NETGEAR Managed Switches Software Administration Manual, Release 8.0

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

202-10515-01
October 2009

Trademarks

NETGEAR and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc.. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders. Portions of this document are copyright Intoto, Inc.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Netgear's 7000 Series Managed Switch is compliant with the following EU Council Directives: 89/336/EEC and LVD 73/23/EEC. Compliance is verified by testing to the following standards: EN55022 Class A, EN55024 and EN60950-1.

Certificate of the Manufacturer/Importer

It is hereby certified that the 7000 Series Managed Switch has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

The Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das7000 Series Managed Switch gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class A category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas. When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

FCC Information to User

Declaration Of Conformity

We NETGEAR, Inc., 4500 Great America Parkway, Santa Clara, CA 95054, declare under our sole responsibility that the model 7000 Series Managed Switch complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and

- This device must accept any interference received, including interference that may cause undesired operation.

FCC Requirements for Operation in the United States

Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and the receiver
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected
- Consult the dealer or an experienced radio/TV technician for help.

7000 Series Managed Switch

Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE

Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (7000 Series Managed Switch) does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Product and Publication Details

Model Number:	7xxx
Publication Date:	October 2009
Product Family:	Managed Switch
Product Name:	7000 Series Managed Switch
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10515-01
Publication Version Number:	1.0

Contents

About This Manual

Chapter 1
Getting Started

Chapter 2
Auto Install Configuration

Chapter 3
Virtual LANs

Chapter 9
Proxy Address Resolution Protocol (ARP)

Chapter 10
Virtual Router Redundancy Protocol

Chapter 11
Access Control Lists (ACLs)

Chapter 12
Class of Service (CoS) Queuing

Chapter 13
Differentiated Services

Chapter 14
IGMP Snooping and Querier

Chapter 15
Security Management

Chapter 16
Simple Network Time Protocol (SNTP)

Chapter 17
Tools

Chapter 18
Syslog

Chapter 19
Managing Switch Stacks

Chapter 20
SNMP

Chapter 21
DNS

Chapter 32
Captive Portal

About This Manual

The *NETGEAR® Managed Switches Software Administration Manual, Release 8.0* describes how to install, configure and troubleshoot the 7000 Series Managed Switch. The information in this manual is intended for readers with intermediate computer and Internet skills.

Note: Product updates are available on the NETGEAR website at *http://kbserver.netgear.com*.

Conventions, Formats, Scope, and Audience

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical Conventions**. This manual uses the following typographical conventions

Italic	Emphasis, books, CDs, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
`Fixed`	Command prompt, CLI text, code
italic	URL links

- **Formats**. This manual uses the following formats to highlight special messages:

Note: This format is used to highlight information of importance or special interest.

Tip: This format is used to highlight a procedure that will save time or resources.

- **Scope**. This manual is written for the 7000 Series Managed Switch according to these specifications:.

Product Version	7000 Series Managed Switch
Manual Publication Date	October 2009

This document provides examples of the use of the switch software in a typical network. It describes the use and advantages of specific functions provided by the 7000 Series Managed Switch, and includes information on configuring those functions using the Command Line Interface and Web Interface.

The switch software can operate as a Layer 2 switch, a Layer 3 router, or a combination switch/router. The switch also includes support for network management and Quality of Service functions such as Access Control Lists and Differentiated Services. Which functions you choose to activate will depend on the size and complexity of your network: this document describes configuration for some of the most-used functions.

- **Audience**. Use this guide if you are a(n):
  - Experienced system administrator who is responsible for configuring and operating a network using switch software
  - Level 1 and Level 2 support provider

To obtain the greatest benefit from this guide, you should have an understanding of the switch software base and should have read the specification for your networking device platform. You should also have a basic knowledge of Ethernet and networking concepts.

Additional Documentation

Before proceeding, read the Release Notes for this switch product. The Release Notes detail the platform specific functionality of the Switching, Routing, SNMP, Config, Management, and other packages. In addition, see the following publications:

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

These documents may be found at *http://www.NETGEAR.com*.

How to Print This Manual

To print this manual, your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Revision History

Part Number	Version Number	Description
202-10515-01	1.0	Product update: New firmware and new user Interface

Chapter 1
Getting Started

Connect a terminal to the switch to begin configuration.

In-band and Out-of-band Connectivity

Ask the system administrator to determine whether you will configure the switch for in-band or out-of-band connectivity.

Configuring for In-band Connectivity

In-band connectivity allows you to access the switch from a remote workstation using the Ethernet network. To use in-band connectivity, you must configure the switch with IP information (IP address, subnet mask, and default gateway).

Configure for In-band connectivity using one of the following methods:

- BootP or DHCP
- EIA-232 port

Using BootP or DHCP

You can assign IP information initially over the network or over the Ethernet service port through BootP or DHCP. Check with your system administrator to determine whether BootP or DHCP is enabled.

You need to configure the BootP or DHCP server with information about the switch—obtain this information through the serial port connection using the **show network** command. Set up the server with the following values:

IP Address Unique IP address for the switch. Each IP parameter is made up of four decimal numbers, ranging from 0 to 255. If there is no DHCP server available to assign an IP address to the switch via DHCP, the default IP address for the switch is 169.254.100.100.

Subnet Subnet mask for the LAN

gateway IP address of the default router, if the switch is a node outside the IP range of the LAN

MAC Address MAC address of the switch

When you connect the switch to the network for the first time after setting up the BootP or DHCP server, it is configured with the information supplied above. The switch is ready for in-band connectivity over the network.

If you do not use BootP or DHCP, access the switch through the EIA-232 port, and configure the network information as described below.

Using the EIA-232 Port

You can use a locally or remotely attached terminal to configure in-band management through the EIA-232 port.

1. To use a locally attached terminal, attach one end of a null-modem serial cable to the EIA-232 port of the switch and the other end to the COM port of the terminal or workstation.
For remote attachment, attach one end of the serial cable to the EIA-232 port of the switch and the other end to the modem.

2. Set up the terminal for VT100 terminal emulation.

a. Set the terminal ON.

b. Launch the VT100 application.

3. Configure the COM port as follows:

a. Set the data rate to 9600 baud.

b. Set the data format to 8 data bits, 1 stop bit, and no parity.

c. Set the flow control to none.

d. Select the proper mode under **Properties**.

e. Select Terminal keys.

The Log-in User prompt displays when the terminal interface initializes.

4. Enter an approved user name and password. The default is *admin* for the user name and the *password* is blank.

The switch is installed and loaded with the default configuration.

5. Reduce network traffic by turning off the Network Configuration Protocol. Enter the following command:

```
configure network protocol none
```

6. Set the IP address, subnet mask, and gateway address by issue the following command:

```
config network parms ipaddress netmask gateway
```

IP Address Unique IP address for the switch. Each IP parameter is made up of four decimal numbers, ranging from 0 to 255. The default IP address is 169.254.100.100.

Subnet	Subnet mask for the LAN. The default value is 255.255.255.0.
gateway	IP address of the default router, if the switch is a node outside the IP range of the LAN.

7. To enable these changes to be retained during a reset of the switch, type **Ctrl-Z** to return to the main prompt, type **save** at the main menu prompt, and type **y** to confirm the changes.
8. To view the changes and verify in-band information, issue the command: **show network**.
9. The switch is configured for in-band connectivity and ready for Web-based management.

Configuring for Out-Of-Band Connectivity

To monitor and configure the switch using out-of-band connectivity, use the console port to connect the switch to a terminal desktop system running terminal emulation software. The console port connector is a male DB-9 connector, implemented as a data terminal equipment (DTE) connector.

The following hardware is required to use the console port:

- VT100-compatible terminal, or a desktop, or a portable system with a serial port running VT100 terminal emulation software.
- An RS-232 crossover cable with a female DB-9 connector for the console port and the appropriate connector for the terminal.

Perform the following tasks to connect a terminal to the switch console port using out-of-band connectivity:

1. Connect an RS-232 crossover cable to the terminal running VT100 terminal emulation software.
2. Configure the terminal emulation software as follows:
   a. Select the appropriate serial port (serial port 1 or serial port 2) to connect to the console.
   b. Set the data rate to 9600 baud.
   c. Set the data format to 8 data bits, 1 stop bit, and no parity.
   d. Set the flow control to none.
   e. Select the proper mode under **Properties**.
   f. Select Terminal keys.

> **Note:** When using HyperTerminal with Microsoft Windows 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. With Windows 2000 Service Pack 2, the arrow keys function properly in HyperTerminal's VT100 emulation. Go to *www.microsoft.com* for more information on Windows 2000 service packs.

3. Connect the female connector of the RS-232 crossover cable directly to the switch console port, and tighten the captive retaining screws.

Starting the Switch

1. Make sure that the switch console port is connected to a VT100 terminal or VT100 terminal emulator via the RS-232 crossover cable.
2. Locate an AC power receptacle.
3. Deactivate the AC power receptacle.
4. Connect the switch to the AC receptacle.
5. Activate the AC power receptacle.

When the power is turned on with the local terminal already connected, the switch goes through a power-on self-test (POST). POST runs every time the switch is initialized and checks hardware components to determine if the switch is fully operational before completely booting. If POST detects a critical problem, the startup procedure stops. If POST passes successfully, a valid executable image is loaded into RAM. POST messages are displayed on the terminal and indicate test success or failure. The boot process runs for approximately 60 seconds.

Initial Configuration

The initial simple configuration procedure is based on the following assumptions:

- The switch was not configured before and is in the same state as when you received it.
- The switch booted successfully.
- The console connection was established and the console prompt appears on the screen of a VT100 terminal or terminal equivalent.

The initial switch configuration is performed through the console port. After the initial configuration, you can manage the switch either from the already-connected console port or remotely through an interface defined during the initial configuration.

The switch is not configured with a default user name and password.

All of the settings below are necessary to allow the remote management of the switch through Telnet (Telnet client) or HTTP (Web browser).

Before setting up the initial configuration of the switch, obtain the following information from your network administrator:

- The IP address to be assigned to the management interface through which the switch is managed.
- The IP subnet mask for the network.
- The IP address of the default gateway.

Initial Configuration Procedure

You can perform the initial configuration using the Easy Setup Wizard or by using the Command Line Interface (CLI). The Setup Wizard automatically starts when the switch configuration file is empty. You can exit the wizard at any point by entering [ctrl+z]. For more information on CLI initial configuration, see the *User's Configuration Guide*. This guide shows how to use the Setup Wizard for initial switch configuration. The wizard sets up the following configuration on the switch:

- Establishes the initial privileged user account with a valid password. The wizard configures one privileged user account during the set up.
- Enables CLI login and HTTP access to use the local authentication setting only.
- Sets up the IP address for the management interface.
- Sets up the SNMP community string to be used by the SNMP manager at a given IP address. You may choose to skip this step if SNMP management is not used for this switch.
- Allows you to specify the management server IP or permit SNMP access from all IP addresses.
- Configures the default gateway IP address.

Software Installation

This section contains procedures to help you become acquainted quickly with the switch software. Before installing switch software, you should verify that the switch operates with the most recent firmware.

Quick Starting the Networking Device

1. Configure the switch for In-band or Out-of-Band connectivity. In-band connectivity allows access to the software locally or from a remote workstation. You must configure the device with IP information (IP address, subnet mask, and default gateway).
2. Turn the Power ON.
3. Allow the device to load the software until the login prompt appears. The device initial state is called the default mode.
4. When the prompt asks for operator login, do the following steps:
   - Type **`admin`** at the login prompt. Since a number of the Quick Setup commands require administrator account rights, log in to an administrator account.
   - Do not enter a password because the default mode does not use a password.
   - Check the CLI User EXEC prompt is displayed.
   - Enter **`enable`** to switch to the Privileged EXEC mode from User EXEC.
   - Enter **`configure`** to switch to the Global Config mode from Privileged EXEC.
   - Enter **`exit`** to return to the previous mode.

– Enter **?** to show a list of commands that are available in the current mode.

System Information and System Setup

This section describes the commands you use to view system information and to setup the network device. Table 1-1 contains the Quick Start commands that allow you to view or configure the following information:

- Software versions
- Physical port data
- User account management
- IP address configuration
- Uploading from Networking Device to Out-of-Band PC (Only XMODEM)
- Downloading from Out-of-Band PC to Networking Device (Only XMODEM)
- Downloading from TFTP Server
- Restoring factory defaults

If you configure any network parameters, you should execute the following command:

```
copy system:running-config nvram:startup-config
```

This command saves the changes to the configuration file. You must be in the correct mode to execute the command. If you do not save the configuration, all changes are lost when a you power down or reset the networking device. In a stacking environment, the running configuration is saved in all units of the stack.

Table 1-1 describes the command syntax, the mode you must be in to execute the command, and the purpose and output of the command.

Table 1-1. Quick Start Commands

Command	Mode	Description
show hardware	Privileged EXEC	Shows hardware version, MAC address, and software version information.
show users	Privileged EXEC	Displays all of the users that are allowed to access the networking device. Access Mode shows whether you can change parameters on the networking device (Read/Write) or can only view them (Read Only). As a factory default, the ‘admin’ user has Read/Write access and the ‘guest’ user has Read Only access. There can only be one Read/Write user. There can be up to five Read Only users.
show loginsession	User EXEC	Displays all of the login session information.

Table 1-1. Quick Start Commands (continued)

Command	Mode	Description
users passwd *<username>*	Global Config	Allows the user to set passwords or change passwords needed to login. A prompt appears after the command is entered requesting the users old password. In the absence of an old password leave the area blank. User password should not be more than eight characters in length.
copy system:running-config nvram:startup-config	Privileged EXEC	Saves passwords and all other changes to the device. If you do not save the configuration, all changes are lost when you power down or reset the networking device. In a stacking environment, the running configuration is saved in all units of the stack.
logout	User EXEC Privileged EXEC	Logs the user out of the networking device.
show network	User EXEC	Displays the following network configuration information: • IP Address - IP Address of the interface (default: 0.0.0.0) • Subnet Mask - IP Subnet Mask for the interface (default: 0.0.0.0) • Default Gateway - The default Gateway for this interface (default: 0.0.0.0) • IPv6 Administrative Mode - Indicates whether IPv6 is enabled. • IPv6 Prefix is - The prefix/prefix length of the IPv6 address. • Burned in MAC Address - The Burned in MAC Address used for in-band connectivity • Locally Administered MAC Address - Can be configured to allow a locally administered MAC address • MAC Address Type - Specifies which MAC address should be used for in-band connectivity • Network Configurations Protocol Current - Indicates which network protocol is being used (default: none) • Configured IPv6 Protocol - Indicates which network protocol is being used (default: none) for IPv6. • Management VLAN Id - Specifies VLAN id
network parms *<ipaddr> <netmask> [gateway]*	Privileged EXEC	Sets the IP address, subnet mask and gateway of the router. The IP address and the gateway must be on the same subnet. IP address range is from 0.0.0.0 to 255.255.255.255.

Table 1-1. Quick Start Commands (continued)

Command	Mode	Description
`copy nvram:startup-config`	Privileged EXEC	Starts the configuration file upload, displays the mode and type of upload and confirms the upload is progressing. The URL must be specified as: `xmodem:<filepath>/<filename>` For example: If the user is using HyperTerminal, the user must specify where the file is going to be received by the PC.
`copy nvram:errorlog`	Privileged EXEC	Starts the error log upload, displays the mode and type of upload and confirms the upload is progressing. The URL must be specified as: `xmodem:<filepath>/<filename>`
`copy nvram:traplog`	Privileged EXEC	Starts the trap log upload, displays the mode and type of upload and confirms the upload is progressing. The URL must be specified as: `xmodem:<filepath>/<filename>`
`copy nvram:startup-config`	Privileged EXEC	Sets the destination (download) datatype to be an image (system:image) or a configuration file (nvram:startup-config). The URL must be specified as: `xmodem:<filepath>/<filename>` For example: If the user is using Hyper Terminal, the user must specify which file is to be sent to the networking device. The Networking Device restarts automatically once the code has been downloaded.
`copy system:image`	Privileged EXEC	Sets the destination (download) datatype to be an image (system:image) or a configuration file (nvram:startup-config). The URL must be specified as: `xmodem:<filepath>/<filename>`
`copy nvram:startup-config`	Privileged EXEC	Sets the destination (download) datatype to be a configuration file. The URL must be specified as: `tftp://<ipaddress>/<filepath>/<filename>` Before starting a TFTP server download, you must configure the IP address.
`copy system:image`	Privileged EXEC	Sets the destination (download) datatype to be an image. The URL must be specified as: `tftp://<ipaddress>/<filepath>/<filename>` The `system:image` option downloads the code file.
`clear config`	Privileged EXEC	Enter yes when the prompt asks if you want to clear all the configurations made to the networking device.

Table 1-1. Quick Start Commands (continued)

Command	Mode	Description
`copy system:running-config nvram:startup-config`	Privileged EXEC	Enter yes when the prompt asks if you want to save the configurations made to the networking device.
`reload` `(or cold boot the networking device)`	Privileged EXEC	Enter yes when the prompt asks if you want to reset the system. You can reset the networking device or cold boot the networking device. Both work effectively.

Loading Firmware Using the Boot Menu

This section contains procedures to help you load firmware using utility menu in case the switch fails to boot up normally and unable to login the CLI User EXEC prompt , that means you cannot use the CLI command to download the new firmware to the switch. 8.0 supports load firmware by xmodem and USB. USB is new feature in 8.0 and it downloads firmware more quickly than does xmodem.

➡ **Note:** The following is only be operated through serial port

1. Power cycle the switch , the following message displays:

```
NetGear Boot code......
Version 01.00.18 06-24-2009
CPU Card ID: 0x508541
Select an option. If no selection in 10 seconds then
operational code will start.
1 - Start operational code.
2 - Start Boot Menu.
Select (1, 2):2
```

2. Enter **2** when you see **Select(1,2):** to display the Boot Menu as well.

```
Boot Menu
Options available
1 - Start operational code
```

```
2  - Change baud rate
3  - Retrieve event log using XMODEM
4  - Load new operational code using XMODEM
5  - Load new operational code using USB
6  - Display operational code vital product data
7  - Run flash diagnostics
8  - Update boot code
9  - Delete backup image
10 - Reset the system
11 - Restore configuration to factory defaults (delete config
files)
12 - Activate Backup Image
13 - Password Recovery Procedure
```

3. If you prefer xmodem, enter **2** in the [Boot Menu] prompt to change the baud rate such that xmodem uses higher rate to transfer data.
4. After that, enter **4** to select xmodem mode.
5. Transfer the firmware through Hyper Terminal on your PC.
6. If you prefer USB, make sure a USB flash is inserted into the USB interface on switch.
7. Enter **5** to select the USB mode, it will ask you to enter file name on USB flash.

   Enter the file name on USB Flash drive '/bd0/filename'):
8. Enter the file name you want to download, e.g. /bd0/ gsm73xxSv2-8.0.0.10.stk, after that it will start to copy that file from USB flash to switch.

Using Ezconfig for Switch Setup

Ezconfig is an interactive utility that provides a simplified procedure for setting up the following switch parameters:

- Switch management IP address
- Switch admin user password
- Switch name and location

Ezconfig can be entered either in Global Config mode (#) or in Display mode (>).

The utility displays the following text when you enter the **`ezconfig`** command

```
(FSM7352S) >ezconfig

NETGEAR EZ Configuration Utility
--------------------------------
Hello and Welcome!
This utility will walk you through assigning the IP address for the switch
management CPU. It will allow you to save the changes at the end. After the
session, simply use the newly assigned IP address to access the Web GUI using
any public domain Web browser.

Admin password not defined. Do you want to change the password? (Y/N/Q)
```

Note: At any point in the setup, you can type **`Q`** to abort the program. At this point, *Ezconfig* will check if there is any change, and prompt you if the changes should be saved.

Changing the Password

The first question it will ask is whether you wish to change the admin password. For security reasons, you should change the password by typing **`Y`**. If you have already set the password and do not wish to change it again, just enter **`N`**.

```
Enter new password:********
Confirm new password:********
Password Changed!

The 'enable' password required for switch configuration via the command line
interface is currently not configured. Do you wish to change it (Y/N/Q)?  y

Enter new password:********
Confirm new password:********
Password Changed!
```

Setting Up the Switch IP Address

After the password for both Admin and Enable mode is changed, you will be prompted to setup the IP address of the switch.

```
Assigning an IP address to your switch management

Current IP Address Configuration
--------------------------------
IP address: 0.0.0.0
Subnet mask: 0.0.0.0

Would you like to assign an IP address now (Y/N/Q)?  y

IP Address:
```

Ezconfig will display the current IP address and subnet mask. By default, the network management IP address uses DHCP protocol to have a DHCP server assign its IP address automatically. However, you can overwrite the DHCP client mode by assigning a fixed IP address here. Once a fixed IP address is assigned, *Ezconfig* automatically disables DHCP client mode and assigns the static IP address to the management VLAN.

If an IP address is already assigned, and you do not wish to change the IP address again, simply type **`N.`**

Assigning Switch Name and Location Information

Ezconfig will proceed to the next step in the setup:

```
Do you want to assign switch name and location information (Y/N/Q)?

System Name: Alpha1-1
System Location: Bld1
System Contact: James

There are changes detected, do you wish to save the changes permanently (Y/N)?
```

Note: The System Name, System Location and System Contact fields accept only alphanumeric characters, characters like "#$…" are not supported. The maximum length of the value cannot be longer than 31 bytes.

Saving the Configuration

After the name and location values are entered, *Ezconfig* will ask if you would like to have the changes be saved into the Flash (permanently storage). Enter **Y** to save the configuration.

```
There are changes detected, do you wish to save the changes permanently (Y/N)?
y

The configuration changes have been saved successfully.
Please enter 'show running-config' to see the final configuration.

Thanks for using EzConfig!
```

If during the session, the switch loses its power, the setup information will be lost if *Ezconfig* does not have the chance to save the changes before power-down.

Using the Web Interface

This chapter is a brief introduction to the web interface; for example, it explains how to access the Web-based management panels to configure and manage the system.

Tip: Use the Web interface for configuration instead of the CLI. Web configuration is quicker and easier than entering the multiple required CLI commands. There are equivalent functions in the Web interface and the terminal interface—that is, both applications usually employ the same menus to accomplish a task. For example, when you log in, there is a main menu with the same functions available.

You can manage your switch through a Web browser and Internet connection. This is referred to as Web-based management. To use Web-based management, the system must be set up for in-band connectivity.

To access the switch, the Web browser must support:

- HTML version 4.0, or later
- HTTP version 1.1, or later
- JavaScript™ version 1.2, or later

There are several differences between the Web and terminal interfaces. For example, on the Web interface the entire forwarding database can be displayed, while the terminal interface only displays 10 entries starting at specified addresses.

To terminate the Web login session, close the web browser.

Configuring for Web Access

To enable Web access to the switch:

1. Configure the switch for in-band connectivity. The switch *Getting Started Guide* provides instructions.

2. Enable Web mode:

   a. At the CLI prompt, enter the **show network** command.

   b. Set **Web Mode** to Enabled.

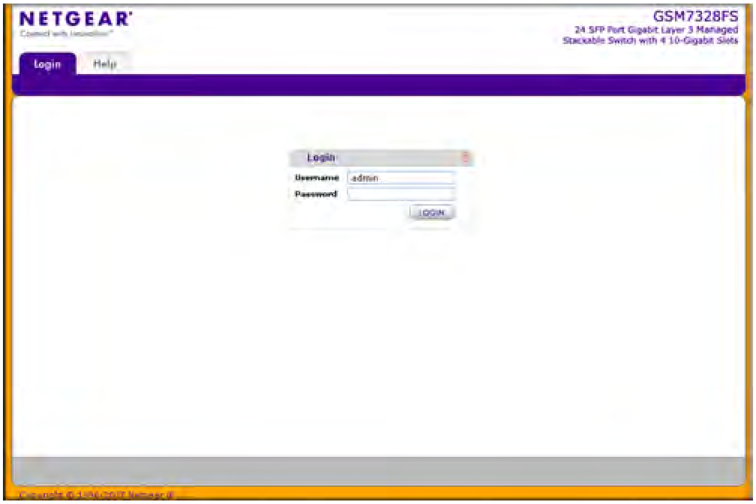
Starting the Web Interface

Follow these steps to start the switch Web interface:

1. Enter the IP address of the switch in the Web browser address field.
2. When the Login panel is displayed click **Login**.
3. Enter the appropriate user name and password. The user name and associated password are the same as those used for the terminal interface. Click the **Login** button.
4. The System Description Menu displays, with the navigation tree appearing to the left of the screen.
5. Make a selection by clicking on the appropriate item in the navigation tree.

Web Interface Layout

The Web interface is called the Prosafe Control Center (PCC). When you use the switch's IP address to log into the switch, the following screen displays:



Username admin

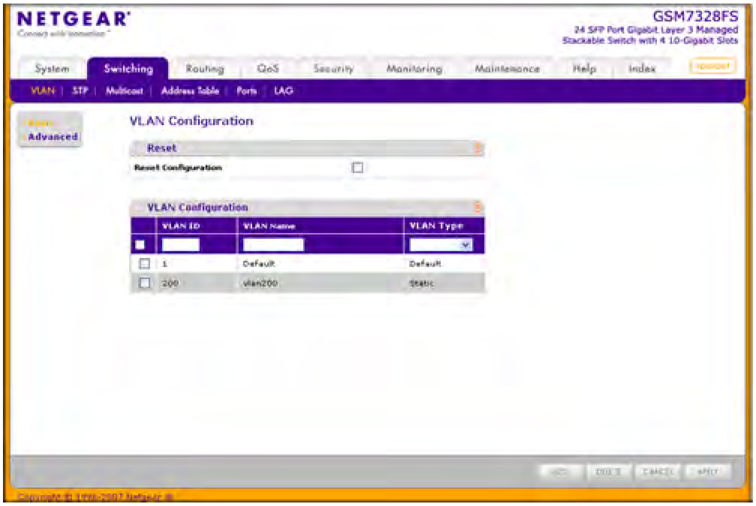
Password

NETGEAR
Connect with Innovation™
GSM7328FS
24 SFP Port Gigabit Layer 3 Managed
Stackable Switch with 4 10-Gigabit Slots
Login
Help
Login
LOGIN
Copyright © 1996-2007 Netgear ®

Figure 1-1

The switch can accommodate two types of users: administrative users and guests. An administrative user may configure the switch for network application, but a guest may not. The guest may only view the settings and status of the network. As shipped from the factory, both users can log in without a password. Netgear strongly recommends that the network administrator creates a unique password for the administrative user before placing the switch into production.

The following screen shows an example of the PCC:


NETGEAR
Connect with Innovation
GSM7328FS
24 SFP Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots
System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
LOGOUT
VLAN | STP | Multicast | Address Table | Ports | LAG
Basic
Advanced
CANCEL
APPLY
Copyright © 1996-2007 Netgear ®

VLAN Configuration

Reset

Reset Configuration □

VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type
□	1	Default	Default
□	200	vlan200	Static

Figure 1-2

The PCC Web interface has the following four significant features:

1. Layout: The navigation pane has two rows of tabs, as shown in the following screen:

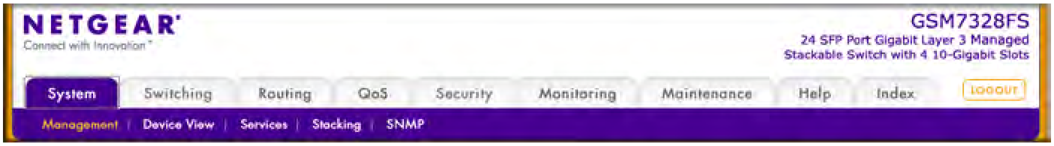

NETGEAR
Connect with Innovation
GSM7328FS
24 SFP Port Gigabit Layer 3 Managed
Stackable Switch with 4 10-Gigabit Slots
System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
LOGOUT
Management | Device View | Services | Stacking | SNMP

Figure 1-3

Tabs		Tab Contents
Main tabs	System	Configuration and status information for system features and services such as the timer, DNS server, IP address, and system resource usage.
	Switching	Features that relate to Layer 2 services such as VLANs, link aggregation, spanning tree protocol, port configuration, and the MAC address table.
	Routing	Layer 3 services such as VLAN routing, port routing, and protocols such as RIP, OSPF, VRRP, and other protocols.
	QoS	Quality of service features such as DiffServ and CoS queue assignment.
	Security	Security services such as 802.1x port authentication, traffic control with various forwarding controls, and ACLs.
	Monitoring	Ethernet port statistics, various system logs, and port mirroring.

Tabs		Tab Contents
Main tabs	Maintenance	Services to perform a firmware upgrade, to save the configuration, and to perform a backup of the configuration.
	Help	Access to the NETGEAR product support website and documentation.
	Index	Tthe site index that allows direct access to any of the pages under the main tabs and sub tabs.
Sub tabs		The sub tab content changes depending on the selected main tab. In turn, each sub tab provides further sub categories of functions.

2. Unified Web Control Buttons: Depending on the selected main tag and sub tag, in the lower right corner, there are buttons that enable you to perform various page-dependent operations:
   - **Add**. Add a new class, group, ACL, or VLAN.
   - **Apply**. Apply all changes that you made to a page.
   - **Cancel**. Cancel all changes that you made to a page.
   - **Delete**. Delete an existing list or group that was created by using an Add operation.
   - **Refresh**. Refresh the data on the page such as log entry, port statistics, and other data.
3. Index Page: One of the unique features of the PCC is the Index page. This page provides links to all available pages on the PCC, allowing you to connect to each page directly. On the Index page, you can use your Web browser’s search function to locate a particular feature, and then connect directly to the page that enables you to view or configure that feature. Note that when you access a page directly from the Index page, the navigation pane does not adjust as it normally would when you navigate to the page by using a main tag and sub tag.
4. Save the Configuration: When you click the **Apply** button to save the changes, the changes are applied to the switch but not saved into the permanent memory of the switch. When you reboot the switch, the changes are lost.To save the changes into the permanent memory of the switch, use the Save Configuration function that you can reach by clicking on the Maintenance tag and then on the Save Config tag.

Configuring an SNMP V3 User Profile

Configuring an SNMP V3 user profile is a part of user configuration. Any user can connect to the switch using the SNMPv3 protocol, but for authentication and encryption, additional steps are needed. Use the following steps to configure an SNMP V3 new user profile.

1. Select **System**>**Configuration**>**User Accounts** from the hierarchical tree on the left side of the web interface.

2. In the **User** field, select **Create** to create a new user.

3. Enter a new user name in the User Name field.

4. Enter a new password in the Password field and then retype it in the Confirm Password field.

> **Note:** If SNMPv3 Authentication is to be used for this user, the password must be eight or more alphanumeric characters.

5. If you do not need authentication, go to Step 9.
6. To enable authentication, in the Authentication Protocol field select either **MD5** or **SHA** for the authentication protocol.
7. If you do not need encryption, go to Step 9.
8. To enable encryption select **DES** for the encryption scheme in the Encryption Protocol field. Then, enter in the Encryption Key field an encryption code of eight or more alphanumeric characters.
9. Click **Apply**.

Chapter 2
Auto Install Configuration

Auto Install is a software feature which provides for the configuration of a switch automatically when the device is initialized and no configuration file is found on the switch. The downloaded configuration file is not distributed across a stack. When an administrator saves configuration, the config file is distributed across a stack.

This chapter includes the following sections:

The Auto Install process requires DHCP to be enabled by default in order for it to be completed. The downloaded config file is not automatically saved to startup-config. An administrator must explicitly issue a save request in order to save the configuration. The Auto Install process depends upon the configuration of other devices in the network, including a DHCP or BOOTP server, a TFTP server and, if necessary, a DNS server.

There are three phases to Auto Install:

1. Configuration or assignment of an IP address for the device.
2. Assignment of a TFTP server.
3. Obtaining a configuration file for the device from the TFTP server.

Switch IP Address Assignment

If BOOTP or DHCP is enabled on the switch and an IP address has not been assigned, the switch issues requests for an IP address assignment. The behavior of BOOTP or DHCP with respect to IP address assignment is unchanged by the addition of the Auto Install feature. That is, the following information returned from the server is recognized.

- The IP address (yiaddr) and subnet mask (option 1) to be assigned to the switch

- The IP address of a default gateway (option 3), if needed for IP communication. Some network configurations require the specification of a default gateway through which some IP communication can occur. The default gateway is specified by Option 3 of a BOOTP or DHCP response.

After an IP address is assigned to the switch, if a hostname is not already assigned, then Auto Install issues a DNS request for the corresponding hostname. This hostname is also displayed as the CLI prompt the same as if the “hostname”command was used.

Assignment of Other Dynamic Configuration

TFTP IP Address and the Configuration File Name

The following information is also processed, any of which may be returned by a BOOTP or DHCP server:

- The name of the configuration file (bootfile or option 67) to be downloaded from the TFTP server.
- The identification of the TFTP server from which to obtain the bootfile. This is given by any of the following fields:
  - The hostname of the TFTP server (option 66 or sname). Either the TFTP address or name is specified, not both, in most network configurations. If a TFTP hostname is given, a DNS server is required to translate the name to an IP address.
  - The IP address of the TFTP server (option 150).
  - The address of the TFTP server (siaddr) to be used for Auto Install requests.

No configuration assigned by BOOTP or DHCP is saved in startup-config.

Handling Conflicting TFTP Server Configuration

The TFTP server IP address can be deduced from the multiple sources. It is selected from one of the following fields, listed from the highest priority to the lowest:

- The **sname** field of a DHCP or BOOTP reply.
- The TFTP server name (option 66) of a DHCP reply.
- The TFTP server address (option 150) field of a DHCP reply.
- The **siaddr** field of a DHCP or BOOTP reply.

DNS Server Requirements

A DNS server is needed to resolve the IP address of the TFTP server only if the sname or option 66 values are used.

Obtaining a Config File

After obtaining IP addresses for both the switch and the TFTP server, the Auto Install process attempts to download a configuration file. A host-specific configuration file is downloaded, if possible. Otherwise, a network configuration file is used as a bridge to get the final configuration. The methods are described below.

Host-Specific Configuration File

The switch attempts to download a host-specific configuration file if a bootfile name was specified by the DHCP or BOOTP server. The switch makes three unicast TFTP requests for the specified bootfile. If the unicast attempts fail, or if a TFTP server address was not provided, the switch makes three broadcast requests to any available TFTP server for the specified bootfile. A TFTP broadcast request is a simple TFTP request with broadcast destination MAC address (ff:ff:ff:ff:ff:ff) and destination IP address (255.255.255.255).

Note: The bootfile is required to have a file type of *.cfg.

Default Network Configuration File

Attempts are made to download a default network configuration file with the name fp-net.cfg if the specified bootfile cannot be found, a failure occurs in the download or the switch was not provided a specific bootfile name by the DHCP server. The switch unicasts or broadcasts TFTP requests for a network configuration file in the same manner as it attempts to download a host-specific configuration file.

The default network configuration file should have IP address to hostname mappings using the command **ip host <hostname> <address>**. If the default network configuration file does not contain the switch IP address, the switch uses DNS to attempt to resolve its hostname.

A sample fp-net.cfg file follows:

```
config
...
ip host switch_to_setup 192.168.1.10
ip host another_switch 192.168.1.11
... <other hostname definitions>
exit
```

Once a hostname has been determined, the switch then issues a TFTP request for a file named **<hostname>.cfg** file, where <hostname> is the first eight characters of the switch’s hostname.

If the switch is unable to map its IP address to a hostname, Auto Install sends TFTP requests for the default configuration file router.cfg.

The following table summarizes the config files that may be downloaded, and the order in which they are sought.

Table 2-1. Configuration File Possibilities

Order Sought	File Name	Description	Final File Sought
1	`<bootfile>.cfg`	Host-specific config file, ending in a *.cfg file extension	Yes
2	`fp-net.cfg`	Default network config file	No
3	`<hostname>.cfg`	Host-specific config file, associated with hostname	Yes
4	`router.cfg`	Default config file	Yes

Table 2-2 displays the determining factors for issuing unicast or broadcast TFTP requests.

Table 2-2. Unicast or Broadcast TFTP Requests

TFTP Server Address Available	Host-specific Router Config Filename Available	TFTP Request Method
Yes	Yes	Issue a unicast request for the host-specific router config file to the TFTP server
Yes	No	Issue a unicast request for a default network or router config file to the TFTP server
No	Yes	Issue a broadcast request for the host-specific router config file to any available TFTP server
No	No	Issue a broadcast request for the default network or router config file to any available TFTP server

Monitoring and Completing the Auto Install Process

Upon bootup in the absence of a saved config, a message appears on the console informing the user that the Auto Install procedure is beginning. A message subsequently appears when Auto Install is complete. The message also indicates that configuration must be saved in order to not perform Auto Install on the next reboot.

When Auto Install has been successfully completed, an administrator can execute a **show running-config** command to validate the contents of configuration.

Saving Configuration

An administrator must explicitly save the downloaded configuration in non-volatile memory. Then a configuration will be available on the next reboot. In the CLI, this is performed by issuing a **copy running-config startup-config** command and should be done after validating the contents of saved configuration.

Host-Specific Config File Not Found

If the Auto Install process fails to download any configuration file as described above, a message is logged. If a “final”configuration file is not downloaded, as described in Table 2-1, the Auto Install procedure continues to issue TFTP broadcast requests. The frequency of the broadcasts is once per 10 minute period.

Terminating the Auto Install Process

A user may terminate the Auto Install process at any time prior to the downloading of the config file. This is most optimally done when the switch is disconnected from the network, or if the requisite configuration files have not been configured on TFTP servers.

Termination of the Auto Install process ends further periodic requests for a host-specific file.

Managing Downloaded Config Files

The configuration files downloaded via Auto Install are stored in the nonvolatile memory. The files may be managed (viewed, displayed, deleted) along with files downloaded via the configuration scripting utility.

A file is not automatically deleted after it is downloaded. However, the file does not take effect upon a reboot. If an administrator opts to save config, the saved configuration takes effect upon reboot. If the user does not opt to save config, the Auto Install process occurs again on a subsequent reboot. This may result in one of the previously downloaded files being overwritten.

Restarting the Auto Install Process

The Auto Install process is automatically started on a subsequent reboot if the configuration file is not found on the switch. This situation can occur if configuration has not ever been saved on the switch, or if the administrator has issued a command to erase the configuration file.

During a particular session, the Auto Install process may be restarted if the administrator has previously stopped the Auto Install process, and then chooses to restart it. This action re-initiates the process for this login session only. It is recommended that this action be performed only when the administrator is certain that configuration is clear in order to have predictable results.

Reinitialization of the switch after a clear config automatically activates the Auto Install process if there is no configuration file stored on the switch.

Logging

A message is logged for each of the following events:

1. The Auto Install component receiving a config file name and other options upon resolving an IP address by DHCP or BOOTP client. The boot options values are logged.
2. The Auto Install component initiating a TFTP request for a boot (config) file, receiving the file, or timing out of that request. Filenames and server IP addresses and/or hostnames are logged.
3. The Auto Install component initiating a request for a hostname. The IP address and resolved hostname are logged.
4. The Auto Install component initiating a TFTP request for a hostname>.cfg file, receiving the file, or timing out of that request. Filenames and server IP addresses and hostnames are logged.
5. The beginning of applying a config script.
6. The failure of the CLI scripting utility to apply a config file.

Configure Auto Install

Stacking

The downloaded configuration file is not distributed across a stack. When an administrator saves configuration, the config file is distributed across a stack.

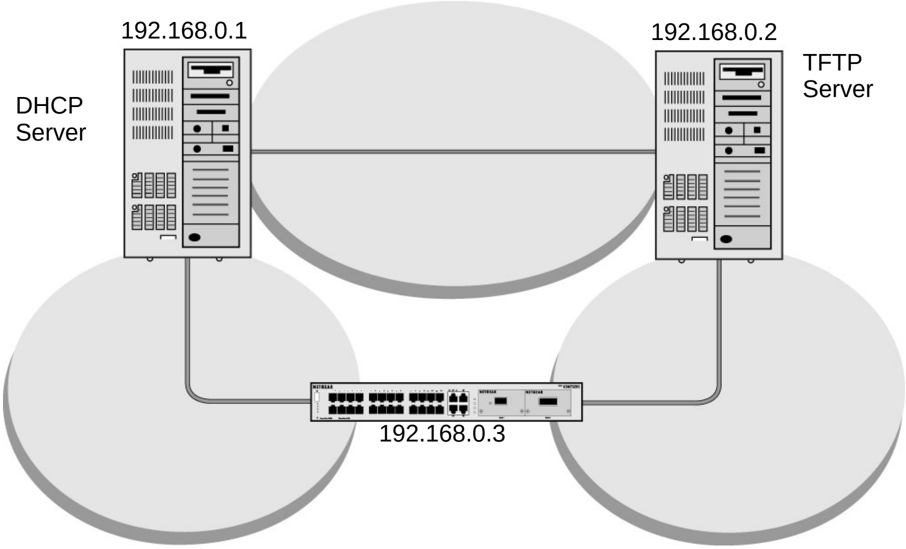


Figure 2-1

DHCP Server Configuration

The following information is configured on the DHCP or BOOTP server:

- The IP address(yiaddr) and subnet mask(option1)
- The name of the configuration file (bootfile or option 67)
- The IP address of the TFTP server (option 150)

TFTP Server Configuration

The configuration file is on the TFTP server (e.g. switch.cfg).

CLI: Switch Configuration

```
(Netgear Switch) #boot autoinstall auto-save
```

Have the configuration file saved after download from TFTP server.

```
(Netgear Switch) #boot autoinstall start
```

Autoinstall starts and waiting for boot options turned by DHCP server.

```
(Netgear Switch) #network protocol dhcp
Changing protocol mode will reset ip configuration.
Are you sure you want to continue? (y/n)y
```

Request an IP address, configuration file name and TFTP IP address from the DHCP server.

```
(Netgear Switch) #
Config file 'startup-config' created successfully.
```

AutoInstalled configuration is saved.

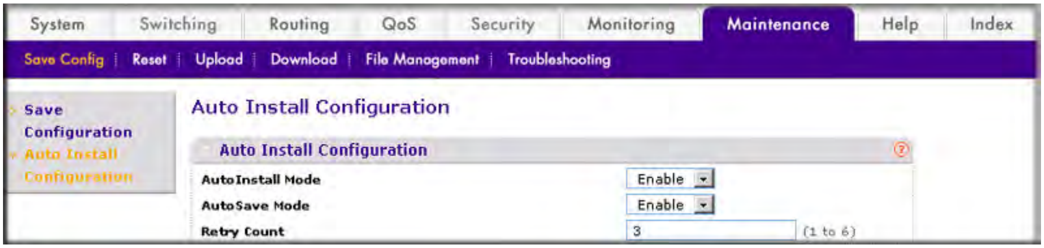
```
(Netgear Switch) #show autoinstall
AutoInstall Mode............................... Started
AutoSave Mode.................................. Enabled
AutoInstall Retry Count........................ 3
AutoInstall State.............................. AutoInstall is completed
```

Autoinstall is completed now.

Web Interface

To use the Web interface to configure the Auto Install, proceed as follows:

1. From the main menu, select Maintenance > Save Config >Auto Install Configuration. A screen similar to the following displays.



Auto Install Configuration

Auto Install Configuration

AutoInstall Mode: Enable

AutoSave Mode: Enable

Retry Count: 3 (1 to 6)

Figure 2-2

2. Select **Enable** in the AutoInstall Mode field.
3. Select **Enable** in the AutoSave Mode field.
4. Click **Apply**.

Chapter 3
Virtual LANs

In this chapter, the following examples are provided:

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, and 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 may omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet may either reject it or insert a tag using its default VLAN ID. A given port may handle traffic for more than one VLAN, but it can only support 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.

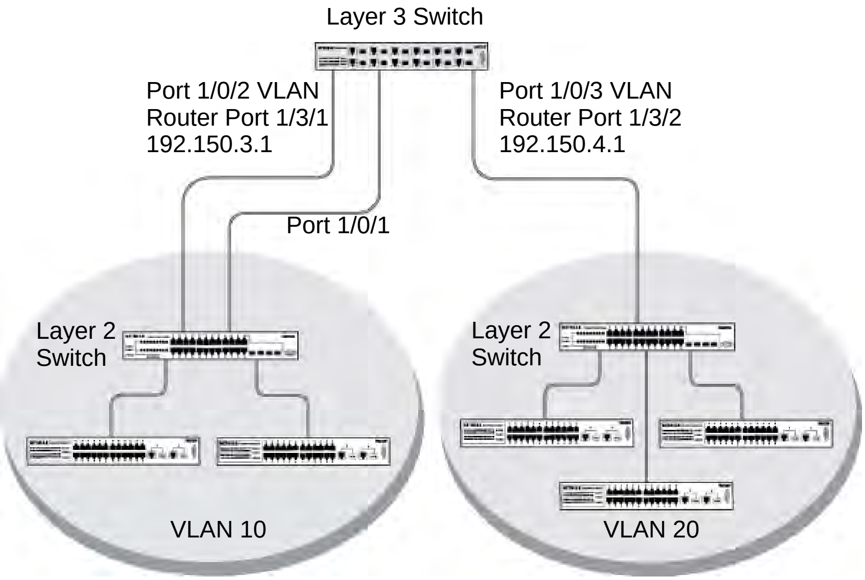


Figure 3-1

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: Creating Two VLANS

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

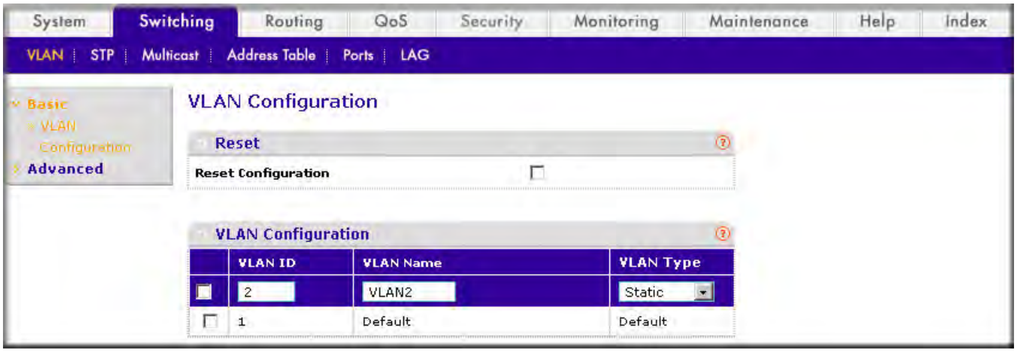
```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 2
(Netgear Switch) (Vlan)#vlan 3
(Netgear Switch) (Vlan)#exit
```

Web Interface: Creating Two VLANS

To use the Web interface to configure the managed switch, proceed as follows:

1. Create VLAN 2.

a. From the main menu, 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

Figure 3-2

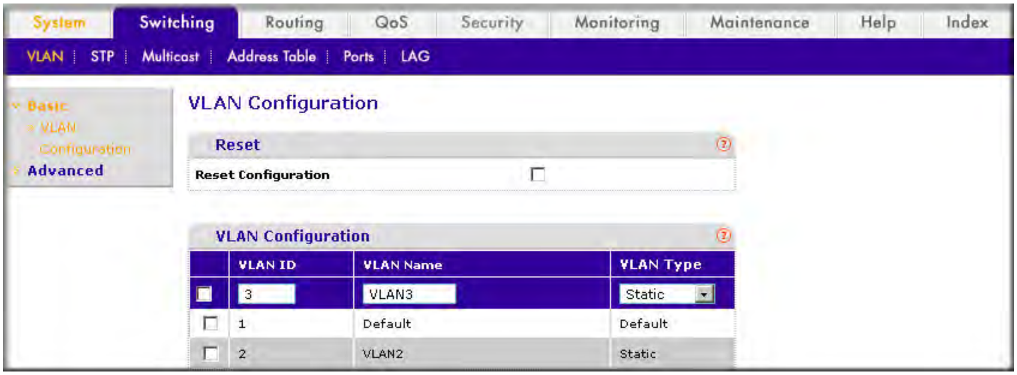
b. Enter the following information in the VLAN Configuration.

- In the VLAN ID field, enter **2**
- In the VLAN Name field, enter **VLAN2**
- Select **Static** in the VLAN Type field.

c. Click **Add.**

2. Create VLAN 3.

a. From the main menu, 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

Figure 3-3

b. Enter the following information in the VLAN Configuration.

- In the VLAN ID field, enter **3**

- In the VLAN Name field, enter **VLAN3**
- Select **Static** in the VLAN Type field.

c. Click **Add.**

Assign Ports to VLAN2

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

CLI: Assigning Ports to VLAN2

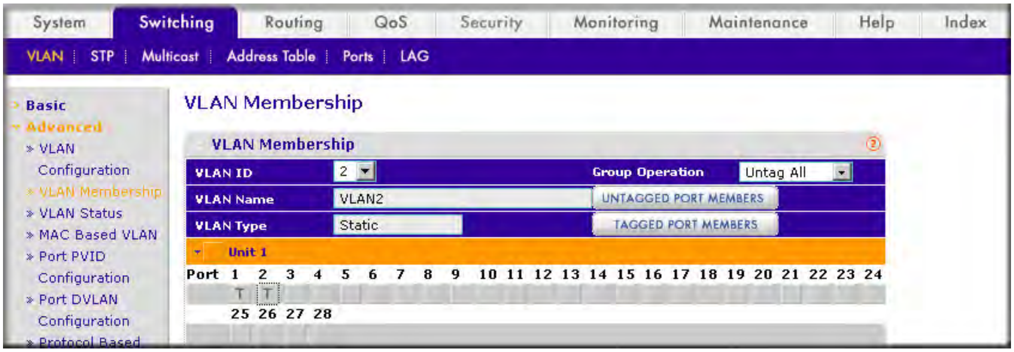
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan participation include 2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan acceptframe vlanonly
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan pvid 2
(Netgear Switch)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

Web Interface: Assigning Ports to VLAN2

To use the Web interface to configure the managed switch, proceed as follows:

1. Assign ports to VLAN 2.

a. From the main menu, 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

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

Figure 3-4

b. Select **2** in the VLAN ID field

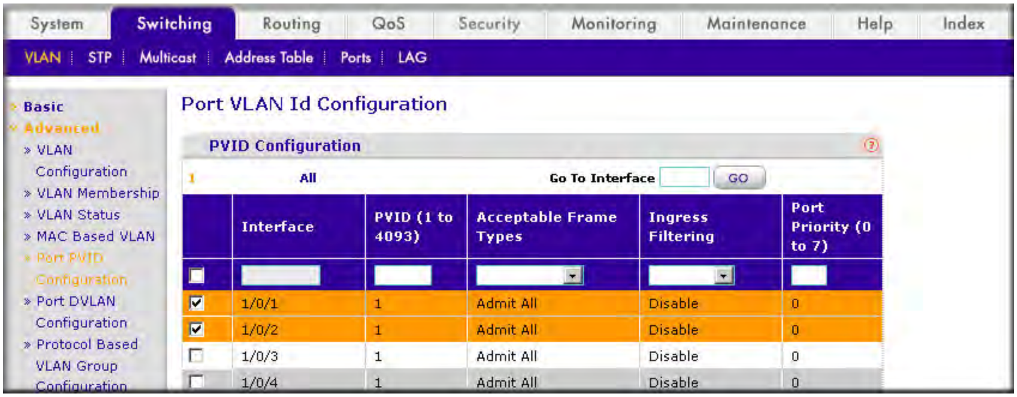
c. Click the Unit 1. The Ports display.

d. Click the gray box under port **1** and **2** until T displays. The T specifies that the egress packet is tagged for the port.

e. Click **Apply**

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

a. From the main menu, 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

	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

Figure 3-5

b. Under PVID Configuration, scroll down to interface 1/0/1 and select the checkbox for **1/0/1**. Then scroll down to the interface 1/0/2 and select the checkbox for **1/0/2**.

c. Enter the following information in the PVID Configuration.

- Select **VLAN Only** in the Acceptable Frame Type polyhedron field.
- Enter **2** in the PVID(1 to 4093) field.

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

Assign Ports to VLAN3

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

CLI: Assigning Ports to VLAN3

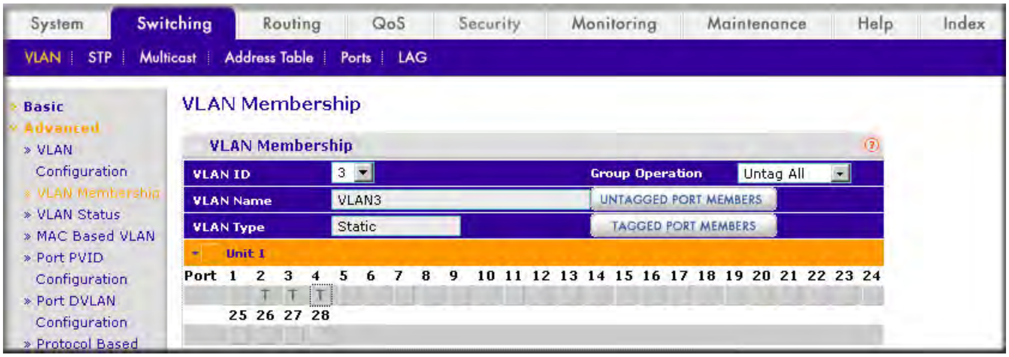
```
(Netgear Switch) (Config)#interface range 1/0/2-1/0/4
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#vlan participation include 3
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#exit
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#vlan acceptframe all
(Netgear Switch) (Interface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

Web Interface: Assigning Ports to VLAN3

To use the Web interface to configure the managed switch, proceed as follows:

1. Assign ports to VLAN 3.

a. From the main menu, 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

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	T																				
	25	26	27	28																				

Figure 3-6

b. Select **3** in the VLAN ID field

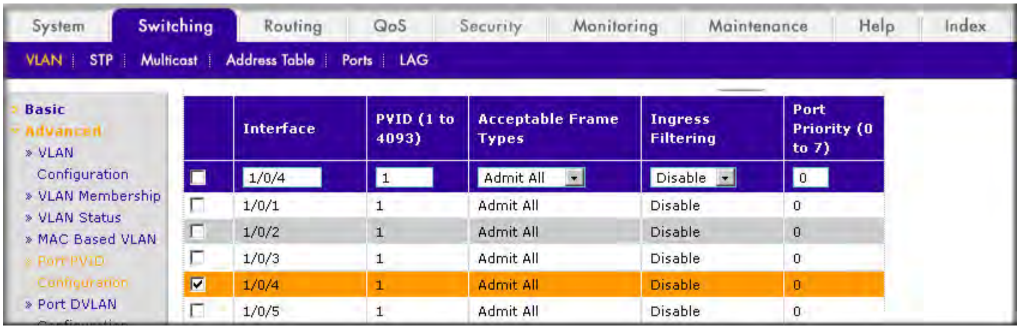
c. Click the **Unit 1.** The Ports display.

d. Click the gray box under port **2**,**3** and **4** until T displays. The T specifies that the egress packet is tagged for the port.

e. Click **Apply**

2. Specify that untagged frames will be accepted on port 1/0/4.

a. From the main menu, 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

Figure 3-7

b. Under PVID Configuration, scroll down to interface **1/0/4** and select the checkbox for that interface. Now 1/0/4 appears in the Interface field at the top.

c. Under PVID Configuration, select **Admit All** in the Acceptable Frame Type polyhedron field.

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

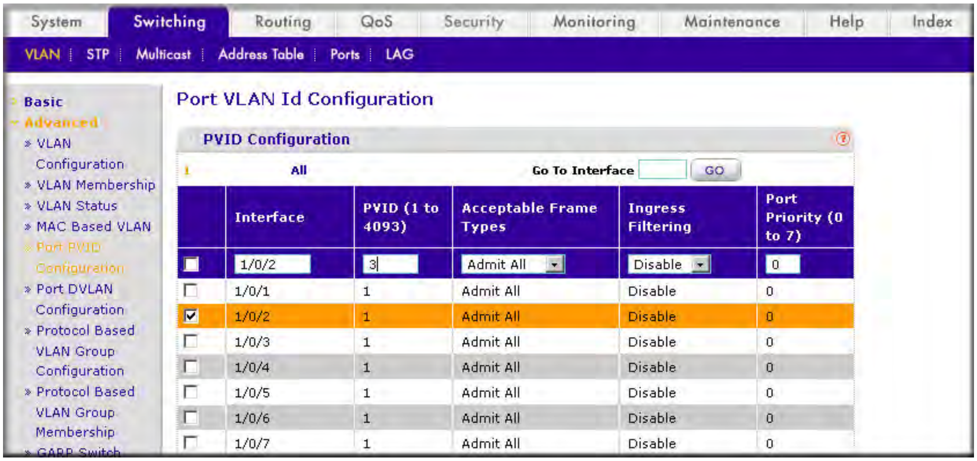
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#vlan pvid 3
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

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

To use the Web interface to configure the managed switch, proceed as follows:

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

a. From the main menu, 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
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)
□	1/0/2	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

Figure 3-8

b. Under PVID Configuration, scroll down to interface **1/0/2** and select the checkbox for that interface. Now 1/0/2 appears in the Interface field at the top.

c. Under PVID Configuration, enter **3** in the PVID(1 to 4093) field.

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

Creating a MAC-based VLAN

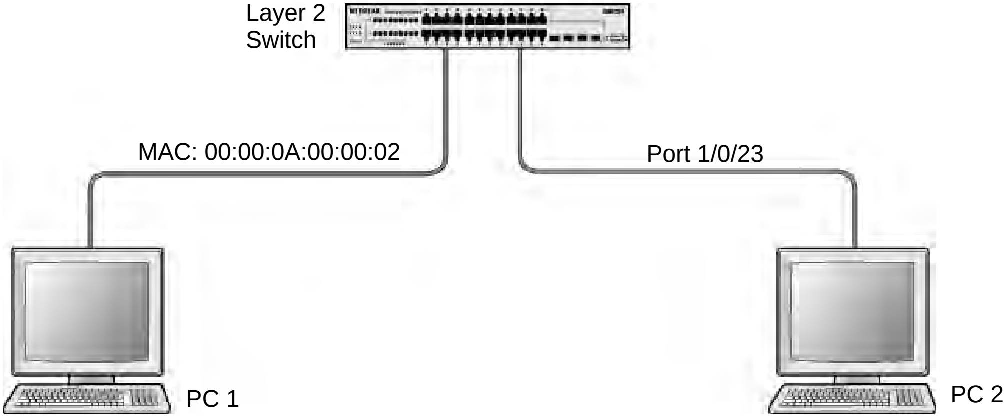


Figure 3-9

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.

A MAC to VLAN mapping is defined by configuring an entry in the MAC to VLAN table. An entry is specified via a source MAC address and the desired 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 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 the user is allowed to configure a MAC address mapping to a VLAN that has not been created on the system.

CLI: Creating a MAC-Based VLAN

Create a VLAN 3

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

Add the port 1/0/23 to the VLAN 3.

```
(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
```

Map the MAC 00:00:0A:00:00:02 to the VLAN 3.

```
(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
```

Add all the ports to VLAN 3.

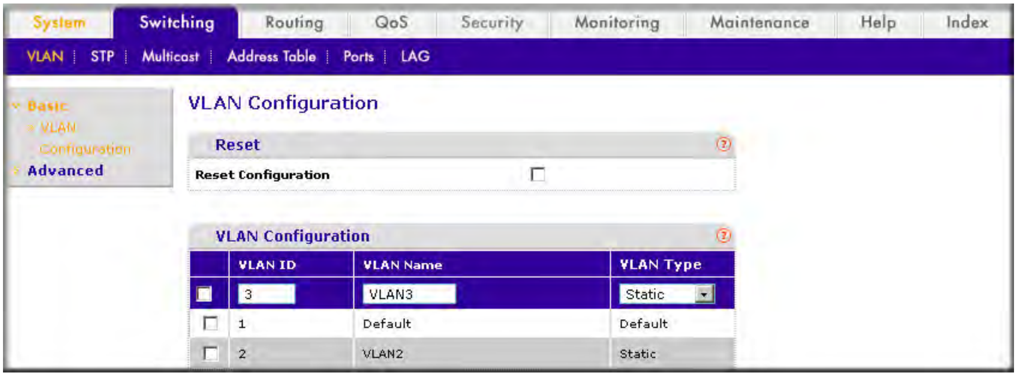
```
(Netgear Switch)#config
(Netgear Switch)(Config)#interface range 1/0/1-1/0/28
(Netgear Switch)(conf-if-range-1/0/1-1/0/28)#vlan participation include 3
(Netgear Switch)(conf-if-range-1/0/1-1/0/28)#exit
(Netgear Switch)(Config)#exit
```

Web Interface Procedure: Assigning a MAC-Based VLAN

To use the Web interface to configure the managed switch, proceed as follows:

1. Create VLAN 3.

   a. From the main menu, 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

Figure 3-10

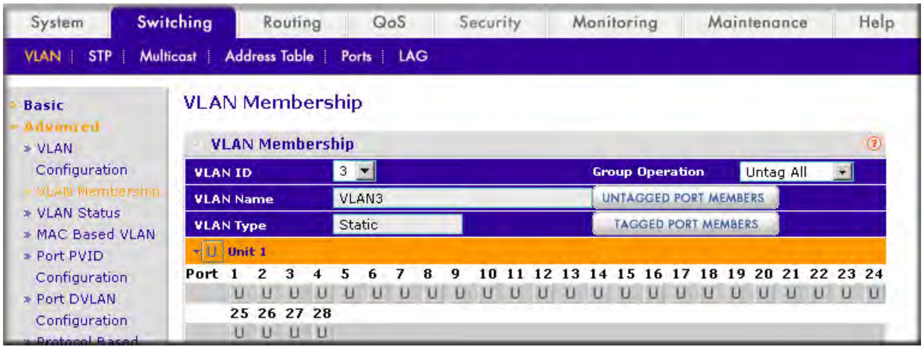
   b. Enter the following information in the VLAN Configuration.

   - In the VLAN ID field, enter **3**
   - In the VLAN Name field, enter **VLAN3**
   - Select **Static** in the VLAN Type field.

   c. Click **Add**

2. Assign ports to VLAN 3.

   a. From the main menu, 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

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																				

Figure 3-11

b. Select **3** in the VLAN ID field.

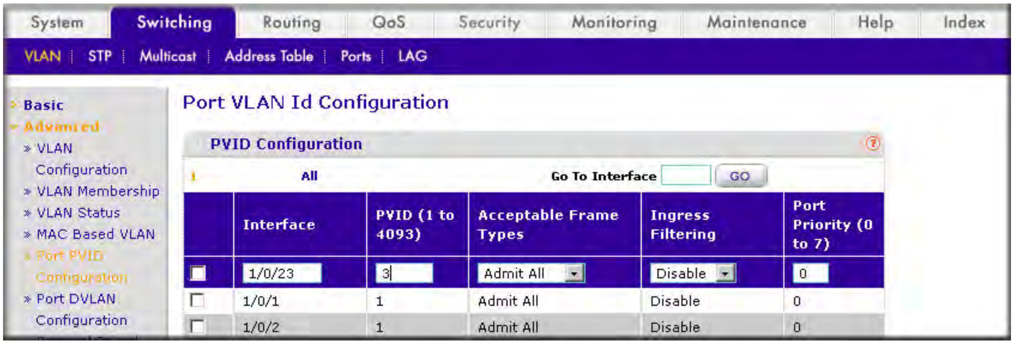
c. Click the **Unit 1.** The Ports display.

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

e. Click **Apply**

3. Assign VPID 3 to the port 1/0/23.

a. From the main menu, select Switching > VLAN> Advanced > Port PVID Configuration. A screen similar to the following displays.



Port VLAN Id Configuration

PVID Configuration

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

Figure 3-12

b. Under PVID Configuration, scroll down to interface **1/0/23** and select the checkbox for 1/0/23.

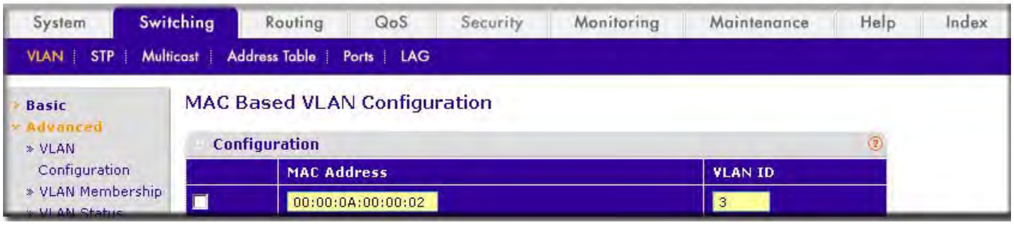
c. Enter the following information in the PVID Configuration.

Enter **3** in the PVID (1 to 4093) field.

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

4. Mapping the specific MAC to the VLAN 3.

a. From the main menu, 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

Figure 3-13

b. Enter the following information in the MAC Based VLAN Configuration.

- Enter **00:00:0A:00:00:02** in the MAC Address field.
- Enter **3** in the PVID(1 to 4093) field.

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 is assigned to VLAN 4, and the untagged IP/ARP packets is assigned to VLAN 5.

CLI: Creating a Protocol-based VLAN

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
```

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
```

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
```

Assign vlan protocol group 2 to VLAN 5.

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

Enable protocol vlan group 1 and 2 on the interface.

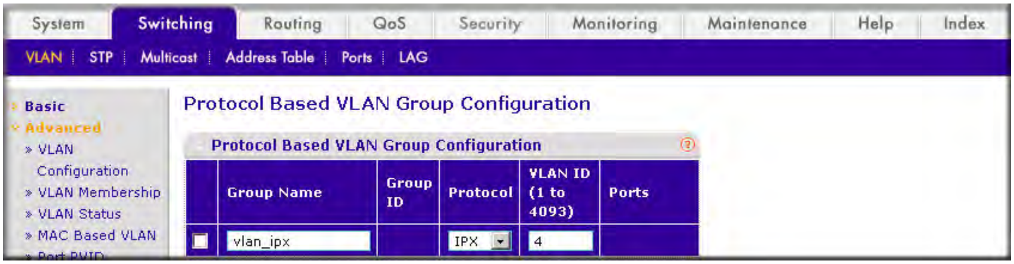
```
(Netgear Switch)(Vlan)#exit
(Netgear Switch)#config
(Netgear Switch)(Config)#interface 1/0/11
(Netgear Switch)(Interface 1/0/11)#protocol vlan group 1
(Netgear Switch)(Interface 1/0/11)#protocol vlan group 2
(Netgear Switch)(Interface 1/0/11)#exit
```

Web Interface: Creating a Protocol-based VLAN

To use the Web interface to configure the managed switch, proceed as follows:

1. Create protocol based VLAN group vlan_ipx.

   a. From the main menu, 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 (1 to 4093)	Ports
□	vlan_ipx		IPX	4	

Figure 3-14

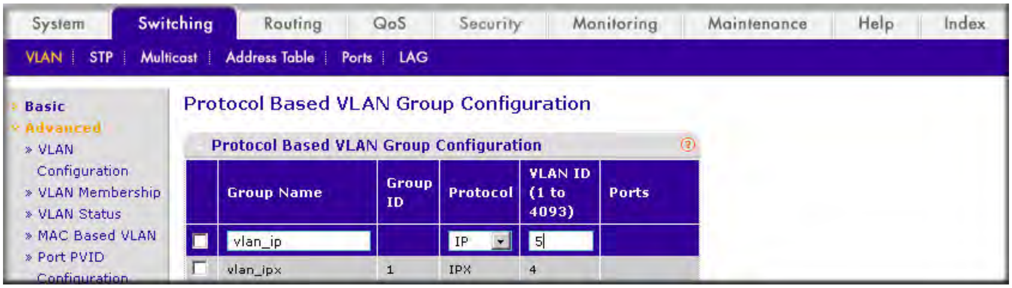
Enter the following information in the Protocol Based VLAN Group Configuration.

- In the Group Name field, enter **vlan_ipx.**
- Select **IPX** in the Protcol field.
- In the VLAN (1 to 4093) field, enter **4.**

   b. Click **Add**

2. Create protocol based VLAN group vlan_ip

a. From the main menu, 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 (1 to 4093)	Ports
□	vlan_ip		IP	5	
□	vlan_ipx	1	IPX	4	

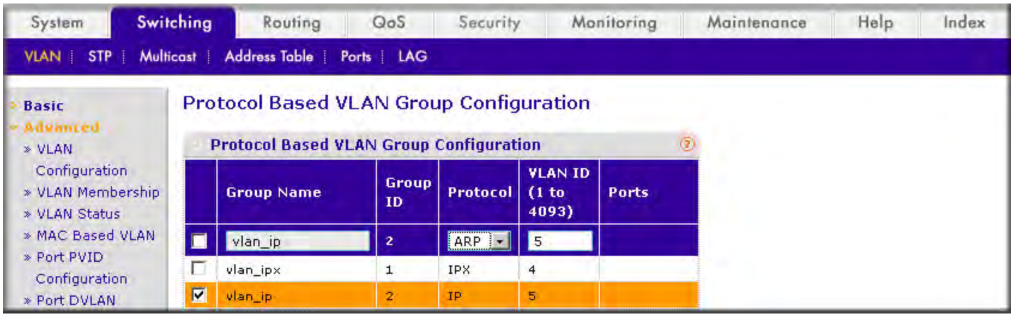
Figure 3-15

b. Enter the following information in the Protocol Based VLAN Group Configuration.

- In the Group Name field, enter **vlan_ipx.**
- Select **IPX** in the Protcol field.
- In the VLAN(1 to 4093) field, enter **4.**

c. Click **Add**.

d. Assign the ARP protocol to the vlan_ip. A screen similar to the following displays.



Protocol Based VLAN Group Configuration

Protocol Based VLAN Group Configuration

	Group Name	Group ID	Protocol	VLAN ID (1 to 4093)	Ports
□	vlan_ip	2	ARP	5	
□	vlan_ipx	1	IPX	4	
☑	vlan_ip	2	IP	5	

Figure 3-16

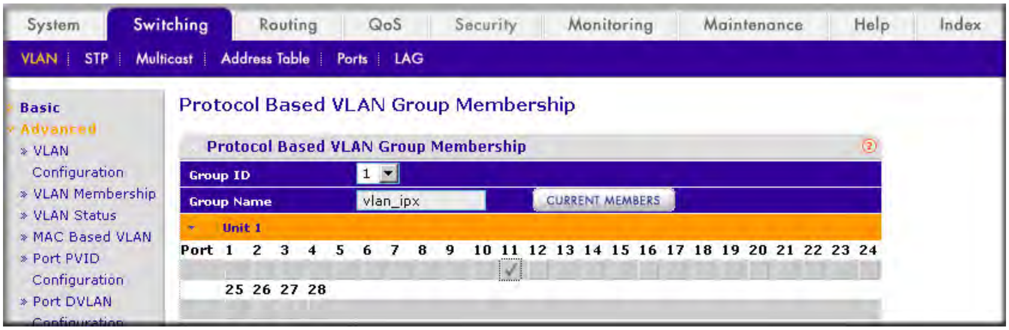
a. Under Protocol Based VLAN Group Configuration, scroll down to **vlan_ip** and select the checkbox for that group. Vlan_ip now appears in the Interface field at the top.

b. Select **IPX** in the Protcol field.

c. Click **Apply**.

3. Add the port 11 to the group vlan_ipx.

a. From the main menu, select Switching > VLAN >Advanced > Protocol Based VLAN Group Membership. A screen similar to the following displays



Protocol Based VLAN Group Membership

Protocol Based VLAN Group Membership

Group ID: 1

Group Name: vlan_ipx

Figure 3-17

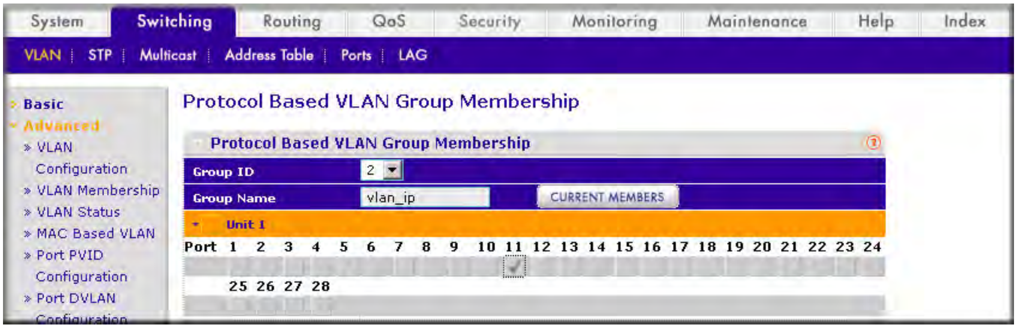
b. Select the **1** in the Group ID field.

c. Click the gray box under port **11**. One flag appears in the box.

d. Click the **Apply** button.

4. Add the port 11 to the group vlan_ip.

a. From the main menu, select Switching > VLAN >Advanced > Protocol Based VLAN Group Membership. A screen similar to the following displays



Protocol Based VLAN Group Membership

Protocol Based VLAN Group Membership

Group ID: 2

Group Name: vlan_ip

Figure 3-18

b. Select the **2** in the Group ID field.

c. Click on the gray box under port **11**. One flag appears 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 classified 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, subnet address for TCP/IP networks) in determining VLAN membership. If a packet is untagged or priority-tagged, the switch will associate 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 only affects the VLAN assignment of a packet. Appropriate 802.1Q VLAN configuration must exist in order for the packet to be switched.

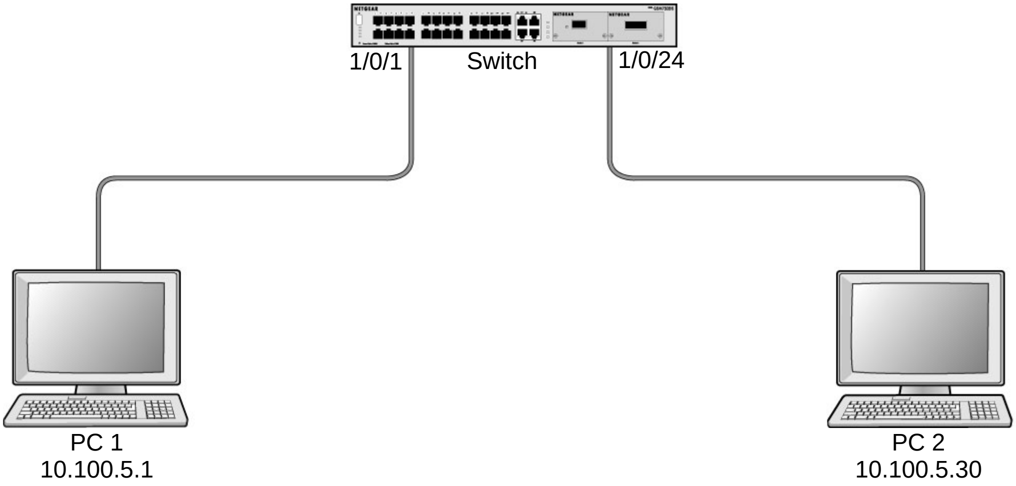


Figure 3-19

CLI: Creating 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)#
```

Have all the ports being member of the VLAN 2000.

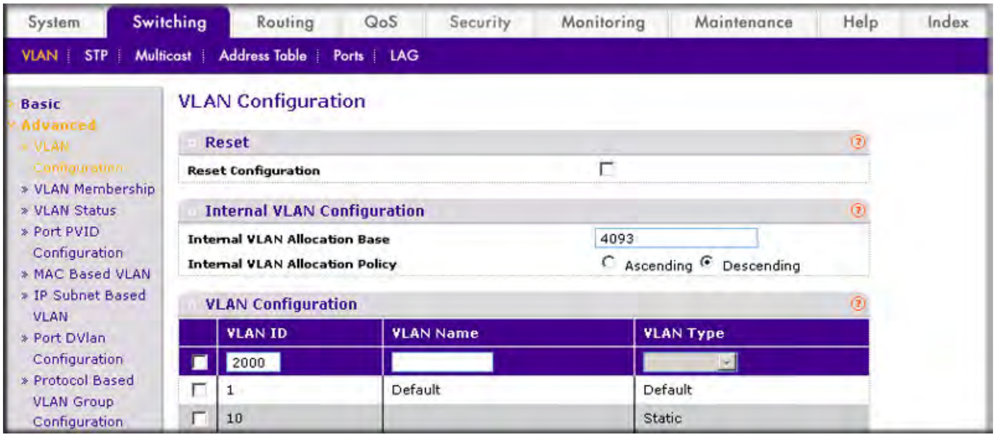
```
(Netgear Switch) #show mac-addr-table vlan 2000
MAC Address      Interface     Status
-----------------  ---------   ------------
00:00:24:58:F5:56  1/0/1       Learned
00:00:24:59:00:62  1/0/24      Learned
```

Web Interface: Creating an IP Subnet Based VLAN

To use the Web interface to configure the IP subnet based VLAN, proceed as follows:

1. Create VLAN 2000.

a. From the main menu, 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

Figure 3-20

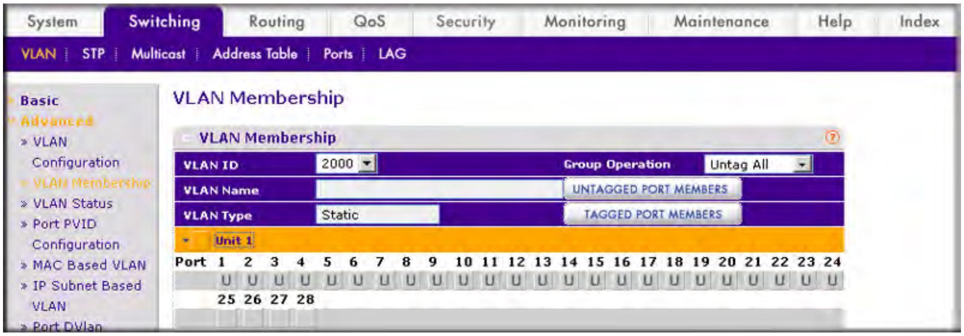
b. Enter the following information in the VLAN Configuration.

- In the **VLAN ID** field, enter **2000**.
- Select **Static** in the **VLAN Type** field.

c. Click **Add**.

2. Assign all of the ports to VLAN 2000.

   a. From the main menu, 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	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																				

Figure 3-21

   b. Select **2000** in the **VLAN ID** field.

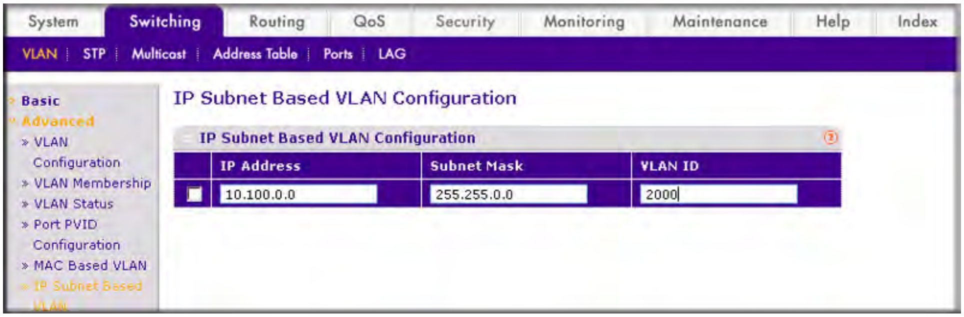
   c. Click the Unit 1. The Ports display.

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

   e. Click **Apply**.

3. Associate the IP subnet with VLAN 2000.

   a. From the main menu, 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

Figure 3-22

   b. Enter the following information in the IP Subnet Based VLAN Configuration.

      - 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 VLAN

The voice VLAN feature enables switch ports to carry voice traffic with defined priority so as to enable separation of voice and data traffic coming onto the port. Voice VLAN is to ensure that sound quality of an IP phone could be safeguarded from deteriorating 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 network attached clients cannot initiate a direct attack on voice components.

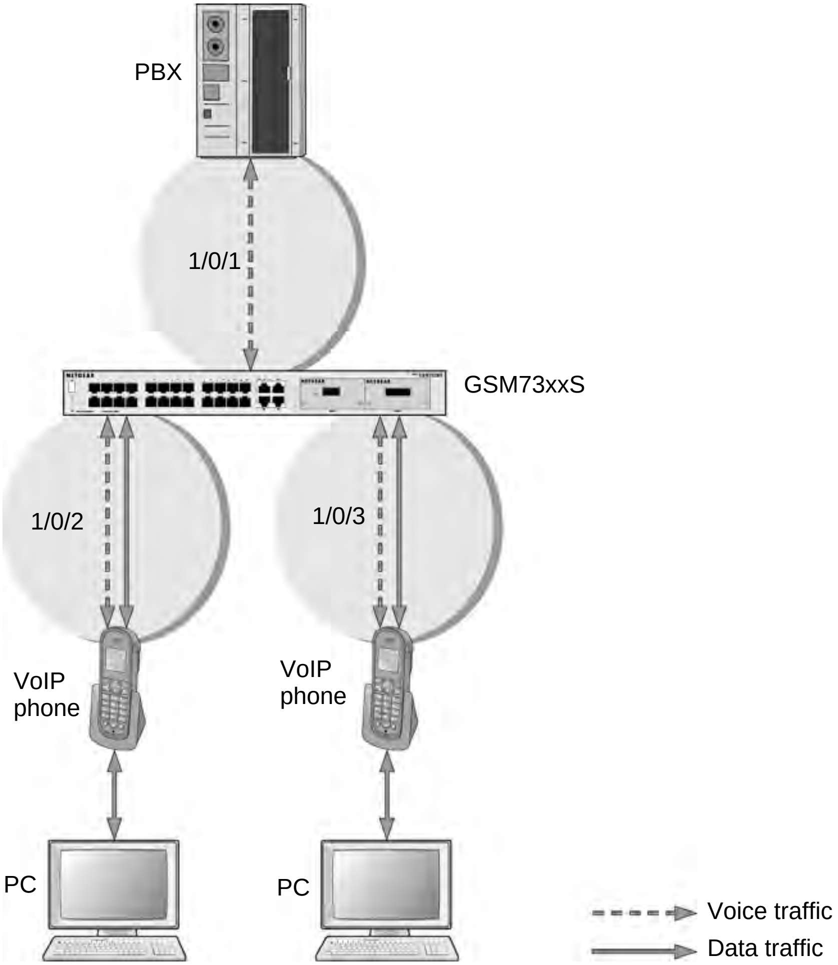


Figure 3-23

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

CLI: Configuring Voice VLAN and Prioritizing Voice Traffic

Create VLAN 10.

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

Include the ports 1/0/1and 1/0/2 in the 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
```

Configure Voice VLAN globally.

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

Configure Voice VLAN Mode in the interfce 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
```

Create the DiffServ Class ClassVoiceVLAN.

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

Configure matching criteria for the class as VLAN 10.

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

Create DiffServ Policy PolicyVoiceVLAN.

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

Map the Policy and Class and assign 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
```

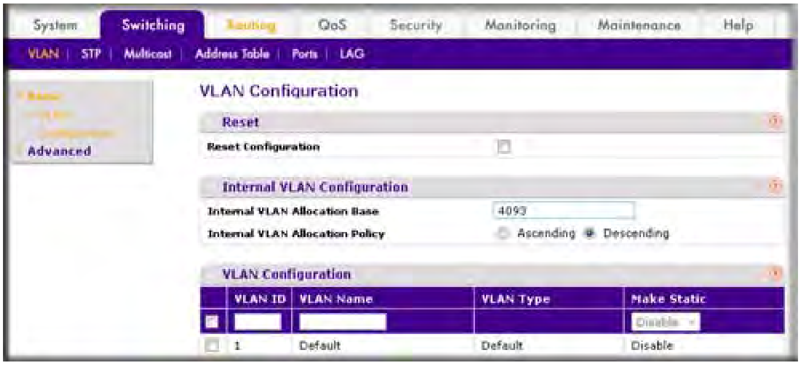
Assign it to the interfaces 1/0/1 and 1/0/2.

```
(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: Voice VLAN and Prioritizing Voice Traffic

1. Create VLAN 10.

a. From the main menu, 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

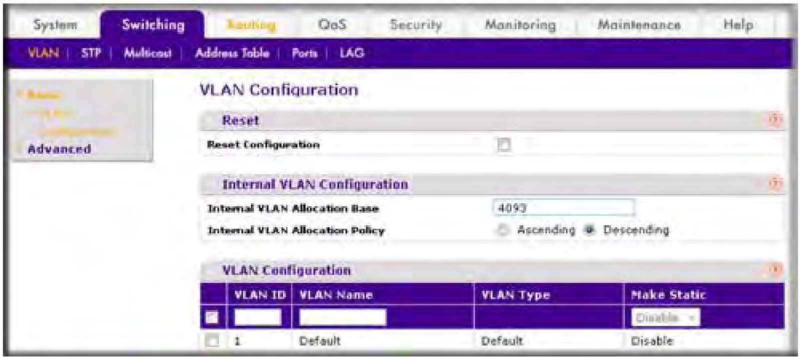
	VLAN ID	VLAN Name	VLAN Type	Make Static
□				Disable
□	1	Default	Default	Disable

Figure 3-24

b. In the VLAN Configuration table, enter VLAN ID as **10**.

c. Enter VLAN Name as **Voice VLAN**.

d. Click **Add**. At the end of this 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

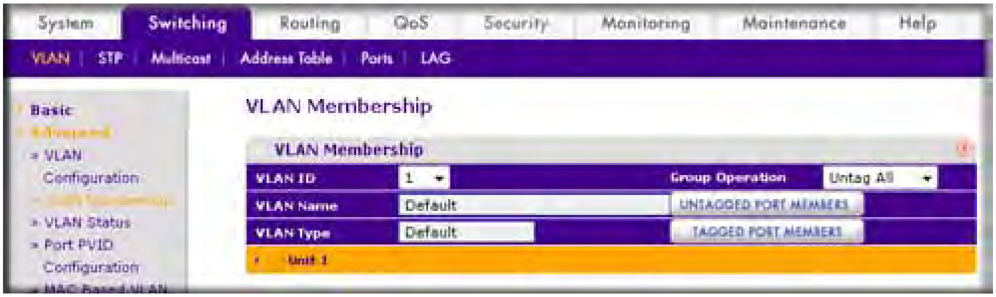
VLAN Configuration

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

Figure 3-25

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

a. From the main menu, select Switching > VLAN > Advanced -> VLAN Membership. A screen similar to the following displays.



VLAN Membership

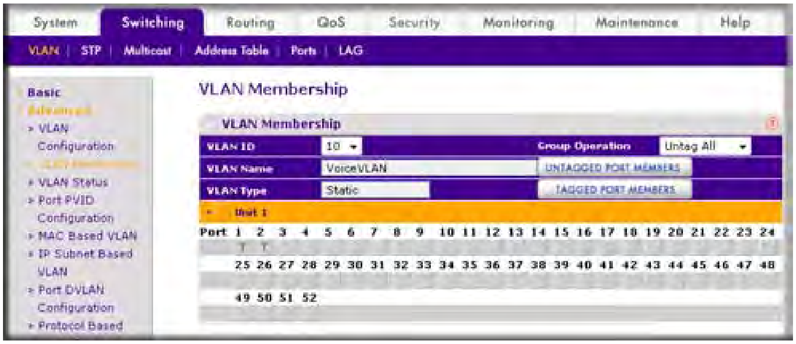
VLAN Membership

VLAN ID	1	Group Operation	Untag All
VLAN Name	Default		
VLAN Type	Default		

Figure 3-26

b. In the VLAN Membership table, select VLAN ID as **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		

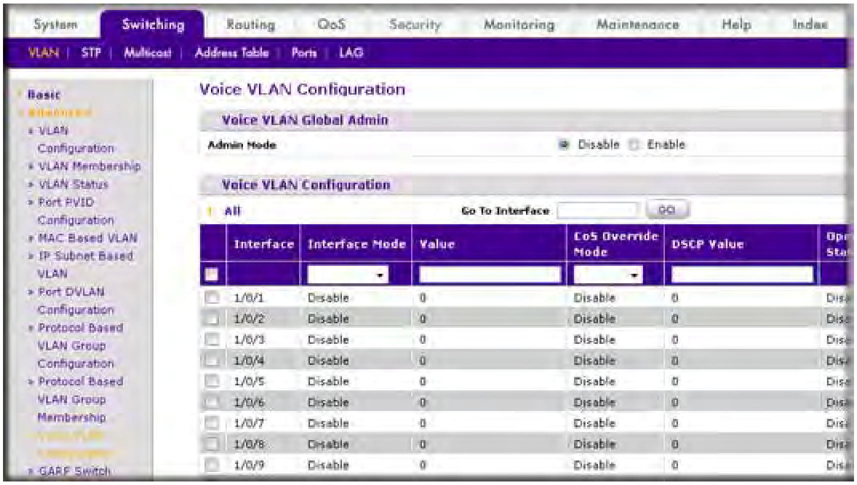
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	T	T																						
	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
	49	50	51	52																				

Figure 3-27

d. Click **Apply**.

3. Configure Voice VLAN globally.

a. From the main menu, 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

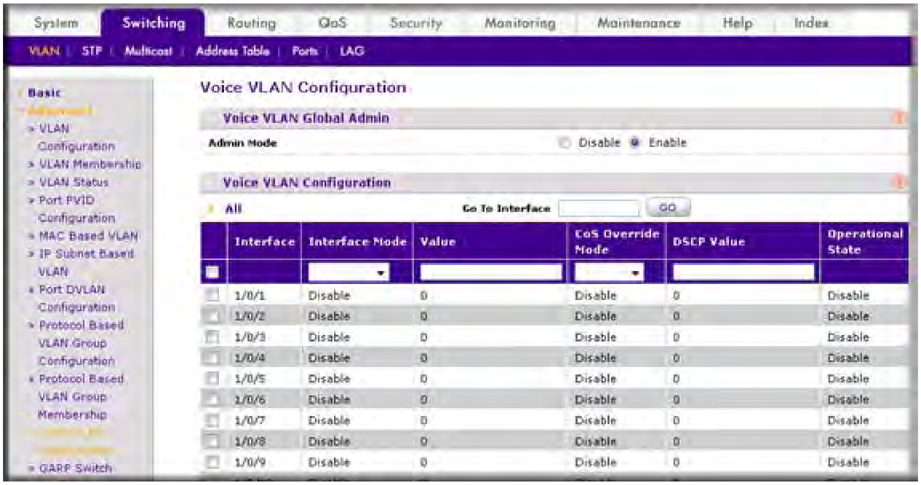
Voice VLAN Configuration

	Interface	Interface Mode	Value	CoS Override Mode	DSCP Value	Op 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

Figure 3-28

b. Select Admin Mode as **Enable**.

c. Click **Apply**. 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
□						
□	1/0/1	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

Figure 3-29

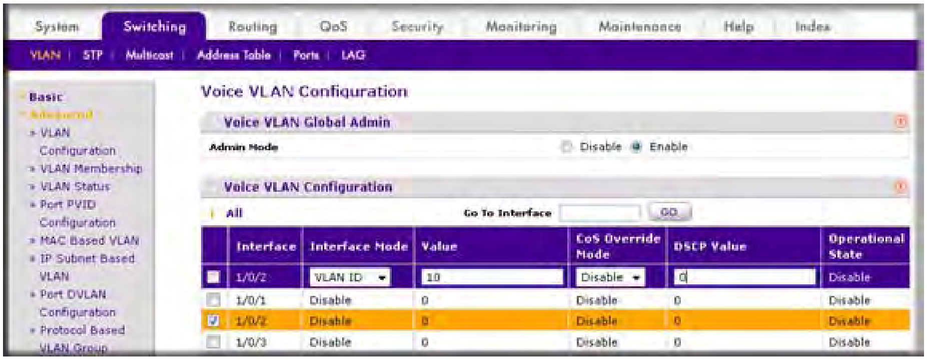
4. Configure Voice VLAN Mode in the interface 1/0/2.

   a. From the main menu, select Switching > VLAN > Advanced -> Voice VLAN Configuration.

   b. Select the checkbox for **1/0/2**.

   c. Set the Interface Mode as **VLAN ID**.

   d. Set the Value at **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

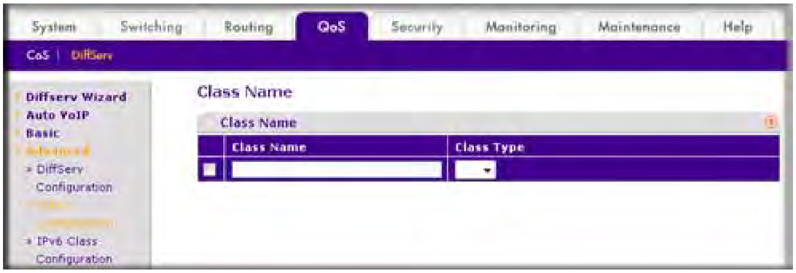
	Interface	Interface Mode	Value	CoS Override Mode	DSCP Value	Operational State
☑	1/0/2	VLAN ID	10	Disable	0	Disable
□	1/0/1	Disable	0	Disable	0	Disable
☑	1/0/2	Disable	0	Disable	0	Disable
□	1/0/3	Disable	0	Disable	0	Disable

Figure 3-30

   e. Click **Apply**.

5. Create the DiffServ Class ClassVoiceVLAN.

a. From the main menu, select QoS > Advanced > Class Configuration. A screen similar to the following displays.

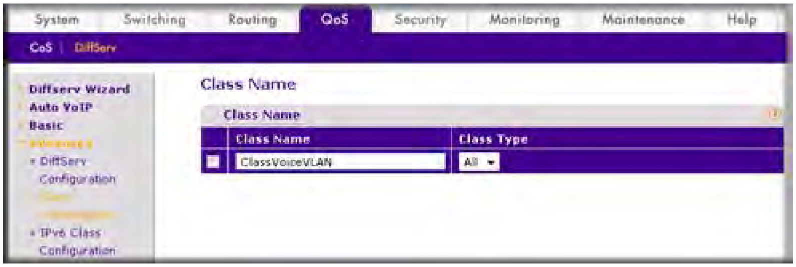


	Class Name	Class Type
□		

Figure 3-31

b. Enter Class Name as **ClassVoiceVLAN**.

c. Select Class Type as **All**. A screen similar to the following displays.



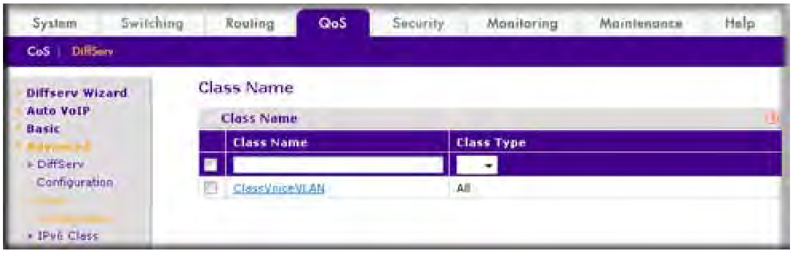
	Class Name	Class Type
□	ClassVoiceVLAN	All

Figure 3-32

d. Click **Add**. A screen similar to the one in Figure 3-33 on page 3-25displays.

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

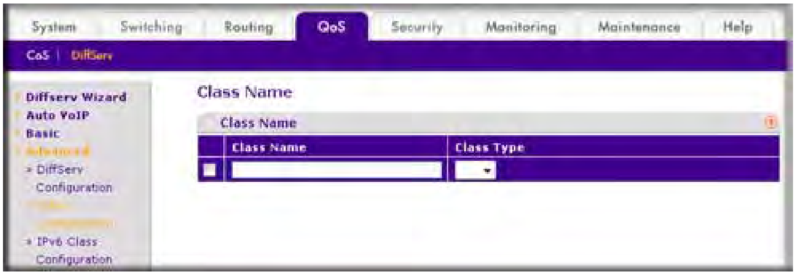
a. From the main menu, select QoS > Advanced > Class Configuration. A screen similar to the following displays.



	Class Name	Class Type
□		
□	ClassVoiceVLAN	All

Figure 3-33

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



Class Name

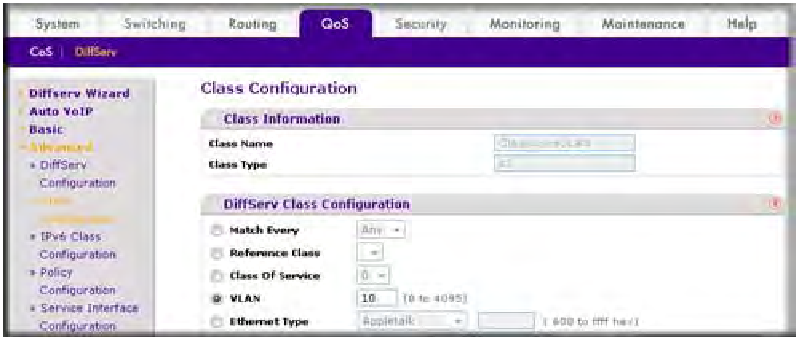
Class Name

□	Class Name	Class Type
□		

Figure 3-34

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

d. Enter VLAN ID as **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

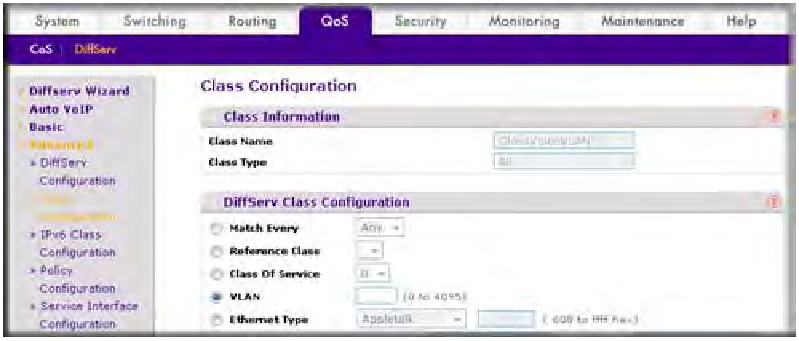
○ Class Of Service 0

● VLAN 10 (0 to 4095)

○ Ethernet Type Appletalk (600 to ffff hex)

Figure 3-35

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

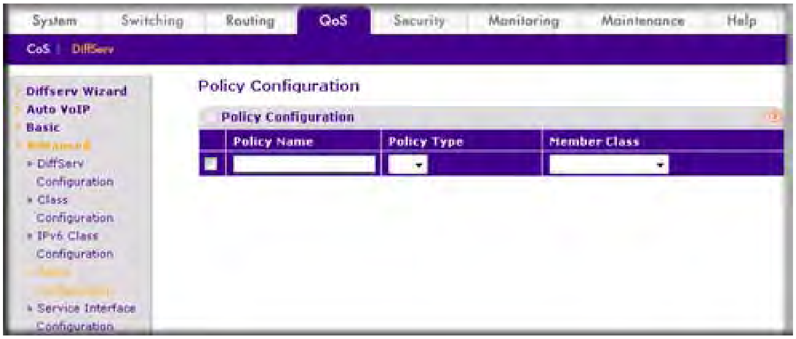
● VLAN (0 to 4095)

○ Ethernet Type Appletalk (600 to ffff hex)

Figure 3-36

7. Create DiffServ Policy PolicyVoiceVLAN.

a. From the main menu, select QoS > Advanced > Policy Configuration. A screen similar to the following displays.



Policy Configuration

Policy Configuration

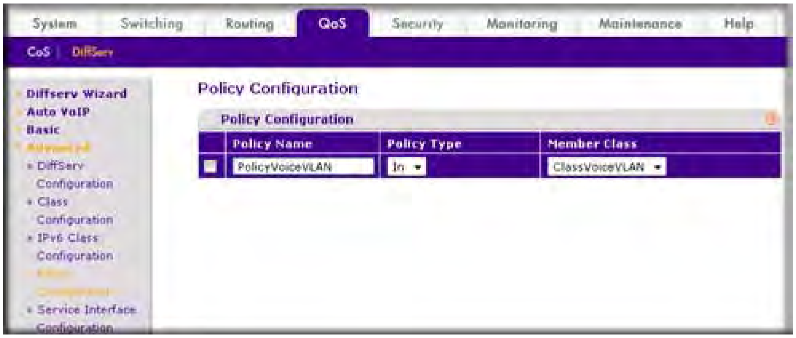
	Policy Name	Policy Type	Member Class
☐			

Figure 3-37

b. Enter Policy Name as **PolicyVoiceVLAN**.

c. Select Policy Type as **In**.

d. Select Member Class as **ClassVoiceVLAN**. A screen similar to the following displays.



Policy Configuration

Policy Configuration

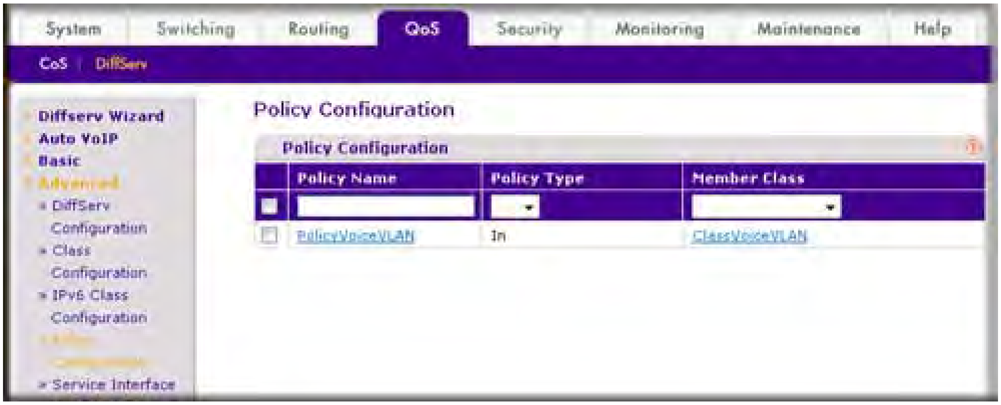
	Policy Name	Policy Type	Member Class
☐	PolicyVoiceVLAN	In	ClassVoiceVLAN

Figure 3-38

e. Click **Add**. A screen similar to the one in Figure 3-39 displays.

8. Map the Policy and Class and assign to the higher priority queue.

a. From the main menu, select QoS > Advanced > Policy Configuration. A screen similar to the following displays.



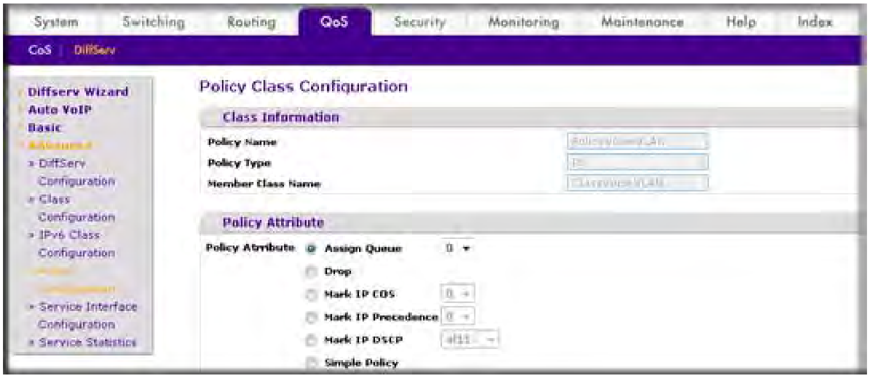
Policy Configuration

Policy Configuration

	Policy Name	Policy Type	Member Class
□			
□	PolicyVoiceVLAN	In	ClassVoiceVLAN

Figure 3-39

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



Policy Class Configuration

Class Information

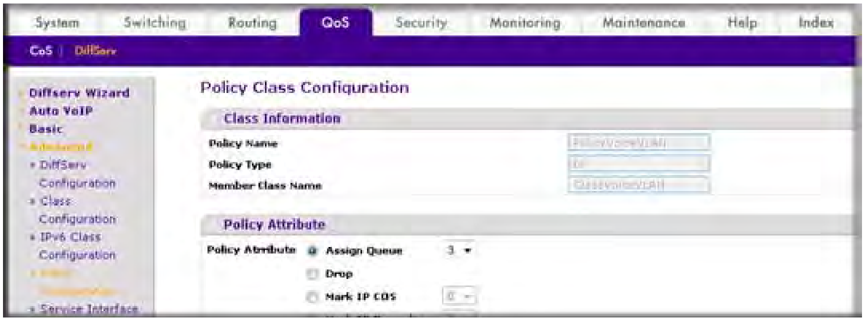
Policy Name	PolicyVoiceVLAN
Policy Type	In
Member Class Name	ClassVoiceVLAN

Policy Attribute

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

Figure 3-40

c. Select Assign Queue as **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

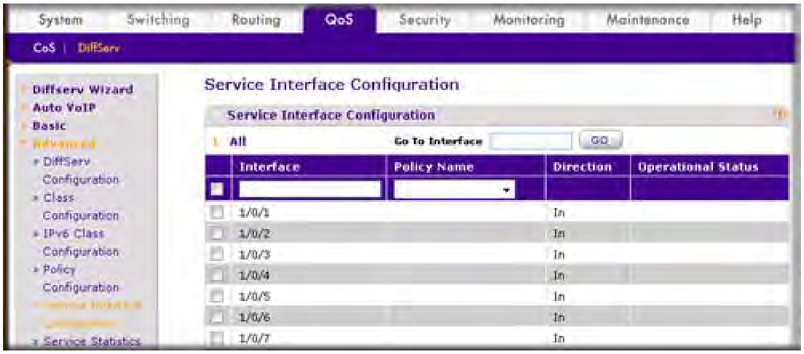
Policy Attribute ● Assign Queue 3
○ Drop
○ Mark IP COS 0

Figure 3-41

d. Click **Apply**.

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

a. From the main menu, select QoS > Advanced > Service Interface Configuration. A screen similar to the following displays.



Service Interface Configuration

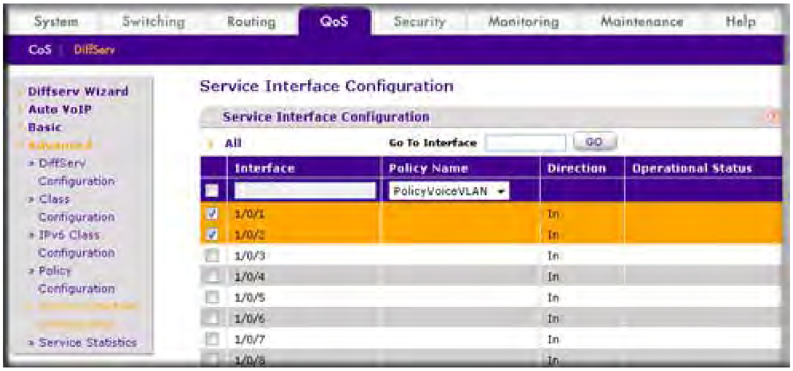
Service Interface Configuration

	Interface	Policy Name	Direction	Operational Status
□				
□	1/0/1		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	

Figure 3-42

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

c. Select Policy Name as **PolicyVoiceVLAN**. A screen similar to the following displays.



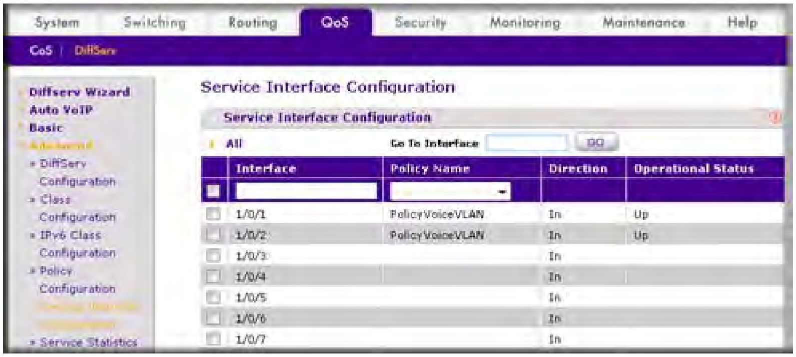
Service Interface Configuration

Service Interface Configuration

☐	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	

Figure 3-43

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	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	

Figure 3-44

Chapter 4
Link Aggregation

This chapter includes instructions for configuring Link Aggregation (LAG). The following examples are provided:

- "Create Two LAGs" on page 4-2
- "Add the Ports to the LAGs" on page 4-3
- "Enable Both LAGs" on page 4-5

Link Aggregation (LAG) allows the switch to treat multiple physical links between two end-points as a single logical link. All the physical links in a given LAG must operate in full-duplex mode at the same speed. LAG 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.

LAG offers the following benefits:

- Increased reliability and availability—if one of the physical links in the LAG goes down, traffic is dynamically and transparently reassigned to one of the other physical links.
- Better use of physical resources—traffic can be load-balanced across the physical links.
- Increased bandwidth—the aggregated physical links deliver higher bandwidth than each individual link.
- Incremental increase in bandwidth—a physical upgrade could produce a 10-times increase in bandwidth; LAG produces a two- or five-times increase, useful if only a small increase is needed.

Create Two LAGs

The following figure shows the example network.

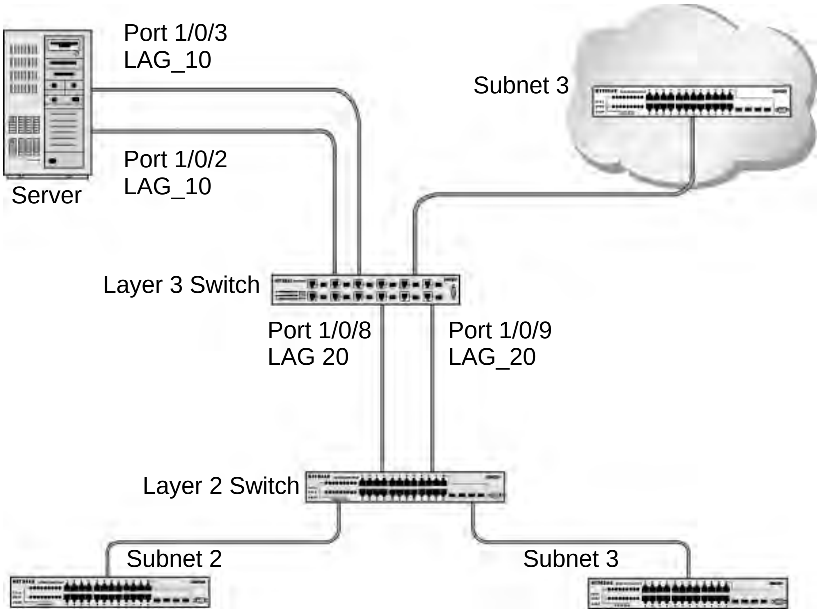


Figure 4-1

CLI: Creating Two LAGs

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

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

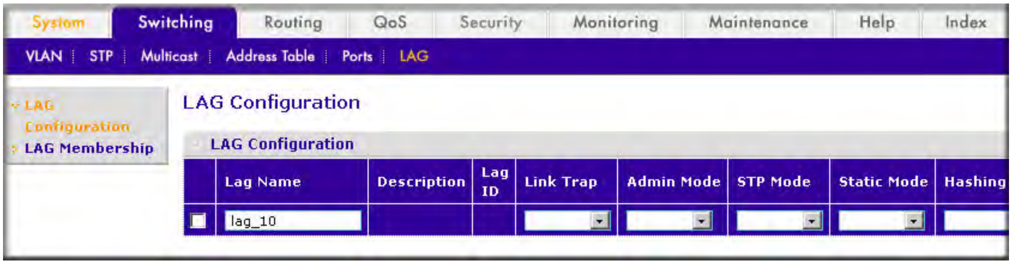
```
(Console) #show port-channel all
            Port-                  Link
Log.       Channel           Adm. Trap  STP           Mbr       Port    Port
Intf        Name        Link  Mode Mode  Mode    Type   Ports     Speed   Active
------ -------------- ------ ---- ---- ------ ------- ------ ---------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

Web Interface: Creating Two LAGs

To use the Web interface to configure the managed switch, proceed as follows:

1. Create LAG lag_10.

   a. From the main menu, 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_10							

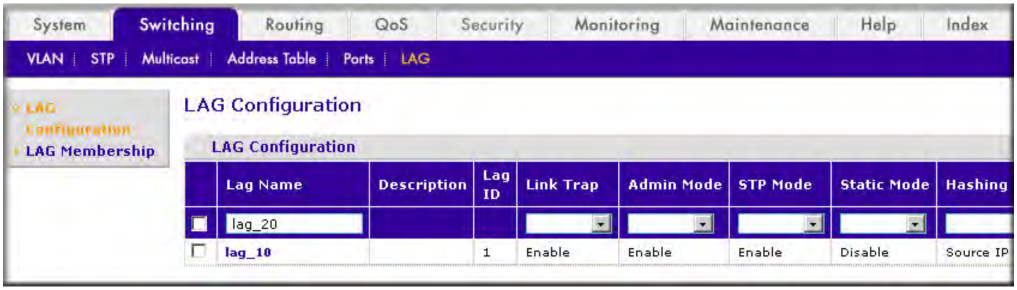
Figure 4-2

   b. In the Lag Name field, enter **lag_10**.

   c. Click the **Add**.

2. Create LAG lag_20.

   a. From the main menu, 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

Figure 4-3

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

   c. Click **Add**.

Add the Ports to the LAGs

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

CLI: Adding the Ports to the LAGs

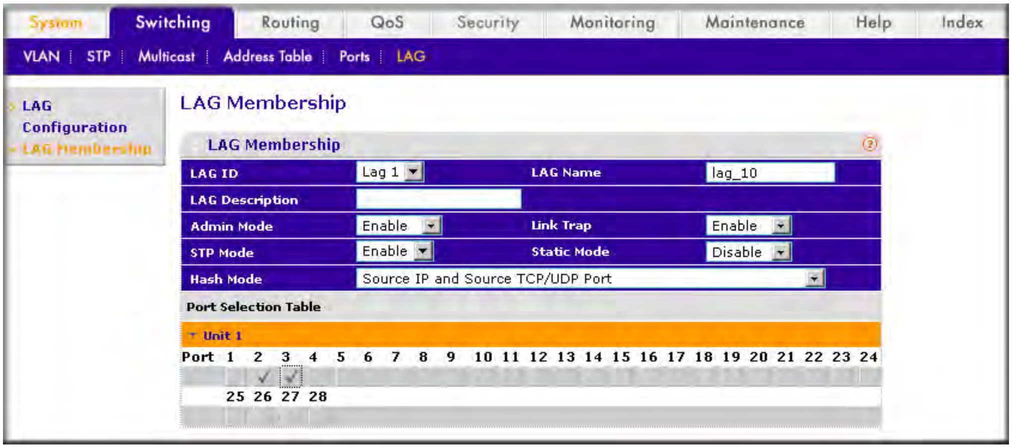
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 0/2
(Netgear Switch) (Interface 0/2)#addport 1/1
(Netgear Switch) (Interface 0/2)#exit
(Netgear Switch) (Config)#interface 0/3
(Netgear Switch) (Interface 0/3)#addport 1/1
(Netgear Switch) (Interface 0/3)#exit
(Netgear Switch) (Config)#interface 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: Adding the Ports to the LAGs

To use the Web interface to configure the switch, proceed as follows:

1. Add ports to the lag_10.

a. From the main menu, 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																				

Figure 4-4

b. Select the **Lag 1** in the LAG ID field.

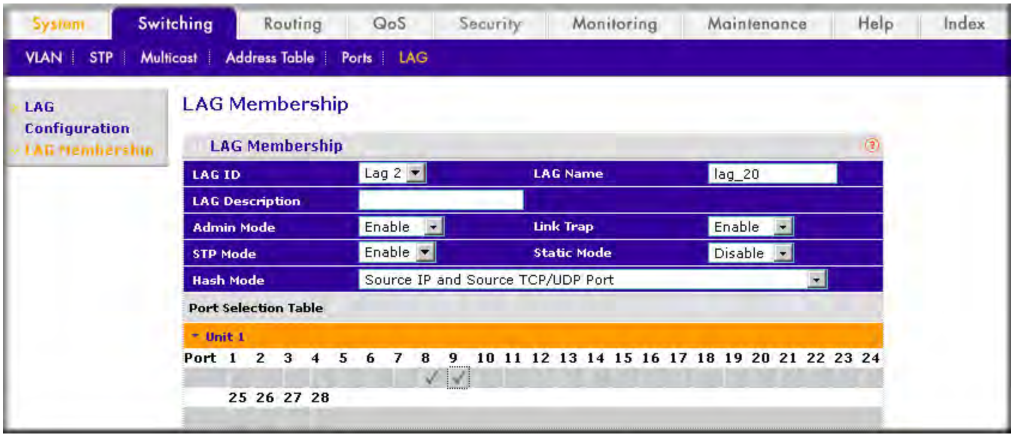
c. Click the **Unit 1.** The Ports display.

d. Click on the gray box under port **2** and **3**. Two flags appear in the box.

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

2. Add ports to the lag_20.

a. From the main menu, 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																				

Figure 4-5

b. Under the LAG Membership Configuration , enter the following information.

Select **Lag 2** in the LAG ID field.

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

d. Click on the gray box under port 8 and 9. Two flags appear in the box.

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

Enable Both LAGs

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

CLI: Enabling Both LAGs

By default, the system enables link trap notification

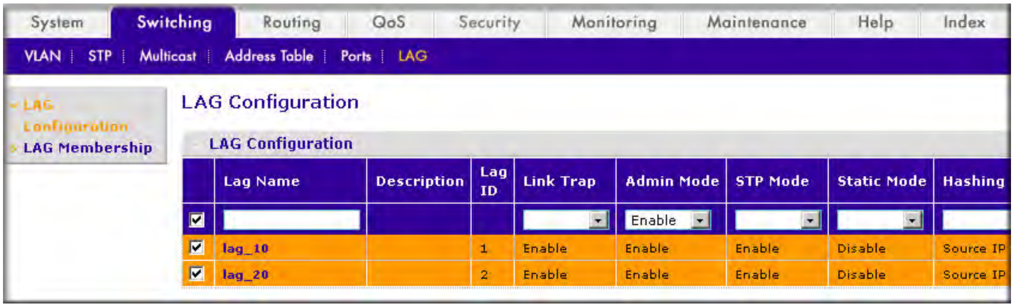
```
(Console) #config
(Console) (Config)#port-channel adminmode all
(Console) (Config)#exit
```

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

Web Interface: Enabling Both LAGs

To use the Web interface to configure the switch, proceed as follows:

a. From the main menu, 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

Figure 4-6

b. Select the checkbox on the top and the checkboxes for **lag_10** and **lag_20** are selected.

c. Select **Enable** in the Admin Mode field.

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

Chapter 5
Port Routing

In this chapter, the following examples are provided:

- "Enable Routing for the Switch" on page 5-2
- "Enable Routing for Ports on the Switch" on page 5-3
- "Adding a Default Route" on page 5-6
- "Adding a Static Route" on page 5-8

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 understand 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
- Recreate the Layer 2 header

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

Port Routing Configuration

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

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

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

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

You may 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.

Enable Routing for the Switch

This diagram shows a Layer 3 switch configured for port routing. It connects three different subnets, each connected to a different port. The script shows the commands you would use to configure a 7000 Series Managed Switch to provide the port routing support shown in the diagram.

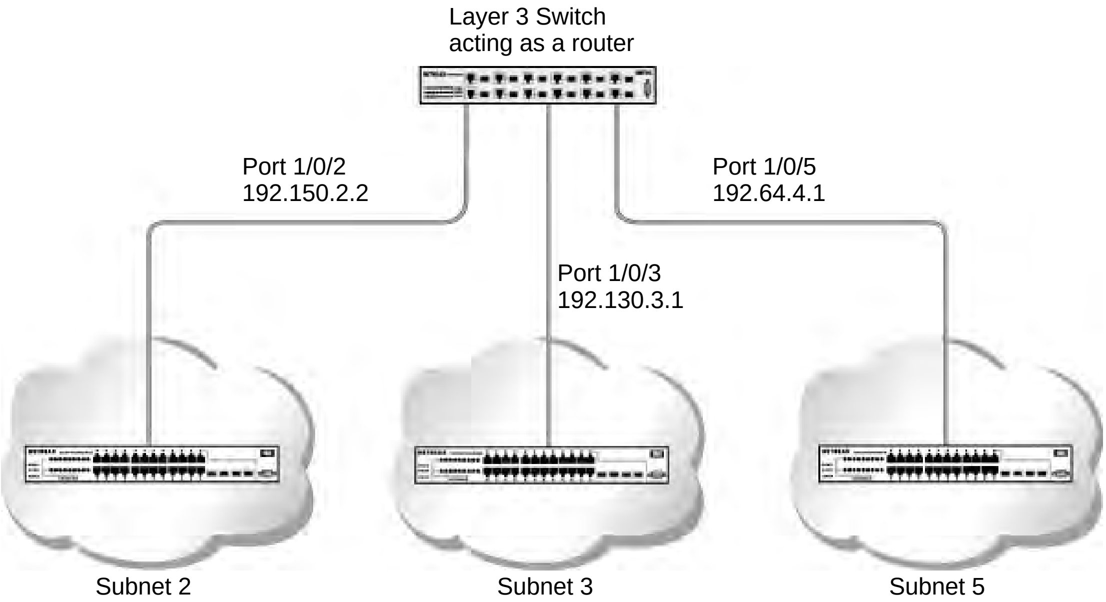


Figure 5-1

CLI: Enabling Routing for the Switch

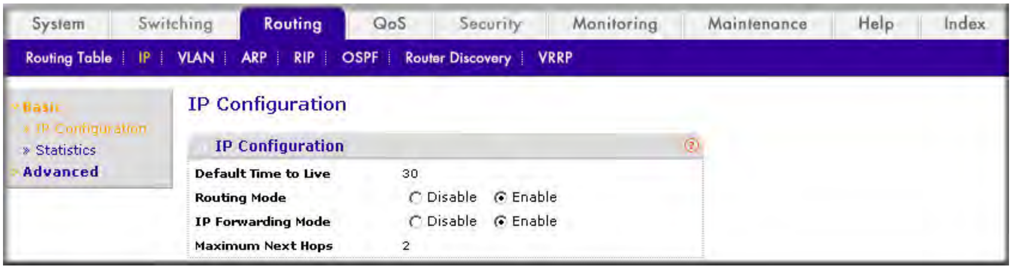
Use the following command to enable routing for the switch. Execution of the command enables IP forwarding by default.

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

Web Interface: Enabling Routing for the Switch

To use the Web interface to configure the managed switch, proceed as follows:

1. From the main menu, 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

Figure 5-2

2. Next to the 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 and the maximum transmission unit (MTU) size is 1500 bytes.

CLI: Enabling Routing for Ports on the Switch

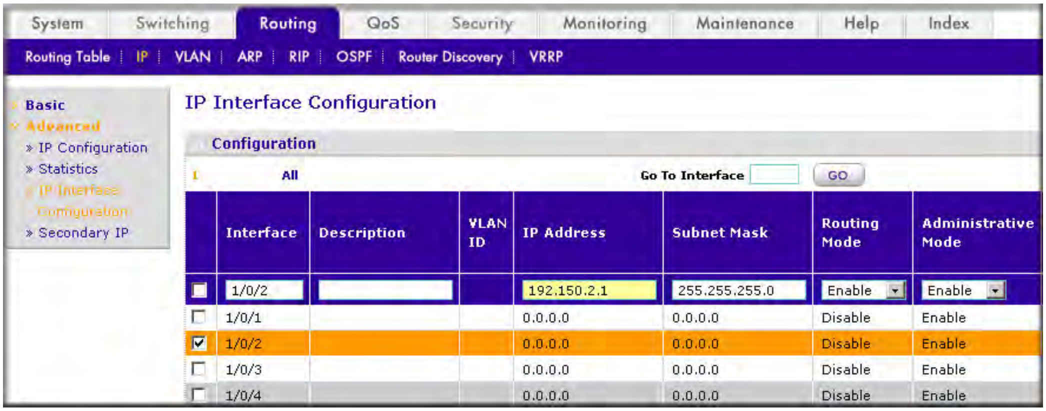
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit

(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: Enabling Routing for Ports on the Switch

To use the Web interface to configure the managed switch, proceed as follows:

1. Assign IP address 192.150.2.1/24 to the interface 1/0/2.

a. From the main menu, select Routing > Advanced >IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

Configuration

All Go To Interface GO

	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

Figure 5-3

b. Under IP Interface Configuration, scroll down to interface **1/0/2** and select the checkbox for that interface. Now 1/0/2 appears in the Interface field at the top.

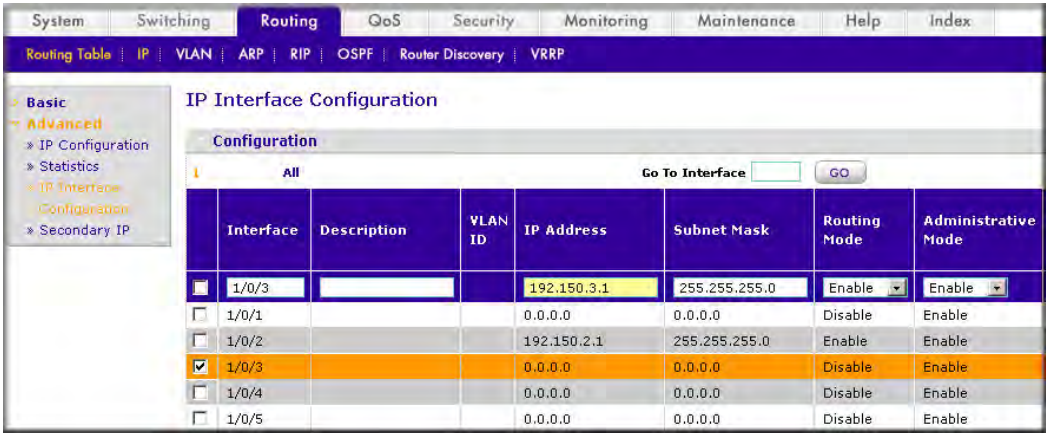
c. Under the IP Interface Configuration, enter the following information.

- In the IP Address field, enter **192.150.2.1**.
- In the Subnet Mask field, enter **255.255.255.0**.
- Select **Enable** in Routing Mode field.

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

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

a. From the main menu, select Routing > 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
□	1/0/3			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

Figure 5-4

b. Under IP Interface Configuration, scroll down to interface **1/0/3** and select the checkbox for that interface. Now 1/0/3 appears in the Interface field at the top.

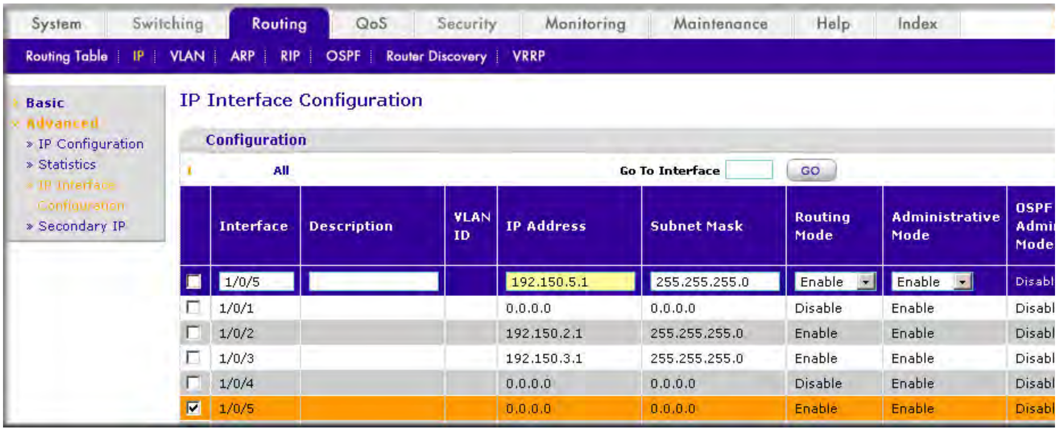
c. Under the IP Interface Configuration, enter the following information.

- In the IP Address field, enter **192.150.3.1**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

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

a. From the main menu, select Routing > Advanced >IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

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

Figure 5-5

b. Under IP Interface Configuration, scroll down to interface **1/0/5** and select the checkbox for that interface. Now 1/0/5 appears in the Interface field at the top.

c. Under the IP Interface Configuration, enter the following information.

- In the IP Address field, enter **192.150.5.1**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

Adding a Default Route

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

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

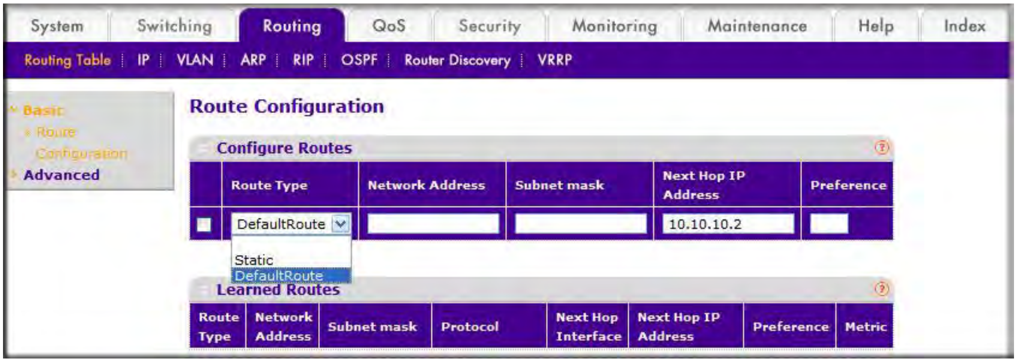
CLI: Add a Default Route

```
(FSM7338S) (Config) #ip route default ?

<nexthopip> Enter the IP Address of the next router.

(FSM7328S) (Config)#ip route default 10.10.10.2
```

Note that IP subnet “10.10.10.0” should be configured via either Port Routing Configuration example either or VLAN Routing Configuration in the next chapter. See

Web Interface: Add a Default Route

1. Go to Routing > Routing Table > Route Configuration. The Route Configuration page 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

Figure 5-6

1. From the Route Type drop down menu, select **DefaultRoute**.
2. Enter one of the routing interface’s IP addresses in the **Next Hop IP Address** field.
   - 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.
3. Click the **Add** button on the bottom of the page. This creates the Default Route entry into the route table.

Adding a Static Route

If your network switch has multiple routing interface that would allow different forwarding path to be taken for reaching the same destination, it may make sense to create static route to force the packet to take certain route (port) instead of the default route. The following procedure shows how to add static route to the switch routing table.

CLI Command Procedure:

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

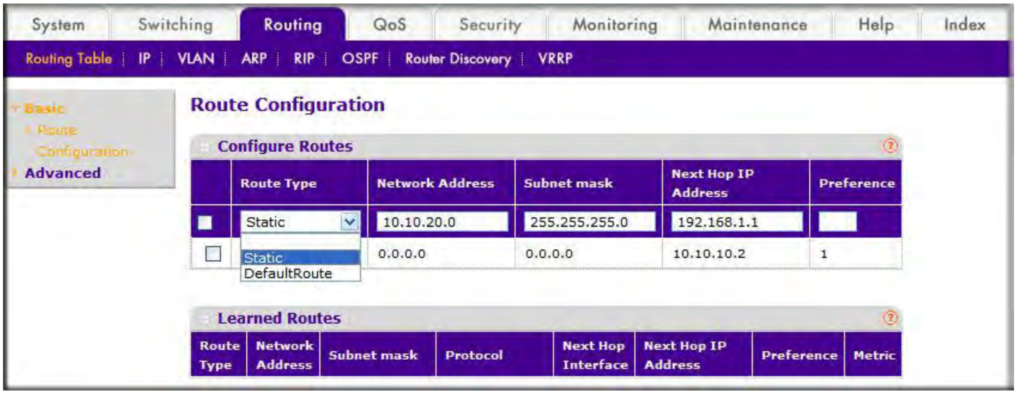
```
(FSM7328S) #show ip route

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 Procedure

To configure a static route:

1. Go to Routing > Routing Table > Route Configuration to display the Route Configuration page.



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	
□	Static DefaultRoute	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

Figure 5-7

2. Select **Static** in the **Route Type** field.
3. Enter **Network Address** field. Noted this field is expecting a network IP address, not a host IP address. Do not put down something like “10,100.100.1”. The last number should always be zero.
4. Enter **Subnet Mask** that matches the subnet range desired.
5. **The Preference** field is optional. A value of one will be chosen if nothing is entered.
6. Click the **Add** button on the bottom of this page. The web page will be updated with static route shown in the route table.
7. To remove the route entry, either static or default, simply check the box on the left hand side of the entry, and click the **Delete** button on the bottom of the page.

Chapter 6
VLAN Routing

In this chapter, the following examples are provided:

- "Create Two VLANs"
- "Set Up VLAN Routing for the VLANs and the Switch" on page 6-6
- "Click Add to save the settings." on page 6-8

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

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

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

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

Create Two VLANs

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

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

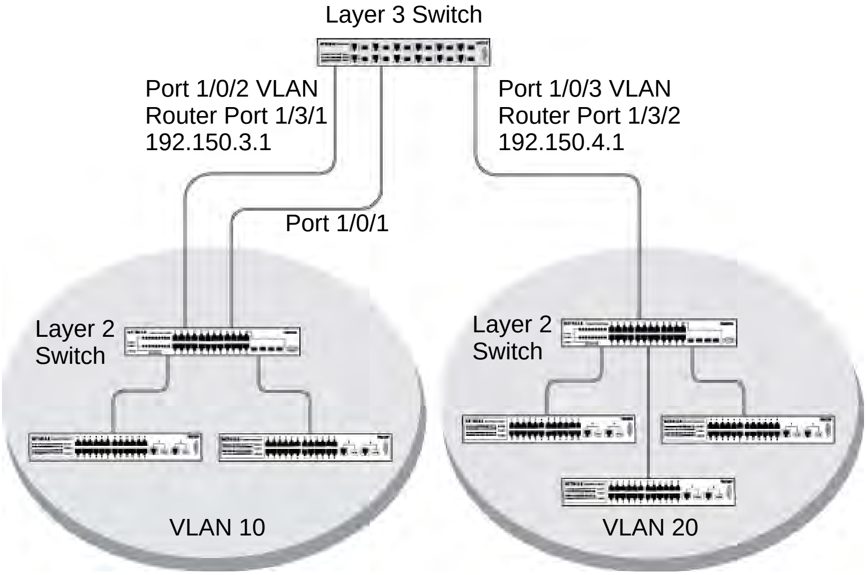


Figure 6-1

CLI: Creating Two VLANs

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

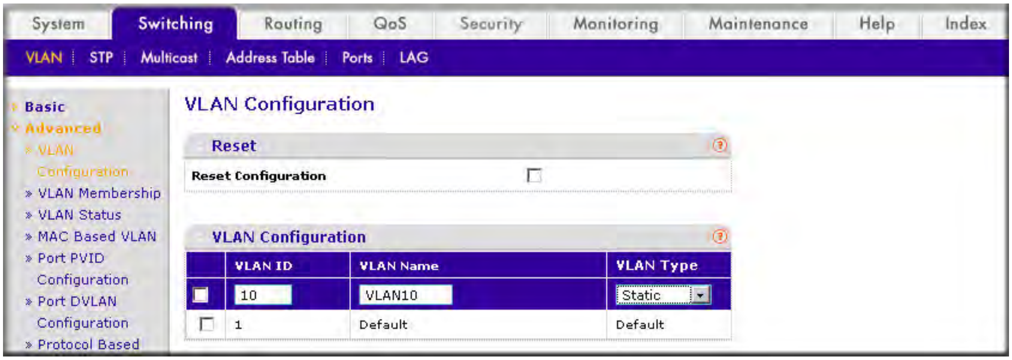
```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 10
(Netgear Switch) (Vlan)#vlan 20
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #conf
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan participation include 10
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan 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: Creating Two VLANs

To use the Web interface to configure the managed switch, proceed as follows:

1. Create VLAN 10, VLAN20.

   a. From the main menu, 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

Figure 6-2

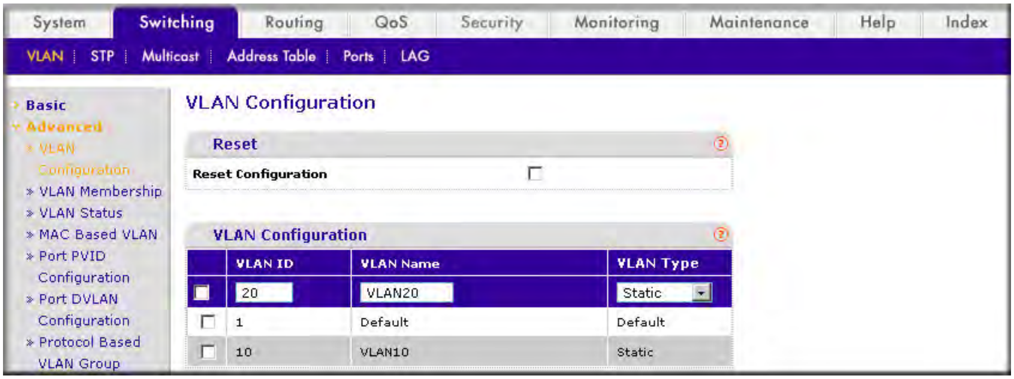
   b. In the VLAN ID field, enter **10**

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

   d. Select **Static** in the VLAN Type field.

   e. Click **Add**.

   f. From the main menu, 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

Figure 6-3

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

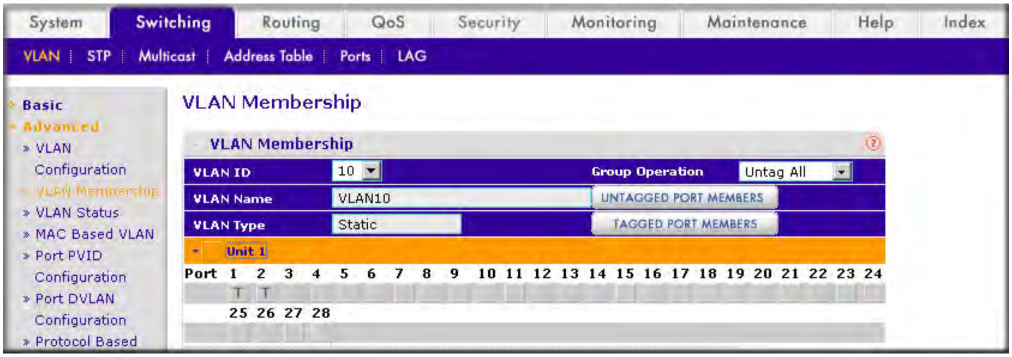
h. In the VLAN Name field, enter **VLAN20**.

i. Select **Static** in the VLAN Type field.

j. Click **Add**.

2. Add ports to the VLAN10 and VLAN20.

a. From the main menu, select Switching > VLAN >Advanced > VLAN Membership. A screen similar to the following displays.



VLAN Membership

VLAN ID: 10

Group Operation: Untag All

VLAN Name: VLAN10

VLAN Type: Static

Port 1: T

Port 2: T

Figure 6-4

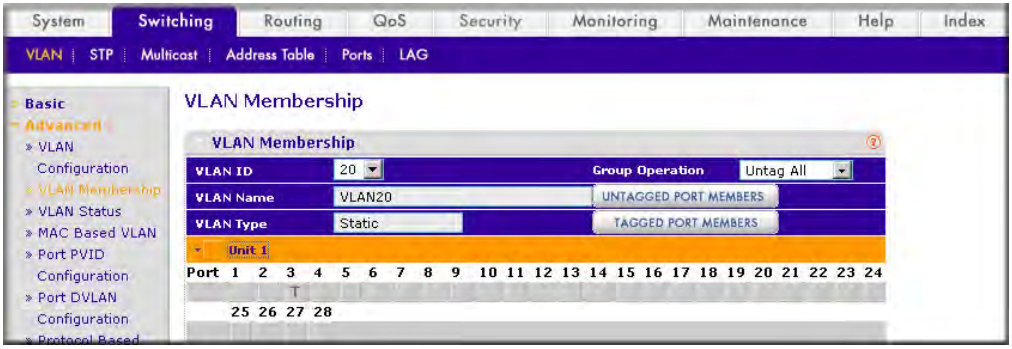
b. Select **10** in the VLAN ID field.

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

d. Click the gray box under port **1** and **2** until T displays. The T specifies that the egress packet is tagged for the port.

e. Click **Apply**.

f. From the main menu, select Switching > VLAN >Advanced > VLAN Membership. A screen similar to the following displays.



VLAN Membership

VLAN ID: 20

Group Operation: Untag All

VLAN Name: VLAN20

VLAN Type: Static

Port 3: T

Figure 6-5

g. Select **20** in the VLAN ID field.

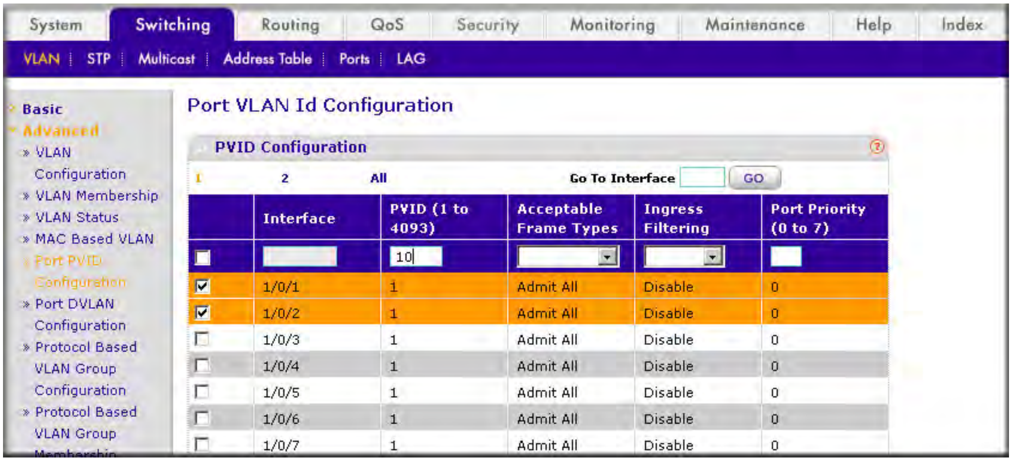
h. Click the **Unit 1**. The Ports display.

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 the VLAN10 and VLAN20.

a. From the main menu, select Switching > VLAN> Advanced > Port PVID Configuraton. 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)
□		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

Figure 6-6

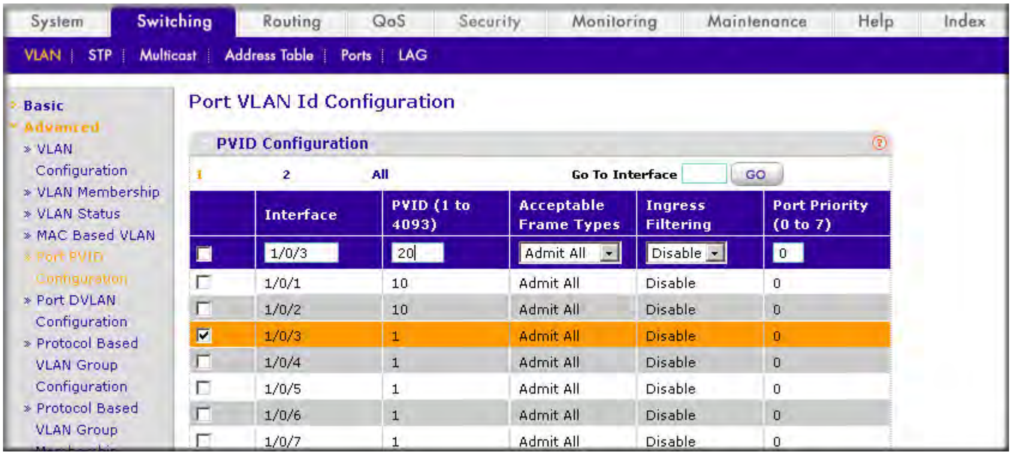
b. Under PVID Configuration, scroll down to interface 1/0/1 and select the checkbox for 1/0/1. Then scroll down to the interface 1/0/2 and select the checkbox for 1/0/2.

c. Enter the following information in the PVID Configuration.

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

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

f. From the main menu, select Switching > VLAN> Advanced > Port PVID Configuraton. 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

Figure 6-7

g. Under PVID Configuration, scroll down to interface 1/0/3 and select the checkbox for 1/0/3.

h. Enter the following information in the PVID Configuration.

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

i. 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: Setting Up VLAN Routing for the VLANs and the Switch

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 slot/port in subsequent routing commands. Assume that VLAN 10 is assigned ID 3/1 and VLAN 20 is assigned ID 3/2.

Enable routing for the switch:

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

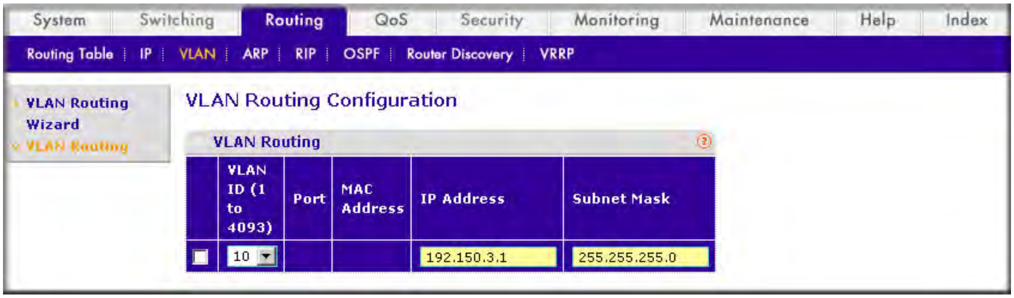
The next sequence shows an example of configuring the IP addresses and subnet masks for the virtual router ports.

```
(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: Setting Up VLAN Routing for the VLANs and the Switch

To use the Web interface to configure the managed switch, proceed as follows:

1. From the main menu, select Routing > VLAN> VLAN Routing > VLAN Routing Configuration. 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

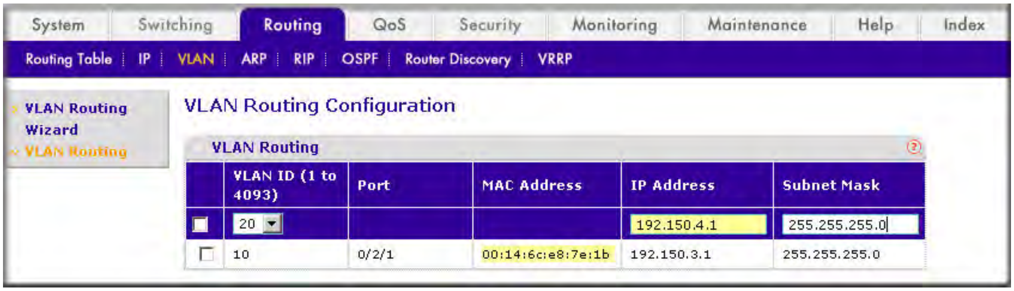
Figure 6-8

2. Under the VLAN Routing Configuration, enter the following information.

- Select **10** in the VLAN ID(1 to 4093) field.
- In the IP Address field, enter **192.150.3.1**.
- In the Subnet Mask filed, enter **255.255.255.0**.

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

4. From the main menu, select Routing > VLAN> VLAN Routing > VLAN Routing Configuration. 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:e8:7e:1b	192.150.3.1	255.255.255.0

Figure 6-9

5. Under the VLAN Routing Configuration, 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 filed, enter **255.255.255.0**.

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

Chapter 7
Routing Information Protocol

In this chapter, the following examples are provided:

- "Enable Routing for the Switch" on page 7-2
- "Enable Routing for Ports" on page 7-3
- "Enable RIP for the Switch" on page 7-5
- "Enable RIP for Ports 1/0/2 and 1/0/3" on page 7-6
- "VLAN Routing RIP Configuration" on page 7-8

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

A router running RIP will send the contents of its routing table to each of its adjacent routers every 30 seconds. When a route is removed from the routing table it will be flagged as unusable by the receiving routers after 180 seconds, and removed from their tables after an additional 120 seconds.

There are two versions of RIP:

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

The 7000 Series Managed Switch supports both versions of RIP. You may configure a given port:

- To receive packets in either or both formats
- To transmit packets formatted for RIPv1 or RIPv2 or to send RIPv2 packets to the RIPv1 broadcast address
- To prevent any RIP packets from being received
- To prevent any RIP packets from being transmitted

The configuration commands used in the following example enable RIP on ports 1/0/2 and 1/0/3 as shown in the network illustrated in Figure 7-1

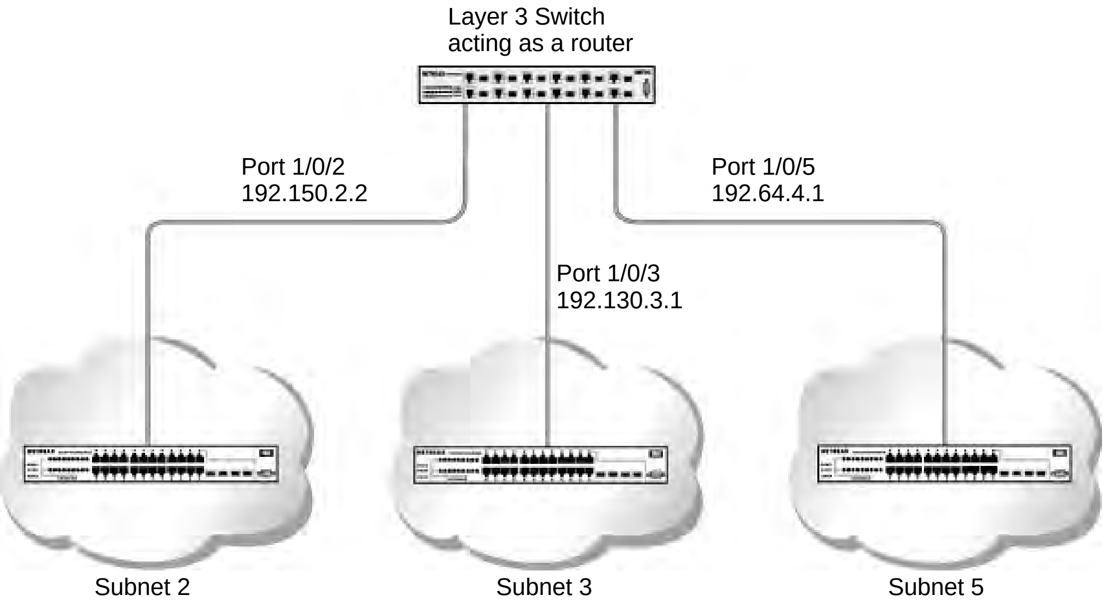


Figure 7-1

Enable Routing for the Switch

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

CLI: Enabling Routing for the Switch

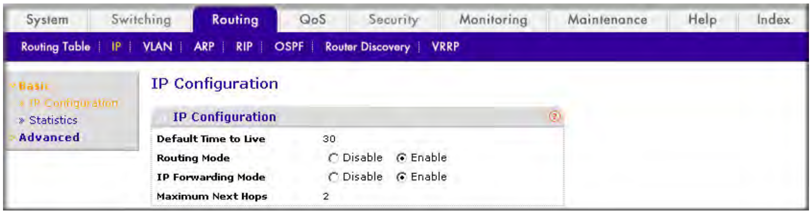
The following sequence enables routing for the switch:

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

Web Configuration: Enabling Routing for the Switch

To use the Web interface to configure the managed switch, proceed as follows:

1. From the main menu, 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

Figure 7-2

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

Enable Routing for Ports

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

CLI: Enabling Routing for Ports

Enable routing and assigns IP addresses for ports 1/0/2 and 1/0/3.

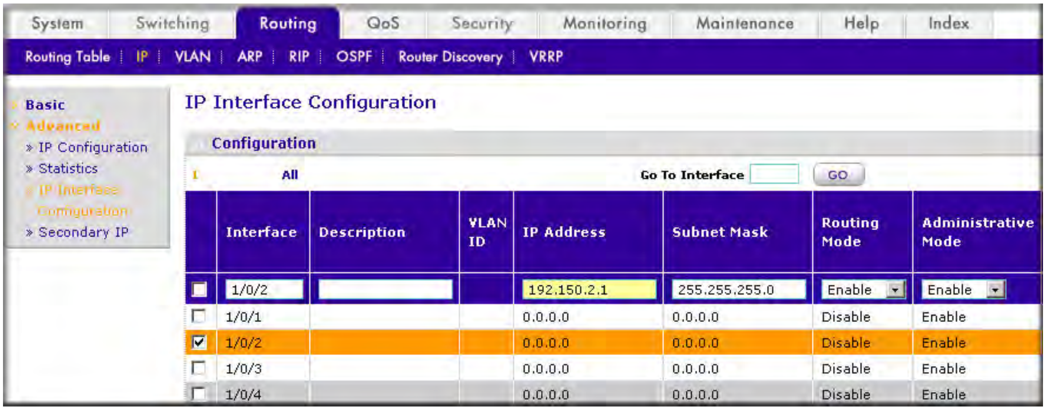
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing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

Web Interface: Enabling Routing for the Ports

To use the Web interface to configure the managed switch, proceed as follows:

1. Assign IP address 192.150.2.1/24 to the interface 1/0/2.

a. From the main menu, 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
□	1/0/2			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

Figure 7-3

b. Under IP Interface Configuration, scroll down to interface **1/0/2** and select the checkbox for that interface. Now 1/0/2 appears in the Interface field at the top.

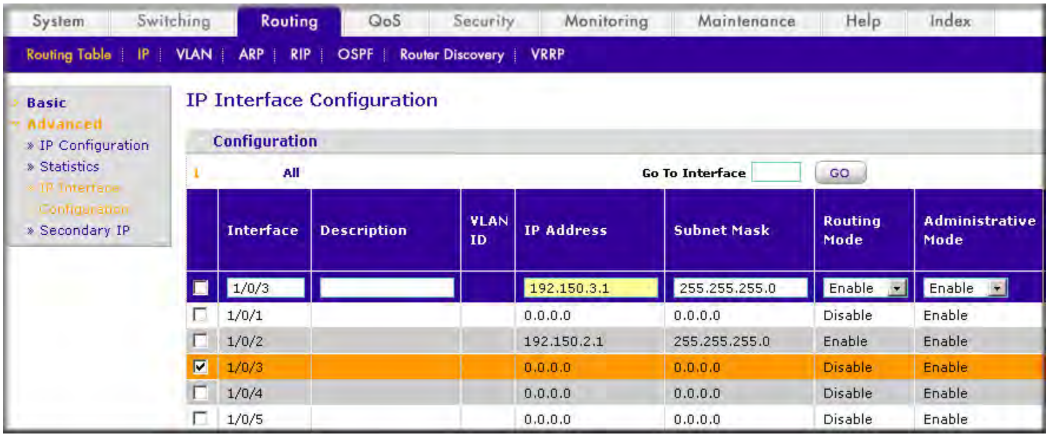
c. Under the IP Interface Configuration, enter the following information.

- In the IP Address field, enter **192.150.2.1**.
- In the Subnet Mask field, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

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

a. From the main menu, select Routing > Advanced >IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

Configuration

1 All

Go To Interface

	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

Figure 7-4

b. Under IP Interface Configuration, scroll down to interface **1/0/3** and select the checkbox for that interface. Now 1/0/3 appears in the Interface field at the top.

c. Under the IP Interface Configuration, enter the following information.

- In the IP Address field, enter **192.150.3.1**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

Enable RIP for the Switch

Note: This step can be skipped since the RIP is enabled by default.

CLI: Enabling RIP for the Switch

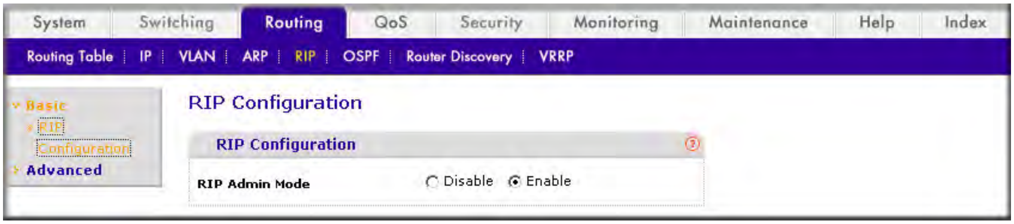
The next sequence enables RIP for the switch. the route preference defaults to 15.

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

Web Interface: Enabling RIP on the Switch

To use the Web interface to configure the managed switch, proceed as follows:

1. From the main menu, select Routing > RIP > Basic>RIP Configuration. A screen similar to the following displays.



RIP Configuration

RIP Configuration

RIP Admin Mode ○ Disable ● Enable

Figure 7-5

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

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

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

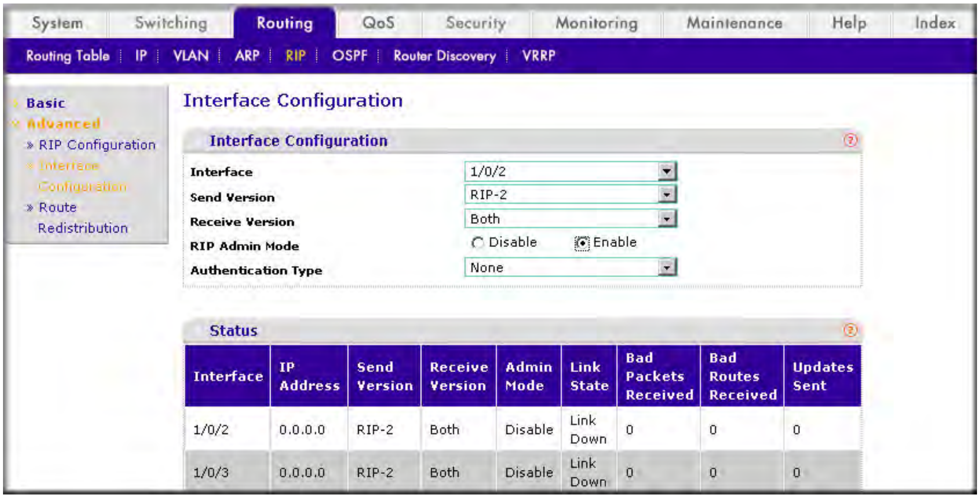
CLI: Enabling RIP for Ports 1/0/2 and 1/0/3

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

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

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

1. From the main menu, select Routing > RIP > Advanced>RIP Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/2
Send Version	RIP-2
Receive Version	Both
RIP Admin Mode	○ Disable ● Enable
Authentication Type	None

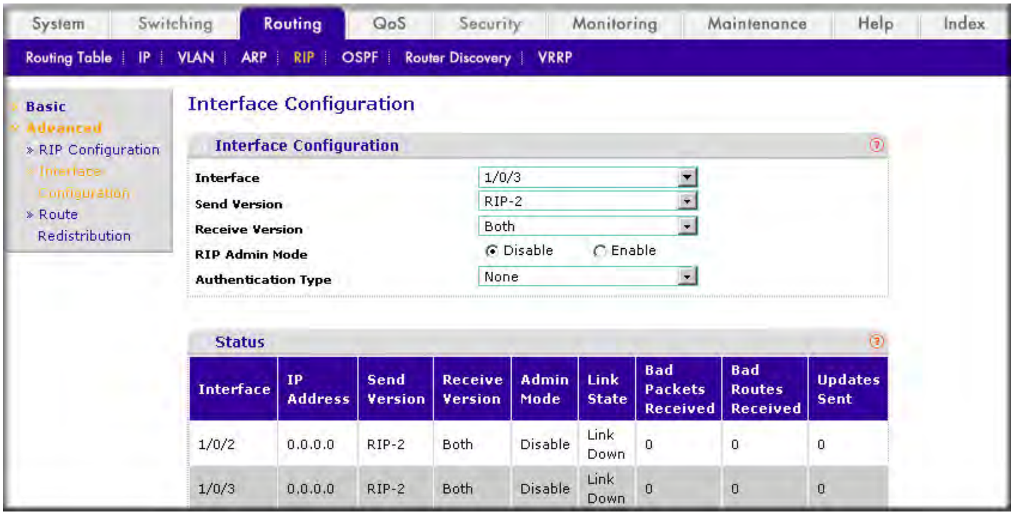
Status

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

Figure 7-6

2. Under the Interface Configuration, enter the following information.
   - Select **1/0/2** in the Interface field.
   - Next to RIP Admin Mode, select the **Enable** Radio button.
   - Select **RIP-2** in the Send Version field.
3. Click **Apply** to save the settings.

4. From the main menu, select Routing > RIP > Advanced>RIP Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/3
Send Version	RIP-2
Receive Version	Both
RIP Admin Mode	● Disable ○ Enable
Authentication Type	None

Status

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

Figure 7-7

5. Under the Interface Configuration, enter the following information.
   - Select **1/0/3** in the Interface field.
   - Next to RIP Admin Mode, select **Enable** Radio button.
   - Select **RIP-2** in the Send Version field.
6. Click **Apply** to save the settings.

VLAN Routing RIP Configuration

Routing Information Protocol (RIP) is one of the protocols which may be used by routers to exchange network topology information. It is characterized as an “interior” gateway protocol, and is typically used in small to medium-sized networks.

A router running RIP will send the contents of its routing table to each of its adjacent routers every 30 seconds. When a route is removed from the routing table it will be flagged as unusable by the receiving routers after 180 seconds, and removed from their tables after an additional 120 seconds.

There are two versions of RIP:

- RIPv1 defined in RFC 1058
  – Routes are specified by IP destination network and hop count
  – The routing table is broadcast to all stations on the attached network

- RIPv2 defined in RFC 1723
  - Route specification is extended to include subnet mask and gateway
  - The routing table is sent to a multicast address, reducing network traffic
  - An authentication method is used for security

The 7000 Series Managed Switch supports both versions of RIP. You may configure a given port to:

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

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

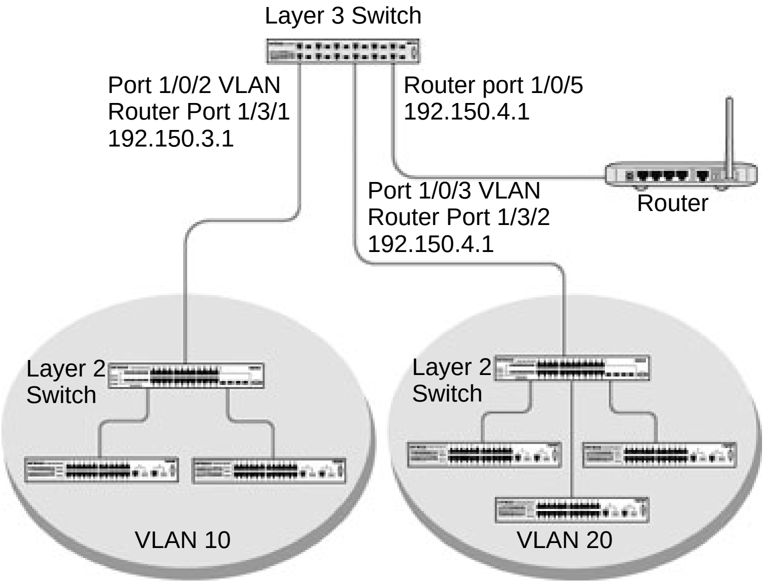


Figure 7-8

CLI: VLAN Routing RIP Configuration

Example of configuring VLAN Routing with RIP support on a 7000 Series Managed Switch.

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

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

Enable RIP for the switch. The route preference will default to 15.

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

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

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

Enable RIP for the VLAN router ports. Authentication will default to none, and no default route entry will be created.

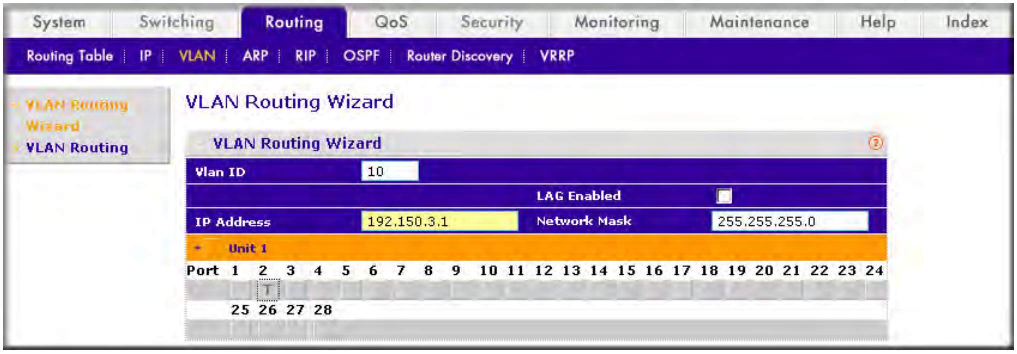
```
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip rip
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip rip
(Netgear Switch) (Interface vlan 20)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: VLAN Routing RIP Configuration

To use the Web interface to configure RIP on the switch, proceed as follows:

1. Configure a VLAN and include ports 1/0/2 in the VLAN:

   a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.



VLAN Routing Wizard

VLAN Routing Wizard

Vlan ID 10

LAG Enabled □

IP Address 192.150.3.1 Network Mask 255.255.255.0

Unit 1

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

T (port 2)

25 26 27 28

Figure 7-9

   b. Enter the following information in the VLAN Routing Wizard:
      - In the Vlan ID field, enter **10**.
      - In the IP Address field, enter **192.150.3.1**.
      - In the Network Mask field, enter **255.255.255.0**.

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

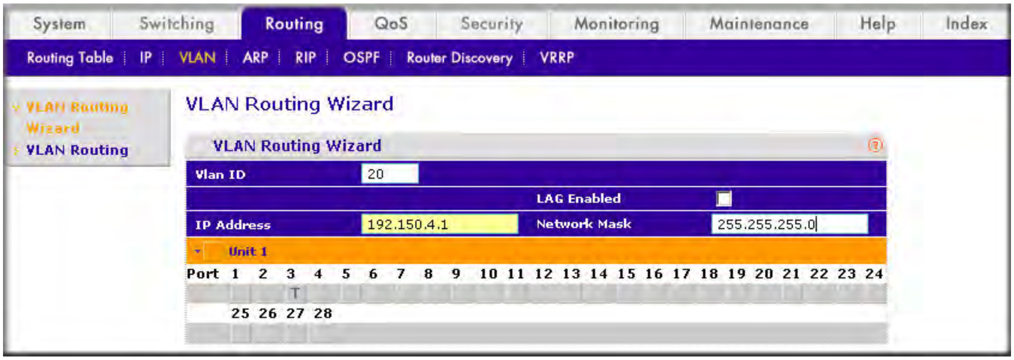
      Click the gray box under port 2 once until **T** displays.

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

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

2. Configure a VLAN and include ports 1/0/3 in the VLAN:

a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.



VLAN Routing Wizard

VLAN Routing Wizard

Vlan ID 20

LAG Enabled □

IP Address 192.150.4.1 Network Mask 255.255.255.0

Unit 1

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

Figure 7-10

b. Enter the following information in the VLAN Routing Wizard:

- In the Vlan ID field, enter **20**.
- In the IP Address field, enter **192.150.4.1**.
- In the Network Mask field, enter **255.255.255.0**.

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

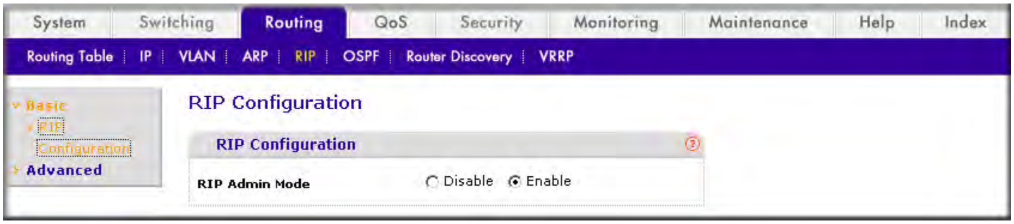
- Click the gray box under port 3 once until **T** displays.

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

d. Click **Apply** to save the VLAN that includes ports 3.

3. Enable RIP on the switch (this step can be skipped since the RIP is enabled by default).

a. From the main menu, select Routing > RIP > Basic>RIP Configuration. A screen similar to the following displays.



RIP Configuration

RIP Configuration

RIP Admin Mode ○ Disable ● Enable

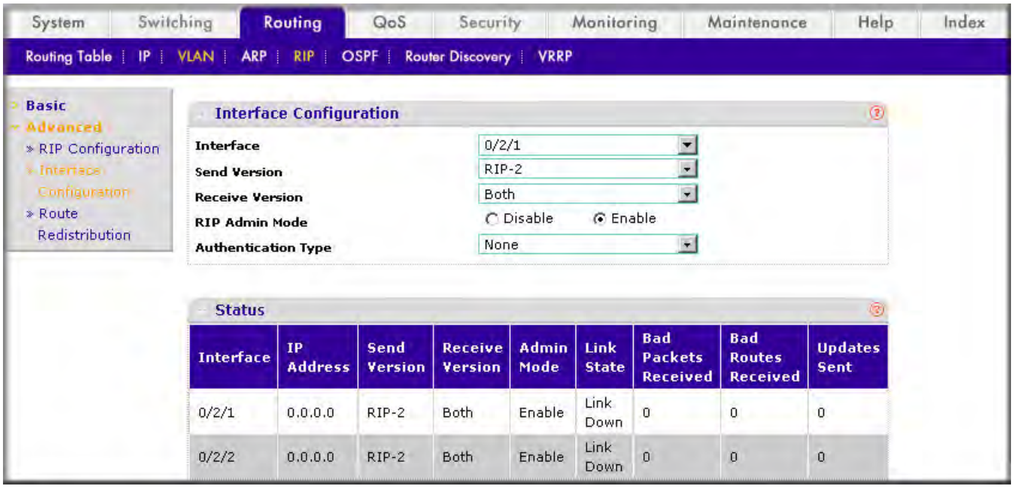
Figure 7-11

b. Next to the RIP Admin Mode, select **Enable** radio button.

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

4. Enable RIP on the VLAN 10 and 20.

a. From the main menu, select Routing > RIP > Advanced>RIP Configuration. A screen similar to the following displays.



Interface Configuration

Interface	0/2/1
Send Version	RIP-2
Receive Version	Both
RIP Admin Mode	○ Disable ● Enable
Authentication Type	None

Status

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

Figure 7-12

b. Under the Interface Configuration, enter the following information.

- Select **0/2/1** in the Interface field.
- Next to RIP Admin Mode, select **Enable** Radio button.

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

Chapter 8
OSPF

In this chapter, the following examples are provided:

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

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

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

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

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

Configure an Inter-Area Router

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

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

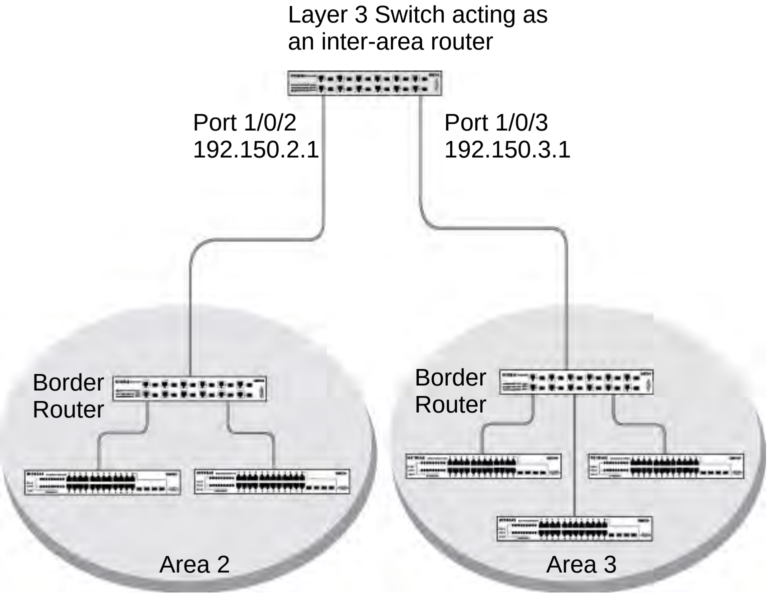


Figure 8-1

CLI: Configuring an Inter-Area Router

Step 1: Enable Routing for the switch.

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

Step 2: Assign IP addresses for ports.

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

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

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

Step 4: Enable OSPF and set the OSPF priority and cost for the ports.

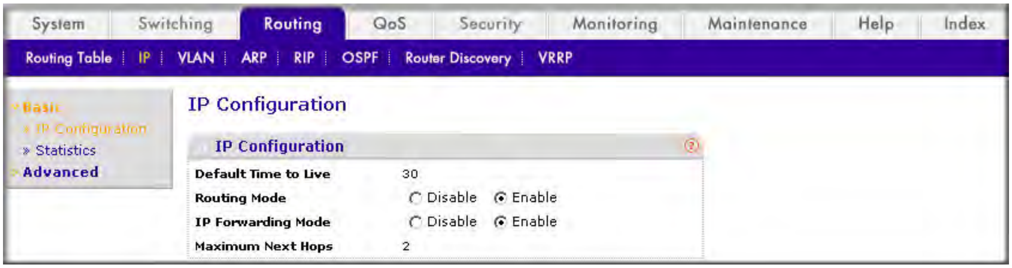
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip ospf
(Netgear Switch) (Interface 1/0/2)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/2)#ip ospf priority 128
(Netgear Switch) (Interface 1/0/2)#ip ospf cost 32
(Netgear Switch) (Interface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

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

Web Interface: Configuring an Inter-Area Router

To use the Web interface to configure OSPF on the switch, proceed as follows:

1. Enable IP routing on the switch:

   a. From the main menu, select Routing > IP > 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

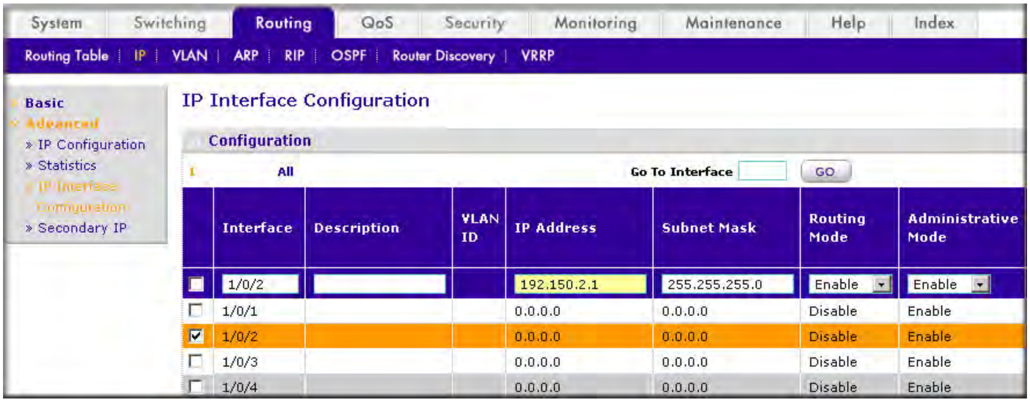
Figure 8-2

   b. Next to the Routing Mode, select the Enable radio button.

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

2. Assign IP address 192.150.2.1 to the port 1/0/2.

   a. From the main menu, select Routing > IP > Advanced> IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

Configuration

1 All Go To Interface

	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

Figure 8-3

   b. Under IP Interface Configuration, scroll down to interface **1/0/2** and select the checkbox for that interface. Now 1/0/2 appears in the Interface field at the top.

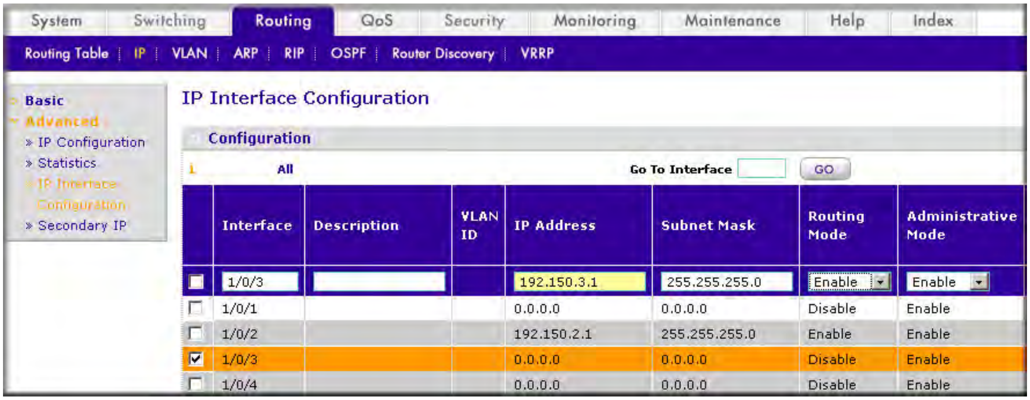
   c. Enter the following information in the IP Interface Configuration:

      - In the IP Address field, enter **192.150.2.1**.
      - In the Subnet Mask field, enter **255.255.255.0**.
      - Select **Enable** in the Administrative Mode field.

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

3. Assign IP address 192.150.3.1 to the port 1/0/3:

a. From the main menu, select Routing > IP > Advanced> IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

	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

Figure 8-4

b. Under IP Interface Configuration, scroll down to interface **1/0/3** and select the checkbox for that interface. Now 1/0/3 appears in the Interface field at the top.

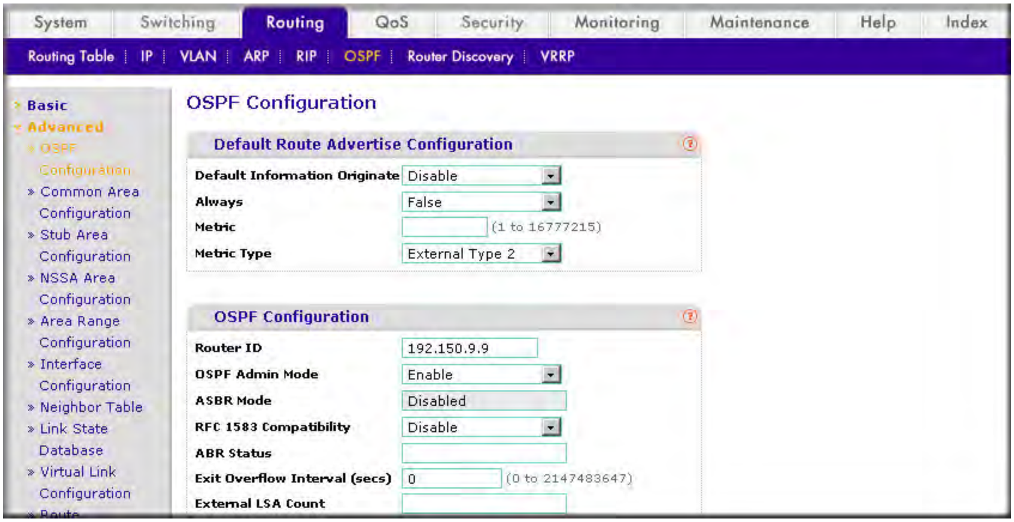
c. Enter the following information in the IP Interface Configuration:

- In the IP Address field, enter **192.150.3.1**.
- In the Network Mask field, enter **255.255.255.0**.
- Select **Enable** in the Admin Mode field.

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

4. Specify the Router ID and Enable OSPF for the switc.h

a. From the main menu, select Routing > OSPF > Advanced> OSPF Configuration. A screen similar to the following displays.



OSPF Configuration

Default Route Advertise Configuration

Default Information Originate	Disable
Always	False
Metric	(1 to 16777215)
Metric Type	External Type 2

OSPF Configuration

Router ID	192.150.9.9
OSPF Admin Mode	Enable
ASBR Mode	Disabled
RFC 1583 Compatibility	Disable
ABR Status	
Exit Overflow Interval (secs)	0 (0 to 2147483647)
External LSA Count	

Figure 8-5

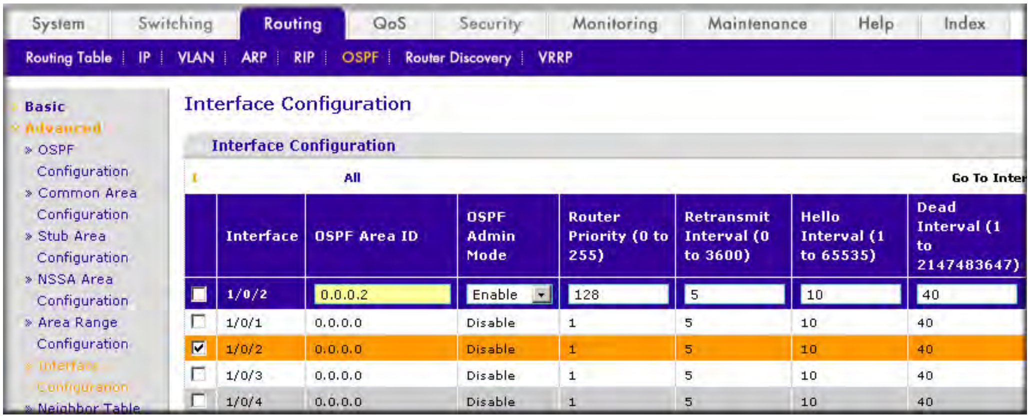
b. Under the OSPF Configuration, enter the following information:

- In the Router ID, enter **192.150.9.9**.
- Select **Enable** in the OSPF Admin Mode field.
- Select **Disable** in the RFC 1583 Compatibility field.

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

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

a. From the main menu, select Routing > OSPF > Advanced> Interface Configuration. A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Routing Table | IP | VLAN | ARP | RIP | OSPF | Router Discovery | VRRP
Basic
Advanced
» OSPF Configuration
» Common Area Configuration
» Stub Area Configuration
» NSSA Area Configuration
» Area Range Configuration
» Interface Configuration
» Neighbor Table
All
Go To Inter

Interface Configuration

Interface Configuration

	Interface	OSPF Area ID	OSPF Admin Mode	Router Priority (0 to 255)	Retransmit Interval (0 to 3600)	Hello Interval (1 to 65535)	Dead Interval (1 to 2147483647)
□	1/0/2	0.0.0.2	Enable	128	5	10	40
□	1/0/1	0.0.0.0	Disable	1	5	10	40
☑	1/0/2	0.0.0.0	Disable	1	5	10	40
□	1/0/3	0.0.0.0	Disable	1	5	10	40
□	1/0/4	0.0.0.0	Disable	1	5	10	40

Figure 8-6

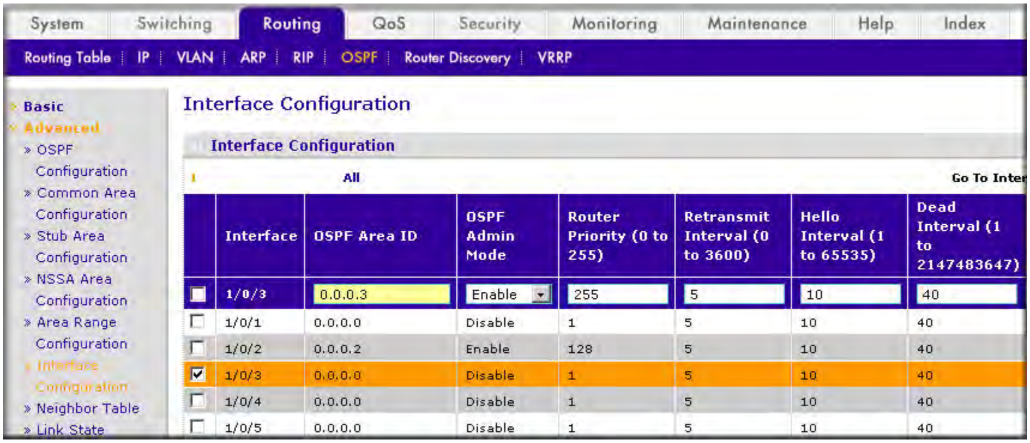
b. Under Interface Configuration, scroll down to interface **1/0/2** and select the checkbox for that interface. Now 1/0/2 appears in the Interface field at the top.

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

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

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

a. From the main menu, select Routing > OSPF > Advanced> Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

	Interface	OSPF Area ID	OSPF Admin Mode	Router Priority (0 to 255)	Retransmit Interval (0 to 3600)	Hello Interval (1 to 65535)	Dead Interval (1 to 2147483647)
□	1/0/3	0.0.0.3	Enable	255	5	10	40
□	1/0/1	0.0.0.0	Disable	1	5	10	40
□	1/0/2	0.0.0.2	Enable	128	5	10	40
☑	1/0/3	0.0.0.0	Disable	1	5	10	40
□	1/0/4	0.0.0.0	Disable	1	5	10	40
□	1/0/5	0.0.0.0	Disable	1	5	10	40

Figure 8-7

b. Under Interface Configuration, scroll down to interface **1/0/3** and select the checkbox for that interface. Now 1/0/3 appears in the Interface field at the top.

- In the OSPF Area ID field, enter **0.0.0.3**.
- Select the **Enable** in the OSPF Admin Mode field.
- In the Priority field, enter **255**.
- In the Metric Cost field, enter **64**.

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

Configure OSPF on a Border Router

The example is shown as CLI commands and as a Web interface procedure. For an OSPF example network, see Figure 8-1 on page 8-2.

CLI: Configuring OSPF on a Border Router

Enable routing for the switch.

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

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

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

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

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

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

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

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

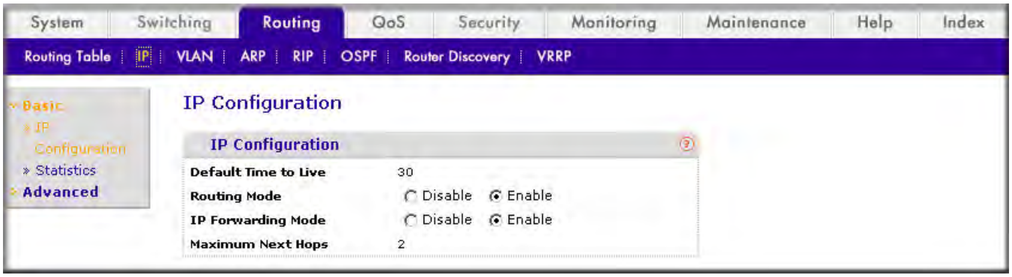
```
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#ip ospf
(Netgear Switch) (Interface 1/0/4)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/4)#ip ospf priority 255
(Netgear Switch) (Interface 1/0/4)#ip ospf cost 64
(Netgear Switch) (Interface 1/0/4)#exit
(Netgear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

Web Interface: Configuring OSPF on a Border Router

To use the Web interface to configure OSPF on the switch, proceed as follows:

1. Enable IP routing on the switch:

a. From the main menu, select Routing > IP > 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

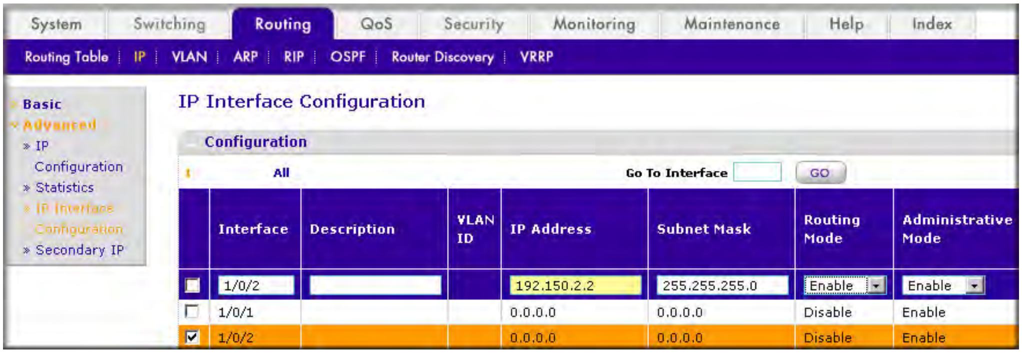
Figure 8-8

b. Next to the Routing Mode, select the **Enable** radio button.

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

2. Assign IP address 192.150.2.2 to the port 1/0/2:

a. From the main menu, 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
□	1/0/2			192.150.2.2	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

Figure 8-9

b. Under IP Interface Configuration, scroll down to interface **1/0/2** and select the checkbox for that interface. Now 1/0/2 appears in the Interface field at the top.

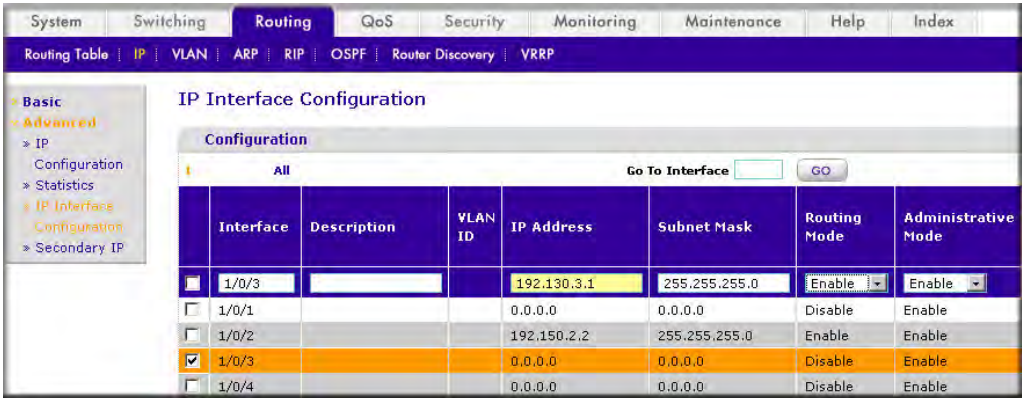
c. Enter the following information in the IP Interface Configuration:

- In the IP Address field, enter **192.150.2.2**.
- In the Network Mask field, enter **255.255.255.0**.
- Select **Enable** in the Admin Mode field.

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

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

a. From the main menu, 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
□	1/0/3			192.130.3.1	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable
□	1/0/2			192.150.2.2	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

Figure 8-10

b. Under IP Interface Configuration, scroll down to interface **1/0/3** and select the checkbox for that interface. Now 1/0/3 appears in the Interface field at the top.

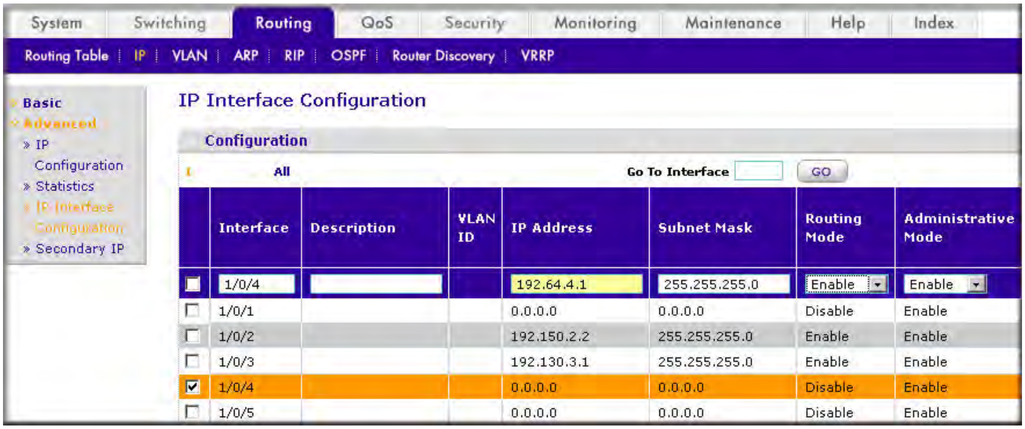
c. Enter the following information in the IP Interface Configuration:

- In the IP Address field, enter **192.130.3.1**.
- In the Network Mask field, enter **255.255.255.0**.
- Select **Enable** in the Admin Mode field.

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

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

a. From the main menu, 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
☐	1/0/4			192.64.4.1	255.255.255.0	Enable	Enable
☐	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable
☐	1/0/2			192.150.2.2	255.255.255.0	Enable	Enable
☐	1/0/3			192.130.3.1	255.255.255.0	Enable	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

Figure 8-11

b. Under IP Interface Configuration, scroll down to interface **1/0/4** and select the checkbox for that interface. Now 1/0/4 appears in the Interface field at the top.

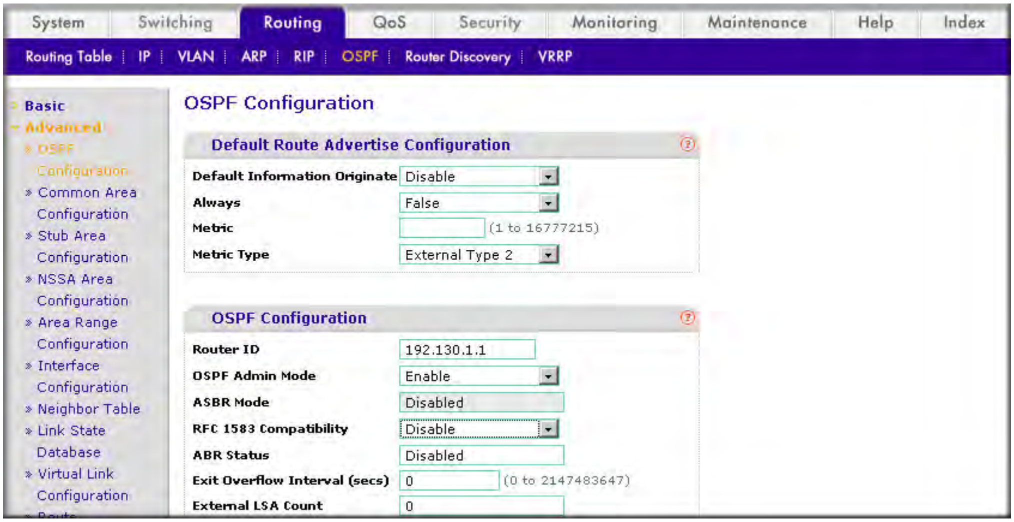
c. Enter the following information in the IP Interface Configuration:

- In the IP Address field, enter **192.64.4.1**.
- In the Network Mask field, enter **255.255.255.0**.
- Select **Enable** in the Admin Mode field.

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

5. Specify the Router ID and Enable OSPF for the switch

a. From the main menu, select Routing > OSPF > Advanced> OSPF Configuration. A screen similar to the following displays.



OSPF Configuration

Default Route Advertise Configuration

Default Information Originate	Disable
Always	False
Metric	(1 to 16777215)
Metric Type	External Type 2

OSPF Configuration

Router ID	192.130.1.1
OSPF Admin Mode	Enable
ASBR Mode	Disabled
RFC 1583 Compatibility	Disable
ABR Status	Disabled
Exit Overflow Interval (secs)	0 (0 to 2147483647)
External LSA Count	0

Figure 8-12

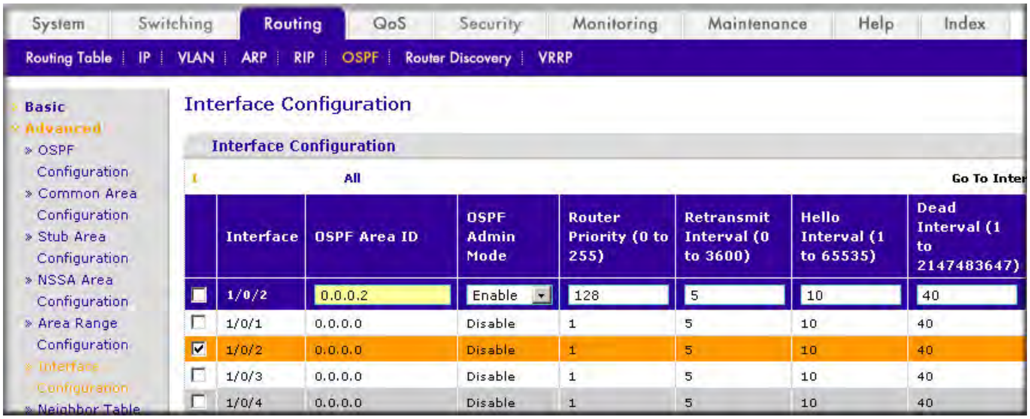
b. Under the OSPF Configuration, enter the following information:

- In the Router ID, enter **192.130.1.1**.
- Select the **Enable** in the OSPF Admin Mode field.
- Select the **Disable** in the RFC 1583 Compatibility field.

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

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

a. From the main menu, select Routing > OSPF > Advanced> Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

	Interface	OSPF Area ID	OSPF Admin Mode	Router Priority (0 to 255)	Retransmit Interval (0 to 3600)	Hello Interval (1 to 65535)	Dead Interval (1 to 2147483647)
□	1/0/2	0.0.0.2	Enable	128	5	10	40
□	1/0/1	0.0.0.0	Disable	1	5	10	40
☑	1/0/2	0.0.0.0	Disable	1	5	10	40
□	1/0/3	0.0.0.0	Disable	1	5	10	40
□	1/0/4	0.0.0.0	Disable	1	5	10	40

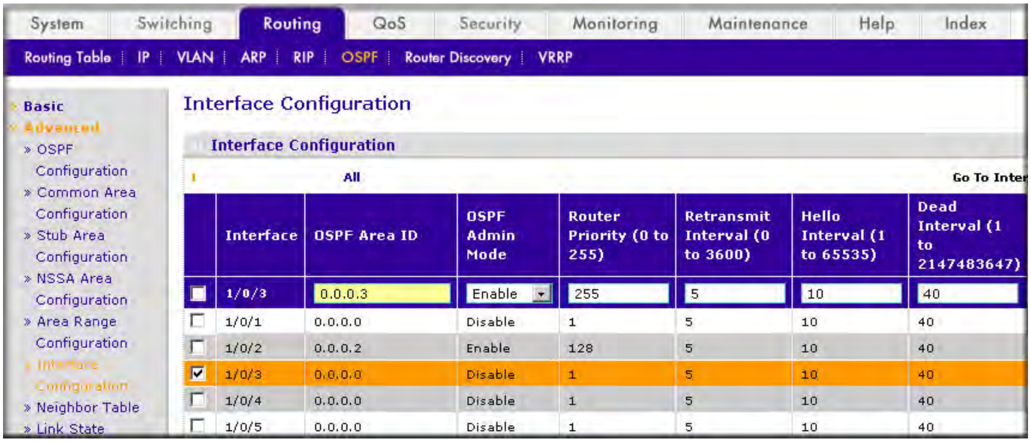
Figure 8-13

b. Under Interface Configuration, scroll down to interface **1/0/2** and select the checkbox for that interface. Now 1/0/2 appears in the Interface field at the top.
  - In the OSPF Area ID field, enter **0.0.0.2**.
  - Select the **Enable** in the OSPF Admin Mode field.
  - In the Priority field, enter **128**.
  - In the Metric Cost field, enter **32**.

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

7. Enable OSPF on the port 1/0/3.

a. From the main menu, select Routing > OSPF > Advanced> Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

All

Go To Inter

	Interface	OSPF Area ID	OSPF Admin Mode	Router Priority (0 to 255)	Retransmit Interval (0 to 3600)	Hello Interval (1 to 65535)	Dead Interval (1 to 2147483647)
□	1/0/3	0.0.0.3	Enable	255	5	10	40
□	1/0/1	0.0.0.0	Disable	1	5	10	40
□	1/0/2	0.0.0.2	Enable	128	5	10	40
☑	1/0/3	0.0.0.0	Disable	1	5	10	40
□	1/0/4	0.0.0.0	Disable	1	5	10	40
□	1/0/5	0.0.0.0	Disable	1	5	10	40

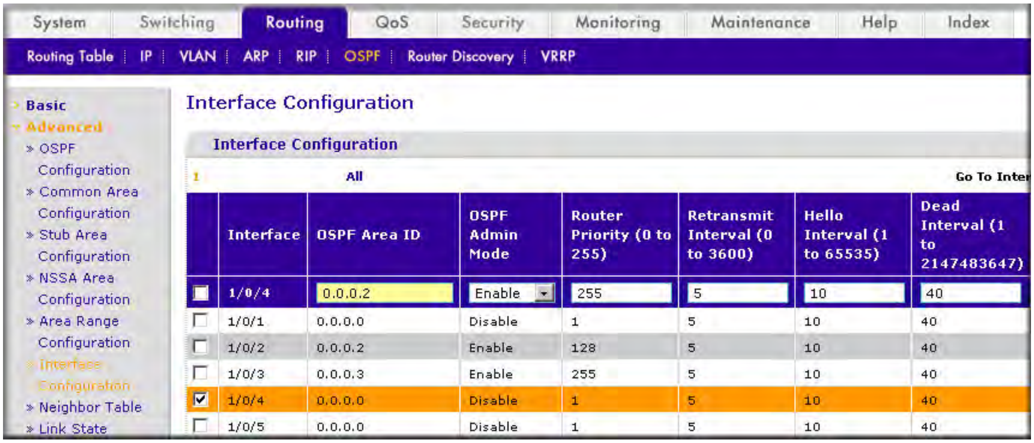
Figure 8-14

b. Under Interface Configuration, scroll down to interface **1/0/3** and select the checkbox for that interface. Now 1/0/3 appears in the Interface field at the top.
  - In the OSPF Area ID field, enter **0.0.0.3**.
  - Select the **Enable** in the OSPF Admin Mode field.
  - In the Priority field, enter **255**.
  - In the Metric Cost field, enter **64**.

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

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

a. From the main menu, select Routing > OSPF > Advanced> Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

1 All Go To Inter

	Interface	OSPF Area ID	OSPF Admin Mode	Router Priority (0 to 255)	Retransmit Interval (0 to 3600)	Hello Interval (1 to 65535)	Dead Interval (1 to 2147483647)
□	1/0/4	0.0.0.2	Enable	255	5	10	40
□	1/0/1	0.0.0.0	Disable	1	5	10	40
□	1/0/2	0.0.0.2	Enable	128	5	10	40
□	1/0/3	0.0.0.3	Enable	255	5	10	40
☑	1/0/4	0.0.0.0	Disable	1	5	10	40
□	1/0/5	0.0.0.0	Disable	1	5	10	40

Figure 8-15

b. Under Interface Configuration, scroll down to interface **1/0/4** and select the checkbox for that interface. Now 1/0/4 appears in the Interface field at the top.

- In the OSPF Area ID field, enter **0.0.0.2**.
- Select the **Enable** in the OSPF Admin Mode field.
- In the Priority field, enter **255**.
- In the Metric Cost field, enter **64**.

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

Configure Area 1 as a Stub Area

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

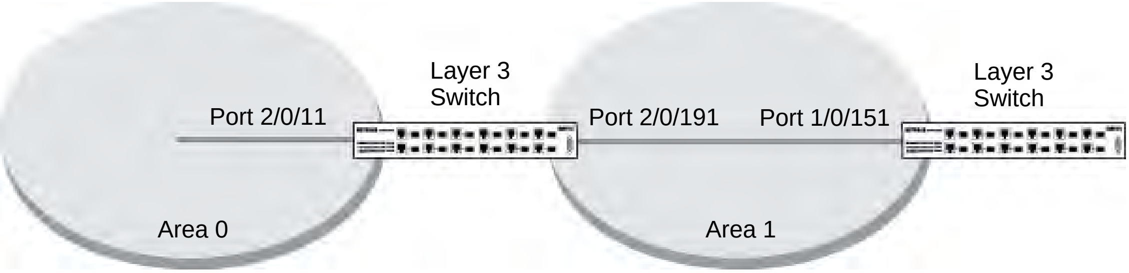


Figure 8-16

CLI: Configuring Area 1 as a Stub Area on A1

Enable routing on the switch.

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

Set the router id to 1.1.1.1.

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

Configure the area 0.0.0.1 as a stub area**.**

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

Switch A only inject a default route to the area 0.0.0.1.

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

Enable OSPF area 0 on the 2/0/11.

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

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

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

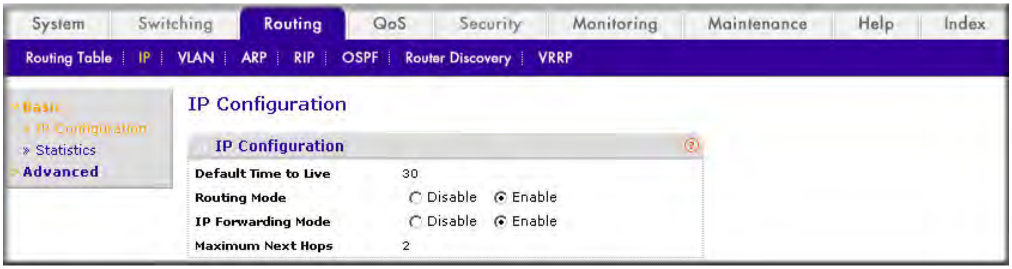
```
(Netgear Switch) (Config)#ex
(Netgear Switch) #show ip ospf neighbor interface all
  Router ID        IP Address    Neighbor Interface    State
----------------   -----------   -------------------   ---------
4.4.4.4            192.168.10.2       2/0/11            Full
2.2.2.2            192.168.20.2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

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

To use the Web interface to configure the switch, proceed as follows:

1. Enable IP routing on the switch:

   a. From the main menu, select Routing > IP > 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

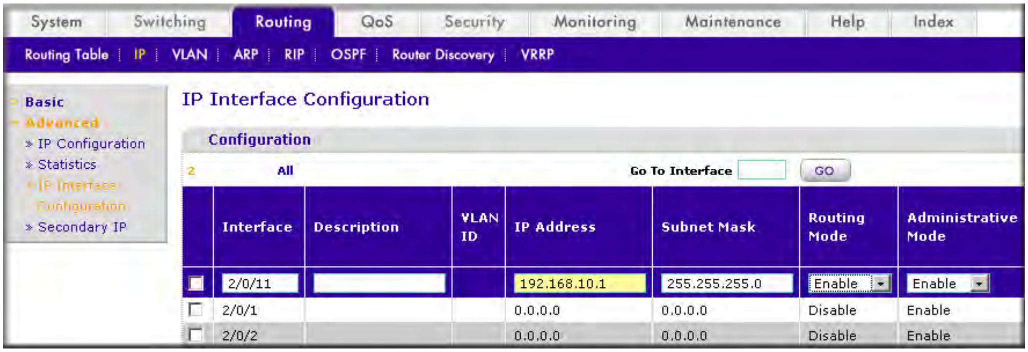
Figure 8-17

   b. Next to the Routing Mode, select the **Enable** radio button.

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

2. Assign IP address 192.168.10.1 to the port 2/0/11:

   a. From the main menu, select Routing > IP > Advanced> IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

Configuration

2 All Go To Interface

	Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☐	2/0/11			192.168.10.1	255.255.255.0	Enable	Enable
☐	2/0/1			0.0.0.0	0.0.0.0	Disable	Enable
☐	2/0/2			0.0.0.0	0.0.0.0	Disable	Enable

Figure 8-18

b. Under IP Interface Configuration, scroll down to interface **2/0/11** and select the checkbox for that interface. 2/0/11 now appears in the Interface field at the top.

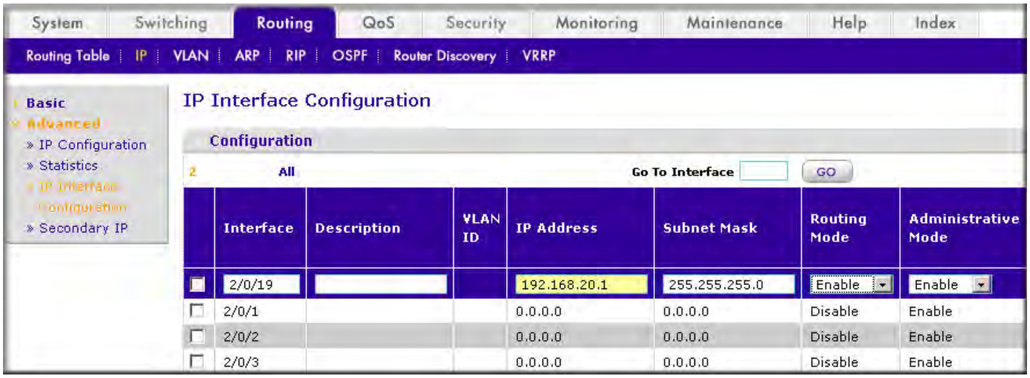
c. Enter the following information in the IP Interface Configuration:

- In the IP Address field, enter **192.168.10.1**.
- In the Network Mask field, enter **255.255.255.0**.
- Select **Enable** in the Admin Mode field.

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

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

a. From the main menu, select Routing > IP > Advanced> IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

Configuration

2 All Go To Interface

	Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☐	2/0/19			192.168.20.1	255.255.255.0	Enable	Enable
☐	2/0/1			0.0.0.0	0.0.0.0	Disable	Enable
☐	2/0/2			0.0.0.0	0.0.0.0	Disable	Enable
☐	2/0/3			0.0.0.0	0.0.0.0	Disable	Enable

Figure 8-19

b. Under IP Interface Configuration, scroll down to interface **2/0/19** and select the checkbox for that interface. 2/0/19 now appears in the Interface field at the top.

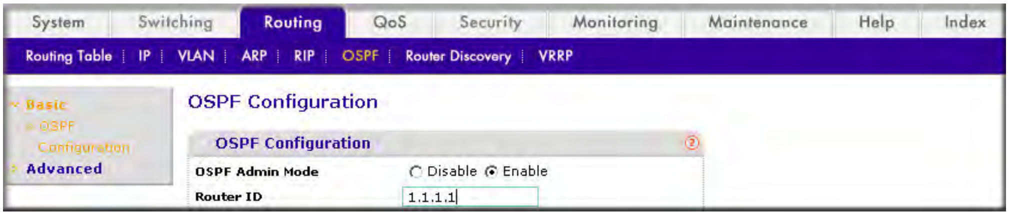
c. Enter the following information in the IP Interface Configuration:

- In the IP Address field, enter **192.168.20.1**.
- In the Network Mask field, enter **255.255.255.0**.
- Select **Enable** in the Admin Mode field.

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

4. Specify the Router ID and Enable OSPF for the switch.

a. From the main menu, select Routing > OSPF > Basic> OSPF Configuration. A screen similar to the following displays.



OSPF Configuration

OSPF Configuration

OSPF Admin Mode	○ Disable ● Enable
Router ID	1.1.1.1

Figure 8-20

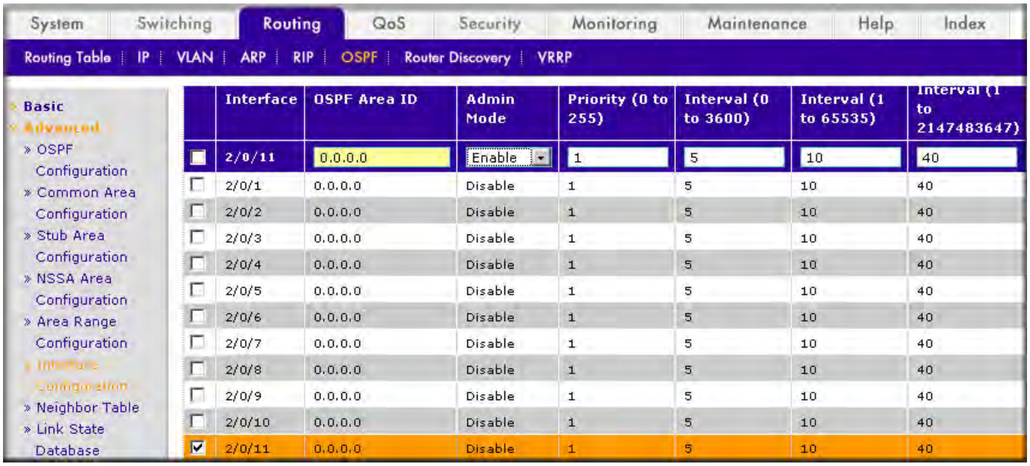
b. Under the OSPF Configuration, enter the following information:

In the Router ID, enter **1.1.1.1**.

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

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

a. From the main menu, select Routing > OSPF > Advanced> Interface Configuration. A screen similar to the following displays.



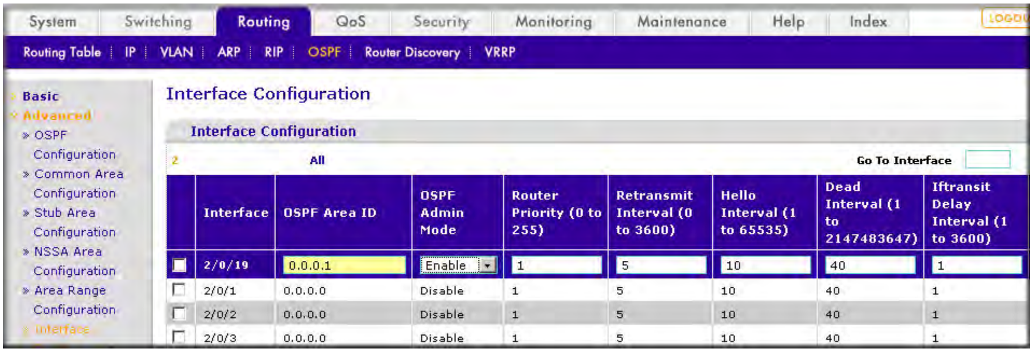
	Interface	OSPF Area ID	Admin Mode	Priority (0 to 255)	Interval (0 to 3600)	Interval (1 to 65535)	Interval (1 to 2147483647)
□	2/0/11	0.0.0.0	Enable	1	5	10	40
□	2/0/1	0.0.0.0	Disable	1	5	10	40
□	2/0/2	0.0.0.0	Disable	1	5	10	40
□	2/0/3	0.0.0.0	Disable	1	5	10	40
□	2/0/4	0.0.0.0	Disable	1	5	10	40
□	2/0/5	0.0.0.0	Disable	1	5	10	40
□	2/0/6	0.0.0.0	Disable	1	5	10	40
□	2/0/7	0.0.0.0	Disable	1	5	10	40
□	2/0/8	0.0.0.0	Disable	1	5	10	40
□	2/0/9	0.0.0.0	Disable	1	5	10	40
□	2/0/10	0.0.0.0	Disable	1	5	10	40
☑	2/0/11	0.0.0.0	Disable	1	5	10	40

Figure 8-21

- **b.** Under Interface Configuration, scroll down to interface **2/0/11** and select the checkbox for that interface. 2/0/11 now appears in the Interface field at the top.
  - In the OSPF Area ID field, enter **0.0.0.0**.
  - Select the **Enable** in the OSPF Admin Mode field.
- **c.** Click **Apply** to save the settings.

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

- **a.** From the main menu, select Routing > OSPF > Advanced> Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

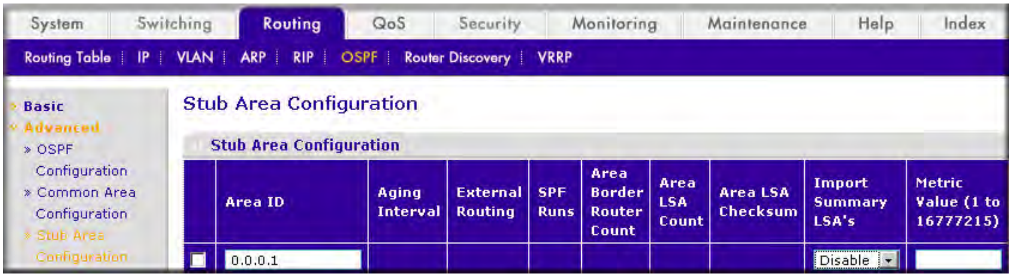
	Interface	OSPF Area ID	OSPF Admin Mode	Router Priority (0 to 255)	Retransmit Interval (0 to 3600)	Hello Interval (1 to 65535)	Dead Interval (1 to 2147483647)	Iftransit Delay Interval (1 to 3600)
□	2/0/19	0.0.0.1	Enable	1	5	10	40	1
□	2/0/1	0.0.0.0	Disable	1	5	10	40	1
□	2/0/2	0.0.0.0	Disable	1	5	10	40	1
□	2/0/3	0.0.0.0	Disable	1	5	10	40	1

Figure 8-22

- **b.** Under Interface Configuration, scroll down to interface **2/0/19** and select the checkbox for that interface. 2/0/19 now appears in the Interface field at the top.
  - In the OSPF Area ID field, enter **0.0.0.1**.
  - Select the **Enable** in the OSPF Admin Mode field.
- **c.** Click the **Apply** button to save the settings.

7. Configure area 0.0.0.1 as a stub area.

- **a.** From the main menu, select Routing > OSPF > Advanced > Stub Area Configuration. A screen similar to the following displays.



Stub Area Configuration

Stub Area Configuration

	Area ID	Aging Interval	External Routing	SPF Runs	Area Border Router Count	Area LSA Count	Area LSA Checksum	Import Summary LSA's	Metric Value (1 to 16777215)
□	0.0.0.1							Disable	

Figure 8-23

b. Enter the following information in the Sub Area Configuration.

- In the Area ID field, enter **0.0.0.1**.
- Select **Disable** in the Import Summary LSA’s field.

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

CLI: Configuring Area 1 as a Stub Area on A2

Enable routing on the switch.

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

Set the router id to 2.2.2.2.

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

Configure the area 0.0.0.1 as a stub area.

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

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

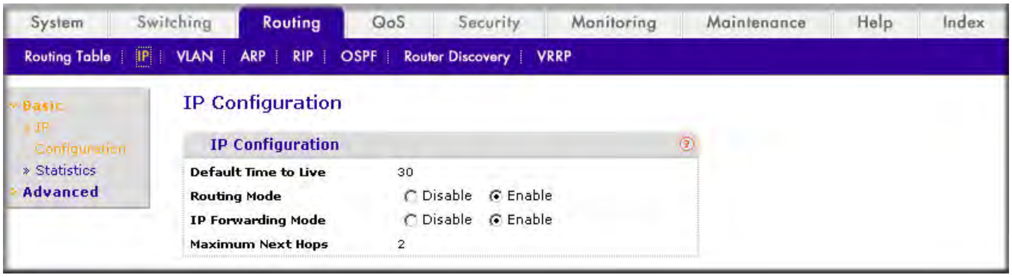
```
(Netgear Switch) (Config-router)#exit
(Netgear Switch) (Config-router)#exit
(Netgear Switch) (Config)#interface 1/0/15
(Netgear Switch) (Interface 1/0/15)#routing
(Netgear Switch) (Interface 1/0/15)#ip address 192.168.20.2  255.255.255.0
(Netgear Switch) (Interface 1/0/15)#ip ospf
(Netgear Switch)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

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

Total Number of Routes......................... 2

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

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

To use the Web interface to configure OSPF on the switch, proceed as follows:

1. Enable IP routing on the switch.

   a. From the main menu, select Routing > IP > 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

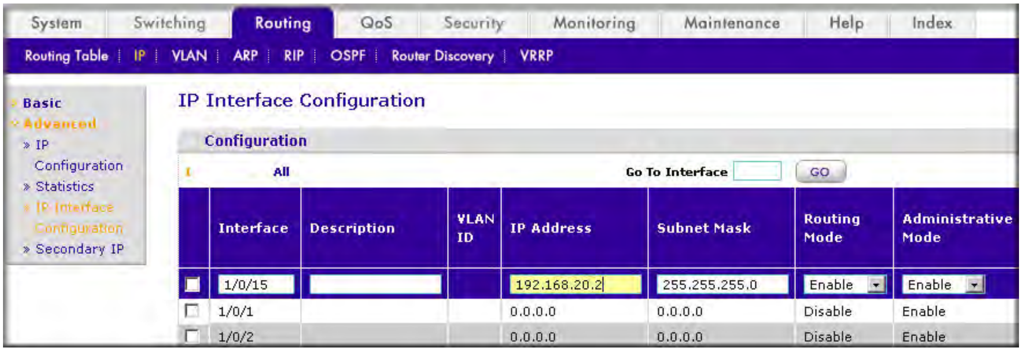
Figure 8-24

   b. Next to the Routing Mode, select the **Enable** radio button.

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

2. Assign IP address 192.168.10.1 to the port 1/0/15.

   a. From the main menu, 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
□	1/0/15			192.168.20.2	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

Figure 8-25

   b. Under IP Interface Configuration, scroll down to interface **1/0/15** and select the checkbox for that interface. Now 1/0/15 appears in the Interface field at the top.

   c. Enter the following information in the IP Interface Configuration:

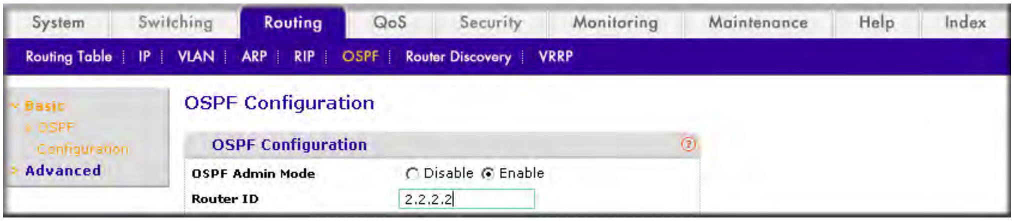
   - In the IP Address field, enter **192.168.20.2**.
   - In the Network Mask field, enter **255.255.255.0**.

- Select **Enable** in the Admin Mode field.

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

3. Specify the Router ID and Enable OSPF for the switch

a. From the main menu, select Routing > OSPF > Basic> OSPF Configuration. A screen similar to the following displays.



OSPF Configuration

OSPF Configuration

OSPF Admin Mode	○ Disable ● Enable
Router ID	2.2.2.2

Figure 8-26

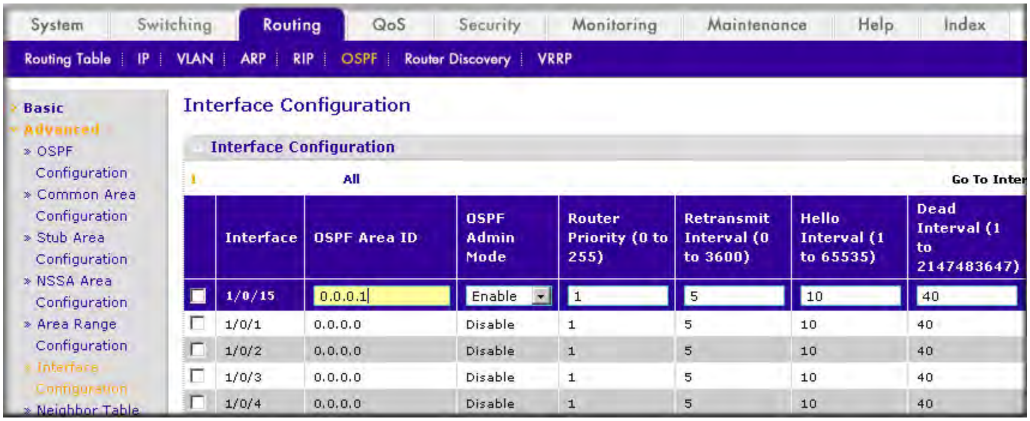
b. Under the OSPF Configuration, enter the following information:

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

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

4. Enable OSPF on the port 1/0/15.

a. From the main menu, select Routing > OSPF > Advanced> Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

	Interface	OSPF Area ID	OSPF Admin Mode	Router Priority (0 to 255)	Retransmit Interval (0 to 3600)	Hello Interval (1 to 65535)	Dead Interval (1 to 2147483647)
□	1/0/15	0.0.0.1	Enable	1	5	10	40
□	1/0/1	0.0.0.0	Disable	1	5	10	40
□	1/0/2	0.0.0.0	Disable	1	5	10	40
□	1/0/3	0.0.0.0	Disable	1	5	10	40
□	1/0/4	0.0.0.0	Disable	1	5	10	40

Figure 8-27

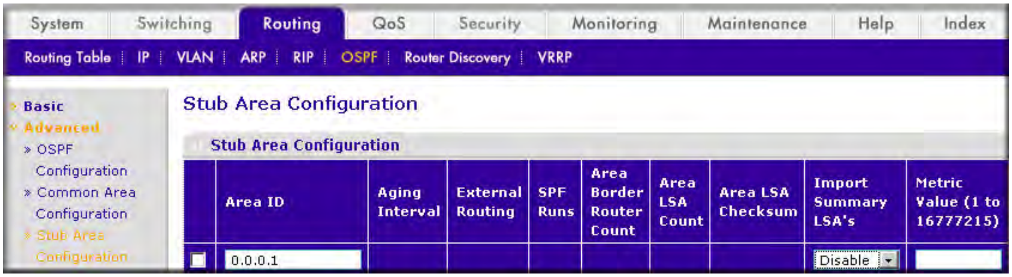
b. Under Interface Configuration, scroll down to interface **1/0/15** and select the checkbox for that interface. Now 1/0/15 appears in the Interface field at the top.

- In the OSPF Area ID field, enter **0.0.0.1**.
- Select the **Enable** in the OSPF Admin Mode field.

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

5. Configure area 0.0.0.1 as a stub area.

a. From the main menu, select Routing > OSPF > Advanced> Stub Area Configuration. A screen similar to the following displays.



Stub Area Configuration

Stub Area Configuration

	Area ID	Aging Interval	External Routing	SPF Runs	Area Border Router Count	Area LSA Count	Area LSA Checksum	Import Summary LSA's	Metric Value (1 to 16777215)
□	0.0.0.1							Disable	

Figure 8-28

b. Enter the following information in the Sub Area Configuration.

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

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

Configure Area 1 as a nssa Area

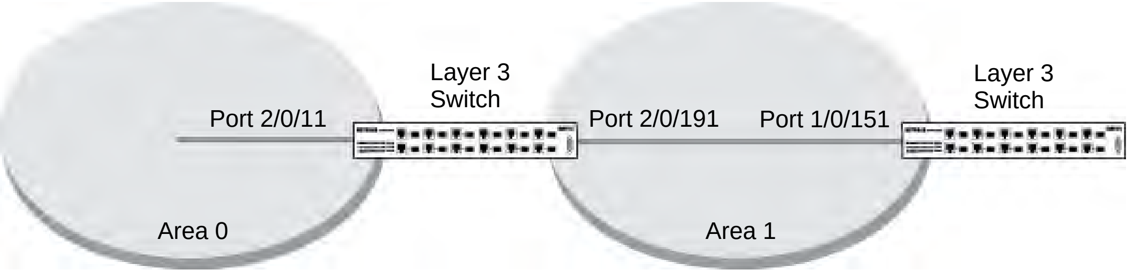


Figure 8-29

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

CLI: Configuring Area 1 as a nssa Area

Enable routing on the switch.

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

Configure area 0.0.0.1 as a nssa area.

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

Stop importing summary LSA to the area 0.0.0.1.

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

Enable area 0.0.0.1 on the 2/0/19.

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

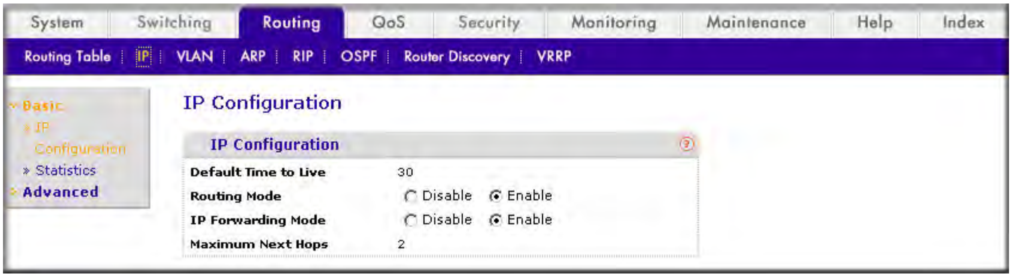
```
(Netgear Switch) (Interface 2/0/19)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #show ip route
Total Number of Routes......................... 2
   Network          Subnet                     Next Hop     Next Hop
   Address           Mask         Protocol      Intf       IP Address
--------------- --------------- ------------ --------- ---------------
 14.1.1.0        255.255.255.0   OSPF Inter    2/0/11     192.168.10.2
14.1.2.0        255.255.255.0   OSPF Inter    2/0/11     192.168.10.2
192.168.10.0    255.255.255.0   Local         2/0/11     192.168.10.1
192.168.20.0    255.255.255.0   Local         2/0/19     192.168.20.1
192.168.40.0    255.255.255.0   OSPF NSSA T2  2/0/19     192.168.20.2
192.168.41.0    255.255.255.0   OSPF NSSA T2  2/0/19     192.168.20.2
192.168.42.0    255.255.255.0   OSPF NSSA T2  2/0/19     192.168.20.2
```

Web Interface: Configuring Area 1 as a nssa Area on A1

To use the Web interface to configure OSPF on the switch, proceed as follows:

1. Enable IP routing on the switch.

   a. From the main menu, select Routing > IP > 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

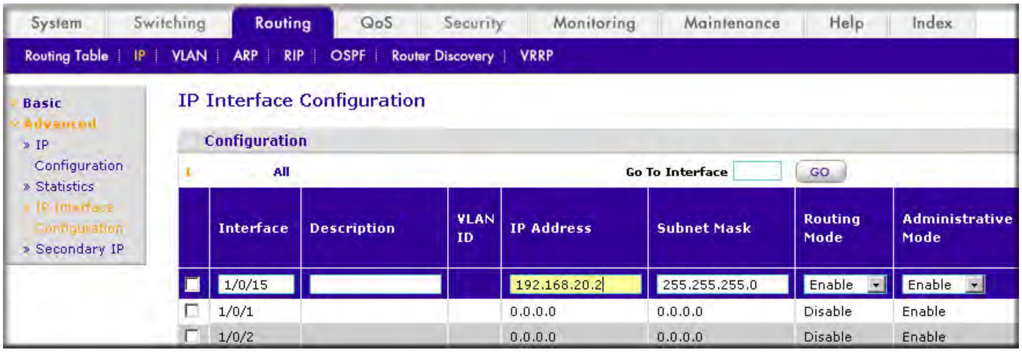
Figure 8-30

   b. Next to the Routing Mode, select the **Enable** radio button.

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

2. Assign IP address 192.168.10.1 to the port 2/0/11:

   a. From the main menu, select Routing > IP > Advanced> IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

Configuration

1 All Go To Interface

	Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
□	1/0/15			192.168.20.2	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

Figure 8-31

b. Under IP Interface Configuration, scroll down to interface **2/0/11** and select the checkbox for that interface. 2/0/11 now appears in the Interface field at the top.

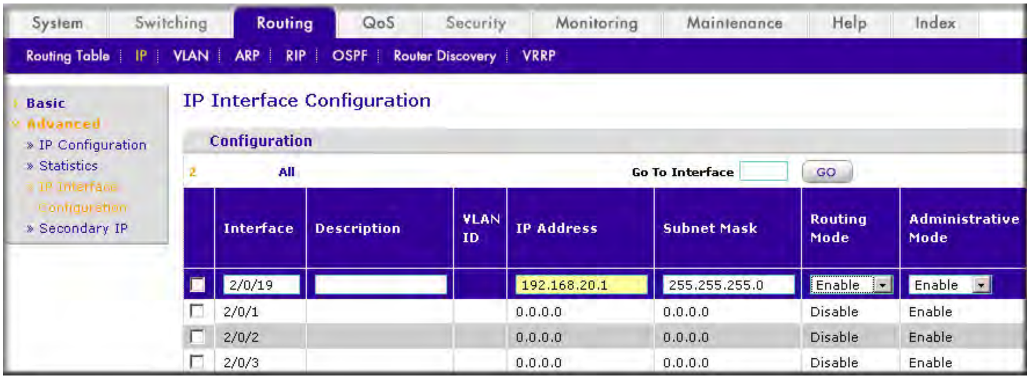
c. Enter the following information in the IP Interface Configuration:

- In the IP Address field, enter **192.168.10.1**.
- In the Network Mask field, enter **255.255.255.0**.
- Select **Enable** in the Admin Mode field.

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

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

a. From the main menu, select Routing > IP > Advanced> IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

Configuration

2 All Go To Interface

	Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
□	2/0/19			192.168.20.1	255.255.255.0	Enable	Enable
□	2/0/1			0.0.0.0	0.0.0.0	Disable	Enable
□	2/0/2			0.0.0.0	0.0.0.0	Disable	Enable
□	2/0/3			0.0.0.0	0.0.0.0	Disable	Enable

Figure 8-32

b. Under IP Interface Configuration, scroll down to interface **2/0/19** and select the checkbox for that interface. 2/0/19 now appears in the Interface field at the top.

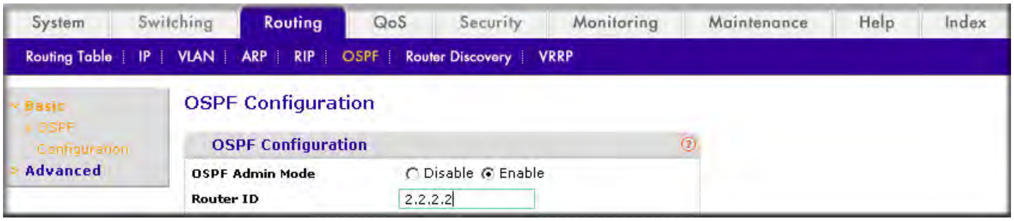
c. Enter the following information in the IP Interface Configuration:

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

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

4. Specify the Router ID and Enable OSPF for the switch.

a. From the main menu, select Routing > OSPF > Basic> OSPF Configuration. A screen similar to the following displays.



OSPF Configuration

OSPF Configuration

OSPF Admin Mode	○ Disable ● Enable
Router ID	2.2.2.2

Figure 8-33

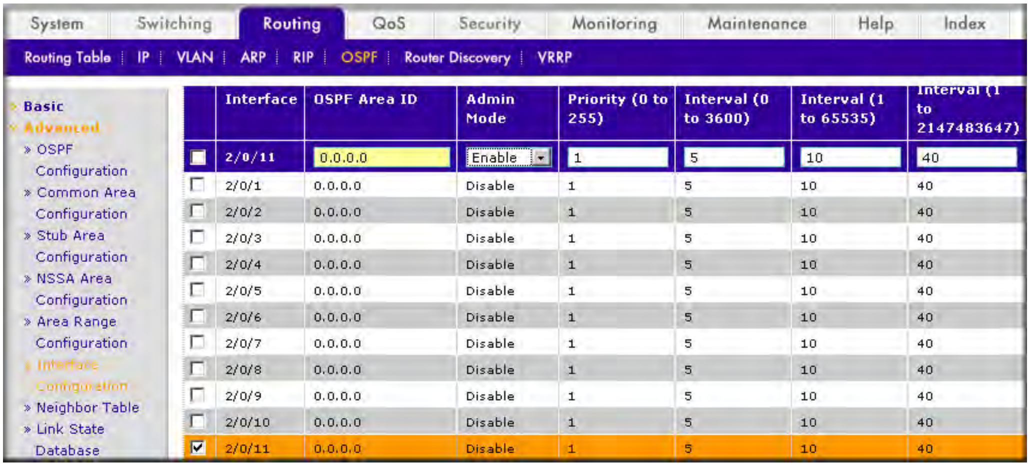
b. Under the OSPF Configuration, enter the following information:

In the Router ID, enter **1.1.1.1**.

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

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

a. From the main menu, select Routing > OSPF > Advanced> Interface Configuration. A screen similar to the following displays.



	Interface	OSPF Area ID	Admin Mode	Priority (0 to 255)	Interval (0 to 3600)	Interval (1 to 65535)	Interval (1 to 2147483647)
☐	2/0/11	0.0.0.0	Enable	1	5	10	40
☐	2/0/1	0.0.0.0	Disable	1	5	10	40
☐	2/0/2	0.0.0.0	Disable	1	5	10	40
☐	2/0/3	0.0.0.0	Disable	1	5	10	40
☐	2/0/4	0.0.0.0	Disable	1	5	10	40
☐	2/0/5	0.0.0.0	Disable	1	5	10	40
☐	2/0/6	0.0.0.0	Disable	1	5	10	40
☐	2/0/7	0.0.0.0	Disable	1	5	10	40
☐	2/0/8	0.0.0.0	Disable	1	5	10	40
☐	2/0/9	0.0.0.0	Disable	1	5	10	40
☐	2/0/10	0.0.0.0	Disable	1	5	10	40
☑	2/0/11	0.0.0.0	Disable	1	5	10	40

Figure 8-34

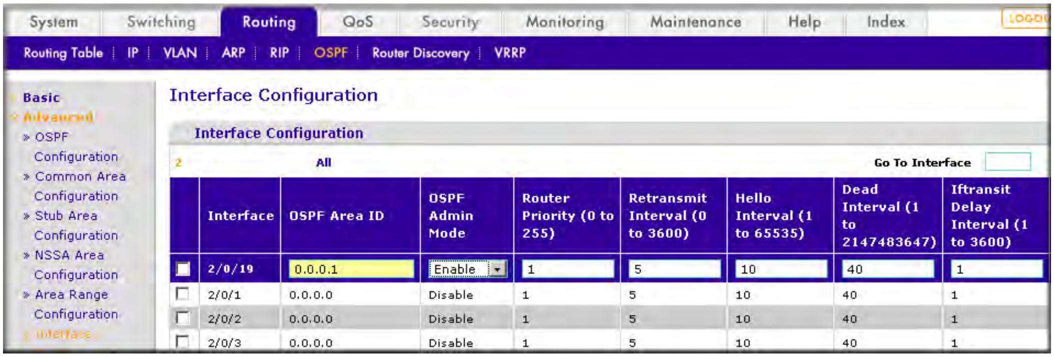
b. Under Interface Configuration, scroll down to interface **2/0/11** and select the checkbox for that interface. 2/0/11 now appears in the Interface field at the top.

- In the OSPF Area ID field, enter **0.0.0.0**.
- Select the **Enable** in the OSPF Admin Mode field.

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

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

a. From the main menu, select Routing > OSPF > Advanced> Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

2 All Go To Interface

	Interface	OSPF Area ID	OSPF Admin Mode	Router Priority (0 to 255)	Retransmit Interval (0 to 3600)	Hello Interval (1 to 65535)	Dead Interval (1 to 2147483647)	Iftransit Delay Interval (1 to 3600)
☐	2/0/19	0.0.0.1	Enable	1	5	10	40	1
☐	2/0/1	0.0.0.0	Disable	1	5	10	40	1
☐	2/0/2	0.0.0.0	Disable	1	5	10	40	1
☐	2/0/3	0.0.0.0	Disable	1	5	10	40	1

Figure 8-35

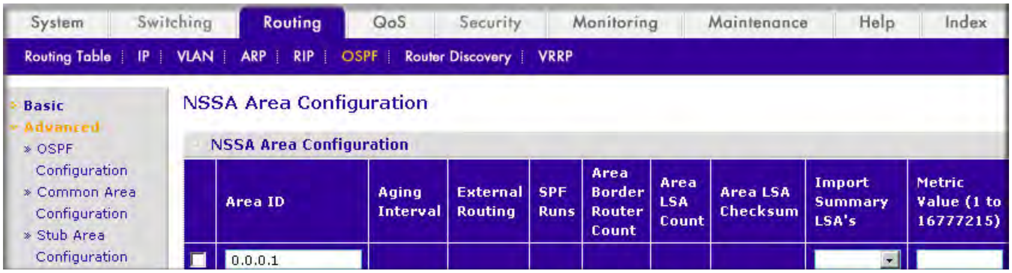
b. Under Interface Configuration, scroll down to interface **2/0/19** and select the checkbox for that interface. 2/0/19 now appears in the Interface field at the top.

- In the OSPF Area ID field, enter **0.0.0.1**.
- Select the **Enable** in the OSPF Admin Mode field.

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

7. Configure area 0.0.0.1 as a nssa area.

a. From the main menu, select Routing > OSPF > Advanced> NSSA Area Configuration. A screen similar to the following displays.



NSSA Area Configuration

NSSA Area Configuration

	Area ID	Aging Interval	External Routing	SPF Runs	Area Border Router Count	Area LSA Count	Area LSA Checksum	Import Summary LSA's	Metric Value (1 to 16777215)
☐	0.0.0.1								

Figure 8-36

b. Enter the following information in the NSSA Area Configuration.

- In the Area ID field, enter **0.0.0.1**.
- Select the **Disable** in the Import Summary LSA's field.

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

CLI: Configuring Area 1 as a nssa Area on A2

Enable routing on the switch.

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

Set the router id to 2.2.2.2.

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

Configure the area 0.0.0.1 as a nssa area.

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

Redistribute the rip routes into the OSPF.

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

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

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

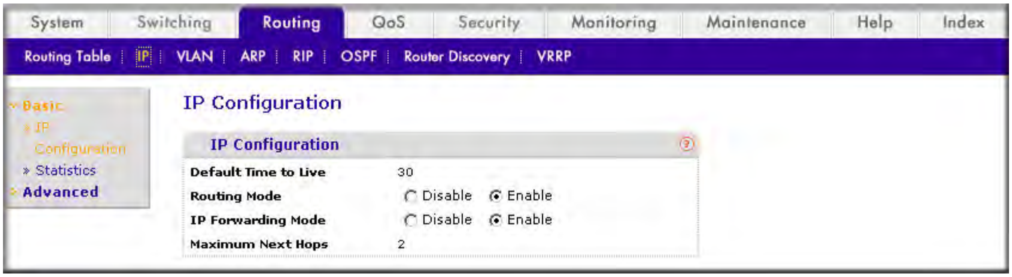
```
(Netgear Switch) (Interface 1/0/15)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #show ip route
Total Number of Routes......................... 6
   Network          Subnet                      Next Hop     Next Hop
   Address           Mask          Protocol      Intf       IP Address
--------------- --------------- ------------ --------- ---------------
0.0.0.0         0.0.0.0         OSPF Inter     1/0/15      192.168.20.1
192.168.20.0    255.255.255.0   Local          1/0/15      192.168.20.2
192.168.30.0    255.255.255.0   Local          1/0/11      192.168.30.1
192.168.40.0    255.255.255.0   RIP            1/0/11      192.168.30.2
192.168.41.0    255.255.255.0   RIP            1/0/11      192.168.30.2
192.168.42.0    255.255.255.0   RIP            1/0/11      192.168.30.2
```

Web Interface: Configuring Area 1 as a nssa Area on A2

To use the Web interface to configure OSPF on the switch, proceed as follows:

1. Enable IP routing on the switch:

   a. From the main menu, select Routing > IP > 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

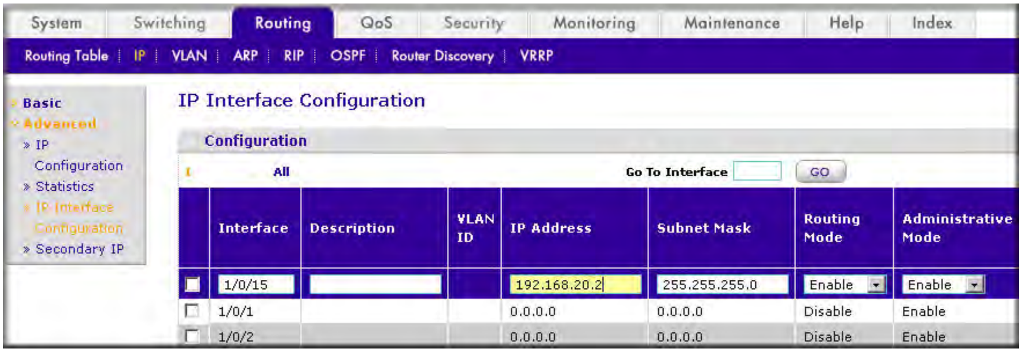
Figure 8-37

   b. Next to the Routing Mode, select the **Enable** radio button.

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

2. Assign IP address 192.168.30.1 to the port 1/0/11:

   a. From the main menu, select Routing > IP > Advanced> IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

Configuration

	Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☐	1/0/15			192.168.20.2	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

Figure 8-38

b. Under IP Interface Configuration, scroll down to interface **1/0/11** and select the checkbox for that interface. Now 1/0/11 appears in the Interface field at the top.

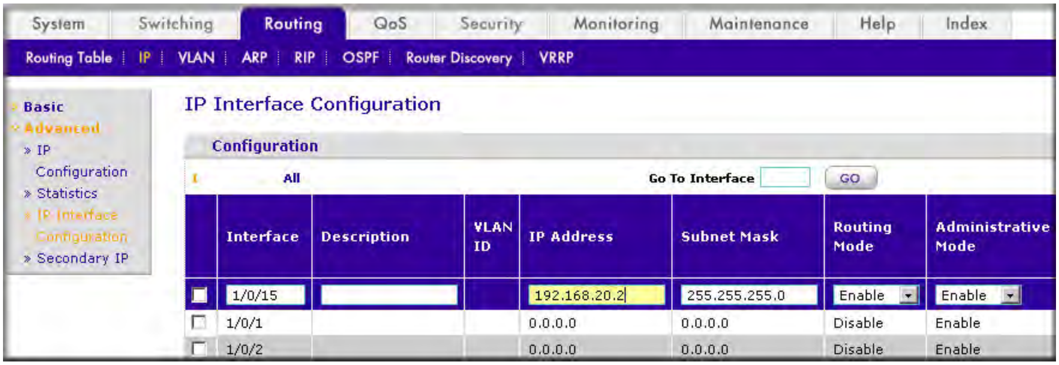
c. Enter the following information in the IP Interface Configuration:

- In the IP Address field, enter **192.168.30.1**.
- In the Network Mask field, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

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

a. From the main menu, select Routing > IP > Advanced> IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

Configuration

	Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☐	1/0/15			192.168.20.2	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

Figure 8-39

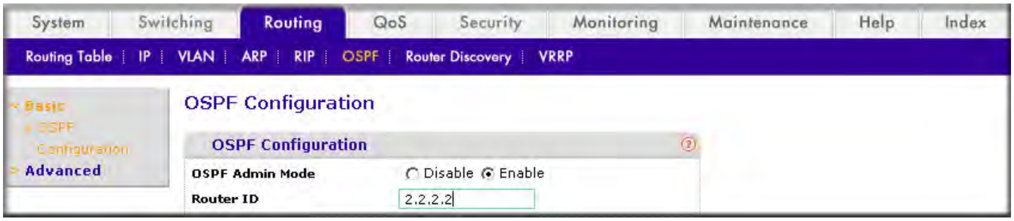
b. Under IP Interface Configuration, scroll down to interface **1/0/15** and select the checkbox for that interface. Now 1/0/15 appears in the Interface field at the top.

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

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

4. Specify the Router ID and Enable OSPF for the switch.

   a. From the main menu, select Routing > OSPF > Basic> OSPF Configuration. A screen similar to the following displays.



OSPF Configuration

OSPF Configuration

OSPF Admin Mode ○ Disable ● Enable

Router ID 2.2.2.2

Figure 8-40

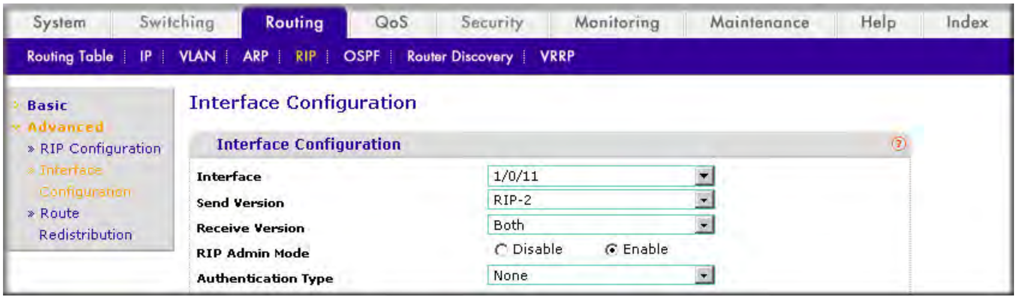
   b. Under the OSPF Configuration, enter the following information:

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

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

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

   a. From the main menu, select Routing > RIP > Advanced> Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface 1/0/11

Send Version RIP-2

Receive Version Both

RIP Admin Mode ○ Disable ● Enable

Authentication Type None

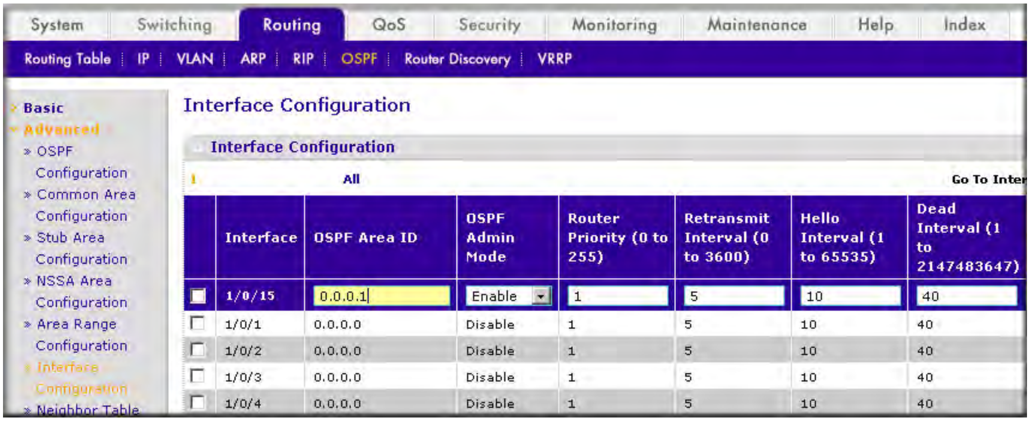
Figure 8-41

   b. Enter the following information in Interface Configuration.
      - Select the **1/0/11** in the Interface field.
      - Next to the RIP Admin Mode, select the **Enable** radio button.

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

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

   a. From the main menu, select Routing > OSPF > Advanced> Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

1 All Go To Inter

	Interface	OSPF Area ID	OSPF Admin Mode	Router Priority (0 to 255)	Retransmit Interval (0 to 3600)	Hello Interval (1 to 65535)	Dead Interval (1 to 2147483647)
☐	1/0/15	0.0.0.1	Enable	1	5	10	40
☐	1/0/1	0.0.0.0	Disable	1	5	10	40
☐	1/0/2	0.0.0.0	Disable	1	5	10	40
☐	1/0/3	0.0.0.0	Disable	1	5	10	40
☐	1/0/4	0.0.0.0	Disable	1	5	10	40

Figure 8-42

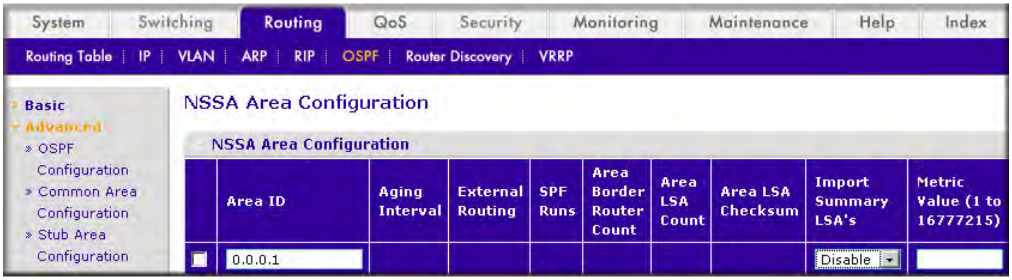
   b. Under IP Interface Configuration, scroll down to interface **1/0/15** and select the checkbox for that interface. Now 1/0/15 appears in the Interface field at the top.

      - In the OSPF Area ID field, enter **0.0.0.1**.
      - Select the **Enable** in the OSPF Admin Mode field.

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

7. Configure area 0.0.0.1 as a nssa area.

   a. From the main menu, select Routing > OSPF > Advanced> NSSA Area Configuration. A screen similar to the following displays.



NSSA Area Configuration

NSSA Area Configuration

	Area ID	Aging Interval	External Routing	SPF Runs	Area Border Router Count	Area LSA Count	Area LSA Checksum	Import Summary LSA's	Metric Value (1 to 16777215)
☐	0.0.0.1							Disable	

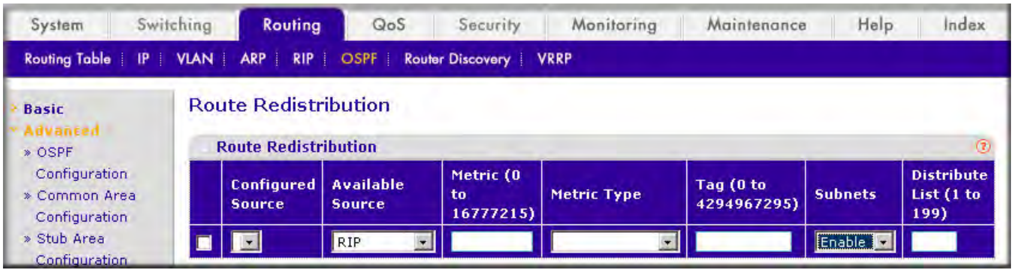
Figure 8-43

   b. In the NSAA Area Configuration, in the Area ID field, enter **0.0.0.1**.

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

8. Redistribute the RIP routes into the OSPF area.

a. From the main menu, select Routing > OSPF > Advanced>Route Redistribution. A screen similar to the following displays.



Route Redistribution

Route Redistribution

	Configured Source	Available Source	Metric (0 to 16777215)	Metric Type	Tag (0 to 4294967295)	Subnets	Distribute List (1 to 199)
□		RIP				Enable	

Figure 8-44

b. In the Route Redistribution, select **RIP** in the Available Source field.

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

VLAN Routing OSPF Configuration

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

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

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

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

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

CLI: VLAN Routing OSPF Configuration

This example adds support for OSPF to the configuration created in the base VLAN routing example in Figure 6-1 on page 6-2. The script shows the commands you would use to configure the 7000 Series Managed Switch as an inter-area router.

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

Specify the router ID and enable OSPF for the switch.

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

Enable OSPF for the VLAN and physical router ports.

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

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

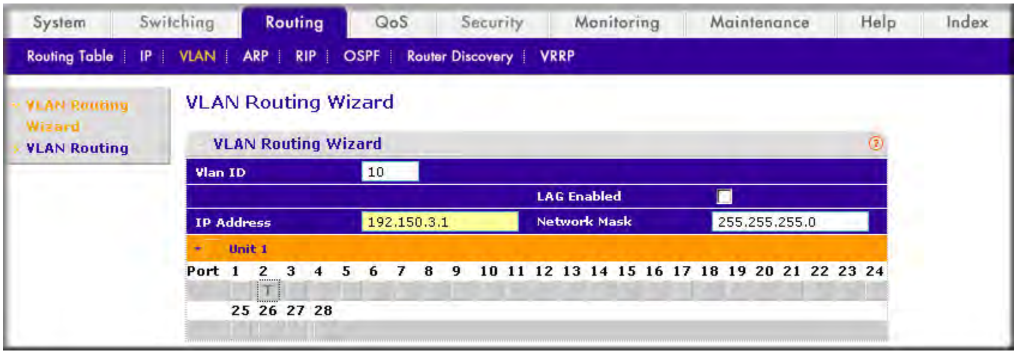
```
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip ospf priority 128
(Netgear Switch) (Interface vlan 10)#ip ospf cost 32
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip ospf priority 255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

Web Interface: VLAN Routing OSPF Configuration

To use the Web interface to configure OSPF on the switch, proceed as follows:

1. Configure a VLAN and include ports 1/0/2 in the VLAN.

   a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.



VLAN Routing Wizard

VLAN Routing Wizard

Vlan ID: 10

LAG Enabled □

IP Address: 192.150.3.1 Network Mask: 255.255.255.0

Unit 1

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

Port 2: T

25 26 27 28

Figure 8-45

b. Enter the following information in the VLAN Routing Wizard.

- In the Vlan ID field, enter **10**.
- In the IP Address field, enter **192.150.3.1**.
- In the Network Mask field, enter **255.255.255.0**.

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

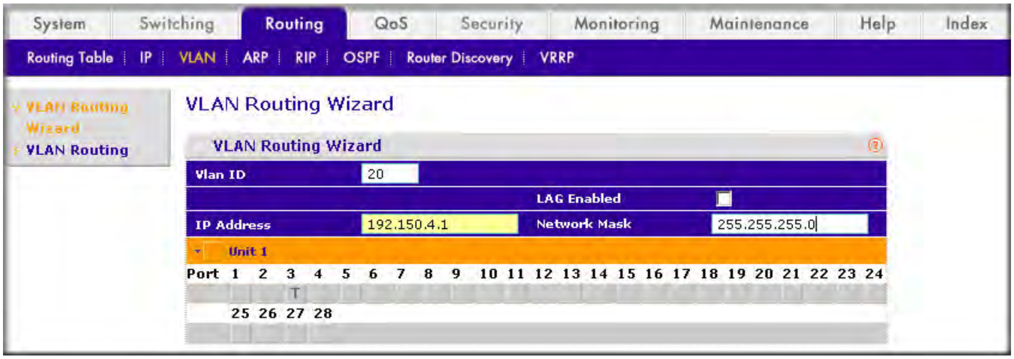
Click the gray box under port 2 once until **T** displays.

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

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

2. Configure a VLAN and include ports 1/0/3 in the VLAN:

a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.



VLAN Routing Wizard

VLAN Routing Wizard

Vlan ID	20		
		LAG Enabled	□
IP Address	192.150.4.1	Network Mask	255.255.255.0

Unit 1

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

Figure 8-46

b. Enter the following information in the VLAN Routing Wizard.

- In the Vlan ID field, enter **20**.
- In the IP Address field, enter **192.150.4.1**.
- In the Network Mask field, enter **255.255.255.0**.

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

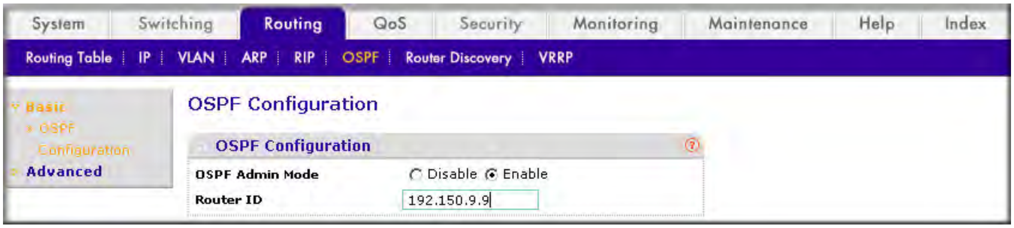
Click the gray box under port 3 once until **T** displays.

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

d. Click **Apply** to save the VLAN that includes ports 3.

3. Enable OSPF on the switch.

a. From the main menu, select Routing > OSPF > Basic>OSPF Configuration. A screen similar to the following displays.



OSPF Configuration

OSPF Configuration

OSPF Admin Mode	○ Disable ● Enable
Router ID	192.150.9.9

Figure 8-47

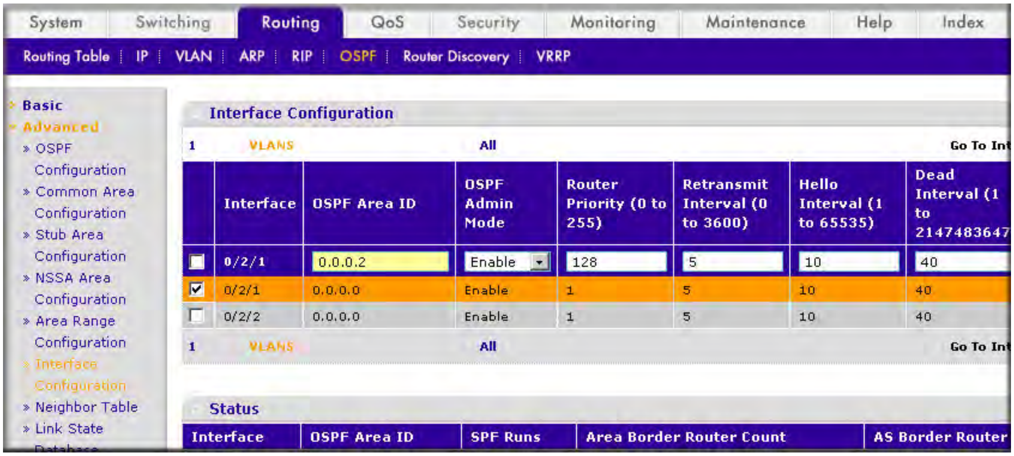
b. Next to the OSPF Admin Mode, select **Enable** Radio button.

c. Enter **192.150.9.9** in the Router ID filed.

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

4. Enable OSPF on the VLAN 10.

a. From the main menu, select Routing > OSPF > Advanced>Interface Configuration. A screen similar to the following displays.



Interface Configuration

1 VLANS All Go To Int

	Interface	OSPF Area ID	OSPF Admin Mode	Router Priority (0 to 255)	Retransmit Interval (0 to 3600)	Hello Interval (1 to 65535)	Dead Interval (1 to 2147483647
☐	0/2/1	0.0.0.2	Enable	128	5	10	40
☑	0/2/1	0.0.0.0	Enable	1	5	10	40
☐	0/2/2	0.0.0.0	Enable	1	5	10	40

1 VLANS All Go To Int

Status

Interface	OSPF Area ID	SPF Runs	Area Border Router Count	AS Border Router

Figure 8-48

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

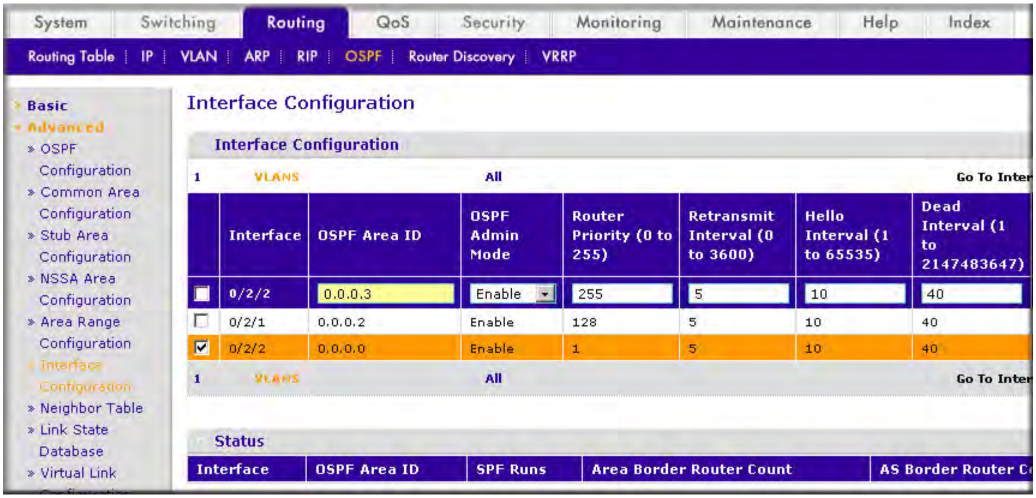
c. Under IP Interface Configuration, scroll down to interface **0/2/1** and select the checkbox for that interface. 0/2/1 now appears in the Interface field at the top.

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

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

5. Enable OSPF on the VLAN 20.

a. From the main menu, select Routing > OSPF > Advanced>Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

1 VLANS All Go To Inter

	Interface	OSPF Area ID	OSPF Admin Mode	Router Priority (0 to 255)	Retransmit Interval (0 to 3600)	Hello Interval (1 to 65535)	Dead Interval (1 to 2147483647)
□	0/2/2	0.0.0.3	Enable	255	5	10	40
□	0/2/1	0.0.0.2	Enable	128	5	10	40
☑	0/2/2	0.0.0.0	Enable	1	5	10	40

1 VLANS All Go To Inter

Status

Interface	OSPF Area ID	SPF Runs	Area Border Router Count	AS Border Router C

Figure 8-49

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

c. Under IP Interface Configuration, scroll down to interface **0/2/2** and select the checkbox for that interface. 0/2/2 now appears in the Interface field at the top.

- In the OSPF Area ID field, enter **0.0.0.3**.
- Select the **Enable** in the OSPF Admin Mode field.
- In the Priority field, enter **255**.
- In the Metric Cost field, enter **64**.

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

OSPFv3 (Open Shortest Path First)

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

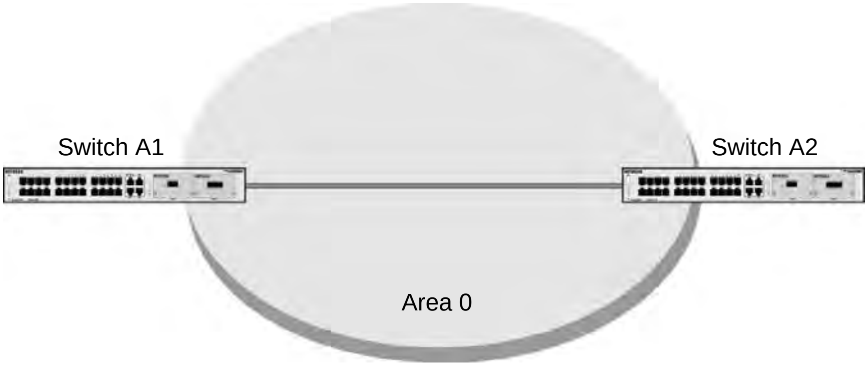


Figure 8-50

CLI: Configuring OSPFv3

On A1, enable IPv6 unitcast routing on the switch:

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

Enable OSPFv3 and assign 1.1.1.1 to router ID.

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

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

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

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

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

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

On A2, Enable IPv6 unitcast routing on the switch.

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

Enable OSPFv3 and assign 2.2.2.2 to router ID.

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

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

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

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

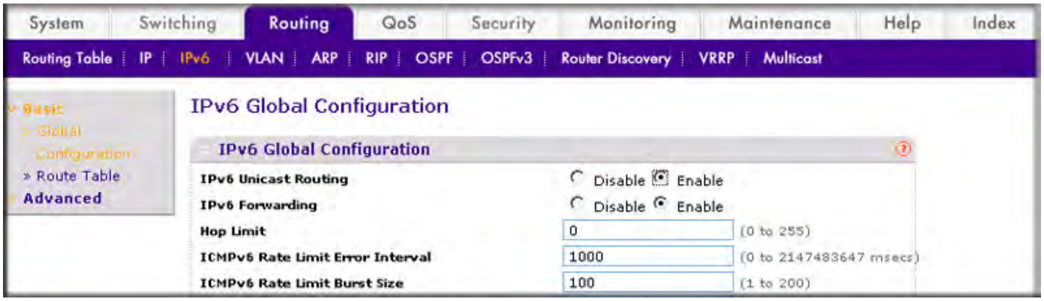
```
(Netgear Switch) (Interface 1/0/13)#ipv6 ospf
(Netgear Switch) (Interface 1/0/13)#ipv6 ospf network broadcast
(Netgear Switch) #show ipv6 ospf neighbor

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

```

Web Interface: Confguring OSPFv3

To use the Web interface to configure OSPF on the switch A1, proceed as follows:

1. Enable IPv6 unicast routing on the switch:

a. From the main menu, select Routing > IPv6 > IPv6 Global Configuration. A screen similar to the following displays.



IPv6 Global Configuration

IPv6 Global Configuration

IPv6 Unicast Routing	○ Disable ● Enable	
IPv6 Forwarding	○ Disable ● Enable	
Hop Limit	0	(0 to 255)
ICMPv6 Rate Limit Error Interval	1000	(0 to 2147483647 msecs)
ICMPv6 Rate Limit Burst Size	100	(1 to 200)

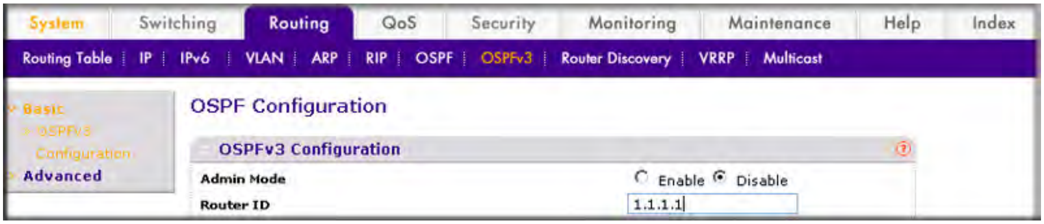
Figure 8-51

b. Next to the IPv6 Unicast Routing Mode, select the Enable radio button.

c. Click Apply to save the settings.

2. Specify the Router ID and Enable OSPFv3 for the switch.

a. From the main menu, select Routing > OSPFv3 > Basic> OSPFv3 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
Basic
OSPFv3
Configuration
Advanced

OSPF Configuration

OSPFv3 Configuration

Admin Mode	○ Enable ● Disable
Router ID	1.1.1.1

Figure 8-52

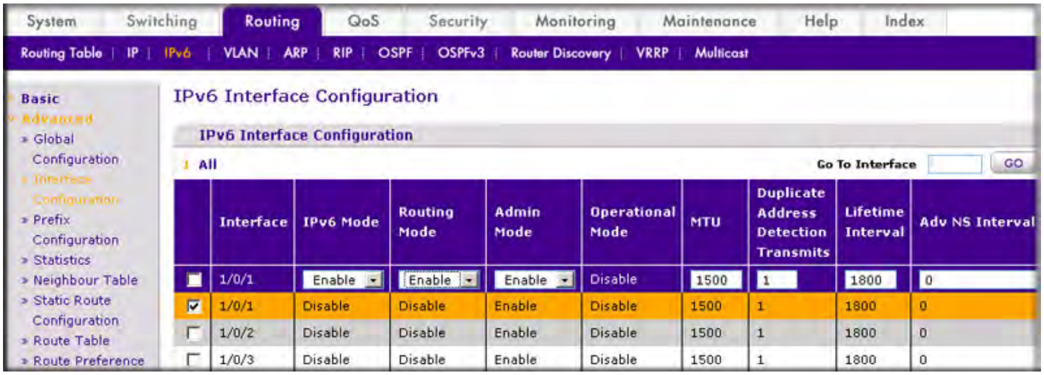
b. Under the OSPF Configuration, enter the following information:

- In the Router ID, enter **1.1.1.1**
- Next to the Admin Mode, select the **Enable** radio button.

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

3. Enable IPv6 on the port 1/0/1.

a. From the main menu, select Routing > IPv6 > Advanced> IP Interface Configuration. A screen similar to the following displays.



IPv6 Interface Configuration

IPv6 Interface Configuration

All

	Interface	IPv6 Mode	Routing Mode	Admin Mode	Operational Mode	MTU	Duplicate Address Detection Transmits	Lifetime Interval	Adv NS Interval
□	1/0/1	Enable	Enable	Enable	Disable	1500	1	1800	0
☑	1/0/1	Disable	Disable	Enable	Disable	1500	1	1800	0
□	1/0/2	Disable	Disable	Enable	Disable	1500	1	1800	0
□	1/0/3	Disable	Disable	Enable	Disable	1500	1	1800	0

Figure 8-53

b. Under IPv6 Interface Configuration, scroll down to interface 1/0/1 and select the checkbox for that interface. Now 1/0/1 appears in the Interface field at the top.

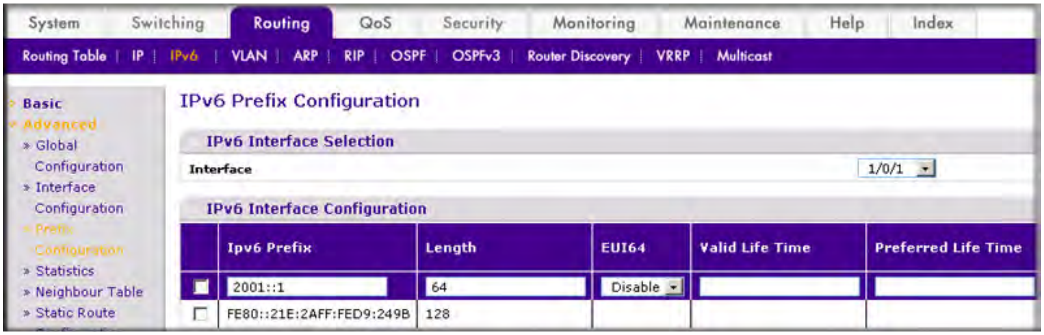
c. Enter the following information in the IP Interface Configuration:

- Select **Enable** in the IPv6 Mode field.
- Select **Enable** in the Routing Mode field.

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

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

a. From the main menu, select Routing > IPv6 > Advanced> IP Interface Configuration. A screen similar to the following displays.



IPv6 Prefix Configuration

IPv6 Interface Selection

Interface 1/0/1

IPv6 Interface Configuration

	Ipv6 Prefix	Length	EUI64	Valid Life Time	Preferred Life Time
□	2001::1	64	Disable		
□	FE80::21E:2AFF:FED9:249B	128			

Figure 8-54

b. Under IPv6 Prefix Configuration, select **1/0/1** in the Interface field.

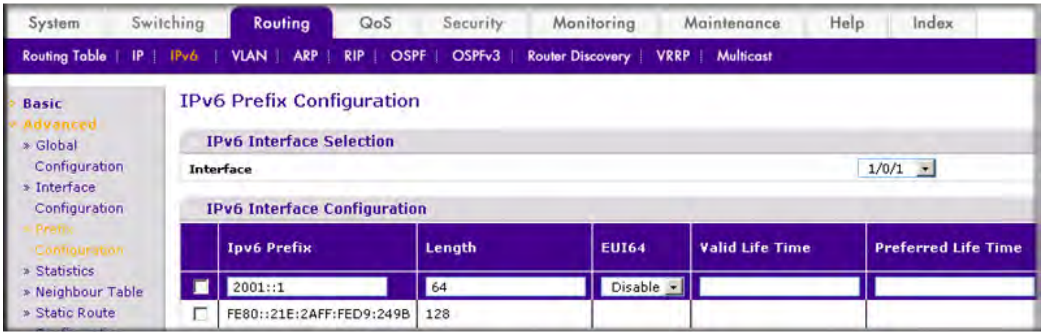
c. Enter the following information in the IPv6 Interface Configuration:

- In the IPv6 Prefix edit box, enter **2001::1**.
- In the Length edit box, enter **64**.
- Select **Disable** in the EUI64 field.
- Select **Disable** in the Onlink Flag field.
- Select **Disable** in the Autonomous Flag field.

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

5. Enable OSPFv3 on the port 1/0/1.

a. From the main menu, select Routing > OSPFv3 > Advanced>Interface Configuration. A screen similar to the following displays.



IPv6 Prefix Configuration

IPv6 Interface Selection

Interface: 1/0/1

IPv6 Interface Configuration

	Ipv6 Prefix	Length	EUI64	Valid Life Time	Preferred Life Time
☐	2001::1	64	Disable		
☐	FE80::21E:2AFF:FED9:249B	128			

Figure 8-55

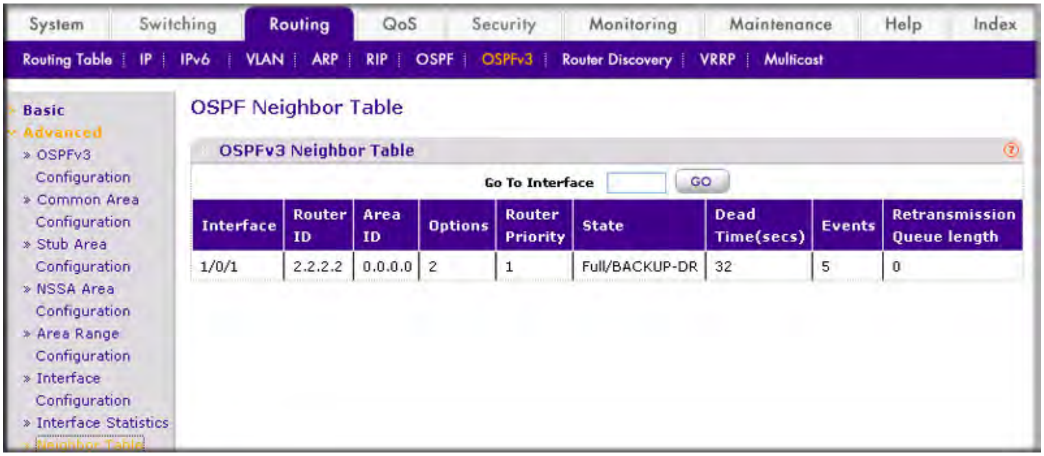
b. Under IP Interface Configuration, scroll down to interface 1/0/1 and select the checkbox for that interface. Now 1/0/1 appears in the Interface field at the top.

- In the OSPF Area ID field, enter **0.0.0.0**.
- Select **Enable** in the Admin Mode field.

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

6. Display OSPFv3 neighbor.

a. From the main menu, select Routing > OSPFv3 > Advanced>Neighbor Table. A screen similar to the following displays.



OSPF Neighbor Table

OSPFv3 Neighbor Table

Go To Interface

Interface	Router ID	Area ID	Options	Router Priority	State	Dead Time(secs)	Events	Retransmission Queue length
1/0/1	2.2.2.2	0.0.0.0	2	1	Full/BACKUP-DR	32	5	0

Figure 8-56

To use the Web interface to configure OSPF on the switch A2, refer to the configuration of switch A1.

Chapter 9
Proxy Address Resolution Protocol (ARP)

This chapter describes the Proxy Address Resolution Protocol (ARP) feature.

- Proxy ARP allows a router to answer ARP requests where the target IP address is not 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 will only respond to an ARP request 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

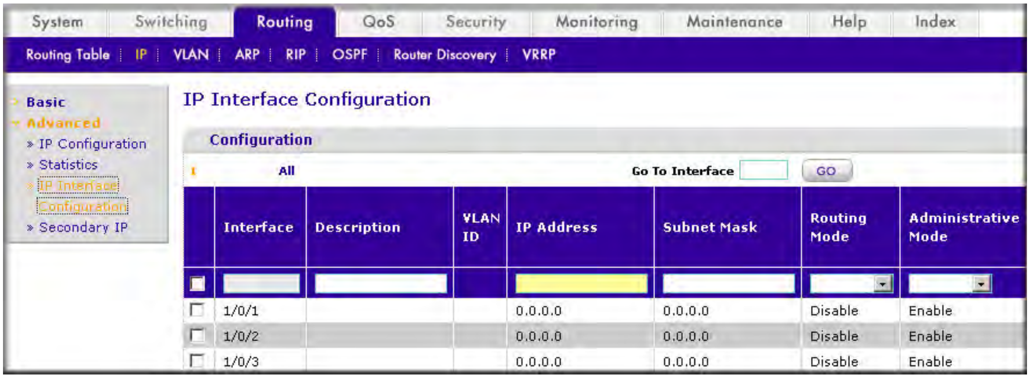
```
(Netgear Switch) (Interface 0/24)#ip proxy-arp ?

<cr>                         Press Enter to execute the command.

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

Web Interface: Configuring Proxy ARP on a Port

To use the Web interface to configure proxy ARP on a port, proceed as follows:

1. Configure proxy ARP.

a. From the main menu, 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
☐							
☐	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

Figure 9-1

b. Under IP Interface Configuration, scroll down to interface **1/0/3** and select the checkbox for that interface. Now 1/0/3 appears in the Interface field at the top.

c. Select the **Enable** in the Proxy Arp field.

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

Chapter 10
Virtual Router Redundancy Protocol

In this chapter, the following examples are provided:

- "Configure VRRP on a Master Router" on page 10-2
- "Configure VRRP on a Backup Router" on page 10-4

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

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

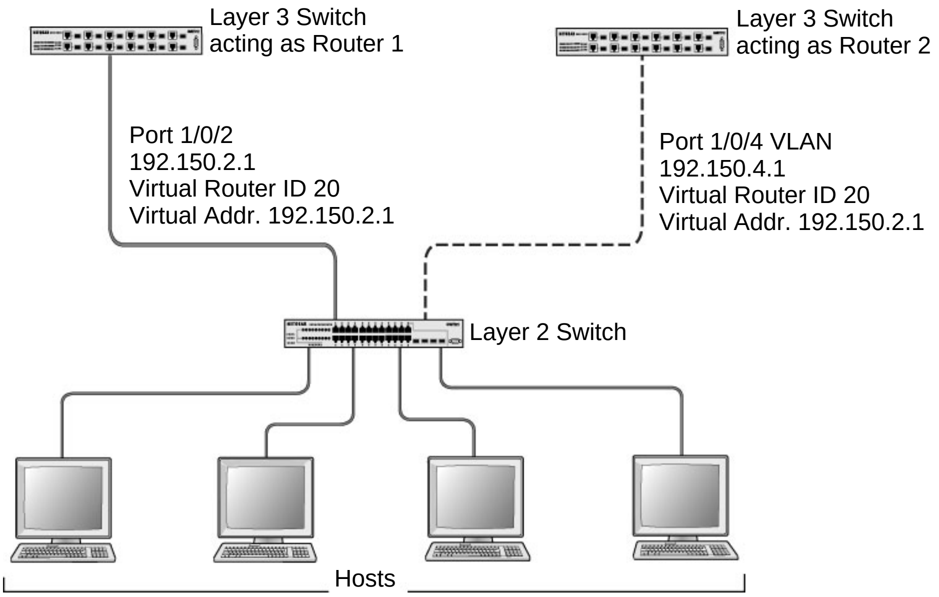


Figure 10-1

Configure VRRP on a Master Router

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

CLI: Configuring VRRP on a Master Router

The following is an example of configuring VRRP on a 7000 Series Managed Switch acting as the master router:

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

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

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

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

Enable VRRP for the switch.

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

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

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

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

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

Enable VRRP on the port.

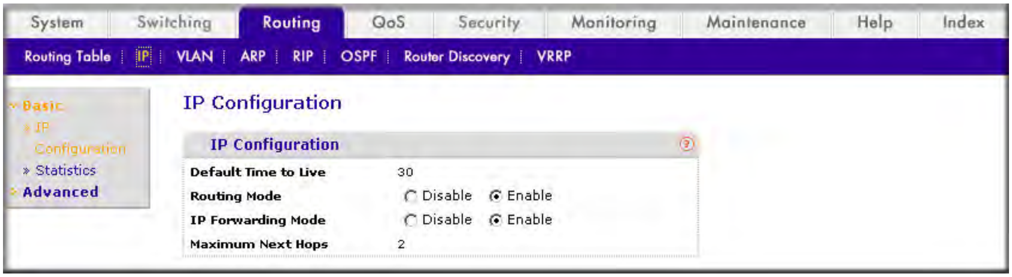
```
(Netgear Switch) (Interface 1/0/2)#ip vrrp 20 mode
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Configuring VRRP on a Master Router

To use the Web interface to configure VRRP on a master router on the switch, proceed as follows:

1. Enable IP routing on the switch:

a. From the main menu, select Routing > IP > 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	

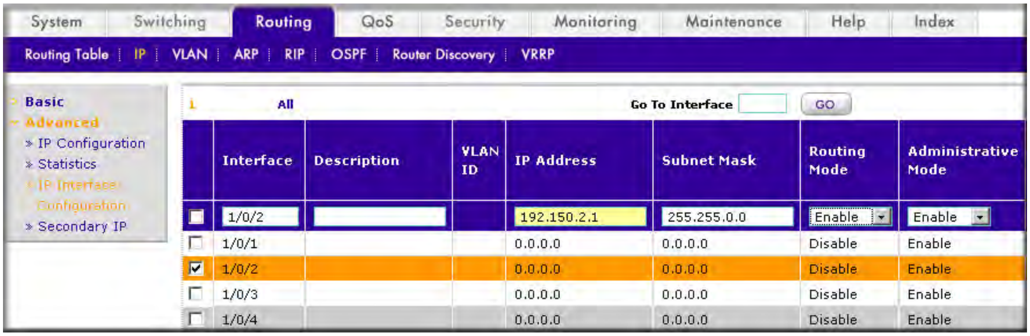
Figure 10-2

b. Next to the Routing Mode, select the **Enable** radio button.

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

2. Assign IP address 192.150.2.1 to the port 1/0/2:

a. From the main menu, 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	255.255.0.0	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

Figure 10-3

b. Under IP Interface Configuration, scroll down to interface **1/0/2** and select the checkbox for that interface. Now 1/0/2 appears in the Interface field at the top.

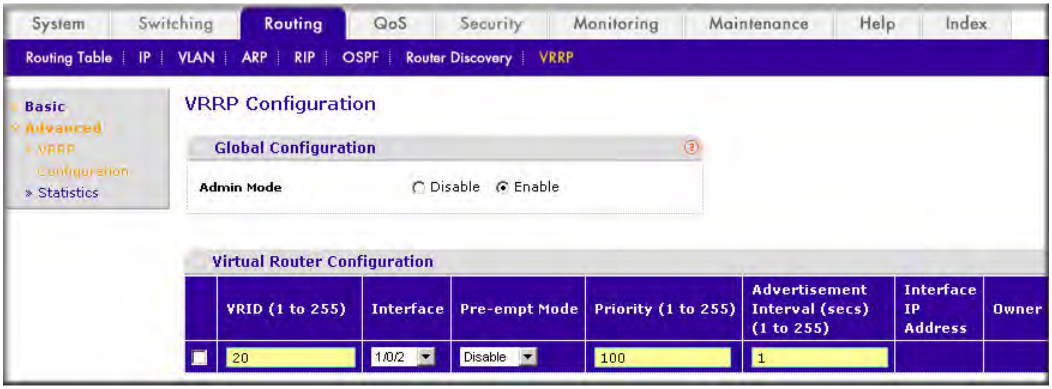
c. Enter the following information in the IP Interface Configuration:

- In the IP Address field, enter **192.150.2.1**.
- In the Network Mask field, enter **255.255.0.0**.
- Select **Enable** in the Routing Mode field.

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

3. Enable VRRP on the 1/0/2:

a. From the main menu, select Routing > VRRP > Advanced> VRRP Configuration. A screen similar to the following displays.



VRRP Configuration

Global Configuration

Admin Mode ○ Disable ● Enable

Virtual Router Configuration

	VRID (1 to 255)	Interface	Pre-empt Mode	Priority (1 to 255)	Advertisement Interval (secs) (1 to 255)	Interface IP Address	Owner
□	20	1/0/2	Disable	100	1		

Figure 10-4

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

c. Enter the following information in the VRRP Configuration:

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

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

Configure VRRP on a Backup Router

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

CLI: Configuring VRRP on a Backup Router

The following is an example of configuring VRRP on a 7000 Series Managed Switch acting as the backup router:

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

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

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

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

Enable VRRP for the switch.

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

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

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

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

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

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

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

Enable VRRP on the port.

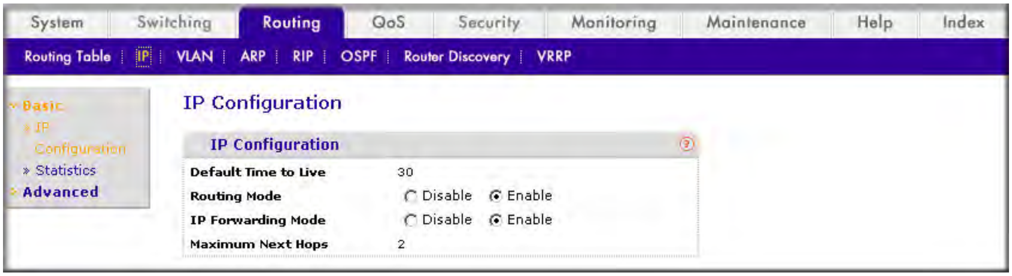
```
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20 mode
(Netgear Switch) (Interface 1/0/4)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Configuring VRRP on a Backup Router

To use the Web interface to configure VRRP on a backup router on the switch, proceed as follows:

1. Enable IP routing on the switch.

   a. From the main menu, select Routing > IP > 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

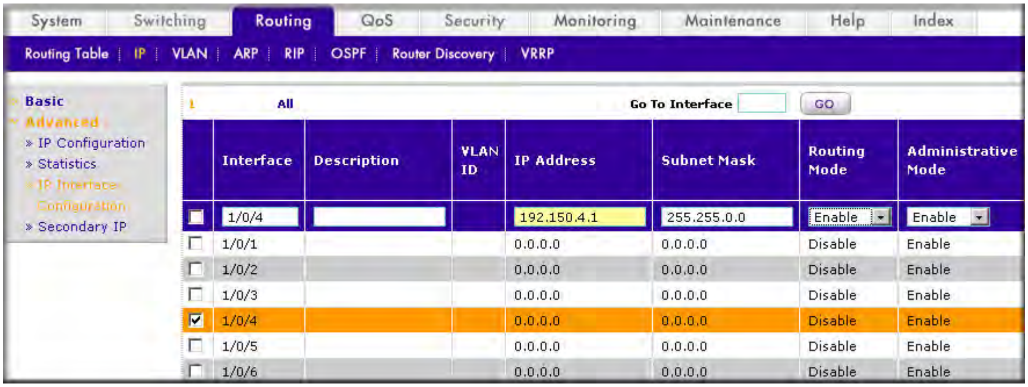
Figure 10-5

   b. Next to the Routing Mode, select the **Enable** radio button.

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

2. Assign IP address 192.150.4.1 to the port 1/0/4.

   a. From the main menu, 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
□	1/0/4			192.150.4.1	255.255.0.0	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
□	1/0/5			0.0.0.0	0.0.0.0	Disable	Enable
□	1/0/6			0.0.0.0	0.0.0.0	Disable	Enable

Figure 10-6

   b. Under IP Interface Configuration, scroll down to interface **1/0/4** and select the checkbox for that interface. Now 1/0/4 appears in the Interface field at the top.

   c. Enter the following information in the IP Interface Configuration:

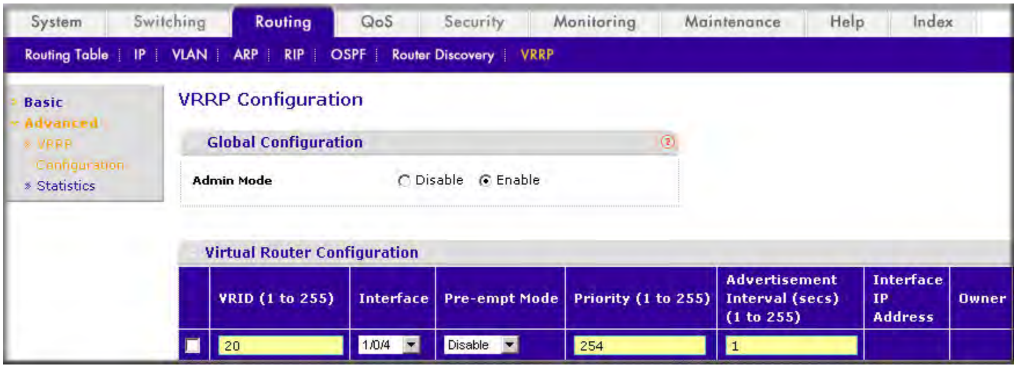
   - In the IP Address field, enter **192.150.4.1**.

- In the Network Mask field, enter **255.255.0.0**.
- Select **Enable**in the Admin Mode field.

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

3. Enable VRRP on the 1/0/4.

a. From the main menu, select Routing > VRRP > Basic> VRRP Configuration. A screen similar to the following displays.



VRRP Configuration

Global Configuration

Admin Mode ○ Disable ● Enable

Virtual Router Configuration

	VRID (1 to 255)	Interface	Pre-empt Mode	Priority (1 to 255)	Advertisement Interval (secs) (1 to 255)	Interface IP Address	Owner
□	20	1/0/4	Disable	254	1		

Figure 10-7

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

c. Enter the following information in the Virtual Router Configuration:

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

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

Chapter 11
Access Control Lists (ACLs)

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

- "Set up an IP ACL with Two Rules" on page 11-3
- "Configure a One-Way Access Using a TCP Flag in an ACL" on page 11-8
- "Configure Isolated VLANs on a Layer 3 Switch by Using ACLs" on page 11-26
- "Set up a MAC ACL with Two Rules" on page 11-39
- "ACL Mirroring" on page 11-43
- "ACL Redirect" on page 11-49
- "Configure IPv6 ACLs" on page 11-55

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 Layer3. MAC ACLs are used for Layer 2. IP ACLs are used for Layers 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.

- Maximum of 100 ACLs
- Maximum 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 - 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

Configuring IP ACLs

IP ACLs classify for Layer 3.

Each ACL is a set of up to ten 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 may 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 will be denied access.

Process

To configure ACLs, follow these steps:

- Create an ACL by specifying a name (MAC ACL) or a number (IP ACL).
- Add new rules to the ACL.
- Configure the match criteria for the rules.
- 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 only be accepted by the 7000 Series Managed Switch if the source and destination stations have IP addresses within the defined sets.

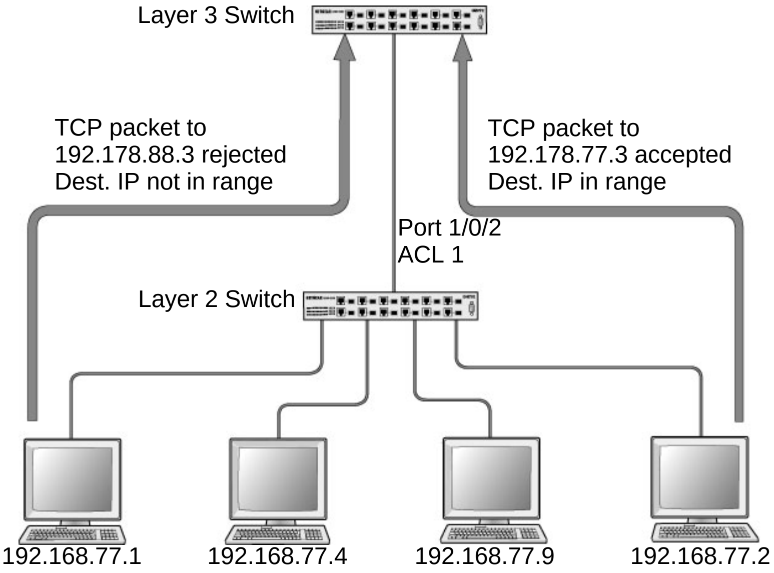


Figure 11-1

CLI: Setting 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 with a match on 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.

CLI Commands

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

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

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

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

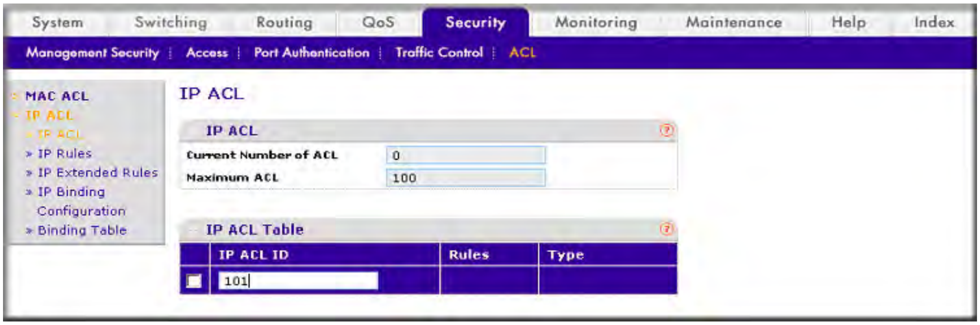
```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip access-group 101 in
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Setting up an IP ACL with Two Rules

To use the Web interface to configure IP ACL on a port on the switch, proceed as follows:

1. Create IP ACL 101 on the switch:

   a. From the main menu, 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		

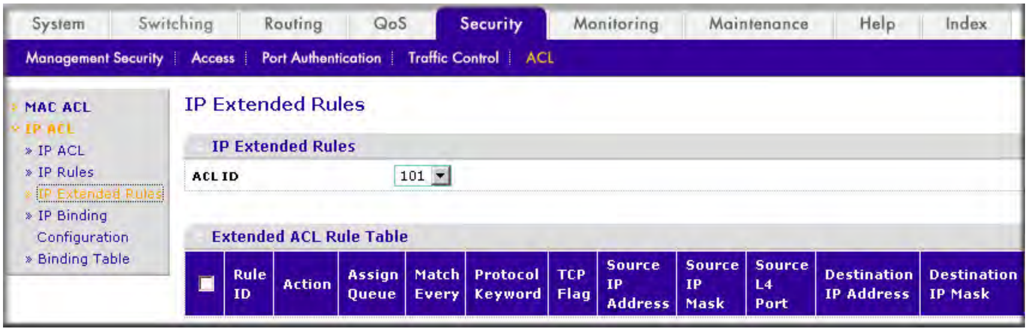
Figure 11-2

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

   c. Click **Add** to create ACL 101.

2. Create a new rule associated with the ACL 101.

   a. From the main menu, 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

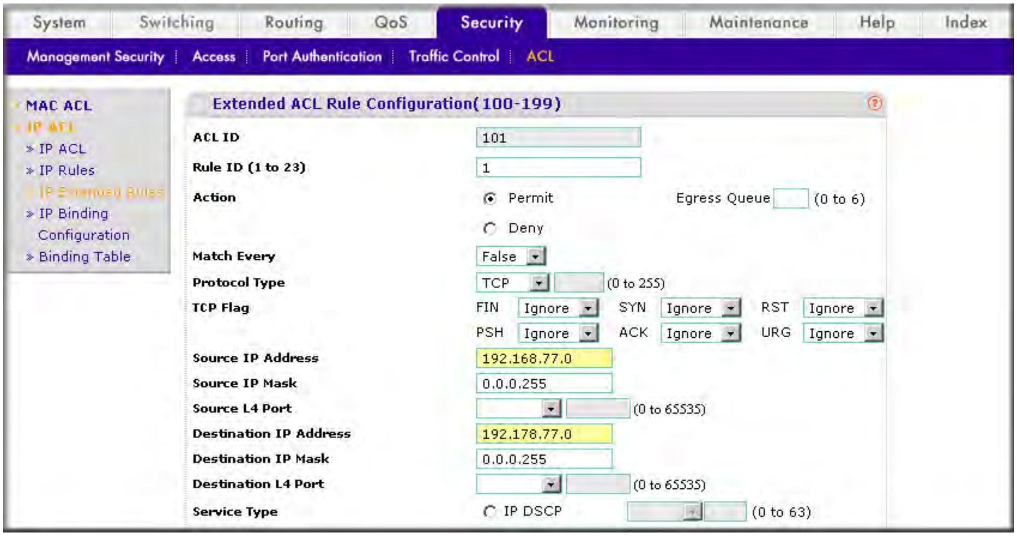
Figure 11-3

b. Next to ACL ID, select **101**.

c. Click **Add** to create a new rule.

3. Create a new ACL rule and add it to the ACL 101.

a. After you click the Add button on the 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)

Figure 11-4

a. Enter the following information in the Extended ACL Rule Configuration.

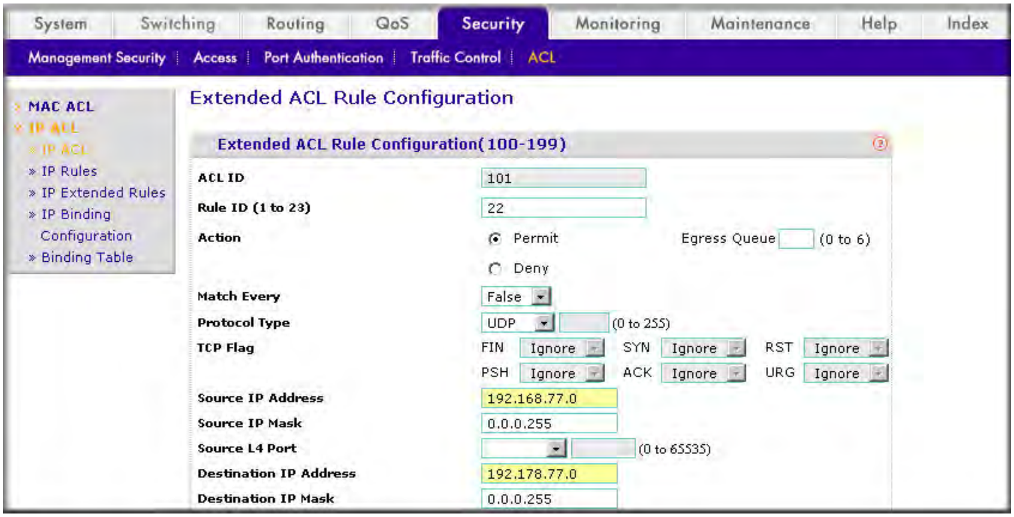
- In the Rule ID(1 to 23) field, enter **1**.
- Next to the Action, select **Permit** radio button.

- Select **TCP** in the Protocol Type field.
- In the Source IP Address, enter **192.168.77.0**.
- In the Source IP Mask, enter **0.0.0.255**.
- In the Destination IP Address, enter **192.178.77.0**.
- In the Destination IP Mask, 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 on the 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	Egress Queue	(0 to 6)
	○ Deny		
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		

Figure 11-5

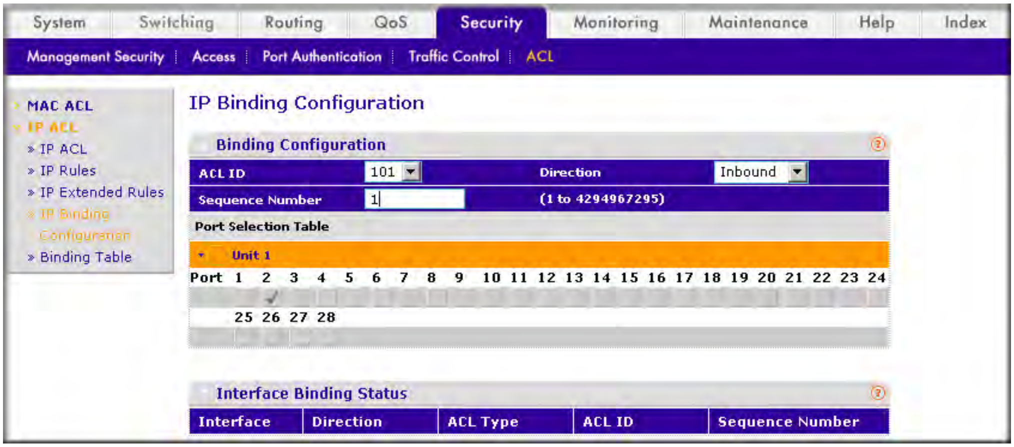
b. Enter the following information in the Extended ACL Rule Configuration.

- In the Rule ID(1 to 23) field, enter **2**.
- Next to the Action, select **Permit** radio button.
- Select the **UDP** in the Protocol Type field.
- In the Source IP Address, enter **192.168.77.0**.
- In the Source IP Mask, enter **0.0.0.255**.
- In the Destination IP Address, enter **192.178.77.0**.
- In the Destination IP Mask, enter **0.0.0.255**.

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

5. Apply the ACL 101 to the port 2.

a. From the main menu, 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

Figure 11-6

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

- Select **101** in the ACL ID field.
- In the Sequence Number field, enter **1**.

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

d. Click the gray box under port **2**. A flag appears in the box.

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

Configure a 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. PC1 can access FTP server1 and FTP server2 but PC2 only access FTP server2.

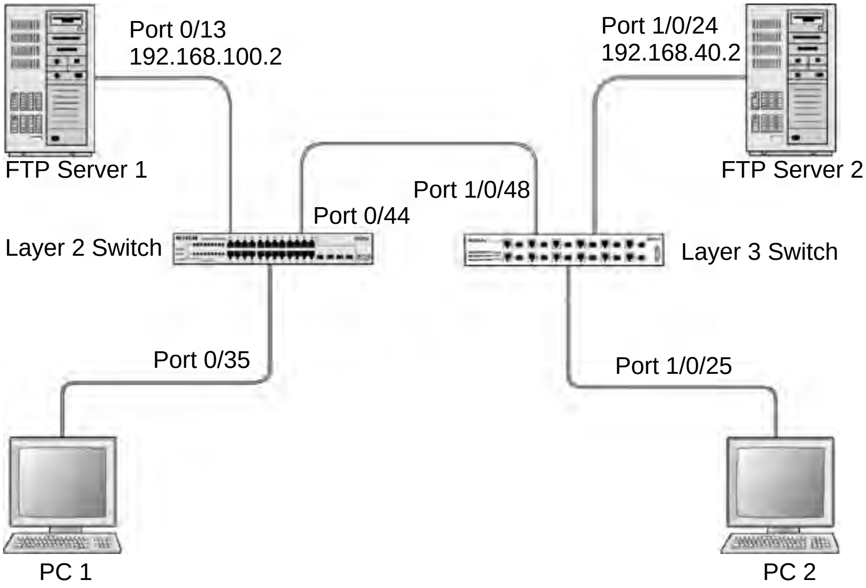


Figure 11-7

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

To use the CLI to configure the switch, enter the following CLI commands:

Step 1: Configure the Switch (see *Figure 11-7*)

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
```

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
```

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
```

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
```

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

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

Create an ACL that permits all the IP packets.

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

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

```
(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
```

Step 2: Configure the GSM7352S (see *Figure 11-7*)

To use the CLI to Configure the GSM7352S, enter the following CLI commands:

```
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
```

```
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

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
```

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
```

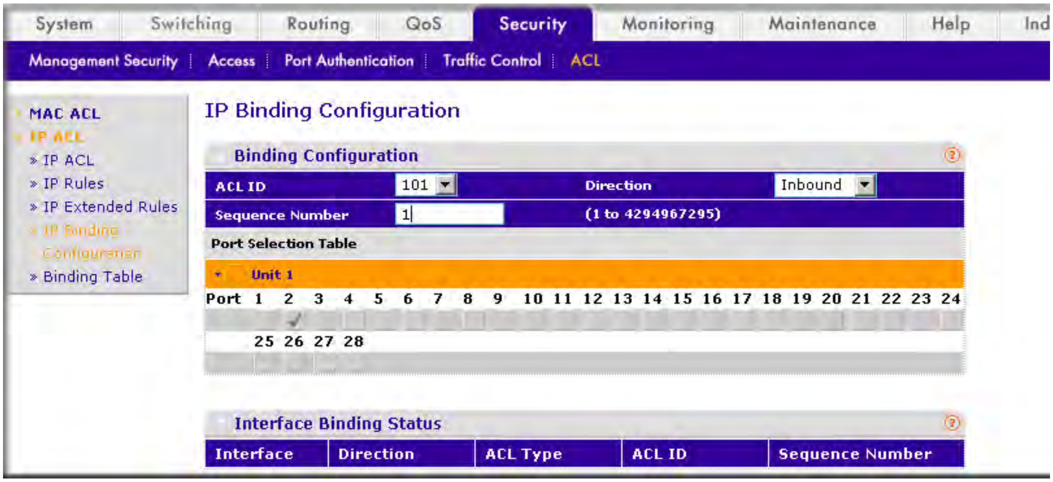
Web Interface: Configuring a One-Way Access Using a TCP Flag in an ACL

Configuring the Switch

To use the Web interface to configure the switch, proceed as follows:

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

a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. 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

Figure 11-8

b. Enter the following information in the VLAN Routing Wizard:

- 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**.

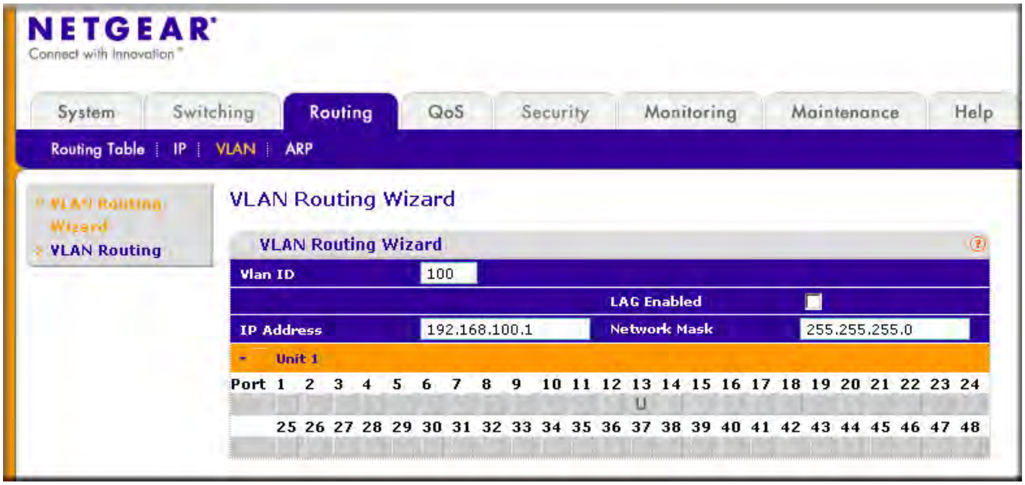
c. Click **Unit 1**. The ports display.

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. From the main menu, 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

Figure 11-9

b. Enter the following information in the VLAN Routing Wizard:

- 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**.

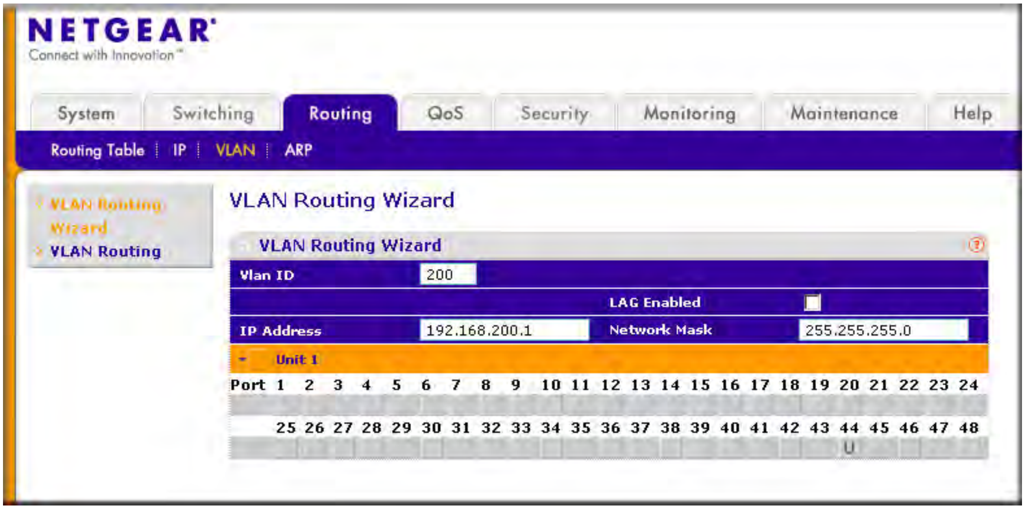
c. Click **Unit 1**. The ports display.

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. From the main menu, 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				

Figure 11-10

b. Enter the following information in the VLAN Routing Wizard:

- 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**.

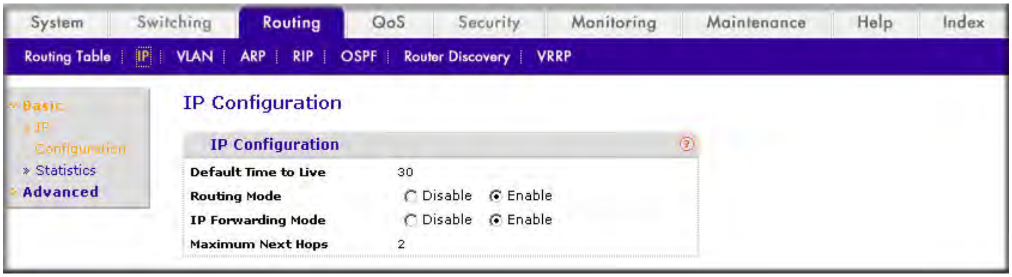
c. Click **Unit 1**. The ports display.

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. From the main menu, 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

Figure 11-11

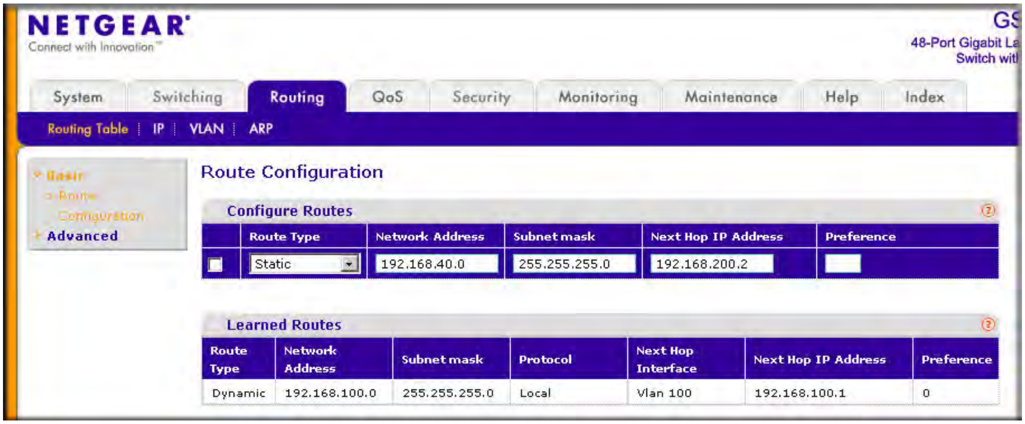
b. Under IP Configuration, make the following selections:

- Next to Routing Mode, select the **Enable** radio button.
- Next to 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. From the main menu, 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

Figure 11-12

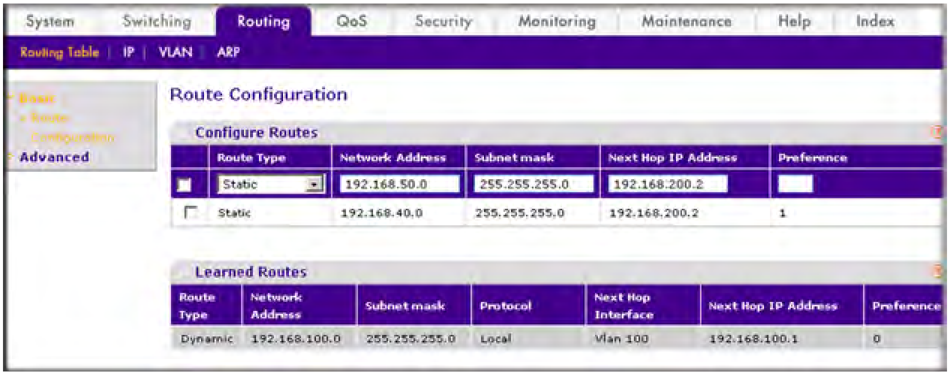
b. Under Configure Routes, make the following selection and enter the following information:

- Select **Static** in the Route Type field.
- 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. From the main menu, 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

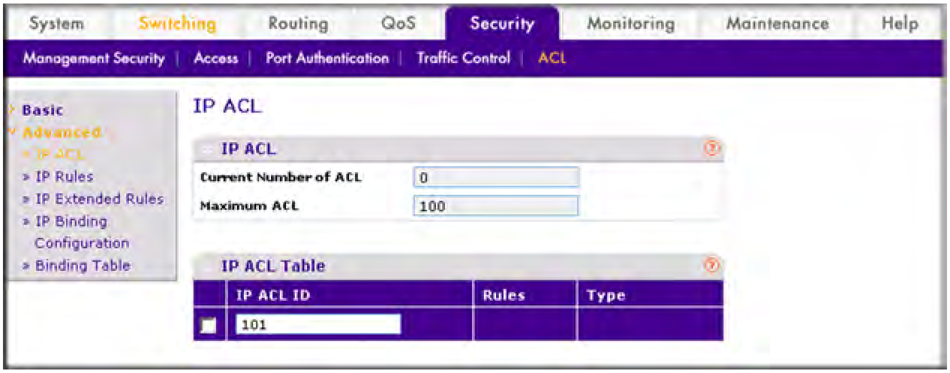
Figure 11-13

b. Under Configure Routes, make the following selection and enter the following information:
   - Select **Static** in the Route Type field.
   - 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. From the main menu, 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		

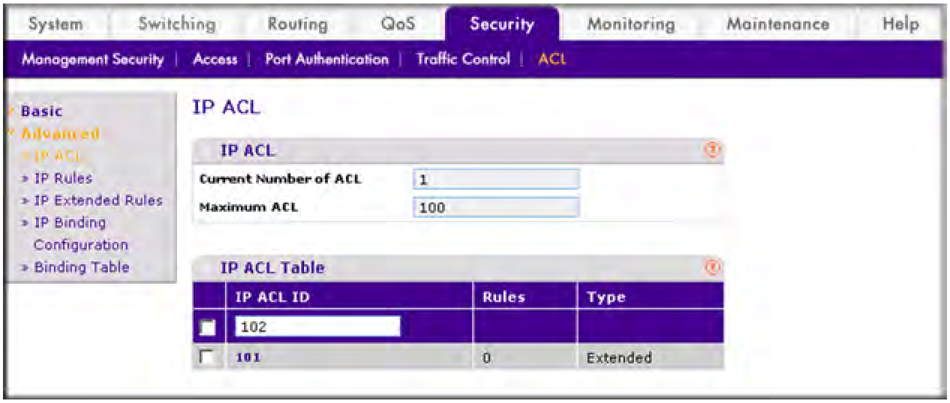
Figure 11-14

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

   c. Click **Add**.

8. Create an ACL with ID 102:

   a. From the main menu, 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

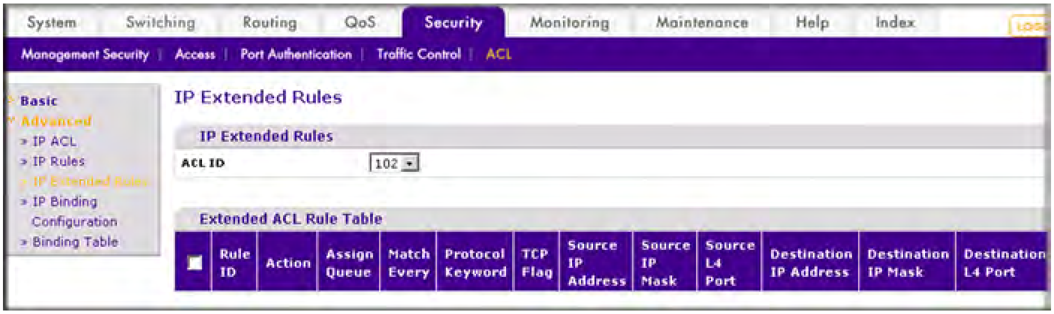
Figure 11-15

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

   c. Click **Add**.

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

   a. From the main menu, select Security > ACL > Advanced > IP Extended Rules. A screen similar to the following displays.



IP Extended Rules

IP Extended Rules

ACL ID	102

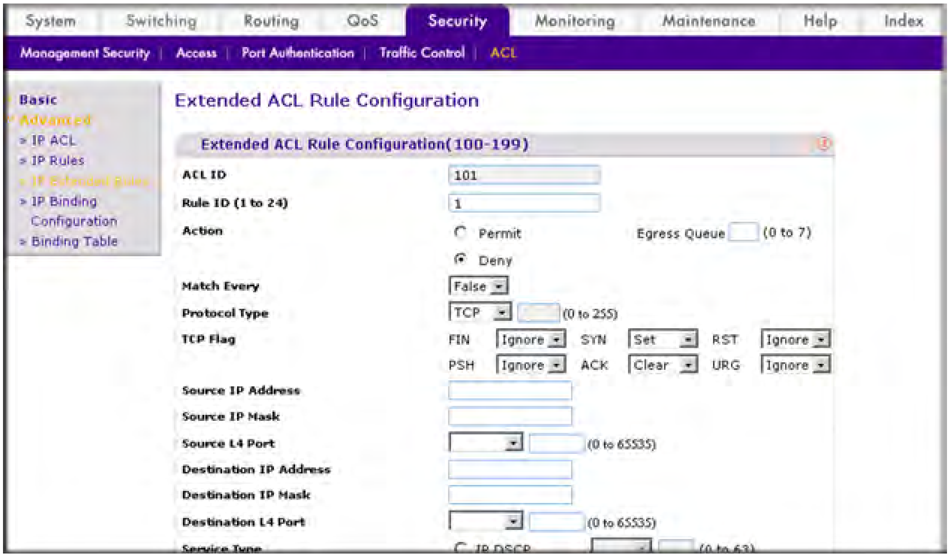
Extended ACL Rule Table

□	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

Figure 11-16

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

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	SYN Set	RST Ignore		
	PSH Ignore	ACK Clear	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)				

Figure 11-17

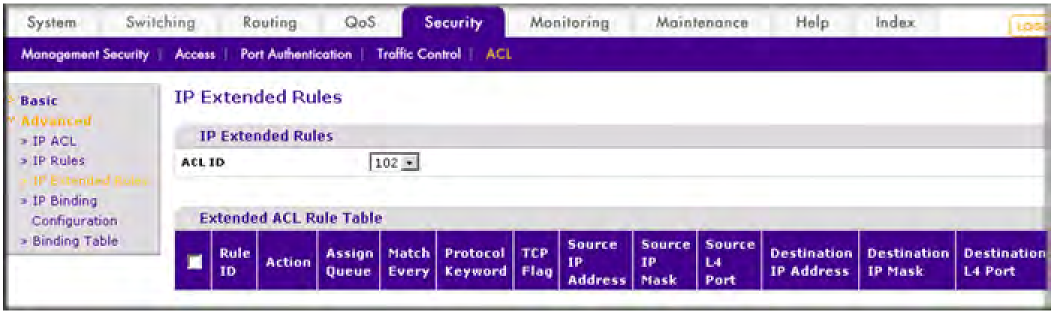
d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

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

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

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

a. From the main menu, select Security > ACL > Advanced > IP Extended Rules. A screen similar to the following displays.



IP Extended Rules

IP Extended Rules

ACL ID 102

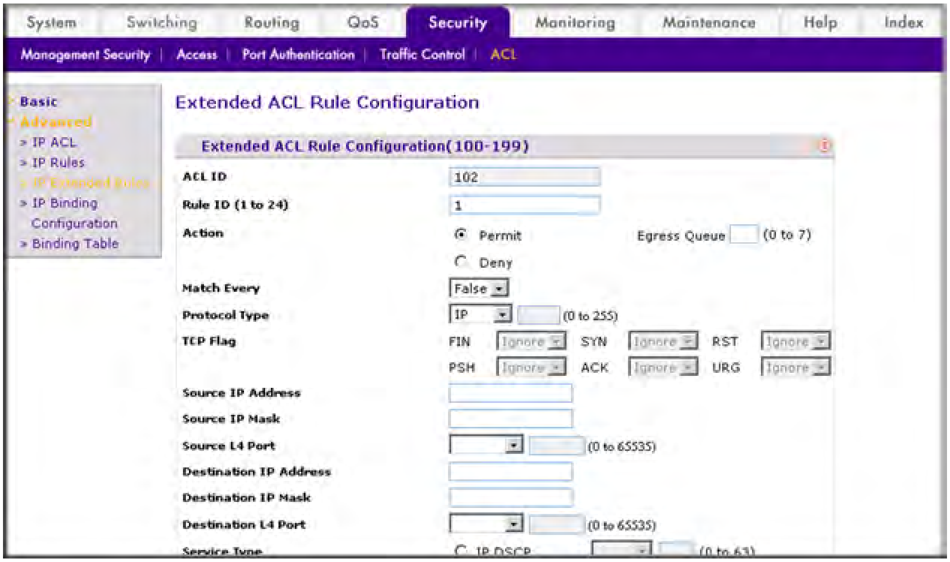
Extended ACL Rule Table

□	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

Figure 11-18

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

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)

Figure 11-19

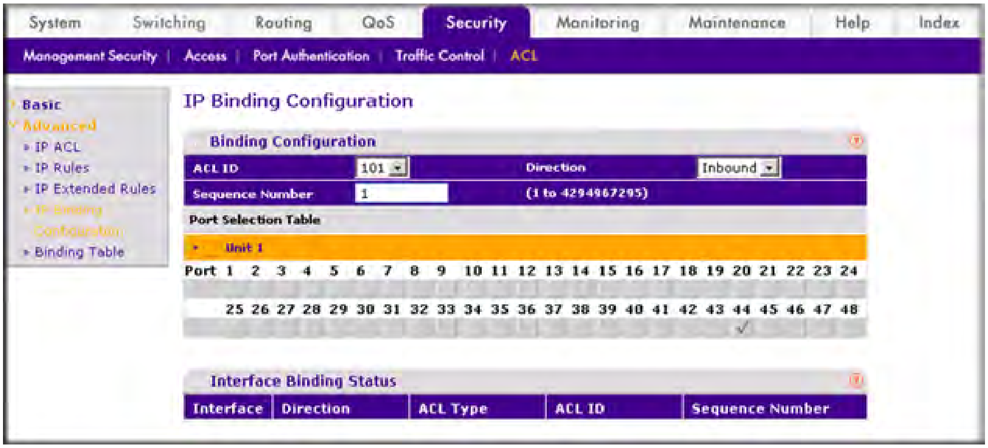
d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

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

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

11. Apply ACL 101 to port 44.

a. From the main menu, 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
																				✓				

Interface Binding Status

Interface	Direction	ACL Type	ACL ID	Sequence Number

Figure 11-20

b. Under Binding Configuration, make the following selection and enter the following information:

- Select **101** in the ACL ID field.
- In the Sequence Number field, enter **1**.

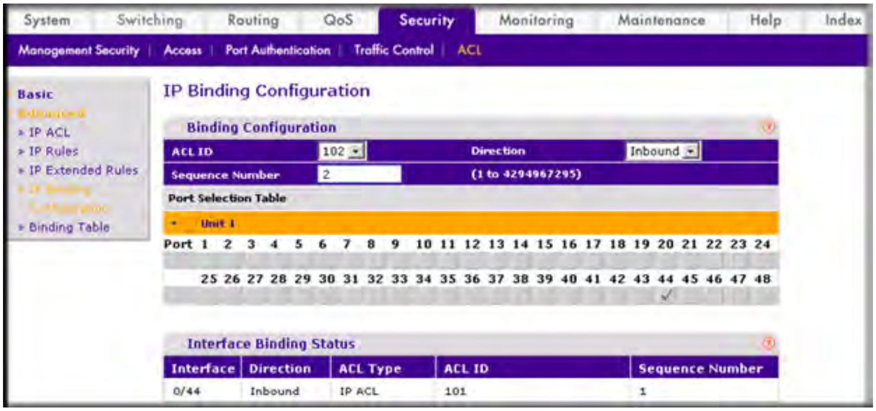
c. Click **Unit 1**. The ports display.

d. Click on the gray box under port 44. A flag appears in the box.

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

12. Apply ACL 102 to port 44.

a. From the main menu, 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)	

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
																				✓				

Interface Binding Status

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

Figure 11-21

b. Under Binding Configuration, make the following selection and enter the following information:

- Select **102** in the ACL ID field.
- In the Sequence Number field, enter **2**.

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

d. Click on the gray box under port 44. A flag appears in the box.

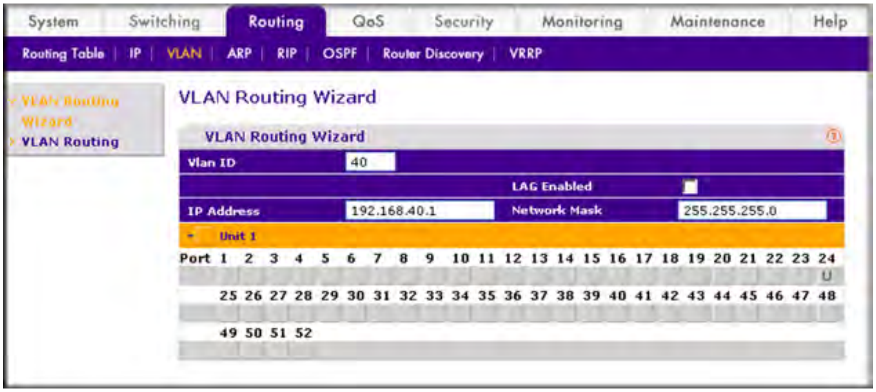
e. Click **Apply** to save the settings.

Configuring GSM7342S

To use the Web interface to configure the GSM7352S, proceed as follows:

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

a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.



VLAN Routing Wizard

VLAN Routing Wizard

Vlan ID 40

LAG Enabled □

IP Address 192.168.40.1 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
	49	50	51	52																				

Figure 11-22

b. Enter the following information in the VLAN Routing Wizard:

- 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**.

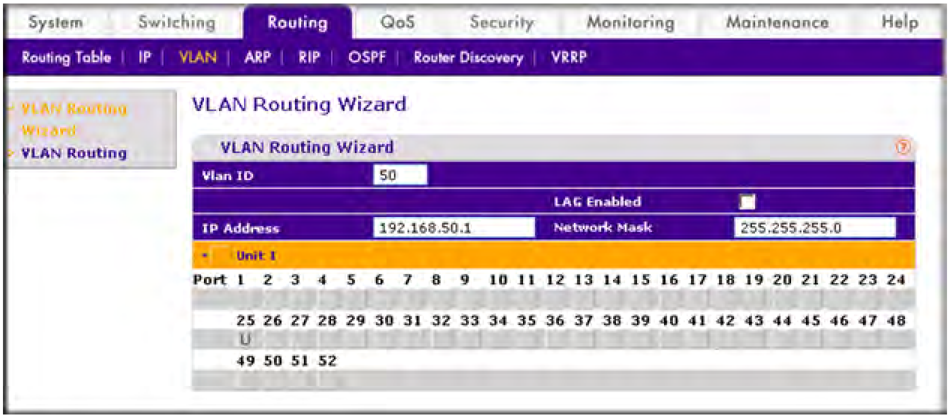
c. Click **Unit 1**. The ports display.

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. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.



VLAN Routing Wizard

VLAN Routing Wizard

Vlan ID 50

LAG Enabled □

IP Address 192.168.50.1 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

49 50 51 52

Figure 11-23

b. Enter the following information in the VLAN Routing Wizard:

- 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**.

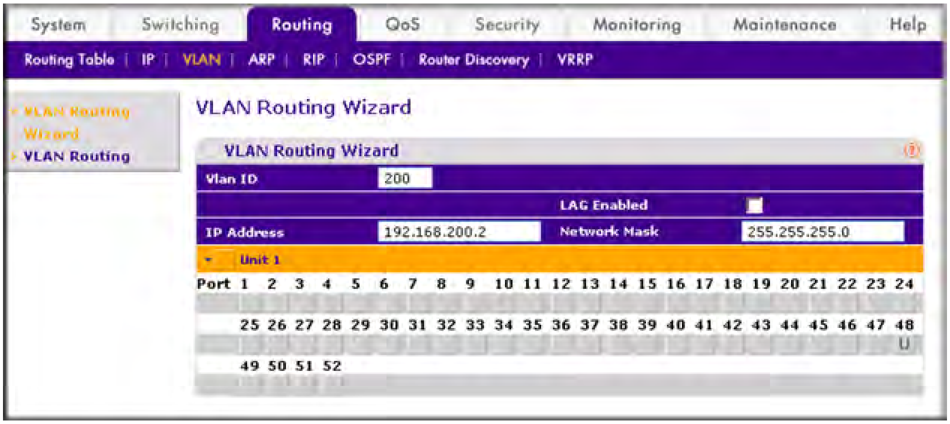
c. Click **Unit 1**. The ports display.

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. From the main menu, 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																				

Figure 11-24

b. Enter the following information in the VLAN Routing Wizard:

- 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**.

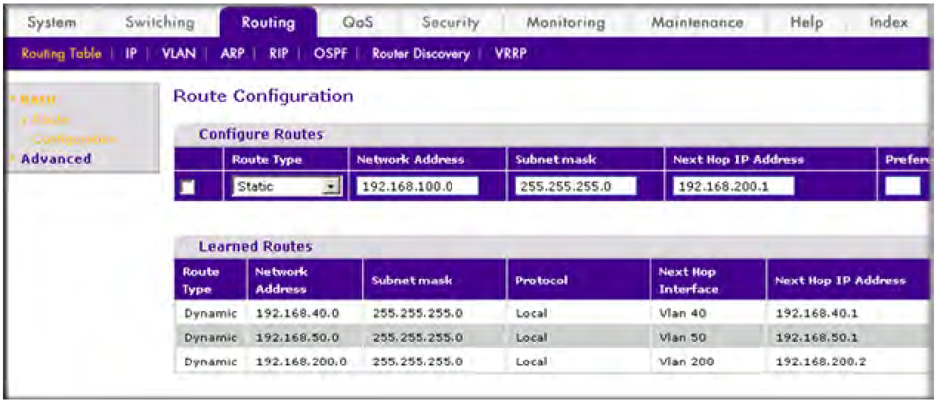
c. Click **Unit 1**. The ports display.

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. From the main menu, 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	192.168.100.0	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

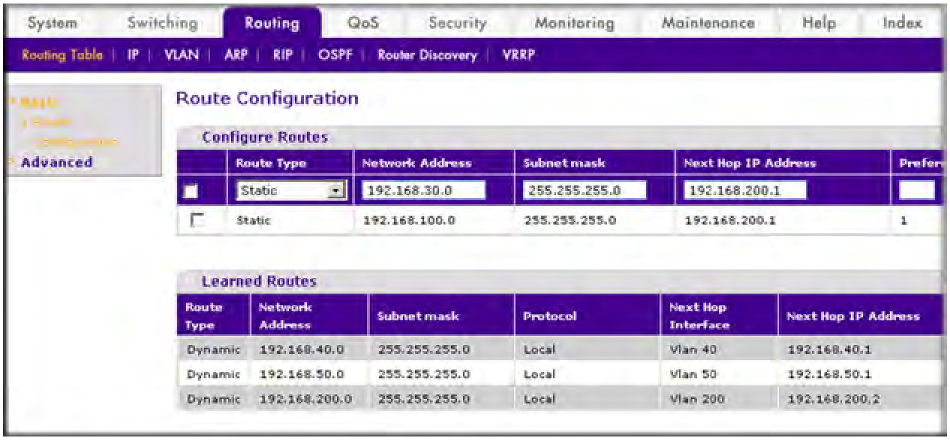
Figure 11-25

b. Under Configure Routes, make the following selection 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. From the main menu, 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

Figure 11-26

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

- Select **Static** in the Route Type field.
- 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**.

Configure Isolated VLANs on a Layer 3 Switch by Using ACLs

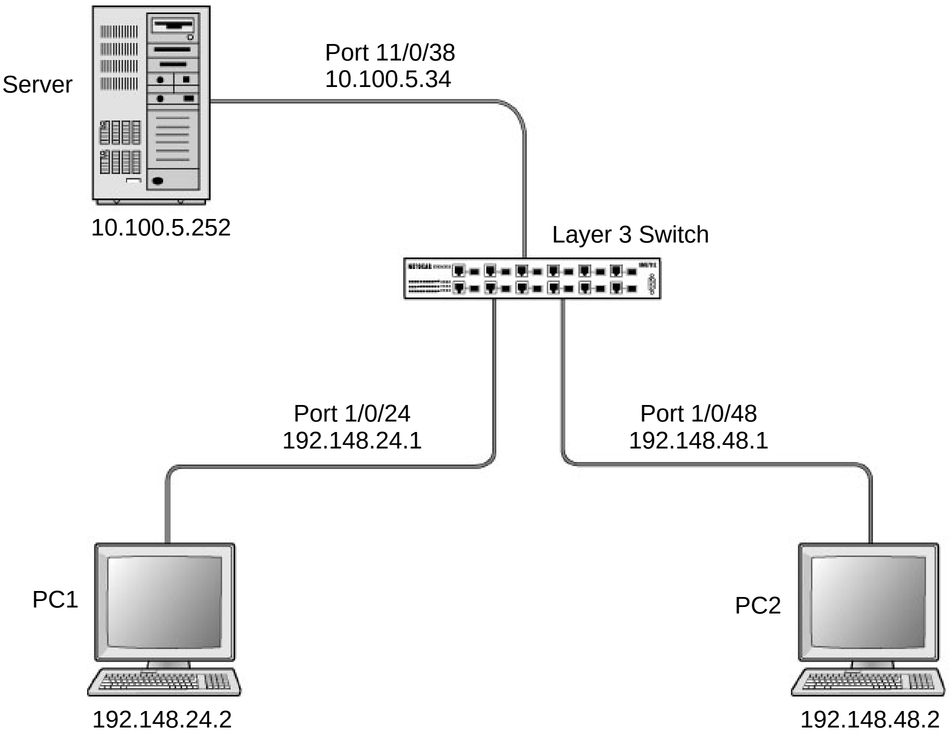


Figure 11-27

This example shows how to isolate VLANs on a Layer 3 switch by using ACLs. In this example, PC1 is in VLAN 24, PC2 is in VLAN 48, and server is in VLAN 38. PC1 and PC2 are isolated by an ACL but can both access the server. The example is shown as CLI commands and as a Web interface procedure.

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

To use the CLI to isolate VLANs on a Layer 3 switch by using ACLs, 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
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
```

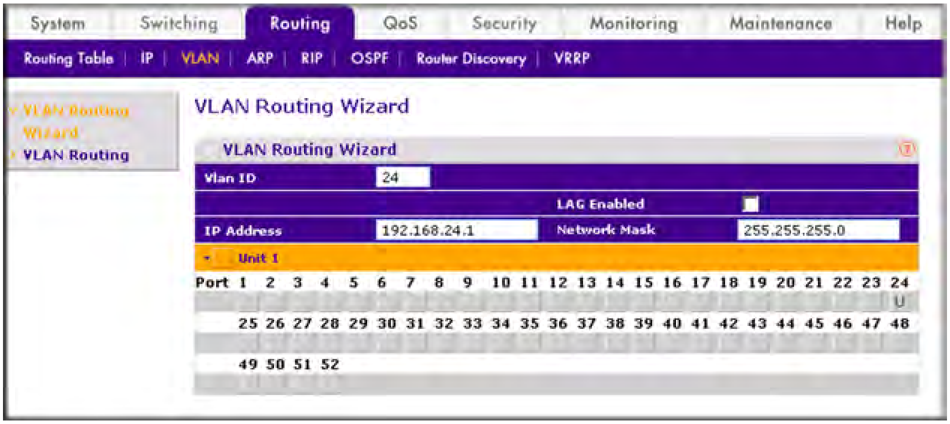
```
Create VLAN 38, add port 1/0/38 to it, and assign IP address 10.100.5.34 to it.
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 38
(Netgear Switch) (Vlan)#vlan routing
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/38
(Netgear Switch) (Interface 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

Enable IP routing on the switch.
(Netgear Switch) (Config)#ip routing

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

Create ACL 101 to deny all traffic that has destination IP 192.168.24.0/24.
(Netgear Switch) (Config)#access-list 101 deny ip any 192.168.24.0 0.0.0.255

Create ACL 102 to deny all traffic that has destination IP 192.168.48.0/24.
(Netgear Switch) (Config)#access-list 102 deny ip any 192.168.48.0 0.0.0.255
Create ACL 103 to permit all other traffic.
(Netgear Switch) (Config)#access-list 103 permit ip any any

Deny all traffic with 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

Deny all traffic with 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: Configuring a One-Way Access Using a TCP Flag in an ACL

To use the Web interface to isolate VLANs on a Layer 3 switch by using ACLs, proceed as follows:

1. Create VLAN 24 with IP address 192.168.24.1:

   a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.



VLAN Routing Wizard

Vlan ID	24		
		LAG Enabled	□
IP Address	192.168.24.1	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 — 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

Figure 11-28

   b. Enter the following information in the VLAN Routing Wizard:
      - 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**.

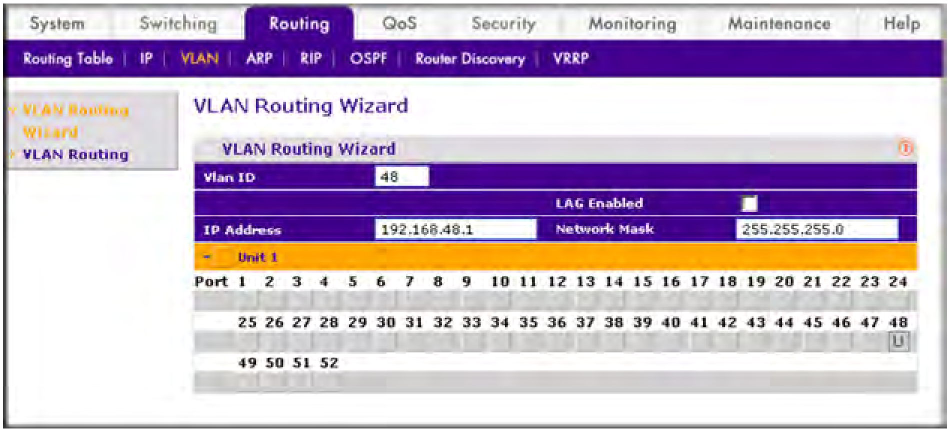
   c. Click **Unit 1**. The ports display.

   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. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.



VLAN Routing Wizard

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

U (port 48)

49 50 51 52

Figure 11-29

b. Enter the following information in the VLAN Routing Wizard:

- 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**.

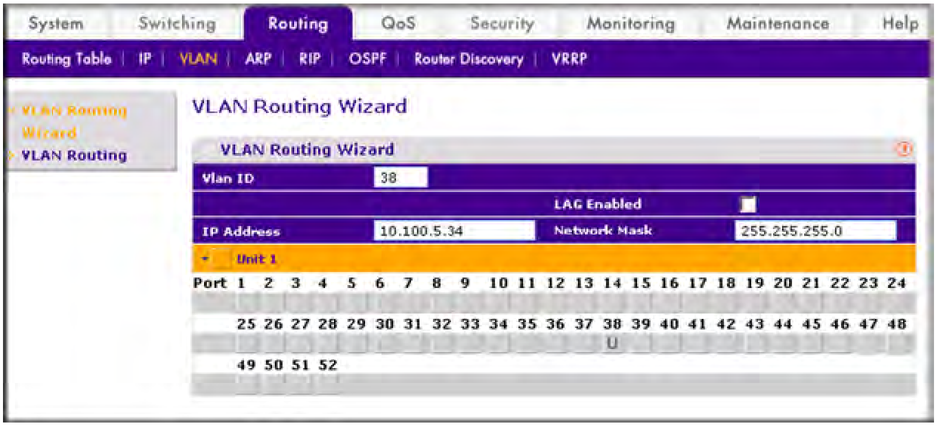
c. Click **Unit 1**. The ports display.

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. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.



VLAN Routing Wizard

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

Figure 11-30

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**.

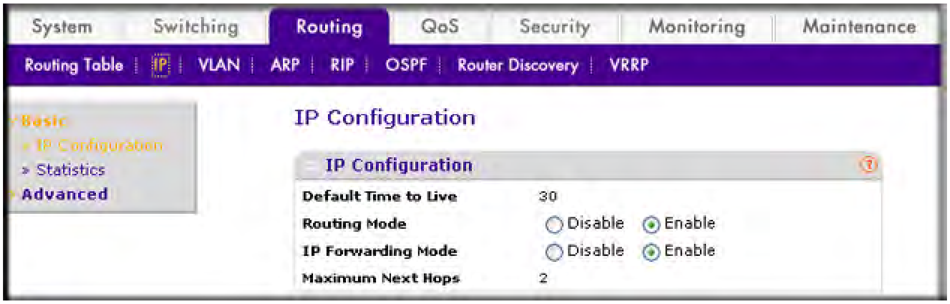
c. Click **Unit 1**. The ports display.

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. From the main menu, 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

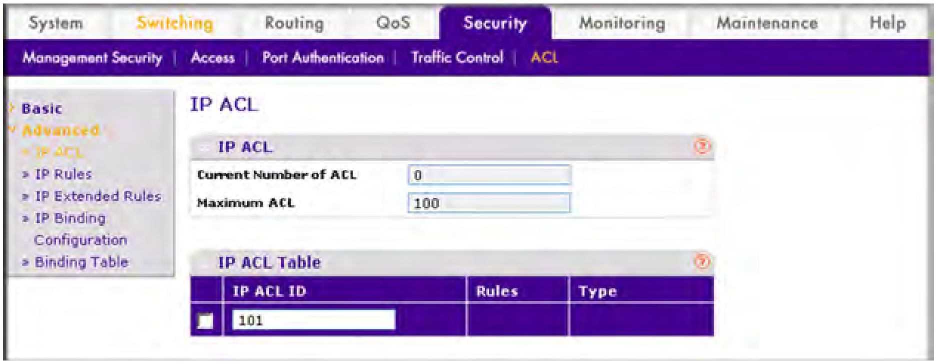
Maximum Next Hops 2

Figure 11-31

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

5. Create an ACL with ID 101:

- **a.** From the main menu, 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

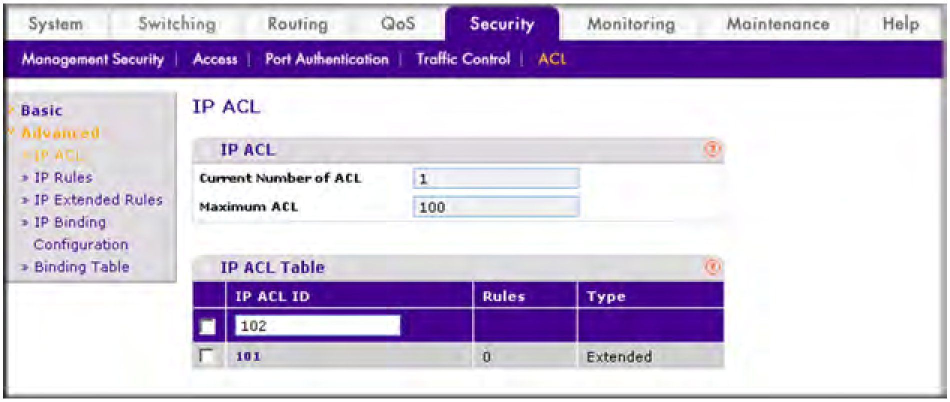
	IP ACL ID	Rules	Type
□	101		

Figure 11-32

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

6. Create an ACL with ID 102:

- **a.** From the main menu, 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

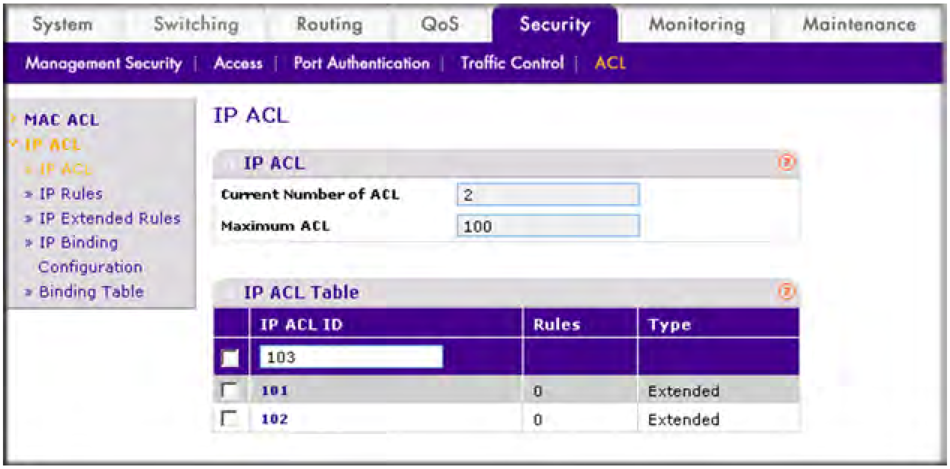
Figure 11-33

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

c. Click **Add**.

7. Create an ACL with ID 103:

a. From the main menu, 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

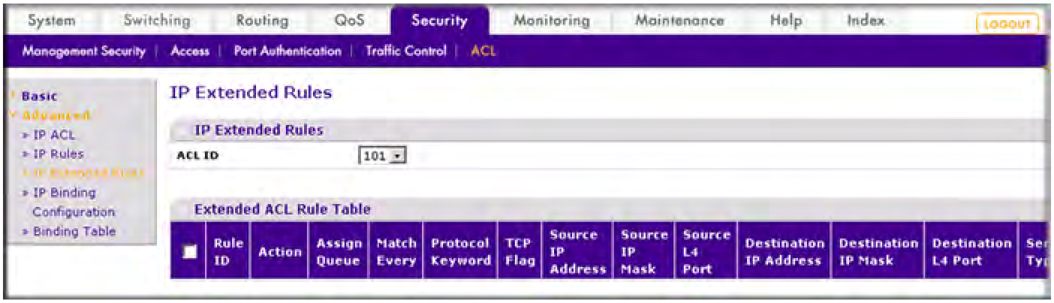
Figure 11-34

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. From the main menu, select Security > ACL > Advanced > IP Extended Rules. A screen similar to the following displays.



IP Extended Rules

IP Extended Rules

ACL ID	101

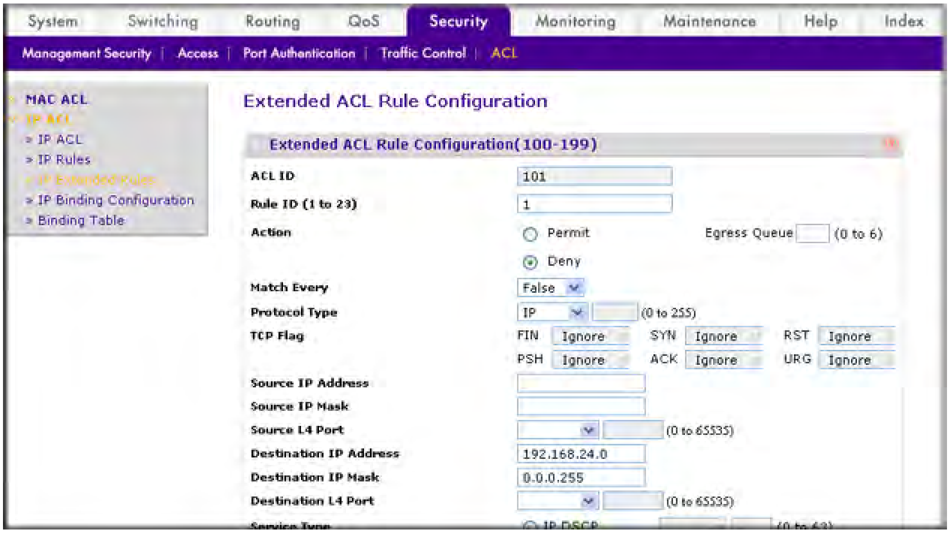
Extended ACL Rule Table

■	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	Ser Ty

Figure 11-35

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

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)

Figure 11-36

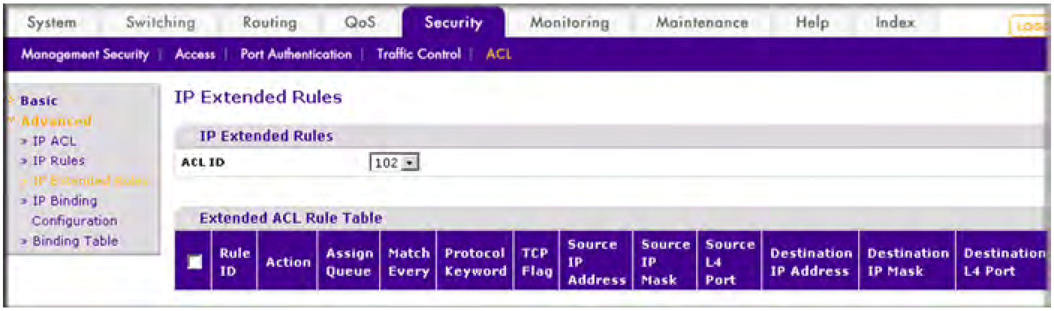
d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

- In the Rule ID field, enter **1**.
- Next to Action mode, select the **Deny** radio button.
- Select **False** in the Match Every field.
- 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. From the main menu, select Security > ACL > Advanced > IP Extended Rules. A screen similar to the following displays.



IP Extended Rules

IP Extended Rules

ACL ID 102

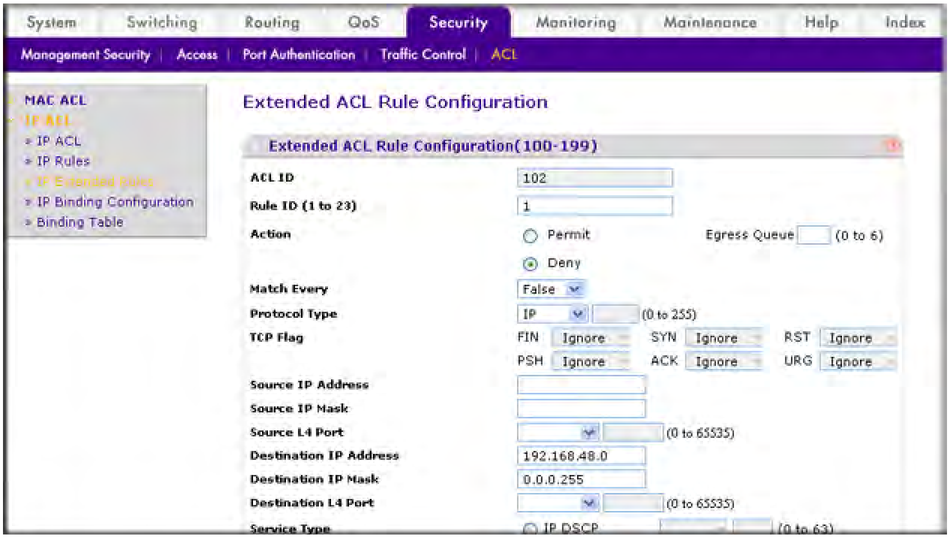
Extended ACL Rule Table

□	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

Figure 11-37

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

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)

Figure 11-38

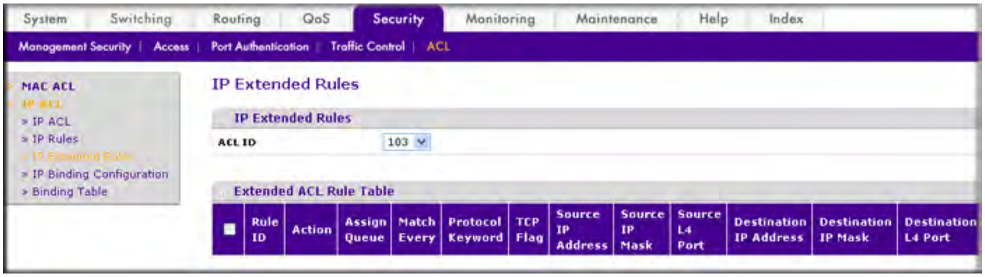
d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

- In the Rule ID field, enter **1**.
- Next to Action mode, select the **Deny** radio button.
- Select **False** in the Match Every field.
- 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. From the main menu, select Security > ACL > Advanced > IP Extended Rules. A screen similar to the following displays.



IP Extended Rules

IP Extended Rules

ACL ID	103

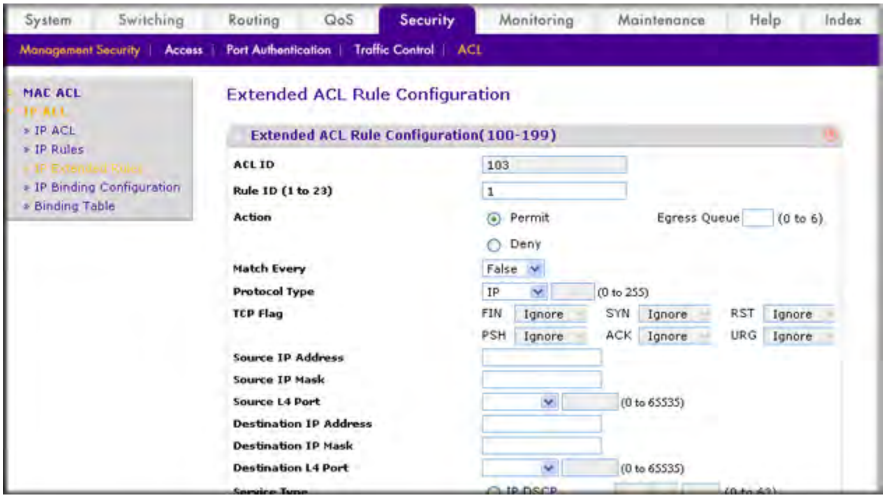
Extended ACL Rule Table

□	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

Figure 11-39

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

   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)

Figure 11-40

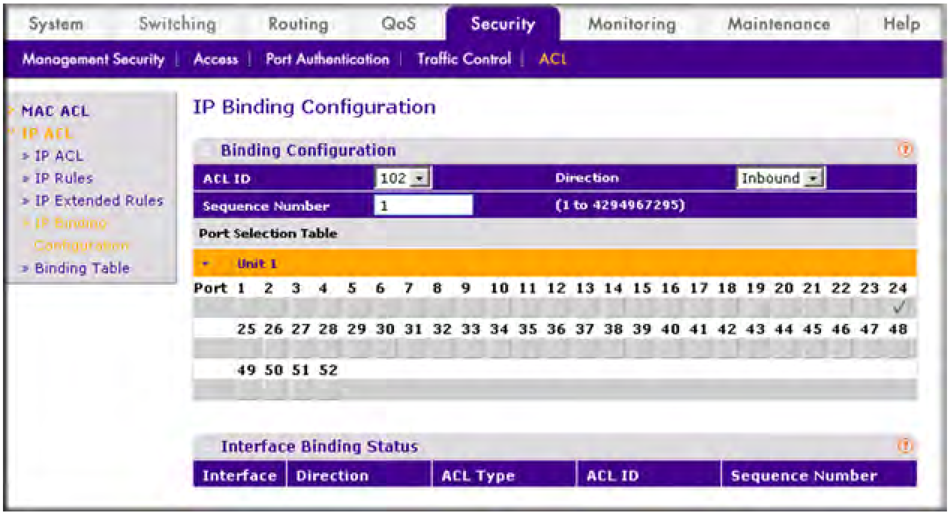
   d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

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

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

11. Apply ACL 102 to port 24:

a. From the main menu, 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 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

Figure 11-41

b. Under Binding Configuration, make the following selection and enter the following information:

- Select **102** in the ACL ID field.
- In the Sequence Number field, enter **1**.

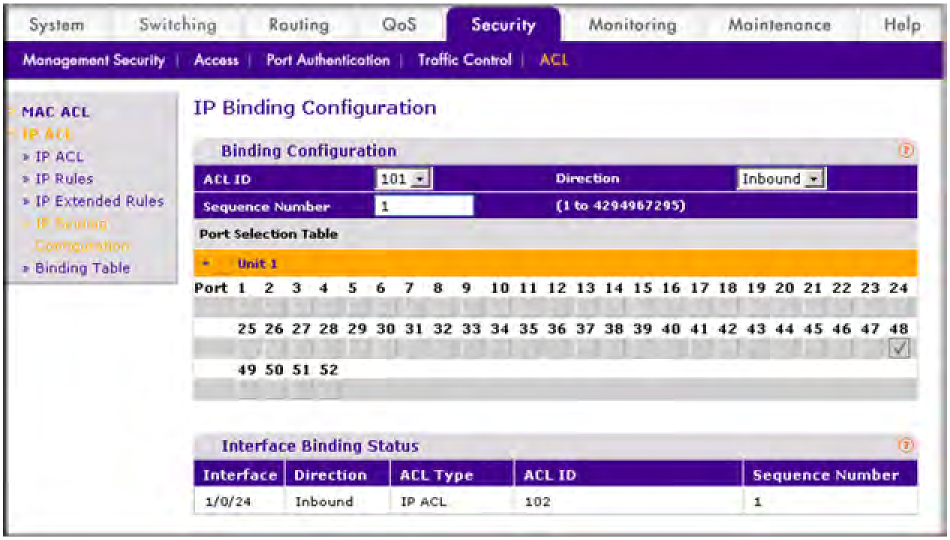
c. Click **Unit 1**. The ports display.

d. Click on the gray box under port 24. A flag appears in the box.

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

12. Apply ACL 101 to port 48:

a. From the main menu, 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 ☑

49 50 51 52

Interface Binding Status

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

Figure 11-42

b. Under Binding Configuration, make the following selection and enter the following information:

- Select **101** in the ACL ID field.
- In the Sequence Number field, enter **1**.

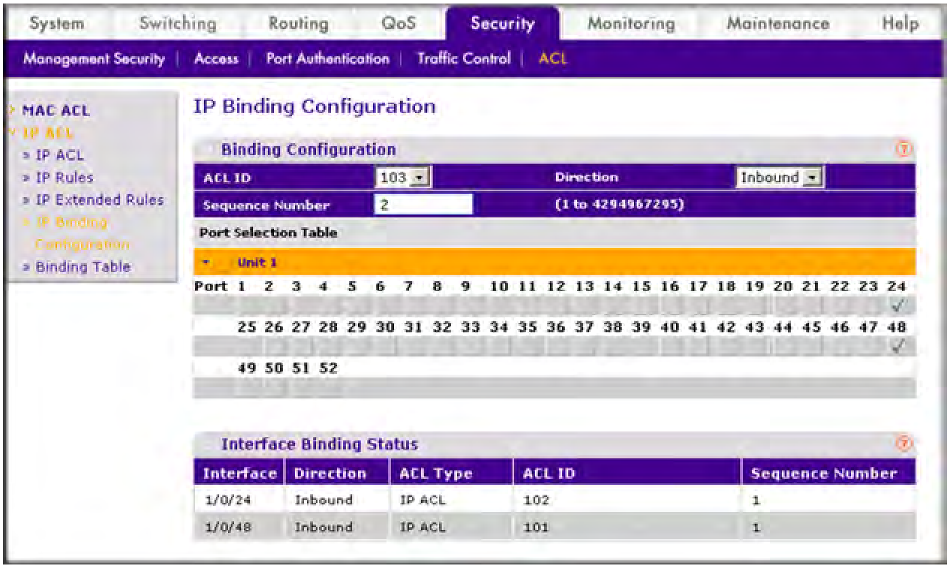
c. Click **Unit 1**. The ports display.

d. Click on the gray box under port 48. A flag appears in the box.

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

13. Apply ACL 103 to port 24 and port 48:

a. From the main menu, 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

Figure 11-43

b. Under Binding Configuration, make the following selection and enter the following information:

- Select **103** in the ACL ID field.
- In the Sequence Number field, enter **2**.

c. Click **Unit 1**. The ports display. Configure the following ports:

- Click on the gray box under port 24. A flag appears in the box.
- Click on the gray box under port 48. A flag appears 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: Setting up a MAC ACL with Two Rules

Create a new MAC ACL acl_bpdu.

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

Deny all the traffic which 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
```

Permit all the other traffic.

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

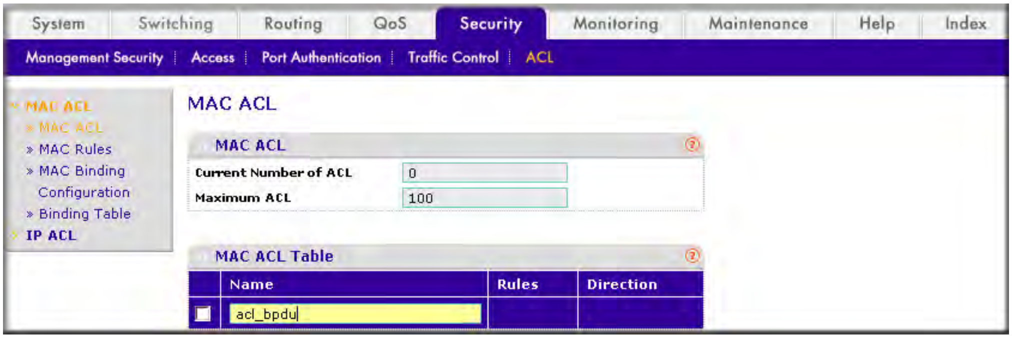
Apply the MAC ACL acl_bpdu to the port 1/0/2.

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

Web Interface: Setting up a MAC ACL with Two Rules

To use the Web interface to configure MAC ACL on a port on the switch, proceed as follows:

1. Create MAC ACL 101 on the switch:
   a. From the main menu, select Security > ACL > MAC ACL. A screen similar to the following displays.



MAC ACL

MAC ACL

Current Number of ACL	0
Maximum ACL	100

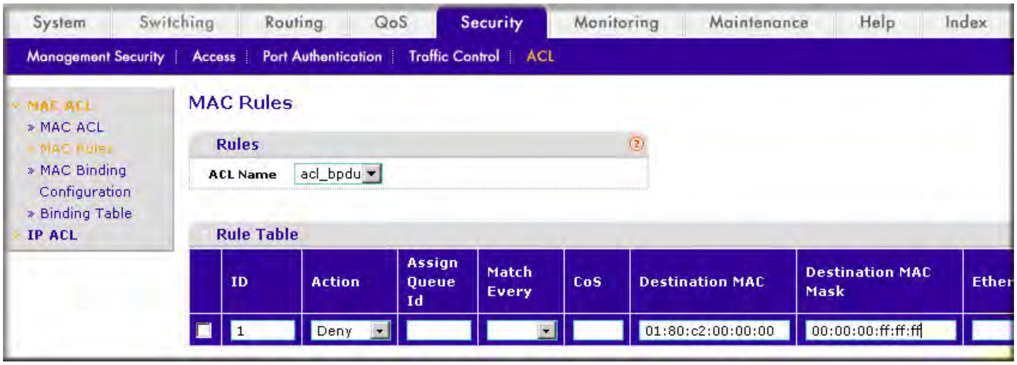
MAC ACL Table

	Name	Rules	Direction
□	acl_bpdu		

Figure 11-44

   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. From the main menu, 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	

Figure 11-45

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

b. Select **Deny** in the Action field.

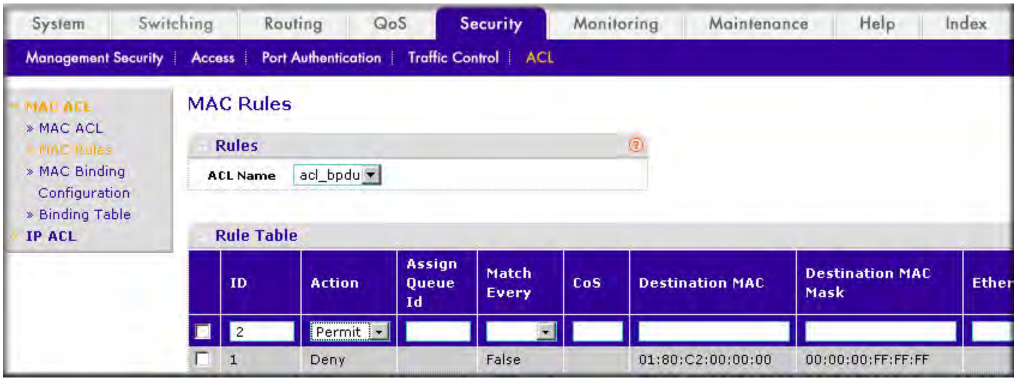
c. Enter the following information in the Rule Table.

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

d. Click the **Add** button.

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

a. From the main menu, 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	

Figure 11-46

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

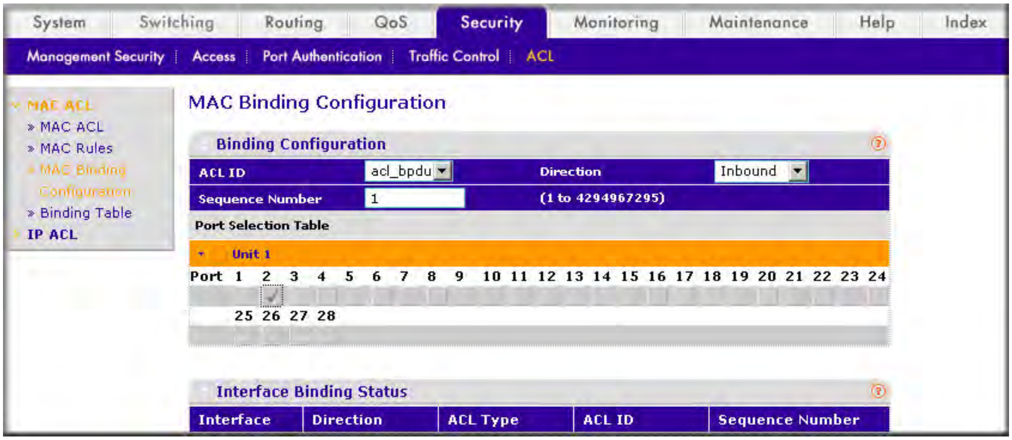
b. Enter the following information in the Rule Table.

- In the ID field, enter **2**.
- Select the **Permit** in the Action field.

c. Click the**Add** button.

4. Apply the ACL acl_bpdu to the port 2.

a. From the main menu, 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

Figure 11-47

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

- Select **acl_bpdu** in the ACL ID field.
- In the Sequence Number field, enter **1**.

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

d. Click the gray box under port **2**. A flag appears in the box.

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

ACL Mirroring

This feature extends the existing port mirroring functionality by allowing to mirror a desired traffic stream in an interface. It helps to mirror the desired traffic stream rather mirroring entire traffic in an interface. It has been associated with ACL functionality. Define ACL Rule matching the desired traffic with the option mirror to an interface. Whatever the traffic matching this rule will be copied to the specified mirrored interface.

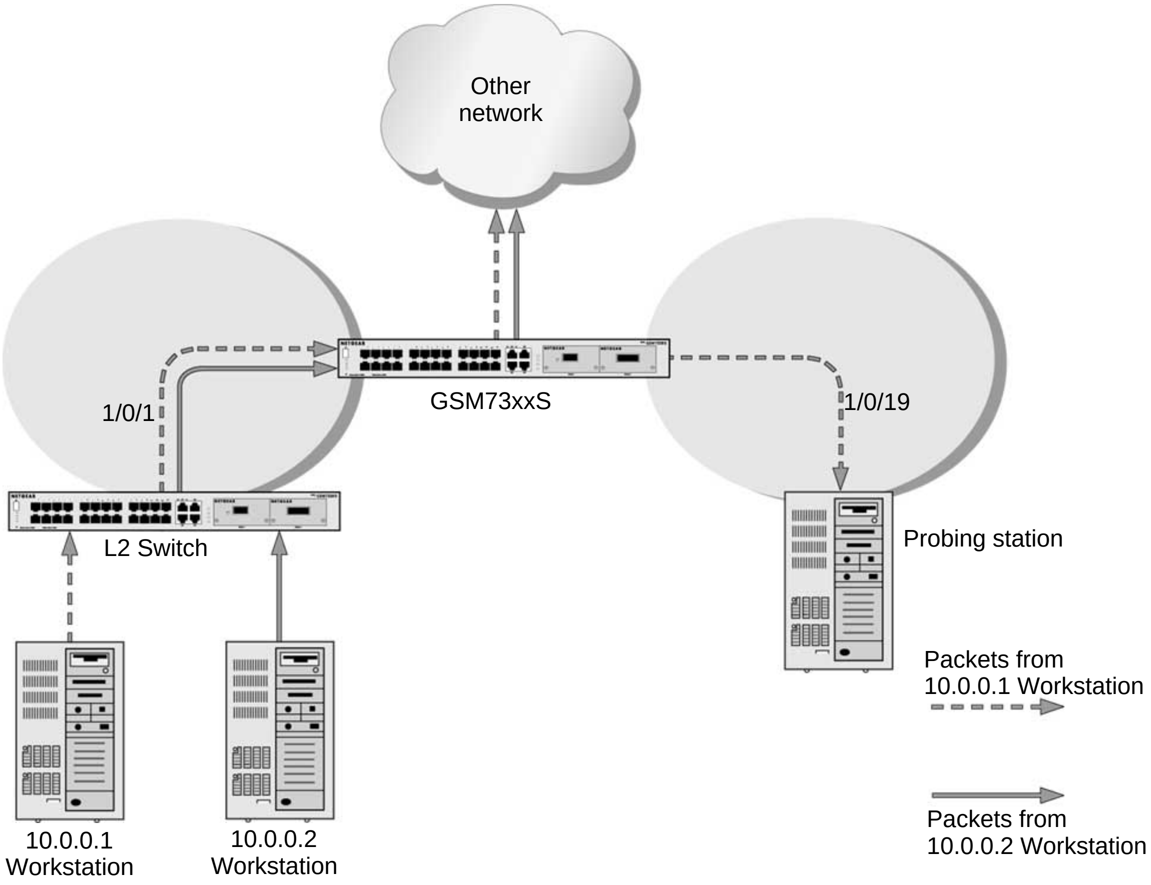


Figure 11-48

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.

CLI: Configuring ACL Mirroring

Create an IP Access Control List with the name monitorHost.

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

Define the rules to match the host 10.0.0.1 and to permit every other.

```
(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
```

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

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

View the configuration.

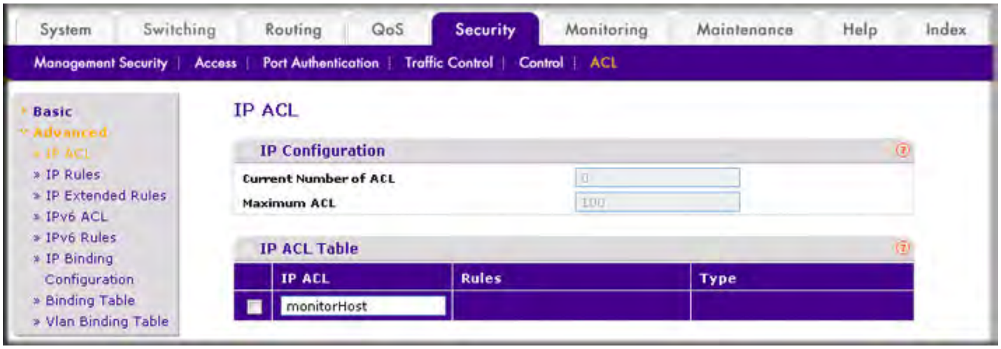
```
(Netgear Switch) # show ip access-lists
Current number of ACLs: 1  Maximum number of ACLs: 100

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: Configuring ACL Mirroring

To use the Web interface to configure IP ACL on a port on the switch, proceed as follows:

1. Create an IP access control list with the name monitorHost on the switch:

   a. From the main menu, 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

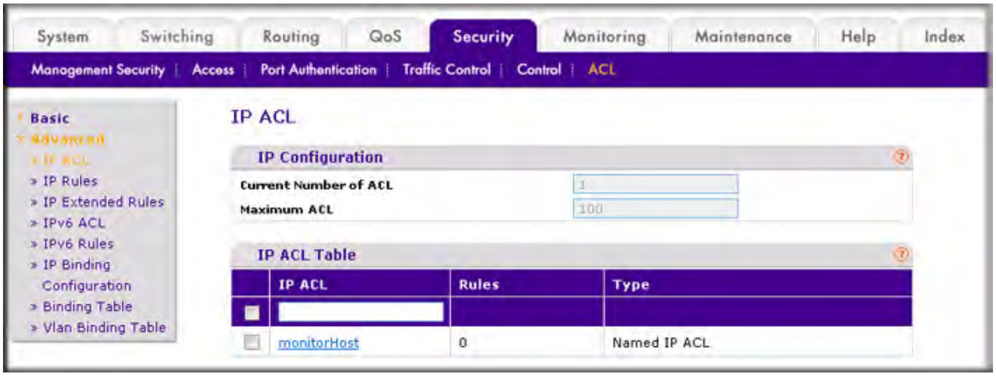
IP ACL Table

	IP ACL	Rules	Type
□	monitorHost		

Figure 11-49

   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

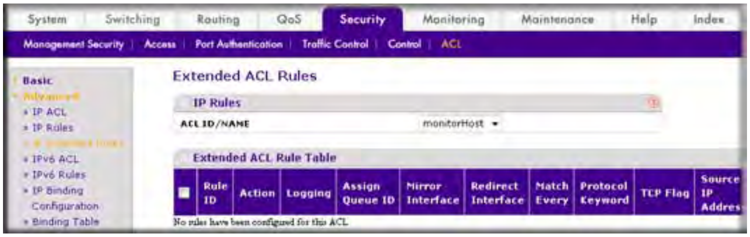
IP ACL Table

	IP ACL	Rules	Type
□			
□	monitorHost	0	Named IP ACL

Figure 11-50

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

a. From the main menu, select Security > ACL > Advanced > IP Extended Rules. A screen similar to the following displays.



Extended ACL Rules

IP Rules

ACL ID/NAME monitorHost

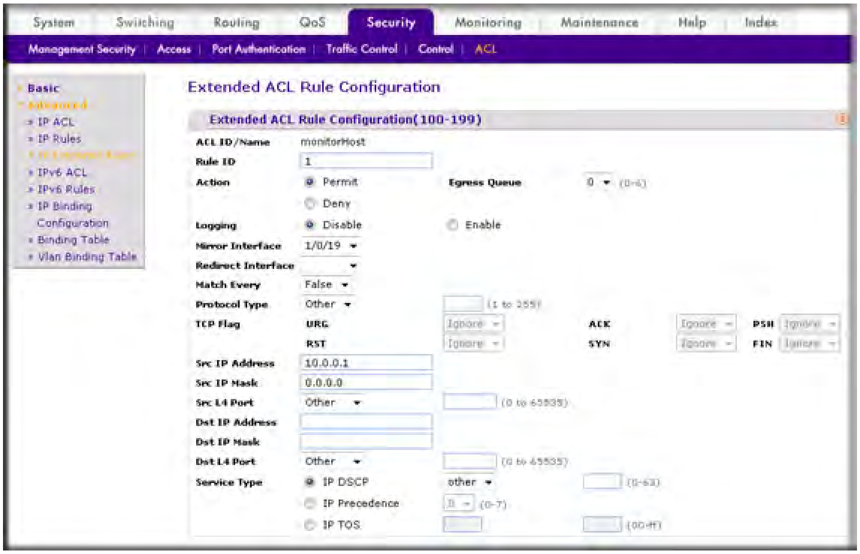
Extended ACL Rule Table

□	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

Figure 11-51

b. Click **Add** to take the Extended ACL Rule Configuration screen similar to the following 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)			

Figure 11-52

c. Enter Rule ID as **1**.

d. Selection Action as **Permit**.

e. Select Mirror Interface as **1/0/19**.

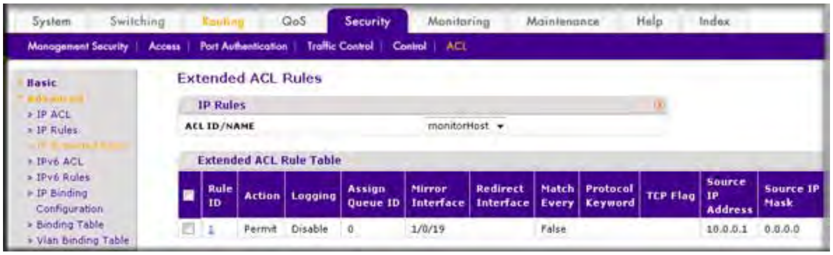
f. Enter Src IP address as **10.0.0.1**.

g. Enter Src IP Mask as **0.0.0.0**.

h. Click **Apply**. At the end of this configuration a screen similar to Figure 11-53 displays.

3. Create a rule to match every other traffic.

a. From the main menu, select Security > ACL > Advanced > IP Extended Rules. A screen similar to the following displays



Extended ACL Rules

IP Rules

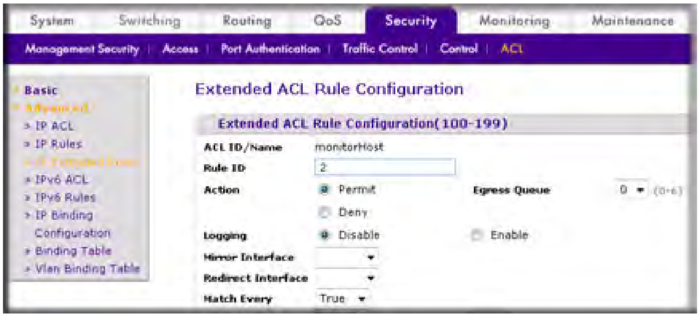
ACL ID/NAME monitorHost

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

Figure 11-53

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 ○ Deny

Egress Queue 0 (0-6)

Logging ● Disable ○ Enable

Mirror Interface

Redirect Interface

Match Every True

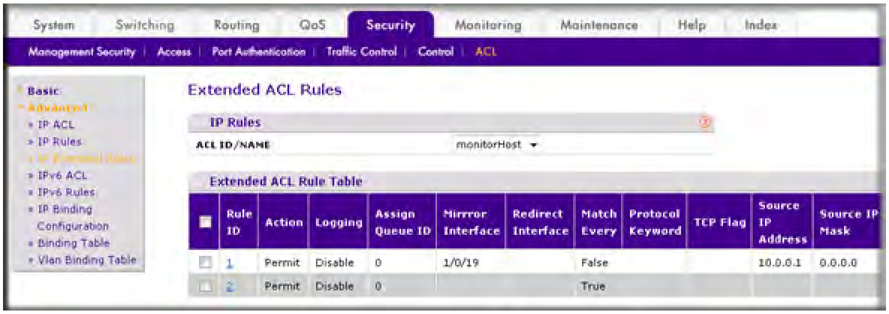
Figure 11-54

c. Enter the Rule ID as **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

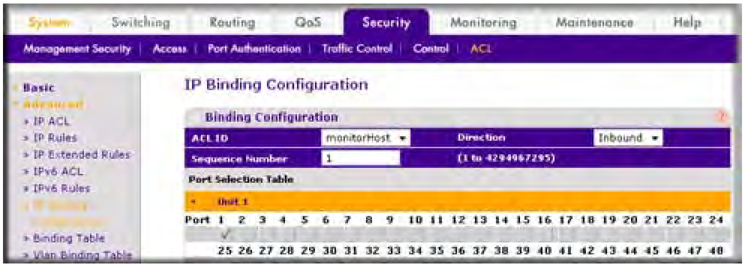
Extended ACL Rule Table

□	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				

Figure 11-55

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

   a. From the main menu, 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

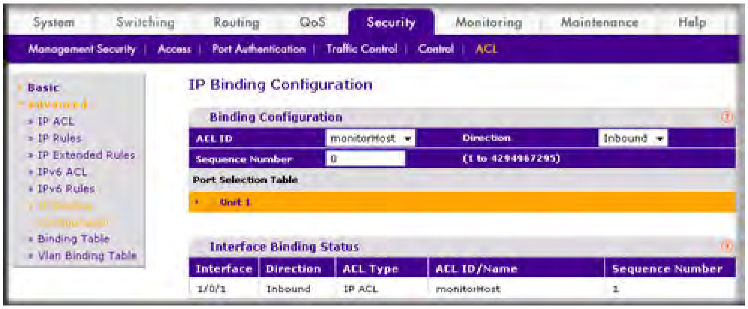
Figure 11-56

   b. Enter Sequence Number as **1**.

   c. Click **Unit 1** in the Port Selection Table to display all the ports for the device.

   d. Select the **Port 1** checkbox.

   e. Click **Apply**. At the end of this configuration 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

Figure 11-57

ACL Redirect

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

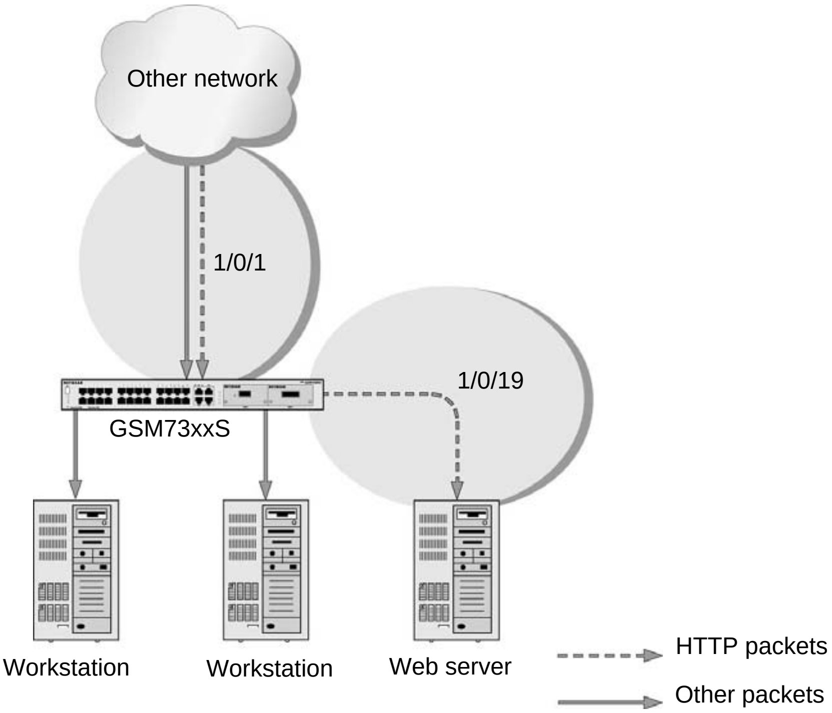


Figure 11-58

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

CLI: Redirecting a Traffic Stream

Create a IP Access Control List with the name redirectHTTP.

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

Define a rule to match the HTTP stream and define a rule to permit every other.

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

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

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

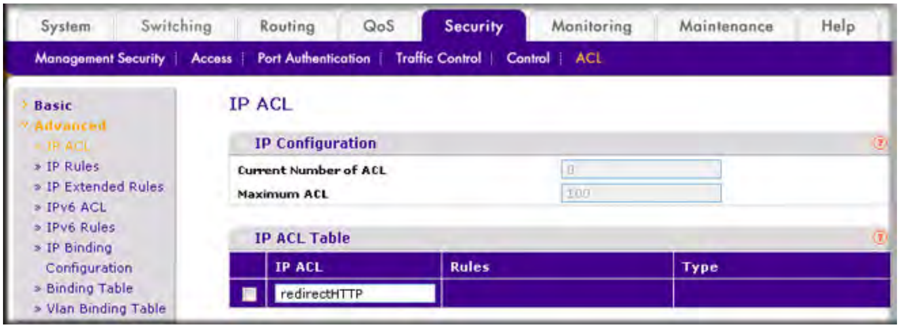
View the configuration.

```
(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: Redirecting

1. Create a IP Access Control List with the name redirectHTTP.

a. From the main menu, 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

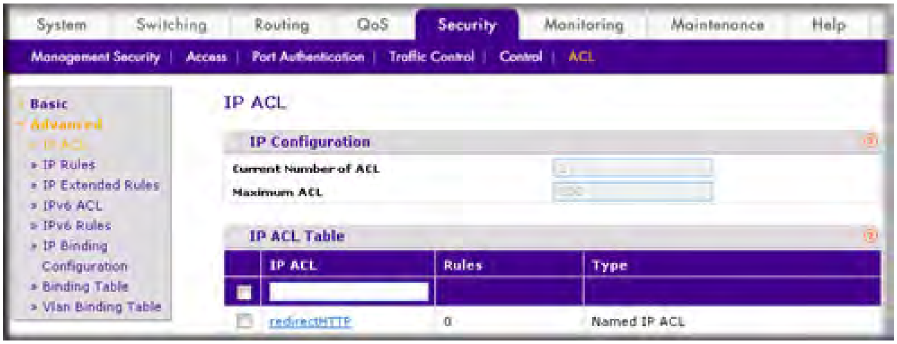
IP ACL Table

	IP ACL	Rules	Type
□	redirectHTTP		

Figure 11-59

b. In the IP ACL filed enter **redirectHTTP**.

c. Click **Add** to create the IP ACL redirectHTTP. At the end of this configuration a screen similar to the following displays.



IP ACL

IP Configuration

Current Number of ACL	1
Maximum ACL	100

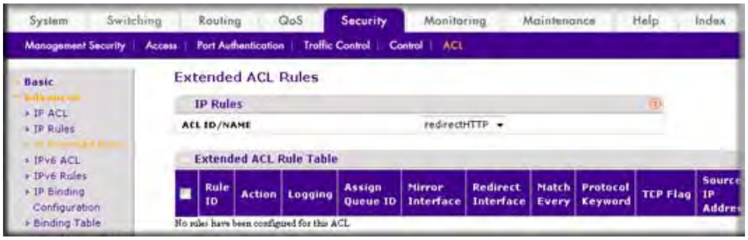
IP ACL Table

	IP ACL	Rules	Type
□			
□	redirectHTTP	0	Named IP ACL

Figure 11-60

2. Create a rule to redirect HTTP traffic.

a. From the main menu, select Security > ACL > Advanced > IP Extended Rules. A screen similar to the following displays.



Extended ACL Rules

IP Rules

ACL ID/NAME: redirectHTTP

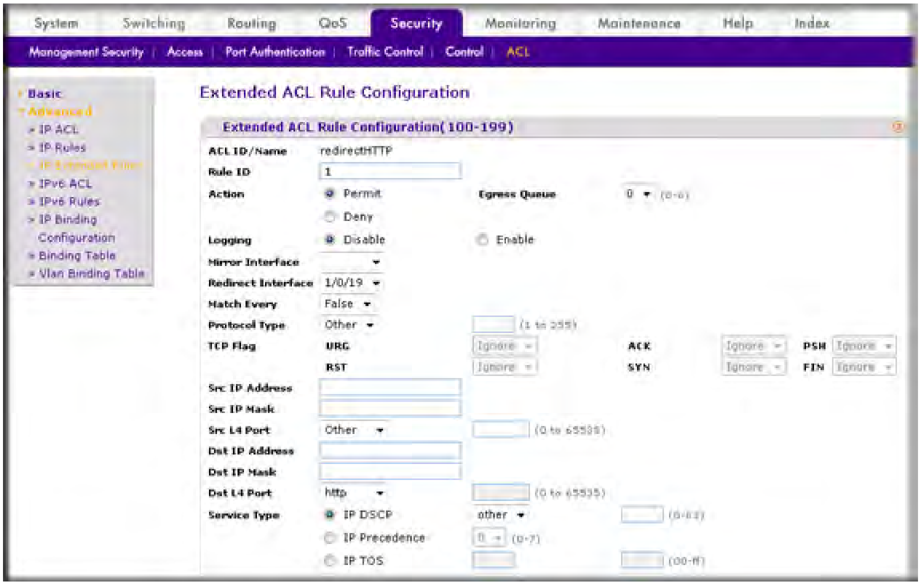
Extended ACL Rule Table

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

No rules have been configured for this ACL

Figure 11-61

b. Click **Add** to take the Extended ACL Rule Configuration screen similar to the following 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)			

Figure 11-62

c. Enter Rule ID as **1**.

d. Selection Action as **Permit**.

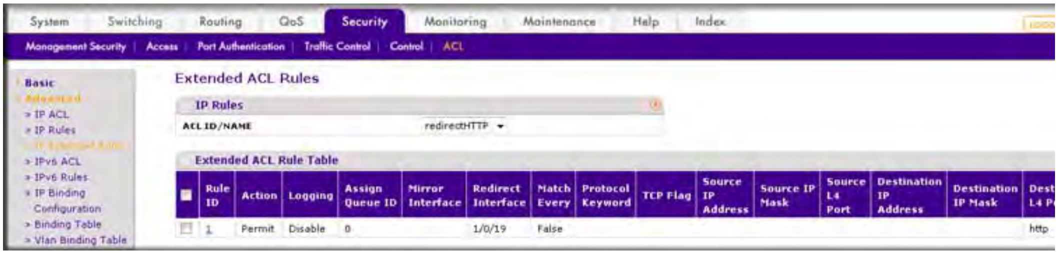
e. Select Redirect Interface as **1/0/19**.

f. Select Dst L4 Port as **http**.

g. Click **Apply**. At the end of this configuration a screen similar to the one in Figure 11-63 displays.

3. Create a rule to match every other traffic.

a. From the main menu, select Security > ACL > Advanced > IP Extended Rules. A screen similar to the following displays.



Extended ACL Rules

IP Rules

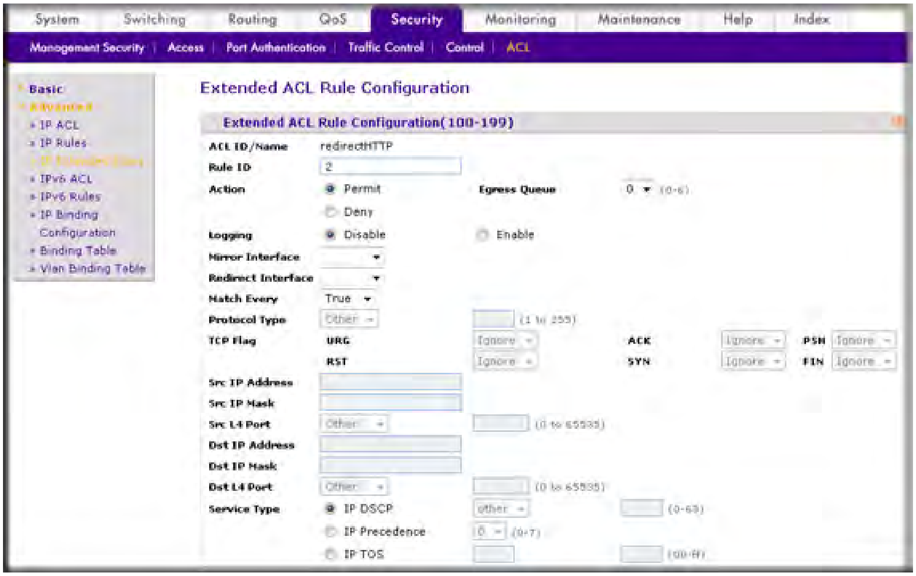
ACL ID/NAME redirectHTTP

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	Dest L4 P
□	1	Permit	Disable	0		1/0/19	False								http

Figure 11-63

b. Click **Add** to take the Extended ACL Rule Configuration screen similar to the following 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)			

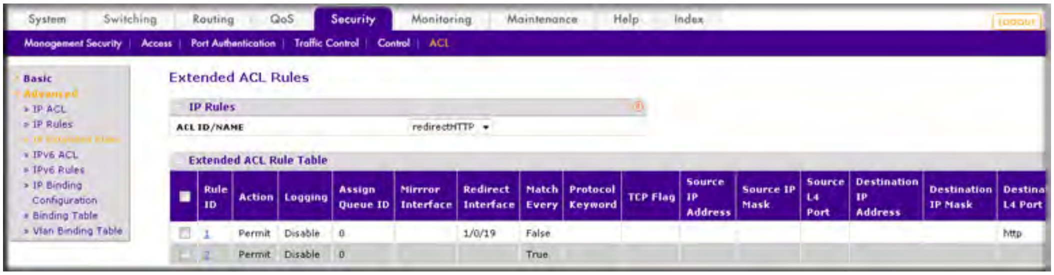
Figure 11-64

c. Enter Rule ID as **2**.

d. Selection Action as **Permit**.

e. Match Every as **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: redirectHTTP

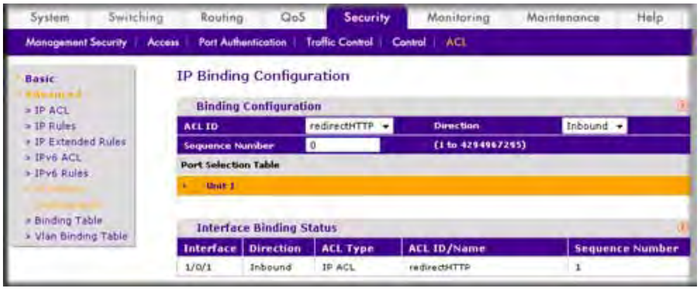
Extended ACL Rule Table

□	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								

Figure 11-65

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

a. From the main menu, 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

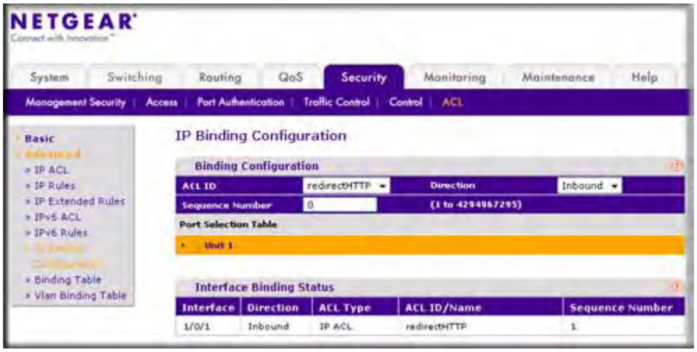
Figure 11-66

b. Enter Sequence Number as **1**.

c. Click **Unit 1** in the Port Selection Table to display all the ports.

d. Click the check box below **Port 1** to select it.

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

Figure 11-67

Configure IPv6 ACLs

This feature extends the existing IPv4 ACL by providing support for IPv6 packet classification. IPv6 ACLs classify for Layer 3 IPv6 traffic. Each ACL is a set of up to twelve 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 may 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 will be denied access.

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

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

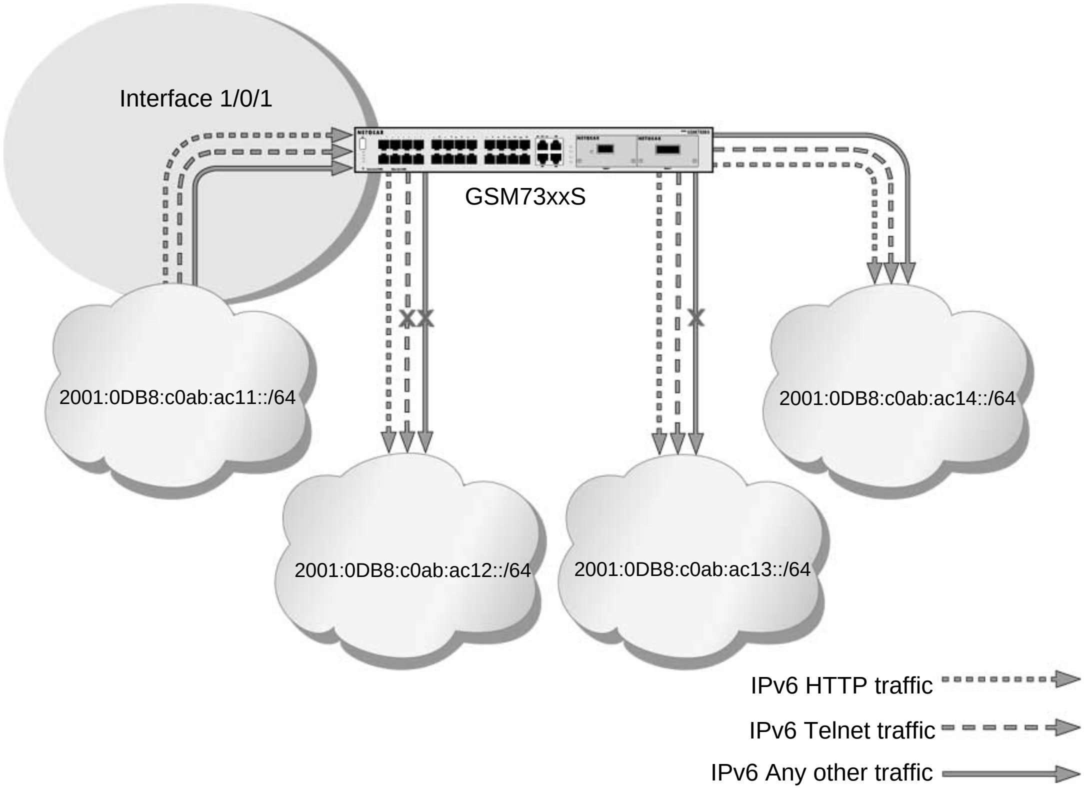


Figure 11-68

CLI: Configuring an IPv6 ACL

Create the Access Control List with the name ipv6-acl.

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

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
```

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

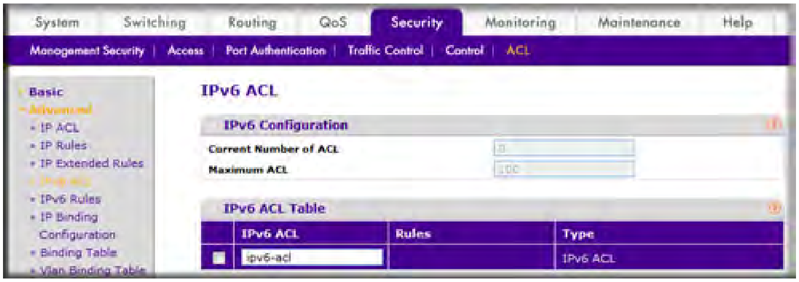
```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ipv6 traffic-filter ipv6-acl in
(Netgear Switch) (Interface 1/0/1)# exit
(Netgear Switch) (Config)#exit
```

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: Configuring an IPv6 ACL

1. Create the Access Control List with the name ipv6-acl
   a. From the main menu, select Security > ACL > Advanced > IPv6 ACL.
   b. In the IPv6 ACL table, enter **ipv6-acl** in the IPv6 ACL field. A screen similar to the following displays.



IPv6 ACL

IPv6 Configuration

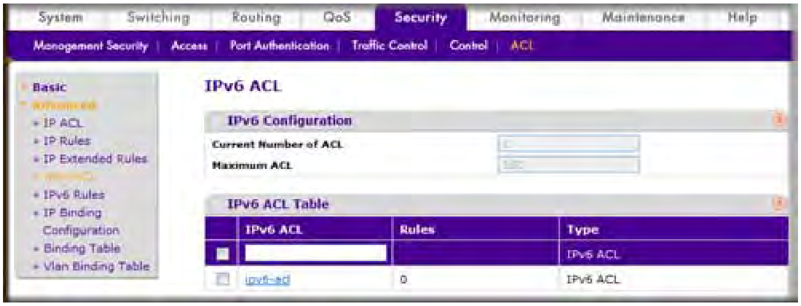
Current Number of ACL	0
Maximum ACL	100

IPv6 ACL Table

	IPv6 ACL	Rules	Type
□	ipv6-acl		IPv6 ACL

Figure 11-69

   c. Click **Add**. At the end of this configuration a screen similar to the following displays.



IPv6 ACL

IPv6 Configuration

Current Number of ACL	[illegible]
Maximum ACL	100

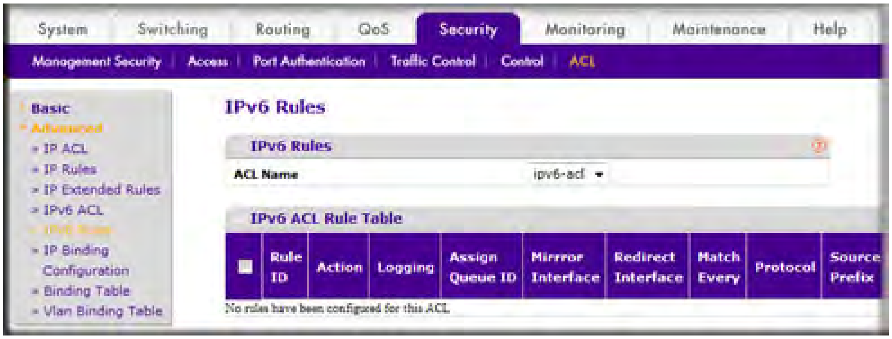
IPv6 ACL Table

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

Figure 11-70

2. Define the first rule (1 of 3).

a. From the main menu, 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.

Figure 11-71

b. Select the ACL Name as **ipv6-acl**.

c. Click **Add**.

d. Enter Rule ID as **1**.

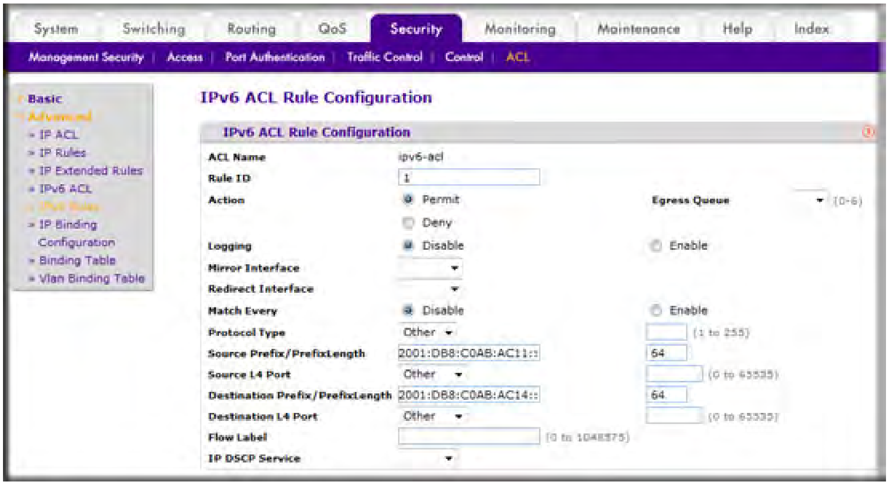
e. Select Action as **Permit**.

f. Enter Source Prefix as **2001:DB8:C0AB:AC11::**.

g. Enter Source Prefix Length as **64**.

h. Enter Destination Prefix as **2001:DB8:C0AB:AC14::**.

i. Enter Destination Prefix Length as **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			

Figure 11-72

j. Click **Apply**.

3. Add Rule 2.

a. Enter Rule ID as **2**.

b. Select Action as **Permit**.

c. Select Protocol Type as **TCP**.

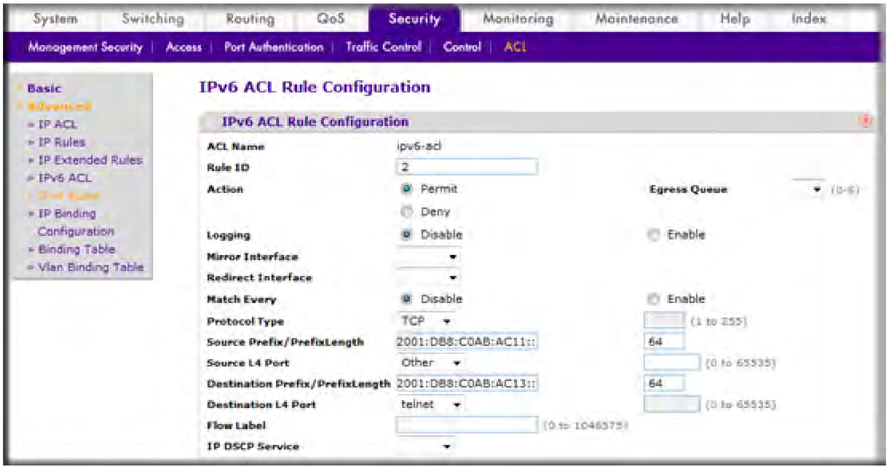
d. Enter Source Prefix as **2001:DB8:C0AB:AC11::**.

e. Enter Source Prefix Length as **64**.

f. Enter Destination Prefix as **2001:DB8:C0AB:AC13::**.

g. Enter Destination Prefix Length as **64**.

h. Select Destination L4 Port as **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			

Figure 11-73

i. Click **Apply**.

4. Add Rule 3.

a. Enter the Rule ID as **3**.

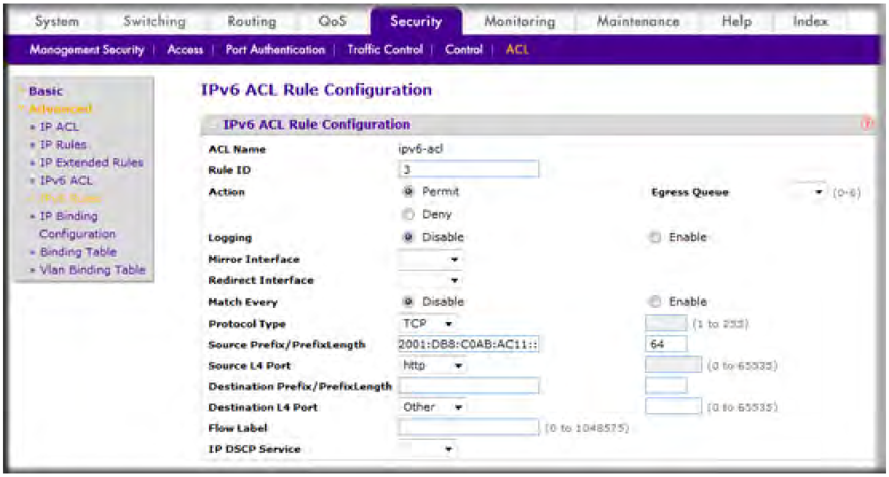
b. Select Action as **Permit**.

c. Select Protocol Type as **TCP**.

d. Enter Source Prefix as **2001:DB8:C0AB:AC11::**.

e. Enter Source Prefix Length as **64**.

f. Select Source L4 Port as **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			

Figure 11-74

g. Click **Apply**.

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

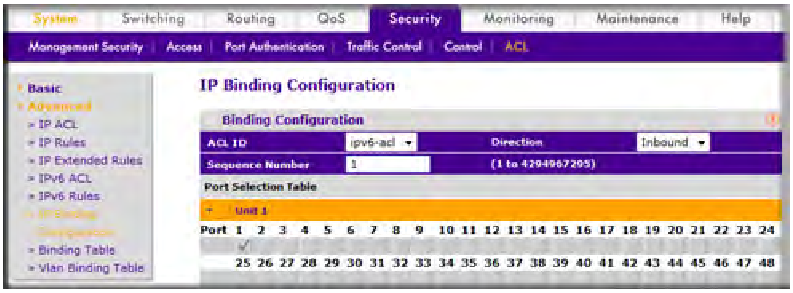
a. From the main menu, select Security > ACL > Advanced > IP Binding Configuration.

b. For the ACL ID, select **ipv6-acl**.

c. In the Sequence Number field, 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)	

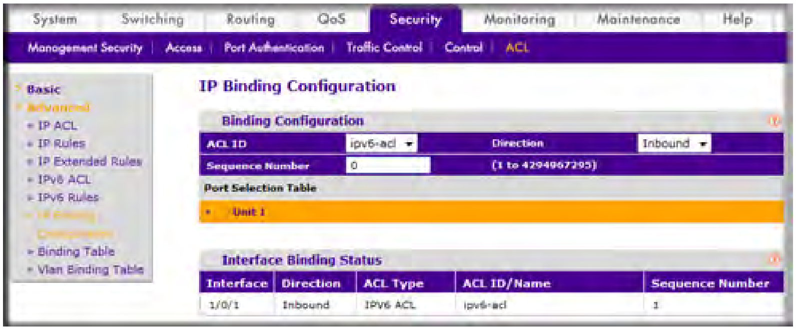
Port Selection Table

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

Figure 11-75

f. Click **Apply**. At the end of this configuration 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

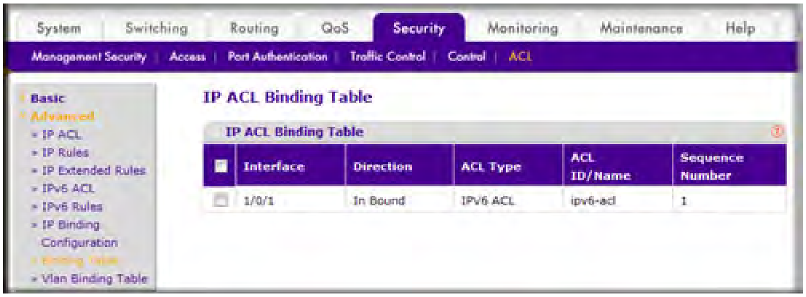
Interface Binding Status

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

Figure 11-76

6. View the binding table.

From the main menu, 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

Figure 11-77

Chapter 12
Class of Service (CoS) Queuing

This section describes the Class of Service (CoS) Queue Mapping and Traffic Shaping features. In this chapter, the following examples are provided:

- "Show classofservice Trust" on page 12-3
- "Set classofservice trust Mode" on page 12-3
- "Show classofservice ip-precedence Mapping" on page 12-5
- "Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode" on page 12-6
- "Set CoS Trust Mode of an Interface" on page 12-8
- "Configure Traffic Shaping" on page 12-9

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

Based on service rate and other criteria you configure, queues provide preference to specified packets. If a delay becomes 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 times of queue congestion.

Select per interface configuration scheme:

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

- System takes at face value certain priority designation for arriving packets.
- Trust applies only to packets that have that trust information.

- Can only have one trust field at a time - per port.
  - 802.1p User Priority (default trust mode - Managed through Switching configuration)
  - IP Precedence
  - IP DiffServ Code Point (DSCP)

The system can assign 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% of available bandwidth
- Queue 1 - Minimum of 33% of available bandwidth
- Queue 0 - Lowest priority, minimum of 17% of available bandwidth

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

Untrusted Ports

- No incoming packet priority designation is trusted, therefore the port default priority value 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 assign queue attribute.
- Used when trusted port mapping is unable to be honored - i.e. 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 the user to create the desired service characteristics for different types of traffic.

Port Egress Queue Configuration

- Scheduler Type, Strict vs. Weighted
- Minimum guaranteed bandwidth
- Maximum allowed bandwidth per queue shaping
- Queue management type, Tail drop vs. WRED

Drop Precedence Configuration (per Queue)

- WRED parameters
  - Minimum threshold
  - Maximum threshold
  - Drop probability
  - Scale factor

- Tail Drop parameters, Threshold

Per-Interface Basis

- Queue management type, Tail Drop vs. WRED

Only if per queue config is not supported

- WRED Decay Exponent
- Traffic Shaping for an entire interface

Show classofservice Trust

CLI: Showing classofservice trust

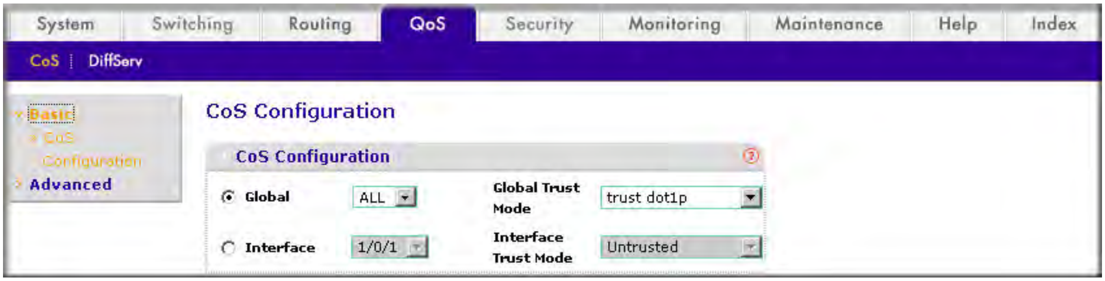
To use the CLI to show CoS trust mode, use these commands.

```
(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: Showing classofservice Trust

To use the Web interface to show CoS trust mode, proceed as follows:

From the main menu, select QoS > 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

Figure 12-1

Set classofservice trust Mode

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

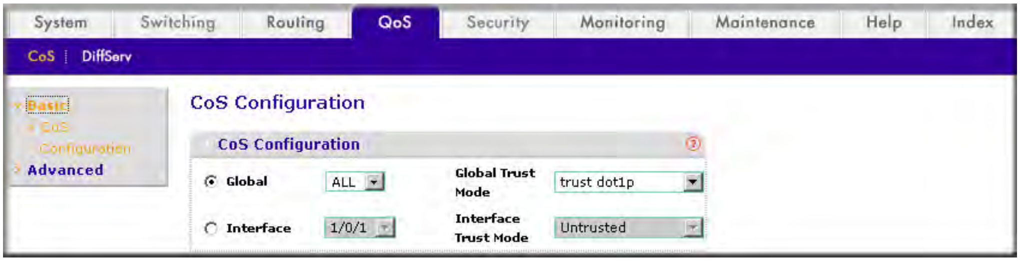
CLI: Setting classofservice Trust Mode

```
(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: Setting classofservice Trust Mode

To use the Web interface to show CoS trust mode, proceed as follows:

1. From the main menu, select QoS > 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

Figure 12-2

2. Select the **Global** radio button.
3. Select the **trust dot1p** in the Global Trust Mode field.
4. Click the **Apply** to save the settings.

Show classofservice ip-precedence Mapping

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

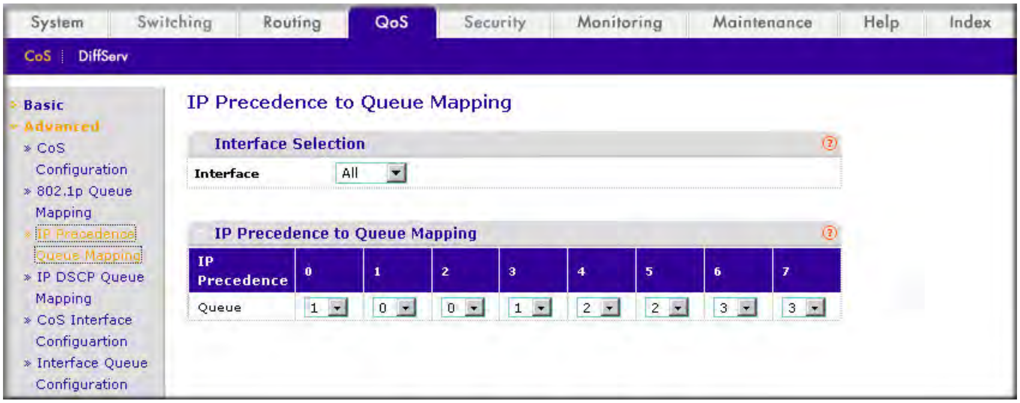
CLI: Showing classofservice ip-precedence Mapping

```
(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: Showing classofservice ip-precedence Mapping

To use the Web interface to show CoS trust mode, proceed as follows:

1. From the main menu, select QoS > 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

Figure 12-3

2. Select the **All** in the Interface field.
3. The global IP precedence to Queue mapping is displayed.
4. Select the specific interface(e.g. 1/0/1) in the Interface field.

5. 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: Configuring Cos-queue Min-bandwidth and Strict Priority Scheduler Mode

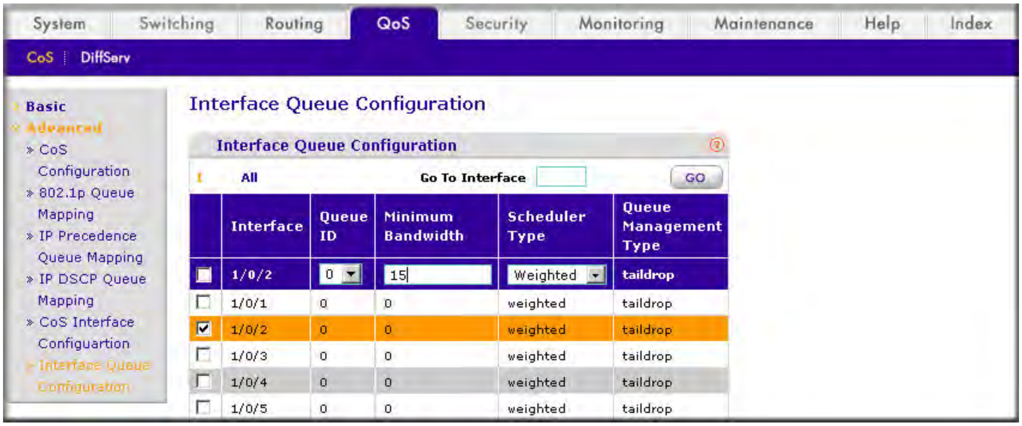
```
(Netgear Switch) (Config)#cos-queue min-bandwidth?

<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: Configuring CoS-queue Min-bandwidth and Strict Priority Scheduler Mode

To use the Web interface to configure CoS queue, proceed as follows:

1. Set min bandwidth 15 to the queue 0 of the interface 1/0/2.

a. From the main menu, select QoS > 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
□	1/0/2	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

Figure 12-4

b. Select the **0** in the Queue ID field.

c. Under Interface Queue Configuration, scroll down to interface **1/0/2** and select the checkbox for 1/0/1. 1/0/2 now appears in the Interface field at the top.

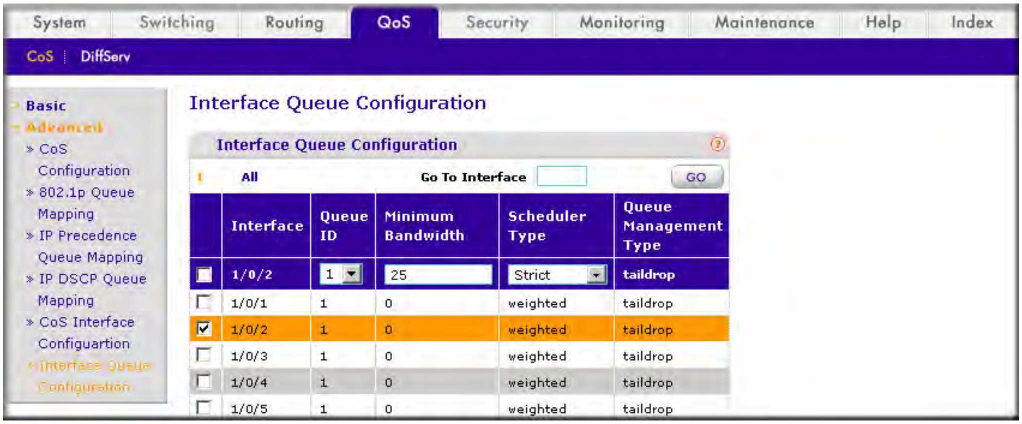
d. Enter the following information in the Interface Queue Configuration.

- In the Minimum Bandwidth, enter **15**.
- Select the **Weighted** in the Scheduler Type field.

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

2. Set min bandwidth 25 to the queue 1 of the interface 1/0/2 and set the scheduler type to strict.

a. From the main menu, select QoS > 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
□	1/0/2	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

Figure 12-5

b. Select the **1** in the Queue ID field.

c. Under Interface Queue Configuration, scroll down to interface **1/0/2** and select the checkbox for 1/0/2. 1/0/2 now appears in the Interface field at the top.

d. Enter the following information in the Interface Queue Configuration.

- In the Minimum Bandwidth, enter **25**.
- Select the **Strict** in the Scheduler Type field.

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

Set CoS Trust Mode of an Interface

CLI: Setting CoS Trust Mode of an Interface

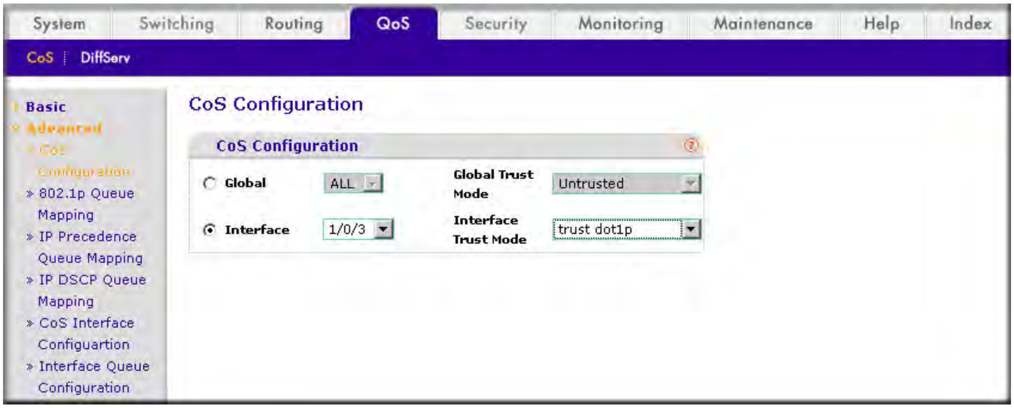
```
(Netgear Switch) (Interface 1/0/3)#classofservice trust?

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 is therefore not configurable by the user.

Web Interface: Setting CoS Trust Mode of an Interface

To use the Web interface to set CoS trust mode of an interface, set Cos Trust Mode to dot1p of the interface 1/0/3:

1. From the main menu, select QoS > 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

Figure 12-6

2. Under CoS Configuration, Select the **Interface** radio button.
3. Select **1/0/3** in the interface field.
4. Select **trust dot1p** in the Interface Trust Mode field.
5. Click the **Apply** to save the settings.

Configure Traffic Shaping

This section describes the Traffic Shaping feature.

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 value(s) 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: Configuring traffic-shape

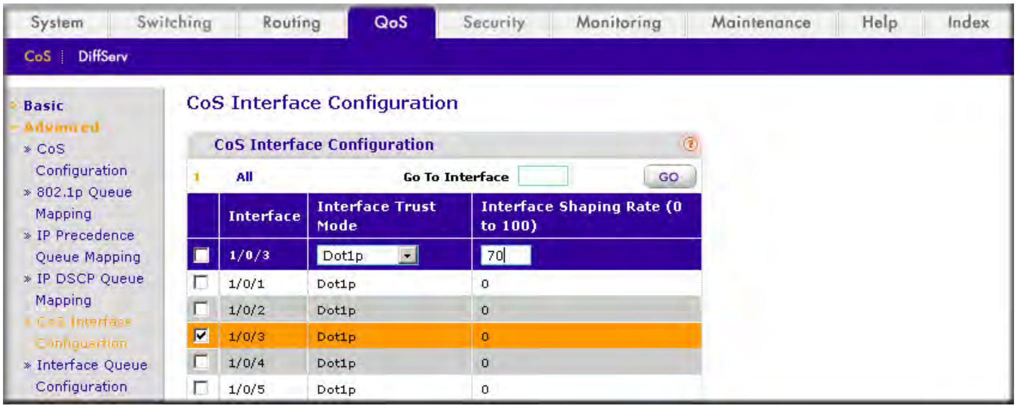
```
(Netgear Switch) (Config)#traffic-shape?

<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: Configuring Traffic-shape

To use the Web interface to configure traffic-shape, proceed as follows:

1. Set the shaping bandwidth percentage to 70%.

a. From the main menu, select QoS > Advanced >CoS Interface Configuration. A screen similar to the following displays.



CoS Interface Configuration

CoS Interface Configuration

1 All Go To Interface

	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

Figure 12-7

b. Under CoS Interface Configuration, scroll down to interface **1/0/3** and select the 1/0/3 checkbox. 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 the **Apply** to save the settings.

Chapter 13
Differentiated Services

In this chapter, the following examples are provided:

- "Differentiated Services" on page 13-2
- "DiffServ for VoIP Configuration" on page 13-20
- "Auto VoIP Configuration" on page 13-29
- "DiffServ for IPv6 Configuration Example" on page 13-33

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

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

- **Edge device.** An edge device handles ingress traffic, flowing towards 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 primarily based on the contents of the Layer 3 and Layer 4 headers, and is recorded in the Differentiated Services Code Point (DSCP) added to a packet's IP header.
- **Interior node.** A switch in the core of the network is responsible for forwarding packets, rather than for classifying them. It decodes the DSCP code point in an incoming packet, and provides buffering and forwarding services using the appropriate queue management algorithms.

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

Rules are defined in terms of classes, policies and services:

- **Class.** A class consists of a set of rules that identify which packets belong to the class. Inbound traffic is separated into traffic classes based on Layer 3 and 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

Differentiated Services

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% of the available bandwidth on the port accessing the Internet.

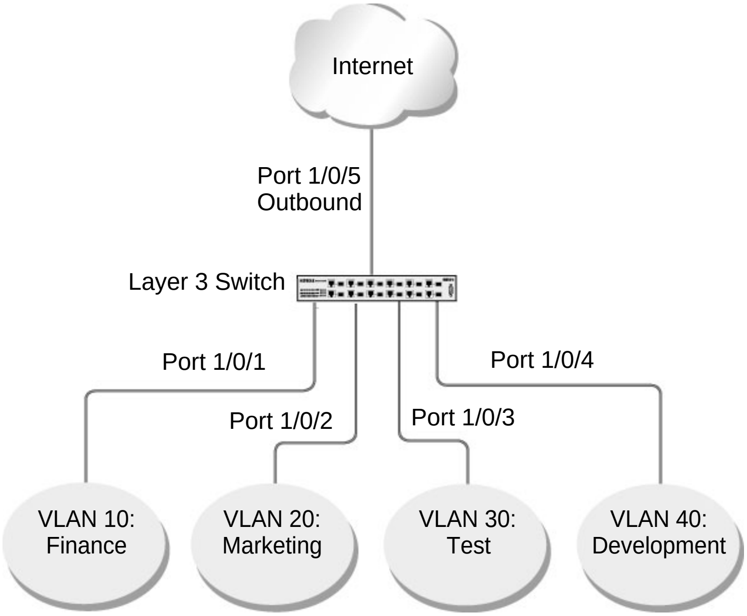


Figure 13-1

CLI: DiffServ

The following example configures DiffServ on a 7000 Series Managed Switch:

Ensure DiffServ operation is enabled for the switch.

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

Create a DiffServ class of type “all” for each of the departments, and name them. Define the match criteria -- 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
```

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 below.

```
(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
```

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
```

Set the CoS queue configuration for the (presumed) egress interface 1/0/5 such that each of queues 1, 2, 3 and 4 get a minimum guaranteed bandwidth of 25%. 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.

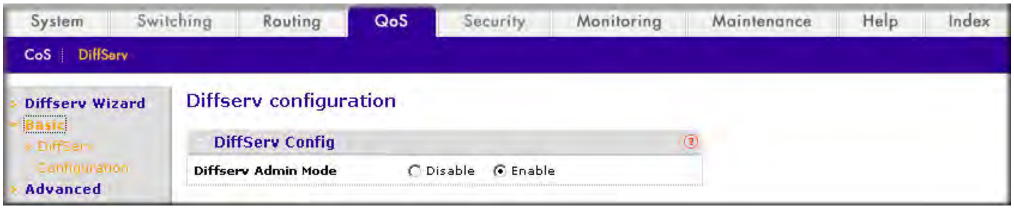
```
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#cos-queue min-bandwidth 0 25 25 25 25 0 0 0
(Netgear Switch) (Interface 1/0/5)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: DiffServ

To use the Web interface to configure diffserv, proceed as follows:

1. Enable Diffserv.

a. From the main menu, select QoS > DiffServ >Basic >DiffServ Configuration. A screen similar to the following displays.



Diffserv configuration

DiffServ Config

Diffserv Admin Mode ○ Disable ● Enable

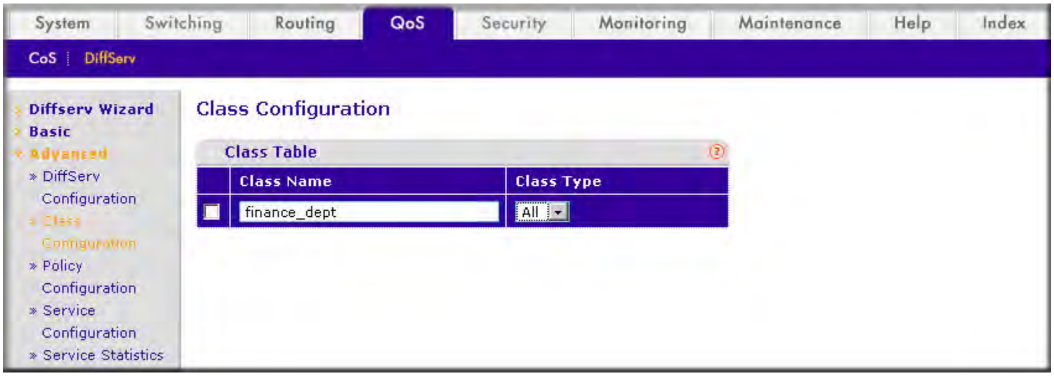
Figure 13-2

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

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

2. Create class finance_dept.

a. From the main menu, select QoS > DiffServ >Advanced >Class Configuration. A screen similar to the following displays.



Class Configuration

Class Table

	Class Name	Class Type
□	finance_dept	All

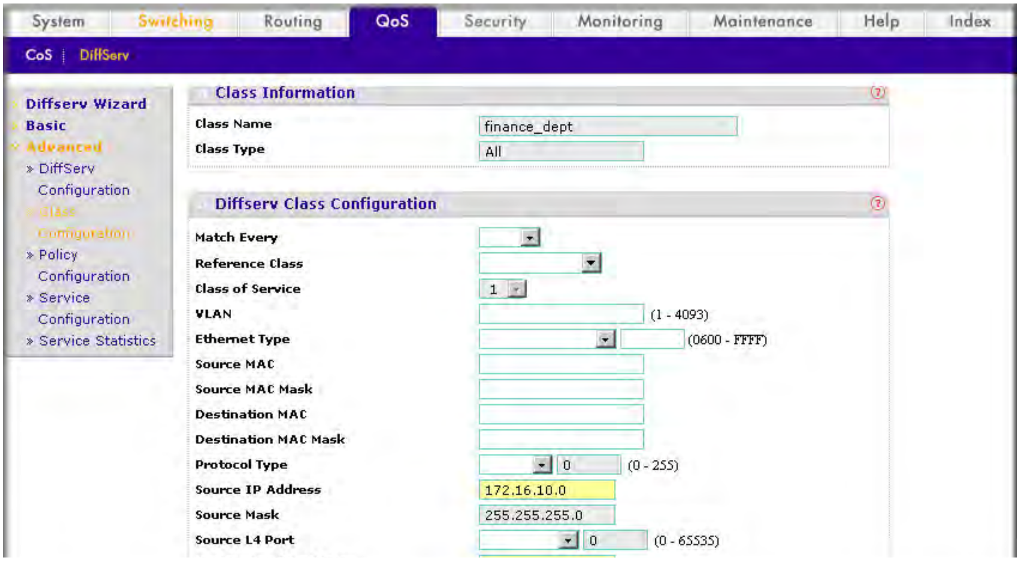
Figure 13-3

b. Enter the following information in the Class Configuration

- In the Class Name field, enter **finance_dept**.
- Select the **All** in the Class Type field.

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)

Figure 13-4

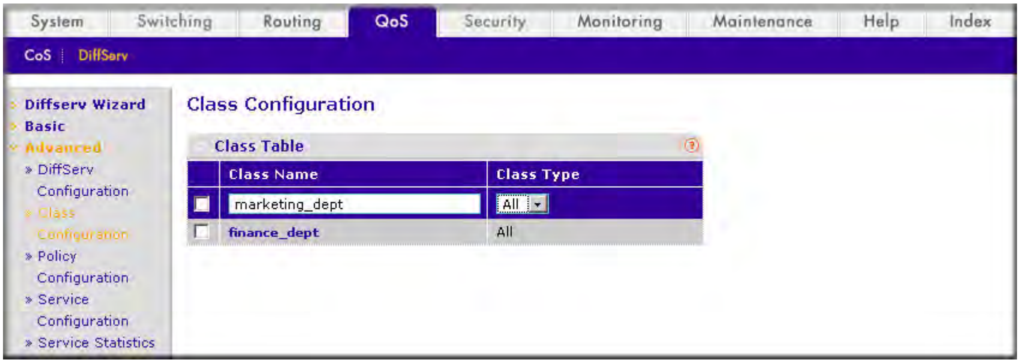
e. Under the Diffserv Class Configuration page, enter the following information:

- 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 class marketing_dept

a. From the main menu, select QoS > DiffServ >Advanced >Class Configuration. A screen similar to the following displays.



Class Configuration

Class Table

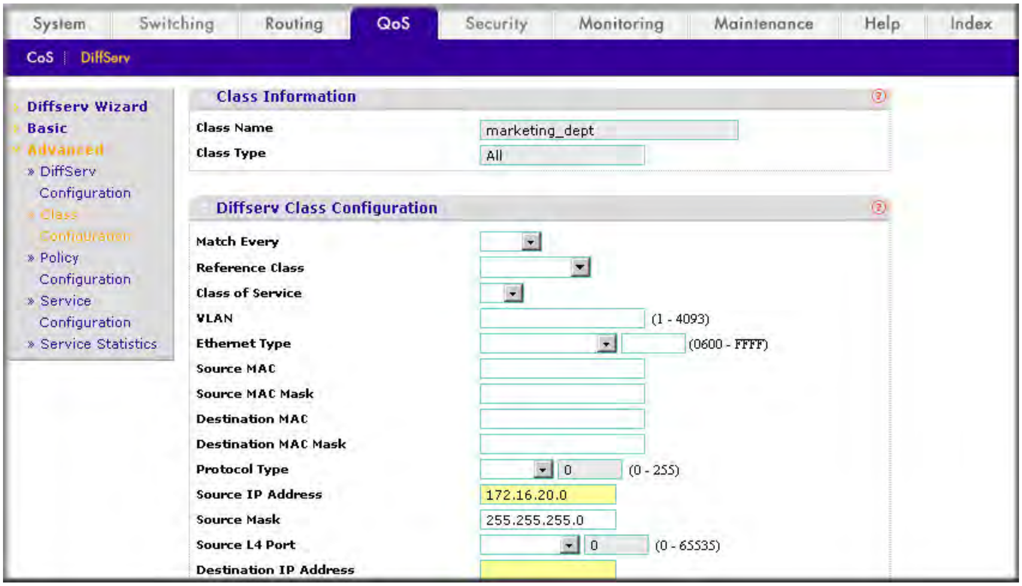
	Class Name	Class Type
□	marketing_dept	All
□	finance_dept	All

Figure 13-5

b. Enter the following information in the Class Configuration
   - In the Class Name field, enter **marketing_dept**.
   - Select **All** in the Class Type field.

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

d. Click the 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	

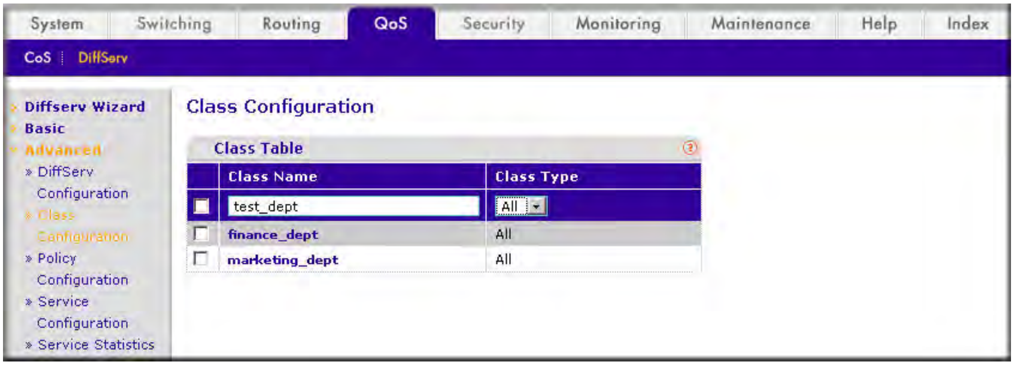
Figure 13-6

e. On the Diffserv Class Configuration page, 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 class test_dept.

a. From the main menu, 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

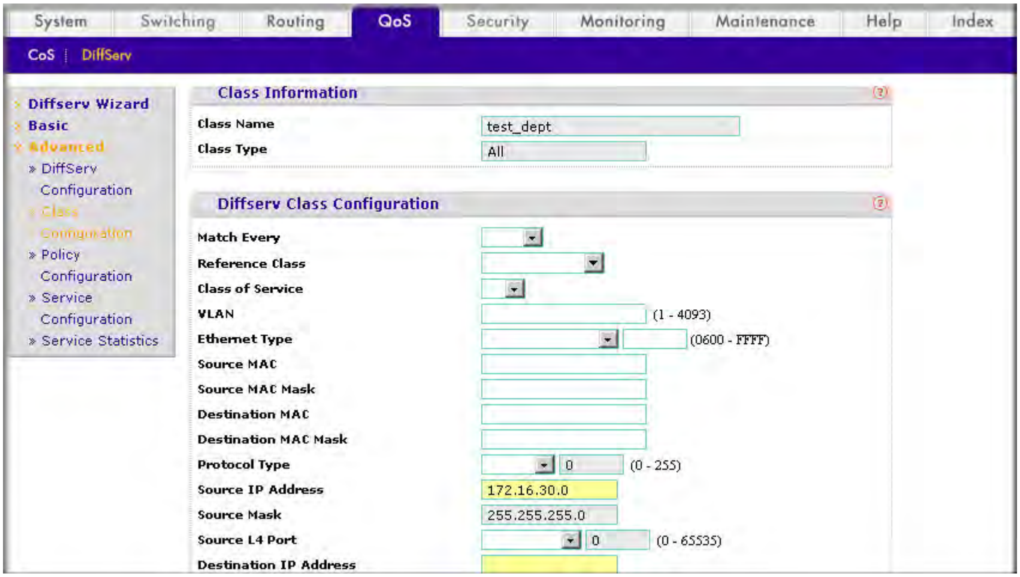
Figure 13-7

b. Enter the following information in the Class Configuration

- In the Class Name field, enter **test_dept**.
- Select **All** in the Class Type field.

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

d. Click the 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		

Figure 13-8

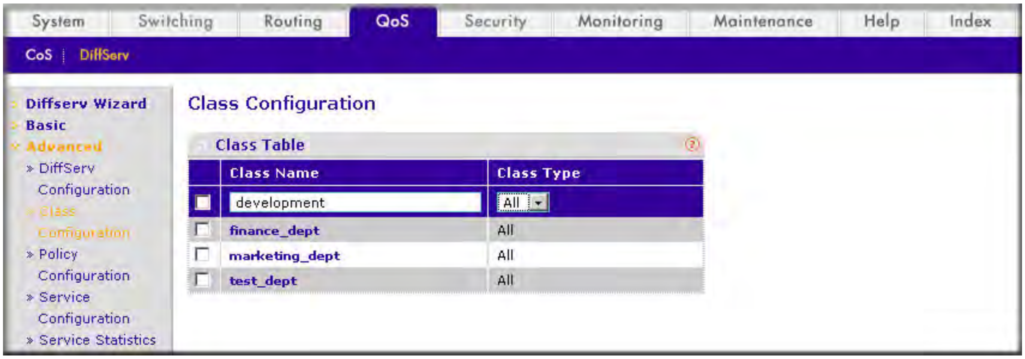
e. Under the Diffserv Class Configuration page, enter the following information:

- 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. From the main menu, 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

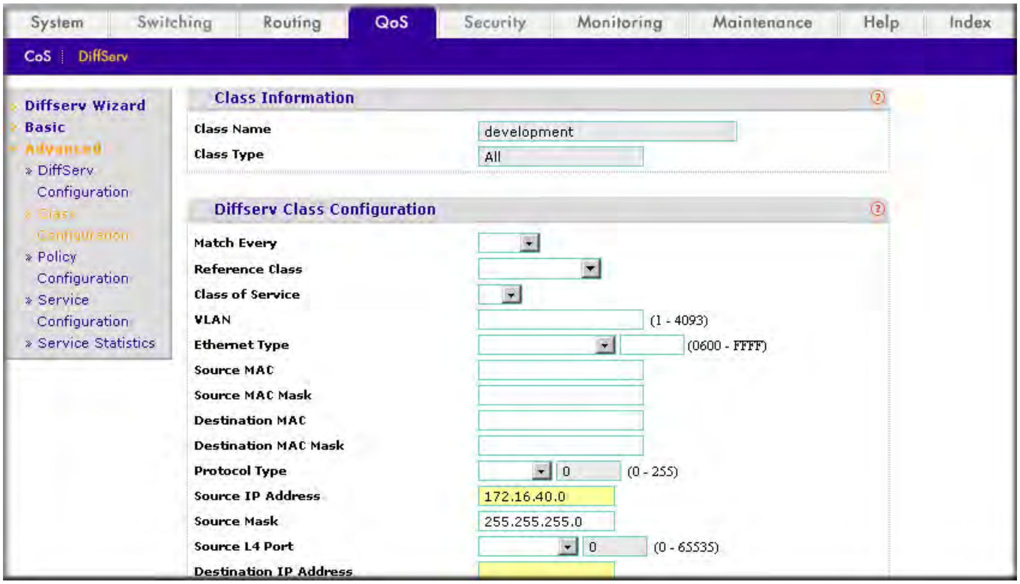
Figure 13-9

b. Enter the following information in the Class Configuration

- In the Class Name field, enter **development_dept**.
- Select the **All** in the Class Type field.

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

d. Click the 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		

Figure 13-10

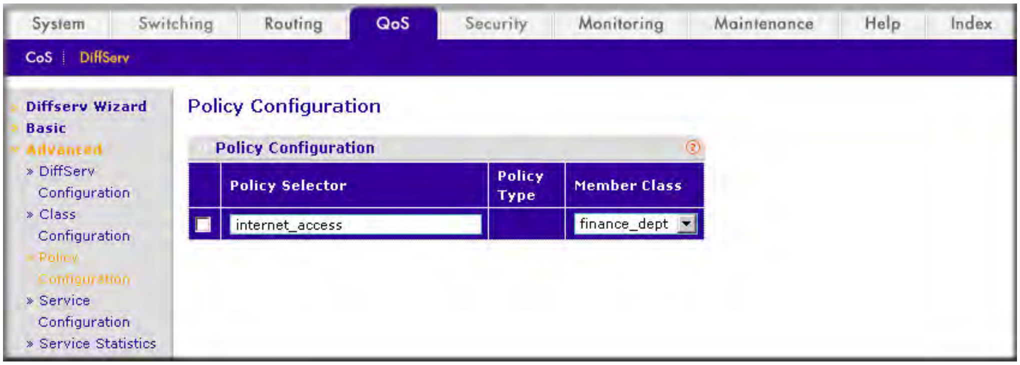
e. Under the Diffserv Class Configuration page, enter the following information:

- 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 into it.

a. From the main menu, 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

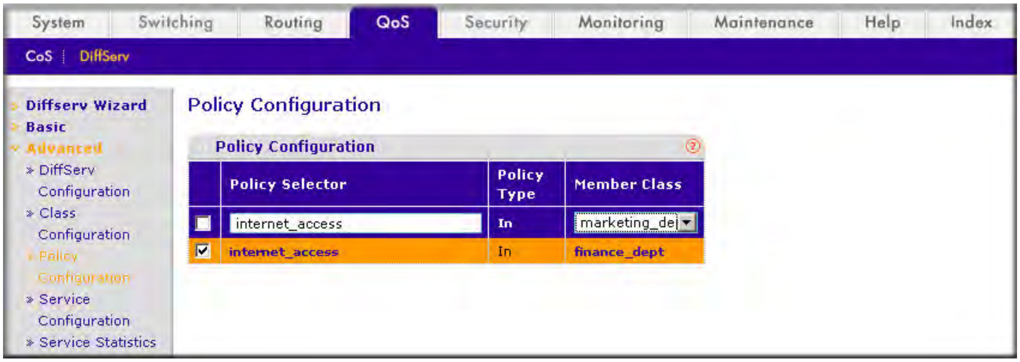
Figure 13-11

b. Enter the following information in the Class Configuration
   - In the Policy Selector field, enter **internet_access**.
   - Select the **finance_dept** in the Member Class field.

c. Click the **Add** to create a new policy internet_access.

7. Add the class marketing_dept into the policy internet_access.

   a. From the main menu, 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

Figure 13-12

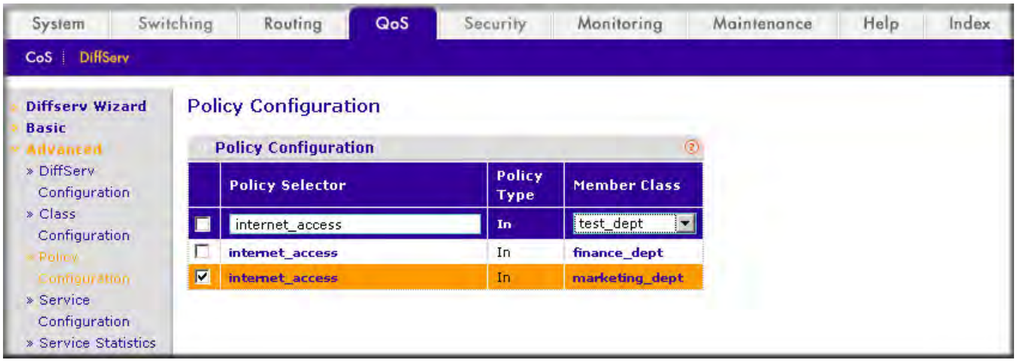
   b. Under Policy Configuration, scroll down to **internet_access** and select the checkbox for internet_access. Internet_access now appears in the Policy Selector field at the top.

   c. Select the marketing_dept in the Member Class field.

   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. From the main menu, 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

Figure 13-13

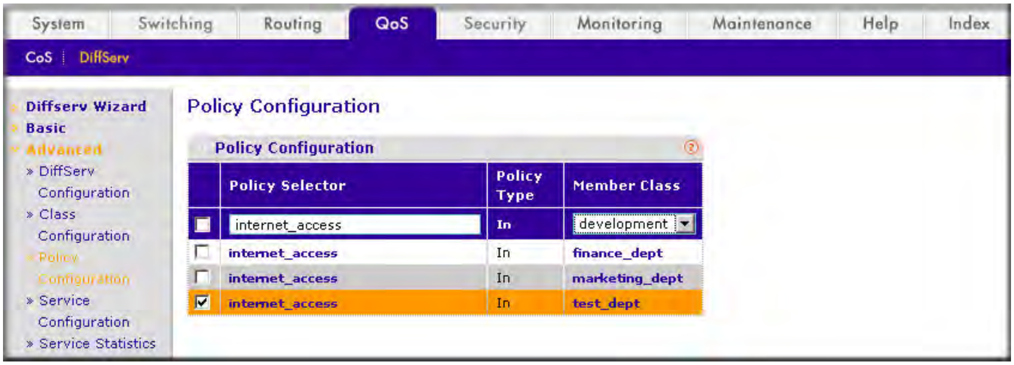
b. Under Policy Configuration, scroll down to **internet_access** and select the checkbox for internet_access. Internet_access now appears in the Policy Selector field at the top.

c. Select the test_dept in the Member Class field.

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. From the main menu, 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

Figure 13-14

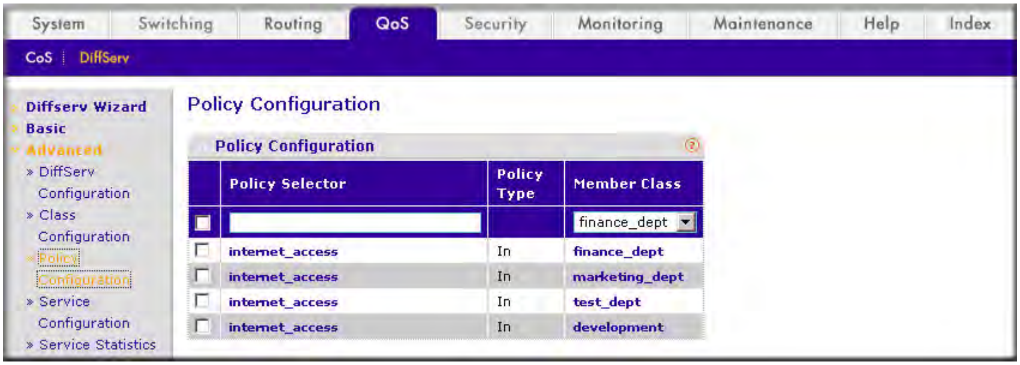
b. Under Policy Configuration, scroll down to **internet_access** and select the checkbox for internet_access. Internet_access now appears in the Policy Selector field at the top.

c. Select the development_dept in the Member Class field.

d. Click **Apply** to add the class development_dept to the policy internet_access.

10. Assign queue 1 to the finance_dept.

a. From the main menu, select QoS > DiffServ > Advanced >Policy Configuration. A screen similar to the following displays.



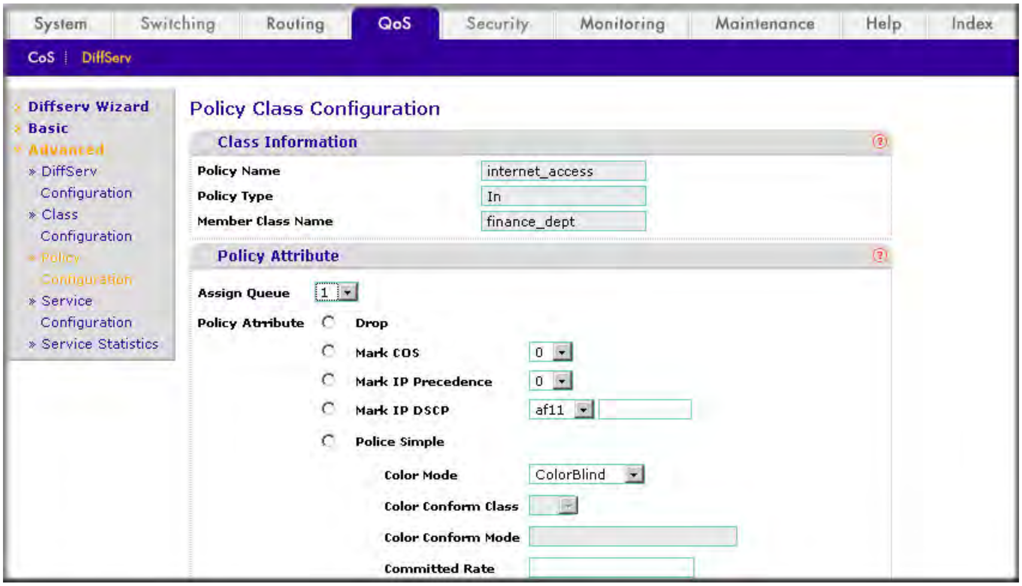
Policy Configuration

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

Figure 13-15

b. Click the internet_access whose member class is finance_dept. another 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:

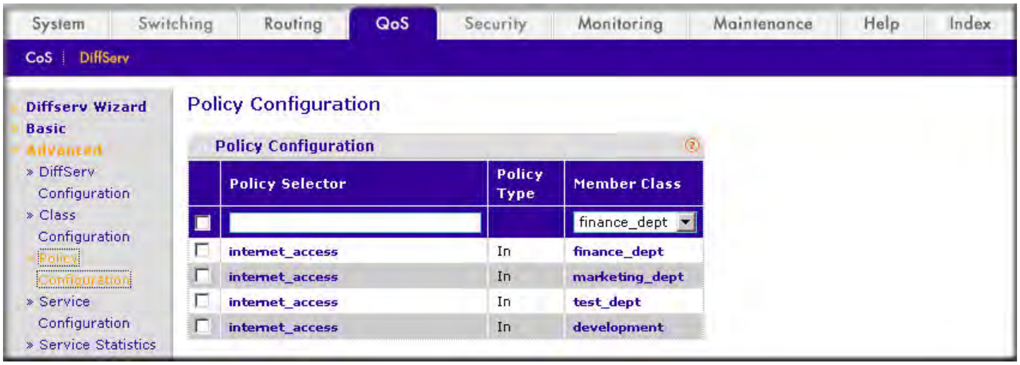
Figure 13-16

c. Select the **1** in the Assign Queue field.

d. Click **Apply**.

11. Assign queue 2 to the marketing_dept.

a. From the main menu, select QoS > DiffServ >Advanced >Policy Configuration. A screen similar to the following displays.



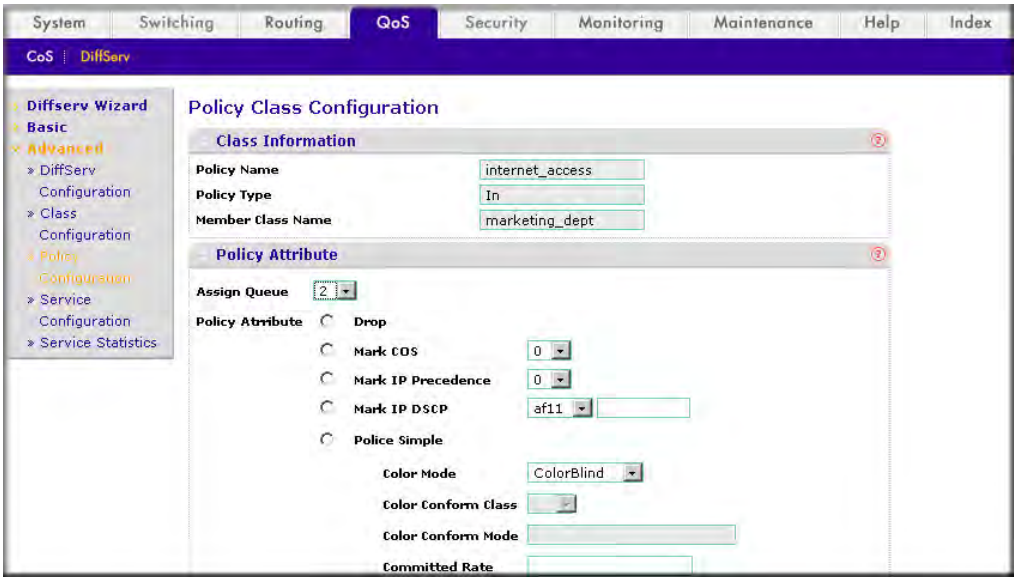
Policy Configuration

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

Figure 13-17

b. Click the internet_access whose member class is marketing_dept. another 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:

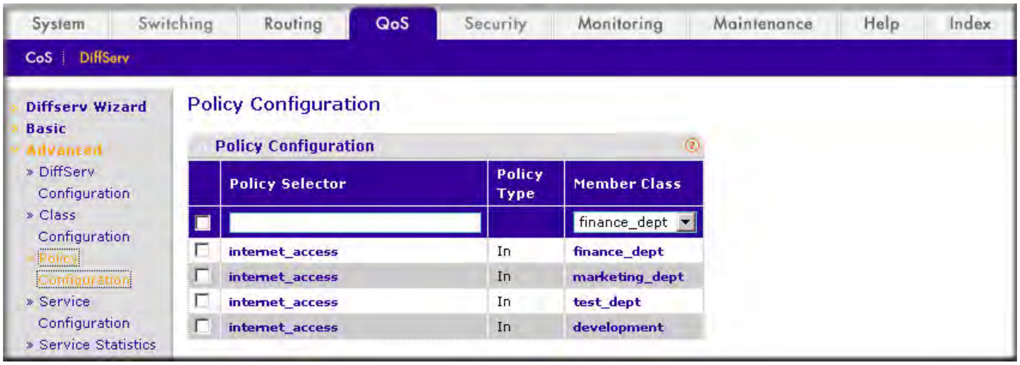
Figure 13-18

c. Select the **2** in the Assign Queue field.

d. Click **Apply**.

12. Assign queue 3 to the test_dept.

a. From the main menu, select QoS > DiffServ > Advanced >Policy Configuration. A screen similar to the following displays.



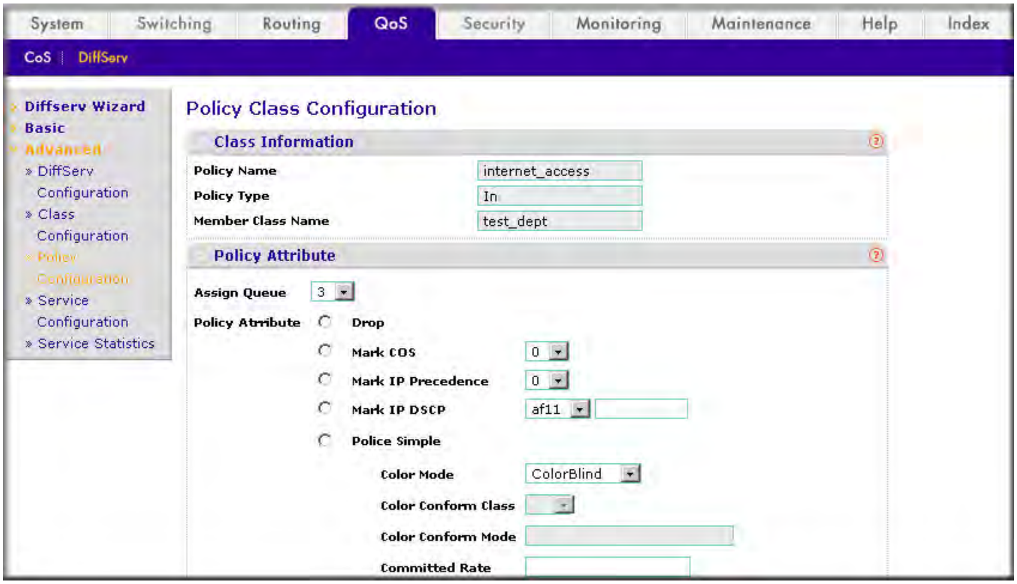
Policy Configuration

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

Figure 13-19

b. Click the internet_access whose member class is test_dept. another 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	

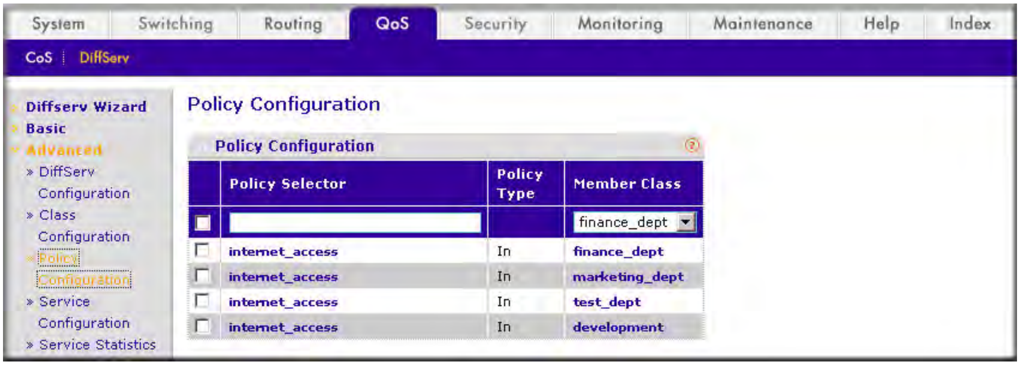
Figure 13-20

c. Select the **3** in the Assign Queue field.

d. Click **Apply**.

13. Assign queue 4 to the development_dept.

a. From the main menu, select QoS > DiffServ >Advanced >Policy Configuration. A screen similar to the following displays.



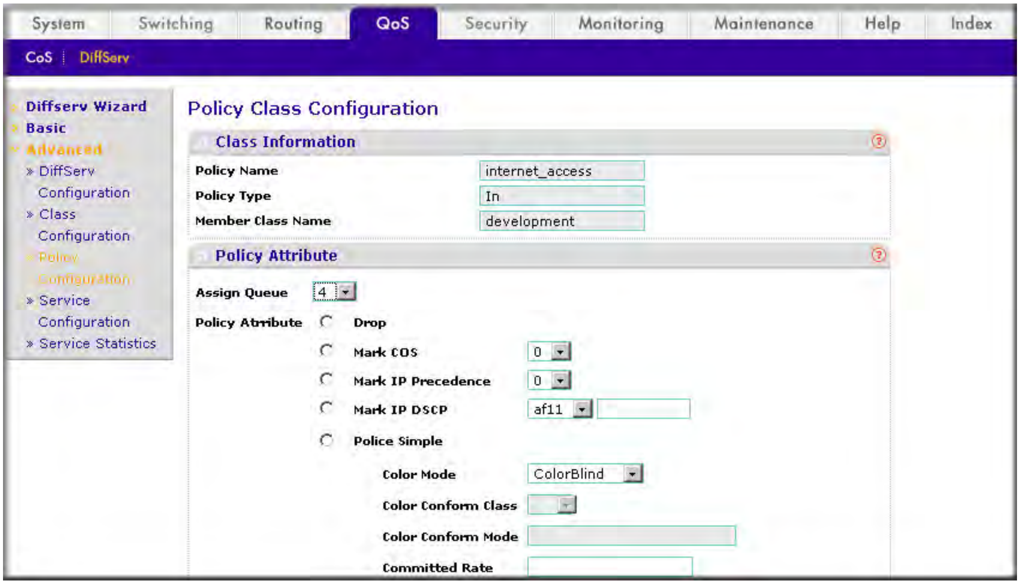
Policy Configuration

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

Figure 13-21

b. Click the internet_access whose member class is development_dept. another 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:

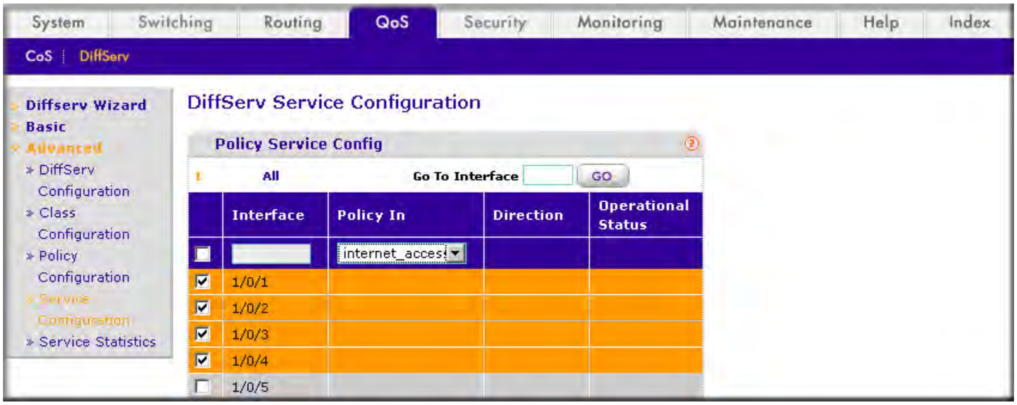
Figure 13-22

c. Select the **4** in the Assign Queue field.

d. Click **Apply**.

14. Attach the defined policy to the interface 1/0/1 through 1/0/4 in the inbound direction

a. From the main menu, select QoS > Advanced >Service Configuration. A screen similar to the following displays.



DiffServ Service Configuration

Policy Service Config

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

Figure 13-23

b. Scroll down to interface **1/0/1** and select the checkbox for 1/0/1.

c. Scroll down to interface **1/0/2** and select the checkbox for 1/0/2.

d. Scroll down to interface **1/0/3** and select the checkbox for 1/0/3.

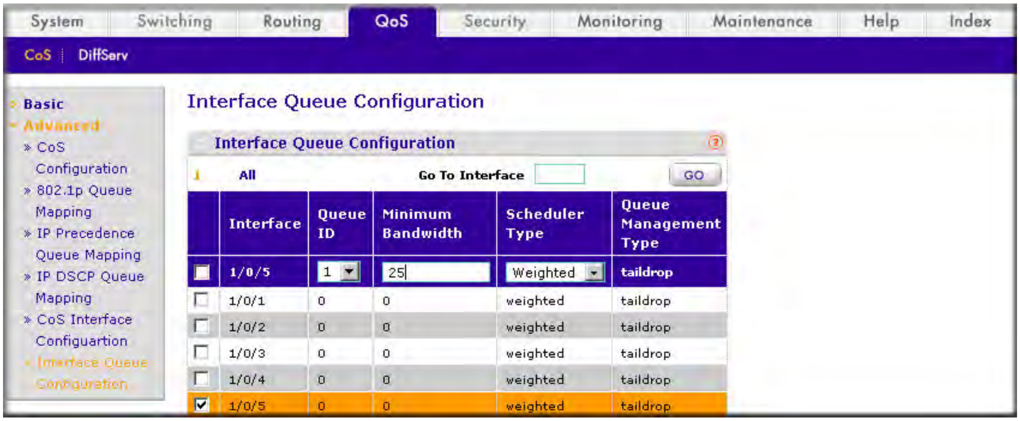
e. Scroll down to interface **1/0/4** and select the checkbox for 1/0/4.

f. Select the **internet_access** in the Policy In field.

g. Click **Apply**.

15. Set the CoS queue 1 configuration for the interface 1/0/5.

a. From the main menu, 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

Figure 13-24

b. Under Interface Queue Configuration, scroll down to interface **1/0/5** and select the checkbox for 1/0/5. 1/0/5 now appears in the Interface field at the top.

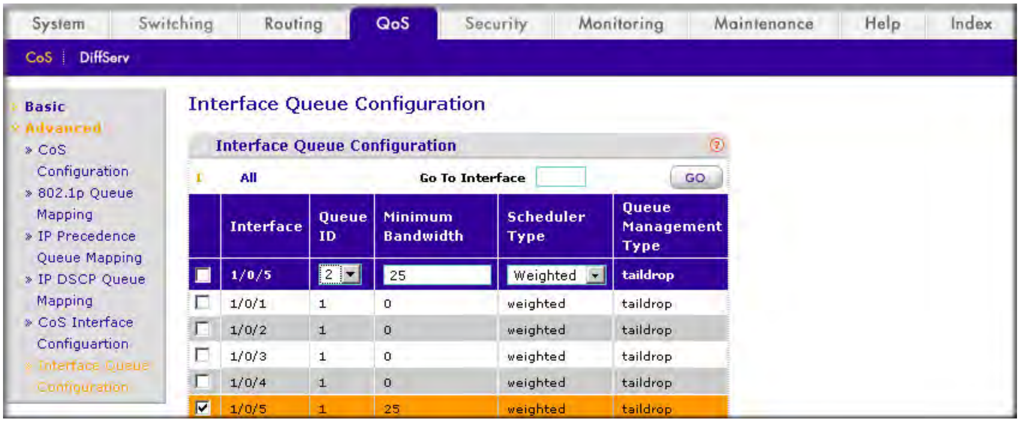
c. Select the **1** in the Queue ID field

d. In the Minimum Bandwidth field, enter **25**.

e. Click **Apply**.

16. Set the CoS queue 2 configuration for the interface 1/0/5

a. From the main menu, 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	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

Figure 13-25

b. Under Interface Queue Configuration, scroll down to interface **1/0/5** and select the checkbox for 1/0/5. Now 1/0/5 appears in the Interface field at the top.

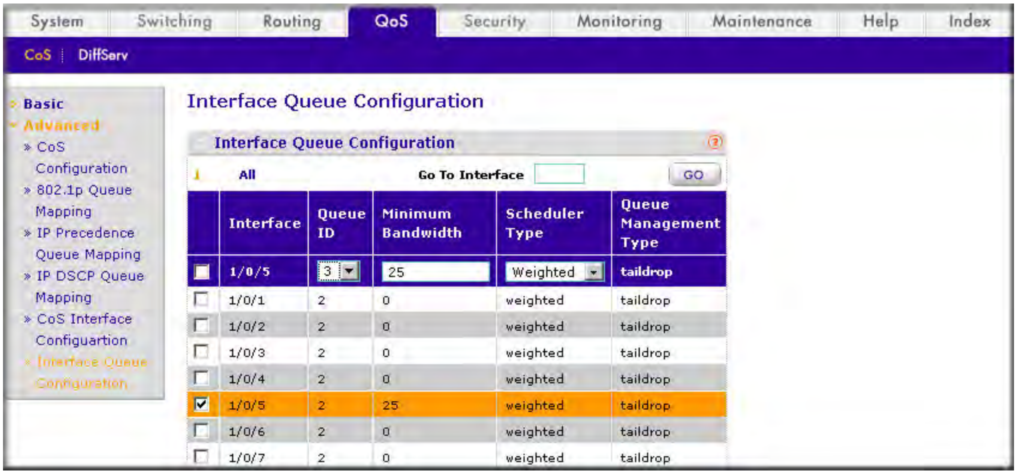
c. Select the **2** in the Queue ID field

d. In the Minimum Bandwidth field, enter **25**.

e. Click **Apply**.

17. Set the CoS queue 3 configuration for the interface 1/0/5.

a. From the main menu, 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

Figure 13-26

b. Under Interface Queue Configuration, scroll down to interface **1/0/5** and select the checkbox for 1/0/5. 1/0/5 now appears in the Interface field at the top.

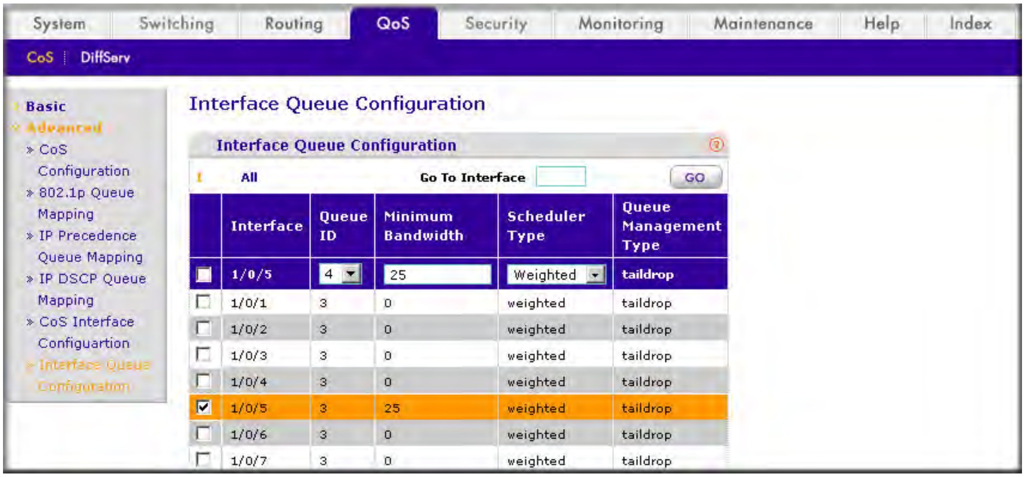
c. Select the **3** in the Queue ID field

d. In the Minimum Bandwidth field, enter **25**.

e. Click **Apply**.

18. Set the CoS queue 4 configuration for the interface 1/0/5.

a. From the main menu, 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	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

Figure 13-27

b. Under Interface Queue Configuration, scroll down to interface **1/0/5** and select the checkbox for 1/0/5. 1/0/5 now appears in the Interface field at the top.

c. Select the **4** in the Queue ID field

d. In the Minimum Bandwidth field, enter **25**.

e. Click **Apply**.

DiffServ for VoIP Configuration

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.

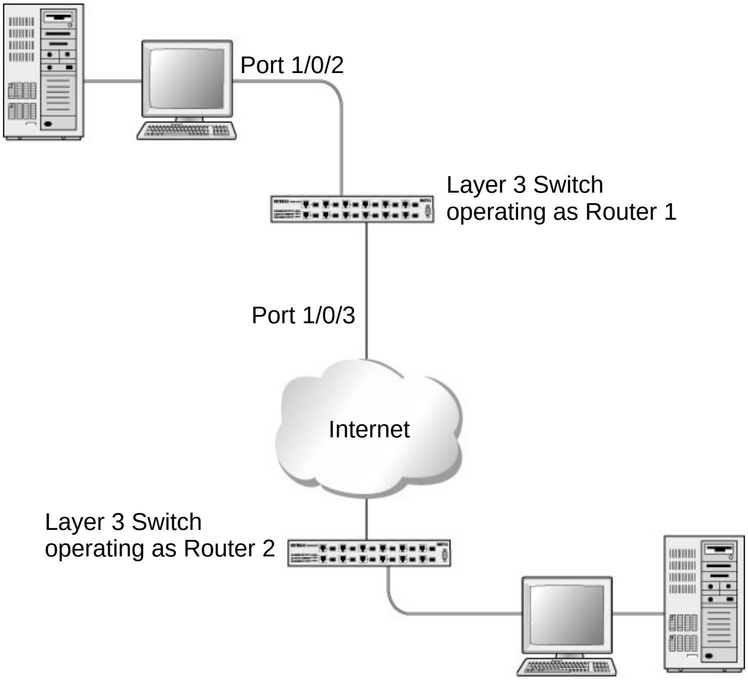


Figure 13-28

CLI: DiffServ for VoIP

The following example configures DiffServ VoIP support:

Enter Global Config mode. Set queue 5 on all ports to use strict priority mode. This queue shall 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
```

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
```

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
```

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' (per 'class_ef' definition), or marks UDP packets per 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
```

Attach the defined policy to an inbound service interface.

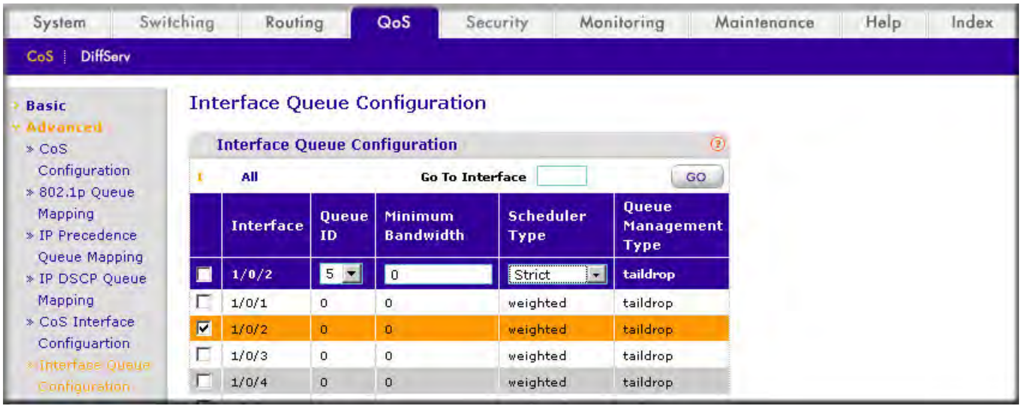
```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#service-policy in pol_voip
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Diffserv for VoIP

To use the Web interface to configure diffserv for VoIP, proceed as follows:

1. Set the queue 5 on all the interfaces to use the strict mode

   a. From the main menu, select QoS > CoS > Advanced > CoS Interface 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	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

Figure 13-29

b. Under Interface Queue Configuration, select all the interfaces.

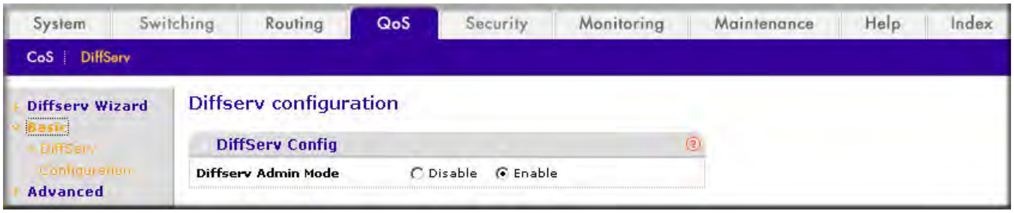
c. Select **5** in the Queue ID field.

d. Select **Strict** in the Scheduler Type field.

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

2. Enable the DiffServ

a. From the main menu, select QoS > DiffServ > Basic >DiffServ Configuration. A screen similar to the following displays.



Diffserv configuration

DiffServ Config

Diffserv Admin Mode ○ Disable ● Enable

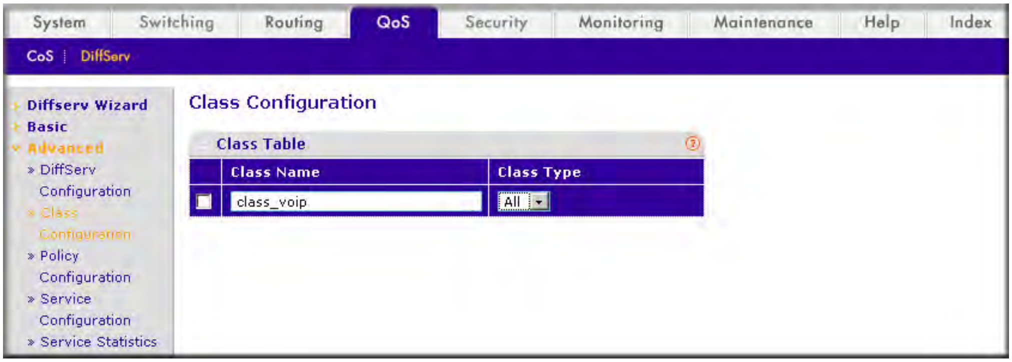
Figure 13-30

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

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

3. Create a class class_voip

a. From the main menu, select QoS > DiffServ > Advanced >DiffServ Configuration. A screen similar to the following displays.



Class Configuration

Class Table

	Class Name	Class Type
□	class_voip	All

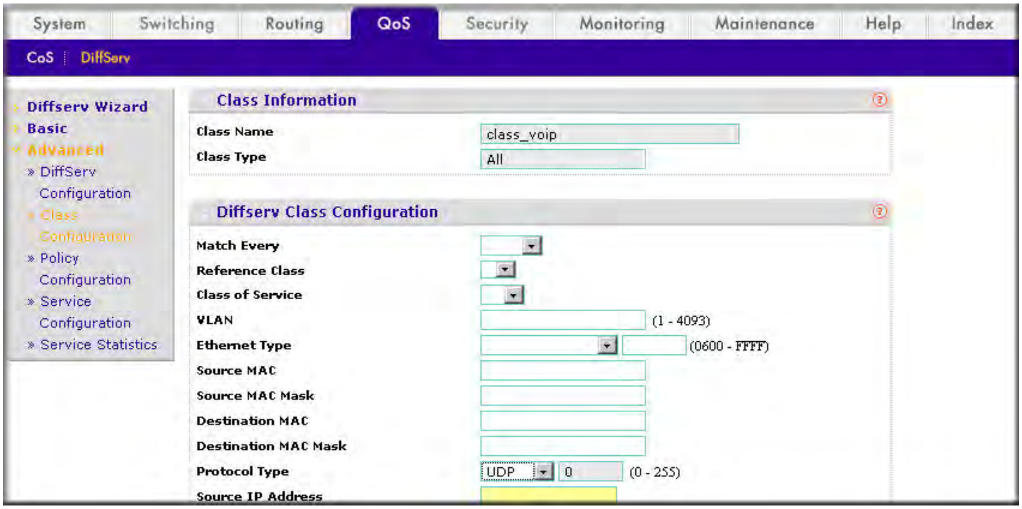
Figure 13-31

b. In the Class Name, enter **class_voip**.

c. Select **All** in the Class Type field.

d. Click **Add** to create a new class.

e. Click the class_voip, another 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		

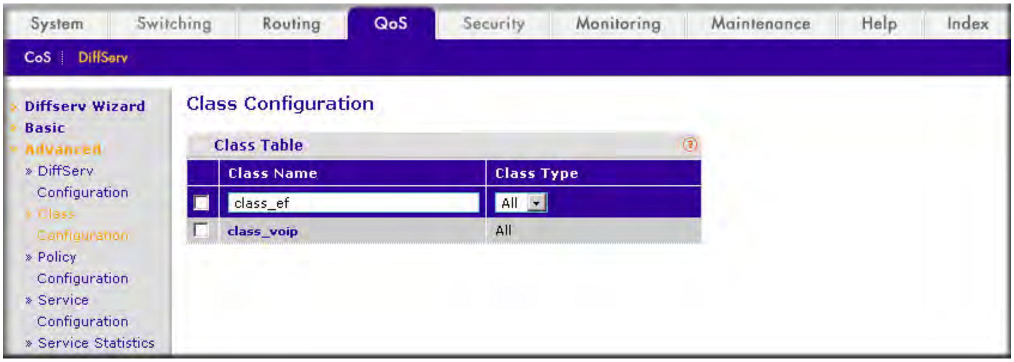
Figure 13-32

f. Select **UDP** in the Protocol Type field.

g. Click the **Apply** to create a new class.

4. Create a class class_ef:

a. From the main menu, 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

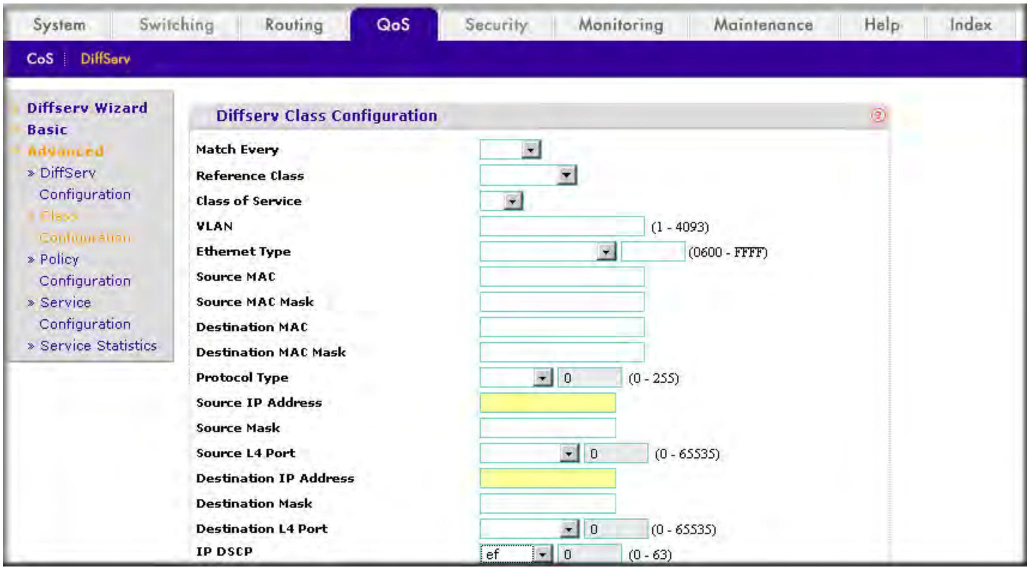
Figure 13-33

b. In the Class Name, enter **class_ef**.

c. Select **All** in the Class Type field.

d. Click the **Add** to create a new class.

e. Click the 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)

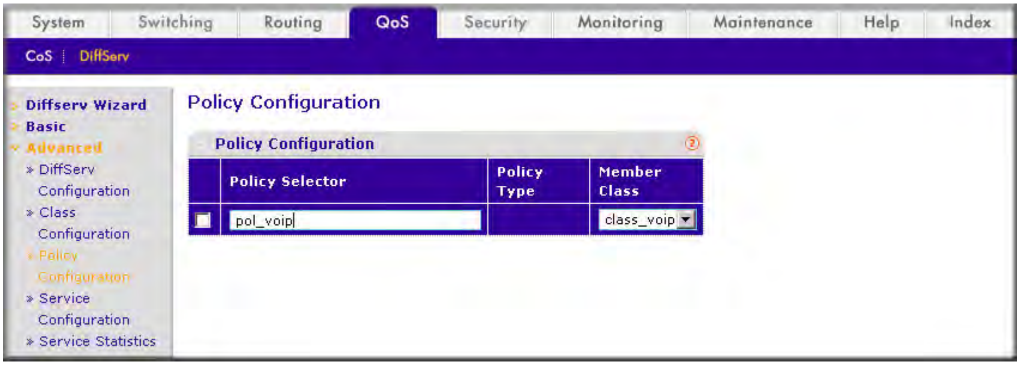
Figure 13-34

f. Select **ef** in the IP DSCP field.

g. Click **Apply** to create a new class.

5. Create a policy pol_voip and add class_voip into this policy

a. From the main menu, 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

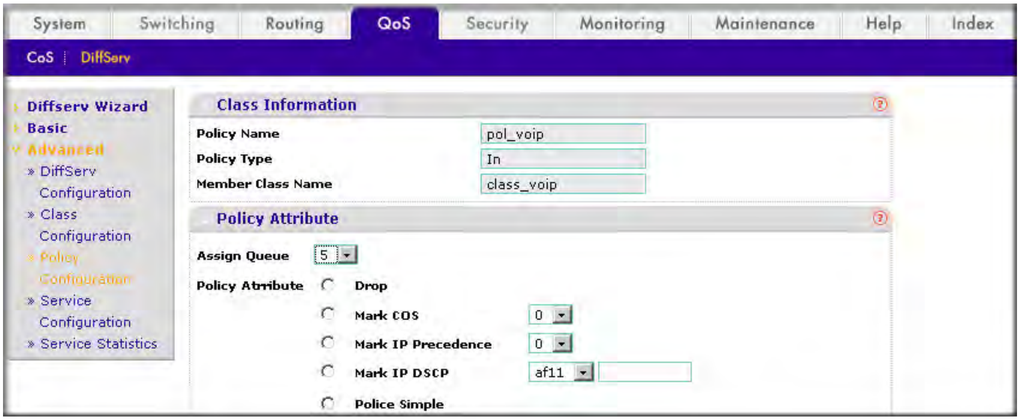
Figure 13-35

b. In the Policy Selector field, enter **pol_voip**

c. Select **class_voip** in the Member Class field.

d. Click **Add** to create a new policy.

e. Click the **pol_voip** whose class member is class_voip, another 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

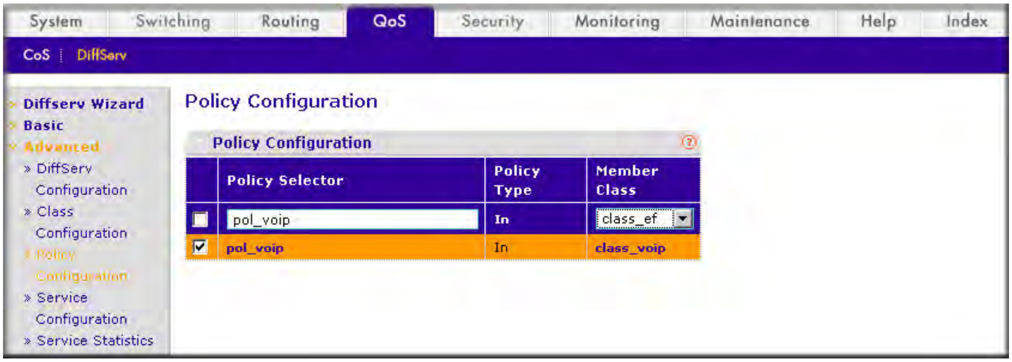
Figure 13-36

f. Select **5** in the Assign Queue field.

- **g.** For the Policy Attribute, click the **Mark IP DSCP** radio button and select **ef** in the Mark IP DSCP field.
- **h.** Click **Apply** to create a new policy.

6. Add class_ef into the policy pol_voip.

- **a.** From the main menu, select QoS > DiffServ > Advanced > Policy Configuration. A screen similar to the following displays.



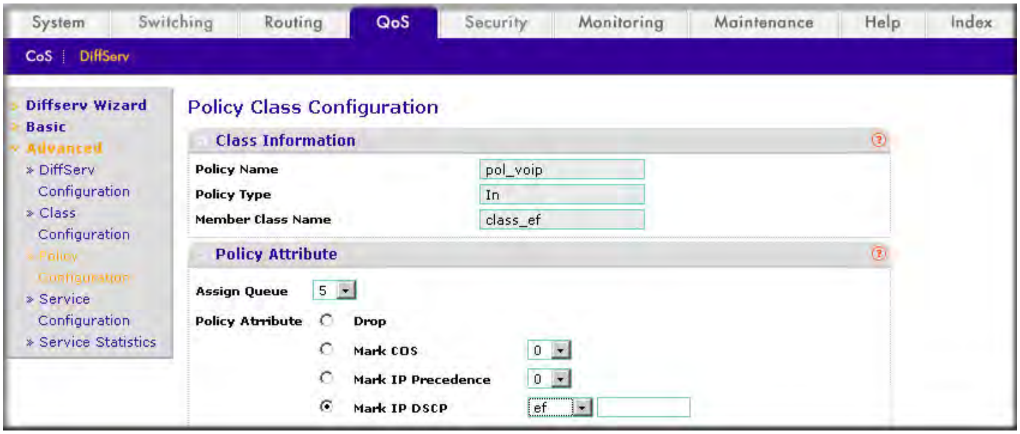
Policy Configuration

Policy Configuration

	Policy Selector	Policy Type	Member Class
□	pol_voip	In	class_ef
☑	pol_voip	In	class_voip

Figure 13-37

- **b.** Under Policy Configuration, scroll down to **pol_voip** and select the checkbox for pol_voip. Pol_voip now appears in the Policy Selector field at the top.
- **c.** Select **class_ef** in the Member Class field.
- **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, another 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

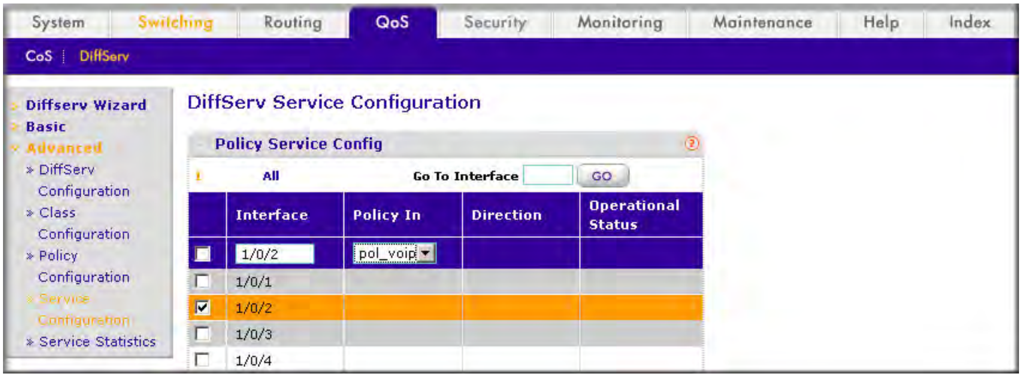
Figure 13-38

f. Select the **5** in the Assign Queue field.

g. Click **Apply** to create a new policy.

7. Attach the defined policy to the interface 1/0/2 in the inbound direction

a. From the main menu, select QoS > DiffServ > Advanced > Service Configuration. A screen similar to the following displays.



DiffServ Service Configuration

Policy Service Config

All Go To Interface

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

Figure 13-39

b. Under DiffServ Service Configuration, scroll down to interface **1/0/2** and select the checkbox for 1/0/2. 1/0/2 now appears in the Interface field at the top.

c. Select **pol_voip** in the Policy In field.

d. Click **Apply** to create a new policy.

Auto VoIP Configuration

The Auto-VoIP feature is intended to provide ease of use for the user in setting 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 will be installed to assign the highest priority to VOIP data packets. As soon as the call ends the filters will be removed.

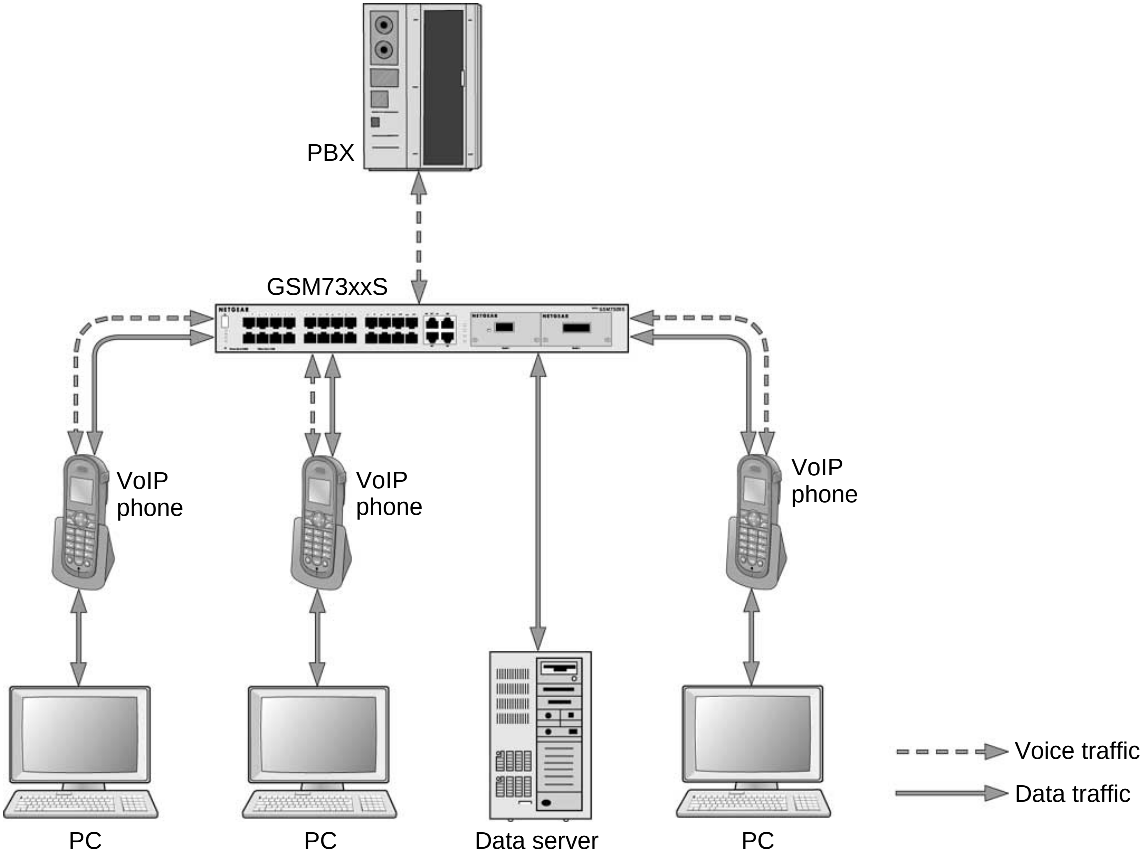


Figure 13-40

This script in this section shows how to setup Auto VoIP system wide.

CLI: Configuring Auto VoIP

Enable Auto VoIP to all the interfaces in the device.

```
(Netgear Switch) (Config)# auto-voip all
```

View the Auto VoIP information:

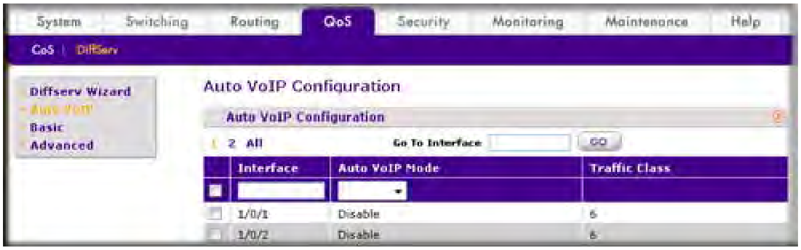
```
(Netgear Switch)  # show auto-voip interface all

        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
```

The Auto VoIP just classify and prioritize the packets and place the packets in the higher priority queue. In the above example, it is placed in Queue 6. Users can override the egress queue setting using the commands cos-queue strict or cos-queue min-bandwidth if they want.

Web Interface: Configuring Auto-VoIP

1. Enable Auto VoIP to all the interfaces in the device.

a. From the main menu, select QoS > DiffServ > Auto VoIP. A screen similar to the following displays.



Auto VoIP Configuration

Auto VoIP Configuration

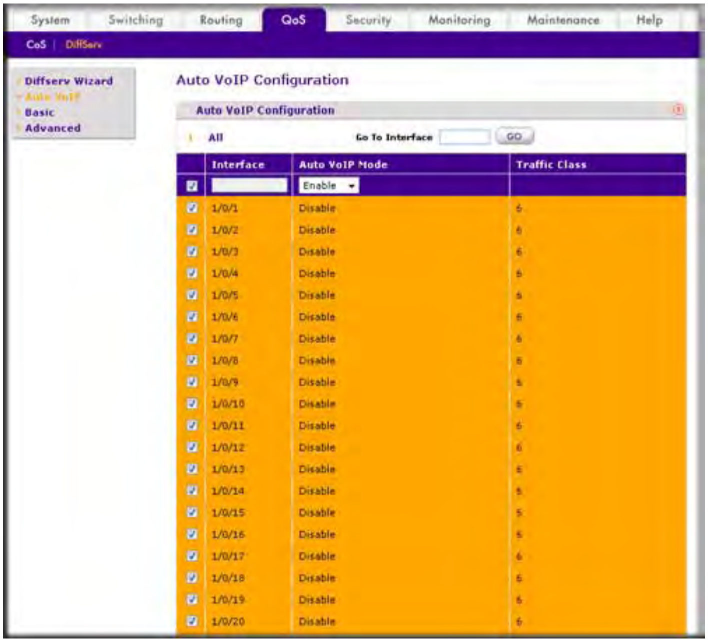
1 2 All

	Interface	Auto VoIP Mode	Traffic Class
□			
□	1/0/1	Disable	6
□	1/0/2	Disable	6

Figure 13-41

b. Select the check box in the first row to select all the interfaces.

c. Select Auto VoIP mode as **Enabled**. A screen similar to the following displays.



Auto VoIP Configuration

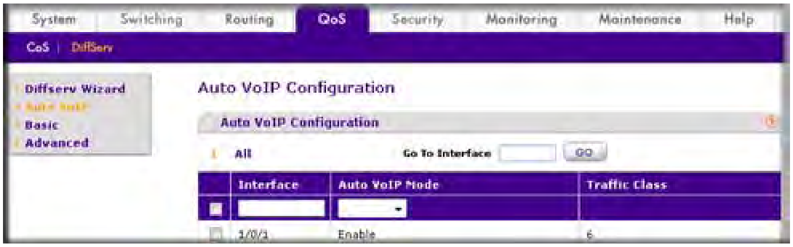
Auto VoIP Configuration

1 All

	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

Figure 13-42

d. Click **Apply**. At the end of this configuration a screen similar to the following displays.



Auto VoIP Configuration

Auto VoIP Configuration

All

Go To Interface

	Interface	Auto VoIP Mode	Traffic Class
□			
□	1/0/1	Enable	6

Figure 13-43

DiffServ for IPv6 Configuration Example

This feature extends the existing QoS ACL and DiffServ functionality by providing support for IPv6 packet classification.

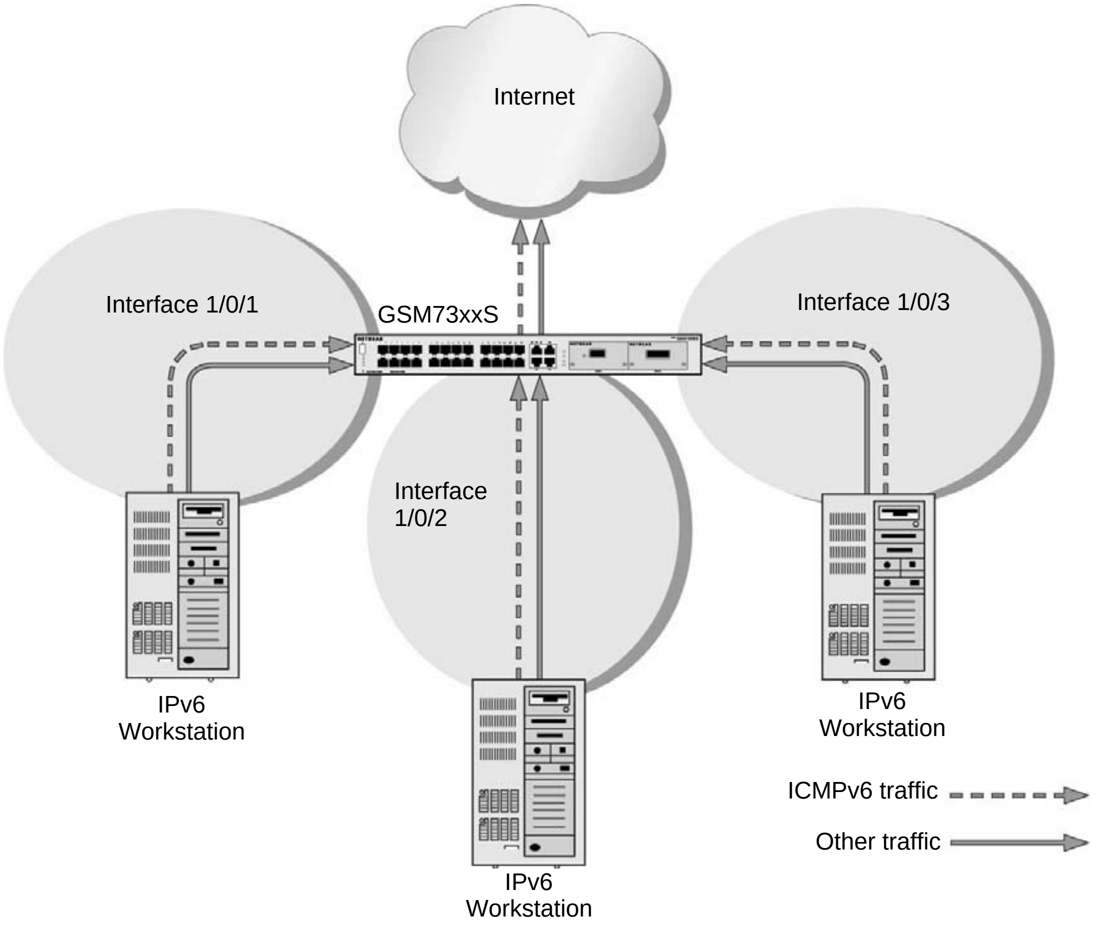


Figure 13-44

This script in this section shows how to prioritize ICMPv6 traffic over other IPv6 traffic.

CLI: Configuring DiffServ for IPv6

Create the IPv6 Class classicmpv6.

```
(Netgear Switch) (Config)# class-map match-all classicmpv6 ipv6
```

Define matching criteria as protocol ICMPv6.

```
(Netgear Switch) (Config-classmap) # match protocol 58
(Netgear Switch) (Config-classmap) # exit
```

Create the policy policyicmpv6.

```
(Netgear Switch) (Config)# policy-map policyicmpv6 in
```

Associate the previously created class classicmpv6.

```
(Netgear Switch) (Config-policy-map)# class classicmpv6
```

Set the attribute as assign queue 6.

```
(Netgear Switch) (Config-policy-classmap)# assign-queue 6
(Netgear Switch) (Config-policy-map)# exit
```

Attach the policy policy_icmpv6 in the interface 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: Configuring DiffServ for IPv6

1. Create the IPv6 Class classicmpv6.

a. From the main menu, select QoS > DiffServ > Advanced > IPv6 Class Configuration. A screen similar to the following displays.

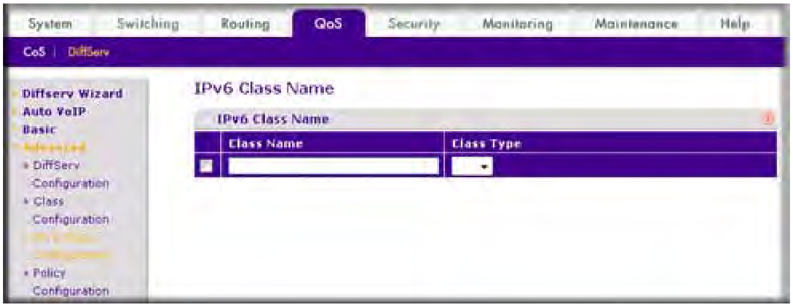
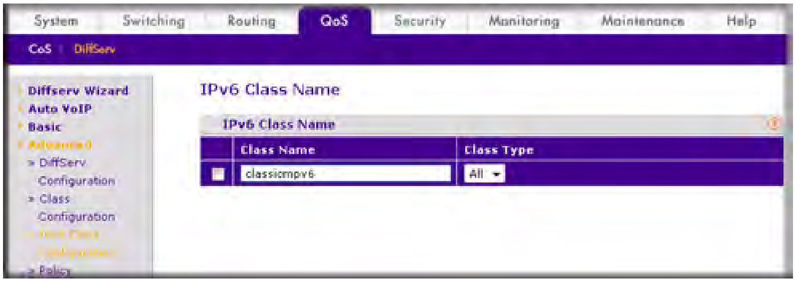


Figure 13-45

b. Enter Class Name as **classicmpv6**.

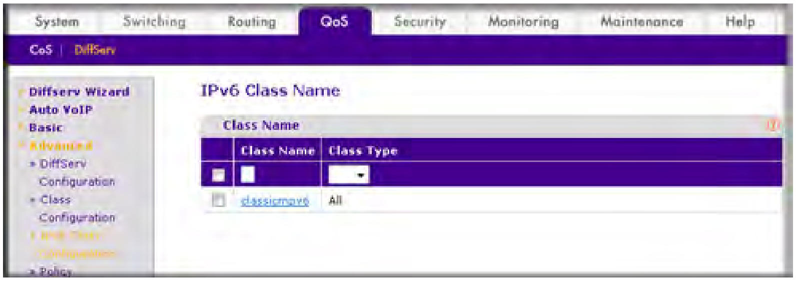
c. Select Class Type as **All**. A screen similar to the following displays.



Class Name	Class Type
classicmpv6	All

Figure 13-46

d. Click **Add** to create the IPv6 Class. At the end of this configuration a screen similar to the following displays.

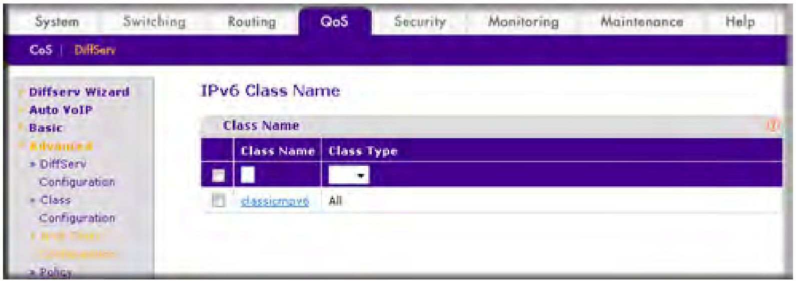


Class Name	Class Type
classicmpv6	All

Figure 13-47

2. Define matching criteria as protocol ICMPv6.

a. From the main menu, select QoS > DiffServ > Advanced > IPv6 Class Configuration. A screen similar to the following displays.



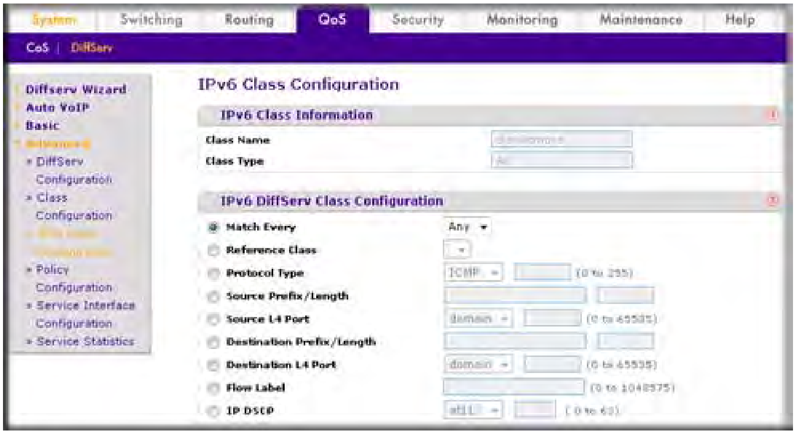
IPv6 Class Name

Class Name

	Class Name	Class Type
□		
□	classicmpv6	All

Figure 13-48

b. Click the class **classicmpv6**. A screen similar to the following displays.



IPv6 Class Configuration

IPv6 Class Information

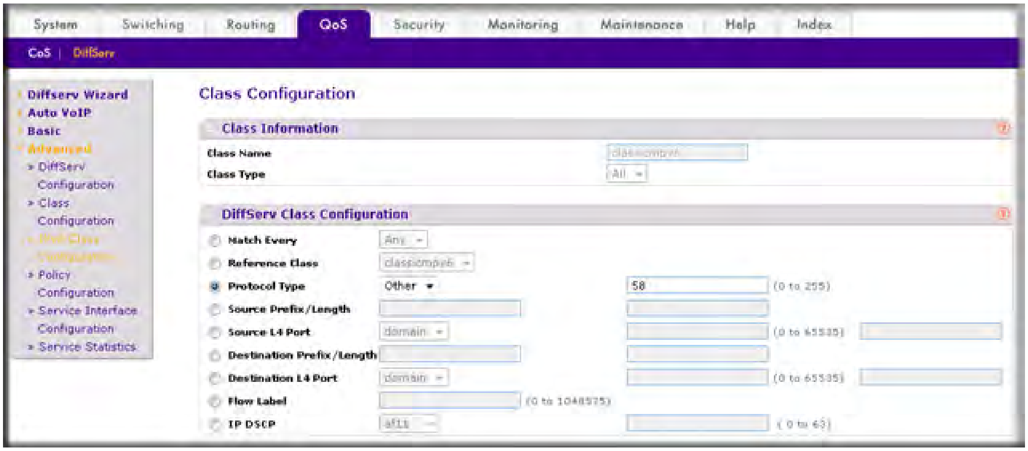
Class Name	classicmpv6
Class Type	All

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)

Figure 13-49

c. For the Protocol Type, select **Other** and enter **58**. A screen similar to the following displays.



Class Configuration

Class Information

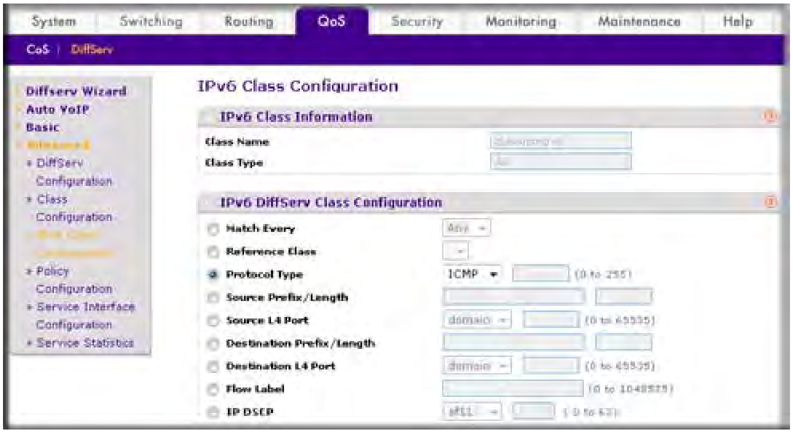
Class Name classicmpv6
Class Type All

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)

Figure 13-50

d. Click **Apply**. At the end of this configuration a screen similar to the following displays.



IPv6 Class Configuration

IPv6 Class Information

Class Name classicmpv6
Class Type All

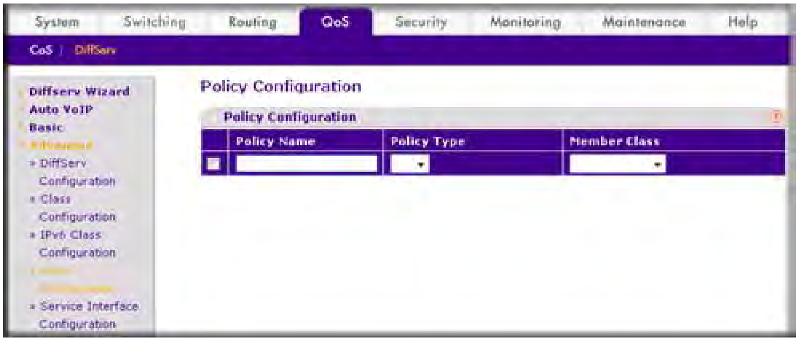
IPv6 DiffServ Class Configuration

○ 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)

Figure 13-51

3. Create the policy policyicmpv6 and associate the previously created class classicmpv6.

a. From the main menu, select QoS > DiffServ > Advanced > Policy Configuration. A screen similar to the following displays.



Policy Configuration

Policy Configuration

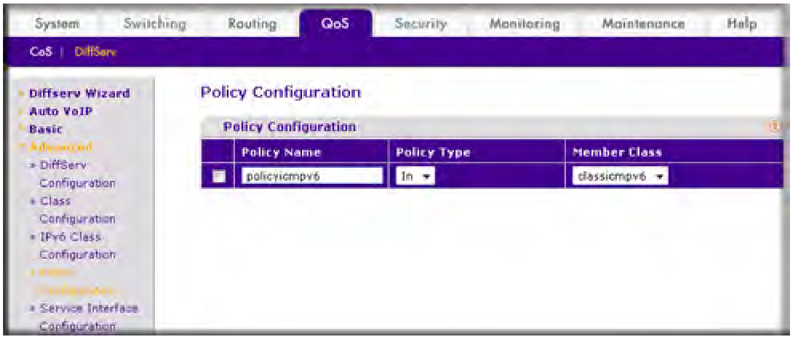
	Policy Name	Policy Type	Member Class
□		▾	▾

Figure 13-52

b. Enter the Policy Name as **policyicmpv6**.

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

d. Select Member Class as **classicmpv6**. A screen similar to the following displays.



Policy Configuration

Policy Configuration

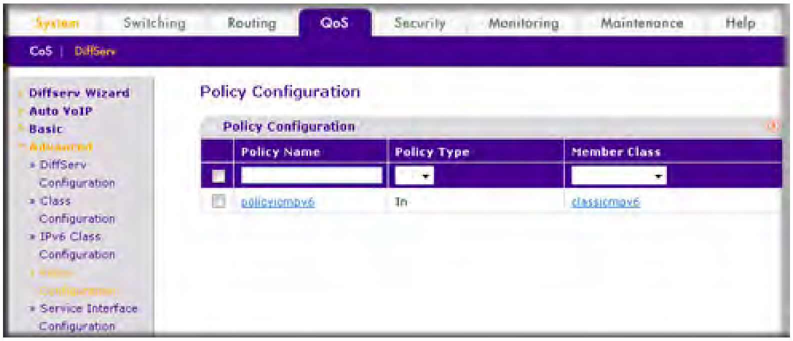
	Policy Name	Policy Type	Member Class
□	policyicmpv6	In ▾	classicmpv6 ▾

Figure 13-53

e. Click **Add**. At the end of this configuration a screen similar to the one in Figure 13-54 displays.

4. Set the attribute as assign queue 6.

a. From the main menu, select QoS > DiffServ > Advanced > Policy Configuration. A screen similar to the following displays.



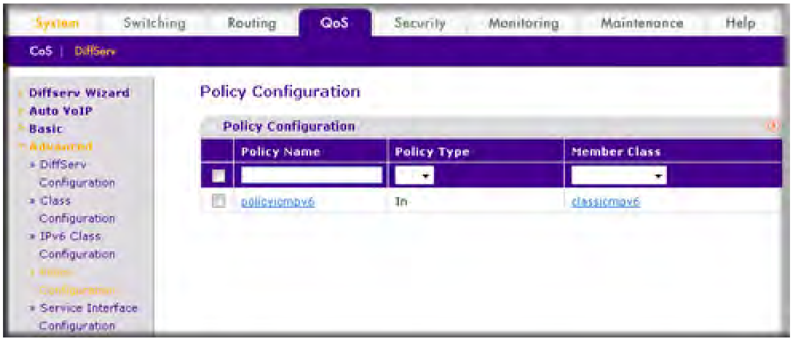
Policy Configuration

Policy Configuration

	Policy Name	Policy Type	Member Class
□	policyicmpv6	In	classicmpv6

Figure 13-54

b. Click the Policy **policyicmpv6** A screen similar to the following displays.



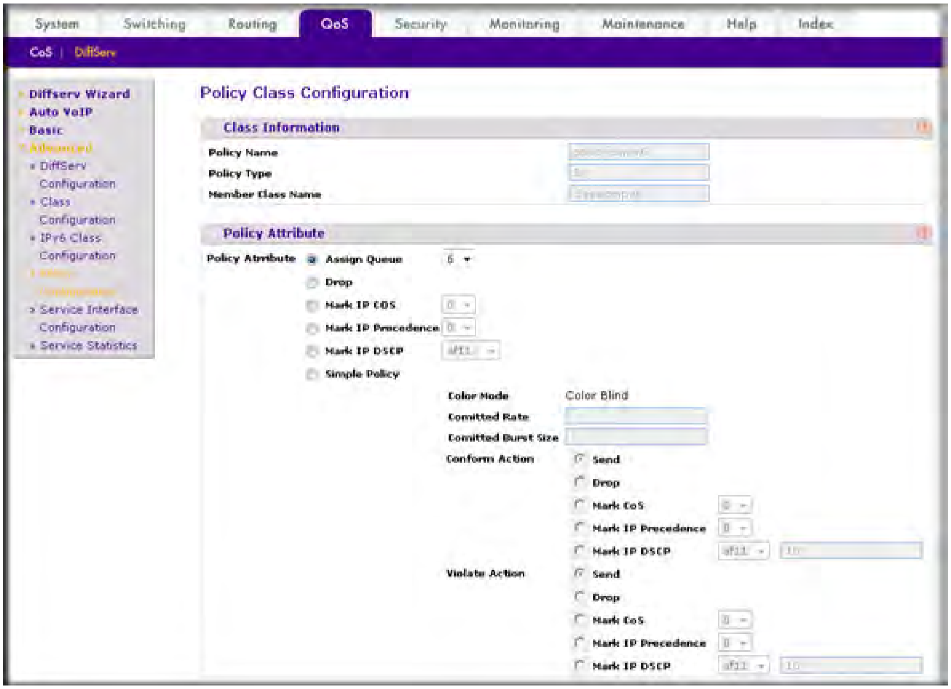
Policy Configuration

Policy Configuration

	Policy Name	Policy Type	Member Class
□	policyicmpv6	In	classicmpv6

Figure 13-55

c. Select Assign Queue as **6**..



Policy Class Configuration

Class Information

Policy Name	[illegible]
Policy Type	[illegible]
Member Class Name	[illegible]

Policy Attribute

Policy Attribute ● Assign Queue 6
○ Drop
○ Mark IP COS 0
○ Mark IP Precedence 0
○ Mark IP DSCP af11
○ Simple Policy

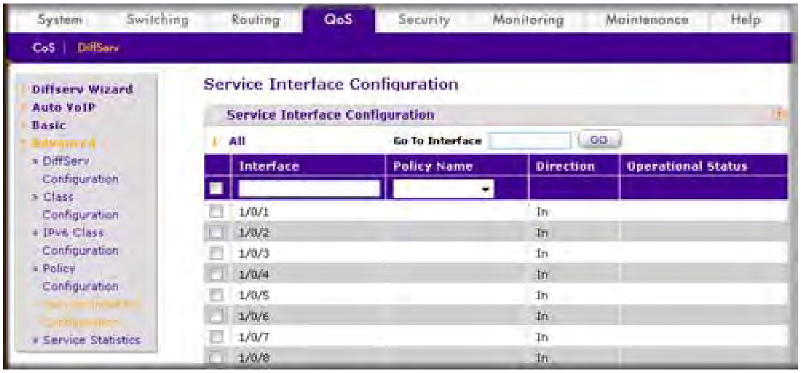
Color Mode Color Blind
Comitted Rate
Comitted Burst Size
Conform Action ● Send
○ Drop
○ Mark CoS 0
○ Mark IP Precedence 0
○ Mark IP DSCP af11 10
Violate Action ● Send
○ Drop
○ Mark CoS 0
○ Mark IP Precedence 0
○ Mark IP DSCP af11 10

Figure 13-56

d. Click **Apply**.

5. Attach the policy policyicmpv6 in the interface 1/0/1,1/0/2 and 1/0/3.

a. From the main menu, select QoS > DiffServ > Advanced > Service Interface Configuration. A screen similar to the following displays.



Service Interface Configuration

Service Interface Configuration

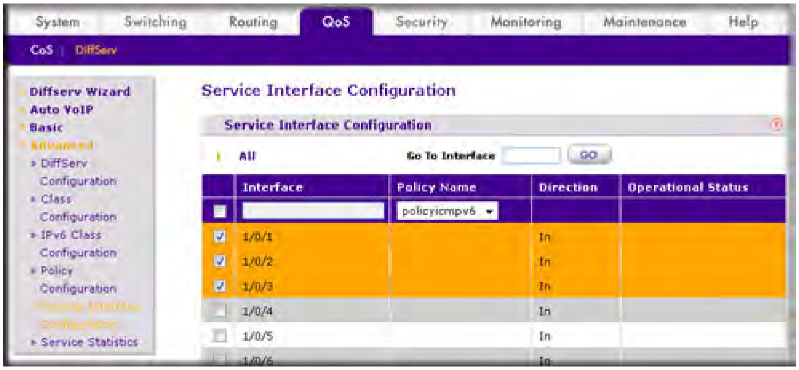
All   Go To Interface

□	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	

Figure 13-57

b. Select Policy Name as **policyicmpv6**.

c. Click the check box for the interfaces 1/0/1, 1/0/2 and 1/0/3. A screen similar to the following displays.

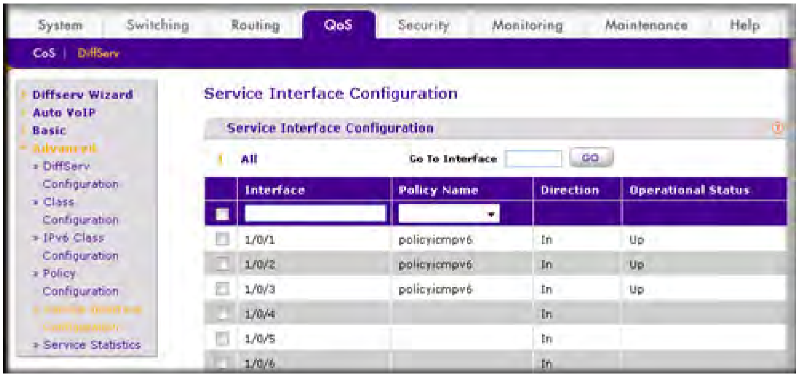


Service Interface Configuration

	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	

Figure 13-58

d. Click **Apply**. At the end of this configuration a screen similar to the following displays.



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	

Figure 13-59

Chapter 14
IGMP Snooping and Querier

In this chapter, the following examples are provided:

- “Enable IGMP Snooping”
- “Show igmpsnooping” on page 14-2
- “Show mac-address-table igmpsnooping” on page 14-3
- “Configure the Switch with an External Multicast Router” on page 14-4
- “Configure the Switch with a Multicast Router Using VLAN” on page 14-6
- “Enable IGMP Querier” on page 14-8
- “Show IGMP Querier Status” on page 14-9

This section describes the Internet Group Management Protocol (IGMP) feature: IGMPv3 and IGMP Snooping. IGMP:

- Uses Version 3 of IGMP
- Includes snooping
- Snooping can be enabled per VLAN

Enable IGMP Snooping

The following are examples of the commands used in the IGMP Snooping feature.

CLI: Enabling IGMP Snooping

The following example shows how to enable IGMP snooping.

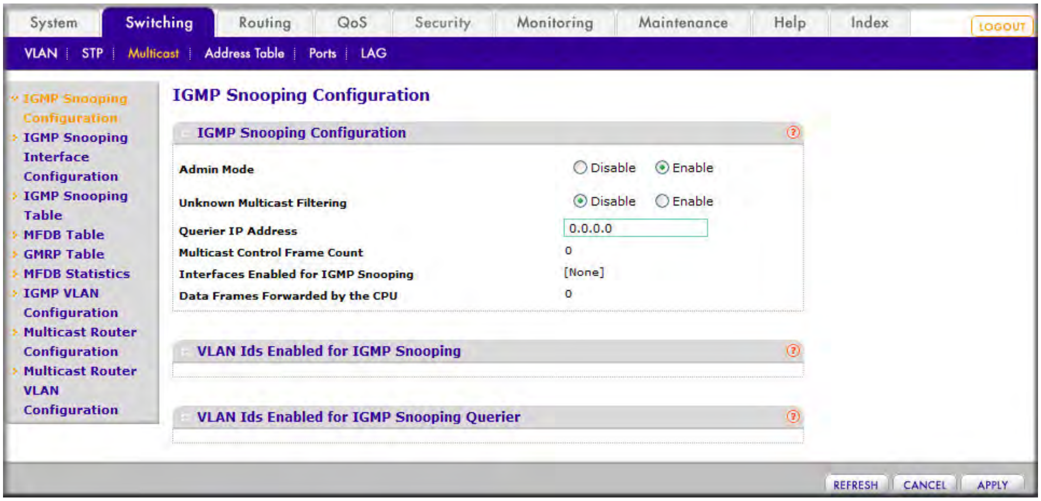
```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip igmpsnooping
(Netgear Switch) (Config)#ip igmpsnooping interfacemode
(Netgear Switch) (Config)#exit
```

Web Interface: Enabling IGMP Snooping

To use the Web interface to configure the managed switch, proceed as follows:

1. Configure the IGMP Snooping Configuration.

a. From the main menu, 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	0.0.0.0
Multicast Control Frame Count	0
Interfaces Enabled for IGMP Snooping	[None]
Data Frames Forwarded by the CPU	0

VLAN Ids Enabled for IGMP Snooping

VLAN Ids Enabled for IGMP Snooping Querier

Figure 14-1

b. Enter the following information in the IGMP Snooping Configuration.

Next to the Admin mode field, select the **Enable** radio button.

c. Click **Apply**.

Show igmpsnooping

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

CLI: Showing igmpsnooping

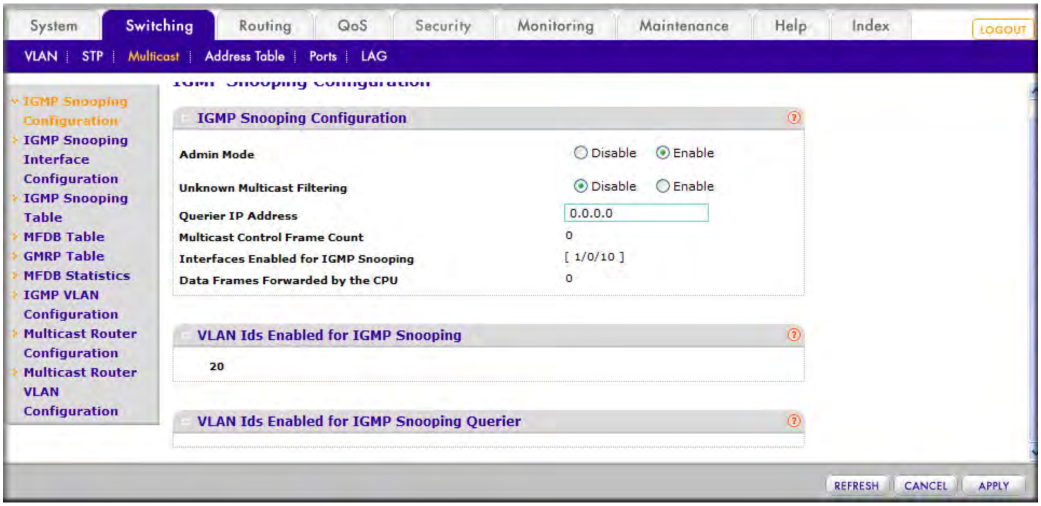
```
(Netgear Switch)     #show igmpsnooping?

<cr>           Press Enter to execute the command.
<slot/port>    Enter interface in slot/port format.
mrouter        Display IGMP Snooping Multicast Router information.
<1-4093>       Display IGMP Snooping valid VLAN ID information.
```

```
(Netgear Switch)     #show igmpsnooping

Admin Mode..............................        Enable
Multicast Control Frame Count...........        0
Interfaces Enabled for IGMP Snooping.....       1/0/10
Vlans enabled for IGMP snooping.........        20
```

Web Interface: Showing igmpsnooping

To use the Web interface to configure the managed switch, proceed as follows:

1. Configure the IGMP Snooping Configuration.
   a. From the main menu, 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	0.0.0.0
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

20

VLAN Ids Enabled for IGMP Snooping Querier

Figure 14-2

Show mac-address-table igmpsnooping

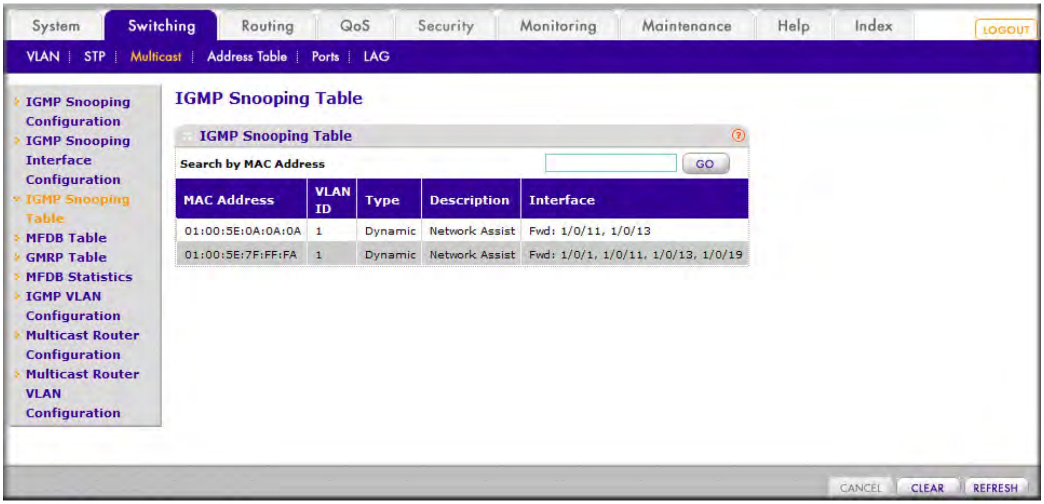
The example is shown as CLI commands and as a Web interface procedure.

CLI: Showing 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: Showing mac-address-table igmpsnooping

From the main menu, select Switching > Multicast > IGMP Snooping Table. A screen similar to the following displays.



IGMP Snooping Table

IGMP Snooping Table

Search by MAC Address GO

MAC Address	VLAN ID	Type	Description	Interface
01:00:5E:0A:0A:0A	1	Dynamic	Network Assist	Fwd: 1/0/11, 1/0/13
01:00:5E:7F:FF:FA	1	Dynamic	Network Assist	Fwd: 1/0/1, 1/0/11, 1/0/13, 1/0/19

Figure 14-3

Configure the Switch with an External Multicast Router

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

CLI: Configuring the Switch with an External Multicast Router

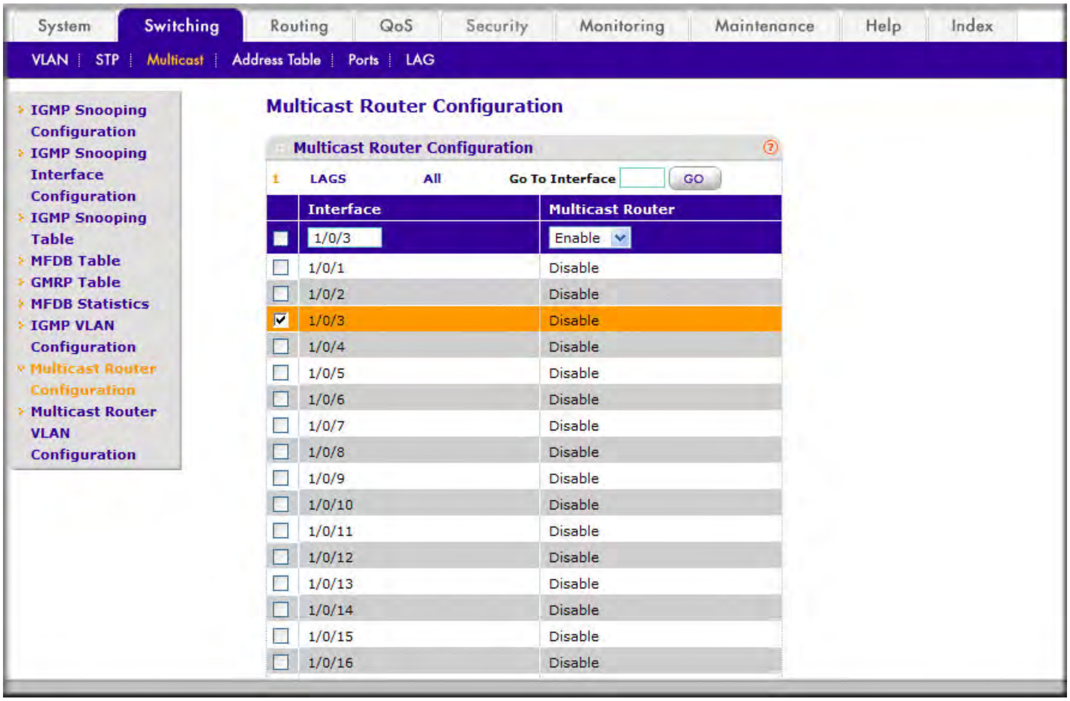
This example configures the interface as the one the multicast router is attached to. All IGMP packets snooped by the switch will be forwarded to the multicast router reachable from this interface.

```
(Netgear Switch)(Interface 1/0/3)# ip igmp mrouter interface
```

Web Interface: Configuring the Switch with an External Multicast Router

To use the Web interface to configure the managed switch, proceed as follows:

1. From the main menu, select Switching > Multicast > Multicast Router Configuration. A screen similar to the following displays.



Multicast Router Configuration

Multicast Router Configuration

1 LAGS All Go To Interface

	Interface	Multicast Router
□	1/0/3	Enable
□	1/0/1	Disable
□	1/0/2	Disable
☑	1/0/3	Disable
□	1/0/4	Disable
□	1/0/5	Disable
□	1/0/6	Disable
□	1/0/7	Disable
□	1/0/8	Disable
□	1/0/9	Disable
□	1/0/10	Disable
□	1/0/11	Disable
□	1/0/12	Disable
□	1/0/13	Disable
□	1/0/14	Disable
□	1/0/15	Disable
□	1/0/16	Disable

Figure 14-4

2. Under Multicast Router Configuration, scroll down to interface **1/0/3** and select the checkbox for that interface. Now 1/0/3 appears in the Interface field at the top.
3. In the Multicast Router field, select **Enable**.
4. Click **Apply**.

Configure the Switch with a 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

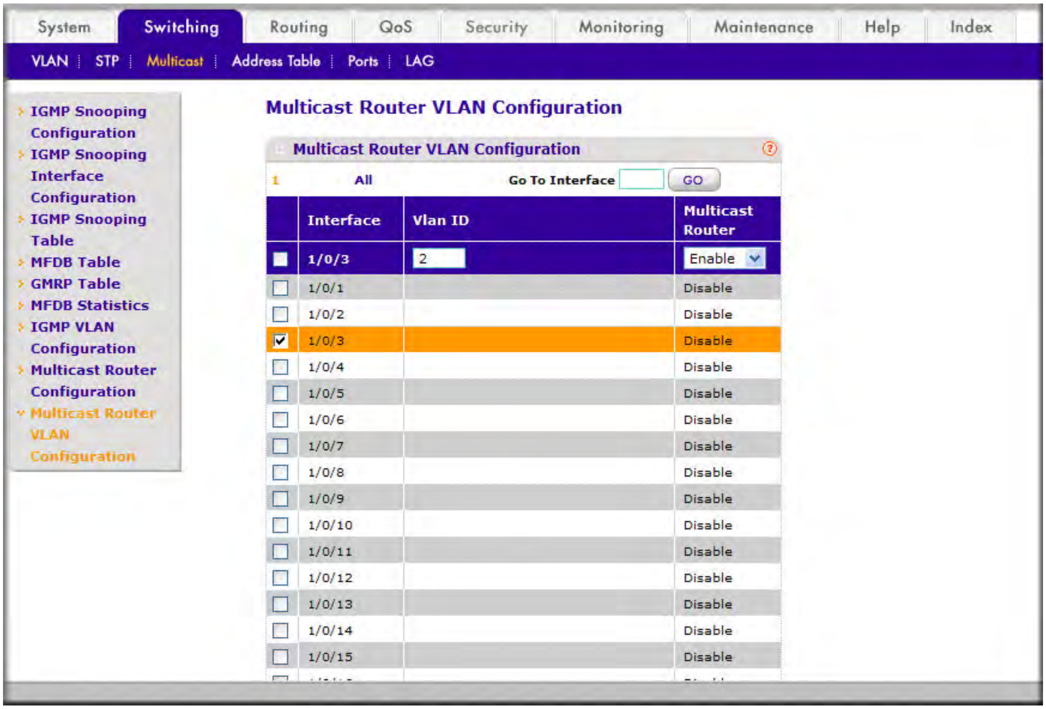
This example configures the interface to only forward the snooped IGMP packets that come from VLAN ID (<VLAN Id>) to the multicast router attached to this interface.

```
(Netgear Switch)(Interface 1/0/3)# ip igmp mrouter 2
```

Web Interface: Configuring the Switch with a Multicast Router Using VLAN

To use the Web interface to configure the managed switch, proceed as follows:

1. From the main menu, select Switching > Multicast > Multicast Router VLAN Configuration. A screen similar to the following displays.



Multicast Router VLAN Configuration

Multicast Router VLAN Configuration

1 All Go To Interface

	Interface	Vlan ID	Multicast Router
□	1/0/3	2	Enable
□	1/0/1		Disable
□	1/0/2		Disable
☑	1/0/3		Disable
□	1/0/4		Disable
□	1/0/5		Disable
□	1/0/6		Disable
□	1/0/7		Disable
□	1/0/8		Disable
□	1/0/9		Disable
□	1/0/10		Disable
□	1/0/11		Disable
□	1/0/12		Disable
□	1/0/13		Disable
□	1/0/14		Disable
□	1/0/15		Disable

Figure 14-5

2. Under Multicast Router VLAN Configuration, scroll down to interface **1/0/3** and select the checkbox for that interface. Now 1/0/3 appears in the Interface field at the top.
3. Enter the following information in the Multicast Router VLAN Configuration**.**
   - In the VLAN ID field, enter **2**.
   - Select **Enable** in the Multicast Router field.
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 would normally be 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—normally a router—that can generate an IGMP membership query and solicit interested nodes to respond. With the build-in IGMP Querier feature inside the switch, such an external device is no longer needed.

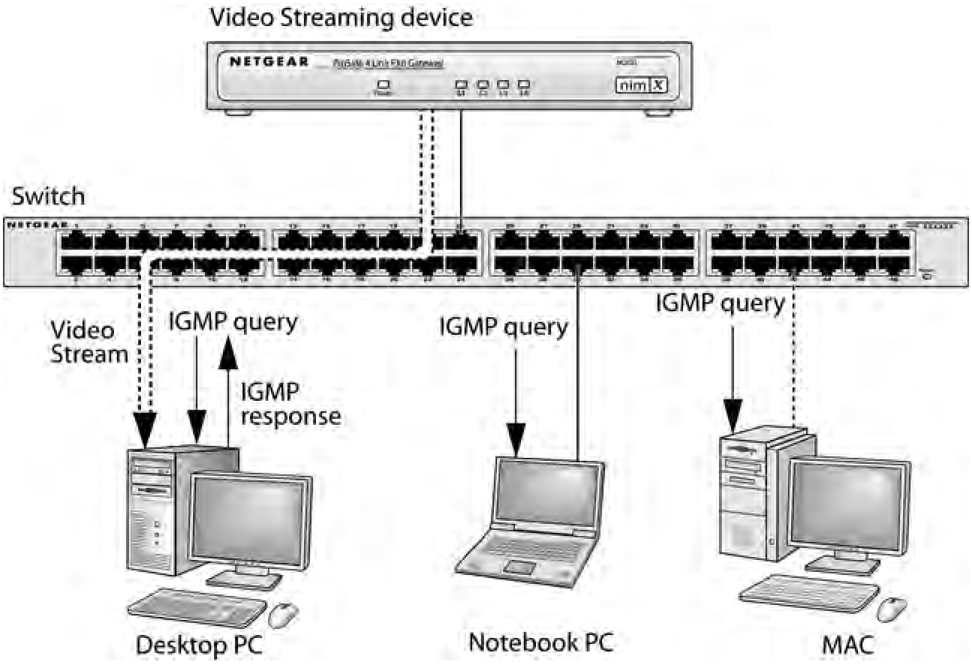


Figure 14-6

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.

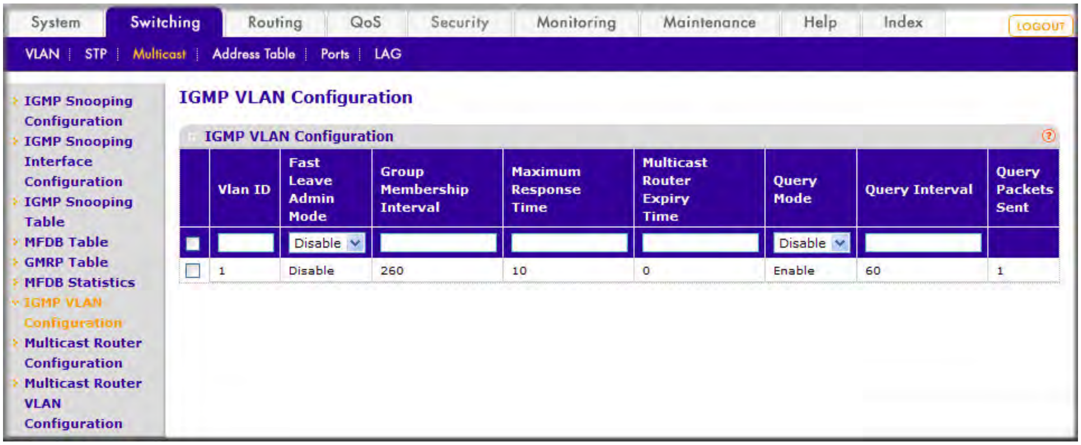
CLI: Enabling IGMP Querier

Use the following CLI commands to set up the switch to generate IGMP querier packet for a designated VLAN. The IGMP packet will be transmitted to every ports on the VLAN. The following example enables the querier for VLAN 1. See the CLI Manual for more details about other IGMP querier command options.

```
(Netgear switch) #vlan database
(Netgear switch) (vlan)#ip igmp 1
(Netgear switch) (vlan)#ip igmpsnooping querier 1
(Netgear switch) (vlan)#exit
(Netgear switch) #config
(Netgear switch) (config)#ip igmpsnooping
(Netgear switch) (config)#exit
```

Web Interface: Enabling IGMP Querier

1. From the main menu, select Switching > Multicast >IGMP VLAN Configuration. A screen similar to the following displays.



IGMP VLAN Configuration

IGMP VLAN Configuration

	Vlan ID	Fast Leave Admin Mode	Group Membership Interval	Maximum Response Time	Multicast Router Expiry Time	Query Mode	Query Interval	Query Packets Sent
□		Disable				Disable		
□	1	Disable	260	10	0	Enable	60	1

Figure 14-7

2. Enter the following information in the IGMP VLAN Configuration.
   - In the VLAN ID field**,** enter **1**.
   - Select **Enable** in the Query Mode field.
   - In the Querier Interval field, enter **60**.

3. Click **Add**.

Show IGMP Querier Status

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

CLI: Showing IGMP Querier Status

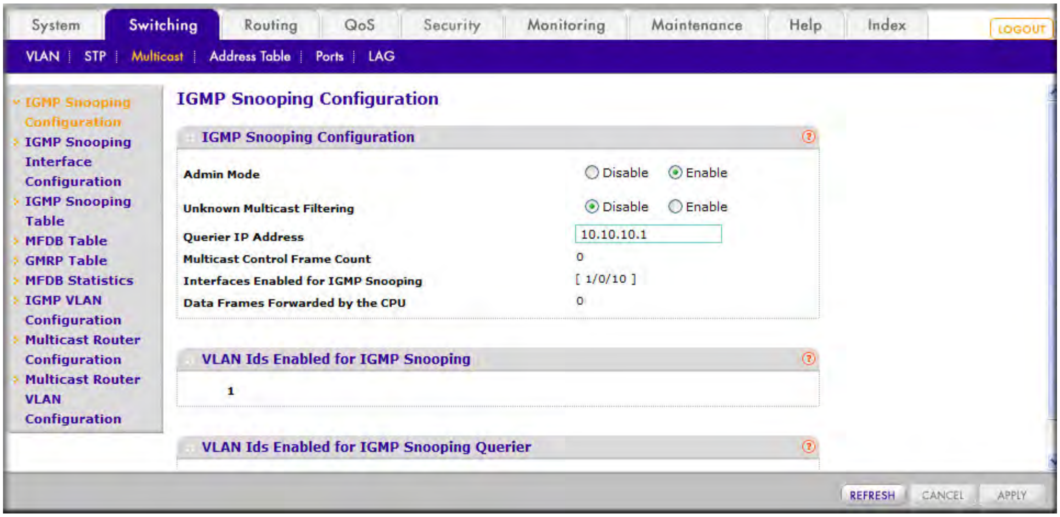
To see the IGMP querier status, use the following command.

```
(Netgear switch) #show ip igmpsnooping querier 1

Vlan ID........................................ 1
Admin Mode..................................... Active
Query IP Address............................... 10.10.10.1
Querier Interval............................... 60
Query Packets Sent Count....................... 242
```

The command shows that the IGMP admin mode is Active. The mode is controlled by the **ip igmpsnooping** command. If the mode is inactive, no query packet is sent.

Web Interface: Showing IGMP Querier Status

1. From the main menu, 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
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

Figure 14-8

2. Click **Refresh**.

Chapter 15
Security Management

In this chapter, exmples are provided for the following topics:

Port Security

This section describes the Port Security feature. Port Security:

- Allows for limiting 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
- Enabled on a per port basis
- When locked, only packets with allowable MAC address will be forwarded
- Supports both dynamic and static
- Implement two traffic filtering methods
  – Dynamic Locking - User specifies 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 address are forwarded.
  – Static Locking - User manually specifies a list of static MAC addresses for a port. Dynamically locked addresses can be converted to statically locked addresses.

  These methods can be used concurrently

Port Security:

- Helps secure network by preventing unknown devices from forwarding packets

- When link goes down, all dynamically locked addresses are ‘freed’
- If a specific MAC address is to be set for a port, set the dynamic entries to 0, then only allow packets with a MAC address matching the MAC address in the static list
- Dynamically locked MAC addresses are aged out if another packet with that address is not seen within the age-out time. The user 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
- Dynamically locked addresses can be converted to statically locked addresses

Set the Dynamic and Static Limit on the Port 1/0/1

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

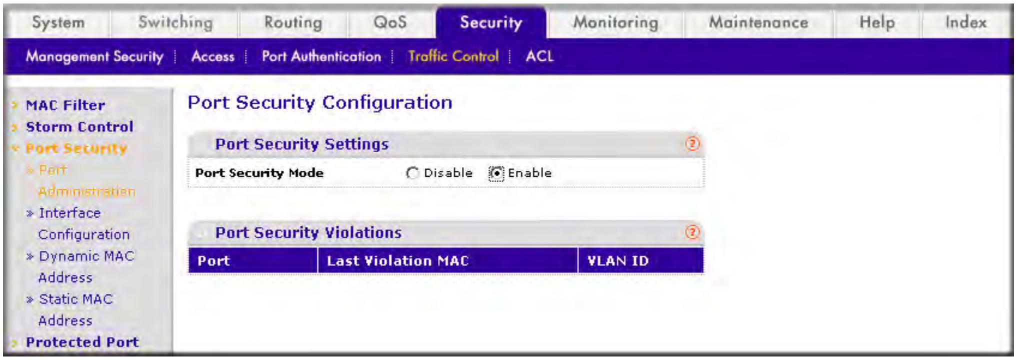
CLI: Setting the Dynamic and Static Limit on the Port 1/0/1

```
(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: Setting the Dynamic and Static Limit on the Port 1/0/1

1. To use the Web interface to enable port-security globally, proceed as follows:

   a. From the main menu, 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

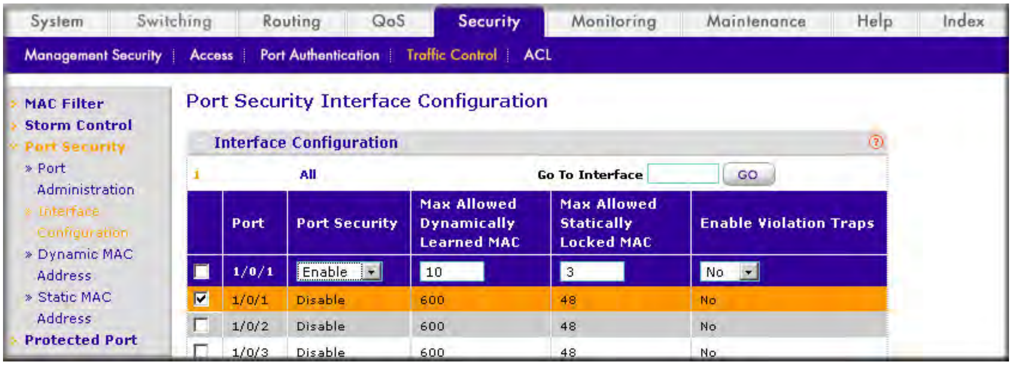
Figure 15-1

b. Under Port Security Configuration, next to the Port Security Mode, select **Enable** radio button.

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

2. Set dynamic and static limit on the port 1/0/1

a. From the main menu, select Security > Traffic Control >Port Security->Interface Configuration. A screen similar to the following displays.



Port Security Interface Configuration

Interface Configuration

1 All Go To Interface

	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

Figure 15-2

b. Under Port Security Interface Configuration, scroll down to interface **1/0/1** and select the checkbox for 1/0/1. 1/0/1 now appears in the Interface field at the top.

c. Enter the following information in the Interface Configuration.

- Select the **Enable** in the Port Security field.
- In the Max Allowed Dynamically Learned MAC field, enter **10**.
- In the Max Allowed Statically Locked MAC filed, enter **3**.

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

Convert the Dynamic Address Learned from 1/0/1 to the Static Address

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

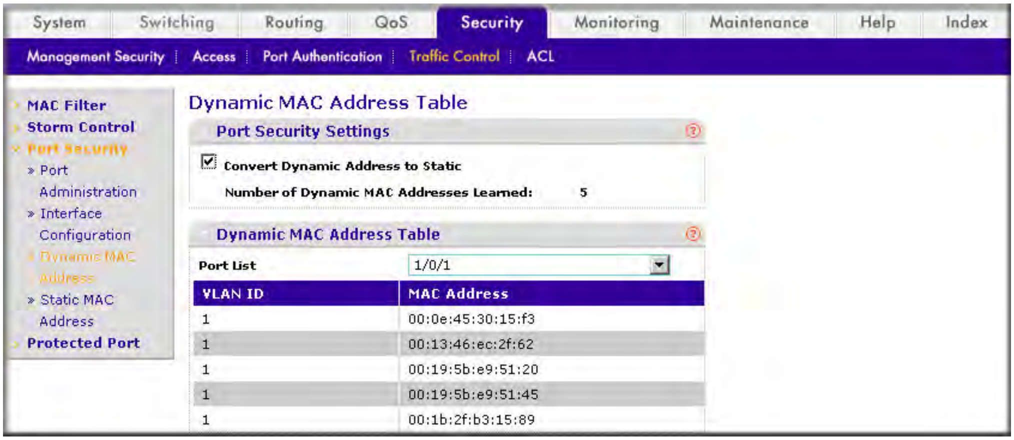
CLI: Converting the Dynamic Address Learned from 1/0/1 to the Static Address

```
(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: Converting the Dynamic Address Learned from 1/0/1 to the Static Address

To use the Web interface to convert the dynamic address to the static address, proceed as follows:

1. From the main menu, 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

Figure 15-3

2. Under Port Security Configuration, select **1/0/1** in the Port List field.
3. Select the **Convert Dynamic Address to Static** checkbox.

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

Create a Static Address

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

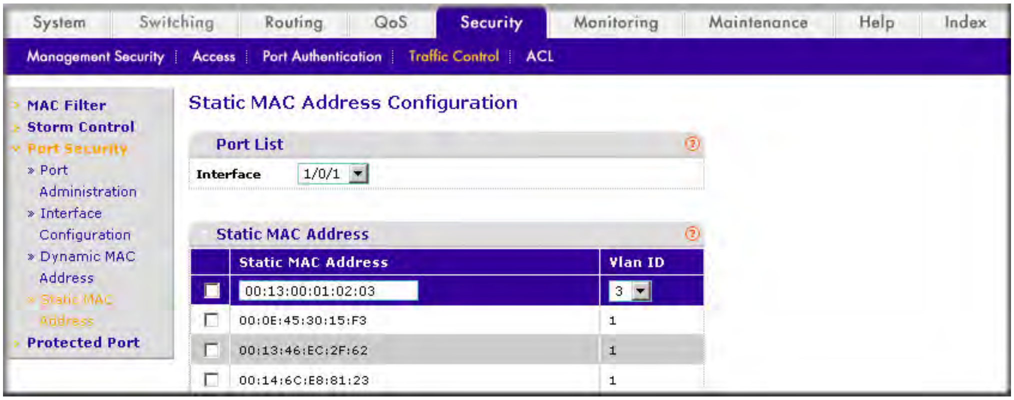
CLI: Creating a Static Address

```
(Netgear Switch) (Interface 1/0/1)#port-security mac-address 00:13:00:01:02:03
```

Web Interface: Creating a Static Address

To use the Web interface to create a static address, proceed as follows:

1. From the main menu, 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:E8:81:23	1

Figure 15-4

2. Under Port List, select **1/0/1** in the Interface field.
3. Enter the following information in the Static MAC Address.
   - In the Static MAC Address field, enter **00:13:00:01:02:03.**
   - Select **3** in the Vlan ID field.
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:

- 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, PC1 and PC2 can access the Internet as usual, but PC1 cannot see the traffic that is generated by PC2, that is, no traffic is forwarded between PC1 and PC2.

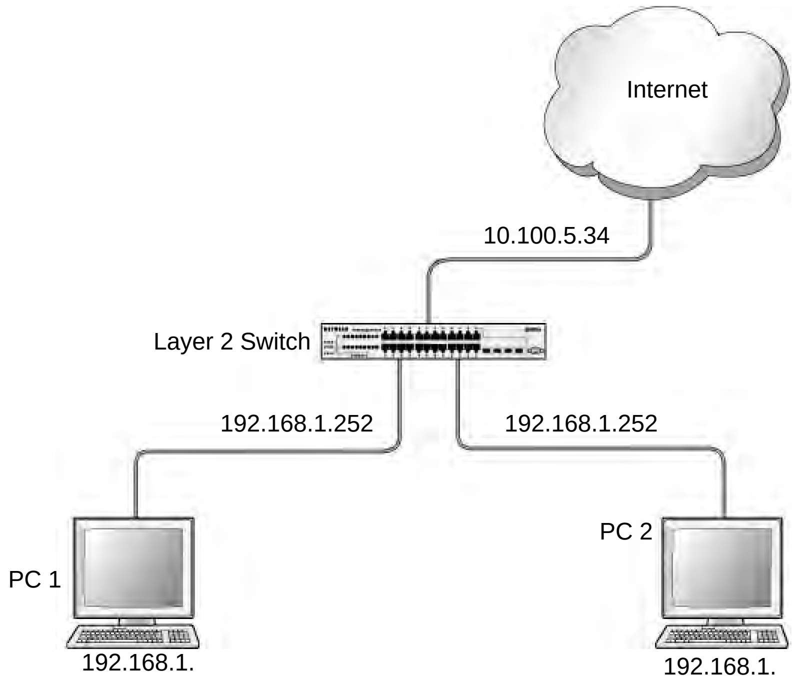


Figure 15-5

CLI: Configuring a Protected Port to Isolate Ports on the Switch

To use the CLI to configure a protected port in order to isolate ports, enter the following CLI commands:

Step 1: Create one VLAN 192 including PC1 and PC2.

```
(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
```

Step 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
```

Step 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
```

Step 4: Enable IProuting 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
```

Step 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
```

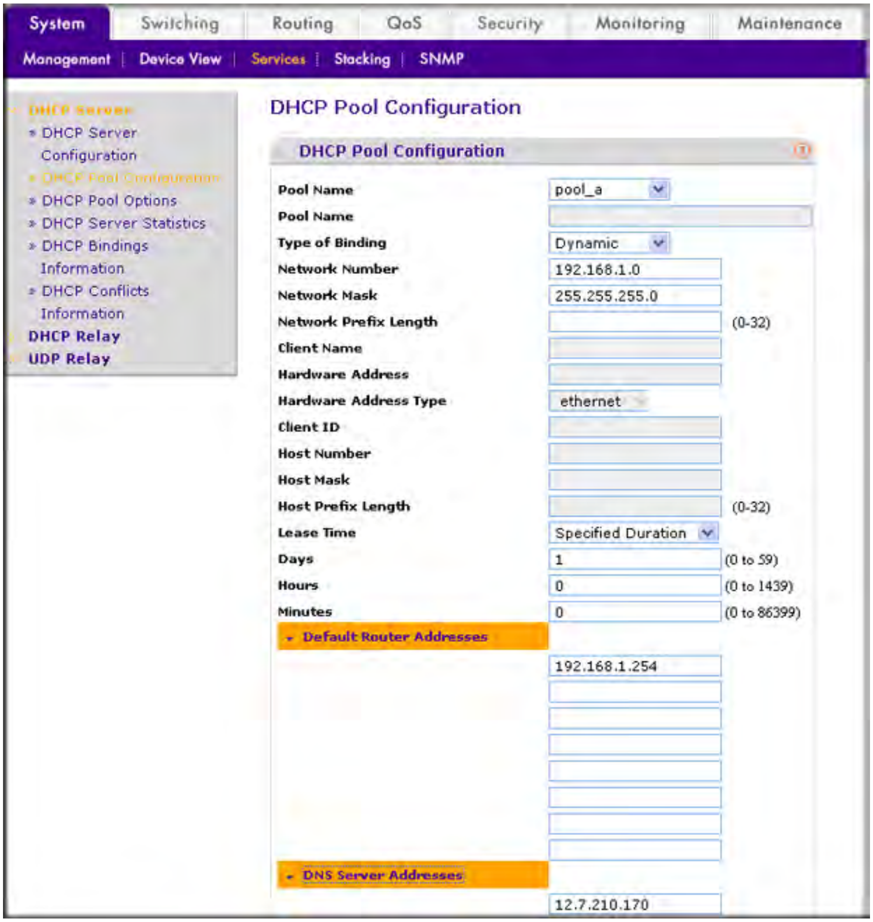
Web Interface: Configuring a Protected Port to Isolate Ports on the Switch

To use the Web Interface to configure a protected port in order to isolate ports, proceed as follows:

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" in Chapter 22

a. From the main menu, select System > Services > DHCP Server > DHCP Server Configuration. A screen similar to the following displays.



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	

Figure 15-6

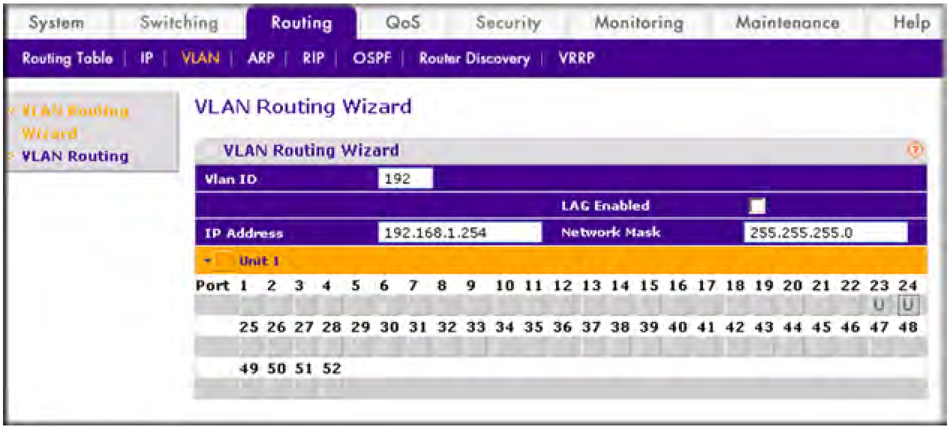
b. Under DHCP Pool Configuration, enter the following information:

- Select **Create** in the Pool Name field.
- In the Pool Name field, enter **pool-a**.
- Select **Dynamic** in the Type of Binding field.
- 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 on **Default Router Addresses**. The DNS server address fields display. In the first router address field, enter **192.168.1.254**.
- Click on **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. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.



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 under 23, U under 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

Figure 15-7

   b. Enter the following information in the VLAN Routing Wizard:

   - 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:

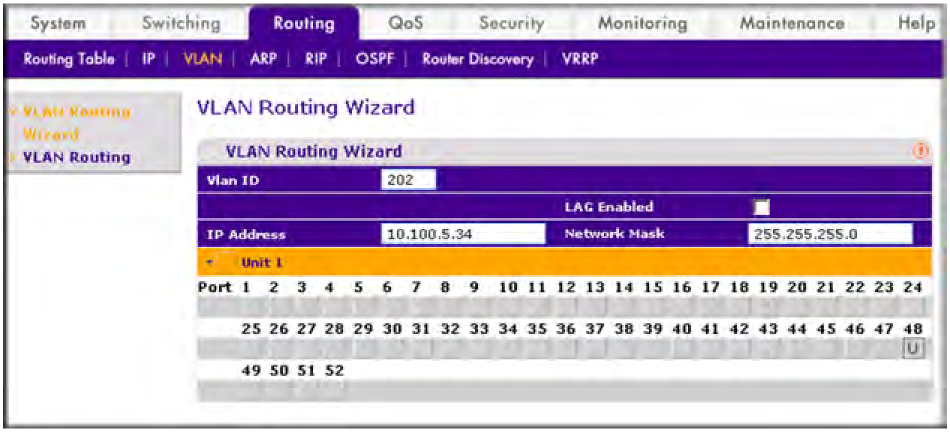
   - Click the gray box under port 23 twice until **U** displays.
   - Click the gray box under port 24 twice until **U** displays.

   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. From the main menu, 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

49 50 51 52

Figure 15-8

b. Enter the following information in the VLAN Routing Wizard:

- 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**.

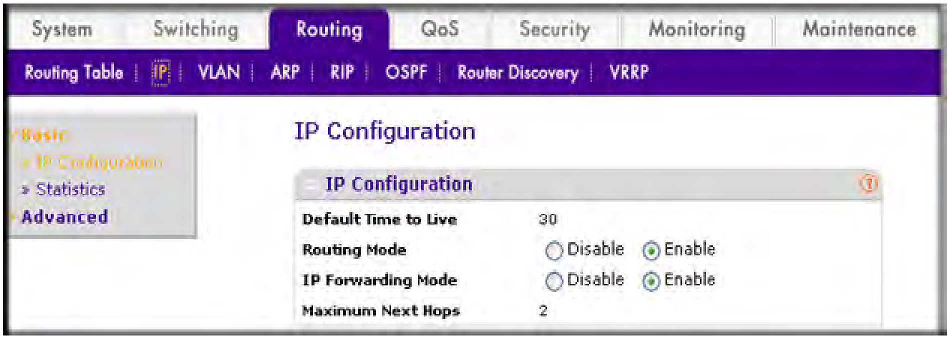
c. Click **Unit 1**. The ports display:

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. From the main menu, 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

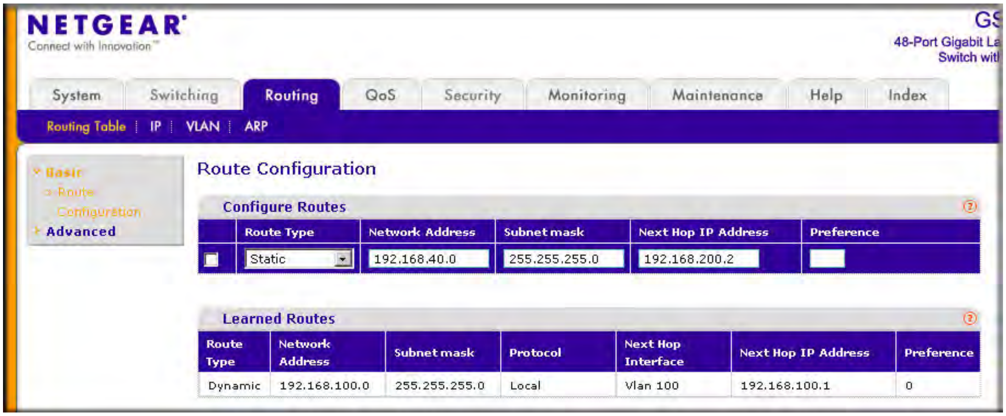
Maximum Next Hops 2

Figure 15-9

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

5. Configure default route for VLAN 202:

- **a.** From the main menu, 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

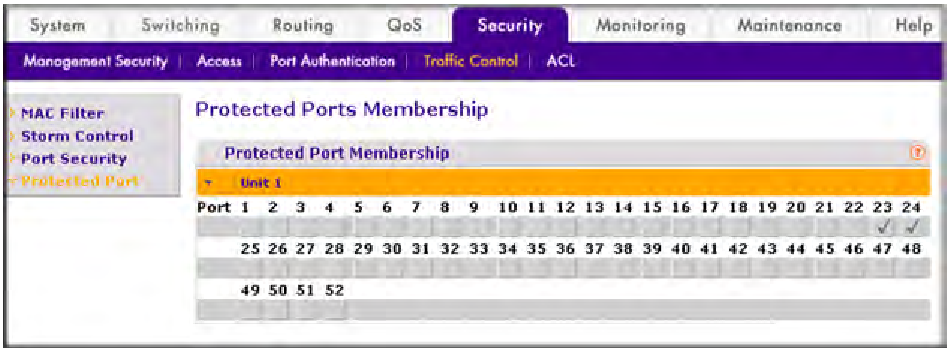
Route Type	Network Address	Subnet mask	Protocol	Next Hop Interface	Next Hop IP Address	Preference
Dynamic	192.168.100.0	255.255.255.0	Local	Vlan 100	192.168.100.1	0

Figure 15-10

- **b.** Under Configure Routes, select **DefaultRoute** in the Route Type field.
- **c.** Under Configure Routes, 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.** From the main menu, select Security > Traffic Control > Protected Port. A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Management Security | Access | Port Authentication | Traffic Control | ACL
MAC Filter
Storm Control
Port Security
Protected Port
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																				

Figure 15-11

b. Under Protected Ports Configuration, Click **Unit 1**. The ports display.
   - Click the gray box under ports 23. A flag appears in the box.
   - Click the gray box under ports 24. A flag appears in the box.

c. Click **Apply** to activate ports 23 and 24 as protected ports.

802.1x Port Security

This section describes how to configure the 802.1x Port Security feature on a switch port. IEEE 802.1x authentication prevents unauthorized clients from connecting to a VLAN unless these clients are authorized by the server.

802.1x Port Security:

- Prevents unauthorized clients from connecting to a VLAN
- Can be configured on a per-port basis

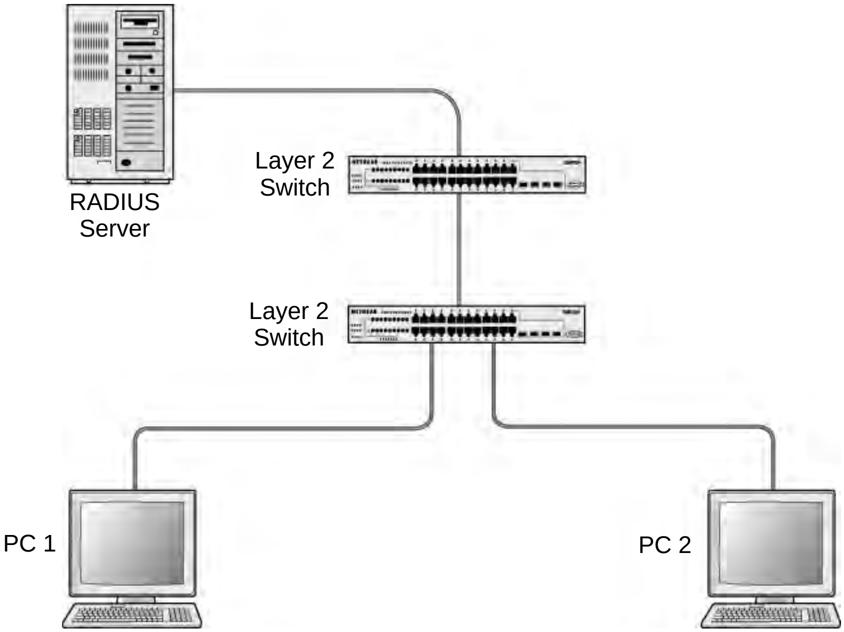


Figure 15-12

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

```
(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
```

Create a username list dot1xList

```
(Netgear Switch) (Config)#aaa authentication dot1x default radius
```

Use radius to authenticate the dot1x users.

```
(Netgear Switch) (Config)#radius server host auth 10.100.5.17
```

To configure a RADIUS authentication server.

```
Netgear Switch) (Config)#radius server key auth 10.100.5.17
Enter secret (16 characters max):123456
Re-enter secret:123456
```

To configure the shared secret between the RADIUS client and the server.

```
(Netgear Switch) (Config)#radius server msgauth 10.100.5.17
(Netgear Switch) (Config)# radius server primary 10.100.5.17
```

To set the RADIUS server as a primary server.

```
(Netgear Switch) (Config)#radius accounting mode
(Netgear Switch) (Config)#radius server host acct 10.100.5.17
```

To configure a accounting server.

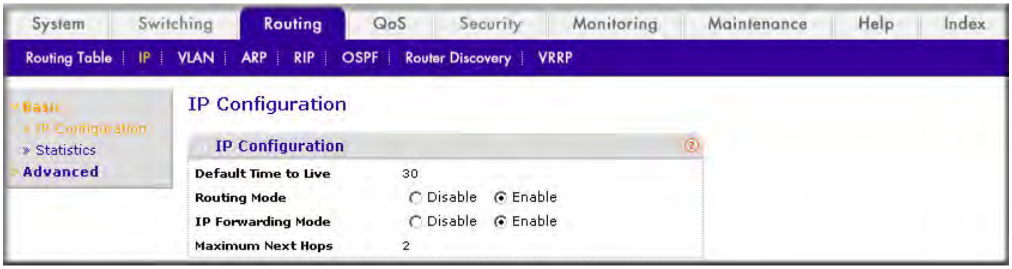
```
(Netgear Switch) (Config)#radius server key acct 10.100.5.17
Enter secret (16 characters max):123456
Re-enter secret:123456
```

To configure the shared secret between the accounting server and the client.

Web Interface: Authenticating dot1x Users by a RADIUS Server

1. Enable routing for the switch.

a. From the main menu, 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

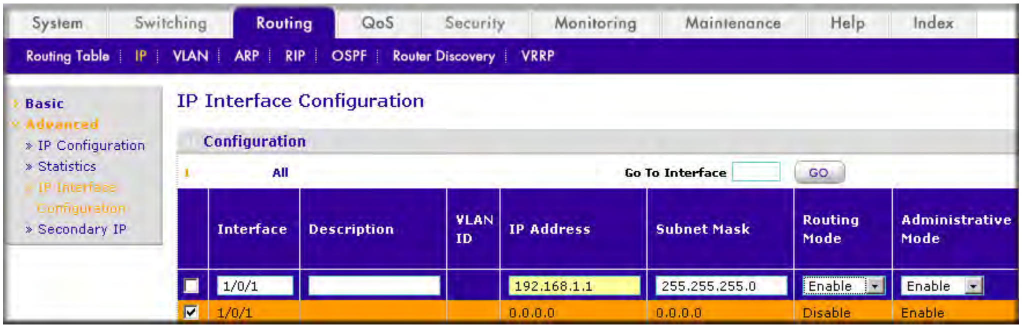
Figure 15-13

b. Next to the 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. From the main menu, select Routing > Advanced >IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

Configuration

	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

Figure 15-14

b. Under IP Interface Configuration, scroll down to interface **1/0/1** and select the checkbox for that interface. Now 1/0/1 appears in the Interface field at the top.

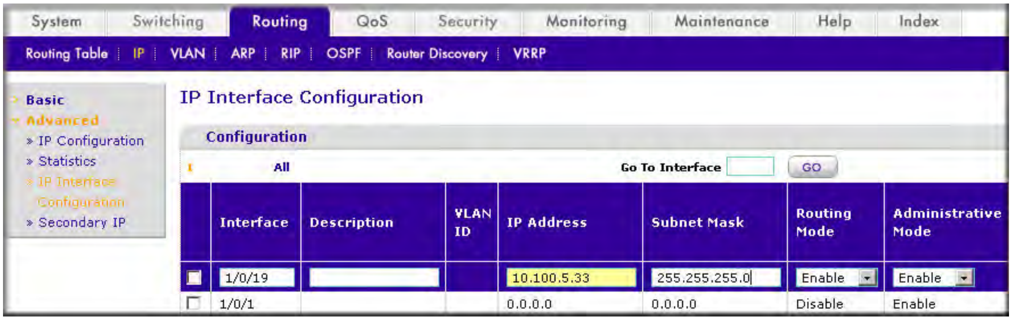
c. Under the IP Interface Configuration, enter the following information.

- Enter **192.168.1.1** in the IP Address field.
- Enter **255.255.255.0** in the Subnet Mask.
- Select **Enable** in the Routing Mode field.

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

3. Assign IP address 10.100.5.33/24 to the interface 1/0/19

a. From the main menu, select Routing > Advanced >IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

Configuration

	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

Figure 15-15

b. Under IP Interface Configuration, scroll down to interface **1/0/19** and select the checkbox for that interface. Nnow 1/0/19appears in the Interface field at the top.

c. Under the IP Interface Configuration, enter the following information.

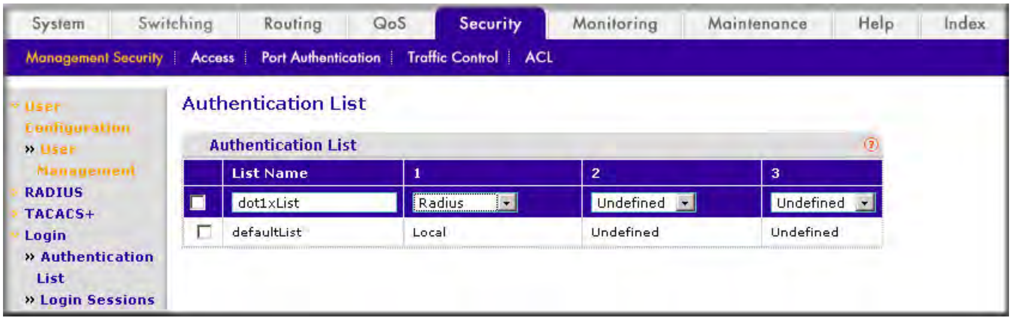
- In the IP Address field, enter **10.100.5.33**.
- In the Subnet Mask, enter **255.255.255.0**.

- Select **Enable** in the Routing Mode field.

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

4. Create an authentication name list.

a. From the main menu, 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

Figure 15-16

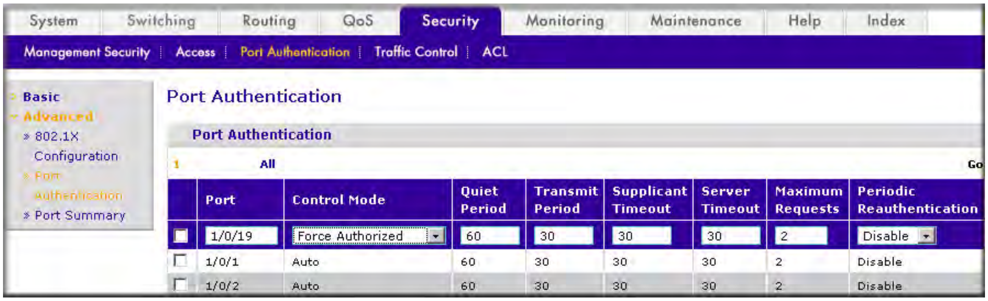
b. Select the checkbox before **dot1xList**.

c. Select **Radius** in the 1 field.

d. Click **Apply**.

5. Set the port 1/0/19 to the Force Authorized mode. (In this case, the Radius server is connected to this interface.)

a. From the main menu, select Security > Port Authentication > Advanced > Port Authentication. A screen similar to the following displays.



Port Authentication

Port Authentication

1 All Go

	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

Figure 15-17

b. Under Port Authentication, scroll down to interface **1/0/19** and select the checkbox for that interface. Now 1/0/19 appears in the Interface field at the top.

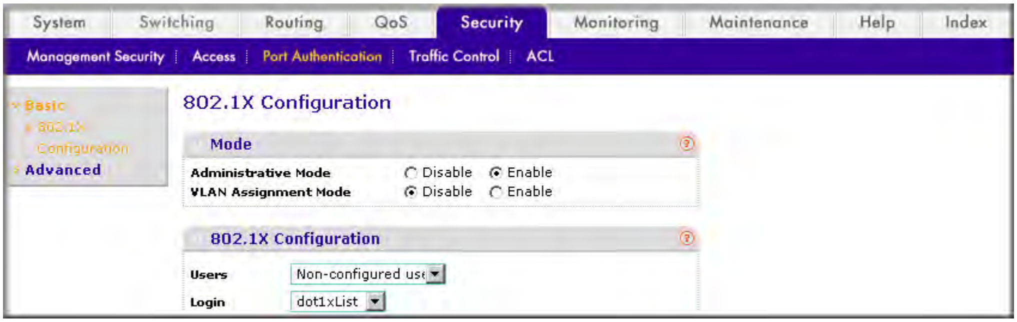
c. Under the Port Authentication, enter the following information.

Select **Force Authorized** in the Control Mode field.

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

6. Enable dot1x on the switch.

a. From the main menu, 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 use
Login	dot1xList

Figure 15-18

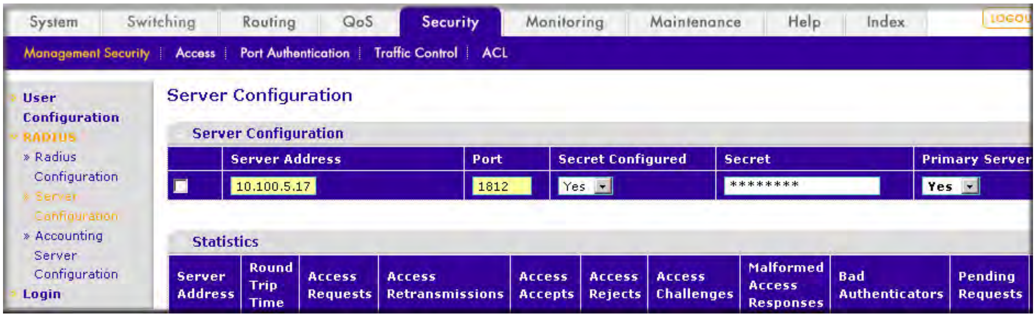
b. Next to the Administrative Mode, select the **Enable** radio button.

c. Select **dot1xList** in the Login field.

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

7. Configure RADIUS authentication server.

a. From the main menu, 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

Figure 15-19

b. In the Server Address, enter **10.100.5.17**.

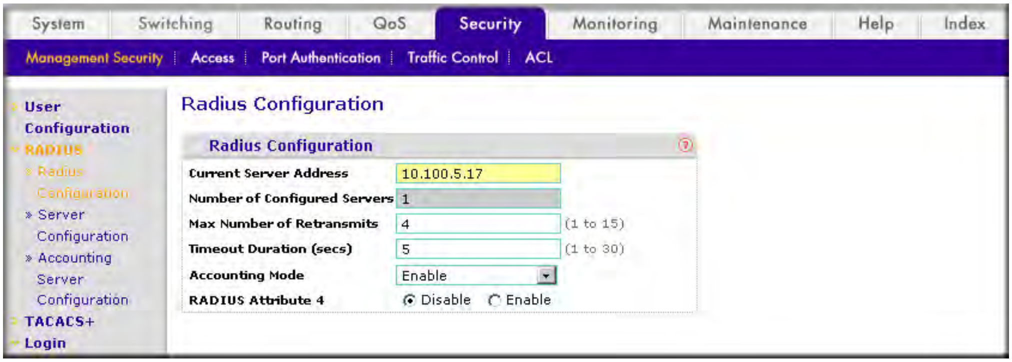
c. Select **Yes** in the Secret Configured field.

d. In the Secret field, enter **123456**.

- **e.** Select **Yes** in the Primary Server field.
- **f.** Select **Enable** in the Message Authenticator field.
- **g.** Click **Add**.

8. Enable Accounting.

- **a.** From the main menu, select Security > Management Security > RADIUS> Radius Configuration. A screen similar to the following displays.



Radius Configuration

Radius Configuration

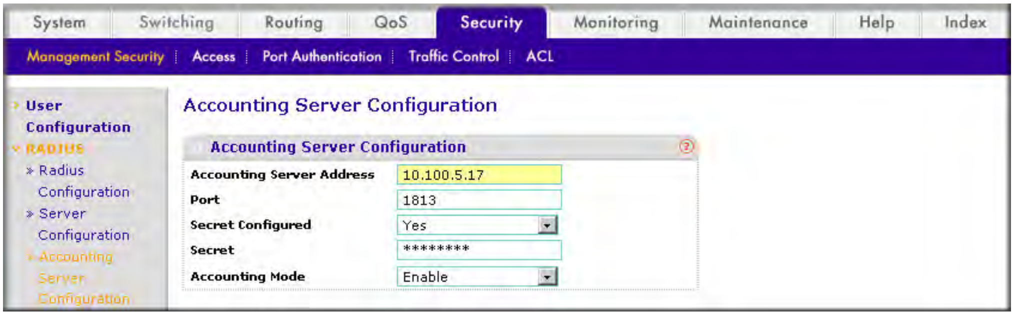
Current Server Address	10.100.5.17	
Number of Configured Servers	1	
Max Number of Retransmits	4	(1 to 15)
Timeout Duration (secs)	5	(1 to 30)
Accounting Mode	Enable	
RADIUS Attribute 4	● Disable ○ Enable	

Figure 15-20

- **b.** In the Server Address, enter **10.100.5.17**.
- **c.** Select **Enable** in the Accounting Mode field.
- **d.** Click the **Apply**.

9. Configure accounting server.

- **a.** From the main menu, 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

Figure 15-21

- **b.** In the Accounting Server Address, enter **10.100.5.17**.

c. Select **Enable** in the Accounting Mode field.

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 external network with no ability to surf internal LAN.

For a port in port-based mode,when a client that does not support 802.1X is connected to an unauthorized port that is 802.1X enabled. Then the client does not respond to the 802.1X requests from the switch ,and the port would remain in the unauthorized state, and the client is not granted access to the network. If the guest VLAN was configured for that port then the port is placed in the configured guest VLAN and the port is moved to 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..

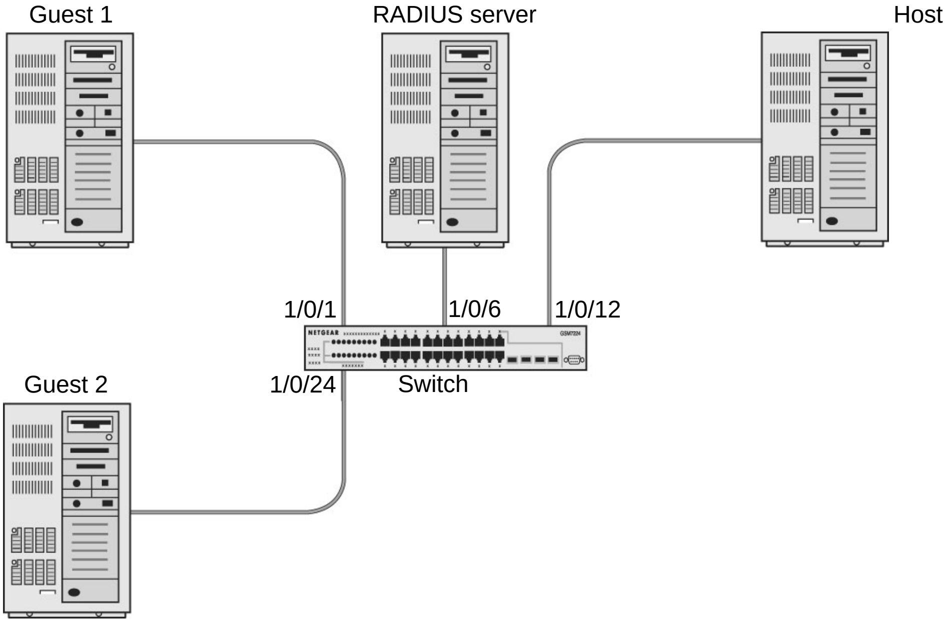


Figure 15-22

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 VLAN 1. On the port 1/0/1 and 1/0/24 , guest vlan is enabled. If guests connect to the port, they will be assigned VLAN 2000. So that guests cannot access the internal VLAN but can access each other in the guest VLAN

CLI: Creating a Guest VLAN

```
(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
```

Create a VLAN 2000 and have 1/0/1 and 1/0/24 being the member 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
```

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
```

Enable guest vlan on port 1/0/1 and 1/0/24.

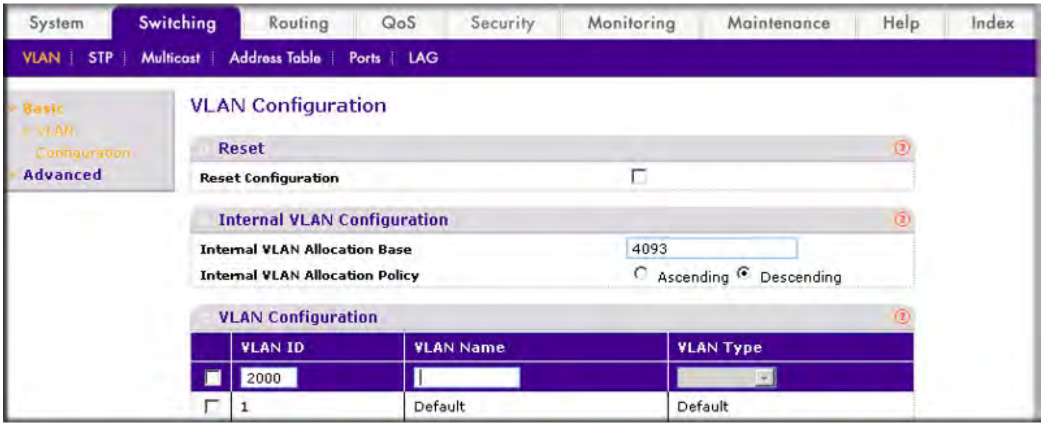
```
(Netgear Switch) #show dot1x detail 1/0/1
Protocol Version............................... 1
PAE Capabilities............................... Authenticator
Control Mode................................... auto
Authenticator PAE State........................ Authenticated
Backend Authentication State................... 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: Creating a Guest VLAN

To use the Web interface to create a guest VLAN, proceed as follows:

1. Create VLAN 2000.

   a. From the main menu, 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

Figure 15-23

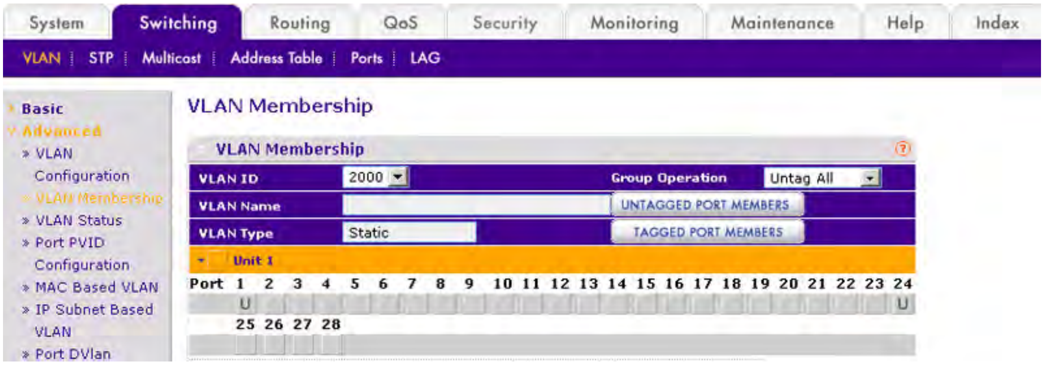
b. In the VLAN ID field, enter **2000**.

c. Select **Static** in the VLAN Ty**pe** field.

d. Click **Add**.

2. Add ports to the VLAN 2000.

a. From the main menu, 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																				

Figure 15-24

b. Select **2000** in the **VLAN ID** field.

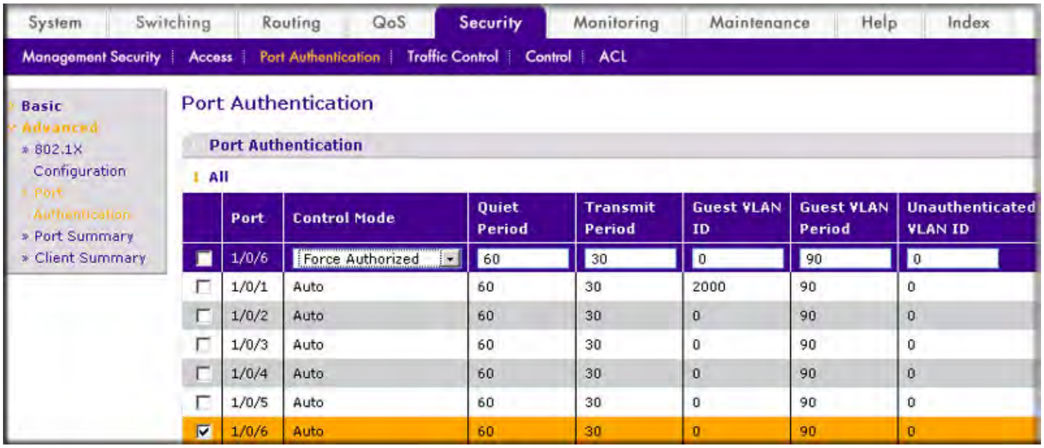
c. Click the Unit 1. The Ports display.

d. Click the gray box under port 1 and 24 until U displays. The U specifies that the egress packet is untagged for the port.

e. Click **Apply**.

3. Setting force authorized mode on the port 1/0/6 and 1/0/12.

a. From the main menu, 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

Figure 15-25

b. Under Port Authentication, scroll down to interface 1/0/6 and 1/0/12, select the checkbox for that interface.

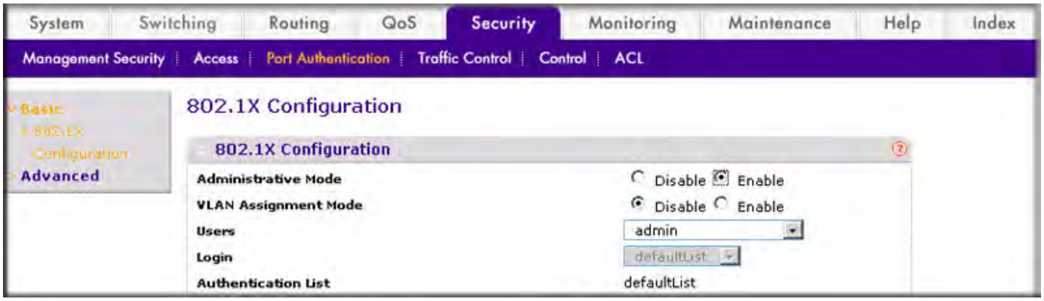
c. Under the Port Authentication, select **Force Authorized** in the Control Mode field.

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

4. Enable dot1x on the switch.

Make sure 1/0/12 and 1/0/6 are configured as force authorized before you do this step, otherwise you cannot access the switch through GUI.

a. From the main menu, 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

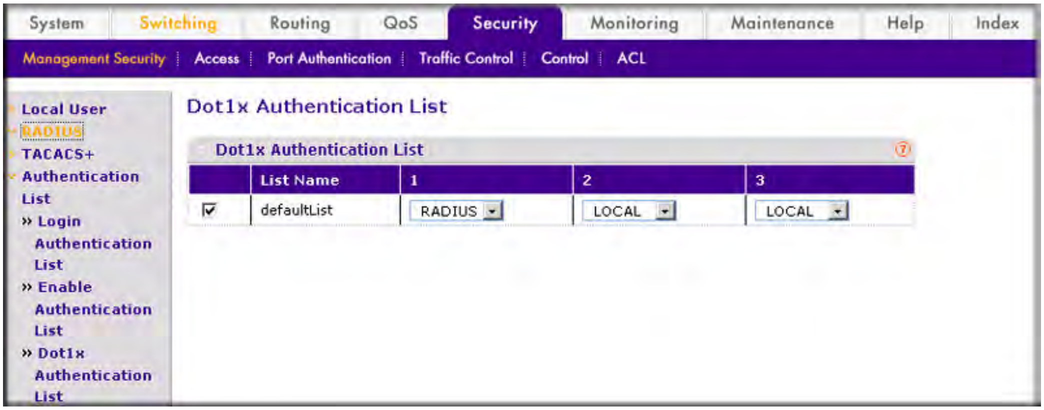
Figure 15-26

b. Next to the Administrative Mode, select the Enable radio button.

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

5. Configure dot1x authentication list.

a. From the main menu, 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

Figure 15-27

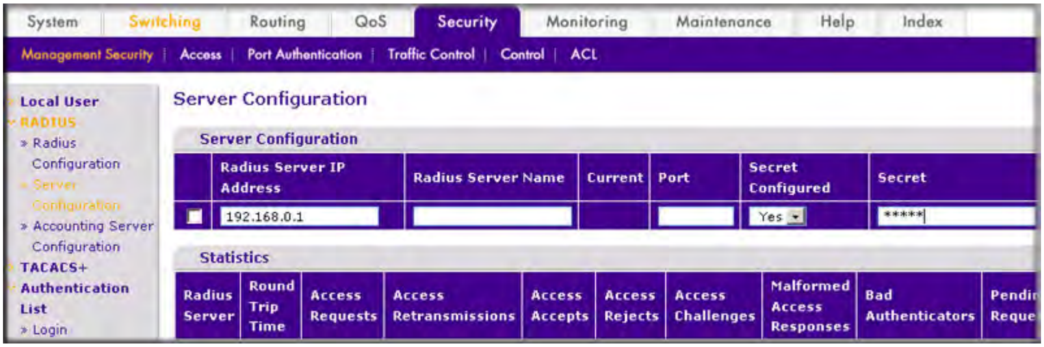
b. Select the **defaultLis**t checkbox.

c. Select **RADIUS** in the 1 field.

d. Click **Add**.

6. Configure the RADIUS authentication server.

a. From the main menu, 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

Figure 15-28

b. In the Radius Server IP Address field, enter **192.168.0.1**.

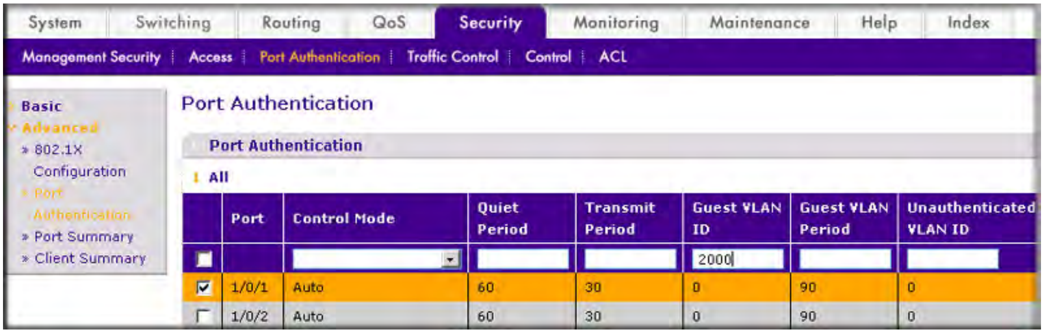
c. Select **Yes** in the Secret Configured field.

d. In the Secret field, enter **12345**.

e. Click **Add**.

7. Configure the Guest VLAN.

a. From the main menu, 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
□					2000		
☑	1/0/1	Auto	60	30	0	90	0
□	1/0/2	Auto	60	30	0	90	0

Figure 15-29

b. Under Port Authentication, scroll down to interface 1/0/1 and 1/0/24, select the checkbox for that interface.

c. Under the Port Authentication, in the **Guest VLAN ID** field, enter **2000**.

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

VLAN Assignment via RADIUS

This feature implies that the client can connect from any port and can get assigned to the appropriate VLAN that it is supposed to be in, this is configured in the RADIUS server. This gives flexibility for the clients to move around the network without requiring the administrator to do much 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.

- If any client initiates dot1x authentication again on the port after the port being in authorized state, then the port clears all first authenticated clients states, and in the process clears the VLAN assigned to the port (if any) and 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.

- If the VLAN assignment is enabled in the RADIUS server then as part of the response message the RADIUS server sends the VLAN id the client is supposed to be in the 802.1x tunnel attributes. This attribute indicates the tunneling protocol to be used or the tunneling protocol in use at the authenticator. The RADIUS server typically indicates the desired VLAN by including tunnel attributes within the Access-Accept. However, the IEEE 802.1X Authenticator may also provide a hint as to the VLAN to be assigned to the Supplicant by including Tunnel attributes within the Access-Request.

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, taking a value between 1 and 4094.

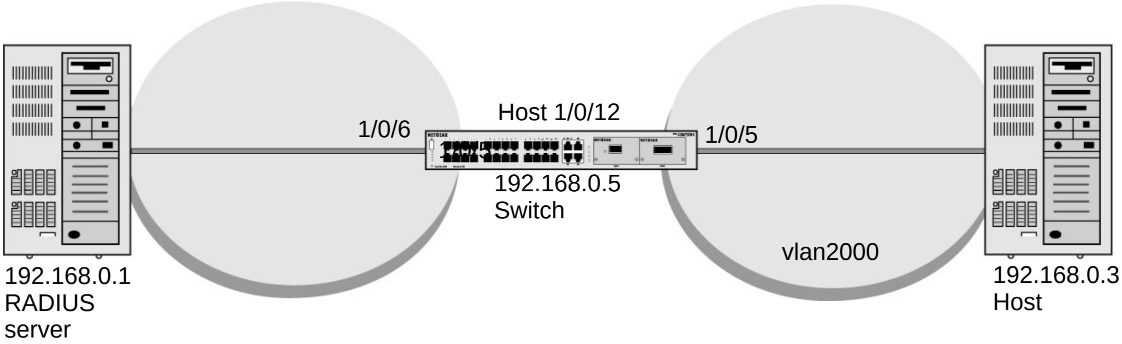


Figure 15-30

In the diagram above, the switch has placed the host in the VLAN (vlan2000) based on the user details of the clients.

Configuration on RADIUS Server

For user (e.g. admin):

- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=2000

CLI: Configuration on the Switch

```
(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
```

Create a VLAN 2000.

```
(Netgear Switch) (Config)#dot1x system-auth-control
```

Enable dot1x authentication on the switch.

```
(Netgear Switch) (Config)#aaa authentication dot1x default radius
```

Use the radius as the authenticator.

```
(Netgear Switch) (Config)#authorization network radius
```

Enable the switch to accept VLAN assignment by the radius server.

```
(Netgear Switch) (Config)#radius server host auth 192.168.0.1
```

Set the Radius server IP address.

```
(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
```

Set the NAS-IP address for 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
```

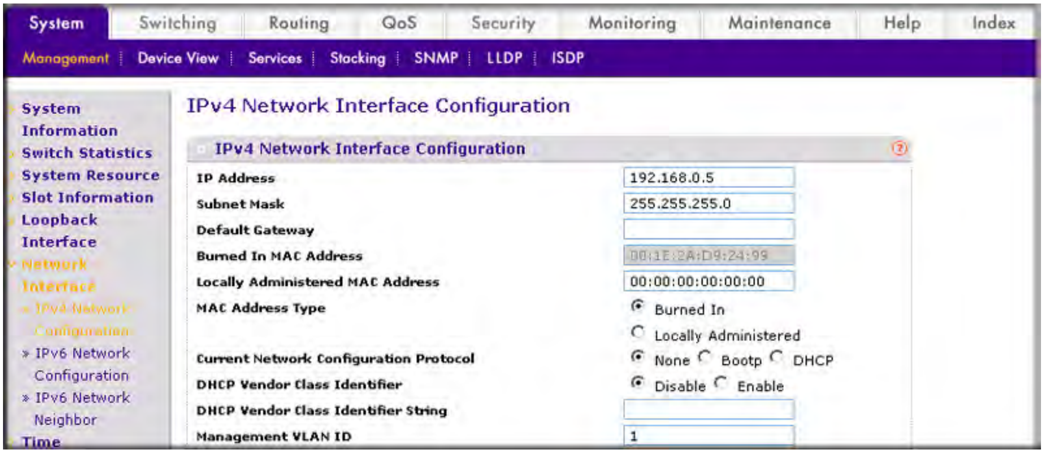
Force the 1/0/6 to be authorized for it connects to the RADIUS server.

```
(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 : VLAN Assignment via RADIUS

To use the Web interface to do VLAN assignment via RADIUS, proceed as follows:

1. Assign IP address for management interface.
   a. From the main menu, 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

Figure 15-31

b. Next to the **Current Network Configuration Protocol**, select the **None** Radio button.

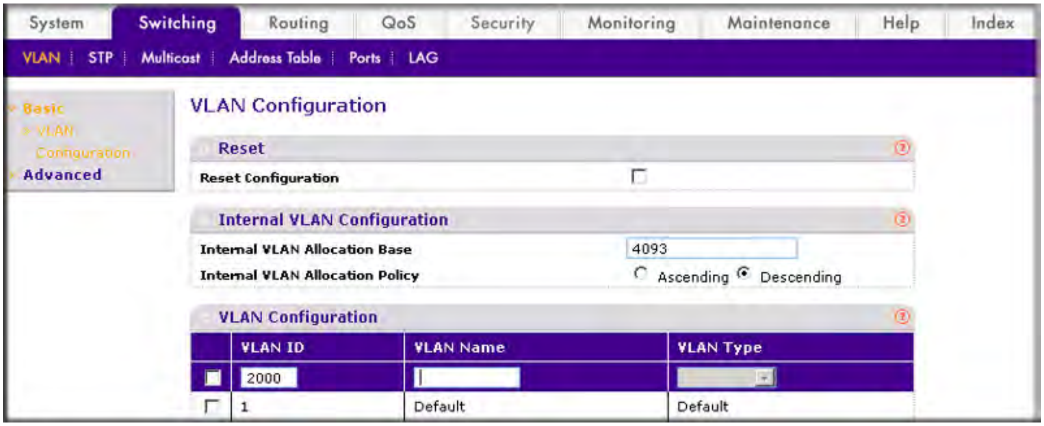
c. In the **IP Address**, enter **192.168.0.5**.

d. In the **Subnet Mask**, enter **255.255.255.0**.

e. Click **Apply**.

2. Create VLAN 2000.

a. From the main menu, 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

Figure 15-32

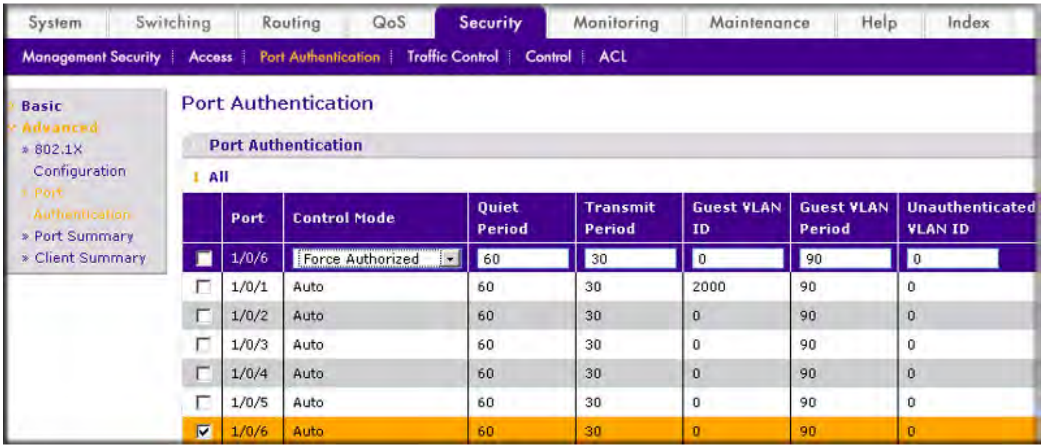
b. In the VLAN ID field, enter **2000**.

c. Select **Static** in the VLAN Type field.

d. Click **Add**.

3. Setting force authorized mode on the port 1/0/6 and 1/0/12.

a. From the main menu, 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

Figure 15-33

b. Under Port Authentication, scroll down to interface 1/0/6 and 1/0/12, select the checkbox for that interface.

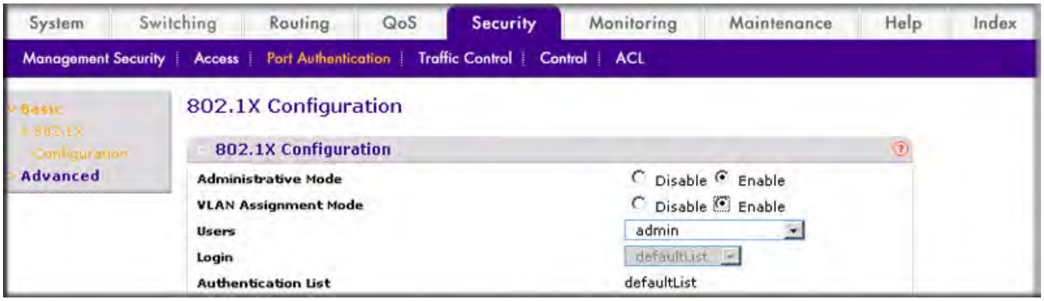
c. Under Port Authentication, select **Force Authorized** in the Control Mode field.

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

4. Enable dot1x on the switch.

Make sure 1/0/12 and 1/0/6 is configured as force authorized before you do this step, otherwise you cannot access the switch through GUI.

a. From the main menu, 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

Figure 15-34

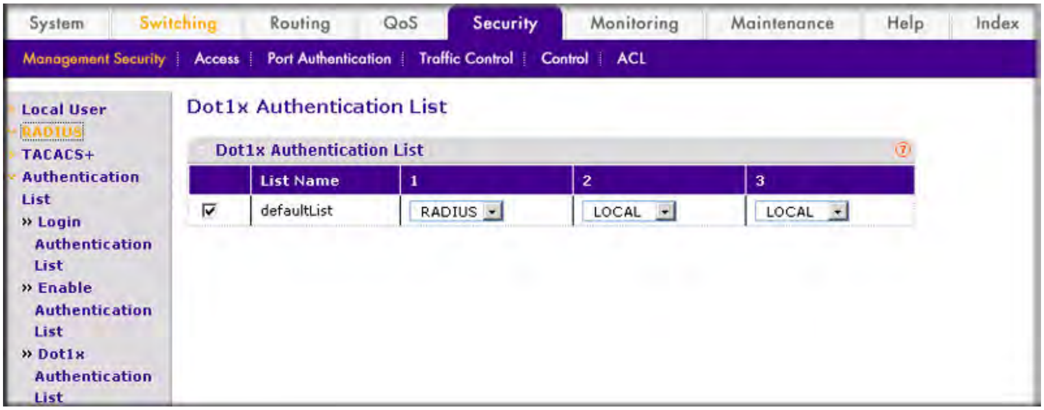
b. Next to the Administrative Mode, select the **Enable** radio button.

c. Next to the VLAN Assignment Mode, select the **Enable** radio button.

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

5. Configure dot1x authentication list.

a. From the main menu, 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

Figure 15-35

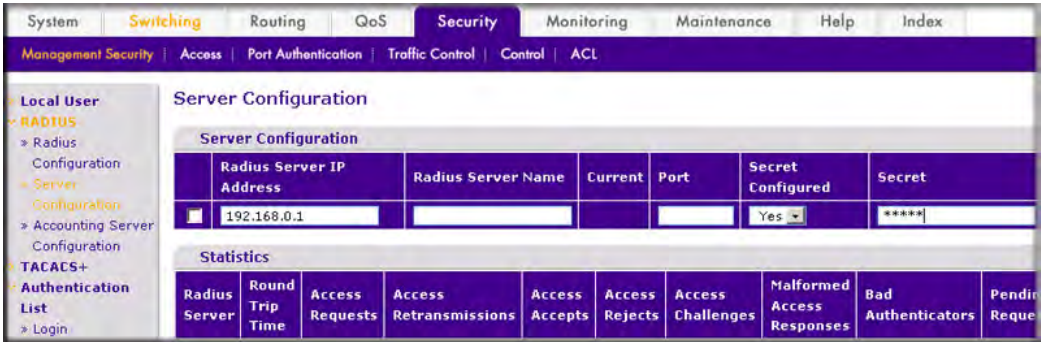
b. Select the check box before **defaultList**.

c. Select **RADIUS** in the 1 field.

d. Click **Add**.

6. Configure RADIUS authentication server.

a. From the main menu, 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

Figure 15-36

b. In the Radius Server IP Address field, enter **192.168.0.1**.

c. Select **Yes** in the Secret Configured field.

d. In the Secret field, enter **12345**.

e. Click **Add**.

Dynamic ARP Inspection

Dynamic ARP Inspect (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 stations's IP address to its own MAC address.

Dynamic ARP Inspection relies on DHCP Snooping DHCP Snooping listens to DHCP message exchanges and builds a bindings database of valid (MAC address, IP address, vlan interface) tuples.

When Dynamic ARP Inspection is enabled, the switch drops ARP packet whose 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.

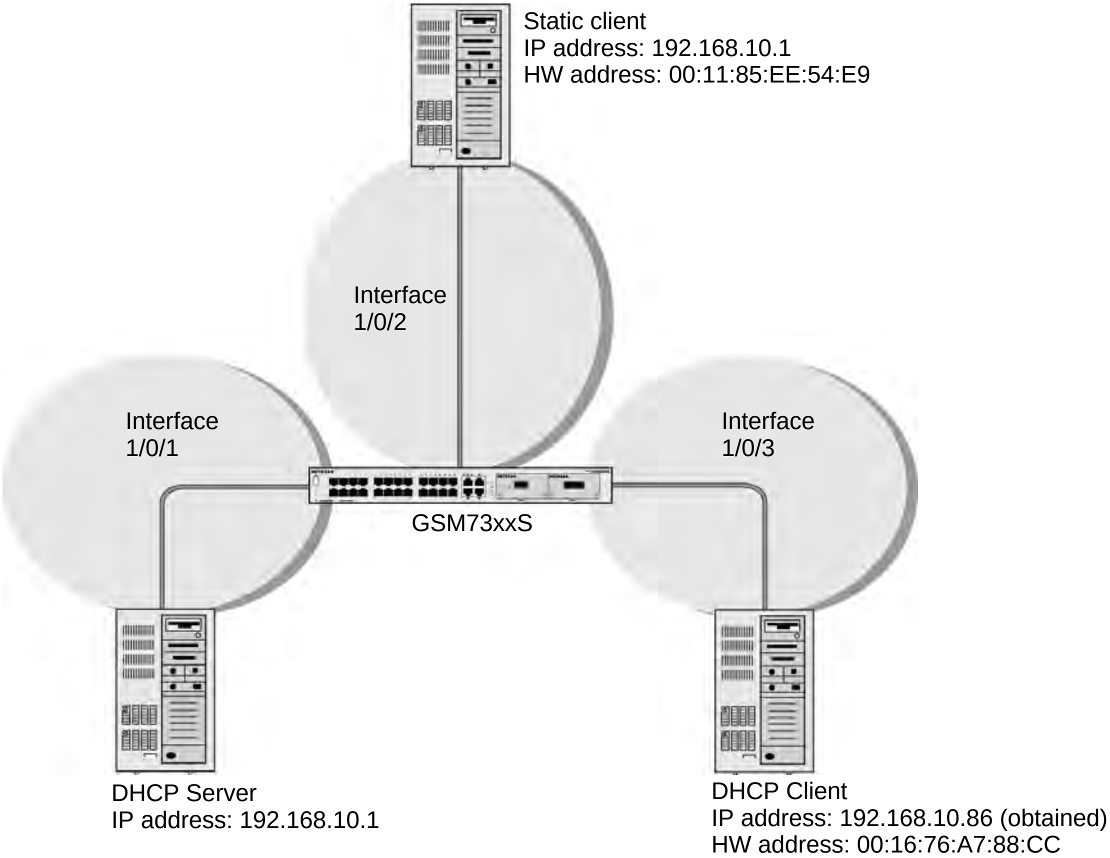


Figure 15-37

This script in this section shows how to configure Dynamic ARP Inspection.

CLI: Dynamic ARP Inspection

Enable DHCP snooping globally.

```
(Netgear Switch) (Config)# ip dhcp snooping
```

Enable DHCP snooping in a VLAN.

```
(Netgear Switch) (Config)# ip dhcp snooping vlan 1
```

Configure the port through which DHCP server is reached as trusted.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip dhcp snooping trust
```

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
```

Enable ARP Inspection in the VLAN 1.

```
(Netgear Switch) (Config)# ip arp inspection vlan 1
```

Now all the ARP packets received on the ports that are member of VLAN are copied to CPU for ARP inspection. If there are trusted ports, it can configured as trusted port as in the next step. ARP packets received on the trusted ports are not copied to the CPU.

Configure a port 1/0/1 as trusted.

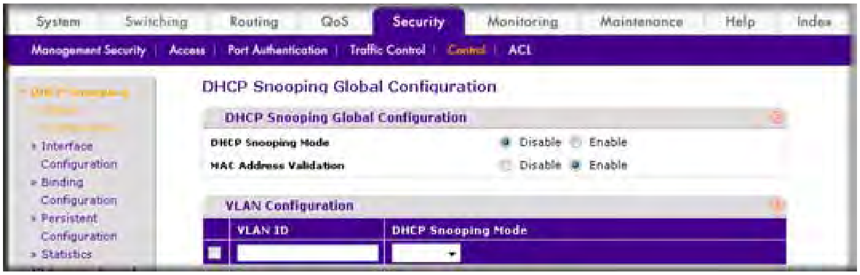
```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip arp inspection trust
```

Now ARP packets from the DHCP client will be through since it has DHCP snooping entry, however ARP packets from the static client is dropped, since it does have a DHCP snooping entry. It can be over come by static configuration as described in the "Configuring Static Mapping" on page 15-41.

Web Interface: Dynamic ARP Inspection

1. Enable DHCP snooping globally.

a. From the main menu, 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
□		

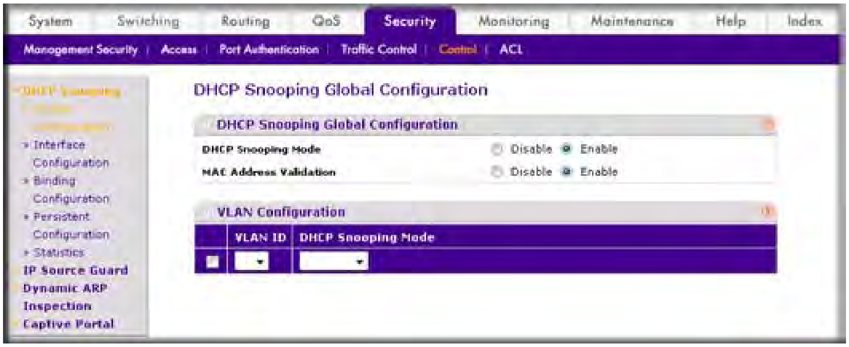
Figure 15-38

b. For the DHCP Snooping Mode, select **Enable**.

c. Click **Apply**. At the end of this configuration a screen similar toFigure 15-38 displays.

2. Enable DHCP snooping in a VLAN.

a. From the main menu, 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

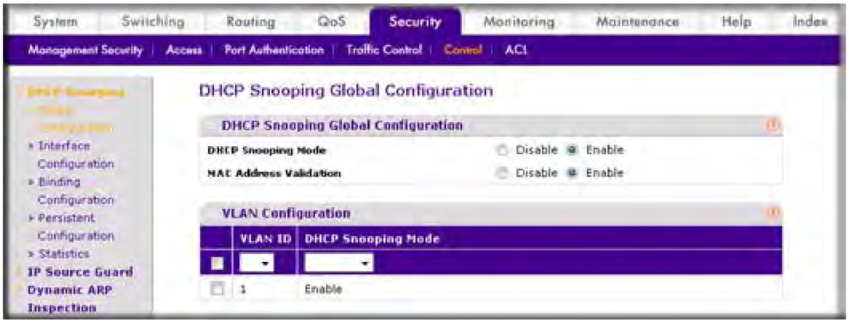
VLAN Configuration

	VLAN ID	DHCP Snooping Mode
□		

Figure 15-39

b. In the VLAN Configuration table, set the VLAN ID as **1**.

c. In the VLAN Configuration table, set DHCP Snooping Mode as **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

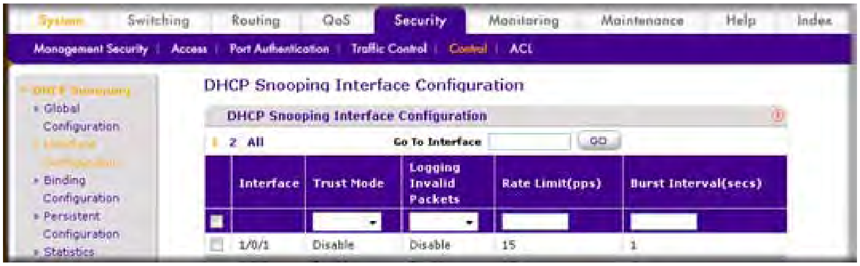
VLAN Configuration

	VLAN ID	DHCP Snooping Mode
□		
□	1	Enable

Figure 15-40

3. Configure the port through which DHCP server is reached as trusted. Here Interface 1/0/1 is trusted.

a. From the main menu, 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

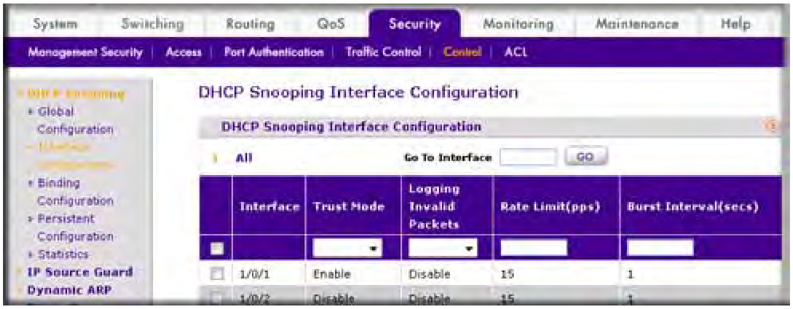
	Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pps)	Burst Interval(secs)
□					
□	1/0/1	Disable	Disable	15	1

Figure 15-41

b. Select the checkbox for Interface **1/0/1**.

c. Set the Trust Mode as **Enable** for Interface 1/0/1.

d. Click **Apply**. At the end of this configuration a screen similar to the following displays.



DHCP Snooping Interface Configuration

DHCP Snooping Interface Configuration

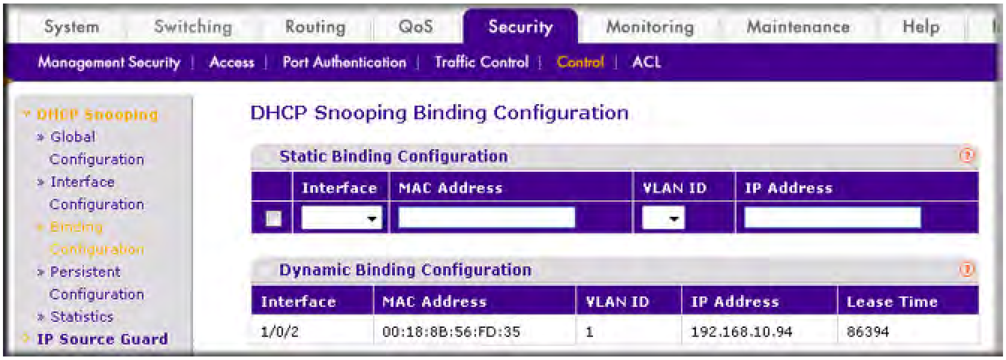
All　Go To Interface

	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

Figure 15-42

4. View the DHCP Snooping Binding table.

a. From the main menu, 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
□				

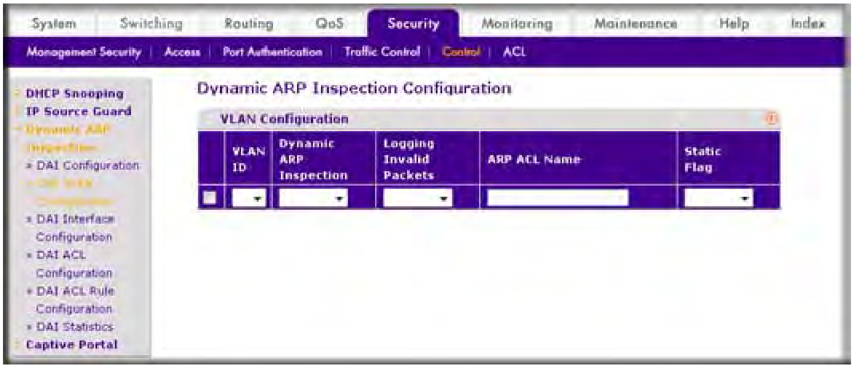
Dynamic Binding Configuration

Interface	MAC Address	VLAN ID	IP Address	Lease Time
1/0/2	00:18:8B:56:FD:35	1	192.168.10.94	86394

Figure 15-43

5. Enable ARP Inspection in the VLAN 1.

a. From the main menu, select Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration. A screen similar to the following displays.



Dynamic ARP Inspection Configuration

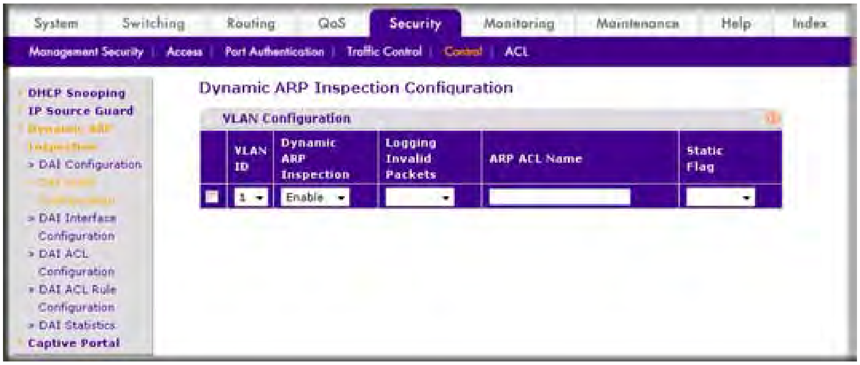
VLAN Configuration

	VLAN ID	Dynamic ARP Inspection	Logging Invalid Packets	ARP ACL Name	Static Flag
□					

Figure 15-44

b. Set the VLAN ID as **1**.

c. Set the Dynamic ARP Inspection field as **Enable**. A screen similar to the following displays.



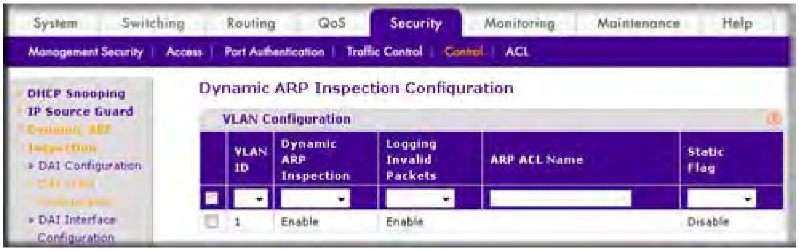
Dynamic ARP Inspection Configuration

VLAN Configuration

	VLAN ID	Dynamic ARP Inspection	Logging Invalid Packets	ARP ACL Name	Static Flag
□	1	Enable			

Figure 15-45

d. Click **Apply**. At the end of this 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
☐					
☐	1	Enable	Enable		Disable

Figure 15-46

Now all the ARP packets received on the ports that are member of VLAN are copied to CPU for ARP inspection. If there are trusted ports, it can configured as trusted port as 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 accessing the device through the trusted port for ARP. Otherwise you may get disconnected from the device.

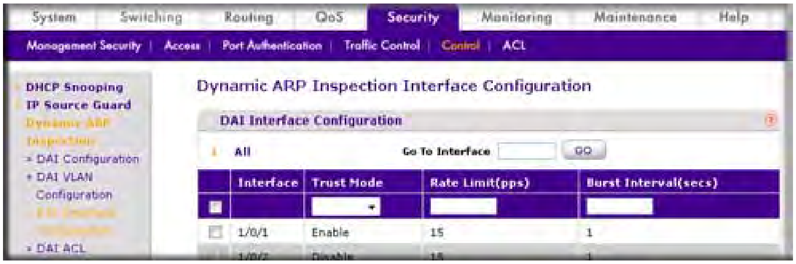
6. Configure a port 1/0/1 as trusted.

a. From the main menu, select Security > Control > Dynamic ARP Inspection > DAI Interface Configuration.

b. Select the checkbox for Interface **1/0/1**.

c. Set the Trust Mode as **Enable**.

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



Dynamic ARP Inspection Interface Configuration

DAI Interface Configuration

All   Go To Interface

	Interface	Trust Mode	Rate Limit(pps)	Burst Interval(secs)
☐				
☐	1/0/1	Enable	15	1
	1/0/2	Disable	15	1

Figure 15-47

Now ARP packets from the DHCP client will be through since it has DHCP snooping entry, however ARP packets from the static client is dropped, since it does have a DHCP snooping entry. It can be over come by static configuration as described in “Configuring Static Mapping” on page 15-41.

Configuring Static Mapping

This script in this section shows how to configure static mapping.

CLI: Configuring Static Mapping

Create an ARP ACL.

```
(Netgear Switch) (Config)# arp access-list ArpFilter
```

Configure 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
```

Configure ARP ACL used for the VLAN 1.

```
(Netgear Switch) (Config)# ip arp inspection filter ArpFilter vlan 1
```

Now the ARP packets from the Static client will be through since it has an entry in the ARP ACL ARP packets from the DHCP client is also through since it has DHCP snooping entry.

This command can have the optional static key word. If the static key word is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings. That is in this example, ARP packets from the DHCP client are dropped since it does not have a matching rule through it has a DHCP snooping entry.

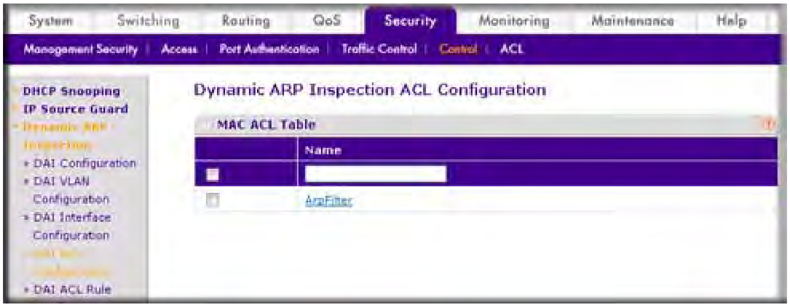
Web Interface: Configuring Static Mapping

1. Create an ARP ACL.

   a. From the main menu, select Security > Control > Dynamic ARP Inspection > DAI ACL Configuration.

   b. Enter the Name as **ArpFilter**.

c. Click **Add**. At the end of this configuration a screen similar to the following displays.



Dynamic ARP Inspection ACL Configuration

MAC ACL Table

	Name
□	
□	ArpFilter

Figure 15-48

2. Configure a rule to allow the static client.

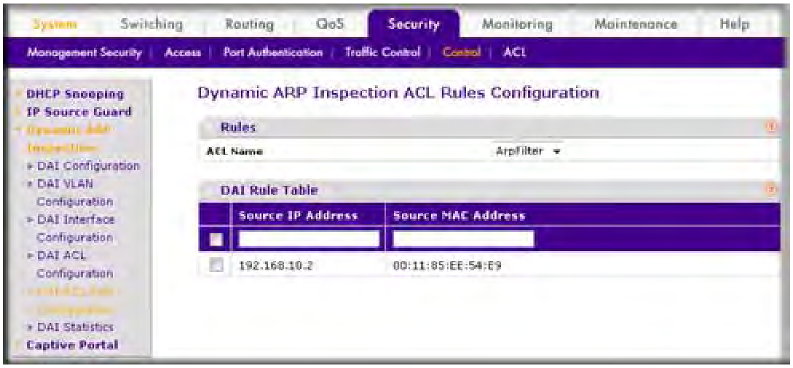
   a. From the main menu, select Security > Control > Dynamic ARP Inspection > DAI ACL Rule Configuration.

   b. Select ACL Name as **ArpFilter**.

   c. Enter Source IP Address as **192.168.10.2**.

   d. Enter the Source MAC Address as **00:11:85:EE:54:E9**.

   e. Click **Add**. At the end of this configuration 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

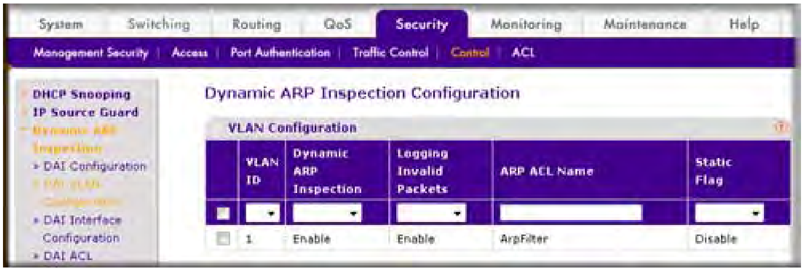
Figure 15-49

3. Configure ARP ACL used for the VLAN 1.

   a. From the main menu, select Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration.

   b. Enter ARP ACL Name as **ArpFilter**.

c. Click **Apply**. At the end of this 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
□					
□	1	Enable	Enable	ArpFilter	Disable

Figure 15-50

DHCP Snooping

DHCP Snooping is a security feature that monitors DHCP messages between a DHCP clinet 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 specifici VLAN’s and configures ports withing the VLAN to be trusted or untrusted. DHCP servers must be reached through trusted ports.

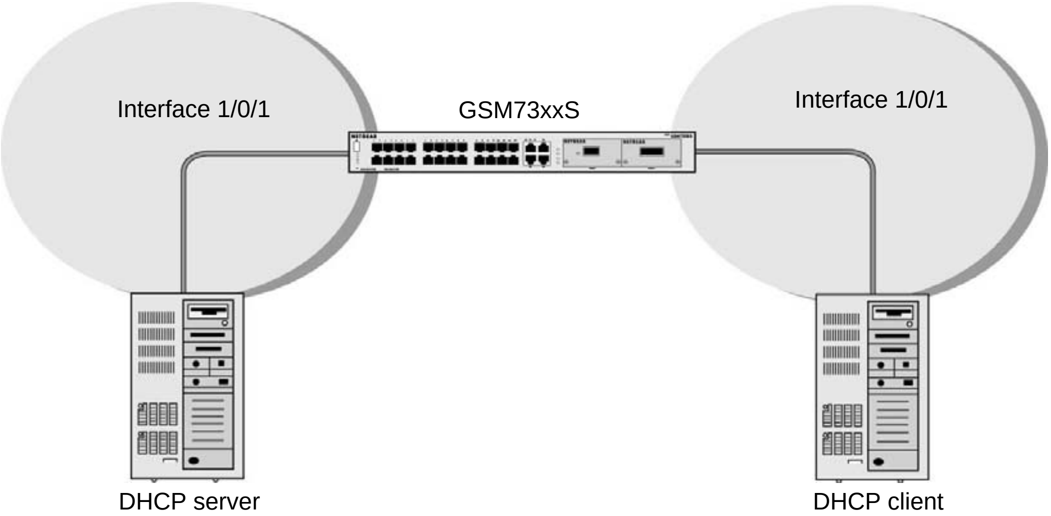


Figure 15-51

This script in this section shows how to configure DHCP Snooping.

CLI: Configuring DHCP Snooping

Enable DHCP snooping globally.

```
(Netgear Switch) (Config)# ip dhcp snooping
```

Enable DHCP snooping in a VLAN.

```
(Netgear Switch) (Config)# ip dhcp snooping vlan 1
```

Configure the port through which DHCP server is reached as trusted.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip dhcp snooping trust
```

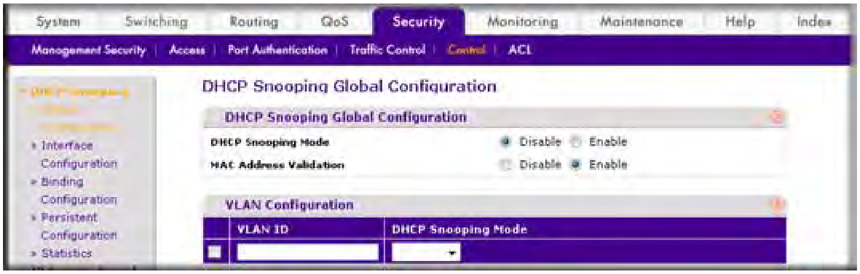
View the DHCP Snooping Binding table.

```
(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: Configuring DHCP Snooping

1. Enable DHCP snooping globally

   a. From the main menu, 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
□		

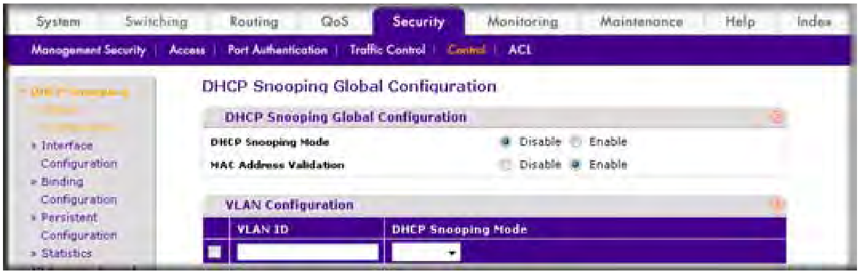
Figure 15-52

   b. Select DHCP Snooping Mode as **Enable**.

c. Click **Apply**. A screen similar to the one in Figure 15-53 displays.

2. Enable DHCP snooping in a VLAN.

a. From the main menu, select Security > Control > DHCP Snooping Global 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
» Interface Configuration
» Binding Configuration
» Persistent Configuration
» Statistics

DHCP Snooping Global Configuration

DHCP Snooping Global Configuration

DHCP Snooping Mode ● Disable ○ Enable

MAC Address Validation ○ Disable ● Enable

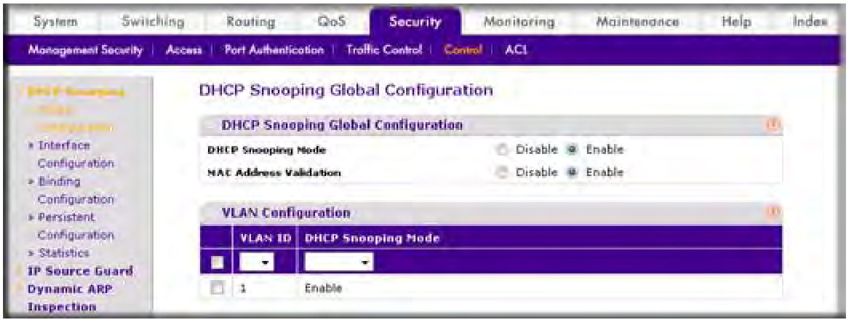
VLAN Configuration

	VLAN ID	DHCP Snooping Mode
□		

Figure 15-53

b. In the VLAN Configuration table, select VLAN ID as **1**.

c. In the VLAN Configuration table, set DHCP Snooping Mode as **Enabled**. 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
» Interface Configuration
» Binding Configuration
» Persistent Configuration
» Statistics
IP Source Guard
Dynamic ARP Inspection

DHCP Snooping Global Configuration

DHCP Snooping Global Configuration

DHCP Snooping Mode ○ Disable ● Enable

MAC Address Validation ○ Disable ● Enable

VLAN Configuration

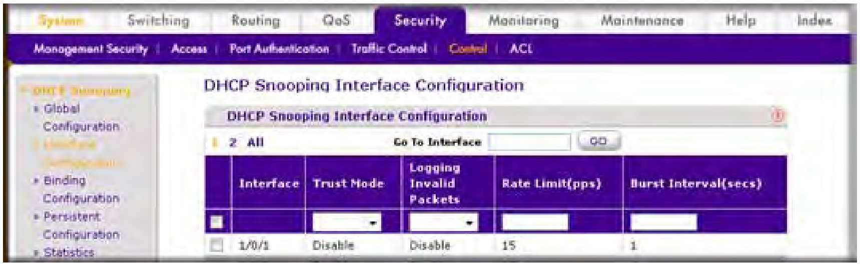
	VLAN ID	DHCP Snooping Mode
□		
□	1	Enable

Figure 15-54

d. Click **Apply**.

3. Configure the port through which DHCP server is reached as trusted.

a. From the main menu, 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

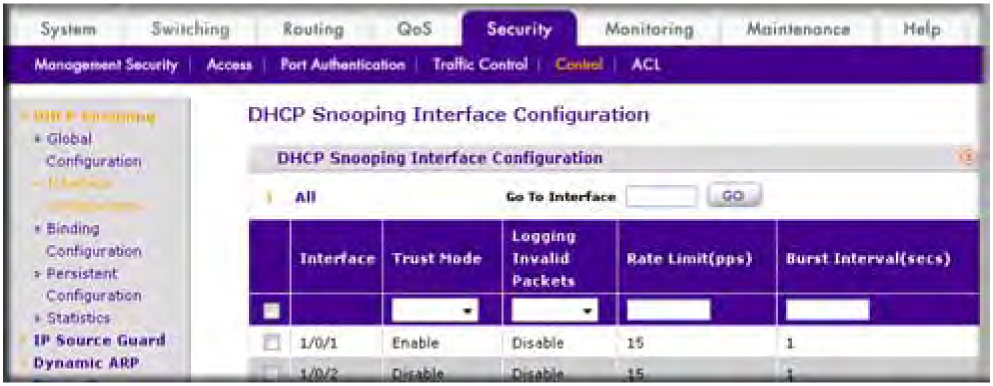
	Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pps)	Burst Interval(secs)
□					
□	1/0/1	Disable	Disable	15	1

Figure 15-55

b. Select the checkbox for Interface **1/0/1**.

c. Select Trust Mode as **Enable** for Interface 1/0/1.

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



DHCP Snooping Interface Configuration

DHCP Snooping Interface Configuration

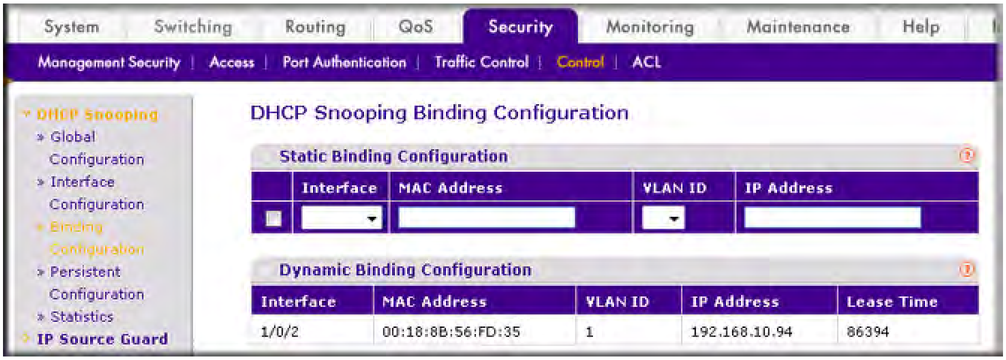
1 All   Go To Interface

	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

Figure 15-56

4. View the DHCP Snooping Binding table.

From the main menu, 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

Figure 15-57

Enter Static Binding into the Binding Database

The administrator can also enter the static binding into the binding database. This script in this section shows how to enter the static binding in the binding database.

CLI: Entering Static Binding into the Binding Database

DHCP Snooping Static Entry.

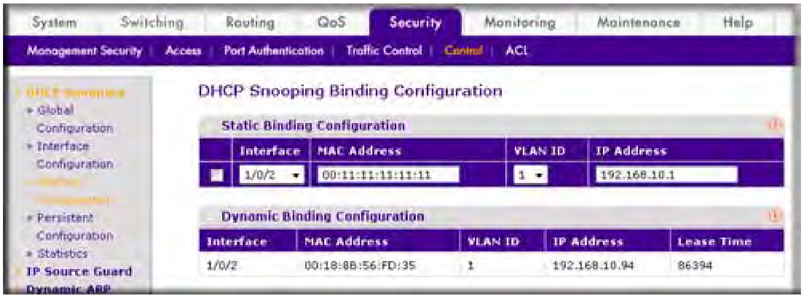
```
(Netgear Switch) (Config)# ip dhcp snooping binding 00:11:11:11:11:11
vlan 1 192.168.10 .1 interface 1/0/2
```

View 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: Entering Static Binding into the Binding Database

1. DHCP Snooping Static Entry.



DHCP Snooping Binding Configuration

Static Binding Configuration

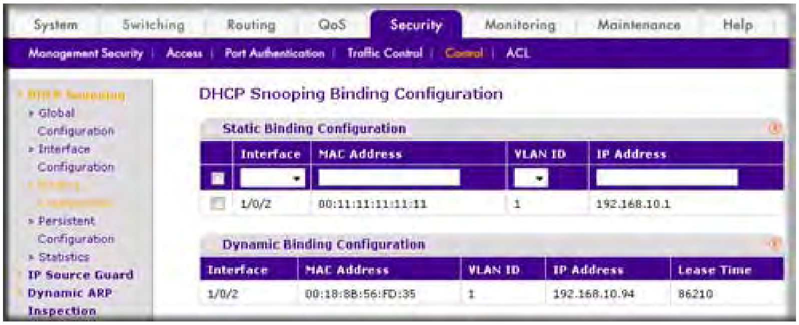
	Interface	MAC Address	VLAN ID	IP Address
□	1/0/2	00:11:11:11:11:11	1	192.168.10.1

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

Figure 15-58

2. View the binding database has the static entry.



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

Figure 15-59

Configure the Maximum Rate of DHCP Messages

To prevent DHCP packets being used as a DoS attach when DHCP snooping is enabled the snooping application enforces a rate limit for DHCP packets received on untrusted interface. DHCP snooping monitors the receive rate on each interface separately. If the receive rate exceeds a configurable limit, DHCP snooping brings down the interface. The user must do “no shutdown” on this interface to further work with that port.

CLI: Configuring the Maximum Rate of DHCP Messages

Control the maximum rate of DHCP messages.

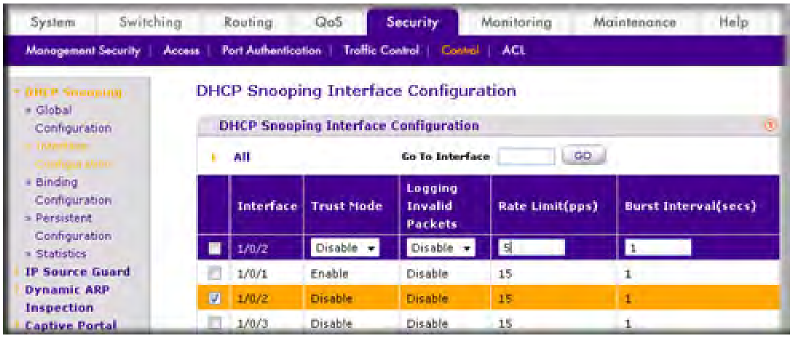
```
(Netgear Switch) (Interface 1/0/2)# ip dhcp snooping limit rate 5
```

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: Configuring the Maxiumum Rate of DHCP Messages

1. Control the maximum rate of DHCP messages.



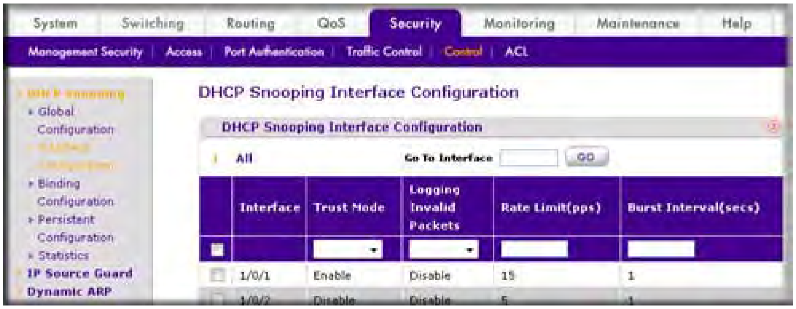
DHCP Snooping Interface Configuration

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

Figure 15-60

2. View the rate configured.



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

Figure 15-61

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.

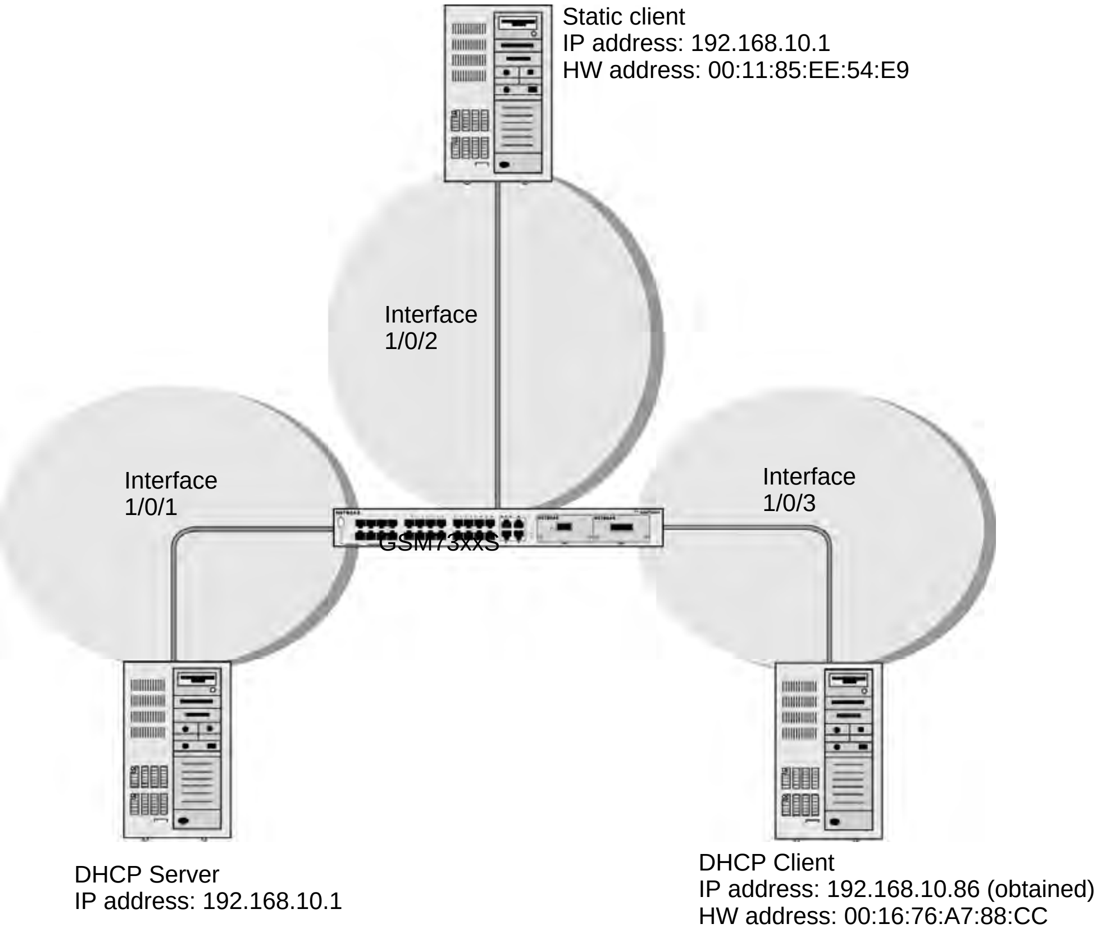


Figure 15-62

This script in this section shows how to configure Dynamic ARP Inspection.

CLI: Configuring Dynamic ARP Inspection

Enable DHCP snooping globally.

```
(Netgear Switch) (Config)# ip dhcp snooping
```

Enable DHCP snooping in a VLAN.

```
(Netgear Switch) (Config)# ip dhcp snooping vlan 1
```

Configure the port through which DHCP server is reached as trusted.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip dhcp snooping trust
```

View the DHCP Snooping Binding table.

```
(GSM7328S) #show ip dhcp snooping binding

Total number of bindings:  1

MAC Address       IP Address     VLAN   Interface    Type    Lease (Secs)
-----------------  ---------------  ----  -----------  -------  -----------
00:16:76:A7:88:CC    192.168.10.86    1        1/0/2  DYNAMIC        86400
```

If the entry does not exist in the DHCP Snooping Binding table, it can statically added through the command “ip verify binding <mac-address> vlan <vlan id> <ip address> interface <interface id>” in the Global Configuration mode.

Enable IP Source Guard in the interface 1/0/2.

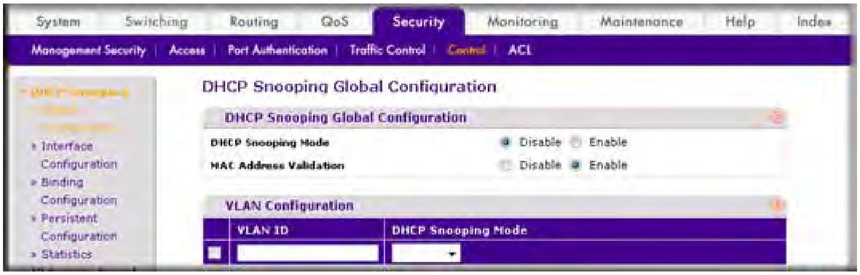
```
(GSM7352Sv2) (Interface 1/0/2)#ip verify source port-security
```

With this configuration device verifies both Source IP Address and Source MAC Address.   If the port-security option is skipped, device verifies only the Source IP Address.

Web Interface: Configuring Dynamic ARP Inspection

1. Enable DHCP snooping globally.

a. From the main menu, select Security > Control > DHCP Snooping Global 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
DHCP Snooping
Global Configuration
» Interface Configuration
» Binding Configuration
» Persistent Configuration
» Statistics

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
□		

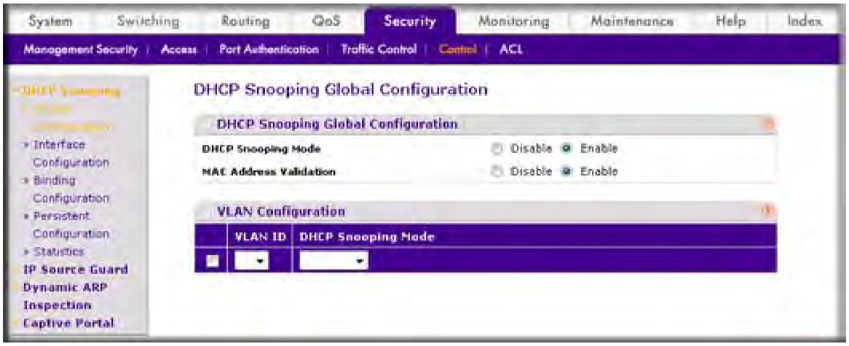
Figure 15-63

b. Select DHCP Snooping Mode as **Enable**.

c. Click **Apply**. At the end of this configuration a screen similar to Figure 15-64 is displayed.

2. Enable DHCP snooping in a VLAN.

a. From the main menu, 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

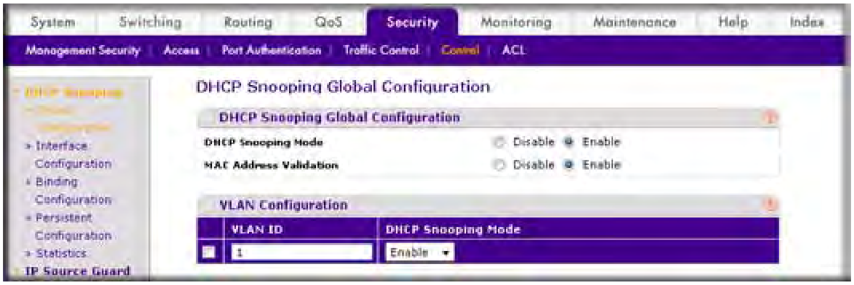
	VLAN ID	DHCP Snooping Mode
□		

Figure 15-64

b. In the VLAN Configuration table, select VLAN ID as **1**.

c. In the VLAN Configuration table, select DHCP Snooping Mode as **Enabled**. A screen similar to the one shown in Figure 15-65 displays.

d. Click **Apply**. At the end of this 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

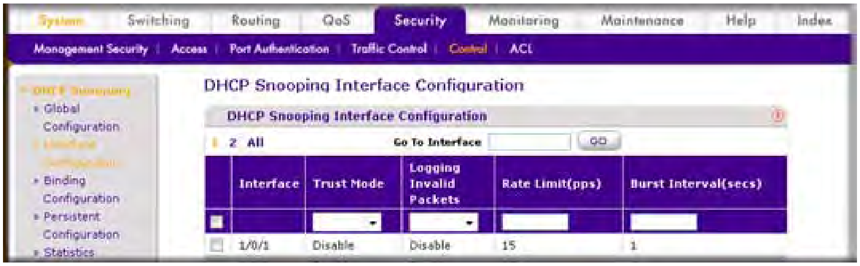
VLAN Configuration

	VLAN ID	DHCP Snooping Mode
□	1	Enable

Figure 15-65

3. Configure the port through which DHCP server is reached as trusted. Here interface 1/0/1 is trusted.

a. From the main menu, select Security > Control > DHCP Snooping Interface Configuration. A screen similar to the following displays. ”



DHCP Snooping Interface Configuration

DHCP Snooping Interface Configuration

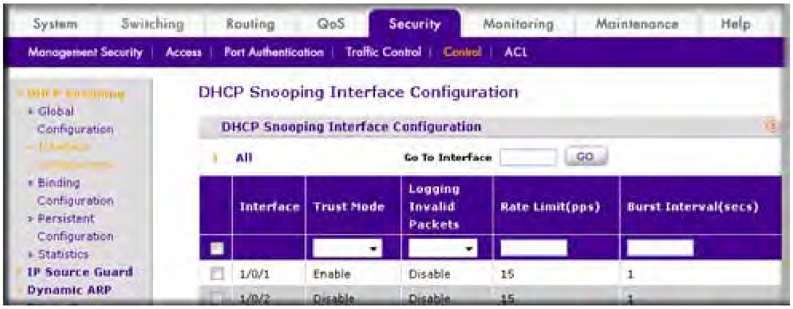
	Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pps)	Burst Interval(secs)
□					
□	1/0/1	Disable	Disable	15	1

Figure 15-66

b. Select the checkbox for Interface **1/0/1**.

c. Set the Trust Mode as **Enable** for Interface 1/0/1.

d. Click **Apply**. At the end of this configuration a screen similar to the following displays.



DHCP Snooping Interface Configuration

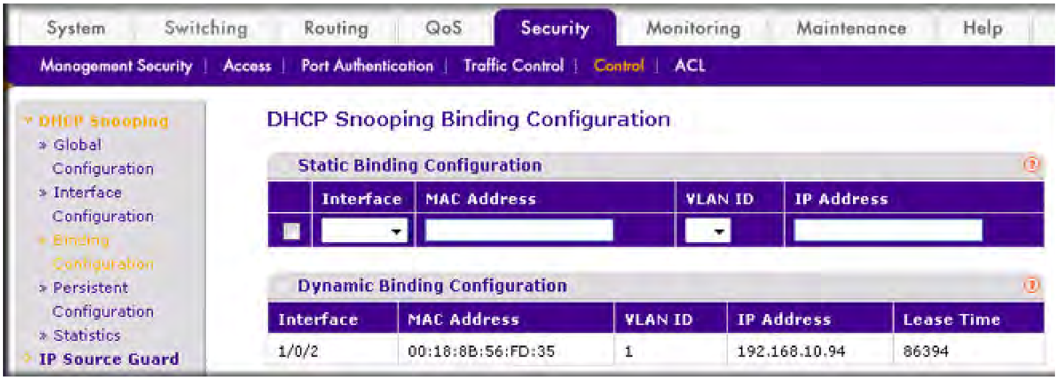
DHCP Snooping Interface Configuration

	Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pps)	Burst Interval(secs)
□					
□	1/0/1	Enable	Disable	15	1
□	1/0/2	Disable	Disable	15	1

Figure 15-67

4. View the DHCP Snooping Binding table.

From the main menu, 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

Figure 15-68

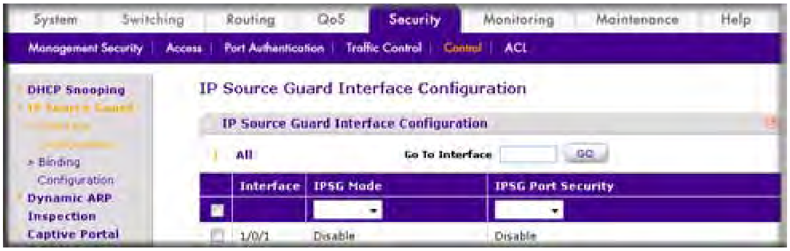
5. Enable IP Source Guard in the interface 1/0/2.

a. From the main menu, select Security > Control > IP Source Guard > Interface Configuration.

b. Select the check box for interface **1/0/2**.

c. Select IPSG mode as Enable.

d. Click **Apply**. At the end of this configuration 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

Figure 15-69

6. IP Source Guard Static Binding

a. From the main menu, select Security - Control > IP Source Guard > Binding Configuration.

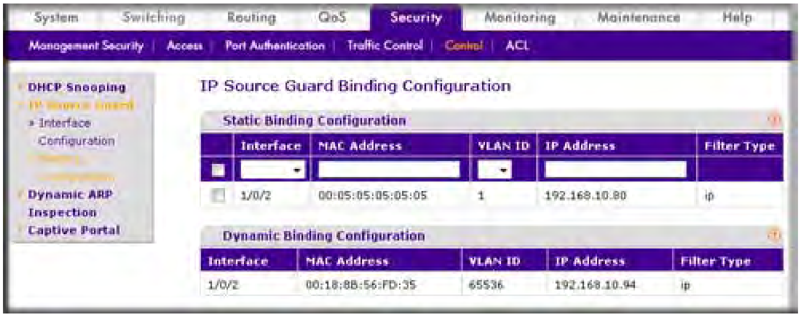
b. In the Static Binding Configuration table, select interface as **1/0/2**.

c. Enter MAC Address as **00:05:05:05:05:05**.

d. Select VLAN ID as **1**.

e. Select IP Address as **192.168.10.80**.

f. Click **Add**. At the end of this configuration 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

Figure 15-70

Chapter 16
Simple Network Time Protocol (SNTP)

In this chapter, the following examples are provided:

- "Show SNTP (CLI Only)"
- "Configure SNTP" on page 16-2
- "Set the Time Zone (CLI Only)" on page 16-5
- "Set Named SNTP Server" on page 16-5

The Simple Network Time Protocol (SNTP) feature:

- Used for synchronizing network resources
- Adaptation of NTP
- Provides synchronized network timestamp
- Can be used in broadcast or unicast mode
- SNTP client implemented over UDP which listens on port 123

Show SNTP (CLI Only)

The following are examples of the commands used in the SNTP feature.

show sntp

```
(Netgear Switch Routing) #show sntp ?

<cr>       Press Enter to execute the command.
client     Display SNTP Client Information.
server     Display SNTP Server Information.
```

show sntp client

```
(Netgear Switch Routing) #show sntp client

Client Supported Modes:    unicast broadcast
SNTP Version:              4
Port:                      123
Client Mode:               unicast
Unicast Poll Interval:     6
Poll Timeout (seconds):    5
Poll Retry:                1
```

show sntp server

```
(Netgear Switch Routing) #show sntp server

Server IP Address:         81.169.155.234
Server Type:               ipv4
Server Stratum:            3
Server Reference Id:       NTP Srv: 212.186.110.32
Server Mode:               Server
Server Maximum Entries:    3
Server Current Entries:    1

SNTP Servers
------------

IP Address:                 81.169.155.234
Address Type:               IPV4
Priority:                   1
Version:                    4
Port:                       123
Last Update Time:           MAY 18 04:59:13 2005
Last Attempt Time:          MAY 18 11:59:33 2005
Last Update Status:         Other
Total Unicast Requests:     1111
Failed Unicast Requests:    361
```

Configure SNTP

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

CLI: Configuring 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 may 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 enabled, the client will wait for the polling interval to send the query to the server. The default value is approximately one minute. After this period, issue the show command to confirm the time has been received. The time will be used in all logging messages.

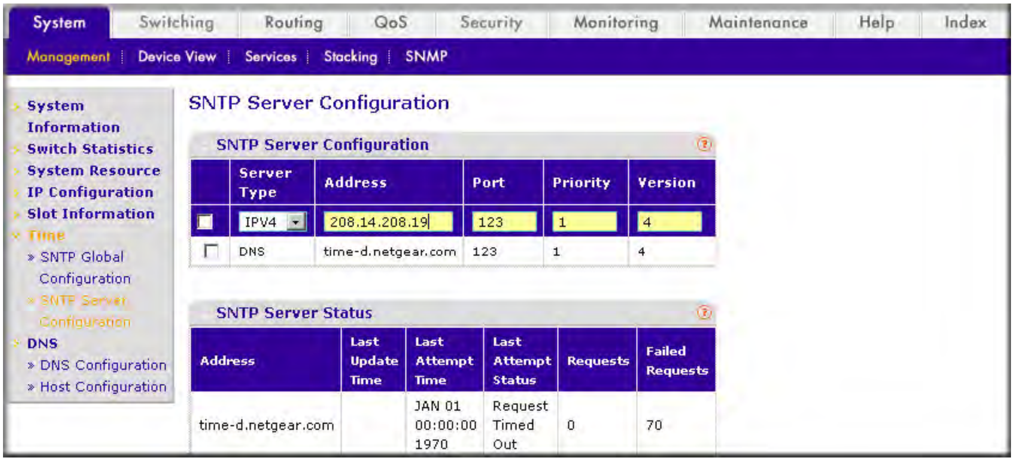
```
(Netgear Switch) #show sntp server
Server IP Address:                 208.14.208.19
Server Type:                       ipv4
Server Stratum:                    4
Server Reference Id:               NTP Srv: 208.14.208.3
Server Mode:                       Server
Server Maximum Entries:            3
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: Configuring SNTP

To use the Web interface to configure SNTP, proceed as follows:

1. Configure SNTP server

   a. From the main menu, 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	208.14.208.19	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

Figure 16-1

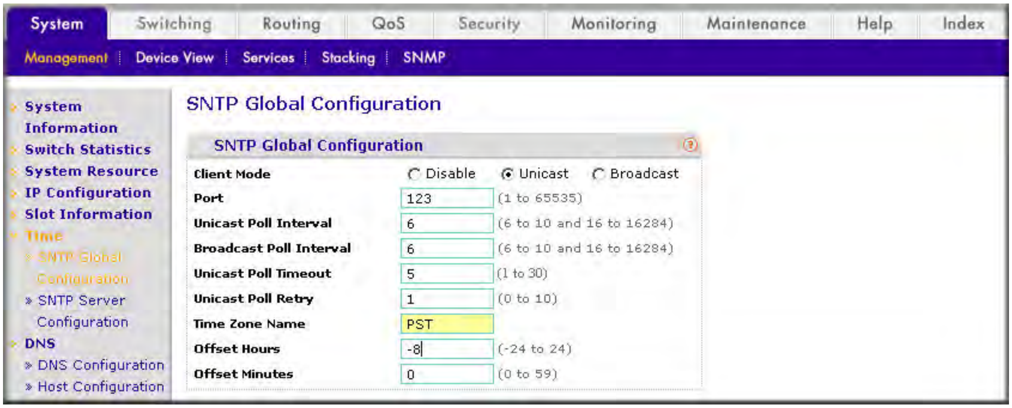
   b. Enter the following information in the SNTP Server Configuration.

   - Select **IPV4** in the Server Type field.
   - 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 global configuration

   a. From the main menu, 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)

Figure 16-2

b. Enter the following information in the SNTP Global Configuration.

- Next to the Client Mode, Select the **Unicast** radio button
- In the Time Zone Name field, enter **PST**
- In the Offset Hours field, enter **-8**

c. Click **Apply**.

Set the Time Zone (CLI Only)

The SNTP/NTP server is set to Coordinated Universal Time (UTC) by default. The following example shows how to set the time zone to Pacific Standard Time (PST) which is 8 hours behind GMT/UTC.

```
(Netgear switch)(config)#clock timezone PST -8
```

Set Named SNTP Server

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

CLI: Setting Named SNTP Server

Netgear provides SNTP servers accessible by Netgear devices.

Because Netgear may change IP addresses assigned to its time servers, it is best to access a 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.

To use this feature, follow the steps below:

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.

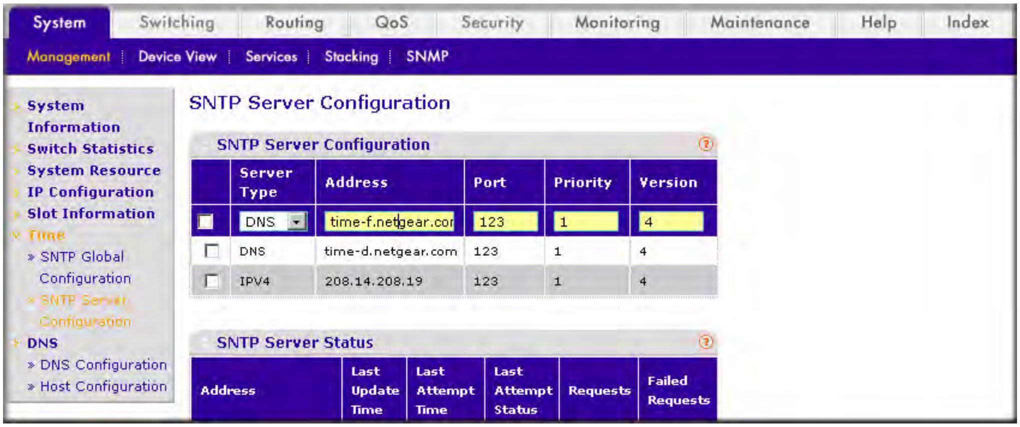
This method of setting DNS name look-up can be used for any other applications that require a public IP address, for example, a RADIUS server.

Web Interface: Setting Named SNTP Server

To use the Web interface to configure SNTP, proceed as follows:

1. Configure SNTP server

a. From the main menu, 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.cor	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

Figure 16-3

b. Enter the following information in the SNTP Server Configuration.

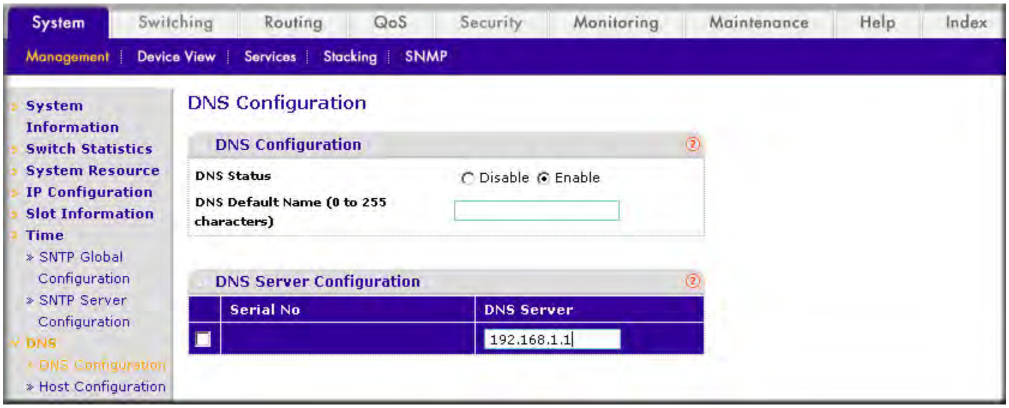
- Select **DNS** in the Server Type field
- In the Address field, enter **time-f.netgear.com**
- In the Port field, enter **123**
- In the Priority field, enter **1**

- In the Version field, enter **4**

c. Click **Add**.

2. Configure the DNS server.

a. From the main menu, 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

Figure 16-4

b. Enter the following information in the DNS Configuration.

- Next to the DNS Status, select the **Enable** radio button
- In the DNS Server field, enter **192.168.1.1**

c. Click **Add**.

Chapter 17
Tools

In this chapter, the following examples are provided:

- “Traceroute”
- “Configuration Scripting” on page 17-3
- “Pre-Login Banner” on page 17-5
- “Port Mirroring” on page 17-6
- “Dual Image” on page 17-8
- “Outbound Telnet” on page 17-11

Traceroute

This section describes the Traceroute feature. Use Traceroute to discover the routes that packets take when traveling on a hop-by-hop basis to their destination through the network.

- Maps network routes by sending packets with small Time-to-Live (TTL) values and watches the ICMP time-out announcements
- Command displays all L3 devices
- Can be used to detect issues on the network
- Tracks up to 20 hops
- Default UPD port used 33343 unless modified 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

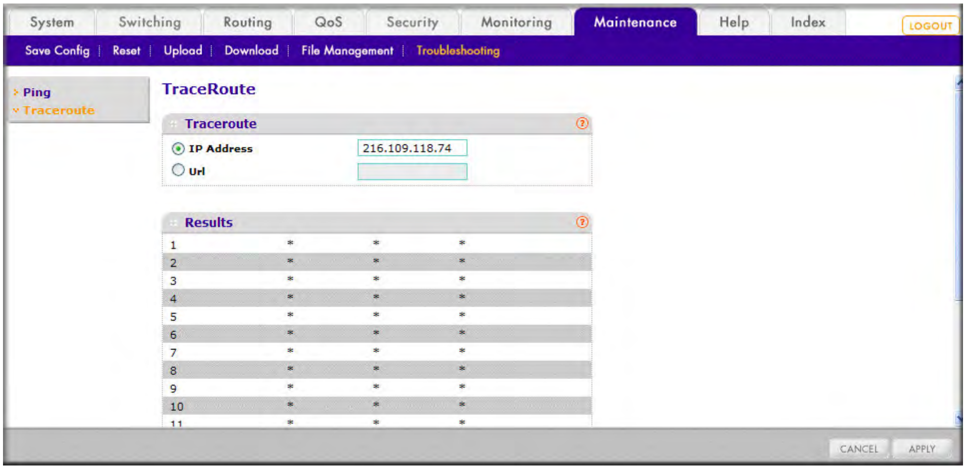
```
(Netgear Switch) #traceroute?
<ipaddr>      Enter IP address.

(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

To use the Web interface to configure the managed switch, proceed as follows:

1. Configure the Traceroute.
   a. From the main menu, 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	*	*	*

Figure 17-1

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.

b. Enter the following information in the Traceroute.

In the IP Address field, enter **216.109.118.74**.

c. Click **Apply**.

Configuration Scripting

In this chapter, the following examples are provided:

- "script" on page 17-4
- "script list and script delete" on page 17-4
- "script apply running-config.scr" on page 17-4
- "Create a Configuration Script" on page 17-5
- "Upload a Configuration Script" on page 17-5

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
- May be applied to several switches
- Can save up to ten scripts or 500K of memory
- Provides List, Delete, Apply, Upload, Download
- Provides script format of one CLI command per line

Some considerations are:

- Total number of scripts stored on box limited by NVRAM/FLASH size.
- Application of scripts is partial if script fails. For example, if the script executes five of ten commands and the script fails, the script stops at five.
- 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.

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

This section describes the Pre-Login Banner feature.

Pre-Login Banner:

- Allows you to create message screens when logging into the CLI Interface
- By default, no Banner file exists
- Can be uploaded or downloaded
- File size cannot be larger than 2K

The Pre-Login Banner feature is only for the CLI interface.

Creating a Pre-Login Banner (CLI Only)

To create a Pre-Login Banner, follow these steps:

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

This section describes the Port Mirroring feature.

Port Mirroring:

- 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.

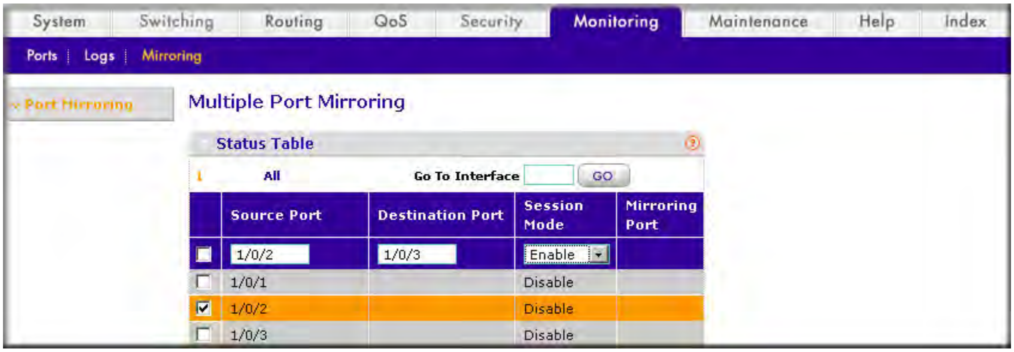
CLI: Specifying the Source (Mirrored) Ports and Destination (Probe)

```
(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: Specifying the Source (Mirrored) Ports and Destination (Probe)

To use the Web interface to show monitor session, proceed as follows:

1. From the main menu, select Monitoring > Mirroring>Port Mirroring. A screen similar to the following displays.



Multiple Port Mirroring

	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	

Figure 17-2

2. Under Multiple Port Mirroring, scroll down to interface **1/0/2** and select the checkbox for 1/0/2. The value 1/0/2 now appears in the Interface field at the top.

3. Enter the following information in the Status Table.
   - In the Destination Port field, enter **1/0/3.**
   - Select **Enable** in the Session Mode field.

4. Click **Apply**.

Dual Image

Traditionally switches contained a single image in the permanent-storage. This image is loaded into memory every time there is a reboot. Dual Image feature allows switches to have two images in the permanent storage. User can denote any of these images as an **active-image** that will be loaded in subsequent reboots and the other image as a **backup-image**. This feature provides for reduced down-time for the switches, when the firmware is being upgraded or downgraded.

The images are stored in the file system with the file names **image1** and **image2**. These names are used in the CLI, Web and the SNMP interfaces. Each of the images can be associated with a textual description. Switch provides commands to associate/retrieve 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 DualImage 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: Downloading a Backup Image and Having It Active

```
(Netgear Switch) #copy tftp://192.168.0.1/gsm73xxseps.stk image2
Mode........................................ TFTP
Set Server IP............................... 192.168.0.1
Path........................................ ./
Filename.................................... gsm73xxseps.stk
Data Type................................... Code
Destination Filename........................ image2
Management access will be blocked for the duration of the transfer Are you sure you
want to start? (y/n) y
```

```
TFTP code transfer starting
101888 bytes transferred...277504 bytes transferred...410112 bytes
transferred...628224 bytes transferred...803328 bytes transferred...978944 bytes
transferred...1154560 bytes transferred...1330176 bytes transferred...1505280 bytes
transferred...1680896 bytes transferred...1861632 bytes transferred...2040320 bytes
transferred...2215936 bytes transferred...2391040 bytes transferred...2566656 bytes
transferred...2741760 bytes transferred...2916864 bytes transferred...3092992 bytes
transferred...3268096 bytes transferred...3443712 bytes transferred...3619328 bytes
transferred...3794432 bytes transferred...3970048 bytes transferred...4145152 bytes
transferred...4320768 bytes transferred...4496384 bytes transferred...4669952 bytes
transferred...4849152 bytes transferred...5027840 bytes transferred...5202944 bytes
transferred...5378560 bytes transferred...5554176 bytes transferred...5729280 by
tes transferred...5904896 bytes transferred...6078976 bytes transferred...6255616
bytes transferred...6423040 bytes transferred...6606336 bytes transferred...6781952
bytes transferred...6957056 bytes transferred...7111168 bytes transferred...7307776
bytes transferred...7483392 bytes transferred...7658496 bytes transferred...
```

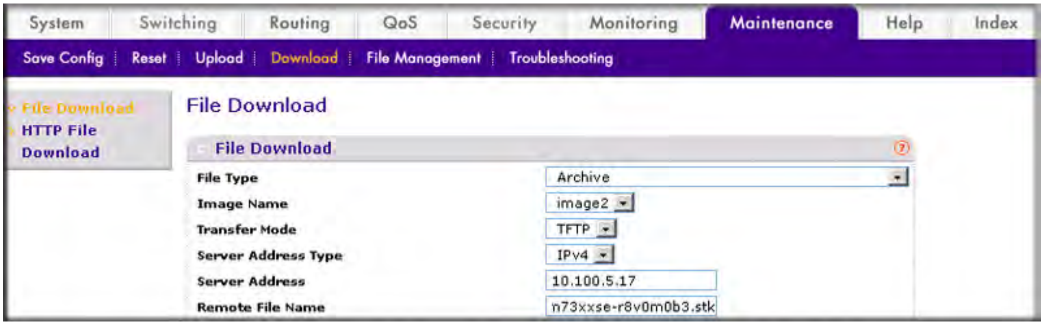
```
Verifying CRC of file in Flash File System
Distributing the code to the members of the stack!
File transfer operation completed successfully.
(Netgear Switch) #
(Netgear Switch) #show bootvar
Image Descriptions
 image1 : default image
 image2 :
 Images currently available on Flash
--------------------------------------------------------------------
 unit      image1      image2     current-active        next-active
--------------------------------------------------------------------

  1   5.11.2.51     8.0.0.2             image1            image1
(Netgear Switch) #boot system image2
Activating image image2 ..
(Netgear Switch) #show bootvar
Image Descriptions
image1 : default image
image2 :
Images currently available on Flash
--------------------------------------------------------------------
unit      image1      image2     current-active        next-active
--------------------------------------------------------------------
1   5.11.2.51     8.0.0.2             image1            image2
                                      Image2 will be executed after reboot.
```

Web Interface: Downloading a Backup Image and Having It Active

To use the Web interface to download a backup image and have it active, proceed as follows:

1. Download a backup image via tftp.

   a. From the main menu, 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

Figure 17-3

   b. Select **Archive** in the File Type field.

   c. Select **image2** in the Image Name field.

   d. Select **TFTP** in the Transfer Mode field.

   e. Select **IPv4** in the Server Address Type field.

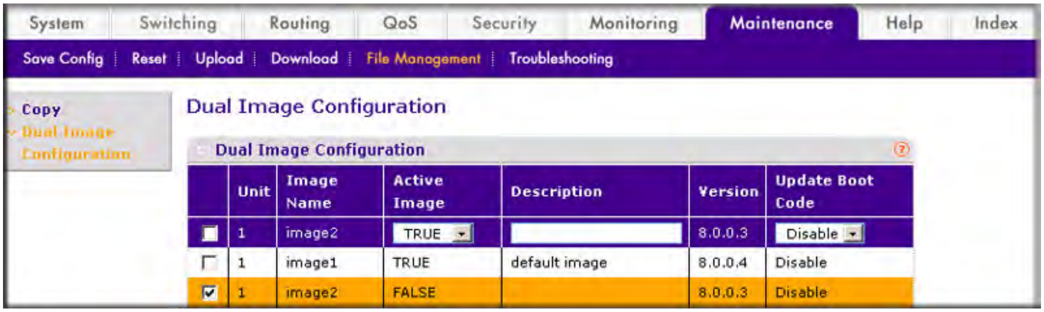
   f. In the Server Address field, enter **10.100.5.17**(tftp server IP address).

   g. In the Remote File Name, enter gsm73xxse-r8v0m0b3.stk.

   h. Click **Apply**.

2. Active imag2.

   a. From the main menu, 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

Figure 17-4

b. Under Dual Image Configuration, scroll down to image 2, select the checkbox for that image. The image2 now appears in the Image name field at the top.

c. Select **TRUE** in the Active Image field.

d. Click **Apply**.

Outbound Telnet

In this section, the following examples are provided:

- "CLI: show network" on page 17-11
- "CLI: transport output telnet" on page 17-12
- "CLI: session-limit and session-timeout" on page 17-13

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
```

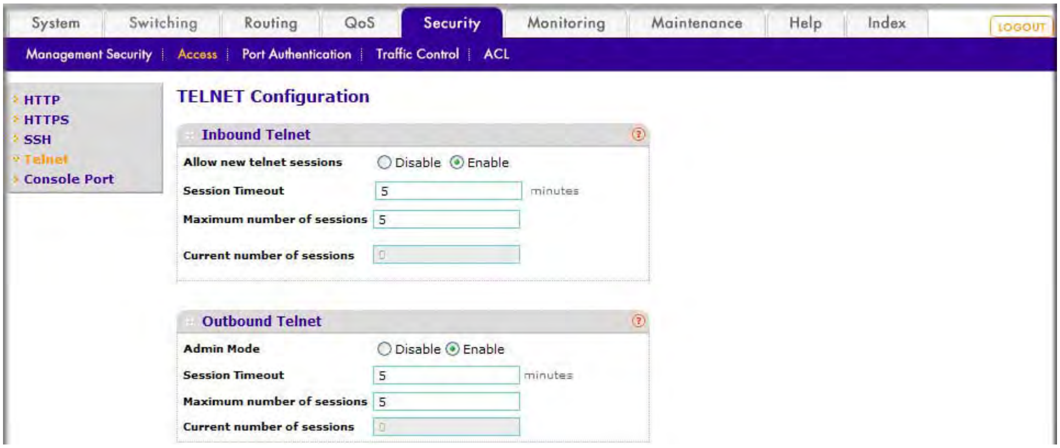
CLI: transport output telnet

```
(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: Configuring Telnet

To use the Web interface to configure the Telnet in the managed switch, proceed as follows:

1. From the main menu, 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 0

Outbound Telnet

Admin Mode ○ Disable ● Enable

Session Timeout 5 minutes

Maximum number of sessions 5

Current number of sessions 0

Figure 17-5

2. Enter the following information in the Outbound Telnet.
3. Next to the Admin Mode, select the **Enable** radio button.
4. Click **Apply**

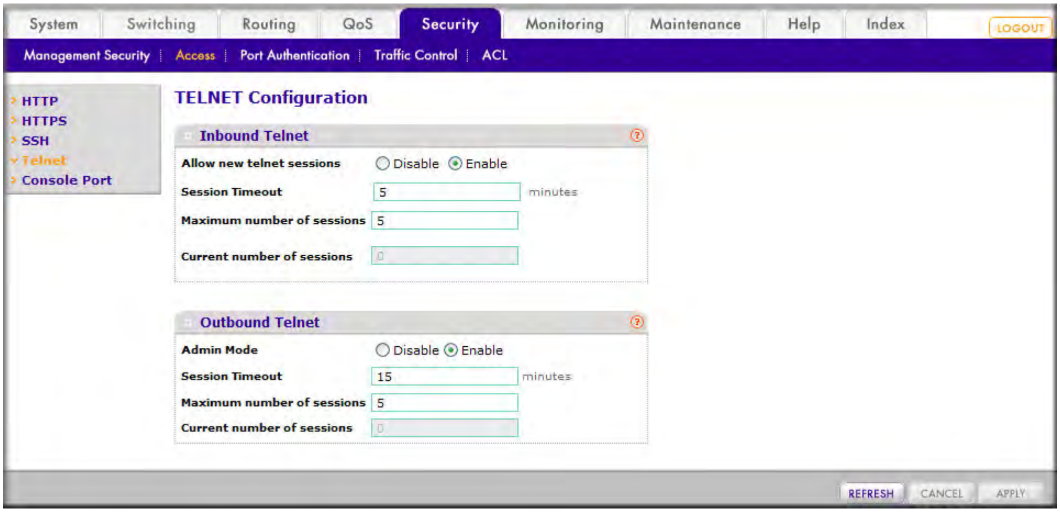
CLI: session-limit and session-timeout

```
(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: Configuring the Session Timeout

To use the Web interface to configure the outbound telnet session in the managed switch, proceed as follows:

1. From the main menu, 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	0

Outbound Telnet

Admin Mode	○ Disable ● Enable
Session Timeout	15 minutes
Maximum number of sessions	5
Current number of sessions	0

Figure 17-6

2. Enter the following information in the Outbound Telnet.
   - In the Session Timeout field, enter **15**.
   - In the Maximum number of sessions, enter **5**.
3. Click **Apply**.

Chapter 18
Syslog

In this chapter, the following examples are provided:

- “Show Logging” on page 18-2
- “Show Logging Buffered” on page 18-5
- “Show Logging Traplogs” on page 18-6
- “Show Logging Hosts” on page 18-7
- “Log Port Configuration” on page 18-8

The Syslog feature:

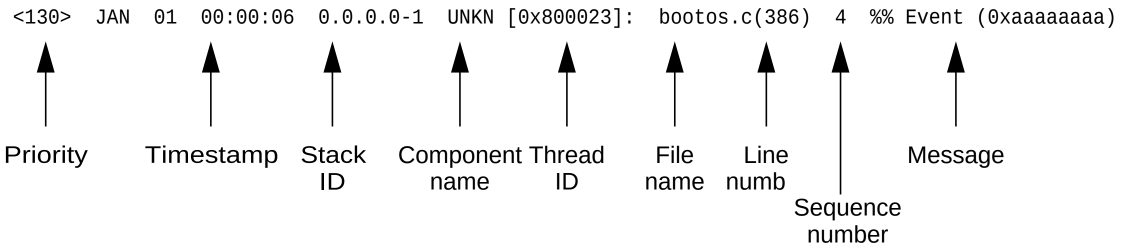
- Allows you to store system messages and/or errors
- Can store to local files on the switch or a remote server running a syslog daemon
- Method of collecting message logs from many systems

Persistent Log Files

- Currently three - one for each of the last three sessions
- Each log has two parts:
  - Start up log is the first 32 messages after system startup
  - Operational log is the last 32 messages received after the startup log is full
- Files are stored in ASCII format
  - slog0.txt - slog2.txt
  - olog0.txt - olog2.txt

    Where 0 is for the boot, 1 is for the last boot, 2 is for the boot before that; the third one overflows upon the next boot.
- Can be saved to local server to monitor at a later point in time

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 18-1

Show Logging

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

CLI: Show Logging

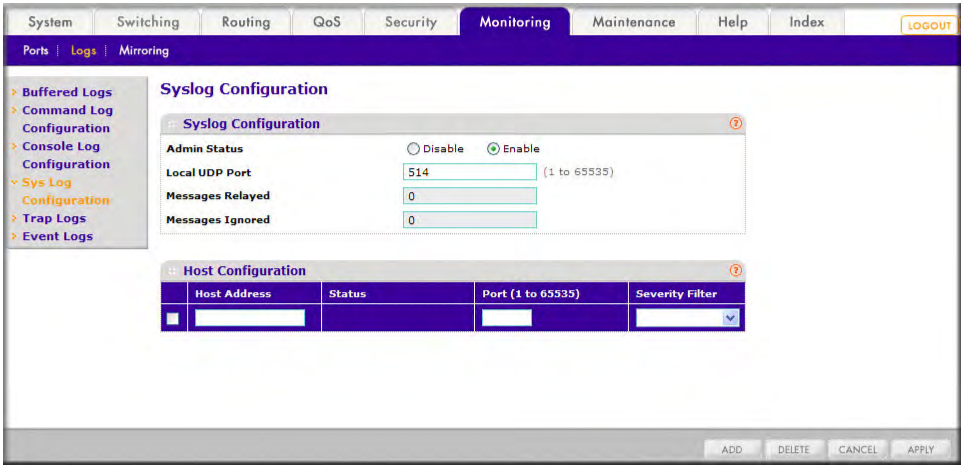
```
(Netgear Switch Routing) #show logging

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

To use the Web interface to configure the managed switch, proceed as follows:

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
□				

Figure 18-2

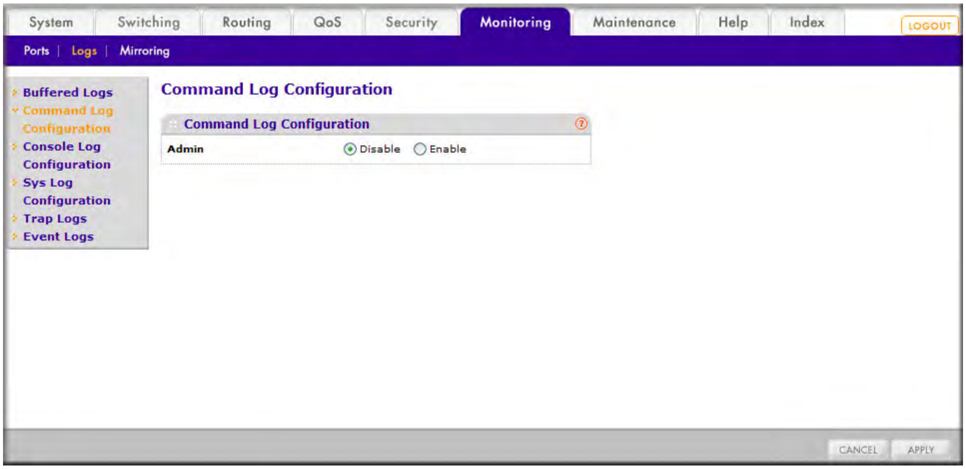
b. Enter the following information in the Syslog Configuration.

Next to the Admin Status**,** select the **Enable** radio button.

c. Click **Apply**.

2. Configure the Command Log

a. From the main menu, select Monitoring > Logs >Command Log.



Command Log Configuration

Command Log Configuration

Admin ● Disable ○ Enable

Figure 18-3

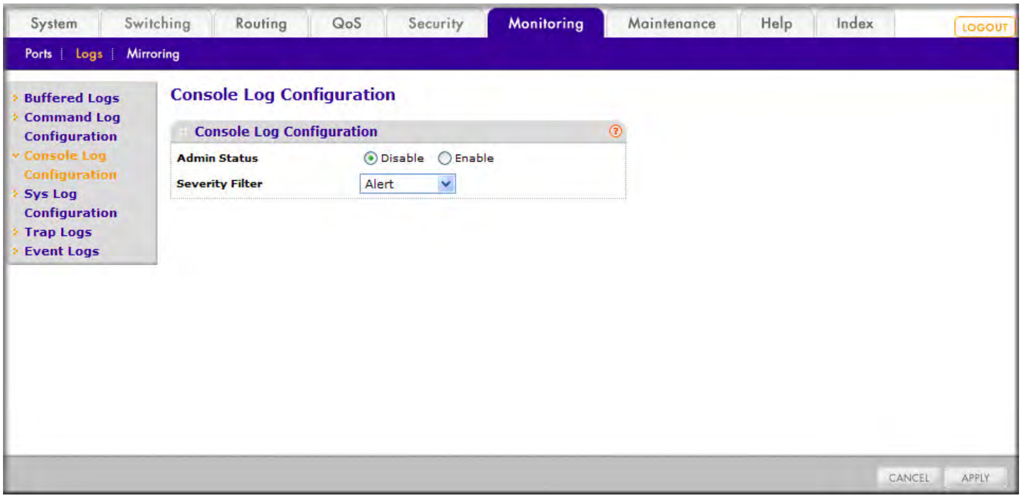
b. Enter the following information in the Command Log.

Next to the Admin Status, click the **Disable** radio button.

c. Click **Apply**.

3. Configure the Console Log.

a. From the main menu, select Monitoring > Logs >Console Log.



Console Log Configuration

Console Log Configuration

Admin Status ● Disable ○ Enable

Severity Filter Alert

Figure 18-4

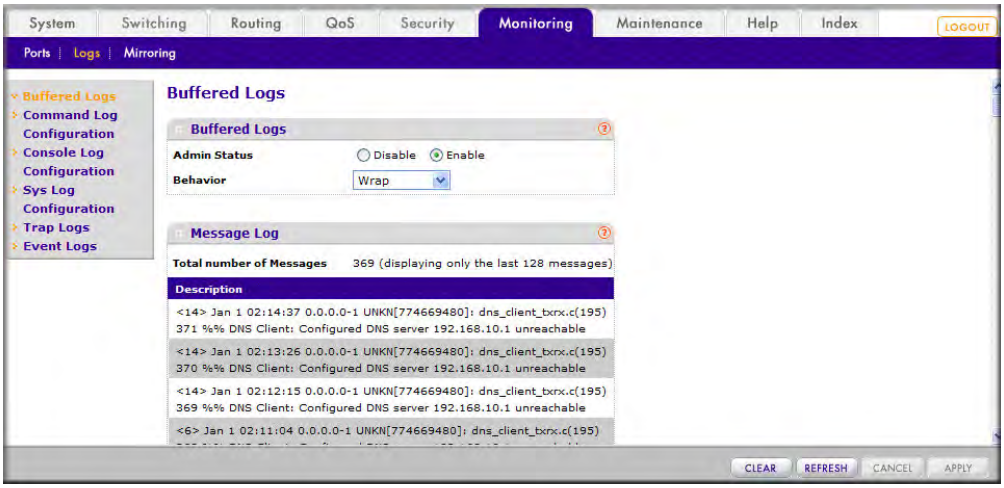
b. Enter the following information in the Console Log Configuration.

Next to the Admin Status**,** click the **Disable** radio button.

c. Click **Apply**.

4. Configure Buffer Logs.

a. From the main menu, 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)
```

Figure 18-5

b. Enter the following information in the Buffer Logs.

Next to the Admin Status**,** click the **Enable** radio button.

c. Click **Apply**.

Show Logging Buffered

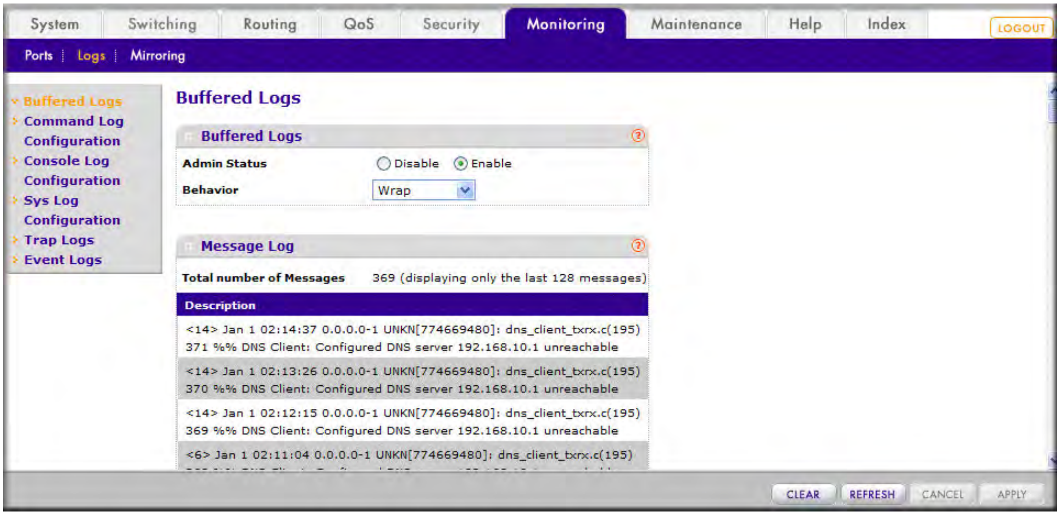
The example is shown as CLI commands and as a Web interface procedure.

CLI: Showing 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: Showing Logging Buffered

From the main menu, 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)
```

Figure 18-6

Show Logging Traplogs

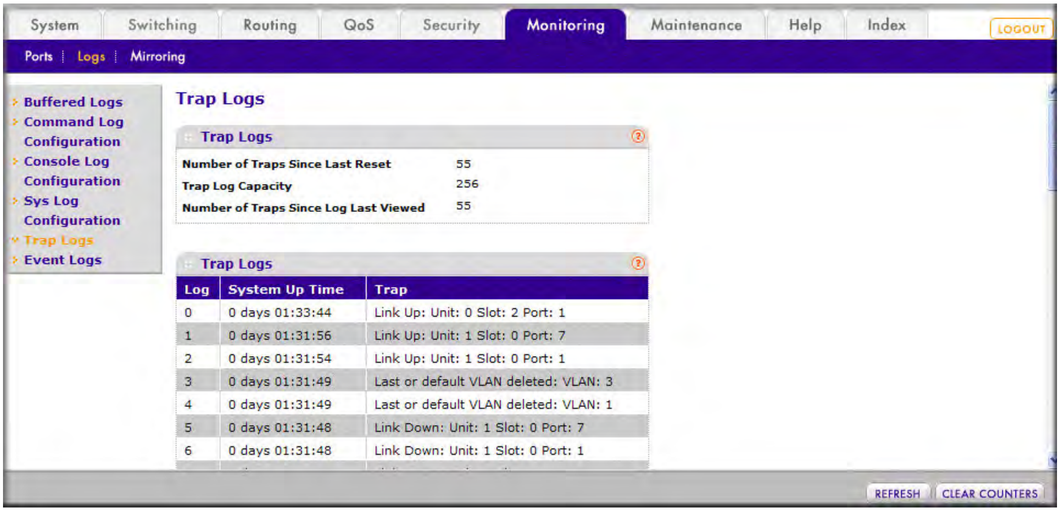
The example is shown as CLI commands and as a Web interface procedure.

CLI: Showing 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: Showing Logging Trap Logs

From the main menu, 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

Figure 18-7

Show Logging Hosts

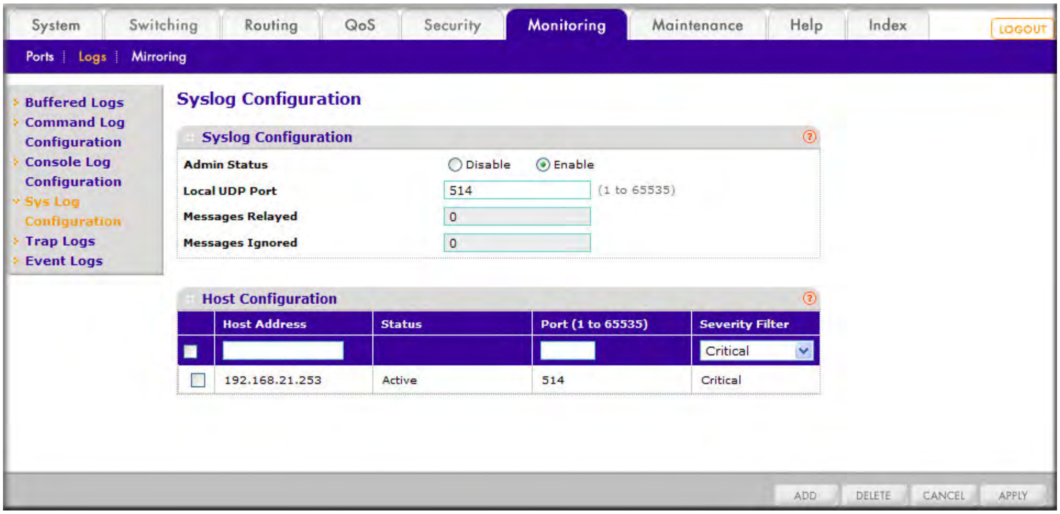
The example is shown as CLI commands and as a Web interface procedure.

CLI: Showing 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: Showing Logging Hosts

From the main menu, 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

Figure 18-8

Log Port Configuration

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

CLI: Logging Port Configuration

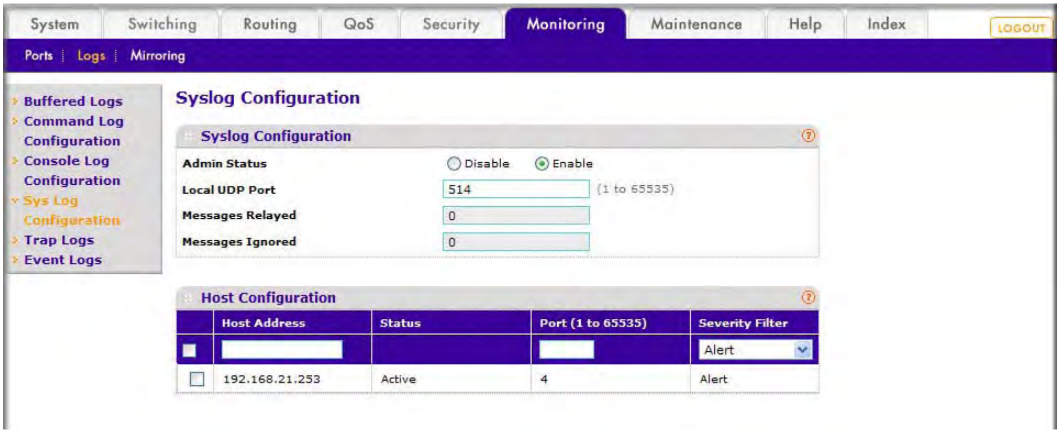
```
(Netgear Switch Routing)     #config

(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: Logging Port Configuration

To use the Web interface to configure the managed switch, proceed as follows:

1. From the main menu, 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

Figure 18-9

2. Enter the following information in the Host Configuration.
   - In the Host Address field, enter your host address **192.168.21.253**.
   - In the Port field, enter **4**.
   - Select **Alert** in the Severity Filter field.
3. Click **Add**.

Chapter 19
Managing Switch Stacks

This chapter describes the concepts and recommended operating procedures to manage NETGEAR stackable managed switches running Release 4.x.x.x or newer. NETGEAR stackable managed switches include the following models:

- FSM7226RS
- FSM7250RS
- FSM7328S
- FSM7328PS
- FSM7352S
- FSM7352PS
- GSM7328S
- GSM7352S
- GSM7328FS

➡	**Note:** The FSM family and GSM family cannot be stacked together at this point.

This chapter includes the following topics:

Understanding Switch Stacks

A *switch stack* is a set of up to eight Ethernet switches connected through their stacking ports. One of the switches controls the operation of the stack and is called the stack master. The *stack master* and the other switches in the stack are *stack members*. The stack members use stacking technology to behave and work together as a unified system. Layer 2 and Layer 3 protocols present the entire switch stack as a single entity to the network.

The stack master is the single point of stack-wide management. From the stack master, you configure:

- System-level (global) features that apply to all stack members
- Interface-level features for all interfaces on any stack member

A switch stack is identified in the network by its network IP address. The network IP address is assigned according to the MAC address of the stack master. Every stack member is uniquely identified by its own *stack member number*.

All stack members are eligible stack masters. If the stack master becomes unavailable, the remaining stack members participate in electing a new stack master from among themselves. A set of factors determine which switch is elected the stack master. These factors are:

1. The switch that is master always has priority to retain the role of master
2. Assigned priority
3. MAC address

If the master cannot be selected by (1), then (2) is used. If (2) does not resolve which stack member becomes stack master, then (3) is used.

The stack master contains the saved and running configuration files for the switch stack. The configuration files include the system-level settings for the switch stack and the interface-level settings for all stack members. Each stack member retains a copy of the saved file for backup purposes.

If the master is removed from the stack, another member will be elected master, and will then run from that saved configuration.

You can use these methods to manage switch stacks:

- Stack web interface
- Command line interface (CLI) over a serial connection to the console port of the master
- A network management application through the Simple Network Management Protocol (SNMP)

Switch Stack Membership

A switch stack has up to eight stack members connected through their stacking ports. A switch stack always has one stack master.

A standalone switch is a switch stack with one stack member that also operates as the stack master. You can connect one standalone switch to another to create a switch stack containing two stack members, with one of them being the stack master. You can connect standalone switches to an existing switch stack to increase the stack membership.

If you replace a stack member with an identical model, the new switch functions with exactly the same configuration as the replaced switch, assuming that the new switch is using the same member number as the replaced switch. For information about the benefits of preconfiguring a switch stack, see "Preconfiguration" on page 19-14.

The operation of the switch stack continues uninterrupted during membership changes unless you remove the stack master or you add powered-on standalone switches or switch stacks.

- Adding powered-on switches (merging) causes the stack masters of the merging switch stacks to elect a stack master from among themselves. The re-elected stack master retains its role and configuration and so do its stack members. All remaining switches, including the former stack masters, reload and join the switch stack as stack members. They change their stack member numbers to the lowest available numbers and use the stack configuration of the re-elected stack master. Therefore, when you merge two powered stacks, you cannot control which unit becomes stack master and which configuration is used. For these reasons, it is recommended that powered switches be powered down before adding to an existing operating stack.
- Removing powered-on stack members can cause the switch stack to divide (partition) into two or more switch stacks, each with the same configuration. However, if cabled properly, the switch stack should not divide.
    - If the switch stack divides, and you want the switch stacks to remain separate, change the IP address or addresses of the newly created switch stacks.
    - If you did not intend to partition the switch stack:
        - Power off the newly created switch stacks
        - Reconnect them to the original switch stack through their stacking ports
        - Power on the switches

Switch Stack Cabling (FSM73xxS)

Figure 19-1 and Figure 19-2 illustrate how individual switches are interconnected to form a stack. You can use the regular Category 5 Ethernet 8 wire cable.

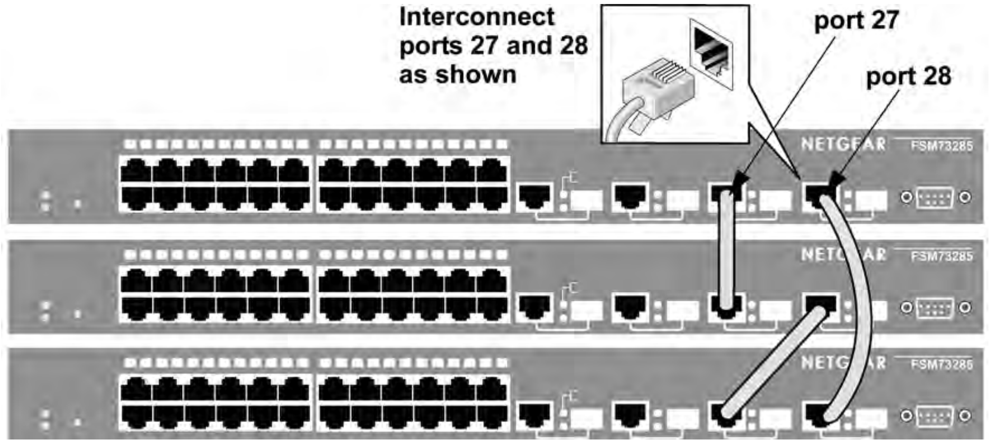


Figure 19-1

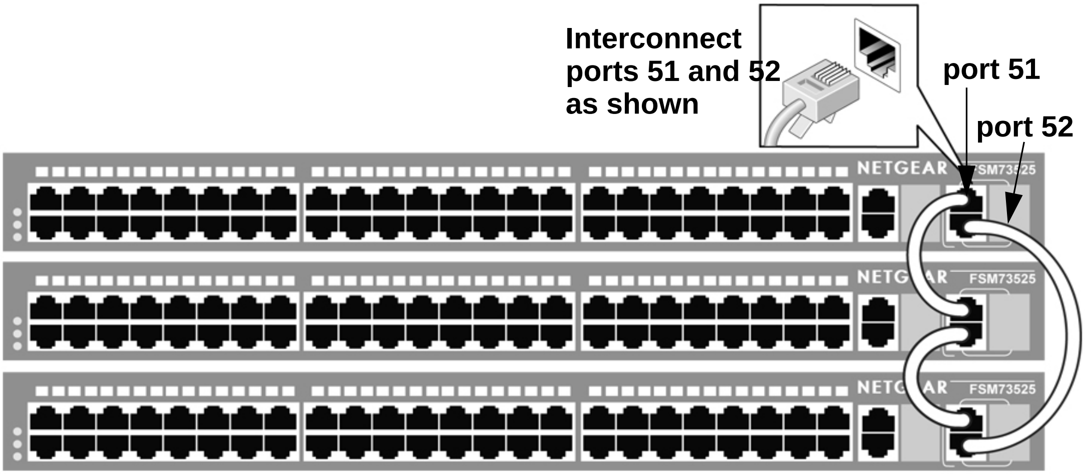


Figure 19-2

Stack Master Election and Re-Election

The stack master is elected or re-elected based on one of these factors and in the order listed:

1. The switch that is currently the stack master

2. The switch with the highest stack member priority value

> **Note:** NETGEAR recommends assigning the highest priority value to the switch that you prefer to be the stack master. This ensures that the switch is re-elected as stack master if a re-election occurs.

3. The switch with the higher MAC address

A stack master retains its role unless one of these events occurs:

- The stack master is removed from the switch stack
- The stack master is reset or powered off
- The stack master has failed
- The switch stack membership is increased by adding powered-on standalone switches or switch stacks

In the case of a master re-election, the new stack master becomes available after a few seconds. In the meantime, the switch stack uses the forwarding tables in memory to minimize network disruption. The physical interfaces on the other available stack members are not affected while a new stack master is elected.

If a new stack master is elected and the previous stack master becomes available, the previous stack master does not resume its role as stack master.

Stack Member Numbers

A stack member number (1 to 8) identifies each member in the switch stack. The member number also determines the interface-level configuration that a stack member uses. You can display the stack member number by using the **show switch** user EXEC command.

A new, out-of-the-box switch (one that has not joined a switch stack or has not been manually assigned a stack member number) ships with a default stack member number of 1. When it joins a switch stack, its default stack member number changes to the lowest available member number in the stack.

Stack members in the same switch stack cannot have the same stack member number. Every stack member, including a standalone switch, retains its member number until you manually change the number or unless the number is already being used by another member in the stack.

See "Renumber Stack Members" and "Merging Two Operational Stacks".

Stack Member Priority Values

A stack member priority can be changed if the user would like change who is the master of the stack. Use the following command to change stack member's priority (this command is in the global config mode):

switch unit **priority** value

Switch Stack Offline Configuration

You can use the offline configuration feature to preconfigure (supply a configuration to) a new switch before it joins the switch stack. You can configure in advance the stack member number, the switch type, and the interfaces associated with a switch that is not currently part of the stack (see "Preconfiguration"

Effects of Adding a Preconfigured Switch to a Switched Stack

When you add a preconfigured switch to the switch stack, the stack applies either the preconfigured configuration or the default configuration. Table 19-1 lists the events that occur when the switch stack compares the preconfigured configuration with the new switch:

Table 19-1. Results of comparing the preconfiguration with the new switch

Scenario	Result
The stack member numbers and the switch types match. • If the stack member number of the preconfigured switch matches the stack member number in the configuration on the stack, and • If the switch type of the preconfigured switch matches the switch type in the configuration on the stack.	The switch stack applies the configuration to the preconfigured new switch and adds it to the stack.
The stack member numbers match but the switch types do not match. • If the stack member number of the preconfigured switch matches the stack member number in the configuration on the stack, but • The switch type of the preconfigured switch does not match the switch type in the configuration on the stack.	• The switch stack applies the default configuration to the preconfigured switch and adds it to the stack. • The configuration in the preconfigured switch is changed to reflect the new information.
The stack member number is not found in the configuration.	• The switch stack applies the default configuration to the new switch and adds it to the stack. • The preconfigured information is changed to reflect the new information.
The stack member number of the preconfigured switch is not found in the configuration.	The switch stack applies the default configuration to the preconfigured switch and adds it to the stack.

Effects of Replacing a Preconfigured Switch in a Switch Stack

When a preconfigured switch in a switch stack fails, is removed from the stack, and is replaced with another switch, the stack applies either the preconfiguration or the default configuration to it. The events that occur when the switch stack compares the configuration with the preconfigured switch are the same as those described in "Effects of Adding a Preconfigured Switch to a Switched Stack".

Effects of Removing a Preconfigured Switch from a Switch Stack

If you remove a preconfigured switch from the switch stack, the configuration associated with the removed stack member remains in the running configuration as configured information. To completely remove the configuration, use the **no member** *unit_number* (this is in the stacking configuration mode).

Switch Stack Software Compatibility Recommendations

All stack members must run the same software version to ensure compatibility between stack members. The software versions on all stack members, including the stack master, must be the same. This helps ensure full compatibility in the stack protocol version among the stack members.

If a stack member is running a software version that is not the same as the stack master, then the stack member is not allowed to join the stack. Use the **show switch** command to list the stack members and software versions. See "Code Mismatch".

Incompatible Software and Stack Member Image Upgrades

You can upgrade a switch that has an incompatible software image by using the **copy** xmodem | ymodem | zmodem | tftp://*ip/filepath/filename* command. It copies the software image from an existing stack member to the one with incompatible software. That switch automatically reloads and joins the stack as a fully functioning member.

Switch Stack Configuration Files

The configuration files record settings for all global and interface specific settings that define the operation of the stack and individual members. Once a **save config** command is issued, all stack members store a copy of the configuration settings. If a stack master becomes unavailable, any stack member assuming the role of stack master will operate from the saved configuration files.

When a new, out-of-box switch joins a switch stack, it uses the system-level settings of that switch stack. However, if you want it to store this system level configuration, you must issue a **save config** command.

You back up and restore the stack configuration in the same way as you would for standalone switch configuration by using the copy command.

Switch Stack Management Connectivity

You manage the switch stack and the stack member interfaces through the stack master. You can use the web interface, the CLI, and SNMP. You cannot manage stack members on an individual switch basis.

- You can connect to the stack master through the console port of the stack master only.
- You can connect to the stack master by using a Telnet connection to the IP address of the stack.

Switch Stack Configuration Scenarios

Table 19-2 provides switch stack configuration scenarios. Most of the scenarios assume at least two switches are connected through their stacking ports.

Table 19-2. Switch stack configuration scenarios

Scenario	Result
Stack master election specifically determined by existing stack masters **Note**: This is not recommended. • Connect two powered-on switch stacks through the stacking ports.	Only one of the two stack masters becomes the new stack master. None of the other stack members become the stack master.
Stack master election specifically determined by the stack member priority value • Connect two switches through their stacking ports. • Use the **switch** *stack-member-number* **priority** *new-priority-number* global configuration command to set one stack member to a higher member priority value. • Restart both stack members at the same time.	The stack member with the higher priority value is elected stack master.
Stack master election specifically determined by the MAC address • Assuming that both stack members have the same priority value and software image, restart both stack members at the same time.	The stack member with the higher MAC address is elected stack master.
Add a stack member • Power off the new switch • Through their stacking ports, connect the new switch to a powered-on switch stack. • Power on the new switch.	The stack master is retained. The new switch is added to the switch stack.
Stack master failure • Remove (or power off) the stack master.	Based on “Stack Master Election and Re-Election”, one of the remaining stack members becomes the new stack master. All other members in the stack remain stack members and do not reboot.

Stacking Recommendations

The purpose of this section is to collect notes on recommended procedures and expected behavior of stacked managed switches. Procedures addressed initially are listed below.

- Initial installation and power-up of a stack.
- Removing a unit from the stack
- Adding a unit to an operating stack
- Replacing a stack member with a new unit
- Renumbering stack members
- Moving the master to a different unit in the stack
- Removing a master unit from an operating stack
- Merging two operational stacks
- Preconfiguration
- Upgrading firmware
- Migration of configuration with a firmware upgrade

General Practices

- When issuing a command (such as move management, or renumber), it is recommended that the command has fully completed before issuing the next command. For example, if a reset is issued to a stack member, use the **show port** command to verify that the unit has re-merged with the stack, and all ports are joined before issuing the next command.
- When physically removing or relocating a unit, always power down the unit before disconnecting stack cables.
- When reconnecting stack cables, connect them before powering up the unit, if possible, and insure a good connection by tightening all connector screws (where applicable).

Initial installation and Power-up of a Stack

1. Install units in rack.
2. Install all stacking cables. Fully connect, including the redundant stack link. It is highly recommended that a redundant link be installed.
3. Identify the unit to be the master. Power this unit up first.
4. Monitor the console port. Allow this unit to come up to the login prompt. If unit has the default configuration, it should come up as unit #1, and will automatically become a master unit. If not, renumber as desired.
5. If desired, preconfigure other units to be added to the stack. Preconfiguration is described in Section "Preconfiguration".

6. Power on a second unit, making sure it is adjacent (next physical unit in the stack) to the unit already powered up. This will insure the second unit comes up as a member of the stack, and not a “Master” of a separate stack.
7. Monitor the master unit to see that the second unit joins the stack. Use the “show switch” command to determine when the unit joins the stack. It will be assigned a unit number (unit #2, if it has the default configuration).
8. Renumber this stack unit, if desired. See section “Renumber Stack Members” on recommendations for renumbering stack members.
9. Repeat steps 6 through 8 to add additional members to the stack. Always power on a unit adjacent to the units already in the stack.

Removing a Unit from the Stack

1. Make sure the redundant stack connection is in place and functional. All stack members should be connected in a logical ring.
2. Power down the unit to be removed.
3. Disconnect stack cables.
4. If unit is not to be replaced, reconnect the stack cable from the stack member above to the stack member below the unit being removed.
5. Remove unit from the rack.
6. If desired, remove the unit from the configuration by issuing the command:
   no member <unit-id>

Adding a Unit to an Operating Stack

1. Make sure the redundant stack connection is in place and functional. All stack members should be connected in a logical ring.
2. Preconfigure the new unit, if desired.
3. Install new unit in the rack. (Assumes installation below the bottom-most unit, or above the top-most unit).
4. Disconnect the redundant stack cable that connects the last unit in the stack back up to the first unit in the stack at the position in the ring where the new unit is to be inserted.
5. Connect this cable to the new unit, following the established order of “stack up” to “stack down” connections
6. Power up the new unit. Verify, by monitoring the master unit console port, that the new unit successfully joins the stack by issuing the **show switch** command. The new unit should always join as a “member” (never as master; the existing master of the stack should not change).
7. If the code version of the newly added member is not the same as the existing stack, update the code as described in section “Upgrading Firmware”.

Replacing a Stack Member with a New Unit

There are two possible situations here. First, if you replace a stack member of a certain model number with another unit of the same model, follow the process below:

- Follow the process in section "Removing a Unit from the Stack" to remove the desired stack member.
- Follow the process in section "Adding a Unit to an Operating Stack" to add a new member to the stack with the following exceptions:
  - Insert the new member in the same position in the stack as the one removed.
  - Preconfiguration described in step "Preconfigure the new unit, if desired." of that procedure is not required.

Second, if you replace a stack member with another unit of a different model number, use the following process:

- Follow the process in section "Removing a Unit from the Stack" to remove the desired stack member.
- Remove the now-absent stack member from the configuration by issuing the command **no member** command.
- Add the new stack unit to the stack using the process described in section "Adding a Unit to an Operating Stack". The unit can be inserted into the same position as the unit just removed, or the unit can be inserted at the bottom of the stack. In either case, make sure all stack cables are connected with the exception of the cable at the position where the new unit is to be inserted to insure that the stack does not get divided into two separate stacks, causing the election of a new master.

Renumber Stack Members

This example is provided as CLI commands and a Web interface procedure.

CLI: Renumbering Stack Members

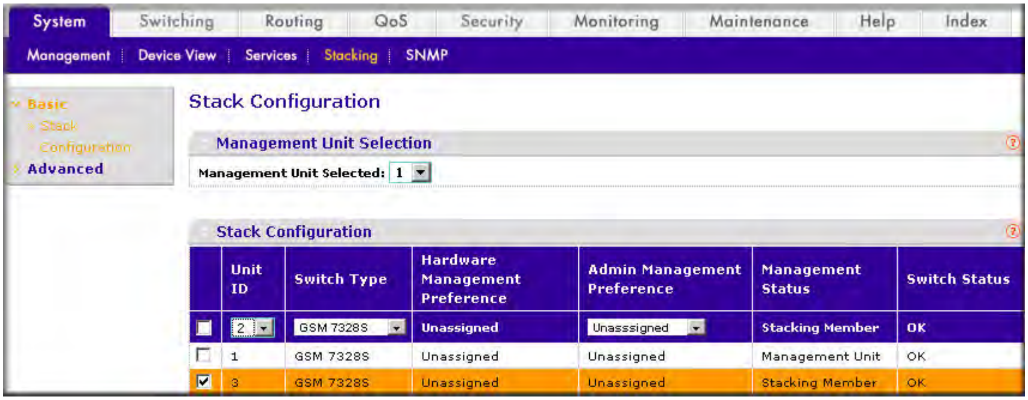
1. If particular numbering is required, it is recommended that stack members be assigned specific numbers when they are first installed and configured in the stack, if possible.
2. If the desired stack unit number for a particular unit is unused, a unit can be renumbered simply by using the **switch** <oldunit-id> **renumber** <newunit-id> CLI command. This command is found in global config mode.
3. If the newunit-id has been preconfigured, you may need to remove the newunit-id from the configuration before renumbering the unit.
4. If reassignment of multiple existing stack unit numbers is necessary, there are a number of implications in terms of mismatching of configuration. In this case, it is recommended that all units except the master be powered down and added back one at a time using the procedure in Section "Adding a Unit to an Operating Stack".

Web Interface: Renumbering Stack Members

To use the Web interface to renumber the stack number, proceed as follows:

1. Renumbering the stacking member’s ID from 3 to 2.

   a. From the main menu, select System > Management > Basic > Stack Configuration. A screen similar to the following displays.



Stack Configuration

Management Unit Selection

Management Unit Selected: 1

Stack Configuration

	Unit ID	Switch Type	Hardware Management Preference	Admin Management Preference	Management Status	Switch Status
☐	2	GSM 7328S	Unassigned	Unassigned	Stacking Member	OK
☐	1	GSM 7328S	Unassigned	Unassigned	Management Unit	OK
☑	3	GSM 7328S	Unassigned	Unassigned	Stacking Member	OK

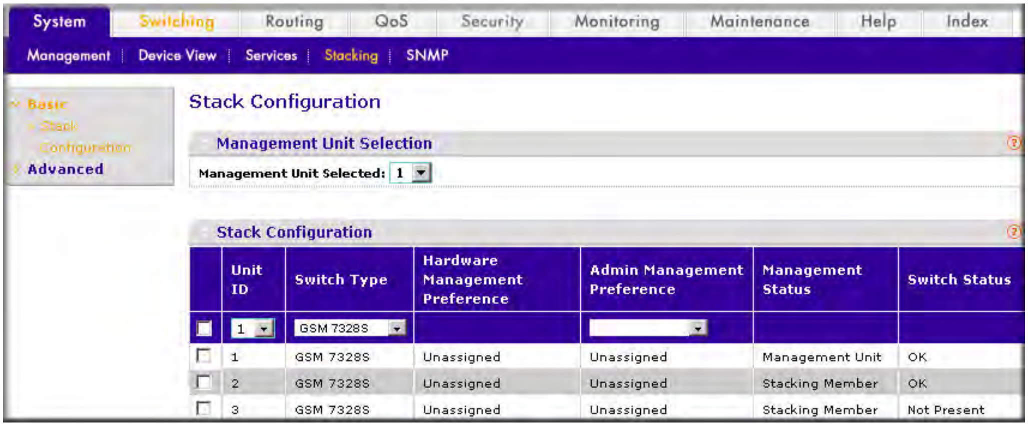
Figure 19-3

   b. Under Stack Configuration, scroll down to Unit ID **3** and select the checkbox for 3. 3 now appears in the Interface field at the top.

   c. Select **2** in the Unit ID field.

   d. Click **Apply**.

   e. Now the unit ID of the stacking member is 2.



Stack Configuration

Management Unit Selection

Management Unit Selected: 1

Stack Configuration

	Unit ID	Switch Type	Hardware Management Preference	Admin Management Preference	Management Status	Switch Status
☐	1	GSM 7328S				
☐	1	GSM 7328S	Unassigned	Unassigned	Management Unit	OK
☐	2	GSM 7328S	Unassigned	Unassigned	Stacking Member	OK
☐	3	GSM 7328S	Unassigned	Unassigned	Stacking Member	Not Present

Figure 19-4

Moving a Master to a Different Unit in the Stack

This example is provided as CLI commands and a Web interface procedure.

CLI: Moving a Master to a Different Unit in the Stack

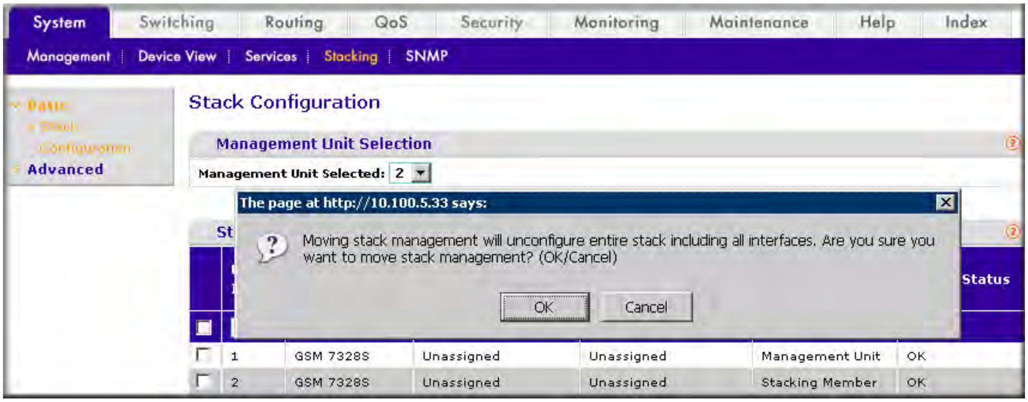
1. Using the **movemanagement** command, move the master to the desired unit number. The operation may take between 30 seconds and 3 minutes depending on the stack size and configuration. The command is **movemanagement** <fromunit-id> <tounit-id>
2. Make sure that you can log in on the console attached to the new master. Use the **show switch** command to verify that all units rejoined the stack.
3. It is recommended that the stack be reset with the **reload** command after moving the master.

Web Interface: Moving a Master to a Different Unit in the Stack

To use the Web interface to move a master to a another unit, proceed as follows:

1. Move a master from unit 1 to unit 2.

   a. From the main menu, select System > Management > Basic > Stack Configuration. A screen similar to the following displays.



Stack Configuration

Management Unit Selection

Management Unit Selected: 2

The page at http://10.100.5.33 says:

Moving stack management will unconfigure entire stack including all interfaces. Are you sure you want to move stack management? (OK/Cancel)

□	1	GSM 7328S	Unassigned	Unassigned	Management Unit	OK
□	2	GSM 7328S	Unassigned	Unassigned	Stacking Member	OK

Figure 19-5

   b. Select **2** in the Management Unit Selected field.

   c. A warning window is popped up, click the **OK** button

d. Click the **Apply**.

> **Note:** If you move a master to a different unit, you may lose the connection to the switch because the IP address may be changed if the switch gets IP address using DHCP.

Removing a Master Unit from an Operating Stack

1. First, move the designated master to a different unit in the stack using "Moving a Master to a Different Unit in the Stack".
2. Second, using "Removing a Unit from the Stack", remove the unit from the stack.

Merging Two Operational Stacks

It is strongly recommended that two functioning stacks (each having an independent master) not be merged simply by the reconnection of stack cables. That process may result in a number of unpredictable results and should be avoided.

1. Always power off all units in one stack before connecting into another stack.
2. Add the units as a group by unplugging one stacking cable in the operational stack and physically connecting all unpowered units at that point.
3. Completely cable the stacking connections, making sure the redundant link is also in place.
4. Then, power up each unit, one at a time, by following "Adding a Unit to an Operating Stack".

Preconfiguration

All configuration on the stack except unit numbers is stored on the management unit. This means that a stack unit may be replaced with another device of the same type without having to reconfigure the switch. Unit numbers are stored independently on each switch, so that after power cycling the stack the units always come back with the same unit numbers. The unit type associated with each unit number may be learned by the management unit automatically as the units are connected or preconfigured by the administrator.

1. Issue the **member** <unit-id> <switchindex> command to preconfigure a unit. Supported unit types are shown by the **show supported switchtype** command.
2. Next, configure the unit you just defined with configuration commands, just as if the unit were physically present.
3. Ports for the preconfigured unit come up in "detached" state and can be seen with the **show port all** command. The detached ports may now be configured for VLAN membership and any other port-specific configuration.

4. After a unit type is preconfigured for a specific unit number, attaching a unit with different unit type for this unit number causes the switch to report an error. The **show switch** command indicates "config mismatch" for the new unit and the ports on that unit don't come up. To resolve this situation the customer may change the unit number of the mismatched unit or delete the preconfigured unit type using the **no member** <unit-id> command.

Upgrading Firmware

New code is downloaded via TFTP or xmodem to the management unit using the **copy** command. Once code is successfully loaded on the management unit, it automatically propagates the code to the other units in the stack. If some error occurs during code propagation to stack units then the **archive** command (in stack configuration mode) may be issued to make another attempt to copy the software to the unit(s) that did not get updated. Errors during code propagation to stack members could be caused by stack cable movement or unit reconfiguration during the propagation phase. An error could also occur in the presence of excessive network traffic (such as a broadcast event).

All units in the stack must run the same code version. Ports on stack units that don't match the management unit code version don't come up and the **show switch** command shows a "code mismatch" error. To resolve this situation the administrator may issue **archive** command. This command copies management unit's software to the other units with mismatched code version. Before issuing this command, be sure the code running on the management unit is the desired code revision for all units in the stack. Once code is loaded to all members of the stack, the units must be reset in order for the new code to start running.

Migration of Configuration With a Firmware Upgrade

In some cases, a configuration may not be carried forward in a code update. For updates where this issue is to be expected, the following procedure should be followed:

1. Save the current configuration by uploading it from the stack, using the copy command from the CLI.
2. Load new code into the stack manager. Reboot the stack.
3. Upon reboot, go into the boot menu and erase the configuration ("restore to factory defaults")
4. Continue with boot of operational code.
5. Once the stack is up, download the saved configuration back to the master. This configuration should then be automatically propagated to all members of the stack.

Code Mismatch

If a unit is added to a stack and it does not have the same version of code as that of the master, the following should happen:

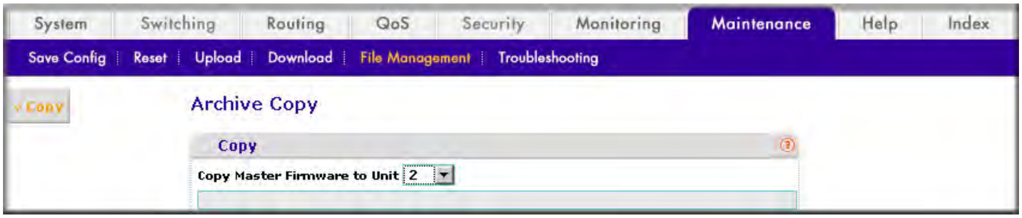
- The "new" unit will boot up and become a "member" of the stack.

- Ports on the added unit should remain in the “detached” state.
- A message should appear on the CLI indicating a code mismatch with the newly added unit.
- To have the newly added unit to merge normally with the stack, code should be loaded to the newly added unit from the master using the copy command. The newly added member should then be reset, and should reboot normally and join the stack.

Web Interface: Upgrading Firmware

To use the Web interface to upgrade a stack member from a master, proceed as follows:

1. From the main menu, select System > Management > Basic > Stack Configuration. A screen similar to the following displays.



Copy Master Firmware to Unit 2

Figure 19-6

2. Select **2** in the Copy Master Firmware to Unit field.

3. Click **Apply**.

Chapter 20 SNMP

In this chapter, the following examples are provided:

- “Add a New Community”
- “Enable SNMP Trap” on page 20-2
- “Configure SNMP V3” on page 20-3
- “sFlow” on page 20-5
- “Configure Time-Based Sampling of Counters with sFlow” on page 20-9

Add a New Community

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

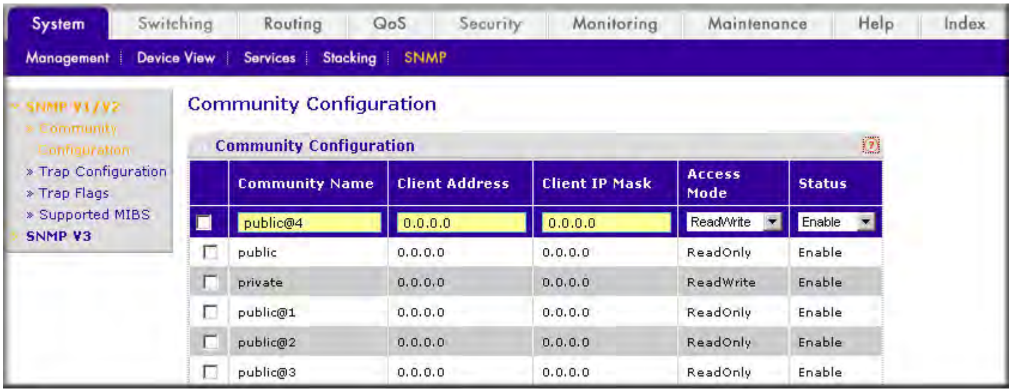
CLI: Adding a New Community

```
(Netgear switch) #config
(Netgear switch) (Config)#snmp-server community rw public@4
```

Web Interface: Adding a New Community

To use the Web interface to add a new community, proceed as follows:

1. From the main menu, 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

Figure 20-1

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. Select the **Read/Write** in the Access Mode field.
6. Select the **Enable** in the Status field.
7. Click the **Add**.

Enable SNMP Trap

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

CLI: Enabling SNMP Trap

This example shows how to send SNMP trap to the SNMP server.

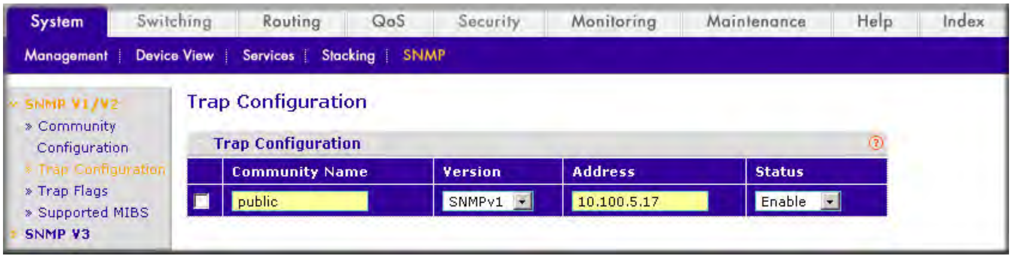
```
(Netgear switch) #config
(Netgear switch) (Config)# snmptrap public 10.100.5.17
                                    Enable send trap to SNMP server 10.100.5.17
(Netgear switch) (Config)#snmp-server traps linkmode
                                     Enable send link status to the SNMP server
when link status changes.
```

Web Interface: Enabling SNMP Trap

To use the Web interface to add a new community, proceed as follows:

1. Enable send SNMP trap to the server 10.100.5.17.

   a. From the main menu, select System > SNMP>SNMP V1/V2>Trap Configuration. A screen similar to the following displays.



Trap Configuration

	Community Name	Version	Address	Status
□	public	SNMPv1	10.100.5.17	Enable

Figure 20-2

   b. In the Community Name field, enter **public**.

   c. Select **SNMPv1** in the Version field.

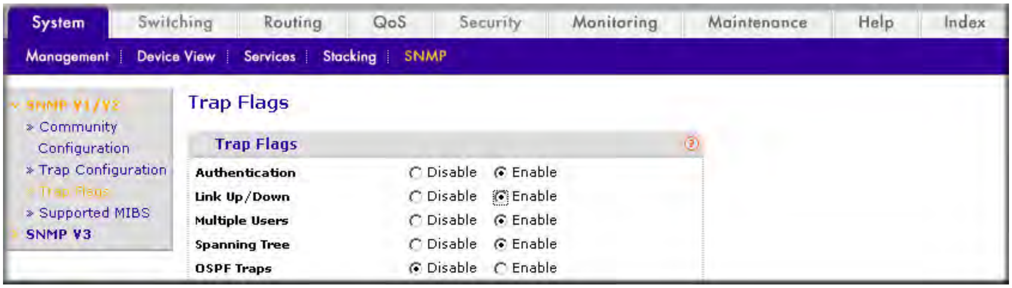
   d. In the Address field, enter **10.100.5.17**.

   e. Select **Enable** in the Status field.

   f. Click the **Add** button.

2. Set the Link Up/Down flag.

   a. From the main menu, 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

Figure 20-3

   b. Next to the Link Up/Down field, select the **Enable** radio button.

   c. Click the **Apply** button.

Configure SNMP V3

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

CLI: Configuring SNMP V3

This example shows how to configure SNMP v3 on the NETGEAR switches.

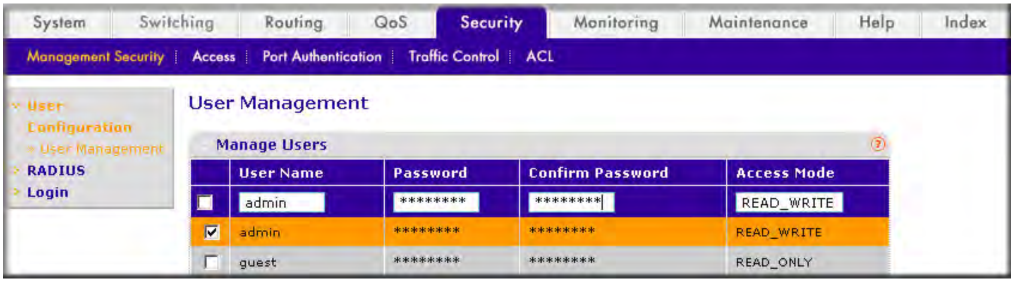
```
(Netgear Switch) #config
(Netgear Switch) (Config)#users passwd admin
Enter old password:
Enter new password:12345678
Confirm new password:12345678
Password Changed!
      change the password to “12345678”
(Netgear Switch) (Config)#users snmpv3 authentication admin md5
      Set the authentication 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: Configuring SNMP V3

1. Change the user password.

If you set the authentication mode to md5, you must make the length of password longer than 8 characters.

a. From the main menu, 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

Figure 20-4

b. Under User Management, scroll down to User Name **admin** and select the checkbox for admin. admin now appears in the Interface field at the top.

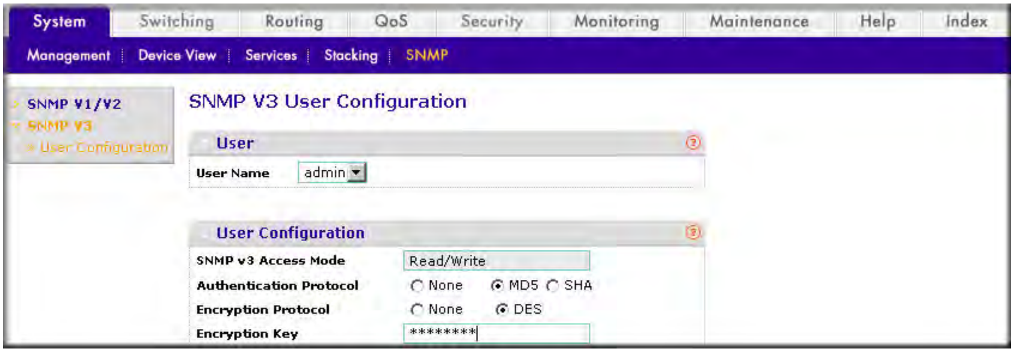
c. In the Password field, enter **12345678**.

d. In the Confirm Password field, enter **12345678**

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

2. Configure SNMP V3 user.

a. From the main menu, 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: ********

Figure 20-5

- **b.** Select the **admin** in the User Name field.
- **c.** Next to Authentication Protocol, click the **MD5** radio button.
- **d.** Next to the Encryption Protocol, click the **DES** radio button.
- **e.** In the Encryption Key field, enter **12345678**.
- **f.** Click the **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 a 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 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.

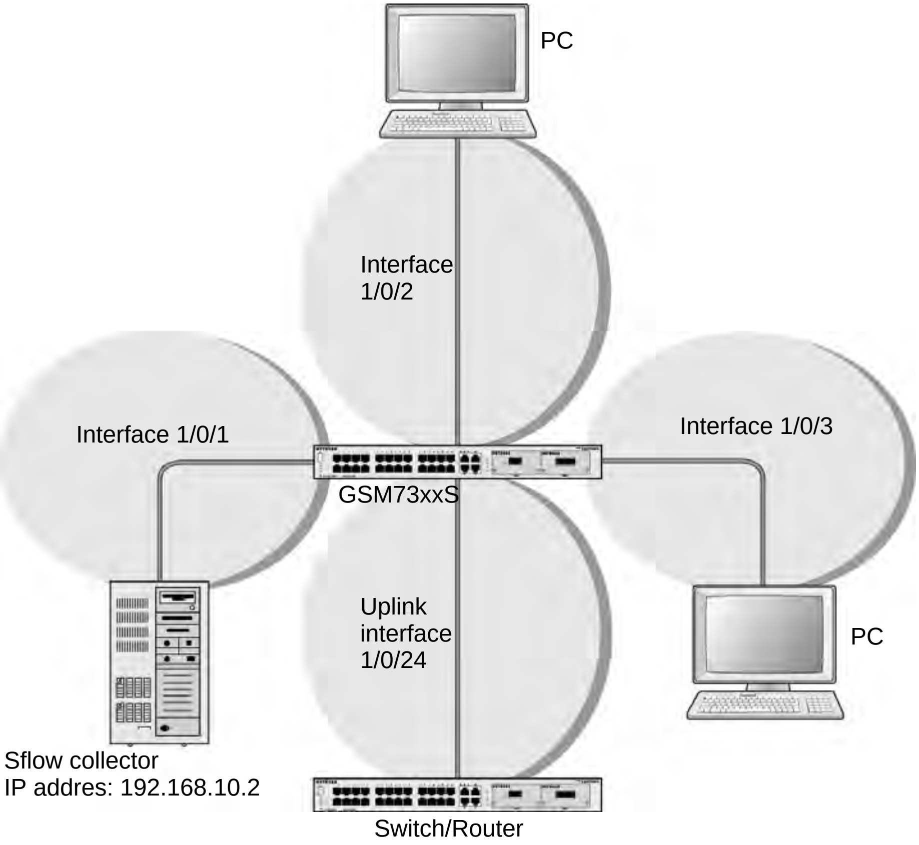


Figure 20-6

CLI: Configuring Statistical Packet-Based Sampling of Packet Flows with sFlow

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
```

Configure the sFlow receiver timeout. Here sFlow samples will be sent to this receiver for the duration of 31536000 seconds. That is approximately one year.

```
(Netgear Switch) (Config)# sflow receiver 1 owner NetMonitor timeout 31536000
```

Here the max datagram size is default 1400. It can be modified to a value between 200 to 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) #
```

Configure sampling ports sFlow receiver index, sampling rate, sampling max header size. It has to be repeated 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
```

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: Configuring Statistical Packet-based Sampling with sFlow

1. Configure the sFlow receiver IP address.

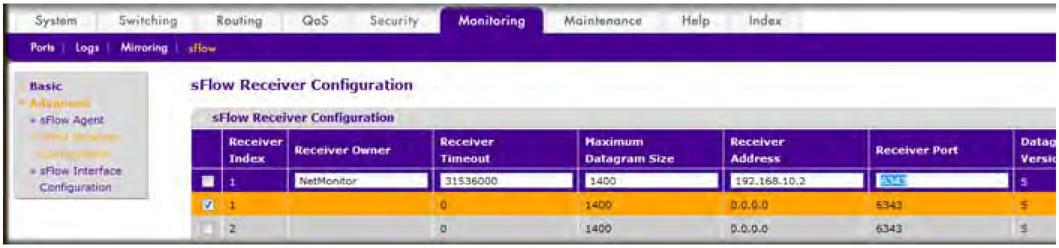
   a. From the main menu, select Monitoring > sFlow > Advanced > sFlow Receiver Configuration.

   b. Select the check box against 1.

   c. Enter Receiver Owner as **NetMonitor**.

   d. Enter Receiver Timeout as **31536000**.

e. Enter Receiver Address as **192.168.10.2**. A screen similar to the following displays.



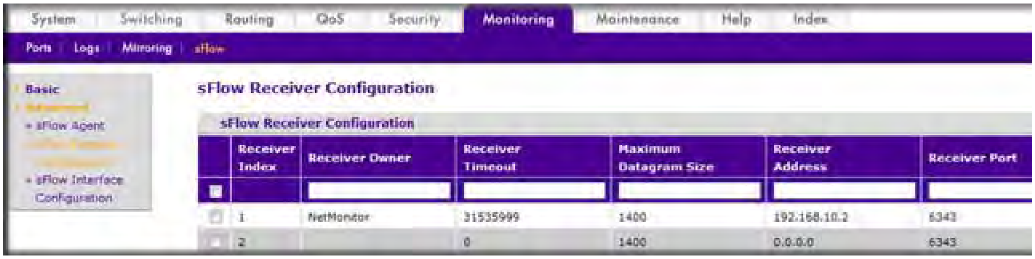
sFlow Receiver Configuration

sFlow Receiver Configuration

	Receiver Index	Receiver Owner	Receiver Timeout	Maximum Datagram Size	Receiver Address	Receiver Port	Datag Versi
□	1	NetMonitor	31536000	1400	192.168.10.2	[illegible]	5
☑	1		0	1400	0.0.0.0	6343	5
□	2		0	1400	0.0.0.0	6343	5

Figure 20-7

f. Click **Apply**. At the end of this configuration a screen similar to the following displays.



sFlow Receiver Configuration

sFlow Receiver Configuration

	Receiver Index	Receiver Owner	Receiver Timeout	Maximum Datagram Size	Receiver Address	Receiver Port
□						
□	1	NetMonitor	31535999	1400	192.168.10.2	6343
□	2		0	1400	0.0.0.0	6343

Figure 20-8

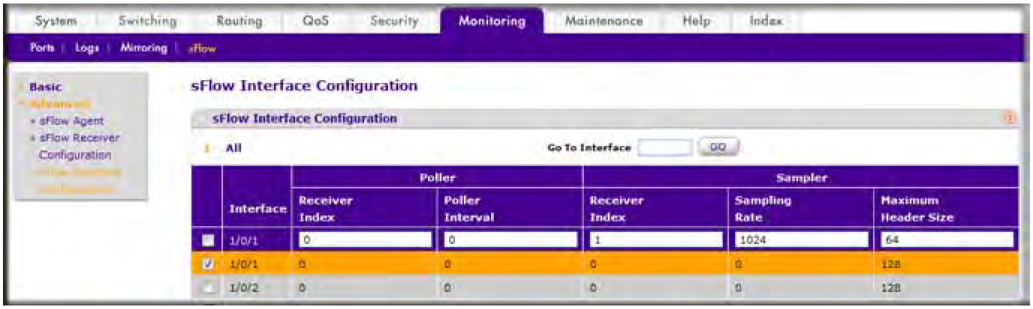
2. Configure sampling ports sFlow receiver index, sampling rate, sampling max header size.

a. From the main menu, select Monitoring -> sFlow -> Advanced -> sFlow Interface Configuration.

b. Select the check box against the interface 1/0/1.

c. Enter Sampling Rate as **1024**.

d. Enter Maximum Header Size as 64. A screen similar to the following displays.



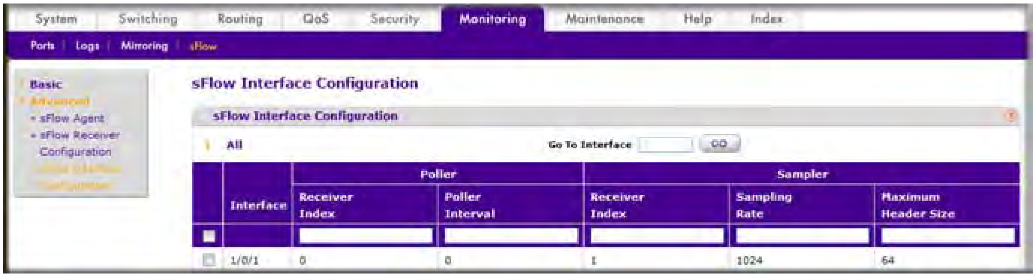
sFlow Interface Configuration

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

Figure 20-9

e. Click **Apply**. At the end of this 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

Figure 20-10

Configure Time-Based Sampling of Counters with sFlow

CLI: Configuring Time-Based Sampling of Counters with sFlow

Configure sampling ports sFlow receiver index, polling interval. It has to be repeated 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
```

View the polling port configurations.

```
(GSM7328S) #show sflow pollers

Poller                   Receiver         Poller
Data Source        Index              Interval
-----------          ---------             ---------
1/0/1                       1                    300
```

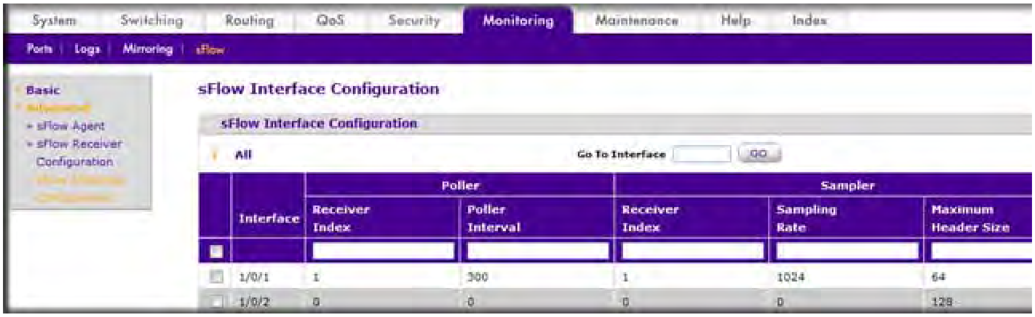
Web Interface: Configuring Time-Based Sampling of Counters with sFlow

1. Configure sampling ports sFlow receiver index, polling interval.

a. From the main menu, select Monitoring > sFlow > Advanced > sFlow Interface Configuration.

b. Select the check box against the interface **1/0/1**.

c. Enter the Poller Interval as **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

Figure 20-11

d. Click **Apply**.

Chapter 21
DNS

In this chapter, the following examples are provided:

- "Specify Two DNS Servers"
- "Manually Add a Host Name and an IP Address" on page 21-2

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
- 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: Specifying Two DNS Servers

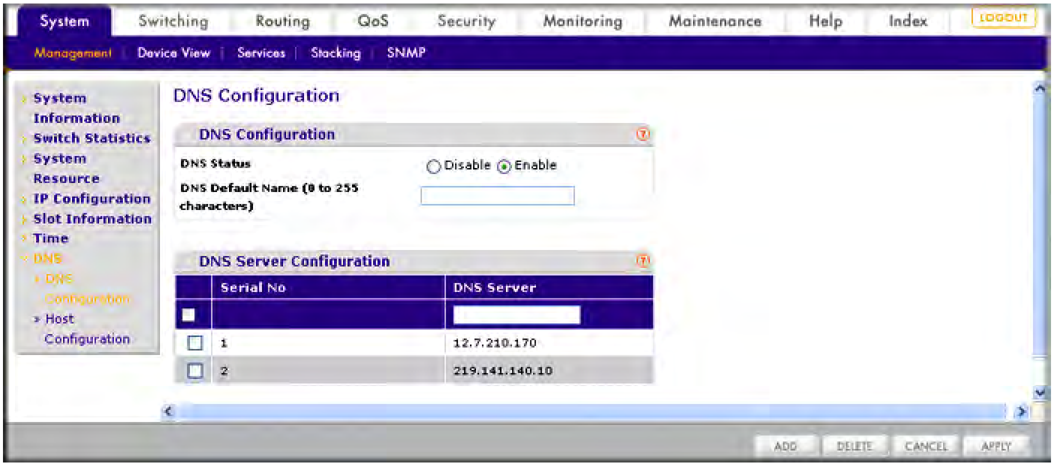
To use the CLI to specify two DNS servers, enter the following CLI commands:

```
(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: Specifying Two DNS Servers

To use the Web interface to specify two DNS servers, proceed as follows:

1. From the main menu, 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

Figure 21-1

2. Under DNS Server Configuration, in the DNS Server field, enter **12.7.210.170**.
3. Click **Add**.
4. Under DNS Server Configuration, 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 Example: Manually Adding a Host Name and an IP Address

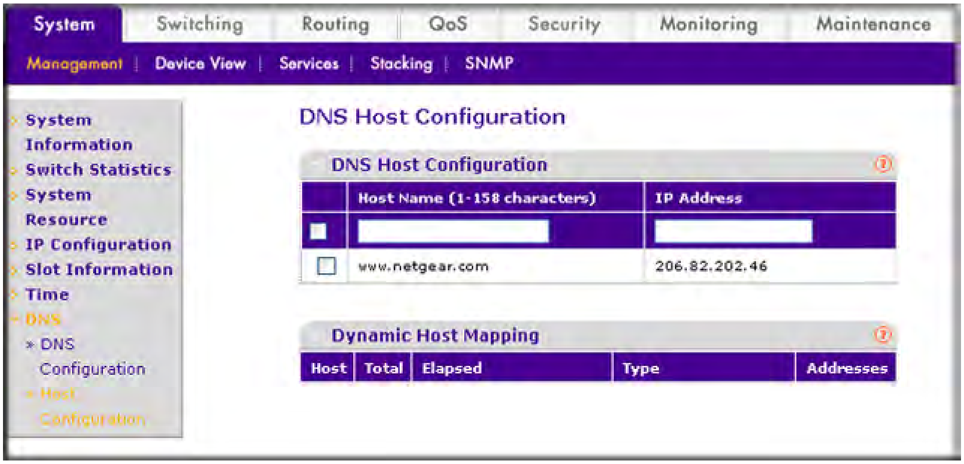
To use the CLI to manually add a host name and an IP address, enter the following CLI commands:

```
(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 Adding a Host Name and an IP Address

To use the Web interface to manually add a host name and an IP address, proceed as follows:

1. From the main menu, 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

Figure 21-2

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.

Chapter 22
DHCP Server

This section describes the DHCP server configuration. 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.
- 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: Configuring a DHCP Server in Dynamic Mode

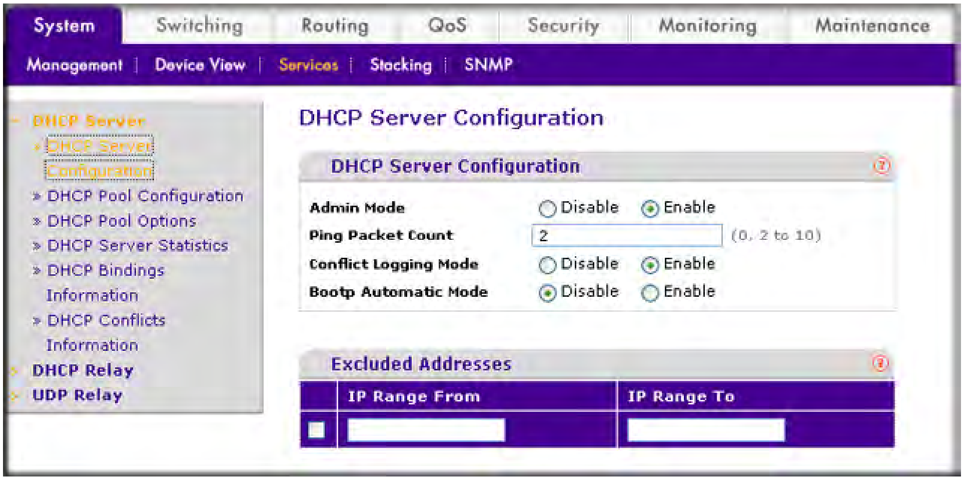
To use the CLI to create a DHCP server with a dynamic pool, enter the following CLI commands:

```
(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
```

Web Interface: Configuring a DHCP Server in Dynamic Mode

To use the Web interface to create a DHCP server with a dynamic pool, proceed as follows:

1. From the main menu, 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 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

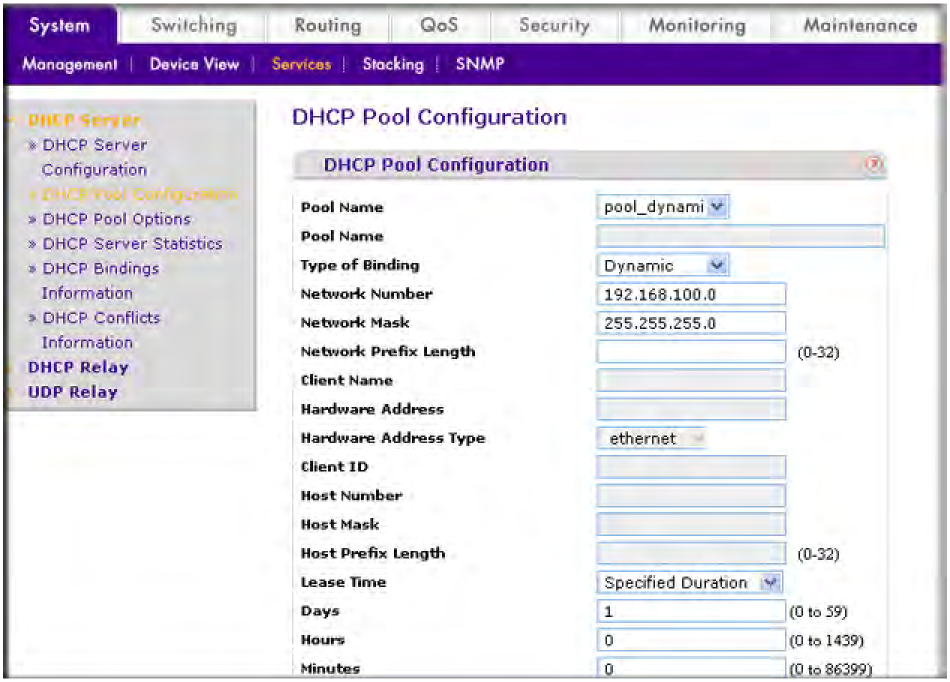
	IP Range From	IP Range To
□		

Figure 22-1

2. Next to Admin Mode, select the **Enable** radio button.

3. Click **Apply** to enable the DHCP service.

4. From the main menu, 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_dynami	
Pool Name		
Type of Binding	Dynamic	
Network Number	192.168.100.0	
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)

Figure 22-2

5. Under DHCP Pool Configuration, enter the following information:

- Select **Create** in the Pool Name field.
- In the Pool Name field, enter **pool_dynamic**.
- Select **Dynamic** in the Type of Binding field.
- 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.
- In the Days field, enter **1**.

6. Click **Add**. The pool_dynamic name is now added to the Pool Name drop-down list.

Configure a DHCP Reservation

The following example shows how to create a DHCP server with an IP address pool that is making fixed IP to MAC address assignments. The example is shown as CLI commands and as a Web interface procedure.

CLI: Configuring a DHCP Reservation

To use the CLI to create a DHCP server with a with a manual pool, enter the following CLI commands:

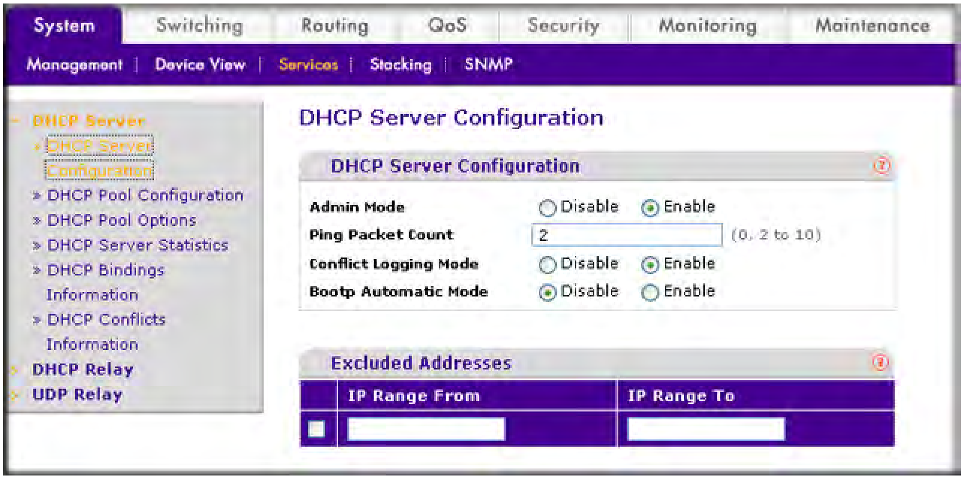
```
(Netgear Switch)#config
(Netgear Switch) (Config)#service dhcp
(Netgear Switch) (Config)#ip dhcp pool pool_manual
(Netgear Switch) (Config)#client-name dhcpclient
(Netgear Switch) (Config)#hardware-address 00:01:02:03:04:05
(Netgear Switch) (Config)#host 192.168.200.1 255.255.255.0
(Netgear Switch) (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: Configuring a DHCP Reservation

To use the Web interface to create a DHCP server with a manual pool, proceed as follows:

1. From the main menu, 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

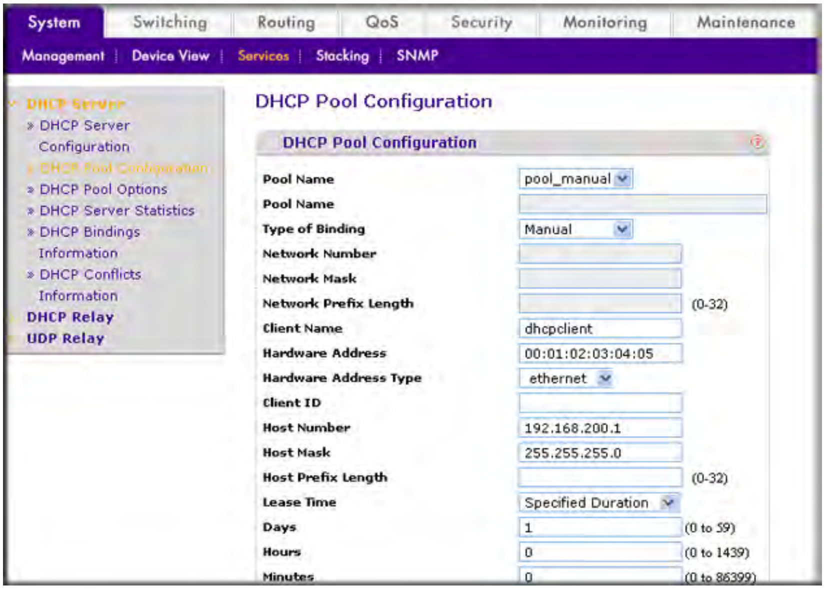
	IP Range From	IP Range To
□		

Figure 22-3

2. Next to Admin Mode, select the **Enable** radio button.

3. Click **Apply** to enable the DHCP service.

4. From the main menu, select System > Services > DHCP Server > DHCP Pool Configuration. A screen similar to the following displays.



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)

Figure 22-4

5. Under DHCP Pool Configuration, enter the following information:
   - Select **Create** in the Pool Name field.
   - In the **Pool Name** field, enter **pool_manual**.
   - Select **Manual** in the Type of Binding field.
   - In the Client Name field, enter **dhcpclient**.
   - In the Hardware Address field, enter **00:01:02:03:04:05**.
   - Select **ethernet** in the Hardware Type field.
   - 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.

Chapter 23
Double VLANs

This section describes how to configure the Double VLAN (DVLAN) feature on the switch. A DVLAN is a way to pass traffic of customers who have multiple VLANs from one customer domain to another customer domain. Custom VLAN IDs are preserved and a provider service VLAN ID is added to the traffic so that the traffic can pass the metro core in a simple and cost-effective manner.

Double VLANs:

- Pass customer traffic from one customer domain to another through the metro core
- Select customer ports and a service provider port

In the following example, the two switches have the same configuration.

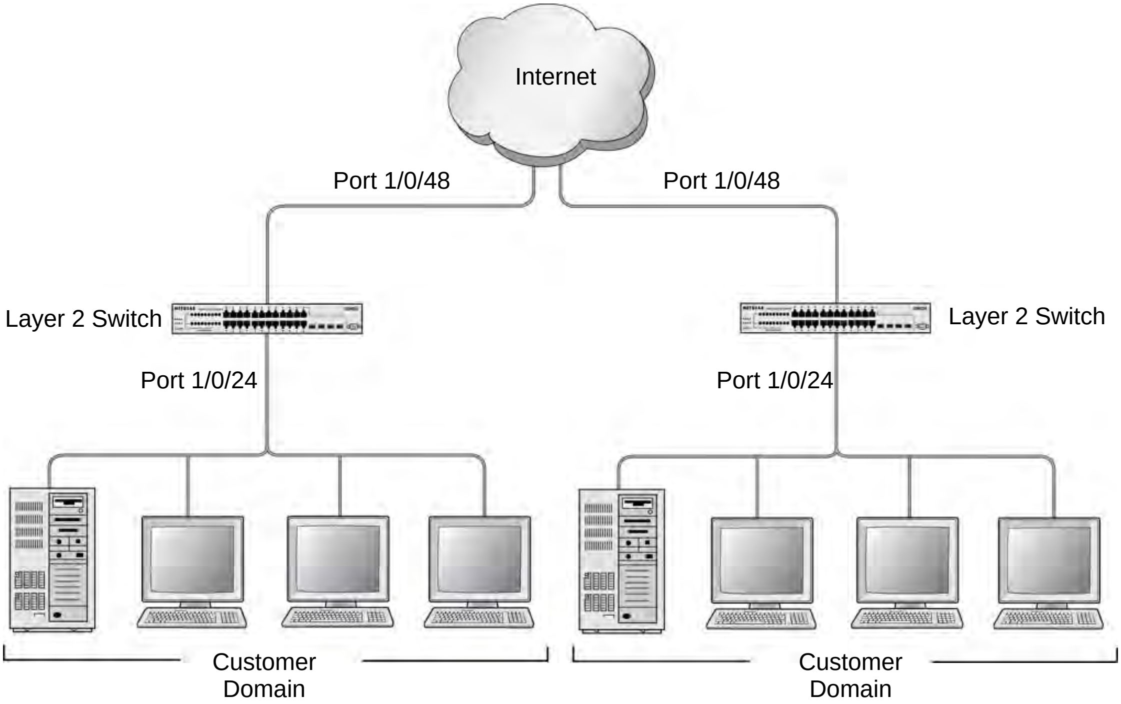


Figure 23-1

Enable a Double VLAN

The following example shows how to configure the switch (the NETGEAR switch) 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. The two NETGEAR switches have the same configuration.

CLI: Enabling a Double VLAN on a VLAN

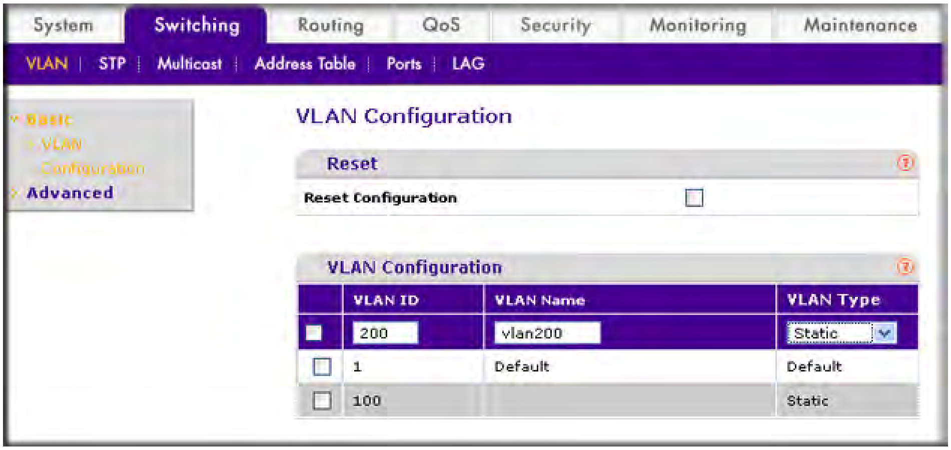
```
Create a VLAN 200.
(Netgear Switch)#vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#exit

Add interface 1/0/24 to VLAN 200, add pvid 200 to the 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: Enabling a Double VLAN on a VLAN

To use the Web Interface to enable a double VLAN on a VLAN, proceed as follows:

1. Create static VLAN 200:

a. From the main menu, 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

Figure 23-2

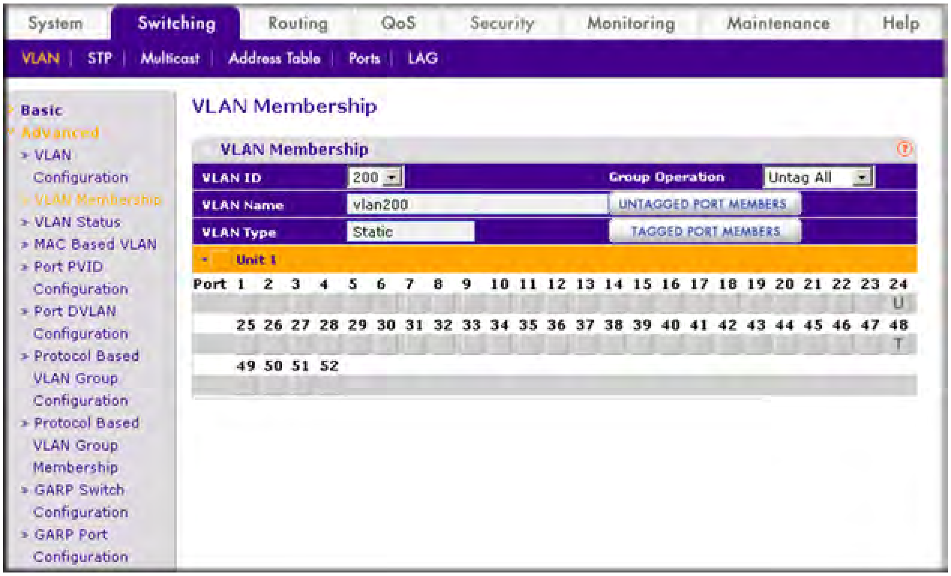
b. Under VLAN Configuration, enter the following information and make the following selection:

- In the VLAN ID field, enter **200**.
- In the VLAN Name field, enter **vlan200**.
- Select **Static** in the VLAN Type field.

c. Click **Add**.

2. Add ports 24 and 48 to VLAN 200.

a. From the main menu, 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		

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																				

Figure 23-3

b. Under VLAN Membership, select **200** in the VLAN ID field.

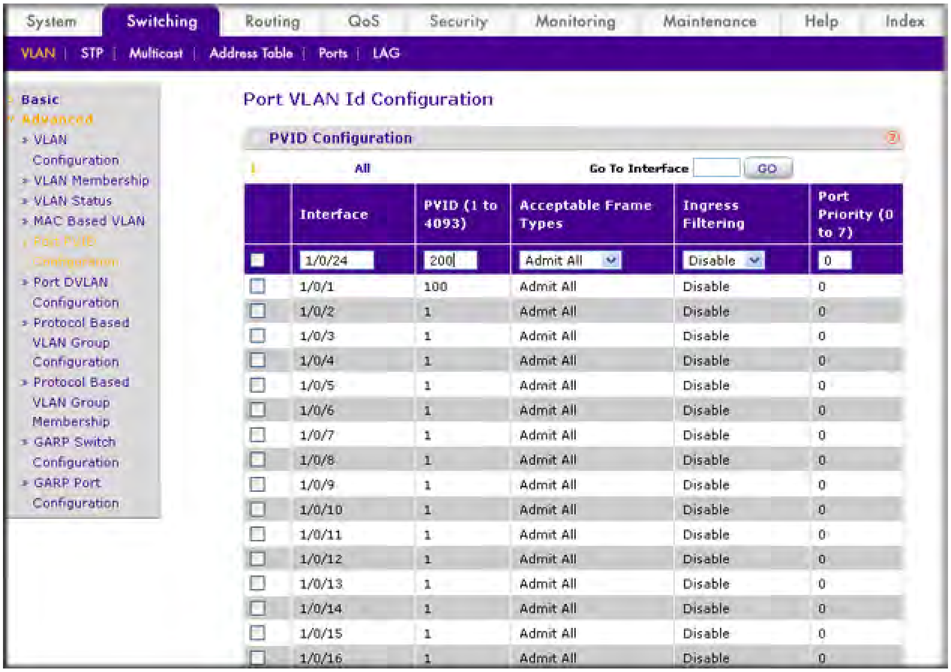
c. Click **Unit 1**. The ports display:

- 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. From the main menu, 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)
☐	1/0/24	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

Figure 23-4

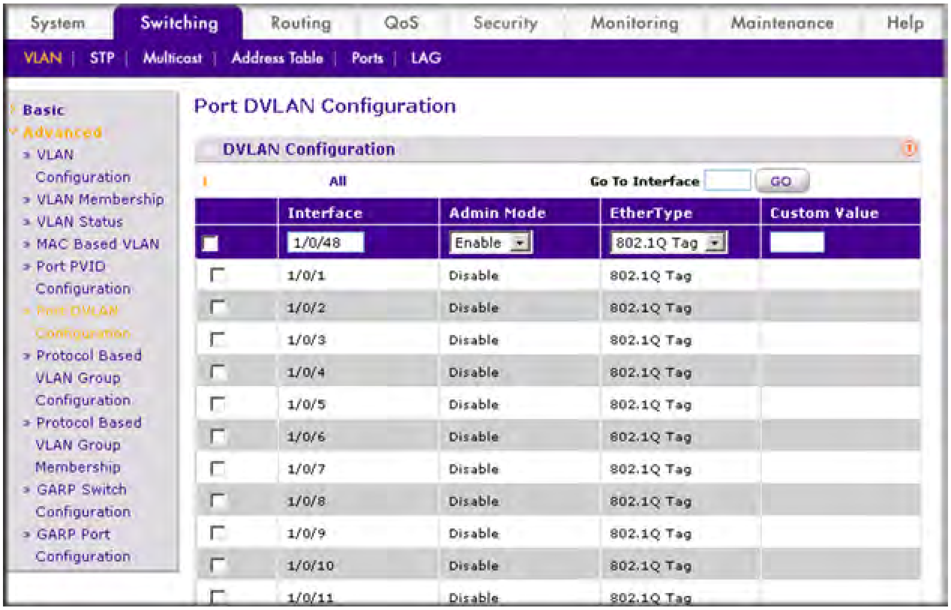
   b. Under PVID Configuration, scroll down to interface 1/0/24 and select the chechbox for that interface. Now 1/0/24 appears in the Interface field at the top.

   c. Under PVID Configuration, 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. From the main menu, select Switching > VLAN > Advanced > Port DVLAN Configuration. A screen similar to the following displays.



Port DVLAN Configuration

DVLAN Configuration

All   Go To Interface [ ] GO

	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	

Figure 23-5

b. Under DVLAN Configuration, scroll down to interface 1/0/48 and select the chechbox for that interface. Now 1/0/48 appears in the Interface field at the top.

c. Select **Enable** in the Admin Mode field.

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

Chapter 24
Private VLAN Groups

The private VLAN Group allows network administrator 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. By default, the mode is “community” mode that 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.

Create a Private VLAN Group

The following example creates two groups. the group1 is in “community” mode and the group2 is in “isolated” mode.

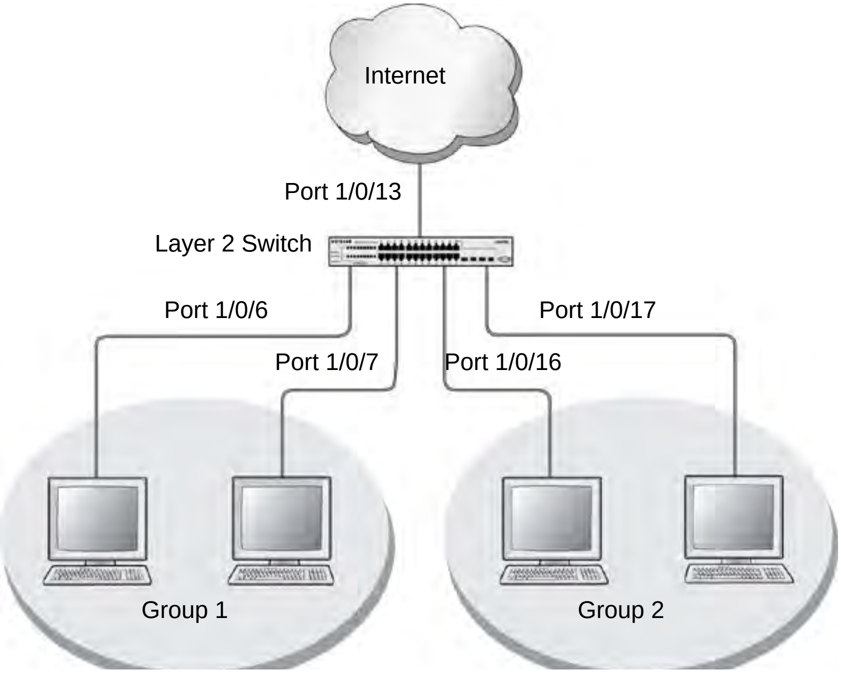


Figure 24-1

CLI: Creating a Private VLAN Group

```
(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
```

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
```

Create a private group with community mode.

```
(Netgear Switch) (Config)#private-group name group2 2 mode  isolated
```

Create a private group with 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
```

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
```

Add 1/0/16 and 1/0/7 to the private group 2.

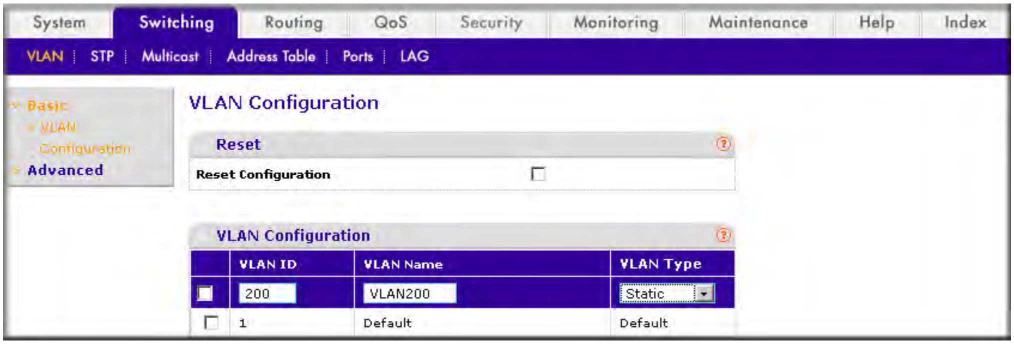
```
(Netgear Switch) (conf-if-range-1/0/16-1/0/17)#exit
```

Web Interface: Creating a Private VLAN Group

To use the Web interface, proceed as follows:

1. Create a VLAN 200.

a. From the main menu, 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

Figure 24-2

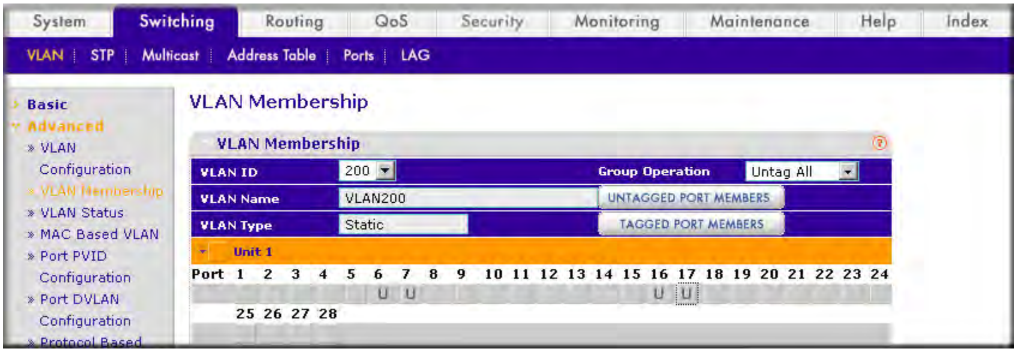
b. Enter the following information in the VLAN Configuration.

- In the VLAN ID field, enter **200**.
- In the VLAN Name field, enter **VLAN200**.
- Select **Static** in the VLAN Type field.

c. Click **Add**.

2. Add port 1/0/6, 1/0/7, 1/0/16 and 1/0/17 to the VLAN 200.

a. From the main menu, 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

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							

	25	26	27	28

Figure 24-3

b. In the VLAN Membership, select **200** in the VLAN ID field.

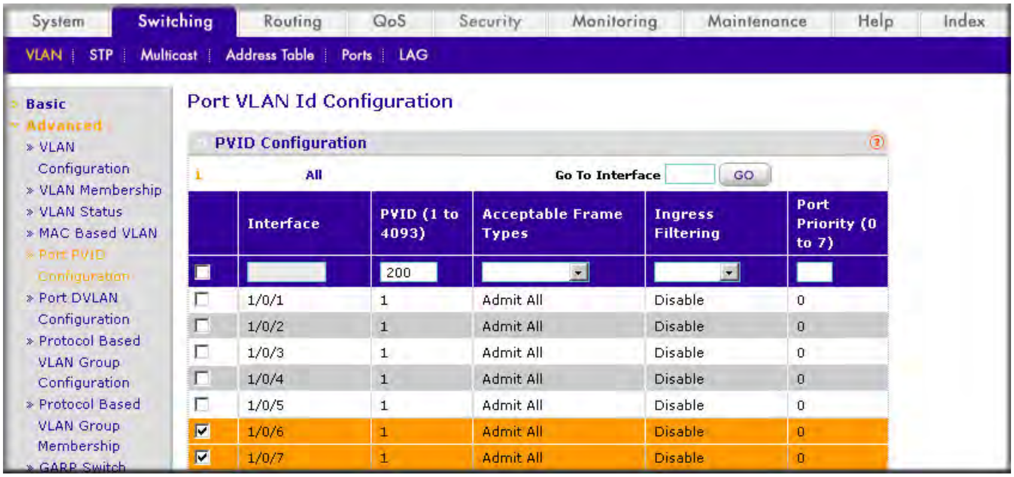
c. Click the **Unit 1.** The Ports display.

d. Click the gray box under port **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 port 1/0/6, 1/0/7, 1/0/16 and 1/0/17.

a. From the main menu, select Switching > VLAN> Advanced > Port PVID Configuraton. 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

Figure 24-4

b. Under PVID Configuration, scroll down to interface 1/0/6,1/0/7,1/0/16 and 1/0/17 and select the checkbox for that interface.

c. Under PVID Configuration, enter **200** in the PVID(1 to 4093) field.

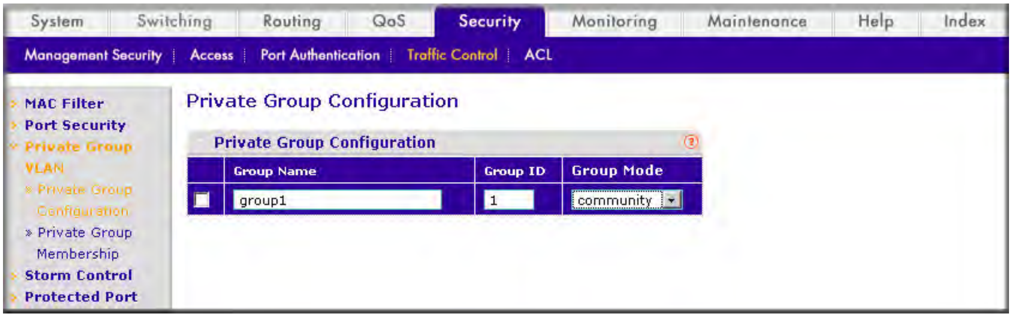
d. Under PVID Configuration, select **Admit All** in the Acceptable Frame Type field.

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

4. Create a private group, group1.

a. From the main menu, 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

Figure 24-5

b. In the Group Name field, enter **group1**.

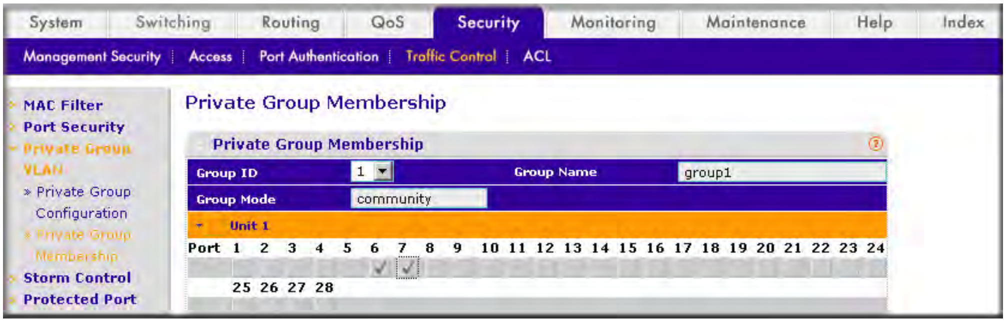
c. In the Group ID field, enter **1**.

d. Select **community** in the Group Mode field.

e. Click **Add**.

5. Add the port 6,7 to the group1.

a. From the main menu, 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
						✓	✓																	
	25	26	27	28																				

Figure 24-6

b. In the Private Group Membership, select **1** in the Group ID field.

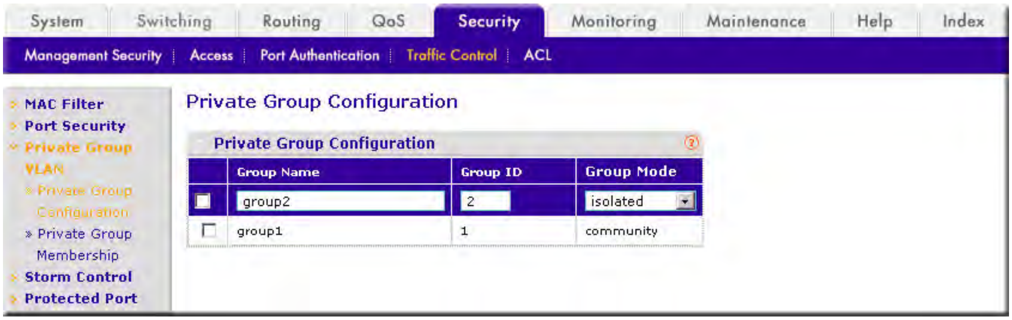
c. Click the **Unit 1.** The Ports display.

d. Click the gray box under port **6** and **7** one flag appears in the box.

e. Click **Apply.**

6. Create a private group, group2.

a. From the main menu, 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

Figure 24-7

b. In the Group Name field, enter **group2**.

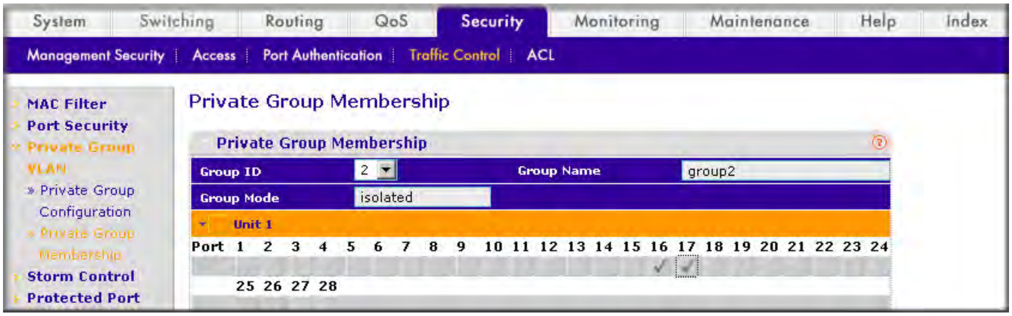
c. In the Group ID field, enter **2**.

d. Select **isolated** in the Group Mode field.

e. Click **Add**.

7. Add the port 16,17 to the group2.

a. From the main menu, 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																				

Figure 24-8

b. In the Private Group Membership, select **2** in the Group ID field

c. Click the **Unit 2.** The Ports display.

d. Click the gray box under port **16** and **17,** and one flag appears in the box.

e. Click **Apply**.

Chapter 25
Spanning Tree Protocol

In this chapter, the following examples are provided:

- "Configure Classic STP (802.1d)"
- "Configure Rapid STP (802.1w)" on page 25-3
- "Configure Multiple STP (802.1s)" on page 25-4

The purpose of spanning tree is to eliminate the 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: Configuring Classic STP (802.1d)

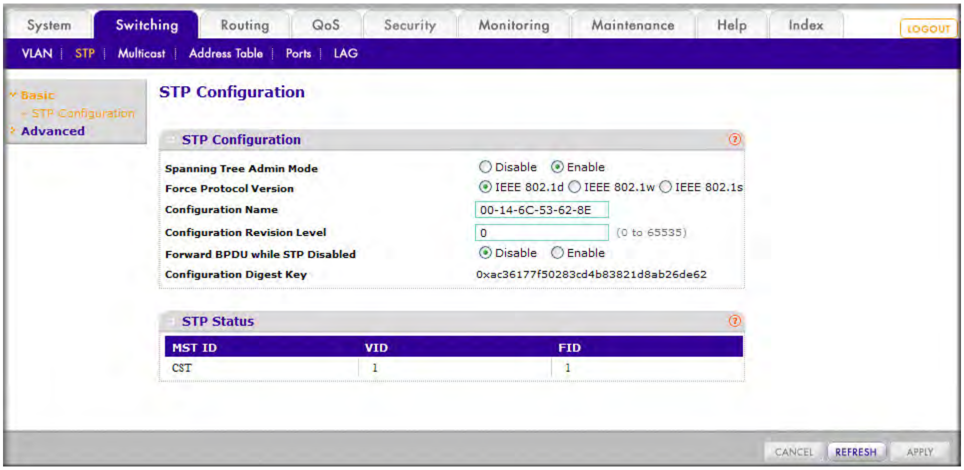
```
(Netgear Switch) (Config)# spanning-tree
(Netgear Switch) (Config)# spanning-tree forceversion 802.1d
(Netgear switch) (Interface 1/0/3)# spanning-tree port mode
```

Web Interface:Configuring Classic STP (802.1d)

To use the Web interface to configure the managed switch, proceed as follows:

1. Enable 802.1d on the switch.

a. From the main menu, 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

Figure 25-1

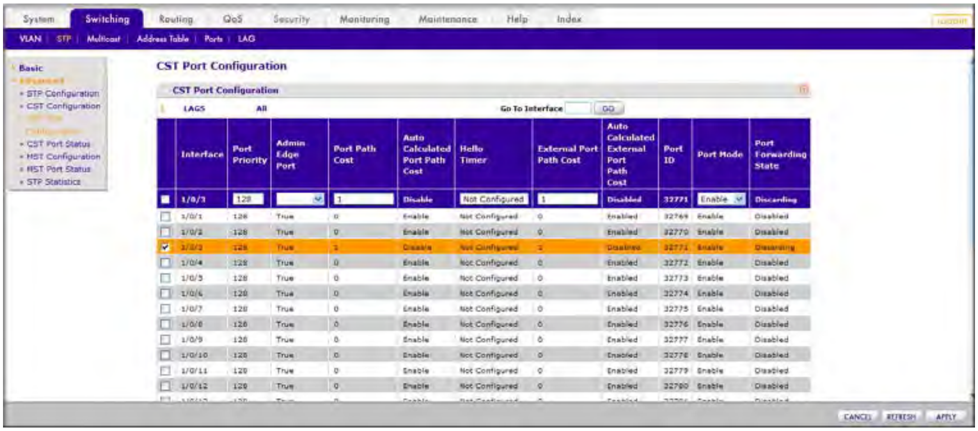
b. Enter the following information in the STP Configuration.

- Next to the Spanning Tree Admin Mode, select the **Enable** radio button.
- Next to the Force Protocol Version, select the **IEEE 802.1d** radio button.

c. Click **Apply**.

2. Configure CST Port Configuration.

a. From the main menu, select Switching > STP > CST Port Configuration. A screen similar to the following displays.



CST Port Configuration

CST Port Configuration

LAGS All Go To Interface GO

	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

Figure 25-2

- **b.** Under CST Port Configuration, scroll down to interface **1/0/3** and select the checkbox for that interface. Now 1/0/3 appears in the Interface field at the top.
- **c.** In the CST Port Configuration, select **Enable** in the Port Mode field.
- **d.** Click **Apply**

Configure Rapid STP (802.1w)

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

CLI: Configuring Rapid STP (802.1w)

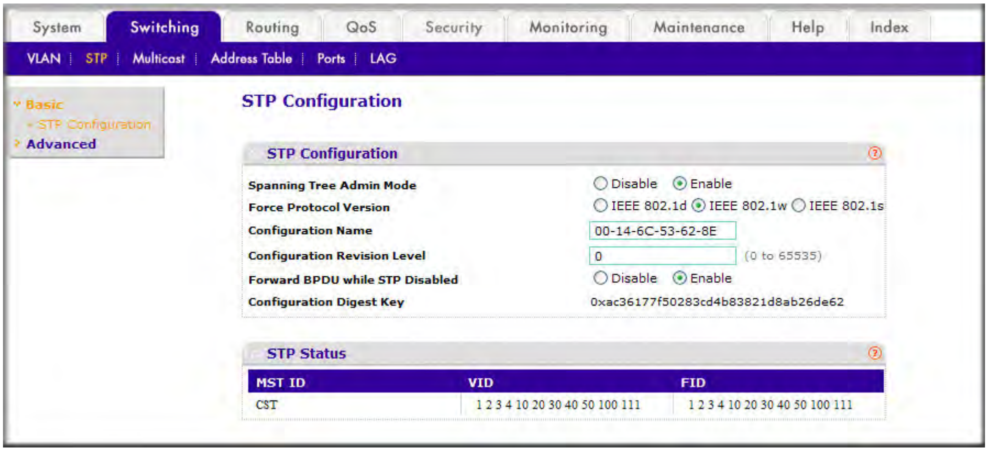
```
(Netgear switch) (Config)# spanning-tree
(Netgear switch) (Config)# spanning-tree forceversion 802.1w
(Netgear switch) (Interface 1/0/3)# spanning-tree port mode
```

Web Interface: Configuring Rapid STP (802.1w)

To use the Web interface to configure the managed switch, proceed as follows:

1. Enable the 802.1w on the switch

- **a.** From the main menu, 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

Figure 25-3

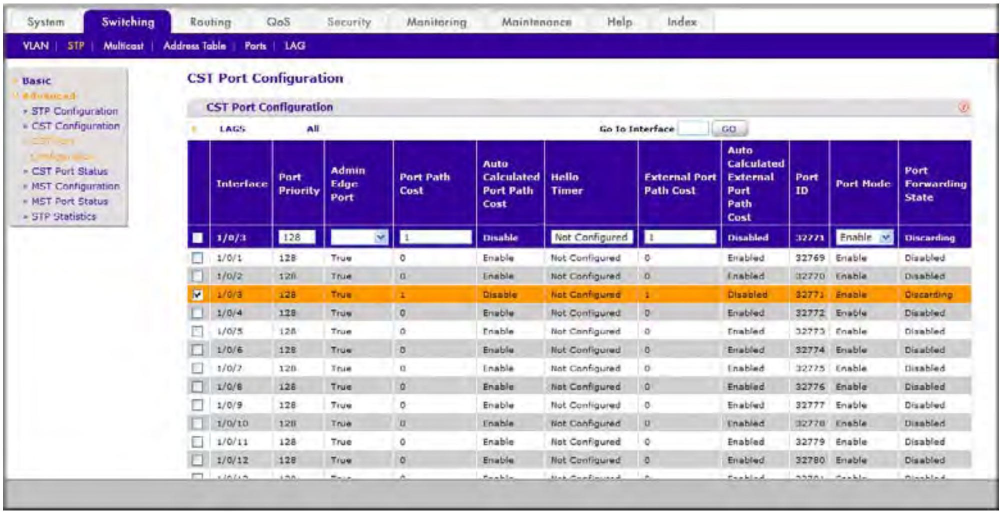
- **b.** Enter the following information in the STP Configuration.
  - Next to the Spanning Tree Admin Mode, select the **Enable** radio button.

- Next to the Force Protocol Version, select the **IEEE 802.1w** radio button.

c. Click **Apply.**

2. Configure CST Port Configuration.

a. From the main menu, 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
□	1/0/13	128	True	0	Enable	Not Configured	0	Enabled	32781	Enable	Disabled

Figure 25-4

b. Under CST Port Configuration, scroll down to interface **1/0/3** and select the checkbox for that interface. Now 1/0/3 appears in the Interface field at the top.

c. In the CST Port Configuration, select **Enable** in the Port Mode field.

d. Click **Apply**

Configure Multiple STP (802.1s)

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

CLI: Configuring Multiple STP (802.1s)

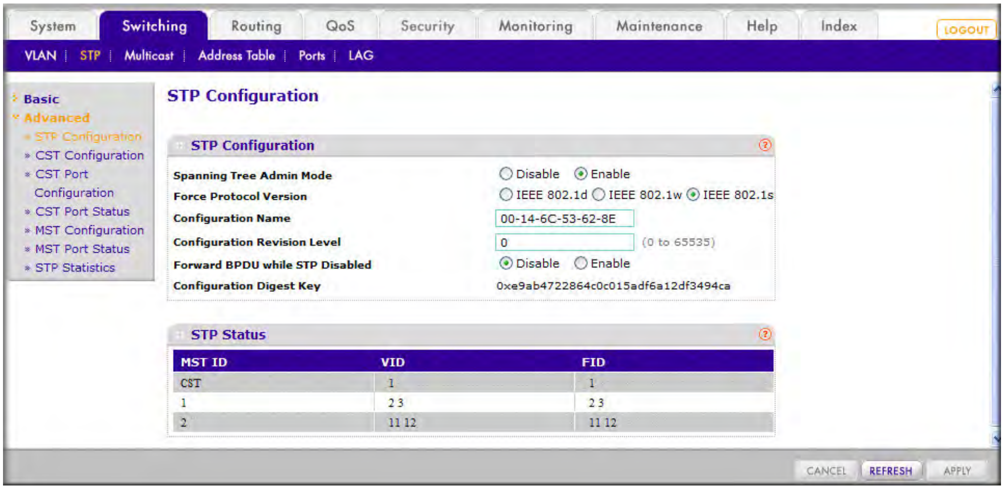
```
(Netgear switch) (Config)# spanning-tree
(Netgear switch) (Config)# spanning-tree forceversion 802.1s
(Netgear switch) (Config)# spanning-tree mst instance 1
       Create a mst instance 1
(Netgear switch) (Config)# spanning-tree mst priority 1 4096
(Netgear switch) (Config)# spanning-tree mst vlan 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: Configuring Multiple STP (802.1s)

To use the Web interface to configure the managed switch, proceed as follows:

1. Enable 802.1s on the switch.

a. From the main menu, 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 0xe9ab4722864c0c015adf6a12df3494ca

STP Status

MST ID	VID	FID
CST	1	1
1	2 3	2 3
2	11 12	11 12

Figure 25-5

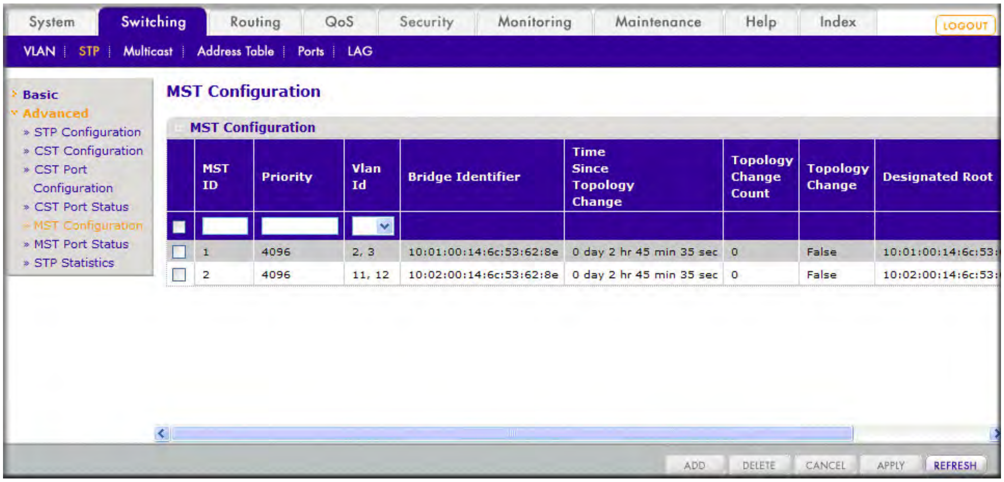
b. Enter the following information in the STP Configuration.

- Next to the Spanning Tree Admin Mode, select the **Enable** radio button.
- Next to the Force Protocol Version, select the **IEEE 802.1s** radio button.

c. Click **Apply**.

2. Configure MST Configuration.

a. From the main menu, 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:53:62:8e	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:53:62:8e	0 day 2 hr 45 min 35 sec	0	False	10:02:00:14:6c:53:

Figure 25-6

b. Configure MST ID 1.

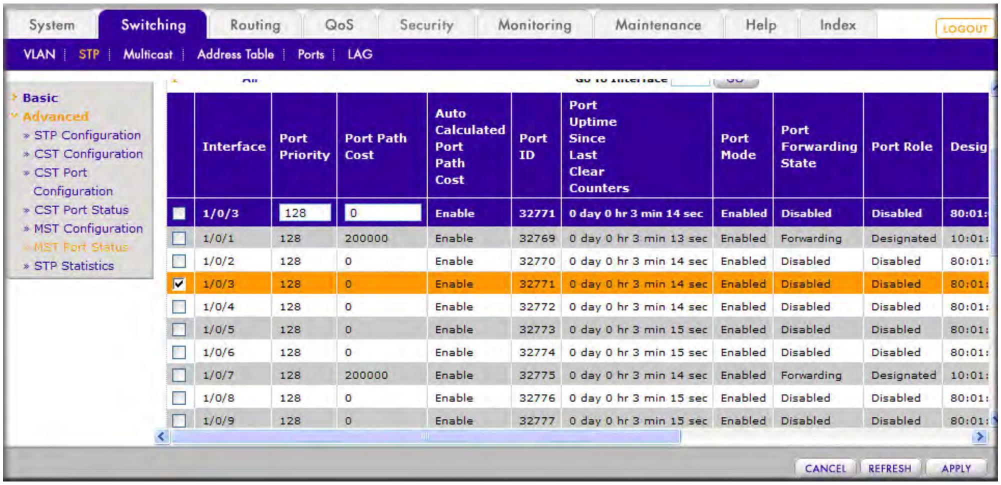
- In the MST ID field, enter **1**.
- In the Priority field, enter **4096**.
- In the VLAN Id field, enter **2**.
- Click **Add**.
- In the VLAN Id field, enter **3**.
- Click **Apply**.

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 MST Port.

a. From the main menu, 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:

Figure 25-7

4. Under MST Port Configuration, scroll down to interface **1/0/3** and select the checkbox for that interface. Now 1/0/3 appears in the Interface field at the top.

5. Enter the following information in the MST Port Status.

- In the Port Priority field, enter **128**.
- In the Port Path Cost field, enter **0**.

6. Click **Apply**.

Chapter 26
Tunnel

There are two methods for Pv6 sites to communicate with each other over the IPv4 network. 6in4 tunnel and 6to4 tunnel. The 6in4 tunnel encapsulate IPv6 traffic over explicitly-configuredIPv4 destination or endport of the tunnel with IP protocol number setting to 41. The 6to4 tunnel IPv6 prefix is constructed by prepending 2002(hex) to the global IPv4 address. for example, if IPv4 address is 4.4.4.1, the tunnel IPv6 prefix would be 2002:404:401::/16..

The 6to4 tunnels are automatically formed IPv4 tunnels carrying IPv6 traffic. The automatic tunnel's IPv4 destination address is derived from the 6to4 IPv6 address of the tunnel's nexthop. It supports the functionality of a 6to4 border router that connects a 6to4 site to a 6to4 domain. It sends/receives tunneled traffic from routers in a 6to4 domain that includes other 6to4 border routers and 6to4 relay routers. The example creates a 6in4 tunnel between GSM7328S_1 and GSM7328S_2. The tunnel carries IPv6 packets over IPv4 packets.

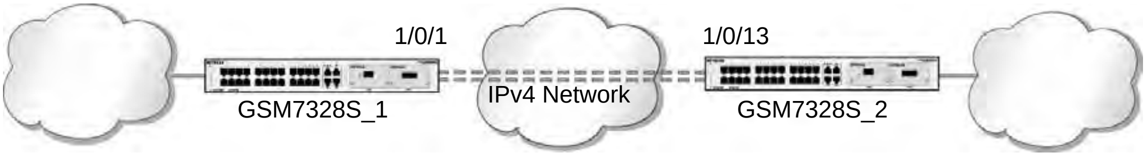


Figure 26-1

CLI: Creating a Tunnel

On GSM7328S_1

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ipv6 forwarding
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.1.1 255.255.255.0
(Netgear Switch) (Interface 1/0/1)#exit
```

```
(Netgear Switch) (Config)#interface tunnel 0
(Netgear Switch) (Interface tunnel 0)#ipv6 enable
(Netgear Switch) (Interface tunnel 0)#ipv6 address 2000::1/64
(Netgear Switch) (Interface tunnel 0)#tunnel mode ipv6ip
(Netgear Switch) (Interface tunnel 0)#tunnel source 192.168.1.1
(Netgear Switch) (Interface tunnel 0)#tunnel destination 192.1.168.1.2
(Netgear Switch) (Interface tunnel 0)#exit
(Netgear Switch) (Config)#exit
```

Note: This example is using 6in4 mode. If you want to use 6to4 mode, please configure each unit as below and be sure the prefix length is 16.

```
interface tunnel 0
tunnel mode ipv6ip 6to4
tunnel source 4.4.4.1
ipv6 enable
ipv6 address 2002:404:401::1/16
exit
```

```
(Netgear Switch) #show interfacet tunnel 0
Interface Link Status.......................... Up
IPv6 is enabled
IPv6 Prefix is ................................ FE80::C0A8:101/128
                                                2000::1/64
MTU size....................................... 1280 bytes
#show interface tunnel
TunnelId  Interface   TunnelMode         SourceAddress      DestinationAddress
--------  ---------   ----------         -------------      ------------------
0          tunnel 0   6 in 4 Configured  192.168.1.1        192.168.1.2
(Netgear Switch) # ping ipv6 2000::2
Send count=3, Receive count=3 from 2000::2
Average round trip time = 1.00 ms
```

On GSM7328S_2

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ipv6 forwarding
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ip address 192.168.1.2 255.255.255.0
(Netgear Switch) (Interface 1/0/13)#exit
```

```
(Netgear Switch) (Config)#interface tunnel 0
(Netgear Switch) (Interface tunnel 0)#ipv6 enable
(Netgear Switch) (Interface tunnel 0)#ipv6 address 2000::2/64
(Netgear Switch) (Interface tunnel 0)#tunnel mode ipv6ip
(Netgear Switch) (Interface tunnel 0)#tunnel source 192.168.1.2
 (Netgear Switch) (Interface tunnel 0)#tunnel destination 192.168.1.1
(Netgear Switch) (Interface tunnel 0)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #show interface tunnel

TunnelId   Interface   TunnelMode          SourceAddress    DestinationAddress
--------   ---------   ----------          -------------    ------------------
0 tunnel    0          6 in 4 Configured    192.168.1.2     192.168.1.1
```

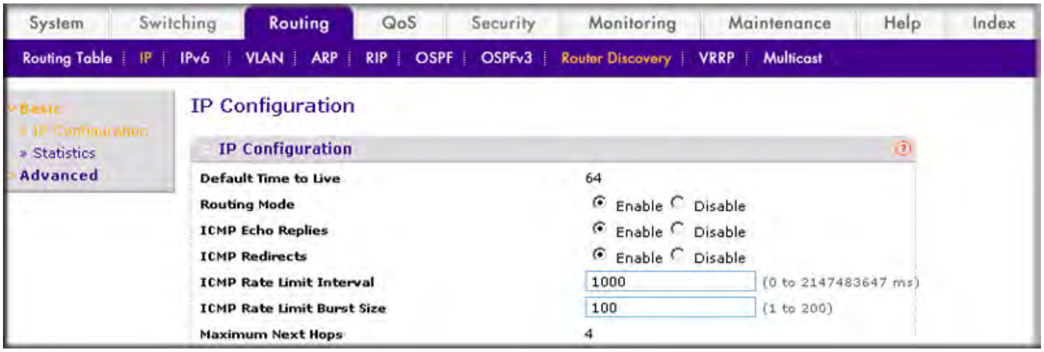
Web Interface: Creating a Tunnel

On GSM7328S_1

To use the Web interface to create a tunnel, proceed as follows:

1. Enable IP routing on the switch.

   a. From the main menu, 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

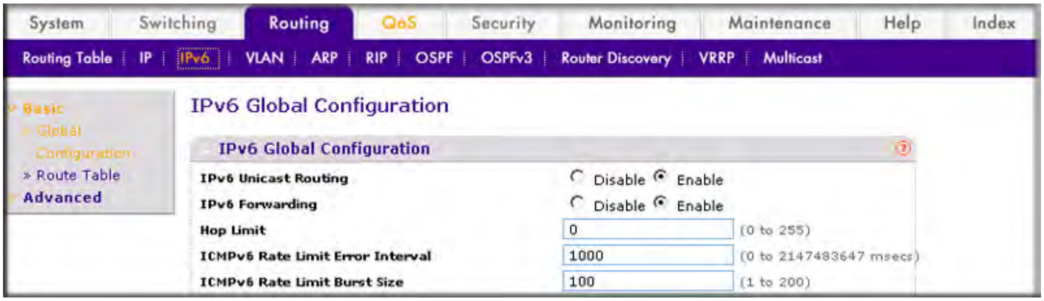
Figure 26-2

   b. Next to the Routing Mode, select the **Enable** Radio button.

   c. Click **Apply**.

2. Enable IPv6 forwarding and unicast routing on the switch.

a. From the main menu, select Routing > IPv6 >Basic>Global Configuration. A screen similar to the following displays.



IPv6 Global Configuration

IPv6 Global Configuration

IPv6 Unicast Routing	○ Disable ● Enable	
IPv6 Forwarding	○ Disable ● Enable	
Hop Limit	0	(0 to 255)
ICMPv6 Rate Limit Error Interval	1000	(0 to 2147483647 msecs)
ICMPv6 Rate Limit Burst Size	100	(1 to 200)

Figure 26-3

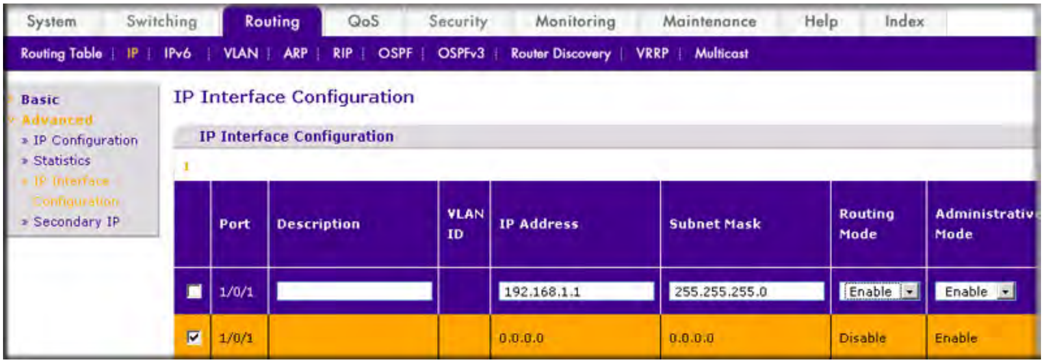
b. Next to the IPv6 Unicast Routing, select the **Enable** Radio button.

c. Next to the IPv6 Forwarding, select the **Enable** Radio button.

d. Click **Apply**.

3. Create a routing interface and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
IP Configuration
Statistics
IP Interface Configuration
Secondary IP

IP Interface Configuration

IP Interface Configuration

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrativ 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

Figure 26-4

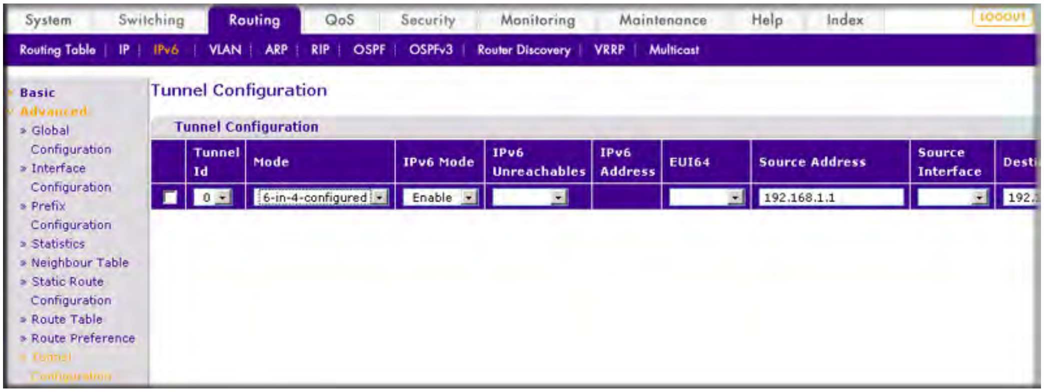
b. Under IP Interface Configuration, scroll down to interface 1/0/1 and select the checkbox for that interface. Now 1/0/1 appears in the Interface field at the top.

- In the IP Address field, enter 192.168.1.1.
- In the Subnet Mask field, enter 255.255.255.0.
- Select **Enable** in the Routing Mode field.

c. Click **Apply**.

4. Create a 6-in-4 tunnel interface.

   a. From the main menu, select Routing > IPv6 >Advanced>Tunnel Configuration. A screen similar to the following displays.



Tunnel Configuration

Tunnel Configuration

	Tunnel Id	Mode	IPv6 Mode	IPv6 Unreachables	IPv6 Address	EUI64	Source Address	Source Interface	Desti
□	0	6-in-4-configured	Enable				192.168.1.1		192.

Figure 26-5

   b. Select **0** in Tunnel Id field.

   c. Select **6-in-4-configured** in the Mode field.

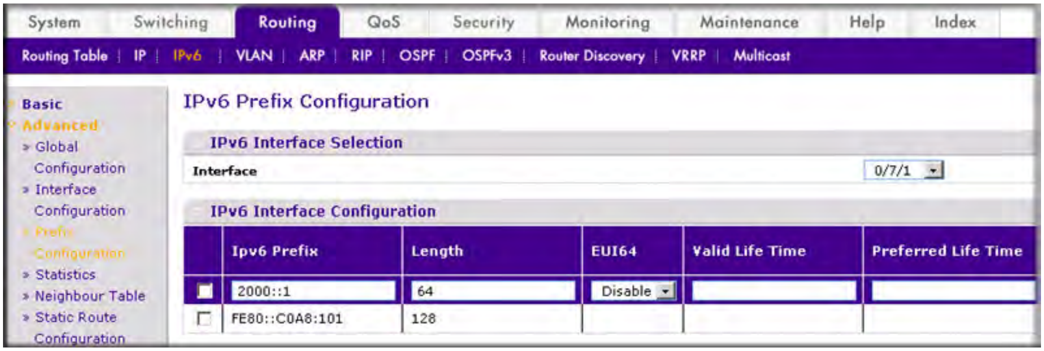
   d. In the Source Address field, enter **192.168.1.1**.

   e. In the Destination Address field, enter **192.168.1.2**.

   f. Click **Apply**.

5. Assign an IPv6 address to the tunnel.

   a. From the main menu, select Routing > IPv6 >Advanced>Prefix Configuration. A screen similar to the following displays.



IPv6 Prefix Configuration

IPv6 Interface Selection

Interface 0/7/1

IPv6 Interface Configuration

	Ipv6 Prefix	Length	EUI64	Valid Life Time	Preferred Life Time
□	2000::1	64	Disable		
□	FE80::C0A8:101	128			

Figure 26-6

   b. Select **0/7/1** in the Interface field.

c. In the IPv6 Prefix field, enter **2000::1**.

d. In the Length field, enter **64**.

e. Select **Disable** in EUI64 field.

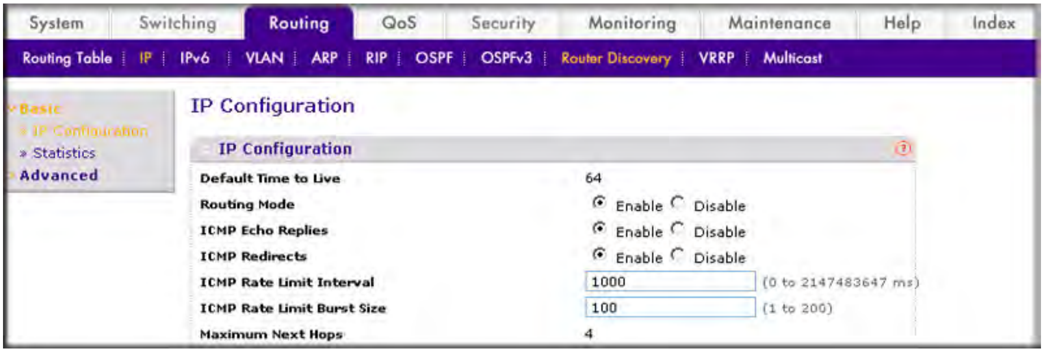
f. Click **Add**.

On GSM7328S_2

To use the Web interface to create a tunnel, proceed as follows:

1. Enable IP routing on the switch.

   a. From the main menu, 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	

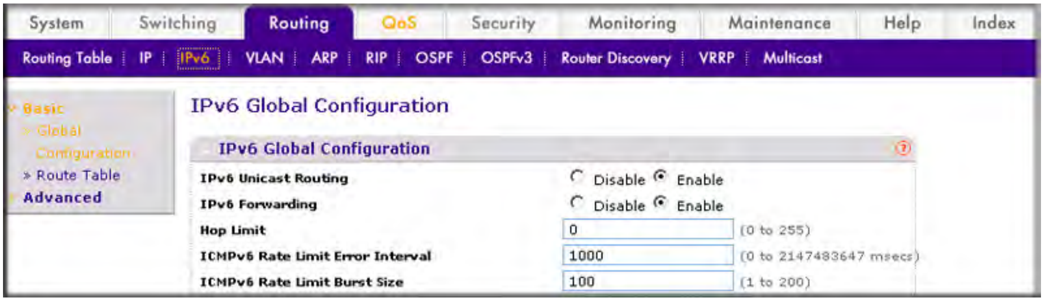
Figure 26-7

   b. Next to the Routing Mode, select the **Enable** Radio button.

   c. Click **Apply**.

2. Enable IPv6 forwarding and unicast routing on the switch.

a. From the main menu, select Routing > IPv6 >Basic>Global Configuration. A screen similar to the following displays.



IPv6 Global Configuration

IPv6 Global Configuration

IPv6 Unicast Routing	○ Disable ● Enable	
IPv6 Forwarding	○ Disable ● Enable	
Hop Limit	0	(0 to 255)
ICMPv6 Rate Limit Error Interval	1000	(0 to 2147483647 msecs)
ICMPv6 Rate Limit Burst Size	100	(1 to 200)

Figure 26-8

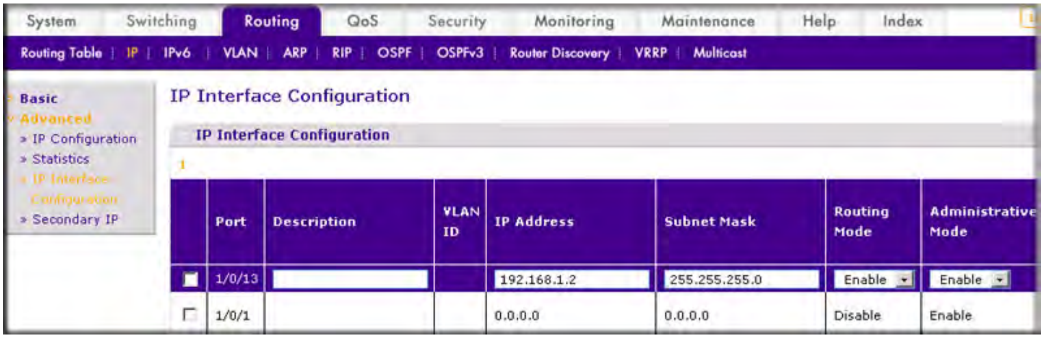
b. Next to the IPv6 Unicast Routing, select the **Enable** Radio button.

c. Next to the IPv6 Forwarding, select the **Enable** Radio button.

d. Click **Apply**.

3. Create a routing interface and assign IP address to it.

a. From the main menu, select Routing > IP >Advanced>IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

IP Interface Configuration

1

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☑	1/0/13			192.168.1.2	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 26-9

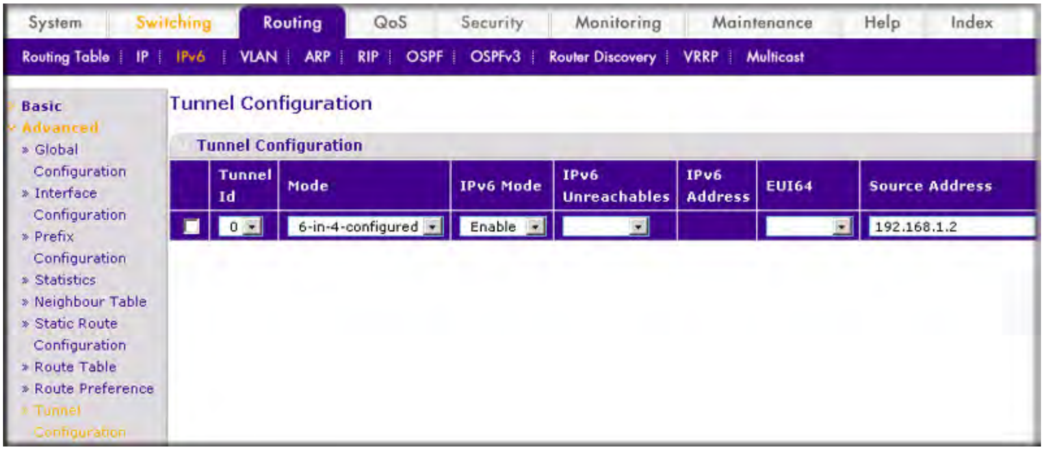
b. Under IP Interface Configuration, scroll down to interface 1/0/13 and select the checkbox for that interface. Now 1/0/1 appears in the Interface field at the top.

- In the IP Address field, enter **192.168.1.2**.
- In the Subnet Mask field, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

c. Click **Apply**.

4. Create a 6-in-4 tunnel interface.

a. From the main menu, select Routing > IPv6 >Advanced>Tunnel Configuration. A screen similar to the following displays.



Tunnel Configuration

Tunnel Configuration

	Tunnel Id	Mode	IPv6 Mode	IPv6 Unreachables	IPv6 Address	EUI64	Source Address
□	0	6-in-4-configured	Enable				192.168.1.2

Figure 26-10

b. Select **0** in the Tunnel Id field.

c. Select **6-in-4-configured** in the Mode field.

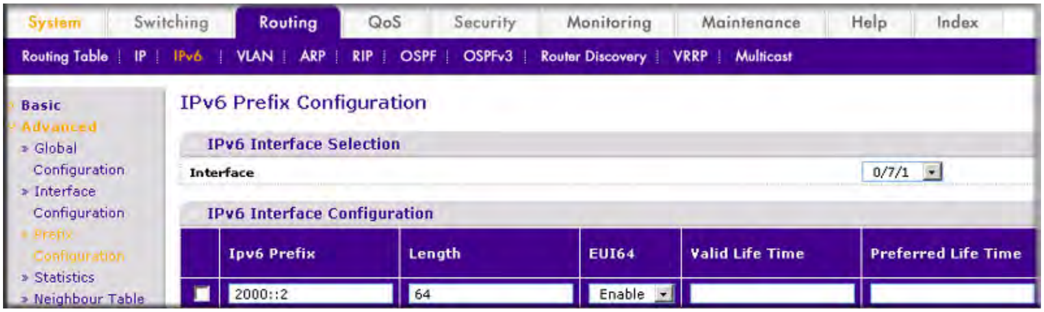
d. In the Source Address field, enter **192.168.1.2**.

e. In the Destination Address field, enter 1**92.168.1.1**.

f. Click **Apply**.

5. Assign an IPv6 address to the tunnel.

a. From the main menu, select Routing > IPv6 > Advanced > Prefix Configuration. A screen similar to the following displays.



IPv6 Prefix Configuration

IPv6 Interface Selection

Interface 0/7/1

IPv6 Interface Configuration

	Ipv6 Prefix	Length	EUI64	Valid Life Time	Preferred Life Time
□	2000::2	64	Enable		

Figure 26-11

b. Select **0/7/1** in the Interface field.

c. In the IPv6 Prefix field, enter **2000::2**.

d. In the Length field, enter 64.

e. Select **Disable** in the EUI64 field.

f. Click **Add**.

Chapter 27
IPv6 Interface Configuration

In this chapter, the following examples are provided:

- "Creating an IPv6 Routing Interface"
- "Create an IPv6 Network Interface" on page 27-4
- "Create an IPv6 Routing VLAN" on page 27-6

Creating an IPv6 Routing Interface

CLI: Create an IPv6 Routing Interface

Enable ipv6 forwarding and unicast routing on the switch.

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

Assign IPv6 address to interface 1/0/1.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#ipv6 enable
(Netgear Switch) (Interface 1/0/1)#ipv6 address 2000::2/64
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) #ping ipv6 2000::2
Send count=3, Receive count=3 from 2000::2
Average round trip time = 1.00 ms
(Netgear Switch) #show ipv6 brief
IPv6 Forwarding Mode........................... Enable
IPv6 Unicast Routing Mode...................... Enable
IPv6 Hop Limit................................. 0
ICMPv6 Rate Limit Error Interval............... 1000 msec
ICMPv6 Rate Limit Burst Size................... 100 messages
Maximum Routes................................. 12
```

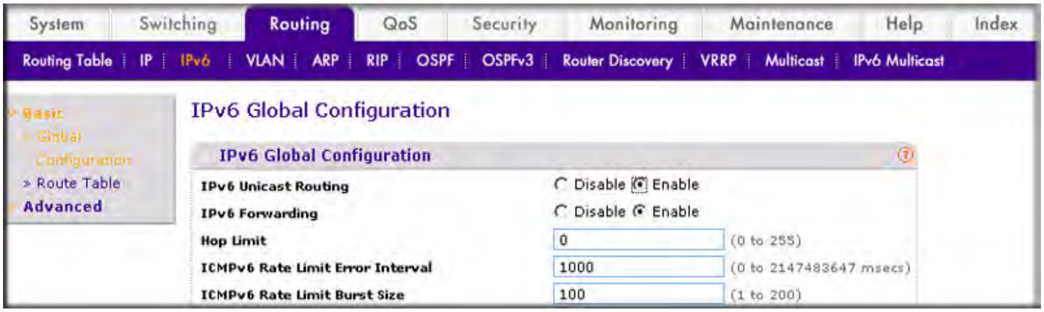
```
(Netgear Switch) #show ipv6 interface 1/0/1
IPv6 is enabled
IPv6 Prefix is ................................ FE80::21E:2AFF:FED9:249B/128
                                                         2000::2/64 [TENT]
Routing Mode................................... Enabled
Administrative Mode............................ Enabled
IPv6 Routing Operational Mode.................. Enabled
Bandwidth...................................... 1000000  kbps
Interface Maximum Transmit Unit................ 1500
Router Duplicate Address Detection Transmits... 1
Router Advertisement NS Interval............... 0
Router Advertisement Lifetime.................. 1800
Router Advertisement Reachable Time............ 0
Router Advertisement Interval.................. 600
Router Advertisement Managed Config Flag....... Disabled
Router Advertisement Other Config Flag......... Disabled
Router Advertisement Suppress Flag............. Disabled
IPv6 Destination Unreachables.................. Enabled

Prefix 2000::2/64
Preferred Lifetime............................. 604800
Valid Lifetime................................. 2592000
Onlink Flag.................................... Enabled
Autonomous Flag................................ Enabled
```

Web Interface: Creating an IPv6 Routing Interface

To use the Web interface to create an IPv6 routing interface, proceed as follows:

1. Enable IPv6 forwarding and unicast routing on the switch.

a. From the main menu, select Routing > IPv6 >Basic>Global Configuration. A screen similar to the following displays.



IPv6 Global Configuration

IPv6 Global Configuration

IPv6 Unicast Routing	○ Disable ● Enable	
IPv6 Forwarding	○ Disable ● Enable	
Hop Limit	0	(0 to 255)
ICMPv6 Rate Limit Error Interval	1000	(0 to 2147483647 msecs)
ICMPv6 Rate Limit Burst Size	100	(1 to 200)

Figure 27-1

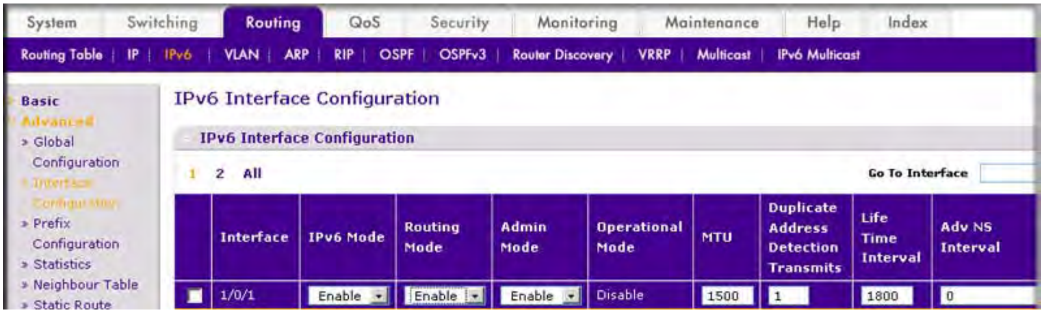
b. Next to the IPv6 Unicast Routing, select the **Enable** Radio button.

c. Next to the IPv6 Forwarding, select the **Enable** Radio button.

d. Click **Apply**.

2. Enable IPv6 routing on the interface 1/0/1

a. From the main menu, select Routing > IPv6 >Advanced>Interface Configuration. A screen similar to the following displays.



IPv6 Interface Configuration

IPv6 Interface Configuration

	Interface	IPv6 Mode	Routing Mode	Admin Mode	Operational Mode	MTU	Duplicate Address Detection Transmits	Life Time Interval	Adv NS Interval
□	1/0/1	Enable	Enable	Enable	Disable	1500	1	1800	0

Figure 27-2

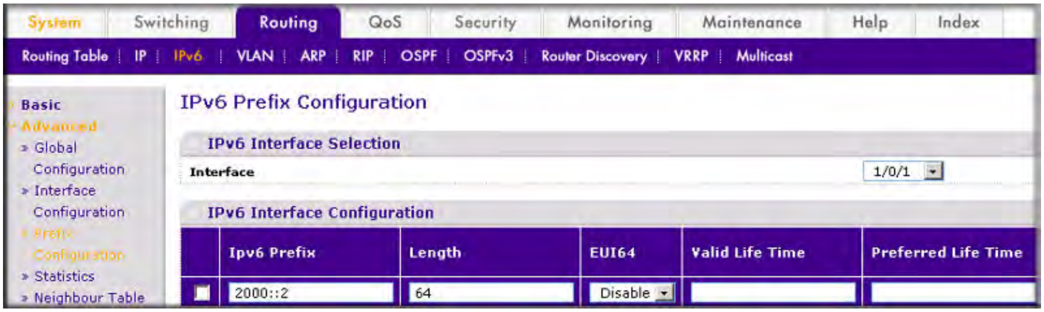
b. Under IPv6 Interface Configuration, scroll down to interface 1/0/1 and select the checkbox for **1/0/1**. Now 1/0/1appears in the Interface field at the top.

c. In the IPv6 Interface Configuration, select **Enable** in the IPv6 Mode field.

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

3. Assign an IPv6 address to the routing interface.

a. From the main menu, select Routing > IPv6 >Advanced>Prefix Configuration. A screen similar to the following displays.



IPv6 Prefix Configuration

IPv6 Interface Selection

Interface: 1/0/1

IPv6 Interface Configuration

	Ipv6 Prefix	Length	EUI64	Valid Life Time	Preferred Life Time
□	2000::2	64	Disable		

Figure 27-3

b. Select **1/0/1** in the Interface field

c. In the IPv6 Prefix field, enter **2000::2**.

d. In the Length field, enter **64**.

e. Select **Disable** in the EUI64 field.

f. Click **Add**.

Create an IPv6 Network Interface

The IPv6 network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

To access the switch over an IPv6 network you must first configure it with IPv6 information (IPv6 prefix, prefix length, and default gateway).

CLI: Configure the IPv6 Network Interface

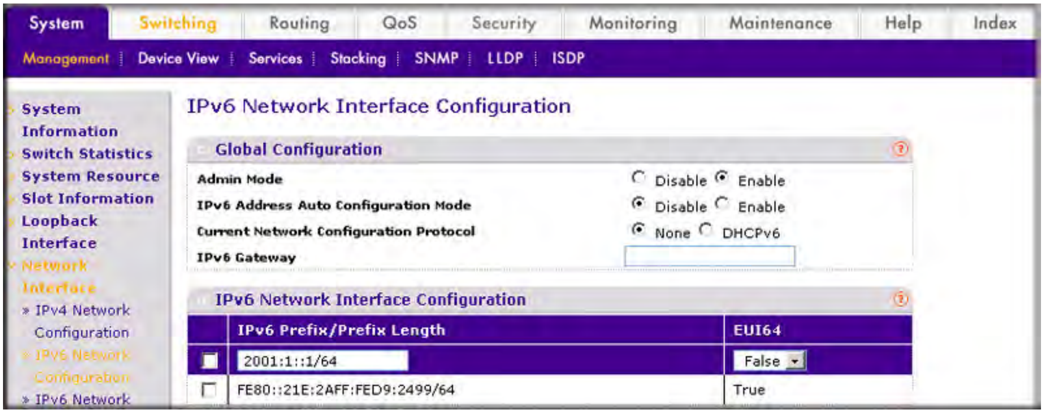
```
(Netgear Switch) #network ipv6 enable
(Netgear Switch) #network ipv6 address 2001:1::1/64
(Netgear Switch) #network ipv6 gateway 2001:1::2
(Netgear Switch) #show network
Interface Status.............................. Always Up
IP Address.................................... 0.0.0.0
Subnet Mask................................... 0.0.0.0
Default Gateway............................... 0.0.0.0
IPv6 Administrative Mode...................... Enabled
IPv6 Prefix is ............................... FE80::2FF:F9FF:FE70:485/64
IPv6 Prefix is ............................... 2001:1::1/64
IPv6 Default Router........................... 2001:1::2
Burned In MAC Address......................... 00:FF:F9:70:04:85
Locally Administered MAC address.............. 00:00:00:00:00:00
MAC Address Type.............................. Burned In
Configured IPv4 Protocol...................... None
Configured IPv6 Protocol...................... None
IPv6 AutoConfig Mode.......................... Disabled
Management VLAN ID...........................1
```

Web Interface: Configuring the IPv6 Network Interface

To use the Web interface to configure the IPv6 network interface, proceed as follows:

1. Add an IPv6 address to the network interface.

a. From the main menu, select System > Management >Network Interface>IPv6 Network Configuration. A screen similar to the following displays.



IPv6 Network Interface Configuration

Global Configuration

Admin Mode	○ Disable ● Enable
IPv6 Address Auto Configuration Mode	● Disable ○ Enable
Current Network Configuration Protocol	● None ○ DHCPv6
IPv6 Gateway	

IPv6 Network Interface Configuration

	IPv6 Prefix/Prefix Length	EUI64
□	2001:1::1/64	False
□	FE80::21E:2AFF:FED9:2499/64	True

Figure 27-4

b. Next to the Admin Mode, select the **Enable** Radio button.

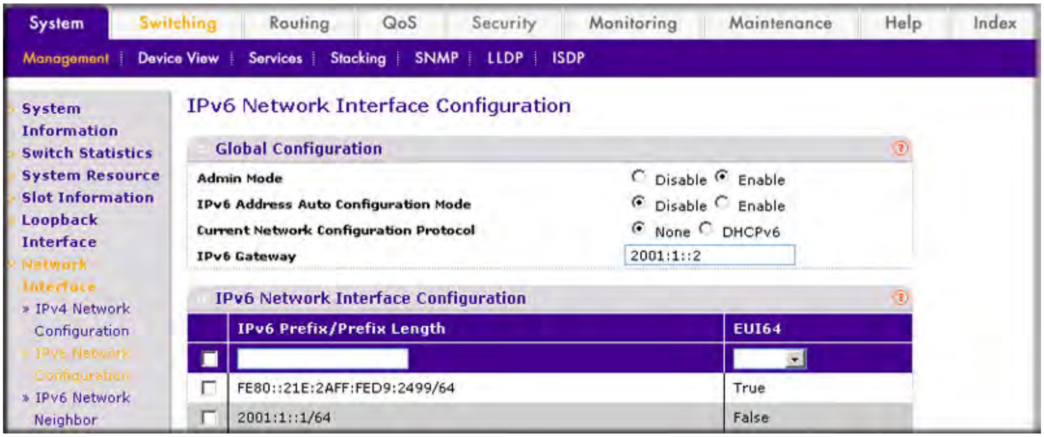
c. In the IPv6 Prefix/Prefix Length field, enter 2**001:1::1/64**.

d. Select **False** in the EUI64 field.

e. Click **Add**.

2. Add an IPv6 gateway to the network interface.

a. From the main menu, select System > Management >Network Interface>IPv6 Network Configuration. A screen similar to the following displays.



IPv6 Network Interface Configuration

Global Configuration

Admin Mode	○ Disable ● Enable
IPv6 Address Auto Configuration Mode	● Disable ○ Enable
Current Network Configuration Protocol	● None ○ DHCPv6
IPv6 Gateway	2001:1::2

IPv6 Network Interface Configuration

	IPv6 Prefix/Prefix Length	EUI64
□		
□	FE80::21E:2AFF:FED9:2499/64	True
□	2001:1::1/64	False

Figure 27-5

b. In the IPv6 Gateway field, enter **2001:1::2**.

c. Click **Apply**.

Create an IPv6 Routing VLAN

CLI: Creating an IPv6 Routing VLAN

Create a routing VLAN with VLAN ID 500.

```
Netgear Switch) (Vlan)#vlan 500
(Netgear Switch) (Vlan)#vlan routing 500
(Netgear Switch) (Vlan)#exit
```

Add the interface 1/0/1 to VLAN 500.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#vlan participation include 500
(Netgear Switch) (Interface 1/0/1)#vlan participation pvid 500
(Netgear Switch) (Interface 1/0/1)#exit
```

Assign IPv6 Address 2000::1/64 to VLAN 500 and enable IPv6 routing.

```
(Netgear Switch) (Config)#interface vlan 0/4/1
(Netgear Switch) (Interface 0/4/1)#routing
(Netgear Switch) (Interface 0/4/1)#ipv6 enable
(Netgear Switch) (Interface 0/4/1)#ipv6 address 2000::1/64
(Netgear Switch) (Interface 0/4/1)#exit
```

Enable ipv6 forwarding and unicast routing on the switch.

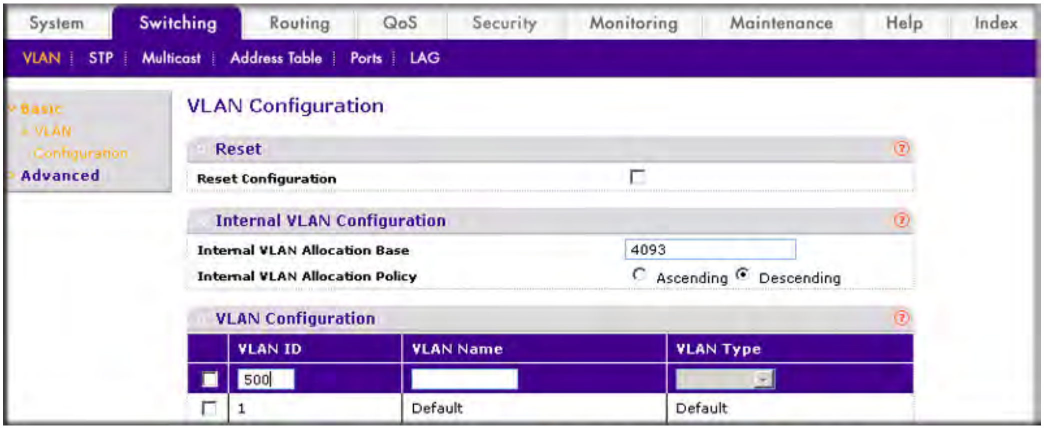
```
(Netgear Switch) (Config)#ipv6 forwarding
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) #ping ipv6 2000::2
Send count=3, Receive count=3 from 2000::2
Average round trip time = 1.00 ms
(Netgear Switch) #show ipv6 brief
IPv6 Forwarding Mode.......................... Enable
IPv6 Unicast Routing Mode..................... Enable
IPv6 Hop Limit................................ 0
ICMPv6 Rate Limit Error Interval.............. 1000 msec
ICMPv6 Rate Limit Burst Size.................. 100 messages
Maximum Routes................................ 128
```

```
(Netgear Switch) #show ipv6 interface 0/4/1
IPv6 is enabled
IPv6 Prefix is ................................ FE80::21E:2AFF:FED9:249B/128
                                                          2000::1/64
Routing Mode................................... Enabled
Administrative Mode............................ Enabled
IPv6 Routing Operational Mode.................. Enabled
Bandwidth...................................... 10000  kbps
Interface Maximum Transmit Unit................ 1500
Router Duplicate Address Detection Transmits... 1
Router Advertisement NS Interval............... 0
Router Advertisement Lifetime.................. 1800
Router Advertisement Reachable Time............ 0
Router Advertisement Interval.................. 600
Router Advertisement Managed Config Flag....... Disabled
Router Advertisement Other Config Flag......... Disabled
Router Advertisement Suppress Flag............. Disabled
IPv6 Destination Unreachables.................. Enabled

Prefix 2000::1/64
Preferred Lifetime............................. 604800
Valid Lifetime................................. 2592000
Onlink Flag.................................... Enabled
Autonomous Flag................................ Enabled
```

Web Interface: Creating an IPv6 VLAN Routing Interface

1. Create VLAN 500.

a. From the main menu, 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
□	500		
□	1	Default	Default

Figure 27-6

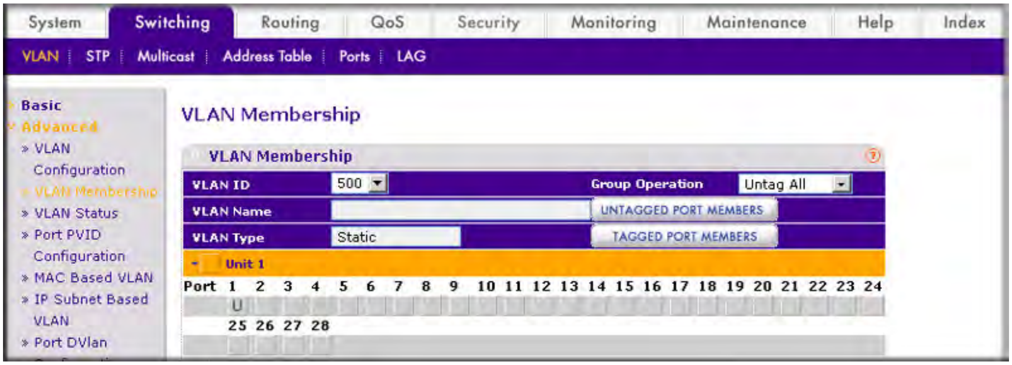
b. In the VLAN ID field, enter **500**.

c. Select **Static** in the VLAN Type field.

d. Click **Add**.

2. Add ports to the VLAN 500.

a. From the main menu, select Switching > VLAN >Advanced > VLAN Membership. A screen similar to the following displays.



VLAN Membership

VLAN Membership

VLAN ID	500	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																				

Figure 27-7

b. Select **500** in the VLAN ID field.

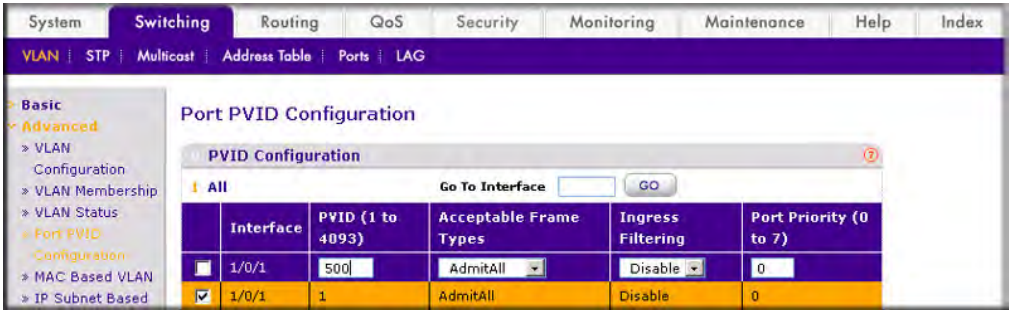
c. Click the Unit 1. The Ports display.

d. Click the gray box under port 1 until U displays, indicating the egress packet is untagged for the port.

e. Click **Apply**.

3. Specify that PVID on port 1/0/1.

a. From the main menu, select Switching > VLAN> Advanced > Port PVID Configuration. A screen similar to the following displays.



Port PVID Configuration

PVID Configuration

All

Go To Interface

	Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)
☐	1/0/1	500	AdmitAll	Disable	0
☑	1/0/1	1	AdmitAll	Disable	0

Figure 27-8

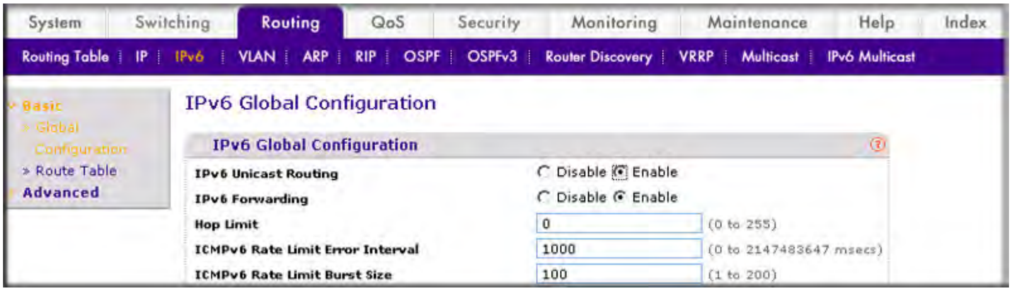
b. Under PVID Configuration, scroll down to interface 1/0/1 and select the checkbox for **1/0/1**.

c. In the PVID Configuration enter **500** in the PVID(1 to 4093) field.

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

4. Enable IPv6 forwarding and unicast routing on the switch.

a. From the main menu, select Routing > IPv6 >Basic>Global Configuration. A screen similar to the following displays.



IPv6 Global Configuration

IPv6 Global Configuration	
IPv6 Unicast Routing	○ Disable ● Enable
IPv6 Forwarding	○ Disable ● Enable
Hop Limit	0 (0 to 255)
ICMPv6 Rate Limit Error Interval	1000 (0 to 2147483647 msecs)
ICMPv6 Rate Limit Burst Size	100 (1 to 200)

Figure 27-9

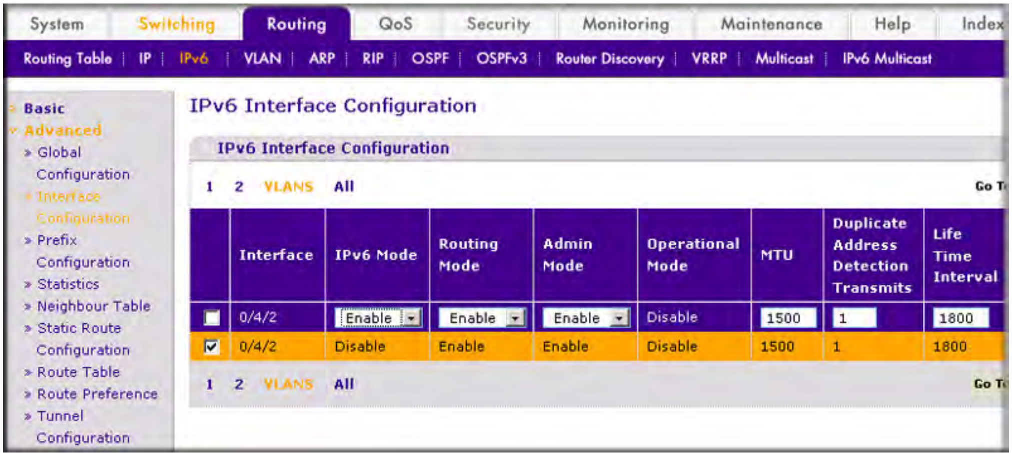
b. Next to the IPv6 Unicast Routing, select the **Enable** Radio button.

c. Next to the IPv6 Forwarding, select the **Enable** Radio button.

d. Click **Apply**.

5. Enable IPv6 routing on the VLAN

a. From the main menu, select Routing > IPv6 >Advanced>Interface Configuration. A screen similar to the following displays.



IPv6 Interface Configuration

IPv6 Interface Configuration

	Interface	IPv6 Mode	Routing Mode	Admin Mode	Operational Mode	MTU	Duplicate Address Detection Transmits	Life Time Interval
☐	0/4/2	Enable	Enable	Enable	Disable	1500	1	1800
☑	0/4/2	Disable	Enable	Enable	Disable	1500	1	1800

Figure 27-10

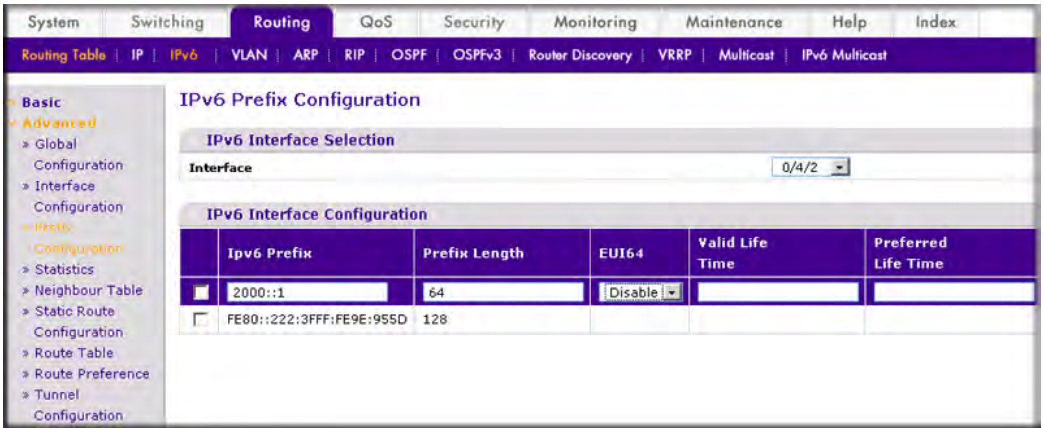
b. Click the tag VLANS, then logical VLAN interface 0/4/2 will be displayed.

c. Select the checkbox for 0/4/2, and in the IPv6 Interface Configuration, select **Enable** in the IPv6 Mode field.

d. Click **Apply**.

6. Assign an IPv6 address to the routing VLAN.

a. From the main menu, select Routing > IPv6 >Advanced>Prefix Configuration. A screen similar to the following displays.



IPv6 Prefix Configuration

IPv6 Interface Selection

Interface: 0/4/2

IPv6 Interface Configuration

	Ipv6 Prefix	Prefix Length	EUI64	Valid Life Time	Preferred Life Time
☐	2000::1	64	Disable		
☐	FE80::222:3FFF:FE9E:955D	128			

Figure 27-11

b. Select **0/4/2** in the Interface field.

c. In the IPv6 Prefix field, enter **2000::1**.

d. In the Length field, enter **64**.

e. Select **Disable** in the EUI64 field.

f. Click **Add**.

Chapter 28
PIM

In this chapter, the following examples are provided:

- "PIM-DM Configuration"
- "PIM-SM Configuration" on page 28-27

Note: The PIM protocol can be configured to operate on IPv4 and IPv6 networks. Separate configuration CLI commands are provided for IPv4 and IPv6 operation; however, most configuration options are common to both protocols. Therefore, this section describes only IPv4 configuration, and IPv6 configuration is similar to IPv4.

Multicast protocols are used to deliver multicast packets from one source to multi-receivers. They facilitate better bandwidth utilization, and use less host and router processing, making them ideal for usage in application such as video/audio conferencing, whiteboard tools, stock distribution tickers, and so on. PIM is a widely used multicast routing protocol. Protocol Independent Multicast (PIM) is a standard multicast routing protocol that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. PIM has two types:

- PIM-Dense Mode (PIM-DM)
- PIM-Sparse Mode (PIM-SM)

PIM-DM Configuration

PIM-DM protocol is a simple, protocol-independent multicast routing protocol. It uses existing Unicast routing table and join/ prune/graft mechanism to build a tree. PIM-DM creates source-based shortest-path distribution trees making use of Reverse Path Forwarding (RPF). PIM-DM cannot be used to build a shared distribution tree, as PIM-SM can. PIM-DM assumes that when a sender starts sending data, all downstream routers and hosts want to receive a multicast datagram. PIM-DM initially floods multicast traffic throughout the network. Routers that do not have any downstream neighbors prune back the unwanted traffic. Apart from the prune messages, PIM-DM makes use of two more messages: graft and assert. Graft messages are used whenever a new host wants to join the group. Assert messages are used to shut off duplicate flows onto the same multi-access network. To minimize the repeated flooding of datagrams and subsequent pruning associated with a particular (S,G) pair, PIM-DM uses a State Refresh message. This message is sent by the router(s) directly connected to the source and is propagated throughout the network. When received by a router on its RPF interface, the State Refresh message causes an existing prune state to be refreshed. State Refresh messages are generated periodically by the router directly attached to the source. There are two versions of PIM-DM. Version 2 does not use IGMP messages; instead, it uses a message that is encapsulated in IP packets with protocol number 103. In Version 2, the Hello message is introduced in place of the query message. PIM-DM is appropriate for:

- Densely distributed receivers
- A ratio of few senders-to-many receivers (due to frequent flooding)
- High volume of multicast traffic
- Constant stream of traffic

The following example describes how to configure and use PIM-DM.

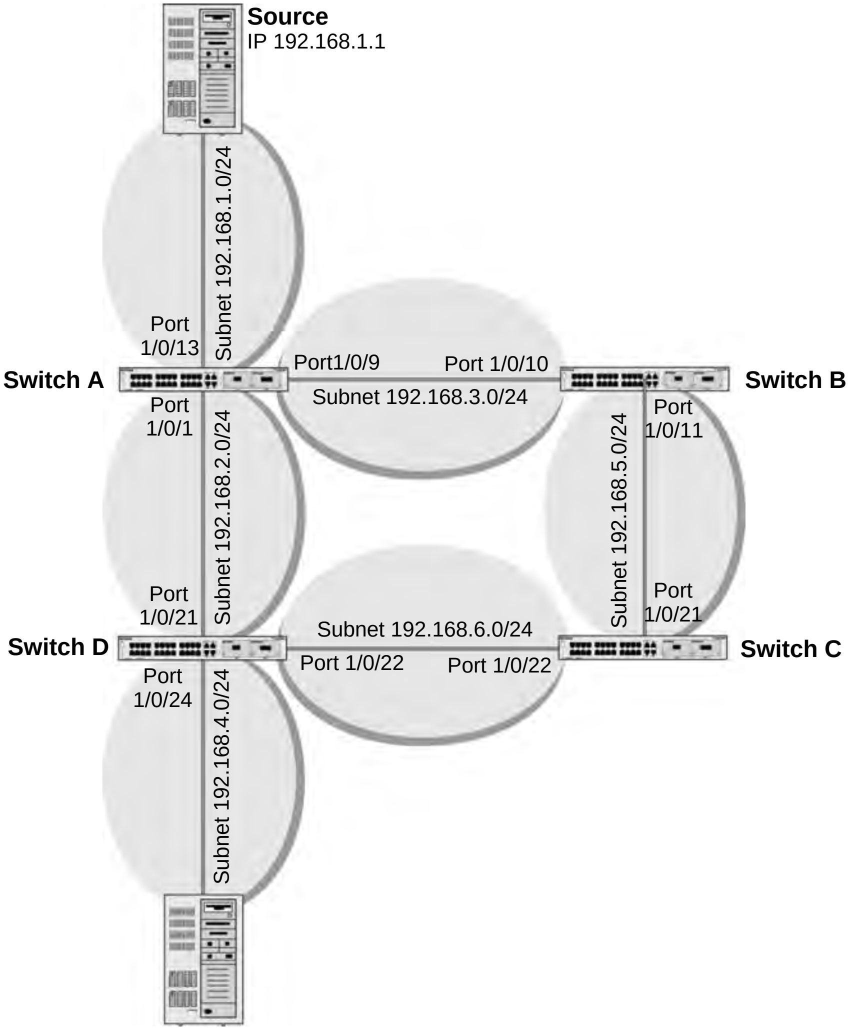


Figure 28-1

CLI: Configuring PIM-DM

On Switch A

Enable IP routing on the switch.

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

Enable pimdm on the switch.

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

Enable ip multicast forwarding on the switch.

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

Enable RIP to build unicst IP routing table.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address  192.168.2.2  255.255.255.0
(Netgear Switch) (Interface 1/0/1)#ip rip
```

Enable PIM-DM on the interface.

```
(Netgear Switch) (Interface 1/0/1)#ip pimdm
(Netgear Switch) (Interface 1/0/1)#exit

(Netgear Switch) (Config)#interface 1/0/9
(Netgear Switch) (Interface 1/0/9)#routing
(Netgear Switch) (Interface 1/0/9)#ip address  192.168.3.1  255.255.255.0
(Netgear Switch) (Interface 1/0/9)#ip rip
(Netgear Switch) (Interface 1/0/9)#ip pimdm
(Netgear Switch) (Interface 1/0/9)#exit

(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ip address  192.168.1.2  255.255.255.0
(Netgear Switch) (Interface 1/0/13)#ip rip
(Netgear Switch) (Interface 1/0/13)#ip pimdm
(Netgear Switch) (Interface 1/0/13)#exit
```

On Switch B

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pimdm
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#interface 1/0/10
(Netgear Switch) (Interface 1/0/10)#routing
(Netgear Switch) (Interface 1/0/10)#ip address  192.168.3.2  255.255.255.0
(Netgear Switch) (Interface 1/0/10)#ip rip
(Netgear Switch) (Interface 1/0/10)#ip pimdm
(Netgear Switch) (Interface 1/0/10)#exit
(Netgear Switch) (Config)#interface 1/0/11
(Netgear Switch) (Interface 1/0/11)#routing
(Netgear Switch) (Interface 1/0/11)#ip address  192.168.5.1  255.255.255.0
(Netgear Switch) (Interface 1/0/11)#ip rip
(Netgear Switch) (Interface 1/0/11)#ip pimdm
(Netgear Switch) (Interface 1/0/11)#exit
```

On Switch C

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pimdm
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address  192.168.5.2  255.255.255.0
(Netgear Switch) (Interface 1/0/21)#ip rip
(Netgear Switch) (Interface 1/0/21)#ip pimdm
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) (Config)#interface 1/0/22
(Netgear Switch) (Interface 1/0/22)#routing
(Netgear Switch) (Interface 1/0/22)#ip address  192.168.6.1  255.255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22)#ip pimdm
(Netgear Switch) (Interface 1/0/22)#exit
```

On Switch D

Enable igmp on the switch.

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pimdm
(Netgear Switch) (Config)#ip igmp
```

```
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address  192.168.2.1  255.255.255.0
(Netgear Switch) (Interface 1/0/21)#ip rip
(Netgear Switch) (Interface 1/0/21)#ip pimdm
(Netgear Switch) (Interface 1/0/21)#exit

(Netgear Switch) (Config)#interface 1/0/22
(Netgear Switch) (Interface 1/0/22)#routing
(Netgear Switch) (Interface 1/0/22)#ip address  192.168.6.2  255.255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22)#ip pimdm
(Netgear Switch) (Interface 1/0/22)#exit
```

Enable igmp on the 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#routing
(Netgear Switch) (Interface 1/0/24)#ip pimdm
(Netgear Switch) (Interface 1/0/24)#ip igmp
(Netgear Switch) (Interface 1/0/24)#ip rip
(Netgear Switch) (Interface 1/0/24)#ip address  192.168.4.1  255.255.255.0
(Netgear Switch) (Interface 1/0/24)#exit
```

After that, PIM-DM builds the multicast routes table on each switch.

```
(A) #show ip mcast mroute summary
                  Multicast Route Table Summary
                                        Incoming      Outgoing
Source IP     Group IP     Protocol     Interface     Interface List
-----------   ----------   ----------   ---------    ---------------
192.168.1.1   225.1.1.1    PIMDM         1/0/13       1/0/1

(B) #show ip mcast mroute summary
                  Multicast Route Table Summary
                                        Incoming       Outgoing
Source IP     Group IP     Protocol     Interface      Interface List
-----------   ---------    ----------   ---------     ---------------
192.168.1.1   225.1.1.1    PIMDM        1/0/10
```

```
(C) #show ip mcast mroute summary
                  Multicast Route Table Summary
                                        Incoming       Outgoing
Source IP     Group IP     Protocol     Interface      Interface List
-----------   ---------    --------     ---------     ---------------
192.168.1.1   225.1.1.1    PIMDM        1/0/21

(D) #show ip mcast mroute summary
                  Multicast Route Table Summary
                                        Incoming        Outgoing
Source IP    Group IP       Protocol    Interface       Interface List
----------   ---------     --------     ----------      ---------------
192.168.1.1  225.1.1.1     PIMDM        7/0/21           7/0/24
```

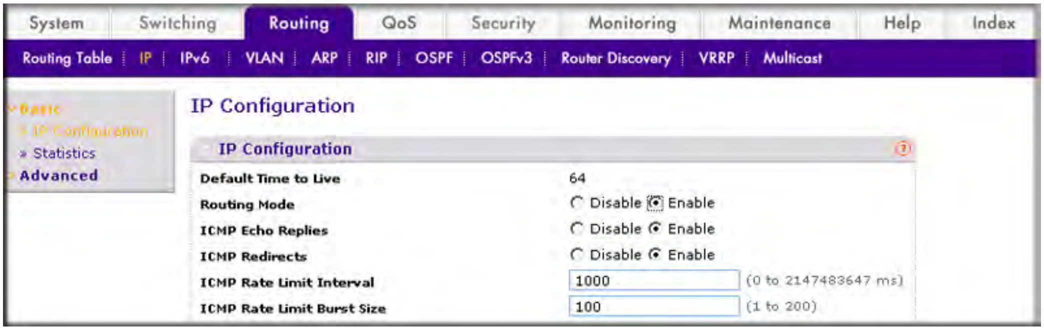
Web Interface: Configuring PIM-DM

To use the Web interface to config PIM-DM, proceed as follows:

On Switch A:

1. Enable IP routing on the switch.

   a. From the main menu, select Routing >IP >Basic >IP configuration. A screen similar to the following displays.



IP Configuration

IP Configuration	
Default Time to Live	64
Routing Mode	○ Disable ● Enable
ICMP Echo Replies	○ Disable ● Enable
ICMP Redirects	○ Disable ● Enable
ICMP Rate Limit Interval	1000 (0 to 2147483647 ms)
ICMP Rate Limit Burst Size	100 (1 to 200)

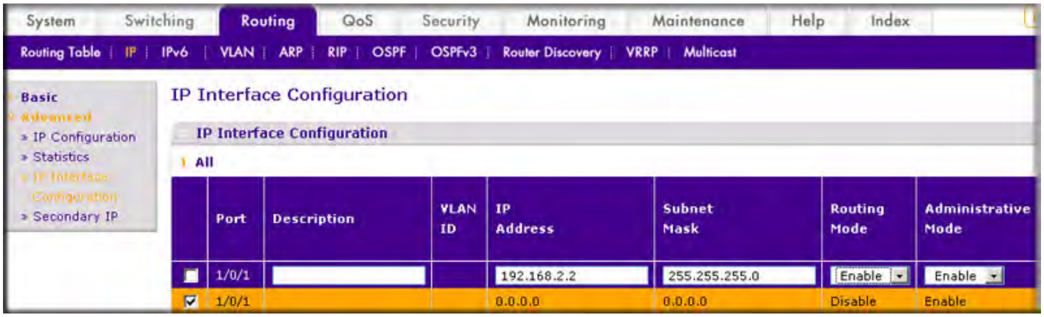
Figure 28-2

   b. Next to the Routing Mode, select the **Enable** radio button.

   c. Click **Apply**.

2. Configure 1/0/1 as a routing port and assign IP address to it.

   a. From the main menu, 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
Basic
Advanced
» IP Configuration
» Statistics
» IP Interface Configuration
» Secondary IP

IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
□	1/0/1			192.168.2.2	255.255.255.0	Enable	Enable
☑	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-3

b. Under IP Interface Configuration, scroll down to interface 1/0/1 and select the checkbox for 1/0/1. 1/0/1 now appears in the Interface field at the top.

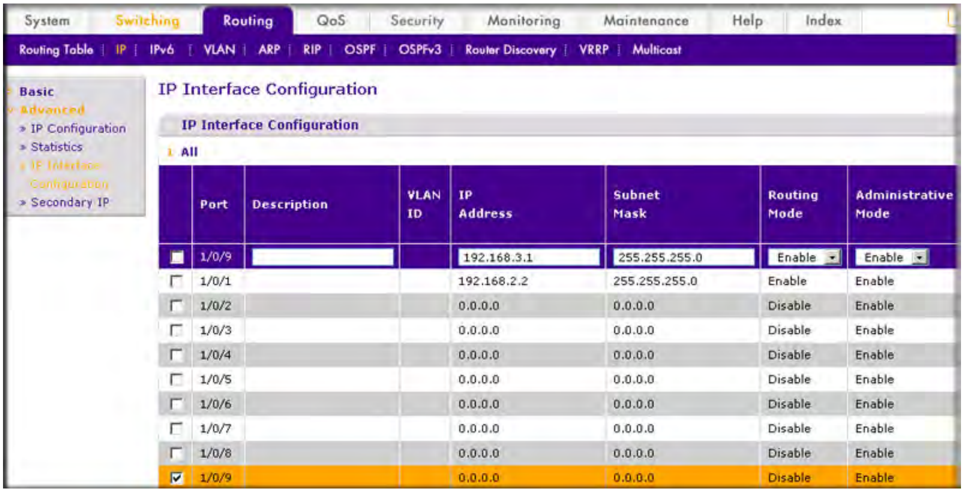
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.2.2**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

3. Configure 1/0/9 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
» IP Configuration
» Statistics
» IP Interface Configuration
» Secondary IP

IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
□	1/0/9			192.168.3.1	255.255.255.0	Enable	Enable
□	1/0/1			192.168.2.2	255.255.255.0	Enable	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
□	1/0/5			0.0.0.0	0.0.0.0	Disable	Enable
□	1/0/6			0.0.0.0	0.0.0.0	Disable	Enable
□	1/0/7			0.0.0.0	0.0.0.0	Disable	Enable
□	1/0/8			0.0.0.0	0.0.0.0	Disable	Enable
☑	1/0/9			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-4

b. Under IP Interface Configuration, scroll down to interface 1/0/9 and select the checkbox for 1/0/9. 1/0/9 now appears in the Interface field at the top.

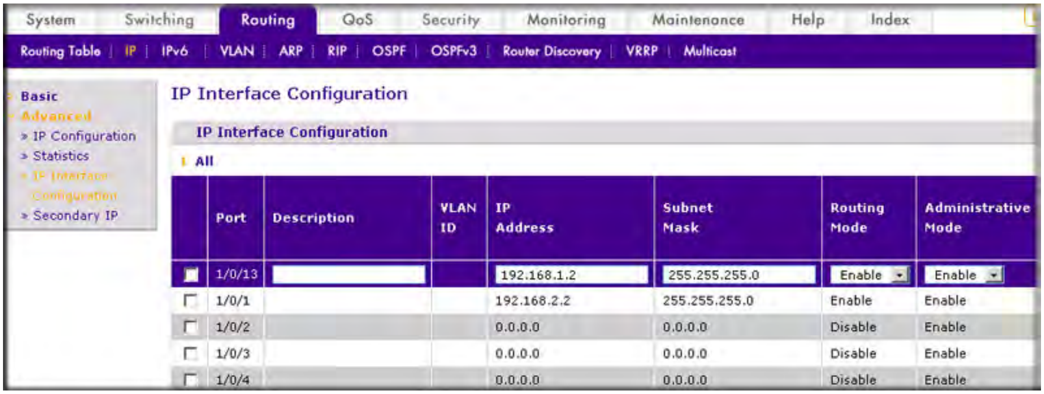
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.3.1**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

d. Click **Apply**.

4. Configure 1/0/13 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
» IP Configuration
» Statistics
» IP Interface Configuration
» Secondary IP

IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☐	1/0/13			192.168.1.2	255.255.255.0	Enable	Enable
☐	1/0/1			192.168.2.2	255.255.255.0	Enable	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

Figure 28-5

b. Under IP Interface Configuration, scroll down to interface 1/0/13 and select the checkbox for 1/0/13. Now 1/0/13 appears in the Interface field at the top.

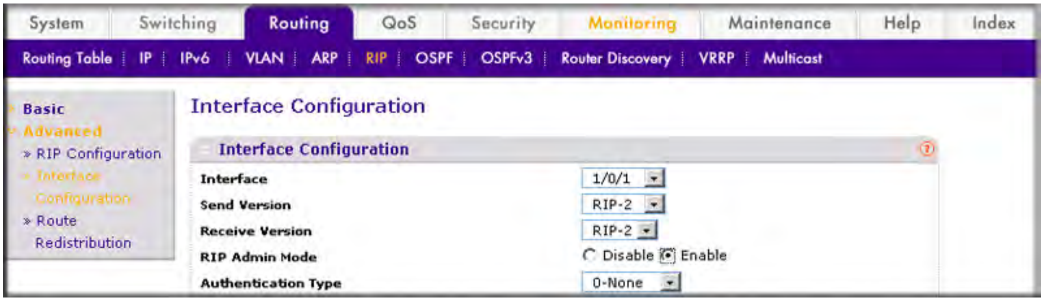
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.1.2**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

5. Enable rip on the interface 1/0/1.

a. From the main menu, select Routing >RIP >Advanced > Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/1
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-6

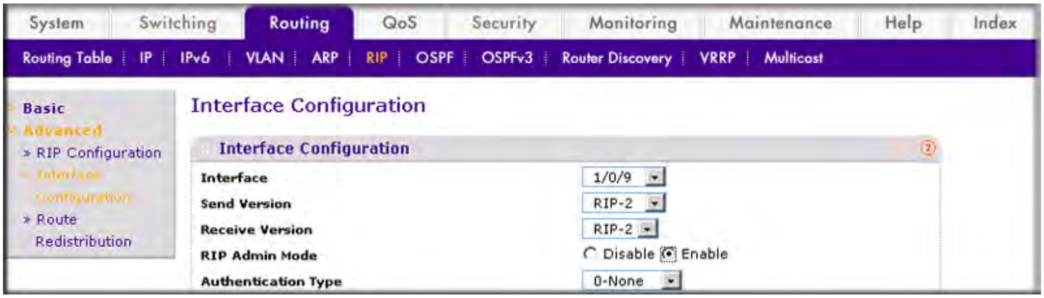
b. Select **1/0/1** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

6. Enable rip on the interface 1/0/9.

a. From the main menu, select Routing > RIP >Advanced > Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/9
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-7

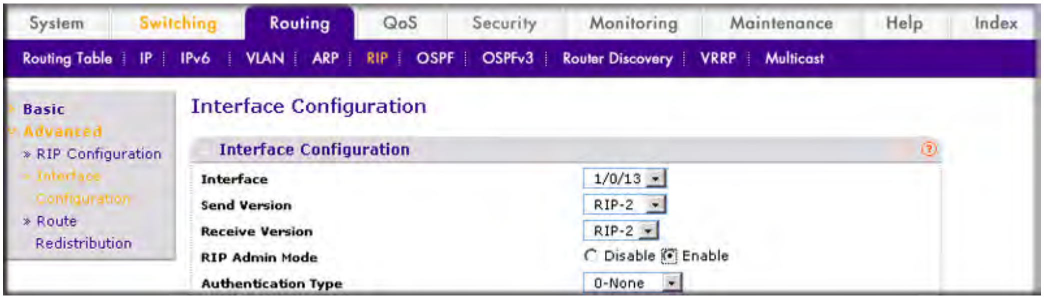
b. Select **1/0/9** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

7. Enable rip on the interface 1/0/13.

a. From the main menu, select Routing > RIP >Advanced > Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/13
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-8

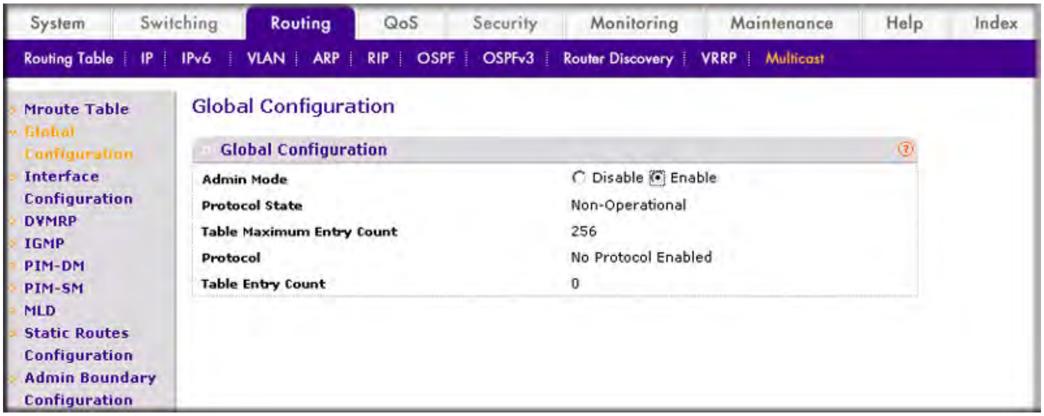
b. Select **1/0/13** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

8. Enable multicast globally.

a. From the main menu, select Routing > Multicast >Global Configuration. A screen similar to the following displays.



Global Configuration

Global Configuration

Admin Mode	○ Disable ● Enable
Protocol State	Non-Operational
Table Maximum Entry Count	256
Protocol	No Protocol Enabled
Table Entry Count	0

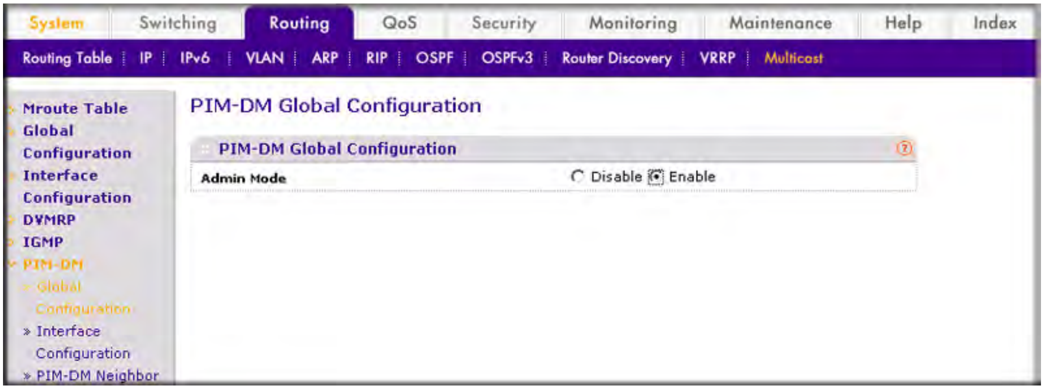
Figure 28-9

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

9. Enable PIM-DM globally.

a. From the main menu, select Routing > Multicast >PIM-DM->Global Configuration. A screen similar to the following displays.



PIM-DM Global Configuration

PIM-DM Global Configuration

Admin Mode ○ Disable ● Enable

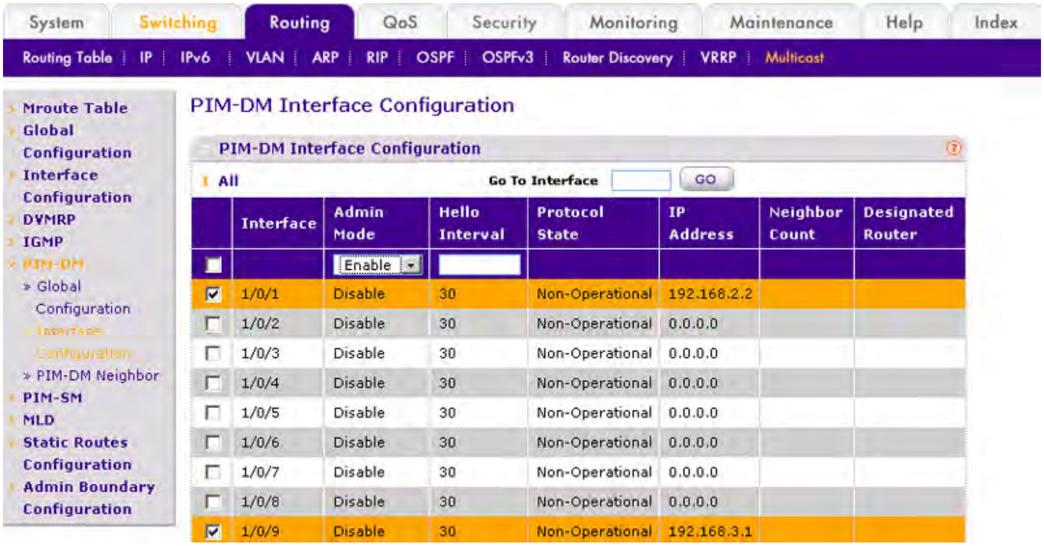
Figure 28-10

b. Next to the Admin Mode, select the Enable radio button.

c. Click **Apply**.

10. Enable PIM-DM on the interface 1/0/1,1/0/9 and 1/0/13.

a. From the main menu, select Routing > Multicast >PIM-DM->Interface Configuration. A screen similar to the following displays.



PIM-DM Interface Configuration

PIM-DM Interface Configuration

All   Go To Interface [ ] GO

	Interface	Admin Mode	Hello Interval	Protocol State	IP Address	Neighbor Count	Designated Router
□		Enable					
☑	1/0/1	Disable	30	Non-Operational	192.168.2.2		
□	1/0/2	Disable	30	Non-Operational	0.0.0.0		
□	1/0/3	Disable	30	Non-Operational	0.0.0.0		
□	1/0/4	Disable	30	Non-Operational	0.0.0.0		
□	1/0/5	Disable	30	Non-Operational	0.0.0.0		
□	1/0/6	Disable	30	Non-Operational	0.0.0.0		
□	1/0/7	Disable	30	Non-Operational	0.0.0.0		
□	1/0/8	Disable	30	Non-Operational	0.0.0.0		
☑	1/0/9	Disable	30	Non-Operational	192.168.3.1		

Figure 28-11

b. Under PIM-DM Interface Configuration, scroll down to interface 1/0/1 and select the checkbox for **1/0/1**. Then select **1/0/9** and **1/0/13**.

c. In the PIM-DM Interface Configuration, select **Enable** in the Admin Mode field.

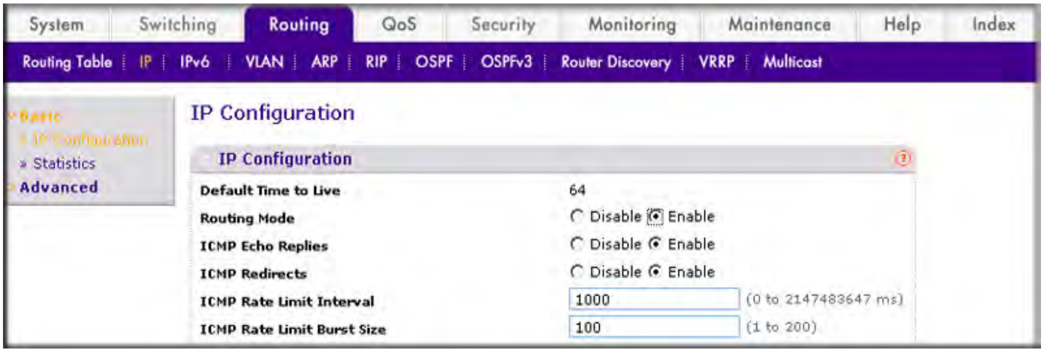
d. Click **Apply** to save the settings.

On Switch B:

To use the Web interface to config PIM-DM, proceed as follows:

1. Enable IP routing on the switch.

a. From the main menu, select Routing >IP >Basic >IP configuration. A screen similar to the following displays.



IP Configuration

IP Configuration

Default Time to Live	64
Routing Mode	○ Disable ● Enable
ICMP Echo Replies	○ Disable ● Enable
ICMP Redirects	○ Disable ● Enable
ICMP Rate Limit Interval	1000 (0 to 2147483647 ms)
ICMP Rate Limit Burst Size	100 (1 to 200)

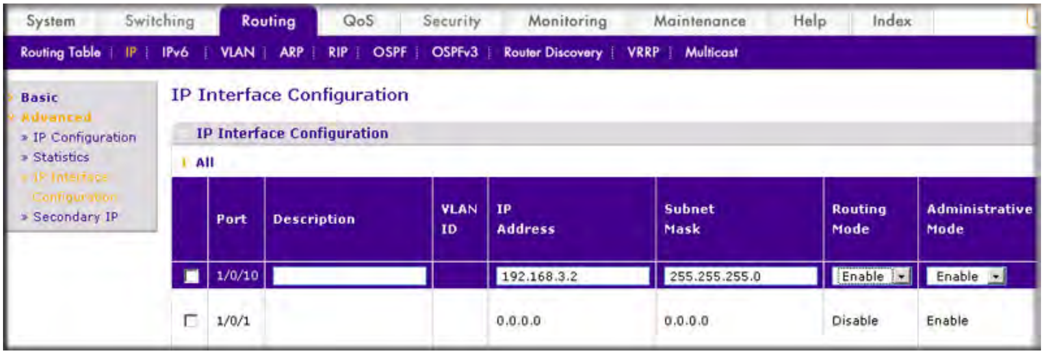
Figure 28-12

b. Next to the Routing Mode, select the **Enable** radio button.

c. Click **Apply**.

2. Configure 1/0/10 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
» IP Configuration
» Statistics
» IP Interface Configuration
» Secondary IP

IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☑	1/0/10			192.168.3.2	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-13

b. Under IP Interface Configuration, scroll down to interface 1/0/10 and select the checkbox for 1/0/10. Now 1/0/10 appears in the Interface field at the top.

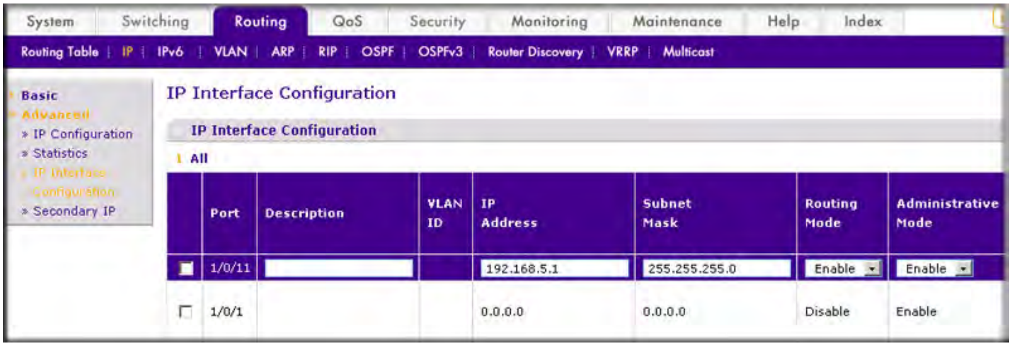
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.3.2**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode.

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

3. Configure 1/0/11 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
» IP Configuration
» Statistics
» IP Interface Configuration
» Secondary IP

IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☑	1/0/11			192.168.5.1	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-14

b. Under IP Interface Configuration, scroll down to interface 1/0/11 and select the checkbox for 1/0/11. Now 1/0/11 appears in the Interface field at the top.

c. Enter the following information in the IP Interface Configuration.

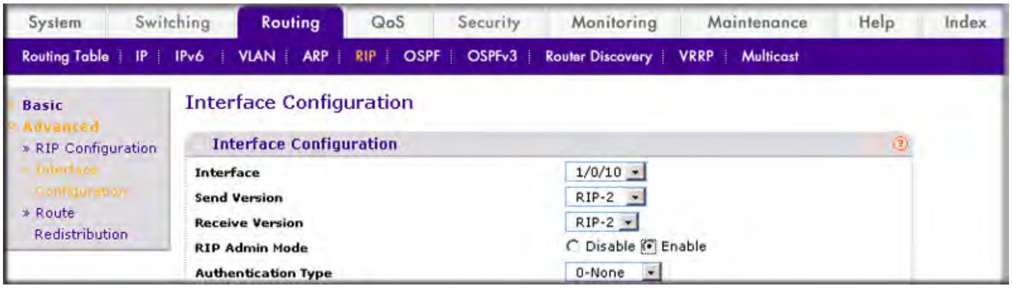
- In the IP address, enter **192.168.5.1**.

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

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

4. Enable rip on the interface 1/0/10.

a. From the main menu, select Routing >RIP >Advanced > Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/10
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-15

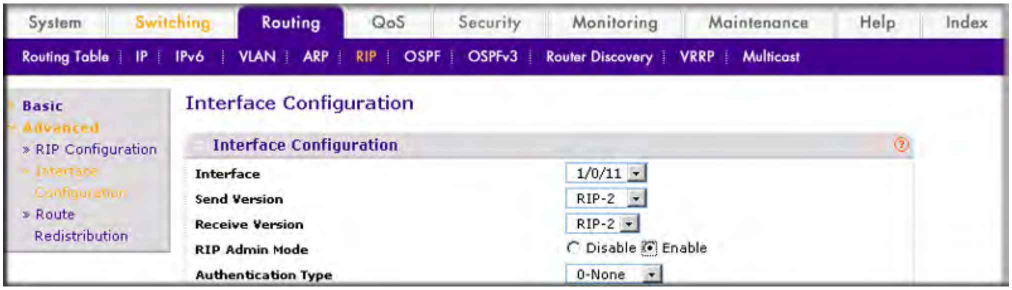
b. Select **1/0/10** in the Interface field.

c. Next to the RIP Admin Mode, select the Enable radio button.

d. Click **Apply**.

5. Enable rip on the interface 1/0/11.

a. From the main menu, select Routing > RIP >Advanced > Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/11
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-16

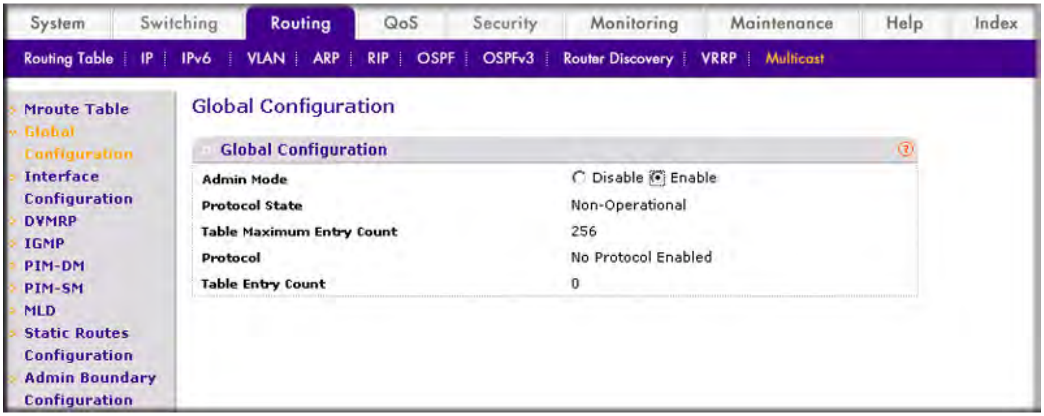
b. Select **1/0/11** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

6. Enable multicast globally.

a. From the main menu, select Routing > Multicast >Global Configuration. A screen similar to the following displays.



Global Configuration

Global Configuration	
Admin Mode	○ Disable ● Enable
Protocol State	Non-Operational
Table Maximum Entry Count	256
Protocol	No Protocol Enabled
Table Entry Count	0

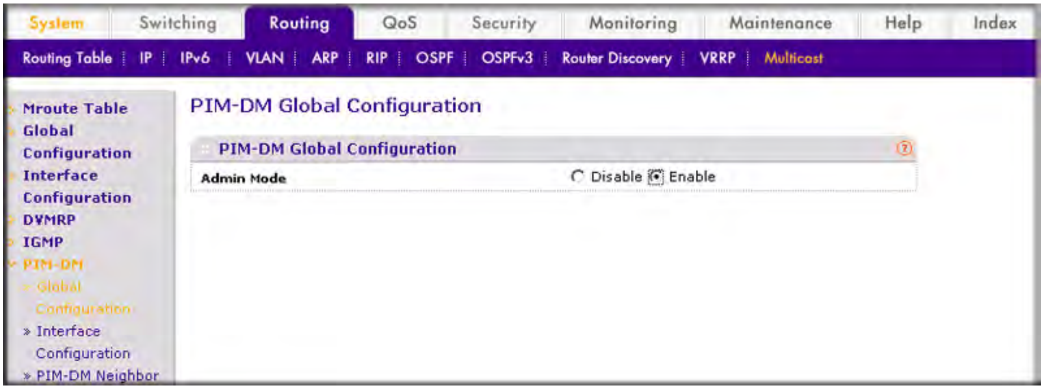
Figure 28-17

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

7. Enable PIM-DM globally.

a. From the main menu, select Routing > Multicast >PIM-DM->Global Configuration. A screen similar to the following displays.



PIM-DM Global Configuration

PIM-DM Global Configuration	
Admin Mode	○ Disable ● Enable

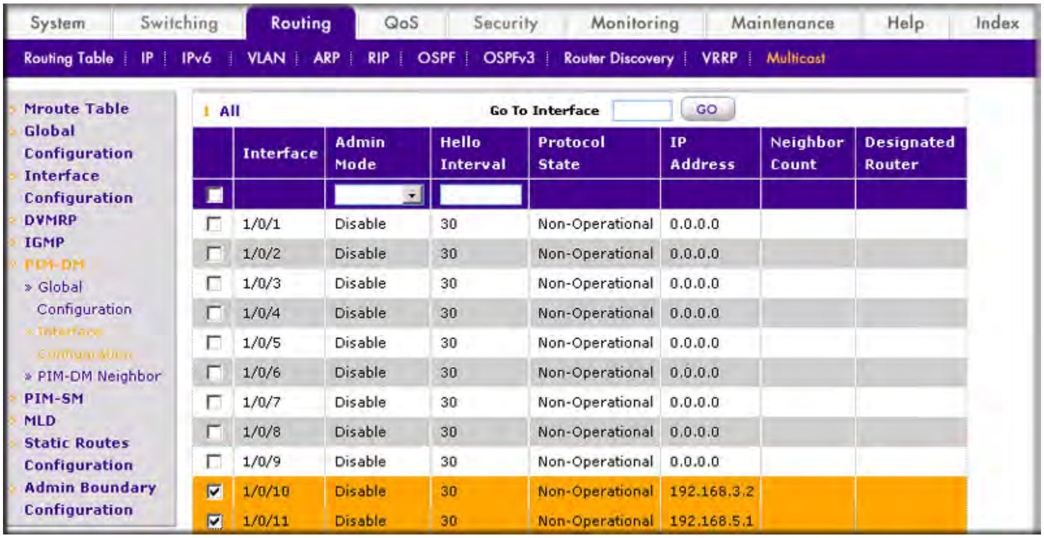
Figure 28-18

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

8. Enable PIM-SM on the interface 1/0/10 and 1/0/11.

a. From the main menu, select Routing > Multicast >PIM-SM->Interface Configuration. A screen similar to the following displays.



	Interface	Admin Mode	Hello Interval	Protocol State	IP Address	Neighbor Count	Designated Router
□							
□	1/0/1	Disable	30	Non-Operational	0.0.0.0		
□	1/0/2	Disable	30	Non-Operational	0.0.0.0		
□	1/0/3	Disable	30	Non-Operational	0.0.0.0		
□	1/0/4	Disable	30	Non-Operational	0.0.0.0		
□	1/0/5	Disable	30	Non-Operational	0.0.0.0		
□	1/0/6	Disable	30	Non-Operational	0.0.0.0		
□	1/0/7	Disable	30	Non-Operational	0.0.0.0		
□	1/0/8	Disable	30	Non-Operational	0.0.0.0		
□	1/0/9	Disable	30	Non-Operational	0.0.0.0		
☑	1/0/10	Disable	30	Non-Operational	192.168.3.2		
☑	1/0/11	Disable	30	Non-Operational	192.168.5.1		

Figure 28-19

b. Under PIM-SM Interface Configuration, scroll down to interface 1/0/10 and select the checkbox for **1/0/10**. Then select the interface **1/0/11**.

c. In the PIM-SM Interface Configuration, select **Enable** in the Admin Mode field.

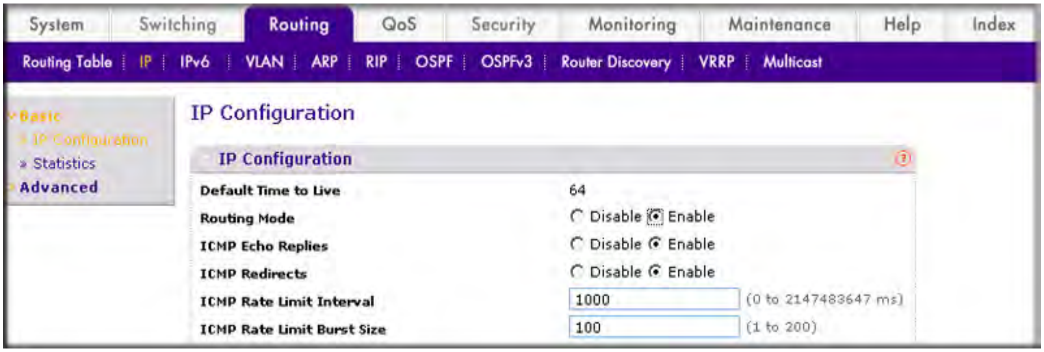
d. Click **Apply** to save the settings.

On Switch C:

To use the Web interface to config PIM-DM, proceed as follows:

1. Enable IP routing on the switch.

a. From the main menu, select Routing >IP >Basic >IP configuration. A screen similar to the following displays.



IP Configuration

IP Configuration

Default Time to Live	64	
Routing Mode	○ Disable ● Enable	
ICMP Echo Replies	○ Disable ● Enable	
ICMP Redirects	○ Disable ● Enable	
ICMP Rate Limit Interval	1000	(0 to 2147483647 ms)
ICMP Rate Limit Burst Size	100	(1 to 200)

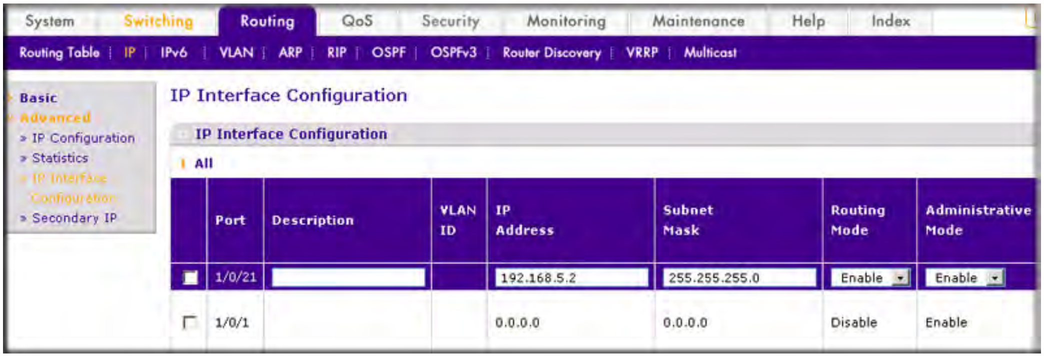
Figure 28-20

b. Next to the Routing Mode, select the **Enable** radio button.

c. Click **Apply**.

2. Configure 1/0/21 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
IP Configuration
Statistics
IP Interface Configuration
Secondary IP

IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☑	1/0/21			192.168.5.2	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-21

b. Under IP Interface Configuration, scroll down to interface 1/0/21 and select the checkbox for 1/0/21. 1/0/21 now appears in the Interface field at the top.

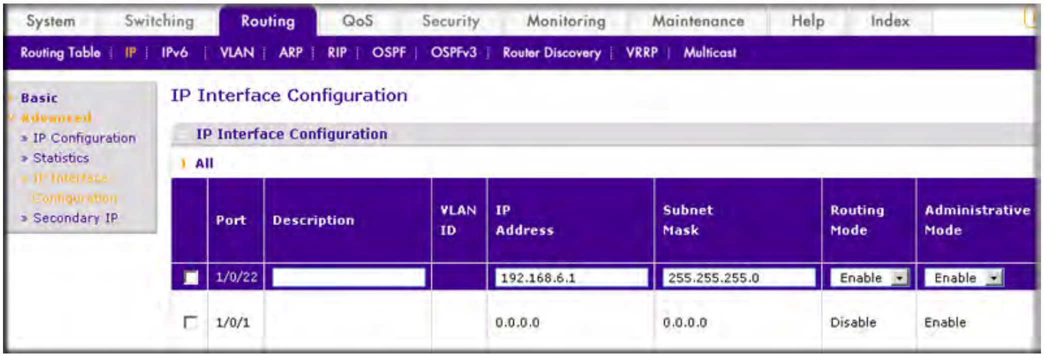
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.5.2**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

3. Configure 1/0/22 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
» IP Configuration
» Statistics
» IP Interface Configuration
» Secondary IP

IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☑	1/0/22			192.168.6.1	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-22

b. Under IP Interface Configuration, scroll down to interface 1/0/22 and select the checkbox for **1/0/22**. Now 1/0/22 appears in the Interface field at the top.

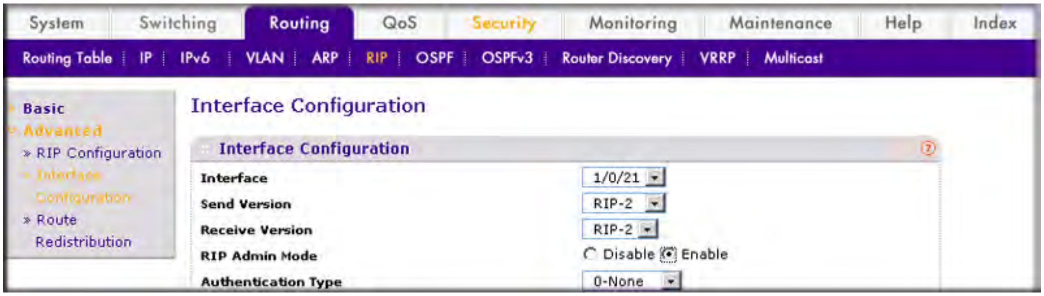
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.6.1**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

4. Enable rip on the interface 1/0/21.

a. From the main menu, select Routing >RIP >Advanced > 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
Basic
Advanced
» RIP Configuration
» Interface Configuration
» Route Redistribution

Interface Configuration

Interface Configuration

Interface	1/0/21
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-23

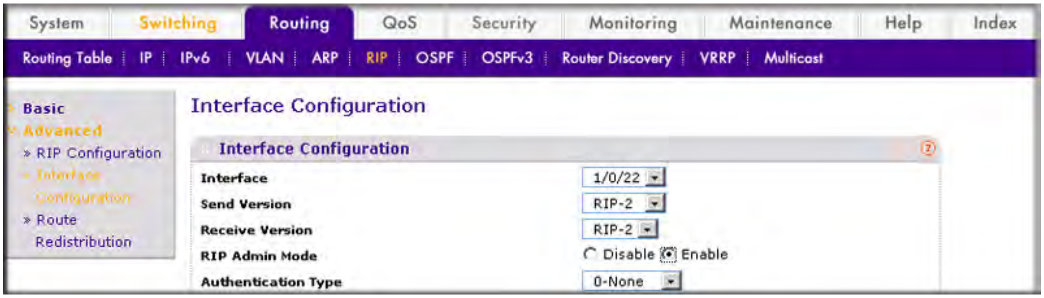
b. Select **1/0/21** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

5. Enable rip on the interface 1/0/22.

a. From the main menu, select Routing > RIP >Advanced > Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/22
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-24

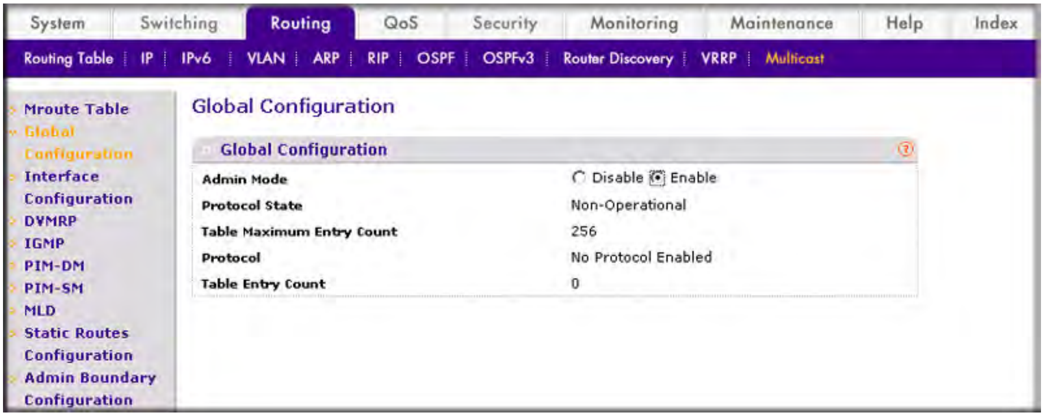
b. Select **1/0/22** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

6. Enable mulicast globally.

a. From the main menu, select Routing > Multicast >Global Configuration. A screen similar to the following displays.



Global Configuration

Global Configuration

Admin Mode	○ Disable ● Enable
Protocol State	Non-Operational
Table Maximum Entry Count	256
Protocol	No Protocol Enabled
Table Entry Count	0

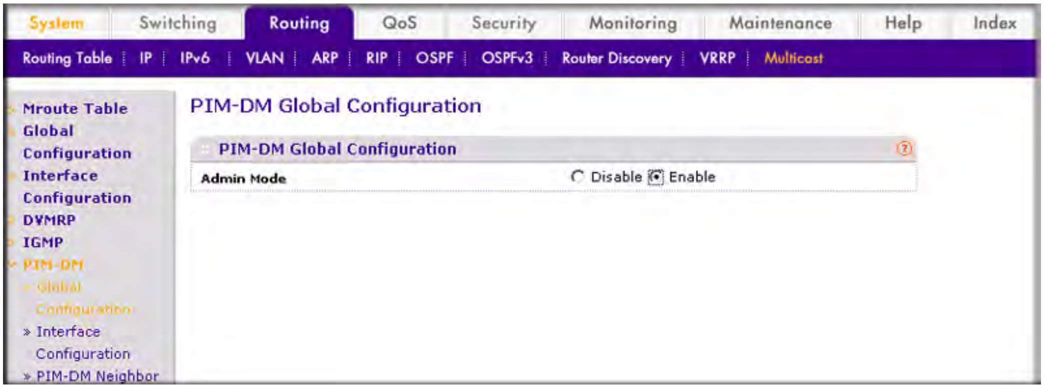
Figure 28-25

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

7. Enable PIM-DM globally.

a. From the main menu, select Routing > Multicast >PIM-DM->Global Configuration. A screen similar to the following displays.



PIM-DM Global Configuration

PIM-DM Global Configuration

Admin Mode ○ Disable ● Enable

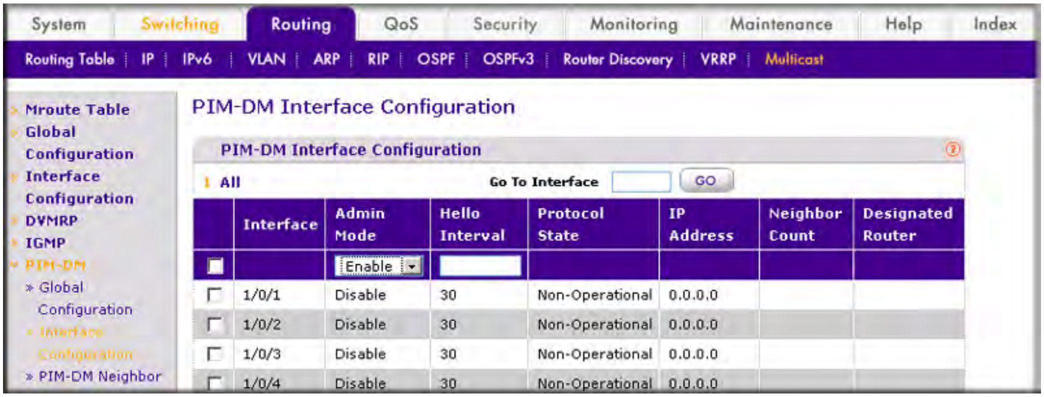
Figure 28-26

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

8. Enable PIM-DM on the interface 1/0/21 and 1/0/22.

a. From the main menu, select Routing > Multicast >PIM-DM->Interface Configuration. A screen similar to the following displays.



PIM-DM Interface Configuration

PIM-DM Interface Configuration

All   Go To Interface

	Interface	Admin Mode	Hello Interval	Protocol State	IP Address	Neighbor Count	Designated Router
□		Enable					
□	1/0/1	Disable	30	Non-Operational	0.0.0.0		
□	1/0/2	Disable	30	Non-Operational	0.0.0.0		
□	1/0/3	Disable	30	Non-Operational	0.0.0.0		
□	1/0/4	Disable	30	Non-Operational	0.0.0.0		

Figure 28-27

b. Under PIM-DM Interface Configuration, scroll down to interface 1/0/21 and select the checkbox for 1/0/21. Then select the interface 1/0/22.

c. In the PIM-DM Interface Configuration, select **Enable** in the Admin Mode field.

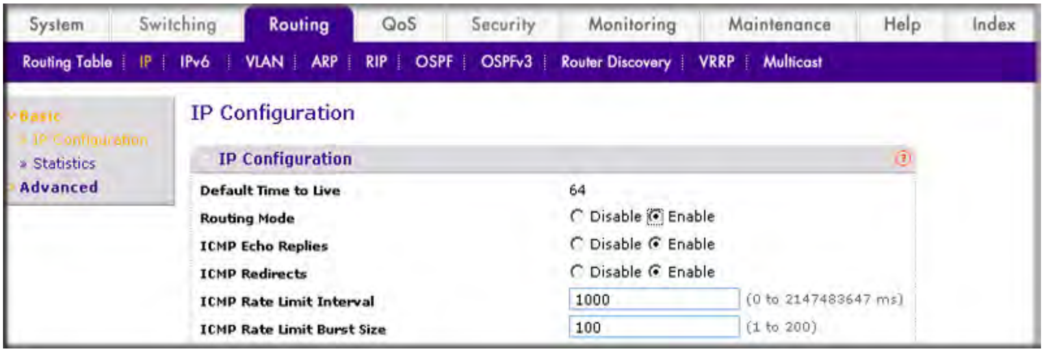
d. Click **Apply** to save the settings.

On Switch D:

To use the Web interface to config PIM-DM, proceed as follows:

1. Enable IP routing on the switch.

   a. From the main menu, select Routing >IP >Basic >IP configuration. A screen similar to the following displays.



IP Configuration

IP Configuration

Default Time to Live	64
Routing Mode	○ Disable ● Enable
ICMP Echo Replies	○ Disable ● Enable
ICMP Redirects	○ Disable ● Enable
ICMP Rate Limit Interval	1000 (0 to 2147483647 ms)
ICMP Rate Limit Burst Size	100 (1 to 200)

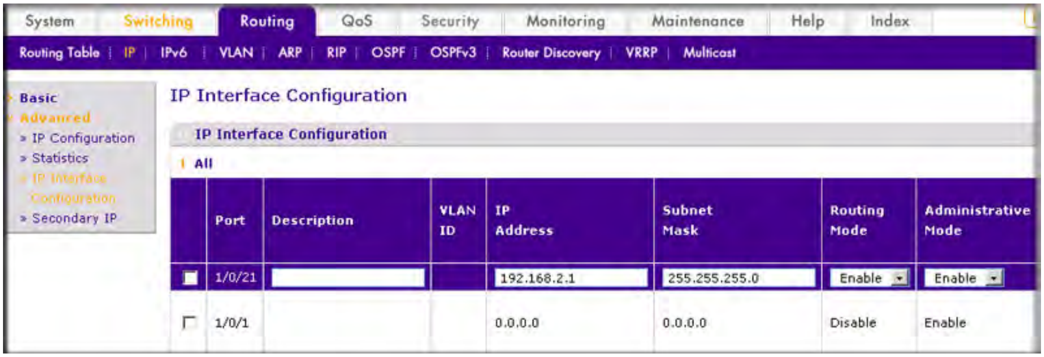
Figure 28-28

   b. Next to the Routing Mode, select the **Enable** radio button.

   c. Click **Apply**.

2. Configure 1/0/21 as a routing port and assign IP address to it.

   a. From the main menu, select Routing > IP >Advanced > IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☑	1/0/21			192.168.2.1	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-29

   b. Under IP Interface Configuration, scroll down to interface 1/0/21 and select the checkbox for 1/0/21. 1/0/21 now appears in the Interface field at the top.

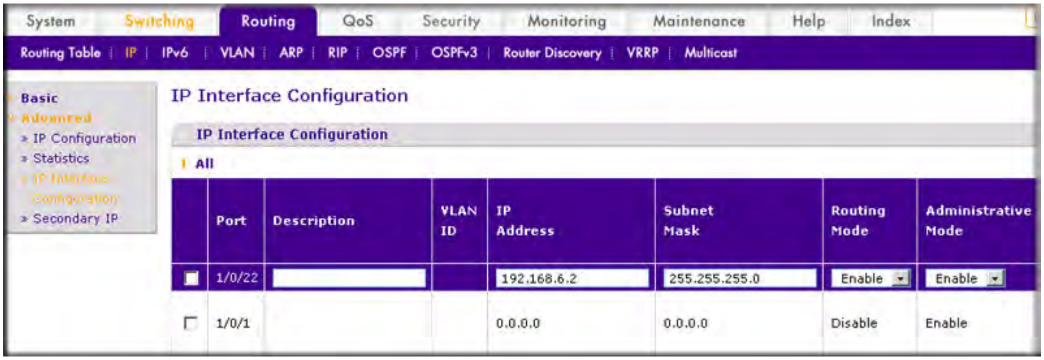
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.2.1**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

3. Configure 1/0/22 as a routing port and assign IP address to it.

a. From the main menu, select Routing > IP >Advanced > IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
□	1/0/22			192.168.6.2	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-30

b. Under IP Interface Configuration, scroll down to interface 1/0/22and select the checkbox for 1/0/22. 1/0/22 now appears in the Interface field at the top.

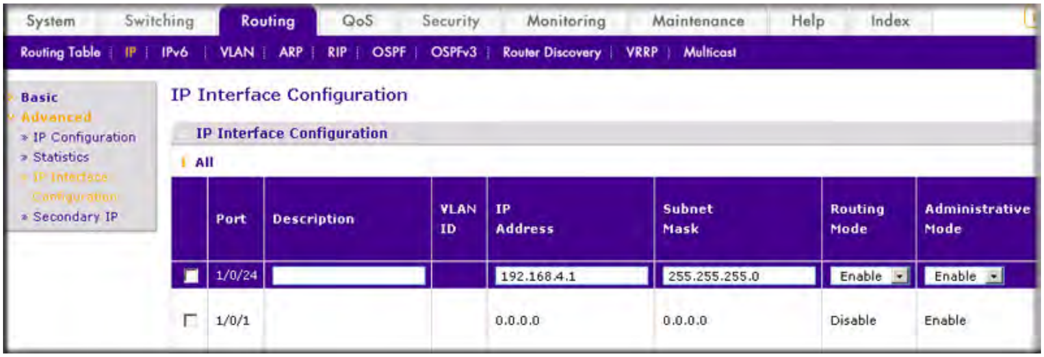
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.6.2**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

4. Configure 1/0/24 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
» IP Configuration
» Statistics
» IP Interface Configuration
» Secondary IP

IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
■	1/0/24			192.168.4.1	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-31

b. Under IP Interface Configuration, scroll down to interface 1/0/24 and select the checkbox for 1/0/24. 1/0/24 now appears in the Interface field at the top.

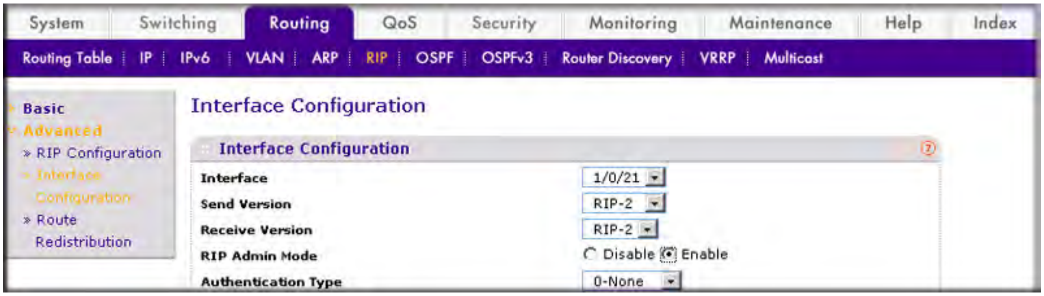
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.4.1**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

5. Enable rip on the interface 1/0/21.

a. From the main menu, select Routing >RIP >Advanced > 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
Basic
Advanced
» RIP Configuration
» Interface Configuration
» Route Redistribution

Interface Configuration

Interface Configuration

Interface	1/0/21
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-32

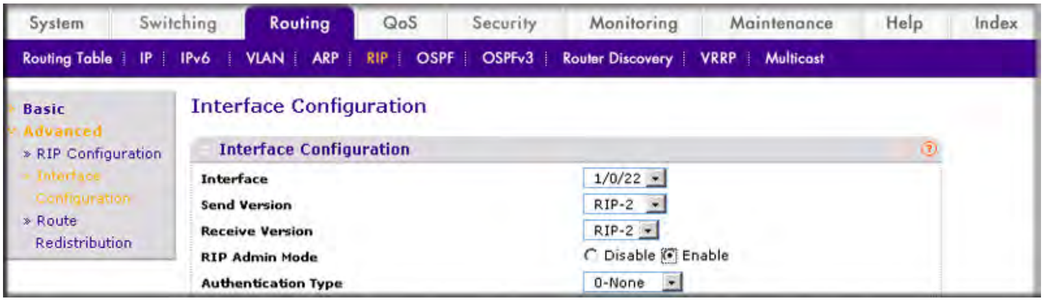
b. Select **1/0/21** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

6. Enable rip on the interface 1/0/22.

a. From the main menu, select Routing > RIP >Advanced > Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/22
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-33

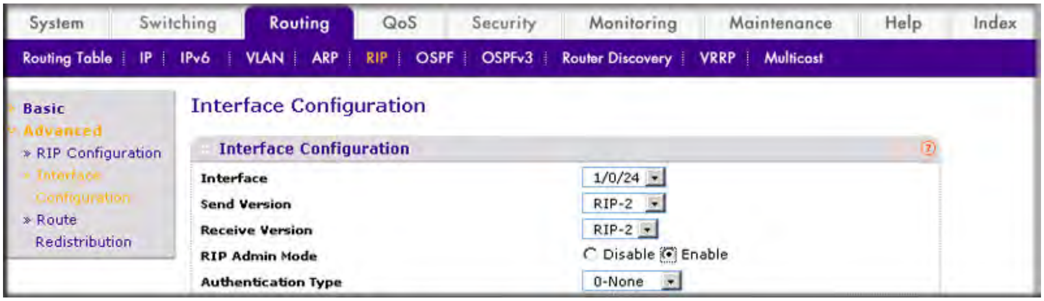
b. Select **1/0/22** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

7. Enable rip on the interface 1/0/24.

a. From the main menu, select Routing > RIP >Advanced > Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/24
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-34

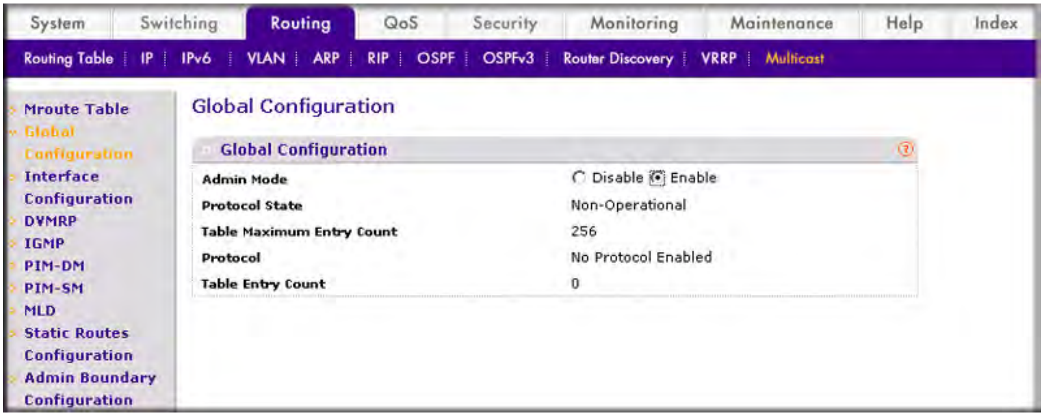
b. Select **1/0/24** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

8. Enable multicast globally.

a. From the main menu, select Routing > Multicast >Global Configuration. A screen similar to the following displays.



Global Configuration

Global Configuration

Admin Mode	○ Disable ● Enable
Protocol State	Non-Operational
Table Maximum Entry Count	256
Protocol	No Protocol Enabled
Table Entry Count	0

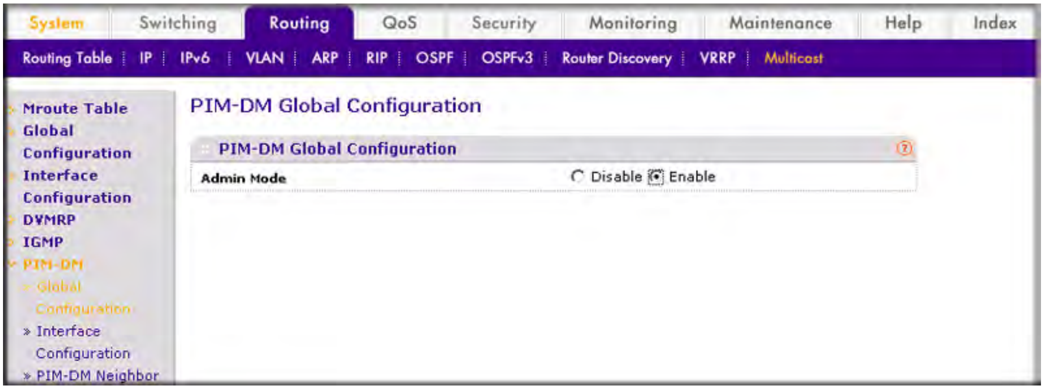
Figure 28-35

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

9. Enable PIM-DM globally.

a. From the main menu, select Routing > Multicast >PIM-DM->Global Configuration. A screen similar to the following displays.



PIM-DM Global Configuration

PIM-DM Global Configuration

Admin Mode	○ Disable ● Enable

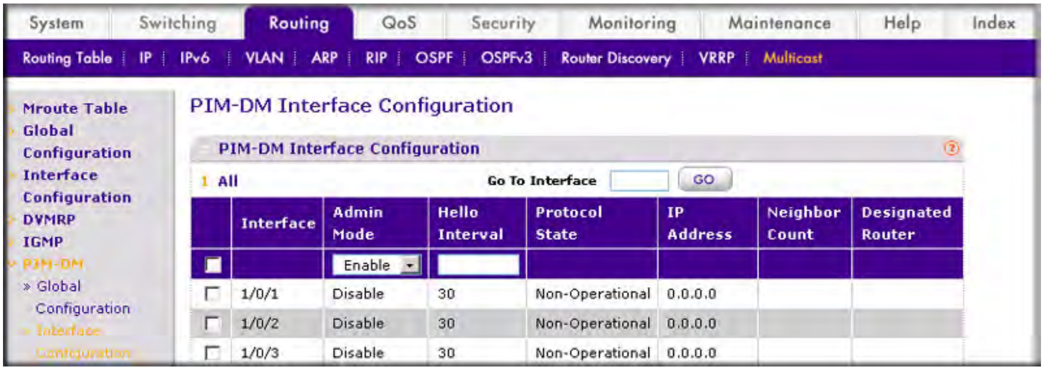
Figure 28-36

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

10. Enable PIM-DM on the interface 1/0/21,1/0/22 and 1/0/24.

a. From the main menu, select Routing > Multicast >PIM-DM->Interface Configuration. A screen similar to the following displays.



PIM-DM Interface Configuration

PIM-DM Interface Configuration

1 All   Go To Interface

	Interface	Admin Mode	Hello Interval	Protocol State	IP Address	Neighbor Count	Designated Router
□		Enable					
□	1/0/1	Disable	30	Non-Operational	0.0.0.0		
□	1/0/2	Disable	30	Non-Operational	0.0.0.0		
□	1/0/3	Disable	30	Non-Operational	0.0.0.0		

Figure 28-37

b. Under PIM-DM Interface Configuration, scroll down to interface 1/0/21 and select the checkbox for **1/0/21**. Then select the **1/0/22** and **1/0/24**.

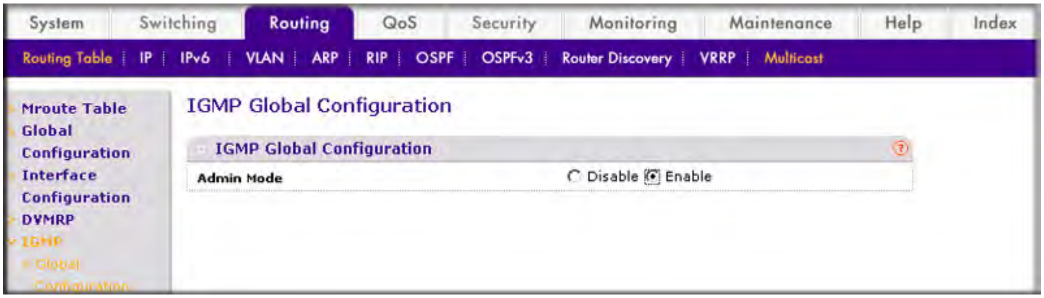
c. Enter the following information in the PIM-DM Interface Configuration.

- Select **Enable** in the Admin Mode field.

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

11. Enable IGMP globally.

a. From the main menu, select Routing > Multicast >IGMP->Global Configuration. A screen similar to the following displays.



IGMP Global Configuration

IGMP Global Configuration

Admin Mode ○ Disable ● Enable

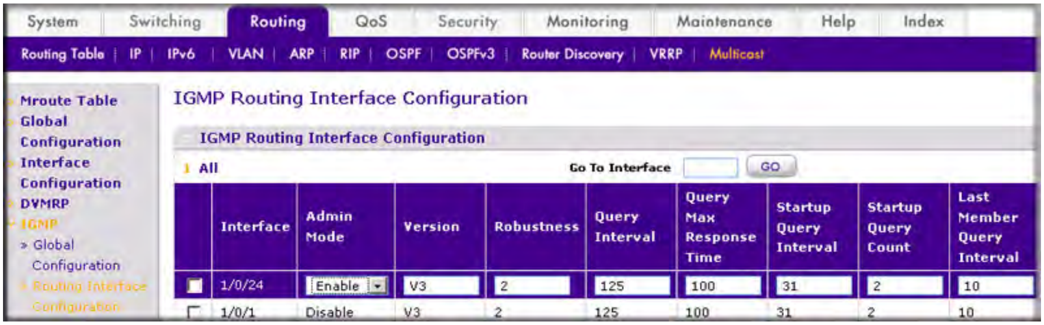
Figure 28-38

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

12. Enable IGMP on the interface 1/0/24.

a. From the main menu, select Routing > Multicast >IGMP->Interface Configuration. A screen similar to the following displays.



IGMP Routing Interface Configuration

IGMP Routing Interface Configuration

All   Go To Interface [ ] GO

	Interface	Admin Mode	Version	Robustness	Query Interval	Query Max Response Time	Startup Query Interval	Startup Query Count	Last Member Query Interval
☐	1/0/24	Enable	V3	2	125	100	31	2	10
☐	1/0/1	Disable	V3	2	125	100	31	2	10

Figure 28-39

b. Under IGMP Routing Interface Configuration, scroll down to interface 1/0/24and select the checkbox for 1/0/24.

c. In the IGMP Routing Interface Configuration, select **Enable** in the Admin Mode field.

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

PIM-SM Configuration

Protocol-Independent Multicast Sparse Mode (PIM-SM) is used to efficiently route multicast traffic to multicast groups that may span wide area networks where bandwidth is a constraint. PIM-SM uses shared trees by default and implements source-based trees for efficiency; it assumes that no hosts want the multicast traffic unless they specifically ask for it. It creates a shared distribution tree centered on a defined “rendezvous point” (RP) from which source traffic is relayed to the receivers. Senders first send the multicast data to the RP, which in turn sends the data down the shared tree to the receivers. Shared trees centered on an RP do not necessarily provide the shortest, most optimal path. In such cases PIM-SM provides a means to switch to more efficient source-specific trees. A data threshold rate is defined for toggling between trees. PIM-SM uses a Bootstrap Router (BSR), which advertises information to other multicast routers about the rendezvous point (RP). In a given network, a set of routers can be administratively enabled as candidate bootstrap routers. If it is not apparent which router should be the BSR, the candidates flood the domain with advertisements. The router with the highest priority is elected. If all the priorities are equal, then the candidate with the highest IP address becomes the BSR. PIM-SM is defined in RFC 4601.

The following example describes how to configure and use PIM-SM. In this case, set the switch B,C,D as RP-candidate and BSR-cadidate. Switch B will become BSR because it has the highest priority. Switch D will become RP after RP election.

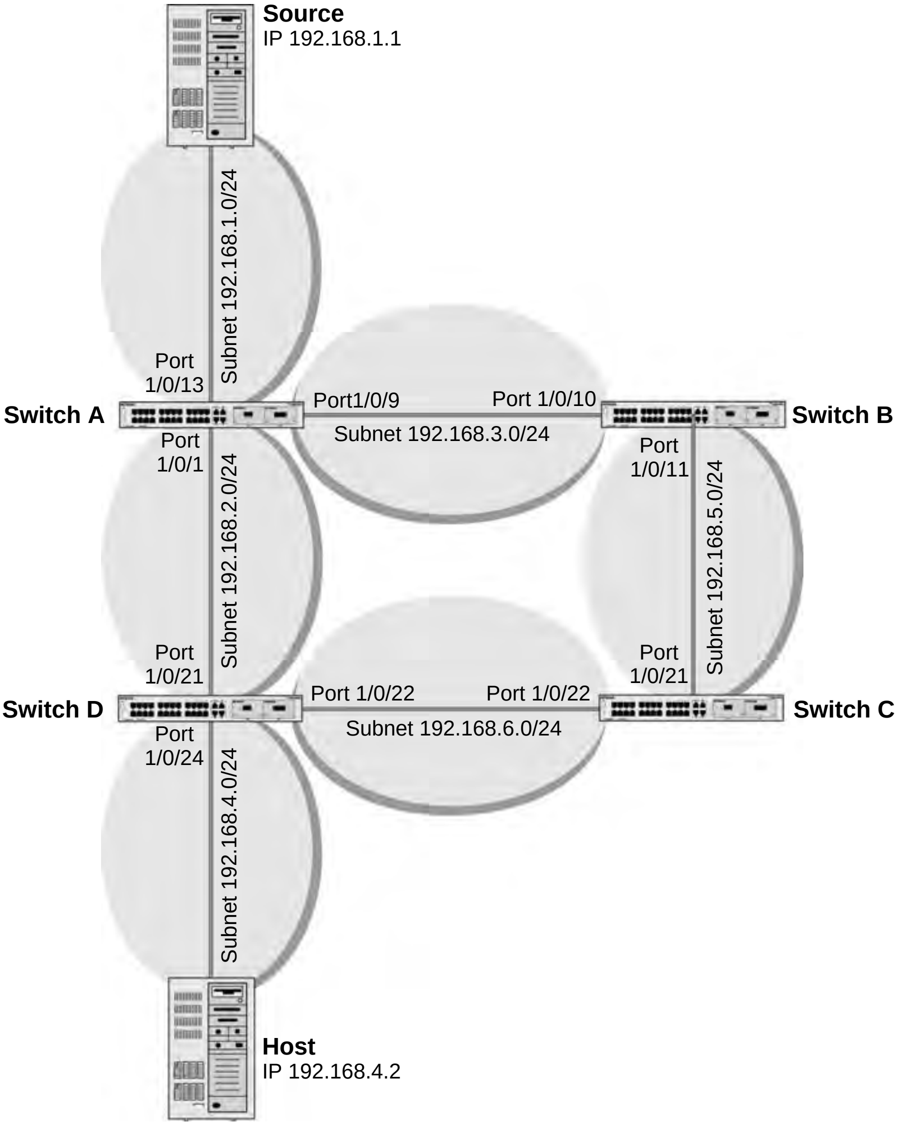

Source
IP 192.168.1.1
Subnet 192.168.1.0/24
Port
1/0/13
Switch A
Port
1/0/1
Port1/0/9
Port 1/0/10
Subnet 192.168.3.0/24
Switch B
Port
1/0/11
Subnet 192.168.2.0/24
Subnet 192.168.5.0/24
Port
1/0/21
Port
1/0/21
Switch D
Port 1/0/22
Port 1/0/22
Subnet 192.168.6.0/24
Switch C
Port
1/0/24
Subnet 192.168.4.0/24
Host
IP 192.168.4.2

Figure 28-40

CLI: Configuring PIM-SM

On Switch A

Enable ip routing on the switch.

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

Enable pim-sm on the switch.

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

Enable ip multicast forwarding on the switch.

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

Enable RIP to build unicast IP routing table.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address  192.168.2.2  255.255.255.0
(Netgear Switch) (Interface 1/0/1)#ip rip
```

```
(Netgear Switch) (Interface 1/0/1)#ip pimsm
(Netgear Switch) (Interface 1/0/1)#exit

(Netgear Switch) (Config)#interface 1/0/9
(Netgear Switch) (Interface 1/0/9)#routing
(Netgear Switch) (Interface 1/0/9)#ip address  192.168.3.1  255.255.255.0
(Netgear Switch) (Interface 1/0/9)#ip rip
(Netgear Switch) (Interface 1/0/9)#ip pimsm
(Netgear Switch) (Interface 1/0/9)#exit

(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ip address  192.168.1.2  255.255.255.0
(Netgear Switch) (Interface 1/0/13)#ip rip
(Netgear Switch) (Interface 1/0/13)#ip pimsm
(Netgear Switch) (Interface 1/0/1)#exit
```

On Switch B

Enable the switch to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

```
(Netgear Switch)#configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pimsm
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#ip pimsm rp-candidate interface 1/0/11 225.1.1.1
255.255.255.0
```

Enable the switch to announce its candidacy as a bootstrap router (BSR).

```
(Netgear Switch) (Config)#ip pimsm bsr-candidate interface 1/0/10 30  7

(Netgear Switch) (Config)#interface 1/0/10
(Netgear Switch) (Interface 1/0/10)#routing
(Netgear Switch) (Interface 1/0/10)#ip address  192.168.3.2  255.255.255.0
(Netgear Switch) (Interface 1/0/10)#ip rip
(Netgear Switch) (Interface 1/0/10)#ip pimsm
(Netgear Switch) (Interface 1/0/10)#exit

(Netgear Switch) (Config)#interface 1/0/11
(Netgear Switch) (Interface 1/0/11)#routing
(Netgear Switch) (Interface 1/0/11)#ip address  192.168.5.1  255.255.255.0
(Netgear Switch) (Interface 1/0/11)#ip rip
(Netgear Switch) (Interface 1/0/11)#ip pimsm
(Netgear Switch) (Interface 1/0/11)#exit
```

On Switch C

```
(Netgear Switch)#configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pimsm
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#ip pimsm rp-candidate interface 1/0/22 225.1.1.1
255.255.255.0
(Netgear Switch) (Config)#ip pimsm bsr-candidate interface 1/0/21  30  5
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address  192.168.5.2  255.255.255.0
(Netgear Switch) (Interface 1/0/21)#ip rip
(Netgear Switch) (Interface 1/0/21)#ip pimsm
(Netgear Switch) (Interface 1/0/21)#exit
```

```
(Netgear Switch) (Config)#interface 1/0/22
(Netgear Switch) (Interface 1/0/22)#routing
(Netgear Switch) (Interface 1/0/22)#ip address  192.168.6.1  255.255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22)#ip pimsm
(Netgear Switch) (Interface 1/0/22)#exit
```

On Switch D

```
(Netgear Switch)#configure
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip igmp
(Netgear Switch) (Config)#ip pimsm
(Netgear Switch) (Config)#ip pimsm rp-candidate interface 1/0/22 225.1.1.1
255.255.255.0
(Netgear Switch) (Config)#ip pimsm bsr-candidate interface 1/0/22  30   3
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address  192.168.2.1  255.255.255.0
(Netgear Switch) (Interface 1/0/21)#ip rip
(Netgear Switch) (Interface 1/0/21)#ip pimsm
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) (Config)#interface 1/0/22
(Netgear Switch) (Interface 1/0/22)#routing
(Netgear Switch) (Interface 1/0/22)#ip address  192.168.6.2  255.255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22)#ip pimsm
(Netgear Switch) (Interface 1/0/22)#exit

(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#routing
(Netgear Switch) (Interface 1/0/24)#ip address  192.168.4.1  255.255.255.0
(Netgear Switch) (Interface 1/0/24)#ip rip
(Netgear Switch) (Interface 1/0/24)#ip igmp
(Netgear Switch) (Interface 1/0/24)#ip pimsm
(Netgear Switch) (Interface 1/0/24)#exit
```

After that, PIM-SM builds the multicast route table on each switch. The following tables show the routes that are built after PIM-SM switches to the source-specific tree from shared tree.

```
(A) #show ip mcast mroute summary
                  Multicast Route Table Summary
                                           Incoming     Outgoing
Source IP       Group IP     Protocol     Interface    Interface List
-----------     ---------    ---------    ---------    ---------------
192.168.1.1     225.1.1.1    PIMSM         1/0/13        1/0/1

(B) #show ip mcast mroute summary
                   Multicast Route Table Summary
                                          Incoming      Outgoing
Source IP       Group IP      Protocol    Interface     Interface List
-----------     ----------   ---------   ---------      ---------------
192.168.1.1     225.1.1.1     PIMSM       1/0/10

(C) #show ip mcast mroute summary
                  Multicast Route Table Summary
                                         Incoming      Outgoing
Source IP       Group IP     Protocol    Interface     Interface List
------------    ---------   ----------   ---------    ---------------
    *           225.1.1.1    PIMSM        1/0/22
192.168.1.1     225.1.1.1    PIMSM        1/0/21

(D) #show ip mcast mroute summary
                  Multicast Route Table Summary
                                         Incoming      Outgoing
Source IP       Group IP      Protocol    Interface    Interface List
----------    -----------    ----------  ---------    ---------------
    *           225.1.1.1       PIMSM    1/0/22          1/0/24
192.168.1.1     225.1.1.1       PIMSM    1/0/21          1/0/24
```

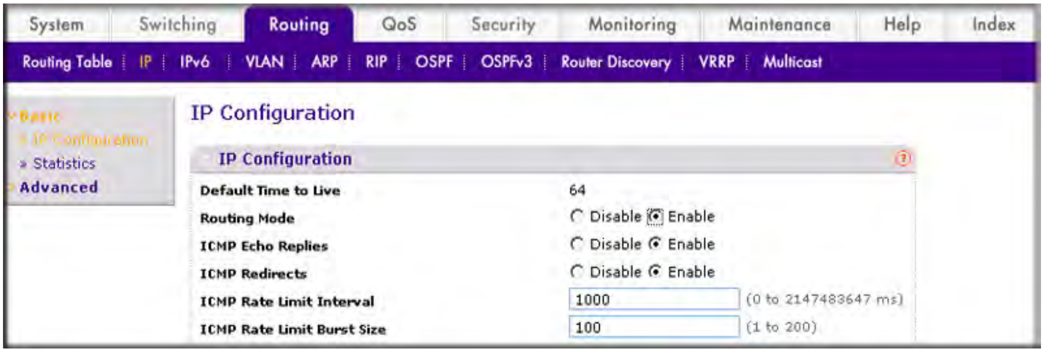
Web Interface: Configuring PIM-SM

On Switch A:

To use the Web interface to config PIM-SM, proceed as follows:

1. Enable IP routing on the switch.

  a. From the main menu, select Routing >IP >Basic >IP configuration. A screen similar to the following displays.



IP Configuration

IP Configuration

Default Time to Live	64	
Routing Mode	○ Disable ● Enable	
ICMP Echo Replies	○ Disable ● Enable	
ICMP Redirects	○ Disable ● Enable	
ICMP Rate Limit Interval	1000	(0 to 2147483647 ms)
ICMP Rate Limit Burst Size	100	(1 to 200)

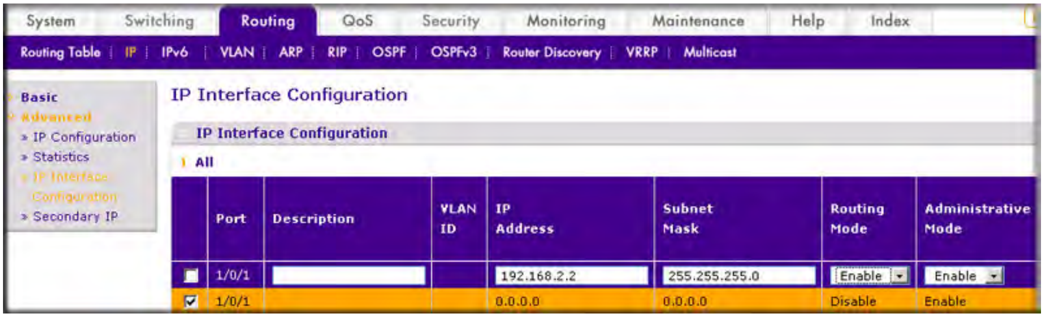
Figure 28-41

b. Next to the Routing Mode, select the **Enable** radio button.

c. Click **Apply**.

2. Configure 1/0/1 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
IP Configuration
Statistics
IP Interface Configuration
Secondary IP

IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
□	1/0/1			192.168.2.2	255.255.255.0	Enable	Enable
☑	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-42

b. Under IP Interface Configuration, scroll down to interface 1/0/1 and select the checkbox for 1/0/1. 1/0/1 now appears in the Interface field at the top.

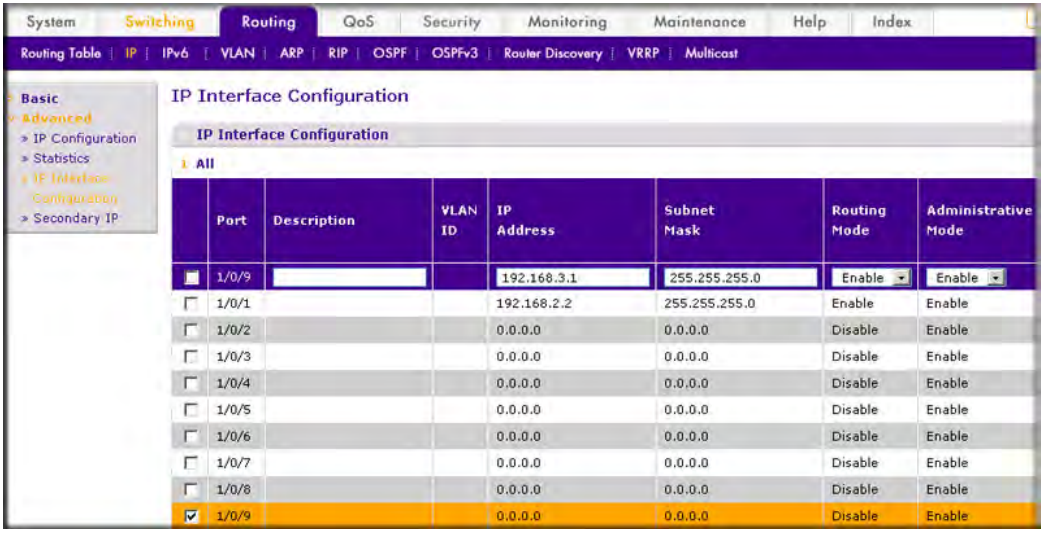
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.2.2**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

3. Configure 1/0/9 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
IP Configuration
Statistics
IP Interface Configuration
Secondary IP

IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
□	1/0/9			192.168.3.1	255.255.255.0	Enable	Enable
□	1/0/1			192.168.2.2	255.255.255.0	Enable	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
□	1/0/5			0.0.0.0	0.0.0.0	Disable	Enable
□	1/0/6			0.0.0.0	0.0.0.0	Disable	Enable
□	1/0/7			0.0.0.0	0.0.0.0	Disable	Enable
□	1/0/8			0.0.0.0	0.0.0.0	Disable	Enable
☑	1/0/9			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-43

b. Under IP Interface Configuration, scroll down to interface 1/0/9 and select teh checkbox for 1/0/9. Now 1/0/9 appears in the Interface field at the top.

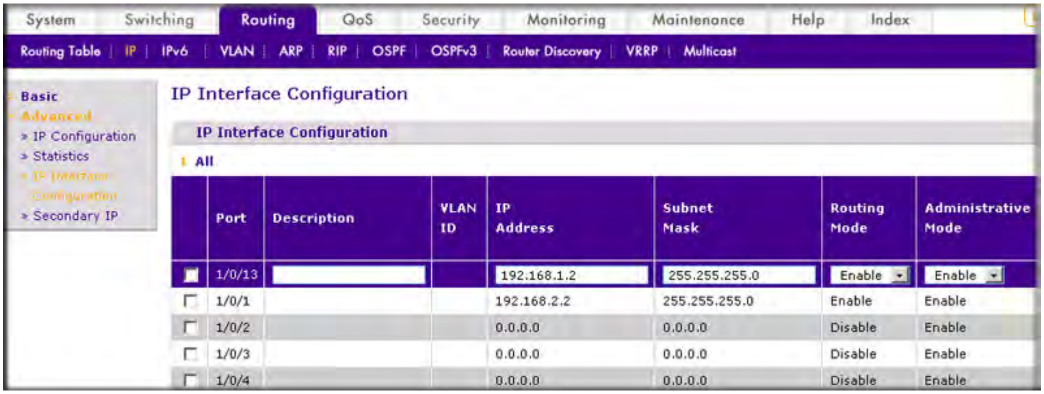
c. Enter the following information in the IP Interface Configuration:

- In the IP address, enter **192.168.3.1**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

d. Click **Apply**.

4. Configure 1/0/13 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
» IP Configuration
» Statistics
» IP Interface Configuration
» Secondary IP

IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☑	1/0/13			192.168.1.2	255.255.255.0	Enable	Enable
□	1/0/1			192.168.2.2	255.255.255.0	Enable	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

Figure 28-44

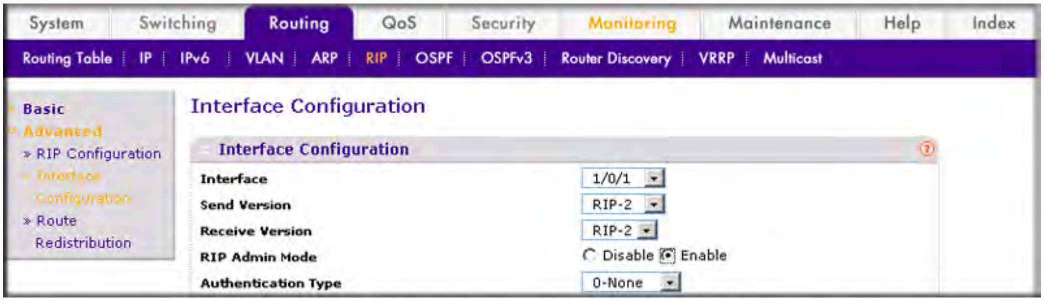
b. Under IP Interface Configuration, scroll down to interface 1/0/13 and select the checkbox for 1/0/13. 1/0/13 now appears in the Interface field at the top.

c. Enter the following information in the IP Interface Configuration.
   - In the IP address, enter **192.168.1.2**.
   - In the Subnet Mask, enter **255.255.255.0**.
   - Select **Enable** in the Routing Mode field.

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

5. Enable rip on the interface 1/0/1.

   a. From the main menu, select Routing >RIP >Advanced > 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
Basic
Advanced
» RIP Configuration
» Interface Configuration
» Route Redistribution

Interface Configuration

Interface Configuration

Interface	1/0/1
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-45

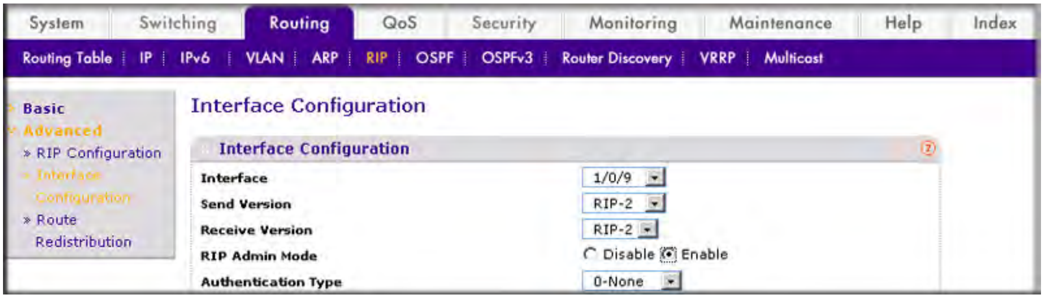
b. Select **1/0/1** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

6. Enable rip on the interface 1/0/9.

a. From the main menu, select Routing > RIP >Advanced > Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/9
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-46

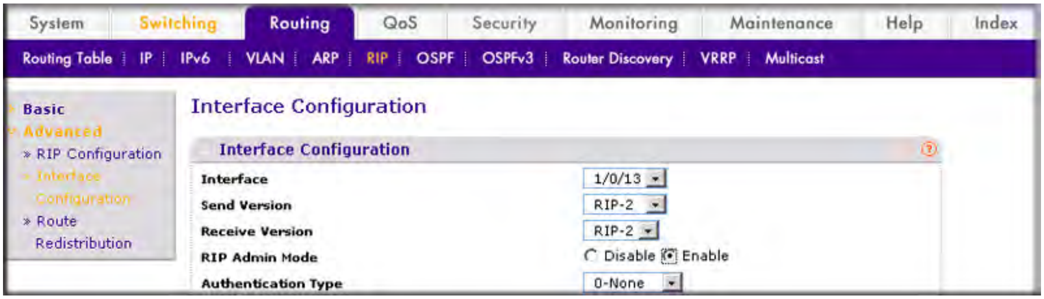
b. Select **1/0/9** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

7. Enable rip on the interface 1/0/13.

a. From the main menu, select Routing > RIP >Advanced > Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/13
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-47

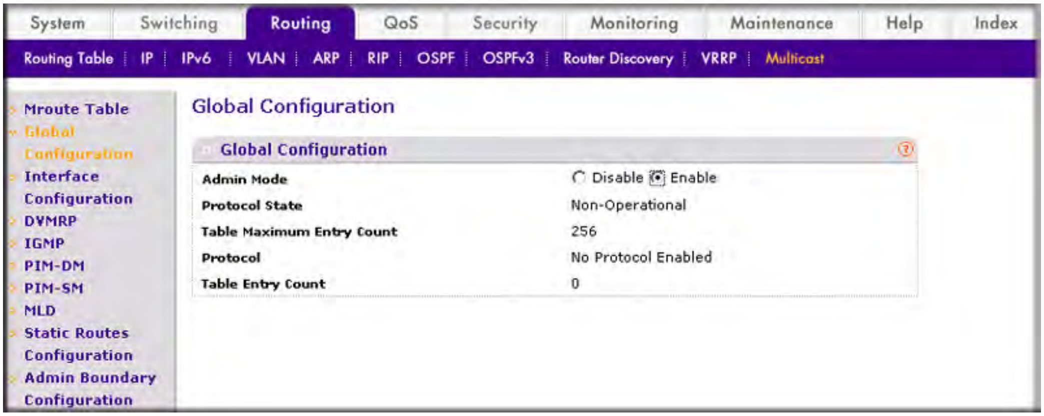
b. Select **1/0/13** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

8. Enable multicast globally.

a. From the main menu, select Routing > Multicast >Global Configuration. A screen similar to the following displays.



Global Configuration

Global Configuration

Admin Mode	○ Disable ● Enable
Protocol State	Non-Operational
Table Maximum Entry Count	256
Protocol	No Protocol Enabled
Table Entry Count	0

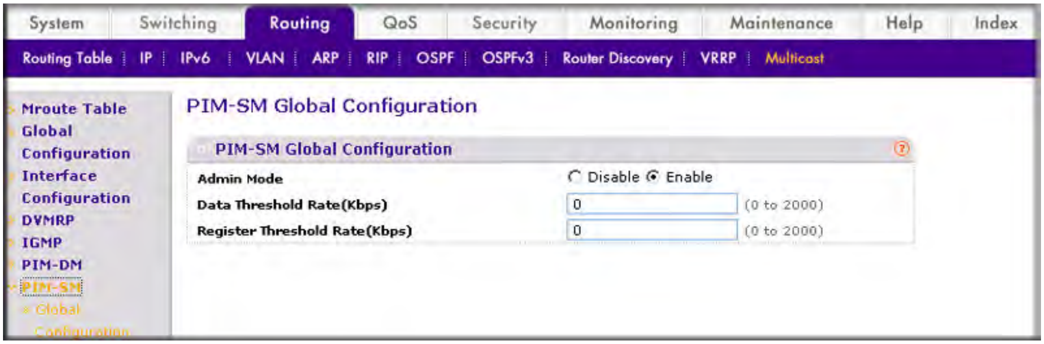
Figure 28-48

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

9. Enable PIM-SM globally.

a. From the main menu, select Routing > Multicast >PIM-SM->Global Configuration. A screen similar to the following displays.



PIM-SM Global Configuration

PIM-SM Global Configuration

Admin Mode	○ Disable ● Enable	
Data Threshold Rate(Kbps)	0	(0 to 2000)
Register Threshold Rate(Kbps)	0	(0 to 2000)

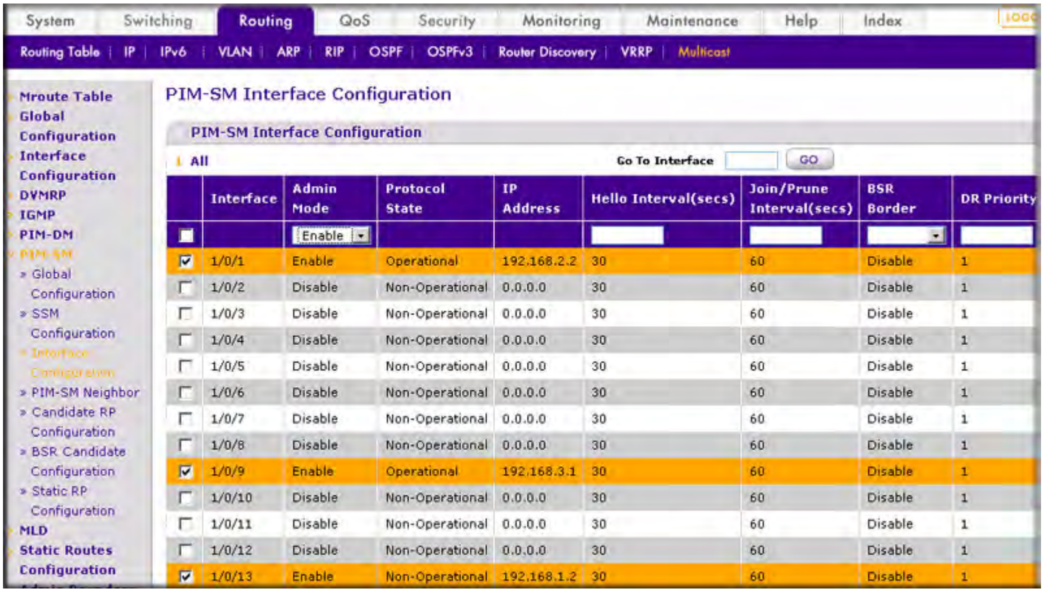
Figure 28-49

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

10. Enable PIM-SM on the interface 1/0/1,1/0/9 and 1/0/13.

a. From the main menu, select Routing > Multicast >PIM-SM->Interface Configuration. A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
LOGO
Routing Table | IP | IPv6 | VLAN | ARP | RIP | OSPF | OSPFv3 | Router Discovery | VRRP | Multicast
Mroute Table
Global Configuration
Interface Configuration
DVMRP
IGMP
PIM-DM
PIM-SM
» Global Configuration
» SSM Configuration
» Interface Configuration
» PIM-SM Neighbor
» Candidate RP Configuration
» BSR Candidate Configuration
» Static RP Configuration
MLD
Static Routes Configuration
All
Go To Interface
GO

PIM-SM Interface Configuration

PIM-SM Interface Configuration

	Interface	Admin Mode	Protocol State	IP Address	Hello Interval(secs)	Join/Prune Interval(secs)	BSR Border	DR Priority
☐		Enable						
☑	1/0/1	Enable	Operational	192.168.2.2	30	60	Disable	1
☐	1/0/2	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
☐	1/0/3	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
☐	1/0/4	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
☐	1/0/5	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
☐	1/0/6	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
☐	1/0/7	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
☐	1/0/8	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
☑	1/0/9	Enable	Operational	192.168.3.1	30	60	Disable	1
☐	1/0/10	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
☐	1/0/11	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
☐	1/0/12	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
☑	1/0/13	Enable	Non-Operational	192.168.1.2	30	60	Disable	1

Figure 28-50

b. Under PIM-SM Interface Configuration, scroll down to interface 1/0/1 and select the checkbox for 1/0/1. Then select the 1/0/9 and 1/0/13.

c. In the PIM-SM Interface Configuration, select **Enable** in the Admin Mode field.

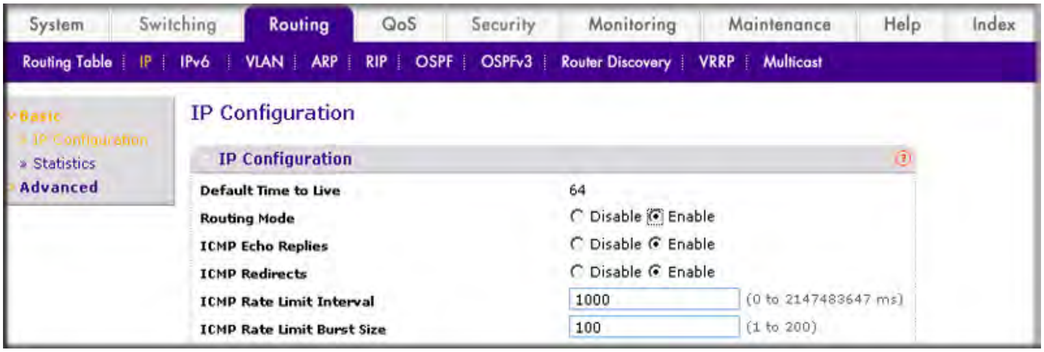
d. Click **Apply** to save the settings.

On Switch B:

To use the Web interface to config PIM-SM, proceed as follows:

1. Enable IP routing on the switch.

a. From the main menu, select Routing >IP >Basic >IP configuration. A screen similar to the following displays.



IP Configuration

IP Configuration

Default Time to Live	64
Routing Mode	○ Disable ● Enable
ICMP Echo Replies	○ Disable ● Enable
ICMP Redirects	○ Disable ● Enable
ICMP Rate Limit Interval	1000 (0 to 2147483647 ms)
ICMP Rate Limit Burst Size	100 (1 to 200)

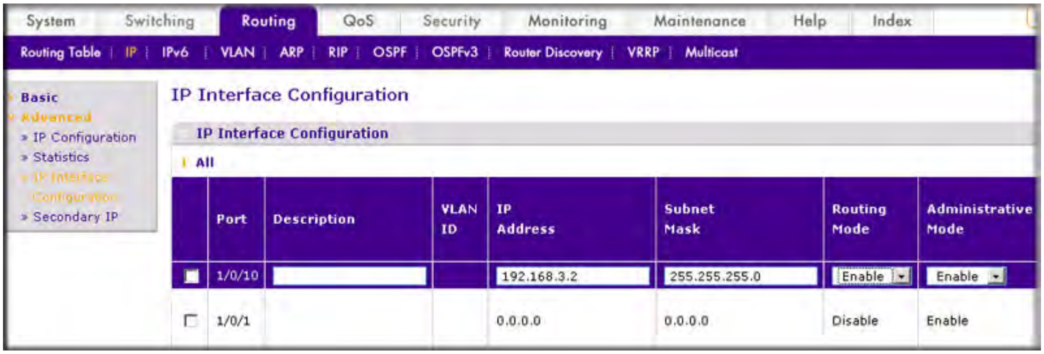
Figure 28-51

b. Next to the Routing Mode, select the **Enable** radio button.

c. Click **Apply**.

2. Configure 1/0/10 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
IP Configuration
Statistics
IP Interface Configuration
Secondary IP

IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☐	1/0/10			192.168.3.2	255.255.255.0	Enable	Enable
☐	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-52

b. Under IP Interface Configuration, scroll down to interface 1/0/10 and select the checkbox for 1/0/10. 1/0/10 now appears in the Interface field at the top.

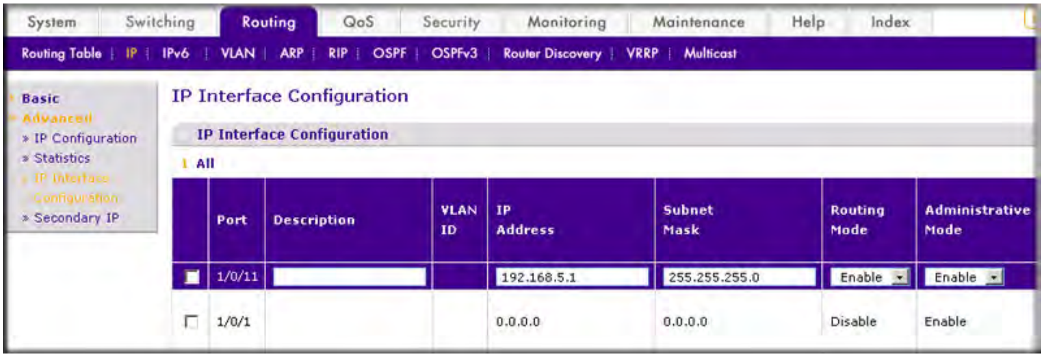
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.3.2**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

3. Configure 1/0/11 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
» IP Configuration
» Statistics
» IP Interface Configuration
» Secondary IP

IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☑	1/0/11			192.168.5.1	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-53

b. Under IP Interface Configuration, scroll down to interface 1/0/11 and select the checkbox for 1/0/11. 1/0/11 now appears in the Interface field at the top.

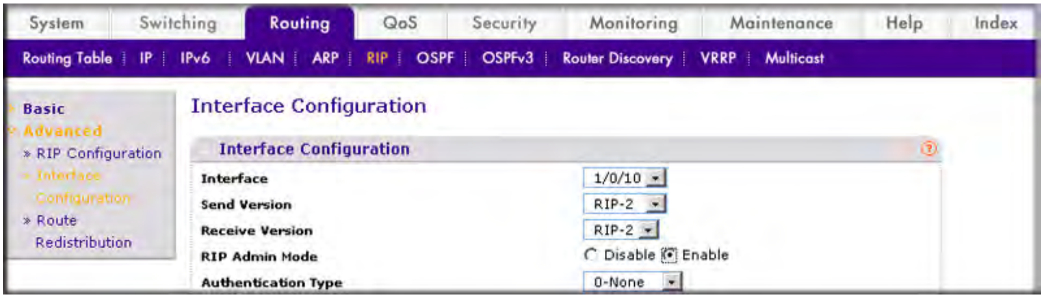
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.5.1**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

4. Enable rip on the interface 1/0/10.

a. From the main menu, select Routing >RIP >Advanced > 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
Basic
Advanced
» RIP Configuration
» Interface Configuration
» Route Redistribution

Interface Configuration

Interface Configuration

Interface	1/0/10
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-54

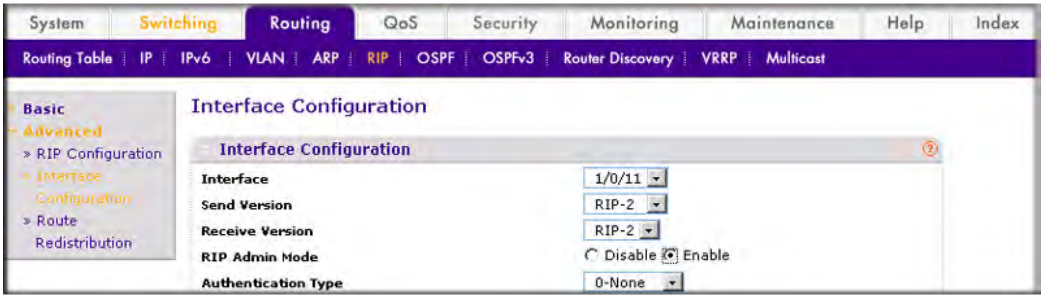
b. Select **1/0/10** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

5. Enable rip on the interface 1/0/11.

   a. From the main menu, select Routing > RIP >Advanced > Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/11
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-55

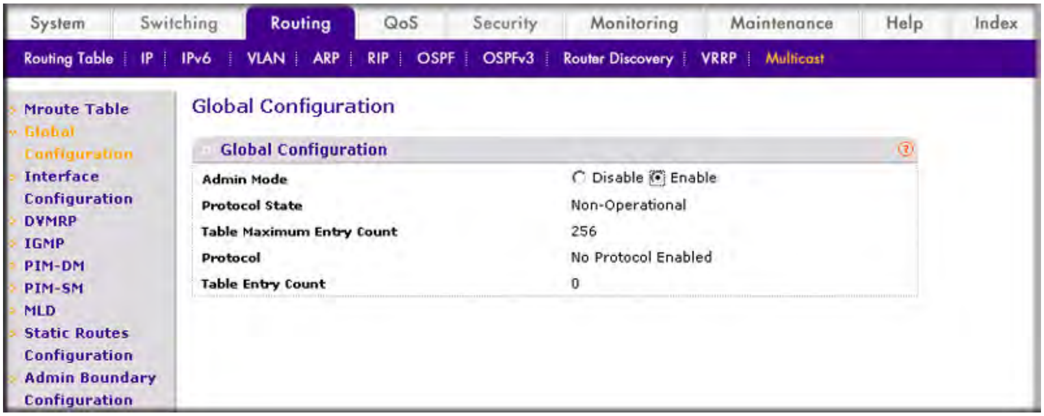
   b. Select **1/0/11** in the Interface field.

   c. Next to the RIP Admin Mode, select the **Enable** radio button.

   d. Click **Apply**.

6. Enable multicast globally.

   a. From the main menu, select Routing > Multicast >Global Configuration. A screen similar to the following displays.



Global Configuration

Global Configuration

Admin Mode	○ Disable ● Enable
Protocol State	Non-Operational
Table Maximum Entry Count	256
Protocol	No Protocol Enabled
Table Entry Count	0

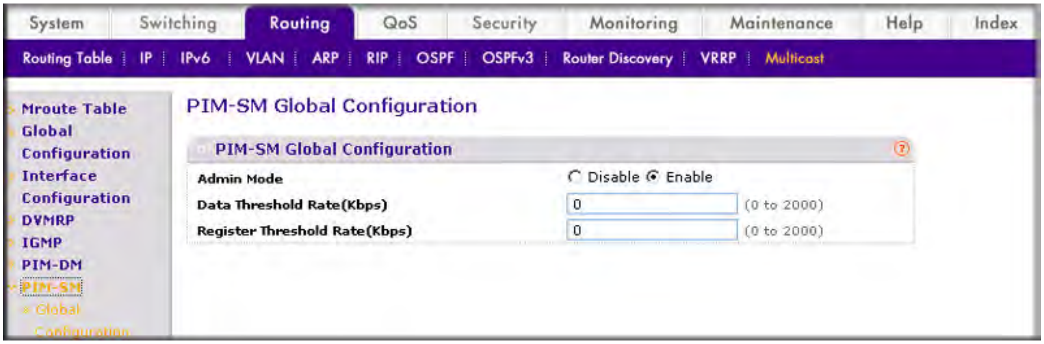
Figure 28-56

   b. Next to the Admin Mode, select the **Enable** radio button.

   c. Click **Apply**.

7. Enable PIM-SM globally.

a. From the main menu, select Routing > Multicast >PIM-SM->Global Configuration. A screen similar to the following displays.



PIM-SM Global Configuration

PIM-SM Global Configuration

Admin Mode	○ Disable ● Enable	
Data Threshold Rate(Kbps)	0	(0 to 2000)
Register Threshold Rate(Kbps)	0	(0 to 2000)

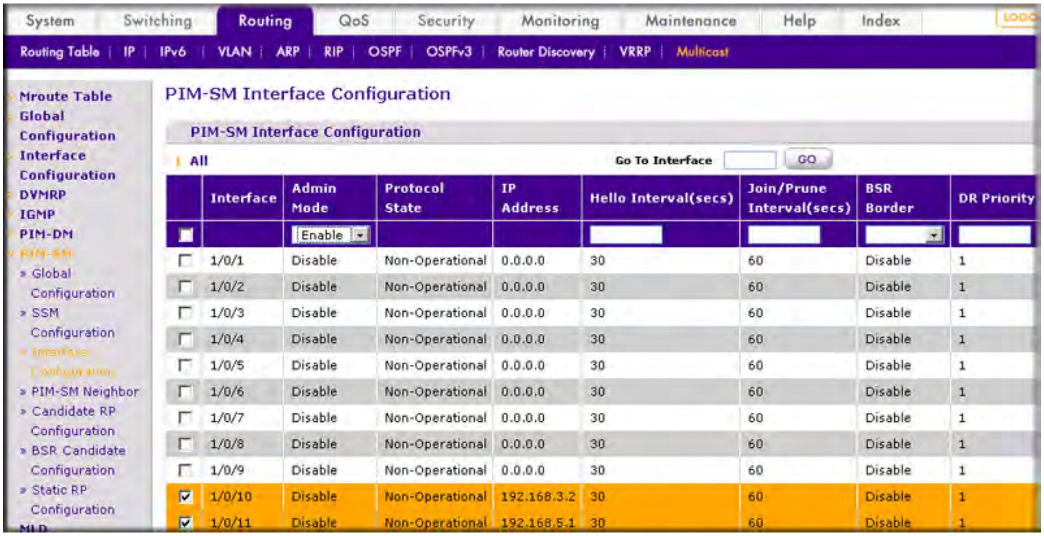
Figure 28-57

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

8. Enable PIM-SM on the interface 1/0/10 and 1/0/11.

a. From the main menu, select Routing > Multicast >PIM-SM->Interface Configuration. A screen similar to the following displays.



PIM-SM Interface Configuration

PIM-SM Interface Configuration

	Interface	Admin Mode	Protocol State	IP Address	Hello Interval(secs)	Join/Prune Interval(secs)	BSR Border	DR Priority
■		Enable						
□	1/0/1	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
□	1/0/2	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
□	1/0/3	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
□	1/0/4	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
□	1/0/5	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
□	1/0/6	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
□	1/0/7	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
□	1/0/8	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
□	1/0/9	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
☑	1/0/10	Disable	Non-Operational	192.168.3.2	30	60	Disable	1
☑	1/0/11	Disable	Non-Operational	192.168.5.1	30	60	Disable	1

Figure 28-58

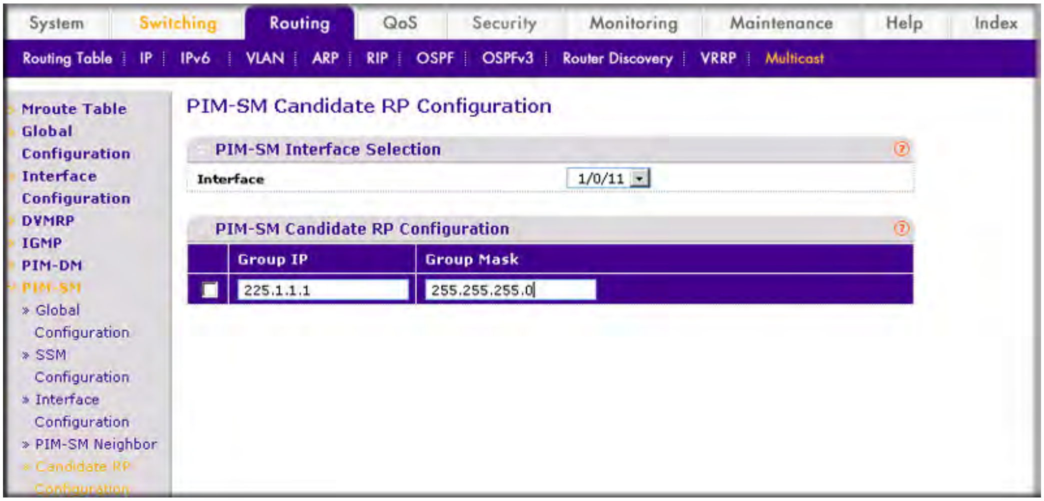
b. Under PIM-SM Interface Configuration, scroll down to interface 1/0/10 and select the checkbox for 1/0/10. Then select the interface 1/0/11.

c. In the PIM-SM Interface Configuration, select **Enable** in the Admin Mode field.

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

9. Candidate RP Configuration.

a. From the main menu, select Routing > Multicast >PIM-SM->Candidate RP Configuration. A screen similar to the following displays.



PIM-SM Candidate RP Configuration

PIM-SM Interface Selection

Interface 1/0/11

PIM-SM Candidate RP Configuration

	Group IP	Group Mask
□	225.1.1.1	255.255.255.0

Figure 28-59

b. Select **1/0/11** in the Interface field.

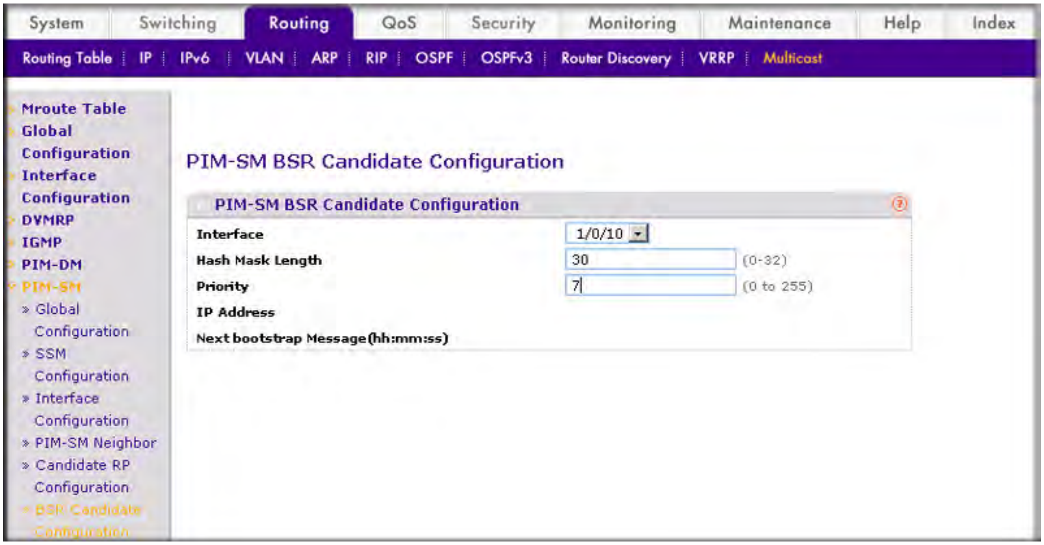
c. In the Group IP, enter 225.1.1.1.

d. In the Group Mask, enter 255.255.255.0.

e. Click **Add**.

10. BSR Candidate Configuration.

a. From the main menu, select Routing > Multicast >PIM-SM->BSR Candidate Configuration. A screen similar to the following displays.



PIM-SM BSR Candidate Configuration

PIM-SM BSR Candidate Configuration

Interface	1/0/10	
Hash Mask Length	30	(0-32)
Priority	7	(0 to 255)
IP Address		
Next bootstrap Message(hh:mm:ss)		

Figure 28-60

b. Select the **1/0/10** in the Interface field.

c. In the Hash Mask Length field, enter **30**.

d. In the Priority field, enter **7**.

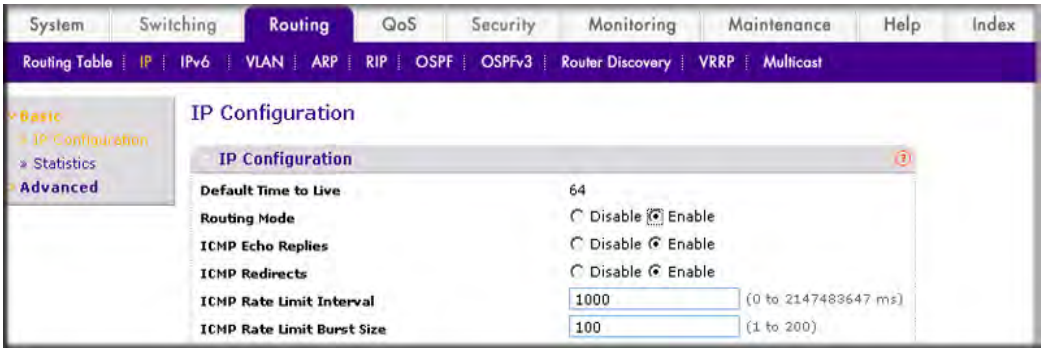
e. Click **Apply**.

On Switch C:

To use the Web interface to config PIM-SM, proceed as follows:

1. Enable IP routing on the switch.

a. From the main menu, select Routing >IP >Basic >IP configuration. A screen similar to the following displays.



IP Configuration

IP Configuration	
Default Time to Live	64
Routing Mode	○ Disable ● Enable
ICMP Echo Replies	○ Disable ● Enable
ICMP Redirects	○ Disable ● Enable
ICMP Rate Limit Interval	1000 (0 to 2147483647 ms)
ICMP Rate Limit Burst Size	100 (1 to 200)

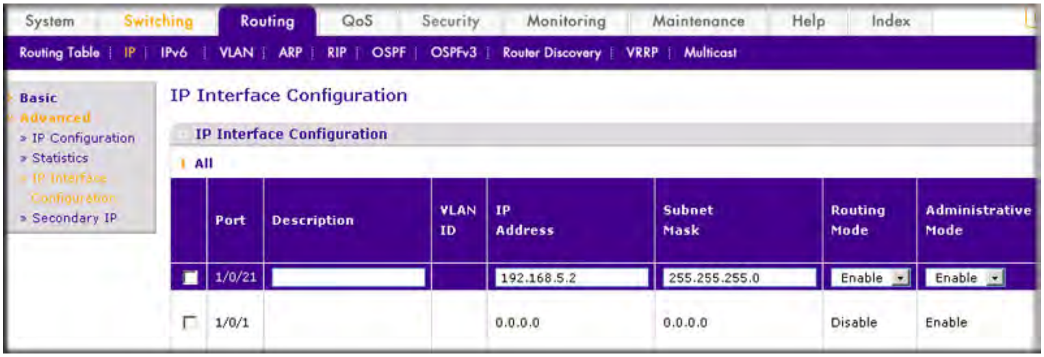
Figure 28-61

b. Next to the Routing Mode, select the **Enable** radio button.

c. Click **Apply**.

2. Configure 1/0/21 as a routing port and assign IP address to it.

a. From the main menu, select Routing > IP >Advanced > IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☑	1/0/21			192.168.5.2	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-62

b. Under IP Interface Configuration, scroll down to interface 1/0/21 and select the checkbox for 1/0/21. 1/0/21 now appears in the Interface field at the top.

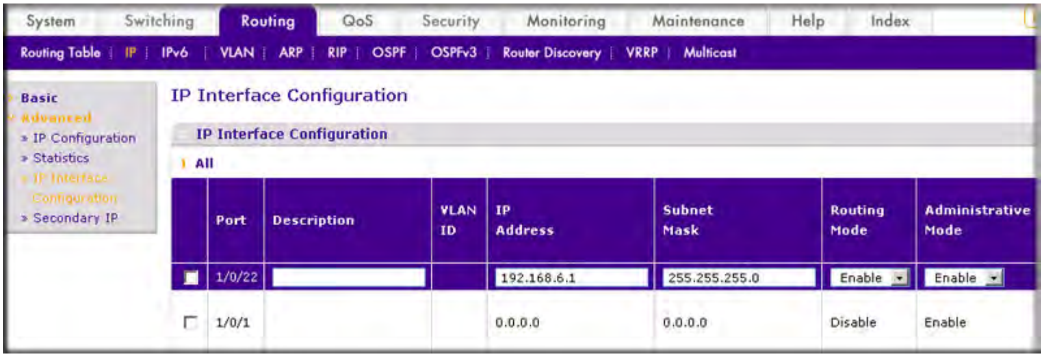
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.5.2**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

3. Configure 1/0/22 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
IP Configuration
Statistics
IP Interface Configuration
Secondary IP

IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☑	1/0/22			192.168.6.1	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-63

b. Under IP Interface Configuration, scroll down to interface 1/0/22 and select the checkbox for 1/0/22. 1/0/22 now appears in the Interface field at the top.

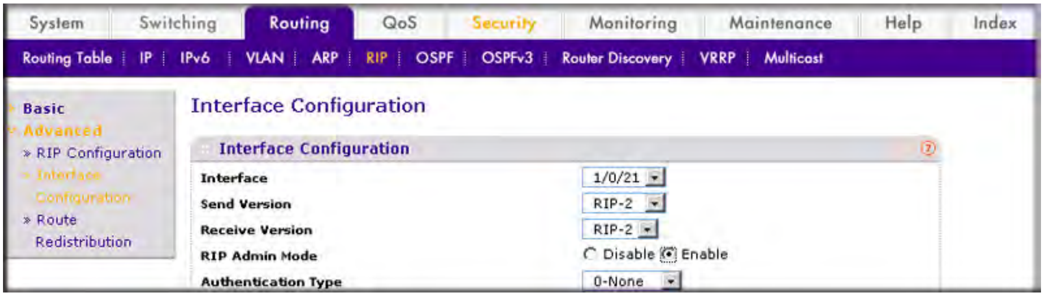
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.6.1**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

4. Enable rip on the interface 1/0/21.

a. From the main menu, select Routing >RIP >Advanced > Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/21
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-64

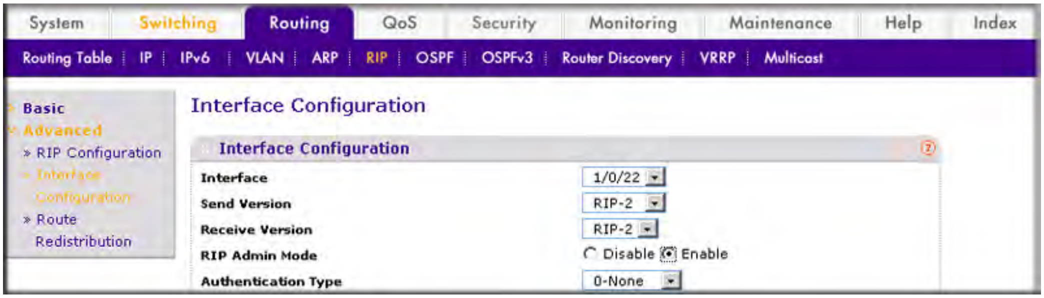
b. Select **1/0/21** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

5. Enable rip on the interface 1/0/22.

a. From the main menu, select Routing > RIP >Advanced > Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/22
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-65

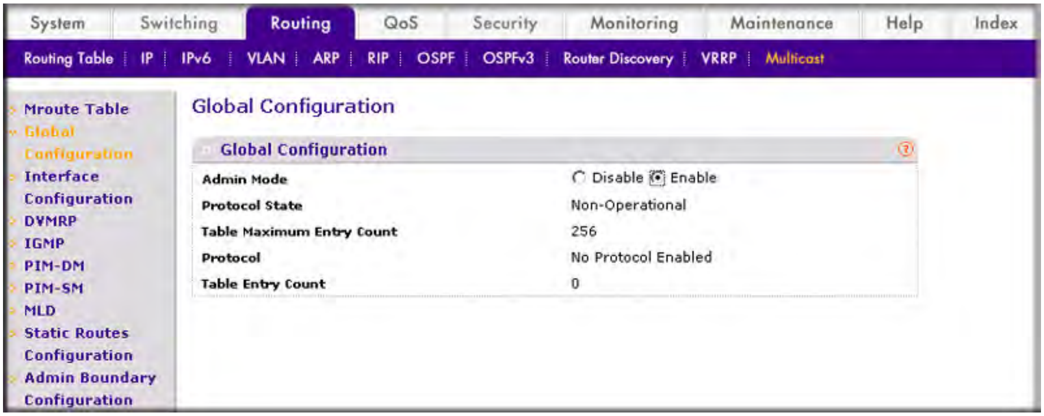
b. Select **1/0/22** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

6. Enable multicast globally.

a. From the main menu, select Routing > Multicast >Global Configuration. A screen similar to the following displays.



Global Configuration

Global Configuration

Admin Mode	○ Disable ● Enable
Protocol State	Non-Operational
Table Maximum Entry Count	256
Protocol	No Protocol Enabled
Table Entry Count	0

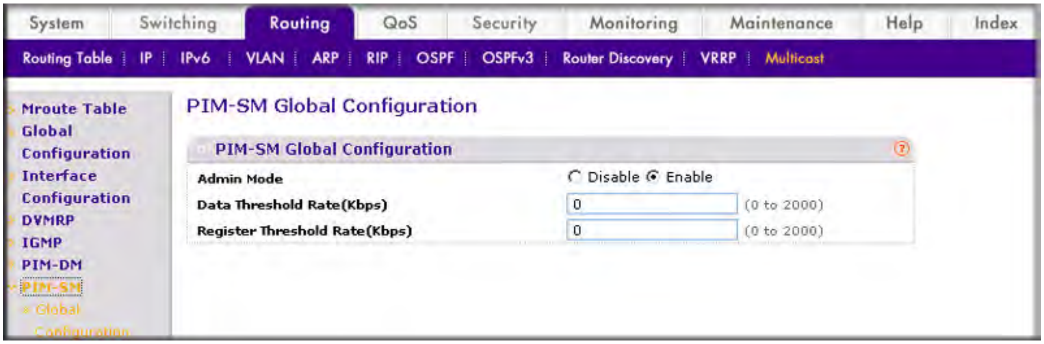
Figure 28-66

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

7. Enable PIM-SM globally.

a. From the main menu, select Routing > Multicast >PIM-SM->Global Configuration. A screen similar to the following displays.



PIM-SM Global Configuration

PIM-SM Global Configuration

Admin Mode	○ Disable ● Enable	
Data Threshold Rate(Kbps)	0	(0 to 2000)
Register Threshold Rate(Kbps)	0	(0 to 2000)

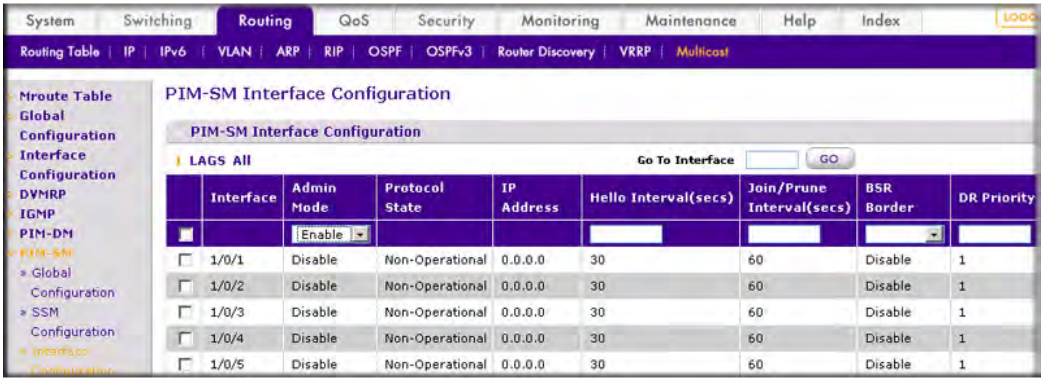
Figure 28-67

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

8. Enable PIM-SM on the interface 1/0/21 and 1/0/22.

a. From the main menu, select Routing > Multicast >PIM-SM->Interface Configuration. A screen similar to the following displays.



PIM-SM Interface Configuration

PIM-SM Interface Configuration

	Interface	Admin Mode	Protocol State	IP Address	Hello Interval(secs)	Join/Prune Interval(secs)	BSR Border	DR Priority
■		Enable						
□	1/0/1	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
□	1/0/2	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
□	1/0/3	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
□	1/0/4	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
□	1/0/5	Disable	Non-Operational	0.0.0.0	30	60	Disable	1

Figure 28-68

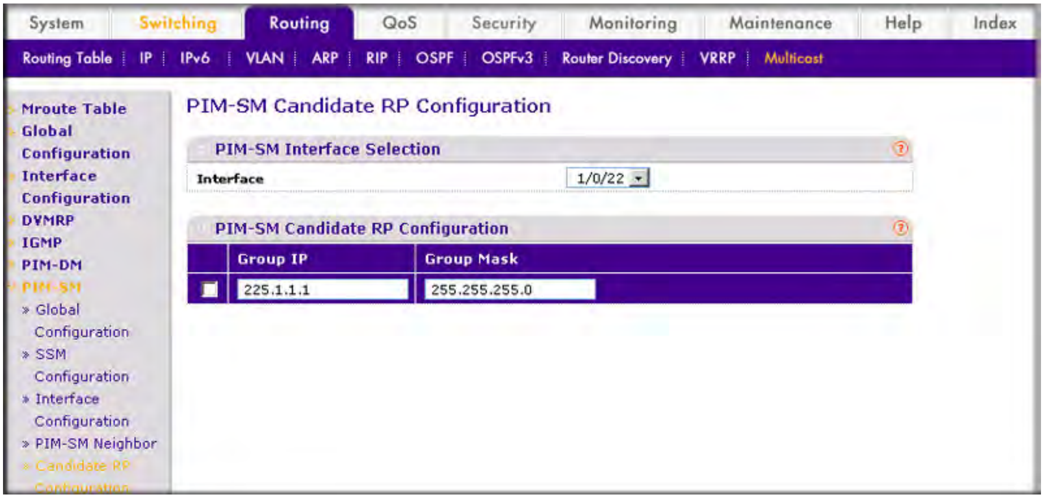
b. Under PIM-SM Interface Configuration, scroll down to interface 1/0/21 and select the checkbox for 1/0/21. Then select the interface 1/0/22.

c. In the PIM-SM Interface Configuration, select **Enable** in the Admin Mode field.

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

9. Candidate RP Configuration.

a. From the main menu, select Routing > Multicast >PIM-SM->Candidate RP Configuration. A screen similar to the following displays.



PIM-SM Candidate RP Configuration

PIM-SM Interface Selection

Interface 1/0/22

PIM-SM Candidate RP Configuration

	Group IP	Group Mask
□	225.1.1.1	255.255.255.0

Figure 28-69

b. Select **1/0/22** in the Interface field.

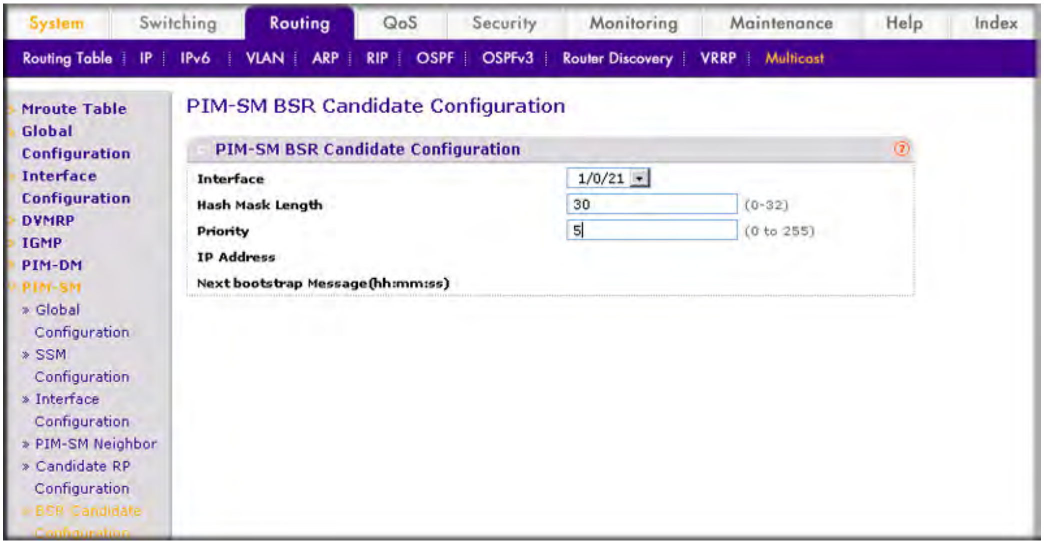
c. In the Group IP, enter **225.1.1.1**.

d. In the Group Mask, enter **255.255.255.0**.

e. Click **Add**.

10. BSR Candidate Configuration.

a. From the main menu, select Routing > Multicast >PIM-SM->BSR Candidate Configuration. A screen similar to the following displays.



PIM-SM BSR Candidate Configuration

PIM-SM BSR Candidate Configuration

Interface	1/0/21	
Hash Mask Length	30	(0-32)
Priority	5	(0 to 255)
IP Address		
Next bootstrap Message(hh:mm:ss)		

Figure 28-70

b. Select the **1/0/21** in the Interface field.

c. In the Hash Mask Length field, enter **30**.

d. In the Priority field, enter **5**.

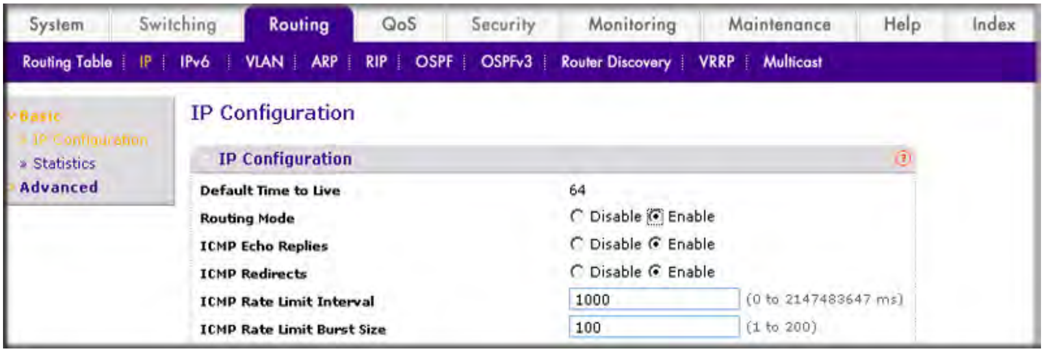
e. Click **Apply**.

On Switch D:

To use the Web interface to config PIM-SM, proceed as follows:

1. Enable IP routing on the switch.

a. From the main menu, select Routing >IP >Basic >IP configuration. A screen similar to the following displays.



IP Configuration

IP Configuration

Default Time to Live	64
Routing Mode	○ Disable ● Enable
ICMP Echo Replies	○ Disable ● Enable
ICMP Redirects	○ Disable ● Enable
ICMP Rate Limit Interval	1000 (0 to 2147483647 ms)
ICMP Rate Limit Burst Size	100 (1 to 200)

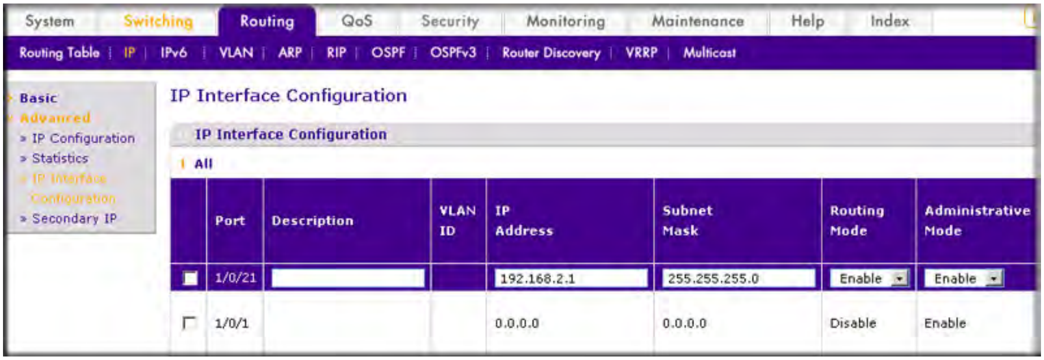
Figure 28-71

b. Next to the Routing Mode, select the **Enable** radio button.

c. Click **Apply**.

2. Configure 1/0/21 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
IP Configuration
Statistics
IP Interface Configuration
Secondary IP

IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☑	1/0/21			192.168.2.1	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-72

b. Under IP Interface Configuration, scroll down to interface 1/0/21 and select the checkbox for 1/0/21. 1/0/21 now appears in the Interface field at the top.

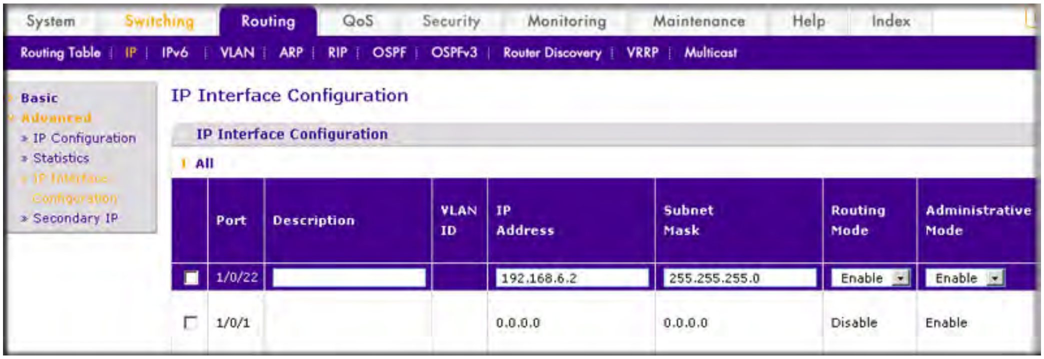
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.2.1**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

3. Configure 1/0/22 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
IP Configuration
Statistics
IP Interface Configuration
Secondary IP

IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☐	1/0/22			192.168.6.2	255.255.255.0	Enable	Enable
☐	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-73

b. Under IP Interface Configuration, scroll down to interface 1/0/22and select the checkbox for 1/0/22. 1/0/22 now appears in the Interface field at the top.

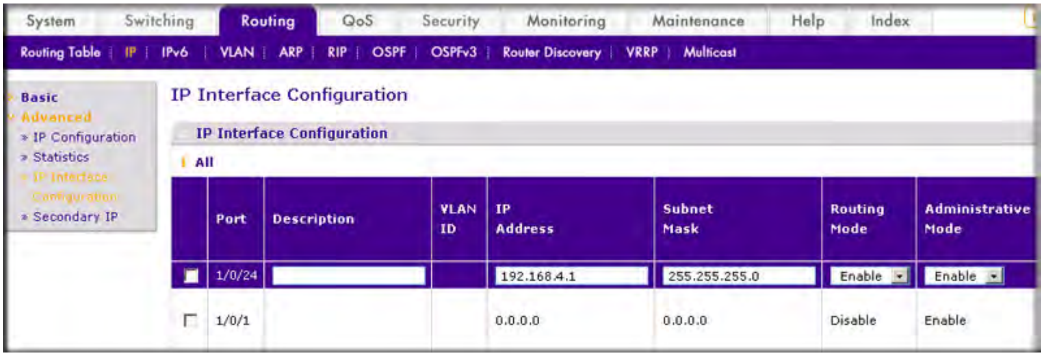
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.6.2**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

4. Configure 1/0/24 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
IP Configuration
Statistics
IP Interface Configuration
Secondary IP

IP Interface Configuration

IP Interface Configuration

All

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☐	1/0/24			192.168.4.1	255.255.255.0	Enable	Enable
☐	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 28-74

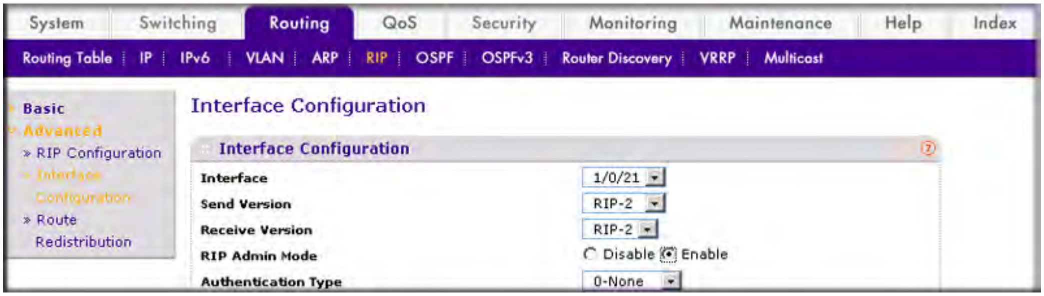
b. Under IP Interface Configuration, scroll down to interface 1/0/24 and select the checkbox for 1/0/24. 1/0/24 now appears in the Interface field at the top.

c. Enter the following information in the IP Interface Configuration.
   - In the IP address, enter **192.168.4.1**.
   - In the Subnet Mask, enter **255.255.255.0**.
   - Select **Enable** in the Routing Mode field.

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

5. Enable rip on the interface 1/0/21.

a. From the main menu, select Routing >RIP >Advanced > Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/21
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-75

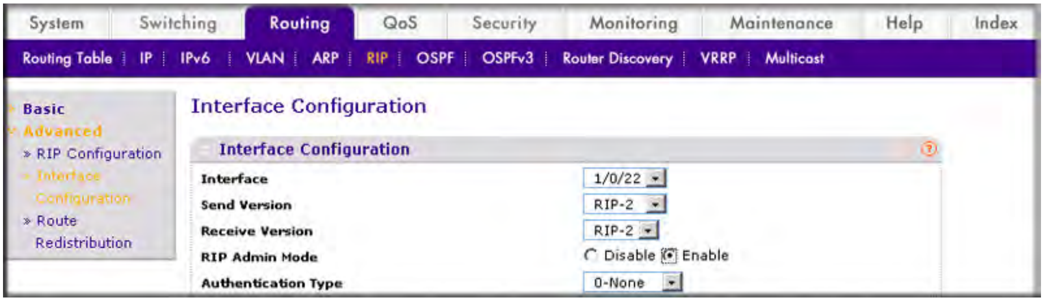
b. Select **1/0/21** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

6. Enable rip on the interface 1/0/22.

a. From the main menu, select Routing > RIP >Advanced > Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/22
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-76

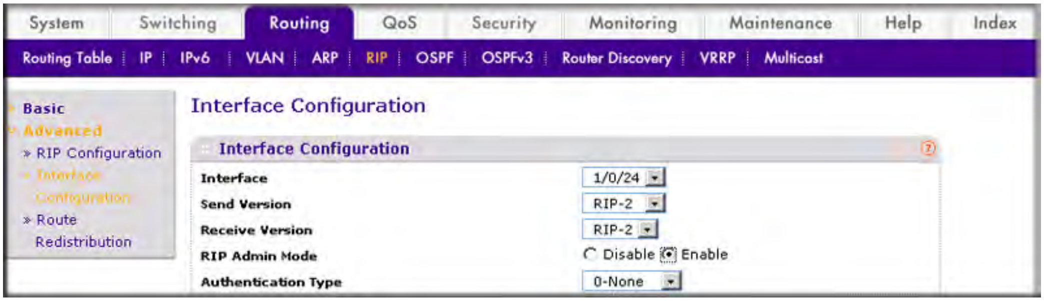
b. Select **1/0/22** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

7. Enable rip on the interface 1/0/24.

a. From the main menu, select Routing > RIP >Advanced > Interface Configuration. A screen similar to the following displays.



Interface Configuration

Interface Configuration

Interface	1/0/24
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	○ Disable ● Enable
Authentication Type	0-None

Figure 28-77

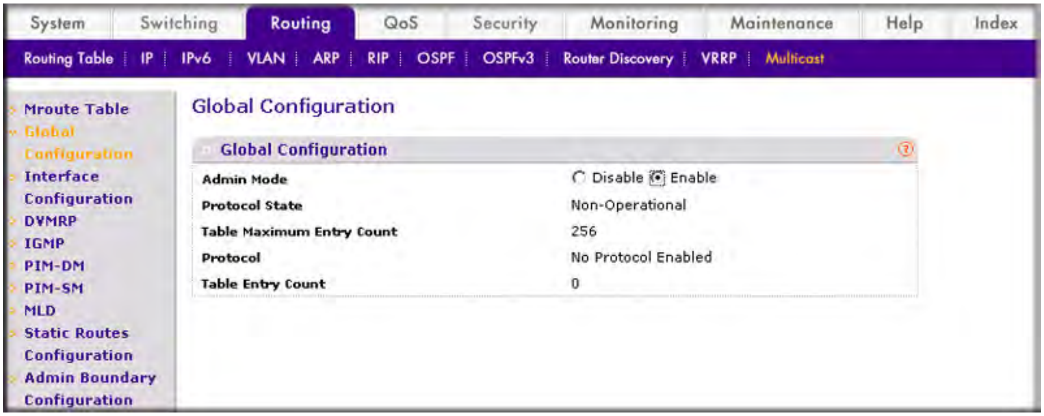
b. Select **1/0/24** in the Interface field.

c. Next to the RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

8. Enable multicast globally.

a. From the main menu, select Routing > Multicast >Global Configuration. A screen similar to the following displays.



Global Configuration

Global Configuration

Admin Mode	○ Disable ● Enable
Protocol State	Non-Operational
Table Maximum Entry Count	256
Protocol	No Protocol Enabled
Table Entry Count	0

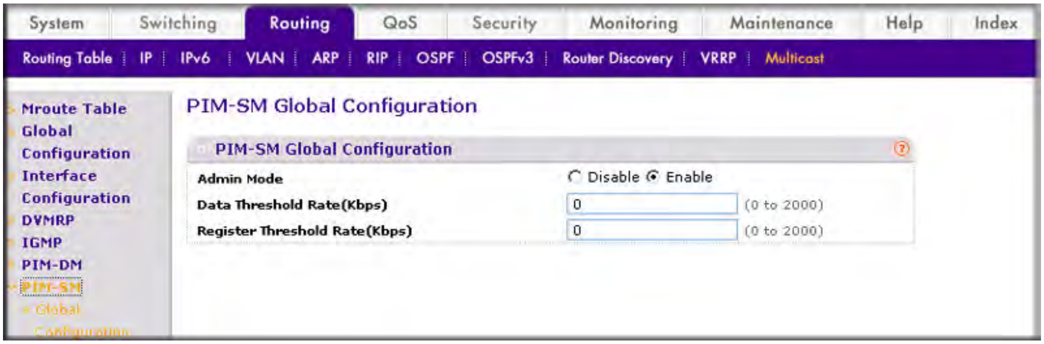
Figure 28-78

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

9. Enable PIM-SM globally.

a. From the main menu, select Routing > Multicast >PIM-SM->Global Configuration. A screen similar to the following displays.



PIM-SM Global Configuration

PIM-SM Global Configuration

Admin Mode	○ Disable ● Enable	
Data Threshold Rate(Kbps)	0	(0 to 2000)
Register Threshold Rate(Kbps)	0	(0 to 2000)

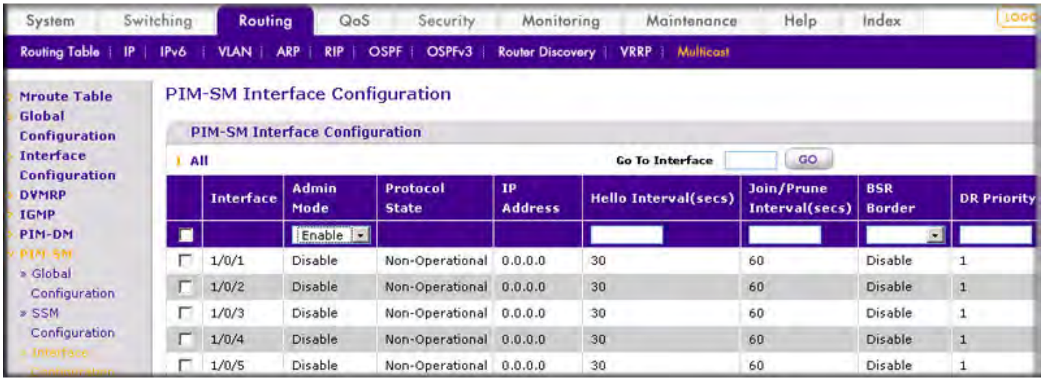
Figure 28-79

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

10. Enable PIM-SM on the interface 1/0/21,1/0/22 and 1/0/24.

a. From the main menu, select Routing > Multicast >PIM-SM->Interface Configuration. A screen similar to the following displays.



PIM-SM Interface Configuration

PIM-SM Interface Configuration

	Interface	Admin Mode	Protocol State	IP Address	Hello Interval(secs)	Join/Prune Interval(secs)	BSR Border	DR Priority
☐		Enable						
☐	1/0/1	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
☐	1/0/2	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
☐	1/0/3	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
☐	1/0/4	Disable	Non-Operational	0.0.0.0	30	60	Disable	1
☐	1/0/5	Disable	Non-Operational	0.0.0.0	30	60	Disable	1

Figure 28-80

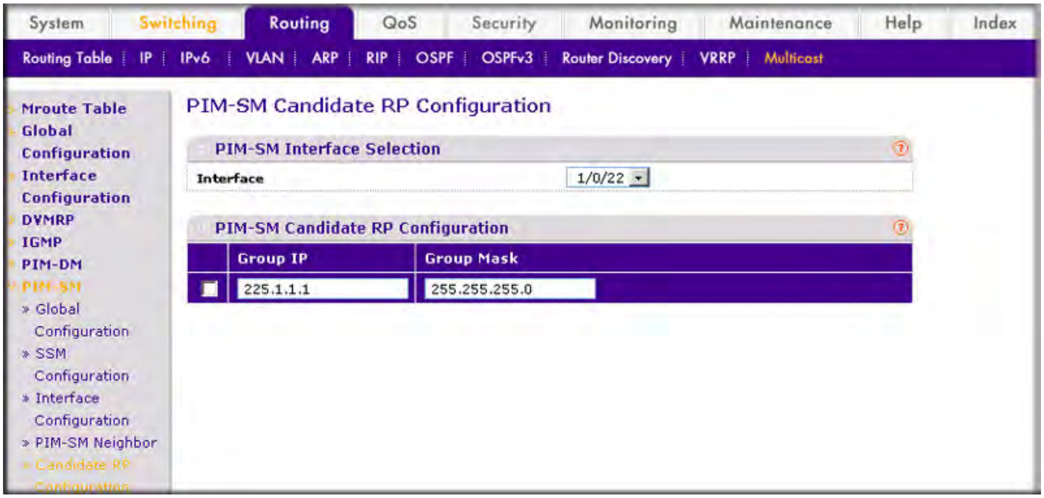
b. Under PIM-SM Interface Configuration, scroll down to interface 1/0/21 and select the checkbox for 1/0/21. Then select the 1/0/22 and 1/0/24.

c. In the PIM-SM Interface Configuration, select **Enable** in the Admin Mode field.

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

11. Candidate RP Configuration.

a. From the main menu, select Routing > Multicast >PIM-SM->Candidate RP Configuration. A screen similar to the following displays.



PIM-SM Candidate RP Configuration

PIM-SM Interface Selection

Interface 1/0/22

PIM-SM Candidate RP Configuration

	Group IP	Group Mask
□	225.1.1.1	255.255.255.0

Figure 28-81

b. Select **1/0/22** in the Interface field.

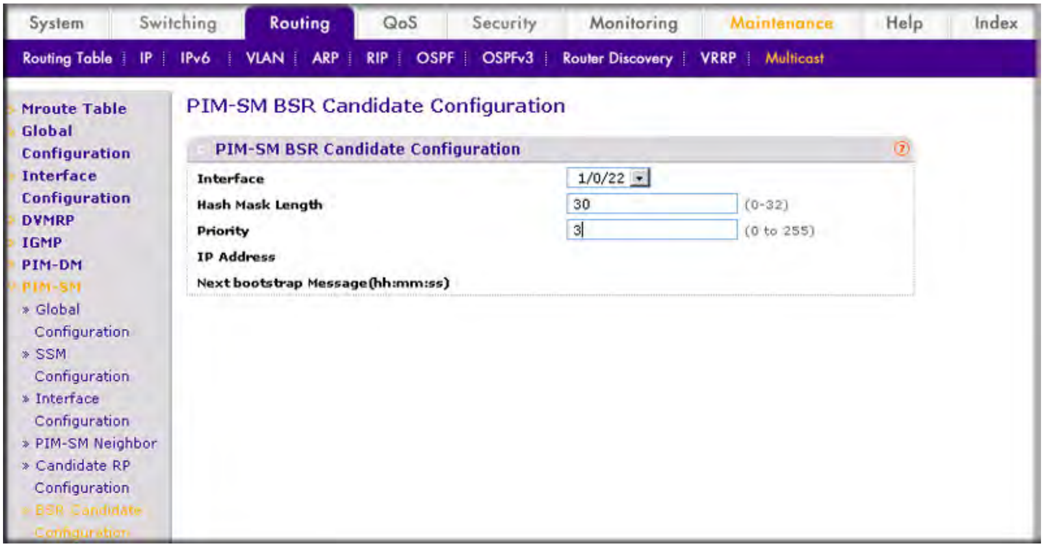
c. In the Group IP, enter **225.1.1.1**.

d. In the Group Mask, enter **255.255.255.0**.

e. Click **Add**.

12. BSR Cansdidate Configuration.

a. From the main menu, select Routing > Multicast >PIM-SM->BSR Candidate Configuration. A screen similar to the following displays.



PIM-SM BSR Candidate Configuration

PIM-SM BSR Candidate Configuration

Interface	1/0/22	
Hash Mask Length	30	(0-32)
Priority	3	(0 to 255)
IP Address		
Next bootstrap Message(hh:mm:ss)		

Figure 28-82

b. Select **1/0/22** in the Interface field.

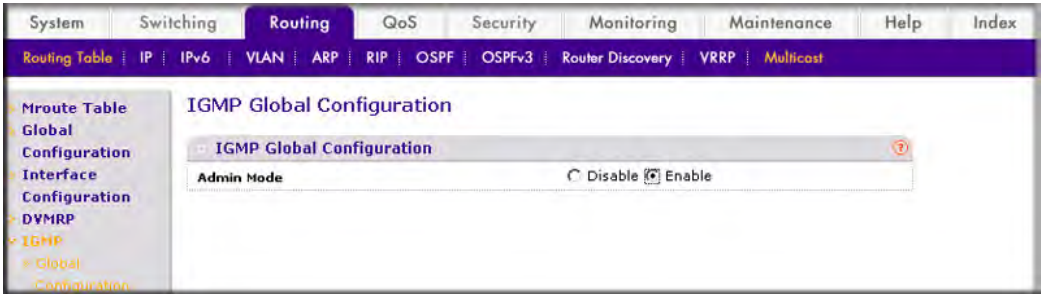
c. In the Hash Mask Length field, enter **30**.

d. In the Priority field, enter **3**.

e. Click **Apply**.

13. Enable IGMP globally.

a. From the main menu, select Routing > Multicast >IGMP->Global Configuration. A screen similar to the following displays.



IGMP Global Configuration

IGMP Global Configuration

Admin Mode ○ Disable ● Enable

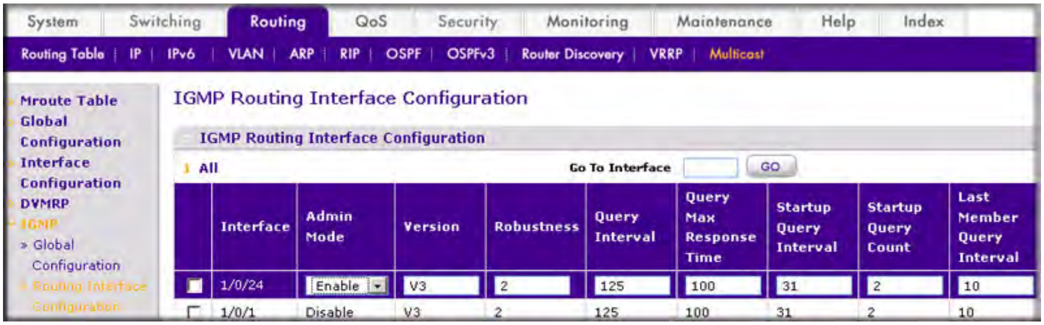
Figure 28-83

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

14. Enable IGMP on the interface 1/0/24.

a. From the main menu, select Routing > Multicast >IGMP->Interface Configuration. A screen similar to the following displays.



IGMP Routing Interface Configuration

IGMP Routing Interface Configuration

	Interface	Admin Mode	Version	Robustness	Query Interval	Query Max Response Time	Startup Query Interval	Startup Query Count	Last Member Query Interval
□	1/0/24	Enable	V3	2	125	100	31	2	10
□	1/0/1	Disable	V3	2	125	100	31	2	10

Figure 28-84

b. Under IGMP Routing Interface Configuration, scroll down to interface 1/0/24and select the checkbox for 1/0/24.

c. In the IGMP Routing Interface Configuration, select **Enable** in the Admin Mode field.

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

Chapter 29 DHCP L2 Relay

DHCP Relay Agents eliminate the necessity of having 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 address and other parameter assignment policies. These DHCP Relay Agents are typically an IP routing aware device and are referred 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. These Layer 2 devices are typically operating only as bridges for the network and may not have an IPv4 address on the network in question. 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 chapter provides information about where a Layer 2 Relay Agent fits in and how it is used.

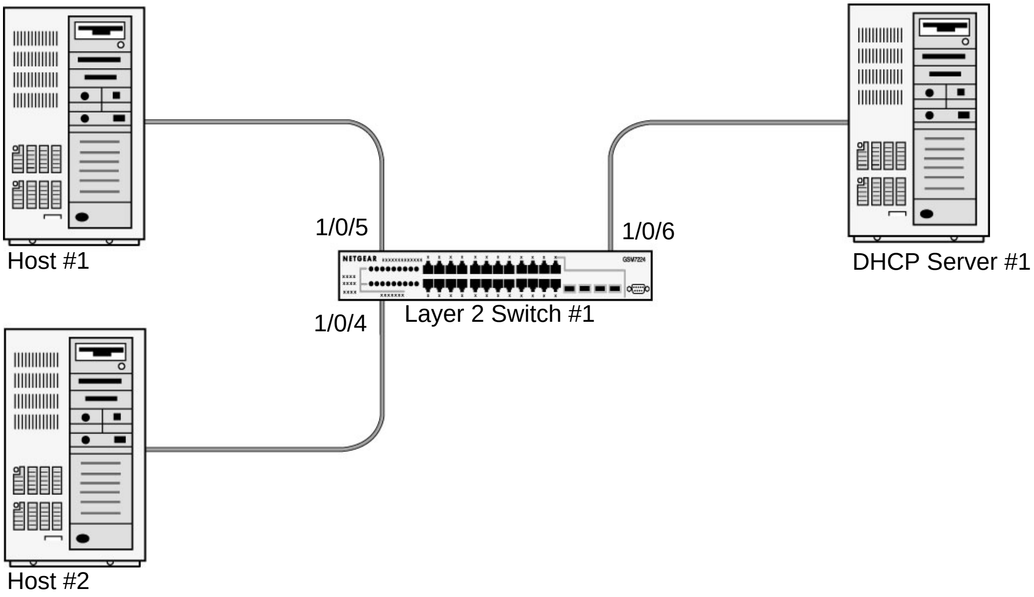


Figure 29-1

CLI: DHCP L2 Relay

```
(Netgear Switch)#vlan database
(Netgear Switch)(Vlan)#vlan 200
(Netgear Switch)(Vlan)#exit
```

Enable DHCP L2relay on the switch.

```
(Netgear Switch) (Config)#dhcp l2relay
(Netgear Switch) (Config)#dhcp l2relay vlan 200
```

Enable Option 82 Circuit ID field.

```
(Netgear Switch) (Config)#dhcp l2relay circuit-id vlan 200
```

Enable Option 82 Remote ID field.

```
(Netgear Switch) (Config)#dhcp l2relay remote-id rem_id vlan 200
```

Enable DHCP L2relay on the 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
```

Enable DHCP L2relay on the 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
```

Enable DHCP L2relay on the port 1/0/6.

```
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)# dhcp l2relay
```

Trust packets with option 82 received on port 1/0/6.

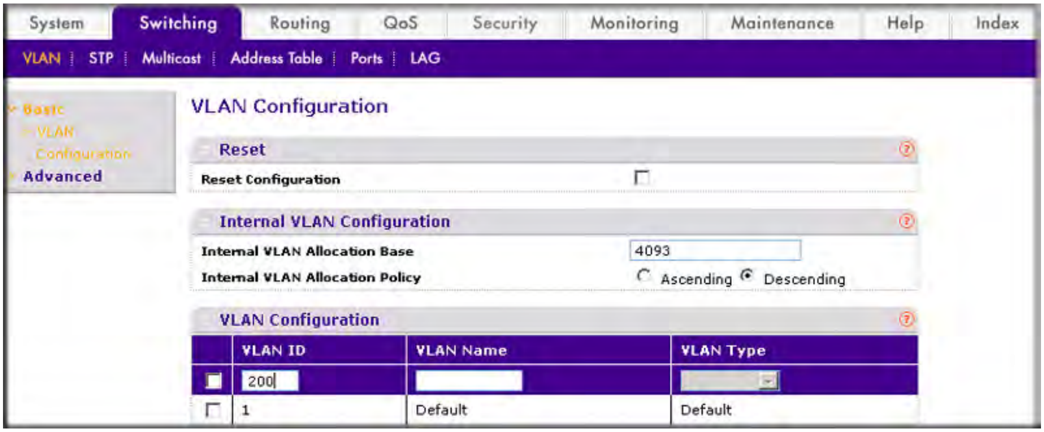
```
(Netgear Switch) (Interface 1/0/6)# dhcp l2relay trust
(Netgear Switch) (Interface 1/0/6)# vlan pvid 200
(Netgear Switch) (Interface 1/0/6)# vlan participation include 200
(Netgear Switch) (Interface 1/0/6)# exit
```

Web Interface: DHCP L2 Relay

To use the Web interface to create a guest VLAN, proceed as follows:

1. Create VLAN 200.

   a. From the main menu, 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

Figure 29-2

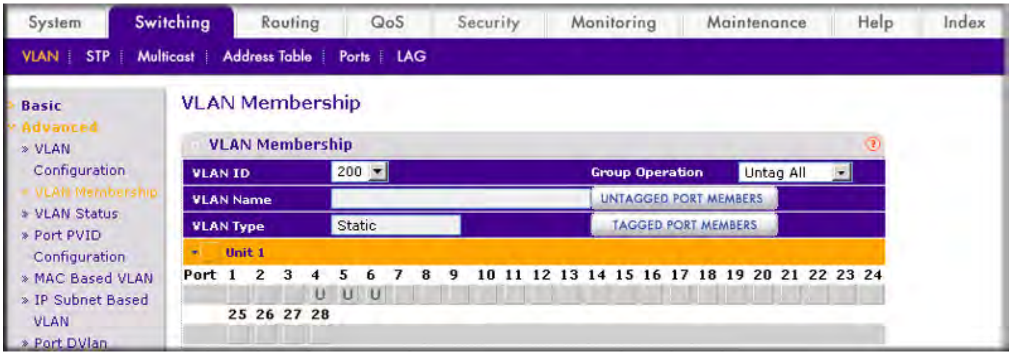
   b. In the VLAN ID field, enter **200**.

   c. Select **Static** in the VLAN Type field.

   d. Click **Add**.

2. Add ports to the VLAN 200.

   a. From the main menu, 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		UNTAGGED PORT MEMBERS	
VLAN Type	Static	TAGGED PORT MEMBERS	

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																				

Figure 29-3

b. Select **200** in the VLAN ID field.

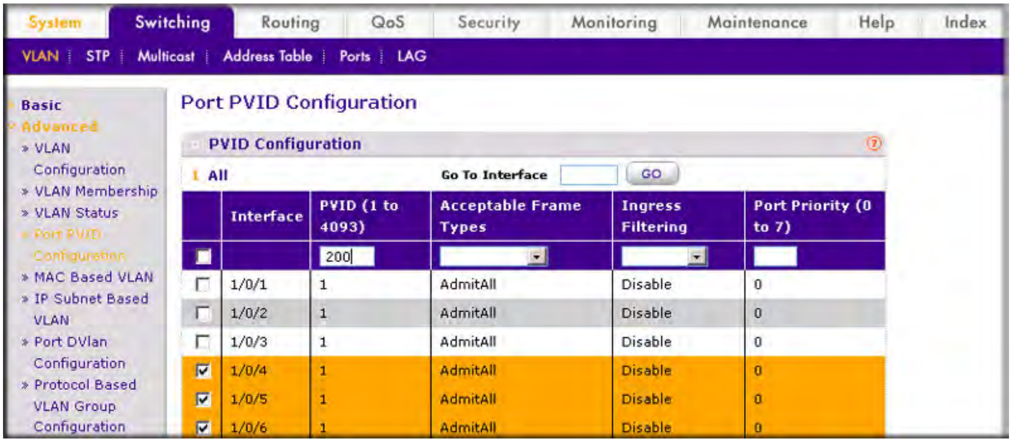
c. Click the Unit 1. The Ports display.

d. Click the gray box under port 4, port 5 and port 6 until U displays. The U specifies that the egress packet is untagged for the port.

e. Click **Apply**.

3. Specify that PVID on port 1/0/4, 1/0/5 and 1/0/6.

a. From the main menu, select Switching > VLAN> Advanced > Port PVID Configuration. A screen similar to the following displays.



Port PVID Configuration

PVID Configuration

1 All   Go To Interface   GO

	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

Figure 29-4

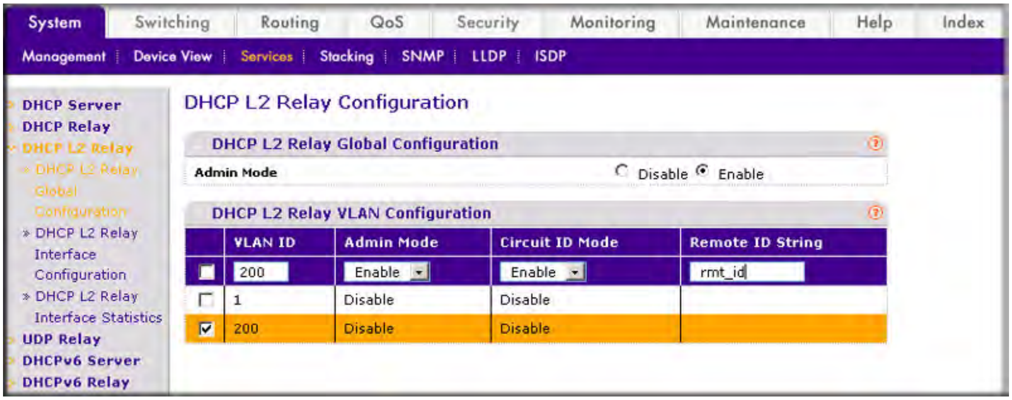
b. Under PVID Configuration, scroll down to interface 1/0/4 and select the checkbox for **1/0/4**. Next select the checkbox for 1/0/5 and 1/0/6.

c. In the PVID Configuration, enter **200** in the PVID (1 to 4093) field.

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

4. Enable DHCP L2 Relay on VLAN 200.

a. From the main menu, select System > Services> DHCP L2 Relay > DHCP L2 Relay Configuration. A screen similar to the following displays.



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	

Figure 29-5

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

c. Under DHCP L2 Relay VLAN Configuration, scroll down to VLAN ID 200 and select the checkbox for VLAN 200.

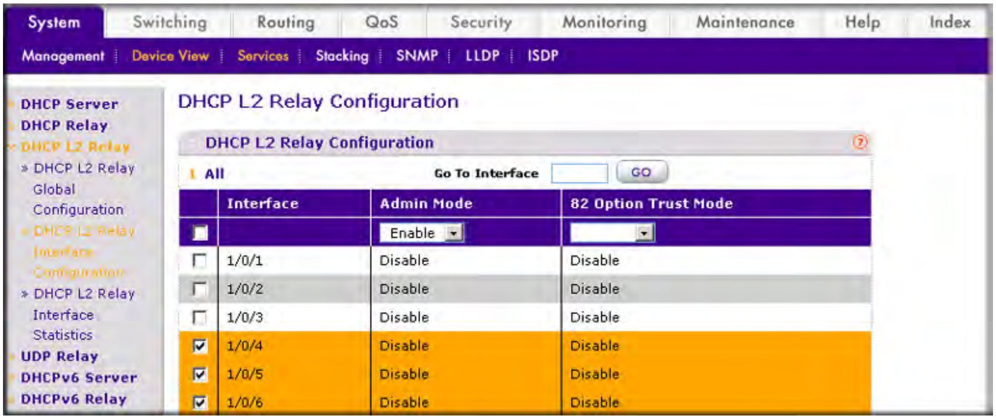
d. Enter the following information in the DHCP L2 Relay VLAN Configuration.

- Select **Enable** in the Admin Mode field.
- Select **Enable** in the Circuit ID Mode field.
- In the Remote ID String field, enter **rmt_id**.

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

5. Enable DHCP L2 Relay on interface 1/0/4,1/0/5 and 1/0/6.

a. From the main menu, select System > Services> DHCP L2 Relay > DHCP L2 Relay Interface Configuration. A screen similar to the following displays.



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

Figure 29-6

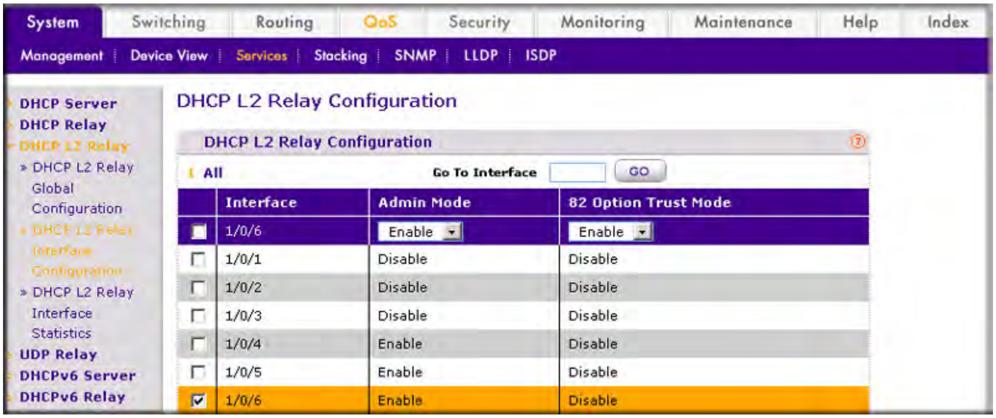
b. Under DHCP L2 Relay Configuration, scroll down to interface 1/0/4 and select the **1/0/4** checkbox. Next select the checkboxes for **1/0/5** and **1/0/6**.

c. Select **Enable** in the Admin Mode field.

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

6. Enable DHCP L2 Relay Trust on interface 1/0/6.

a. From the main menu, select System > Services> DHCP L2 Relay > DHCP L2 Relay Interface Configuration. A screen similar to the following displays.



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

Figure 29-7

b. Under DHCP L2 Relay Configuration, scroll down to interface 1/0/6 and select the **1/0/6** checkbox.

c. Select **Enable** in the 82 Option Trust Mode field.

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

Chapter 30
MLD

In this chapter, the following examples are provided:

- “Configure MLD” on page 32-2
- “MLD Snooping” on page 32-5

Multicast Listener Discovery (MLD) protocol enables IPv6 routers to discover the presence of multicast listeners, the nodes who wish to receive the 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. The Multicast router sends General Queries periodically to request multicast address listeners information from systems on an attached network. These queries are used to build and refresh the multicast address listener state on attached networks. Multicast listeners respond to these queries by reporting their multicast addresses listener state and their desired set of sources with Current-State Multicast address Records in the MLD2 Membership Reports. The Multicast router also processes unsolicited Filter-Mode-Change records and Source-List-Change Records from systems that want to indicate interest in receiving or not receiving traffic from particular sources.

Configure MLD

In this case, PIM-DM is enabled on Switch A and B, and MLD is enabled on Switch B’s 1/0/24 to discover the multicast listeners.

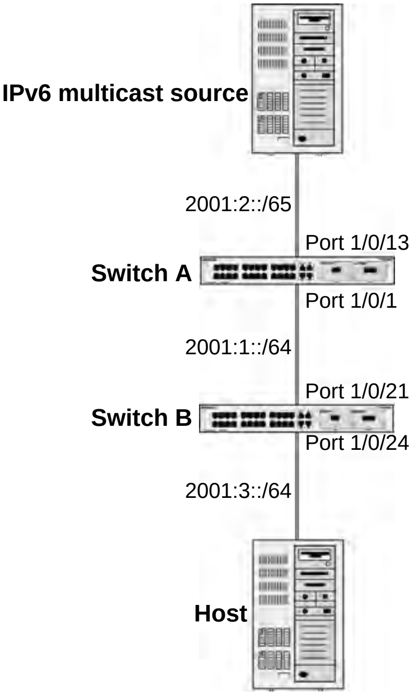


Figure 30-1

CLI: Configuring MLD

On Switch A

```
(Netgear Switch)#configure
(Netgear Switch) (Config)#ipv6 router ospf
(Netgear Switch) (Config-rtr)#router-id 1.1.1.1
(Netgear Switch) (Config)#exit
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) (Config)#ipv6 pimdm
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ipv6 address 2001:1::1/64
(Netgear Switch) (Interface 1/0/1)#ipv6 enable
(Netgear Switch) (Interface 1/0/1)#ipv6 pimdm
(Netgear Switch) (Interface 1/0/1)#ipv6 ospf
(Netgear Switch) (Interface 1/0/1)#exit
```

```
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ipv6 address 2001:2::1/64
(Netgear Switch) (Interface 1/0/13)#ipv6 enable
(Netgear Switch) (Interface 1/0/13)#ipv6 pimdm
(Netgear Switch) (Interface 1/0/13)#ipv6 ospf
(Netgear Switch) (Interface 1/0/13)#exit
```

On Switch B

Enable OSPFv3 to build unicast route table.

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

Enable ipv6 unicast routing on the switch.

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

Enable ipv6 MLD on the switch.

```
(Netgear Switch) (Config)#ipv6 mld router
```

Enable ipv6 PIM-DM on the switch.

```
(Netgear Switch) (Config)#ipv6 pimdm
```

Enable ip multicast forwarding on the switch.

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

Enable MLD on the 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ipv6 address 2001:1::2/64
(Netgear Switch) (Interface 1/0/21)#ipv6 enable
(Netgear Switch) (Interface 1/0/21)#ipv6 pimdm
(Netgear Switch) (Interface 1/0/21)#ipv6 ospf
(Netgear Switch) (Interface 1/0/21)#exit

(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#routing
(Netgear Switch) (Interface 1/0/24)#ipv6 address 2001:3::1/64
(Netgear Switch) (Interface 1/0/24)#ipv6 enable
(Netgear Switch) (Interface 1/0/24)#ipv6 mld router

(Netgear Switch) (Interface 1/0/24)#ipv6 pimdm
(Netgear Switch) (Interface 1/0/24)#exit

The MLD group information on switch B:
(B) #show ipv6 mld groups ff32::1

Interface...................................... 71/1/24
Group Address.................................. FF32::1
Last Reporter.................................. FE80::200:4FF:FEE8:5EFC
Up Time (hh:mm:ss)............................. 00:00:18
Expiry Time (hh:mm:ss)......................... ------
Filter Mode.................................... Include
Version1 Host Timer............................ ------
Group compat mode.............................. v2
Source Address    ExpiryTime
-----------------  -----------
  2001:2::2       00:04:02
```

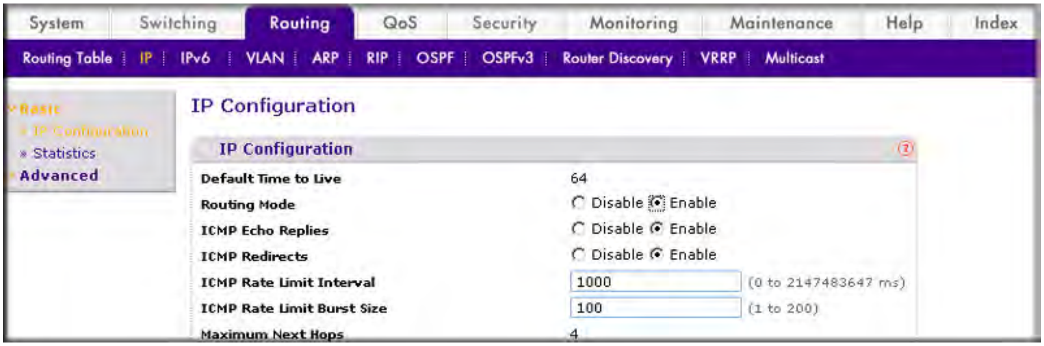
Web Interface: Configuring MLD

On Switch A:

To use the Web interface to config MLD, proceed as follows:

1. Enable IP routing on the switch.

a. From the main menu, select Routing >IP >Basic >IP configuration. A screen similar to the following displays.



IP Configuration

IP Configuration

Default Time to Live	64
Routing Mode	○ Disable ● Enable
ICMP Echo Replies	○ Disable ● Enable
ICMP Redirects	○ Disable ● Enable
ICMP Rate Limit Interval	1000 (0 to 2147483647 ms)
ICMP Rate Limit Burst Size	100 (1 to 200)
Maximum Next Hops	4

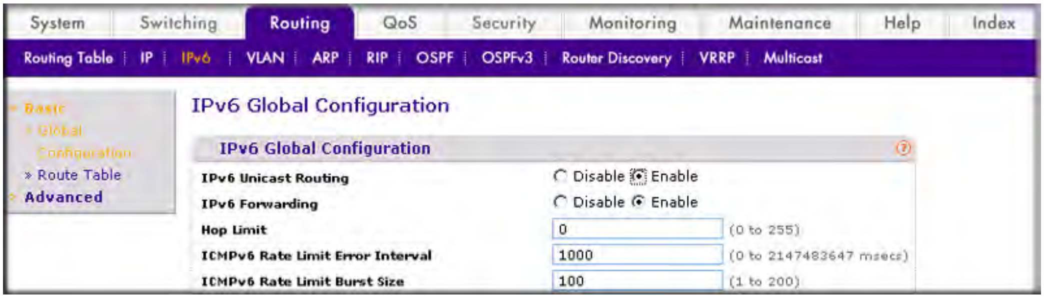
Figure 30-2

b. Next to the Routing Mode, select the **Enable** radio button.

c. Click **Apply**.

2. Enable IPv6 Unicast routing on the switch.

a. From the main menu, select Routing >IPv6 >Basic >Global configuration. A screen similar to the following displays.



IPv6 Global Configuration

IPv6 Global Configuration

IPv6 Unicast Routing	○ Disable ● Enable
IPv6 Forwarding	○ Disable ● Enable
Hop Limit	0 (0 to 255)
ICMPv6 Rate Limit Error Interval	1000 (0 to 2147483647 msecs)
ICMPv6 Rate Limit Burst Size	100 (1 to 200)

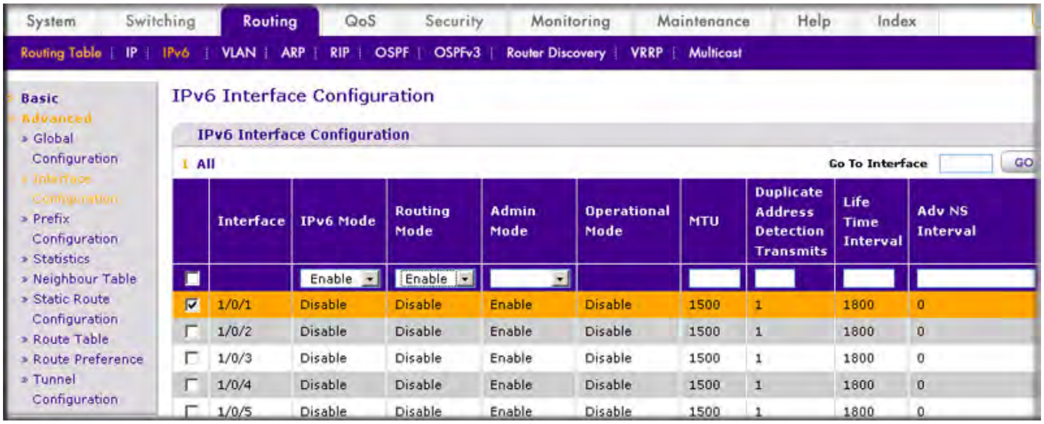
Figure 30-3

b. Next to the IPv6 Unicast Routing, select the **Enabl**e radio button.

c. Click **Apply**.

3. Configure 1/0/1 and 1/0/13 as a IPv6 routing port.

a. From the main menu, select Routing > IP v6>Advanced > Interface Configuration. A screen similar to the following displays.



IPv6 Interface Configuration

IPv6 Interface Configuration

	Interface	IPv6 Mode	Routing Mode	Admin Mode	Operational Mode	MTU	Duplicate Address Detection Transmits	Life Time Interval	Adv NS Interval
☐		Enable	Enable						
☑	1/0/1	Disable	Disable	Enable	Disable	1500	1	1800	0
☐	1/0/2	Disable	Disable	Enable	Disable	1500	1	1800	0
☐	1/0/3	Disable	Disable	Enable	Disable	1500	1	1800	0
☐	1/0/4	Disable	Disable	Enable	Disable	1500	1	1800	0
☐	1/0/5	Disable	Disable	Enable	Disable	1500	1	1800	0

Figure 30-4

b. Under IPv6 Interface Configuration, scroll down to interface 1/0/1 and select the checkbox for 1/0/1. then select the checkbox for 1/0/13.

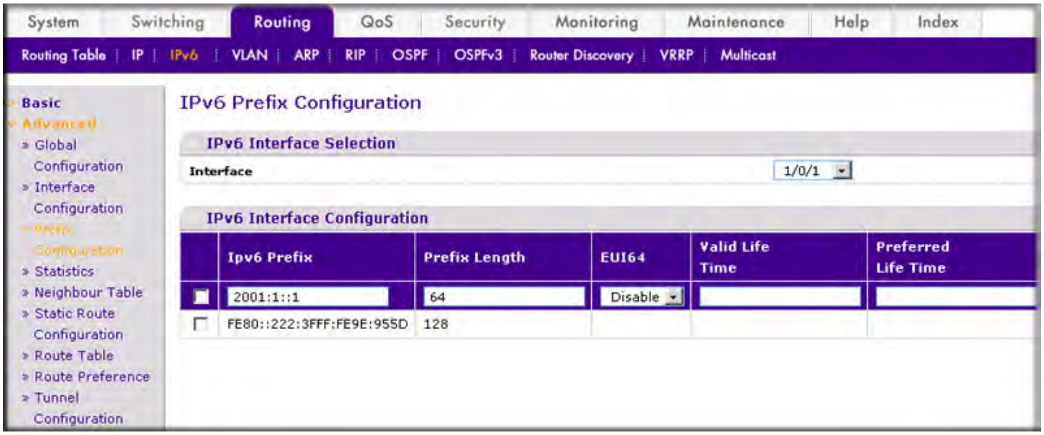
c. Enter the following information in the IPv6 Interface Configuration.

- Select **Enable** in the IPv6 Mode field.
- Select **Enable** in the Routing Mode field.
- Select **Enable** in the Admin Modefield.

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

4. Assign IPv6 address to 1/0/1.

a. From the main menu, select Routing > IP v6>Advanced > Prefix Configuration. A screen similar to the following displays.



IPv6 Prefix Configuration

IPv6 Interface Selection

Interface: 1/0/1

IPv6 Interface Configuration

	Ipv6 Prefix	Prefix Length	EUI64	Valid Life Time	Preferred Life Time
□	2001:1::1	64	Disable		
□	FE80::222:3FFF:FE9E:955D	128			

Figure 30-5

b. Under IPv6 Interface Selection, select **1/0/1** in the Interface field.

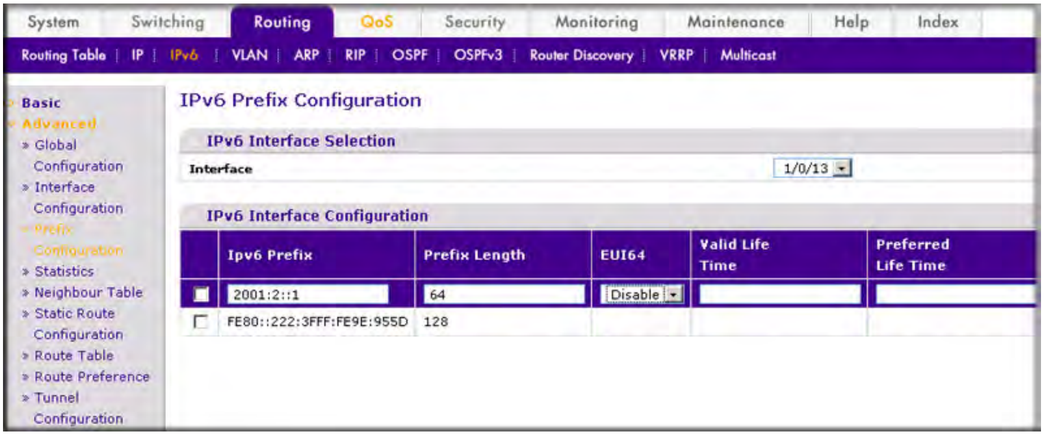
c. Enter the following information in the IP Interface Configuration.

- In the IPv6 Prefix, enter **2001:1::1**.
- In the Prefix Length, enter **64**.
- Select **Disable** in the EUI64 field.

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

5. Assign IPv6 address to 1/0/13.

a. From the main menu, select Routing > IP v6>Advanced > Prefix Configuration. A screen similar to the following displays.



IPv6 Prefix Configuration

IPv6 Interface Selection

Interface: 1/0/13

IPv6 Interface Configuration

	Ipv6 Prefix	Prefix Length	EUI64	Valid Life Time	Preferred Life Time
□	2001:2::1	64	Disable		
□	FE80::222:3FFF:FE9E:955D	128			

Figure 30-6

b. Under IPv6 Interface Selection, select the **1/0/13** in the Interface field.

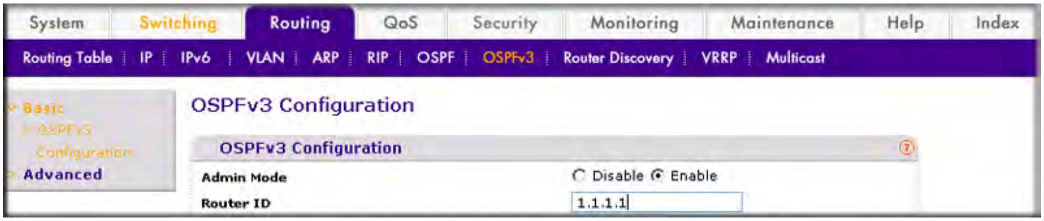
c. Enter the following information in the IP Interface Configuration.

- In the IPv6 Prefix, enter **2001:2::1**.
- In the Prefix Length, enter **64**.
- Select **Disable** in the EUI64 field.

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

6. Configure router ID of OSPFv3.

a. From the main menu, select Routing > OSPFv3 >Basic > OSPFv3 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
Basic
» OSPFv3 Configuration
Advanced

OSPFv3 Configuration

OSPFv3 Configuration

Admin Mode ○ Disable ● Enable

Router ID 1.1.1.1

Figure 30-7

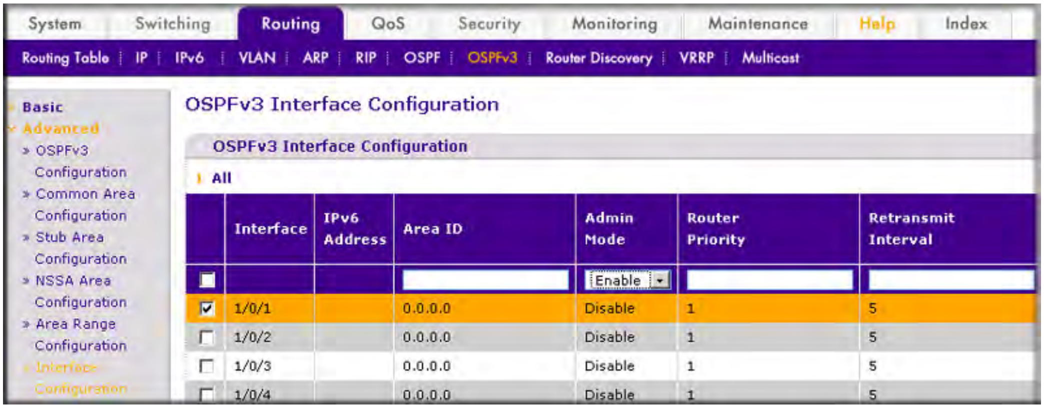
b. In the Router ID field, enter **1.1.1.1**.

c. Next to the Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

7. Enable OSPFv3 on the interface 1/0/1 and 1/0/13.

a. From the main menu, select Routing > OSPFv3 >Advanced > Interface Configuration. A screen similar to the following displays.



OSPFv3 Interface Configuration

OSPFv3 Interface Configuration

All

	Interface	IPv6 Address	Area ID	Admin Mode	Router Priority	Retransmit Interval
□				Enable		
☑	1/0/1		0.0.0.0	Disable	1	5
□	1/0/2		0.0.0.0	Disable	1	5
□	1/0/3		0.0.0.0	Disable	1	5
□	1/0/4		0.0.0.0	Disable	1	5

Figure 30-8

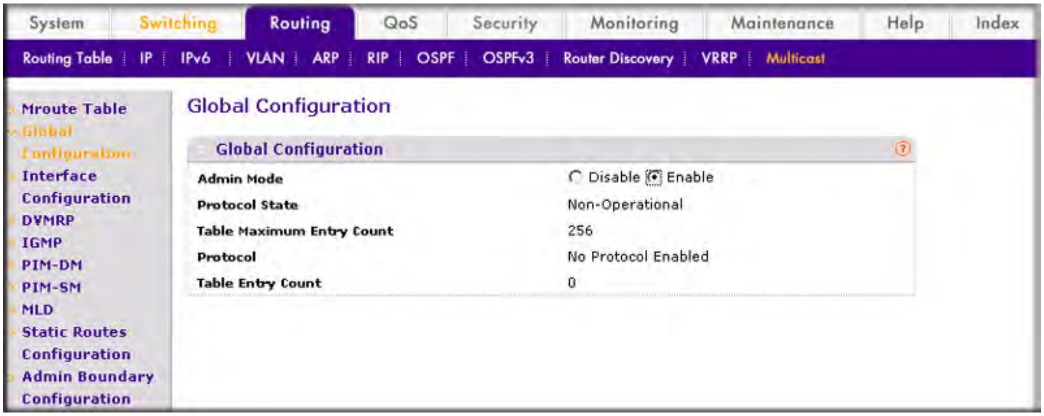
b. Under OSPFv3 Interface Configuration, scroll down to interface 1/0/1 and select the checkbox for **1/0/1**. Then select the checkbox for **1/0/13**.

c. In the OSPFv3 Interface Configuration, select **Enable** in the Admin Mode field.

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

8. Enable multicast globally.

a. From the main menu, select Routing > Multicast >Global Configuration. A screen similar to the following displays.



Global Configuration

Global Configuration

Admin Mode	○ Disable ● Enable
Protocol State	Non-Operational
Table Maximum Entry Count	256
Protocol	No Protocol Enabled
Table Entry Count	0

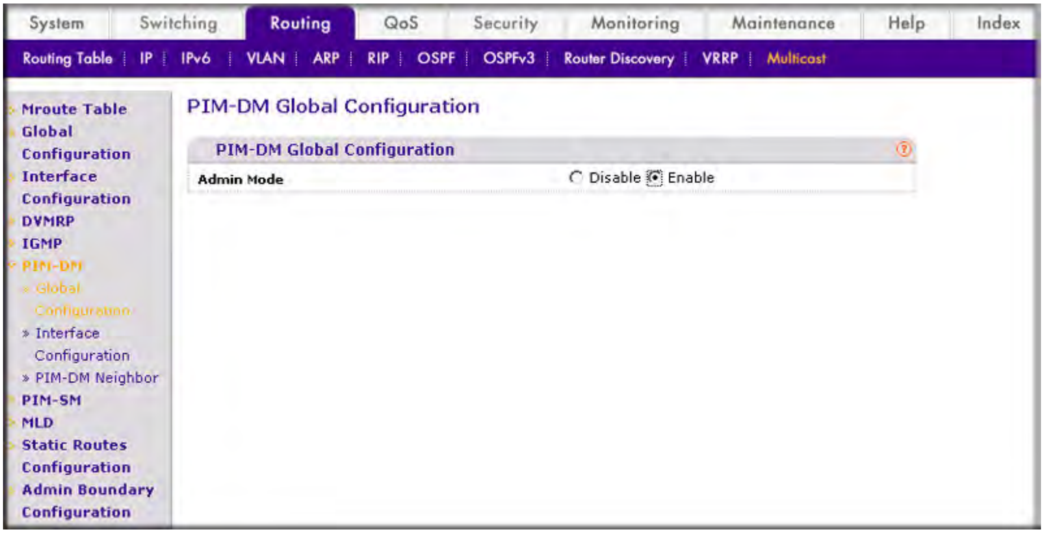
Figure 30-9

  b. Next to the Admin Mode, select the **Enable** radio button.

  c. Click **Apply**.

9. Enable PIM-DM globally.

  a. From the main menu, select Routing > Multicast >PIM-DM->Global Configuration. A screen similar to the following displays.



PIM-DM Global Configuration

PIM-DM Global Configuration

Admin Mode ○ Disable ● Enable

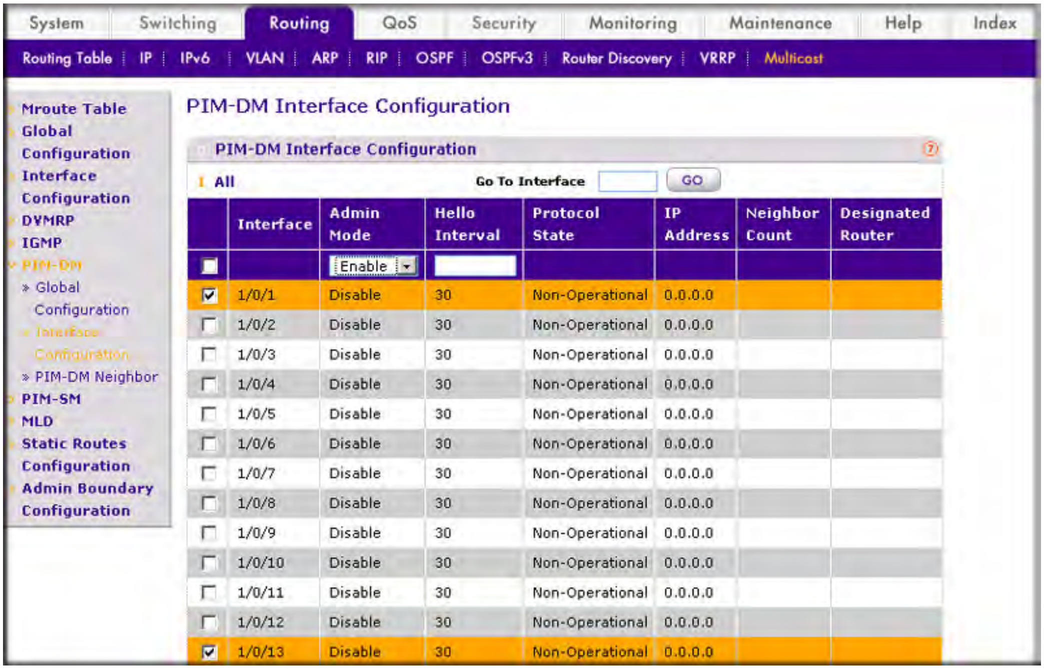
Figure 30-10

  b. Next to the Admin Mode, select the **Enable** radio button.

  c. Click **Apply**.

10. Enable PIM-DM on the interface 1/0/1and 1/0/13.

a. From the main menu, select Routing > Multicast >PIM-DM->Interface Configuration. A screen similar to the following displays.



PIM-DM Interface Configuration

PIM-DM Interface Configuration

	Interface	Admin Mode	Hello Interval	Protocol State	IP Address	Neighbor Count	Designated Router
☐		Enable					
☑	1/0/1	Disable	30	Non-Operational	0.0.0.0		
☐	1/0/2	Disable	30	Non-Operational	0.0.0.0		
☐	1/0/3	Disable	30	Non-Operational	0.0.0.0		
☐	1/0/4	Disable	30	Non-Operational	0.0.0.0		
☐	1/0/5	Disable	30	Non-Operational	0.0.0.0		
☐	1/0/6	Disable	30	Non-Operational	0.0.0.0		
☐	1/0/7	Disable	30	Non-Operational	0.0.0.0		
☐	1/0/8	Disable	30	Non-Operational	0.0.0.0		
☐	1/0/9	Disable	30	Non-Operational	0.0.0.0		
☐	1/0/10	Disable	30	Non-Operational	0.0.0.0		
☐	1/0/11	Disable	30	Non-Operational	0.0.0.0		
☐	1/0/12	Disable	30	Non-Operational	0.0.0.0		
☑	1/0/13	Disable	30	Non-Operational	0.0.0.0		

Figure 30-11

b. Under PIM-DM Interface Configuration, scroll down to interface 1/0/1 and select the checkbox for **1/0/1**. Then select the checkbox for 1/0/13.

c. In the PIM-DM Interface Configuration, select **Enable** in the Admin Mode field.

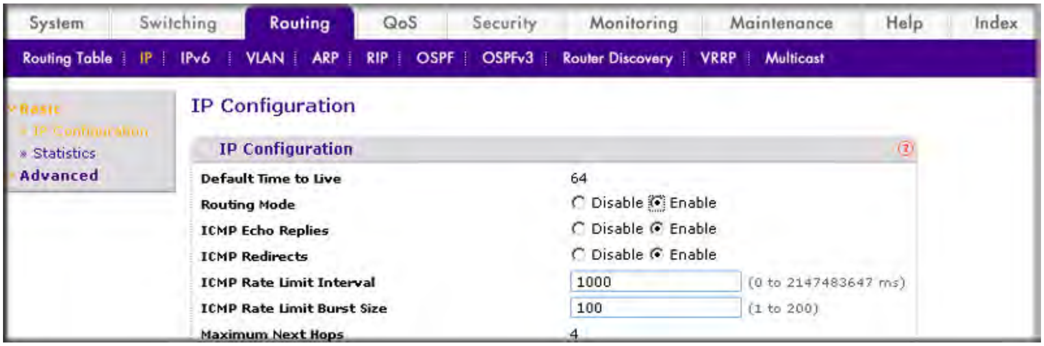
d. Click **Apply** to save the settings.

On Switch B:

To use the Web interface to config MLD, proceed as follows:

1. Enable IP routing on the switch.

a. From the main menu, select Routing >IP >Basic >IP configuration. A screen similar to the following displays.



IP Configuration

IP Configuration

Default Time to Live 64

Routing Mode ○ Disable ● Enable

ICMP Echo Replies ○ Disable ● Enable

ICMP Redirects ○ Disable ● Enable

ICMP Rate Limit Interval 1000 (0 to 2147483647 ms)

ICMP Rate Limit Burst Size 100 (1 to 200)

Maximum Next Hops 4

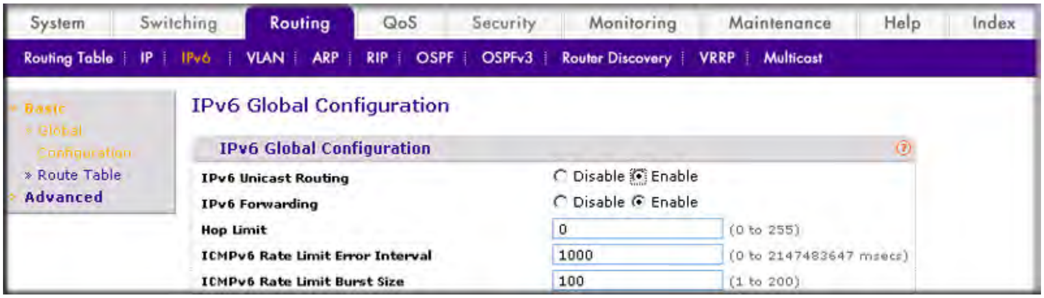
Figure 30-12

b. Next to the Routing Mode, select the **Enable** radio button.

c. Click **Apply**.

2. Enable IPv6 Unicast routing on the switch.

a. From the main menu, select Routing >IPv6 >Basic >Global configuration. A screen similar to the following displays.



IPv6 Global Configuration

IPv6 Global Configuration

IPv6 Unicast Routing ○ Disable ● Enable

IPv6 Forwarding ○ Disable ● Enable

Hop Limit 0 (0 to 255)

ICMPv6 Rate Limit Error Interval 1000 (0 to 2147483647 msecs)

ICMPv6 Rate Limit Burst Size 100 (1 to 200)

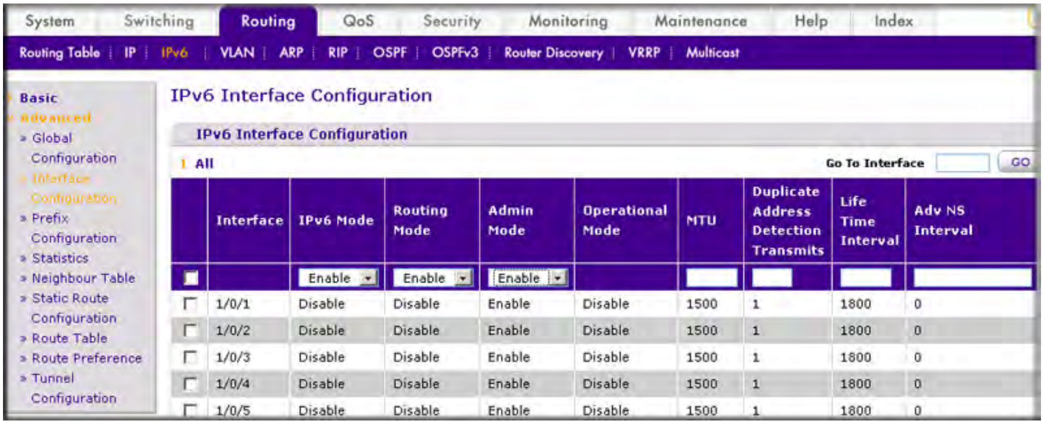
Figure 30-13

b. Next to the IPv6 Unicast Routing, select the **Enable** radio button.

c. Click **Apply**.

3. Configure 1/0/21 and 1/0/24 as a IPv6 routing port.

a. From the main menu, select Routing > IP v6>Advanced > Interface Configuration. A screen similar to the following displays.



IPv6 Interface Configuration

IPv6 Interface Configuration

	Interface	IPv6 Mode	Routing Mode	Admin Mode	Operational Mode	MTU	Duplicate Address Detection Transmits	Life Time Interval	Adv NS Interval
☐		Enable	Enable	Enable					
☐	1/0/1	Disable	Disable	Enable	Disable	1500	1	1800	0
☐	1/0/2	Disable	Disable	Enable	Disable	1500	1	1800	0
☐	1/0/3	Disable	Disable	Enable	Disable	1500	1	1800	0
☐	1/0/4	Disable	Disable	Enable	Disable	1500	1	1800	0
☐	1/0/5	Disable	Disable	Enable	Disable	1500	1	1800	0

Figure 30-14

b. Under IPv6 Interface Configuration, scroll down to interface 1/0/21 and select the checkbox for **1/0/21**. Then select the checkbox for **1/0/24**.

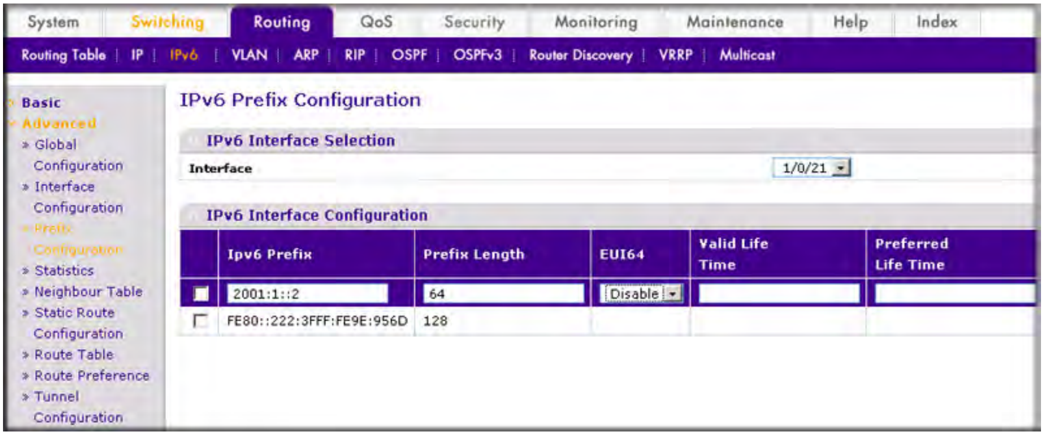
c. Enter the following information in the IPv6 Interface Configuration.

- Select **Enable** in the IPv6 Mode field.
- Select **Enable** in the Routing Mode field.
- Select **Enable** in the Admin Mode field.

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

4. Assign IPv6 address to 1/0/21.

a. From the main menu, select Routing > IP v6>Advanced > Prefix Configuration. A screen similar to the following displays.



IPv6 Prefix Configuration

IPv6 Interface Selection

Interface 1/0/21

IPv6 Interface Configuration

	Ipv6 Prefix	Prefix Length	EUI64	Valid Life Time	Preferred Life Time
□	2001:1::2	64	Disable		
□	FE80::222:3FFF:FE9E:956D	128			

Figure 30-15

b. Under IPv6 Interface Selection, select **1/0/21** in the Interface field.

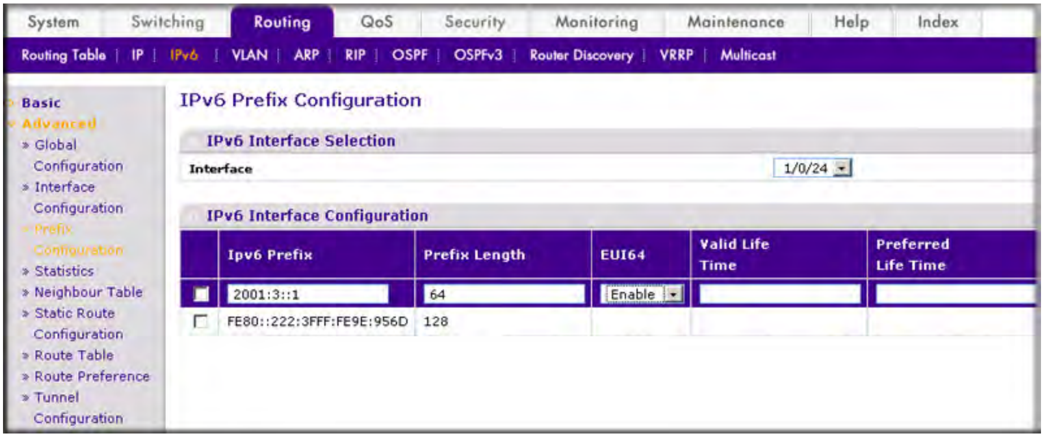
c. Enter the following information in the IP Interface Configuration.

- In the IPv6 Prefix, enter **2001:1::2**.
- In the Prefix Length, enter **64**.
- Select **Disable** in the EUI64 field.

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

5. Assign IPv6 address to 1/0/24.

a. From the main menu, select Routing > IP v6>Advanced > Prefix Configuration. A screen similar to the following displays.



IPv6 Prefix Configuration

IPv6 Interface Selection

Interface: 1/0/24

IPv6 Interface Configuration

	Ipv6 Prefix	Prefix Length	EUI64	Valid Life Time	Preferred Life Time
☐	2001:3::1	64	Enable		
☐	FE80::222:3FFF:FE9E:956D	128			

Figure 30-16

b. Under IPv6 Interface Selection, select **1/0/24** in the Interface field.

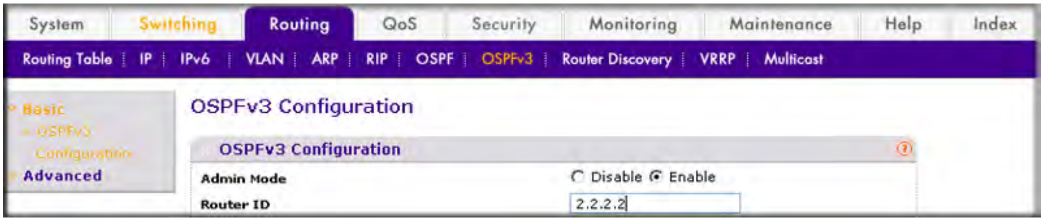
c. Enter the following information in the IP Interface Configuration.

- In the IPv6 Prefix, enter **2001:3::1**.
- In the Prefix Length, enter **64**.
- Select **Disable** in the EUI64 field.

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

6. Configure router ID of OSPFv3.

a. From the main menu, select Routing > OSPFv3 >Basic > OSPFv3 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
Basic
» OSPFv3 Configuration
Advanced

OSPFv3 Configuration

OSPFv3 Configuration

Admin Mode: ○ Disable ● Enable

Router ID: 2.2.2.2

Figure 30-17

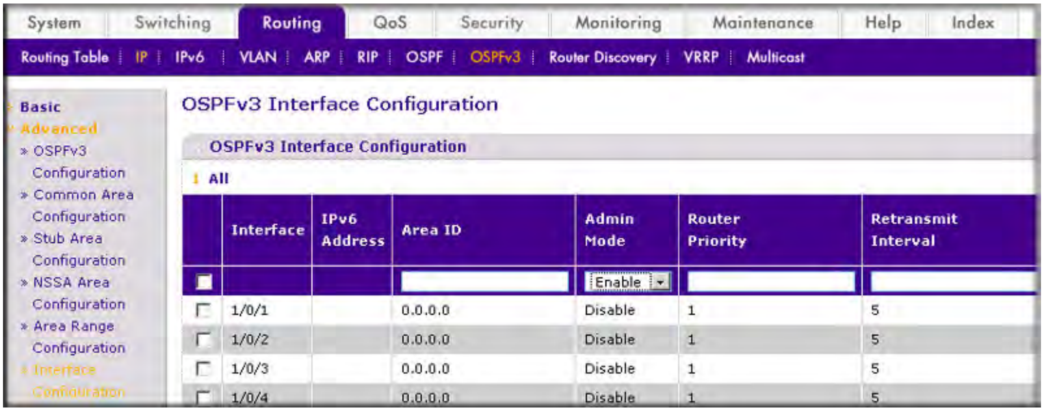
b. In the Router ID field, enter **2.2.2.2**.

c. Next to the Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

7. Enable OSPFv3 on the interface 1/0/21 and 1/0/24.

a. From the main menu, select Routing > OSPFv3 >Advanced > Interface Configuration. A screen similar to the following displays.



OSPFv3 Interface Configuration

OSPFv3 Interface Configuration

All

	Interface	IPv6 Address	Area ID	Admin Mode	Router Priority	Retransmit Interval
☐				Enable		
☐	1/0/1		0.0.0.0	Disable	1	5
☐	1/0/2		0.0.0.0	Disable	1	5
☐	1/0/3		0.0.0.0	Disable	1	5
☐	1/0/4		0.0.0.0	Disable	1	5

Figure 30-18

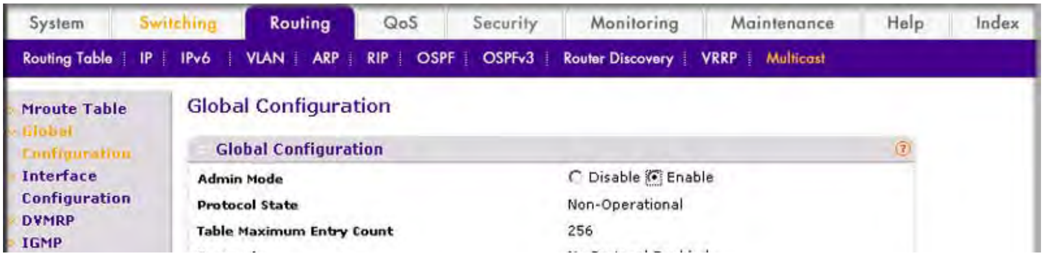
b. Under OSPFv3 Interface Configuration, scroll down to interface 1/0/21 and select the checkbox for **1/0/21**. Then select the checkbox for **1/0/24**.

c. In the OSPFv3 Interface Configuration, select **Enable** in the Admin Mode field.

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

8. Enable multicast globally.

a. From the main menu, select Routing > Multicast >Global Configuration. A screen similar to the following displays.



Global Configuration

Global Configuration

Admin Mode	○ Disable ● Enable
Protocol State	Non-Operational
Table Maximum Entry Count	256

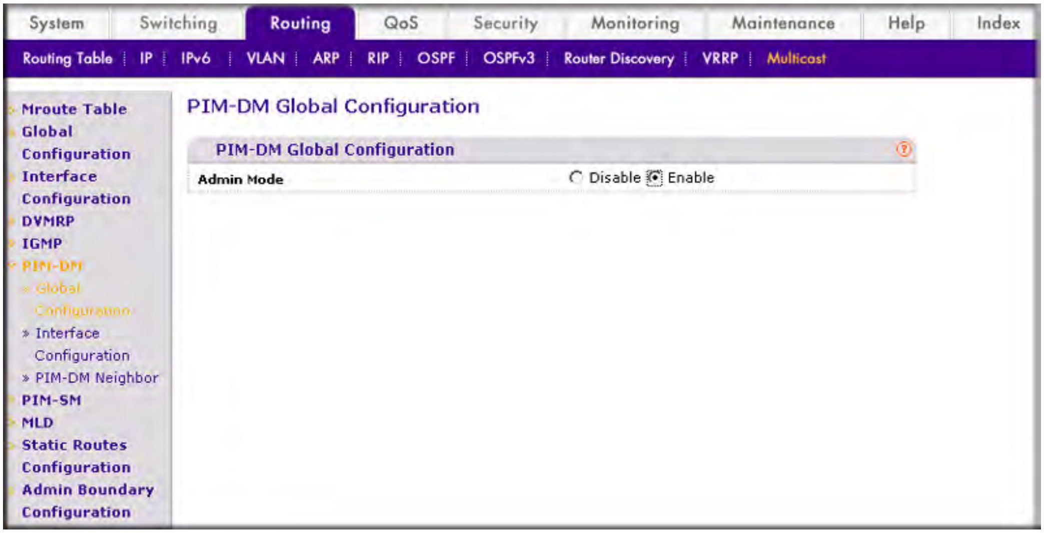
Figure 30-19

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

9. Enable PIM-DM globally.

a. From the main menu, select Routing > Multicast >PIM-DM->Global Configuration. A screen similar to the following displays.



PIM-DM Global Configuration

PIM-DM Global Configuration

Admin Mode ○ Disable ● Enable

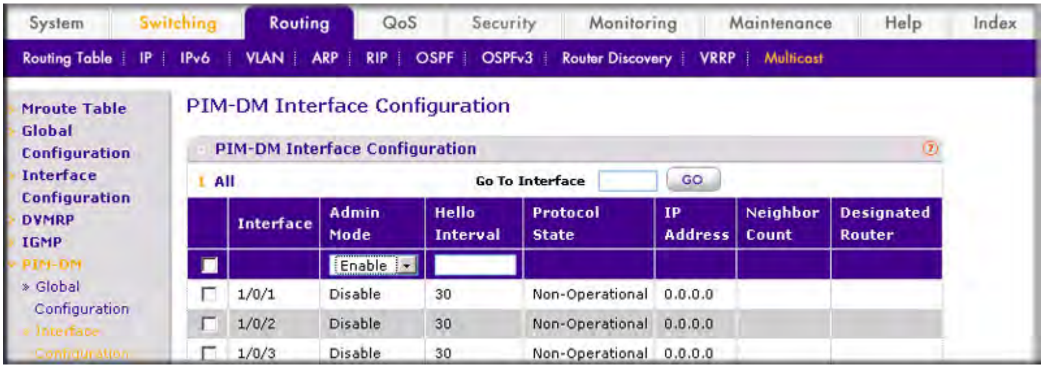
Figure 30-20

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

10. Enable PIM-DM on the interface 1/0/21and 1/0/24.

a. From the main menu, select Routing > Multicast >PIM-DM->Interface Configuration. A screen similar to the following displays.



PIM-DM Interface Configuration

PIM-DM Interface Configuration

1 All Go To Interface GO

	Interface	Admin Mode	Hello Interval	Protocol State	IP Address	Neighbor Count	Designated Router
□		Enable					
□	1/0/1	Disable	30	Non-Operational	0.0.0.0		
□	1/0/2	Disable	30	Non-Operational	0.0.0.0		
□	1/0/3	Disable	30	Non-Operational	0.0.0.0		

Figure 30-21

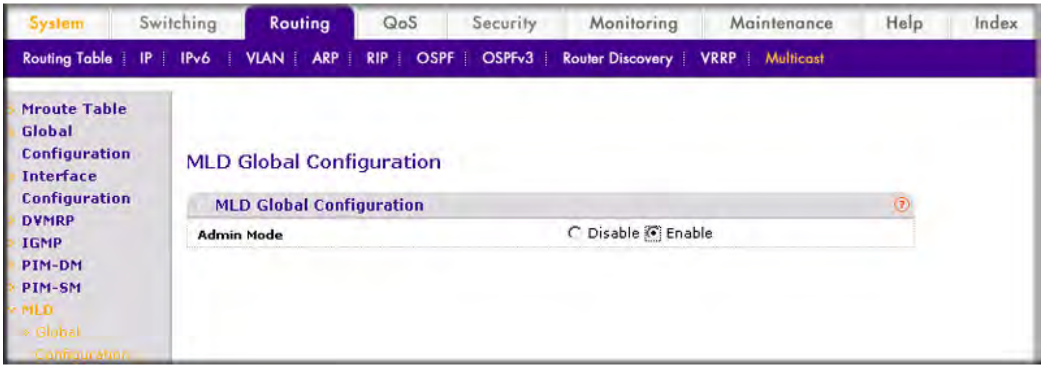
b. Under PIM-DM Interface Configuration, scroll down to interface 1/0/21 and select the checkbox for **1/0/21**. Then select the checkbox for **1/0/24**.

c. In the PIM-DM Interface Configuration, select **Enable** in the Admin Mode field.

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

11. Enable MLD on the switch.

a. From the main menu, select Routing >Multicast >MLD >Global configuration. A screen similar to the following displays.



MLD Global Configuration

MLD Global Configuration

Admin Mode ○ Disable ● Enable

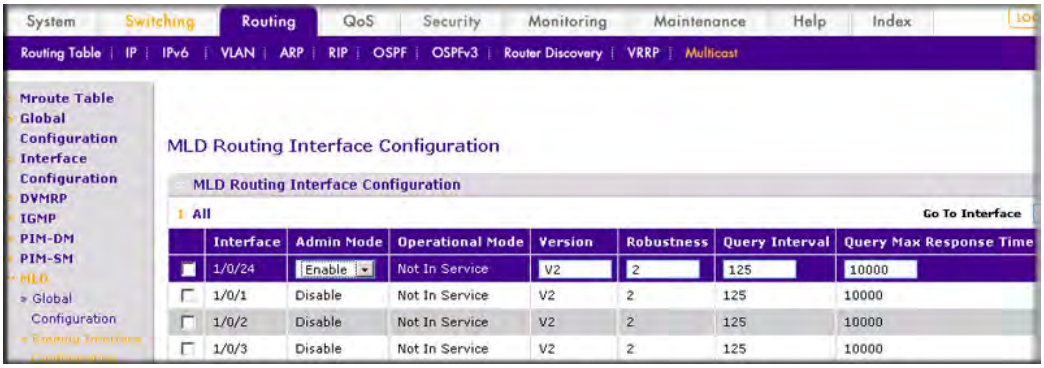
Figure 30-22

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

12. Enable MLD on the interface 1/0/24.

a. From the main menu, select Routing > Multicast >MLD > Routing Interface Configuration. A screen similar to the following displays.



MLD Routing Interface Configuration

MLD Routing Interface Configuration

1 All

	Interface	Admin Mode	Operational Mode	Version	Robustness	Query Interval	Query Max Response Time
☑	1/0/24	Enable	Not In Service	V2	2	125	10000
□	1/0/1	Disable	Not In Service	V2	2	125	10000
□	1/0/2	Disable	Not In Service	V2	2	125	10000
□	1/0/3	Disable	Not In Service	V2	2	125	10000

Figure 30-23

b. Under MLD Routing Interface Configuration, scroll down to interface 1/0/24 and select the checkbox for **1/0/24**. Now 1/0/24 appears in the Interface field at the top.

c. In the MLD Routing Interface Configuration, select **Enable** in the Admin Mode field.

d. Click **Apply**.

MLD Snooping

In IPv4, Layer 2 switches can use IGMP Snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast address. In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes wishing 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: MLD Snooping

```
(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
```

Enable MLDSnooping on the VLAN 300.

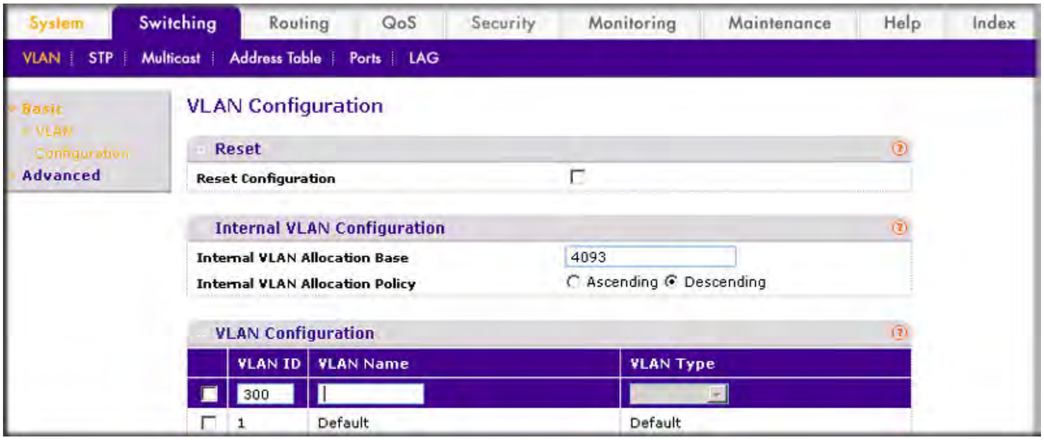
```
(Netgear Switch) #show mldsnooping
Admin Mode..................................... Enable
Multicast Control Frame Count.................. 0
Interfaces Enabled for MLD Snooping............ None
VLANs enabled for MLD snooping................. 300
(Netgear Switch) #
```

Web Interface: MLD Snooping

To use the Web interface to configure the MLD Snooping, proceed as follows:

1. Create VLAN 300.

a. From the main menu, 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

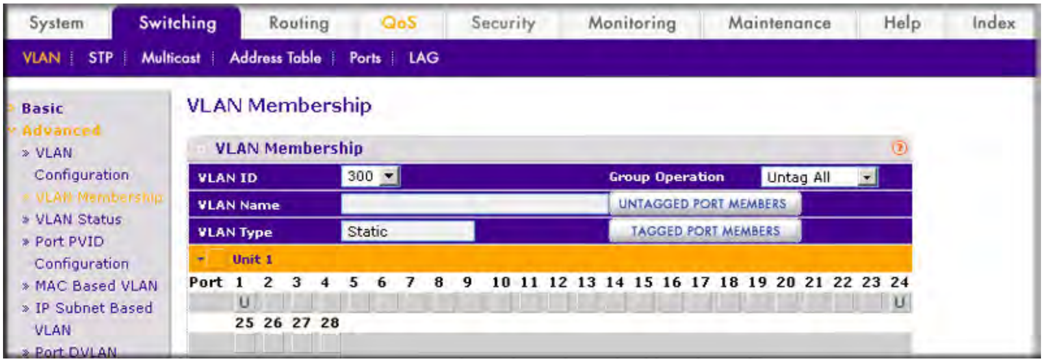
Figure 30-24

b. In the VLAN Configuration, VLAN ID field, enter 300

c. Click **Add**.

2. Assign all of the ports to VLAN 300.

a. From the main menu, select Switching > VLAN >Advanced > VLAN Membership. A screen similar to the following displays.



VLAN Membership

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																				

Figure 30-25

b. Select **300** in the VLAN ID field.

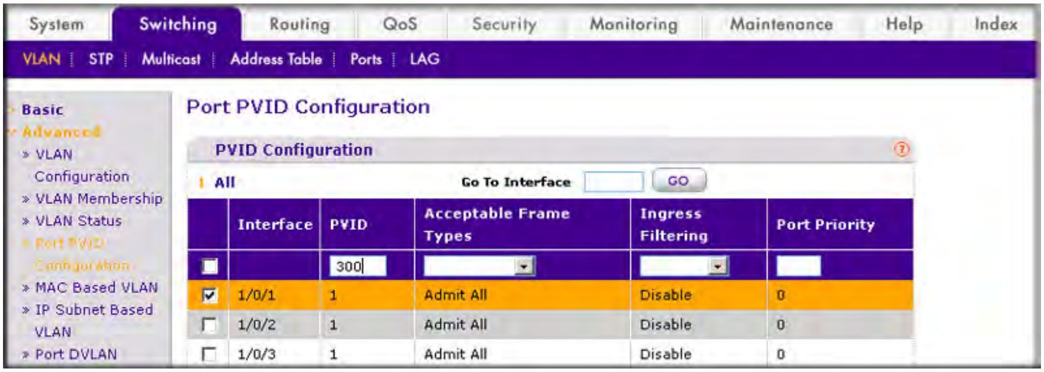
c. Click the Unit 1. The Ports display.

d. Click the gray box under port 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 port 1/0/1 and 1/0/24.

   a. From the main menu, select Switching > VLAN> Advanced > Port PVID Configuraton. A screen similar to the following displays.



Port PVID Configuration

PVID Configuration

All

	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

Figure 30-26

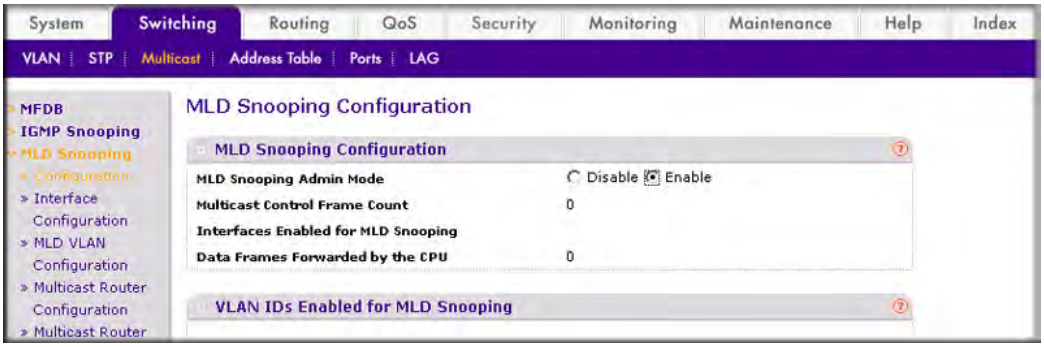
   b. Under PVID Configuration, scroll down to interface 1/0/1 and select the checkbox for 1/0/1. Then scroll down to the interface 1/0/24 and select the checkbox for 1/0/24.

   c. In the PVID Configuration, PVID (1 to 4093) field, enter 300.

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

4. Enable MLD Snooping on the switch.

   a. From the main menu, 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

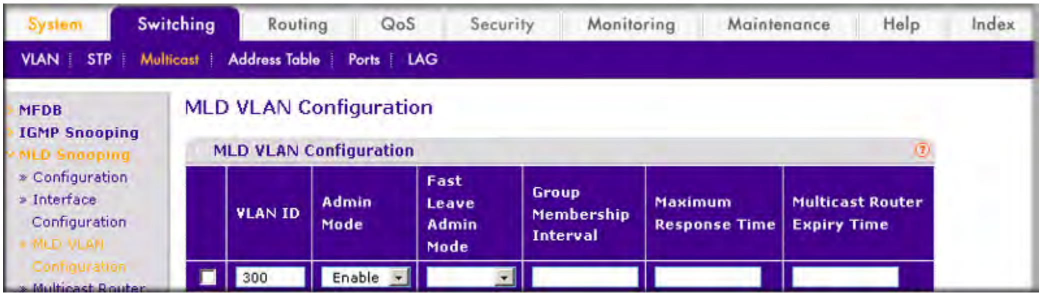
Figure 30-27

   b. Next to the MLD Snooping Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

5. Enable MLD Snooping on the VLAN 300.

a. From the main menu, 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				

Figure 30-28

b. Enter the following information in the MLD VLAN Configuration.

- In the VLAN ID field, enter **300**.
- Select **Enable** in the Admin Mode field.

6. Click **Add**.

Chapter 31
DVMRP

The Distance Vector Multicast Routing Protocol (DVMRP) is used for multicasting over IP networks without routing protocols to support multicast. The DVMRP is based on the RIP protocol but more complicated than RIP. DVRMP maintains a link-state database to keep track of the return paths to the source of multicast packages.

The DVMRP protocol operates as follows:

- The first message for any source-group pair is forwarded to the entire multicast network, with respect to the time-to-live (TTL) of the packet.
- TTL restricts the area to be flooded by the message.
- All the leaf routers that do not have members on directly attached subnetworks send back prune messages to the upstream router.
- The branch that transmitted a prune message is deleted from the delivery tree.
- The delivery tree, which is spanning to all the members in the multicast group, is constructed.

Configure DVMRP on a NETGEAR Switch

In this example, DVMRP is running on the switch A,B and C. IGMP is also running on the Switch C which is connected to the host directly. After host sends a IGMP report to switch C. Multicast streams will be sent from multicast resource to the host along the path built by DVMRP.

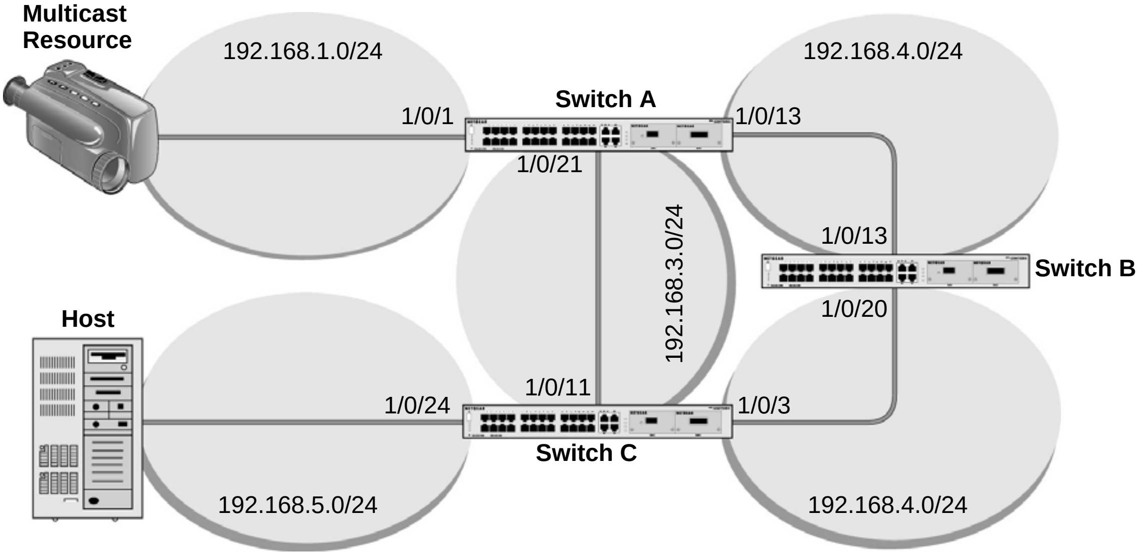


Figure 31-1

CLI: Configuring DVMRP

On Switch A:

Create routing interface 1/0/1,1/0/13 and 1/0/21.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.1.1  255.255.255.0
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ip address 192.168.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address 192.168.3.2 255.255.255.0
(Netgear Switch)(Interface 1/0/21)#exit
```

Enable ip multicast forwarding on the switch.

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

Enable DVMRP protocol on the switch.

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

Enable DVMRP mode on the interface 1/0/1,1/0/13 and 1/0/21.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#ip dvmrp
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#ip dvmrp
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#ip dvmrp
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) #show ip dvmrp neighbor
Interface ..................................... 1/0/13
Neighbor IP Address ........................... 192.168.2.2
State ......................................... Active
Up Time (hh:mm:ss) ............................ 00:02:40
Expiry Time (hh:mm:ss) ........................ 00:00:25
Generation ID ................................. 1116347719
Major Version ................................. 3
Minor Version ................................. 255
Capabilities .................................. Prune GenID Missing 11441
Received Routes ............................... 0
Received Bad Packets .......................... 0
Received Bad Routes ........................... 0
Interface ..................................... 1/0/21
Neighbor IP Address ........................... 192.168.3.1
State ......................................... Active
Up Time (hh:mm:ss) ............................ 00:01:44
Expiry Time (hh:mm:ss) ........................ 00:00:28
Generation ID ................................. 1116595047
Major Version ................................. 3
Minor Version ................................. 255
 More Entries or quit(q)
Capabilities .................................. Prune GenID Missing 11441
Received Routes ............................... 0
Received Bad Packets .......................... 0
Received Bad Routes ........................... 0
(Netgear Switch) #show ip mcast mroute summary

             Multicast Route Table Summary
                                           Incoming      Outgoing
Source IP       Group IP       Protocol    Interface   Interface List
-------------  ------------   ----------   ---------   ---------------
192.168.1.2     225.0.0.1       DVMRP      1/0/1          1/0/21
```

On Switch B

Create the routing port 1/0/13 and 1/0/20.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ip address 192.168.2.2 255.255.255.0
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#interface 1/0/20
(Netgear Switch) (Interface 1/0/20)#routing
(Netgear Switch) (Interface 1/0/20)#ip address 192.l.168.4.1 255.255.255.0
(Netgear Switch) (Interface 1/0/20)#exit
(Netgear Switch) (Config)#exit
```

Enable ip multicast forwarding on the switch.

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

Enable DVMRP protocol on the switch.

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

Enable DVMRP mode on the interface 1/0/13 and 1/0/20.

```
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#ip dvmrp
(Netgear Switch) (Interface 1/0/13)#ex
(Netgear Switch) (Config)#interface 1/0/20
(Netgear Switch) (Interface 1/0/20)#ip dvmrp
(Netgear Switch) (Interface 1/0/20)#exit
(Netgear Switch) (Config)#exit
```

```
(Netgear Switch) #show ip dvmrp neighbor
Interface ..................................... 1/0/13
Neighbor IP Address ........................... 192.168.2.1
State ......................................... Active
Up Time (hh:mm:ss) ............................ 00:02:26
Expiry Time (hh:mm:ss) ........................ 00:00:20
Generation ID ................................. 88091
Major Version ................................. 3
Minor Version ................................. 255
Capabilities .................................. Prune GenID Missing 11441
Received Routes ............................... 0
Received Bad Packets .......................... 0
Received Bad Routes ........................... 0
Interface ..................................... 1/0/20
Neighbor IP Address ........................... 192.168.4.2
State ......................................... Active
Up Time (hh:mm:ss) ............................ 00:01:44
Expiry Time (hh:mm:ss) ........................ 00:00:29
Generation ID ................................. 1116595033
Major Version ................................. 3
Minor Version ................................. 255
Capabilities .................................. Prune GenID Missing 11441
Received Routes ............................... 0
Received Bad Packets .......................... 0
Received Bad Routes ........................... 0

(Netgear Switch) #show ip mcast mroute detail summary

                  Multicast Route Table Summary
                                          Incoming       Outgoing
Source IP       Group IP      Protocol    Interface   Interface List

--------------  ------------  ----------  ---------   --------------

192.168.1.2      225.0.0.1       DVMRP      1/0/13
```

On Switch C:

Create the routing interface 1/0/11,1/0/3 and 1/0/24.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip interface 1/0/11
(Netgear Switch) (Interface 1/0/11)#ip routing
(Netgear Switch) (Interface 1/0/11)#ip address 192.168.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/11)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.168.4.2 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#routing
(Netgear Switch) (Interface 1/0/24)#ip address 192.168.5.1 255.255.255.0
(Netgear Switch) (Interface 1/0/24)#exit
```

Enable ip multicast forwarding on the switch.

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

Enable ip DVMRP protocol on the switch.

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

Enable DVMRP mode on the interface 1/0/3,1/0/11 and 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip dvmrp
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#interface 1/0/11
(Netgear Switch) (Interface 1/0/11)#ip dvmrp
(Netgear Switch) (Interface 1/0/11)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#ip dvrmp
(Netgear Switch) (Interface 1/0/24)#exit
```

Enable IGMP protocol on the switch.

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

Enable IGMP mode on the interface 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#ip igmp
(Netgear Switch) (Interface 1/0/24)#exit
```

```
(Netgear Switch) #show ip dvmrp neighbor
Interface ..................................... 1/0/11
Neighbor IP Address ........................... 192.168.3.2
State ......................................... Active
Up Time (hh:mm:ss) ............................ 00:01:03
Expiry Time (hh:mm:ss) ........................ 00:00:24
Generation ID ................................. 88099
Major Version ................................. 3
Minor Version ................................. 255
Capabilities .................................. Prune GenID Missing 11441
Received Routes ............................... 0
Received Bad Packets .......................... 0
Received Bad Routes ........................... 0
Interface ..................................... 1/0/3
Neighbor IP Address ........................... 192.168.4.1
State ......................................... Active
Up Time (hh:mm:ss) ............................ 00:01:17
Expiry Time (hh:mm:ss) ........................ 00:00:23
Generation ID ................................. 1116347728
Major Version ................................. 3
Minor Version ................................. 255

More Entries or quit(q)
Capabilities .................................. Prune GenID Missing 11441
Received Routes ............................... 0
Received Bad Packets .......................... 0
Received Bad Routes ........................... 0
(Netgear Switch) #show ip mcast mroute detail summary

                  Multicast Route Table Summary
                                            Incoming      Outgoing
Source IP       Group IP        Protocol    Interface   Interface List
-------------   ------------   ----------   ---------   ---------------
 192.168.1.2     225.0.0.1       DVMRP      1/0/11      1/0/24
```

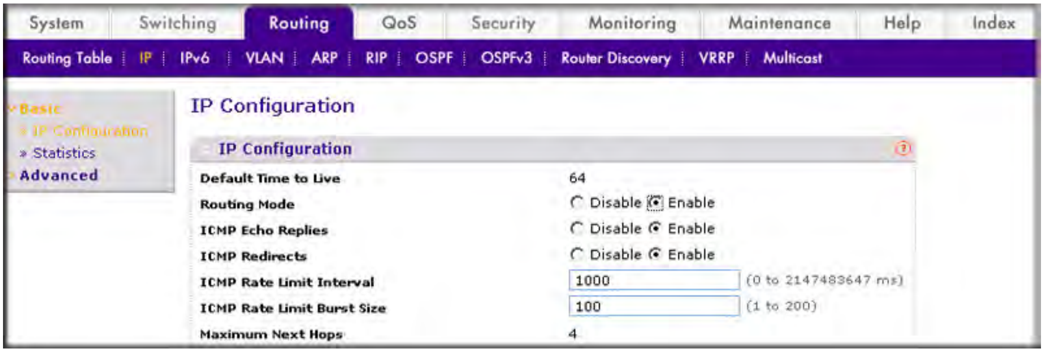
Web Interface: Configuring DVMRP

On Switch A:

To use the Web interface to config DVMRP, proceed as follows:

1. Enable IP routing on the switch.

   a. From the main menu, select Routing >IP >Basic >IP configuration. A screen similar to the following displays.



IP Configuration

IP Configuration

Default Time to Live	64
Routing Mode	○ Disable ● Enable
ICMP Echo Replies	○ Disable ● Enable
ICMP Redirects	○ Disable ● Enable
ICMP Rate Limit Interval	1000 (0 to 2147483647 ms)
ICMP Rate Limit Burst Size	100 (1 to 200)
Maximum Next Hops	4

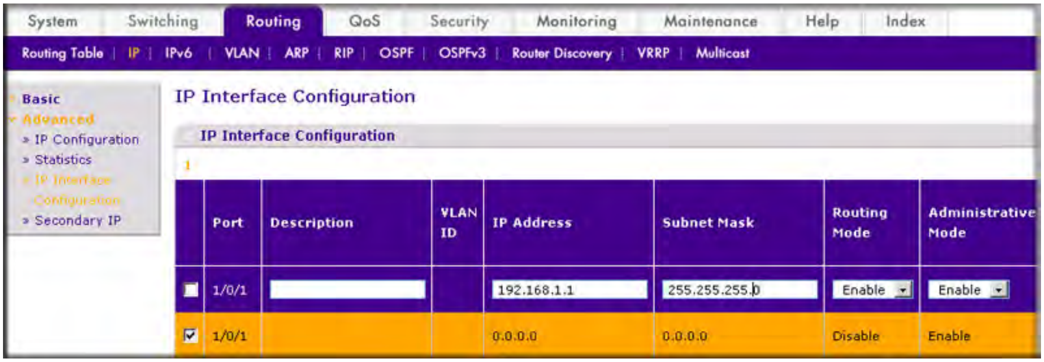
Figure 31-2

   b. Next to the Routing Mode, select the **Enable** radio button.

   c. Click **Apply**.

2. Configure 1/0/1 as a routing port and assign IP address to it.

   a. From the main menu, 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
Basic
Advanced
IP Configuration
Statistics
IP Interface Configuration
Secondary IP

IP Interface Configuration

IP Interface Configuration

1

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
□	1/0/1			192.168.1.1	255.255.255.0	Enable	Enable
☑	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 31-3

   b. Under IP Interface Configuration, scroll down to interface 1/0/1 and select the checkbox for **1/0/1**. Now 1/0/1appears in the Interface field at the top.

   c. Enter the following information in the IP Interface Configuration.

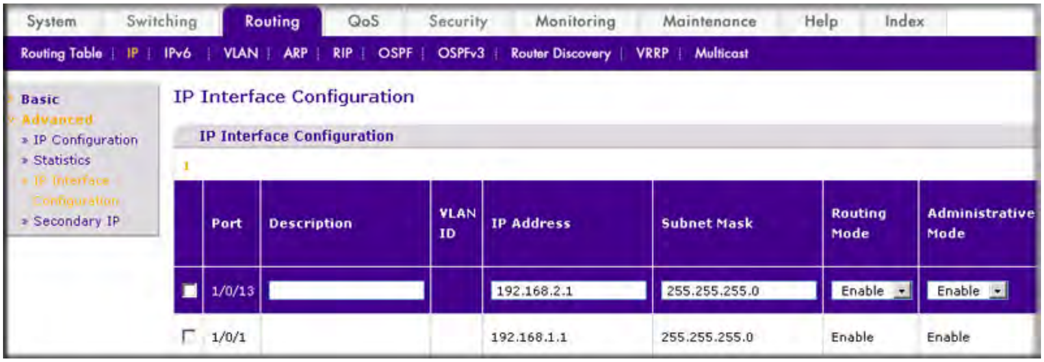
   - In the IP address, enter **192.168.1.1**.
   - In the Subnet Mask, enter **255.255.255.0**.

- Select **Enable** in the Routing Mode field.

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

3. Configure 1/0/13 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
» IP Configuration
» Statistics
» IP Interface Configuration
» Secondary IP

IP Interface Configuration

IP Interface Configuration

1

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☑	1/0/13			192.168.2.1	255.255.255.0	Enable	Enable
□	1/0/1			192.168.1.1	255.255.255.0	Enable	Enable

Figure 31-4

b. Under IP Interface Configuration, scroll down to interface 1/0/13 and select the checkbox for 1/0/13. 1/0/13 now appears in the Interface field at the top.

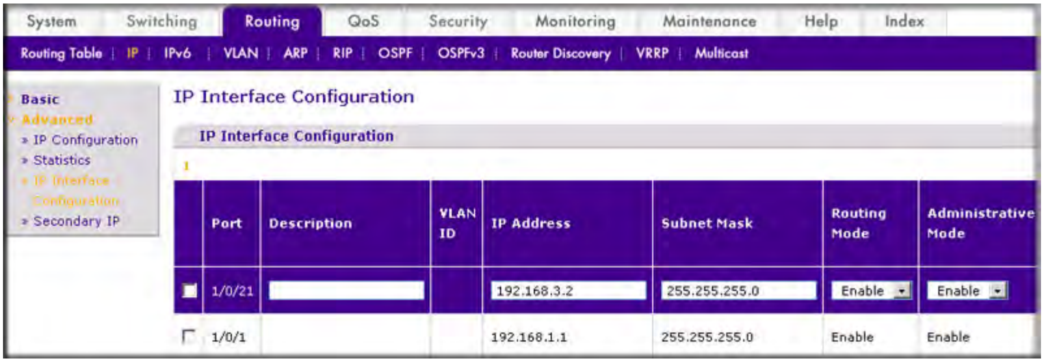
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.2.1**.
- In the Subnet Mask, enter **255.255.255.**0.
- Select **Enable** in the Routing Mode field.

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

4. Configure 1/0/21 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
IP Configuration
Statistics
IP Interface Configuration
Secondary IP

IP Interface Configuration

IP Interface Configuration

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
■	1/0/21			192.168.3.2	255.255.255.0	Enable	Enable
□	1/0/1			192.168.1.1	255.255.255.0	Enable	Enable

Figure 31-5

b. Under IP Interface Configuration, scroll down to interface 1/0/13 and select the checkbox for 1/0/13. Now 1/0/13 appears in the Interface field at the top.

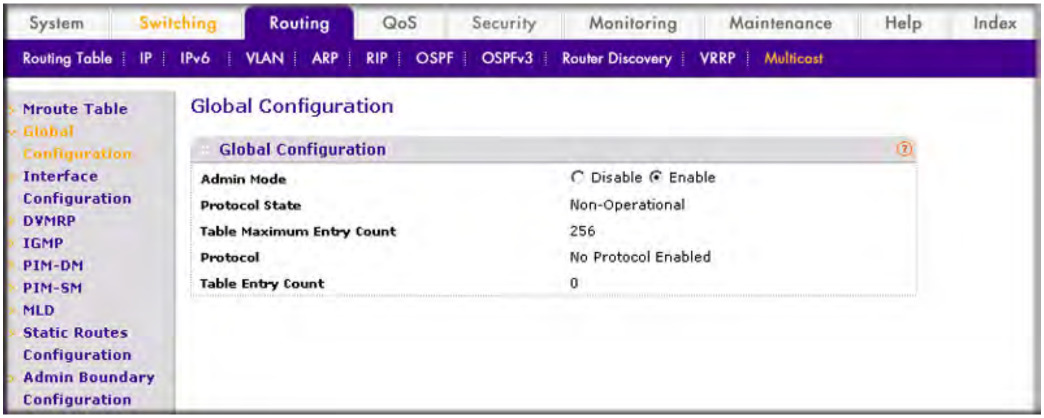
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.3.2**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

5. Enable IP multicast on the switch.

a. From the main menu, select Routing > Multicast >Global Configuration. A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Routing Table | IP | IPv6 | VLAN | ARP | RIP | OSPF | OSPFv3 | Router Discovery | VRRP | Multicast
Mroute Table
Global Configuration
Interface Configuration
DVMRP
IGMP
PIM-DM
PIM-SM
MLD
Static Routes Configuration
Admin Boundary Configuration

Global Configuration

Global Configuration

Admin Mode	○ Disable ● Enable
Protocol State	Non-Operational
Table Maximum Entry Count	256
Protocol	No Protocol Enabled
Table Entry Count	0

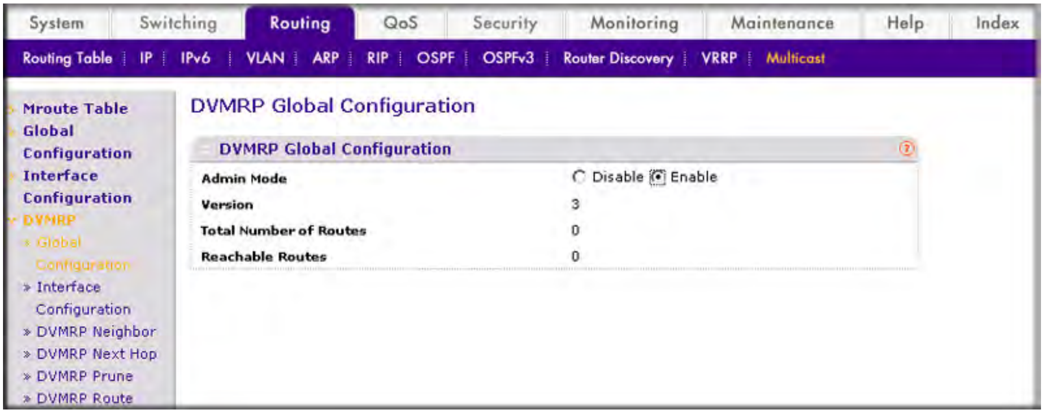
Figure 31-6

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

6. Enable DVMRP on the switch.

a. From the main menu, select Routing > Multicast >DVMRP>Global Configuration. A screen similar to the following displays.



DVMRP Global Configuration

DVMRP Global Configuration

Admin Mode	○ Disable ● Enable
Version	3
Total Number of Routes	0
Reachable Routes	0

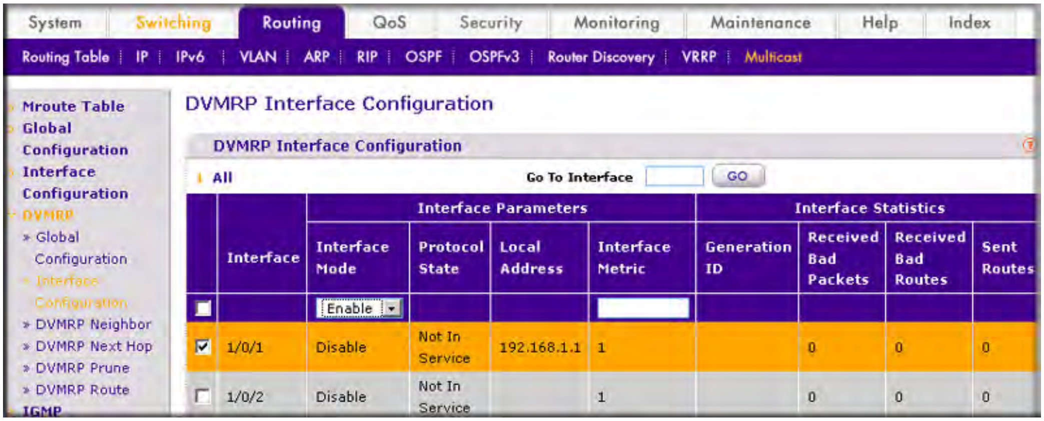
Figure 31-7

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

7. Enable DVMRP on the interface.

a. From the main menu, select Routing > Multicast >DVMRP>Interface Configuration. A screen similar to the following displays.



DVMRP Interface Configuration

DVMRP Interface Configuration

		Interface Parameters				Interface Statistics			
	Interface	Interface Mode	Protocol State	Local Address	Interface Metric	Generation ID	Received Bad Packets	Received Bad Routes	Sent Routes
□		Enable							
☑	1/0/1	Disable	Not In Service	192.168.1.1	1		0	0	0
□	1/0/2	Disable	Not In Service		1		0	0	0

Figure 31-8

b. Under DVMRP Interface Configuration, scroll down to interface 1/0/1 and select the **1/0/1** checkbox. Select the **1/0/13** checkbox and the **1/0/21** checkbox.

c. Select **Enable** in the Interface Mode field.

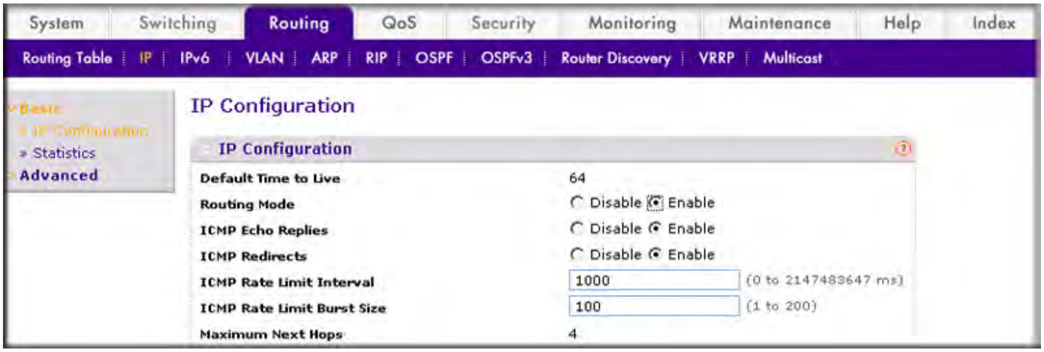
d. Click **Apply** to save the settings.

On Switch B

To use the Web interface to config DVMRP, proceed as follows:

1. Enable IP routing on the switch.

   a. From the main menu, select Routing >IP >Basic >IP configuration. A screen similar to the following displays.



IP Configuration

IP Configuration

Default Time to Live	64
Routing Mode	○ Disable ● Enable
ICMP Echo Replies	○ Disable ● Enable
ICMP Redirects	○ Disable ● Enable
ICMP Rate Limit Interval	1000 (0 to 2147483647 ms)
ICMP Rate Limit Burst Size	100 (1 to 200)
Maximum Next Hops	4

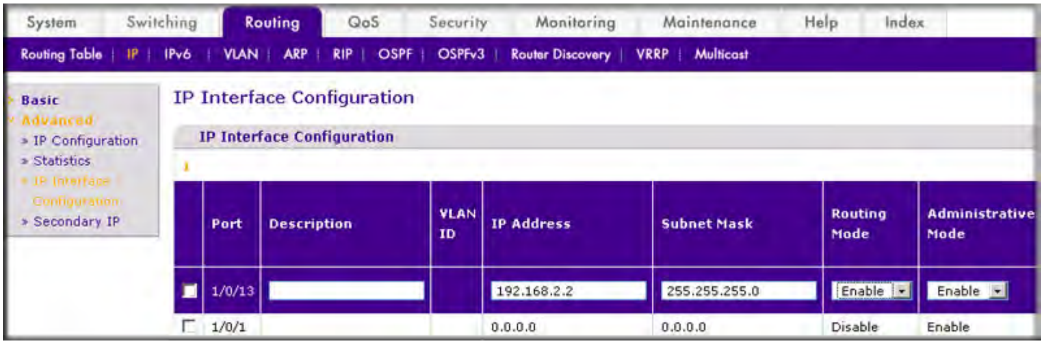
Figure 31-9

   b. Next to the Routing Mode, select the **Enable** radio button.

   c. Click **Apply**.

2. Configure 1/0/13 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
IP Configuration
Statistics
IP Interface Configuration
Secondary IP

IP Interface Configuration

IP Interface Configuration

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☑	1/0/13			192.168.2.2	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 31-10

b. Under IP Interface Configuration, scroll down to interface 1/0/13 and select the **1/0/13** checkbox. Now 1/0/13 appears in the Interface field at the top.

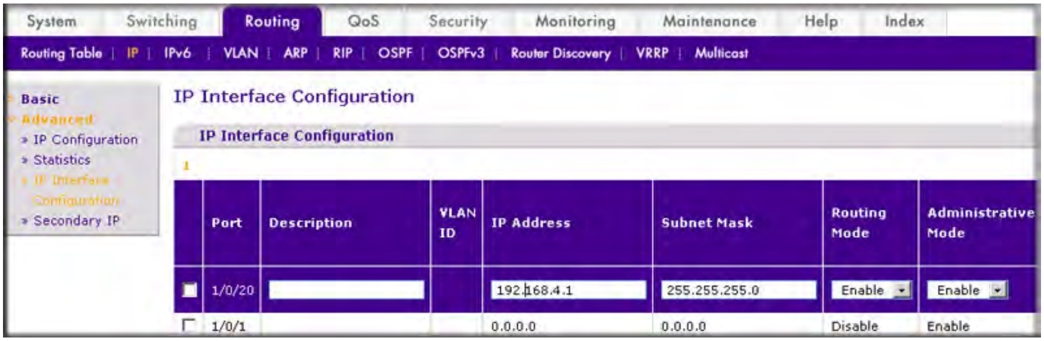
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.2.2**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

3. Configure 1/0/20 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
IP Configuration
Statistics
IP Interface Configuration
Secondary IP

IP Interface Configuration

IP Interface Configuration

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☑	1/0/20			192.168.4.1	255.255.255.0	Enable	Enable
□	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

Figure 31-11

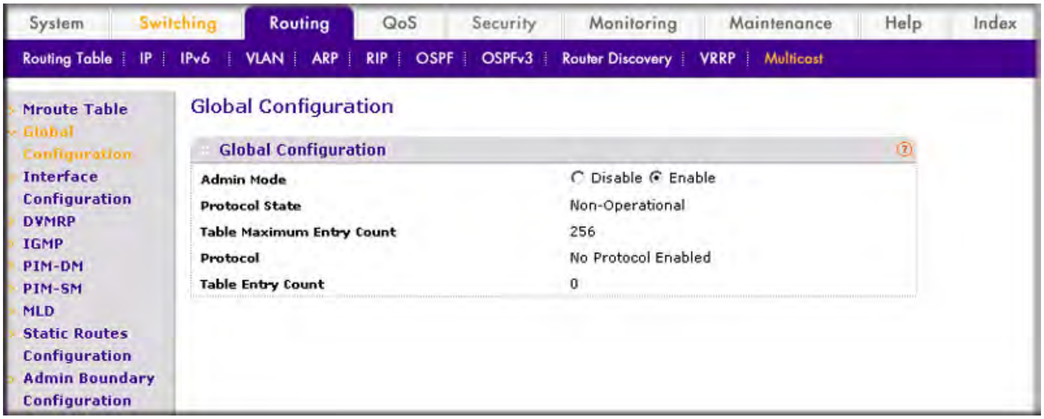
b. Under IP Interface Configuration, scroll down to interface 1/0/20 and select the checkbox for **1/0/20**. Now 1/0/20 appears in the Interface field at the top.

c. Enter the following information in the IP Interface Configuration.
   - In the IP address, enter **192.168.4.1**.
   - In the Subnet Mask, enter **255.255.255.0**.
   - Select **Enable** in the Routing Mode field.

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

4. Enable IP multicast on the switch.

a. From the main menu, select Routing > Multicast >Global Configuration. A screen similar to the following displays.



Global Configuration

Global Configuration	
Admin Mode	○ Disable ● Enable
Protocol State	Non-Operational
Table Maximum Entry Count	256
Protocol	No Protocol Enabled
Table Entry Count	0

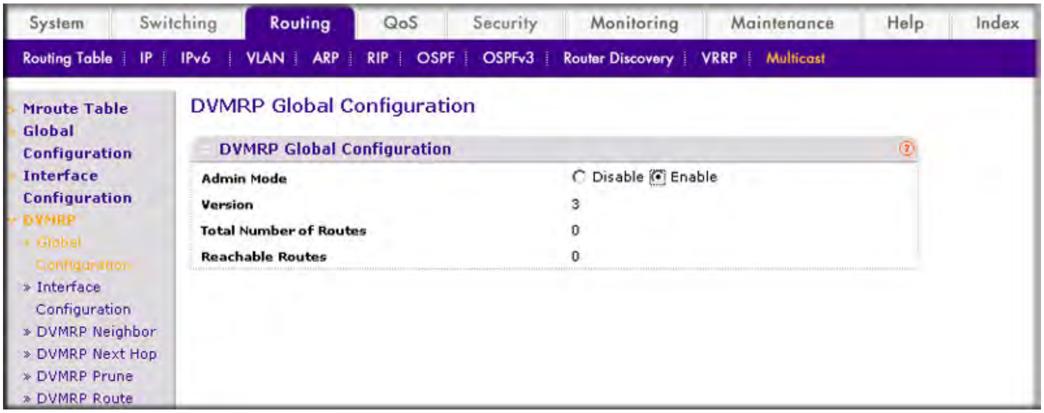
Figure 31-12

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

5. Enable DVMRP on the switch.

a. From the main menu, select Routing > Multicast >DVMRP>Global Configuration. A screen similar to the following displays.



DVMRP Global Configuration

DVMRP Global Configuration	
Admin Mode	○ Disable ● Enable
Version	3
Total Number of Routes	0
Reachable Routes	0

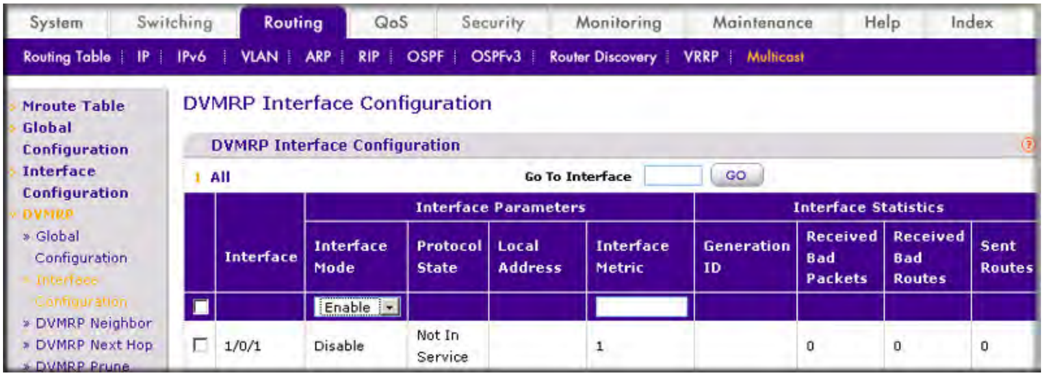
Figure 31-13

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

6. Enable DVMRP on the interface.

a. From the main menu, select Routing > Multicast >DVMRP>Interface Configuration. A screen similar to the following displays.



DVMRP Interface Configuration

DVMRP Interface Configuration

		Interface Parameters				Interface Statistics			
	Interface	Interface Mode	Protocol State	Local Address	Interface Metric	Generation ID	Received Bad Packets	Received Bad Routes	Sent Routes
□		Enable							
□	1/0/1	Disable	Not In Service		1		0	0	0

Figure 31-14

b. Under DVMRP Interface Configuration, scroll down to interface 1/0/13 and select the checkbox for **1/0/13**. Select the checkbox for **1/0/20**.

c. Select **Enable** in the Interface Mode field.

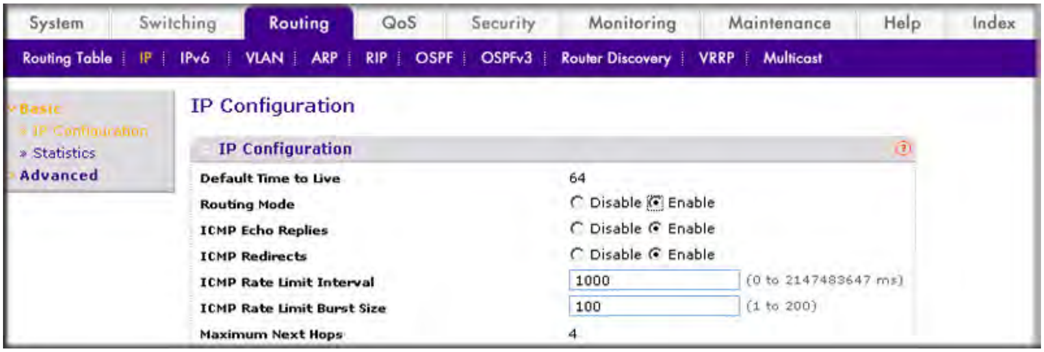
d. Click **Apply** to save the settings.

On Switch C:

To use the Web interface to config DVMRP, proceed as follows:

1. Enable IP routing on the switch.

a. From the main menu, select Routing >IP >Basic >IP configuration. A screen similar to the following displays.



IP Configuration

IP Configuration

Default Time to Live	64
Routing Mode	○ Disable ● Enable
ICMP Echo Replies	○ Disable ● Enable
ICMP Redirects	○ Disable ● Enable
ICMP Rate Limit Interval	1000 (0 to 2147483647 ms)
ICMP Rate Limit Burst Size	100 (1 to 200)
Maximum Next Hops	4

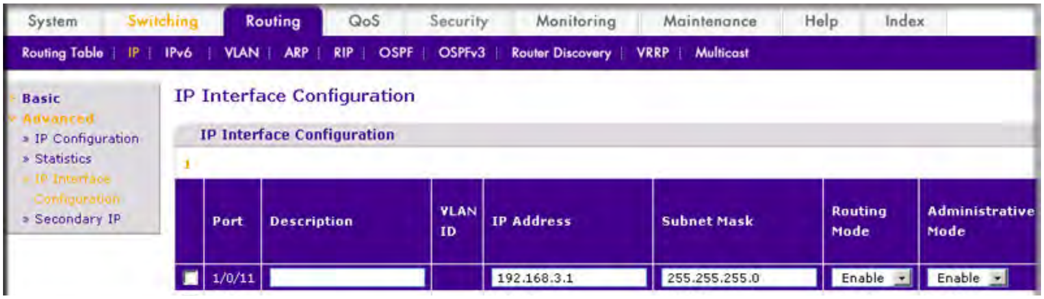
Figure 31-15

b. Next to the Routing Mode, select the **Enable** radio button.

c. Click **Apply**.

2. Configure 1/0/11 as a routing port and assign IP address to it.

a. From the main menu, select Routing > IP >Advanced > IP Interface Configuration. A screen similar to the following displays.



IP Interface Configuration

IP Interface Configuration

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
☐	1/0/11			192.168.3.1	255.255.255.0	Enable	Enable

Figure 31-16

b. Under IP Interface Configuration, scroll down to interface 1/0/11 and select the **1/0/11**checkbox. Now 1/0/11 appears in the Interface field at the top.

c. Enter the following information in the IP Interface Configuration.

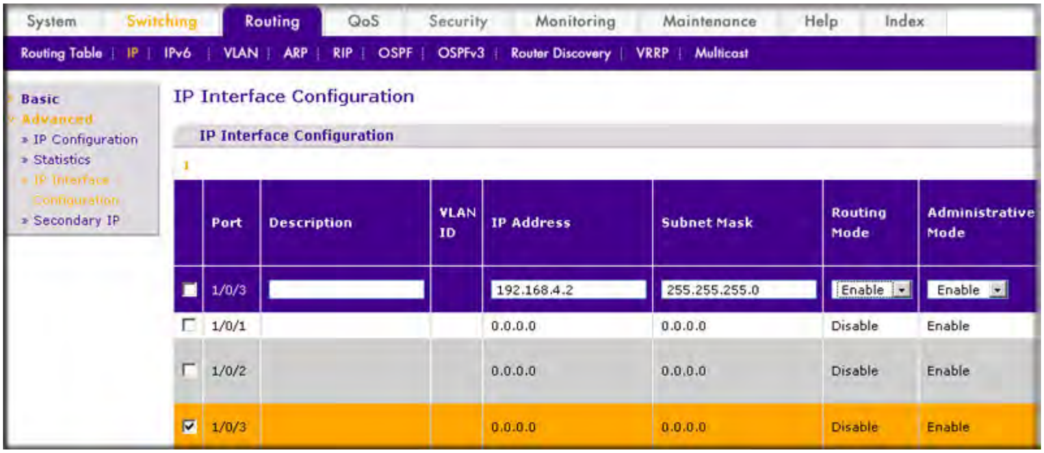
- In the IP address, enter **192.168.3.1**.

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

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

3. Configure 1/0/3 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
IP Configuration
Statistics
IP Interface Configuration
Secondary IP

IP Interface Configuration

IP Interface Configuration

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
□	1/0/3			192.168.4.2	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

Figure 31-17

b. Under IP Interface Configuration, scroll down to interface 1/0/3 and select the **1/0/3** checkbox. Now 1/0/3 appears in the Interface field at the top.

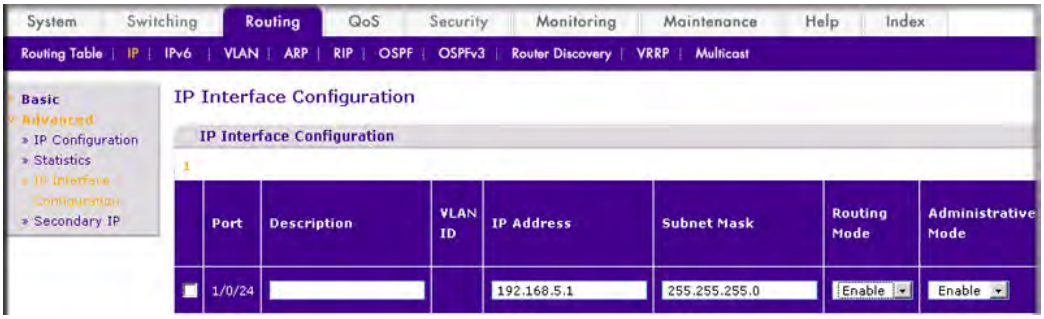
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.4.**2.
- In the Subnet Mask, enter **255.255.255.**0.
- Select **Enable** in the Routing Mode field.

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

4. Configure 1/0/24 as a routing port and assign IP address to it.

a. From the main menu, 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
Basic
Advanced
» IP Configuration
» Statistics
» IP Interface Configuration
» Secondary IP

IP Interface Configuration

IP Interface Configuration

1

	Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode
□	1/0/24			192.168.5.1	255.255.255.0	Enable	Enable

Figure 31-18

b. Under IP Interface Configuration, scroll down to interface 1/0/24 and select the **1/0/24** checkbox. Now 1/0/24 appears in the Interface field at the top.

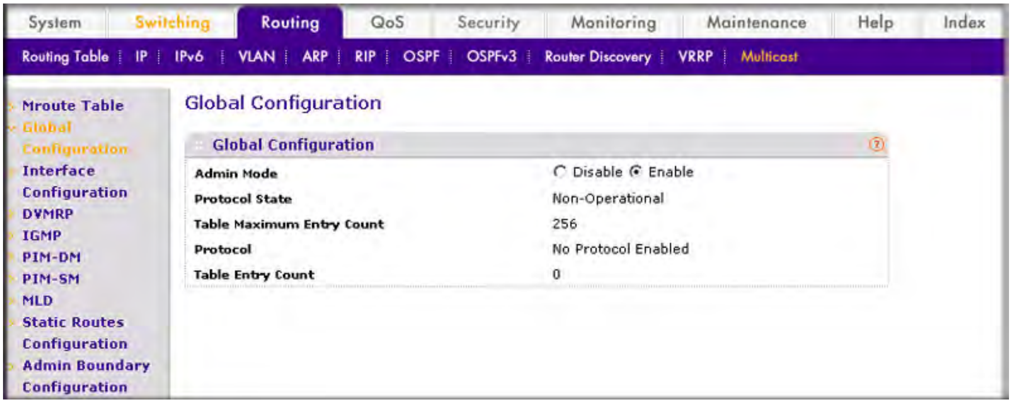
c. Enter the following information in the IP Interface Configuration.

- In the IP address, enter **192.168.5.1**.
- In the Subnet Mask, enter **255.255.255.0**.
- Select **Enable** in the Routing Mode field.

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

5. Enable IP multicast on the switch.

a. From the main menu, select Routing > Multicast >Global Configuration. A screen similar to the following displays.


System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Index
Routing Table | IP | IPv6 | VLAN | ARP | RIP | OSPF | OSPFv3 | Router Discovery | VRRP | Multicast
Mroute Table
Global Configuration
Interface Configuration
DVMRP
IGMP
PIM-DM
PIM-SM
MLD
Static Routes Configuration
Admin Boundary Configuration

Global Configuration

Global Configuration

Admin Mode	○ Disable ● Enable
Protocol State	Non-Operational
Table Maximum Entry Count	256
Protocol	No Protocol Enabled
Table Entry Count	0

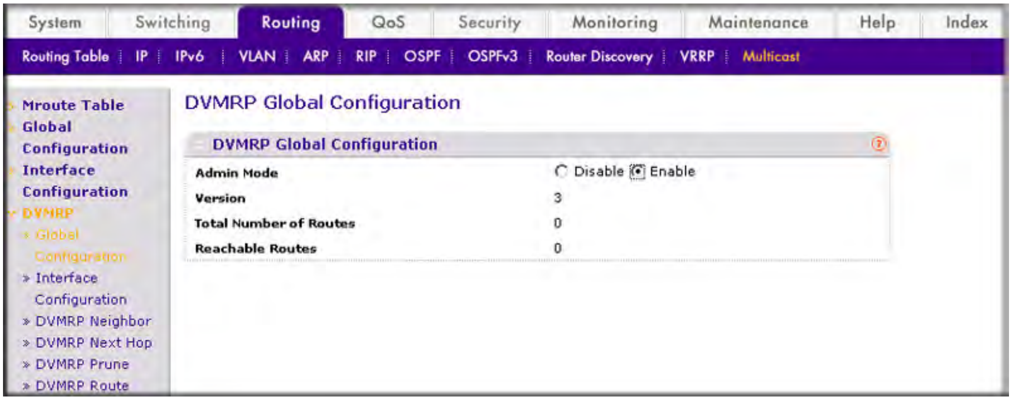
Figure 31-19

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

6. Enable DVMRP on the switch.

a. From the main menu, select Routing > Multicast >DVMRP>Global Configuration. A screen similar to the following displays.



DVMRP Global Configuration

DVMRP Global Configuration

Admin Mode	○ Disable ● Enable
Version	3
Total Number of Routes	0
Reachable Routes	0

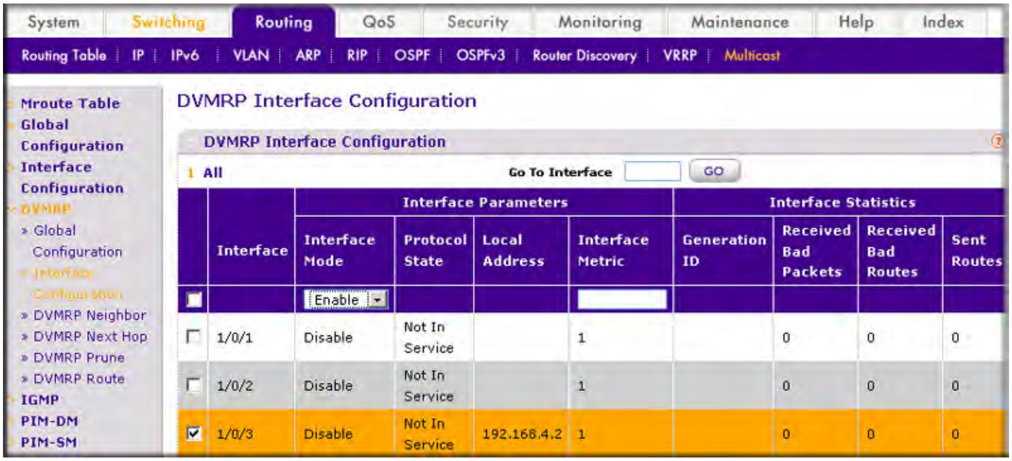
Figure 31-20

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

7. Enable DVMRP on the interface.

a. From the main menu, select Routing > Multicast >DVMRP>Interface Configuration. A screen similar to the following displays.



DVMRP Interface Configuration

DVMRP Interface Configuration

1 All   Go To Interface

		Interface Parameters				Interface Statistics			
	Interface	Interface Mode	Protocol State	Local Address	Interface Metric	Generation ID	Received Bad Packets	Received Bad Routes	Sent Routes
□		Enable							
□	1/0/1	Disable	Not In Service		1		0	0	0
□	1/0/2	Disable	Not In Service		1		0	0	0
☑	1/0/3	Disable	Not In Service	192.168.4.2	1		0	0	0

Figure 31-21

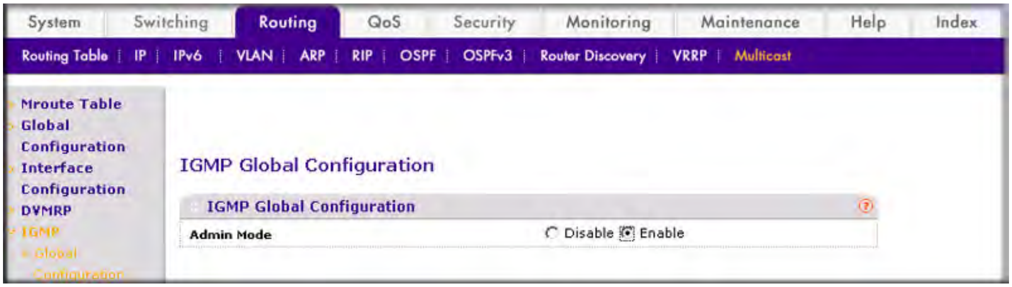
b. Under DVMRP Interface Configuration, scroll down to interface **1/0/3** and select the 1/0/3 checkbox. Select the **1/0/11** checkbox and the **1/0/24** checkbox.

c. Select **Enable** in the Interface Mode field.

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

8. Enable IGMP on the switch.

a. From the main menu, select Routing > Multicast >IGMP>Global Configuration. A screen similar to the following displays.



IGMP Global Configuration

IGMP Global Configuration

Admin Mode ○ Disable ● Enable

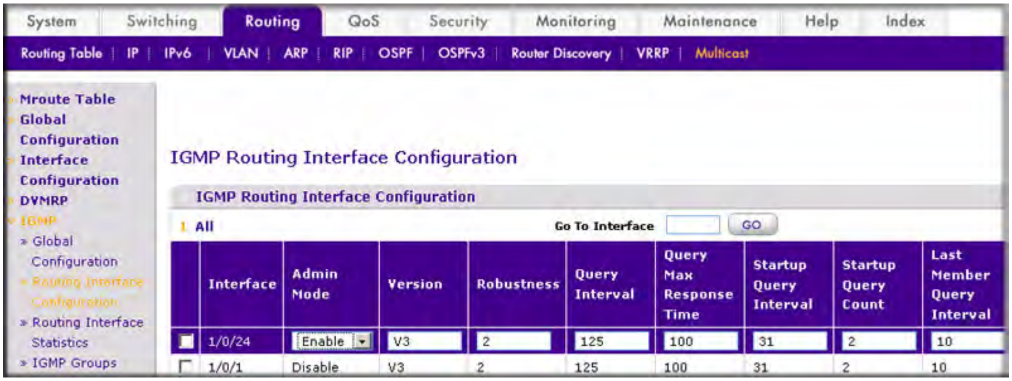
Figure 31-22

b. Next to the Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

9. Enable IGMP on the interface.

a. From the main menu, select Routing > Multicast >IGMP>Routing INterface Configuration. A screen similar to the following displays.



IGMP Routing Interface Configuration

IGMP Routing Interface Configuration

1 All Go To Interface

	Interface	Admin Mode	Version	Robustness	Query Interval	Query Max Response Time	Startup Query Interval	Startup Query Count	Last Member Query Interval
□	1/0/24	Enable	V3	2	125	100	31	2	10
□	1/0/1	Disable	V3	2	125	100	31	2	10

Figure 31-23

b. Under IGMP Interface Configuration, scroll down to interface 1/0/24 and select the **1/0/24** checkbox. Now 1/0/24 appears in the Interface field at the top.

c. Select **Enable** in the Admin Mode field.

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

Chapter 32
Captive Portal

This chapter includes the following sections:

The Captive Portal feature is a software implementation that blocks clients from accessing the network until user verification has been established. Verification can be configured to allow access for both guest and authenticated users. Authenticated users must be validated against a database of authorized Captive Portal users before access is granted.

The Authentication server supports both HTTP and HTTPS web connections. In addition, Captive Portal can be configured to use an optional HTTP port (in support of HTTP Proxy networks). If configured, this additional port is then used exclusively by Captive Portal. Note that this optional port is in addition to the standard HTTP port 80 which is currently being used for all other web traffic.

Captive Portal for wired interfaces allows the clients directly connected to the switch be authenticated using a Captive Portal mechanism before the client is given access to the network.

When a wired physical port is enabled for Captive Portal then the port would be set in captive-portal-enabled state such that all the traffic coming onto the port from the unauthenticated clients are ropped except for the ARP, DHCP, DNS and NETBIOS packets. These packets are allowed to be forwarded by the switch so that the unauthenticated clients can get an IP address and be able to resolve the hostname or domain names. The data traffic from the authenticated clients would go through normally and the above rules do not apply to these packets.

All the HTTP/HTTPS packets from unauthenticated clients are directed to the CPU on the switch for all the ports that are enabled for Captive Portal. So when an unauthenticated client opens a web browser and tries to connect to network, the Captive Portal redirects all the HTTP/HTTPS traffic from unauthenticated clients to the authenticating server on the switch. A Captive portal web page is sent back to the unauthenticated client and the client can authenticate and based upon the authentication the client is given access to the port.

The Captive Portal feature can be enabled on all the physical ports on the switch. It is not supported for VLAN interfaces, loopback interfaces or logical interfaces. The Captive Portal feature is Mac-based authentication and not port-based authentication. This means that all the clients connected to the captive portal interface have to get authenticated before they can get access to the network.

The clients connecting to the Captive Portal interface have three states; the "Unknown State", the "Unauthenticated State", and the "Authenticated" state. In the unknown state the CP doesn't redirect HTTP/S traffic to the switch, but instead asks the switch whether the client is authenticated or unauthenticated. In the Unauthenticated state the CP directs the HTTP/S traffic to the switch so that the client can authenticate with the switch. Once the client is authenticated the client is placed in Authenticated state and in this state all the traffic emerging from the client will be forwarded through the switch.

Captive Portal Configuration

This section introduces the objects that comprise the Captive Portal and describes the interaction between the Captive Portal and the network administrator without delving into the underlying mechanisms involved in gathering information and controlling the Captive Portal. It explains what configurations are visible to the network administrator and enumerates the events.

All of the configurations included in this section are managed using the standard management interfaces (e.g. Web, CLI, and SNMP) with one exception; Captive Portal customized web pages are only configurable via the Web Interface.

The Captive Portal configuration provides the network administrator control over verification and authentication, assignment to interfaces, client sessions, and web page customization.

The administrator can create multiple captive portal configuration instances. Each captive portal configuration contains various flags and definitions used to control client access and content to customize the user verification web page. A captive portal configuration can be applied to one or more interfaces. An interface may only be a physical port on the switch. 8.0 can contain up to 10 Captive Portal configurations.

Enable Captive Portal

CLI: Enabling Captive Portal

Enable captive portal on the switch.

```
(Netgear Switch) (config)#captive-portal
(Netgear Switch) (Config-CP)#enable
```

Enable captive portal instance 1.

```
(Netgear Switch) (Config-CP)#configuration 1
 (Netgear Switch) (Config-CP 1)#enable
```

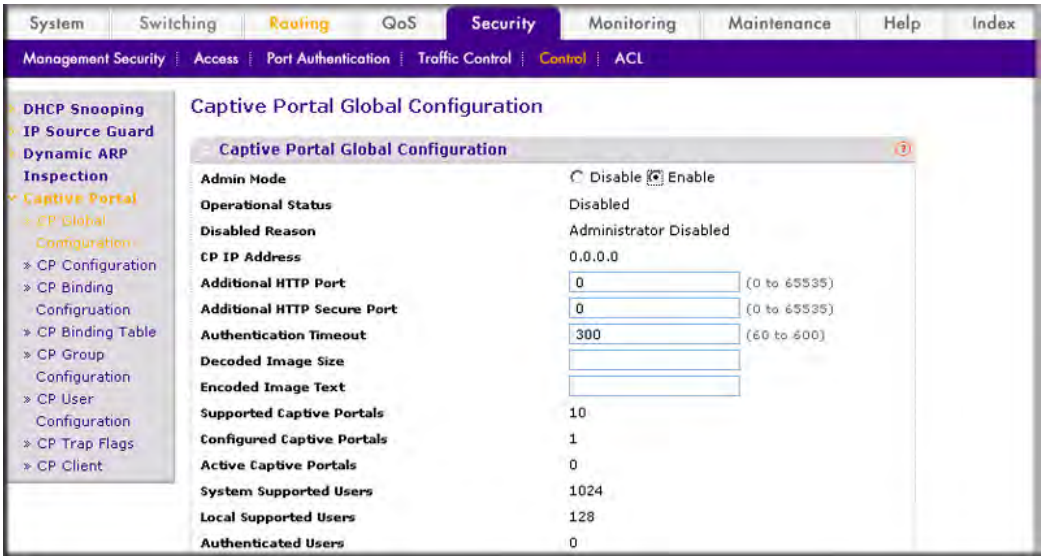
Enable captive portal instance 1 on port 1/0/1.

```
(Netgear Switch) (Config-CP 1)#interface 1/0/1
```

Web Interface: Enabling Captive Portal

To use the Web interface to configure the Captive Portal, proceed as follows:

1. Enable Captive Portal on the switch.
   a. From the main menu, select Security > Control >Captive Portal> CP Global Configuration. A screen similar to the following displays.



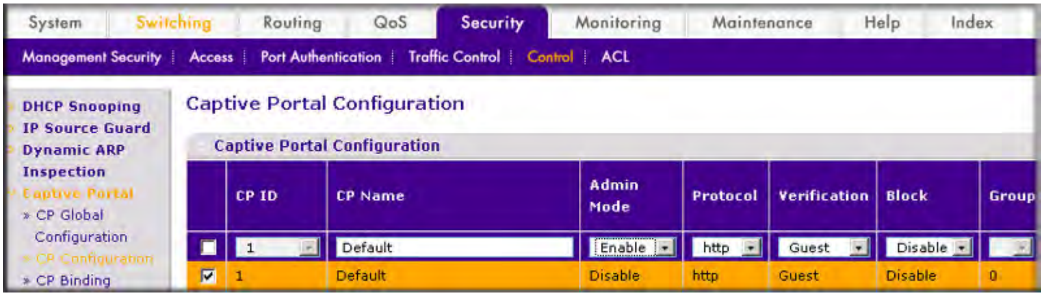
Captive Portal Global Configuration

Captive Portal Global Configuration		
Admin Mode	○ Disable ● Enable	
Operational Status	Disabled	
Disabled Reason	Administrator Disabled	
CP IP Address	0.0.0.0	
Additional HTTP Port	0	(0 to 65535)
Additional HTTP Secure Port	0	(0 to 65535)
Authentication Timeout	300	(60 to 600)
Decoded Image Size		
Encoded Image Text		
Supported Captive Portals	10	
Configured Captive Portals	1	
Active Captive Portals	0	
System Supported Users	1024	
Local Supported Users	128	
Authenticated Users	0	

Figure 32-1

   b. Next to the Admin Mode, Select the **Enable** radio button.
   c. Click **Apply**.
2. Enable Captive Portal instance 1 on the switch.

a. From the main menu, select Security > Control >Captive Portal> CP Configuration. A screen similar to the following displays.



Captive Portal Configuration

Captive Portal Configuration

	CP ID	CP Name	Admin Mode	Protocol	Verification	Block	Group
□	1	Default	Enable	http	Guest	Disable	
☑	1	Default	Disable	http	Guest	Disable	0

Figure 32-2

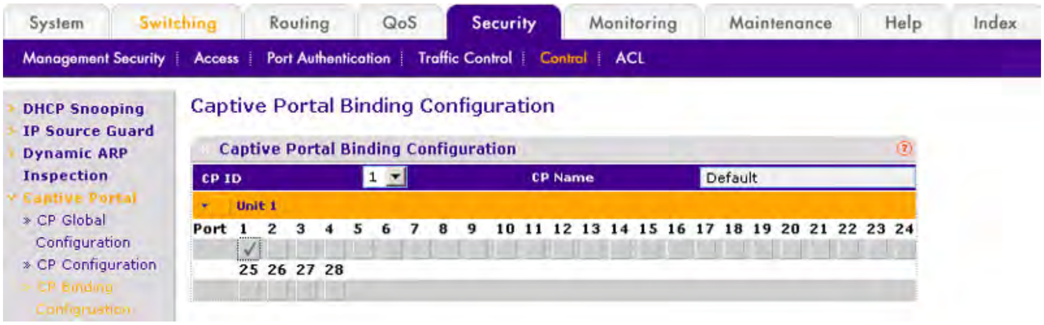
b. Under Captive Portal Configuration, scroll down to CP ID 1 and select the **CP 1** checkbox. Now CP 1appears in the CP ID field at the top.

c. In the Captive Portal Configuration, select **Enable** in the Admin Mode field.

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

3. Enable CP 1 on the interface 1/0/1.

a. From the main menu, select Security > Controls >Captive Portal > CP Binding Configuration. A screen similar to the following displays.



Captive Portal Binding Configuration

Captive Portal Binding Configuration

CP ID 1 CP Name Default

Unit 1

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

Figure 32-3

b. Select **1** from the CP ID field.

c. Click the Unit 1. The Ports display.

d. Click the gray box under port 1.

e. Click **Apply**.

Client Access, Authentication, and Control

User verification can be configured to allow access for guest users; users that do not have assigned user names and passwords. User verification can also be configured to allow access for authenticated users. Authenticated users are required to enter a valid user name and password that must first be validated against the local database or a RADIUS server. Network access is granted once user verification has been confirmed. The administrator can block access to a captive portal configuration. When an instance is blocked no client traffic is allowed through any interfaces associated with that captive portal configuration. Blocking a captive portal instance is a temporary command executed by the administrator and not saved in the configuration.

Block a Captive Portal Instance

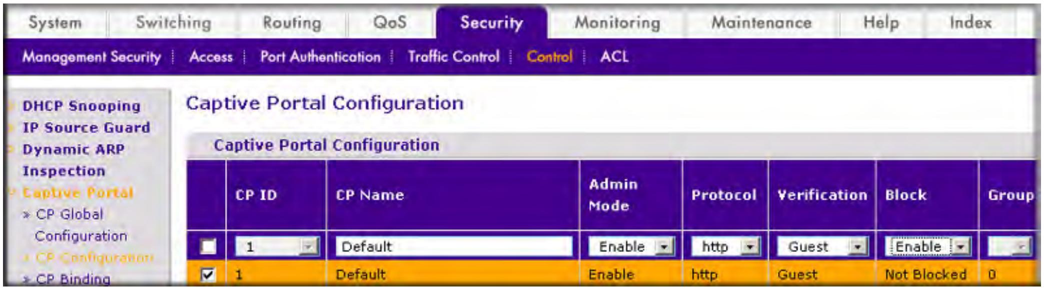
CLI: Blocking a Captive Portal Instance

```
(Netgear Switch )(Config-CP 1)#block
```

GUI: Blocking a Captive Portal Instance

To use the Web interface to block a captive portal instance, proceed as follows:

1. From the main menu, select Security > Control >Captive Portal> CP Configuration. A screen similar to the following displays.



Captive Portal Configuration

Captive Portal Configuration

	CP ID	CP Name	Admin Mode	Protocol	Verification	Block	Group
□	1	Default	Enable	http	Guest	Enable	
☑	1	Default	Enable	http	Guest	Not Blocked	0

Figure 32-4

2. Under Captive Portal Configuration, scroll down to CP ID 1 and select the **CP 1** checkbox. Now CP 1 appears in the CP ID field at the top.
3. In the Captive Portal Configuration, select **Enable** in the Block field.
4. Click **Apply** to save the settings.

Local Authorization User/Group Configuration

When using Local authentication, the administrator provides user identities for Captive Portal by adding unique user names and passwords to the Local User Database. This configuration is global to the captive portal component and can contain up to 128 user entries (a RADIUS server should be used if more users are required). A local user may belong to one or more groups. There is one group created by default with the group name “Default” to which all new users are assigned. All new captive portal instances are also assigned to the “Default” group. The administrator can create new groups and modify the user/group association to only allow a subset of users access to a specific captive portal instance. Network access is granted upon successful user name, password and group verification.

CLI: Creating Users and Groups

Create a group whose group ID is 2.

```
(Netgear Switch) #config
(Netgear Switch) (config)#captive-portal
(Netgear Switch )(Config-CP)# user group 2
```

Create a user whose name is user1.

```
(Netgear Switch) (Config-CP)#user 2 name user1
```

Configure the user’s password.

```
(Netgear Switch) (Config-CP)#user 2 password
Enter password (8 to 64 characters): 12345678
Re-enter password: 12345678
```

Add the user to the group.

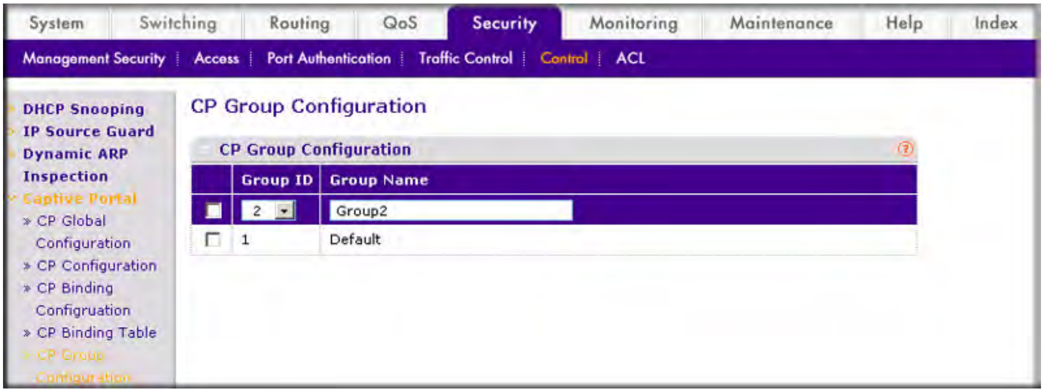
```
(Netgear Switch) (Config-CP)#user 2 group 2
```

Web Interface: Creating Users and Groups

To use the Web interface to create users and groups, proceed as follows:

1. Create a group.

a. From the main menu, select Security > Control >Captive Portal > CP Group Configuration. A screen similar to the following displays.



CP Group Configuration

CP Group Configuration

	Group ID	Group Name
□	2	Group2
□	1	Default

Figure 32-5

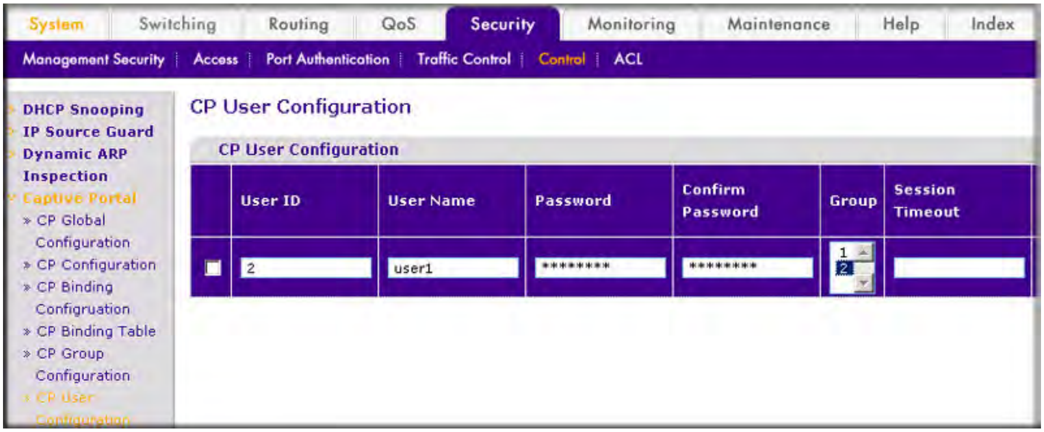
b. Enter the following information in the CP Group Configuration.

- Select **2** from the Group ID field.
- Enter **Group2** in the Group Name field.

c. Click **Add**.

2. Create an user.

a. From the main menu, select Security > Control >Captive Portal > CP User Configuration. A screen similar to the following displays.



CP User Configuration

CP User Configuration

	User ID	User Name	Password	Confirm Password	Group	Session Timeout
□	2	user1	********	********	1 2	

Figure 32-6

b. Enter the following information in the CP User Configuration.

- In the User ID Field, enter **2**.
- In the User Name field, enter **user1**.
- In the Password field, enter **12345678**.
- In the Confirm Password field, enter **12345678**.
- In the Group field, select **2**.

c. Click **Add**.

Remote Authorization (RADIUS) User Configuration

A remote RADIUS server can be used for client authentication. The RADIUS authentication and accounting servers are configured in 8.0 separate from the captive portal configuration. In order to perform authentication/accounting via RADIUS, the administrator configures one or more RADIUS servers and then references the server(s) using their name in the captive portal configuration, each captive portal instance can be assigned one RADIUS authentication server and one RADIUS accounting server.

If RADIUS is enabled for a captive portal configuration and no RADIUS servers are assigned, the captive portal activation status will indicate the instance is disabled with an appropriate reason code.

The following table indicates the RADIUS attributes that are used to configure captive portal users. The table indicates both RADIUS attributes and vendor specific attributes (VSA) that are used to configure Captive Portal. VSAs are denoted in the id column and are comma delimited (vendor id, attribute id).

Table 32-1. RADIUS Attributes for Configuring Captive Portal Users

RADIUS Attribute	No.	Description	Range	Usage	Default
User-Name	1	User name to be authorized	1-32 characters	Required	None
User-Password	2	User password	8-64 characters	Required	None
Session-Timeout	27	Logout once session timeout is reached (seconds). If the attribute is 0 or not present then use the value configured for the captive portal.	Integer (seconds)	Optional	0
Idle-Timeout	28	Logout once idle timeout is reached (seconds). If the attribute is 0 or not present then use the value configured for the captive portal.	Integer (seconds)	Optional	0

Table 32-1. RADIUS Attributes for Configuring Captive Portal Users (continued)

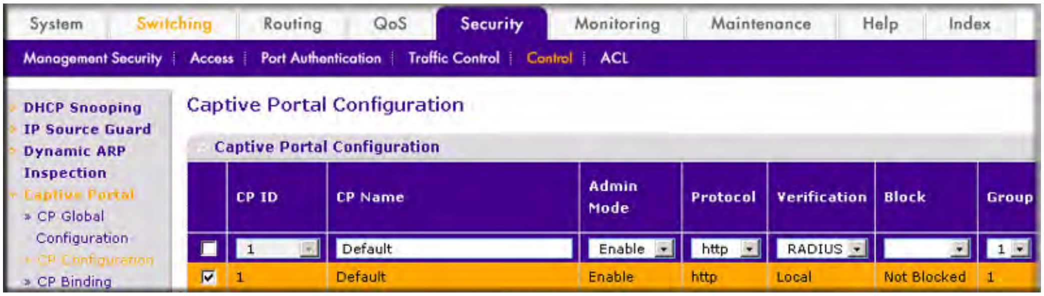
RADIUS Attribute	No.	Description	Range	Usage	Default
WISPr-Max-Bandwidth-Up	14122, 7	Maximum client transmit rate (b/s). Limits the bandwidth at which the client can send data into the network. If the attribute is 0 or not present then use the value configured for the captive portal.	Integer	Optional	0
WISPr-Max-Bandwidth-Down	14122, 8	Maximum client receive rate (b/s). Limits the bandwidth at which the client can receive data from the network. If the attribute is 0 or not present then use the value configured for the captive portal.	Integer	Optional	0

CLI: Configuiring RADIUS as the Verification Mode

```
(Netgear Switch ) (Config-CP 1)#radius-auth-server Default-RADIUS-Server
(Netgear Switch ) (Config-CP 1)#verification radius
```

Web Interface: Configuring RADIUS as the Verification Mode

1. From the main menu, select Security > Control >Captive Portal> CP Configuration. A screen similar to the following displays.



Captive Portal Configuration

Captive Portal Configuration

	CP ID	CP Name	Admin Mode	Protocol	Verification	Block	Group
□	1	Default	Enable	http	RADIUS		1
☑	1	Default	Enable	http	Local	Not Blocked	1

Figure 32-7

2. Under Captive Portal Configuration, scroll down to CP ID 1 and select the **CP 1** checkbox. Now CP 1 appears in the CP ID field at the top.

3. Enter the following information in the Captive Portal Configuration.
   - Select **RADIUS** from the Verification field.
   - In the Radius Auth Server field, enter the radius server name **Default-RADIUS-Server**.

4. Click **Apply**.

SSL Certificates

A Captive Portal instance can be configured to use the HTTPS protocol during its user verification process. The connection method for HTTPS uses the Secure Sockets Layer (SSL) protocol which requires a certificate to provide encryption. The certificate is presented to the user at connection time.

The Captive Portal uses the same certificate that is used by 8.0 for Secure HTTP connections. This certificate can be generated by the administrator using a CLI command. If a captive portal instance is configured for the HTTPS protocol and there is not a valid certificate present on the system, the captive portal instance status will show Disabled with an appropriate reason code.

Index