VoIP Mode Traffic Class
        ---------  -------------- -------------
        1/0/1      Enabled        6
        1/0/2      Enabled        6
        1/0/3      Enabled        6
        1/0/4      Enabled        6
        1/0/5      Enabled        6
        1/0/6      Enabled        6
        1/0/7      Enabled        6
        1/0/8      Enabled        6
        1/0/9      Enabled        6
        1/0/10     Enabled        6
        1/0/11     Enabled        6
        1/0/12     Enabled        6
        1/0/13     Enabled        6
        1/0/14     Enabled        6
        1/0/15     Enabled        6
        1/0/16     Enabled        6
        1/0/17     Enabled        6
        1/0/18     Enabled        6
        1/0/19     Enabled        6
        1/0/20     Enabled        6

        --More-- or (q)uit

        Interface  Auto VoIP Mode Traffic Class
        ---------  -------------- -------------
        1/0/21     Enabled        6
        1/0/22     Enabled        6
        1/0/23     Enabled        6
        1/0/24     Enabled        6
        1/0/25     Enabled        6
        1/0/26     Enabled        6
        1/0/27     Enabled        6
        1/0/28     Enabled        6
```

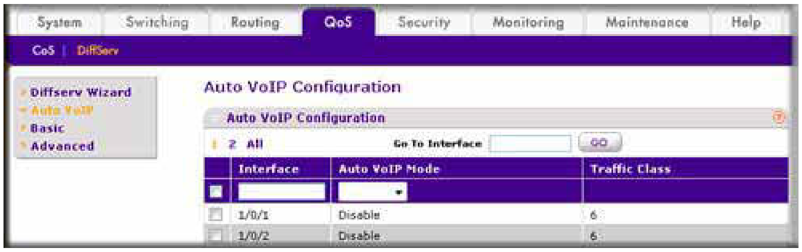
Auto VoIP classifies and prioritizes the packets and places only the packets in the higher-priority queue. In the previous example, the packets are placed in queue 6. You can override the egress queue setting using the **cos-queue strict** or **cos-queue min-bandwidth** command.

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

Auto VoIP Configuration

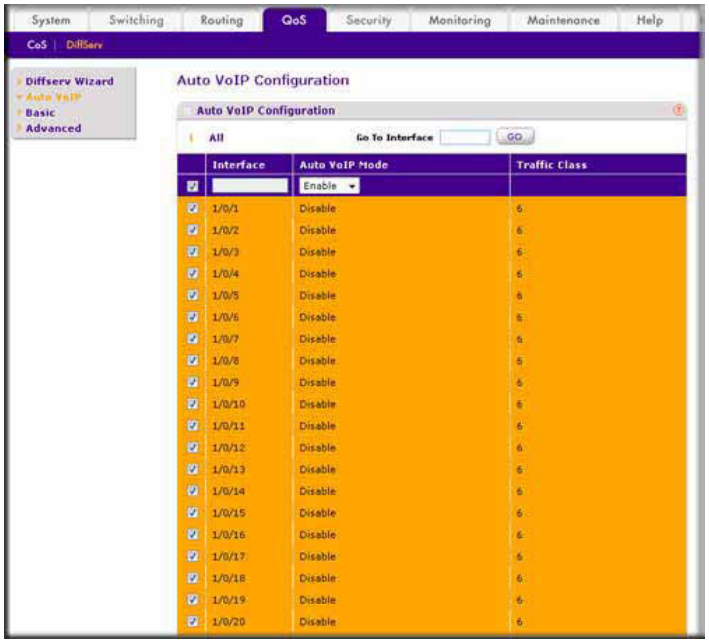
1 2 All Go To Interface

	Interface	Auto VoIP Mode	Traffic Class
□			
□	1/0/1	Disable	6
□	1/0/2	Disable	6

   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

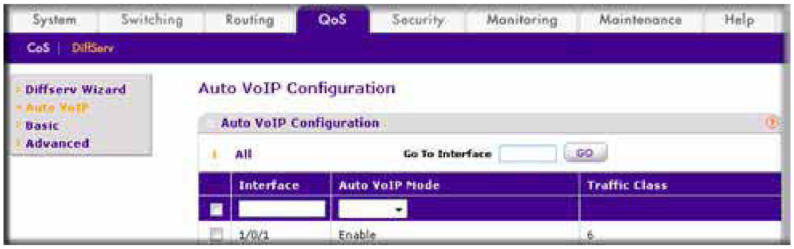
Auto VoIP Configuration

1 All Go To Interface

	Interface	Auto VoIP Mode	Traffic Class
☑		Enable	
☑	1/0/1	Disable	6
☑	1/0/2	Disable	6
☑	1/0/3	Disable	6
☑	1/0/4	Disable	6
☑	1/0/5	Disable	6
☑	1/0/6	Disable	6
☑	1/0/7	Disable	6
☑	1/0/8	Disable	6
☑	1/0/9	Disable	6
☑	1/0/10	Disable	6
☑	1/0/11	Disable	6
☑	1/0/12	Disable	6
☑	1/0/13	Disable	6
☑	1/0/14	Disable	6
☑	1/0/15	Disable	6
☑	1/0/16	Disable	6
☑	1/0/17	Disable	6
☑	1/0/18	Disable	6
☑	1/0/19	Disable	6
☑	1/0/20	Disable	6

   d. Click **Apply**.

   A screen similar to the following displays.



Auto VoIP Configuration

Auto VoIP Configuration

1 All Go To Interface

	Interface	Auto VoIP Mode	Traffic Class
□			
□	1/0/1	Enable	6

DiffServ for IPv6

This feature extends the existing QoS ACL and DiffServ functionality by providing support for IPv6 packet classification.

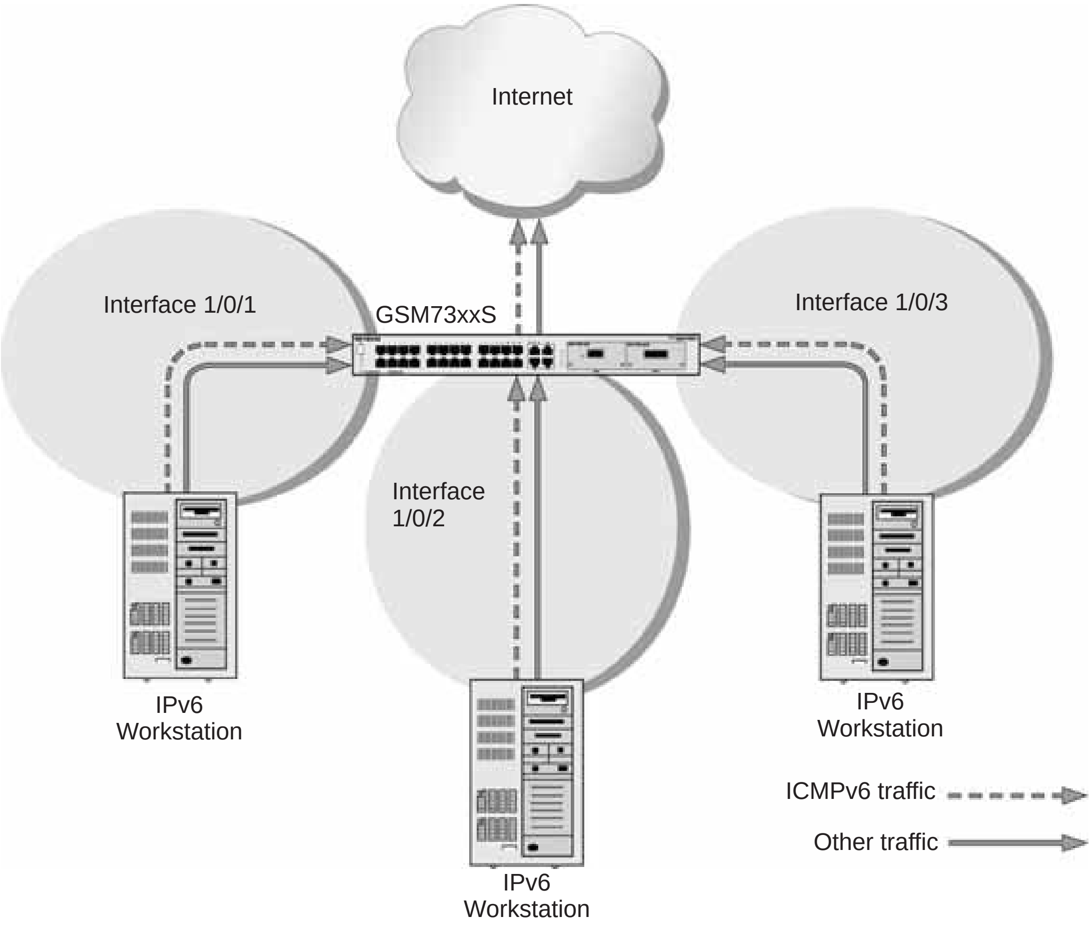


Figure 18. DiffServ for IPv6

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

CLI: Configure DiffServ for IPv6

The script in this section shows how to prioritize ICMPv6 traffic over other IPv6 traffic.

1. Create the IPv6 class classicmpv6.

```
(Netgear Switch) (Config)# class-map match-all classicmpv6 ipv6
```

2. Define matching criteria as protocol ICMPv6.

```
(Netgear Switch) (Config-classmap) # match protocol 58
(Netgear Switch) (Config-classmap) # exit
```

3. Create the policy policyicmpv6.

```
(Netgear Switch) (Config)# policy-map policyicmpv6 in
```

4. Associate the previously created class classicmpv6.

```
(Netgear Switch) (Config-policy-map)# class classicmpv6
```

5. Set the attribute as assign queue 6.

```
(Netgear Switch) (Config-policy-classmap)# assign-queue 6
(Netgear Switch) (Config-policy-map)# exit
```

6. Attach the policy policy_icmpv6 to interfaces 1/0/1,1/0/2 and 1/0/3:

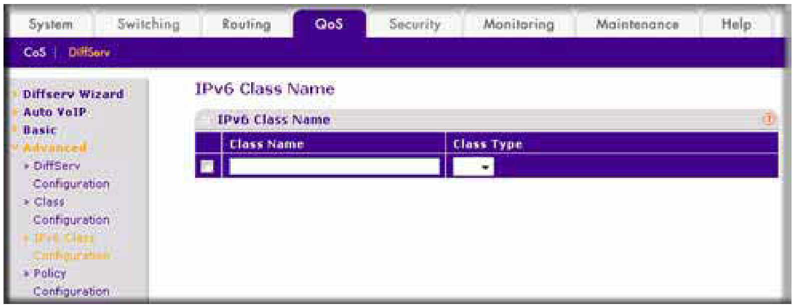
```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# service-policy in policyicmpv6
(Netgear Switch) (Interface 1/0/1)# exit

(Netgear Switch) (Config)# interface 1/0/2
(Netgear Switch) (Interface 1/0/2)# service-policy in policyicmpv6
(Netgear Switch) (Interface 1/0/2)# exit

(Netgear Switch) (Config)# interface 1/0/3
(Netgear Switch) (Interface 1/0/3)# service-policy in policyicmpv6
(Netgear Switch) (Interface 1/0/3)# exit
```

Web Interface: Configure DiffServ for IPv6

1. Create the IPv6 class classicmpv6.

   a. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**.

   A screen similar to the following displays.



IPv6 Class Name

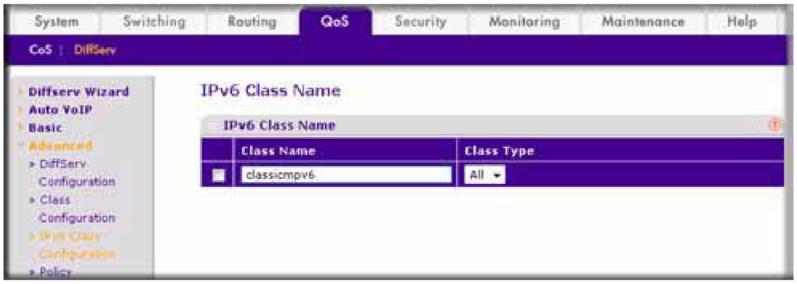
IPv6 Class Name

	Class Name	Class Type
□		▾

   b. In the **Class Name** field, enter **classicmpv6**.

   c. In the **Class Type** list, select **All**.

   A screen similar to the following displays.



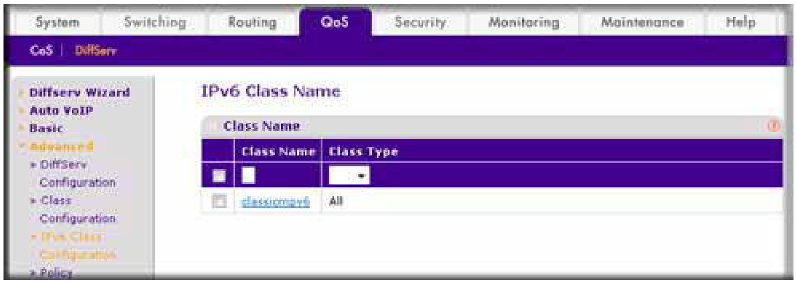
IPv6 Class Name

IPv6 Class Name

	Class Name	Class Type
□	classicmpv6	All ▾

   d. Click **Add** to create the IPv6 class.

   A screen similar to the following displays.



IPv6 Class Name

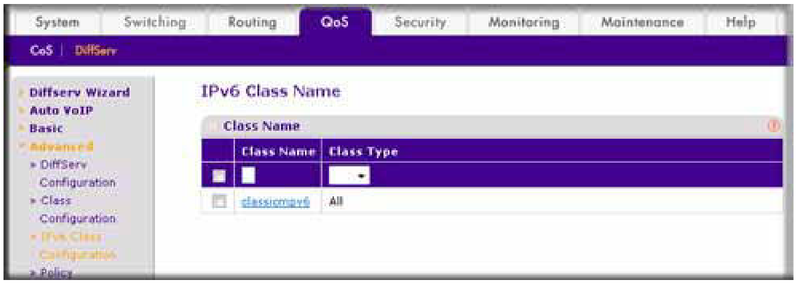
Class Name

	Class Name	Class Type
□		▾
□	classicmpv6	All

2. Define matching criteria as protocol ICMPv6.

   a. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**.

A screen similar to the following displays.



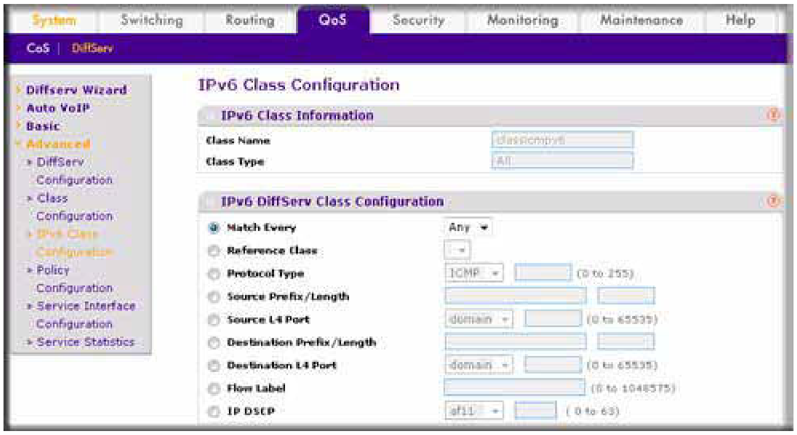
IPv6 Class Name

Class Name

	Class Name	Class Type
☐	classicmpv6	All

b. Click the class **classicmpv6**.

A screen similar to the following displays.



IPv6 Class Configuration

IPv6 Class Information

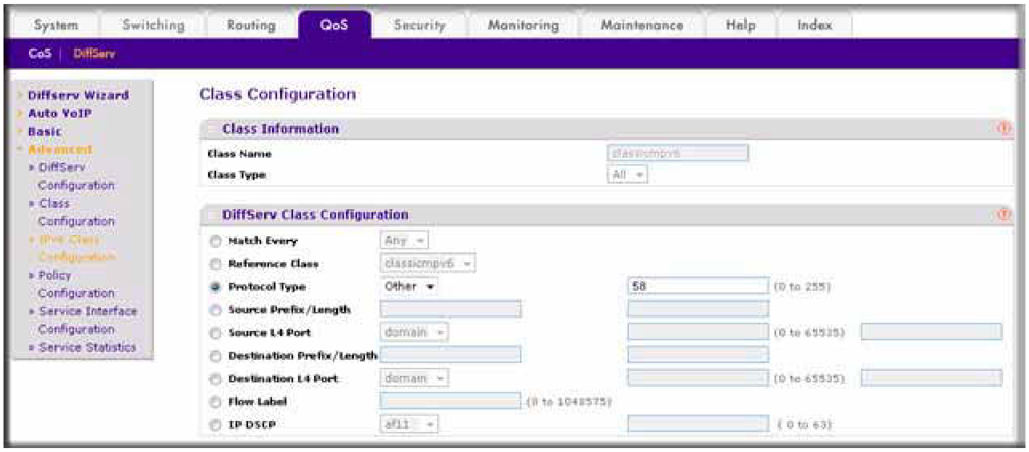
Class Name	classicmpv6
Class Type	All

IPv6 DiffServ Class Configuration

● Match Every	Any		
○ Reference Class			
○ Protocol Type	ICMP		(0 to 255)
○ Source Prefix/Length			
○ Source L4 Port	domain		(0 to 65535)
○ Destination Prefix/Length			
○ Destination L4 Port	domain		(0 to 65535)
○ Flow Label			(0 to 1048575)
○ IP DSCP	af11		(0 to 63)

c. Select the **Protocol Type** radio button, select **Other**, and enter **58**.

A screen similar to the following displays.



Class Configuration

Class Information

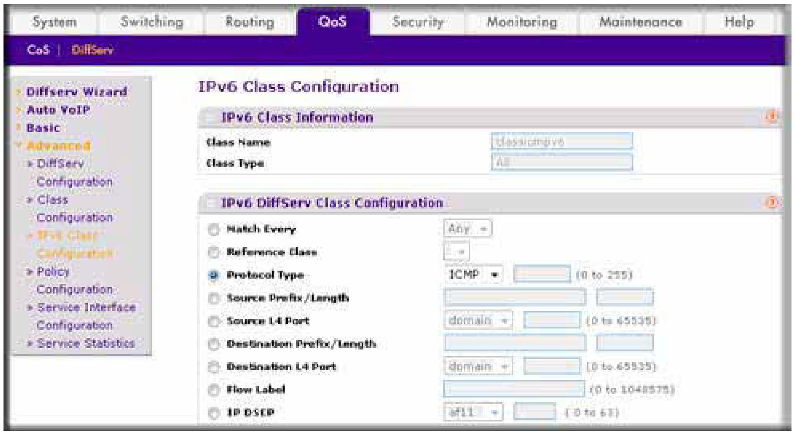
Class Name	classicmpv6
Class Type	All

DiffServ Class Configuration

○ Match Every	Any		
○ Reference Class	classicmpv6		
● Protocol Type	Other	58	(0 to 255)
○ Source Prefix/Length			
○ Source L4 Port	domain		(0 to 65535)
○ Destination Prefix/Length			
○ Destination L4 Port	domain		(0 to 65535)
○ Flow Label	(0 to 1048575)		
○ IP DSCP	af11		(0 to 63)

d. Click **Apply**.

A screen similar to the following displays.



IPv6 Class Configuration

IPv6 Class Information

Class Name	classicmpv6
Class Type	All

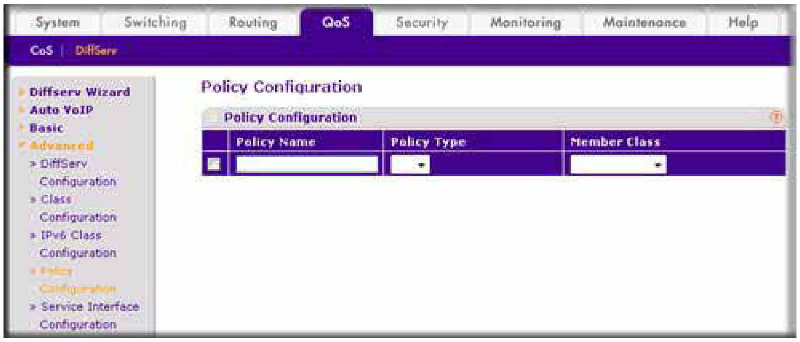
IPv6 DiffServ Class Configuration

○ Match Every	Any		
○ Reference Class			
● Protocol Type	ICMP		(0 to 255)
○ Source Prefix/Length			
○ Source L4 Port	domain		(0 to 65535)
○ Destination Prefix/Length			
○ Destination L4 Port	domain		(0 to 65535)
○ Flow Label			(0 to 1048575)
○ IP DSEP	af11		(0 to 63)

3. Create the policy policyicmpv6, and associate the previously created class classicmpv6.

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

   A screen similar to the following displays.



Policy Configuration

Policy Configuration

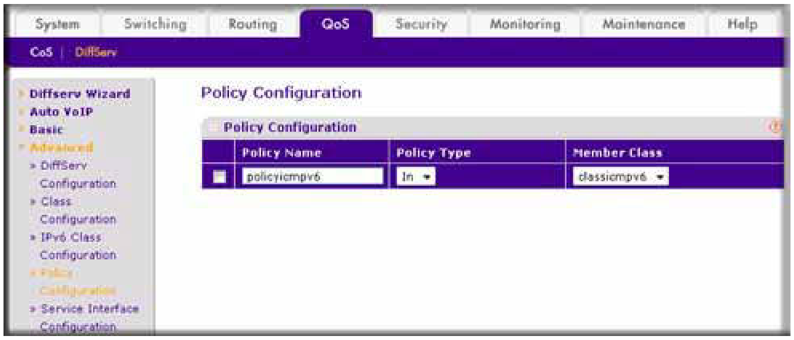
	Policy Name	Policy Type	Member Class
□			

   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.



Policy Configuration

Policy Configuration

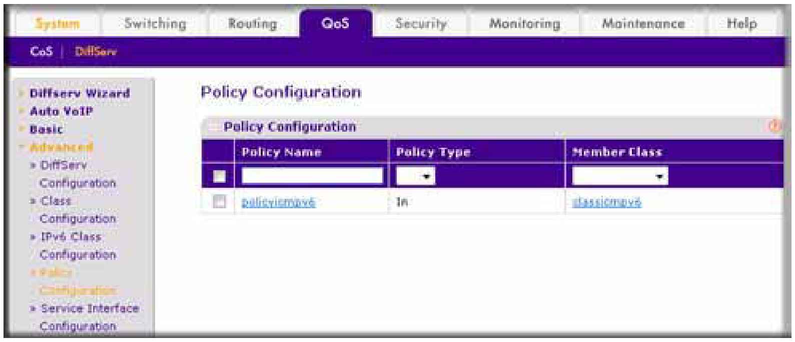
	Policy Name	Policy Type	Member Class
□	policyicmpv6	In	classicmpv6

   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.



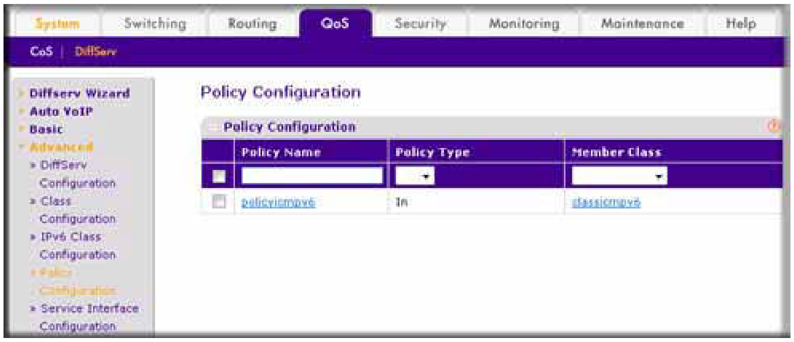
Policy Configuration

Policy Configuration

	Policy Name	Policy Type	Member Class
□	policyicmpv6	In	classicmpv6

   b. Click the policy **policyicmpv6**.

   A screen similar to the following displays.

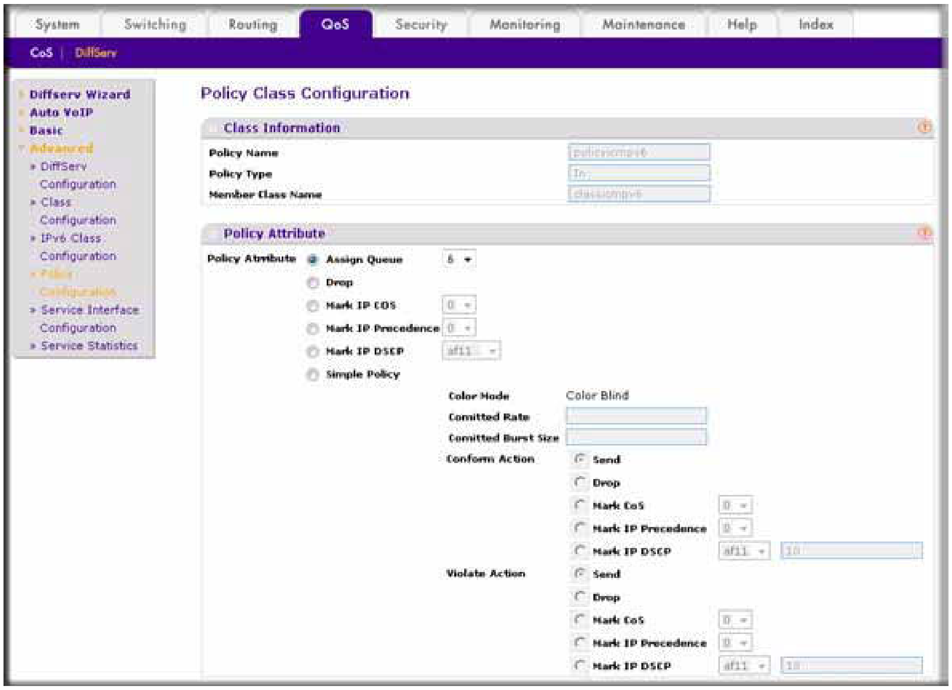


Policy Configuration

Policy Configuration

	Policy Name	Policy Type	Member Class
□	policyicmpv6	In	classicmpv6

c. In the **Assign Queue** list, select **6**.



Policy Class Configuration

Class Information

Policy Name	policyicmpv6
Policy Type	In
Member Class Name	classicmpv6

Policy Attribute

Policy Attribute
- ● Assign Queue 6
- ○ Drop
- ○ Mark IP COS 0
- ○ Mark IP Precedence 0
- ○ Mark IP DSCP af11
- ○ Simple Policy

Color Mode Color Blind

Comitted Rate

Comitted Burst Size

Conform Action
- ● Send
- ○ Drop
- ○ Mark CoS 0
- ○ Mark IP Precedence 0
- ○ Mark IP DSCP af11 10

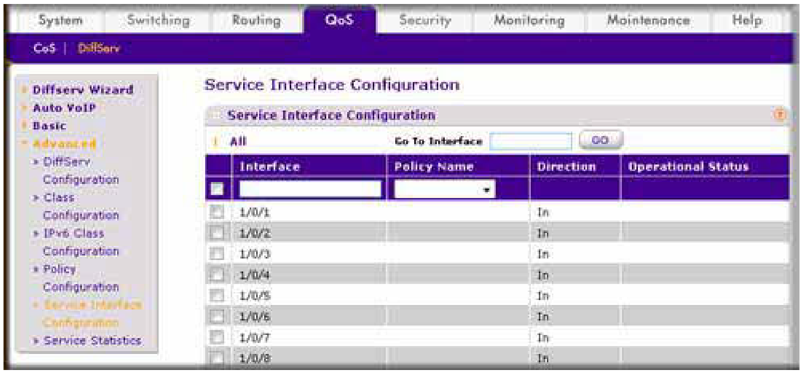
Violate Action
- ● Send
- ○ Drop
- ○ Mark CoS 0
- ○ Mark IP Precedence 0
- ○ Mark IP DSCP af11 10

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.



Service Interface Configuration

Service Interface Configuration

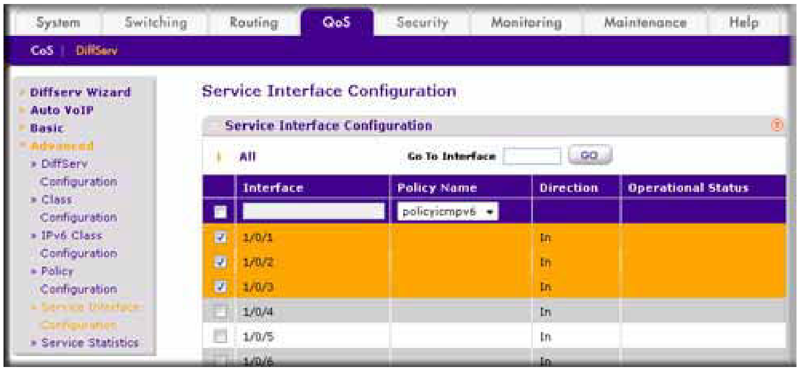
All Go To Interface

	Interface	Policy Name	Direction	Operational Status
□				
□	1/0/1		In	
□	1/0/2		In	
□	1/0/3		In	
□	1/0/4		In	
□	1/0/5		In	
□	1/0/6		In	
□	1/0/7		In	
□	1/0/8		In	

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.



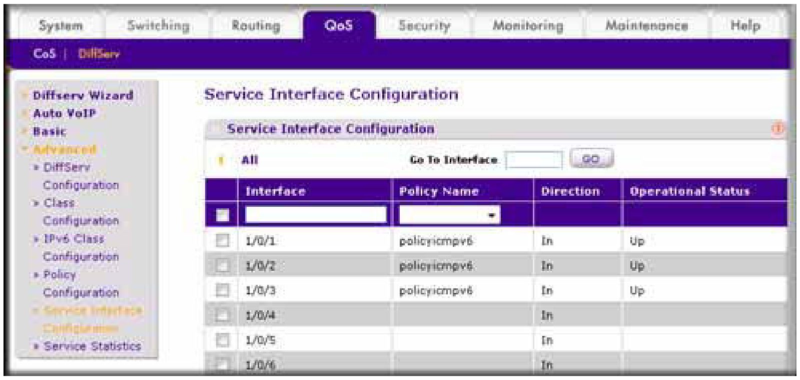
Service Interface Configuration

Service Interface Configuration

	Interface	Policy Name	Direction	Operational Status
□		policyicmpv6		
☑	1/0/1		In	
☑	1/0/2		In	
☑	1/0/3		In	
□	1/0/4		In	
□	1/0/5		In	
□	1/0/6		In	

d. Click **Apply**.

A screen similar to the following displays.



Service Interface Configuration

Service Interface Configuration

	Interface	Policy Name	Direction	Operational Status
□				
□	1/0/1	policyicmpv6	In	Up
□	1/0/2	policyicmpv6	In	Up
□	1/0/3	policyicmpv6	In	Up
□	1/0/4		In	
□	1/0/5		In	
□	1/0/6		In	

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
```

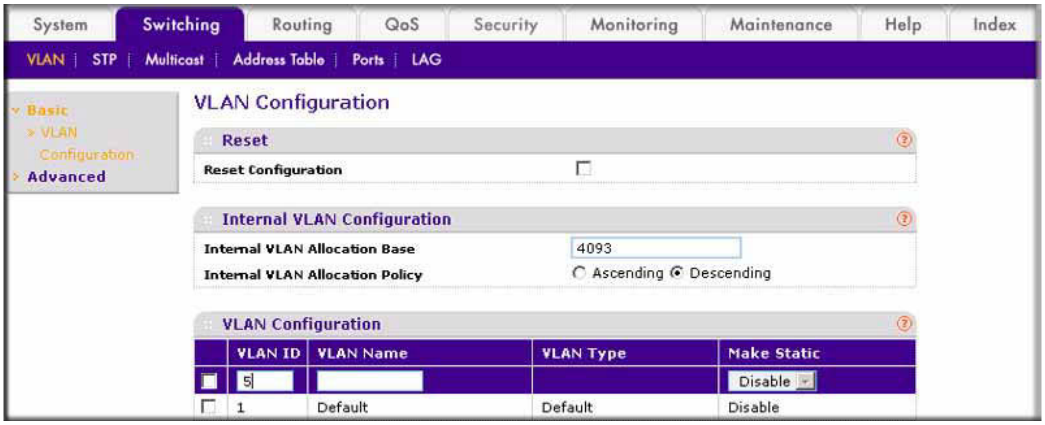
4. Apply this policy to port 1/0/13.

```
(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

Reset

Reset Configuration □

Internal VLAN Configuration

Internal VLAN Allocation Base 4093

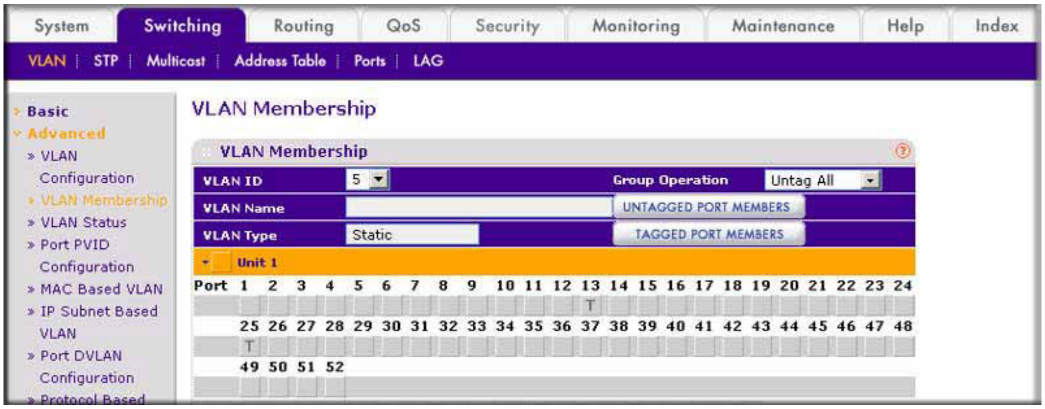
Internal VLAN Allocation Policy ○ Ascending ● Descending

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type	Make Static
☑	5			Disable
□	1	Default	Default	Disable

   b. In the **VLAN ID** field, enter **5**.
   c. Click **Add**.
2. Add ports 1/0/13 and 1/0/25 to VLAN 5.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A screen similar to the following displays.



VLAN Membership

VLAN ID 5

Group Operation Untag All

VLAN Name

VLAN Type Static

   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.

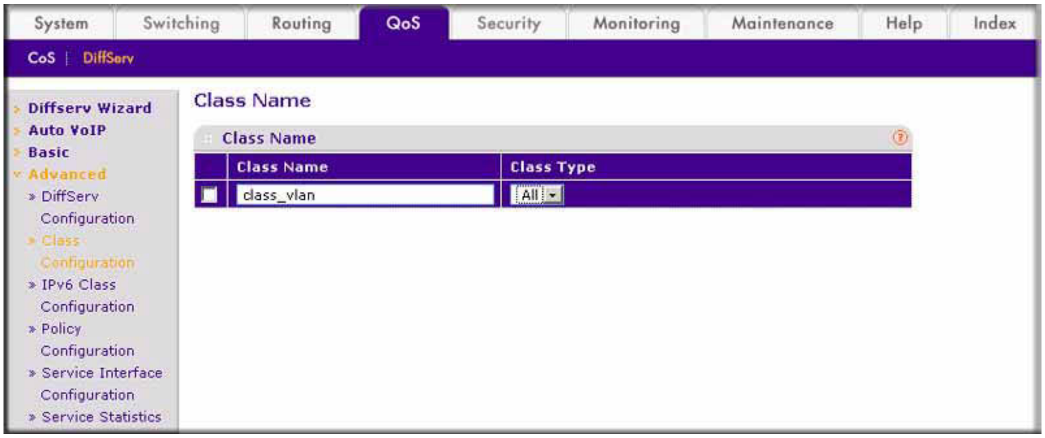
   The T specifies that the egress packet is tagged for the port.

e. Click **Apply**.

3. Create a class class_vlan:

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

   A screen similar to the following displays.



Class Name

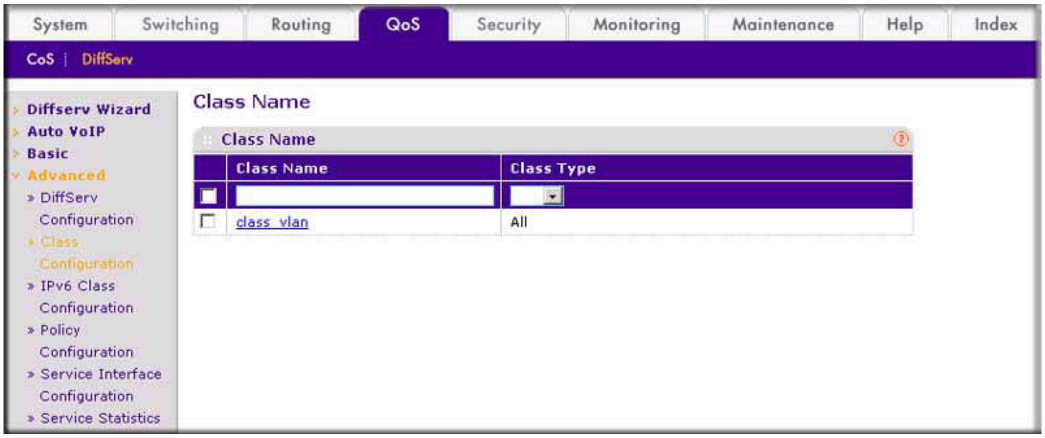
Class Name

	Class Name	Class Type
□	class_vlan	All

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.



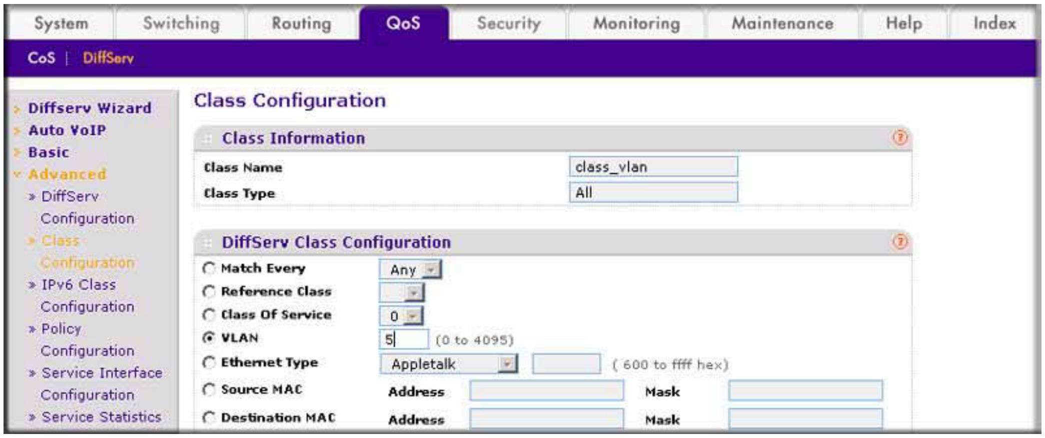
Class Name

Class Name

	Class Name	Class Type
□		
□	class_vlan	All

d. Click **class_vlan** to configure this class.

A screen similar to the following displays:



Class Configuration

Class Information

Class Name	class_vlan
Class Type	All

DiffServ Class Configuration

○ Match Every	Any			
○ Reference Class				
○ Class Of Service	0			
● VLAN	5	(0 to 4095)		
○ Ethernet Type	Appletalk	(600 to ffff hex)		
○ Source MAC	Address		Mask	
○ Destination MAC	Address		Mask	

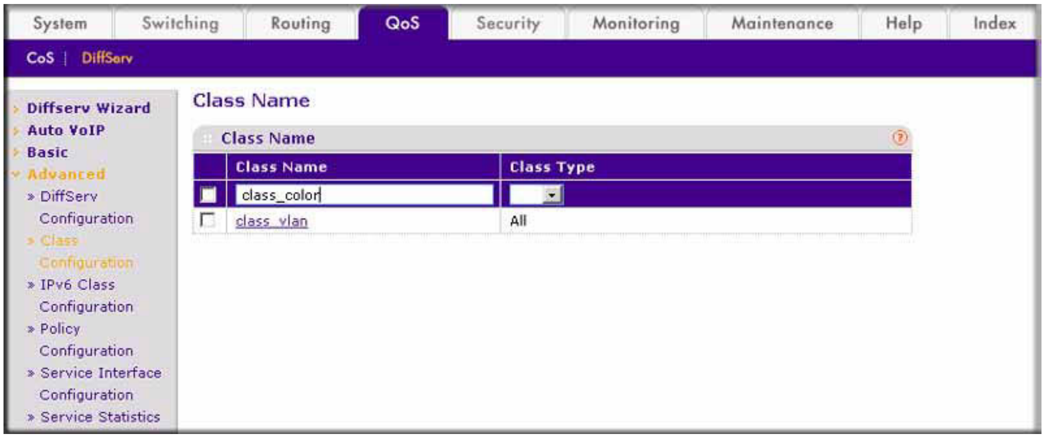
e. Under Diffserv Class Configuration, in the **VLAN** field, enter **5**.

f. Click **Apply**.

4. Create a class class_color.

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

A screen similar to the following displays.



Class Name

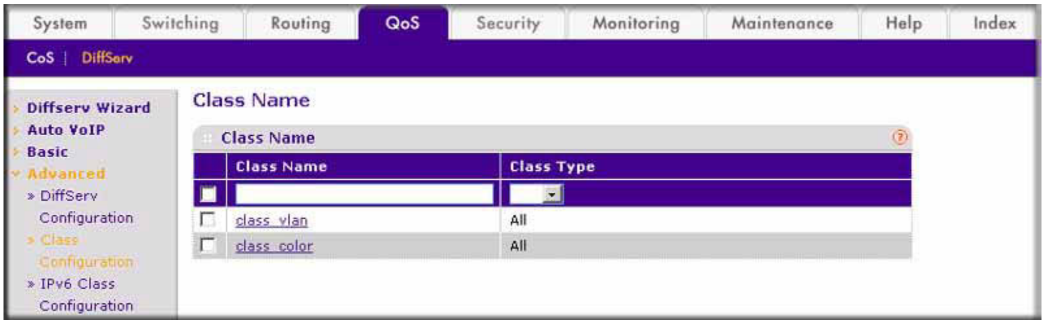
Class Name

	Class Name	Class Type
□	class_color	
□	class_vlan	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.



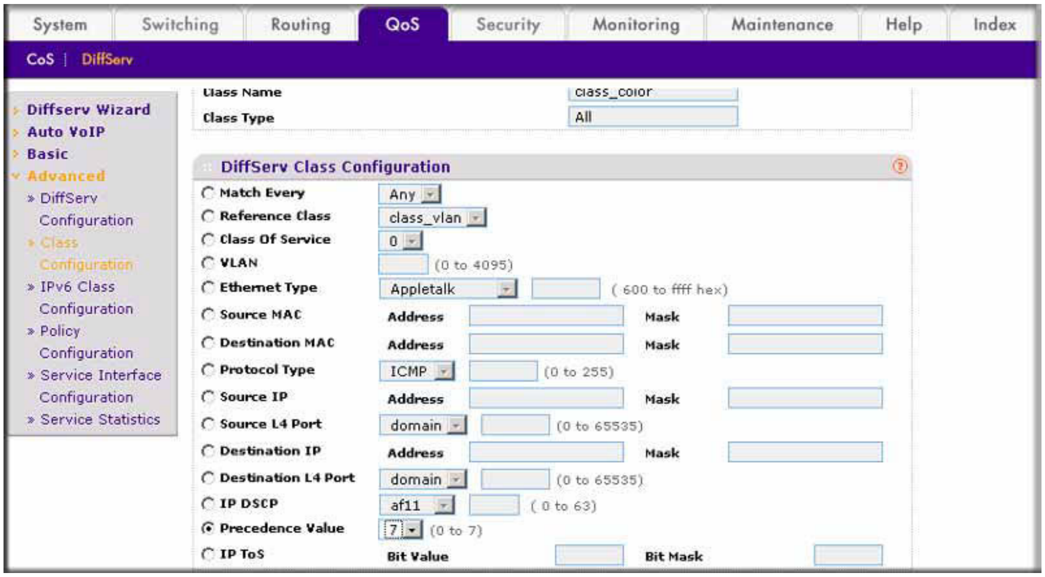
Class Name

Class Name

	Class Name	Class Type
☐		
☐	class_vlan	All
☐	class_color	All

d. Click **class_color** to configure this class.

A screen similar to the following displays:



Class Name	class_color
Class Type	All

DiffServ Class Configuration

○ Match Every	Any			
○ Reference Class	class_vlan			
○ Class Of Service	0			
○ VLAN		(0 to 4095)		
○ Ethernet Type	Appletalk	(600 to ffff hex)		
○ Source MAC	Address		Mask	
○ Destination MAC	Address		Mask	
○ Protocol Type	ICMP	(0 to 255)		
○ Source IP	Address		Mask	
○ Source L4 Port	domain	(0 to 65535)		
○ Destination IP	Address		Mask	
○ Destination L4 Port	domain	(0 to 65535)		
○ IP DSCP	af11	(0 to 63)		
● Precedence Value	7	(0 to 7)		
○ IP ToS	Bit Value		Bit Mask	

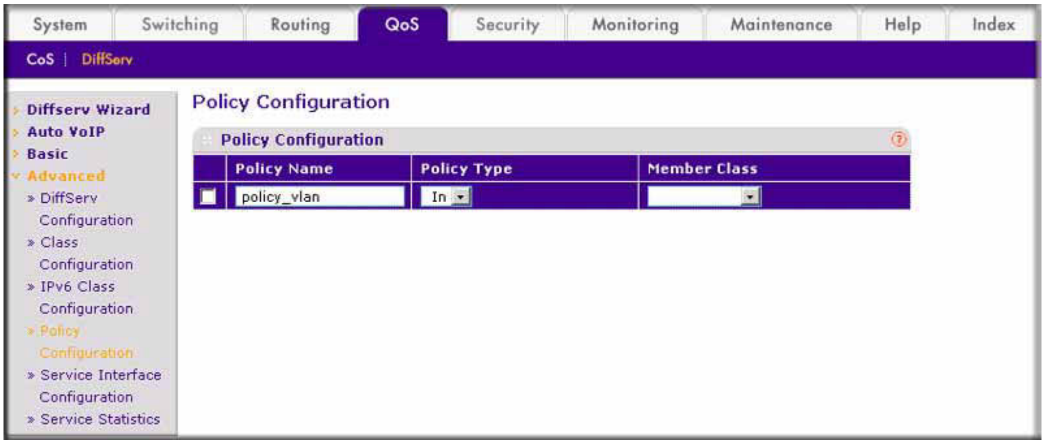
e. Under Diffserv Class Configuration, in the **Precedence Value** list, select **7**.

f. Click **Apply**.

5. Create a policy policy_vlan.

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

A screen similar to the following displays.



Policy Configuration

Policy Configuration

	Policy Name	Policy Type	Member Class
□	policy_vlan	In	

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

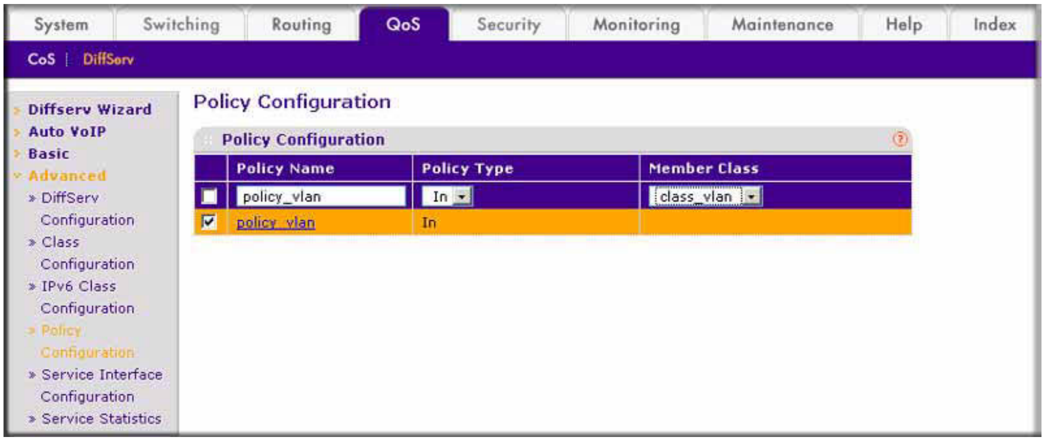
c. In the **Policy Type** list, select **In**.

d. Click **Add**.

6. Associate policy_vlan with class_vlan.

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

A screen similar to the following displays.



Policy Configuration

Policy Configuration

	Policy Name	Policy Type	Member Class
□	policy_vlan	In	class_vlan
☑	policy_vlan	In	

b. Under Policy Configuration, scroll down and select the **policy_vlan** check box.

c. In the **Member Class** field, enter **class_vlan**.

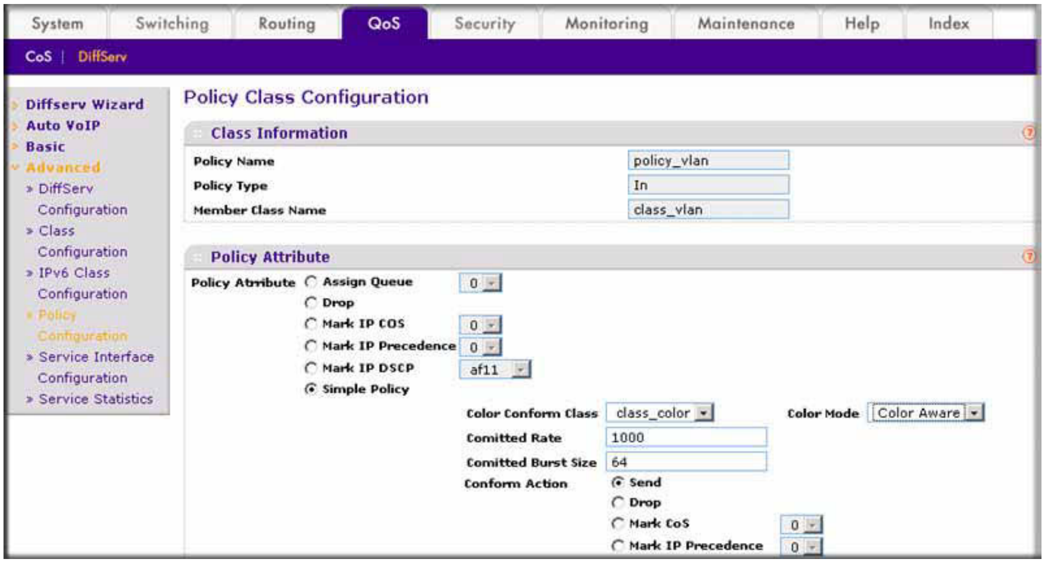
d. Click **Apply**.

7. Configure policy_vlan.

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

b. Click **policy_vlan**.

A screen similar to the following displays.



Policy Class Configuration

Class Information

Policy Name	policy_vlan
Policy Type	In
Member Class Name	class_vlan

Policy Attribute

Policy Attribute
○ Assign Queue 0
○ Drop
○ Mark IP COS 0
○ Mark IP Precedence 0
○ Mark IP DSCP af11
● Simple Policy

Color Conform Class: class_color
Color Mode: Color Aware
Comitted Rate: 1000
Comitted Burst Size: 64
Conform Action
● Send
○ Drop
○ Mark CoS 0
○ Mark IP Precedence 0

c. Select the **Simple Policy** radio button.

d. In the **Color Mode** list, select **Color Aware**.

e. In the **Color Conform Class** list, select **class_color**.

f. In the **Committed Rates** field, enter **1000**.

g. In the **Committed Burst Size** field, enter **64**.

h. For Conform Action, select the **Send** radio button.

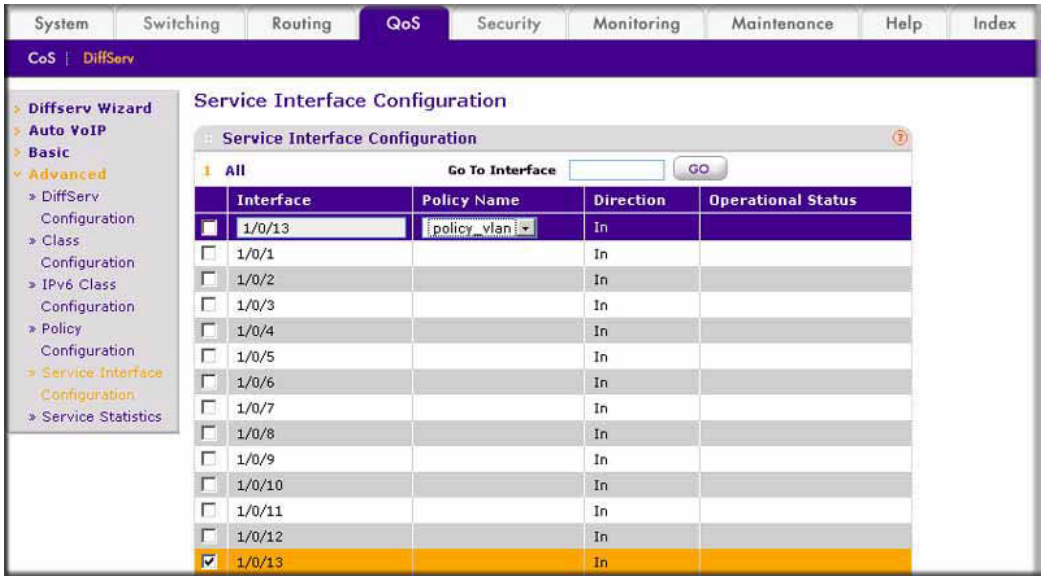
i. For Violate Action, select the **Drop** radio button.

j. Click **Apply.**

8. Apply policy_vlan to interface 1/0/13.

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

A screen similar to the following displays.



Service Interface Configuration

Service Interface Configuration

	Interface	Policy Name	Direction	Operational Status
☐	1/0/13	policy_vlan	In	
☐	1/0/1		In	
☐	1/0/2		In	
☐	1/0/3		In	
☐	1/0/4		In	
☐	1/0/5		In	
☐	1/0/6		In	
☐	1/0/7		In	
☐	1/0/8		In	
☐	1/0/9		In	
☐	1/0/10		In	
☐	1/0/11		In	
☐	1/0/12		In	
☑	1/0/13		In	

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.

10. IGMP Snooping and Querier

10

Internet Group Management Protocol features

This chapter includes the following sections:

- *Internet Group Management Protocol Concepts*
- *IGMP Snooping*
- *Show igmpsnooping*
- *Show mac-address-table igmpsnooping*
- *External Multicast Router*
- *Multicast Router Using VLAN*
- *IGMP Querier*
- *Enable IGMP Querier*
- *Show IGMP Querier Status*

Internet Group Management Protocol Concepts

NETGEAR implements Internet Group Management Protocol (IGMP) in the following way:

- IGMP uses version 1, version 2, or version 3.
- IGMP includes snooping.
- You can enable IGMP snooping on a per-VLAN basis.

IGMP Snooping

The following are examples of the commands used in the IGMP snooping feature.

CLI: Enable IGMP Snooping

The following example shows how to enable IGMP snooping.

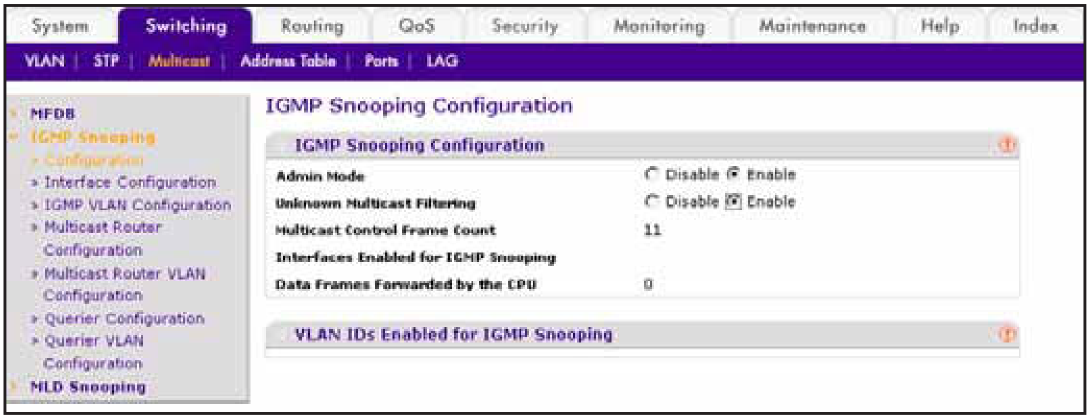
```
(Netgear Switch) #config
(Netgear Switch) (Config)#set igmp
(Netgear Switch) (Config)# set igmp unknown-multicast filter
(Netgear Switch) (Config)#exit
```

Web Interface: Enable IGMP Snooping

Configure IGMP snooping:

1. Select **Switching > Multicast > IGMP Snooping Configuration**.

   A screen similar to the following displays.



IGMP Snooping Configuration

IGMP Snooping Configuration

Admin Mode	○ Disable ● Enable
Unknown Multicast Filtering	○ Disable ☒ Enable
Multicast Control Frame Count	11
Interfaces Enabled for IGMP Snooping	
Data Frames Forwarded by the CPU	0

VLAN IDs Enabled for IGMP Snooping

2. For Admin Mode select the **Enable** radio button.
3. For Unknown Multicast Filtering, select the **Enable** radio button.
4. Click **Apply**.

Show igmpsnooping

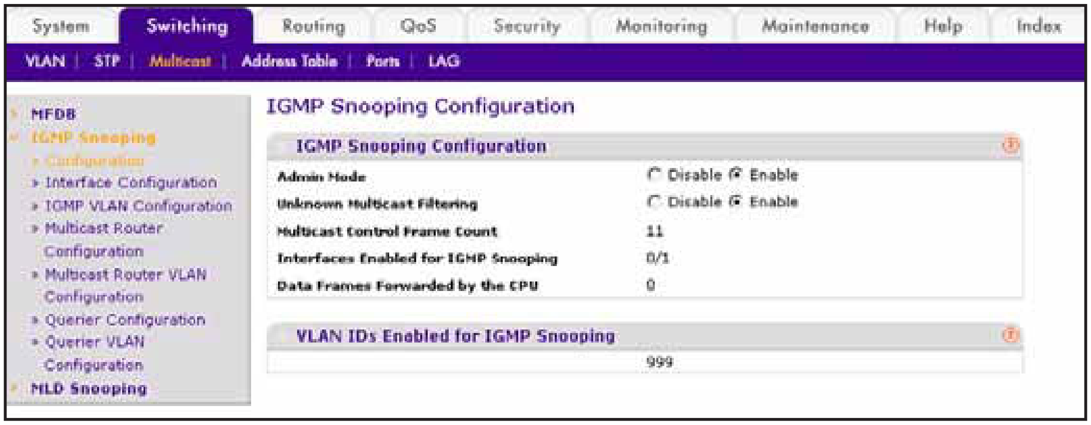
The example is shown as CLI commands and as a Web interface procedure.

CLI: Show igmpsnooping

```
(Netgear Switch) #show igmpsnooping
Admin Mode.................................... Disable
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.



IGMP Snooping Configuration

IGMP Snooping Configuration

Admin Mode	○ Disable ● Enable
Unknown Multicast Filtering	○ Disable ● Enable
Multicast Control Frame Count	11
Interfaces Enabled for IGMP Snooping	0/1
Data Frames Forwarded by the CPU	0

VLAN IDs Enabled for IGMP Snooping

999

Show mac-address-table igmpsnooping

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

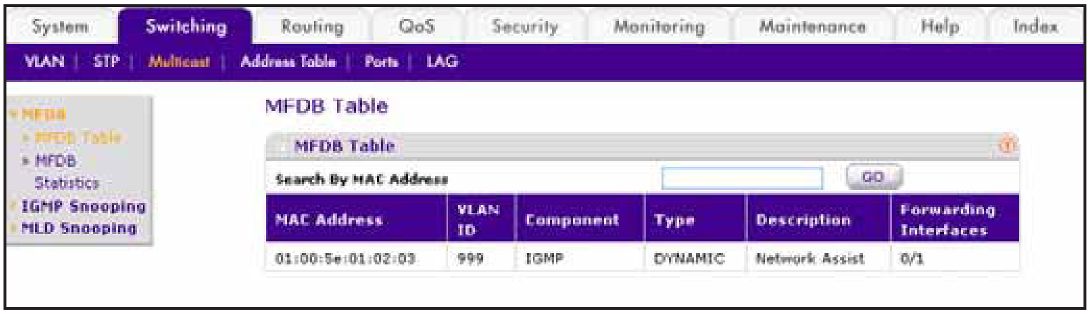
CLI: Show mac-address-table igmpsnooping

```
(Netgear Switch) #show mac-address-table igmpsnooping ?

<cr>                     Press Enter to execute the command.

(Netgear Switch) #show mac-address-table igmpsnooping

                           Type       Description       Interfaces
-----------------------    -------    --------------    -----------
00:01:01:00:5E:00:01:16    Dynamic    Network Assist    Fwd: 1/0/47
00:01:01:00:5E:00:01:18    Dynamic    Network Assist    Fwd: 1/0/47
00:01:01:00:5E:37:96:D0    Dynamic    Network Assist    Fwd: 1/0/47
00:01:01:00:5E:7F:FF:FA    Dynamic    Network Assist    Fwd: 1/0/47
00:01:01:00:5E:7F:FF:FE    Dynamic    Network Assist    Fwd: 1/0/47
```

Web Interface: Show mac-address-table igmpsnooping

Select **Switching > Multicast > IGMP Snooping Table**.

A screen similar to the following displays.



MFDB Table

MFDB Table

Search By MAC Address

MAC Address	VLAN ID	Component	Type	Description	Forwarding Interfaces
01:00:5e:01:02:03	999	IGMP	DYNAMIC	Network Assist	0/1

External Multicast Router

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

CLI: Configure the Switch with an External Multicast Router

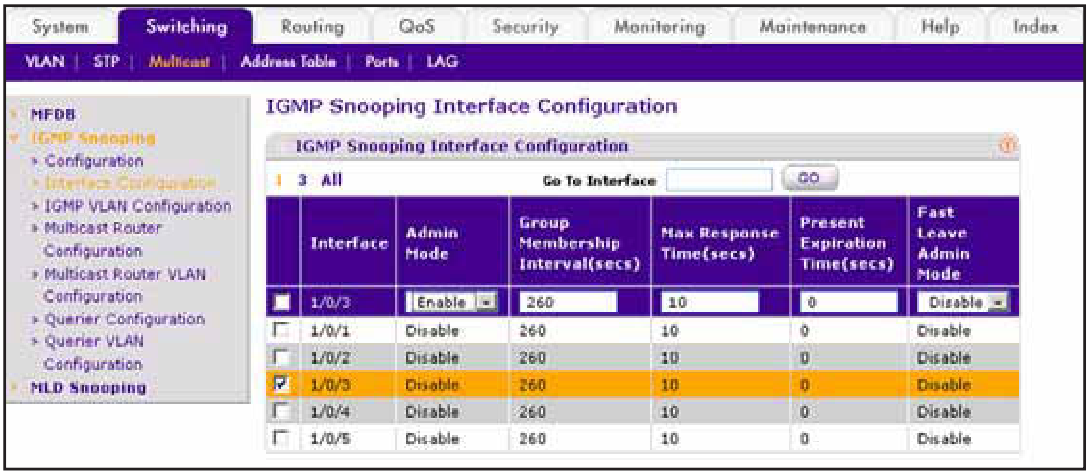
This example configures the interface as the one the multicast router is attached to. All IGMP packets snooped by the switch is forwarded to the multicast router reachable from this interface.

```
(Netgear Switch)(Interface 1/0/3)# set igmp mrouter interface
```

Web Interface: Configure the Switch with an External Multicast Router

1. Select **Switching > Multicast > Multicast Router Configuration**.

   A screen similar to the following displays.



IGMP Snooping Interface Configuration

IGMP Snooping Interface Configuration

1 3 All Go To Interface

	Interface	Admin Mode	Group Membership Interval(secs)	Max Response Time(secs)	Present Expiration Time(secs)	Fast Leave Admin Mode
□	1/0/3	Enable	260	10	0	Disable
□	1/0/1	Disable	260	10	0	Disable
□	1/0/2	Disable	260	10	0	Disable
☑	1/0/3	Disable	260	10	0	Disable
□	1/0/4	Disable	260	10	0	Disable
□	1/0/5	Disable	260	10	0	Disable

2. Under Multicast Router Configuration, scroll down and select the Interface **1/0/3** check box.

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

3. In the Admin Mode field, select **Enable**.

4. Click **Apply**.

Multicast Router Using VLAN

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

CLI: Configure the Switch with a Multicast Router Using VLAN

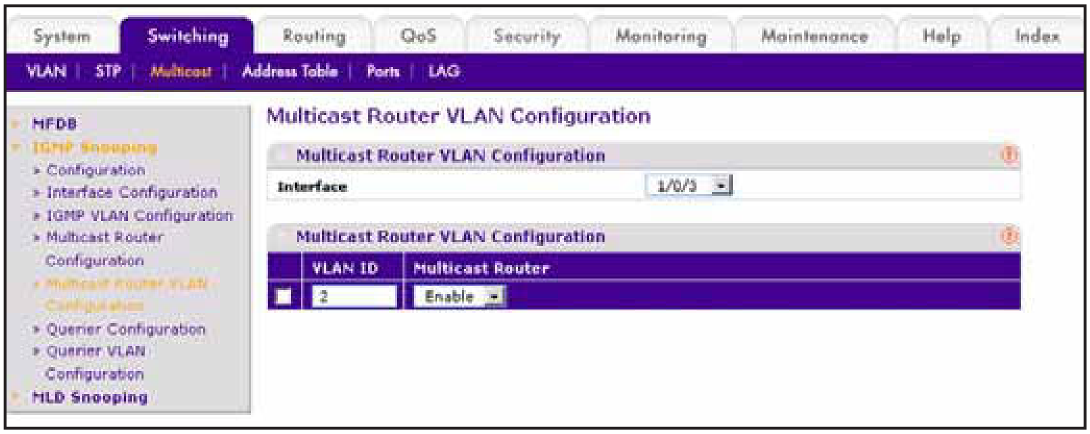
This example configures the interface to forward only the snooped IGMP packets that come from VLAN ID (<VLAN Id>) to the multicast router attached to this interface.

```
(Netgear Switch)(Interface 1/0/3)# set igmp mrouter 2
```

Web Interface: Configure the Switch with a Multicast Router Using VLAN

1. Select **Switching > Multicast > Multicast Router VLAN Configuration**.

   A screen similar to the following displays.



Multicast Router VLAN Configuration

Multicast Router VLAN Configuration

Interface 1/0/3

Multicast Router VLAN Configuration

	VLAN ID	Multicast Router
□	2	Enable

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.

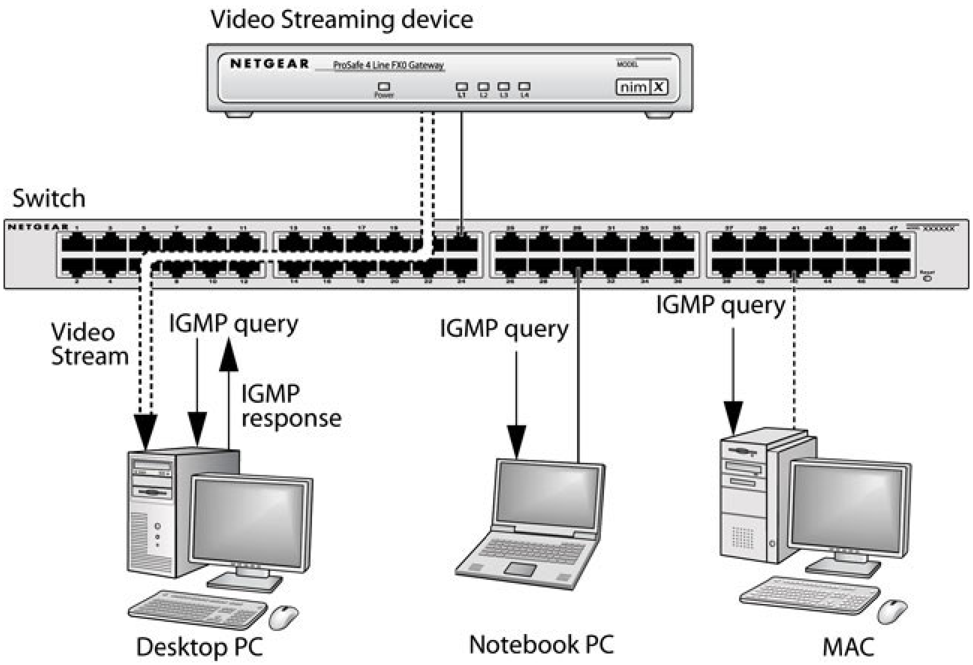


Figure 19. IGMP querier

Since the IGMP querier is designed to work with IGMP snooping, it is necessary to enable IGMP snooping when using it. The following figure shows a network application for video streaming service using the IGMP querier feature.

Enable IGMP Querier

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

CLI: Enable IGMP Querier

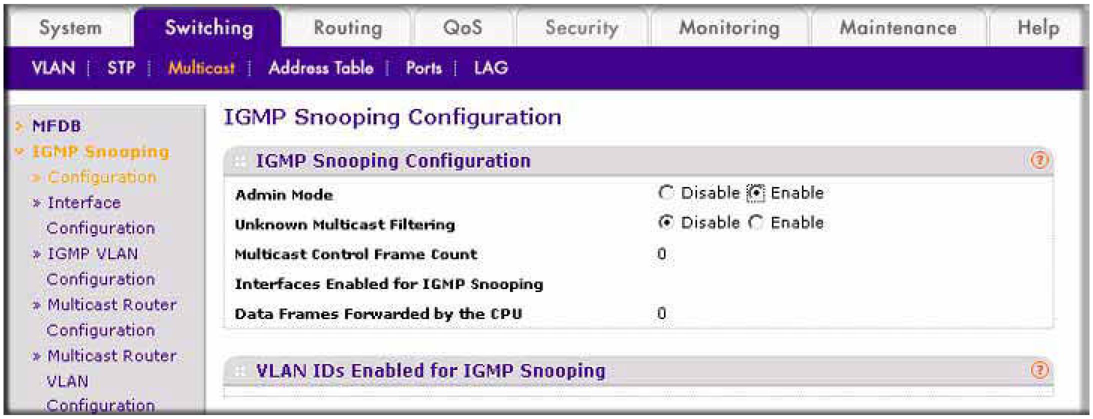
Use the following CLI commands to set up the switch to generate an IGMP querier packet for a designated VLAN. The IGMP packet will be transmitted to every port on the VLAN. The following example enables the querier for VLAN 1 and uses 10.10.10.1 as the source IP address in querier packets. See the *Command Line Reference* for more details about other IGMP querier command options.

```
(Netgear switch) #vlan database
(Netgear switch) (vlan)#set igmp 1
(Netgear switch) (vlan)#set igmp querier 1
(Netgear switch) (vlan)#exit
(Netgear switch) #config
(Netgear switch) (config)#set igmp querier
(Netgear switch) (config)#set igmp querier address 10.10.10.1
(Netgear switch) (config)#exit
```

Web Interface: Enable IGMP Querier

1. Select **Switching > Multicast > IGMP VLAN Configuration**.

   A screen similar to the following displays.



IGMP Snooping Configuration

IGMP Snooping Configuration

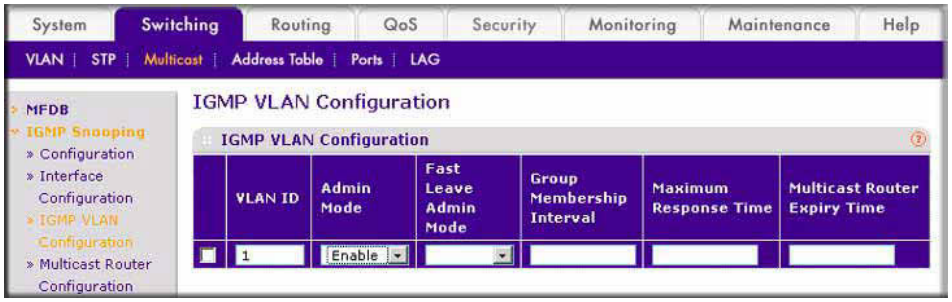
Admin Mode ○ Disable ● Enable
Unknown Multicast Filtering ● Disable ○ Enable
Multicast Control Frame Count 0
Interfaces Enabled for IGMP Snooping
Data Frames Forwarded by the CPU 0

VLAN IDs Enabled for IGMP Snooping

2. Enable IGMP snooping on VLAN 1.

   a. Select **Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration**.

A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
VLAN | STP | Multicast | Address Table | Ports | LAG
MFDB
IGMP Snooping
» Configuration
» Interface Configuration
» IGMP VLAN Configuration
» Multicast Router Configuration

IGMP VLAN Configuration

IGMP VLAN Configuration

	VLAN ID	Admin Mode	Fast Leave Admin Mode	Group Membership Interval	Maximum Response Time	Multicast Router Expiry Time
□	1	Enable				

b. Enter the following information:

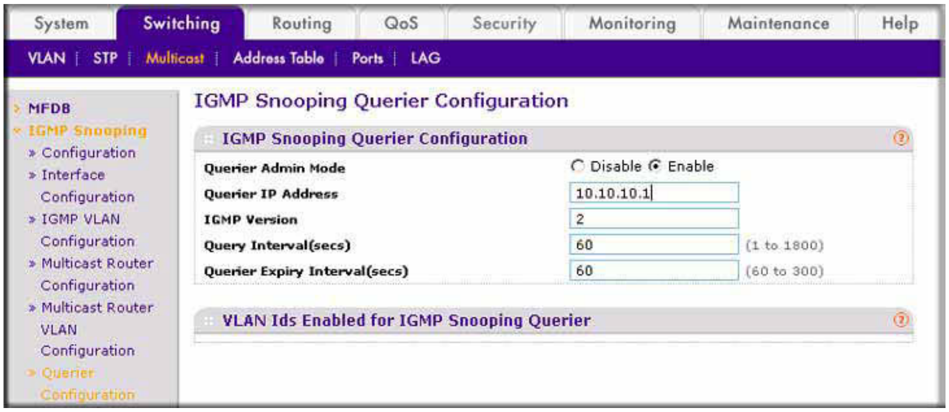
- In the **VLAN ID** field, enter **1**.
- In the **Admin Mode** field, select **Enable**.

c. Click **Add**.

3. Enable the IGMP snooping querier globally.

a. Select **Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration**.

A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
VLAN | STP | Multicast | Address Table | Ports | LAG
MFDB
IGMP Snooping
» Configuration
» Interface Configuration
» IGMP VLAN Configuration
» Multicast Router Configuration
» Multicast Router VLAN Configuration
» Querier Configuration

IGMP Snooping Querier Configuration

IGMP Snooping Querier Configuration

Querier Admin Mode	○ Disable ● Enable	
Querier IP Address	10.10.10.1	
IGMP Version	2	
Query Interval(secs)	60	(1 to 1800)
Querier Expiry Interval(secs)	60	(60 to 300)

VLAN Ids Enabled for IGMP Snooping Querier

b. Enter the following information:

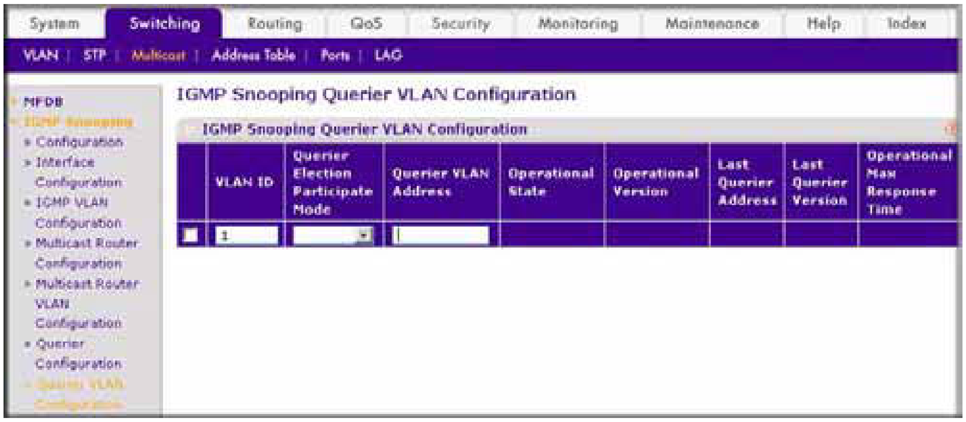
- For Querier Admin Mode, select the **Enable** radio button.
- In the **Querier IP Address** field, enter **10.10.10.1**.

c. Click **Apply**.

4. Enable the IGMP snooping querier on VLAN 1.

a. Select **Switching > Multicast > IGMP Snooping Querier VLAN Configuration**.

A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
VLAN | STP | Multicast | Address Table | Ports | LAG
MFDB
IGMP Snooping
» Configuration
» Interface Configuration
» IGMP VLAN Configuration
» Multicast Router Configuration
» Multicast Router VLAN Configuration
» Querier Configuration
» Querier VLAN Configuration

IGMP Snooping Querier VLAN Configuration

IGMP Snooping Querier VLAN Configuration

	VLAN ID	Querier Election Participate Mode	Querier VLAN Address	Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Max Response Time
□	1							

b. In the **VLAN ID** field, enter **1**.

5. Click **Add**.

Show IGMP Querier Status

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

CLI: Show IGMP Querier Status

To see the IGMP querier status, use the following command.

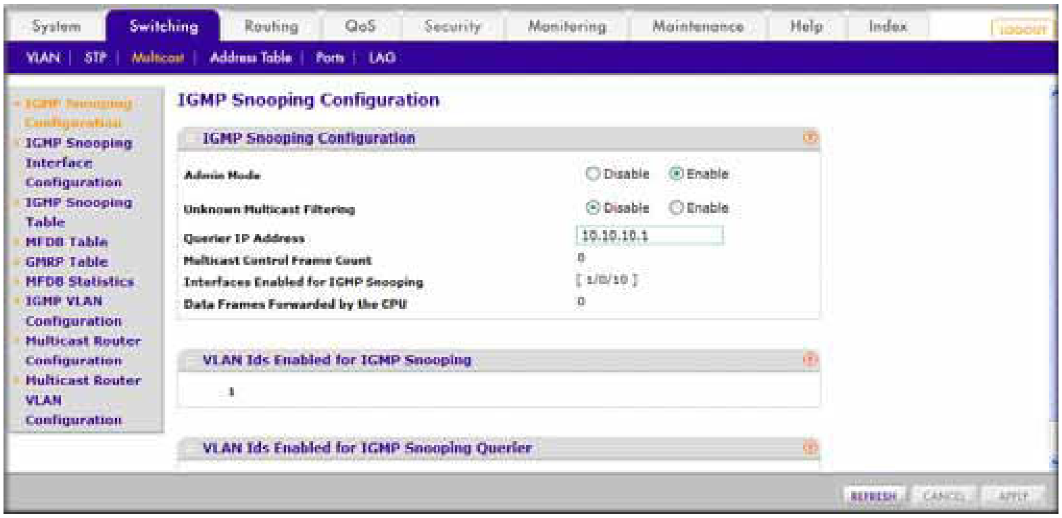
```
(Netgear Switch) #show igmpsnooping querier vlan 1
VLAN 1 : IGMP Snooping querier status
----------------------------------------------
IGMP Snooping Querier VLAN Mode................ Enable
Querier Election Participate Mode............. Disable
Querier VLAN Address.......................... 0.0.0.0
Operational State............................. Disabled
Operational version........................... 2
```

The command shows that the IGMP admin mode is Active. The mode is controlled by the **set igmp** command. If the mode is inactive, no query packet is sent.

Web Interface: Show IGMP Querier Status

1. Select **Switching > Multicast > IGMP Snooping Configuration**.

A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
LOGOUT
VLAN | STP | Multicast | Address Table | Ports | LAG
IGMP Snooping Configuration
IGMP Snooping Interface Configuration
IGMP Snooping Table
MFDB Table
GMRP Table
MFDB Statistics
IGMP VLAN Configuration
Multicast Router Configuration
Multicast Router VLAN Configuration
REFRESH
CANCEL
APPLY

IGMP Snooping Configuration

IGMP Snooping Configuration

Admin Mode	○ Disable ● Enable
Unknown Multicast Filtering	● Disable ○ Enable
Querier IP Address	10.10.10.1
Multicast Control Frame Count	0
Interfaces Enabled for IGMP Snooping	[1/0/10]
Data Frames Forwarded by the CPU	0

VLAN Ids Enabled for IGMP Snooping

1

VLAN Ids Enabled for IGMP Snooping Querier

2. Click **Refresh**.

11. MVR 11

Multicast VLAN Registration

This chapter includes the following sections:

MVR Concepts

The IGMP Layer 3 protocol is widely used for IPv4 network multicasting. In Layer 2 networks, the IGMP protocol uses resources inefficiently. For example, a Layer 2 switch multicast traffic to all ports even if there are receivers connected to only a few ports.

To address this problem, the IGMP Snooping protocol was developed. But the problem reappears when receivers are in different VLANs. Multicast VLAN registration (MVR) is intended to solve the problem of receivers in different VLANs. It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.

MVR, like the IGMP Snooping protocol, allows a Layer 2 switch to snoop on the IGMP control protocol. Both protocols operate independently of each other. Both protocols can be enabled on the switch interfaces at the same time. In such a case, MVR listens to the join and report messages only for groups configured statically. All other groups are managed by IGMP snooping.

There are two types of MVR ports: source and receiver.

- The source port is the port to which the multicast traffic flows using the multicast VLAN.
- The receiver port is the port where a listening host is connected to the switch. It can utilize any (or no) VLAN, except the multicast VLAN. This implies that the MVR switch performs VLAN tag substitution from the multicast VLAN source port to the VLAN tag used by the receiver port.

The Multicast VLAN is the VLAN that is configured in the specific network for MVR purposes. It has to be manually specified by the operator for all source ports in the network. It is a VLAN that is used to transfer multicast traffic over the network to avoid duplication of multicast streams for clients in different VLANs. A diagram of a network configured for MVR is shown in the following illustration. SP is the source port and RP is the receiver port.

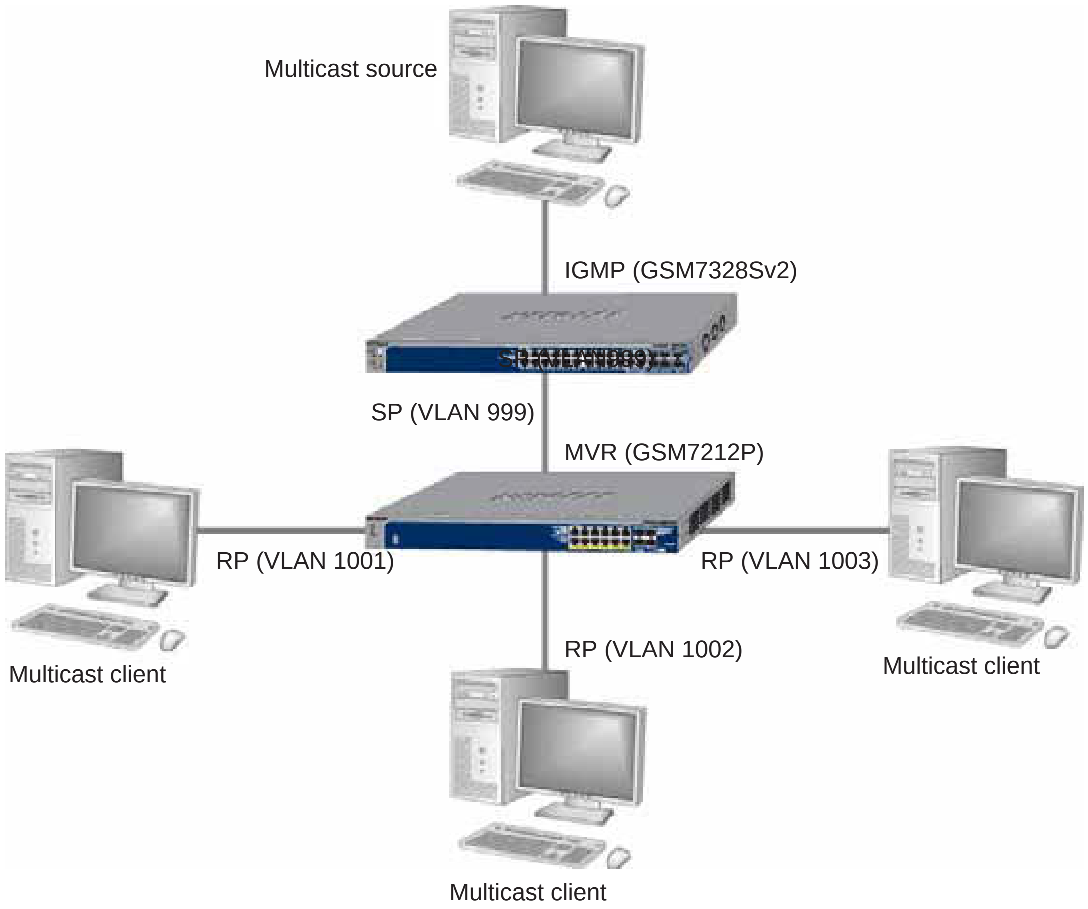


Figure 20. Network configured for MVR

Note: The following examples show how to configure the MVR on the MVR switch (GSM7212P in this case).

Configure MVR in Compatible Mode

In compatible mode, the MVR switch does not learn multicast groups; the groups have to be configured by the operator as the MVR does not forward IGMP reports from the hosts (RP port) to the IGMP router (SP port). To operate in this mode, the IGMP router has to be statically configured to transmit all required multicast streams to the MVR switch.

CLI: Configure MVR in Compatible Mode

1. Create mVlan, VLAN1, VLAN2, and VLAN3.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 999,1001, 1002, 1003
(Netgear Switch) (Vlan)#vlan name 999 mVlan
(Netgear Switch) (Vlan)#vlan name 1001 Vlan1
(Netgear Switch) (Vlan)#vlan name 1002 Vlan2
(Netgear Switch) (Vlan)#vlan name 1003 Vlan3
(Netgear Switch) (Vlan)#exit
```

2. Enable MVR, configure VLAN 999 as a multicast VLAN, and add group 224.1.2.3 to MVR.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#mvr
(Netgear Switch) (Config)#mvr vlan 999
(Netgear Switch) (Config)#mvr group 224.1.2.3
```

3. Configure multicast VLAN on the source port.

```
(Netgear Switch) (Config)#interface 0/9
(Netgear Switch) (Interface 0/9)#vlan participation include 999
(Netgear Switch) (Interface 0/9)#vlan tagging 999
(Netgear Switch) (Interface 0/9)#mvr
(Netgear Switch) (Interface 0/9)#mvr type source
(Netgear Switch) (Interface 0/9)#exit
```

4. Configure the receive ports.

Note: The receive port can participate in only one VLAN.

```
(Netgear Switch) (Config)#interface 0/1
(Netgear Switch) (Interface 0/1)#vlan participation include 1001
(Netgear Switch) (Interface 0/1)#vlan pvid 1001
(Netgear Switch) (Interface 0/1)#vlan participation exclude 1
(Netgear Switch) (Interface 0/1)#mvr
(Netgear Switch) (Interface 0/1)#mvr type receiver
(Netgear Switch) (Interface 0/1)#mvr vlan 999 group 224.1.2.3
(Netgear Switch) (Interface 0/1)#exit

(Netgear Switch) (Config)#interface 0/5
(Netgear Switch) (Interface 0/5)#vlan participation include 1002
(Netgear Switch) (Interface 0/5)#vlan pvid 1002
(Netgear Switch) (Interface 0/5)#vlan participation exclude 1
(Netgear Switch) (Interface 0/5)#mvr
(Netgear Switch) (Interface 0/5)#mvr stype receiver
(Netgear Switch) (Interface 0/5)#mvr vlan 999 group 224.1.2.3
(Netgear Switch) (Interface 0/5)#exit

(Netgear Switch) (Config)#interface 0/7
(Netgear Switch) (Interface 0/7)#vlan participation include1003
(Netgear Switch) (Interface 0/7)#vlan pvid 1003
(Netgear Switch) (Interface 0/7)#vlan participation exclude 1
(Netgear Switch) (Interface 0/7)#mvr
(Netgear Switch) (Interface 0/7)#mvr type receiver
(Netgear Switch) (Interface 0/7)#mvr vlan 999 group 224.1.2.3
(Netgear Switch) (Interface 0/7)#exit
```

5. Show mvr status.

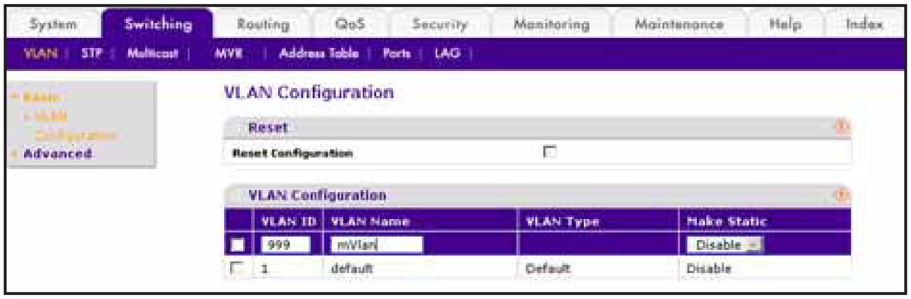
```
(Netgear Switch) #show mvr
MVR Running....................... TRUE
MVR multicast VLAN................ 999
MVR Max Multicast Groups.......... 256
MVR Current multicast groups...... 1
MVR Global query response time.... 5 (tenths of sec)
MVR Mode.......................... compatible
 (Netgear Switch) #show mvr interface
Port           Type               Status               Immediate Leave
-----------     ---------------           -------------------
---------------
0/1          RECEIVER           ACTIVE/InVLAN          DISABLED
0/5          RECEIVER           ACTIVE/InVLAN          DISABLED
0/7          RECEIVER           ACTIVE/InVLAN          DISABLED
0/9          SOURCE             ACTIVE/InVLAN          DISABLED
```

Web Interface: Configure MVR in Compatible Mode

1. Create MVLAN 999, VLAN1 1001, VLAN2 1002 and VLAN3 1003.

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

   A screen similar to the following displays:



Reset Configuration □

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type	Make Static
□	999	mVlan		Disable
□	1	default	Default	Disable

   b. In the VLAN ID field, enter **999**, and in the VLAN Name field, enter **mVlan**.

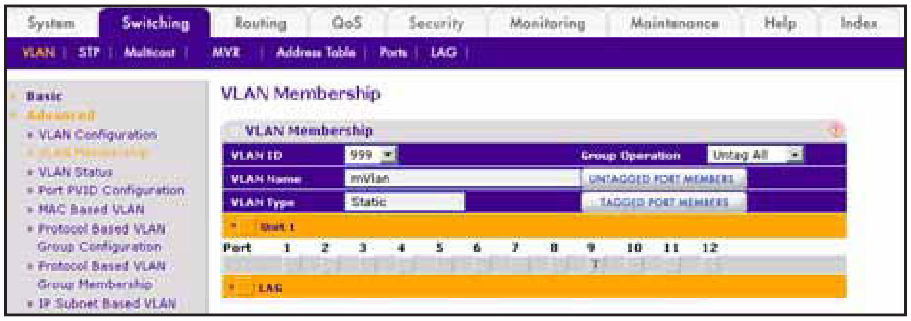
   c. Click **Add**.

   d. Repeat step b and c to create VLAN1 1001, VLAN2 1002, and VLAN3 1003.

2. Add port 9 into MVLAN 999 with tagged mode.

   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

   A screen similar to the following displays:



VLAN Membership

VLAN ID 999
Group Operation Untag All
VLAN Name mVlan
VLAN Type Static

Port	1	2	3	4	5	6	7	8	9	10	11	12
									T			

   b. In the VLAN ID list, select **999**.

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

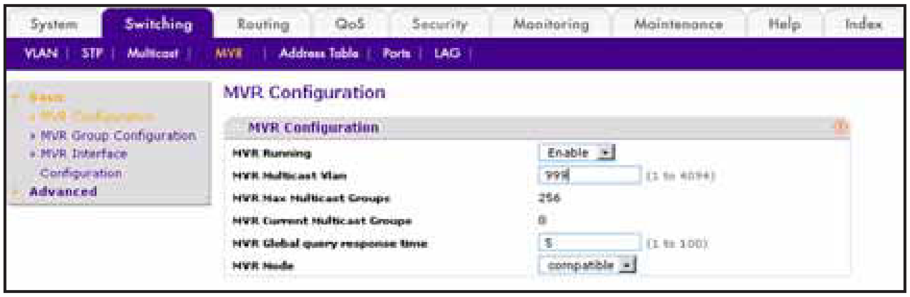
   d. Click the gray box under port 9 until T displays. The T specifies that the egress packet is tagged for the ports.

   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:


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
VLAN | STP | Multicast | MVR | Address Table | Ports | LAG |
Basic
» MVR Configuration
» MVR Group Configuration
» MVR Interface Configuration
Advanced

MVR Configuration

MVR Configuration	
MVR Running	Enable
MVR Multicast Vlan	999 (1 to 4094)
MVR Max Multicast Groups	256
MVR Current Multicast Groups	0
MVR Global query response time	5 (1 to 100)
MVR Mode	compatible

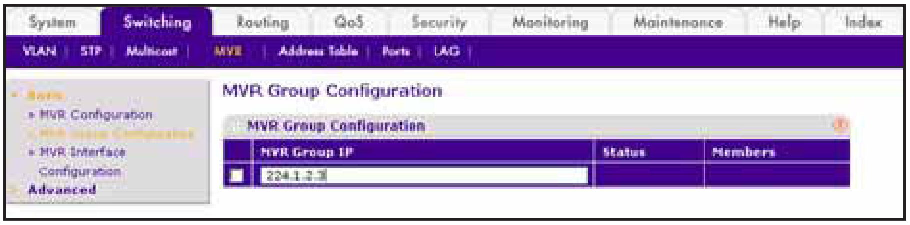
b. For MVR Running, select **Enable**.

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:


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
VLAN | STP | Multicast | MVR | Address Table | Ports | LAG |
Basic
» MVR Configuration
» MVR Group Configuration
» MVR Interface Configuration
Advanced

MVR Group Configuration

MVR Group Configuration

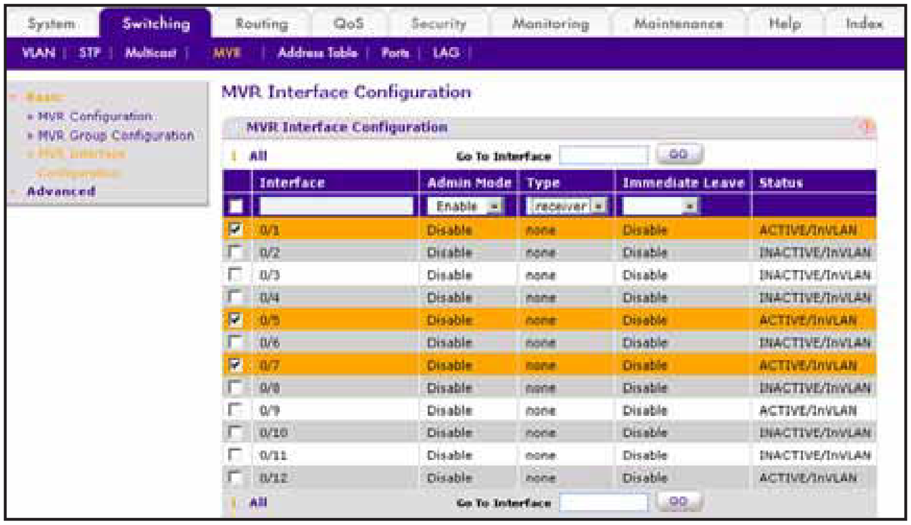
	MVR Group IP	Status	Members
□	224.1.2.3		

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:


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
VLAN | STP | Multicast | MVR | Address Table | Ports | LAG |
Basic
» MVR Configuration
» MVR Group Configuration
» MVR Interface Configuration
Advanced
GO

MVR Interface Configuration

MVR Interface Configuration

All   Go To Interface

	Interface	Admin Mode	Type	Immediate Leave	Status
□		Enable	receiver		
☑	0/1	Disable	none	Disable	ACTIVE/InVLAN
□	0/2	Disable	none	Disable	INACTIVE/InVLAN
□	0/3	Disable	none	Disable	INACTIVE/InVLAN
□	0/4	Disable	none	Disable	INACTIVE/InVLAN
☑	0/5	Disable	none	Disable	ACTIVE/InVLAN
□	0/6	Disable	none	Disable	INACTIVE/InVLAN
☑	0/7	Disable	none	Disable	ACTIVE/InVLAN
□	0/8	Disable	none	Disable	INACTIVE/InVLAN
□	0/9	Disable	none	Disable	ACTIVE/InVLAN
□	0/10	Disable	none	Disable	INACTIVE/InVLAN
□	0/11	Disable	none	Disable	INACTIVE/InVLAN
□	0/12	Disable	none	Disable	ACTIVE/InVLAN

All   Go To Interface

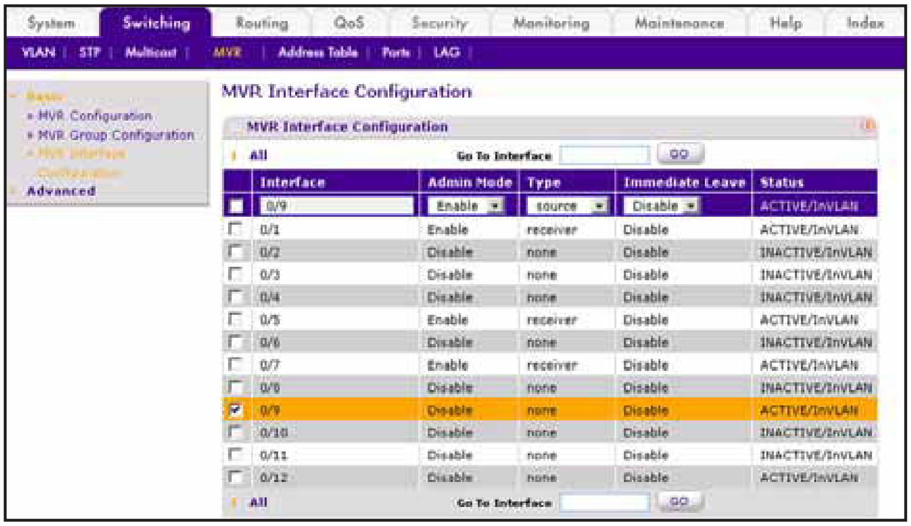
b. Under MVR Interface Configuration, scroll down and select the Interface **0/1**, **0/5** and **0/7** check boxes.

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

MVR Interface Configuration

	Interface	Admin Mode	Type	Immediate Leave	Status
□	0/9	Enable	source	Disable	ACTIVE/InVLAN
□	0/1	Enable	receiver	Disable	ACTIVE/InVLAN
□	0/2	Disable	none	Disable	INACTIVE/InVLAN
□	0/3	Disable	none	Disable	INACTIVE/InVLAN
□	0/4	Disable	none	Disable	INACTIVE/InVLAN
□	0/5	Enable	receiver	Disable	ACTIVE/InVLAN
□	0/6	Disable	none	Disable	INACTIVE/InVLAN
□	0/7	Enable	receiver	Disable	ACTIVE/InVLAN
□	0/8	Disable	none	Disable	INACTIVE/InVLAN
☑	0/9	Disable	none	Disable	ACTIVE/InVLAN
□	0/10	Disable	none	Disable	INACTIVE/InVLAN
□	0/11	Disable	none	Disable	INACTIVE/InVLAN
□	0/12	Disable	none	Disable	ACTIVE/InVLAN

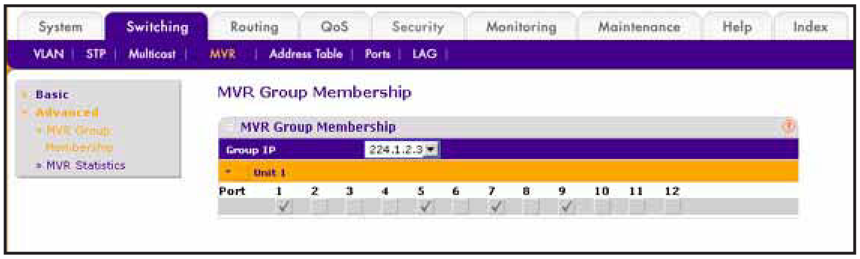
b. Under MVR Interface Configuration, scroll down and select the Interface **0/9** check box.

c. Enter the following information:
   - In the Admin Mode list, select **Enable**.
   - In the Type list, select **source**.

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

7. Configure MVR Group Membership.

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



MVR Group Membership

MVR Group Membership

Group IP 224.1.2.3

Port	1	2	3	4	5	6	7	8	9	10	11	12
	✓				✓		✓		✓			

b. In the Group IP list, select **224.1.2.3**.

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

d. Click the gray boxes under ports **1**, **5**, and **7**. (Port 9 is already in MVR group 224.1.2.3 because it is configured as the source port.)

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

Configure MVR in Dynamic Mode

CLI: Configure MVR in Dynamic Mode

In dynamic mode, the MVR switch learns existing multicast groups by snooping the IGMP queries from router on source ports and forwarding the IGMP reports from the hosts to the IGMP router on the Multicast VLAN (with appropriate translation of the VLAN ID).

1. Create MVLAN, VLAN1, VLAN2, and VLAN3.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 999,1001, 1002, 1003
(Netgear Switch) (Vlan)#vlan name 999 mVlan
(Netgear Switch) (Vlan)#vlan name 1001 Vlan1
(Netgear Switch) (Vlan)#vlan name 1002 Vlan2
(Netgear Switch) (Vlan)#vlan name 1003 Vlan3
(Netgear Switch) (Vlan)#exit
```

2. Enable MVR, configure VLAN 999 as a multicast VLAN, and add group 224.1.2.3 to MVR.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#mvr
(Netgear Switch) (Config)#mvr vlan 999
(Netgear Switch) (Config)#mvr group 224.1.2.3
```

3. Configure MVR in dynamic mode.

```
(Netgear Switch) (Config)#mvr mode dynamic
```

4. Configure multicast VLAN on the source port.

```
(Netgear Switch) (Config)#interface 0/9
(Netgear Switch) (Interface 0/9)#vlan participation include 999
(Netgear Switch) (Interface 0/9)#vlan tagging 999
(Netgear Switch) (Interface 0/9)#mvr
(Netgear Switch) (Interface 0/9)#mvr type source
(Netgear Switch) (Interface 0/9)#exit
```

5. Configure the receive ports.

Note: A receive port can participate in only one VLAN.

```
(Netgear Switch) (Config)#interface 0/1
(Netgear Switch) (Interface 0/1)#vlan participation include 1001
(Netgear Switch) (Interface 0/1)#vlan pvid 1001
(Netgear Switch) (Interface 0/1)#vlan participation exclude 1
(Netgear Switch) (Interface 0/5)#mvr
(Netgear Switch) (Interface 0/1)#mvr type receiver
(Netgear Switch) (Interface 0/1)#exit

(Netgear Switch) (Config)#interface 0/5
(Netgear Switch) (Interface 0/5)#vlan participation include 1002
(Netgear Switch) (Interface 0/5)#vlan pvid 1002
(Netgear Switch) (Interface 0/5)#vlan participation exclude 1
(Netgear Switch) (Interface 0/5)#mvr
(Netgear Switch) (Interface 0/5)#mvr stype receiver
(Netgear Switch) (Interface 0/5)#exit

(Netgear Switch) (Config)#interface 0/7
(Netgear Switch) (Interface 0/7)#vlan participation include1003
(Netgear Switch) (Interface 0/7)#vlan pvid 1003
(Netgear Switch) (Interface 0/7)#vlan participation exclude 1
(Netgear Switch) (Interface 0/7)#mvr
(Netgear Switch) (Interface 0/7)#mvr type receiver
(Netgear Switch) (Interface 0/7)#exit
```

6. Show the MVR status.

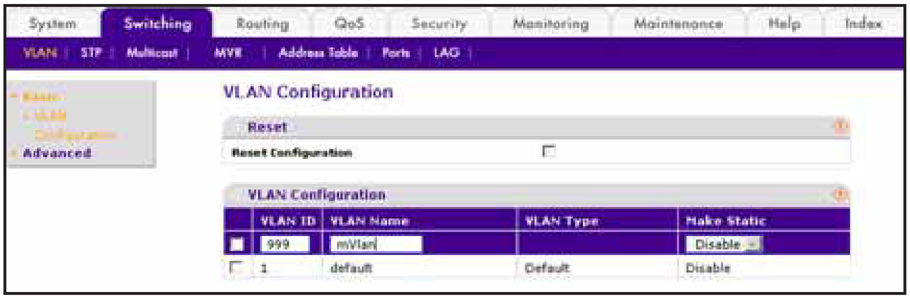
```
(Netgear Switch) #show mvr
MVR Running....................... TRUE
MVR multicast VLAN................ 999
MVR Max Multicast Groups.......... 256
MVR Current multicast groups...... 1
MVR Global query response time.... 5 (tenths of sec)
MVR Mode.......................... compatible
 (Netgear Switch) #show mvr interface
Port           Type                Status                Immediate Leave
-----------     ---------------           -------------------
---------------
0/1          RECEIVER           ACTIVE/InVLAN          DISABLED
0/5          RECEIVER           ACTIVE/InVLAN          DISABLED
0/7          RECEIVER           ACTIVE/InVLAN          DISABLED
0/9          SOURCE             ACTIVE/InVLAN          DISABLED
```

7. After port 0/1 receive IGMP report for Multicast Group 224.1.2.3, it will be added to the MVR Group 224.1.2.3.

```
(Netgear Switch) #show mvr members

MVR Group IP        Status              Members
---------------     ---------------     -------------------------------------
224.1.2.3           ACTIVE              0/1(d)
```

Web Interface: Configure MVR in Dynamic Mode

1. Create MVLAN 999, VLAN1 1001, VLAN2 1002, and VLAN3 1003.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**. A screen similar to the following displays:



VLAN Configuration

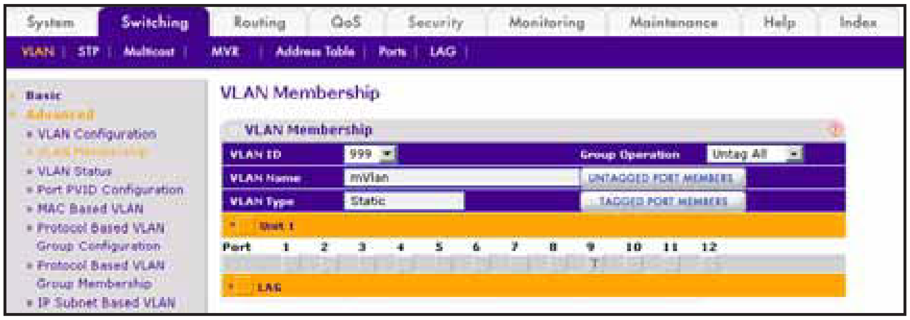
Reset

Reset Configuration □

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type	Make Static
□	999	mVlan		Disable
□	1	default	Default	Disable

   b. In the VLAN ID field, enter **999**, and in the VLAN Name field, enter **mVlan**.
   c. Click **Add**.
   d. Repeat step b and c to create VLAN1 1001, VLAN2 1002, and VLAN3 1003.
   e. Add port 9 into MVLAN 999 with tagged mode.
   f. Select **Switching > VLAN > Advanced > VLAN Membership**. A screen similar to the following displays:



VLAN Membership

VLAN ID 999
Group Operation Untag All
VLAN Name mVlan
VLAN Type Static

Port 1 2 3 4 5 6 7 8 9 10 11 12

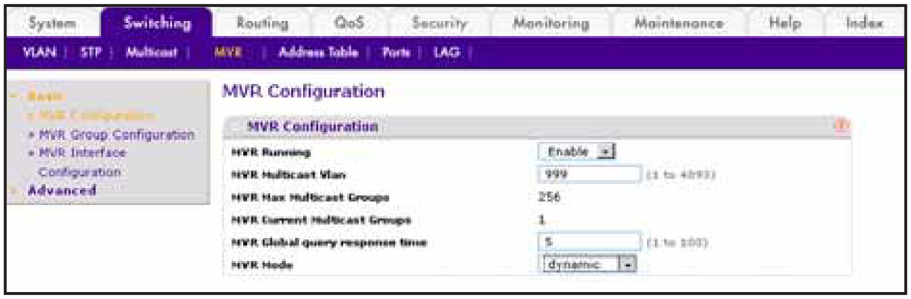
T

   g. In the VLAN ID list, select **999**.
   h. Click **Unit 1**. The ports display.
   i. Click the gray boxes under port **9** until T displays. The T specifies that the egress packet is tagged for the ports.
   j. Click **Apply** to save the settings.

k. Repeat steps from b to e, add port 0/1 to VLAN1 1001, add port 0/5 to VLAN2 1002, and add port 0/7 to VLAN3 1003.

2. Enable MVR and multicast VLAN.

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



MVR Configuration

MVR Configuration		
MVR Running	Enable	
MVR Multicast Vlan	999	(1 to 4093)
MVR Max Multicast Groups	256	
MVR Current Multicast Groups	1	
MVR Global query response time	5	(1 to 100)
MVR Mode	dynamic	

   b. From the MVR Running list, select **Enable**.

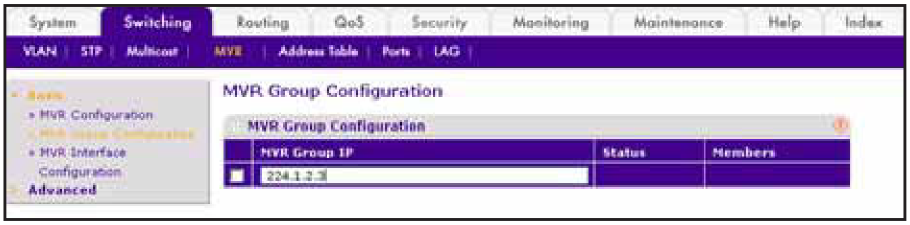
   c. In the MVR Multicast Vlan field, enter **999**.

   d. From the MVR mode list, select **dynamic**.

   e. Click **Apply**.

3. Add multicast group 224.1.2.3 to the MVR.

   a. Select **Switching > MVR > Basic > MVR Group Configuration**. A screen similar to the following displays:



MVR Group Configuration

MVR Group Configuration

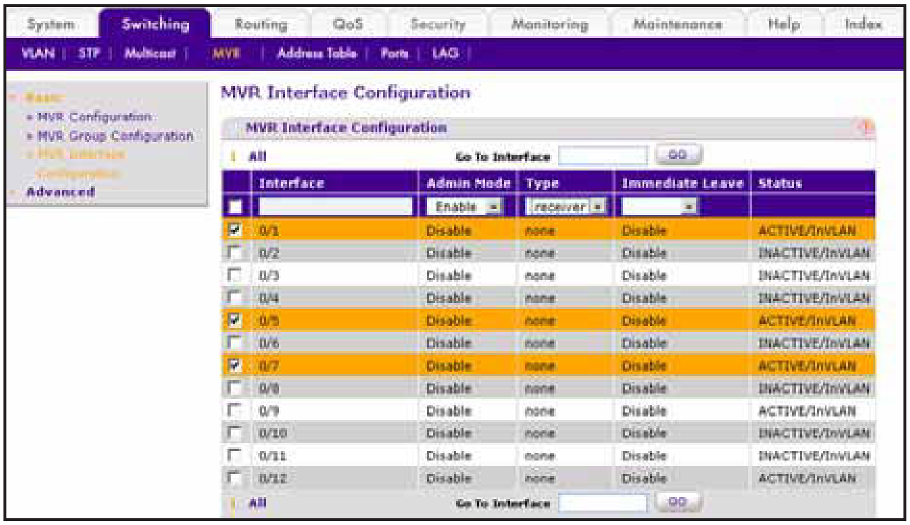
	MVR Group IP	Status	Members
□	224.1.2.3		

   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

MVR Interface Configuration

	Interface	Admin Mode	Type	Immediate Leave	Status
□		Enable	receiver		
☑	0/1	Disable	none	Disable	ACTIVE/InVLAN
□	0/2	Disable	none	Disable	INACTIVE/InVLAN
□	0/3	Disable	none	Disable	INACTIVE/InVLAN
□	0/4	Disable	none	Disable	INACTIVE/InVLAN
☑	0/5	Disable	none	Disable	ACTIVE/InVLAN
□	0/6	Disable	none	Disable	INACTIVE/InVLAN
☑	0/7	Disable	none	Disable	ACTIVE/InVLAN
□	0/8	Disable	none	Disable	INACTIVE/InVLAN
□	0/9	Disable	none	Disable	ACTIVE/InVLAN
□	0/10	Disable	none	Disable	INACTIVE/InVLAN
□	0/11	Disable	none	Disable	INACTIVE/InVLAN
□	0/12	Disable	none	Disable	ACTIVE/InVLAN

b. Under MVR Interface Configuration, scroll down and select the Interface **0/1**, **0/5** and **0/7** check boxes

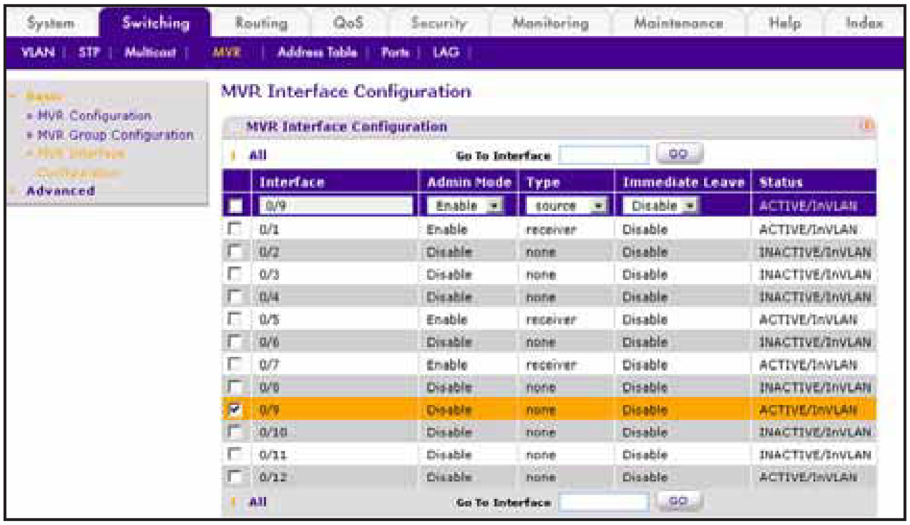
c. Enter the following information:

- In the Admin Mode list, select **Enable**.
- In the Type list, select **Receiver**.

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

5. Configure a source interface.

a. Select **Switching > MVR > Basic > MVR Interface Configuration**. A screen similar to the following displays:



MVR Interface Configuration

MVR Interface Configuration

	Interface	Admin Mode	Type	Immediate Leave	Status
□	0/9	Enable	source	Disable	ACTIVE/InVLAN
□	0/1	Enable	receiver	Disable	ACTIVE/InVLAN
□	0/2	Disable	none	Disable	INACTIVE/InVLAN
□	0/3	Disable	none	Disable	INACTIVE/InVLAN
□	0/4	Disable	none	Disable	INACTIVE/InVLAN
□	0/5	Enable	receiver	Disable	ACTIVE/InVLAN
□	0/6	Disable	none	Disable	INACTIVE/InVLAN
□	0/7	Enable	receiver	Disable	ACTIVE/InVLAN
□	0/8	Disable	none	Disable	INACTIVE/InVLAN
☑	0/9	Disable	none	Disable	ACTIVE/InVLAN
□	0/10	Disable	none	Disable	INACTIVE/InVLAN
□	0/11	Disable	none	Disable	INACTIVE/InVLAN
□	0/12	Disable	none	Disable	ACTIVE/InVLAN

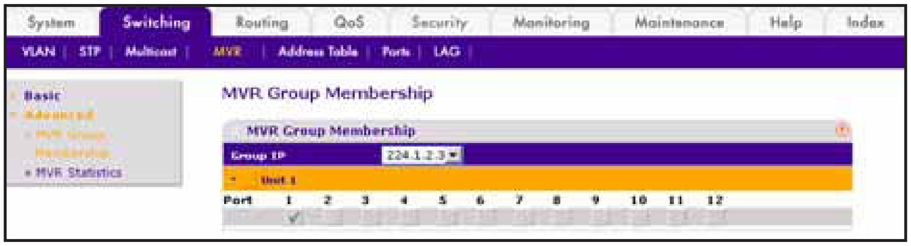
b. Under MVR Interface Configuration, scroll down and select the Interface **0/9** check box.

c. Enter the following information:
   - In the Admin Mode list, select **Enable**.
   - In the Type list, select **source**.

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

6. After port 1 receives an IGMP report for multicast group 224.1.2.3, it is added into MVR group 224.1.2.3.

a. Select **Switching > MVR > Advanced > MVR Group Membership**. A screen similar to the following displays:



MVR Group Membership

MVR Group Membership

Group IP: 224.1.2.3

Unit 1

Port	1	2	3	4	5	6	7	8	9	10	11	12
	✓											

Security Management

Port security features

12

This chapter includes the following sections:

- *Port Security*
- *Set the Dynamic and Static Limit on Port 1/0/1*
- *Convert the Dynamic Address Learned from 1/0/1 to a Static Address*
- *Create a Static Address*
- *Protected Ports*
- *802.1x Port Security*
- *Create a Guest VLAN*
- *Assign VLANs Using RADIUS*
- *Dynamic ARP Inspection*
- *Static Mapping*
- *DHCP Snooping*
- *Enter Static Binding into the Binding Database*
- *Maximum Rate of DHCP Messages*
- *IP Source Guard*

Port Security

Port Security helps secure the network by preventing unknown devices from forwarding packets. When a link goes down, all dynamically locked addresses are freed. The port security feature offers the following benefits:

- You can limit the number of MAC addresses on a given port. Packets that have a matching MAC address (secure packets) are forwarded; all other packets (unsecure packets) are restricted.
- You can enable port security on a per port basis.

Port security implements two traffic filtering methods, dynamic locking and static locking. These methods can be used concurrently.

- **Dynamic locking**. You can specify the maximum number of MAC addresses that can be learned on a port. The maximum number of MAC addresses is platform dependent and is given in the software Release Notes. After the limit is reached, additional MAC addresses are not learned. Only frames with an allowable source MAC addresses are forwarded.

  Note: If you want to set a specific MAC address for a port, set the dynamic entries to 0, then allow only packets with a MAC address matching the MAC address in the static list.

  Dynamically locked addresses can be converted to statically locked addresses. Dynamically locked MAC addresses are aged out if another packet with that address is not seen within the age-out time. You can set the time out value. Dynamically locked MAC addresses are eligible to be learned by another port. Static MAC addresses are not eligible for aging.
- **Static locking**. You can manually specify a list of static MAC addresses for a port. Dynamically locked addresses can be converted to statically locked addresses.

Set the Dynamic and Static Limit on Port 1/0/1

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

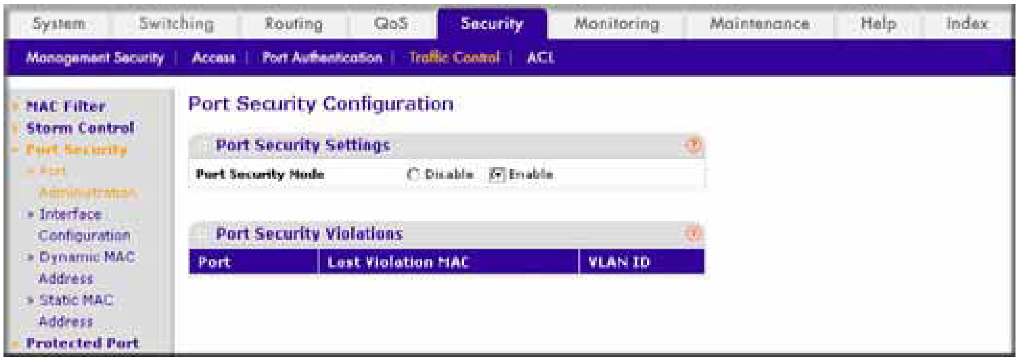
CLI: Set the Dynamic and Static Limit on Port 1/0/1

```
(Netgear Switch) (Config)#port-security
Enable port-security globally
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#port-security
Enable port-security on port 1/0/1
(Netgear Switch) (Interface 1/0/1)#port-security max-dynamic 10
Set the dynamic limit to 10
(Netgear Switch) (Interface 1/0/1)#port-security max-static 3
Set the static limit to 3
(Netgear Switch) (Interface 1/0/1)#ex
(Netgear Switch) (Config)#ex
(Netgear Switch) #show port-security 1/0/1
             Admin           Dynamic          Static           Violation
 Intf         Mode            Limit            Limit            Trap Mode
------      -------          ----------       ---------        ----------
1/0/1       Disabled         10               3                Disabled
```

Web Interface: Set the Dynamic and Static Limit on Port 1/0/1

1. Select **Security > Traffic Control > Port Security >Port Administrator**.

   A screen similar to the following displays.



Port Security Configuration

Port Security Settings

Port Security Mode ○ Disable ● Enable

Port Security Violations

Port	Last Violation MAC	VLAN ID

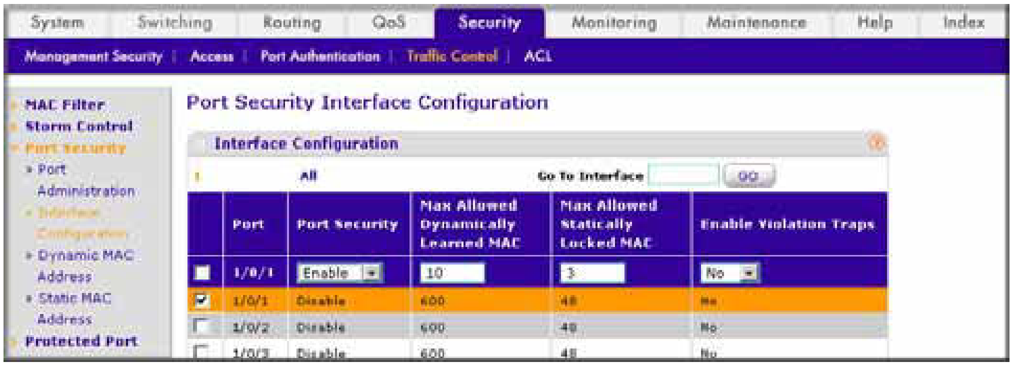
   b. Under Port Security Configuration, next to Port Security Mode, select the **Enable** radio button.

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

2. Set the dynamic and static limit on the port 1/0/1:

   a. Select **Security > Traffic Control > Port Security >Interface Configuration**.

A screen similar to the following displays.



Port Security Interface Configuration

Interface Configuration

	Port	Port Security	Max Allowed Dynamically Learned MAC	Max Allowed Statically Locked MAC	Enable Violation Traps
□	1/0/1	Enable	10	3	No
☑	1/0/1	Disable	600	48	No
□	1/0/2	Disable	600	48	No
□	1/0/3	Disable	600	48	No

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

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

c. Enter the following information:

- In the **Port Security** field, select **Enable**.
- In the **Max Allowed Dynamically Learned MAC** field, enter **10**.
- In the **Max Allowed Statically Locked MAC** field, enter **3**.

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

Convert the Dynamic Address Learned from 1/0/1 to a Static Address

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

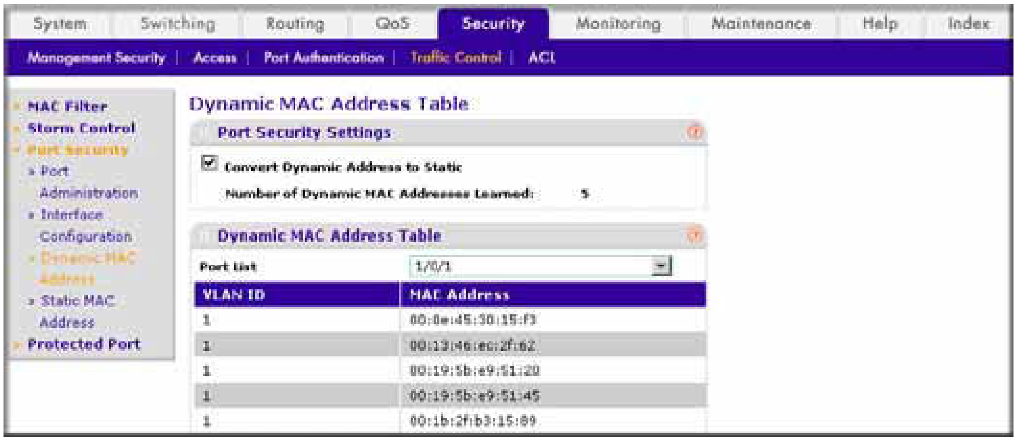
CLI: Convert the Dynamic Address Learned from 1/0/1 to the Static Address

```
(Netgear Switch)(Interface 1/0/1)#port-security mac-address move
Convert the dynamic address learned from 1/0/1 to the static address
(Netgear Switch)(Interface 1/0/1)#exit
(Netgear Switch)(Config)#exit
(Netgear Switch)#show port-security static 1/0/1
 Number of static MAC addresses configured: 3
 Statically configured MAC Address VLAN ID
 ---------------------------------------------
 00:0E:45:30:15:F3  1
 00:13:46:EC:2F:62  1
 00:14:6C:E8:81:23  1
```

Web Interface: Convert the Dynamic Address Learned from 1/0/1 to the Static Address

1. Select **Security > Traffic Control > Port Security > Dynamic MAC Address**.

   A screen similar to the following displays.



Dynamic MAC Address Table

Port Security Settings

☑ Convert Dynamic Address to Static

Number of Dynamic MAC Addresses Learned: 5

Dynamic MAC Address Table

Port List: 1/0/1

VLAN ID	MAC Address
1	00:0e:45:30:15:f3
1	00:13:46:ec:2f:62
1	00:19:5b:e9:51:20
1	00:19:5b:e9:51:45
1	00:1b:2f:b3:15:89

2. Under Port Security Configuration, in the **Port List** field, select **1/0/1**.
3. Select the **Convert Dynamic Address to Static** check box.
4. Click **Apply** to save the settings.

Create a Static Address

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

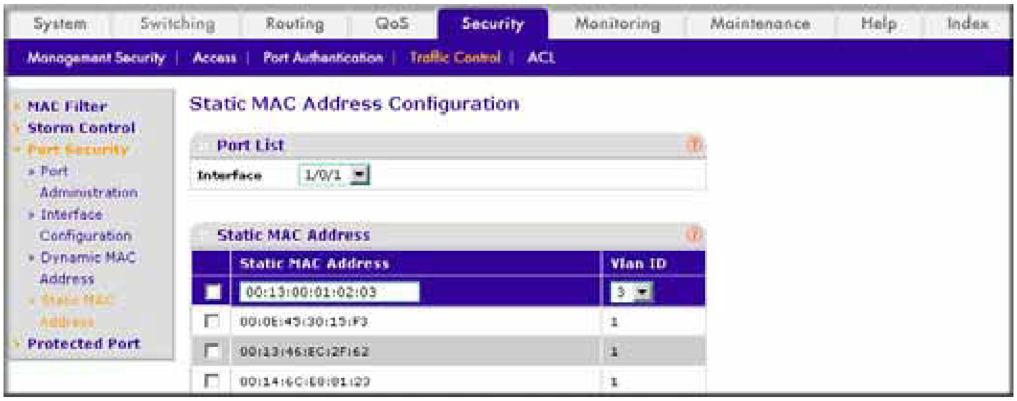
CLI: Create a Static Address

```
(Netgear Switch) (Interface 1/0/1)#port-security mac-address 00:13:00:01:02:03
```

Web Interface: Create a Static Address

1. Select **Security > Traffic Control > Port Security > Static MAC address**.

   A screen similar to the following displays.



Static MAC Address Configuration

Port List

Interface 1/0/1

Static MAC Address

	Static MAC Address	Vlan ID
□	00:13:00:01:02:03	3
□	00:0E:45:30:15:F3	1
□	00:13:46:EC:2F:62	1
□	00:14:6C:E0:01:23	1

2. Under Port List, in the **Interface** list, select **1/0/1**.
3. In the Static MAC Address section of the screen, enter the following information:
   - In the **Static MAC Address** field, enter **00:13:00:01:02:03.**
   - In the **Vlan ID** list, select **3**.
4. Click **Add**.

Protected Ports

This section describes how to set up protected ports on the switch. Some situations might require that traffic is prevented from being forwarded between any ports at Layer 2 so that one user cannot see the traffic of another user on the same switch. Protected ports can:

- Prevent traffic from being forwarded between protected ports.
- Allow traffic to be forwarded between a protected port and a non-protected port.

In following example, PC 1 and PC 2 can access the Internet as usual, but PC 1 cannot see the traffic that is generated by PC 2, that is, no traffic is forwarded between PC 1 and PC 2.

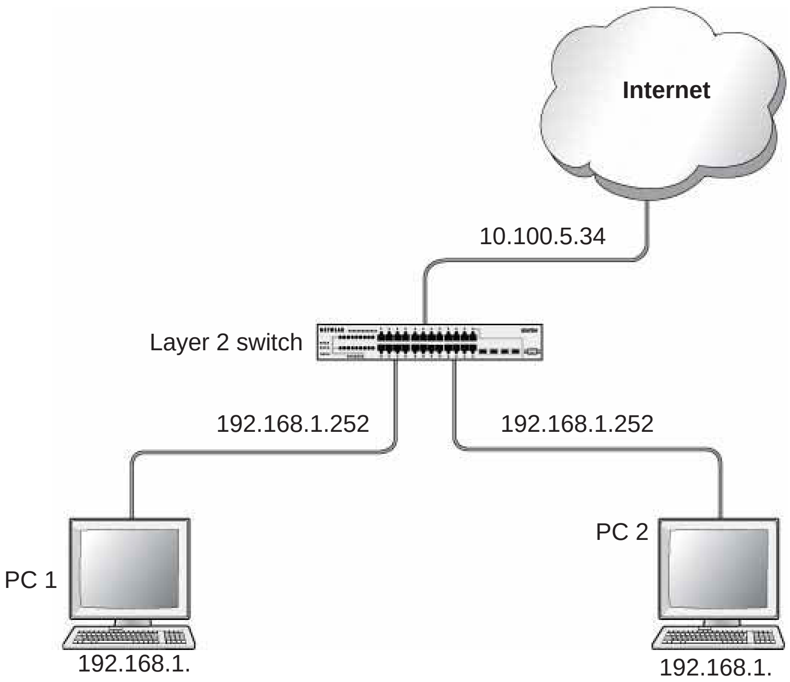


Figure 21. Protected ports

CLI: Configure a Protected Port to Isolate Ports on the Switch

1. Create one VLAN 192 including PC 1 and PC 2.

```
(Netgear Switch) #vlan database
(Netgear Switch) #vlan 192
(Netgear Switch) #vlan routing 192
(Netgear Switch) #exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/23
(Netgear Switch) (Interface 1/0/23)#vlan pvid 192
(Netgear Switch) (Interface 1/0/23)#vlan participation include 192
(Netgear Switch) (Interface 1/0/23)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan pvid 192
(Netgear Switch) (Interface 1/0/24)#vlan participation include 192
(Netgear Switch) (Interface 1/0/24)#exit
(Netgear Switch) (Interface-vlan 192)#interface vlan 192
(Netgear Switch) (Interface-vlan 192)#routing
(Netgear Switch) (Interface-vlan 192)#ip address 192.168.1.254 255.255.255.0
(Netgear Switch) (Interface-vlan 192)#exit
```

2. Create one VLAN 202 connected to the Internet.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 202
(Netgear Switch) (Vlan)#vlan routing 202
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan pvid 202
(Netgear Switch) (Interface 1/0/48)#vlan participation include 202
(Netgear Switch) (Interface 1/0/48)#exit
(Netgear Switch) (Config)#interface vlan 202
(Netgear Switch) (Interface-vlan 202)#routing
(Netgear Switch) (Interface-vlan 202)ip address 10.100.5.34 255.255.255.0
(Netgear Switch) (Interface-vlan 202)#exit
```

3. Create a DHCP pool to allocated IP addresses to PCs.

```
(Netgear Switch) (config)#service dhcp
(Netgear Switch) (config)#ip dhcp pool pool-a
(Netgear Switch) (Config-dhcp-pool)#dns-server 12.7.210.170
(Netgear Switch) (Config-dhcp-pool)#default-router 192.168.1.254
(Netgear Switch) (Config-dhcp-pool)#network 192.168.1.0 255.255.255.0
(Netgear Switch) (Config-dhcp-pool)#exit
```

4. Enable IP routing and configure a default route.

```
(Netgear Switch)(config)#ip routing
(Netgear Switch)(config)#ip route 0.0.0.0 0.0.0.0 10.100.5.252
```

5. Enable a protected port on 1/0/23 and 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/23
(Netgear Switch) (Interface 1/0/23)#switchport protected
(Netgear Switch) (Interface 1/0/23)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#switchport protected
(Netgear Switch) (Interface 1/0/24)#exit
```

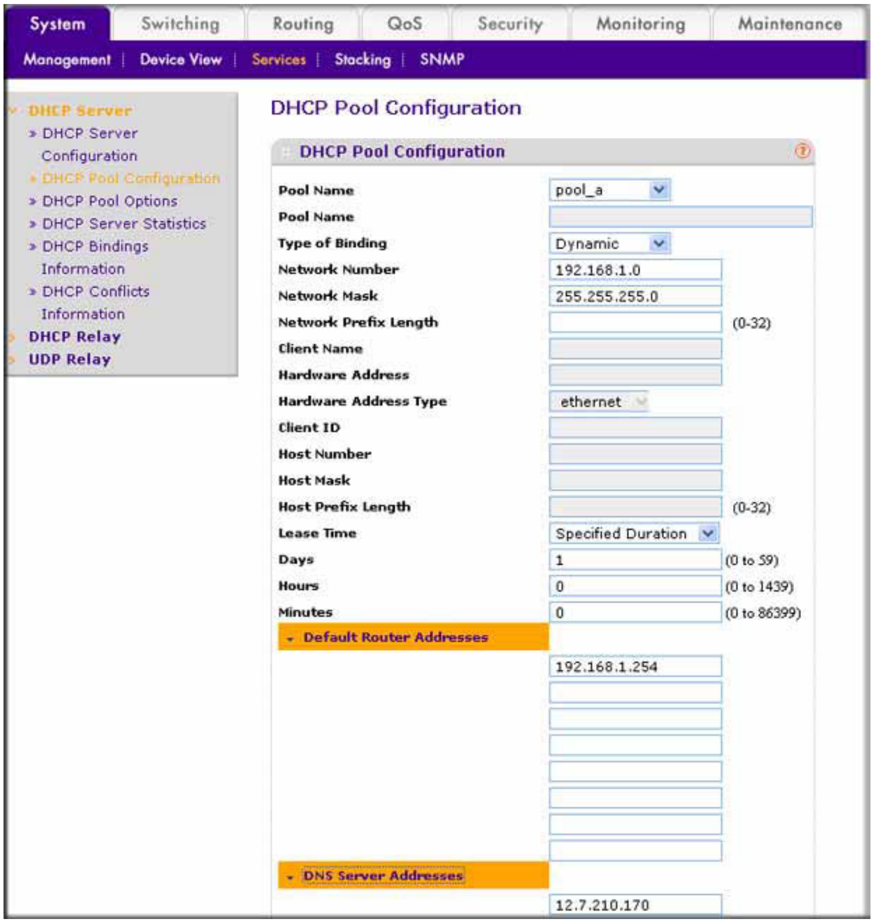
Web Interface: Configure a Protected Port to Isolate Ports on the Switch

1. Create a DHCP pool:

Note: This example assumes that the DHCP service is enabled. For information about how to enable the DHCP service, see the Web interface procedure in *Configure a DHCP Server in Dynamic Mode* on page 305.

a. Select **System > Services > DHCP Server > DHCP Server Configuration**.

A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Management | Device View | Services | Stacking | SNMP
DHCP Server
» DHCP Server Configuration
» DHCP Pool Configuration
» DHCP Pool Options
» DHCP Server Statistics
» DHCP Bindings Information
» DHCP Conflicts Information
DHCP Relay
UDP Relay

DHCP Pool Configuration

DHCP Pool Configuration

Pool Name	pool_a	
Pool Name		
Type of Binding	Dynamic	
Network Number	192.168.1.0	
Network Mask	255.255.255.0	
Network Prefix Length		(0-32)
Client Name		
Hardware Address		
Hardware Address Type	ethernet	
Client ID		
Host Number		
Host Mask		
Host Prefix Length		(0-32)
Lease Time	Specified Duration	
Days	1	(0 to 59)
Hours	0	(0 to 1439)
Minutes	0	(0 to 86399)
Default Router Addresses	192.168.1.254	
DNS Server Addresses	12.7.210.170	

b. Under DHCP Pool Configuration, enter the following information:

- In the **Pool Name** field, select **Create**.
- In the **Pool Name** field, enter **pool-a**.
- In the **Type of Binding** field, select **Dynamic**.

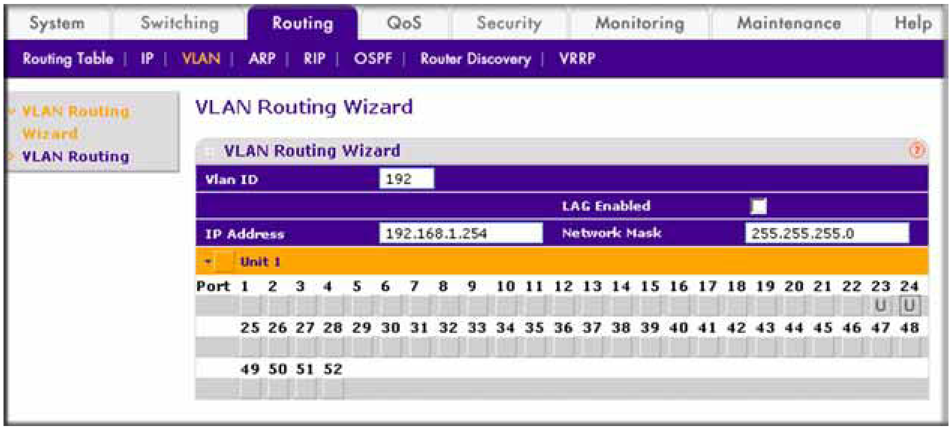
- In the **Network Number** field, enter **192.168.1.0**.
- In the **Network Mask** field, enter **255.255.255.0**.
- In the **Days** field, enter **1**.
- Click **Default Router Addresses**. The DNS server address fields display. In the first **Router Address** field, enter **192.168.1.254**.
- Click **DNS Server Addresses**. The router address fields display. In the first **DNS Server Address** field, enter **12.7.210.170**.

c. Click **Add**.

2. Configure a VLAN and include ports 1/0/23 and 1/0/24 in the VLAN:

a. Select **Routing > VLAN > VLAN Routing Wizard**.

A screen similar to the following displays.



VLAN Routing Wizard

VLAN Routing Wizard

Vlan ID: 192

LAG Enabled: ☐

IP Address: 192.168.1.254

Network Mask: 255.255.255.0

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
																							U	U
	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
	49	50	51	52																				

b. Enter the following information:

- In the **Vlan ID** field, enter **192**.
- In the **IP Address** field, enter **192.168.1.254**.
- In the **Network Mask** field, enter **255.255.255.0**.

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

- Click the gray box under port **23** twice until **U** displays.
- Click the gray box under port **24** twice until **U** displays.

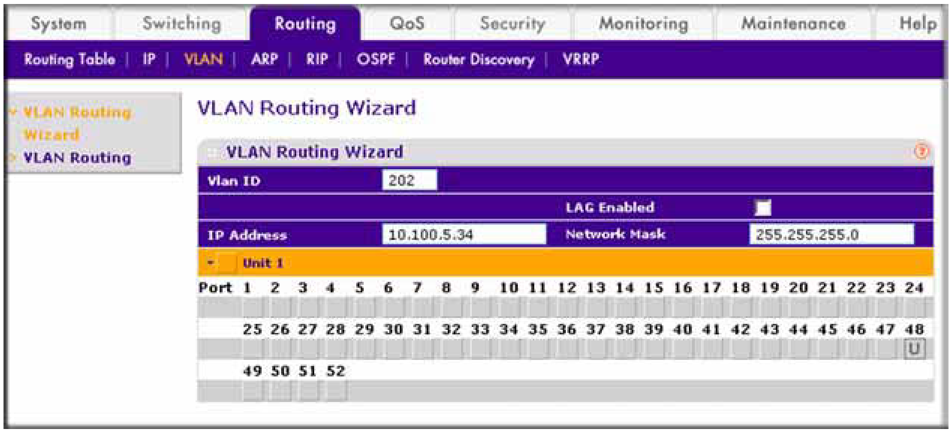
The U specifies that the egress packet is untagged for the port.

d. Click **Apply** to save the VLAN that includes ports 23 and 24.

3. Configure a VLAN and include port 1/0/48 in the VLAN:

a. Select **Routing > VLAN > VLAN Routing Wizard**.

A screen similar to the following displays.



VLAN Routing Wizard

VLAN Routing Wizard

Vlan ID 202

LAG Enabled □

IP Address 10.100.5.34 Network Mask 255.255.255.0

Unit 1

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

25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48

U (port 48)

49 50 51 52

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:

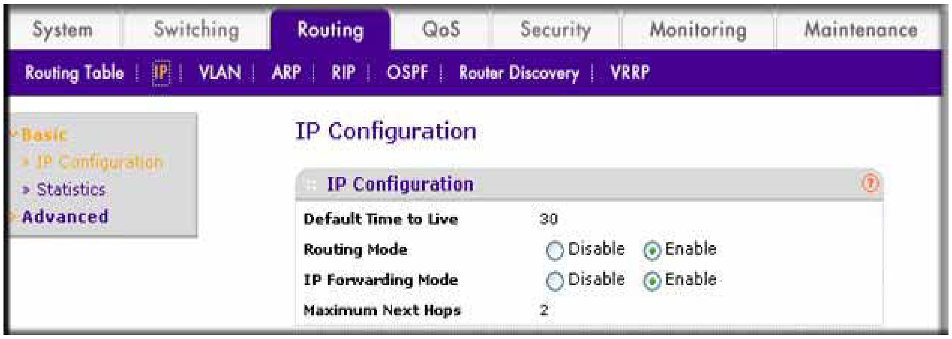
d. Click the gray box under port **48** twice until **U** displays. The U specifies that the egress packet is untagged for the port.

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

IP Configuration

Default Time to Live 30

Routing Mode ○ Disable ● Enable

IP Forwarding Mode ○ Disable ● Enable

Maximum Next Hops 2

b. Under IP Configuration, make the following selections:

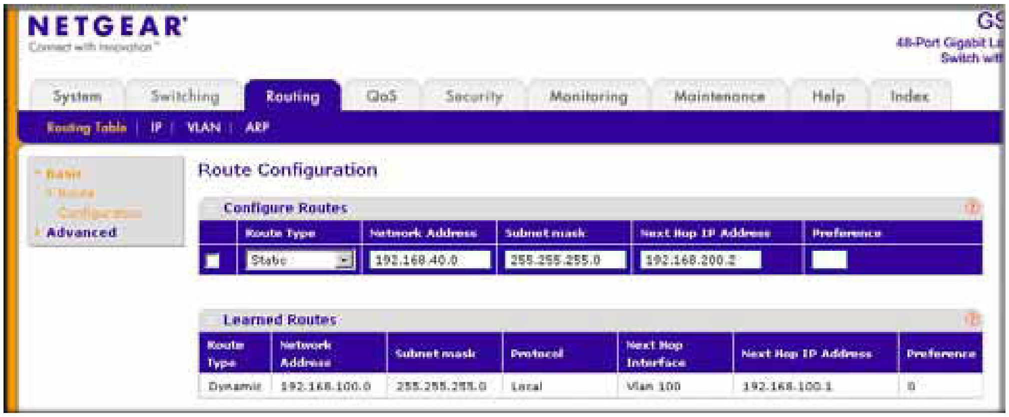
- For Routing Mode, select the **Enable** radio button.
- For IP Forwarding Mode, select the **Enable** radio button.

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.



Route Configuration

Configure Routes

	Route Type	Network Address	Subnet mask	Next Hop IP Address	Preference
□	Static	192.168.40.0	255.255.255.0	192.168.200.2	

Learned Routes

Route Type	Network Address	Subnet mask	Protocol	Next Hop Interface	Next Hop IP Address	Preference
Dynamic	192.168.100.0	255.255.255.0	Local	Vlan 100	192.168.100.1	0

b. Under Configure Routes, in the **Route Type** list, select **Default Route**.

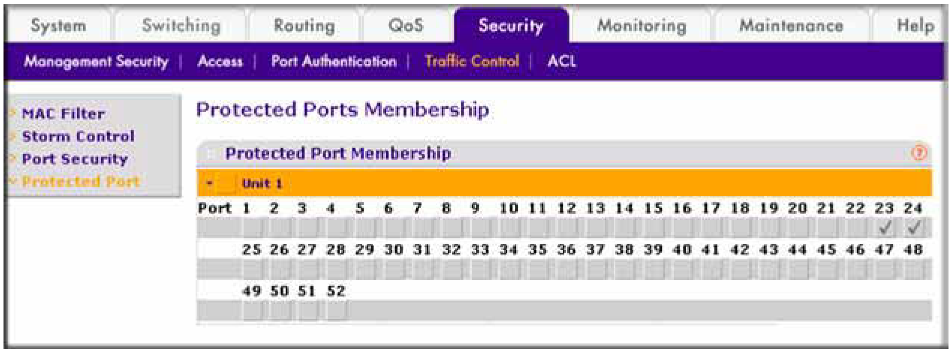
c. In the **Next Hop IP Address** field, enter **10.100.5.252**.

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

Protected Port Membership

Unit 1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
																							✓	✓
	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
	49	50	51	52																				

b. Under Protected Ports Configuration, click **Unit 1**. The ports display.

- Click the gray box under port **23**. A check mark displays in the box.
- Click the gray box under port **24**. A check mark displays in the box.

c. Click **Apply** to activate ports 23 and 24 as protected ports.

802.1x Port Security

This section describes how to configure the 802.1x port security feature on a switch port. IEEE 802.1x authentication prevents unauthorized clients from connecting to a VLAN unless these clients are authorized by the server. 802.1x port security prevent unauthorized clients from connecting to a VLAN. It can be configured on a per-port basis.

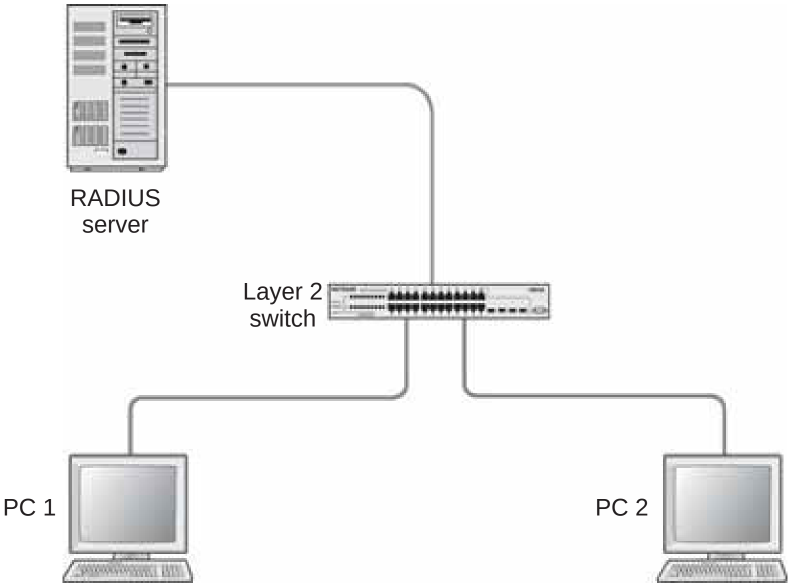


Figure 22. Using 802.1x port security

The following example shows how to authenticate the dot1x users by a RADIUS server. The management IP address is 10.100.5.33/24. The example is shown as CLI commands and as a Web interface procedure.

CLI: Authenticating dot1x Users by a RADIUS Server

1. Assign an IP address to 1/0/19, and set force authorized mode to this port, and create a user name list dot1xList.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.1.1 255.255.255.0
(Netgear Switch) (Config)#dot1x system-auth-control
(Netgear Switch) (Config)#interface 1/0/19
(Netgear Switch) (Interface 1/0/19)#routing
(Netgear Switch) (Interface 1/0/19)#ip address 10.100.5.33 255.255.255.0
(Netgear Switch) (Interface 1/0/19)#dot1x port-control force-authorized
```

2. Use RADIUS to authenticate the dot1x users.

```
(Netgear Switch) (Config)#aaa authentication dot1x default radius
```

3. Configure a RADIUS authentication server.

```
(Netgear Switch) (Config)#radius server host auth 10.100.5.17
```

4. Configure the shared secret between the RADIUS client and the server.

```
Netgear Switch) (Config)#radius server key auth 10.100.5.17
Enter secret (16 characters max):123456
Re-enter secret:123456
```

5. Set the RADIUS server as a primary server.

```
(Netgear Switch) (Config)#radius server msgauth 10.100.5.17
(Netgear Switch) (Config)# radius server primary 10.100.5.17
```

6. Configure an accounting server.

```
(Netgear Switch) (Config)#radius accounting mode
(Netgear Switch) (Config)#radius server host acct 10.100.5.17
```

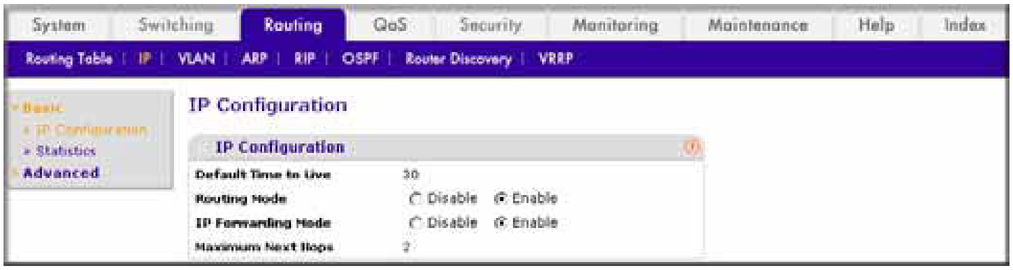
7. Configure the shared secret between the accounting server and the client.

```
(Netgear Switch) (Config)#radius server key acct 10.100.5.17
Enter secret (16 characters max):123456
Re-enter secret:123456
```

Web Interface: Authenticating dot1x Users by a RADIUS Server

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

      A screen similar to the following displays.



IP Configuration

IP Configuration

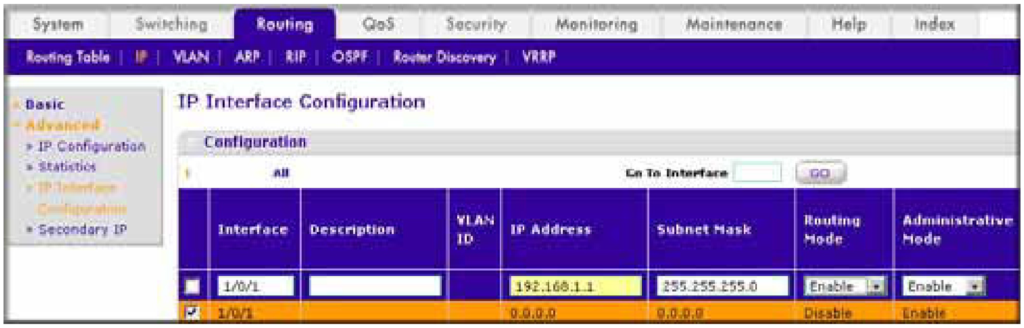
Default Time to Live	30	
Routing Mode	○ Disable	● Enable
IP Forwarding Mode	○ Disable	● Enable
Maximum Next Hops	2	

   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.



IP Interface Configuration

Configuration

All — Go To Interface

	Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
□	1/0/1			192.168.1.1	255.255.255.0	Enable	Enable
☑	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

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

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

   c. Enter the following information:

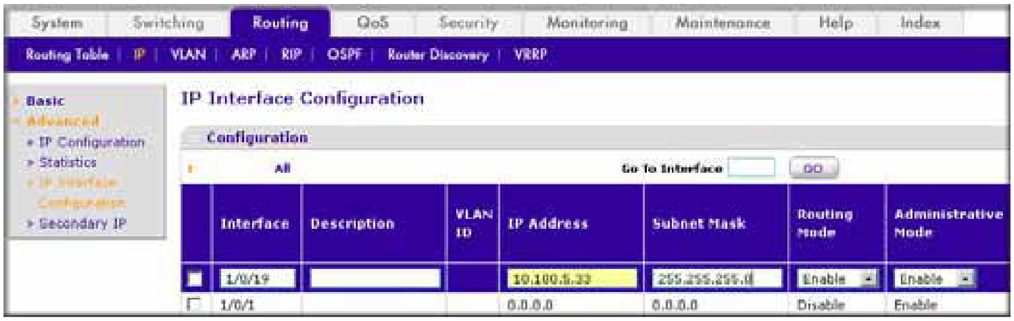
      - In the **IP Address** field, enter **192.168.1.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** field, select **Enable**.

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

3. Assign IP address 10.100.5.33/24 to interface 1/0/19:

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

      A screen similar to the following displays.



IP Interface Configuration

Configuration

All — Go To Interface

	Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
□	1/0/19			10.100.5.33	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

   b. Scroll down and select the interface **1/0/19** check box.

      Now 1/0/19 appears in the Interface field at the top.

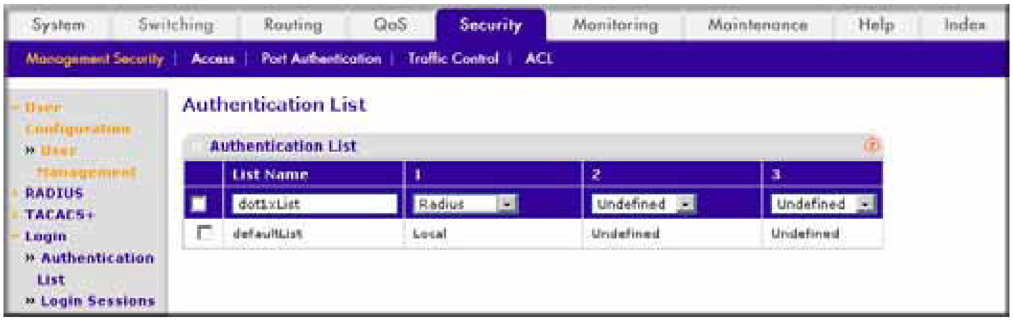
   c. Enter the following information:

      - In the **IP Address** field, enter **10.100.5.33**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** field, select **Enable**.

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

4. Create an authentication name list.
   a. Select **Security > Management Security > Login > Authentication List**.

      A screen similar to the following displays.



Authentication List

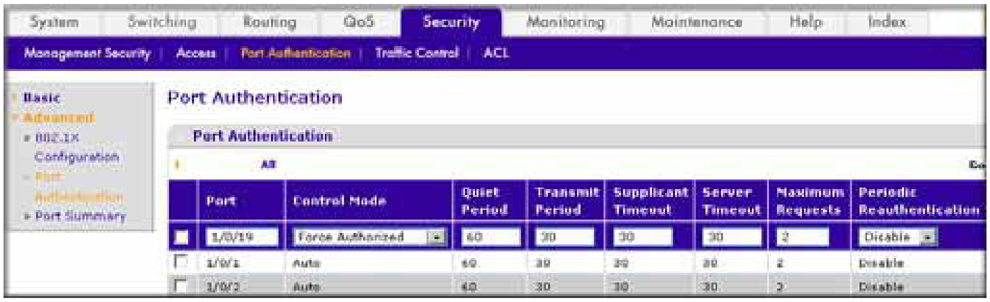
Authentication List

	List Name	1	2	3
☐	dot1xList	Radius	Undefined	Undefined
☐	defaultList	Local	Undefined	Undefined

   b. Select the check box before **dot1xList**.
   c. In the **1** list, select **Radius**.
   d. Click **Apply**.

5. Set port 1/0/19 to force authorized mode. (In this case, the RADIUS server is connected to this interface.)
   a. Select **Security > Port Authentication > Advanced > Port Authentication**.

      A screen similar to the following displays.



Port Authentication

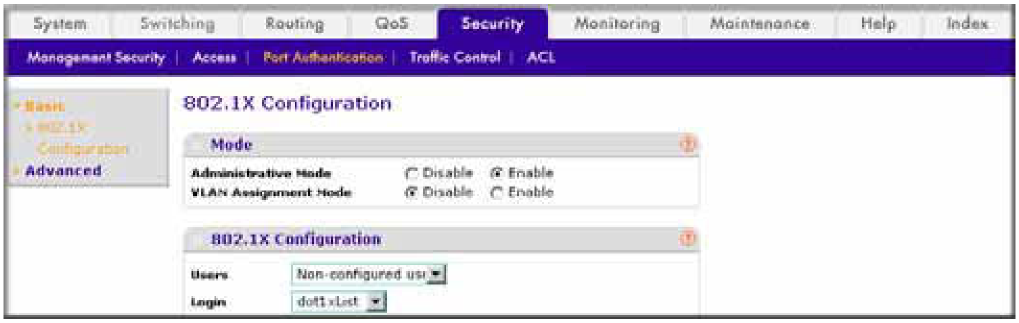
Port Authentication

	Port	Control Mode	Quiet Period	Transmit Period	Supplicant Timeout	Server Timeout	Maximum Requests	Periodic Reauthentication
☐	1/0/19	Force Authorized	60	30	30	30	2	Disable
☐	1/0/1	Auto	60	30	30	30	2	Disable
☐	1/0/2	Auto	60	30	30	30	2	Disable

   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.



802.1X Configuration

Mode

Administrative Mode ○ Disable ● Enable
VLAN Assignment Mode ● Disable ○ Enable

802.1X Configuration

Users: Non-configured usi
Login: dot1xList

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

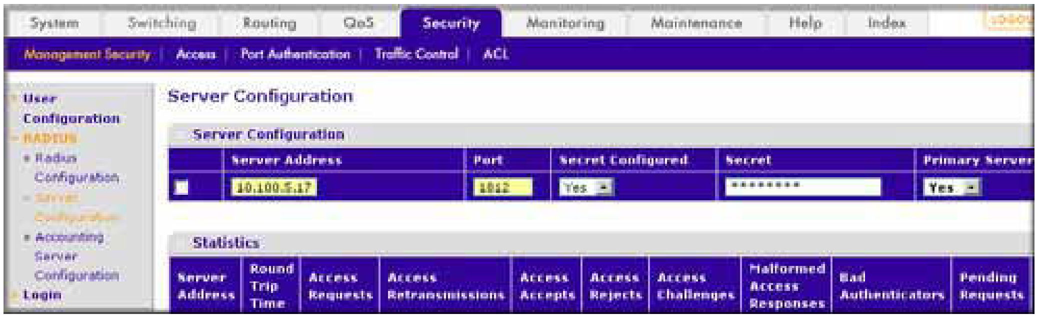
c. In the **Login** list, select **dot1xList**.

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.



Server Configuration

Server Configuration

	Server Address	Port	Secret Configured	Secret	Primary Server
□	10.100.5.17	1812	Yes	********	Yes

Statistics

Server Address	Round Trip Time	Access Requests	Access Retransmissions	Access Accepts	Access Rejects	Access Challenges	Malformed Access Responses	Bad Authenticators	Pending Requests

b. In the **Server Address** field, enter **10.100.5.17**.

c. In the **Secret Configured** field, select **Yes**.

d. In the **Secret** field, enter **123456**.

e. In the **Primary Server** field, select **Yes**.

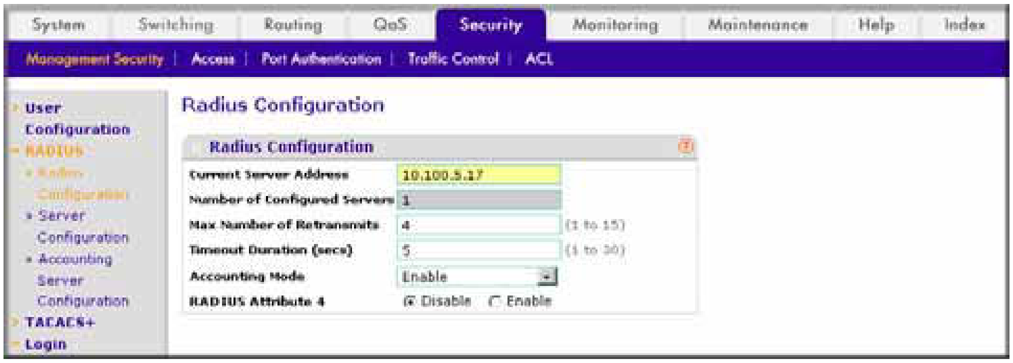
f. In the **Message Authenticator** field, select **Enable**.

g. Click **Add**.

8. Enable accounting.

a. Select **Security > Management Security > RADIUS > Radius Configuration**.

A screen similar to the following displays.



Radius Configuration

Radius Configuration

Current Server Address	10.100.5.17	
Number of Configured Servers	1	
Max Number of Retransmits	4	(1 to 15)
Timeout Duration (secs)	5	(1 to 30)
Accounting Mode	Enable	
RADIUS Attribute 4	● Disable ○ Enable	

b. In the **Server Address** field, enter **10.100.5.17**.

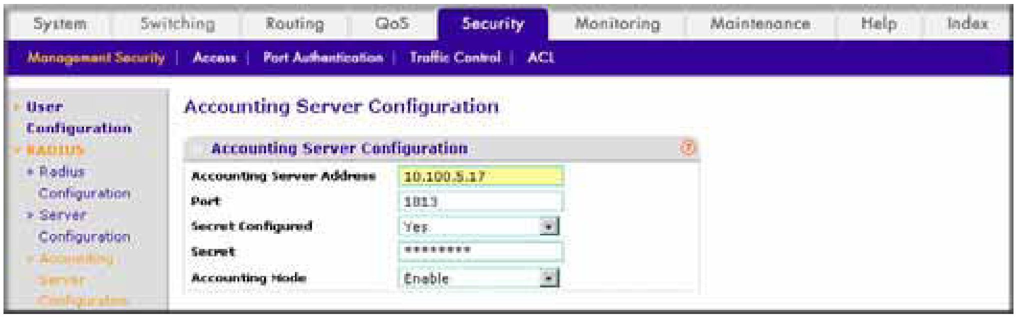
c. In the **Accounting Mode** field, select **Enable**.

d. Click **Apply**.

9. Configure the accounting server.

a. Select **Security > Management Security > RADIUS > Radius Accounting Server Configuration**.

A screen similar to the following displays.



Accounting Server Configuration

Accounting Server Configuration

Accounting Server Address	10.100.5.17
Port	1813
Secret Configured	Yes
Secret	********
Accounting Mode	Enable

b. In the **Accounting Server Address** field, enter **10.100.5.17**.

c. In the **Accounting Mode** field, select **Enable**.

d. Click **Apply**.

Create a Guest VLAN

The guest VLAN feature allows a switch to provide a distinguished service to dot1x unaware clients (not rogue users who fail authentication). This feature provides a mechanism to allow visitors and contractors to have network access to reach an external network with no ability to surf the internal LAN.

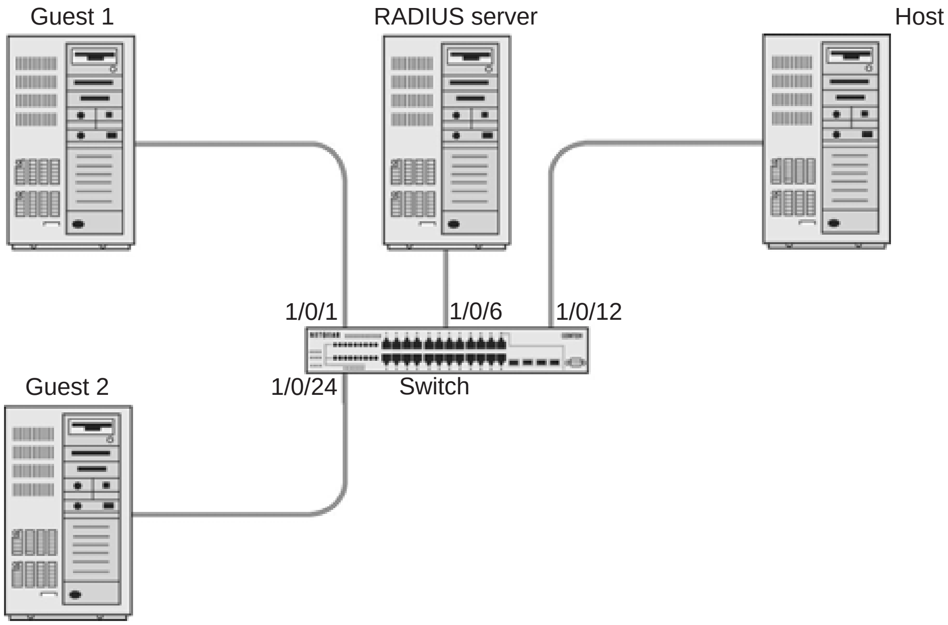


Figure 23. Guest VLAN

If a port is in port-based mode, and a client that does not support 802.1X is connected to an unauthorized port that has 802.1X enabled, the client does not respond to the 802.1X requests from the switch. The port remains in the unauthorized state, and the client is not granted access to the network. If the guest VLAN is configured for that port, then the port is placed in the configured guest VLAN and the port is moved to the authorized state, allowing access to the client after a certain amount of time (determined by the guest VLAN period). If the client attached is 802.1x aware, then this allows the client to respond to 802.1X requests from the switch.

For a port in MAC-based mode, if traffic from 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.

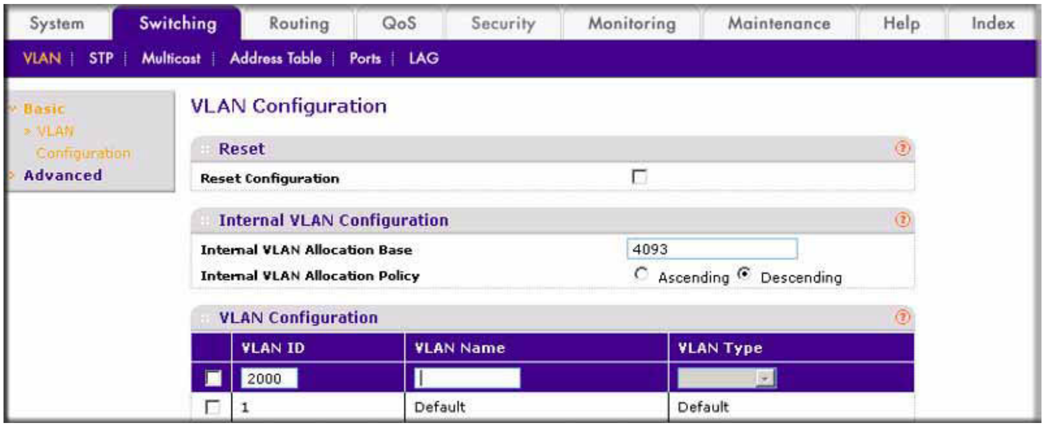
```
(Netgear Switch) #show dot1x detail 1/0/1
Protocol Version............................... 1
PAE Capabilities............................... Authenticator
Control Mode................................... auto
Authenticator PAE State........................ Authenticated
Backend Authentication State................... 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

1. Create VLAN 2000.

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

   A screen similar to the following displays.



VLAN Configuration

Reset

Reset Configuration □

Internal VLAN Configuration

Internal VLAN Allocation Base 4093

Internal VLAN Allocation Policy ○ Ascending ● Descending

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type
□	2000		
□	1	Default	Default

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

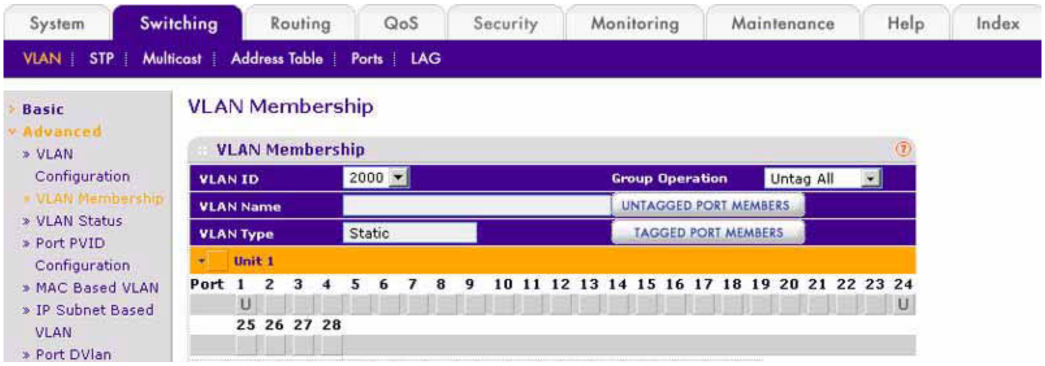
c. In the **VLAN Type** field, select **Static**.

d. Click **Add**.

2. Add ports to VLAN 2000.

a. Select **Switching > VLAN > Advanced > VLAN Membership**.

A screen similar to the following displays.



VLAN Membership

VLAN Membership

VLAN ID	2000	Group Operation	Untag All
VLAN Name			
VLAN Type	Static		

Unit 1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	U																							U
	25	26	27	28																				

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.

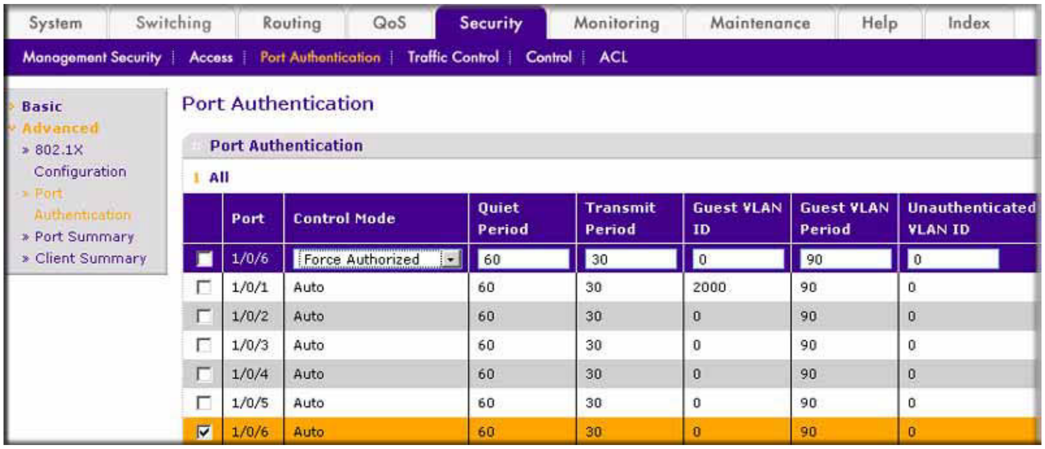
The U specifies that the egress packet is untagged for the port.

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

Port Authentication

All

	Port	Control Mode	Quiet Period	Transmit Period	Guest VLAN ID	Guest VLAN Period	Unauthenticated VLAN ID
☐	1/0/6	Force Authorized	60	30	0	90	0
☐	1/0/1	Auto	60	30	2000	90	0
☐	1/0/2	Auto	60	30	0	90	0
☐	1/0/3	Auto	60	30	0	90	0
☐	1/0/4	Auto	60	30	0	90	0
☐	1/0/5	Auto	60	30	0	90	0
☑	1/0/6	Auto	60	30	0	90	0

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**.

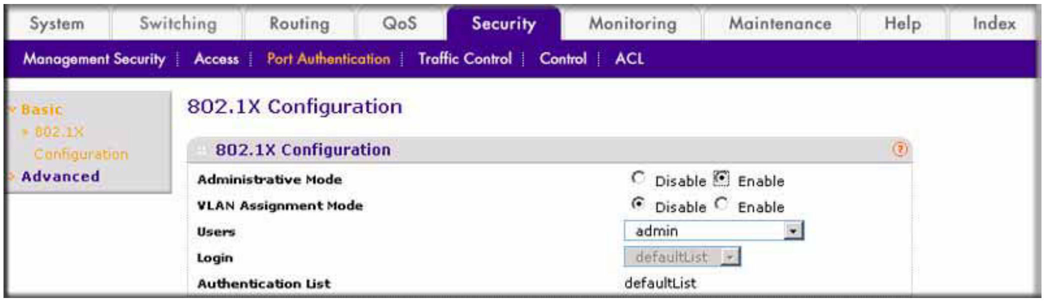
d. Click **Apply** to save settings.

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

802.1X Configuration

Administrative Mode	○ Disable ● Enable
VLAN Assignment Mode	● Disable ○ Enable
Users	admin
Login	defaultList
Authentication List	defaultList

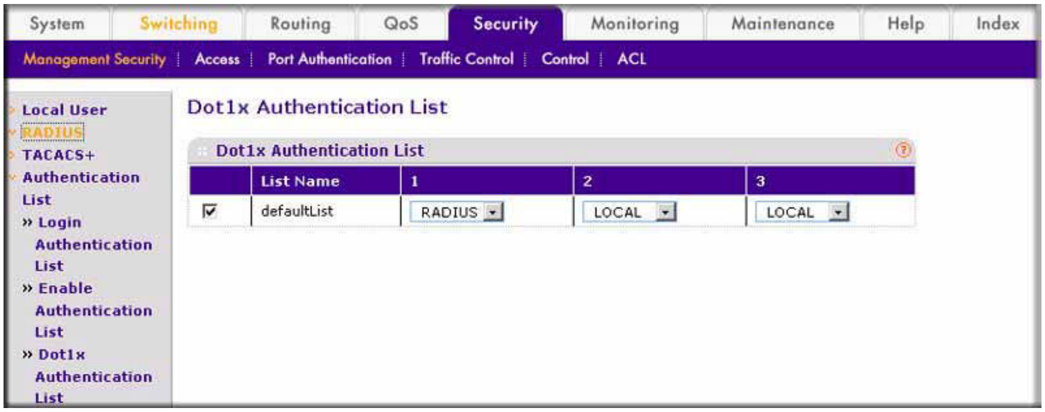
b. For Administrative Mode, select the **Enable** radio button.

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

Dot1x Authentication List

	List Name	1	2	3
☑	defaultList	RADIUS	LOCAL	LOCAL

b. Select the **defaultList** check box.

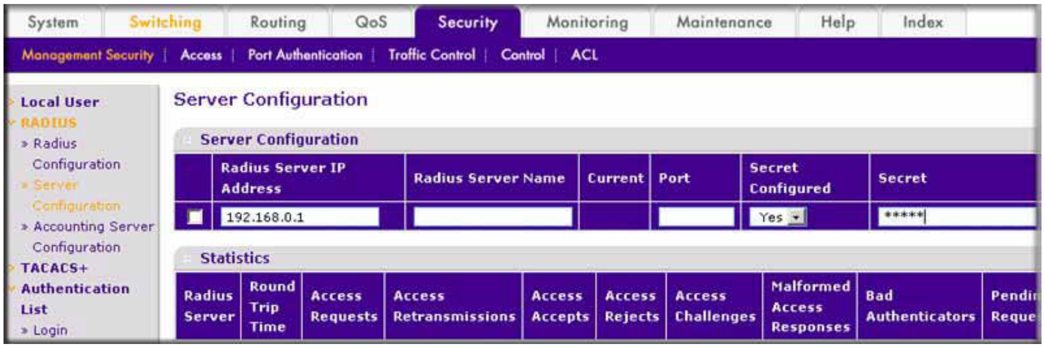
c. In the **1** list, select **RADIUS**.

d. Click **Add**.

6. Configure the RADIUS authentication server.

a. Select **Security > Management Security > Radius > Server Configuration**.

A screen similar to the following displays.



Server Configuration

Server Configuration

	Radius Server IP Address	Radius Server Name	Current	Port	Secret Configured	Secret
□	192.168.0.1				Yes	*****

Statistics

Radius Server	Round Trip Time	Access Requests	Access Retransmissions	Access Accepts	Access Rejects	Access Challenges	Malformed Access Responses	Bad Authenticators	Pendi Reque

b. In the **Radius Server IP Address** field, enter **192.168.0.1**.

c. In the **Secret Configured** field, select **Yes**.

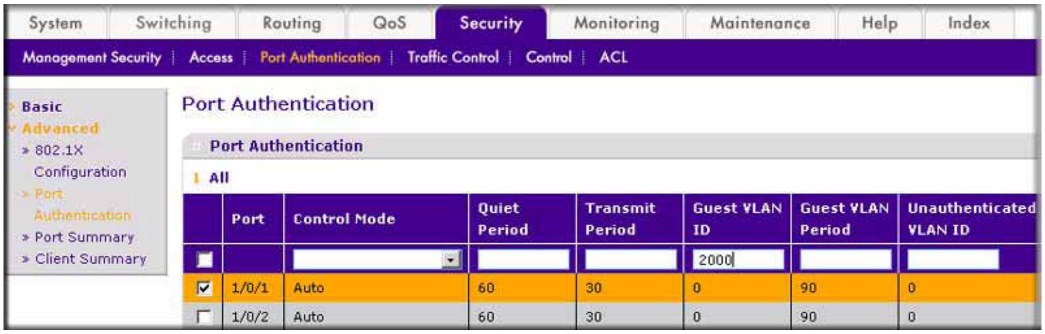
d. In the **Secret** field, enter **12345**.

e. Click **Add**.

7. Configure the guest VLAN.

a. Select **Security > Port Authentication > Advanced > Port Authentication**.

A screen similar to the following displays.



Port Authentication

Port Authentication

1 All

	Port	Control Mode	Quiet Period	Transmit Period	Guest VLAN ID	Guest VLAN Period	Unauthenticated VLAN ID
□					2000		
☑	1/0/1	Auto	60	30	0	90	0
□	1/0/2	Auto	60	30	0	90	0

b. Scroll down and select the port 1/0/1 and 1/0/24 check boxes.

c. In the **Guest VLAN ID** field, enter **2000**.

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

Assign VLANs Using RADIUS

This feature allows the client to connect from any port and be assigned to the appropriate VLAN assigned by the RADIUS server. This gives flexibility for the clients to move around the network without requiring the administrator to do static VLAN configuration. When multiple hosts are connected to the switch on the same port, only one host uses authentication. If any VLAN information is applied on the port based on the authenticated host, the VLAN applies that information to all the hosts that are connected to that port.

- After a port is in an authorized state, if any client initiates dot1x authentication, the port clears authenticated clients' states, and in the process clears the VLAN assigned to the port (if any). Then the port continues with the new client authentication and authorization process.
- When a client authenticates itself initially on the network, the switch acts as the authenticator to the clients on the network and forwards the authentication request to the RADIUS server in the network.

For use in VLAN assignment, the following tunnel attributes are used:

- Tunnel-Type = VLAN (13)
- Tunnel-Medium-Type = 802
- Tunnel-Private-Group-ID = VLANID where VLANID is 12 bits, with a value between 1 and 4094.

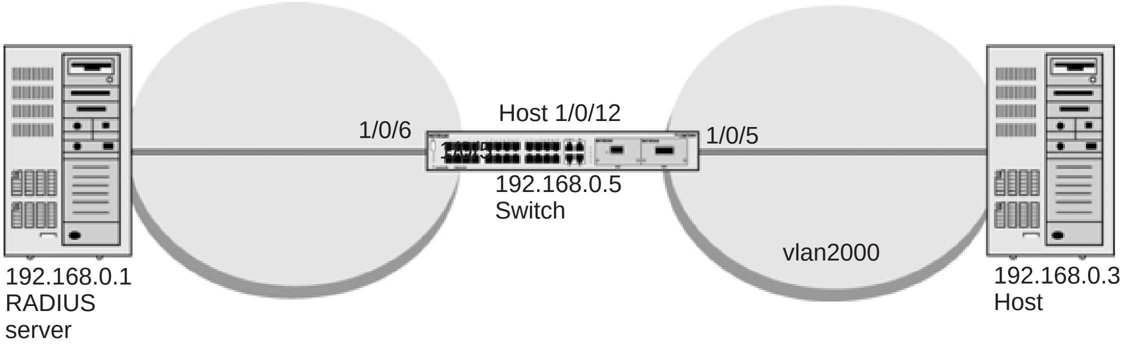


Figure 24. VLAN assignment using RADIUS

In the previous figure, the switch has placed the host in the VLAN (vlan2000) based on the user details of the clients.

The configuration on a RADIUS server for a user logged in as admin is:

- Tunnel-Type = VLAN (13)
- Tunnel-Medium-Type = 802
- Tunnel-Private-Group-ID = 2000

CLI: Assign VLANS Using RADIUS

1. Create VLAN 2000.

```
(Netgear Switch) #network protocol none
Changing protocol mode will reset ip configuration.
Are you sure you want to continue? (y/n) y
(Netgear Switch) #network parms 192.168.0.5 255.255.255.0
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 2000
(Netgear Switch) #exit
```

2. Enable dot1x authentication on the switch

```
(Netgear Switch) (Config)#dot1x system-auth-control
```

3. Use the RADIUS as the authenticator.

```
(Netgear Switch) (Config)#aaa authentication dot1x default radius
```

4. Enable the switch to accept VLAN assignment by the RADIUS server.

```
(Netgear Switch) (Config)#authorization network radius
```

5. Set the RADIUS server IP address.

```
(Netgear Switch) (Config)#radius server host auth 192.168.0.1
```

6. Set the NAS-IP address for the RADIUS server.

```
(Netgear Switch) (Config)#radius server key auth 192.168.0.1
Enter secret (16 characters max):12345
Re-enter secret:12345
Set the radius server key.
(Netgear Switch) (Config)#radius server attribute 4 192.168.0.1
```

7. Force 1/0/6 to be authorized for it to connect to the RADIUS server.

```
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)#dot1x port-control force-authorized
(Netgear Switch) (Interface 1/0/6)#exit
```

8. Show the dot1x detail for 1/0/5.

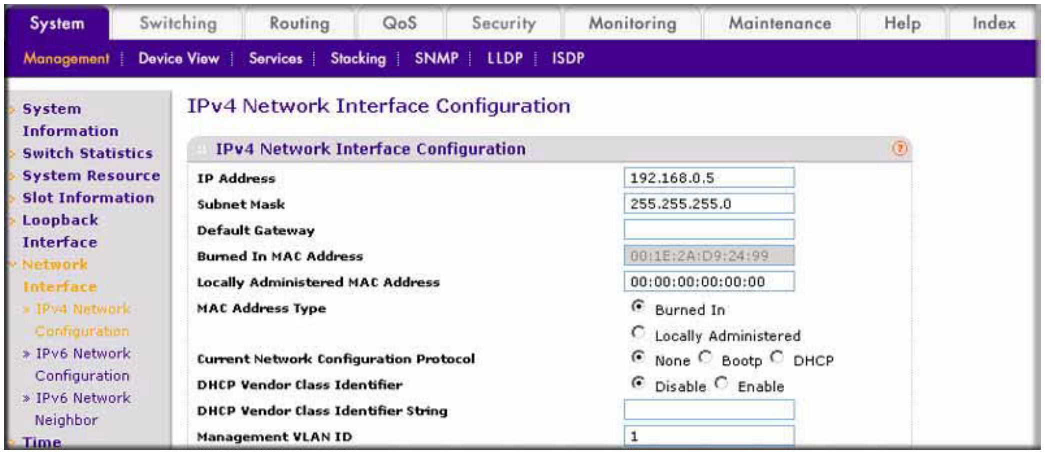
```
(Netgear Switch) #show dot1x detail 1/0/5
Port........................................... 1/0/5
Protocol Version............................... 1
PAE Capabilities............................... Authenticator
Control Mode................................... auto
Authenticator PAE State........................ Authenticated
Backend Authentication State................... Idle
Quiet Period (secs)............................ 60
Transmit Period (secs)......................... 30
Guest VLAN ID.................................. 0
Guest VLAN Period (secs)....................... 90
Supplicant Timeout (secs)...................... 30
Server Timeout (secs).......................... 30
Maximum Requests............................... 2
VLAN Id........................................ 2000
VLAN Assigned Reason........................... RADIUS
Reauthentication Period (secs)................. 3600
Reauthentication Enabled....................... FALSE
Key Transmission Enabled....................... FALSE
Control Direction.............................. both
Maximum Users.................................. 16
Unauthenticated VLAN ID........................ 0
Session Timeout................................ 0
Session Termination Action..................... Default
```

Web Interface: Assign VLANS Using RADIUS

1. Assign the IP address for the Web Management Interface.

   a. Select **System > Management > Network Interface > IPv4 Network Configuration**.

A screen similar to the following displays.



IPv4 Network Interface Configuration

IPv4 Network Interface Configuration

IP Address	192.168.0.5
Subnet Mask	255.255.255.0
Default Gateway	
Burned In MAC Address	00:1E:2A:D9:24:99
Locally Administered MAC Address	00:00:00:00:00:00
MAC Address Type	● Burned In ○ Locally Administered
Current Network Configuration Protocol	● None ○ Bootp ○ DHCP
DHCP Vendor Class Identifier	● Disable ○ Enable
DHCP Vendor Class Identifier String	
Management VLAN ID	1

b. For Current Network Configuration Protocol, select the **None** radio button.

c. In the **IP Address** field, enter **192.168.0.5**.

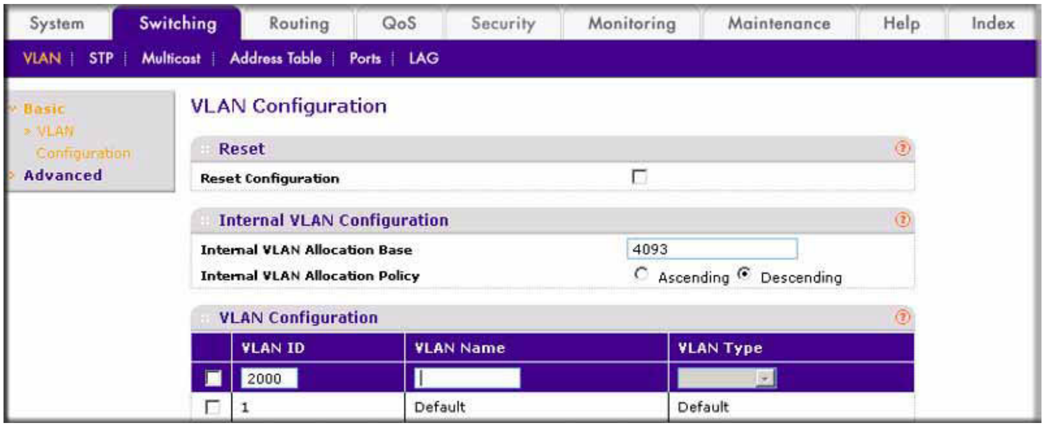
d. In the **Subnet Mask** field, enter **255.255.255.0**.

e. Click **Apply**.

2. Create VLAN 2000.

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

A screen similar to the following displays.



VLAN Configuration

Reset

Reset Configuration	□

Internal VLAN Configuration

Internal VLAN Allocation Base	4093
Internal VLAN Allocation Policy	○ Ascending ● Descending

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type
□	2000		
□	1	Default	Default

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

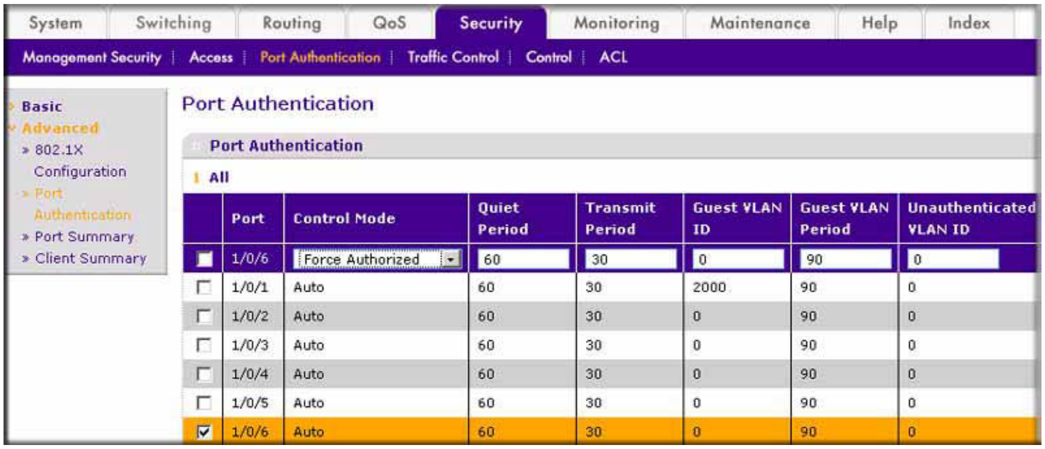
c. In the **VLAN Type** field, select **Static**.

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.



Port Authentication

Port Authentication

All

	Port	Control Mode	Quiet Period	Transmit Period	Guest VLAN ID	Guest VLAN Period	Unauthenticated VLAN ID
□	1/0/6	Force Authorized	60	30	0	90	0
□	1/0/1	Auto	60	30	2000	90	0
□	1/0/2	Auto	60	30	0	90	0
□	1/0/3	Auto	60	30	0	90	0
□	1/0/4	Auto	60	30	0	90	0
□	1/0/5	Auto	60	30	0	90	0
☑	1/0/6	Auto	60	30	0	90	0

b. Under Port Authentication, scroll down and select the 1/0/6 and 1/0/12 check boxes.

c. In the **Control Mode** list, select **Force Authorized**.

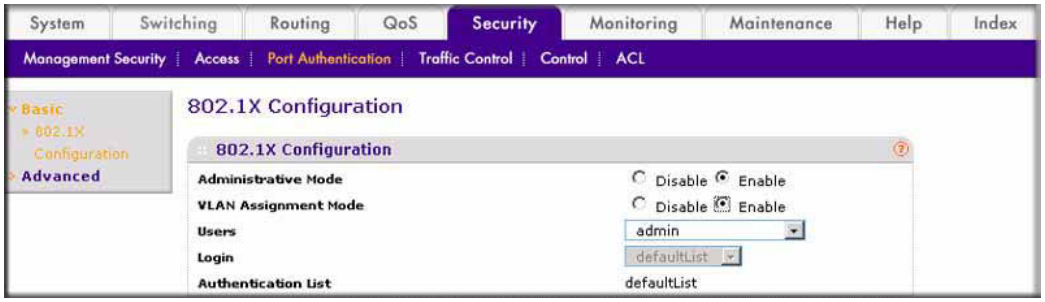
d. Click **Apply** to save settings.

4. Enable dot1x on the switch.

   Make sure that 1/0/12 and 1/0/6 are configured as force authorized before you do this step; otherwise, you cannot access the switch through the Web Management Interface.

   a. Select **Security > Port Authentication > Basic > 802.1x Configuration**.

   A screen similar to the following displays.



802.1X Configuration

802.1X Configuration

Administrative Mode	○ Disable ● Enable
VLAN Assignment Mode	○ Disable ● Enable
Users	admin
Login	defaultList
Authentication List	defaultList

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

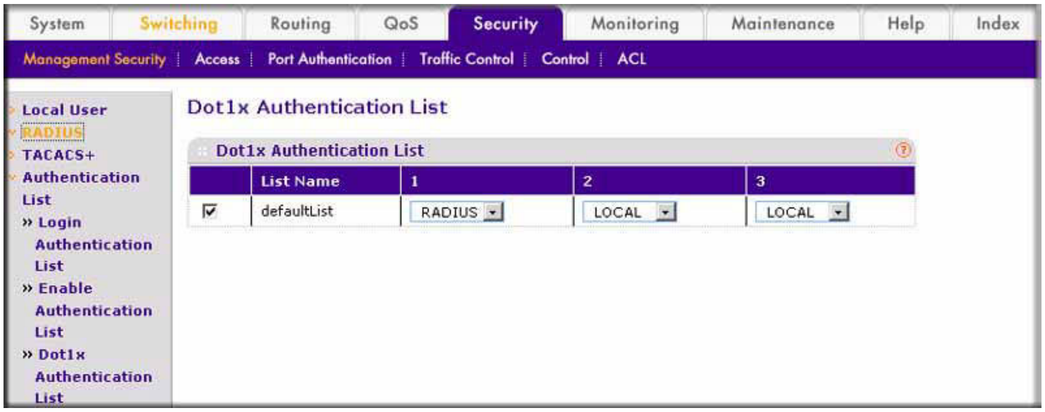
c. For VLAN Assignment Mode, select the **Enable** radio button.

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.



Dot1x Authentication List

Dot1x Authentication List

	List Name	1	2	3
☑	defaultList	RADIUS	LOCAL	LOCAL

b. Select the **defaultList** check box.

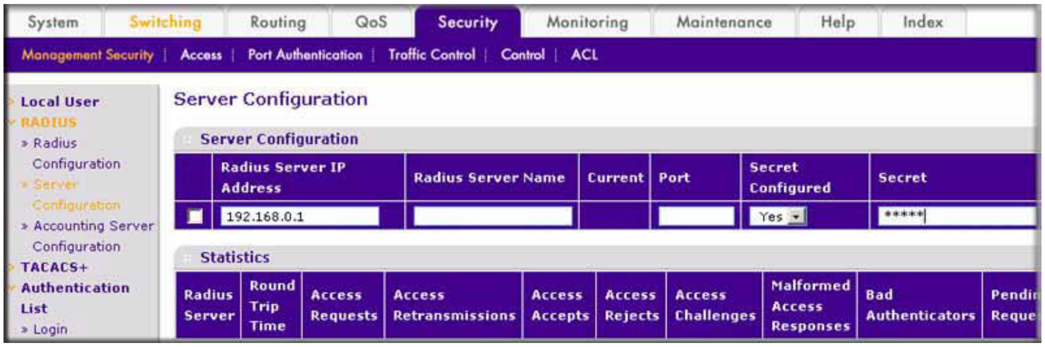
c. In the **1** list, select **RADIUS**.

d. Click **Add**.

6. Configure the RADIUS authentication server.

a. Select **Security > Management Security > Radius > Server Configuration**.

A screen similar to the following displays.



Server Configuration

Server Configuration

	Radius Server IP Address	Radius Server Name	Current	Port	Secret Configured	Secret
☐	192.168.0.1				Yes	*****

Statistics

Radius Server	Round Trip Time	Access Requests	Access Retransmissions	Access Accepts	Access Rejects	Access Challenges	Malformed Access Responses	Bad Authenticators	Pendi Reque

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.

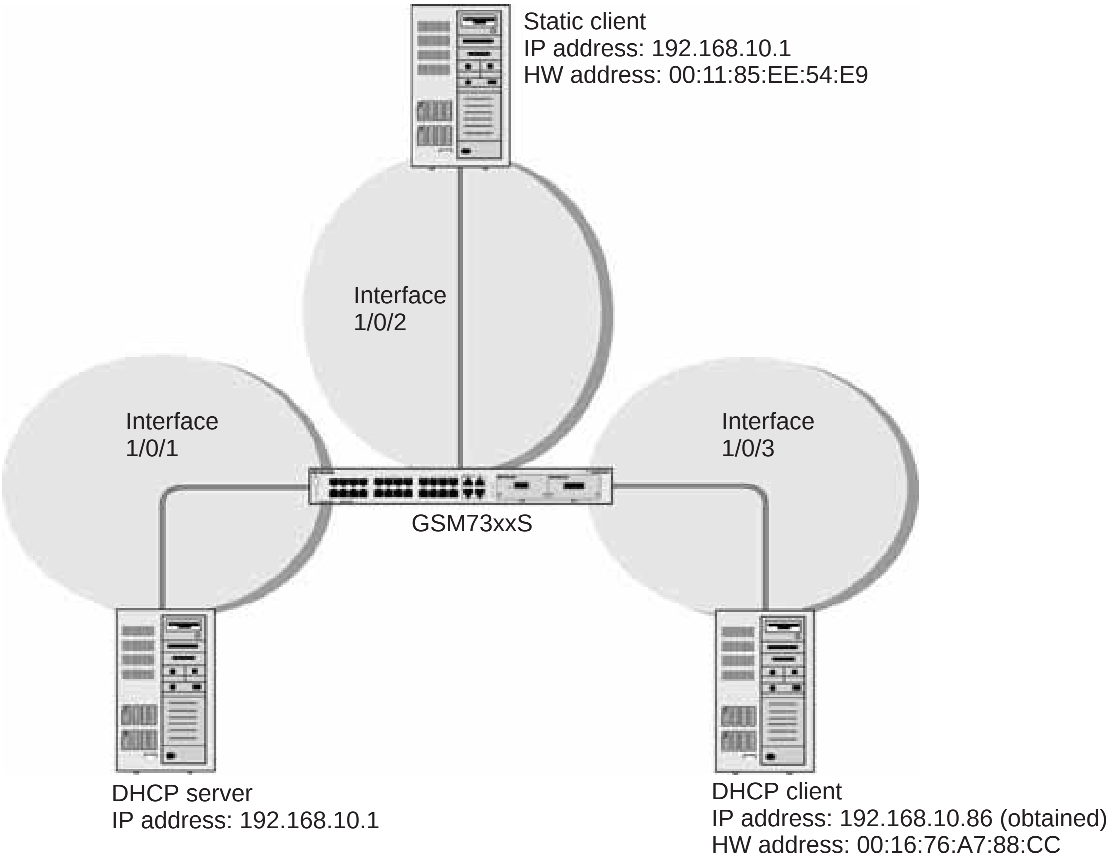


Figure 25. Dynamic ARP inspection

CLI: Configure Dynamic ARP Inspection

1. Enable DHCP snooping globally.

```
(Netgear Switch) (Config)# ip dhcp snooping
```

2. Enable DHCP snooping in a VLAN.

```
(Netgear Switch) (Config)# ip dhcp snooping vlan 1
```

3. Configure the port through which the DHCP server is reached as trusted.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip dhcp snooping trust
```

4. View the DHCP Snooping Binding table.

```
(GSM7328S) #show ip dhcp snooping binding
Total number of bindings:  1

         MAC Address       IP Address     VLAN  Interface    Type     Lease (Secs)
      -----------------  ---------------  ----  -----------  -------  -----------
      00:16:76:A7:88:CC    192.168.10.86    1   1/0/2        DYNAMIC  86400
```

5. Enable ARP inspection in VLAN 1.

```
(Netgear Switch) (Config)# ip arp inspection vlan 1
```

   Now all ARP packets received on ports that are members of the VLAN are copied to the CPU for ARP inspection. If there are trusted ports, you can configure them as trusted in the next step. ARP packets received on trusted ports are not copied to the CPU.

6. Configure port 1/0/1 as trusted.

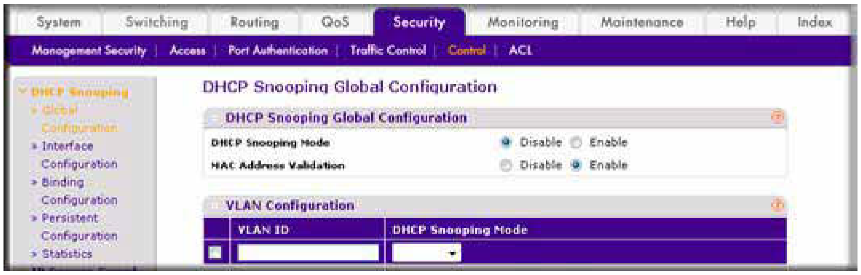
```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip arp inspection trust
```

Now ARP packets from the DHCP client go through because there is a DHCP snooping entry; however ARP packets from the static client are dropped. It can be overcome by static configuration as described in *Static Mapping* on page 246.

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.



DHCP Snooping Global Configuration

DHCP Snooping Global Configuration

DHCP Snooping Mode ● Disable ○ Enable

MAC Address Validation ○ Disable ● Enable

VLAN Configuration

	VLAN ID	DHCP Snooping Mode
□		

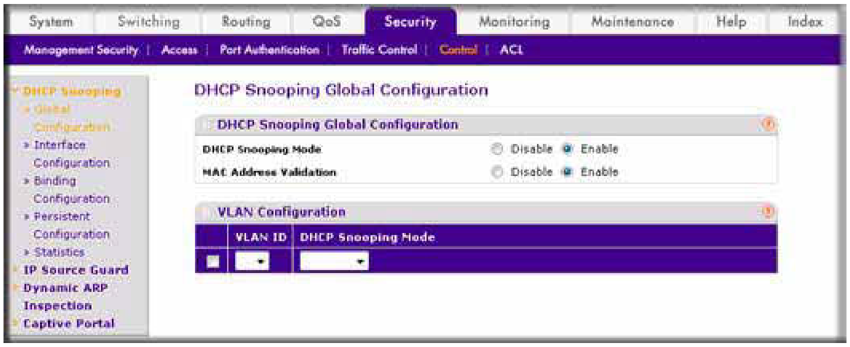
b. For DHCP Snooping Mode, select the **Enable** radio button.

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

DHCP Snooping Global Configuration

DHCP Snooping Mode ○ Disable ● Enable

MAC Address Validation ○ Disable ● Enable

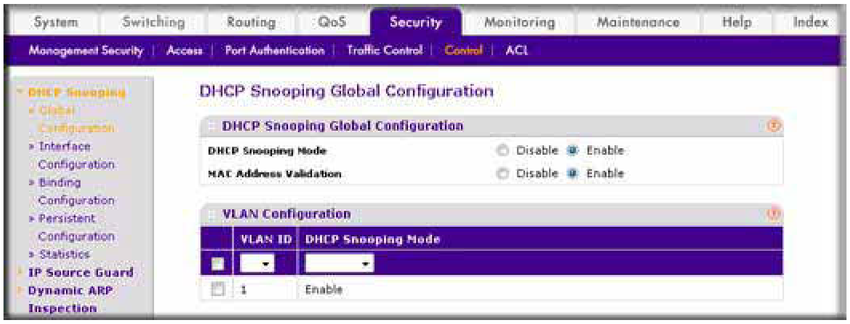
VLAN Configuration

	VLAN ID	DHCP Snooping Mode
□		

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

DHCP Snooping Global Configuration

DHCP Snooping Mode ○ Disable ● Enable

MAC Address Validation ○ Disable ● Enable

VLAN Configuration

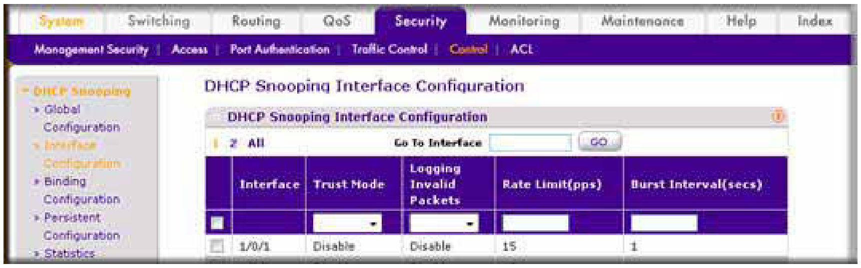
	VLAN ID	DHCP Snooping Mode
□		
□	1	Enable

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

DHCP Snooping Interface Configuration

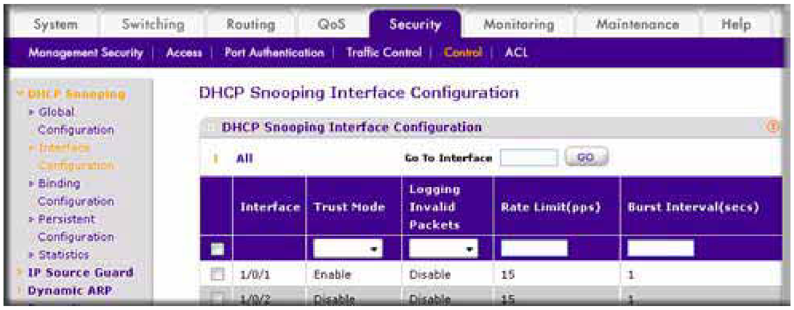
1 2 All Go To Interface

	Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pps)	Burst Interval(secs)
□	1/0/1	Disable	Disable	15	1

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

DHCP Snooping Interface Configuration

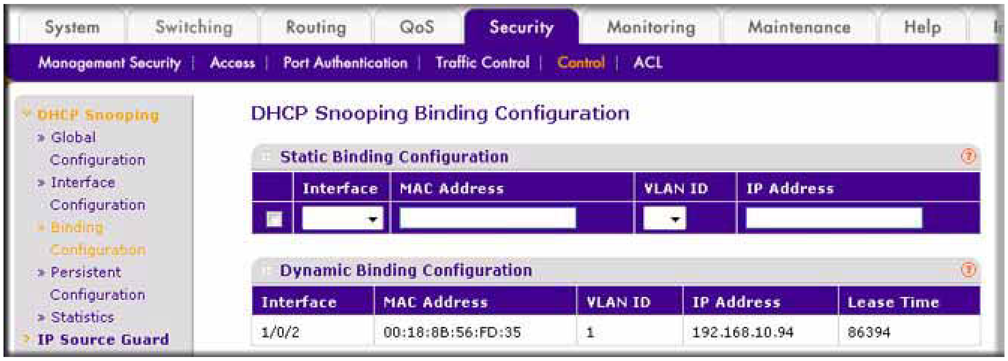
1 All Go To Interface

	Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pps)	Burst Interval(secs)
□	1/0/1	Enable	Disable	15	1
□	1/0/2	Disable	Disable	15	1

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

Static Binding Configuration

	Interface	MAC Address	VLAN ID	IP Address
□				

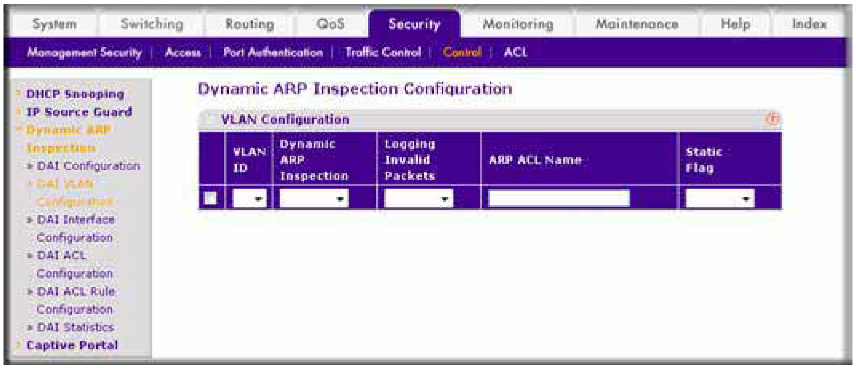
Dynamic Binding Configuration

Interface	MAC Address	VLAN ID	IP Address	Lease Time
1/0/2	00:18:8B:56:FD:35	1	192.168.10.94	86394

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

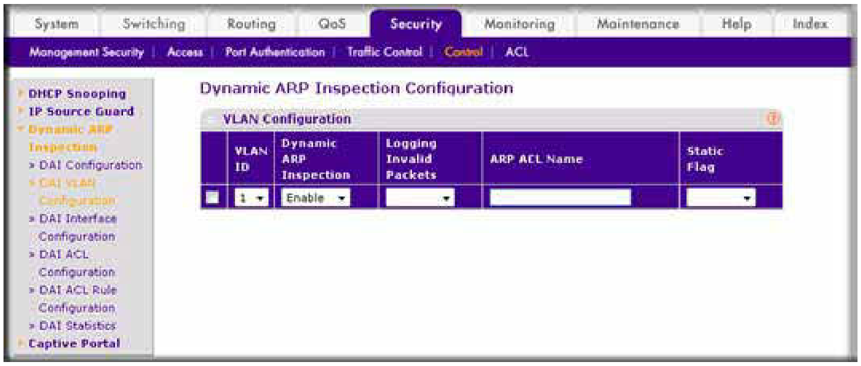
VLAN Configuration

	VLAN ID	Dynamic ARP Inspection	Logging Invalid Packets	ARP ACL Name	Static Flag
□					

b. In the **VLAN ID** field, enter **1**.

c. In the **Dynamic ARP Inspection** field, select **Enable**.

A screen similar to the following displays.



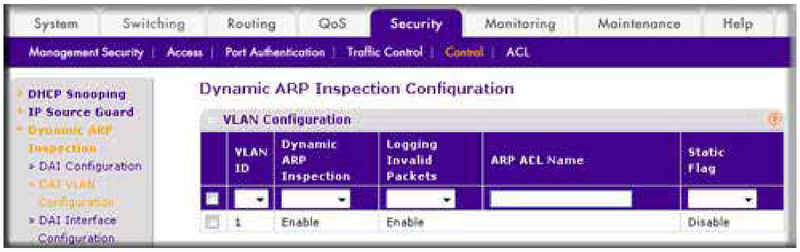
Dynamic ARP Inspection Configuration

VLAN Configuration

	VLAN ID	Dynamic ARP Inspection	Logging Invalid Packets	ARP ACL Name	Static Flag
□	1	Enable			

d. Click **Apply**.

A screen similar to the following displays.



Dynamic ARP Inspection Configuration

VLAN Configuration

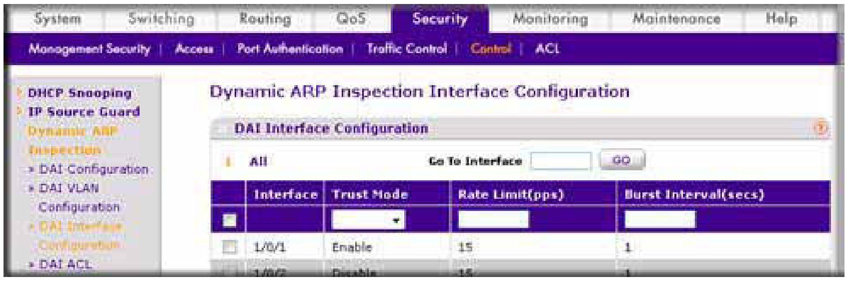
	VLAN ID	Dynamic ARP Inspection	Logging Invalid Packets	ARP ACL Name	Static Flag
□					
□	1	Enable	Enable		Disable

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.



Dynamic ARP Inspection Interface Configuration

DAI Interface Configuration

	Interface	Trust Mode	Rate Limit(pps)	Burst Interval(secs)
□				
□	1/0/1	Enable	15	1
□	1/0/2	Disable	15	1

Now ARP packets from the DHCP client will go through; however ARP packets from the static client are dropped, since it does have a DHCP snooping entry. It can be overcome by static configuration as described in the following section, *Static Mapping* on page 246.

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

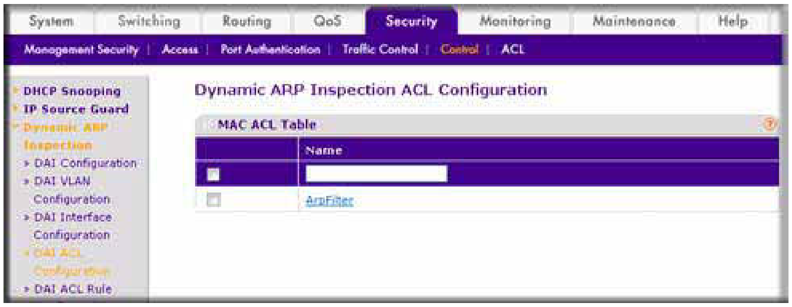
1. Create an ARP ACL.

   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.



Dynamic ARP Inspection ACL Configuration

MAC ACL Table

	Name
□	
□	ArpFilter

2. Configure a rule to allow the static client.

   a. Select **Security > Control > Dynamic ARP Inspection > DAI ACL Rule Configuration**.

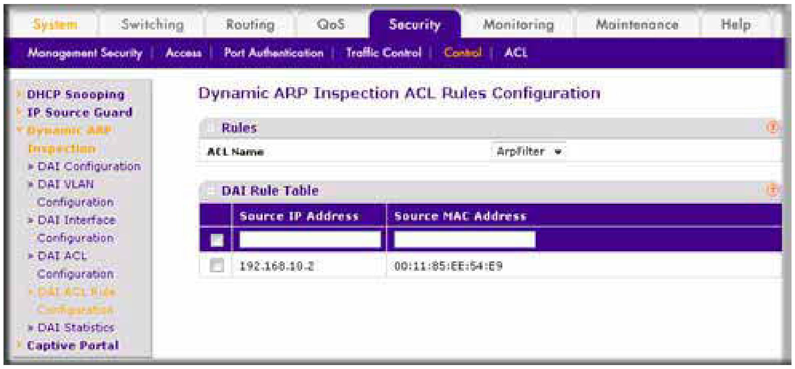
   b. In the **ACL Name** list, select **ArpFilter**.

   c. In the **Source IP Address** field, enter **192.168.10.2**.

   d. In the **Source MAC Address** field, enter **00:11:85:EE:54:E9**.

   e. Click **Add**.

A screen similar to the following displays.



Dynamic ARP Inspection ACL Rules Configuration

Rules

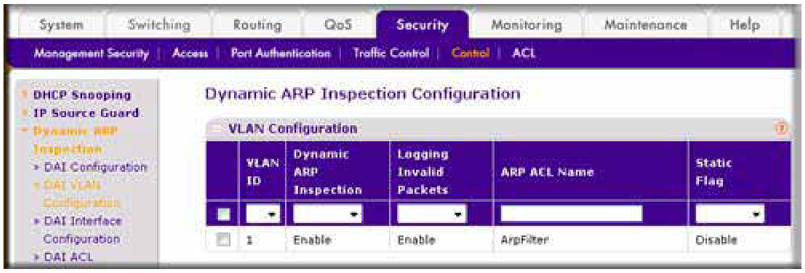
ACL Name: ArpFilter

DAI Rule Table

	Source IP Address	Source MAC Address
☐	192.168.10.2	00:11:85:EE:54:E9

3. Configure the ARP ACL used for VLAN 1.
   a. Select **Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration**.
   b. In the **ARP ACL Name** field, enter **ArpFilter**.
   c. Click **Apply**.

   A screen similar to the following displays.



Dynamic ARP Inspection Configuration

VLAN Configuration

	VLAN ID	Dynamic ARP Inspection	Logging Invalid Packets	ARP ACL Name	Static Flag
☐	1	Enable	Enable	ArpFilter	Disable

DHCP Snooping

DHCP snooping is a security feature that monitors DHCP messages between a DHCP client and DHCP server to filter harmful DHCP message and to build a bindings database of (MAC address, IP address, VLAN ID, port) tuples that are considered authorized. The network administrator enables DHCP snooping globally and on specific VLANs and configures ports within the VLAN to be trusted or untrusted. DHCP servers must be reached through trusted ports.

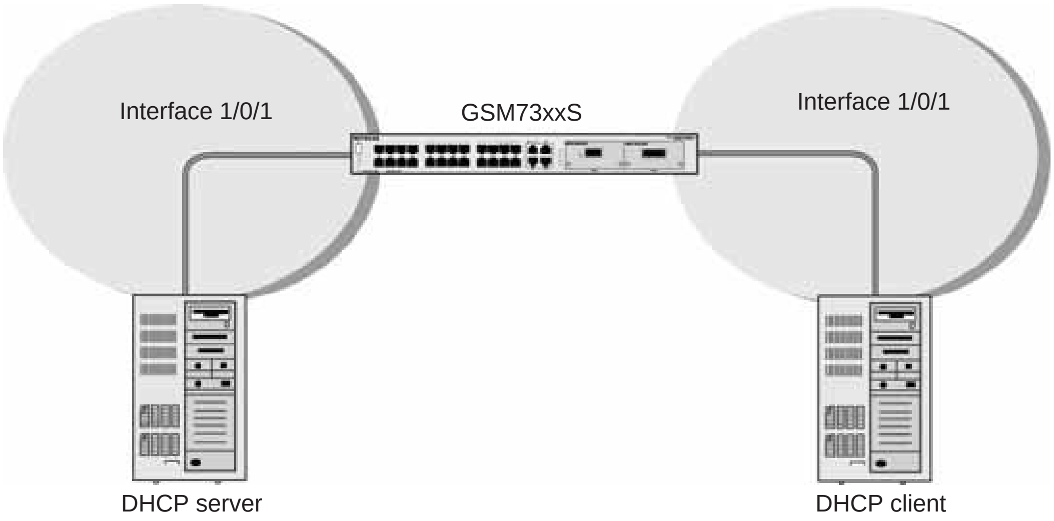


Figure 26. DHCP Snooping

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

CLI: Configure DHCP Snooping

1. Enable DHCP snooping globally.

```
(Netgear Switch) (Config)# ip dhcp snooping
```

2. Enable DHCP snooping in a VLAN.

```
(Netgear Switch) (Config)# ip dhcp snooping vlan 1
```

3. Configure the port through which the DHCP server is reached as trusted.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip dhcp snooping trust
```

4. View the DHCP Snooping Binding table.

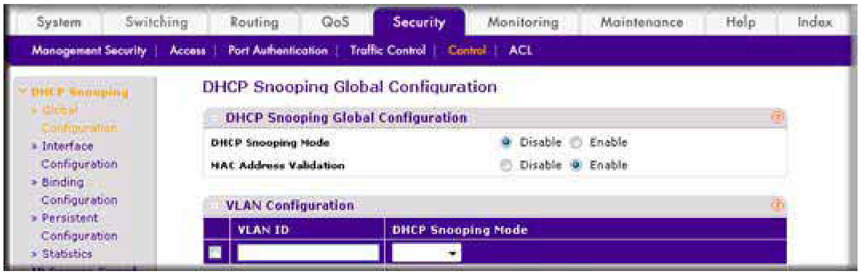
```
(GSM7328S) #show ip dhcp snooping binding

Total number of bindings:  1

MAC Address        IP Address       VLAN  Interface    Type     Lease (Secs)
-----------------  ---------------  ----  -----------  -------  -----------
00:16:76:A7:88:CC  192.168.10.89     1    1/0/2        DYNAMIC  86400
```

Web Interface: Configure DHCP Snooping

1. Enable DHCP snooping globally:

   a. Select **Security > Control > DHCP Snooping Global Configuration**.

   A screen similar to the following displays.



DHCP Snooping Global Configuration

DHCP Snooping Global Configuration

DHCP Snooping Mode	● Disable ○ Enable
MAC Address Validation	○ Disable ● Enable

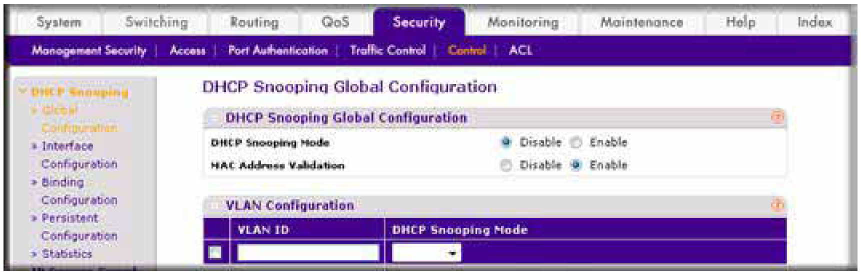
VLAN Configuration

	VLAN ID	DHCP Snooping Mode
□		

   b. For DHCP Snooping Mode, select **Enable**.

   c. Click **Apply**.

   A screen similar to the following displays:.



DHCP Snooping Global Configuration

DHCP Snooping Global Configuration

DHCP Snooping Mode	● Disable ○ Enable
MAC Address Validation	○ Disable ● Enable

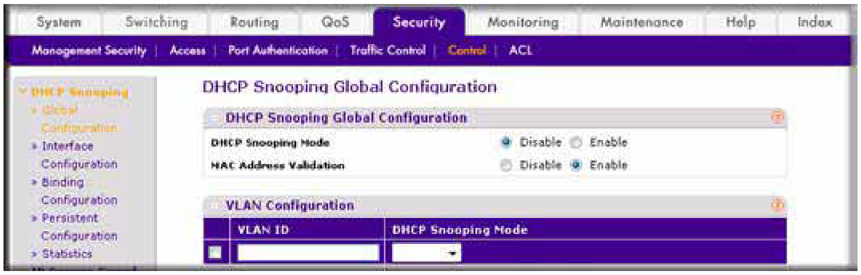
VLAN Configuration

	VLAN ID	DHCP Snooping Mode
□		

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 Global Configuration

DHCP Snooping Mode	● Disable ○ Enable
MAC Address Validation	○ Disable ● Enable

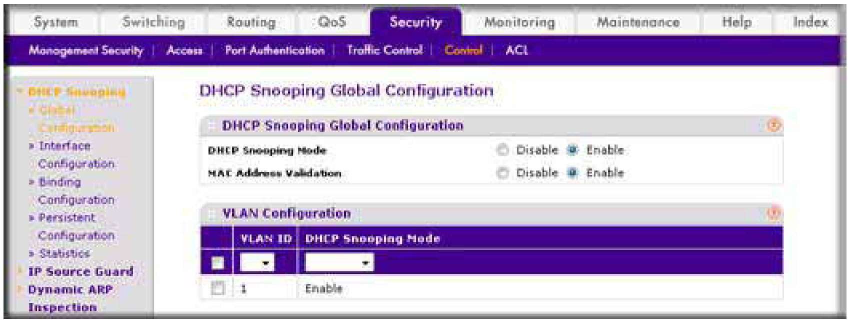
VLAN Configuration

	VLAN ID	DHCP Snooping Mode
□		

   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 Global Configuration

DHCP Snooping Mode ○ Disable ● Enable

MAC Address Validation ○ Disable ● Enable

VLAN Configuration

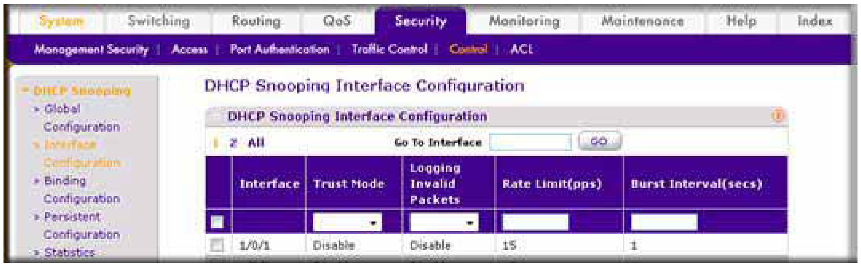
	VLAN ID	DHCP Snooping Mode
□	1	Enable

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

DHCP Snooping Interface Configuration

1 2 All Go To Interface

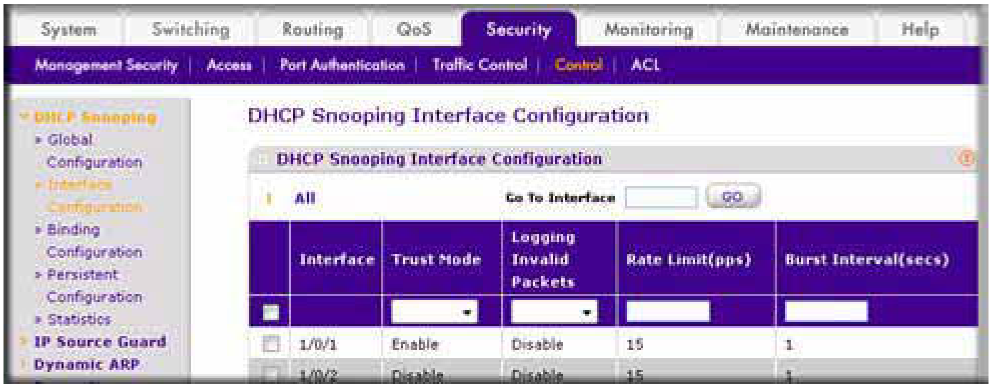
	Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pps)	Burst Interval(secs)
□	1/0/1	Disable	Disable	15	1

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

c. For Interface 1/01/, in the Trust Mode field, select **Enable**.

d. Click **Apply**.

A screen similar to the following displays.



DHCP Snooping Interface Configuration

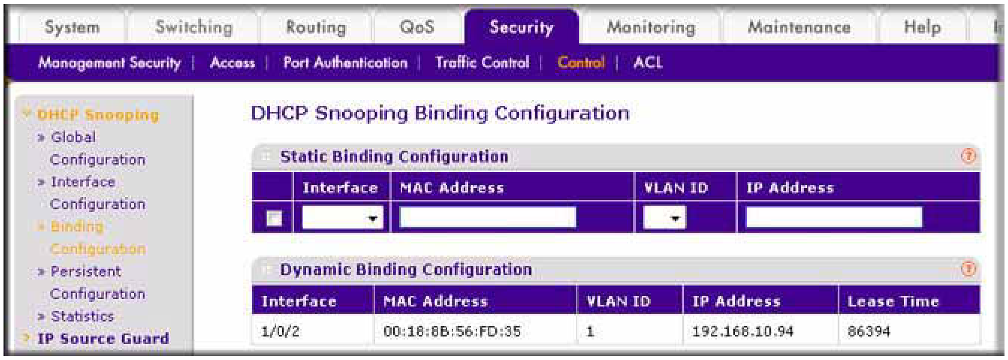
DHCP Snooping Interface Configuration

1 All Go To Interface

	Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pps)	Burst Interval(secs)
□	1/0/1	Enable	Disable	15	1
□	1/0/2	Disable	Disable	15	1

4. Select **Security > Control > DHCP Snooping Binding Configuration**.

A screen similar to the following displays.



DHCP Snooping Binding Configuration

Static Binding Configuration

	Interface	MAC Address	VLAN ID	IP Address
□				

Dynamic Binding Configuration

Interface	MAC Address	VLAN ID	IP Address	Lease Time
1/0/2	00:18:8B:56:FD:35	1	192.168.10.94	86394

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
```

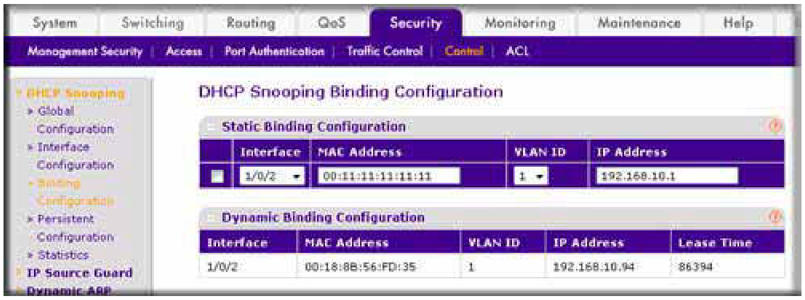
2. Check to make sure the binding database has the static entry.

```
(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**.

   A screen similar to the following displays.



DHCP Snooping Binding Configuration

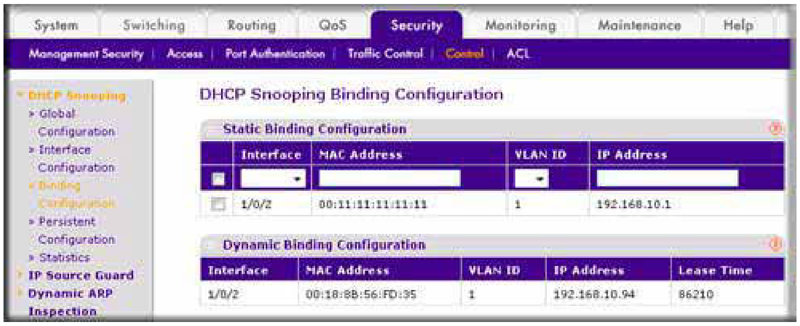
Static Binding Configuration

	Interface	MAC Address	VLAN ID	IP Address
□	1/0/2	00:11:11:11:11:11	1	192.168.10.1

Dynamic Binding Configuration

Interface	MAC Address	VLAN ID	IP Address	Lease Time
1/0/2	00:18:8B:56:FD:35	1	192.168.10.94	86394

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.



DHCP Snooping Binding Configuration

Static Binding Configuration

	Interface	MAC Address	VLAN ID	IP Address
□				
□	1/0/2	00:11:11:11:11:11	1	192.168.10.1

Dynamic Binding Configuration

Interface	MAC Address	VLAN ID	IP Address	Lease Time
1/0/2	00:18:8B:56:FD:35	1	192.168.10.94	86210

Maximum Rate of DHCP Messages

To prevent DHCP packets being used as DoS attachments when DHCP snooping is enabled, the snooping application enforces a rate limit for DHCP packets received on untrusted interfaces. DHCP snooping monitors the receive rate on each interface separately. If the receive rate exceeds the configured limit, DHCP snooping brings down the interface. The user must specify “no shutdown” on this interface to further work with that port.

CLI: Configure the Maximum Rate of DHCP Messages

1. Control the maximum rate of DHCP messages.

```
(Netgear Switch) (Interface 1/0/2)# ip dhcp snooping limit rate 5
```

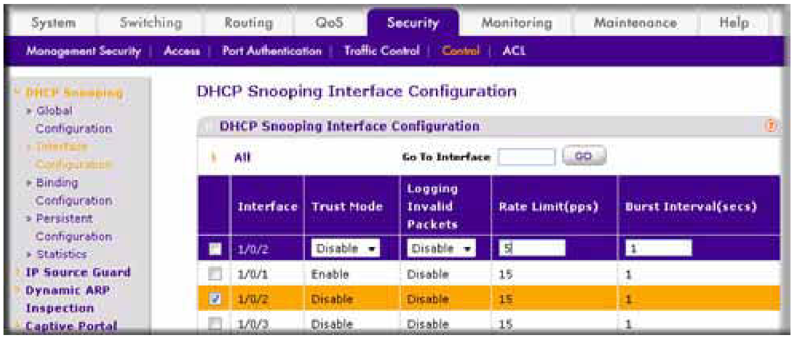
2. View the rate configured.

```
(GSM7328S) #show ip dhcp snooping interfaces 1/0/2

Interface      Trust State      Rate Limit      Burst Interval
                                   (pps)           (seconds)
----------    -------------    -------------   ---------------

1/0/2               No                5                 1
```

Web Interface: Configure the Maximum Rate of DHCP Messages

1. Select **Security > Control > DHCP Snooping > Interface Configuration**.

   A screen similar to the following displays:



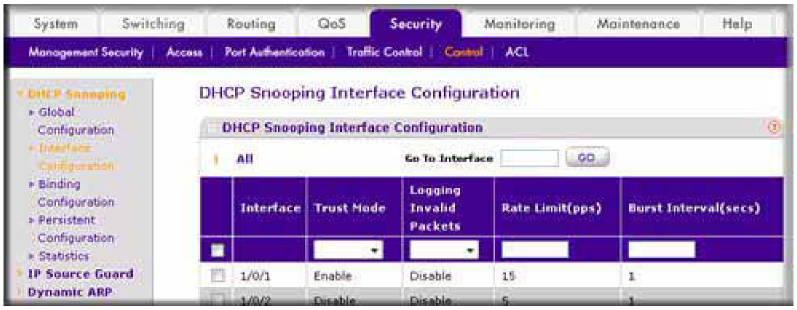
DHCP Snooping Interface Configuration

DHCP Snooping Interface Configuration

	Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pps)	Burst Interval(secs)
□	1/0/2	Disable	Disable	5	1
□	1/0/1	Enable	Disable	15	1
☑	1/0/2	Disable	Disable	15	1
□	1/0/3	Disable	Disable	15	1

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.



DHCP Snooping Interface Configuration

DHCP Snooping Interface Configuration

	Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pps)	Burst Interval(secs)
□					
□	1/0/1	Enable	Disable	15	1
□	1/0/2	Disable	Disable	5	1

IP Source Guard

IP Source Guard uses the DHCP snooping bindings database. When IP Source Guard is enabled, the switch drops incoming packets that do not match a binding in the bindings database. IP Source Guard can be configured to enforce just the source IP address or both the source IP address and source MAC address.

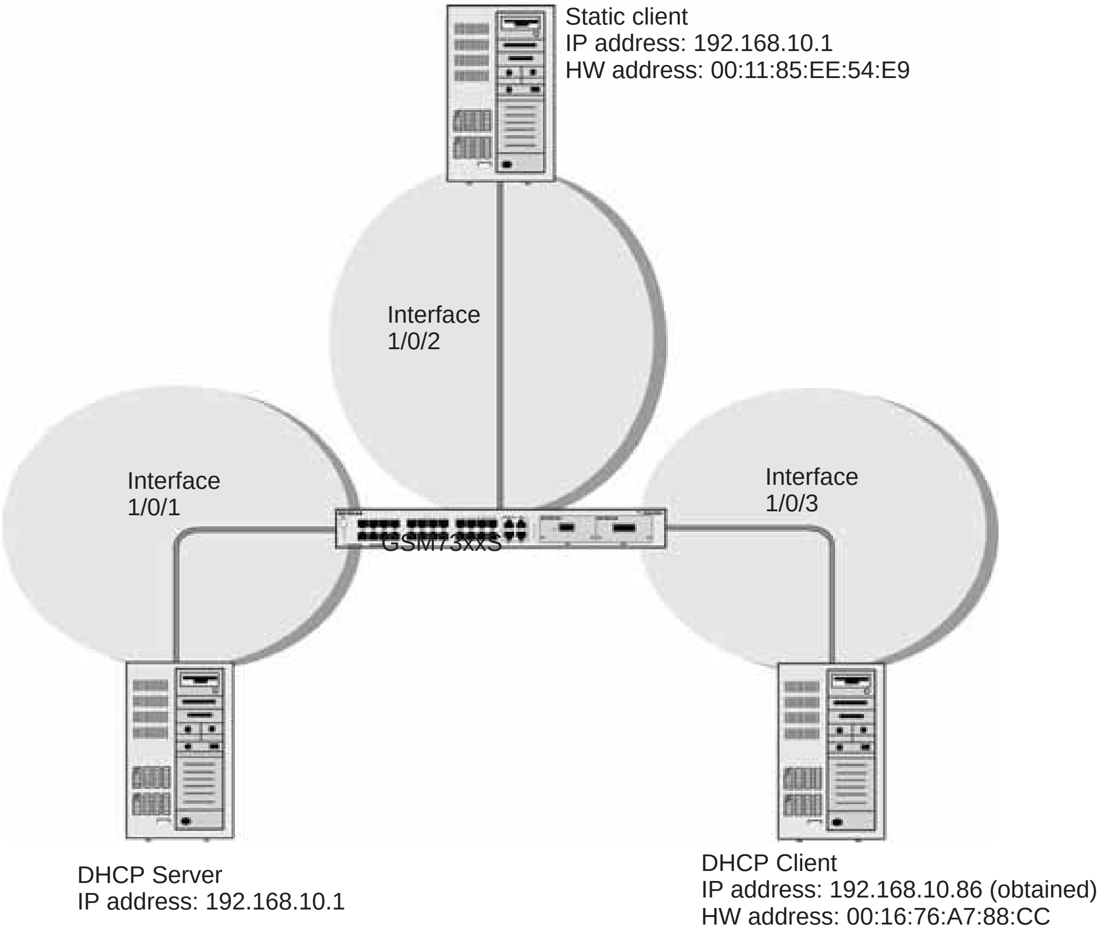


Figure 27. IP Source Guard

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

CLI: Configure Dynamic ARP Inspection

1. Enable DHCP snooping globally.

```
(Netgear Switch) (Config)# ip dhcp snooping
```

2. Enable DHCP snooping in a VLAN.

```
(Netgear Switch) (Config)# ip dhcp snooping vlan 1
```

3. Configure the port through which the DHCP server is reached as trusted.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip dhcp snooping trust
```

4. View the DHCP Snooping Binding table.

```
(GSM7328S) #show ip dhcp snooping binding

Total number of bindings:  1

MAC Address        IP Address       VLAN  Interface    Type     Lease (Secs)
-----------------  ---------------  ----  -----------  -------  -----------
00:16:76:A7:88:CC  192.168.10.86    1     1/0/2        DYNAMIC  86400
```

If the entry does not exist in the DHCP Snooping Binding table, you can add it statically through the **`ip verify binding`** *`mac-address`* **`vlan`** *`vlan id ip address`* **`interface`** *`interface id`* command in global configuration mode.

5. Enable IP Source Guard in interface 1/0/2.

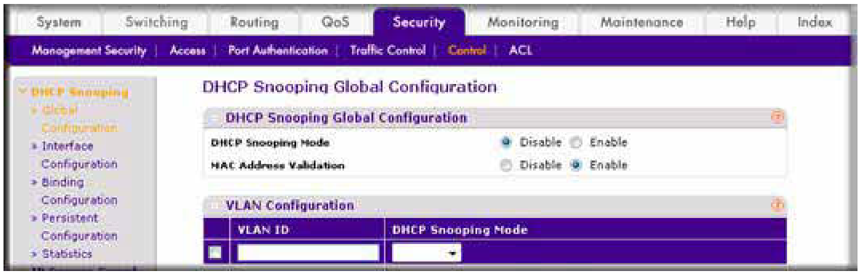
```
(GSM7352Sv2) (Interface 1/0/2)#ip verify source port-security
```

With this configuration, the device verifies both the source IP address and the source MAC address. If the port-security option is skipped, the device verifies only the source IP address.

Web Interface: Configure Dynamic ARP Inspection

1. Enable DHCP snooping globally.
   a. Select **Security > Control > DHCP Snooping Global Configuration**.

      A screen similar to the following displays.



DHCP Snooping Global Configuration

DHCP Snooping Global Configuration

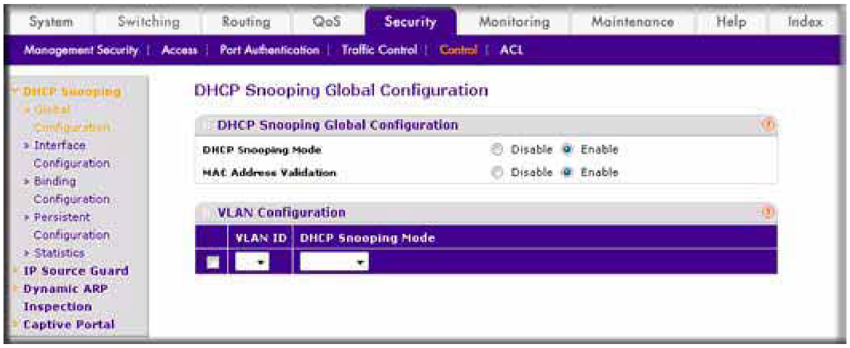
DHCP Snooping Mode	● Disable ○ Enable
MAC Address Validation	○ Disable ● Enable

VLAN Configuration

	VLAN ID	DHCP Snooping Mode
□		

   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

DHCP Snooping Global Configuration

DHCP Snooping Mode	○ Disable ● Enable
MAC Address Validation	○ Disable ● Enable

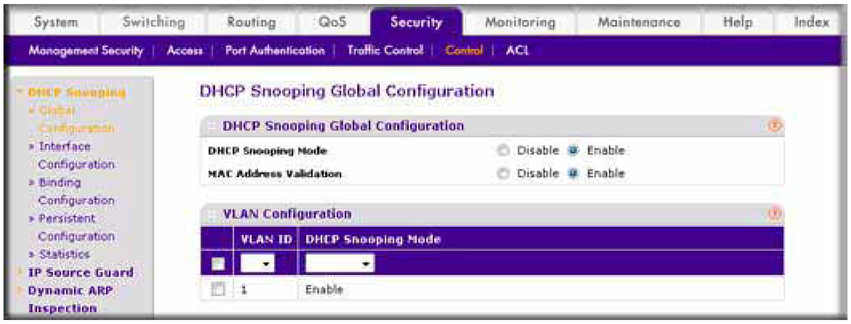
VLAN Configuration

	VLAN ID	DHCP Snooping Mode
□		

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.



DHCP Snooping Global Configuration

DHCP Snooping Global Configuration

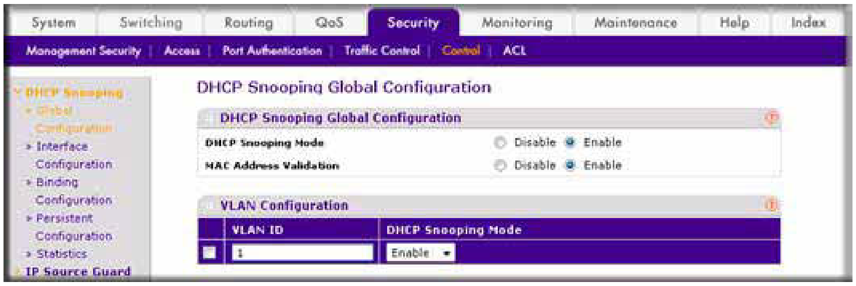
DHCP Snooping Mode	○ Disable ● Enable
MAC Address Validation	○ Disable ● Enable

VLAN Configuration

	VLAN ID	DHCP Snooping Mode
□		
□	1	Enable

d. Click **Apply**.

A screen similar to the following displays.



DHCP Snooping Global Configuration

DHCP Snooping Global Configuration

DHCP Snooping Mode	○ Disable ● Enable
MAC Address Validation	○ Disable ● Enable

VLAN Configuration

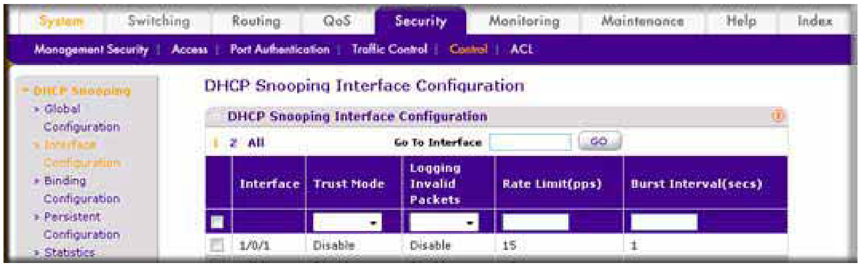
	VLAN ID	DHCP Snooping Mode
□	1	Enable

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

DHCP Snooping Interface Configuration

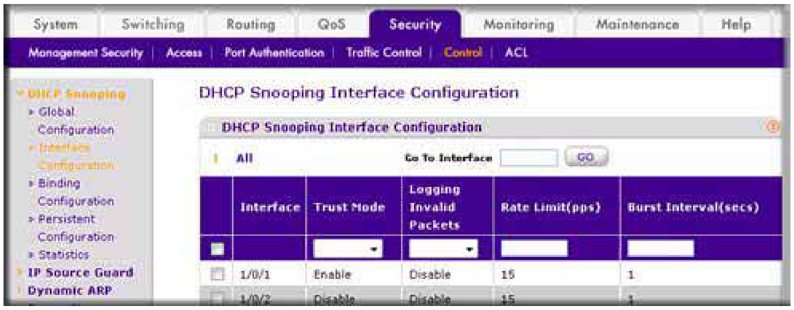
	Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pps)	Burst Interval(secs)
□					
□	1/0/1	Disable	Disable	15	1

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

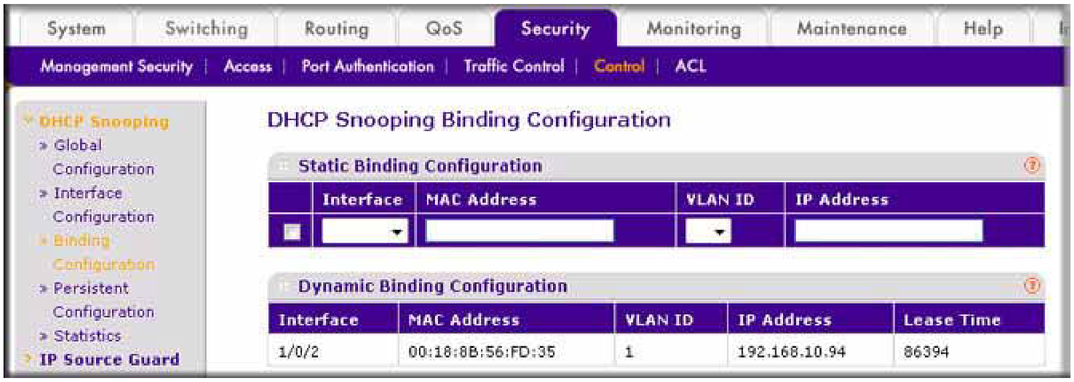
DHCP Snooping Interface Configuration

	Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pps)	Burst Interval(secs)
□					
□	1/0/1	Enable	Disable	15	1
□	1/0/2	Disable	Disable	15	1

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

Static Binding Configuration

	Interface	MAC Address	VLAN ID	IP Address
□				

Dynamic Binding Configuration

Interface	MAC Address	VLAN ID	IP Address	Lease Time
1/0/2	00:18:8B:56:FD:35	1	192.168.10.94	86394

5. Enable IP source guard in the interface 1/0/2.

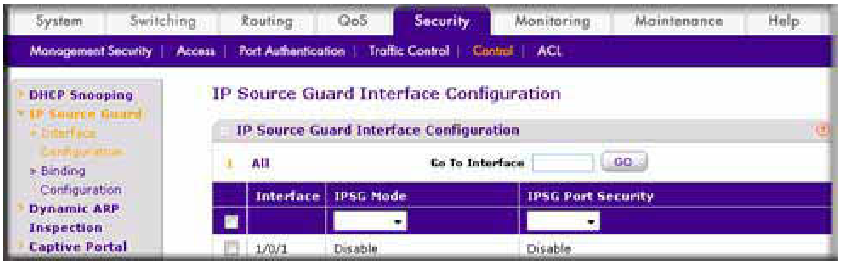
   a. Select **Security > Control > IP Source Guard > Interface Configuration**.

   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.

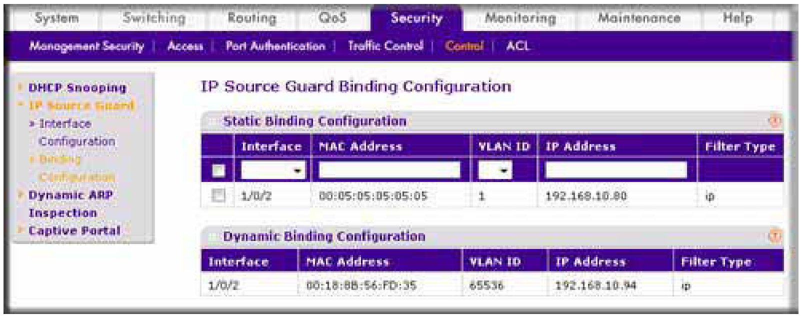


IP Source Guard Interface Configuration

IP Source Guard Interface Configuration

	Interface	IPSG Mode	IPSG Port Security
□	1/0/1	Disable	Disable

6. Set up IP source guard static binding.
   a. Select **Security > Control > IP Source Guard > Binding Configuration**.
   b. Select the Interface **1/0/2** check box.
   c. In the **MAC Address** field, enter **00:05:05:05:05:05**.
   d. In the **VLAN ID** field, enter **1**.
   e. In the **IP Address** field, enter **192.168.10.80**.
   f. Click **Add**. A screen similar to the following displays.



IP Source Guard Binding Configuration

Static Binding Configuration

	Interface	MAC Address	VLAN ID	IP Address	Filter Type
□	1/0/2	00:05:05:05:05:05	1	192.168.10.80	ip

Dynamic Binding Configuration

Interface	MAC Address	VLAN ID	IP Address	Filter Type
1/0/2	00:18:8B:56:FD:35	65536	192.168.10.94	ip

13. SNTP

Simple Network Time Protocol

13

This chapter includes the following sections:

- *SNTP Concepts*
- *Show SNTP*
- *Configure SNTP*
- *Set the Time Zone*
- *Set the Named SNTP Server*

SNTP Concepts

Simple Network Time Protocol (SNTP) can provide the following benefits:

- It can be used to synchronize network resources and for adaptation of NTP.
- SNTP provides synchronized network timestamp.
- It can be used in broadcast or unicast mode.
- It supports SNTP client implemented over UDP, which listens on port 123.

Show SNTP

The following are examples of the commands used in the SNTP feature. These examples are provided for thew CLI only.

show sntp

```
(Netgear Switch Routing) #show sntp?

<cr>      Press Enter to execute the command.
client    Display SNTP Client Information.
server    Display SNTP Server Information.
```

show sntp client

```
(Netgear Switch Routing) #show sntp client

Client Supported Modes:    unicast broadcast
SNTP Version:              4
Port:                      123
Client Mode:               unicast
Unicast Poll Interval:     6
Poll Timeout (seconds):    5
Poll Retry:                1
```

show sntp server

```
(Netgear Switch Routing) #show sntp server

Server IP Address:          81.169.155.234
Server Type:                ipv4
Server Stratum:             3
Server Reference Id:        NTP Srv: 212.186.110.32
Server Mode:                Server
Server Maximum Entries:     3
Server Current Entries:     1

SNTP Servers
------------

IP Address:                  81.169.155.234
Address Type:                IPV4
Priority:                    1
Version:                     4
Port:                        123
Last Update Time:            MAY 18 04:59:13 2005
Last Attempt Time:           MAY 18 11:59:33 2005
Last Update Status:          Other
Total Unicast Requests:      1111
Failed Unicast Requests:     361
```

Configure SNTP

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

CLI: Configure SNTP

NETGEAR switches do not have a built-in real-time clock. However, it is possible to use SNTP to get the time from a public SNTP/NTP server over the Internet. You may need permission from those public time servers. The following steps configure SNTP on the switch:

1. Configure the SNTP server IP address. The IP address can be either from the public NTP server or your own. You can search the Internet to locate the public server. The servers available could be listed in domain-name format instead of address format. In that case, use the `ping` command on the PC to find the server's IP address. The following example configures the SNTP server IP address to 208.14.208.19.

```
(Netgear Switch) (Config)#sntp server 208.14.208.19
```

2. After configuring the IP address, enable SNTP client mode. The client mode can be either broadcast mode or unicast mode. If the NTP server is not your own, you must use unicast mode.

```
(Netgear Switch) (Config)#sntp client mode unicast
```

3. Once SNTP client mode is enabled, the client waits for the polling interval to send the query to the server. The default value is approximately 1 minute. After this period, issue the **show** command to confirm that the time has been received. The time will be used in all logging messages.

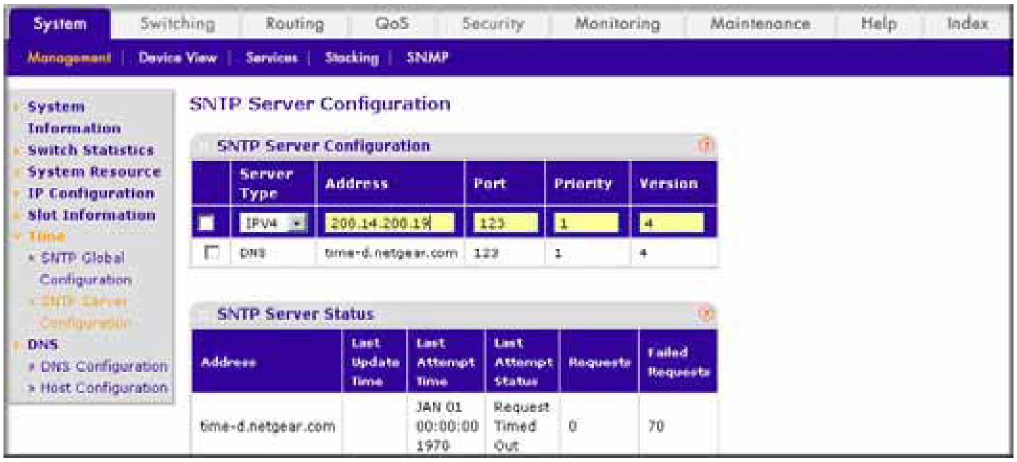
```
(Netgear Switch) #show sntp server
Server IP Address:                   208.14.208.19
Server Type:                         ipv4
Server Stratum:                      4
Server Reference Id:                 NTP Srv: 208.14.208.3
Server Mode:                         Server
Server Maximum Entries:              3
Server Current Entries:              1
SNTP Servers
------------

IP Address: 208.14.208.19
Address Type: IPV4
Priority: 1
Version: 4
Port: 123
Last Update Time: Mar 26 03:36:09 2006
Last Attempt Time: Mar 26 03:36:09 2006
Last Update Status: Success
Total Unicast Requests: 2
Failed Unicast Requests: 0
```

Web Interface: Configure SNTP

1. Configure the SNTP server.

   a. Select **System > Management >Time > SNTP Server Configuration**.

A screen similar to the following displays.



SNTP Server Configuration

SNTP Server Configuration

	Server Type	Address	Port	Priority	Version
□	IPV4	200.14.200.19	123	1	4
□	DNS	time-d.netgear.com	123	1	4

SNTP Server Status

Address	Last Update Time	Last Attempt Time	Last Attempt Status	Requests	Failed Requests
time-d.netgear.com		JAN 01 00:00:00 1970	Request Timed Out	0	70

b. Enter the following information:

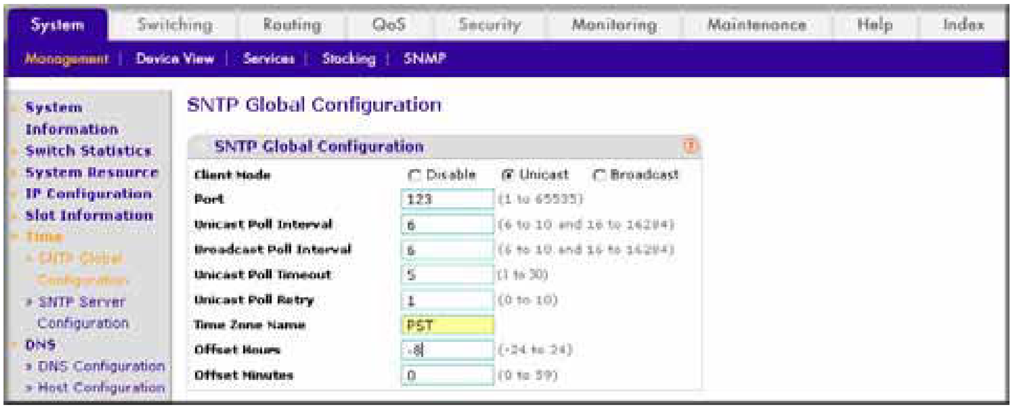
- In the **Server Type** field, select **IPV4**.
- In the **Address** field, enter **208.14.208.19**.
- In the **Port** field, enter **123**.
- In the **Priority** field, enter **1**.
- In the **Version** field, enter **4**.

c. Click **Add**.

2. Configure SNTP globally.

a. Select **System > Management > Time > SNTP Global Configuration**.

A screen similar to the following displays.



SNTP Global Configuration

SNTP Global Configuration

Client Mode	○ Disable ● Unicast ○ Broadcast	
Port	123	(1 to 65535)
Unicast Poll Interval	6	(6 to 10 and 16 to 16284)
Broadcast Poll Interval	6	(6 to 10 and 16 to 16284)
Unicast Poll Timeout	5	(1 to 30)
Unicast Poll Retry	1	(0 to 10)
Time Zone Name	PST	
Offset Hours	-8	(-24 to 24)
Offset Minutes	0	(0 to 59)

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

This example is provided for the 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
```

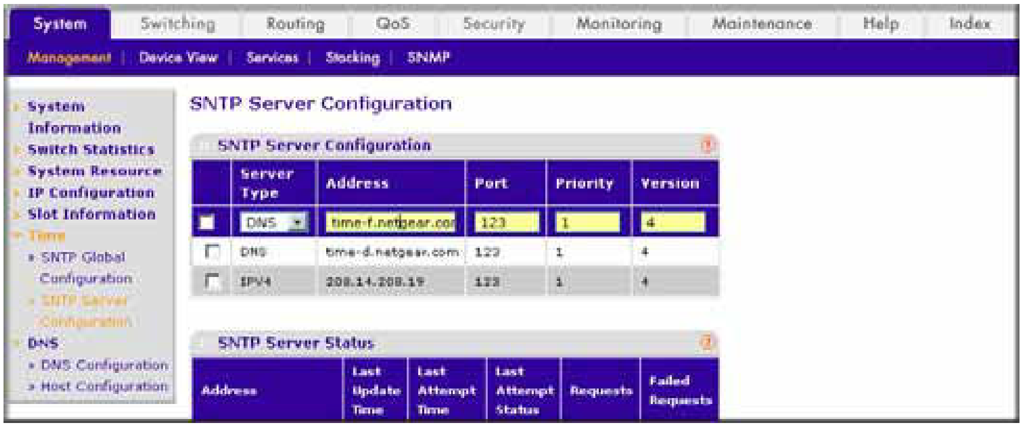
where *192.168.1.1* is the public network gateway IP address for your device.

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

SNTP Server Configuration

	Server Type	Address	Port	Priority	Version
☐	DNS	time-f.netgear.com	123	1	4
☐	DNS	time-d.netgear.com	123	1	4
☐	IPV4	208.14.208.19	123	1	4

SNTP Server Status

Address	Last Update Time	Last Attempt Time	Last Attempt Status	Requests	Failed Requests

b. Enter the following information:

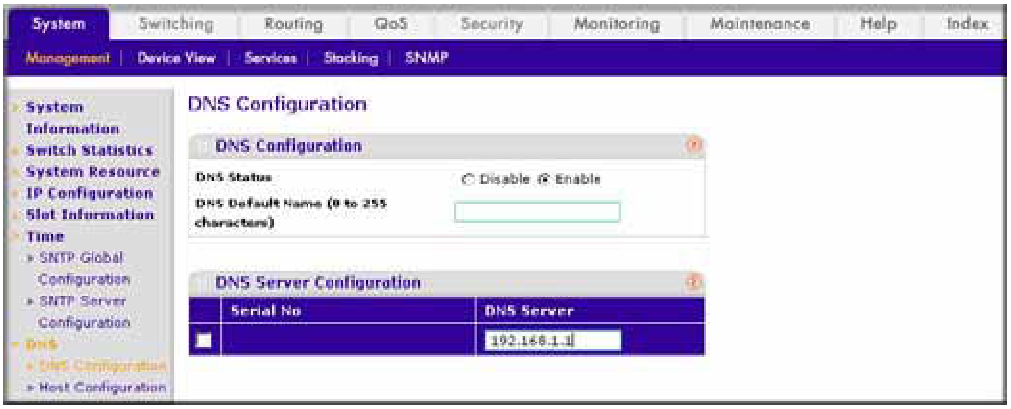
- In the **Server Type** list, select **DNS**.
- In the **Address** field, enter **time-f.netgear.com**
- In the **Port** field, enter **123**.
- In the **Priority** field, enter **1**.
- In the **Version** field, enter **4**.

c. Click **Add**.

2. Configure the DNS server.

a. Select **System > Management > DNS > DNS Configuration**.

A screen similar to the following displays.



DNS Configuration

DNS Configuration

DNS Status ○ Disable ● Enable

DNS Default Name (0 to 255 characters)

DNS Server Configuration

	Serial No	DNS Server
☐		192.168.1.1

b. Enter the following information:

- For DNS Status, select the **Enable** radio button
- In the **DNS Server** field, enter **192.168.1.1**.

c. Click **Add**.

14. Tools

14

Tools to manage, monitor, and personalize the switch and network

This chapter includes the following sections:

- *Traceroute*
- *Configuration Scripting*
- *Pre-Login Banner*
- *Port Mirroring*
- *Dual Image*
- *Outbound Telnet*

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.

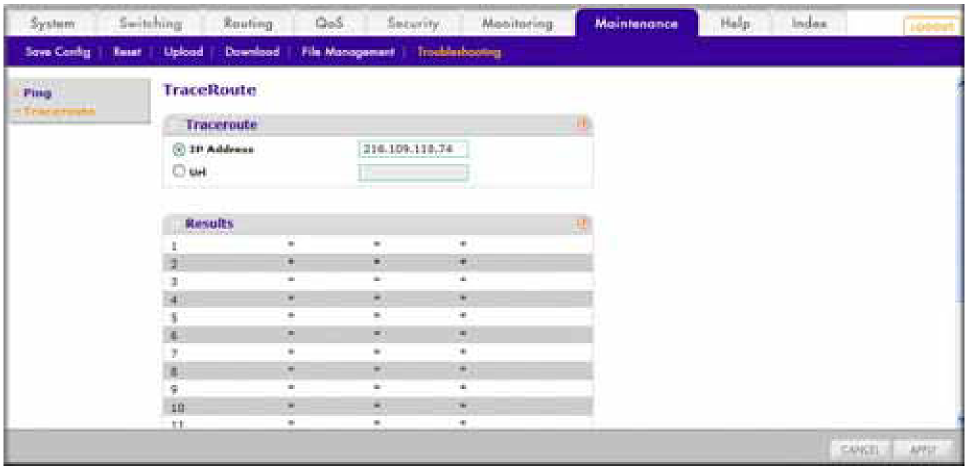
CLI: Traceroute

```
(Netgear Switch) #traceroute?
<ipaddr>      Enter IP address.

(Netgear Switch) #traceroute 216.109.118.74 ?
<cr>    Press Enter to execute the command.
<port>        Enter port no.

(Netgear Switch) #traceroute 216.109.118.74
tracing route over a maximum of 20 hops
1  10.254.24.1        40 ms       9 ms      10 ms
 2  10.254.253.1       30 ms      49 ms      21 ms
 3  63.237.23.33       29 ms      10 ms      10 ms
 4  63.144.4.1         39 ms      63 ms      67 ms
 5  63.144.1.141       70 ms      50 ms      50 ms
 6  205.171.21.89      39 ms      70 ms      50 ms
 7  205.171.8.154      70 ms      50 ms      70 ms
 8  205.171.8.222      70 ms      50 ms      80 ms
 9  205.171.251.34     60 ms      90 ms      50 ms
10  209.244.219.181    60 ms      70 ms      70 ms
11  209.244.11.9       60 ms      60 ms      50 ms
12  4.68.121.146       50 ms      70 ms      60 ms
13  4.79.228.2         60 ms      60 ms      60 ms
14  216.115.96.185    110 ms      59 ms      70 ms
15  216.109.120.203    70 ms      66 ms      95 ms
16  216.109.118.74     78 ms     121 ms      69 ms
```

Web Interface: Traceroute

1. Select **Maintenance > Troubleshooting > Traceroute**.

   A screen similar to the following displays.



TraceRoute

Traceroute

● IP Address 216.109.118.74

○ Url

Results

1	*	*	*
2	*	*	*
3	*	*	*
4	*	*	*
5	*	*	*
6	*	*	*
7	*	*	*
8	*	*	*
9	*	*	*
10	*	*	*
11	*	*	*

   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 270
- *script list and script delete* on page 270
- *script apply running-config.scr* on page 271
- *Create a Configuration Script* on page 271
- *Upload a Configuration Script* on page 271

Configuration scripting:

- Allows you to generate text-formatted files.
- Provides scripts that can be uploaded and downloaded to the system.
- Provides flexibility to create command configuration scripts.
- Can be applied to several switches.
- Can save up to 10 scripts or 500 K of memory.
- Provides script format of one CLI command per line.

Here are some considerations:

- The total number of scripts stored is limited by the NVRAM/FLASH size.
- Application of scripts is partial if a script fails. For example, if the script executes 5 of 10 commands and the script fails, the script stops at 5.
- Scripts cannot be modified or deleted while being applied.
- Validation of scripts checks for syntax errors only. It does not validate that the script will run successfully.

script

```
(Netgear Switch) #script ?

apply       Applies configuration script to the switch.
delete      Deletes a configuration script file from the switch.
list        Lists all configuration script files present on the switch.
show        Displays the contents of configuration script.
validate    Validate the commands of configuration script.
```

script list and script delete

```
(Netgear Switch) #script list

Configuration Script Name        Size(Bytes)
-------------------------        -----------
basic.scr                        93
running-config.scr               3201

2 configuration script(s) found.
1020706 bytes free.

(Netgear Switch) #script delete basic.scr

Are you sure you want to delete the configuration script(s)? (y/n) y

1 configuration script(s) deleted.
```

script apply running-config.scr

```
(Netgear Switch) #script apply running-config.scr

Are you sure you want to apply the configuration script? (y/n) y

The system has unsaved changes.
Would you like to save them now? (y/n) y

Configuration Saved!
```

Create a Configuration Script

```
(Netgear Switch) #show running-config running-config.scr

Config script created successfully.

(Netgear Switch)                     #script list

Configuration Script Name        Size(Bytes)
-------------------------        ----------
running-config.scr               3201

1 configuration script(s) found.
1020799 bytes free.
```

Upload a Configuration Script

```
(Netgear Switch) #copy nvram: script running-config.scr
tftp://192.168.77.52/running-config.scr

Mode.........................        TFTP
Set TFTP Server IP...........        192.168.77.52
TFTP Path....................        ./
TFTP Filename................        running-config.scr
Data Type....................        Config Script
Source Filename..............        running-config.scr

Are you sure you want to start? (y/n) y

File transfer operation completed successfully.
```

Pre-Login Banner

Pre-login banner:

- Allows you to create message screens that display when a user logs in to the CLI.
- By default, no banner file exists.
- You can upload or download.
- File size cannot be larger than 2 K.

The Pre-Login Banner feature is only for the CLI interface.

Create a Pre-Login Banner

This command is provided for the 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.

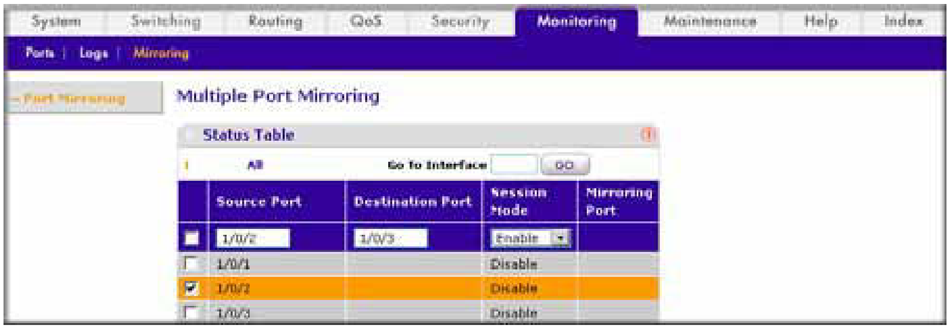
CLI: Specify the Source (Mirrored) Ports and Destination (Probe)

```
(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.



Multiple Port Mirroring

Status Table

	All	Go To Interface	GO	
	Source Port	**Destination Port**	**Session Mode**	**Mirroring Port**
□	1/0/2	1/0/3	Enable	
□	1/0/1		Disable	
☑	1/0/2		Disable	
□	1/0/3		Disable	

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 **i**`mage2`. 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-imag**e 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 Back up an Image and Make It Active

```
(Netgear Switch) #copy tftp://192.168.0.1/gsm73xxseps.stk image2
Mode........................................... TFTP
Set Server IP.................................. 192.168.0.1
Path........................................... ./
Filename....................................... gsm73xxseps.stk
Data Type...................................... Code
Destination Filename........................... image2
Management access will be blocked for the duration of the transfer Are you sure you
want to start? (y/n) y


TFTP code transfer starting
101888 bytes transferred...277504 bytes transferred...410112 bytes
transferred...628224 bytes transferred....803328 bytes transferred...978944 bytes
transferred...1154560 bytes transferred...1330176 bytes transferred...1505280 bytes
transferred...1680896 bytes transferred...1861632 bytes transferred...2040320 bytes
transferred...2215936 bytes transferred...2391040 bytes transferred...2566656 bytes
transferred...2741760 bytes transferred...2916864 bytes transferred...3092992 bytes
transferred...3268096 bytes transferred...3443712 bytes transferred...3619328 bytes
transferred...3794432 bytes transferred...3970048 bytes transferred...4145152 bytes
transferred...4320768 bytes transferred...4496384 bytes transferred...4669952 bytes
transferred...4849152 bytes transferred...5027840 bytes transferred...5202944 bytes
transferred...5378560 bytes transferred...5554176 bytes transferred...5729280 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...7307776 bytes
transferred...7483392 bytes transferred...7658496 bytes transferred...
Verifying CRC of file in Flash File System
Distributing the code to the members of the stack!
File transfer operation completed successfully.
(Netgear Switch) #
(Netgear Switch) #show bootvar
Image Descriptions
 image1 : default image
 image2 :
 Images currently available on Flash
```

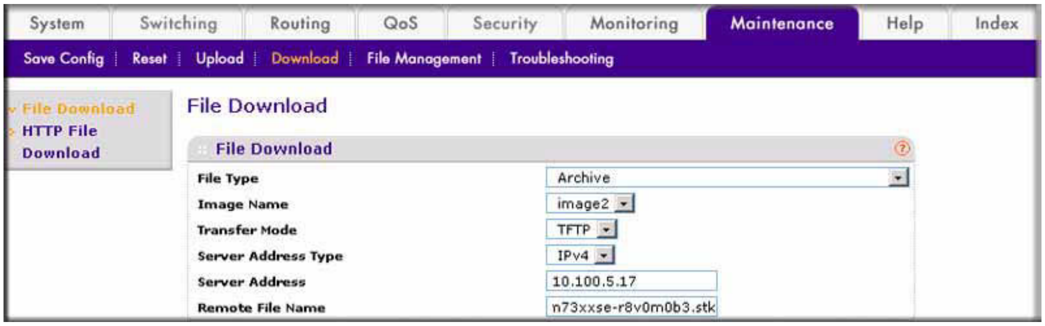
```
--------------------------------------------------------------------
 unit      image1      image2     current-active        next-active
--------------------------------------------------------------------
1   5.11.2.51     8.0.0.2            image1             image1
(Netgear Switch) #boot system image2
Activating image image2 ..
(Netgear Switch) #show bootvar
Image Descriptions
image1 : default image
image2 :
Images currently available on Flash
--------------------------------------------------------------------
unit      image1      image2     current-active        next-active
--------------------------------------------------------------------
1   5.11.2.51     8.0.0.2            image1             image2
                                      Image2 will be executed after reboot.
```

Web Interface: Download a Backup Image and Make It Active

1. Download a backup image using tftp.

   a. Select **Maintenance > Download > File Download**.

   A screen similar to the following displays.



File Download

File Download

File Type	Archive
Image Name	image2
Transfer Mode	TFTP
Server Address Type	IPv4
Server Address	10.100.5.17
Remote File Name	n73xxse-r8v0m0b3.stk

   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).

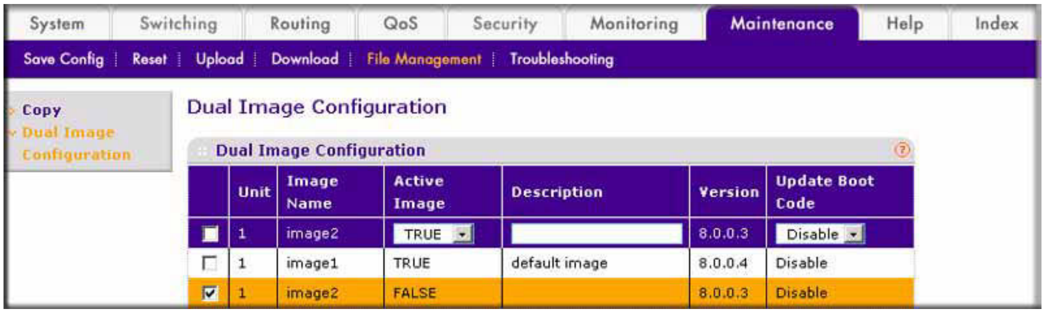
   g. In the **Remote File Name**, enter **gsm73xxse-r8v0m0b3.stk**.

   h. Click **Apply**.

2. Activate image2.

   a. Select **Maintenance > File Management > Dual Image Configuration**.

A screen similar to the following displays.



Dual Image Configuration

Dual Image Configuration

	Unit	Image Name	Active Image	Description	Version	Update Boot Code
☐	1	image2	TRUE		8.0.0.3	Disable
☐	1	image1	TRUE	default image	8.0.0.4	Disable
☑	1	image2	FALSE		8.0.0.3	Disable

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 278
- *CLI: transport output telnet* on page 279
- *Web Interface: Configure Telnet* on page 279
- *CLI: Configure the session-limit and session-timeout* on page 280
- *Web Interface: Configure the Session Timeout* on page 280

Outbound Telnet:

- Establishes an outbound Telnet connection between a device and a remote host.
- A Telnet connection is initiated, each side of the connection is assumed to originate and terminate at a network virtual terminal (NVT).
- Server and user hosts do not maintain information about the characteristics of each other’s terminals and terminal handling conventions.
- Must use a valid IP address.

CLI: show network

```
(Netgear Switch Routing) >telnet 192.168.77.151
Trying 192.168.77.151...
(Netgear Switch Routing)
User:admin
Password:
(Netgear Switch Routing)    >en
Password:

(Netgear Switch Routing)    #show network

IP Address............................... 192.168.77.151
Subnet Mask.............................. 255.255.255.0
Default Gateway.......................... 192.168.77.127
Burned In MAC Address.................... 00:10:18.82.04:E9
Locally Administered MAC Address......... 00:00:00:00:00:00
MAC Address Type......................... Burned In
Network Configuration Protocol Current... DHCP
Management VLAN ID....................... 1
Web Mode................................. Enable
Java Mode ............................... Disable
```

CLI: show telnet

```
(Netgear Switch Routing)#show telnet

Outbound Telnet Login Timeout (minutes)........ 5
Maximum Number of Outbound Telnet Sessions..... 5
Allow New Outbound Telnet Sessions............. Yes
```

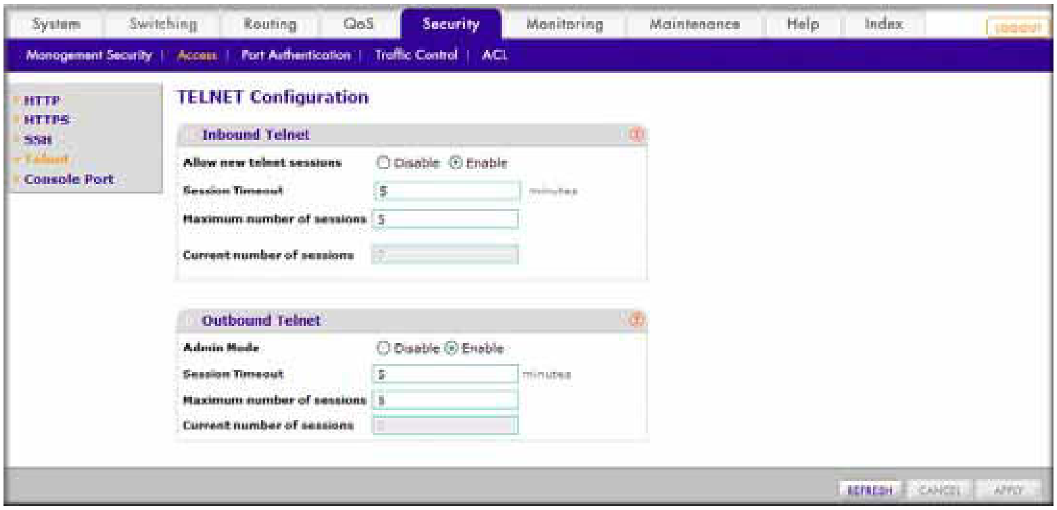
CLI: transport output telnet

```
(Netgear Switch Routing) (Config)#lineconfig ?

<cr>                      Press Enter to execute the command.

(Netgear Switch Routing) (Config)#lineconfig

(Netgear Switch Routing) (Line)#transport ?

input                     Displays the protocols to use to connect to a
                          specific line of the router.
output                    Displays the protocols to use for outgoing
                          connections from a line.

(Netgear Switch Routing) (Line)#transport output ?

telnet                    Allow or disallow new telnet sessions.

(Netgear Switch Routing) (Line)#transport output telnet ?

<cr>                      Press Enter to execute the command.

(Netgear Switch Routing) (Line)#transport output telnet

(Netgear Switch Routing) (Line)#
```

Web Interface: Configure Telnet

1. Select **Security > Access > Telnet**.

   A screen similar to the following displays.



TELNET Configuration

Inbound Telnet

Allow new telnet sessions	○ Disable ● Enable
Session Timeout	5 minutes
Maximum number of sessions	5
Current number of sessions	1

Outbound Telnet

Admin Mode	○ Disable ● Enable
Session Timeout	5 minutes
Maximum number of sessions	5
Current number of sessions	0

2. Under Outbound Telnet, for Admin Mode, select the **Enable** radio button.
3. Click **Apply**.

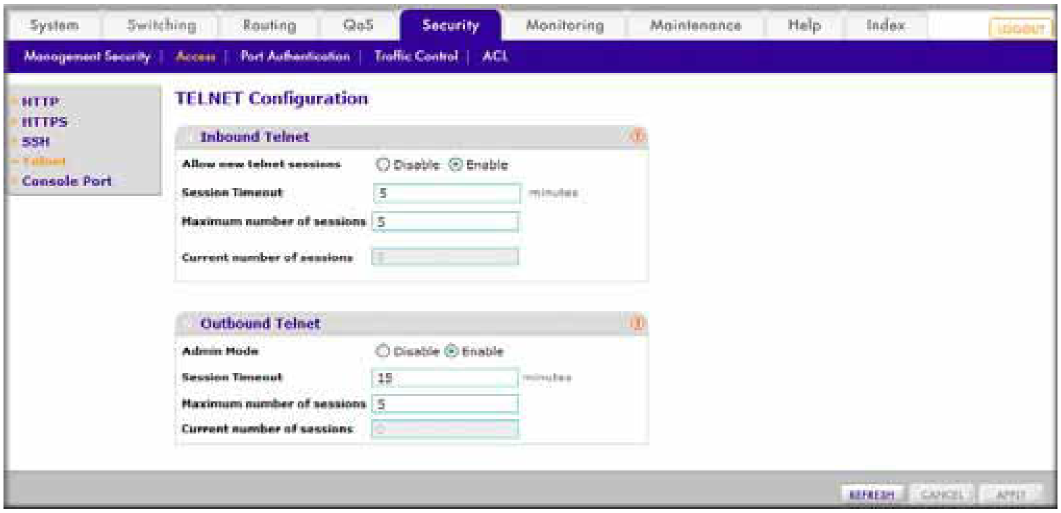
CLI: Configure the session-limit and session-timeout

```
(Netgear Switch Routing) (Line)#session-limit ?
<0-5>                    Configure the maximum number of outbound telnet sessions
allowed.

(Netgear Switch Routing) (Line)#session-limit 5

(Netgear Switch Routing) (Line)#session-timeout ?

<1-160>                  Enter time in minutes.

(Netgear Switch Routing) (Line)#session-timeout 15
```

Web Interface: Configure the Session Timeout

1. Select **Security > Access > Telnet**.

   A screen similar to the following displays.



TELNET Configuration

Inbound Telnet

Allow new telnet sessions ○ Disable ● Enable
Session Timeout 5 minutes
Maximum number of sessions 5
Current number of sessions

Outbound Telnet

Admin Mode ○ Disable ● Enable
Session Timeout 15 minutes
Maximum number of sessions 5
Current number of sessions

2. Enter the following information:
   - In the **Session Timeout** field, enter **15**.
   - In the **Maximum number of sessions** field, enter **5**.
3. Click **Apply**.

15. Syslog

System logging

15

This chapter includes the following sections:

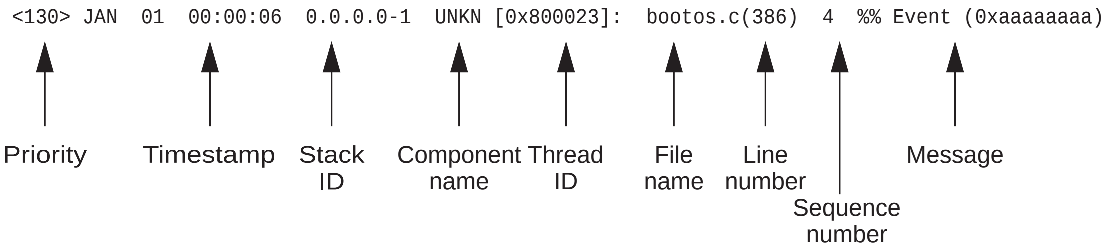
- *Syslog Concepts*
- *Show Logging*
- *Show Logging Buffered*
- *Show Logging Traplogs*
- *Show Logging Hosts*
- *Configure Logging for a Port*
- *Email Alerting*

Syslog Concepts

The syslog feature:

- Allows you to store system messages and errors.
- Can store to local files on the switch or a remote server running a syslog daemon.
- Provides a method of collecting message logs from many systems.

The following illustration explains how to interpret log files.



```
<130> JAN  01  00:00:06  0.0.0.0-1  UNKN [0x800023]:  bootos.c(386)  4  %% Event (0xaaaaaaaa)
```

Figure 28. Log Files

Show Logging

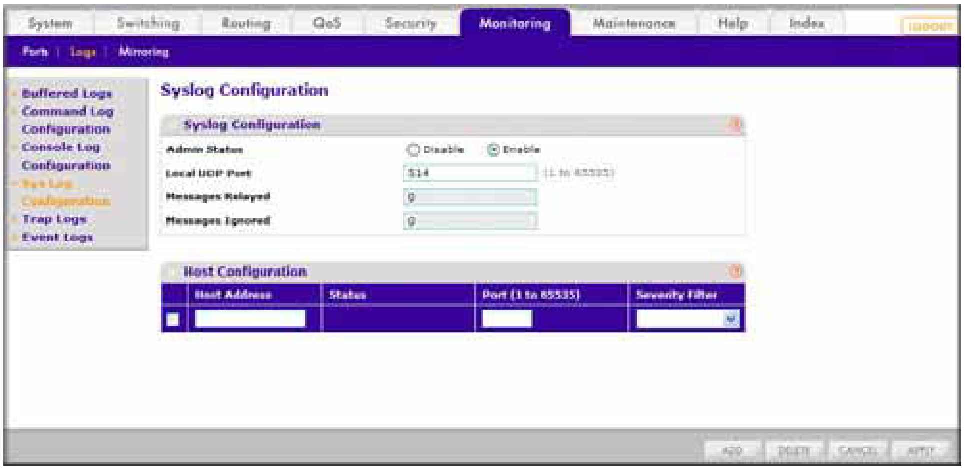
The example is shown as CLI commands and as a Web interface procedure.

CLI: Show Logging

```
(Netgear Switch Routing) #show logging

Logging Client Local Port          :    514
CLI Command Logging                :    disabled
Console Logging                    :    disabled
Console Logging Severity Filter :    alert
Buffered Logging                   :    enabled

Syslog Logging                     :    enabled

Log Messages Received              :    66
Log Messages Dropped               :    0
Log Messages Relayed               :    0
Log Messages Ignored               :    0
```

Web Interface: Show Logging

1. Configure the syslog.
   a. From the main menu, select **Monitoring > Logs > Sys Log Configuration**.



Syslog Configuration

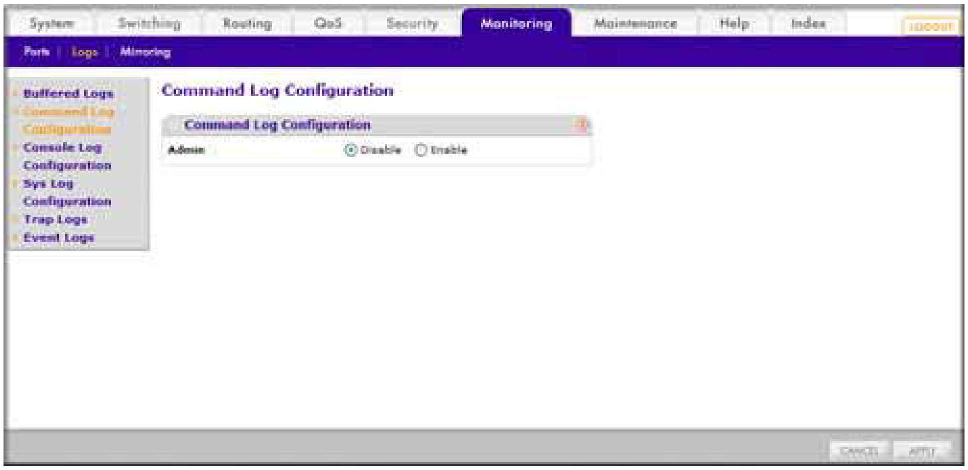
Syslog Configuration

Admin Status	○ Disable ● Enable
Local UDP Port	514 (1 to 65535)
Messages Relayed	0
Messages Ignored	0

Host Configuration

	Host Address	Status	Port (1 to 65535)	Severity Filter
□				

   b. In the Syslog Configuration, next to the Admin Status**,** select the **Enable** radio button.
   c. Click **Apply**.
2. Configure the command log.
   a. Select **Monitoring > Logs > Command Log**.



Command Log Configuration

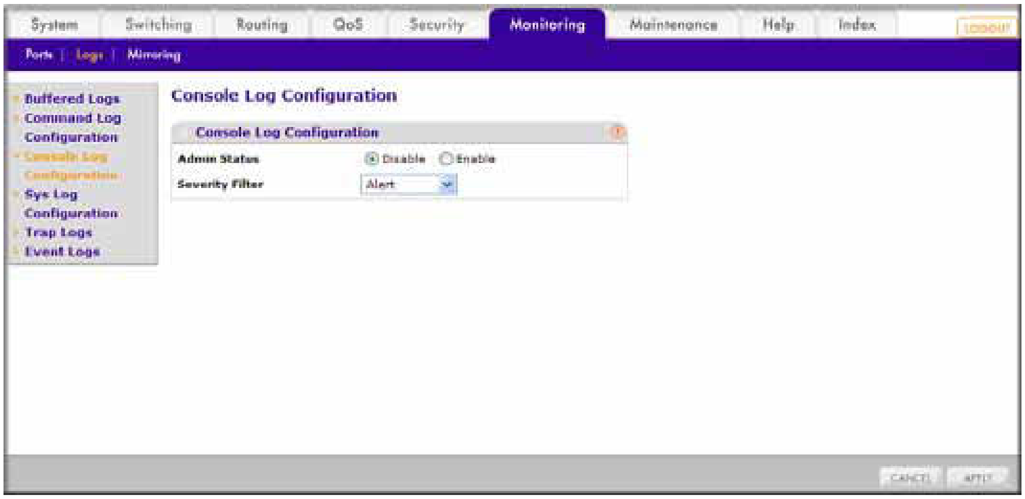
Command Log Configuration

Admin	● Disable ○ Enable

   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**.



Console Log Configuration

Console Log Configuration

Admin Status ● Disable ○ Enable

Severity Filter Alert

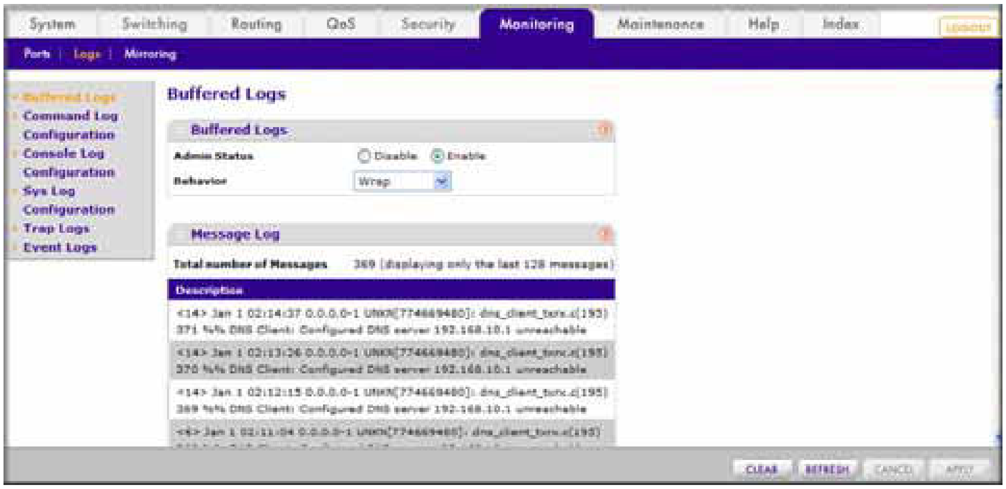
   b. Under Console Log Configuration, for Admin Status**,** select the **Disable** radio button.

   c. Click **Apply**.

4. Configure the buffer logs.

   a. Select **Monitoring > Logs > Buffer Logs**.

      A screen similar to the following displays.



Buffered Logs

Buffered Logs

Admin Status ○ Disable ● Enable

Behavior Wrap

Message Log

Total number of Messages 369 (displaying only the last 128 messages)

Description

```
<14> Jan 1 02:14:37 0.0.0.0-1 UNKN[774669480]: dns_client_txrx.c(195)
371 %% DNS Client: Configured DNS server 192.168.10.1 unreachable
<14> Jan 1 02:13:26 0.0.0.0-1 UNKN[774669480]: dns_client_txrx.c(195)
370 %% DNS Client: Configured DNS server 192.168.10.1 unreachable
<14> Jan 1 02:12:15 0.0.0.0-1 UNKN[774669480]: dns_client_txrx.c(195)
369 %% DNS Client: Configured DNS server 192.168.10.1 unreachable
<6> Jan 1 02:11:04 0.0.0.0-1 UNKN[774669480]: dns_client_txrx.c(195)
```

   b. Under Buffer Logs, for Admin Status**,** select the **Enable** radio button.

   c. Click **Apply**.

Show Logging Buffered

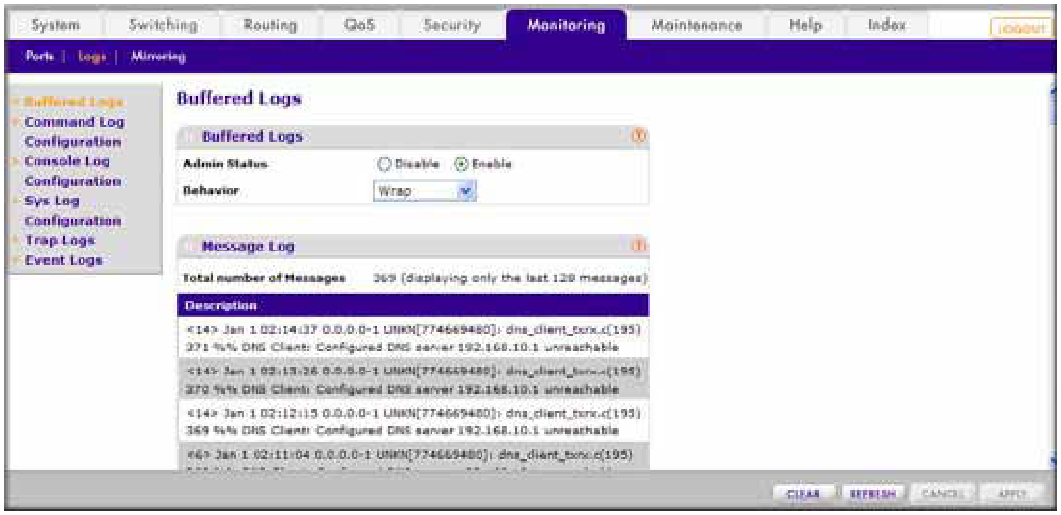
The example is shown as CLI commands and as a Web interface procedure.

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

Buffered Logs

Admin Status	○ Disable ● Enable
Behavior	Wrap

Message Log

Total number of Messages	369 (displaying only the last 128 messages)

Description
<14> Jan 1 02:14:37 0.0.0.0-1 UNKN[774669480]: dns_client_txrx.c(195) 371 %% DNS Client: Configured DNS server 192.168.10.1 unreachable
<14> Jan 1 02:13:26 0.0.0.0-1 UNKN[774669480]: dns_client_txrx.c(195) 370 %% DNS Client: Configured DNS server 192.168.10.1 unreachable
<14> Jan 1 02:12:15 0.0.0.0-1 UNKN[774669480]: dns_client_txrx.c(195) 369 %% DNS Client: Configured DNS server 192.168.10.1 unreachable
<6> Jan 1 02:11:04 0.0.0.0-1 UNKN[774669480]: dns_client_txrx.c(195)

Show Logging Traplogs

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

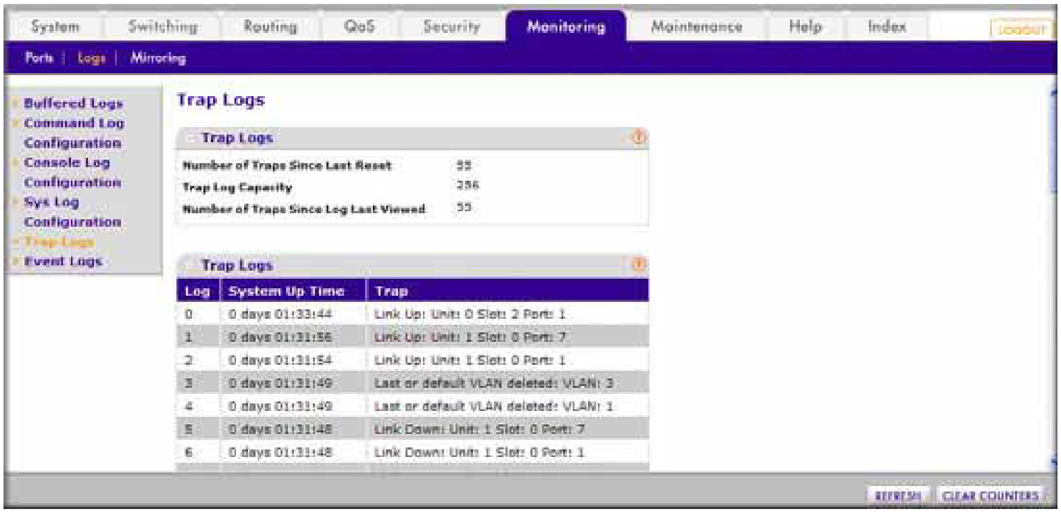
CLI: Show Logging Traplogs

```
(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

Trap Logs

Number of Traps Since Last Reset	55
Trap Log Capacity	256
Number of Traps Since Log Last Viewed	55

Trap Logs

Log	System Up Time	Trap
0	0 days 01:33:44	Link Up: Unit: 0 Slot: 2 Port: 1
1	0 days 01:31:56	Link Up: Unit: 1 Slot: 0 Port: 7
2	0 days 01:31:54	Link Up: Unit: 1 Slot: 0 Port: 1
3	0 days 01:31:49	Last or default VLAN deleted: VLAN: 3
4	0 days 01:31:49	Last or default VLAN deleted: VLAN: 1
5	0 days 01:31:48	Link Down: Unit: 1 Slot: 0 Port: 7
6	0 days 01:31:48	Link Down: Unit: 1 Slot: 0 Port: 1

Show Logging Hosts

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

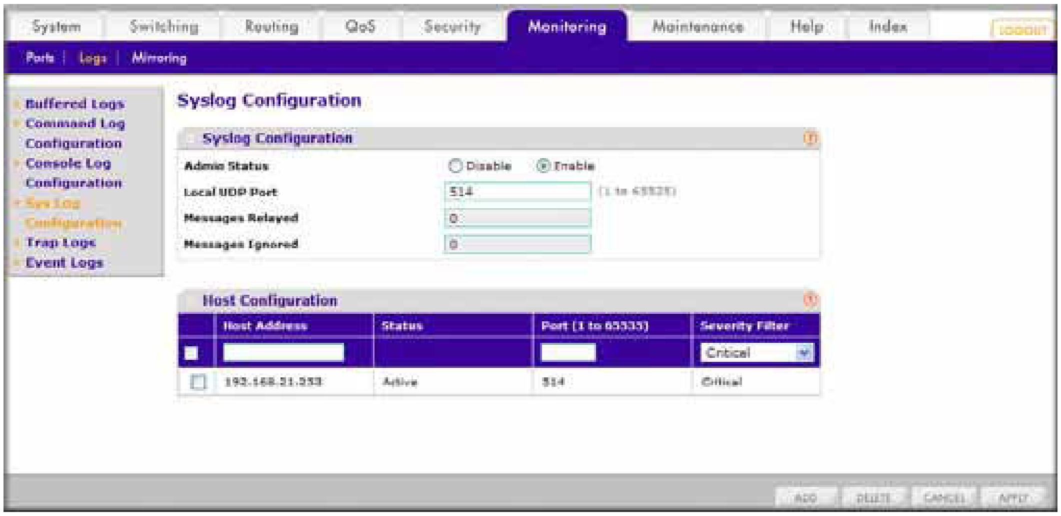
CLI: Show Logging Hosts

```
(Netgear Switch Routing) #show logging hosts ?

<cr>                      Press Enter to execute the command.

(Netgear Switch Routing) #show logging hosts

Index     IP Address       Severity   Port     Status
-----  ----------------- ----------  ----  -------------
1      192.168.21.253     critical    514   Active
```

Web Interface: Show Logging Hosts

Select **Monitoring > Logs > Sys Log Configuration**.

A screen similar to the following displays.



Syslog Configuration

Syslog Configuration

Admin Status	○ Disable ● Enable
Local UDP Port	514 (1 to 65535)
Messages Relayed	0
Messages Ignored	0

Host Configuration

	Host Address	Status	Port (1 to 65535)	Severity Filter
□				Critical
□	192.168.21.253	Active	514	Critical

Configure Logging for a Port

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

CLI: Configure Logging for the Port

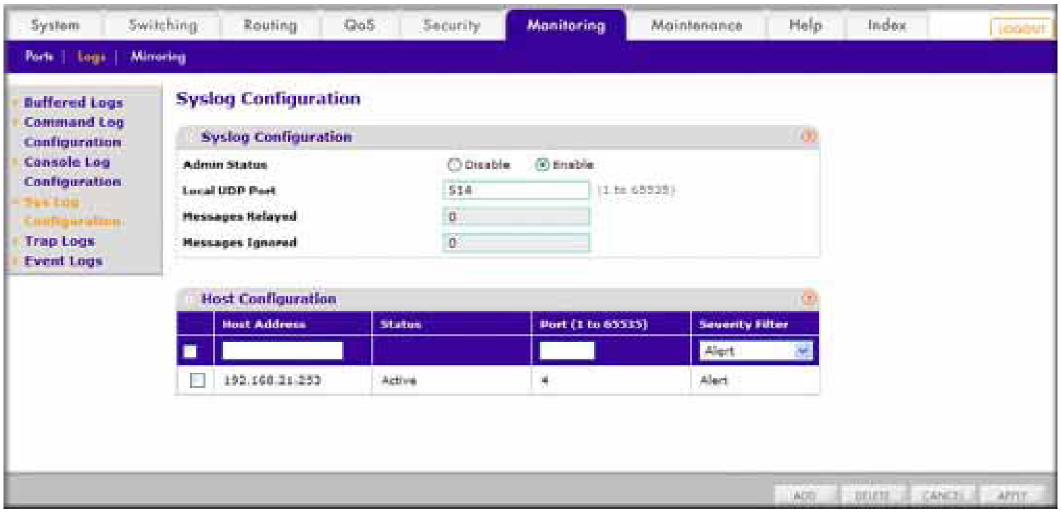
```
(Netgear Switch Routing)     #config

(Netgear Switch Routing) (Config)#logging ?

buffered           Buffered (In-Memory) Logging Configuration.
cli-command        CLI Command Logging Configuration.
console            Console Logging Configuration.
host               Enter IP Address for Logging Host
syslog             Syslog Configuration.

(Netgear Switch Routing) (Config)#logging host ?
<hostaddress>        Enter Logging Host IP Address
reconfigure          Logging Host Reconfiguration
remove                Logging Host Removal
(Netgear Switch Routing) (Config)#logging host 192.168.21.253 ?

<cr>              Press Enter to execute the command.
<port>            Enter Port Id
```

```
(Netgear Switch Routing) (Config)#logging host 192.168.21.253 4 ?

<cr>              Press Enter to execute the command.
<severitylevel>   Enter Logging Severity Level (emergency|0, alert|1, critical|2,
error|3, warning|4, notice|5, info|6, debug|7).

(Netgear Switch Routing) (Config)#logging host 192.168.21.253 4 1 ?

<cr>              Press Enter to execute the command.

(Netgear Switch Routing) (Config)#logging host 192.168.21.253 4 1

(Netgear Switch Routing) #show logging hosts

Index     IP Address       Severity   Port     Status
-----  -----------------  ----------  ----   -------------
1      192.168.21.253     alert       4     Active
```

Web Interface: Configure Logging for the Port

1. Select **Monitoring > Logs > Sys Log Configuration**.

   A screen similar to the following displays.



Syslog Configuration

Syslog Configuration

Admin Status	○ Disable ● Enable
Local UDP Port	514 (1 to 65535)
Messages Relayed	0
Messages Ignored	0

Host Configuration

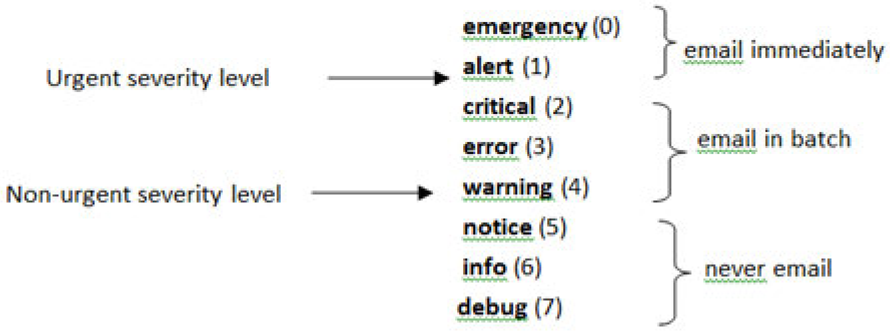
	Host Address	Status	Port (1 to 65535)	Severity Filter
□				Alert
□	192.168.21.253	Active	4	Alert

2. Enter the following information:
   - In the **Host Address** field, enter your host address **192.168.21.253**.
   - In the **Port** field, enter **4**.
   - In the **Severity Filter** list, select **Alert**.
3. Click **Add**.

Email Alerting

Email Alerting is an extension of the logging system. The logging system allows you to configure a set of destinations for log messages. This feature adds the email configuration, through which the log message 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.



FOR POSITION ONLY (FPO)

Figure 29. Log message severity levels

The network administrator can adjust the urgent and non-urgent severity levels. These levels are global and apply to all destination email addresses. Log messages in the urgent group are sent immediately to the SMTP server with each log message in a separate mail. Log messages in the non-urgent group are batched into a single email message and after a configurable delay.

Email alerting also provides a configuration option that allows the network administrator to specify the severity level at which SNMP traps are logged. Using this option, the administrator can put traps in the urgent group, the non-urgent group, or the never group for emailing. Traps are not emailed by default. For traps to be emailed, the network administrator has to either increase the severity at which traps are logged, or lower the severity level of log messages that are emailed.

The network administrator can configure multiple destination email addresses, and for each email address, specify whether to deliver urgent log messages, non-urgent log messages, or both.

There is an exception to the sending of the messages periodically to the SMTP server. When the log buffer is completely full before the expiry of the periodic timer sending of the log messages to the SMTP server does not until the expiry of the timer. When the log buffer is full, a connection is opened immediately with the SMTP server, and all the messages that have not previously been emailed are sent to it.

CLI: Send Log Messages to admin@switch.com Using Account aaaa@netgear.com

1. Configure an SMTP server, for example, smtp.netgear.com. Before you configure the SMTP server, you need to have an account on SMTP server.

```
(Netgear Switch) (Config)#mail-server "smtp.netgear.com" port 465
(Netgear Switch) (Mail-Server)#security tlsv1
(Netgear Switch) (Mail-Server)# username  aaaa
(Netgear Switch) (Mail-Server)# password  xxxxxx
(Netgear Switch) (Mail-Server)#exit
```

2. Configure logging mail. From-addr is the source address of email and to-addr is the destination address of email.

```
(Netgear Switch) (Config)#logging email
(Netgear Switch) (Config)#logging email from-addr aaaa@netgear.com
(Netgear Switch) (Config)#logging email message-type urgent to-addr
admin@switch.com
(Netgear Switch) (Config)#logging email message-type non-urgent to-addr
admin@switch.com
```

3. Increase the severity of traps to 3 (error). By default, it is 6 (informational).

```
(Netgear Switch) (Config)#logging traps 3
```

16. SNMP

Simple Network Management Protocol

16

This chapter includes the following sections:

- *Add a New Community*
- *Enable SNMP Trap*
- *SNMPv3*
- *sFlow*
- *Time-Based Sampling of Counters with sFlow*

Add a New Community

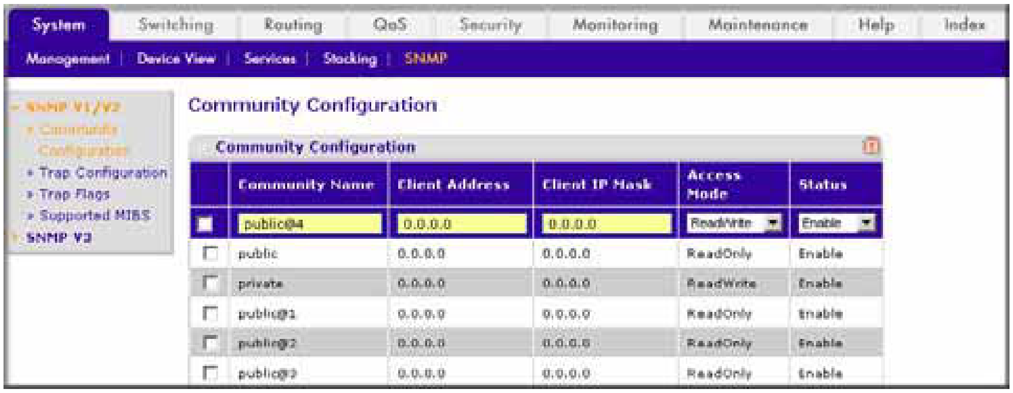
The example is shown as CLI commands and as a Web interface procedure.

CLI: Add a New Community

```
(Netgear switch) #config
(Netgear switch) (Config)#snmp-server community rw public@4
```

Web Interface: Add a New Community

1. Select **System > SNMP > SNMP V1/V2 > Community Configuration**. A screen similar to the following displays.



Community Configuration

Community Configuration

	Community Name	Client Address	Client IP Mask	Access Mode	Status
□	public@4	0.0.0.0	0.0.0.0	ReadWrite	Enable
□	public	0.0.0.0	0.0.0.0	ReadOnly	Enable
□	private	0.0.0.0	0.0.0.0	ReadWrite	Enable
□	public@1	0.0.0.0	0.0.0.0	ReadOnly	Enable
□	public@2	0.0.0.0	0.0.0.0	ReadOnly	Enable
□	public@3	0.0.0.0	0.0.0.0	ReadOnly	Enable

2. In the **Community Name** field, enter **public@4**.
3. In the **Client Address** field, enter **0.0.0.0**.
4. In the **Client IP Mask** field, enter **0.0.0.0**.
5. In the **Access Mode** field, select **Read/Write**.
6. In the **Status** field, select **Enable**.
7. Click **Add**.

Enable SNMP Trap

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

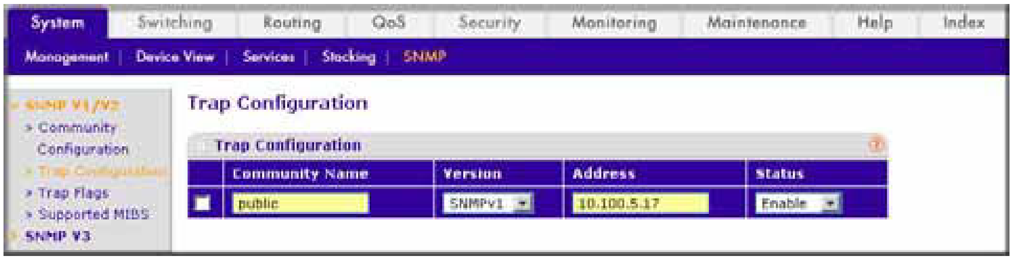
CLI: Enable SNMP Trap

This example shows how to send SNMP trap to the SNMP server.

```
(Netgear switch) #config
(Netgear switch) (Config)# snmptrap public 10.100.5.17
                                   Enable send trap to SNMP server 10.100.5.17
(Netgear switch) (Config)#snmp-server traps linkmode
                                   Enable send link status to the SNMP server
when link status changes.
```

Web Interface: Enable SNMP Trap

1. Enable SNMP trap for the server 10.100.5.17.
    a. Select **System > SNMP > SNMP V1/V2 > Trap Configuration**. A screen similar to the following displays.



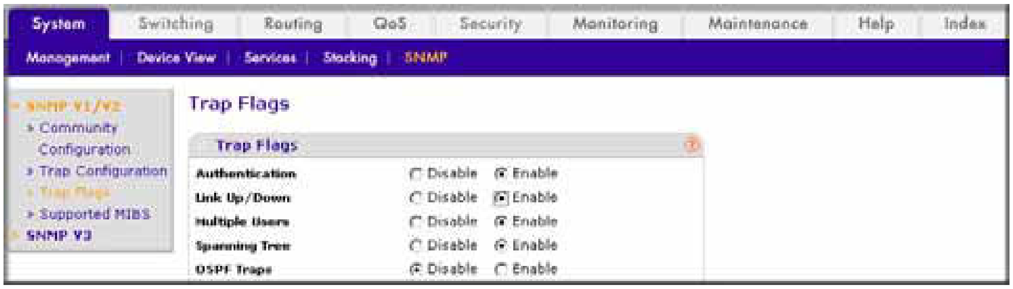
Trap Configuration

Trap Configuration

	Community Name	Version	Address	Status
□	public	SNMPv1	10.100.5.17	Enable

    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.



Trap Flags

Trap Flags

Authentication	○ Disable	● Enable
Link Up/Down	○ Disable	● Enable
Multiple Users	○ Disable	● Enable
Spanning Tree	○ Disable	● Enable
OSPF Traps	● Disable	○ Enable

b. For Link Up/Down, select the **Enable** radio button.

c. Click **Apply**.

SNMPv3

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

CLI: Configure SNMPv3

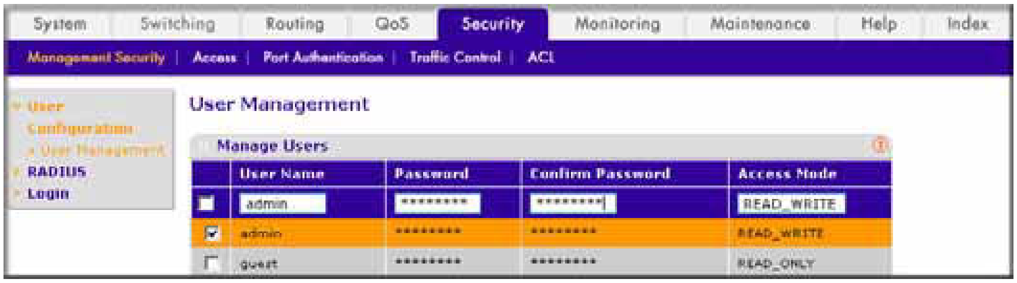
```
(Netgear Switch) #config
(Netgear Switch) (Config)#users passwd admin
Enter old password:
Enter new password:12345678
Confirm new password:12345678
Password Changed!
change the password to “12345678”
(Netgear Switch) (Config)#users snmpv3 authentication admin md5
Set the authentication mode to md5
(Netgear Switch) (Config)#users snmpv3 encryption admin des 12345678
Set the encryption mode to des and the key is “12345678”
```

Web Interface: Configure SNMPv3

1. Change the user password.

   If you set the authentication mode to MD5, you must make the length of password longer than 8 characters.

a. Select **Security > Management Security > User Configuration > User Management**. A screen similar to the following displays.



User Management

Manage Users

	User Name	Password	Confirm Password	Access Mode
□	admin	********	********	READ_WRITE
☑	admin	********	********	READ_WRITE
□	guest	********	********	READ_ONLY

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.

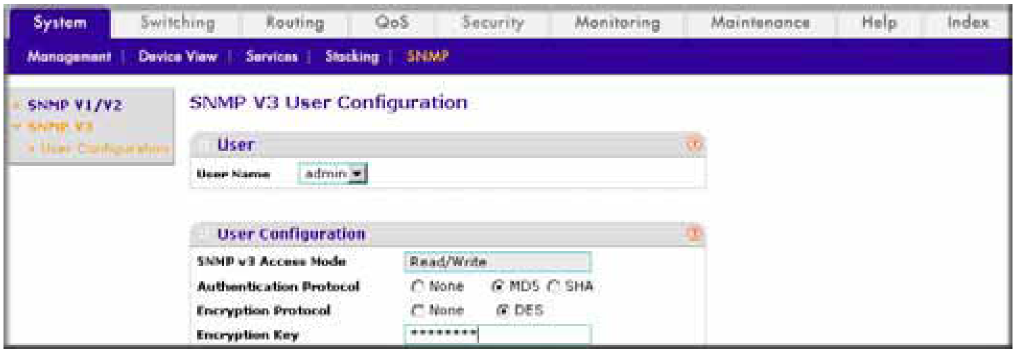
c. In the **Password** field, enter **12345678**.

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.



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.

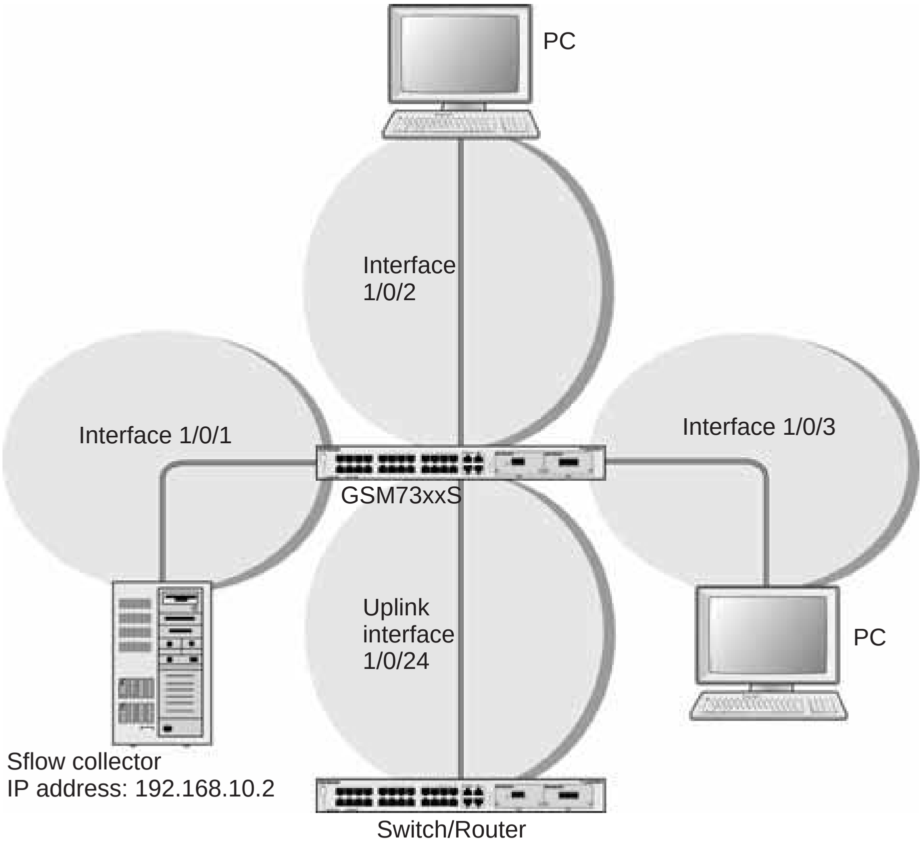


Figure 30. sFlow

CLI: Configure Statistical Packet-Based Sampling of Packet Flows with sFlow

1. Configure the sFlow receiver (sFlow collector) IP address. In this example, sFlow samples will be sent to the destination address 192.168.10.2.

```
(Netgear Switch) (Config)# sflow receiver 1 ip 192.168.10.2
```

2. Configure the sFlow receiver timeout. Here sFlow samples will be sent to this receiver for the duration of 31536000 seconds. That is approximately 1 year.

```
(Netgear Switch) (Config)# sflow receiver 1 owner NetMonitor timeout 31536000
```

3. Here the default maximum datagram size is 1400. It can be modified to a value between 200 and 9116 using the command `sflow receiver 1 maxdatagram <size>`.

```
(GSM7328S) #show sflow receivers

Receiver Owner    Time out   Max Datagram Port  IP Address
Index    String              Size
-------- -------- ---------- ------------ ----- ------------------------------
       1        NetMonit 31535988   1400        6343  192.168.10.2
        2                0          1400        6343  0.0.0.0
        3                0          1400        6343  0.0.0.0
        4                0          1400        6343  0.0.0.0
        5                0          1400        6343  0.0.0.0
        6                0          1400        6343  0.0.0.0
        7                0          1400        6343  0.0.0.0
        8                0          1400        6343  0.0.0.0

(GSM7328S) #
```

4. Configure the sampling port sFlow receiver index, sampling rate, and sampling maximum header size. You need to repeat these for all the ports to be sampled.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# sflow sampler 1
(Netgear Switch) (Interface 1/0/1)# sflow sampler rate 1024
(Netgear Switch) (Interface 1/0/1)# sflow sampler maxheadersize 64
```

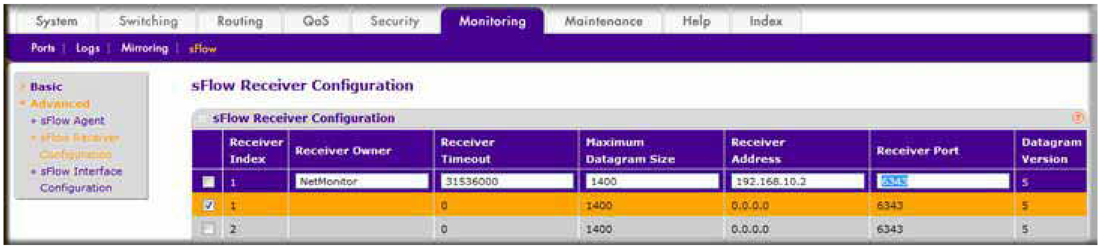
5. View the sampling port configurations.

```
(GSM7328S) #show sflow samplers
Sampler            Receiver                Packet         Max Header
Data Source        Index                 Sampling Rate       Size
-----------       ---------------     -----------------  ------------------
1/0/1                     1              1024                 64
```

Web Interface: Configure Statistical Packet-based Sampling with sFlow

1. Configure the sFlow receiver IP address.
   a. Select **Monitoring > sFlow > Advanced > sFlow Receiver Configuration**.
   b. Select the **1** check box.
   c. In the **Receiver Owner** field, enter **NetMonitor**.
   d. In the **Receiver Timeout** field, enter **31536000**.

e. In the **Receiver Address** field, enter **192.168.10.2**. A screen similar to the following displays.

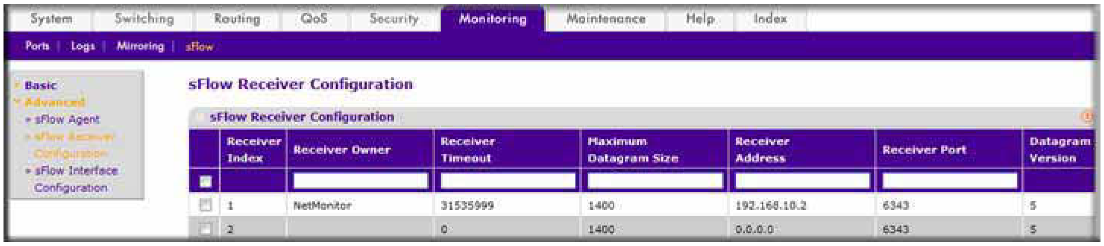

System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Ports | Logs | Mirroring | sFlow
Basic
Advanced
sFlow Agent
sFlow Receiver Configuration
sFlow Interface Configuration

sFlow Receiver Configuration

sFlow Receiver Configuration

	Receiver Index	Receiver Owner	Receiver Timeout	Maximum Datagram Size	Receiver Address	Receiver Port	Datagram Version
□	1	NetMonitor	31536000	1400	192.168.10.2	6343	5
☑	1		0	1400	0.0.0.0	6343	5
□	2		0	1400	0.0.0.0	6343	5

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


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Ports | Logs | Mirroring | sFlow
Basic
Advanced
sFlow Agent
sFlow Receiver Configuration
sFlow Interface Configuration

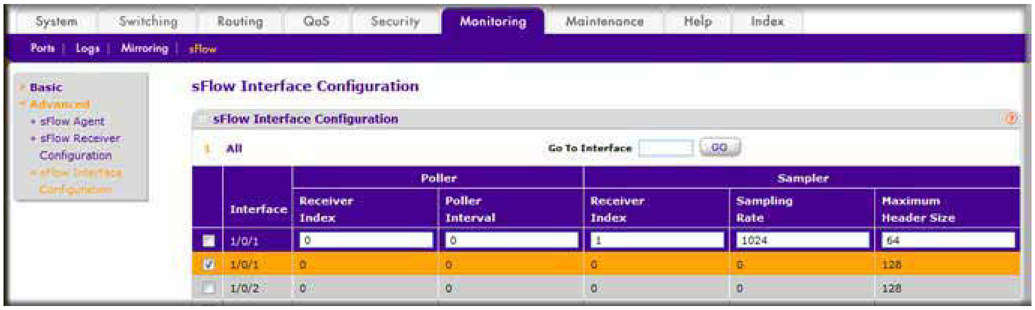
sFlow Receiver Configuration

sFlow Receiver Configuration

	Receiver Index	Receiver Owner	Receiver Timeout	Maximum Datagram Size	Receiver Address	Receiver Port	Datagram Version
□							
□	1	NetMonitor	31535999	1400	192.168.10.2	6343	5
□	2		0	1400	0.0.0.0	6343	5

2. Configure the sampling ports sFlow receiver index, sampling rate, and sampling maximum header size.

a. Select **Monitoring > sFlow > Advanced > sFlow Interface Configuration**. A screen similar to the following displays.



sFlow Interface Configuration

sFlow Interface Configuration

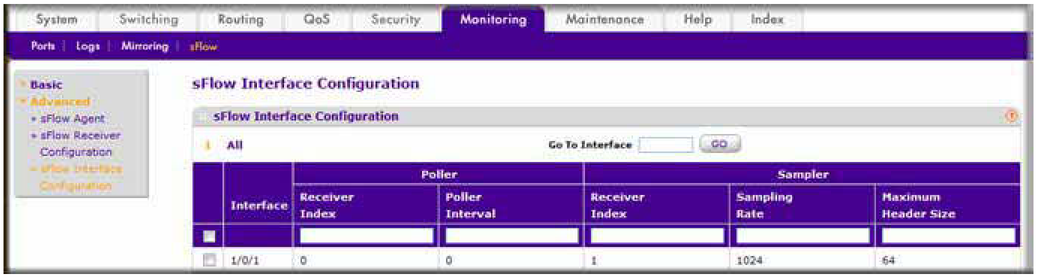
		Poller		Sampler		
	Interface	Receiver Index	Poller Interval	Receiver Index	Sampling Rate	Maximum Header Size
□	1/0/1	0	0	1	1024	64
☑	1/0/1	0	0	0	0	128
□	1/0/2	0	0	0	0	128

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

c. In the **Sampling Rate** field, enter **1024**.

d. In the **Maximum Header Size** field, enter 64.

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



sFlow Interface Configuration

sFlow Interface Configuration

		Poller		Sampler		
	Interface	Receiver Index	Poller Interval	Receiver Index	Sampling Rate	Maximum Header Size
□						
□	1/0/1	0	0	1	1024	64

Time-Based Sampling of Counters with sFlow

CLI: Configure Time-Based Sampling of Counters with sFlow

1. Configure the sampling port sFlow receiver index, and polling interval. You need to repeat this for all the ports to be polled.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# sflow poller 1
(Netgear Switch) (Interface 1/0/1)# sflow poller interval  300
```

2. View the polling port configurations.

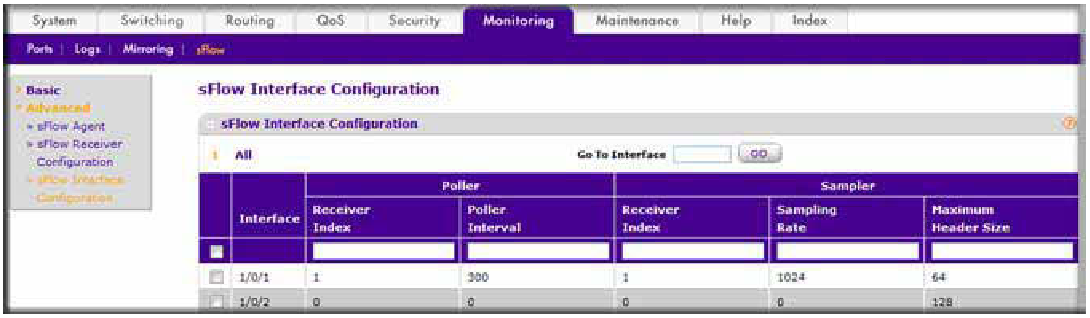
```
(GSM7328S) #show sflow pollers
Poller                  Receiver          Poller
Data Source       Index               Interval
-----------              ---------            ---------
1/0/1                       1                   300
```

Web Interface: Configure Time-Based Sampling of Counters with sFlow

Configure the sampling ports sFlow receiver index, and polling interval:

3. Select **Monitoring > sFlow > Advanced > sFlow Interface Configuratio**n.
4. Select the Interface **1/0/1** check box.
5. In the **Poller Interval** field, enter **300**.

A screen similar to the following displays.



sFlow Interface Configuration

sFlow Interface Configuration

		Poller		Sampler		
	Interface	Receiver Index	Poller Interval	Receiver Index	Sampling Rate	Maximum Header Size
☐						
☐	1/0/1	1	300	1	1024	64
☐	1/0/2	0	0	0	0	128

6. Click **Apply**.

17. DNS

17

Domain Name System

This chapter includes the following sections:

- *DNS Concepts*
- *Specify Two DNS Servers*
- *Manually Add a Host Name and an IP Address*

DNS Concepts

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.

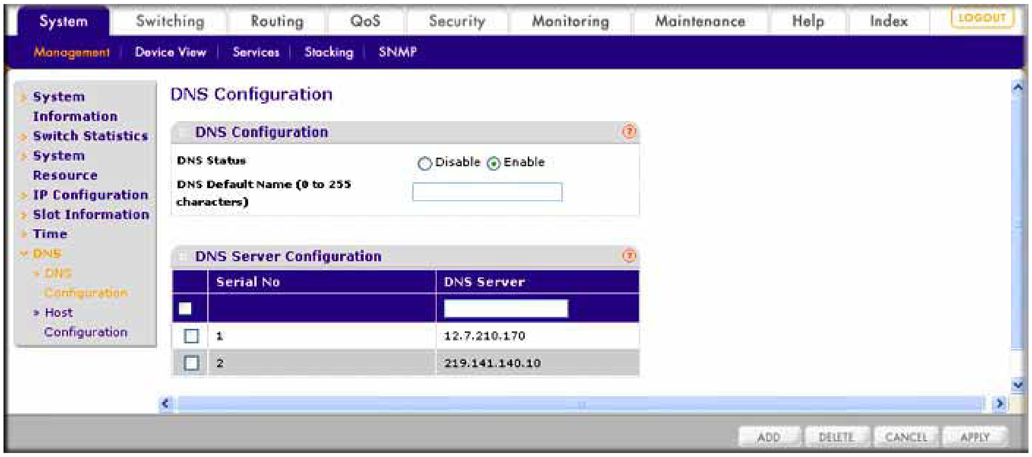
CLI: Specify Two DNS Servers

```
(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.



DNS Configuration

DNS Configuration

DNS Status ○ Disable ● Enable

DNS Default Name (0 to 255 characters)

DNS Server Configuration

	Serial No	DNS Server
□		
□	1	12.7.210.170
□	2	219.141.140.10

2. Under DNS Server Configuration, in the **DNS Server** field, enter **12.7.210.170**.
3. Click **Add**.
4. In the **DNS Server** field, enter **219.141.140.10**.
5. Click **Add**.

Both DNS servers now show in the DNS Server Configuration table.

Manually Add a Host Name and an IP Address

The following example shows commands to add a static host name entry to the switch so that you can use this entry to resolve the IP address. The example is shown as CLI commands and as a Web interface procedure.

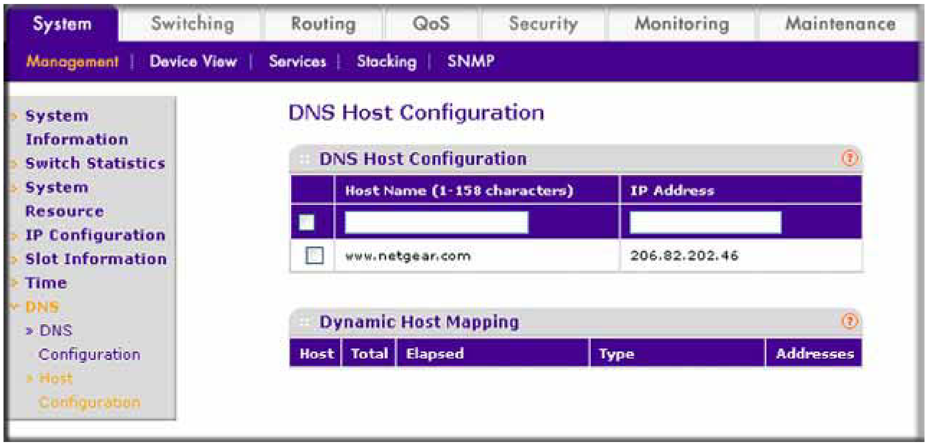
CLI: Manually Add a Host Name and an IP Address

```
(Netgear Switch)#config
(Netgear Switch) (Config)#ip host www.netgear.com 206.82.202.46
(Netgear Switch) (Config)#ip domain-lookup
(Netgear Switch) (Config)#ping www.netgear.com

Send count=3, Receive count=3 from 206.82.202.46
```

Web Interface: Manually Add a Host Name and an IP Address

1. Select **System > Management > DNS > Host Configuration**.

   A screen similar to the following displays.



DNS Host Configuration

DNS Host Configuration

	Host Name (1-158 characters)	IP Address
□		
□	www.netgear.com	206.82.202.46

Dynamic Host Mapping

Host	Total	Elapsed	Type	Addresses

2. Under DNS Host Configuration, enter the following information:
   - In the **Host Name** field, enter **www.netgear.com**.
   - In the **IP Address** field, enter **206.82.202.46**.
3. Click **Add**.

The host name and IP address now show in the DNS Host Configuration table.

18. DHCP Server

18

Dynamic Host Configuration Protocol Server

This chapter includes the following sections:

DHCP Server Concepts

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
```

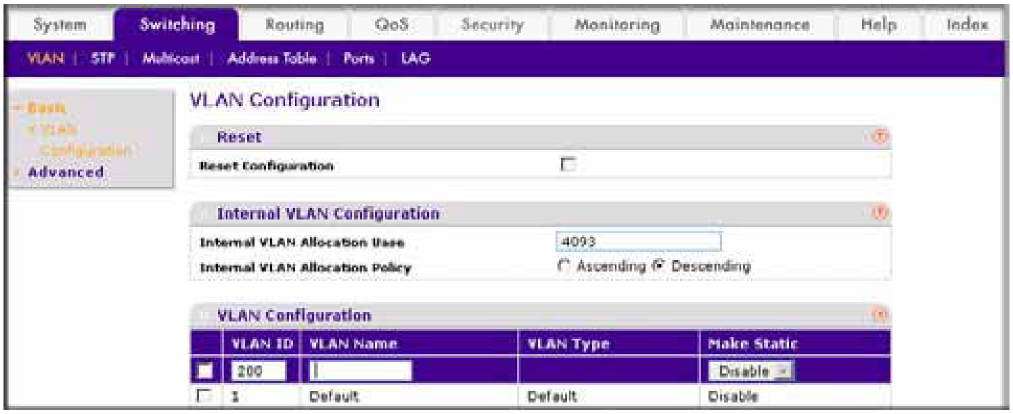
Note: If there is no DHCP L3 relay between client PC and DHCP server, there must be an active route whose subnet is the same as the DHCP dynamic pool's subnet.

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

Reset

Reset Configuration □

Internal VLAN Configuration

Internal VLAN Allocation Base: 4093

Internal VLAN Allocation Policy: ○ Ascending ● Descending

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type	Make Static
□	200			Disable
□	1	Default	Default	Disable

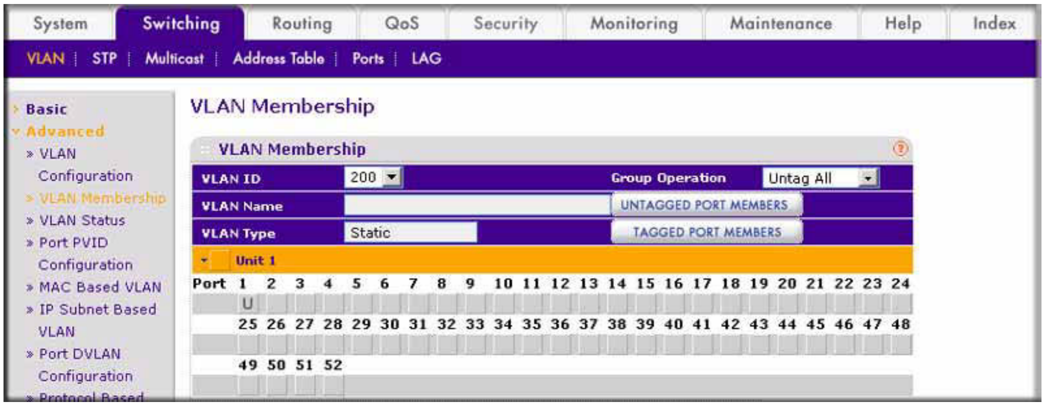
   b. Under VLAN Configuration, in the **VLAN ID** field, enter **200**.

   c. Click **Add**.

2. Add port 1/0/1 to VLAN 200.

   a. Select **Switching > VLAN >Advanced > VLAN Membership**.

   A screen similar to the following displays.



VLAN Membership

VLAN Membership

VLAN ID: 200

Group Operation: Untag All

VLAN Name:

VLAN Type: Static

Unit 1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	U																							
	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
	49	50	51	52																				

   b. In the **VLAN ID** field, select **200**.

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

   d. Click the gray boxes under ports **1** and **24** until **U** displays.

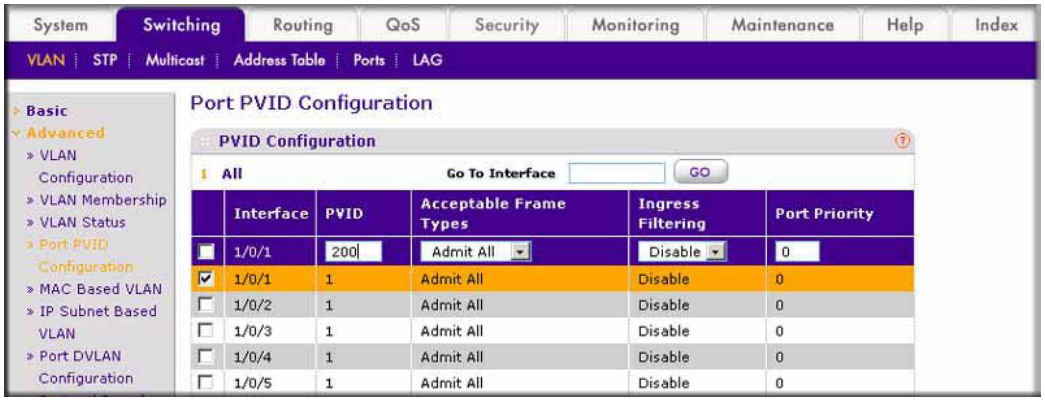
   The U specifies that the egress packet is untagged for the port.

   e. Click **Apply**.

3. Assign PVID to the VLAN 200.

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

A screen similar to the following displays.



Port PVID Configuration

PVID Configuration

1 All Go To Interface

	Interface	PVID	Acceptable Frame Types	Ingress Filtering	Port Priority
□	1/0/1	200	Admit All	Disable	0
☑	1/0/1	1	Admit All	Disable	0
□	1/0/2	1	Admit All	Disable	0
□	1/0/3	1	Admit All	Disable	0
□	1/0/4	1	Admit All	Disable	0
□	1/0/5	1	Admit All	Disable	0

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

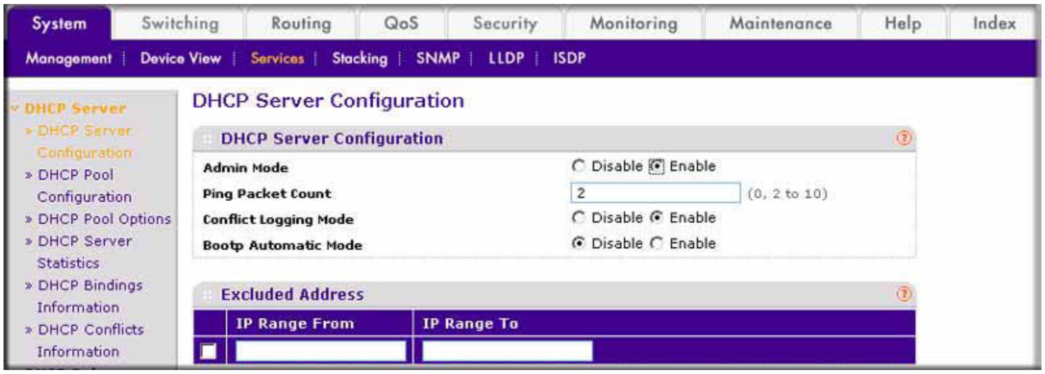
c. In the **PVID (1 to 4093)** field, enter **200**.

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

4. Create a new DHCP pool.

a. Select **System > Services > DHCP Server > DHCP Server Configuration**.

A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Management | Device View | Services | Stacking | SNMP | LLDP | ISDP
DHCP Server
» DHCP Server Configuration
» DHCP Pool Configuration
» DHCP Pool Options
» DHCP Server Statistics
» DHCP Bindings Information
» DHCP Conflicts Information

DHCP Server Configuration

DHCP Server Configuration

Admin Mode	○ Disable ● Enable
Ping Packet Count	2 (0, 2 to 10)
Conflict Logging Mode	○ Disable ● Enable
Bootp Automatic Mode	● Disable ○ Enable

Excluded Address

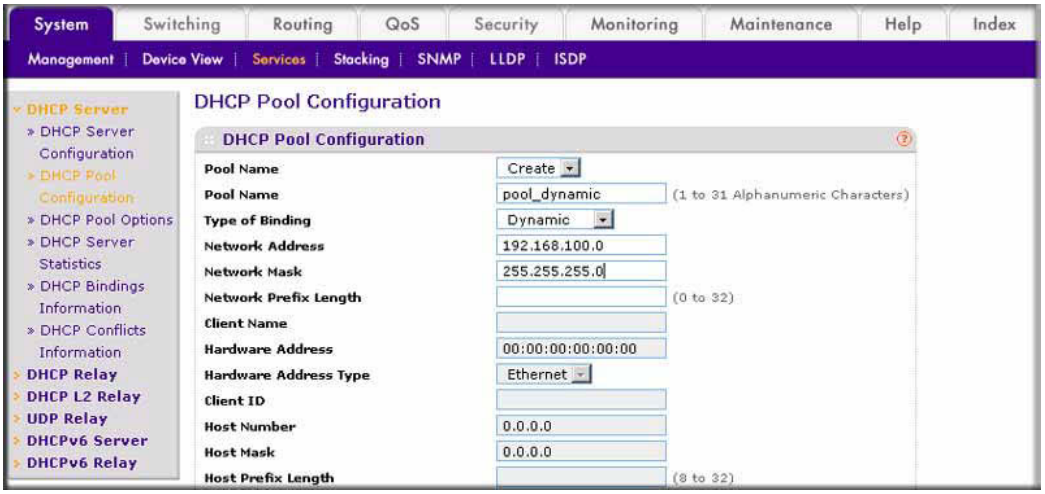
	IP Range From	IP Range To
□		

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.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Management | Device View | Services | Stacking | SNMP | LLDP | ISDP
DHCP Server
» DHCP Server Configuration
» DHCP Pool Configuration
» DHCP Pool Options
» DHCP Server Statistics
» DHCP Bindings Information
» DHCP Conflicts Information
DHCP Relay
DHCP L2 Relay
UDP Relay
DHCPv6 Server
DHCPv6 Relay

DHCP Pool Configuration

DHCP Pool Configuration

Pool Name	Create	
Pool Name	pool_dynamic	(1 to 31 Alphanumeric Characters)
Type of Binding	Dynamic	
Network Address	192.168.100.0	
Network Mask	255.255.255.0	
Network Prefix Length		(0 to 32)
Client Name		
Hardware Address	00:00:00:00:00:00	
Hardware Address Type	Ethernet	
Client ID		
Host Number	0.0.0.0	
Host Mask	0.0.0.0	
Host Prefix Length		(8 to 32)

e. Under DHCP Pool Configuration, enter the following information:

- In the **Pool Name** list, select **Create**.
- In the **Pool Name** field, enter **pool_dynamic**.
- In the **Type of Binding** list, select **Dynamic**.
- In the **Network Number** field, enter **192.168.100.0**.
- In the **Network Mask** field, enter **255.255.255.0**. As an alternate, you can enter **24** in the **Network Prefix Length** field. Do not fill in both the Network Mask field and Network Prefix Length fields.
- In the **Days** field, enter **1**.

f. Click **Add**.

The pool_dynamic name is now added to the Pool Name drop-down list.

Configure a DHCP Server that Assigns a Fixed IP Address

The following example shows how to set up a DHCP server with an IP address pool and let the DHCP server assign a fixed IP address based on a MAC address. The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure a DHCP Server that a Assigns Fixed IP Address

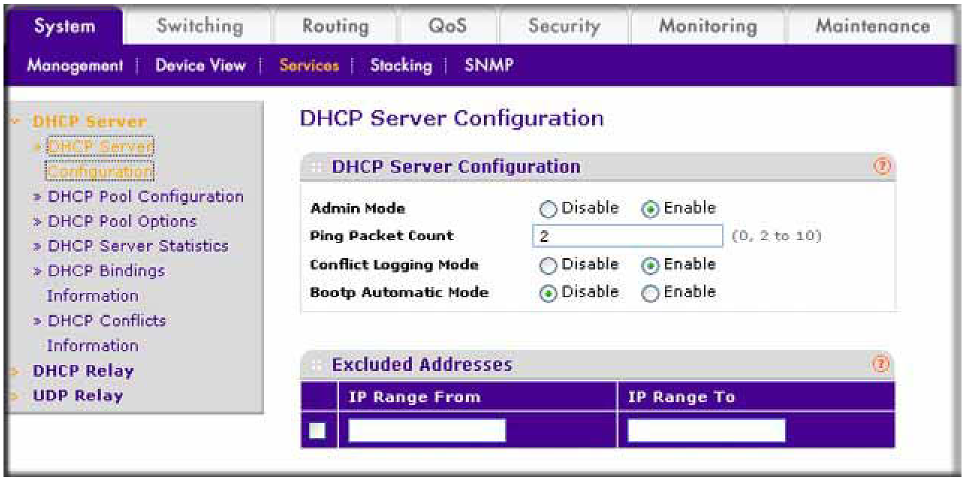
```
(Netgear Switch)#config
(Netgear Switch) (Config)#service dhcp
(Netgear Switch) (Config)#ip dhcp pool pool_manual
(Netgear Switch) (Config)#client-name dhcpclient
(Netgear Switch) (Config)#hardware-address 00:01:02:03:04:05
(Netgear Switch) (Config)#host 192.168.200.1 255.255.255.0
(Netgear Switch) (Config)#client-identifier 01:00:01:02:03:04:05
```

Note: The unique identifier is a concatenation of the media type and MAC addresses. For example, the Microsoft client identifier for Ethernet address c8:19:24:88:f1:77 is 01:c8:19:24:88:f1:77, where 01 represents the Ethernet media type. For more information, see the “Address Resolution Protocol Parameters” section of RFC 1700.

Web Interface: Configure a DHCP Server that Assigns a Fixed IP Address

1. Select **System > Services > DHCP Server > DHCP Server Configuration**.

   A screen similar to the following displays.



DHCP Server Configuration

DHCP Server Configuration

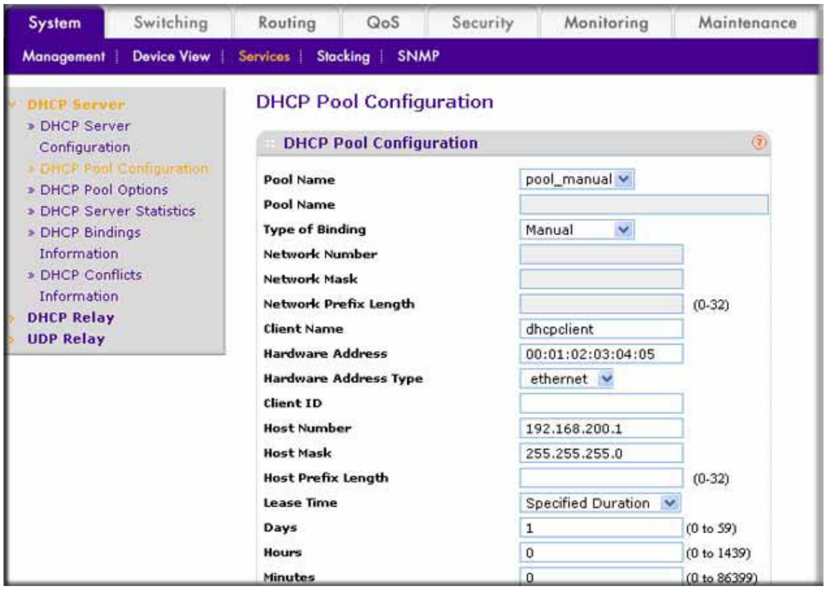
Admin Mode	○ Disable ● Enable
Ping Packet Count	2 (0, 2 to 10)
Conflict Logging Mode	○ Disable ● Enable
Bootp Automatic Mode	● Disable ○ Enable

Excluded Addresses

	IP Range From	IP Range To
□		

2. For Admin Mode, select the **Enable** radio button.
3. Click **Apply** to enable the DHCP service.
4. Select **System > Services > DHCP Server > DHCP Pool Configuration**.

A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Management | Device View | Services | Stacking | SNMP
DHCP Server
» DHCP Server Configuration
» DHCP Pool Configuration
» DHCP Pool Options
» DHCP Server Statistics
» DHCP Bindings Information
» DHCP Conflicts Information
DHCP Relay
UDP Relay

DHCP Pool Configuration

DHCP Pool Configuration

Pool Name	pool_manual	
Pool Name		
Type of Binding	Manual	
Network Number		
Network Mask		
Network Prefix Length		(0-32)
Client Name	dhcpclient	
Hardware Address	00:01:02:03:04:05	
Hardware Address Type	ethernet	
Client ID		
Host Number	192.168.200.1	
Host Mask	255.255.255.0	
Host Prefix Length		(0-32)
Lease Time	Specified Duration	
Days	1	(0 to 59)
Hours	0	(0 to 1439)
Minutes	0	(0 to 86399)

5. Under DHCP Pool Configuration, enter the following information:
   - In the **Pool Name** list, select **Create**.
   - In the **Pool Name** field, enter **pool_manual**.
   - In the **Type of Binding** list, select **Manual**.
   - In the **Client Name** field, enter **dhcpclient**.
   - In the **Hardware Address** field, enter **00:01:02:03:04:05**.
   - In the **Hardware Type** list, select **ethernet**.
   - In the **Host Number** field, enter **192.168.200.1**.
   - In the **Network Mask** field, enter **255.255.255.0**. As an alternate, you can enter **24** in the **Network Prefix Length** field.
   - In the **Days** field, enter **1**.
6. Click **Add**. The pool_manual name is now added to the Pool Name drop-down list.

19. DVLANs and Private VLANs

Double VLANS and private VLAN groups

19

This chapter includes the following sections:

- *Double VLANs*
- *Private VLAN Groups* on page 316

Double VLANs

This section describes how to enable the double DVLAN feature. Double VLANs pass traffic from one customer domain to another through the metro core. Custom VLAN IDs are preserved and a provider service VLAN ID is added to the traffic so the traffic can pass the metro core in a simple and cost-effective manner. You can use VLANs to specify customer ports and a service provider port. In this example, the switches have the same configuration.

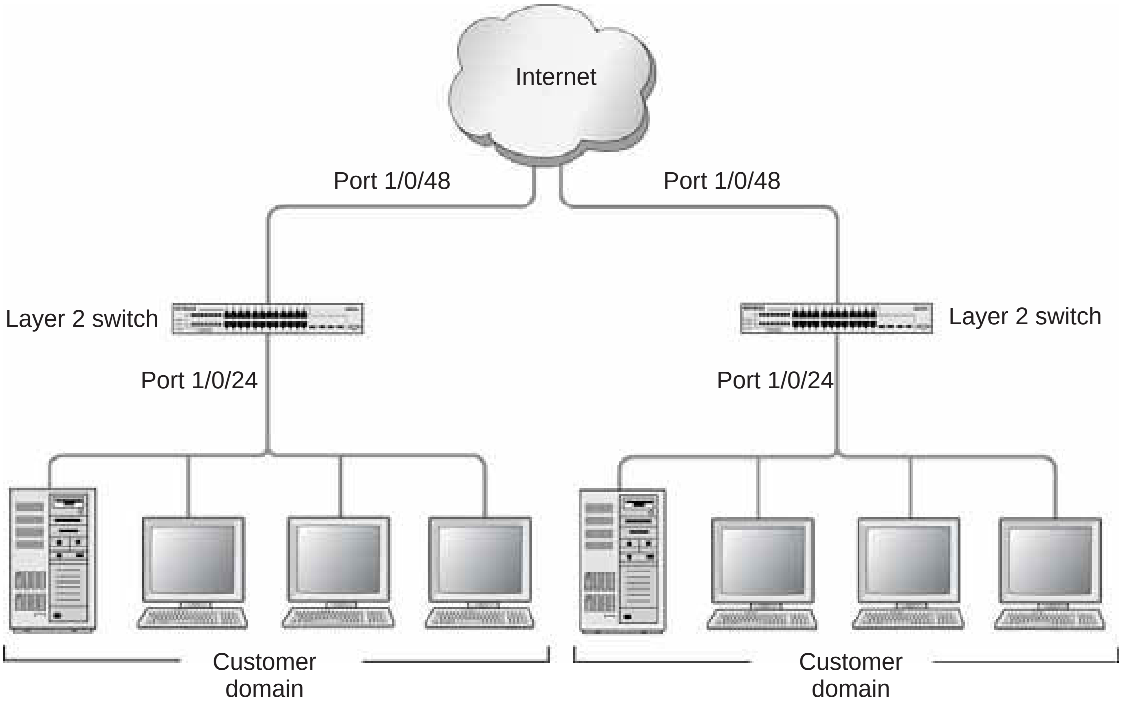


Figure 31. Double VLANS

The following example shows how to configure the NETGEAR switch shown in the preceding figure to add a double VLAN tag for traffic going from the subnet domain connected to port 1/0/24. This example assumes there is a Layer 2 switch connecting all these devices in your domain. The Layer 2 switch tags the packet going to the NETGEAR switch port 1/0/24. The example is shown as CLI commands and as a Web interface procedure.

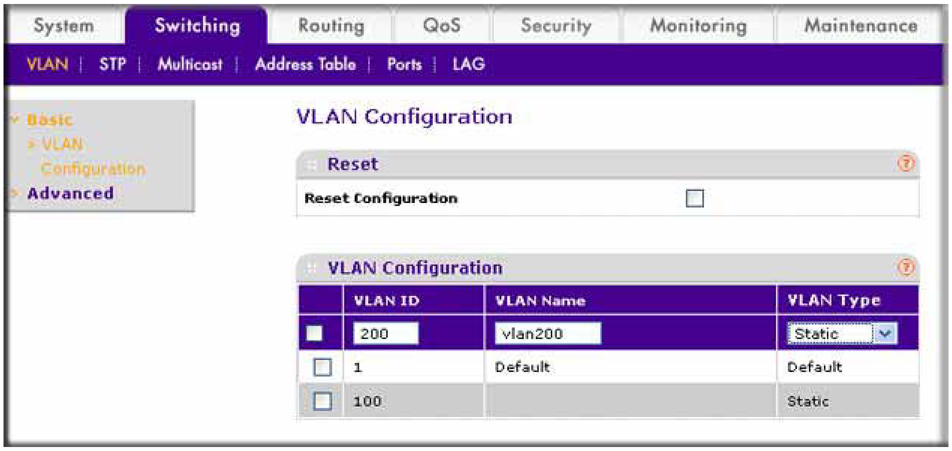
CLI: Enable a Double VLAN

```
Create a VLAN 200.
(Netgear Switch)#vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#exit

Add interface 1/0/24 to VLAN 200, add pvid 200 to port.
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan pvid 200
(Netgear Switch) (Interface 1/0/24)#vlan participation include 200
(Netgear Switch) (Interface 1/0/24)#exit

Add interface 1/0/48 to the VLAN 200 in a tagging mode.
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan participation include 200
(Netgear Switch) (Interface 1/0/48)#vlan tagging 200
(Netgear Switch) (Interface 1/0/48)#exit

Select interface 1/0/48 as the provider port.
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#mode dvlan-tunnel
(Netgear Switch) (Interface 1/0/48)#exit
```

Web Interface: Enable a Double VLAN

1. Create static VLAN 200:

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



VLAN Configuration

Reset

Reset Configuration □

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type
□	200	vlan200	Static
□	1	Default	Default
□	100		Static

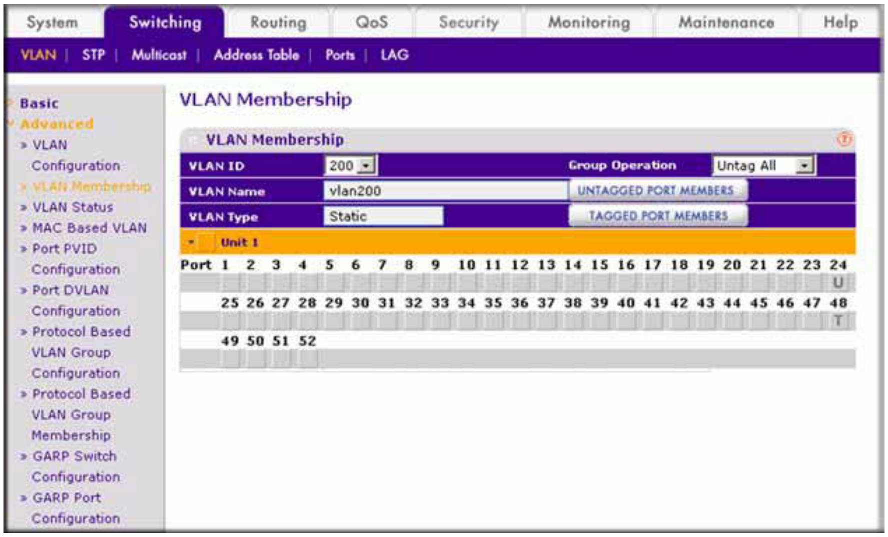
b. Under VLAN Configuration, enter the following information:

- 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

VLAN ID 200

VLAN Name vlan200

VLAN Type Static

Group Operation Untag All

Unit 1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
																								U
	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
																								T
	49	50	51	52																				

b. Under VLAN Membership, in the **VLAN ID** field, select **200**.

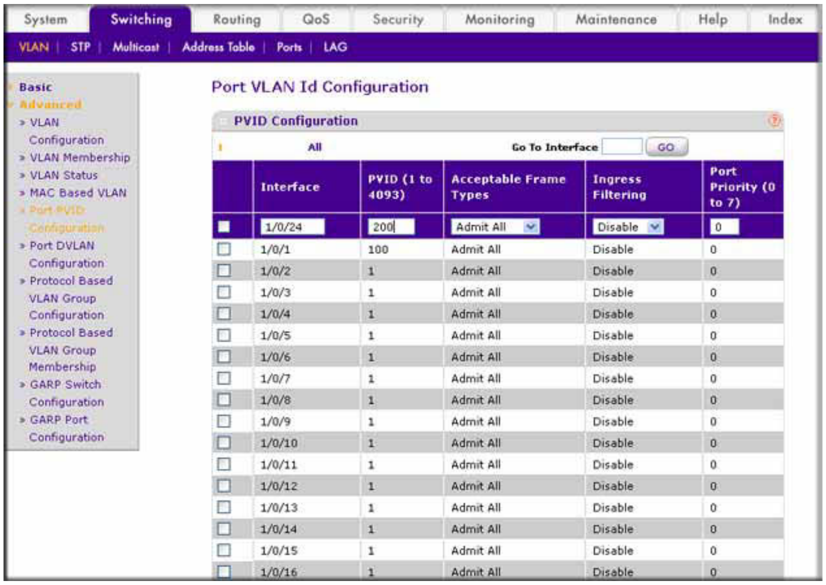
c. Click **Unit 1**. The ports display:

- 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.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
VLAN | STP | Multicast | Address Table | Ports | LAG
Basic
Advanced
» VLAN Configuration
» VLAN Membership
» VLAN Status
» MAC Based VLAN
» Port PVID Configuration
» Port DVLAN Configuration
» Protocol Based VLAN Group Configuration
» Protocol Based VLAN Group Membership
» GARP Switch Configuration
» GARP Port Configuration
GO

Port VLAN Id Configuration

PVID Configuration

All   Go To Interface

	Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)
□	1/0/24	200	Admit All	Disable	0
□	1/0/1	100	Admit All	Disable	0
□	1/0/2	1	Admit All	Disable	0
□	1/0/3	1	Admit All	Disable	0
□	1/0/4	1	Admit All	Disable	0
□	1/0/5	1	Admit All	Disable	0
□	1/0/6	1	Admit All	Disable	0
□	1/0/7	1	Admit All	Disable	0
□	1/0/8	1	Admit All	Disable	0
□	1/0/9	1	Admit All	Disable	0
□	1/0/10	1	Admit All	Disable	0
□	1/0/11	1	Admit All	Disable	0
□	1/0/12	1	Admit All	Disable	0
□	1/0/13	1	Admit All	Disable	0
□	1/0/14	1	Admit All	Disable	0
□	1/0/15	1	Admit All	Disable	0
□	1/0/16	1	Admit All	Disable	0

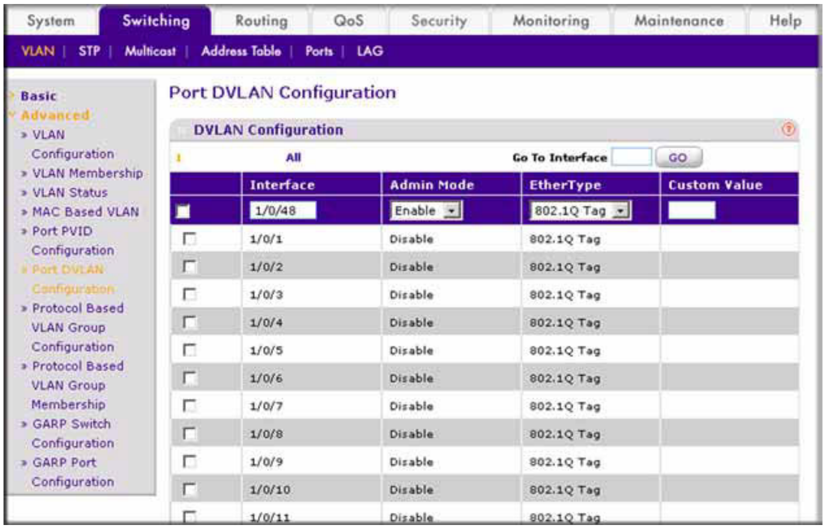
b. Scroll down and select the Interface **1/0/24** check box. Now 1/0/24 appears in the Interface field at the top.

c. In the **PVID (1 to 4093)** field, enter **200**.

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

4. Configure port 48 as the provider service port:

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


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
VLAN | STP | Multicast | Address Table | Ports | LAG
Basic
Advanced
» VLAN Configuration
» VLAN Membership
» VLAN Status
» MAC Based VLAN
» Port PVID Configuration
» Port DVLAN Configuration
» Protocol Based VLAN Group Configuration
» Protocol Based VLAN Group Membership
» GARP Switch Configuration
» GARP Port Configuration
GO

Port DVLAN Configuration

DVLAN Configuration

All   Go To Interface

	Interface	Admin Mode	EtherType	Custom Value
□	1/0/48	Enable	802.1Q Tag	
□	1/0/1	Disable	802.1Q Tag	
□	1/0/2	Disable	802.1Q Tag	
□	1/0/3	Disable	802.1Q Tag	
□	1/0/4	Disable	802.1Q Tag	
□	1/0/5	Disable	802.1Q Tag	
□	1/0/6	Disable	802.1Q Tag	
□	1/0/7	Disable	802.1Q Tag	
□	1/0/8	Disable	802.1Q Tag	
□	1/0/9	Disable	802.1Q Tag	
□	1/0/10	Disable	802.1Q Tag	
□	1/0/11	Disable	802.1Q Tag	

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.

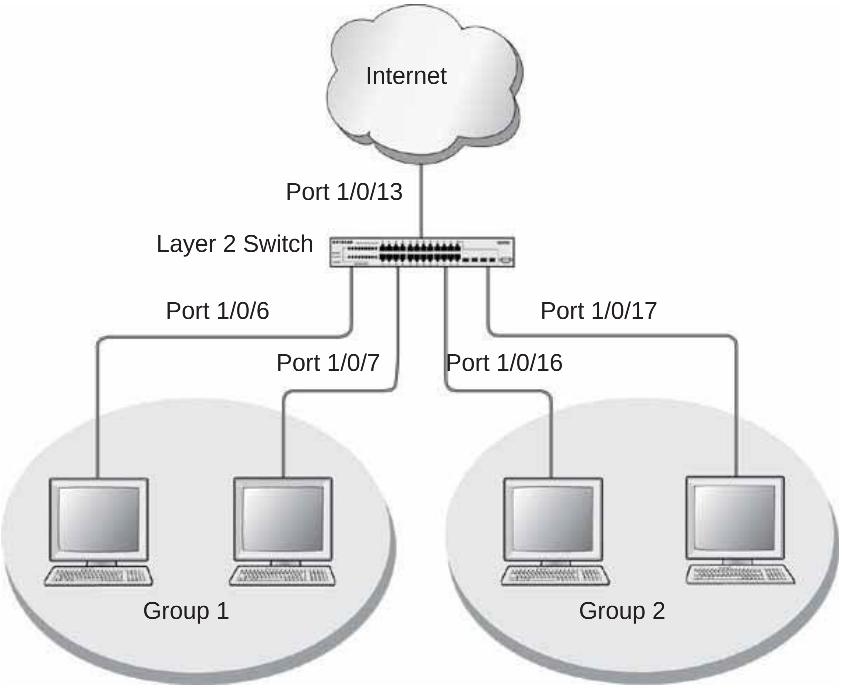


Figure 32. Private VLAN groups in community mode and isolated mode

CLI: Create a Private VLAN Group

1. Enter the following commands.

```
(Netgear Switch) #
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#exit

(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)#vlan participation include 200
(Netgear Switch) (Interface 1/0/6)#vlan pvid 200
(Netgear Switch) (Interface 1/0/6)#exit

(Netgear Switch) (Config)#interface 1/0/7
(Netgear Switch) (Interface 1/0/7)#vlan participation include 200
(Netgear Switch) (Interface 1/0/7)#vlan pvid 200
(Netgear Switch) (Interface 1/0/7)#exit
(Netgear Switch) (Config)#interface 1/0/16
(Netgear Switch) (Interface 1/0/16)#vlan participation include 200
(Netgear Switch) (Interface 1/0/16)#vlan participation pvid 200
(Netgear Switch) (Interface 1/0/16)#exit

(Netgear Switch) (Config)#interface 1/0/17
(Netgear Switch) (Interface 1/0/17)#vlan participation include 200
(Netgear Switch) (Interface 1/0/17)#vlan pvid 200
(Netgear Switch) (Interface 1/0/17)#exit
```

2. Create a VLAN 200 and include 1/0/6,1/0/7, 1/0/16, and 1/0/17.

```
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#private-group name group1 1 mode community
```

3. Create a private group in community mode.

```
(Netgear Switch) (Config)#private-group name group2 2 mode isolated
```

4. Create a private group in isolated mode.

```
(Netgear Switch) (Config)#interface range 1/0/6-1/0/7
(Netgear Switch) (conf-if-range-1/0/6-1/0/7)#switchport private-group 1
(Netgear Switch) (conf-if-range-1/0/6-1/0/7)#exit
```

5. Add 1/0/16 and 1/0/7 to the private group 1.

```
(Netgear Switch) (Config)#interface range 1/0/16-1/0/17
(Netgear Switch) (conf-if-range-1/0/16-1/0/17)#switchport private-group 2
```

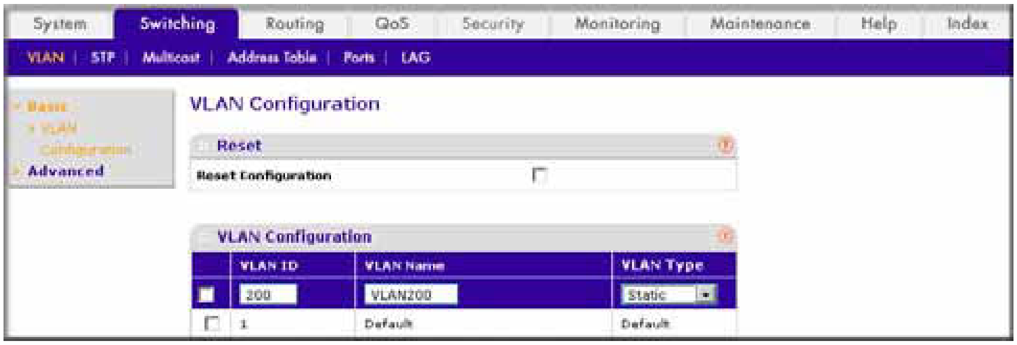
6. Add 1/0/16 and 1/0/7 to the private group 2.

```
(Netgear Switch) (conf-if-range-1/0/16-1/0/17)#exit
```

Web Interface: Create a Private VLAN Group

1. Create VLAN 200.

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



VLAN Configuration

Reset

Reset Configuration □

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type
□	200	VLAN200	Static
□	1	Default	Default

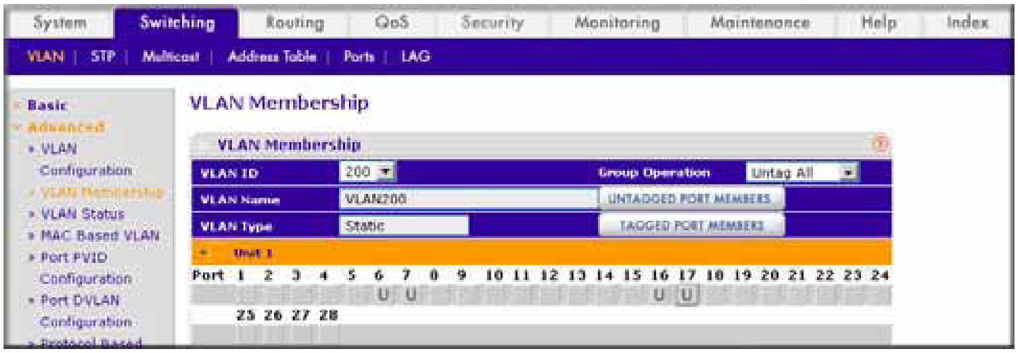
   b. Enter the following information:

   - In the **VLAN ID** field, enter **200**.
   - In the **VLAN Name** field, enter **VLAN200**.
   - In the **VLAN Type** field, select **Static**.

   c. Click **Add**.

2. Add ports 1/0/6, 1/0/7, 1/0/16, and 1/0/17 to VLAN 200.

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



VLAN Membership

VLAN Membership

VLAN ID 200

Group Operation Untag All

VLAN Name VLAN200

VLAN Type Static

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
						U	U									U	U							
	25	26	27	28																				

b. Under VLAN Membership, in the **VLAN ID** list, select **200**.

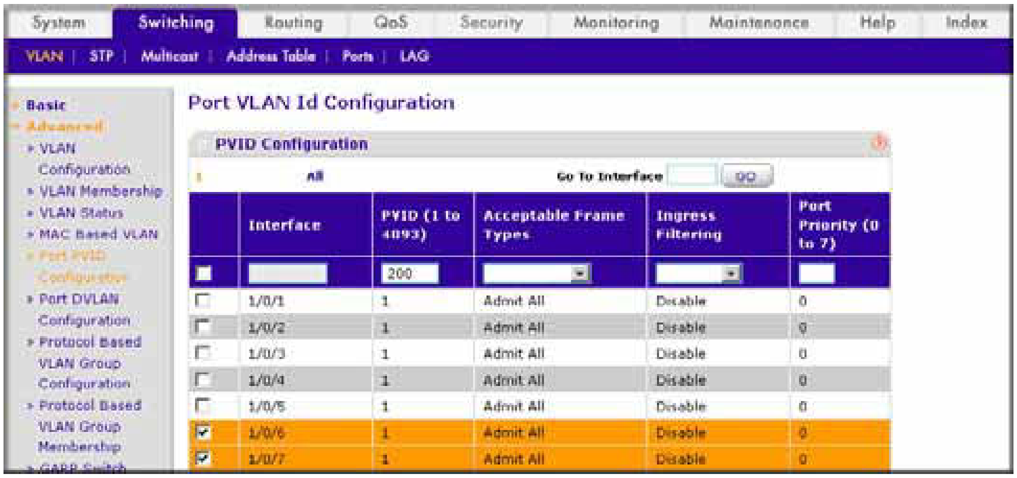
c. Click **Unit 1.** The ports display.

d. Click the gray boxes under ports **6**, **7**, **16** and **17** until **U** displays. The U specifies that the egress packet is untagged for the port.

e. Click **Apply**.

3. Specify the PVID on ports 1/0/6, 1/0/7, 1/0/16, and 1/0/17.

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



Port VLAN Id Configuration

PVID Configuration

	Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)
□		200			
□	1/0/1	1	Admit All	Disable	0
□	1/0/2	1	Admit All	Disable	0
□	1/0/3	1	Admit All	Disable	0
□	1/0/4	1	Admit All	Disable	0
□	1/0/5	1	Admit All	Disable	0
☑	1/0/6	1	Admit All	Disable	0
☑	1/0/7	1	Admit All	Disable	0

b. Under PVID Configuration, scroll down and select the Interface **1/0/6**,**1/0/7**,**1/0/16**, and **1/0/17** check boxes.

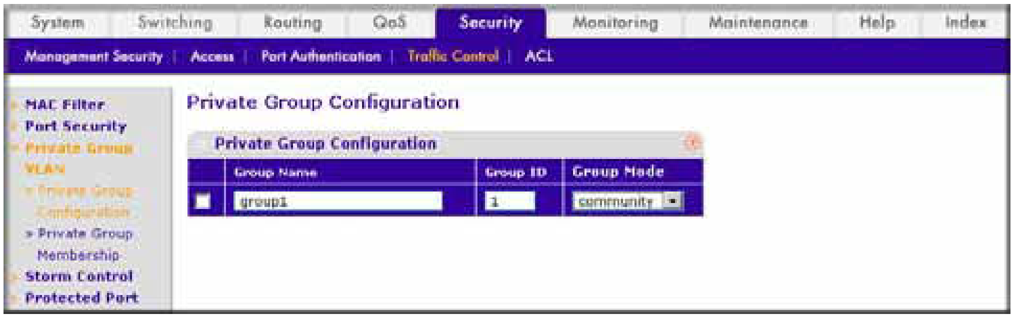
c. In the **PVID (1 to 4093)** field, enter **200**.

d. In the **Acceptable Frame Type** list, select **Admit All**.

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

4. Create a private group, group1.

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



Private Group Configuration

Private Group Configuration

	Group Name	Group ID	Group Mode
□	group1	1	community

b. In the **Group Name** field, enter **group1**.

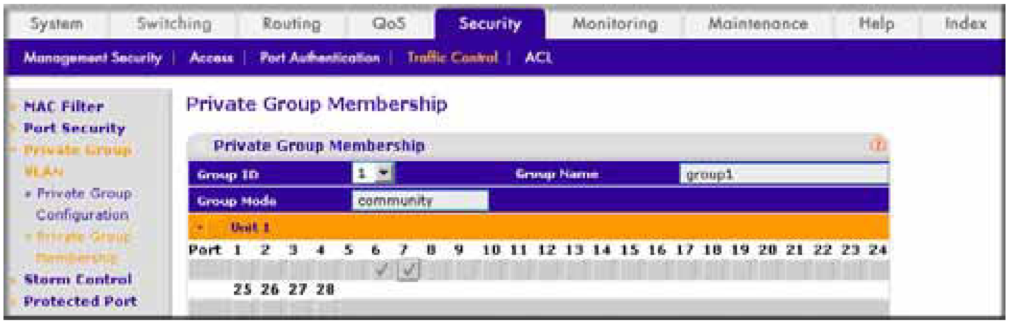
c. In the **Group ID** field, enter **1**.

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.



Private Group Membership

Private Group Membership

Group ID	1	Group Name	group1
Group Mode	community		

Unit 1

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

25 26 27 28

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

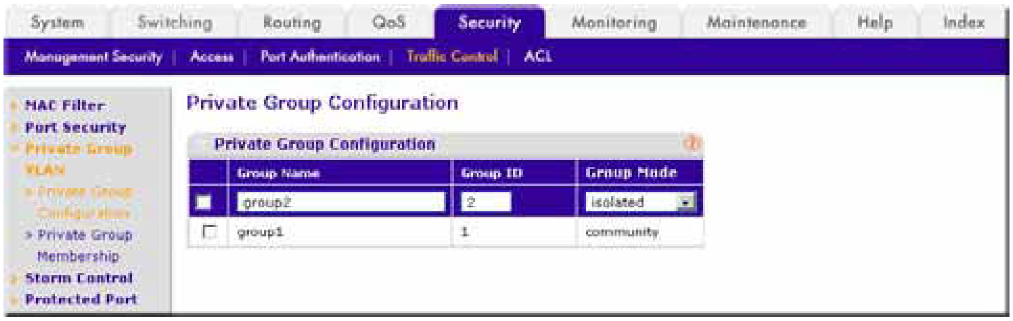
   c. Click **Unit 1.** The ports display.

   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.



Private Group Configuration

Private Group Configuration

	Group Name	Group ID	Group Mode
☐	group2	2	isolated
☐	group1	1	community

   b. In the **Group Name** field, enter **group2**.

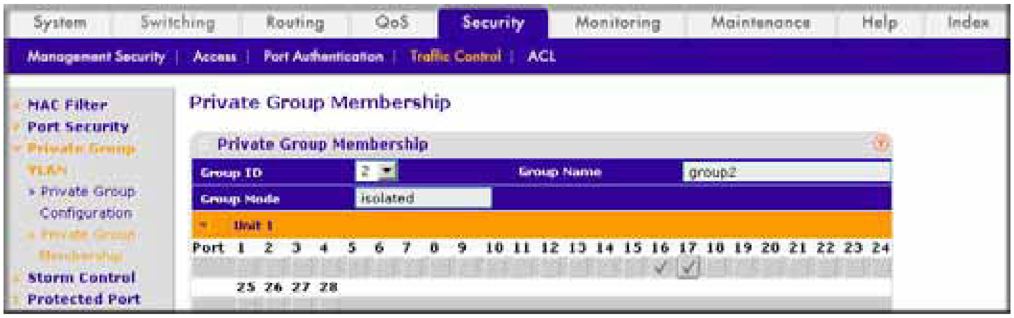
   c. In the **Group ID** field, enter **2**.

   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.



Private Group Membership

Private Group Membership

Group ID: 2

Group Name: group2

Group Mode: isolated

Unit 1

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

☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☑ ☑ ☐ ☐ ☐ ☐ ☐ ☐ ☐

25 26 27 28

☐ ☐ ☐ ☐

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**.

20.

STP

Spanning Tree Protocol

20

This chapter includes the following sections:

SPT Concepts

The purpose of Spanning Tree is to eliminate loops in the switch system. There are three STPs: Classic STP (802.1d), Rapid STP (RSTP, 802.1w), and Multiple STP (MSTP, 802.1s).

While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a few seconds. RSTP can revert back to 802.1d in order to interoperate with legacy bridges on a per-port basis. This drops the benefits it introduces.

In Multiple Spanning Tree Protocol (MSTP), each Spanning Tree instance can contain several VLANs. Each Spanning Tree instance is independent of other instances. This approach provides multiple forwarding paths for data traffic, enabling load balancing, and reducing the number of Spanning Tree instances required to support a large number of VLANs.

Configure Classic STP (802.1d)

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

CLI: Configure Classic STP (802.1d)

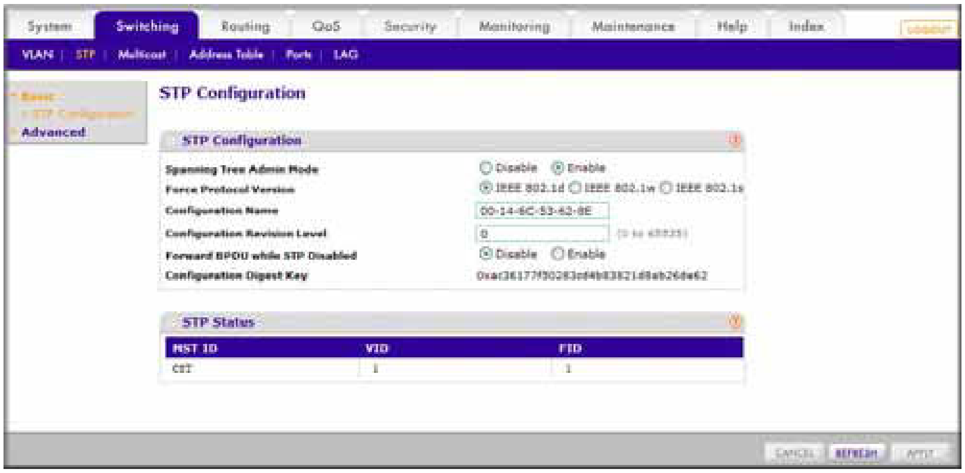
```
(Netgear Switch) (Config)# spanning-tree
(Netgear Switch) (Config)# spanning-tree forceversion 802.1d
(Netgear switch) (Interface 1/0/3)# spanning-tree port mode
```

Web Interface: Configure Classic STP (802.1d)

1. Enable 802.1d on the switch.

   a. Select **Switching > STP > STP Configuration**.

   A screen similar to the following displays.



STP Configuration

STP Configuration

Spanning Tree Admin Mode	○ Disable ● Enable
Force Protocol Version	● IEEE 802.1d ○ IEEE 802.1w ○ IEEE 802.1s
Configuration Name	00-14-6C-53-62-8E
Configuration Revision Level	0 (0 to 65535)
Forward BPDU while STP Disabled	● Disable ○ Enable
Configuration Digest Key	0xac36177f50283cd4b83821d8ab26de62

STP Status

MST ID	VID	FID
CST	1	1

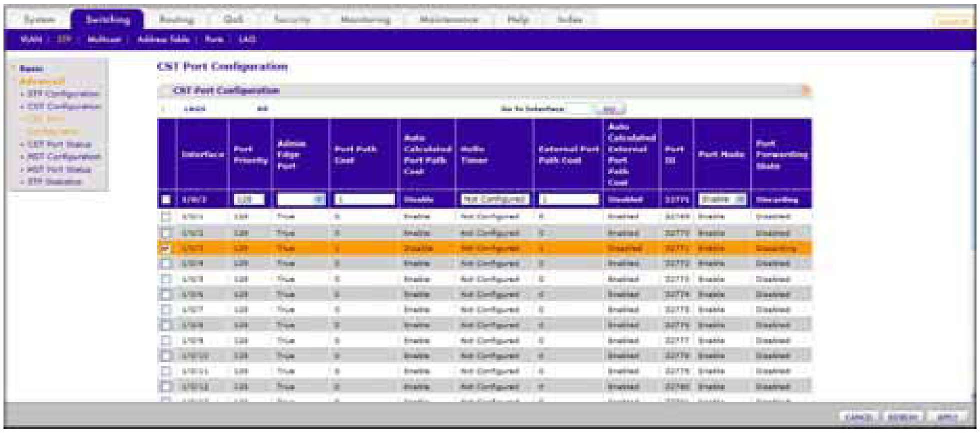
b. Enter the following information:
   - For Spanning Tree Admin Mode, select the **Enable** radio button.
   - For Force Protocol Version, select the **IEEE 802.1d** radio button.

c. Click **Apply**.

2. Configure the CST port.

   a. Select **Switching > STP > CST Port Configuration**.

   A screen similar to the following displays.



CST Port Configuration

CST Port Configuration

	Interface	Port Priority	Admin Edge Port	Port Path Cost	Auto Calculated Port Path Cost	Hello Timer	External Port Path Cost	Auto Calculated External Port Path Cost	Port ID	Port Mode	Port Forwarding State
□	1/0/3	128		1	Disable	Not Configured	1	Disabled	32771	Enable	Discarding
□	1/0/1	128	True	0	Enable	Not Configured	0	Enabled	32769	Enable	Disabled
□	1/0/2	128	True	0	Enable	Not Configured	0	Enabled	32770	Enable	Disabled
☑	1/0/3	128	True	1	Disable	Not Configured	1	Disabled	32771	Enable	Discarding
□	1/0/4	128	True	0	Enable	Not Configured	0	Enabled	32772	Enable	Disabled
□	1/0/5	128	True	0	Enable	Not Configured	0	Enabled	32773	Enable	Disabled
□	1/0/6	128	True	0	Enable	Not Configured	0	Enabled	32774	Enable	Disabled
□	1/0/7	128	True	0	Enable	Not Configured	0	Enabled	32775	Enable	Disabled
□	1/0/8	128	True	0	Enable	Not Configured	0	Enabled	32776	Enable	Disabled
□	1/0/9	128	True	0	Enable	Not Configured	0	Enabled	32777	Enable	Disabled
□	1/0/10	128	True	0	Enable	Not Configured	0	Enabled	32778	Enable	Disabled
□	1/0/11	128	True	0	Enable	Not Configured	0	Enabled	32779	Enable	Disabled
□	1/0/12	128	True	0	Enable	Not Configured	0	Enabled	32780	Enable	Disabled

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

   c. In the **Port Mode** field, select **Enable**.

   d. Click **Apply**.

Configure Rapid STP (802.1w)

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

CLI: Configure Rapid STP (802.1w)

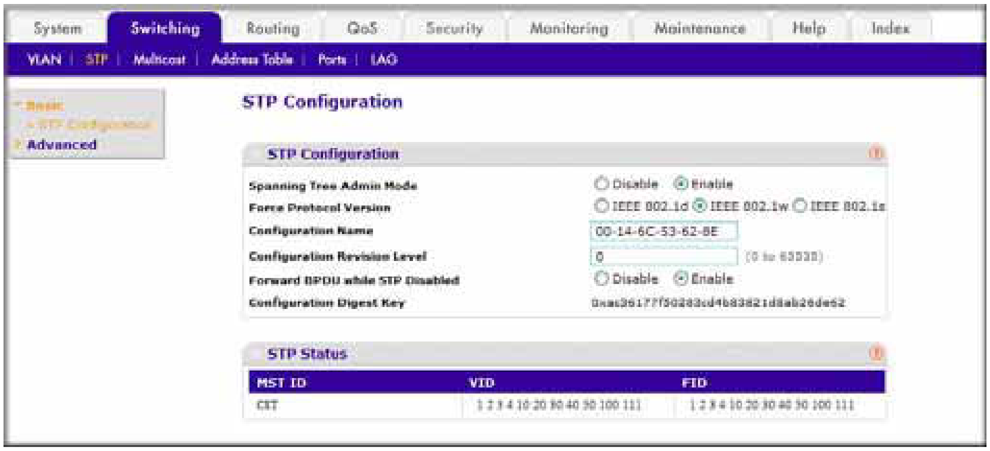
```
(Netgear switch) (Config)# spanning-tree
(Netgear switch) (Config)# spanning-tree forceversion 802.1w
(Netgear switch) (Interface 1/0/3)# spanning-tree port mode
```

Web Interface: Configure Rapid STP (802.1w)

1. Enable 802.1w on the switch:

   a. Select **Switching > STP > STP Configuration**.

A screen similar to the following displays.



STP Configuration

STP Configuration

Spanning Tree Admin Mode	○ Disable ● Enable
Force Protocol Version	○ IEEE 802.1d ● IEEE 802.1w ○ IEEE 802.1s
Configuration Name	00-14-6C-53-62-8E
Configuration Revision Level	0 (0 to 65535)
Forward BPDU while STP Disabled	○ Disable ● Enable
Configuration Digest Key	0xac36177f50283cd4b83821d8ab26de62

STP Status

MST ID	VID	FID
CST	1 2 3 4 10 20 30 40 50 100 111	1 2 3 4 10 20 30 40 50 100 111

b. Enter the following information:

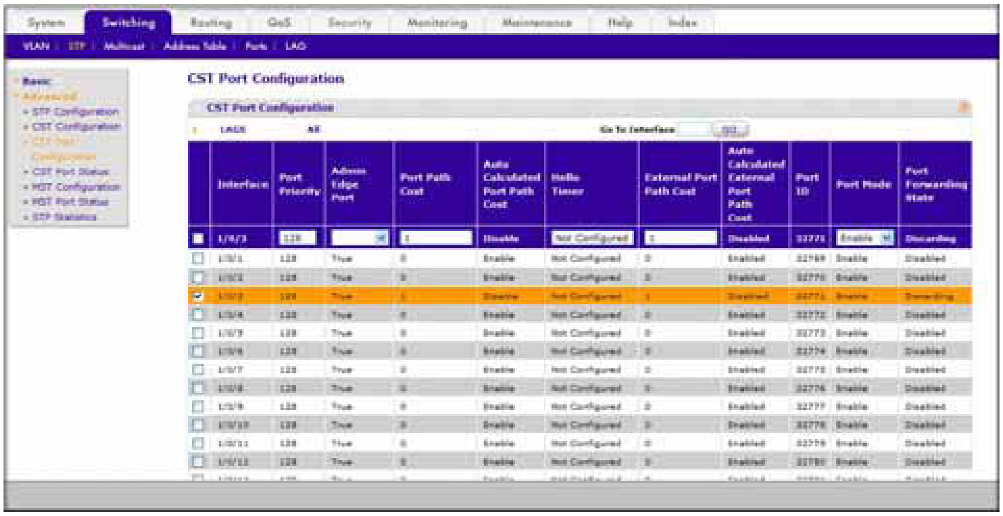
- For Spanning Tree Admin Mode, select the **Enable** radio button.
- For Force Protocol Version, select the **IEEE 802.1w** radio button.

c. Click **Apply.**

2. Configure the CST port.

a. Select **Switching > STP > CST Port Configuration**.

A screen similar to the following displays.



CST Port Configuration

CST Port Configuration

1 LAGS All Go To Interface

	Interface	Port Priority	Admin Edge Port	Port Path Cost	Auto Calculated Port Path Cost	Hello Timer	External Port Path Cost	Auto Calculated External Port Path Cost	Port ID	Port Mode	Port Forwarding State
□	1/0/3	128		1	Disable	Not Configured	1	Disabled	32771	Enable	Discarding
□	1/0/1	128	True	0	Enable	Not Configured	0	Enabled	32769	Enable	Disabled
□	1/0/2	128	True	0	Enable	Not Configured	0	Enabled	32770	Enable	Disabled
☑	1/0/3	128	True	1	Disable	Not Configured	1	Disabled	32771	Enable	Discarding
□	1/0/4	128	True	0	Enable	Not Configured	0	Enabled	32772	Enable	Disabled
□	1/0/5	128	True	0	Enable	Not Configured	0	Enabled	32773	Enable	Disabled
□	1/0/6	128	True	0	Enable	Not Configured	0	Enabled	32774	Enable	Disabled
□	1/0/7	128	True	0	Enable	Not Configured	0	Enabled	32775	Enable	Disabled
□	1/0/8	128	True	0	Enable	Not Configured	0	Enabled	32776	Enable	Disabled
□	1/0/9	128	True	0	Enable	Not Configured	0	Enabled	32777	Enable	Disabled
□	1/0/10	128	True	0	Enable	Not Configured	0	Enabled	32778	Enable	Disabled
□	1/0/11	128	True	0	Enable	Not Configured	0	Enabled	32779	Enable	Disabled
□	1/0/12	128	True	0	Enable	Not Configured	0	Enabled	32780	Enable	Disabled

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

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

c. In the **Port Mode** field, select **Enable**.

d. Click **Apply**.

Configure Multiple STP (802.1s)

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

CLI: Configure Multiple STP (802.1s)

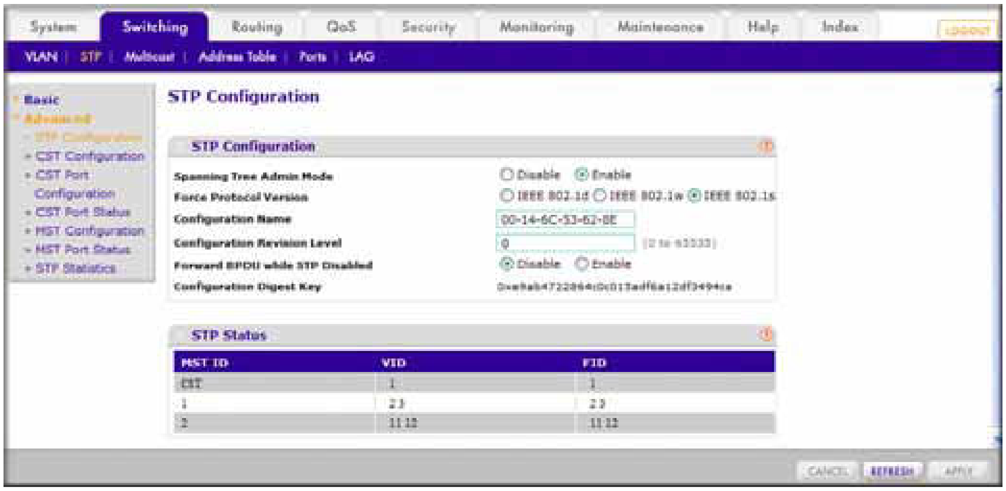
```
(Netgear switch) (Config)# spanning-tree
(Netgear switch) (Config)# spanning-tree forceversion 802.1s
(Netgear switch) (Config)# spanning-tree mst instance 1
Create a mst instance 1
(Netgear switch) (Config)# spanning-tree mst priority 1 4096
(Netgear switch) (Config)# spanning-tree mst vlan 1 2
(Netgear switch) (Config)# spanning-tree mst vlan 1 3
Associate the mst instance 1 with the VLAN 2 and 3
(Netgear switch) (Config)# spanning-tree mst instance 2
Create a mst instance 2
(Netgear switch) (Config)# spanning-tree mst priority 2 4096
(Netgear switch) (Config)# spanning-tree mst vlan 2 11
(Netgear switch) (Config)# spanning-tree mst vlan 2 12
Associate the mst instance 2 with the VLAN 11 and 12
(Netgear switch) (Interface 1/0/3)# spanning-tree mst 1 port-priority 128
(Netgear switch) (Interface 1/0/3)# spanning-tree mst 1 cost 0
```

Web Interface: Configure Multiple STP (802.1s)

1. Enable 802.1s on the switch.

   a. Select **Switching > STP > STP Configuration**.

   A screen similar to the following displays.



STP Configuration

STP Configuration

Spanning Tree Admin Mode ○ Disable ● Enable

Force Protocol Version ○ IEEE 802.1d ○ IEEE 802.1w ● IEEE 802.1s

Configuration Name 00-14-6C-53-62-8E

Configuration Revision Level 0 (0 to 65535)

Forward BPDU while STP Disabled ● Disable ○ Enable

Configuration Digest Key 0xe8ab4722064c0c015adf6a12df3494ca

STP Status

MST ID	VID	FID
CST	1	1
1	2 3	2 3
2	11 12	11 12

b. Enter the following information:

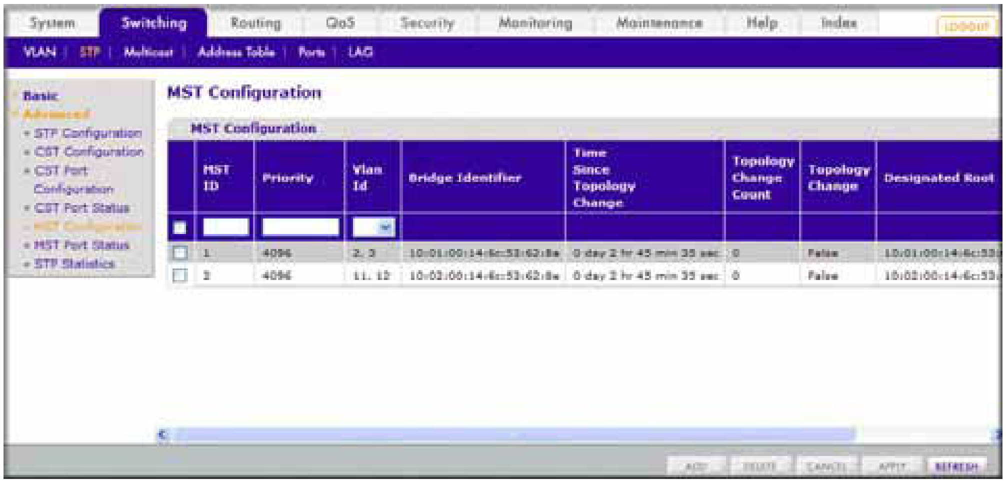
- For Spanning Tree Admin Mode, select the **Enable** radio button.
- For Force Protocol Version, select the **IEEE 802.1s** radio button.

c. Click **Apply**.

2. Configure MST.

a. Select **Switching > STP > MST Configuration**.

A screen similar to the following displays.



MST Configuration

MST Configuration

	MST ID	Priority	Vlan Id	Bridge Identifier	Time Since Topology Change	Topology Change Count	Topology Change	Designated Root
□								
□	1	4096	2, 3	10:01:00:14:6c:53:62:8a	0 day 2 hr 45 min 35 sec	0	False	10:01:00:14:6c:53
□	2	4096	11, 12	10:02:00:14:6c:53:62:8a	0 day 2 hr 45 min 35 sec	0	False	10:02:00:14:6c:53

b. Configure MST ID 1.

- In the **MST ID** field, enter **1**.
- In the **Priority** field, enter **4096**.
- In the **VLAN Id** field, enter **2**.
- Click **Add**.
- In the **VLAN Id** field, enter **3**.
- Click **Apply**.

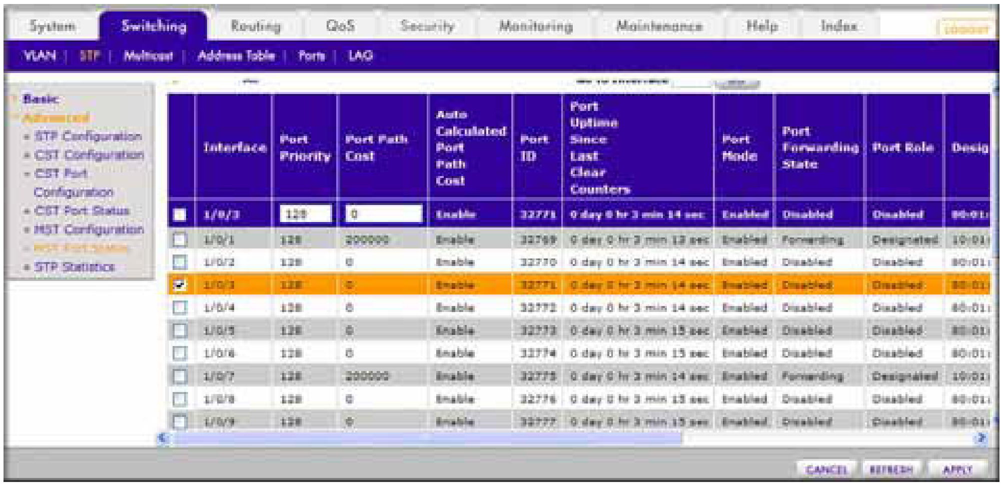
c. Configure MST ID 2.

- In the **MST ID** field, enter **2**.
- In the **Priority** field, enter **4096**.
- In the **VLAN Id** field, enter **11**.
- Click **Add**.
- In the **VLAN Id** field, enter **12**.
- Click **Apply**.

3. Configure the MST port.

a. Select **Switching > STP > MST Port Status**.

A screen similar to the following displays.



	Interface	Port Priority	Port Path Cost	Auto Calculated Port Path Cost	Port ID	Port Uptime Since Last Clear Counters	Port Mode	Port Forwarding State	Port Role	Desig
□	1/0/3	128	0	Enable	32771	0 day 0 hr 3 min 14 sec	Enabled	Disabled	Disabled	80:01:
□	1/0/1	128	200000	Enable	32769	0 day 0 hr 3 min 13 sec	Enabled	Forwarding	Designated	10:01:
□	1/0/2	128	0	Enable	32770	0 day 0 hr 3 min 14 sec	Enabled	Disabled	Disabled	80:01:
☑	1/0/3	128	0	Enable	32771	0 day 0 hr 3 min 14 sec	Enabled	Disabled	Disabled	80:01:
□	1/0/4	128	0	Enable	32772	0 day 0 hr 3 min 14 sec	Enabled	Disabled	Disabled	80:01:
□	1/0/5	128	0	Enable	32773	0 day 0 hr 3 min 15 sec	Enabled	Disabled	Disabled	80:01:
□	1/0/6	128	0	Enable	32774	0 day 0 hr 3 min 15 sec	Enabled	Disabled	Disabled	80:01:
□	1/0/7	128	200000	Enable	32775	0 day 0 hr 3 min 14 sec	Enabled	Forwarding	Designated	10:01:
□	1/0/8	128	0	Enable	32776	0 day 0 hr 3 min 15 sec	Enabled	Disabled	Disabled	80:01:
□	1/0/9	128	0	Enable	32777	0 day 0 hr 3 min 15 sec	Enabled	Disabled	Disabled	80:01:

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**.

DHCP L2 Relay and L3 Relay

21

Dynamic Host Configuration Protocol Relays

This chapter includes the following sections:

- *DHCP L2 Relay*
- *DHCP L3 Relay*

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.

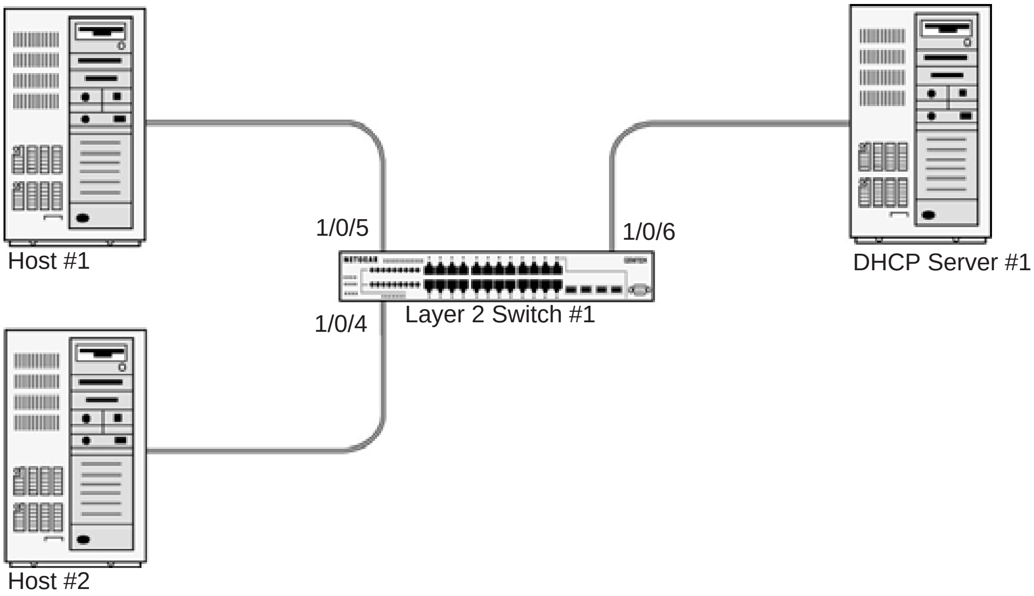


Figure 33. DHCP L2 Relay

These Layer 2 devices typically operate only as bridges for the network and might not have an IPv4 address on the network. Lacking a valid IPv4 source address, they cannot relay packets directly to a DHCP server located on another network. These Layer 2 devices append the Relay agent information option and broadcast the DHCP message. This section provides information about where a Layer 2 relay agent fits in and how it is used.

CLI: Enable DHCP L2 Relay

1. Enter the following commands:

```
(Netgear Switch)#vlan database
(Netgear Switch)(Vlan)#vlan 200
(Netgear Switch)(Vlan)#exit
```

2. Enable the DHCP L2 relay on the switch.

```
(Netgear Switch) (Config)#dhcp l2relay
(Netgear Switch) (Config)#dhcp l2relay vlan 200
```

3. Enable the Option 82 Circuit ID field.

```
(Netgear Switch) (Config)#dhcp l2relay circuit-id vlan 200
```

4. Enable the Option 82 Remote ID field.

```
(Netgear Switch) (Config)#dhcp l2relay remote-id rem_id vlan 200
```

5. Enable DHCP L2 relay on port 1/0/4.

```
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)# dhcp l2relay
```

```
(Netgear Switch) (Interface 1/0/4)# vlan pvid 200
(Netgear Switch) (Interface 1/0/4)# vlan participation include 200
(Netgear Switch) (Interface 1/0/4)# exit
```

6. Enable DHCP L2 relay on port 1/0/5.

```
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)# dhcp l2relay
(Netgear Switch) (Interface 1/0/5)# vlan pvid 200
(Netgear Switch) (Interface 1/0/5)# vlan participation include 200
(Netgear Switch) (Interface 1/0/5)# exit
```

7. Enable DHCP L2 relay on port 1/0/6.

```
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)# dhcp l2relay
```

8. Trust packets with option 82 received on port 1/0/6.

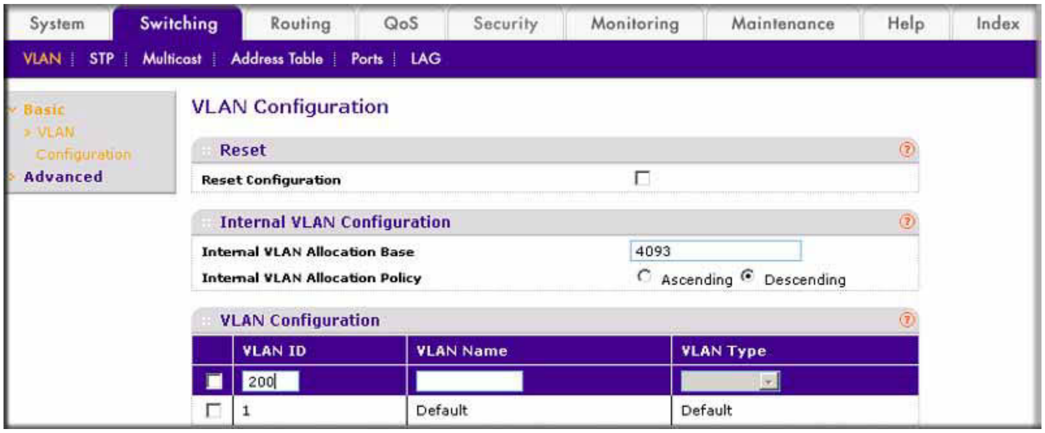
```
(Netgear Switch) (Interface 1/0/6)# dhcp l2relay trust
(Netgear Switch) (Interface 1/0/6)# vlan pvid 200
(Netgear Switch) (Interface 1/0/6)# vlan participation include 200
(Netgear Switch) (Interface 1/0/6)# exit
```

Web Interface: Enable DHCP L2 Relay

1. Create VLAN 200.

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

   A screen similar to the following displays.



VLAN Configuration

Reset

Reset Configuration □

Internal VLAN Configuration

Internal VLAN Allocation Base 4093

Internal VLAN Allocation Policy ○ Ascending ● Descending

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type
□	200		
□	1	Default	Default

   b. In the **VLAN ID** field, enter **200**.

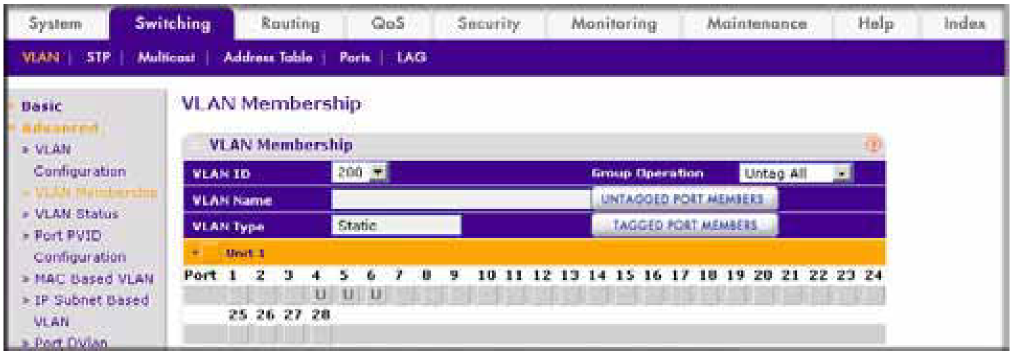
   c. In the **VLAN Type** field, select **Static**.

   d. Click **Add**.

2. Add ports to VLAN 200.

   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

   A screen similar to the following displays.



VLAN Membership

VLAN Membership

VLAN ID 200 Group Operation Untag All

VLAN Name

VLAN Type Static

Unit 1

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

25	26	27	28

   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.

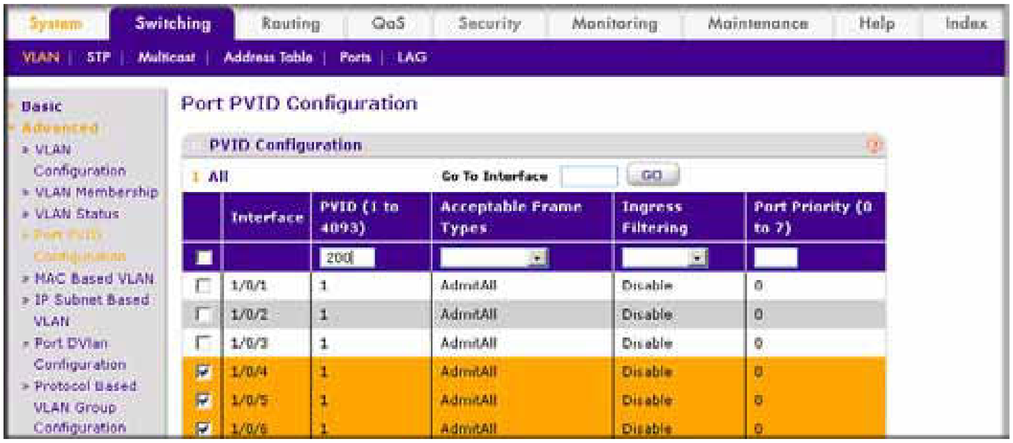
   The U specifies that the egress packet is untagged for the port.

   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

PVID Configuration

1 All Go To Interface

	Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)
□		200			
□	1/0/1	1	AdmitAll	Disable	0
□	1/0/2	1	AdmitAll	Disable	0
□	1/0/3	1	AdmitAll	Disable	0
☑	1/0/4	1	AdmitAll	Disable	0
☑	1/0/5	1	AdmitAll	Disable	0
☑	1/0/6	1	AdmitAll	Disable	0

b. Scroll down and select the Interface **1/0/4**, **1/0/5**, and **1/0/6** check boxes.

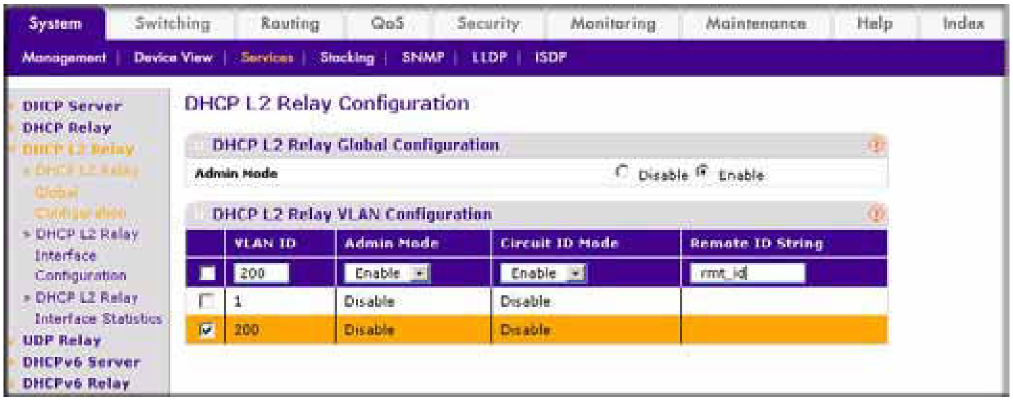
c. In the **PVID (1 to 4093)** field, enter **200**.

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.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Management | Device View | Services | Stacking | SNMP | LLDP | ISDP
DHCP Server
DHCP Relay
DHCP L2 Relay
DHCP L2 Relay Global Configuration
DHCP L2 Relay Interface Configuration
DHCP L2 Relay Interface Statistics
UDP Relay
DHCPv6 Server
DHCPv6 Relay

DHCP L2 Relay Configuration

DHCP L2 Relay Global Configuration

Admin Mode ○ Disable ● Enable

DHCP L2 Relay VLAN Configuration

	VLAN ID	Admin Mode	Circuit ID Mode	Remote ID String
□	200	Enable	Enable	rmt_id
□	1	Disable	Disable	
☑	200	Disable	Disable	

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

c. Scroll down and select the VLAN ID **200** check box.

d. Enter the following information:

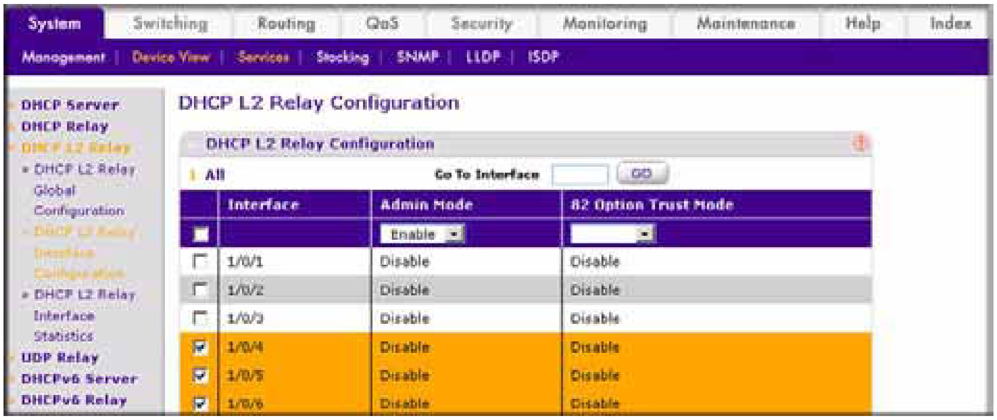
- In the **Admin Mode** field, select **Enable**.
- In the **Circuit ID Mode** field, select **Enable**.
- In the **Remote ID String** field, enter **rmt_id**.

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

5. Enable DHCP L2 Relay on interfaces 1/0/4,1/0/5, and 1/0/6.

a. Select **System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration**.

A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Management | Device View | Services | Stacking | SNMP | LLDP | ISDP
DHCP Server
DHCP Relay
DHCP L2 Relay
DHCP L2 Relay Global Configuration
DHCP L2 Relay Interface Configuration
DHCP L2 Relay Interface Statistics
UDP Relay
DHCPv6 Server
DHCPv6 Relay
GO

DHCP L2 Relay Configuration

DHCP L2 Relay Configuration

All Go To Interface

	Interface	Admin Mode	82 Option Trust Mode
□		Enable	
□	1/0/1	Disable	Disable
□	1/0/2	Disable	Disable
□	1/0/3	Disable	Disable
☑	1/0/4	Disable	Disable
☑	1/0/5	Disable	Disable
☑	1/0/6	Disable	Disable

b. Scroll down and select the **1/0/4**, **1/0/5**, and **1/0/6** check boxes.

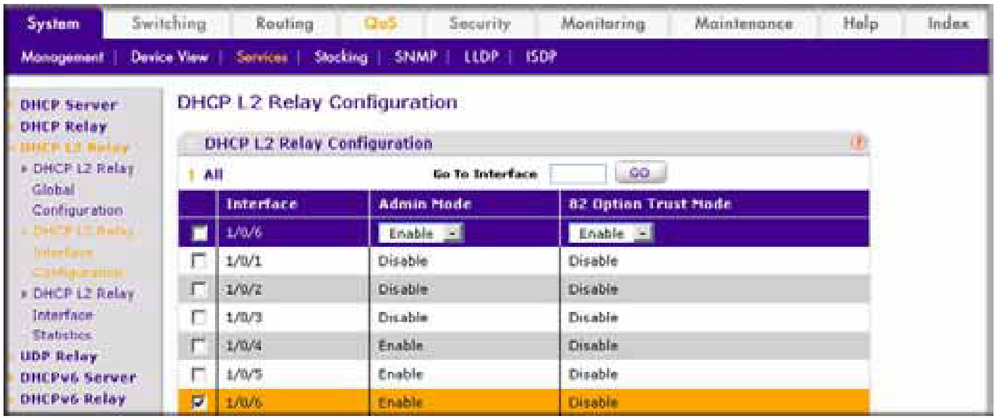
c. In the **Admin Mode** field, select **Enable**.

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

6. Enable DHCP L2 relay trust on interface 1/0/6.

a. Select **System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration**.

A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Management | Device View | Services | Stacking | SNMP | LLDP | ISDP
DHCP Server
DHCP Relay
DHCP L2 Relay
DHCP L2 Relay Global Configuration
DHCP L2 Relay Interface Configuration
DHCP L2 Relay Interface Statistics
UDP Relay
DHCPv6 Server
DHCPv6 Relay
GO

DHCP L2 Relay Configuration

DHCP L2 Relay Configuration

All Go To Interface

	Interface	Admin Mode	82 Option Trust Mode
□	1/0/6	Enable	Enable
□	1/0/1	Disable	Disable
□	1/0/2	Disable	Disable
□	1/0/3	Disable	Disable
□	1/0/4	Enable	Disable
□	1/0/5	Enable	Disable
☑	1/0/6	Enable	Disable

b. Under DHCP L2 Relay Configuration, scroll down and select the Interface **1/0/6** check box.

c. In the **82 Option Trust Mode** field, select **Enable**.

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

DHCP L3 Relay

This case has two steps, DHCP server configuration and DHCP L3 relay configuration. This example shows how to configure a DHCP L3 relay on a NETGEAR switch and how to configure DHCP pool to assign IP addresses to DHCP clients using DHCP L3 relay.

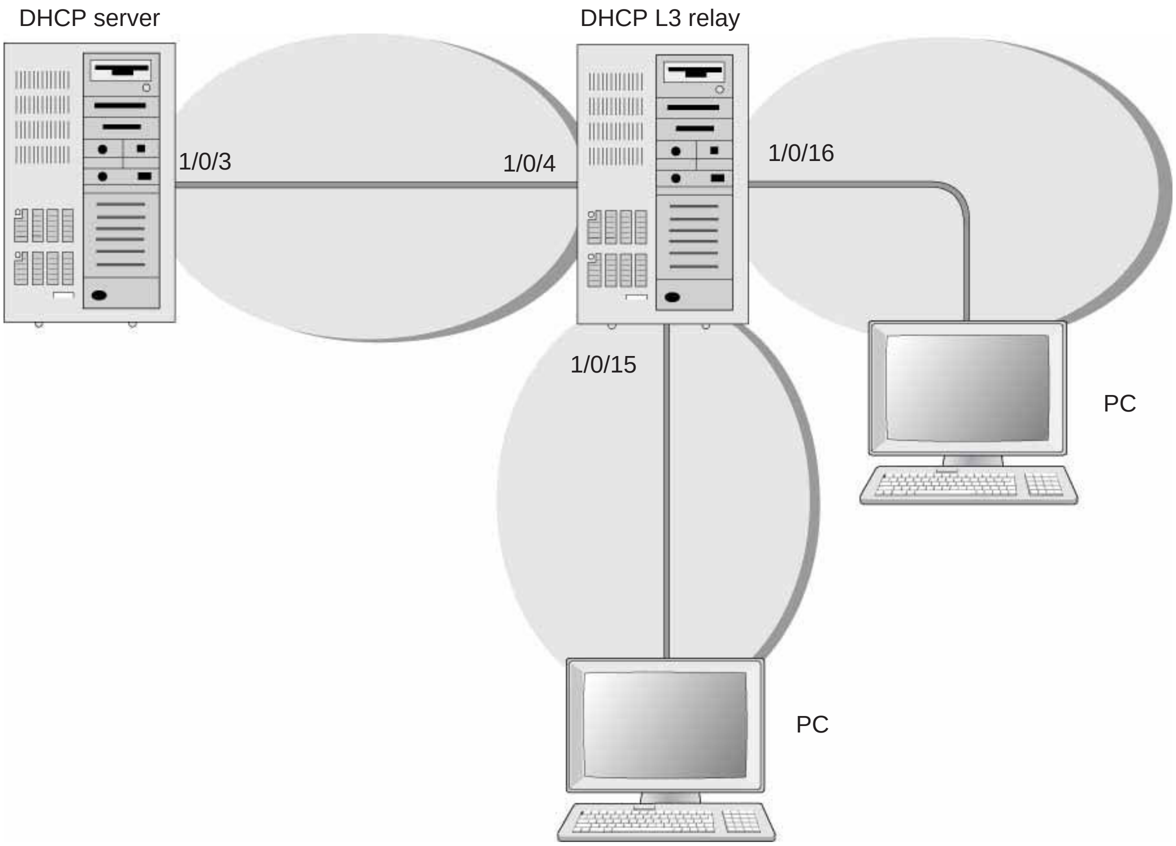


Figure 34. DHCP L3 relay

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
```

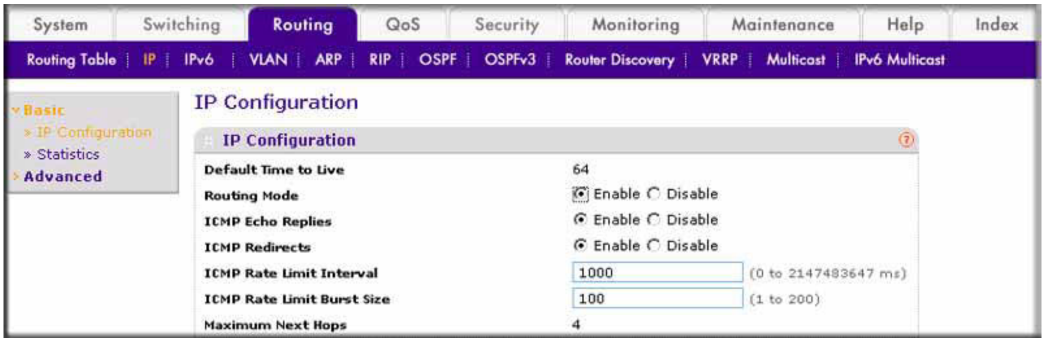
4. Exclude the IP address 10.200.1.1 and 10.200.2.1 from the DHCP pool because it has been used on the DHCP L3 relay.

```
(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.



IP Configuration

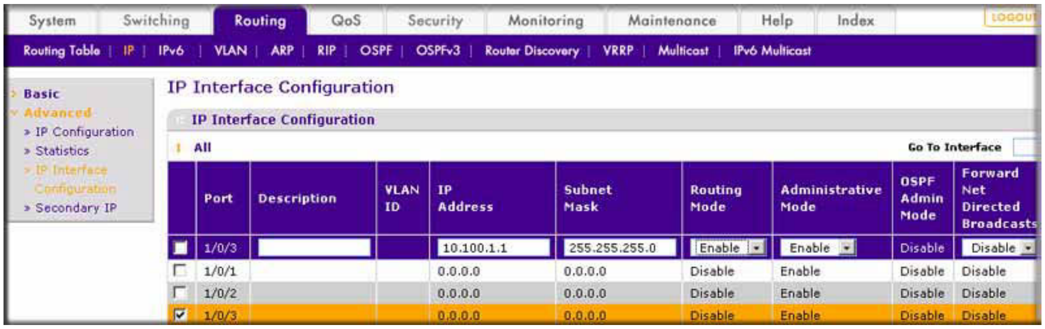
IP Configuration

Default Time to Live	64
Routing Mode	● Enable ○ Disable
ICMP Echo Replies	● Enable ○ Disable
ICMP Redirects	● Enable ○ Disable
ICMP Rate Limit Interval	1000 (0 to 2147483647 ms)
ICMP Rate Limit Burst Size	100 (1 to 200)
Maximum Next Hops	4

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

2. Create a routing interface and assign 10.100.1.1/24 to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuratio**n.

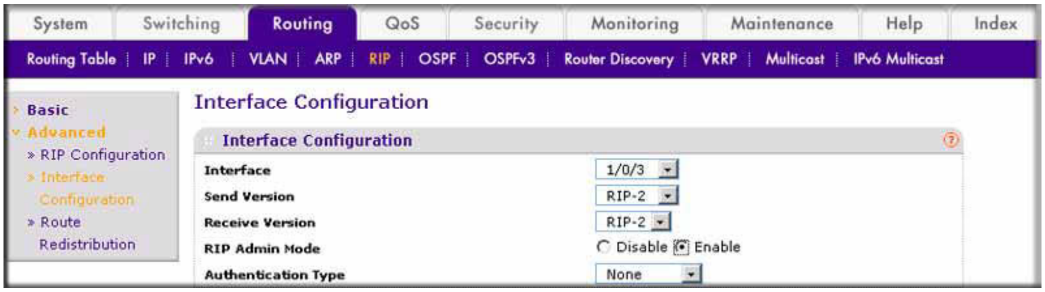
      A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
LOGOUT
Routing Table | IP | IPv6 | VLAN | ARP | RIP | OSPF | OSPFv3 | Router Discovery | VRRP | Multicast | IPv6 Multicast
Basic
Advanced
IP Configuration
Statistics
IP Interface Configuration
Secondary IP
IP Interface Configuration
IP Interface Configuration
All
Go To Interface

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode	OSPF Admin Mode	Forward Net Directed Broadcasts
□	1/0/3			10.100.1.1	255.255.255.0	Enable	Enable	Disable	Disable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable
□	1/0/2			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable
☑	1/0/3			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable

   b. Scroll down and select the **1/0/3** check box.
   c. In the **IP Address** field, enter **10.100.1.1**.
   d. In the **Subnet Mask** field, enter **255.255.255.0**.
   e. In the **Routing Mode** field, select **Enable**.
   f. Click **Apply** to save the settings.
3. Enable RIP on interface 1/0/3.
   a. Select **Routing > RIP >Advanced > Interface Configuration**.

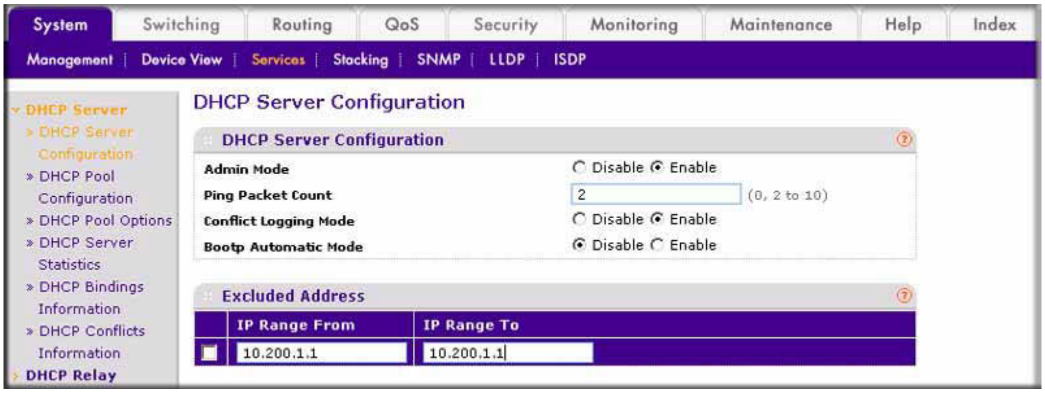
      A screen similar to the following displays.



Interface	1/0/3
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	None

   b. In the **Interface** field, select **1/0/3**.
   c. For RIP Admin Mode, select the **Enable** radio button.
   d. Click **Apply** to save the settings.
4. Set up the DHCP global configuration.
   a. Select **System > Services > DHCP Server > DHCP Server Configuration**.

A screen similar to the following displays.



DHCP Server Configuration

DHCP Server Configuration

Admin Mode	○ Disable ● Enable
Ping Packet Count	2 (0, 2 to 10)
Conflict Logging Mode	○ Disable ● Enable
Bootp Automatic Mode	● Disable ○ Enable

Excluded Address

	IP Range From	IP Range To
□	10.200.1.1	10.200.1.1

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

c. In the **IP Range From** field, enter **10.200.1.1**.

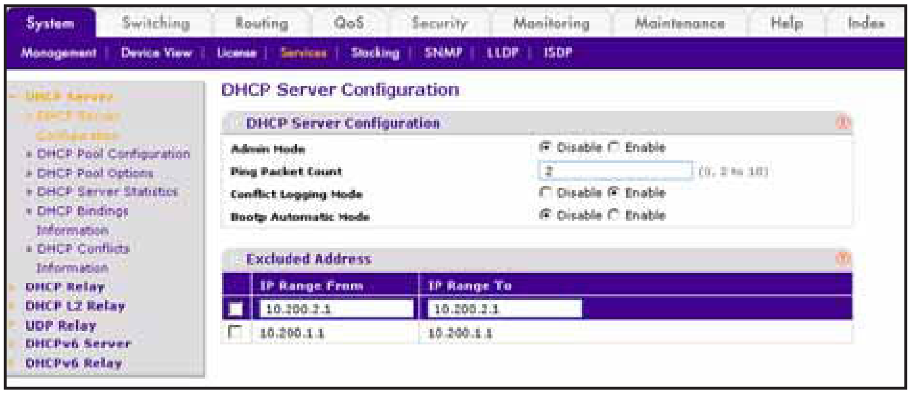
d. In the **IP Range To** field, enter **10.200.1.1**.

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:



DHCP Server Configuration

DHCP Server Configuration

Admin Mode	● Disable ○ Enable
Ping Packet Count	2 (0, 2 to 10)
Conflict Logging Mode	○ Disable ● Enable
Bootp Automatic Mode	● Disable ○ Enable

Excluded Address

	IP Range From	IP Range To
□	10.200.2.1	10.200.2.1
□	10.200.1.1	10.200.1.1

b. In the IP Range From field, enter **10.200.2.1**.

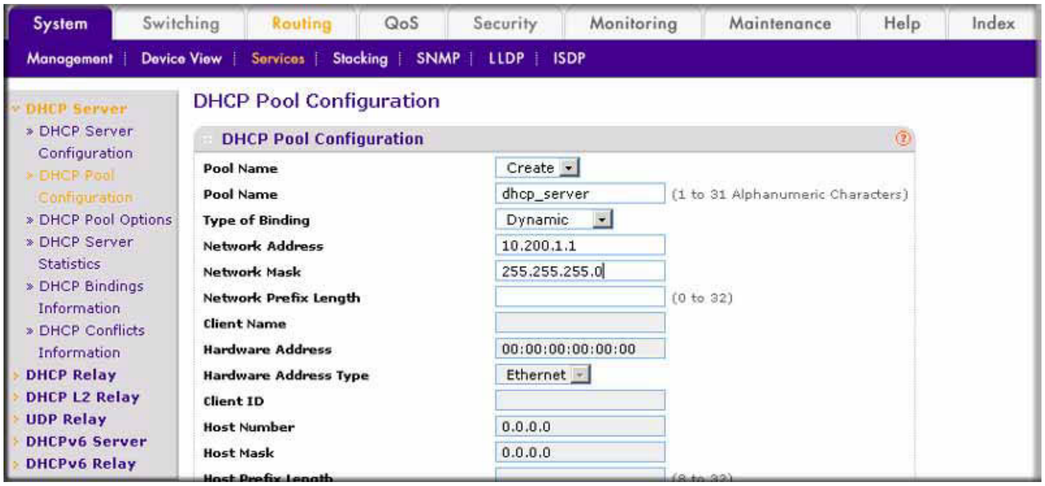
c. In the IP Range To field, enter **10.200.2.1**.

d. Click **Add**.

6. Create a DHCP pool named dhcp_server.

a. Select **System > Services > DHCP Server > DHCP Pool Configuration**.

A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Management | Device View | Services | Stacking | SNMP | LLDP | ISDP
DHCP Server
» DHCP Server Configuration
» DHCP Pool Configuration
» DHCP Pool Options
» DHCP Server Statistics
» DHCP Bindings Information
» DHCP Conflicts Information
DHCP Relay
DHCP L2 Relay
UDP Relay
DHCPv6 Server
DHCPv6 Relay

DHCP Pool Configuration

DHCP Pool Configuration

Pool Name	Create	
Pool Name	dhcp_server	(1 to 31 Alphanumeric Characters)
Type of Binding	Dynamic	
Network Address	10.200.1.1	
Network Mask	255.255.255.0	
Network Prefix Length		(0 to 32)
Client Name		
Hardware Address	00:00:00:00:00:00	
Hardware Address Type	Ethernet	
Client ID		
Host Number	0.0.0.0	
Host Mask	0.0.0.0	
Host Prefix Length		(8 to 32)

b. Under DHCP Pool Configuration, enter the following information:

- In the **Pool Name** list, select **Create**.
- In the **Pool Name** field, enter **dhcp_server**.
- In the **Type of Binding** list, select **Dynamic**.
- In the **Network Number** field, enter **10.200.1.0**.
- In the **Network Mask** field, enter **255.255.255.0**. As an alternate, you can enter **24** in the **Network Prefix Length** field.

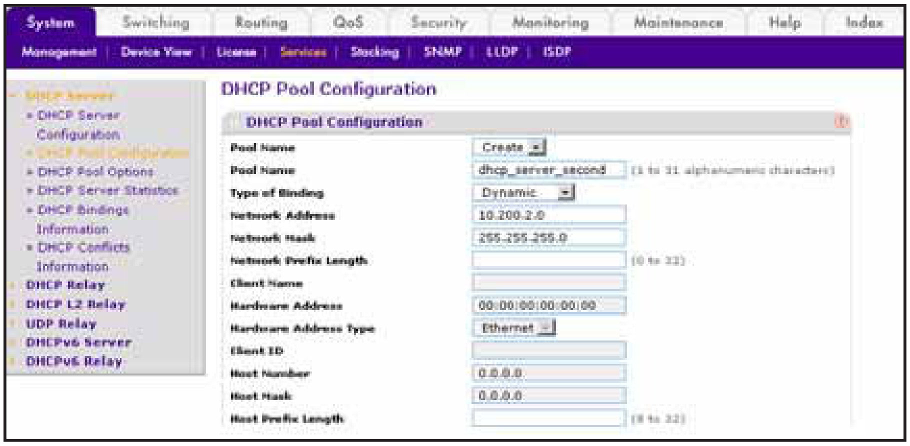
Note: Do not fill in the Network Mask field and Network Prefix Length field at the same time.

c. Click **Add**. The pool_dynamic name is now added to the **Pool Name** drop-down list.

7. Create a DHCP pool named dhcp_server_second.

a. Select **System > Services > DHCP Server > DHCP Pool Configuration**.

A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Management | Device View | License | Services | Stacking | SNMP | LLDP | ISDP
DHCP Server
» DHCP Server Configuration
» DHCP Pool Configuration
» DHCP Pool Options
» DHCP Server Statistics
» DHCP Bindings Information
» DHCP Conflicts Information
DHCP Relay
DHCP L2 Relay
UDP Relay
DHCPv6 Server
DHCPv6 Relay

DHCP Pool Configuration

DHCP Pool Configuration

Pool Name	Create	
Pool Name	dhcp_server_second	(1 to 31 alphanumeric characters)
Type of Binding	Dynamic	
Network Address	10.200.2.0	
Network Mask	255.255.255.0	
Network Prefix Length		(0 to 32)
Client Name		
Hardware Address	00:00:00:00:00:00	
Hardware Address Type	Ethernet	
Client ID		
Host Number	0.0.0.0	
Host Mask	0.0.0.0	
Host Prefix Length		(8 to 32)

b. Under DHCP Pool Configuration, enter the following information:
   - In the Pool Name list, select **Create**.
   - In the Pool Name field, enter **dhcp_server_second**.
   - In the Type of Binding list, select **Dynamic**.
   - In the Network Number field, enter **10.200.2.0**.
   - In the Network Mask field, enter **255.255.255.0**. As an alternate, you can enter **24** in the Network Prefix Length field.

c. Click **Add**. The dhcp_server_second name is now added to the Pool Name drop-down list.

Configure a DHCP L3 Switch

CLI: Configure a DHCP L3 Relay

1. Enable routing on the switch.

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

2. Create a routing interface and enable RIP on it.

```
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#routing
(Netgear Switch) (Interface 1/0/4)#ip address 10.100.1.2 255.255.255.0
(Netgear Switch) (Interface 1/0/4)#ip rip
(Netgear Switch) (Interface 1/0/4)#exit
```

3. Create a routing interface connecting to the client.

```
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#interface 1/0/16
(Netgear Switch) (Interface 1/0/16)#routing
(Netgear Switch) (Interface 1/0/16)#ip address 10.200.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/16)#exit
```

4. Configure the DHCP Server IP address and enable the DHCP L3 relay.

```
(Netgear Switch) (Config)#ip helper-address 10.100.1.1 dhcp
(Netgear Switch) (Config)#ip helper enable
```

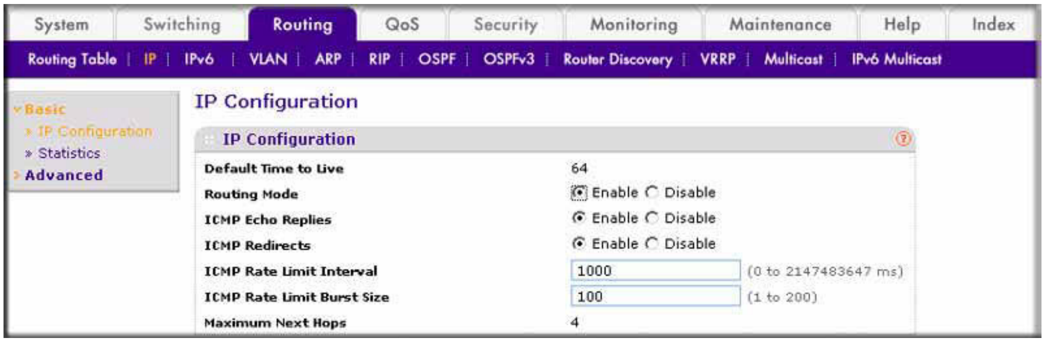
5. Redistribute 10.200.1.0/24 and 10.200.2.0/24 to the RIP such that RIP advertises this route to the DHCP server.

```
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#router rip
(Netgear Switch) (Config-router)#redistribute connected
(Netgear Switch) (Config-router)#exit
```

Web Interface: Configure a DHCP L3 Relay

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

      A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Routing Table | IP | IPv6 | VLAN | ARP | RIP | OSPF | OSPFv3 | Router Discovery | VRRP | Multicast | IPv6 Multicast
Basic
» IP Configuration
» Statistics
Advanced

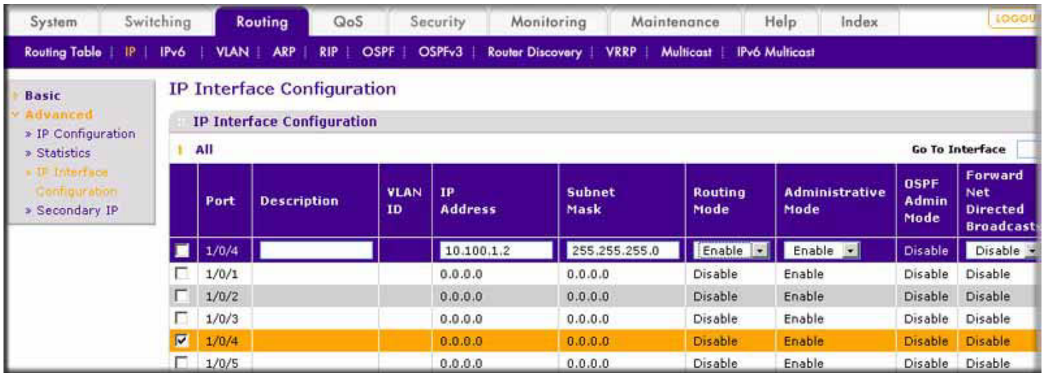
IP Configuration

IP Configuration

Default Time to Live	64
Routing Mode	● Enable ○ Disable
ICMP Echo Replies	● Enable ○ Disable
ICMP Redirects	● Enable ○ Disable
ICMP Rate Limit Interval	1000 (0 to 2147483647 ms)
ICMP Rate Limit Burst Size	100 (1 to 200)
Maximum Next Hops	4

   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply**.
2. 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.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
LOGOU
Routing Table | IP | IPv6 | VLAN | ARP | RIP | OSPF | OSPFv3 | Router Discovery | VRRP | Multicast | IPv6 Multicast
Basic
Advanced
» IP Configuration
» Statistics
» IP Interface Configuration
» Secondary IP
All
Go To Interface

IP Interface Configuration

IP Interface Configuration

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode	OSPF Admin Mode	Forward Net Directed Broadcast
□	1/0/4			10.100.1.2	255.255.255.0	Enable	Enable	Disable	Disable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable
□	1/0/2			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable
□	1/0/3			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable
☑	1/0/4			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable
□	1/0/5			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable

   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**.

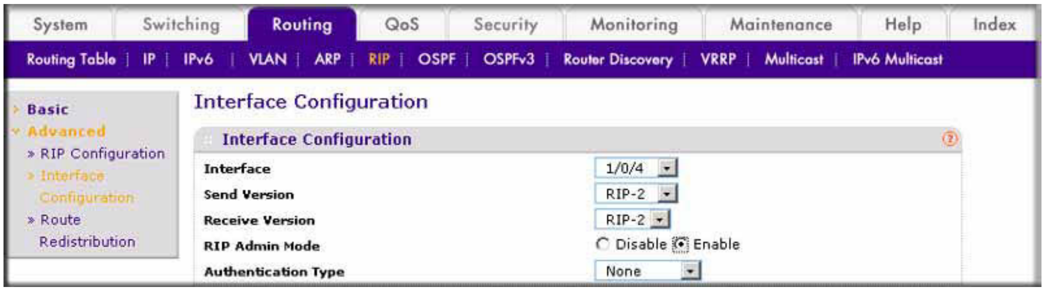
e. In the **Routing Mode** field, select **Enable**.

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

Interface Configuration

Interface	1/0/4
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	None

   b. In the **Interface** list, select **1/0/4**.

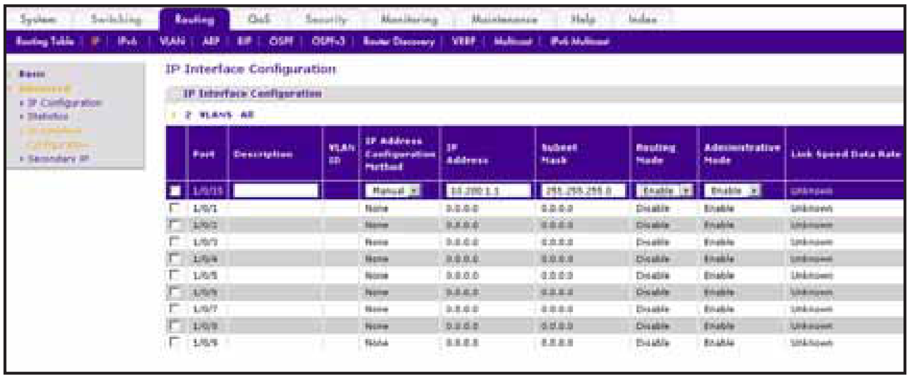
   c. For RIP Admin Mode, select the **Enable** radio button.

   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.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Routing Table | IP | IPv6 | VLAN | ARP | RIP | OSPF | OSPFv3 | Router Discovery | VRRP | Multicast | IPv6 Multicast
Basic
Advanced
IP Configuration
Statistics
IP Interface Configuration
Secondary IP

IP Interface Configuration

IP Interface Configuration

2 VLANS All

	Port	Description	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Routing Mode	Administrative Mode	Link Speed Data Rate
☑	1/0/15			Manual	10.200.1.1	255.255.255.0	Enable	Enable	Unknown
□	1/0/1			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
□	1/0/2			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
□	1/0/3			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
□	1/0/4			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
□	1/0/5			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
□	1/0/6			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
□	1/0/7			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
□	1/0/8			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
□	1/0/9			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown

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

   c. In the **IP Address Configuration Method** field, enter **Manual**.

   d. In the **IP Address** field, enter **10.200.1.1**.

   e. In the **Subnet Mask** field, enter **255.255.255.0**.

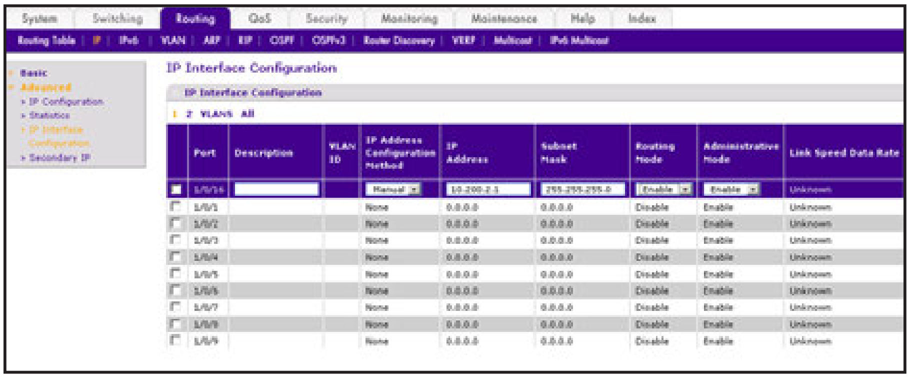
   f. In the **Routing Mode** field, select **Enable**.

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

5. Create a routing interface and assign 10.200.2.1/24 to it.

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

A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Routing Table | IP | IPv6 | VLAN | ARP | RIP | OSPF | OSPFv3 | Router Discovery | VRRP | Multicast | IPv6 Multicast
Basic
Advanced
IP Configuration
Statistics
IP Interface Configuration
Secondary IP

IP Interface Configuration

IP Interface Configuration

1 2 VLANS All

	Port	Description	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Routing Mode	Administrative Mode	Link Speed Data Rate
☑	1/0/16			Manual	10.200.2.1	255.255.255.0	Enable	Enable	Unknown
□	1/0/1			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
□	1/0/2			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
□	1/0/3			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
□	1/0/4			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
□	1/0/5			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
□	1/0/6			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
□	1/0/7			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
□	1/0/8			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown
□	1/0/9			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown

b. Under IP Interface Configuration, scroll down and select the Port **1/0/16** check box.

c. In the IP Address Configuration Method field, enter **Manual**.

d. In the IP Address field, enter **10.200.2.1**.

e. In the Subnet Mask field, enter **255.255.255.0**.

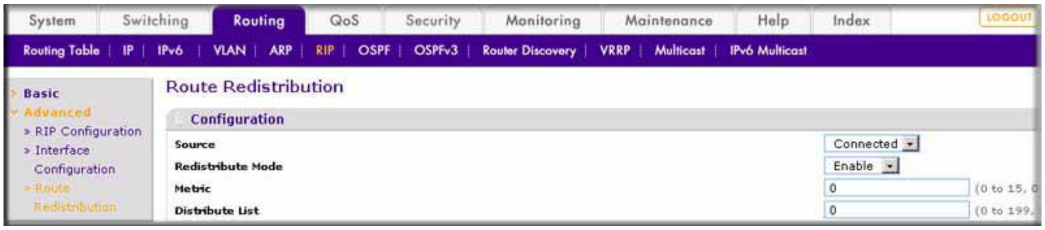
f. In the Routing Mode field, select **Enable**.

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

6. Redistribute the connected routes to RIP.

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

A screen similar to the following displays.



Route Redistribution

Configuration

Source	Connected	
Redistribute Mode	Enable	
Metric	0	(0 to 15, 0
Distribute List	0	(0 to 199,

b. In the **Source** field, select **Connected**.

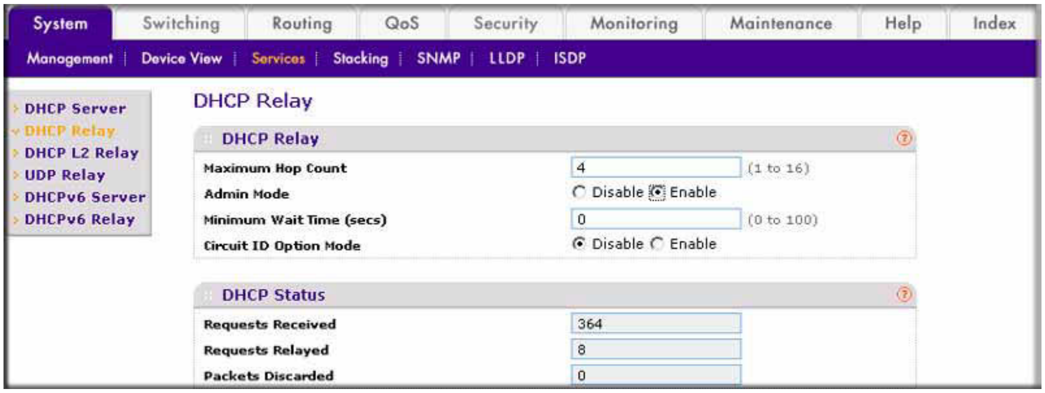
c. In the **Redistribute Mode** field, select **Enable**.

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.



DHCP Relay

DHCP Relay

Maximum Hop Count	4	(1 to 16)
Admin Mode	○ Disable ● Enable	
Minimum Wait Time (secs)	0	(0 to 100)
Circuit ID Option Mode	● Disable ○ Enable	

DHCP Status

Requests Received	364
Requests Relayed	8
Packets Discarded	0

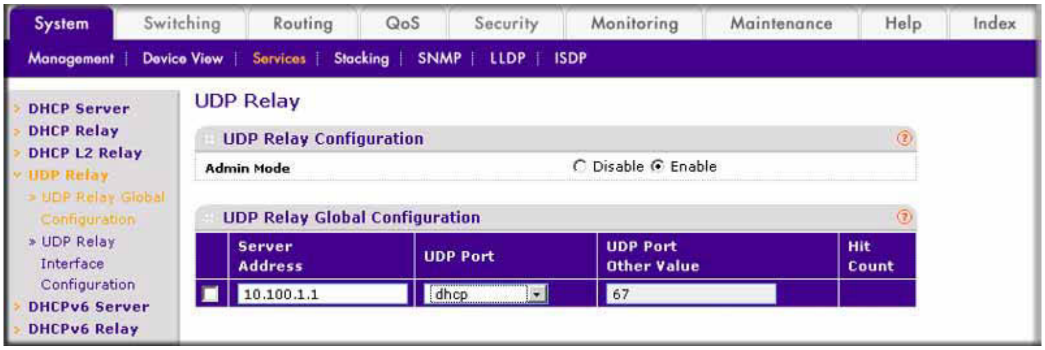
b. For Admin Mode, select the **Enable** radio button.

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

8. Configure the DHCP server IP address.

a. Select **System > Services > UDP Relay**.

A screen similar to the following displays.



UDP Relay

UDP Relay Configuration

Admin Mode ○ Disable ● Enable

UDP Relay Global Configuration

	Server Address	UDP Port	UDP Port Other Value	Hit Count
□	10.100.1.1	dhcp	67	

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.

22. MLD Snooping

Multicast Listener Discovery

22

This chapter includes the following sections:

Multicast Listener Discovery Concepts

Multicast Listener Discovery (MLD) protocol enables IPv6 routers to discover multicast listeners, the nodes that are configured to receive multicast data packets, on its directly attached interfaces. The protocol specifically discovers which multicast addresses are of interest to its neighboring nodes and provides this information to the active multicast routing protocol that 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.

MLD Snooping Concepts

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
```

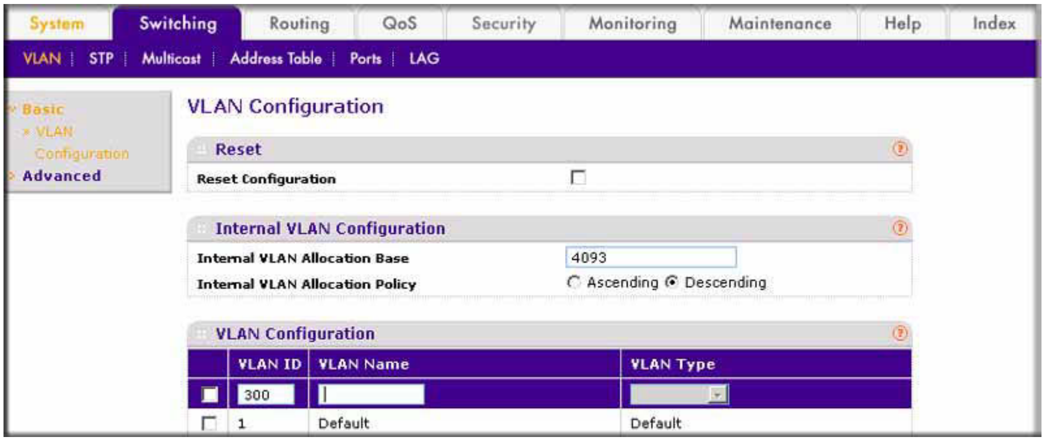
2. Enable MLD snooping on VLAN 300.

```
(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

Reset

Reset Configuration □

Internal VLAN Configuration

Internal VLAN Allocation Base 4093

Internal VLAN Allocation Policy ○ Ascending ● Descending

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type
□	300		
□	1	Default	Default

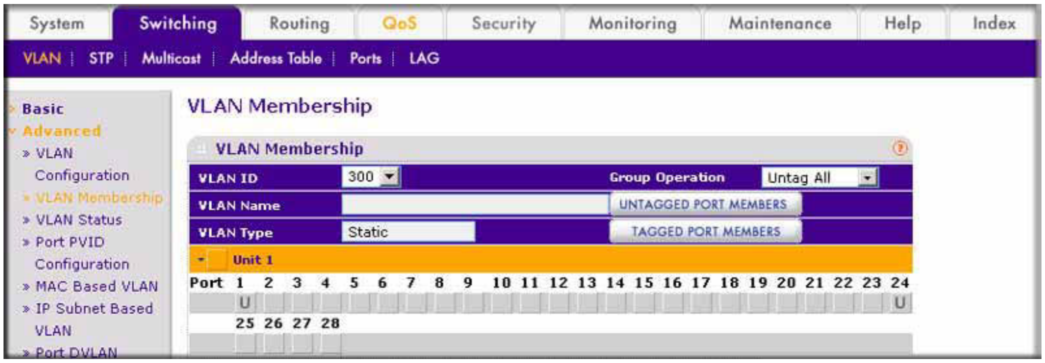
b. In the **VLAN ID** field, enter **300**.

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

VLAN ID 300 Group Operation Untag All

VLAN Name

VLAN Type Static

Unit 1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	U																							U
	25	26	27	28																				

b. In the **VLAN ID** list, select **300**.

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

d. Click the gray boxes under ports **1** and **24** until **U** displays.

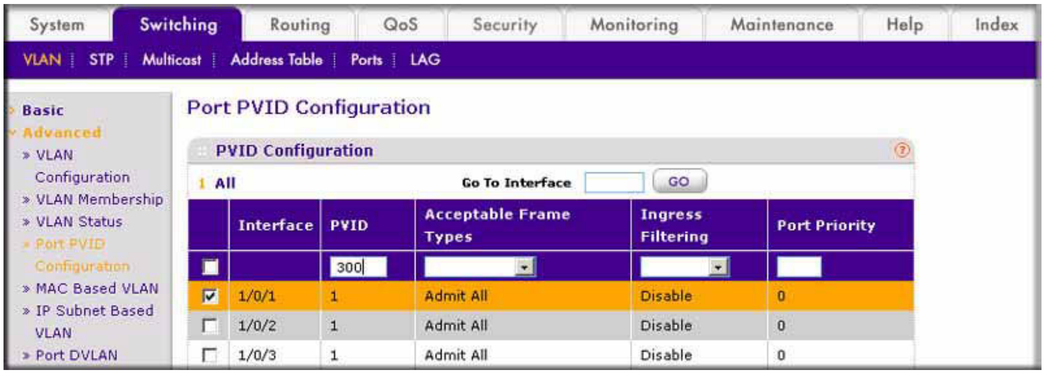
The U specifies that the egress packet is untagged for the port.

e. Click **Apply**.

3. Assign PVID to ports 1/0/1 and 1/0/24.

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

A screen similar to the following displays.



Port PVID Configuration

PVID Configuration

1 All Go To Interface

	Interface	PVID	Acceptable Frame Types	Ingress Filtering	Port Priority
☐		300			
☑	1/0/1	1	Admit All	Disable	0
☐	1/0/2	1	Admit All	Disable	0
☐	1/0/3	1	Admit All	Disable	0

b. Scroll down and select the interface **1/0/1** and 1/0/24 check boxes.

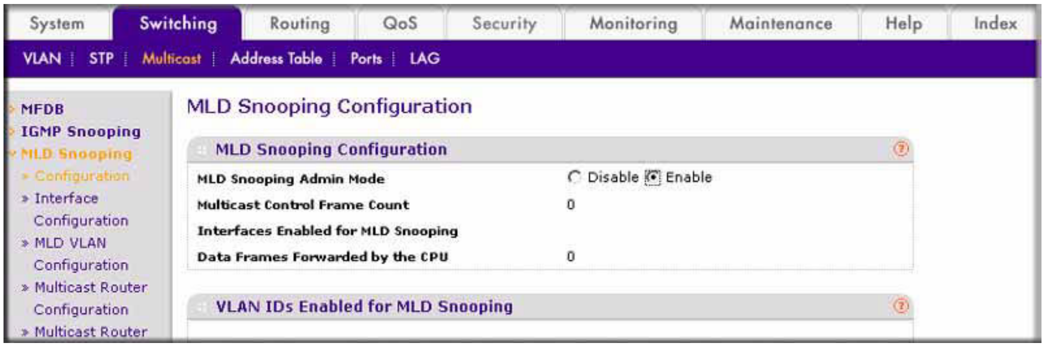
c. In the **PVID (1 to 4093)** field, enter **300**.

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.



MLD Snooping Configuration

MLD Snooping Configuration

MLD Snooping Admin Mode	○ Disable ● Enable
Multicast Control Frame Count	0
Interfaces Enabled for MLD Snooping	
Data Frames Forwarded by the CPU	0

VLAN IDs Enabled for MLD Snooping

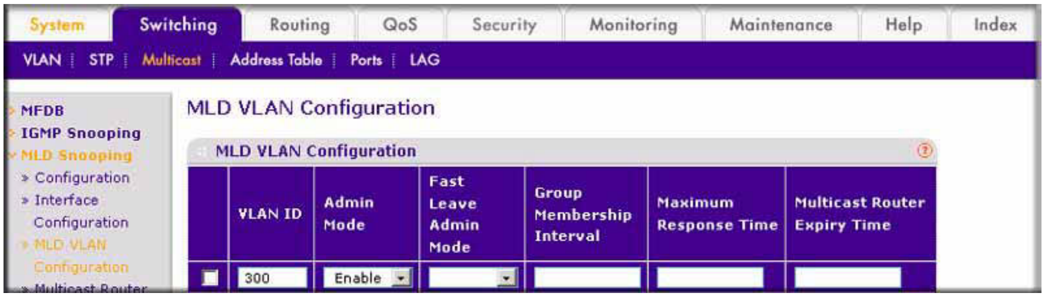
b. For MLD Snooping Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

5. Enable MLD snooping on the VLAN 300.

a. Select **Routing > Multicast > MLD Snooping > MLD VLAN Configuration**.

A screen similar to the following displays.



MLD VLAN Configuration

MLD VLAN Configuration

	VLAN ID	Admin Mode	Fast Leave Admin Mode	Group Membership Interval	Maximum Response Time	Multicast Router Expiry Time
☐	300	Enable				

b. Enter the following information:
   - In the **VLAN ID** field, enter **300**.
   - In the **Admin Mode** field, select **Enable**.

6. Click **Add**.

Index