



IP Internetworking Lab Manual

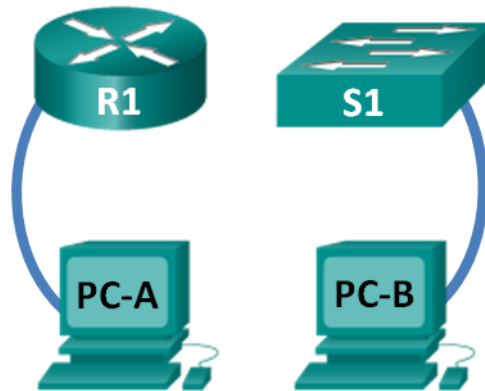
BSc (Hons) Cloud Computing
School of Applied Computing
Faculty of Architecture, Computing and Engineering
University of Wales Trinity St David
Swansea.



2015-2016
Module Code: ACCC4007
Module Leader
Mr Ethan Court

1 - Initializing and Reloading a Router and Switch

Topology



Objectives

Part 1: Set Up Devices in the Network as Shown in the Topology

Part 2: Initialize the Router and Reload

Part 3: Initialize the Switch and Reload

Background / Scenario

Before starting a CCNA hands-on lab that makes use of either a Cisco router or switch, ensure that the devices in use have been erased and have no startup configurations present. Otherwise, the results of your lab may be unpredictable. This lab provides a detail procedure for initializing and reloading a Cisco router and a Cisco switch.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS software, Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports

Part 1: Set Up Devices in the Network as Shown in the Topology

Step 1: Cable the network as shown in the topology.

Attach console cables to the devices shown in the topology diagram.

Step 2: Power on all the devices in the topology.

Wait for all devices to finish the software load process before moving to Part 2.

Part 2: Initialize the Router and Reload

Step 1: Connect to the router.

Console into the router and enter privileged EXEC mode using the **enable** command.

```
Router> enable
Router#
```

Step 2: Erase the startup configuration file from NVRAM.

Type the **erase startup-config** command to remove the startup configuration from nonvolatile random-access memory (NVRAM).

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

Step 3: Reload the router.

Issue the **reload** command to remove an old configuration from memory. When prompted to Proceed with reload, press Enter to confirm the reload. Pressing any other key will abort the reload.

```
Router# reload
Proceed with reload? [confirm]
```

```
*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

Note: You may receive a prompt to save the running configuration prior to reloading the router. Respond by typing **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

Step 4: Bypass the initial configuration dialog.

After the router reloads, you are prompted to enter the initial configuration dialog. Enter **no** and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Step 5: Terminate the autoinstall program.

You will be prompted to terminate the autoinstall program. Respond **yes** and then press Enter.

```
Would you like to terminate autoinstall? [yes]: yes
Router>
```

Part 3: Initialize the Switch and Reload

Step 1: Connect to the switch.

Console into the switch and enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Step 2: Determine if there have been any virtual local-area networks (VLANs) created.

Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash

Directory of flash:/

   2  -rwx           1919   Mar 1 1993 00:06:33 +00:00 private-config.text
   3  -rwx           1632   Mar 1 1993 00:06:33 +00:00 config.text
   4  -rwx          13336   Mar 1 1993 00:06:33 +00:00 multiple-fs
   5  -rwx        11607161   Mar 1 1993 02:37:06 +00:00 c2960-lanbasek9-mz.150-2.SE.bin
   6  -rwx           616    Mar 1 1993 00:07:13 +00:00 vlan.dat

32514048 bytes total (20886528 bytes free)
Switch#
```

Step 3: Delete the VLAN file.

- a. If the **vlan.dat** file was found in flash, then delete this file.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

You will be prompted to verify the file name. At this point, you can change the file name or just press Enter if you have entered the name correctly.

- b. When you are prompted to delete this file, press Enter to confirm the deletion. (Pressing any other key will abort the deletion.)

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

Step 4: Erase the startup configuration file.

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. When you are prompted to remove the configuration file, press Enter to confirm the erase. (Pressing any other key will abort the operation.)

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

Step 5: Reload the switch.

Reload the switch to remove any old configuration information from memory. When you are prompted to reload the switch, press Enter to proceed with the reload. (Pressing any other key will abort the reload.)

```
Switch# reload
Proceed with reload? [confirm]
```

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Type **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

Step 6: Bypass the initial configuration dialog.

After the switch reloads, you should see a prompt to enter the initial configuration dialog. Type **no** at the prompt and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```

Reflection

1. Why is it necessary to erase the startup configuration before reloading the router?

2. You find a couple configurations issues after saving the running configuration to the startup configuration, so you make the necessary changes to fix those issues. If you were to reload the device now, what configuration would be restored to the device after the reload?

2 - Installing the IPv6 Protocol and Assigning Host Addresses with Windows XP

Objectives

Part 1: Install the IPv6 Protocol on a Windows XP PC

- Install the IPv6 protocol.
- Examine IPv6 address information.

Part 2: Use the Network Shell (netsh) Utility

- Work inside the **netsh** utility.
- Configure a static IPv6 address on the local-area network (LAN) interface.
- Exit the **netsh** utility.
- Display IPv6 address information using **netsh**.
- Issue **netsh** instructions from the command prompt.

Background / Scenario

The Internet Protocol Version 6 (IPv6) is not enabled by default in Windows XP. Windows XP includes IPv6 implementation, but the IPv6 protocol must be installed. XP does not provide a way to configure IPv6 static addresses from the Graphical User Interface (GUI), so all IPv6 static address assignments must be done using the Network Shell (**netsh**) utility.

In this lab, you will install the IPv6 protocol on a Windows XP PC. You will then assign a static IPv6 address to the LAN interface.

Required Resources

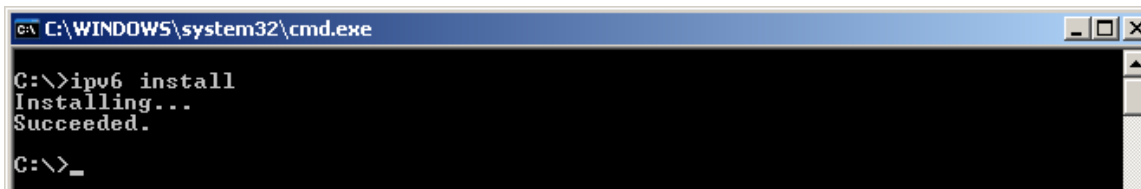
1 Windows XP PC

Part 1: Install the IPv6 Protocol on a Windows XP PC

In Part 1, you will install the IPv6 protocol on a PC running Windows XP. You will also use two commands to view the IPv6 addresses assigned to the PC.

Step 1: Install the IPv6 protocol.

From the command prompt window, type **ipv6 install** to install the IPv6 protocol.



```
C:\WINDOWS\system32\cmd.exe
C:\>ipv6 install
Installing...
Succeeded.
C:\>_
```

Step 2: Examine IPv6 Address Information.

Use the **ipconfig /all** command to view IPv6 address information.

```
C:\WINDOWS\system32\cmd.exe

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : VMware Accelerated AMD PCNet Adapter
    Physical Address. . . . . : 00-50-56-BE-25-87
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Autoconfiguration IP Address. . . : 169.254.39.128
    Subnet Mask . . . . . : 255.255.0.0
    IP Address. . . . . : fe80::250:56ff:febe:2587%5
    Default Gateway . . . . . : 
    DNS Servers . . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : Teredo Tunneling Pseudo-Interface
    Physical Address. . . . . : FF-FF-FF-FF-FF-FF-FF-FF
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : fe80::ffff:ffff:ffffd%4
    Default Gateway . . . . . : 
    NetBIOS over Tcpip. . . . . : Disabled

Tunnel adapter Automatic Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : Automatic Tunneling Pseudo-Interface
    Physical Address. . . . . : A9-FE-27-80
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : fe80::5efe:169.254.39.128%2
    Default Gateway . . . . . : 
    DNS Servers . . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1
    NetBIOS over Tcpip. . . . . : Disabled

C:\>
```

Part 2: Use the Network Shell (netsh) Utility

Network Shell (**netsh**) is a command-line utility included with Windows XP and newer Windows operating systems, such as Vista and Windows 7. It allows you to configure the IPv6 address information on your LAN. In Part 2, you will use the **netsh** utility to configure static IPv6 address information on a Windows XP PC LAN interface. You will also use the **netsh** utility to display the PC LAN interface IPv6 address information.

Step 1: Work inside the Network Shell utility.

- From the command prompt window, type **netsh** and press Enter to start the **netsh** utility. The command prompt changes from **C:\>** to **netsh>**.

```
C:\WINDOWS\system32\cmd.exe - netsh

C:\>netsh
netsh>
```

- At the prompt, enter a question mark (?) and press Enter to provide the list of available parameters.

```

netsh>?

The following commands are available:

Commands in this context:
..          - Goes up one context level.
?          - Displays a list of commands.
abort      - Discards changes made while in offline mode.
add        - Adds a configuration entry to a list of entries.
alias      - Adds an alias.
bridge     - Changes to the 'netsh bridge' context.
bye        - Exits the program.
commit     - Commits changes made while in offline mode.
delete     - Deletes a configuration entry from a list of entries.
diag       - Changes to the 'netsh diag' context.
dump       - Displays a configuration script.
exec       - Runs a script file.
exit       - Exits the program.
firewall   - Changes to the 'netsh firewall' context.
help       - Displays a list of commands.
interface  - Changes to the 'netsh interface' context.
lan        - Changes to the 'netsh lan' context.
nap        - Changes to the 'netsh nap' context.
offline    - Sets the current mode to offline.
online     - Sets the current mode to online.
popd       - Pops a context from the stack.
pushd      - Pushes current context on stack.
quit       - Exits the program.
ras        - Changes to the 'netsh ras' context.
routing    - Changes to the 'netsh routing' context.
set        - Updates configuration settings.
show       - Displays information.
unalias    - Deletes an alias.
winsock    - Changes to the 'netsh winsock' context.

The following sub-contexts are available:
bridge diag firewall interface lan nap ras routing winsock

To view help for a command, type the command, followed by a space, and then
type ?.

netsh>

```

- c. Type **interface ?** and press Enter to provide the list of interface commands.

```

netsh>interface ?

The following commands are available:

Commands in this context:
?          - Displays a list of commands.
add        - Adds a configuration entry to a table.
delete     - Deletes a configuration entry from a table.
dump       - Displays a configuration script.
help       - Displays a list of commands.
ip         - Changes to the 'netsh interface ip' context.
ipv6       - Changes to the 'netsh interface ipv6' context.
portproxy  - Changes to the 'netsh interface portproxy' context.
reset      - Resets information.
set        - Sets configuration information.
show       - Displays information.

The following sub-contexts are available:
ip ipv6 portproxy

To view help for a command, type the command, followed by a space, and then
type ?.

netsh>_

```

Note: You can use the question mark (?) at any level in the **netsh** utility to list the available options. The up arrow can be used to scroll through previous **netsh** commands. The **netsh** utility also allows you to abbreviate commands, as long as the abbreviation is unique.

Step 2: Configure a static IPv6 address on the LAN interface.

To add a static IPv6 address to the LAN interface, issue the **interface ipv6 add address** command from inside the **netsh** utility.

```
netsh>interface ipv6 add address "Local Area Connection" 2001:db8:acad:a::3
Ok.
netsh>
```

Step 3: Display IPv6 address information using the netsh utility.

You can display IPv6 address information using the **interface ipv6 show address** command.

```
netsh>interface ipv6 show address
Querying active state...

Interface 5: Local Area Connection
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Manual     Preferred  infinite   infinite    2001:db8:acad:a::3
Link       Preferred  infinite   infinite    fe80::250:56ff:febe:2587

Interface 4: Teredo Tunneling Pseudo-Interface
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Link       Preferred  infinite   infinite    fe80::ffff:ffff:fffd

Interface 2: Automatic Tunneling Pseudo-Interface
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Link       Preferred  infinite   infinite    fe80::5efe:169.254.39.128

Interface 1: Loopback Pseudo-Interface
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Loopback   Preferred  infinite   infinite    ::1
Link       Preferred  infinite   infinite    fe80::1

netsh>
```

Step 4: Exit the netsh utility.

Use the **exit** command to exit from the **netsh** utility.

```
netsh>exit

C:\>
```

Step 5: Issue netsh instructions from the command prompt.

All **netsh** instructions can be entered from the command prompt, outside the **netsh** utility, by preceding the instruction with the **netsh** command.

```
C:\>netsh interface ipv6 show address
Querying active state...

Interface 5: Local Area Connection
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Manual      Preferred  infinite   infinite    2001:db8:acad:a::3
Link        Preferred  infinite   infinite    fe80::250:56ff:febe:2587

Interface 4: Teredo Tunneling Pseudo-Interface
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Link        Preferred  infinite   infinite    fe80::ffff:ffff:fffd

Interface 2: Automatic Tunneling Pseudo-Interface
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Link        Preferred  infinite   infinite    fe80::5efe:169.254.39.128

Interface 1: Loopback Pseudo-Interface
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Loopback    Preferred  infinite   infinite    ::1
Link        Preferred  infinite   infinite    fe80::1

C:\>
```

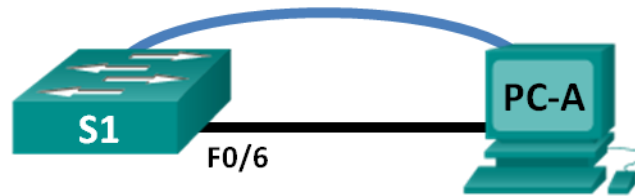
Reflection

1. How would you renew your LAN interface address information from the **netsh** utility?

Hint: Use the question mark (?) for help in obtaining the parameter sequence.

3 – Configuring Basic Switch Settings

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objectives

Part 1: Cable the Network and Verify the Default Switch Configuration

Part 2: Configure Basic Network Device Settings

- Configure basic switch settings.
- Configure the PC IP address.

Part 3: Verify and Test Network Connectivity

- Display device configuration.
- Test end-to-end connectivity with ping.
- Test remote management capabilities with Telnet.
- Save the switch running configuration file.

Part 4: Manage the MAC Address Table

- Record the MAC address of the host.
- Determine the MAC addresses that the switch has learned.
- List the **show mac address-table** command options.
- Set up a static MAC address.

Background / Scenario

Cisco switches can be configured with a special IP address known as Switched Virtual Interface (SVI). The SVI or management address can be used for remote access to the switch to display or configure settings. If the VLAN 1 SVI is assigned an IP address, by default, all ports in VLAN 1 have access to the SVI management IP address.

In this lab, you will build a simple topology using Ethernet LAN cabling and access a Cisco switch using the console and remote access methods. You will examine default switch configurations before configuring basic switch settings. These basic switch settings include device name, interface description, local passwords, message of the day (MOTD) banner, IP addressing, setting up a static MAC address, and demonstrating the

use of a management IP address for remote switch management. The topology consists of one switch and one host using only Ethernet and console ports.

Note: The switch used is a Cisco Catalyst 2960 with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Note: Make sure that the switch has been erased and has no startup configuration. Refer to Appendix A for the procedures to initialize and reload devices.

Required Resources

- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term, and Telnet capability)
- Console cable to configure the Cisco IOS device via the console port
- Ethernet cable as shown in the topology

Part 1: Cable the Network and Verify the Default Switch Configuration

In Part 1, you will set up the network topology and verify default switch settings.

Step 1: Cable the network as shown in the topology.

- a. Cable the console connection as shown in the topology. Do not connect the PC-A Ethernet cable at this time.

Note: If you are using Netlab, you can shut down F0/6 on S1 which has the same effect as not connecting PC-A to S1.

- b. Create a console connection to the switch from PC-A using Tera Term or other terminal emulation program.

Why must you use a console connection to initially configure the switch? Why is it not possible to connect to the switch via Telnet or SSH?

Step 2: Verify the default switch configuration.

In this step, you will examine the default switch settings, such as current switch configuration, IOS information, interface properties, VLAN information, and flash memory.

You can access all the switch IOS commands in privileged EXEC mode. Access to privileged EXEC mode should be restricted by password protection to prevent unauthorized use because it provides direct access to global configuration mode and commands used to configure operating parameters. You will set passwords later in this lab.

The privileged EXEC mode command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes is gained. Use the **enable** command to enter privileged EXEC mode.

- a. Assuming the switch had no configuration file stored in nonvolatile random-access memory (NVRAM), you will be at the user EXEC mode prompt on the switch with a prompt of Switch>. Use the **enable** command to enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Notice that the prompt changed in the configuration to reflect privileged EXEC mode.

Verify a clean configuration file with the **show running-config** privileged EXEC mode command. If a configuration file was previously saved, it must be removed. Depending on switch model and IOS version, your configuration may look slightly different. However, there should be no configured passwords or IP address. If your switch does not have a default configuration, erase and reload the switch.

Note: Appendix A details the steps to initialize and reload the devices.

- b. Examine the current running configuration file.

```
Switch# show running-config
```

How many FastEthernet interfaces does a 2960 switch have? _____

How many Gigabit Ethernet interfaces does a 2960 switch have? _____

What is the range of values shown for the vty lines? _____

- c. Examine the startup configuration file in NVRAM.

```
Switch# show startup-config
```

```
startup-config is not present
```

Why does this message appear? _____

- d. Examine the characteristics of the SVI for VLAN 1.

```
Switch# show interface vlan1
```

Is there an IP address assigned to VLAN 1? _____

What is the MAC address of this SVI? Answers will vary. _____

Is this interface up?

- e. Examine the IP properties of the SVI VLAN 1.

```
Switch# show ip interface vlan1
```

What output do you see?

- f. Connect PC-A Ethernet cable to port 6 on the switch and examine the IP properties of the SVI VLAN 1. Allow time for the switch and PC to negotiate duplex and speed parameters.

Note: If you are using Netlab, enable interface F0/6 on S1.

```
Switch# show ip interface vlan1
```

What output do you see?

- g. Examine the Cisco IOS version information of the switch.

```
Switch# show version
```

What is the Cisco IOS version that the switch is running? _____

What is the system image filename? _____

What is the base MAC address of this switch? Answers will vary.

- h. Examine the default properties of the FastEthernet interface used by PC-A.

```
Switch# show interface f0/6
```

Is the interface up or down? _____

What event would make an interface go up? _____

What is the MAC address of the interface? _____

What is the speed and duplex setting of the interface? _____

- i. Examine the default VLAN settings of the switch.

```
Switch# show vlan
```

What is the default name of VLAN 1? _____

Which ports are in this VLAN? _____

Is VLAN 1 active? _____

What type of VLAN is the default VLAN? _____

- j. Examine flash memory.

Issue one of the following commands to examine the contents of the flash directory.

```
Switch# show flash
```

```
Switch# dir flash:
```

Files have a file extension, such as .bin, at the end of the filename. Directories do not have a file extension.

What is the filename of the Cisco IOS image? _____

Part 2: Configure Basic Network Device Settings

In Part 2, you configure basic settings for the switch and PC.

Step 1: Configure basic switch settings including hostname, local passwords, MOTD banner, management address, and Telnet access.

In this step, you will configure the PC and basic switch settings, such as hostname and an IP address for the switch management SVI. Assigning an IP address on the switch is only the first step. As the network administrator, you must specify how the switch is managed. Telnet and SSH are the two most common management methods. However, Telnet is not a secure protocol. All information flowing between the two devices is sent in plain text. Passwords and other sensitive information can be easily looked at if captured by a packet sniffer.

- a. Assuming the switch had no configuration file stored in NVRAM, verify you are at privileged EXEC mode. Enter **enable** if the prompt has changed back to Switch>.

```
Switch> enable
```

```
Switch#
```

- b. Enter global configuration mode.

```
Switch# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)#
```

The prompt changed again to reflect global configuration mode.

- c. Assign the switch hostname.

```
Switch(config)# hostname S1
S1(config)#
```

- d. Configure password encryption.

```
S1(config)# service password-encryption
S1(config)#
```

- e. Assign **class** as the secret password for privileged EXEC mode access.

```
S1(config)# enable secret class
S1(config)#
```

- f. Prevent unwanted DNS lookups.

```
S1(config)# no ip domain-lookup
S1(config)#
```

- g. Configure a MOTD banner.

```
S1(config)# banner motd #
Enter Text message. End with the character '#'.
Unauthorized access is strictly prohibited. #
```

- h. Verify your access settings by moving between modes.

```
S1(config)# exit
S1#
*Mar  1 00:19:19.490: %SYS-5-CONFIG_I: Configured from console by console
S1# exit
S1 con0 is now available
```

Press RETURN to get started.

```
Unauthorized access is strictly prohibited.
S1>
```

Which shortcut keys are used to go directly from global configuration mode to privileged EXEC mode?

-
- i. Go back to privileged EXEC mode from user EXEC mode. Enter **class** as the password when prompted.

```
S1> enable
Password:
S1#
```

Note: The password does not display when entering.

- j. Enter global configuration mode to set the SVI IP address of the switch. This allows remote management of the switch.

Before you can manage S1 remotely from PC-A, you must assign the switch an IP address. The default configuration on the switch is to have the management of the switch controlled through VLAN 1. However, a best practice for basic switch configuration is to change the management VLAN to a VLAN other than VLAN 1.

For management purposes, use VLAN 99. The selection of VLAN 99 is arbitrary and in no way implies that you should always use VLAN 99.

First, create the new VLAN 99 on the switch. Then set the IP address of the switch to 192.168.1.2 with a subnet mask of 255.255.255.0 on the internal virtual interface VLAN 99.

```
S1# configure terminal
S1(config)# vlan 99
S1(config-vlan)# exit
S1(config)# interface vlan99
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)#
```

Notice that the VLAN 99 interface is in the down state even though you entered the **no shutdown** command. The interface is currently down because no switch ports are assigned to VLAN 99.

- k. Assign all user ports to VLAN 99.

```
S1(config)# interface range f0/1 - 24,g0/1 - 2
S1(config-if-range)# switchport access vlan 99
S1(config-if-range)# exit
S1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

To establish connectivity between the host and the switch, the ports used by the host must be in the same VLAN as the switch. Notice in the above output that the VLAN 1 interface goes down because none of the ports are assigned to VLAN 1. After a few seconds, VLAN 99 comes up because at least one active port (F0/6 with PC-A attached) is now assigned to VLAN 99.

- l. Issue **show vlan brief** command to verify that all the user ports are in VLAN 99.

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	
99	VLAN0099	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

- m. Configure the IP default gateway for S1. If no default gateway is set, the switch cannot be managed from a remote network that is more than one router away. It does respond to pings from a remote network. Although this activity does not include an external IP gateway, assume that you will eventually connect the LAN to a router for external access. Assuming that the LAN interface on the router is 192.168.1.1, set the default gateway for the switch.

```
S1(config)# ip default-gateway 192.168.1.1
S1(config)#
```

- n. Console port access should also be restricted. The default configuration is to allow all console connections with no password needed. To prevent console messages from interrupting commands, use the **logging synchronous** option.

```
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# logging synchronous
S1(config-line)# exit
S1(config)#
```

- o. Configure the virtual terminal (vty) lines for the switch to allow Telnet access. If you do not configure a vty password, you are unable to telnet to the switch.

```
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
S1#
```

```
*Mar  1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console
```

Why is the **login** command required? _____

Step 2: Configure an IP address on PC-A.

Assign the IP address and subnet mask to the PC as shown in the Addressing Table. An abbreviated version of the procedure is described here. A default gateway is not required for this topology; however, you can enter **192.168.1.1** to simulate a router attached to S1.

- 1) Click the Windows **Start** icon > **Control Panel**.
- 2) Click **View By:** and choose **Small icons**.
- 3) Choose **Network and Sharing Center** > **Change adapter settings**.
- 4) Select **Local Area Network Connection**, right click and choose **Properties**.
- 5) Choose **Internet Protocol Version 4 (TCP/IPv4)** > **Properties**.
- 6) Click the **Use the following IP address** radio button and enter the IP address and subnet mask.

Part 3: Verify and Test Network Connectivity

In Part 3, you will verify and document the switch configuration, test end-to-end connectivity between PC-A and S1, and test the switch's remote management capability.

Step 1: Display the switch configuration.

From your console connection on PC-A, display and verify your switch configuration. The **show run** command displays the entire running configuration, one page at a time. Use the spacebar to advance paging.

- a. A sample configuration displays here. The settings you configured are highlighted in yellow. The other configuration settings are IOS defaults.

```
S1# show run
```

```
Building configuration...
```

```
Current configuration : 2206 bytes
```

```
!
```

```
version 15.0
```

```
no service pad
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
service password-encryption
```

```
!
```

```
hostname S1
```

```
!
```

```
boot-start-marker
```

```
boot-end-marker
```

```
!
```

```
enable secret 4 06YFDUHH6lwAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
```

```
!
```

```
no aaa new-model
```

```
system mtu routing 1500
```

```
!
```

```
!
```

```
no ip domain-lookup
```

```
!
```

```
<output omitted>
```

```
!
```

```
interface FastEthernet0/24
```

```
switchport access vlan 99
```

```
!
```

```
interface GigabitEthernet0/1
```

```
!
```

```
interface GigabitEthernet0/2
```

```
!
```

```
interface Vlan1
```

```
no ip address
```

```
no ip route-cache
```

```
!
```

```
interface Vlan99
```

```
ip address 192.168.1.2 255.255.255.0
```

```
no ip route-cache
```

```
!
```

```
ip default-gateway 192.168.1.1
```

```
ip http server
```

```
ip http secure-server
```

```
!
```

```
banner motd ^C
```

```
Unauthorized access is strictly prohibited. ^C
```

```

!
line con 0
password 7 104D000A0618
logging synchronous
login
line vty 0 4
password 7 14141B180F0B
login
line vty 5 15
password 7 14141B180F0B
login
!
end

```

S1#

- b. Verify the management VLAN 99 settings.

S1# **show interface vlan 99**

```

Vlan99 is up, line protocol is up
  Hardware is EtherSVI, address is 0cd9.96e2.3d41 (bia 0cd9.96e2.3d41)
  Internet address is 192.168.1.2/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:06, output 00:08:45, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    175 packets input, 22989 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    1 packets output, 64 bytes, 0 underruns
    0 output errors, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out

```

What is the bandwidth on this interface? _____

What is the VLAN 99 state? _____

What is the line protocol state? _____

Step 2: Test end-to-end connectivity with ping.

- a. From the command prompt on PC-A, ping your own PC-A address first.

```
C:\Users\User1> ping 192.168.1.10
```

- b. From the command prompt on PC-A, ping the SVI management address of S1.

```
C:\Users\User1> ping 192.168.1.2
```

Because PC-A needs to resolve the MAC address of S1 through ARP, the first packet may time out. If ping results continue to be unsuccessful, troubleshoot the basic device configurations. You should check both the physical cabling and logical addressing if necessary.

Step 3: Test and verify remote management of S1.

You will now use Telnet to remotely access the switch. In this lab, PC-A and S1 reside side by side. In a production network, the switch could be in a wiring closet on the top floor while your management PC is located on the ground floor. In this step, you will use Telnet to remotely access switch S1 using its SVI management address. Telnet is not a secure protocol; however, you will use it to test remote access. With Telnet, all information, including passwords and commands, are sent across the session in plain text. In subsequent labs, you will use SSH to remotely access network devices.

Note: If you are using Windows 7, the administrator may need to enable the Telnet protocol. To install the Telnet client, open a cmd window and type **pkgmgr /iu:"TelnetClient"**. An example is shown below.

```
C:\Users\User1> pkgmgr /iu:"TelnetClient"
```

- a. With the cmd window still open on PC-A, issue a Telnet command to connect to S1 via the SVI management address. The password is **cisco**.

```
C:\Users\User1> telnet 192.168.1.2
```

- b. After entering the password **cisco**, you will be at the user EXEC mode prompt. Access privileged EXEC mode.
- c. Type **exit** to end the Telnet session.

Step 4: Save the switch running configuration file.

Save the configuration.

```
S1# copy running-config startup-config
Destination filename [startup-config]? [Enter]
Building configuration...
[OK]
S1#
```

Part 4: Manage the MAC Address Table

In Part 4, you will determine the MAC address that the switch has learned, set up a static MAC address on one interface of the switch, and then remove the static MAC address from that interface.

Step 1: Record the MAC address of the host.

From a command prompt on PC-A, issue **ipconfig /all** command to determine and record the Layer 2 (physical) addresses of the PC NIC.

Step 2: Determine the MAC addresses that the switch has learned.

Display the MAC addresses using the **show mac address-table** command.

```
S1# show mac address-table
```

How many dynamic addresses are there? _____

How many MAC addresses are there in total? _____

Does the dynamic MAC address match the PC-A MAC address? _____

Step 3: List the show mac address-table options.

- a. Display the MAC address table options.

```
S1# show mac address-table ?
```

How many options are available for the **show mac address-table** command? _____

- b. Issue the **show mac address-table dynamic** command to display only the MAC addresses that were learned dynamically.

```
S1# show mac address-table dynamic
```

How many dynamic addresses are there? _____

- c. View the MAC address entry for PC-A. The MAC address formatting for the command is xxxx.xxxx.xxxx.

```
S1# show mac address-table address <PC-A MAC here>
```

Step 4: Set up a static MAC address.

- a. Clear the MAC address table.

To remove the existing MAC addresses, use the **clear mac address-table** command from privileged EXEC mode.

```
S1# clear mac address-table dynamic
```

- b. Verify that the MAC address table was cleared.

```
S1# show mac address-table
```

How many static MAC addresses are there? _____

How many dynamic addresses are there? _____

- c. Examine the MAC table again.

More than likely, an application running on your PC has already sent a frame out the NIC to S1. Look at the MAC address table again in privileged EXEC mode to see if S1 has relearned the MAC address for PC-A.

```
S1# show mac address-table
```

How many dynamic addresses are there? _____

Why did this change from the last display? _____

If S1 has not yet relearned the MAC address for PC-A, ping the VLAN 99 IP address of the switch from PC-A, and then repeat the **show mac address-table** command.

- d. Set up a static MAC address.

To specify which ports a host can connect to, one option is to create a static mapping of the host MAC address to a port.

Set up a static MAC address on F0/6 using the address that was recorded for PC-A in Part 4, Step 1. The MAC address 0050.56BE.6C89 is used as an example only. You must use the MAC address of your PC-A, which is different than the one given here as an example.

```
S1(config)# mac address-table static 0050.56BE.6C89 vlan 99 interface  
fastethernet 0/6
```

- e. Verify the MAC address table entries.

```
S1# show mac address-table
```

How many total MAC addresses are there? _____

How many static addresses are there? _____

- f. Remove the static MAC entry. Enter global configuration mode and remove the command by putting a **no** in front of the command string.

Note: The MAC address 0050.56BE.6C89 is used in the example only. Use the MAC address for your PC-A.

```
S1(config)# no mac address-table static 0050.56BE.6C89 vlan 99 interface
fastethernet 0/6
```

- g. Verify that the static MAC address has been cleared.

```
S1# show mac address-table
```

How many total static MAC addresses are there? _____

Reflection

1. Why should you configure the vty lines for the switch?

2. Why change the default VLAN 1 to a different VLAN number?

3. How can you prevent passwords from being sent in plain text?

4. Why configure a static MAC address on a port interface?

Appendix A: Initializing and Reloading a Router and Switch

Step 1: Initialize and reload the router.

- a. Console into the router and enable privileged EXEC mode.

```
Router> enable
```

```
Router#
```

- b. Enter the **erase startup-config** command to remove the startup configuration from NVRAM.

```
Router# erase startup-config
```

```
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
```

```
Erase of nvram: complete
```

```
Router#
```

- c. Issue the **reload** command to remove an old configuration from memory. When prompted to Proceed with reload?, press Enter. (Pressing any other key aborts the reload.)

```
Router# reload
```

```
Proceed with reload? [confirm]
```

```
*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

Note: You may receive a prompt asking to save the running configuration prior to reloading the router. Respond by typing **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

- d. After the router reloads, you are prompted to enter the initial configuration dialog. Enter **no** and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

- e. Another prompt asks to terminate autoinstall. Respond by typing **yes** press Enter.

```
Would you like to terminate autoinstall? [yes]: yes
```

Step 2: Initialize and reload the switch.

- a. Console into the switch and enter privileged EXEC mode.

```
Switch> enable  
Switch#
```

- b. Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash  
Directory of flash:/  
  
 2  -rwx          1919   Mar 1 1993 00:06:33 +00:00  private-config.text  
 3  -rwx          1632   Mar 1 1993 00:06:33 +00:00  config.text  
 4  -rwx        13336   Mar 1 1993 00:06:33 +00:00  multiple-fs  
 5  -rwx       11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin  
 6  -rwx           616   Mar 1 1993 00:07:13 +00:00  vlan.dat  
  
32514048 bytes total (20886528 bytes free)  
Switch#
```

- c. If the **vlan.dat** file was found in flash, then delete this file.

```
Switch# delete vlan.dat  
Delete filename [vlan.dat]?
```

- d. You are prompted to verify the filename. If you have entered the name correctly, press Enter; otherwise, you can change the filename.

- e. You are prompted to confirm to delete this file. Press Enter to confirm.

```
Delete flash:/vlan.dat? [confirm]  
Switch#
```

- f. Use the **erase startup-config** command to erase the startup configuration file from NVRAM. You are prompted to remove the configuration file. Press Enter to confirm.

```
Switch# erase startup-config  
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]  
[OK]  
Erase of nvram: complete  
Switch#
```

- g. Reload the switch to remove any old configuration information from memory. You will then receive a prompt to confirm to reload the switch. Press Enter to proceed.

```
Switch# reload  
Proceed with reload? [confirm]
```

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Respond by typing **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

- h. After the switch reloads, you should see a prompt to enter the initial configuration dialog. Respond by entering **no** at the prompt and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

```
Switch>
```

4 – Configuring Switch Security Features

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Basic Device Settings and Verify Connectivity

Part 3: Configure and Verify SSH Access on S1

- Configure SSH access.
- Modify SSH parameters.
- Verify the SSH configuration.

Part 4: Configure and Verify Security Features on S1

- Configure and verify general security features.
- Configure and verify port security.

Background / Scenario

It is quite common to lock down access and install good security features on PCs and servers. It is important that your network infrastructure devices, such as switches and routers, are also configured with security features.

In this lab, you will follow some best practices for configuring security features on LAN switches. You will only allow SSH and secure HTTPS sessions. You will also configure and verify port security to lock out any device with a MAC address not recognized by the switch.

Note: The router used with CCNA hands-on labs is a Cisco 1941 Integrated Services Router (ISR) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switch used is a Cisco Catalyst 2960 with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the router and switch have been erased and have no startup configurations. If you are unsure, contact your instructor or refer to the previous lab for the procedures to initialize and reload devices.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Set Up the Topology and Initialize Devices

In Part 1, you will set up the network topology and clear any configurations if necessary.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the router and switch.

If configuration files were previously saved on the router or switch, initialize and reload these devices back to their basic configurations.

Part 2: Configure Basic Device Settings and Verify Connectivity

In Part 2, you configure basic settings on the router, switch, and PC. Refer to the Topology and Addressing Table at the beginning of this lab for device names and address information.

Step 1: Configure an IP address on PC-A.

Step 2: Configure basic settings on R1.

- Configure the device name.
- Disable DNS lookup.
- Configure interface IP address as shown in the Addressing Table.
- Assign **class** as the privileged EXEC mode password.
- Assign **cisco** as the console and vty password and enable login.
- Encrypt plain text passwords.
- Save the running configuration to startup configuration.

Step 3: Configure basic settings on S1.

A good security practice is to assign the management IP address of the switch to a VLAN other than VLAN 1 (or any other data VLAN with end users). In this step, you will create VLAN 99 on the switch and assign it an IP address.

- Configure the device name.
- Disable DNS lookup.
- Assign **class** as the privileged EXEC mode password.
- Assign **cisco** as the console and vty password and then enable login.
- Configure a default gateway for S1 using the IP address of R1.
- Encrypt plain text passwords.

- g. Save the running configuration to startup configuration.
- h. Create VLAN 99 on the switch and name it **Management**.

```
S1(config)# vlan 99  
S1(config-vlan)# name Management  
S1(config-vlan)# exit  
S1(config)#
```

- i. Configure the VLAN 99 management interface IP address, as shown in the Addressing Table, and enable the interface.

```
S1(config)# interface vlan 99  
S1(config-if)# ip address 172.16.99.11 255.255.255.0  
S1(config-if)# no shutdown  
S1(config-if)# end  
S1#
```

- j. Issue the **show vlan** command on S1. What is the status of VLAN 99? _____
- k. Issue the **show ip interface brief** command on S1. What is the status and protocol for management interface VLAN 99?

Why is the protocol down, even though you issued the **no shutdown** command for interface VLAN 99?

- l. Assign ports F0/5 and F0/6 to VLAN 99 on the switch.

```
S1# config t  
S1(config)# interface f0/5  
S1(config-if)# switchport mode access  
S1(config-if)# switchport access vlan 99  
S1(config-if)# interface f0/6  
S1(config-if)# switchport mode access  
S1(config-if)# switchport access vlan 99  
S1(config-if)# end
```

- m. Issue the **show ip interface brief** command on S1. What is the status and protocol showing for interface VLAN 99? _____

Note: There may be a delay while the port states converge.

Step 4: Verify connectivity between devices.

- a. From PC-A, ping the default gateway address on R1. Were your pings successful? _____
- b. From PC-A, ping the management address of S1. Were your pings successful? _____
- c. From S1, ping the default gateway address on R1. Were your pings successful? _____
- d. From PC-A, open a web browser and go to <http://172.16.99.11>. If it prompts you for a username and password, leave the username blank and use **class** for the password. If it prompts for secured connection, answer **No**. Were you able to access the web interface on S1? _____
- e. Close the browser session on PC-A.

Note: The non-secure web interface (HTTP server) on a Cisco 2960 switch is enabled by default. A common security measure is to disable this service, as described in Part 4.

Part 3: Configure and Verify SSH Access on S1

Step 1: Configure SSH access on S1.

- a. Enable SSH on S1. From global configuration mode, create a domain name of **CCNA-Lab.com**.

```
S1(config)# ip domain-name CCNA-Lab.com
```

- b. Create a local user database entry for use when connecting to the switch via SSH. The user should have administrative level access.

Note: The password used here is NOT a strong password. It is merely being used for lab purposes.

```
S1(config)# username admin privilege 15 secret sshadmin
```

- c. Configure the transport input for the vty lines to allow SSH connections only, and use the local database for authentication.

```
S1(config)# line vty 0 15
```

```
S1(config-line)# transport input ssh
```

```
S1(config-line)# login local
```

```
S1(config-line)# exit
```

- d. Generate an RSA crypto key using a modulus of 1024 bits.

```
S1(config)# crypto key generate rsa modulus 1024
```

The name for the keys will be: S1.CCNA-Lab.com

```
% The key modulus size is 1024 bits
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...
```

```
[OK] (elapsed time was 3 seconds)
```

```
S1(config)#
```

```
S1(config)# end
```

- e. Verify the SSH configuration and answer the questions below.

```
S1# show ip ssh
```

What version of SSH is the switch using? _____

How many authentication attempts does SSH allow? _____

What is the default timeout setting for SSH? _____

Step 2: Modify the SSH configuration on S1.

Modify the default SSH configuration.

```
S1# config t
```

```
S1(config)# ip ssh time-out 75
```

```
S1(config)# ip ssh authentication-retries 2
```

How many authentication attempts does SSH allow? _____

What is the timeout setting for SSH? _____

Step 3: Verify the SSH configuration on S1.

- a. Using SSH client software on PC-A (such as Tera Term), open an SSH connection to S1. If you receive a message on your SSH client regarding the host key, accept it. Log in with **admin** for username and **cisco** for the password.

Was the connection successful? _____

What prompt was displayed on S1? Why?

- b. Type **exit** to end the SSH session on S1.

Part 4: Configure and Verify Security Features on S1

In Part 4, you will shut down unused ports, turn off certain services running on the switch, and configure port security based on MAC addresses. Switches can be subject to MAC address table overflow attacks, MAC spoofing attacks, and unauthorized connections to switch ports. You will configure port security to limit the number of MAC addresses that can be learned on a switch port and disable the port if that number is exceeded.

Step 1: Configure general security features on S1.

- a. Configure a message of the day (MOTD) banner on S1 with an appropriate security warning message.
- b. Issue a **show ip interface brief** command on S1. What physical ports are up?

- c. Shut down all unused physical ports on the switch. Use the **interface range** command.

```
S1(config)# interface range f0/1 - 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range f0/7 - 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range g0/1 - 2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

- d. Issue the **show ip interface brief** command on S1. What is the status of ports F0/1 to F0/4?

- e. Issue the **show ip http server status** command.

What is the HTTP server status? _____

What server port is it using? _____

What is the HTTP secure server status? _____

What secure server port is it using? _____

- f. HTTP sessions send everything in plain text. You will disable the HTTP service running on S1.

```
S1(config)# no ip http server
```

- g. From PC-A, open a web browser session to <http://172.16.99.11>. What was your result?

- h. From PC-A, open a secure web browser session at <https://172.16.99.11>. Accept the certificate. Log in with no username and a password of **class**. What was your result?
-
- i. Close the web session on PC-A.

Step 2: Configure and verify port security on S1.

- a. Record the R1 G0/1 MAC address. From the R1 CLI, use the **show interface g0/1** command and record the MAC address of the interface.

```
R1# show interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia
3047.0da3.1821)
```

What is the MAC address of the R1 G0/1 interface?

- b. From the S1 CLI, issue a **show mac address-table** command from privileged EXEC mode. Find the dynamic entries for ports F0/5 and F0/6. Record them below.

F0/5 MAC address: _____

F0/6 MAC address: _____

- c. Configure basic port security.

Note: This procedure would normally be performed on all access ports on the switch. F0/5 is shown here as an example.

- 1) From the S1 CLI, enter interface configuration mode for the port that connects to R1.

```
S1(config)# interface f0/5
```

- 2) Shut down the port.

```
S1(config-if)# shutdown
```

- 3) Enable port security on F0/5.

```
S1(config-if)# switchport port-security
```

Note: Entering the **switchport port-security** command sets the maximum MAC addresses to 1 and the violation action to shutdown. The **switchport port-security maximum** and **switchport port-security violation** commands can be used to change the default behavior.

- 4) Configure a static entry for the MAC address of R1 G0/1 interface recorded in Step 2a.

```
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

(xxxx.xxxx.xxxx is the actual MAC address of the router G0/1 interface)

Note: Optionally, you can use the **switchport port-security mac-address sticky** command to add all the secure MAC addresses that are dynamically learned on a port (up to the maximum set) to the switch running configuration.

- 5) Enable the switch port.

```
S1(config-if)# no shutdown
```

```
S1(config-if)# end
```

- d. Verify port security on S1 F0/5 by issuing a **show port-security interface** command.

```
S1# show port-security interface f0/5
```

```

Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 1
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

```

What is the port status of F0/5?

-
- e. From R1 command prompt, ping PC-A to verify connectivity.

```
R1# ping 172.16.99.3
```

- f. You will now violate security by changing the MAC address on the router interface. Enter interface configuration mode for G0/1 and shut it down.

```

R1# config t
R1(config)# interface g0/1
R1(config-if)# shutdown

```

- g. Configure a new MAC address for the interface, using **aaaa.bbbb.cccc** as the address.

```
R1(config-if)# mac-address aaaa.bbbb.cccc
```

- h. If possible, have a console connection open on S1 at the same time that you do this step. You will see various messages displayed on the console connection to S1 indicating a security violation. Enable the G0/1 interface on R1.

```
R1(config-if)# no shutdown
```

- i. From R1 privilege EXEC mode, ping PC-A. Was the ping successful? Why or why not?

-
- j. On the switch, verify port security with the following commands shown below.

```
S1# show port-security
```

```

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
              (Count)          (Count)          (Count)
-----

```

```

Fa0/5          1          1          1          Shutdown
-----

```

```
Total Addresses in System (excluding one mac per port) :0
```

```
Max Addresses limit in System (excluding one mac per port) :8192
```

```
S1# show port-security interface f0/5
```

```

Port Security          : Enabled
Port Status            : Secure-shutdown
Violation Mode         : Shutdown
Aging Time             : 0 mins

```

```

Aging Type           : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses   : 1
Configured MAC Addresses : 1
Sticky MAC Addresses   : 0
Last Source Address:Vlan : aaaa.bbbb.cccc:99
Security Violation Count : 1

```

S1# **show interface f0/5**

```

FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
<output omitted>

```

S1# **show port-security address**

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
99	30f7.0da3.1821	SecureConfigured	Fa0/5	-

```

Total Addresses in System (excluding one mac per port) :0
Max Addresses limit in System (excluding one mac per port) :8192

```

- k. On the router, shut down the G0/1 interface, remove the hard-coded MAC address from the router, and re-enable the G0/1 interface.

```

R1(config-if)# shutdown
R1(config-if)# no mac-address aaaa.bbbb.cccc
R1(config-if)# no shutdown
R1(config-if)# end

```

- l. From R1, ping PC-A again at 172.16.99.3. Was the ping successful? _____
- m. Issue the **show interface f0/5** command to determine the cause of ping failure. Record your findings.

- n. Clear the S1 F0/5 error disabled status.

```

S1# config t
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown

```

Note: There may be a delay while the port states converge.

- o. Issue the **show interface f0/5** command on S1 to verify F0/5 is no longer in error disabled mode.

```

S1# show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)

```

```
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,  
reliability 255/255, txload 1/255, rxload 1/255
```

p. From the R1 command prompt, ping PC-A again. You should be successful.

Reflection

1. Why would you enable port security on a switch?

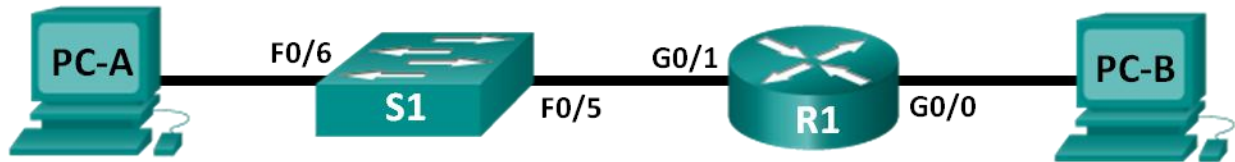
2. Why should unused ports on a switch be disabled?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

5 – Configuring Basic Router Settings with IOS CLI

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

- Cable equipment to match the network topology.
- Initialize and restart the router and switch.

Part 2: Configure Devices and Verify Connectivity

- Assign static IPv4 information to the PC interfaces.
- Configure basic router settings.
- Verify network connectivity.
- Configure the router for SSH.

Part 3: Display Router Information

- Retrieve hardware and software information from the router.
- Interpret the output from the startup configuration.
- Interpret the output from the routing table.
- Verify the status of the interfaces.

Part 4: Configure IPv6 and Verify Connectivity

Background / Scenario

This is a comprehensive lab to review previously covered IOS router commands. In Parts 1 and 2, you will cable the equipment and complete basic configurations and IPv4 interface settings on the router.

In Part 3, you will use SSH to connect to the router remotely and utilize IOS commands to retrieve information from the device to answer questions about the router. In Part 4, you will configure IPv6 on the router so that PC-B can acquire an IP address and then verify connectivity.

For review purposes, this lab provides the commands necessary for specific router configurations.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960 with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the router and switch have been erased and have no startup configurations. Refer to Appendix A for the procedures to initialize and reload devices.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Gigabit Ethernet interfaces on Cisco 1941 ISRs are autosensing and an Ethernet straight-through cable can be used between the router and PC-B. If using another model Cisco router, it may be necessary to use an Ethernet crossover cable.

Part 1: Set Up the Topology and Initialize Devices

Step 1: Cable the network as shown in the topology.

- Attach the devices as shown in the topology diagram, and cable as necessary.
- Power on all the devices in the topology.

Step 2: Initialize and reload the router and switch.

Note: Appendix A details the steps to initialize and reload the devices.

Part 2: Configure Devices and Verify Connectivity

Step 1: Configure the PC interfaces.

- Configure the IP address, subnet mask, and default gateway settings on PC-A.
- Configure the IP address, subnet mask, and default gateway settings on PC-B.

Step 2: Configure the router.

- Console into the router and enable privileged EXEC mode.

```
Router> enable
Router#
```

- Enter into global configuration mode.

```
Router# config terminal
Router(config)#
```

- Assign a device name to the router.

```
Router(config)# hostname R1
```

- d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.

```
R1(config)# no ip domain-lookup
```

- e. Require that a minimum of 10 characters be used for all passwords.

```
R1(config)# security passwords min-length 10
```

Besides setting a minimum length, list other ways to strengthen passwords.

-
- f. Assign **cisco12345** as the privileged EXEC encrypted password.

```
R1(config)# enable secret cisco12345
```

- g. Assign **ciscoconpass** as the console password, establish a timeout, enable login, and add the **logging synchronous** command. The **logging synchronous** command synchronizes debug and Cisco IOS software output and prevents these messages from interrupting your keyboard input.

```
R1(config)# line con 0
```

```
R1(config-line)# password ciscoconpass
```

```
R1(config-line)# exec-timeout 5 0
```

```
R1(config-line)# login
```

```
R1(config-line)# logging synchronous
```

```
R1(config-line)# exit
```

```
R1(config)#
```

For the **exec-timeout** command, what do the **5** and **0** represent?

-
- h. Assign **ciscovtypass** as the vty password, establish a timeout, enable login, and add the **logging synchronous** command.

```
R1(config)# line vty 0 4
```

```
R1(config-line)# password ciscovtypass
```

```
R1(config-line)# exec-timeout 5 0
```

```
R1(config-line)# login
```

```
R1(config-line)# logging synchronous
```

```
R1(config-line)# exit
```

```
R1(config)#
```

- i. Encrypt the clear text passwords.

```
R1(config)# service password-encryption
```

- j. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

```
R1(config)# banner motd #Unauthorized access prohibited!#
```

- k. Configure an IP address and interface description. Activate both interfaces on the router.

```
R1(config)# int g0/0
```

```
R1(config-if)# description Connection to PC-B
```

```
R1(config-if)# ip address 192.168.0.1 255.255.255.0
```

```
R1(config-if)# no shutdown
```

```
R1(config-if)# int g0/1
```

```
R1(config-if)# description Connection to S1
```

```
R1(config-if)# ip address 192.168.1.1 255.255.255.0
```

```
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# exit
R1#
```

- l. Set the clock on the router; for example:

```
R1# clock set 17:00:00 18 Feb 2013
```

- m. Save the running configuration to the startup configuration file.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

What would be the result of reloading the router prior to completing the **copy running-config startup-config** command?

Step 3: Verify network connectivity.

- a. Ping PC-B from a command prompt on PC-A.

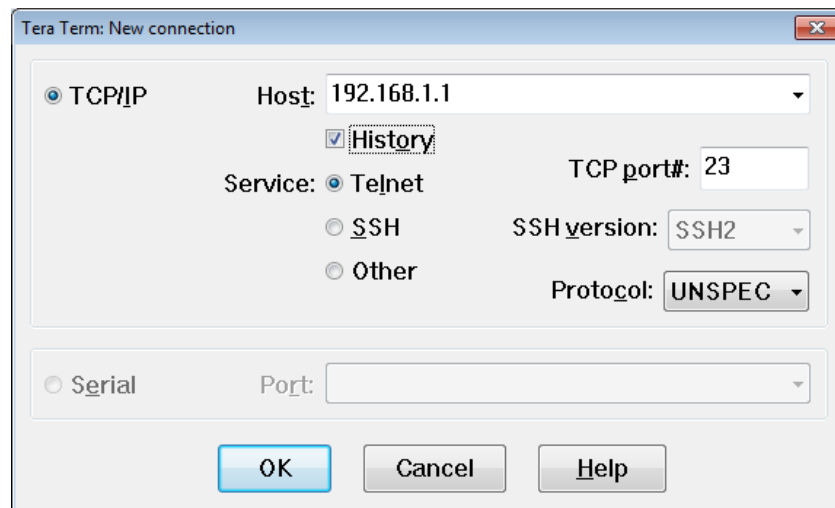
Note: It may be necessary to disable the PCs firewall.

Were the pings successful? _____

After completing this series of commands, what type of remote access could be used to access R1?

- b. Remotely access R1 from PC-A using the Tera Term Telnet client.

Open Tera Term and enter the G0/1 interface IP address of R1 in the Host: field of the Tera Term: New Connection window. Ensure that the **Telnet** radio button is selected and then click **OK** to connect to the router.



Was remote access successful? _____

Why is the Telnet protocol considered to be a security risk?

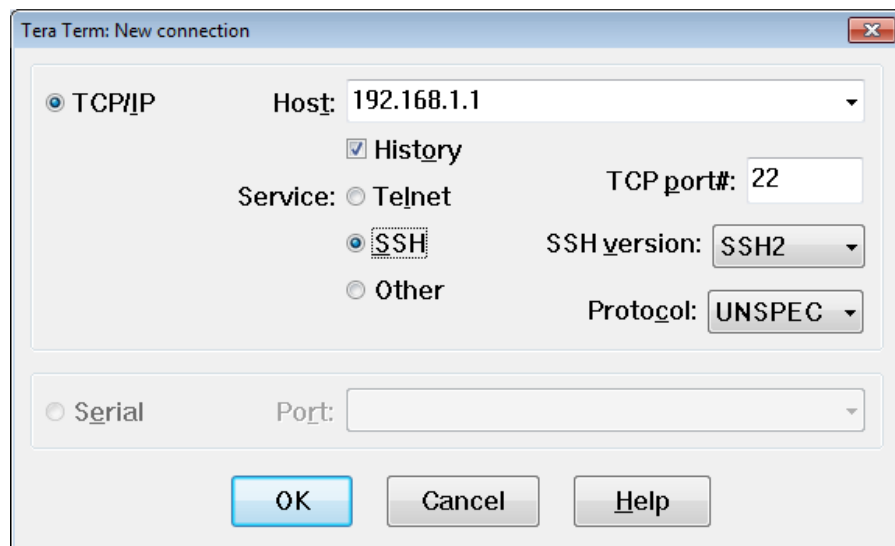
Step 4: Configure the router for SSH access.

- a. Enable SSH connections and create a user in the local database of the router.

```
R1# configure terminal
R1(config)# ip domain-name CCNA-lab.com
R1(config)# username admin privilege 15 secret adminpass1
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
R1(config-line)# exit
R1(config)# crypto key generate rsa modulus 1024
R1(config)# exit
```

- b. Remotely access R1 from PC-A using the Tera Term SSH client.

Open Tera Term and enter the G0/1 interface IP address of R1 in the Host: field of the Tera Term: New Connection window. Ensure that the **SSH** radio button is selected and then click **OK** to connect to the router.



Was remote access successful? _____

Part 3: Display Router Information

In Part 3, you will use **show** commands from an SSH session to retrieve information from the router.

Step 1: Establish an SSH session to R1.

Using Tera Term on PC-B, open an SSH session to R1 at IP address 192.168.0.1 and log in as **admin** with the password **adminpass1**.

Step 2: Retrieve important hardware and software information.

- a. Use the **show version** command to answer questions about the router.

What is the name of the IOS image that the router is running?

How much non-volatile random-access memory (NVRAM) does the router have?

How much Flash memory does the router have?

- b. The **show** commands often provide multiple screens of outputs. Filtering the output allows a user to display certain sections of the output. To enable the filtering command, enter a pipe (|) character after a **show** command, followed by a filtering parameter and a filtering expression. You can match the output to the filtering statement by using the **include** keyword to display all lines from the output that contain the filtering expression. Filter the **show version** command, using **show version | include register** to answer the following question.

What is the boot process for the router on the next reload?

Step 3: Display the startup configuration.

Use the **show startup-config** command on the router to answer the following questions.

How are passwords presented in the output?

Use the **show startup-config | begin vty** command.

What is the result of using this command?

Step 4: Display the routing table on the router.

Use the **show ip route** command on the router to answer the following questions.

What code is used in the routing table to indicate a directly connected network?

How many route entries are coded with a C code in the routing table? _____

Step 5: Display a summary list of the interfaces on the router.

Use the **show ip interface brief** command on the router to answer the following question.

What command changed the status of the Gigabit Ethernet ports from administratively down to up?

Part 4: Configure IPv6 and Verify Connectivity

Step 1: Assign IPv6 addresses to R1 G0/0 and enable IPv6 routing.

Note: Assigning an IPv6 address in addition to an IPv4 address on an interface is known as dual stacking, because both the IPv4 and IPv6 protocol stacks are active. By enabling IPv6 unicast routing on R1, PC-B receives the R1 G0/0 IPv6 network prefix and can autoconfigure its IPv6 address and its default gateway.

- a. Assign an IPv6 global unicast address to interface G0/0, assign the link-local address in addition to the unicast address on the interface, and enable IPv6 routing.

```
R1# configure terminal
R1(config)# interface g0/0
R1(config-if)# ipv6 address 2001:db8:acad:a::1/64
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# ipv6 unicast-routing
R1(config)# exit
```

- b. Use the **show ipv6 int brief** command to verify IPv6 settings on R1.

If no IPv6 address is assigned to G0/1, why is it listed as [up/up]?

- c. Issue the **ipconfig** command on PC-B to examine the IPv6 configuration.

What is the IPv6 address assigned to PC-B?

What is the default gateway assigned to PC-B? _____

Issue a ping from PC-B to the R1 default gateway link local address. Was it successful? _____

Issue a ping from PC-B to the R1 IPv6 unicast address 2001:db8:acad:a::1. Was it successful? _____

Reflection

1. In researching a network connectivity issue, a technician suspects that an interface was not enabled. What **show** command could the technician use to troubleshoot this issue?

2. In researching a network connectivity issue, a technician suspects that an interface was assigned an incorrect subnet mask. What **show** command could the technician use to troubleshoot this issue?

3. After configuring IPv6 on the R1 G0/0 PC-B LAN, if you were to ping from PC-A to the PC-B IPv6 address, would the ping succeed? Why or why not?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Appendix A: Initializing and Reloading a Router and Switch

Step 2: Initialize and reload the router.

- Console into the router and enable privileged EXEC mode.

```
Router> enable
Router#
```

- Type the **erase startup-config** command to remove the startup configuration from NVRAM.

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

- Issue the **reload** command to remove an old configuration from memory. When prompted to **Proceed with reload**, press Enter to confirm the reload. (Pressing any other key aborts the reload.)

```
Router# reload
Proceed with reload? [confirm]
*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

Note: You may be prompted to save the running configuration prior to reloading the router. Type **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

- d. After the router reloads, you are prompted to enter the initial configuration dialog. Enter **no** and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

- e. You are prompted to terminate autoinstall. Type **yes** and then press Enter.

```
Would you like to terminate autoinstall? [yes]: yes
```

Step 3: Initialize and reload the switch.

- a. Console into the switch and enter privileged EXEC mode.

```
Switch> enable
```

```
Switch#
```

- b. Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash
```

```
Directory of flash:/
```

2	-rwx	1919	Mar 1 1993 00:06:33 +00:00	private-config.text
3	-rwx	1632	Mar 1 1993 00:06:33 +00:00	config.text
4	-rwx	13336	Mar 1 1993 00:06:33 +00:00	multiple-fs
5	-rwx	11607161	Mar 1 1993 02:37:06 +00:00	c2960-lanbasek9-mz.150-2.SE.bin
6	-rwx	616	Mar 1 1993 00:07:13 +00:00	vlan.dat

```
32514048 bytes total (20886528 bytes free)
```

```
Switch#
```

- c. If the **vlan.dat** file was found in flash, then delete this file.

```
Switch# delete vlan.dat
```

```
Delete filename [vlan.dat]?
```

- d. You are prompted to verify the filename. At this point, you can change the filename or just press Enter if you have entered the name correctly.

- e. You are prompted to confirm deleting this file. Press Enter to confirm deletion. (Pressing any other key aborts the deletion.)

```
Delete flash:/vlan.dat? [confirm]
```

```
Switch#
```

- f. Use the **erase startup-config** command to erase the startup configuration file from NVRAM. You are prompted to confirm removing the configuration file. Press Enter to confirm to erase this file. (Pressing any other key aborts the operation.)

```
Switch# erase startup-config
```

```
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
```

```
[OK]
```

```
Erase of nvram: complete
```

```
Switch#
```

- g. Reload the switch to remove any old configuration information from memory. You are prompted to confirm reloading the switch. Press Enter to proceed with the reload. (Pressing any other key aborts the reload.)

```
Switch# reload
```

```
Proceed with reload? [confirm]
```

Note: You may be prompted to save the running configuration prior to reloading the switch. Type **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

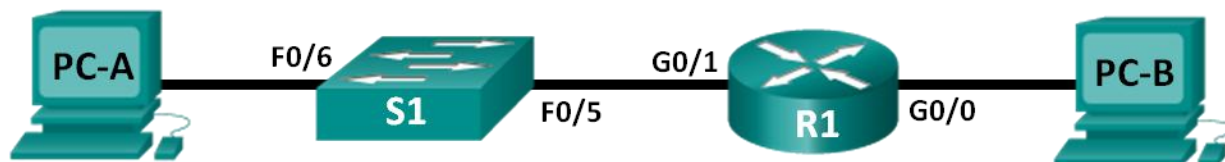
- h. After the switch reloads, you should be prompted to enter the initial configuration dialog. Type **no** and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

```
Switch>
```

6 – Configuring Basic Router Settings with CCP

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	N/A	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Devices and Verify Connectivity

Part 3: Configure Router to Allow CCP Access

Part 4: (Optional) Install and Set Up CCP on PC-A

Part 5: Configure R1 Settings Using CCP

Part 6: Use CCP Utilities

Background / Scenario

Cisco Configuration Professional (CCP) is a PC-based application that provides GUI-based device management for Integrated Services Routers (ISRs). It simplifies the configuration of routing, firewall, VPN, WAN, LAN, and other settings through menus and easy-to-use wizards.

In this lab, you will configure the router settings using the configuration from the previous lab in this chapter. Layer 3 connectivity must be established between the PC running CCP (PC-A) and R1 before CCP can establish a connection. In addition, HTTP access and authentication must be configured on R1.

You will download and install CCP on the PC and then use it to monitor R1's interface status, configure an interface, set the date and time, add a user to the local database, and edit vty settings. You will also use some of the utilities included in CCP.

Note: Router configurations performed using CCP generate IOS CLI commands. CCP can be very useful for configuring more complex router features because it does not require specific knowledge of the Cisco IOS command syntax.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used.

Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the router and switch have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: PC system requirements for CCP version 2.6 are:

- 2 GHz processor or faster
- 1 GB DRAM minimum; 2 GB recommended
- 400 MB of available hard disk space
- Internet Explorer 6.0 or above
- Screen resolution of 1024x768 or higher
- Java Runtime Environment (JRE) version 1.6.0_11 or later.
- Adobe Flash Player version 10.0 or later, with Debug set to No

Note: The Gigabit Ethernet interfaces on Cisco 1941 ISRs are autosensing and an Ethernet straight-through cable may be used between the router and PC-B. If using another model Cisco router, it may be necessary to use an Ethernet crossover cable.

Part 1: Set Up the Topology and Initialize Devices

Step 1: Cable the network as shown in the topology.

- a. Attach the devices shown in the topology diagram, and cable as necessary.
- b. Power on all the devices in the topology.

Step 2: Initialize and reload the router and switch.

Part 2: Configure Devices and Verify Connectivity

In Part 2, you will configure basic settings, such as the interface IP addresses (G0/1 only), secure device access, and passwords. Refer to the Topology and Addressing Table for device names and address information.

Step 1: Configure the PC interfaces.

- a. Configure the IP address, subnet mask, and default gateway settings on PC-A.
- b. Configure the IP address, subnet mask, and default gateway settings on PC-B.

Step 2: Configure the router.

Note: Do NOT configure interface G0/0 at this time. You will configure this interface using CCP later in the lab.

- a. Console into the router and enable privileged EXEC mode.
- b. Enter into global configuration mode.
- c. Disable DNS lookup.
- d. Assign a device name to the router.
- e. Require that a minimum of 10 characters be used for all passwords.
- f. Assign **cisco12345** as the privileged EXEC encrypted password.
- g. Assign **ciscoconpass** as the console password and enable login.
- h. Assign **ciscovtypass** as the vty password and enable login.
- i. Configure **logging synchronous** on the console and vty lines.
- j. Encrypt the clear text passwords.
- k. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
- l. Configure the IP addresses, an interface description, and activate G0/1 interface on the router.
- m. Save the running configuration to the startup configuration file.

Step 3: Verify network connectivity.

Verify that you can ping R1 G0/1 from PC-A.

Part 3: Configure the Router to Allow CCP Access

In Part 3, you will set up the router to allow CCP access by enabling HTTP and HTTPS server services. You will also enable HTTP authentication to use the local database.

Step 1: Enable HTTP and HTTPS server services on the router.

```
R1(config)# ip http server
R1(config)# ip http secure-server
```

Step 2: Enable HTTP authentication to use the local database on the router.

```
R1(config)# ip http authentication local
```

Step 3: Configure the router for CCP access.

Assign a user in the router local database for accessing CCP using username **admin** and password **adminpass1**.

```
R1(config)# username admin privilege 15 secret adminpass1
```

Part 4: (Optional) Install and Set Up CCP on PC-A

Step 1: Install CCP.

Note: This step can be skipped if CCP is already installed on PC-A.

- a. Download CCP 2.6 from Cisco's website:

<http://software.cisco.com/download/release.html?mdfid=281795035&softwareid=282159854&release=2.6&rellifecycle=&relind=AVAILABLE&reltype=all>

- b. Choose the **cisco-config-pro-k9-pkg-2_6-en.zip** file.

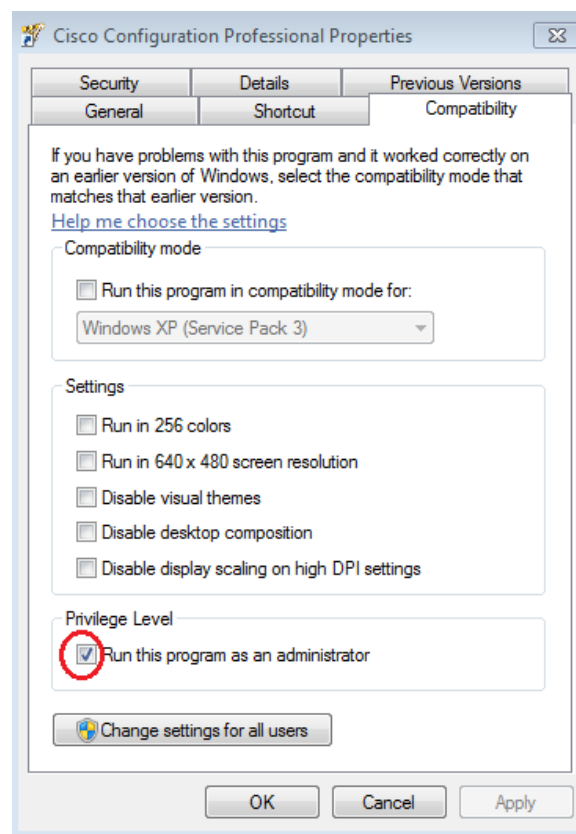
Note: Verify that you select the correct CCP file and not CCP Express. If there is a more current release of CCP, you may choose to download it; however, this lab is based on CCP 2.6.

- c. Agree to the terms and conditions, and download and save the file to the desired location.
- d. Open the zip file and run the CCP executable.
- e. Follow the on-screen instructions to install CCP 2.6 on your PC.

Step 2: Change settings to run as the administrator.

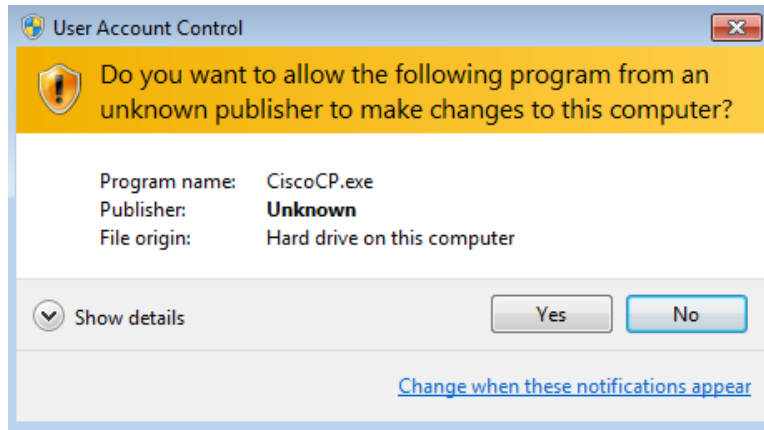
CCP may fail to launch correctly if it is not run as an administrator. You can change the launch settings so that it automatically runs in administrator mode.

- a. Right-click the **CCP** desktop icon (or click the **Start** button) and then right-click **Cisco Configuration Professional**. In the drop-down list, select **Properties**.
- b. In the Properties dialog box, select the **Compatibility** tab. In the Privilege Level section, click the **Run this program as an administrator** checkbox, and then click **OK**.

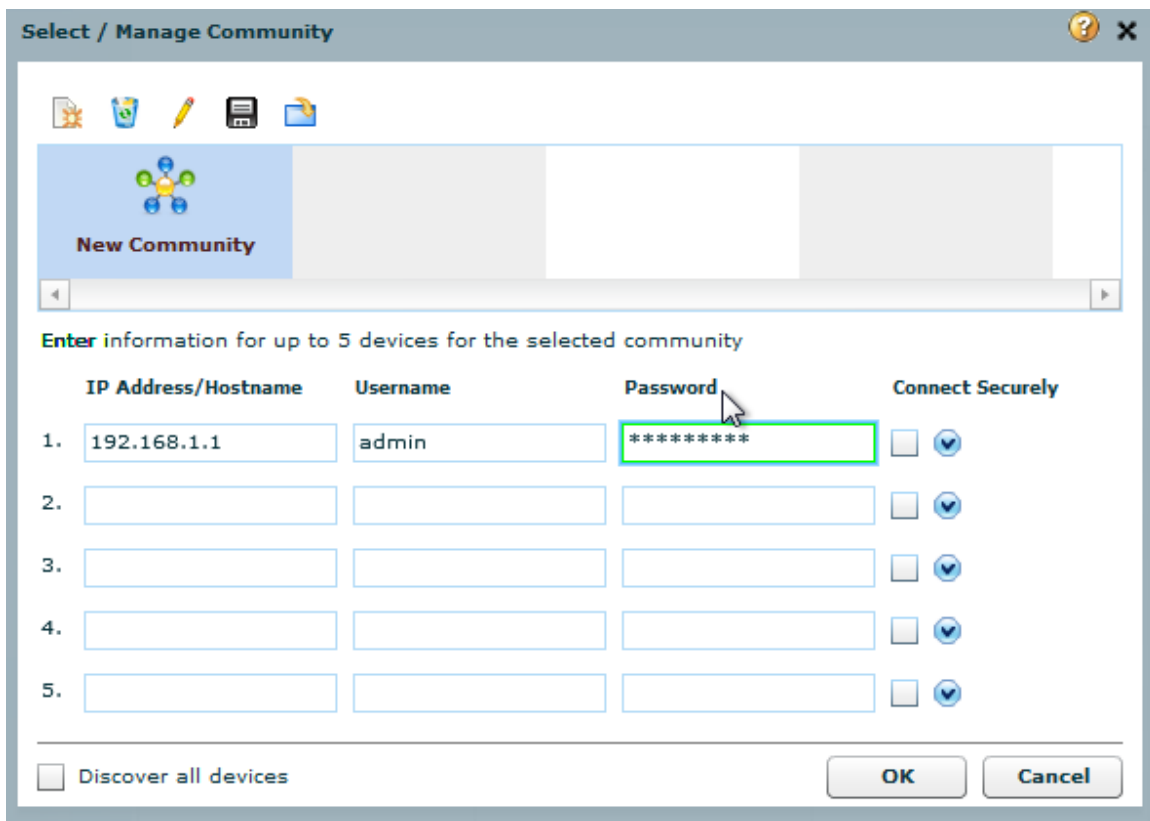


Step 3: Create or manage communities.

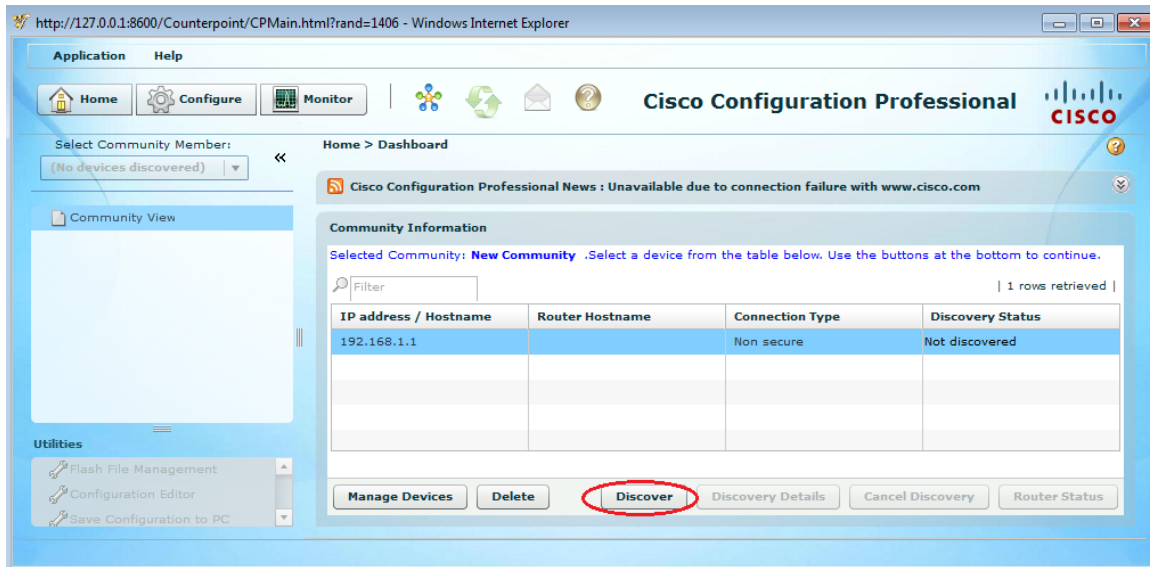
- a. On PC-A, start CCP. (Double-click the CCP desktop icon or click **Start > Cisco Configuration Professional**.)
- b. If you receive a security warning message prompting to allow the CiscoCP.exe program to make changes to the computer, click **Yes**.



- c. When CCP starts, the **Select / Manage Community** dialog box displays. Enter the IP address for R1 G0/1, and the username **admin** and password **adminpass1** that you added to the local database during the router configuration in Part 2. Click **OK**.



- d. In the Community Information window, click **Discover**.



If you have configured the router correctly, the Discovery Status changes from **Not discovered** to **Discovered**, and R1 appears in the Router Hostname column.

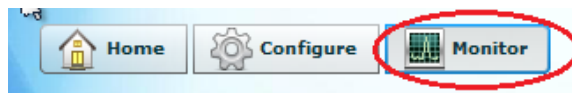
Note: If there is a problem with your configuration, you will see a "Discovery failed" status. Click **Discovery Details** to determine why the discovery process failed and then troubleshoot the problem.

Part 5: Configure R1 Settings Using CCP

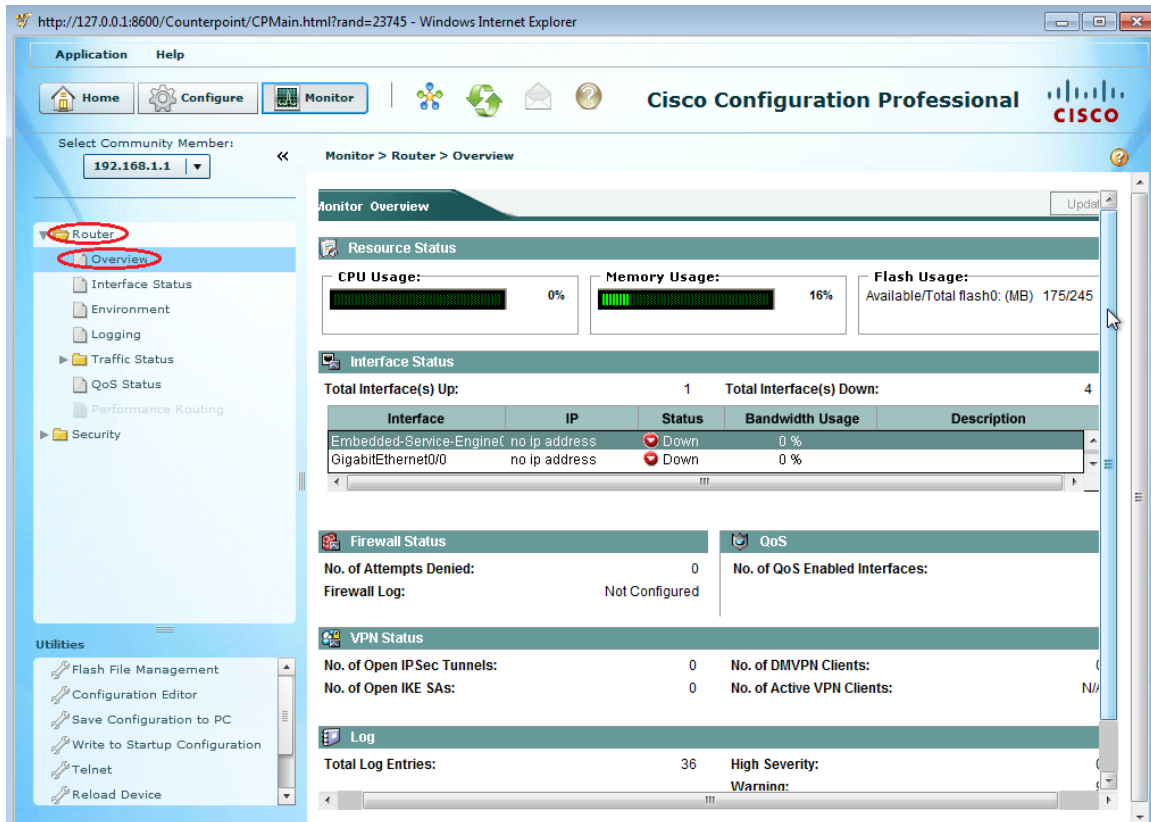
In Part 5, you will use CCP to display information about R1, configure interface G0/0, set the date and time, add a user to the local database, and change your vty settings.

Step 1: View the status of the interfaces on R1.

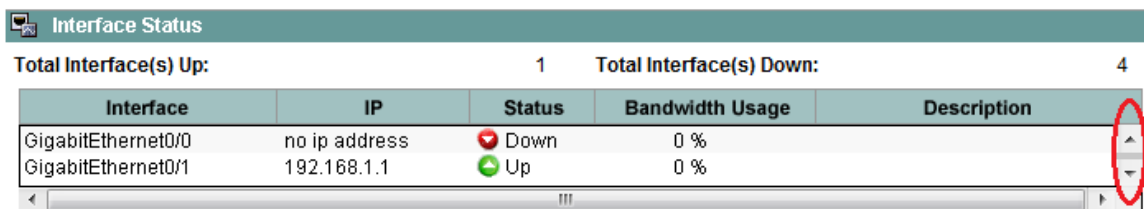
- On the CCP toolbar, click **Monitor**.



- In the left navigation pane, click **Router > Overview** to display the Monitor Overview screen in the right content pane.



- c. Use the up and down arrows to the right of the interface list to scroll through the list of interfaces for the router.

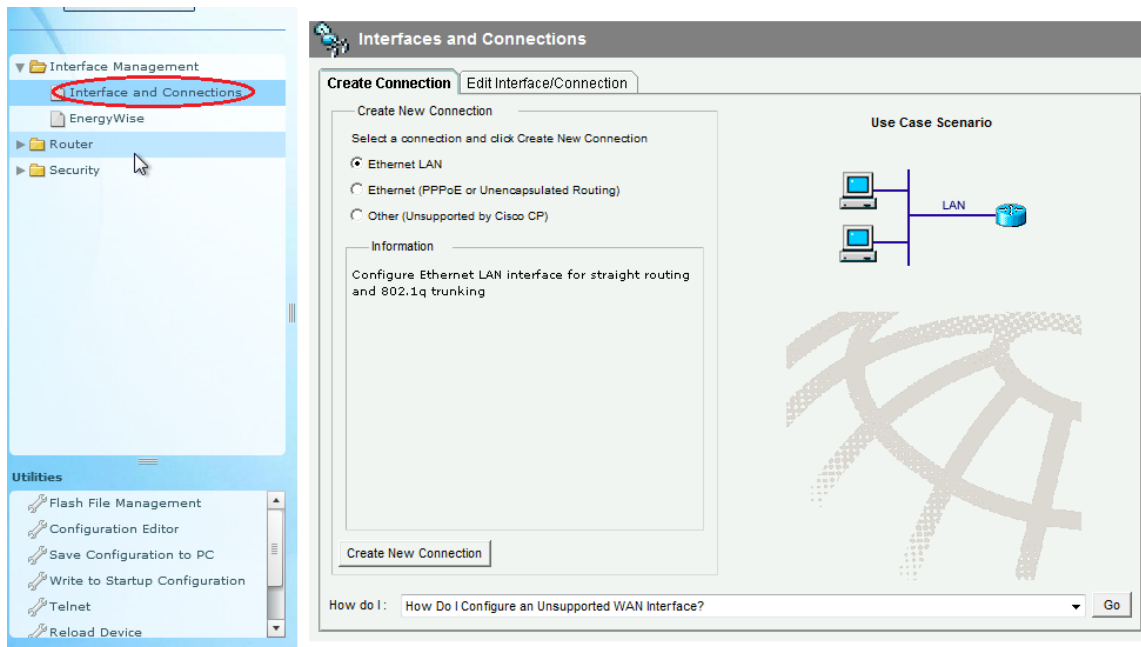


Step 2: Use the Ethernet LAN wizard to configure interface G0/0.

- a. On the CCP toolbar, click **Configure**.



- b. In the left navigation pane, click **Interface Management > Interface and Connections** to display the Interfaces and Connections screen in the right content pane.

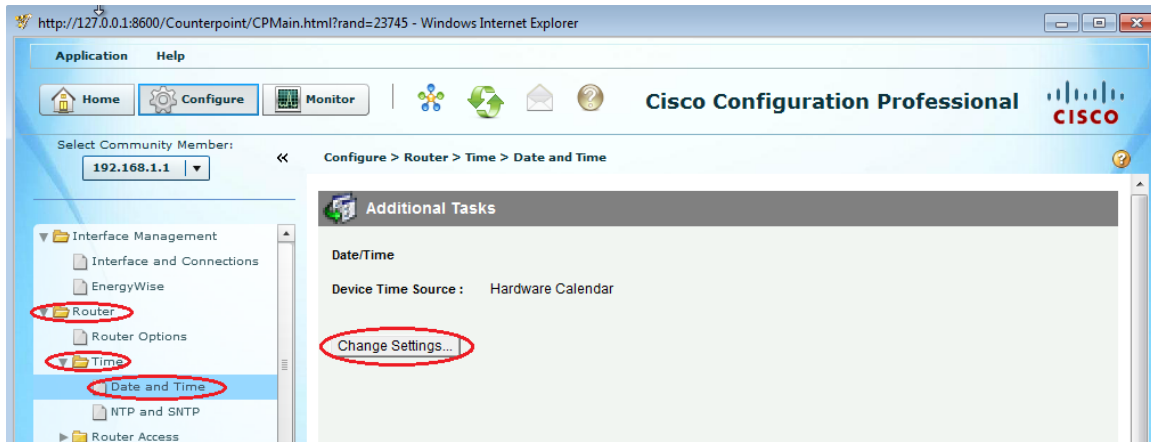


- c. Click **Create New Connection** to start the Ethernet LAN wizard.
- d. When you are prompted to enable AAA on the router, click **No**.
- e. Click **Next** to be guided through the Layer 3 Ethernet interface creation process.
- f. Keep the **Configure this interface for straight routing** radio button selected and click **Next**.
- g. Enter **192.168.0.1** in the IP address field and **255.255.255.0** in the Subnet mask field and click **Next**.
- h. Keep the **No** radio button selected on the DHCP server screen and click **Next**.
- i. Review the summary screen and click **Finish**.
- j. Click the **Save running config to device's startup config** check box, and then click **Deliver**. This adds the commands shown in the preview window to the running configuration, and then saves the running configuration to the startup configuration on the router.
- k. The Commands Delivery Status window displays. Click **OK** to close this window. You will be routed back to the Interfaces and Connections screen; G0/0 should have turned green and displayed as Up in the Status column.

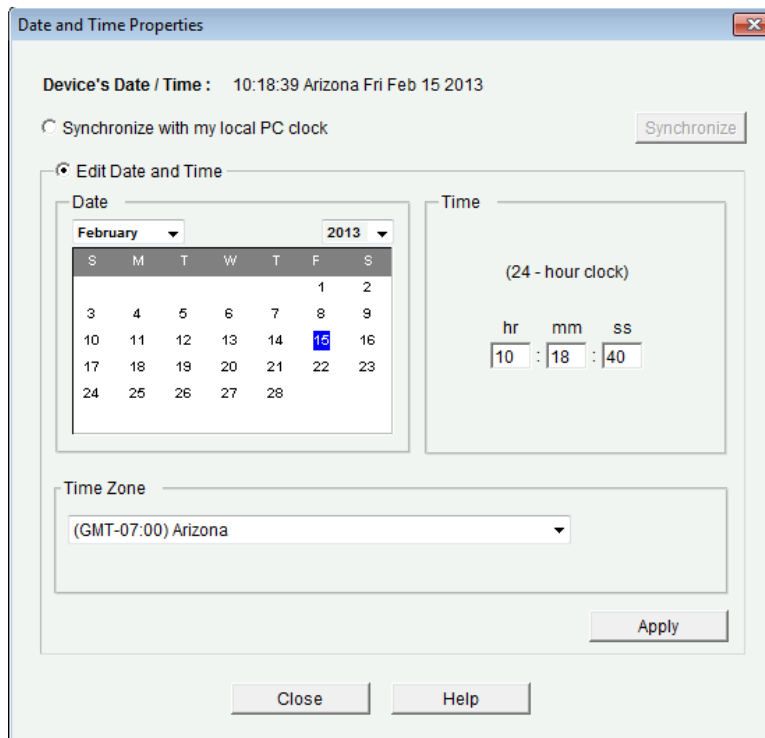
Interface	IP	Type	Slot	Status	Description
Embedded-Service-Engi	no IP address	Embedded-Service-Engine	0	Down	
GigabitEthernet0/0	192.168.0.1	GigabitEthernet	0	Up	
GigabitEthernet0/1	192.168.1.1	GigabitEthernet	0	Up	Connection to S1 F0/5
Serial0/0/0	no IP address	Serial	0	Down	
Serial0/0/1	no IP address	Serial	0	Down	

Step 3: Set the date and time on the router.

- a. In the left navigation pane, select **Router > Time > Date and Time** to display the Additional Tasks > Date/Time screen in the right content pane. Click **Change Settings...**



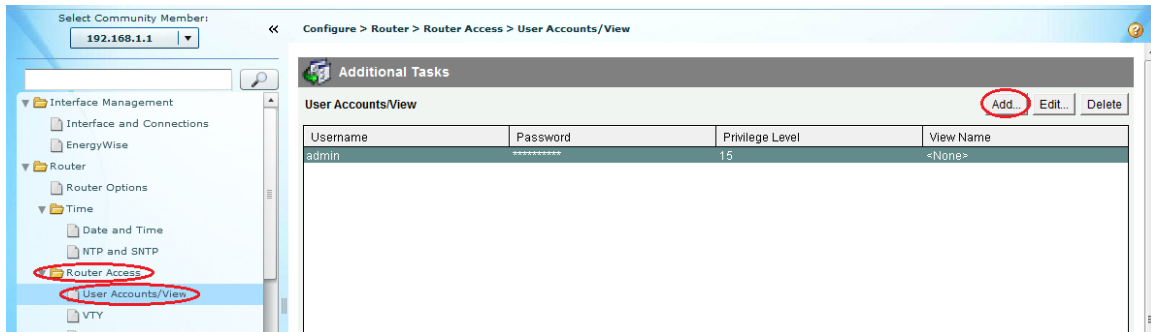
- b. In the Date and Time Properties window, edit the Date, Time, and Time Zone. Click **Apply**.



- c. In the Router's clock configured window, click **OK**. In the Date and Time Properties window, click **Close**.

Step 4: Add a new user account to the local database.

- a. In the left navigation pane, select **Router > Router Access > User Accounts/View** to display the Additional Tasks > User Accounts/View screen in the content pane on the right. Click the **Add...** button.



- b. Enter **ccpadmin** in the Username: field. Enter **ciscocccpass** in the New Password: and Confirm New Password: fields. Select **15** in the Privilege Level: drop-down list. Click **OK** to add this user to the local database.

Add an Account

Enter the username and password

Username:

Password:

New Password:

Confirm New Password:

☒ Encrypt password using MD5 hash algorithm

Privilege Level:

☐ Associate a View with the user

View Name:

- c. In the Deliver Configuration to Device window, click the **Save running config to device's startup config** check box, and then click **Deliver**.
- d. Review the information in the Commands Delivery Status window, and click **OK**. The new user account should now appear in the content pane on the right.

Additional Tasks			
User Accounts/View			
			Add... Edit... Delete
Username	Password	Privilege Level	View Name
admin	*****	15	<None>
ccpadmin	*****	15	<None>

Step 5: Edit vty line settings.

- In the left navigation pane, select **Router Access > VTY** to display the Additional Tasks > VTYS screen in the content pane on the right. Click **Edit...**

Item Name	Item Value
Line Range	0-4
Input Protocols Allowed	ssh
Output Protocols Allowed	None
EXEC timeout	5
Inbound Access-class	None
Outbound Access-class	None

- In the Edit VTY Lines window, change the Time out: field to **15** minutes. Click the **Input Protocol > Telnet** check box. Review the other options available. Also select the **SSH** checkbox. Then click **OK**.

Edit VTY Lines

Line Range

Lines: --

Time out: minutes

Input Protocol

☒ Telnet ☒ SSH ☐ all

Output Protocol

☐ Telnet ☐ SSH ☐ all

Access Rule

Inbound: ...

Outbound: ...

OK Cancel Help

- c. Review the commands that will be delivered to the running configuration on the Deliver Configuration to Device screen and click **Deliver**. In the Commands Delivery Status window, click **OK**. The content pane on the right should reflect the changes to the EXEC timeout value.

Configure > Router > Router Access > VTY

Additional Tasks

VTYs Edit...

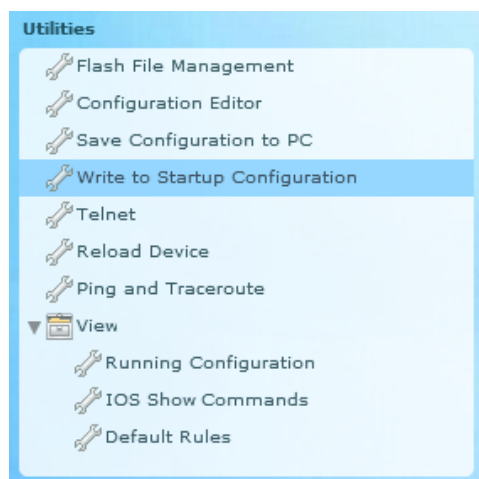
Item Name	Item Value
Line Range	0-4
Input Protocols Allowed	ssh telnet
Output Protocols Allowed	None
EXEC timeout	15
Inbound Access-class	None
Outbound Access-class	None

Part 6: Use CCP Utilities

In Part 6, you will use the Utilities pane to save the router's running configuration to the startup configuration. The Ping utility will be used to test network connectivity, and the View utility will be used to show the router's running configuration. Finally, you will close CCP.

Step 1: Save the router's running configuration to the startup configuration.

- a. At the bottom of the left navigation pane, locate the Utilities pane. Click **Write to Startup Configuration**.



- b. The content pane displays a confirmation screen. Click **Confirm**. An Information window displays, letting you know that the configuration was saved successfully. Click **OK**.

Step 2: Use the Ping utility to test connectivity to PC-B.

- a. In the Utilities pane, click **Ping and Traceroute** to display the Ping and Traceroute screen in the content pane. Enter **192.168.0.3** in the Destination*: field and then click **Ping**. Use the scrollbar to the right of the results box to view the results of your ping.

Utilities > Ping and Traceroute

Destination*: Advanced ▾
 (IP Address or Hostname)

Ping Traceroute

Sending 5, 100-byte ICMP Echos to 192.168.0.3, timeout is 2 seconds:

!!!!

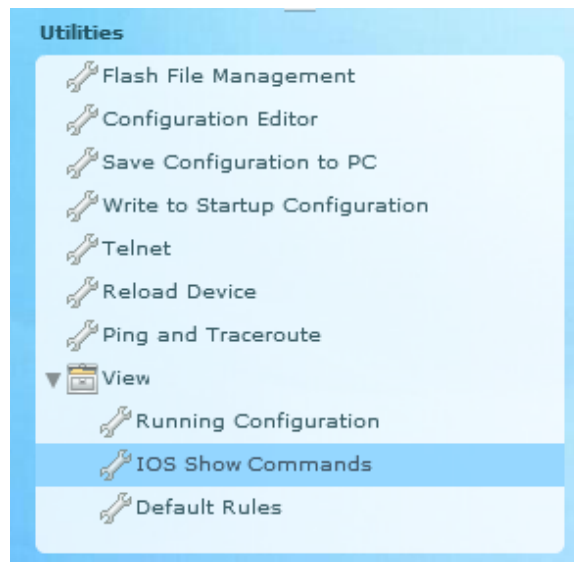
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

Clear

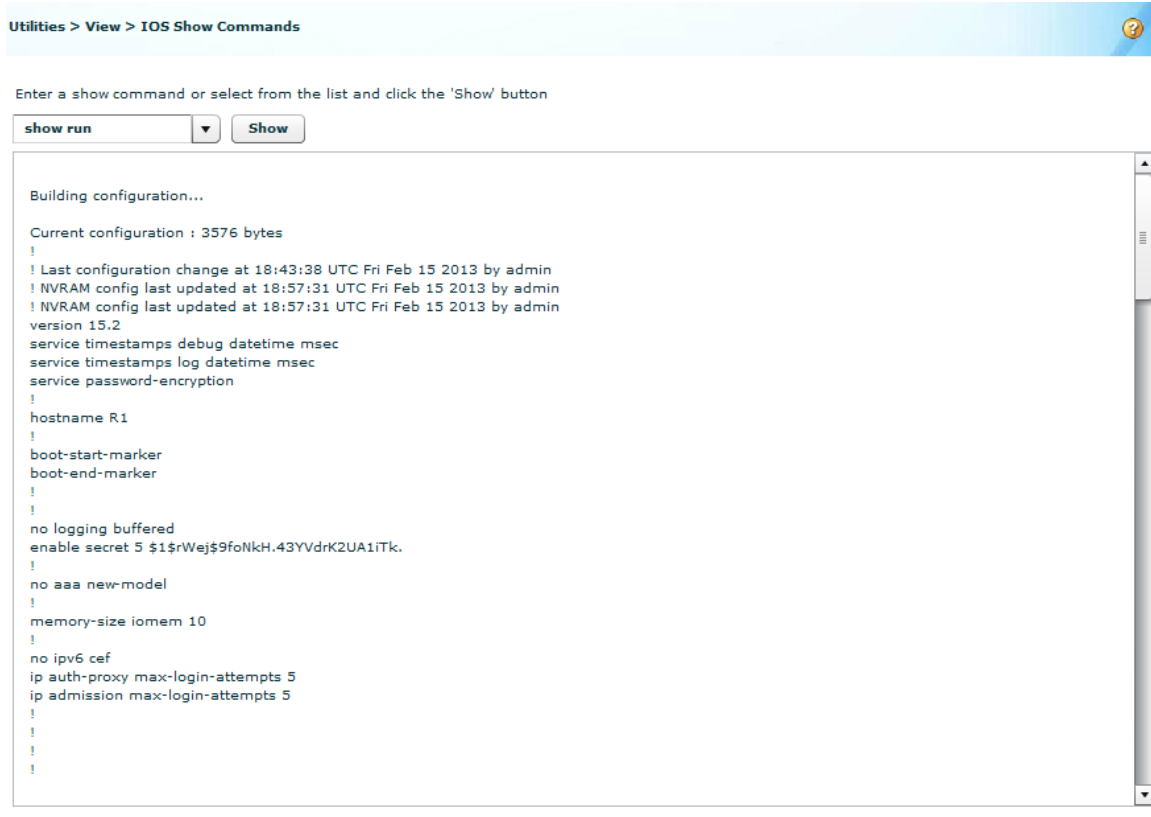
* - indicates mandatory field

Step 3: Use the View utility to show the running configuration for the router.

- In the Utilities pane, click **View > IOS Show Commands** to display the IOS Show Commands screen in the content pane.

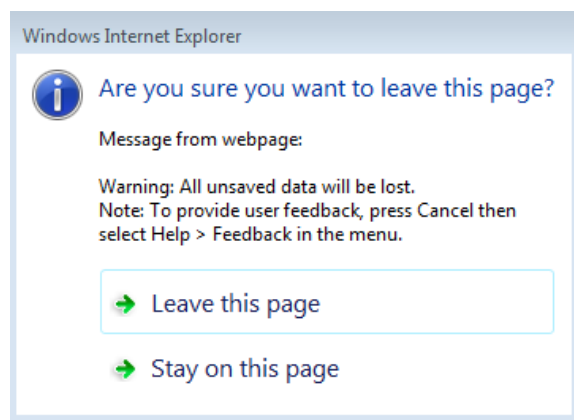


- Select **show run** from the drop-down list and click **Show**. The router's running configuration is displayed in the content pane.



Step 4: Close CCP.

Close the CCP window. When a Windows Internet Explorer confirmation window displays, click **Leave this page**.



Reflection

1. What transport protocol does CCP use to access the router and what commands are used to allow access?

2. What router command tells CCP to use the local database to authenticate?

3. What other **show** commands are available in the Utilities pane of CCP?

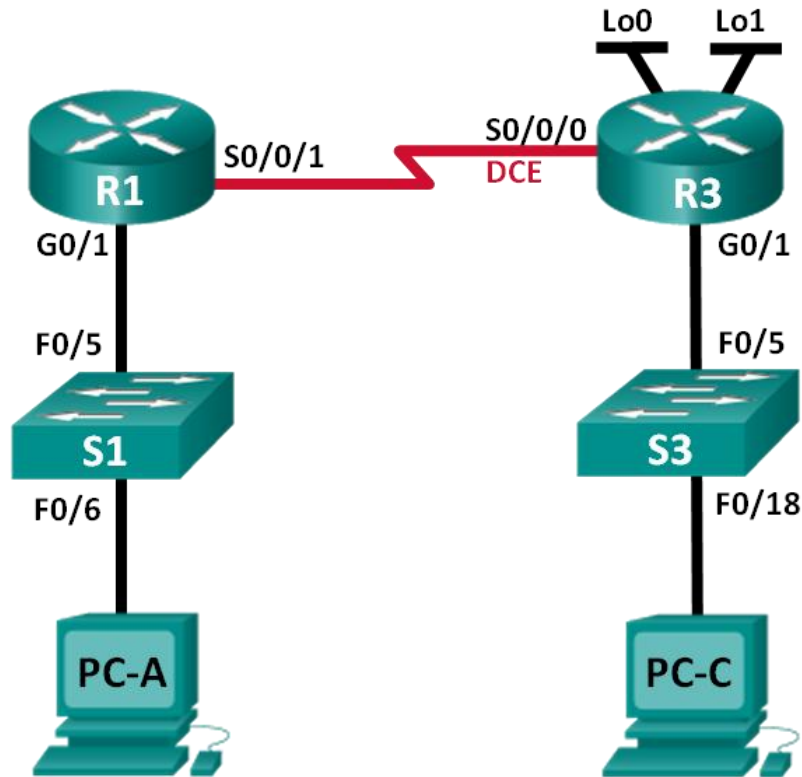
4. Why would you want to use CCP instead of the IOS CLI?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

7 – Configuring IPv4 Static and Default Routes

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.0.1	255.255.255.0	N/A
	S0/0/1	10.1.1.1	255.255.255.252	N/A
R3	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
	Lo1	198.133.219.1	255.255.255.0	N/A
PC-A	NIC	192.168.0.10	255.255.255.0	192.168.0.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Basic Device Settings and Verify Connectivity

Part 3: Configure Static Routes

- Configure a recursive static route.
- Configure a directly connected static route.
- Configure and remove static routes.

Part 4: Configure and Verify a Default Route

Background / Scenario

A router uses a routing table to determine where to send packets. The routing table contains a set of routes that describe which gateway or interface the router uses to reach a specified network. Initially, the routing table contains only directly connected networks. To communicate with distant networks, routes must be specified and added to the routing table.

In this lab, you will manually configure a static route to a specified distant network based on a next-hop IP address or exit interface. You will also configure a static default route. A default route is a type of static route that specifies a gateway to use when the routing table does not contain a path for the destination network.

Note: This lab provides minimal assistance with the actual commands necessary to configure static routing. However, the required commands are provided in Appendix A. Test your knowledge by trying to configure the devices without referring to the appendix.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Set Up the Topology and Initialize Devices

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the router and switch.

Part 2: Configure Basic Device Settings and Verify Connectivity

In Part 2, you will configure basic settings, such as the interface IP addresses, device access, and passwords. You will verify LAN connectivity and identify routes listed in the routing tables for R1 and R3.

Step 1: Configure the PC interfaces.

Step 2: Configure basic settings on the routers.

- Configure device names, as shown in the Topology and Addressing Table.
- Disable DNS lookup.
- Assign **class** as the enable password and assign **cisco** as the console and vty password.
- Save the running configuration to the startup configuration file.

Step 3: Configure IP settings on the routers.

- Configure the R1 and R3 interfaces with IP addresses according to the Addressing Table.
- The S0/0/0 connection is the DCE connection and requires the **clock rate** command. The R3 S0/0/0 configuration is displayed below.

```
R3(config)# interface s0/0/0
R3(config-if)# ip address 10.1.1.2 255.255.255.252
R3(config-if)# clock rate 128000
R3(config-if)# no shutdown
```

Step 4: Verify connectivity of the LANs.

- Test connectivity by pinging from each PC to the default gateway that has been configured for that host.
From PC-A, is it possible to ping the default gateway? _____
From PC-C, is it possible to ping the default gateway? _____
- Test connectivity by pinging between the directly connected routers.
From R1, is it possible to ping the S0/0/0 interface of R3? _____
If the answer is **no** to any of these questions, troubleshoot the configurations and correct the error.
- Test connectivity between devices that are not directly connected.
From PC-A, is it possible to ping PC-C? _____
From PC-A, is it possible to ping Lo0? _____
From PC-A, is it possible to ping Lo1? _____
Were these pings successful? Why or why not?

Note: It may be necessary to disable the PC firewall to ping between PCs.

Step 5: Gather information.

- Check the status of the interfaces on R1 with the **show ip interface brief** command.
How many interfaces are activated on R1? _____
- Check the status of the interfaces on R3.
How many interfaces are activated on R3? _____
- View the routing table information for R1 using the **show ip route** command.
What networks are present in the Addressing Table of this lab, but not in the routing table for R1?

- d. View the routing table information for R3.

What networks are present in the Addressing Table in this lab, but not in the routing table for R3?

Why are all the networks not in the routing tables for each of the routers?

Part 3: Configure Static Routes

In Part 3, you will employ multiple ways to implement static and default routes, you will confirm that the routes have been added to the routing tables of R1 and R3, and you will verify connectivity based on the introduced routes.

Note: This lab provides minimal assistance with the actual commands necessary to configure static routing. However, the required commands are provided in Appendix A. Test your knowledge by trying to configure the devices without referring to the appendix.

Step 1: Configure a recursive static route.

With a recursive static route, the next-hop IP address is specified. Because only the next-hop IP is specified, the router must perform multiple lookups in the routing table before forwarding packets. To configure recursive static routes, use the following syntax:

```
Router(config)# ip route network-address subnet-mask ip-address
```

- a. On the R1 router, configure a static route to the 192.168.1.0 network using the IP address of the Serial 0/0/0 interface of R3 as the next-hop address. Write the command you used in the space provided.
-

- b. View the routing table to verify the new static route entry.

How is this new route listed in the routing table?

From host PC-A, is it possible to ping the host PC-C? _____

These pings should fail. If the recursive static route is correctly configured, the ping arrives at PC-C. PC-C sends a ping reply back to PC-A. However, the ping reply is discarded at R3 because R3 does not have a return route to the 192.168.0.0 network in the routing table.

Step 2: Configure a directly connected static route.

With a directly connected static route, the *exit-interface* parameter is specified, which allows the router to resolve a forwarding decision in one lookup. A directly connected static route is typically used with a point-to-point serial interface. To configure directly connected static routes with an exit interface specified, use the following syntax:

```
Router(config)# ip route network-address subnet-mask exit-intf
```

- a. On the R3 router, configure a static route to the 192.168.0.0 network using S0/0/0 as the exit interface. Write the command you used in the space provided. _____

- b. View the routing table to verify the new static route entry.

How is this new route listed in the routing table?

- c. From host PC-A, is it possible to ping the host PC-C? _____

This ping should be successful.

Note: It may be necessary to disable the PC firewall to ping between PCs.

Step 3: Configure a static route.

- a. On the R1 router, configure a static route to the 198.133.219.0 network using one of the static route configuration options from the previous steps. Write the command you used in the space provided.
-
- b. On the R1 router, configure a static route to the 209.165.200.224 network on R3 using the other static route configuration option from the previous steps. Write the command you used in the space provided.
-

- c. View the routing table to verify the new static route entry.

How is this new route listed in the routing table?

- d. From host PC-A, is it possible to ping the R1 address 198.133.219.1? _____

This ping should be successful.

Step 4: Remove static routes for loopback addresses.

- a. On R1, use the **no** command to remove the static routes for the two loopback addresses from the routing table. Write the commands you used in the space provided.
-
-

- b. View the routing table to verify the routes have been removed.

How many network routes are listed in the routing table on R1? _____

Is the Gateway of last resort set? _____

Part 4: Configure and Verify a Default Route

In Part 4, you will implement a default route, confirm that the route has been added to the routing table, and verify connectivity based on the introduced route.

A default route identifies the gateway to which the router sends all IP packets for which it does not have a learned or static route. A default static route is a static route with 0.0.0.0 as the destination IP address and subnet mask. This is commonly referred to as a “quad zero” route.

In a default route, either the next-hop IP address or exit interface can be specified. To configure a default static route, use the following syntax:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 {ip-address or exit-intf}
```

- a. Configure the R1 router with a default route using the exit interface of S0/0/1. Write the command you used in the space provided.
-

- b. View the routing table to verify the new static route entry.

How is this new route listed in the routing table?

What is the Gateway of last resort?

- c. From host PC-A, is it possible to ping the 209.165.200.225? _____
- d. From host PC-A, is it possible to ping the 198.133.219.1? _____

These pings should be successful.

Reflection

1. A new network 192.168.3.0/24 is connected to interface G0/0 on R1. What commands could be used to configure a static route to that network from R3?

2. Is there a benefit to configuring a directly connected static route instead of a recursive static route?

3. Why is it important to configure a default route on a router?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Appendix A: Configuration Commands for Parts 2, 3, and 4

The commands listed in Appendix A are for reference only. This Appendix does not include all the specific commands necessary to complete this lab.

Basic Device Settings

Configure IP settings on the router.

```
R3(config)# interface s0/0/0
R3(config-if)# ip address 10.1.1.2 255.255.255.252
R3(config-if)# clock rate 128000
R3(config-if)# no shutdown
```

Static Route Configurations

Configure a recursive static route.

```
R1(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.2
```

Configure a directly connected static route.

```
R3(config)# ip route 192.168.0.0 255.255.255.0 s0/0/0
```

Remove static routes.

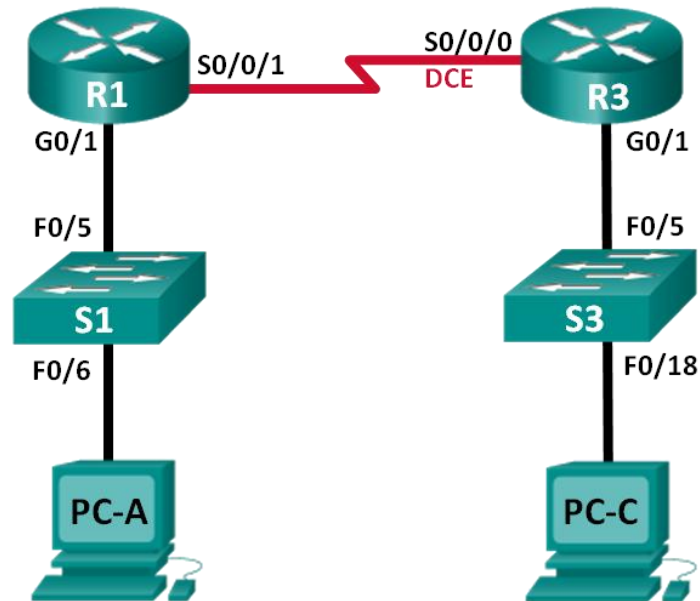
```
R1(config)# no ip route 209.165.200.224 255.255.255.224 serial0/0/1
or
R1(config)# no ip route 209.165.200.224 255.255.255.224 10.1.1.2
or
R1(config)# no ip route 209.165.200.224 255.255.255.224
```

Default Route Configuration

```
R1(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1
```

8 – Configuring IPv6 Static and Default Routes

Topology



Addressing Table

Device	Interface	IPv6 Address / Prefix Length	Default Gateway
R1	G0/1	2001:DB8:ACAD:A::/64 eui-64	N/A
	S0/0/1	FC00::1/64	N/A
R3	G0/1	2001:DB8:ACAD:B::/64 eui-64	N/A
	S0/0/0	FC00::2/64	N/A
PC-A	NIC	SLAAC	SLAAC
PC-C	NIC	SLAAC	SLAAC

Objectives

Part 1: Build the Network and Configure Basic Device Settings

- Enable IPv6 unicast routing and configure IPv6 addressing on the routers.
- Disable IPv4 addressing and enable IPv6 SLAAC for the PC network interfaces.
- Use **ipconfig** and **ping** to verify LAN connectivity.
- Use **show** commands to verify IPv6 settings.

Part 2: Configure IPv6 Static and Default Routes

- Configure a directly attached IPv6 static route.
- Configure a recursive IPv6 static route.
- Configure a default IPv6 static route.

Background / Scenario

In this lab, you will configure the entire network to communicate using only IPv6 addressing, including configuring the routers and PCs. You will use stateless address auto-configuration (SLAAC) for configuring the IPv6 addresses for the hosts. You will also configure IPv6 static and default routes on the routers to enable communication to remote networks that are not directly connected.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will cable and configure the network to communicate using IPv6 addressing.

Step 1: Cable the network as shown in the topology diagram.

Step 2: Initialize and reload the routers and switches.

Step 3: Enable IPv6 unicast routing and configure IPv6 addressing on the routers.

- Using Tera Term, console into the router labeled R1 in the topology diagram and assign the router the name R1.
- Within global configuration mode, enable IPv6 routing on R1.

```
R1(config)# ipv6 unicast-routing
```

- Configure the network interfaces on R1 with IPv6 addresses. Notice that IPv6 is enabled on each interface. The G0/1 interface has a globally routable unicast address and EUI-64 is used to create the interface identifier portion of the address. The S0/0/1 interface has a privately routable, unique-local address, which is recommended for point-to-point serial connections.

```
R1(config)# interface g0/1
```

```
R1(config-if)# ipv6 address 2001:DB8:ACAD:A::/64 eui-64
```

```
R1(config-if)# no shutdown
```

```
R1(config-if)# interface serial 0/0/1
```

```
R1(config-if)# ipv6 address FC00::1/64
```

```
R1(config-if)# no shutdown
```

```
R1(config-if)# exit
```

- Assign a device name to router R3.

- e. Within global configuration mode, enable IPv6 routing on R3.

```
R3(config)# ipv6 unicast-routing
```

- f. Configure the network interfaces on R3 with IPv6 addresses. Notice that IPv6 is enabled on each interface. The G0/1 interface has a globally routable unicast address and EUI-64 is used to create the interface identifier portion of the address. The S0/0/0 interface has a privately routable, unique-local address, which is recommended for point-to-point serial connections. The clock rate is set because it is the DCE end of the serial cable.

```
R3(config)# interface gigabit 0/1
```

```
R3(config-if)# ipv6 address 2001:DB8:ACAD:B::/64 eui-64
```

```
R3(config-if)# no shutdown
```

```
R3(config-if)# interface serial 0/0/0
```

```
R3(config-if)# ipv6 address FC00::2/64
```

```
R3(config-if)# clock rate 128000
```

```
R3(config-if)# no shutdown
```

```
R3(config-if)# exit
```

Step 4: Disable IPv4 addressing and enable IPv6 SLAAC for the PC network interfaces.

- a. On both PC-A and PC-C, navigate to the **Start** menu > **Control Panel**. Click the **Network and Sharing Center** link while viewing with icons. In the Network and Sharing Center window, click the **Change adapter settings** link on the left side of the window to open the Network Connections window.
- b. In the Network Connections window, you see the icons for your network interface adapters. Double-click the Local Area Connection icon for the PC network interface that is connected to the switch. Click the **Properties** to open the Local Area Connection Properties dialogue window.
- c. With the Local Area Connection Properties window open, scroll down through the items and uncheck the item **Internet Protocol Version 4 (TCP/IPv4)** check box to disable the IPv4 protocol on the network interface.
- d. With the Local Area Connection Properties window still open, click the **Internet Protocol Version 6 (TCP/IPv6)** check box, and then click **Properties**.
- e. With the Internet Protocol Version 6 (TCP/IPv6) Properties window open, check to see if the radio buttons for **Obtain an IPv6 address automatically** and **Obtain DNS server address automatically** are selected. If not, select them.
- f. With the PCs configured to obtain an IPv6 address automatically, they will contact the routers to obtain the network subnet and gateway information, and auto-configure their IPv6 address information. In the next step, you will verify the settings.

Step 5: Use ipconfig and ping to verify LAN connectivity.

- a. From PC-A, open a command prompt, type **ipconfig /all** and press Enter. The output should look similar to that shown below. In the output, you should see that the PC now has an IPv6 global unicast address, a link-local IPv6 address, and a link-local IPv6 default gateway address. You may also see a temporary IPv6 address and under the DNS server addresses, three site-local addresses that start with FEC0. Site-local addresses are private addresses that were meant to be backwards compatible with NAT. However, they are not supported in IPv6 and are replaced by unique-local addresses.

```
C:\Users\User1> ipconfig /all
```

```
Windows IP Configuration
```

```
<Output omitted>
```

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . :  
Description . . . . . : Intel(R) 82577LC Gigabit Network Connection  
Physical Address. . . . . : 1C-C1-DE-91-C3-5D  
DHCP Enabled. . . . . : No  
Autoconfiguration Enabled . . . . : Yes  
IPv6 Address. . . . . : 2001:db8:acad:a:7c0c:7493:218d:2f6c (Preferred)  
Temporary IPv6 Address. . . . . : 2001:db8:acad:a:bc40:133a:54e7:d497 (Preferred)  
Link-local IPv6 Address . . . . . : fe80::7c0c:7493:218d:2f6c%13 (Preferred)  
Default Gateway . . . . . : fe80::6273:5cff:fe0d:1a61%13  
DNS Servers . . . . . : fec0:0:0:ffff::1%1  
                        fec0:0:0:ffff::2%1  
                        fec0:0:0:ffff::3%1  
NetBIOS over Tcpip. . . . . : Disabled
```

Based on your network implementation and the output of the **ipconfig /all** command, did PC-A receive IPv6 addressing information from R1?

b. What is the PC-A global unicast IPv6 address?

c. What is the PC-A link-local IPv6 address?

d. What is the PC-A default gateway IPv6 address?

e. From PC-A, use the **ping -6** command to issue an IPv6 ping to the link-local default gateway address. You should see replies from the R1 router.

C:\Users\User1> **ping -6 <default-gateway-address>**

Did PC-A receive replies to the ping from PC-A to R1? _____

f. Repeat Step 5a from PC-C.

Did PC-C receive IPv6 addressing information from R3? _____

g. What is the PC-C global unicast IPv6 address?

h. What is the PC-C link-local IPv6 address?

i. What is the PC-C default gateway IPv6 address?

j. From PC-C, use the **ping -6** command to ping the PC-C default gateway.

Did PC-C receive replies to the pings from PC-C to R3? _____

k. Attempt an IPv6 **ping -6** from PC-A to the PC-C IPv6 address.

C:\Users\User1> **ping -6 PC-C-IPv6-address**

Was the ping successful? Why or why not?

Step 6: Use show commands to verify IPv6 settings.

- a. Check the status of the interfaces on R1 with the **show ipv6 interface brief** command.

What are the two IPv6 addresses for the G0/1 interface and what kind of IPv6 addresses are they?

What are the two IPv6 addresses for the S0/0/1 interface and what kind of IPv6 addresses are they?

- b. To see more detailed information on the IPv6 interfaces, type a **show ipv6 interface** command on R1 and press Enter.

What are the multicast group addresses for the Gigabit Ethernet 0/1 interface?

What are the multicast group addresses for the S0/0/1 interface?

What is an FF02::1 multicast address used for?

What is an FF02::2 multicast address used for?

What kind of multicast addresses are FF02::1:FF00:1 and FF02::1:FF0D:1A60, and what are they used for?

- c. View the IPv6 routing table information for R1 using the **show ipv6 route** command. The IPv6 routing table should have two connected routes, one for each interface, and three local routes, one for each interface and one for multicast traffic to a Null0 interface.

In what way does the routing table output of R1 reveal why you were unable to ping PC-C from PC-A?

Part 2: Configure IPv6 Static and Default Routes

In Part 2, you will configure IPv6 static and default routes three different ways. You will confirm that the routes have been added to the routing tables, and you will verify successful connectivity between PC-A and PC-C.

You will configure three types of IPv6 static routes:

- **Directly Connected IPv6 Static Route** – A directly connected static route is created when specifying the outgoing interface.
- **Recursive IPv6 Static Route** – A recursive static route is created when specifying the next-hop IP address. This method requires the router to execute a recursive lookup in the routing table in order to identify the outgoing interface.
- **Default IPv6 Static Route** – Similar to a quad zero IPv4 route, a default IPv6 static route is created by making the destination IPv6 prefix and prefix length all zeros, ::/0.

Step 1: Configure a directly connected IPv6 static route.

In a directly connected IPv6 static route, the route entry specifies the router outgoing interface. A directly connected static route is typically used with a point-to-point serial interface. To configure a directly attached IPv6 static route, use the following command format:

```
Router(config)# ipv6 route <ipv6-prefix/prefix-length> <outgoing-interface-type> <outgoing-interface-number>
```

- On router R1, configure an IPv6 static route to the 2001:DB8:ACAD:B::/64 network on R3, using the R1 outgoing S0/0/1 interface.

```
R1(config)# ipv6 route 2001:DB8:ACAD:B::/64 serial 0/0/1
```

```
R1(config)#
```

- View the IPv6 routing table to verify the new static route entry.

What is the code letter and routing table entry for the newly added route in the routing table?

- Now that the static route has been configured on R1, is it now possible to ping the host PC-C from PC-A?

These pings should fail. If the recursive static route is correctly configured, the ping arrives at PC-C. PC-C sends a ping reply back to PC-A. However, the ping reply is discarded at R3 because R3 does not have a return route to the 2001:DB8:ACAD:A::/64 network in the routing table. To successfully ping across the network, you must also create a static route on R3.

- On router R3, configure an IPv6 static route to the 2001:DB8:ACAD:A::/64 network, using the R3 outgoing S0/0/0 interface.

```
R3(config)# ipv6 route 2001:DB8:ACAD:A::/64 serial 0/0/0
```

```
R3(config)#
```

- Now that both routers have static routes, attempt an IPv6 **ping -6** from PC-A to the PC-C global unicast IPv6 address.

Was the ping successful? Why? _____

Step 2: Configure a recursive IPv6 static route.

In a recursive IPv6 static route, the route entry has the next-hop router IPv6 address. To configure a recursive IPv6 static route, use the following command format:

```
Router(config)# ipv6 route <ipv6-prefix/prefix-length> <next-hop-ipv6-address>
```

- On router R1, delete the directly attached static route and add a recursive static route.

```
R1(config)# no ipv6 route 2001:DB8:ACAD:B::/64 serial 0/0/1
```

```
R1(config)# ipv6 route 2001:DB8:ACAD:B::/64 FC00::2
```

```
R1(config)# exit
```

- b. On router R3, delete the directly attached static route and add a recursive static route.

```
R3(config)# no ipv6 route 2001:DB8:ACAD:A::/64 serial 0/0/0
R3(config)# ipv6 route 2001:DB8:ACAD:A::/64 FC00::1
R3(config)# exit
```

- c. View the IPv6 routing table on R1 to verify the new static route entry.

What is the code letter and routing table entry for the newly added route in the routing table?

- d. Verify connectivity by issuing a **ping -6** command from PC-A to PC-C.

Was the ping successful? _____

Note: It may be necessary to disable the PC firewall to ping between PCs.

Step 3: Configure a default IPv6 static route.

In a default static route, the destination IPv6 prefix and prefix length are all zeros.

```
Router(config)# ipv6 route ::/0 <outgoing-interface-type> <outgoing-
interface-number> {and/or} <next-hop-ipv6-address>
```

- a. On router R1, delete the recursive static route and add a default static route.

```
R1(config)# no ipv6 route 2001:DB8:ACAD:B::/64 FC00::2
R1(config)# ipv6 route ::/0 serial 0/0/1
R1(config)#
```

- b. Delete the recursive static route and add a default static route on R3.

- c. View the IPv6 routing table on R1 to verify the new static route entry.

What is the code letter and routing table entry for the newly added default route in the routing table?

- d. Verify connectivity by issuing a **ping -6** command from PC-A to PC-C.

Was the ping successful? _____

Note: It may be necessary to disable the PC firewall to ping between PCs.

Reflection

1. This lab focuses on configuring IPv6 static and default routes. Can you think of a situation where you would need to configure both IPv6 and IPv4 static and default routes on a router?

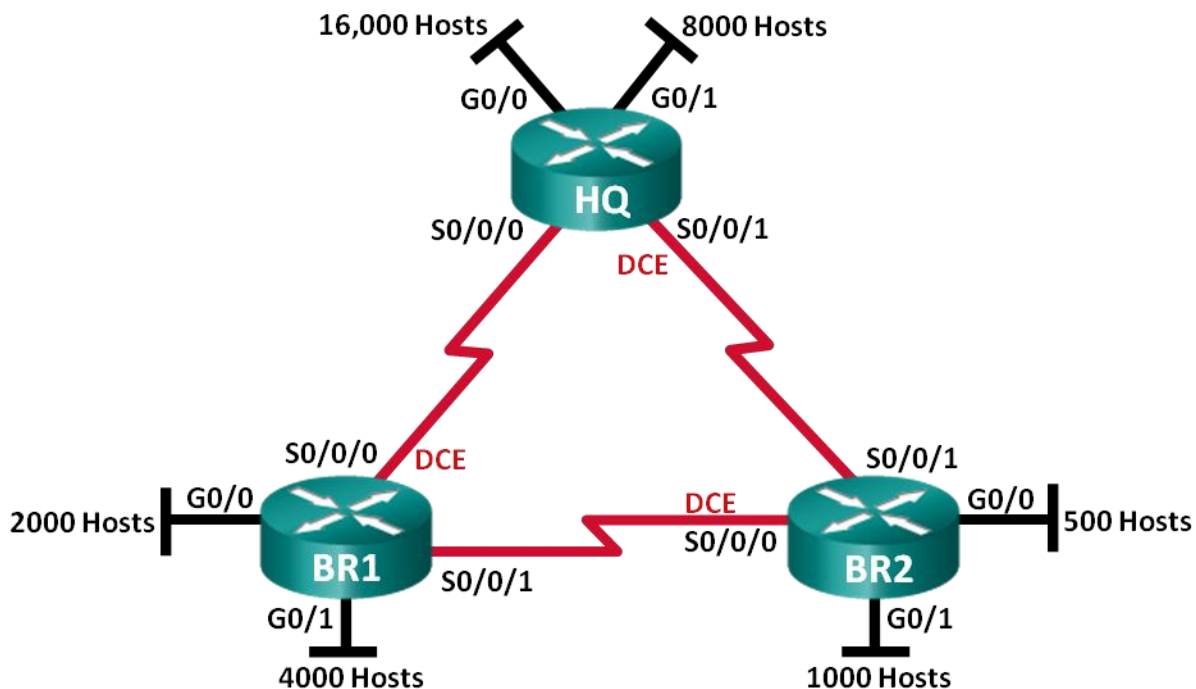
2. In practice, configuring an IPv6 static and default route is very similar to configuring an IPv4 static and default route. Aside from the obvious differences between the IPv6 and IPv4 addressing, what are some other differences when configuring and verifying an IPv6 static route as compared to an IPv4 static route?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

9 – Designing and Implementing IPv4 Addressing with VLSM

Topology



Objectives

Part 1: Examine the Network Requirements

Part 2: Design the VLSM Address Scheme

Part 3: Cable and Configure the IPv4 Network

Background / Scenario

The Variable Length Subnet Mask (VLSM) was designed to help conserve IP addresses. With VLSM, a network is subnetted and then subnetted again. This process can be repeated multiple times to create subnets of various sizes based on the number of hosts required in each subnet. Effective use of VLSM requires address planning.

In this lab, you are given the network address 172.16.128.0/17 to develop an address scheme for the network shown in the Topology diagram. VLSM will be used so that the addressing requirements can be met. After you have designed the VLSM address scheme, you will configure the interfaces on the routers with the appropriate IP address information.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). Other routers and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 PC (with terminal emulation program, such as Tera Term, to configure routers)
- Console cable to configure the Cisco IOS devices via the console ports
- Ethernet (optional) and serial cables as shown in the topology
- Windows Calculator (optional)

Part 1: Examine the Network Requirements

In Part 1, you will examine the network requirements to develop a VLSM address scheme for the network shown in the Topology diagram using the network address of 172.16.128.0/17.

Note: You may use the Windows Calculator application and the www.ipcalc.org IP subnet calculator to help with your calculations.

Step 1: Determine how many host addresses are available and how many subnets are needed.

How many host addresses are available in a /17 network? _____

What is the total number of host addresses needed in the topology diagram? _____

How many subnets are needed in the network topology? _____

Step 2: Determine the largest subnet needed.

Subnet description (e.g. BR1 G0/1 LAN or BR1-HQ WAN link) _____

How many IP addresses are needed in the largest subnet? _____

What is the smallest subnet that supports that many addresses? _____

How many host addresses does that subnet support? _____

Can the 172.16.128.0/17 network be subnetted to support this subnet? _____

What are the two network addresses that would result from this subnetting?

Use the first network address for this subnet.

Step 3: Determine the second largest subnet needed.

Subnet description _____

How many IP addresses are needed for the second largest subnet? _____

What is the smallest subnet that supports that many hosts? _____

How many host addresses does that subnet support? _____

Can the remaining subnet be subnetted again and still support this subnet? _____

What are the two network addresses that would result from this subnetting?

Use the first network address for this subnet.

Step 4: Determine the next largest subnet needed.

Subnet description _____

How many IP addresses are needed for the next largest subnet? _____

What is the smallest subnet that supports that many hosts?

How many host addresses does that subnet support? _____

Can the remaining subnet be subnetted again and still support this subnet? _____

What are the two network addresses that would result from this subnetting?

Use the first network address for this subnet.

Step 5: Determine the next largest subnet needed.

Subnet description _____

How many IP addresses are needed for the next largest subnet? _____

What is the smallest subnet that supports that many hosts?

How many host addresses does that subnet support? _____

Can the remaining subnet be subnetted again and still support this subnet? _____

What are the two network addresses that would result from this subnetting?

Use the first network address for this subnet.

Step 6: Determine the next largest subnet needed.

Subnet description _____

How many IP addresses are needed for the next largest subnet? _____

What is the smallest subnet that supports that many hosts?

How many host addresses does that subnet support? _____

Can the remaining subnet be subnetted again and still support this subnet? _____

What are the two network addresses that would result from this subnetting?

Use the first network address for this subnet.

Step 7: Determine the next largest subnet needed.

Subnet description _____

How many IP addresses are needed for the next largest subnet? _____

What is the smallest subnet that supports that many hosts?

How many host addresses does that subnet support? _____

Can the remaining subnet be subnetted again and still support this subnet? _____

What are the two network addresses that would result from this subnetting?

Use the first network address for this subnet.

Step 8: Determine the subnets needed to support the serial links.

How many host addresses are needed for each serial subnet link? _____

What is the smallest subnet that supports that many host addresses?

- a. Subnet the remaining subnet and write the network addresses that result from this subnetting below.

- b. Continue subnetting the first subnet of each new subnet until you have four /30 subnets. Write the first three network addresses of these /30 subnets below.

- c. Enter the subnet descriptions for these three subnets below.

Part 2: Design the VLSM Address Scheme

Step 1: Calculate the subnet information.

Use the information that you obtained in Part 1 to fill in the table below.

Subnet Description	Number of Hosts Needed	Network Address /CIDR	First Host Address	Broadcast Address
HQ G0/0	16,000			
HQ G0/1	8,000			
BR1 G0/1	4,000			
BR1 G0/0	2,000			
BR2 G0/1	1,000			
BR2 G0/0	500			
HQ S0/0/0 – BR1 S0/0/0	2			
HQ S0/0/1 – BR2 S0/0/1	2			
BR1 S0/0/1 – BR2 S0/0/0	2			

Step 2: Complete the device interface address table.

Assign the first host address in the subnet to the Ethernet interfaces. HQ should be given the first host address on the serial links to BR1 and BR2. BR1 should be given the first host address for the serial link to BR2.

Device	Interface	IP Address	Subnet Mask	Device Interface
HQ	G0/0			16,000 Host LAN
	G0/1			8,000 Host LAN
	S0/0/0			BR1 S0/0/0
	S0/0/1			BR2 S0/0/1
BR1	G0/0			2,000 Host LAN
	G0/1			4,000 Host LAN
	S0/0/0			HQ S0/0/0
	S0/0/1			BR2 S0/0/0
BR2	G0/0			500 Host LAN
	G0/1			1,000 Host LAN
	S0/0/0			BR1 S0/0/1
	S0/0/1			HQ S0/0/1

Part 3: Cable and Configure the IPv4 Network

In Part 3, you will cable the network topology and configure the three routers using the VLSM address scheme that you developed in Part 2.

Step 1: Cable the network as shown in the topology.

Step 2: Configure basic settings on each router.

- Assign the device name to the router.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- Assign **cisco** as the vty password and enable login.
- Encrypt the clear text passwords.
- Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

Step 3: Configure the interfaces on each router.

- Assign an IP address and subnet mask to each interface using the table that you completed in Part 2.
- Configure an interface description for each interface.
- Set the clocking rate on all DCE serial interfaces to 128000.

```
HQ(config-if)# clock rate 128000
```
- Activate the interfaces.

Step 4: Save the configuration on all devices.

Step 5: Test Connectivity.

- From HQ, ping BR1's S0/0/0 interface address.
- From HQ, ping BR2's S0/0/1 interface address.
- From BR1, ping BR2's S0/0/0 interface address.
- Troubleshoot connectivity issues if pings were not successful.

Note: Pings to the GigabitEthernet interfaces on other routers are unsuccessful. The LANs defined for the GigabitEthernet interfaces are simulated. Because no devices are attached to these LANs, they are in a down/down state. A routing protocol must be in place for other devices to be aware of those subnets. The GigabitEthernet interfaces must also be in an up/up state before a routing protocol can add the subnets to the routing table. These interfaces remain in a down/down state until a device is connected to the other end of the Ethernet interface cable. The focus of this lab is on VLSM and configuring the interfaces.

Reflection

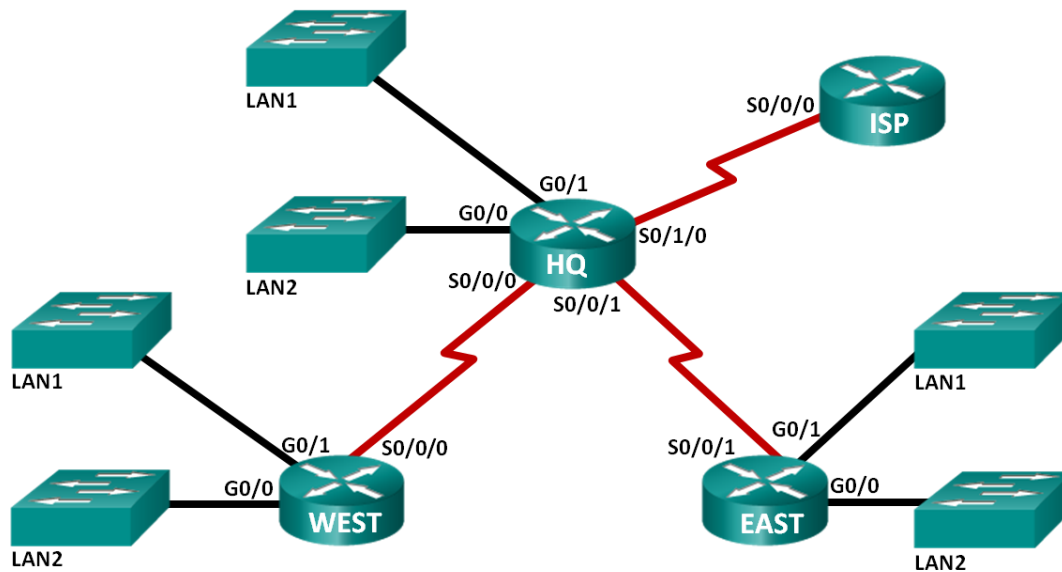
Can you think of a shortcut for calculating the network addresses of consecutive /30 subnets?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

10 – Calculating Summary Routes with IPv4 and IPv6

Topology



Addressing Table

Subnet	IPv4 Address	IPv6 Address
HQ LAN1	192.168.64.0/23	2001:DB8:ACAD:E::/64
HQ LAN2	192.168.66.0/23	2001:DB8:ACAD:F::/64
EAST LAN1	192.168.68.0/24	2001:DB8:ACAD:1::/64
EAST LAN2	192.168.69.0/24	2001:DB8:ACAD:2::/64
WEST LAN1	192.168.70.0/25	2001:DB8:ACAD:9::/64
WEST LAN2	192.168.70.128/25	2001:DB8:ACAD:A::/64
Link from HQ to EAST	192.168.71.4/30	2001:DB8:ACAD:1000::/64
Link from HQ to WEST	192.168.71.0/30	2001:DB8:ACAD:2000::/64
Link from HQ to ISP	209.165.201.0/30	2001:DB8:CC1E:1::/64

Objectives

Part 1: Calculate IPv4 Summary Routes

- Determine the summary route for the HQ LANs.
- Determine the summary route for the EAST LANs.
- Determine the summary route for the WEST LANs.
- Determine the summary route for the HQ, EAST, and WEST LANs.

Part 2: Calculate IPv6 Summary Routes

- Determine the summary route for the HQ LANs.
- Determine the summary route for the EAST LANs.
- Determine the summary route for the WEST LANs.
- Determine the summary route for the HQ, EAST, and WEST LANs.

Background / Scenario

Summary routes reduce the number of entries in routing tables and make the routing table lookup process more efficient. This process also reduces the memory requirements for the router. A single static route can be used to represent a few routes or thousands of routes.

In this lab, you will determine the summary routes for different subnets of a network. You will then determine the summary route for the entire network. Summary routes will be determined for both IPv4 and IPv6 addresses. Because IPv6 uses hexadecimal (hex) values, you will be required to convert hex to binary.

Required Resources

- 1 PC (Windows 7, Vista, or XP with Internet access)
- Optional: calculator for converting hex and decimal to binary

Part 1: Calculate IPv4 Summary Routes

In Part 1, you will determine summarized routes that can be used to reduce the size of routing tables. Fill in the tables, after each set of steps, with the appropriate IPv4 addressing information.

Step 1: List the HQ LAN1 and HQ LAN2 IP subnet mask in decimal form.

Step 2: List the HQ LAN1 and HQ LAN2 IP address in binary form.

Step 3: Count the number of far left matching bits to determine the subnet mask for the summary route.

- a. How many far left matching bits are present in the two networks? _____
- b. List the subnet mask for the summary route in decimal form.

Step 4: Copy the matching binary bits and then add all zeros to determine the summarized network address.

- a. List the matching binary bits for HQ LAN1 and HQ LAN2 subnets.
- b. Add zeros to comprise the remainder of the network address in binary form.
- c. List the summarized network address in decimal form.

Subnet	IPv4 Address	Subnet Mask	Subnet IP Address in Binary Form
HQ LAN1	192.168.64.0		
HQ LAN2	192.168.66.0		
HQ LANs Summary Address			

Step 5: List the EAST LAN1 and EAST LAN2 IP subnet mask in decimal form.

Step 6: List the EAST LAN1 and EAST LAN2 IP address in binary form.

Step 7: Count the number of far left matching bits to determine the subnet mask for the summary route.

- How many far left matching bits are present in the two networks? _____
- List the subnet mask for the summary route in decimal form.

Step 8: Copy the matching binary bits and then add all zeros to determine the summarized network address.

- List the matching binary bits for EAST LAN1 and EAST LAN2 subnets.
- Add zeros to comprise the remainder of the network address in binary form.
- List the summarized network address in decimal form.

Subnet	IPv4 Address	Subnet Mask	Subnet Address in Binary Form
EAST LAN1	192.168.68.0		
EAST LAN2	192.168.69.0		
EAST LANs Summary Address			

Step 9: List the WEST LAN1 and WEST LAN2 IP subnet mask in decimal form.

Step 10: List the WEST LAN1 and WEST LAN2 IP address in binary form.

Step 11: Count the number of far left matching bits to determine the subnet mask for the summary route.

- How many far left matching bits are present in the two networks? _____
- List the subnet mask for the summary route in decimal form.

Step 12: Copy the matching binary bits and then add all zeros to determine the summarized network address.

- List the matching binary bits for WEST LAN1 and WEST LAN2 subnets.

- b. Add zeros to comprise the remainder of the network address in binary form.
- c. List the summarized network address in decimal form.

Subnet	IPv4 Address	Subnet Mask	Subnet IP Address in Binary Form
WEST LAN1	192.168.70.0		
WEST LAN2	192.168.70.128		
WEST LANs Summary Address			

Step 13: List the HQ, EAST, and WEST summary route IP address and subnet mask in decimal form.

Step 14: List the HQ, EAST, and WEST summary route IP address in binary form.

Step 15: Count the number of far left matching bits to determine the subnet mask for the summary route.

- a. How many far left matching bits are present in the three networks? _____
- b. List the subnet mask for the summary route in decimal form.

Step 16: Copy the matching binary bits and then add all zeros to determine the summarized network address.

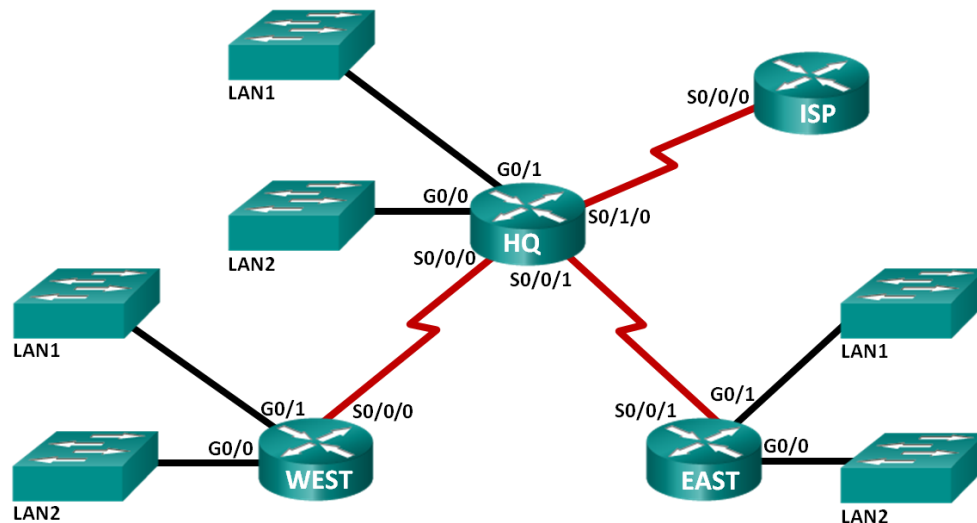
- a. List the matching binary bits for HQ, EAST, and WEST subnets.
- b. Add zeros to comprise the remainder of the network address in binary form.
- c. List the summarized network address in decimal form.

Subnet	IPv4 Address	Subnet Mask	Subnet IP Address in Binary Form
HQ			
EAST			
WEST			
Network Address Summary Route			

Part 2: Calculate IPv6 Summary Routes

In Part 2, you will determine summarized routes that can be used to reduce the size of routing tables. Complete the tables after each set of steps, with the appropriate IPv6 addressing information.

Topology



Addressing Table

Subnet	IPv6 Address
HQ LAN1	2001:DB8:ACAD:E::/64
HQ LAN2	2001:DB8:ACAD:F::/64
EAST LAN1	2001:DB8:ACAD:1::/64
EAST LAN2	2001:DB8:ACAD:2::/64
WEST LAN1	2001:DB8:ACAD:9::/64
WEST LAN2	2001:DB8:ACAD:A::/64
Link from HQ to EAST	2001:DB8:ACAD:1000::/64
Link from HQ to WEST	2001:DB8:ACAD:2000::/64
Link from HQ to ISP	2001:DB8:CC1E:1::/64

Step 1: List the first 64 bits of the HQ LAN1 and HQ LAN2 IP subnet mask in hexadecimal form.

Step 2: List the HQ LAN1 and HQ LAN2 subnet ID (bits 48-64) in binary form.

Step 3: Count the number of far left matching bits to determine the subnet mask for the summary route.

- How many far left matching bits are present in the two subnet IDs? _____
- List the subnet mask for the first 64 bits of the summary route in decimal form.

Step 4: Copy the matching binary bits and then add all zeros to determine the summarized network address.

- List the matching subnet ID binary bits for HQ LAN1 and HQ LAN2 subnets.
- Add zeros to comprise the remainder of the subnet ID address in binary form.
- List the summarized network address in decimal form.

Subnet	IPv6 Address	Subnet Mask for First 64 bits	Subnet ID in Binary Form
HQ LAN1	2001:DB8:ACAD:E::/64		
HQ LAN2	2001:DB8:ACAD:F::/64		
HQ LANs Summary Address			

Step 5: List the first 64 bits of the EAST LAN1 and EAST LAN2 IP subnet mask in hexadecimal form.

Step 6: List the EAST LAN1 and EAST LAN2 subnet ID (bits 48-64) in binary form.

Step 7: Count the number of far left matching bits to determine the subnet mask for the summary route.

- How many far left matching bits are present in the two subnet IDs? _____
- List the subnet mask for the first 64 bits of the summary route in decimal form.

Step 8: Copy the matching binary bits and then add all zeros to determine the summarized network address.

- List the matching binary bits for EAST LAN1 and EAST LAN2 subnets.
- Add zeros to comprise the remainder of the subnet ID address in binary form.
- List the summarized network address in decimal form.

Subnet	IPv6 Address	Subnet Mask for First 64 bits	Subnet ID in Binary Form
EAST LAN1	2001:DB8:ACAD:1::/64		
EAST LAN2	2001:DB8:ACAD:2::/64		
EAST LANs Summary Address			

Step 9: List the first 64 bits of the WEST LAN1 and WEST LAN2 IP subnet mask in decimal form.

Step 10: List the WEST LAN1 and WEST LAN2 subnet ID (bits 48-64) in binary form.

Step 11: Count the number of far left matching bits to determine the subnet mask for the summary route.

- How many far left matching bits are present in the two subnet IDs? _____
- List the subnet mask for the first 64 bits of the summary route in decimal form.

Step 12: Copy the matching binary bits and then add all zeros to determine the summarized network address.

- List the matching binary bits for WEST LAN1 and WEST LAN2 subnets.
- Add zeros to comprise the remainder of the subnet ID address in binary form.
- List the summarized network address in decimal form.

Subnet	IPv6 Address	Subnet Mask for First 64 bits	Subnet ID in Binary Form
WEST LAN1	2001:DB8:ACAD:9::/64		
WEST LAN2	2001:DB8:ACAD:A::/64		
WEST LANs Summary Address			

Step 13: List the HQ, EAST, and WEST summary route IP address and the first 64 bits of the subnet mask in decimal form.

Step 14: List the HQ, EAST, and WEST summary route subnet ID in binary form.

Step 15: Count the number of far left matching bits to determine the subnet mask for the summary route.

- How many far left matching bits are present in the three subnet IDs? _____
- List the subnet mask for the first 64 bits of the summary route in decimal form.

Step 16: Copy the matching binary bits and then add all zeros to determine the summarized network address.

- a. List the matching binary bits for HQ, EAST, and WEST subnets.
- b. Add zeros to comprise the remainder of the subnet ID address in binary form.
- c. List the summarized network address in decimal form.

Subnet	IPv6 Address	Subnet Mask for first 64 bits	Subnet ID in Binary Form
HQ			
EAST			
WEST			
Network Address Summary Route			

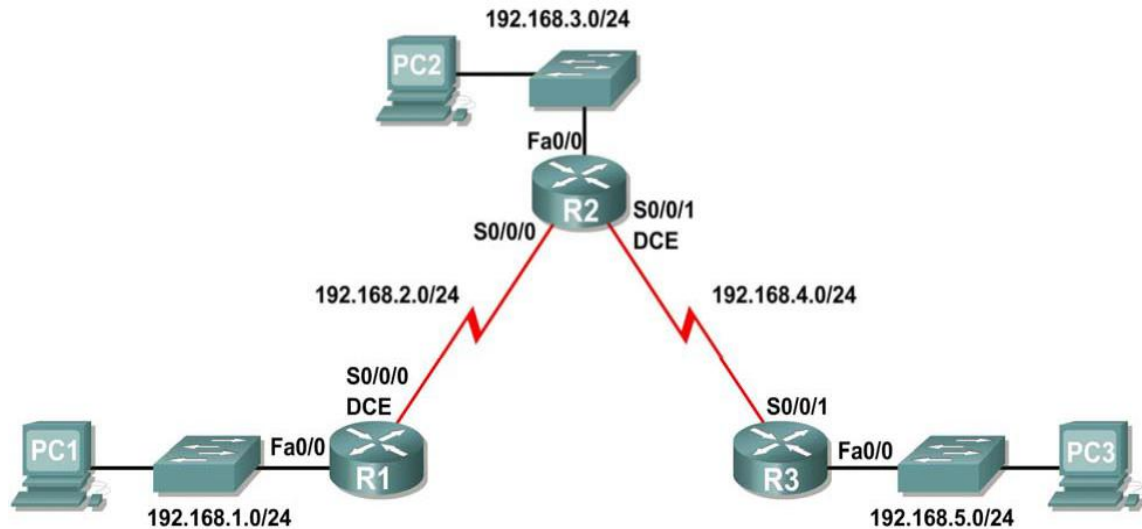
Reflection

1. How is determining the summary route for IPv4 different from IPv6?

2. Why are summary routes beneficial to a network?

11 - Basic RIP Configuration

Topology Diagram



Learning Objectives

Upon completion of this lab,
you will be able to:

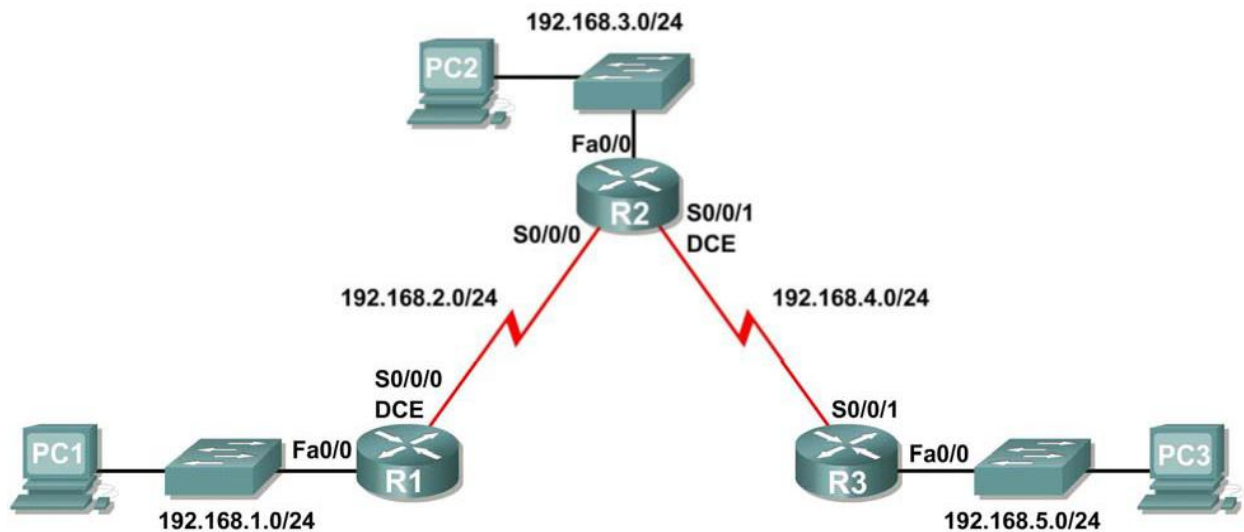
- Cable a network according to the Topology Diagram.
- Erase the startup configuration and reload a router to the default state.
- Perform basic configuration tasks on a router.
- Configure and activate interfaces.
- Configure RIP routing on all routers.
- Verify RIP routing using **show** and **debug** commands.
- Reconfigure the network to make it contiguous.
- Observe automatic summarization at boundary router.
- Gather information about RIP processing using the **debug ip rip** command.
- Configure a static default route.
- Propagate default routes to RIP neighbors.
- Document the RIP configuration.

Scenarios

- Scenario A: Running RIPv1 on Classful Networks
- Scenario B: Running RIPv1 with Subnets and Between Classful Networks
- Scenario C: Running RIPv1 on a Stub Network.

Scenario A: Running RIPv1 on Classful Networks

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	Fa0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
	S0/0/1	192.168.4.2	255.255.255.0	N/A
R3	Fa0/0	192.168.5.1	255.255.255.0	N/A
	S0/0/1	192.168.4.1	255.255.255.0	N/A
PC1	NIC	192.168.1.10	255.255.255.0	192.168.1.1
PC2	NIC	192.168.3.10	255.255.255.0	192.168.3.1
PC3	NIC	192.168.5.10	255.255.255.0	192.168.5.1

Task 1: Prepare the Network.

Step 1: Cable a network that is similar to the one in the Topology Diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

Note: If you use 1700, 2500, or 2600 routers, the router outputs and interface descriptions will appear different.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations.

Perform basic configuration of the R1, R2, and R3 routers according to the following guidelines:

1. Configure the router hostname.
2. Disable DNS lookup.
3. Configure an EXEC mode password.
4. Configure a message-of-the-day banner.
5. Configure a password for console connections.
6. Configure a password for VTY connections.

Task 3: Configure and Activate Serial and Ethernet Addresses.

Step 1: Configure interfaces on R1, R2, and R3.

Configure the interfaces on the R1, R2, and R3 routers with the IP addresses from the table under the Topology Diagram.

Step 2: Verify IP addressing and interfaces.

Use the `show ip interface brief` command to verify that the IP addressing is correct and that the interfaces are active.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 3: Configure Ethernet interfaces of PC1, PC2, and PC3.

Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses and default gateways from the table under the Topology Diagram.

Step 4: Test the PC configuration by pinging the default gateway from the PC.

Task 4: Configure RIP.

Step 1: Enable dynamic routing.

To enable a dynamic routing protocol, enter global configuration mode and use the `router` command. Enter `router ?` at the global configuration prompt to see a list of available routing protocols on your router.

To enable RIP, enter the command `router rip` in global configuration mode.

```
R1(config)#router rip
R1(config-router)#
```

Step 2: Enter classful network addresses.

Once you are in routing configuration mode, enter the classful network address for each directly connected network, using the **network** command.

```
R1(config-router)#network 192.168.1.0  
R1(config-router)#network 192.168.2.0  
R1(config-router)#
```

The **network** command:

- Enables RIP on all interfaces that belong to this network. These interfaces will now both send and receive RIP updates.
- Advertises this network in RIP routing updates sent to other routers every 30 seconds.

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

```
R1(config-router)#end  
%SYS-5-CONFIG_I: Configured from console by console  
R1#copy run start
```

Step 3: Configure RIP on the R2 router using the `router rip` and `network` commands.

```
R2(config)#router rip  
R2(config-router)#network 192.168.2.0  
R2(config-router)#network 192.168.3.0  
R2(config-router)#network 192.168.4.0  
R2(config-router)#end  
%SYS-5-CONFIG_I: Configured from console by console  
R2#copy run start
```

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

Step 4: Configure RIP on the R3 router using the `router rip` and `network` commands.

```
R3(config)#router rip  
R3(config-router)#network 192.168.4.0  
R3(config-router)#network 192.168.5.0  
R3(config-router)#end  
%SYS-5-CONFIG_I: Configured from console by console  
R3# copy run start
```

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

Task 5: Verify RIP Routing.

Step 1: Use the `show ip route` command to verify that each router has all of the networks in the topology entered in the routing table.

Routes learned through RIP are coded with an **R** in the routing table. If the tables are not converged as shown here, troubleshoot your configuration. Did you verify that the configured interfaces are active? Did you configure RIP correctly? Return to Task 3 and Task 4 to review the steps necessary to achieve convergence.

R1#**show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

```
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
R    192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:04, Serial0/0/0
R    192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:04, Serial0/0/0
R    192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:04, Serial0/0/0
R1#
```

R2#**show ip route**

<Output omitted>

```
R    192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:22, Serial0/0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial0/0/1
R    192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:23, Serial0/0/1
R2#
```

R3#**show ip route**

<Output omitted>

```
R    192.168.1.0/24 [120/2] via 192.168.4.2, 00:00:18, Serial0/0/1
R    192.168.2.0/24 [120/1] via 192.168.4.2, 00:00:18, Serial0/0/1
R    192.168.3.0/24 [120/1] via 192.168.4.2, 00:00:18, Serial0/0/1
C    192.168.4.0/24 is directly connected, Serial0/0/1
C    192.168.5.0/24 is directly connected, FastEthernet0/0
R3#
```

Step 2: Use the `show ip protocols` command to view information about the routing processes.

The `show ip protocols` command can be used to view information about the routing processes that are occurring on the router. This output can be used to verify most RIP parameters to confirm that:

- RIP routing is configured
- The correct interfaces send and receive RIP updates
- The router advertises the correct networks
- RIP neighbors are sending updates

```
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 16 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface          Send Recv  Triggered RIP  Key-chain
FastEthernet0/0      1       2 1
Serial0/0/0          1       2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  192.168.1.0
  192.168.2.0
Passive Interface(s):
Routing Information Sources:
  Gateway         Distance      Last Update
  192.168.2.2          120
Distance: (default is 120)
R1#
```

R1 is indeed configured with RIP. R1 is sending and receiving RIP updates on FastEthernet0/0 and Serial0/0/0. R1 is advertising networks 192.168.1.0 and 192.168.2.0. R1 has one routing information source. R2 is sending R1 updates.

Step 3: Use the `debug ip rip` command to view the RIP messages being sent and received.

Rip updates are sent every 30 seconds so you may have to wait for debug information to be displayed.

```
R1#debug ip rip
R1#RIP: received v1 update from 192.168.2.2 on Serial0/0/0
  192.168.3.0 in 1 hops
  192.168.4.0 in 1 hops
  192.168.5.0 in 2 hops
RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (192.168.1.1)
RIP: build update entries
```

The debug output shows that R1 receives an update from R2. Notice how this update includes all the networks that R1 does not already have in its routing table. Because the FastEthernet0/0 interface belongs to the 192.168.1.0 network configured under RIP, R1 builds an update to send out that interface. The update includes all networks known to R1 except the network of the interface. Finally, R1 builds an update to send to R2. Because of split horizon, R1 only includes the 192.168.1.0 network in the update.

```
R1#undebug all
All possible debugging has been turned off
```

Topology Diagram



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.30.1.1	255.255.255.0	N/A
	S0/0/0	172.30.2.1	255.255.255.0	N/A
R2	Fa0/0	172.30.3.1	255.255.255.0	N/A
	S0/0/0	172.30.2.2	255.255.255.0	N/A
	S0/0/1	192.168.4.9	255.255.255.252	N/A
R3	Fa0/0	192.168.5.1	255.255.255.0	N/A
	S0/0/1	192.168.4.10	255.255.255.252	N/A
PC1	NIC	172.30.1.10	255.255.255.0	172.30.1.1
PC2	NIC	172.30.3.10	255.255.255.0	172.30.3.1
PC3	NIC	192.168.5.10	255.255.255.0	192.168.5.1

Task 1: Make Changes between Scenario A and Scenario B

Step 1: Change the IP addressing on the interfaces as shown in the Topology Diagram and the Addressing Table.

Sometimes when changing the IP address on a serial interface, you may need to reset that interface by using the **shutdown** command, waiting for the **LINK-5-CHANGED** message, and then using the **no shutdown** command. This process will force the IOS to starting using the new IP address.

```
R1(config)#int s0/0/0
```

```
R1(config-if)#ip add 172.30.2.1 255.255.255.0
```

```
R1(config-if)#shutdown
```

```
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to
administratively down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to
down
```

```
R1(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
```

```
R1(config-if)#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
```

Step 2: Verify that routers are active.

After reconfiguring all the interfaces on all three routers, verify that all necessary interfaces are active with the **show ip interface brief** command.

Step 3: Remove the RIP configurations from each router.

Although you can remove the old **network** commands with the **no** version of the command, it is more efficient to simply remove RIP and start over. Remove the RIP configurations from each router

with the **no router rip** global configuration command. This will remove all the RIP configuration commands including the **network** commands.

```
R1 (config) #no      router
rip
R2 (config) #no
router      rip
R3 (config) #no      router
rip
```

Task 2: Configure RIP

Step 1: Configure RIP routing on R1 as shown below.

```
R1 (config) #router rip
R1 (config-router) #network 172.30.0.0
```

Notice that only a single network statement is needed for R1. This statement includes both interfaces on different subnets of the 172.30.0.0 major network.

Step 2: Configure R1 to stop sending updates out the FastEthernet0/0 interface.

Sending updates out this interface wastes the bandwidth and processing resources of all devices on the LAN. In addition, advertising updates on a broadcast network is a security risk. RIP updates can be intercepted with packet sniffing software. Routing updates can be modified and sent back to the router, corrupting the router table with false metrics that misdirects traffic.

The **passive-interface fastethernet 0/0** command is used to disable sending RIPv1 updates out that interface. When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

```
R1 (config-router) #passive-interface fastethernet 0/0
R1 (config-router) #end
%SYS-5-CONFIG_I: Configured from console by console
R1 #copy run start
```

Step 3: Configure RIP routing on R2 as shown below.

```
R2 (config) #router rip
R2 (config-router) #network 172.30.0.0
R2 (config-router) #network 192.168.4.0
R2 (config-router) #passive-interface fastethernet 0/0
R2 (config-router) #end
%SYS-5-CONFIG_I: Configured from console by console
R2 #copy run start
```

Again notice that only a single network statement is needed for the two subnets of 172.30.0.0. This statement includes both interfaces, on different subnets, of the 172.30.0.0 major network. The network for the WAN link between R2 and R3 is also configured.

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

Step 4: Configure RIP routing on R3 as shown below.

```
R3(config)#router rip
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#passive-interface fastethernet 0/0
R3(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R3#copy run start
```

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

Task 3: Verify RIP Routing

Step 1: Use the `show ip route` command to verify that each router has all of the networks in the topology in the routing table.

```
R1#show ip route
```

<Output omitted>

```
      172.30.0.0/24 is subnetted, 3 subnets
C      172.30.1.0 is directly connected, FastEthernet0/0
C      172.30.2.0 is directly connected, Serial0/0/0
R      172.30.3.0 [120/1] via 172.30.2.2, 00:00:22, Serial0/0/0
R      192.168.4.0/24 [120/1] via 172.30.2.2, 00:00:22, Serial0/0/0
R      192.168.5.0/24 [120/2] via 172.30.2.2, 00:00:22, Serial0/0/0
R1#
```

Note: RIPv1 is a classful routing protocol. Classful routing protocols do not send the subnet mask with network in routing updates. For example, 172.30.1.0 is sent by R2 to R1 without any subnet mask information.

```
R2#show ip route
```

<Output omitted>

```
      172.30.0.0/24 is subnetted, 3 subnets
R      172.30.1.0 [120/1] via 172.30.2.1, 00:00:04, Serial0/0/0
C      172.30.2.0 is directly connected, Serial0/0/0
C      172.30.3.0 is directly connected, FastEthernet0/0
      192.168.4.0/30 is subnetted, 1 subnets
C      192.168.4.8 is directly connected, Serial0/0/1
R      192.168.5.0/24 [120/1] via 192.168.4.10, 00:00:19, Serial0/0/1
R2#
```

```
R3#show ip route
```

<Output omitted>

```
R    172.30.0.0/16 [120/1] via 192.168.4.9, 00:00:22, Serial0/0/1
    192.168.4.0/30 is subnetted, 1 subnets
C    192.168.4.8 is directly connected, Serial0/0/1
C    192.168.5.0/24 is directly connected, FastEthernet0/0
```

Step 2: Verify that all necessary interfaces are active.

If one or more routing tables does not have a converged routing table, first make sure that all necessary interfaces are active with **show ip interface brief**.

Then use **show ip protocols** to verify the RIP configuration. Notice in the output from this command that the FastEthernet0/0 interface is no longer listed under **Interface** but is now listed under a new section of the output: **Passive Interface(s)**.

```
R1#show ip protocols
```

Routing Protocol is "rip"

Sending updates every 30 seconds, next due in 20 seconds

Invalid after 180 seconds, hold down 180, flushed after 240

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Redistributing: rip

Default version control: send version 2, receive version 2

Interface	Send	Recv	Triggered	RIP	Key-chain
Serial0/1/0	2	2			

Automatic network summarization is in effect

Maximum path: 4

Routing for Networks:

172.30.0.0

209.165.200.0

Passive Interface(s):

FastEthernet0/0

Routing Information Sources:

Gateway	Distance	Last Update
209.165.200.229	120	00:00:15

Distance: (default is 120)

Step 3: View the RIP messages being sent and received.

To view the RIP messages being sent and received use the **debug ip rip** command. Notice that RIP updates are not sent out of the fa0/0 interface because of the **passive-interface fastethernet 0/0** command.

```
R1#debug ip rip
```

```
R1#RIP: sending v1 update to 255.255.255.255 via Serial0/0/0 (172.30.2.1)
```

```
RIP: build update entries
```

```

network 172.30.1.0 metric 1
RIP: received v1 update from 172.30.2.2 on Serial0/0/0
172.30.3.0 in 1 hops

```

Step 4: Discontinue the debug output with the `undebg all` command.

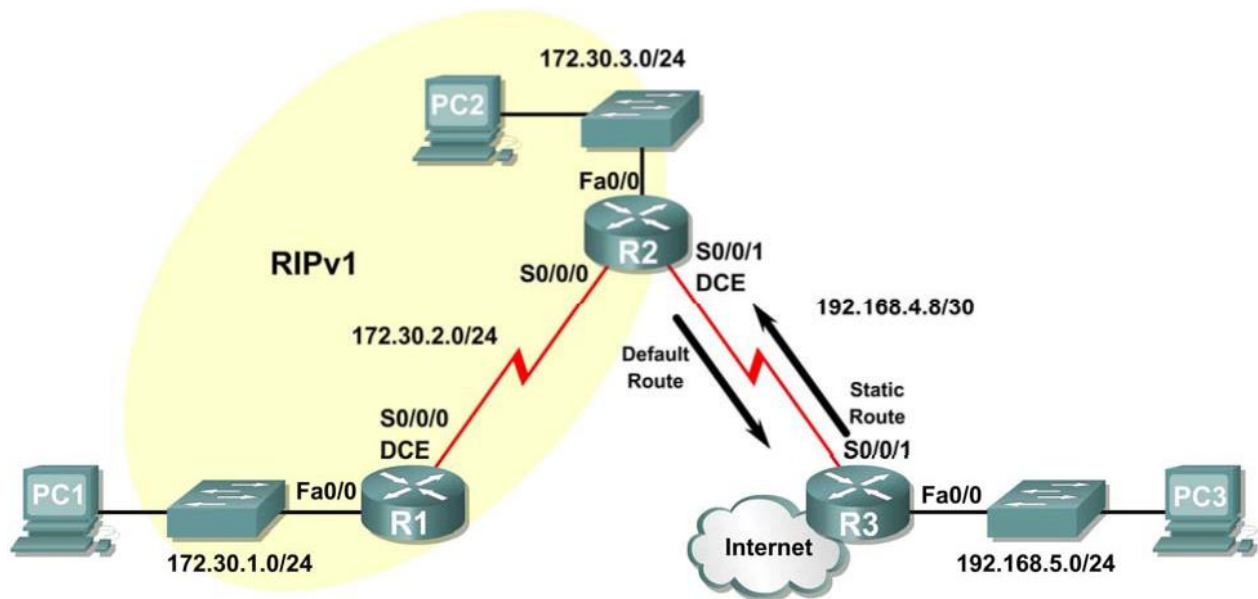
```

R1#undebg all
All possible debugging has been turned off

```

Scenario C: Running RIPv1 on a Stub Network

Topology Diagram



Background

In this scenario we will modify Scenario B to only run RIP between R1 and R2. Scenario C is a typical configuration for most companies connecting a stub network to a central headquarters router or an ISP. Typically, a company runs a dynamic routing protocol (RIPv1 in our case) within the local network but finds it unnecessary to run a dynamic routing protocol between the company's gateway router and the ISP. For example, colleges with multiple campuses often run a dynamic routing protocol between campuses but use default routing to the ISP for access to the Internet. In some cases, remote campuses may even use default routing to the main campus, choosing to use dynamic routing only locally.

To keep our example simple, for Scenario C, we left the addressing intact from Scenario B. Let's assume that R3 is the ISP for our Company XYZ, which consists of the R1 and R2 routers using the 172.30.0.0/16 major network, subnetted with a /24 mask. Company XYZ is a stub network, meaning that there is only one way in and one way out of the 172.30.0.0/16 network—in via R2 (the gateway router) and out via R3 (the ISP). It doesn't make sense for R2 to send R3 RIP updates for the 172.30.0.0 network every 30 seconds, because R3 has no other way to get to 172.30.0.0 except through R2. It makes more sense for R3 to have a static route configured for the 172.30.0.0/16 network pointing to R2.

How about traffic from Company XYZ toward the Internet? It makes no sense for R3 to send over

120,000 summarized Internet routes to R2. All R2 needs to know is that if a packet is not destined for a host on the 172.30.0.0 network, then it should send the packet to the ISP, R3. This is the same for all other Company XYZ routers (only R1 in our case). They should send all traffic not destined for the 172.30.0.0 network to R2. R2 would then forward the traffic to R3.

Task 1: Make Changes between Scenario B and Scenario C.

Step 1: Remove network 192.168.4.0 from the RIP configuration for R2.

Remove network 192.168.4.0 from the RIP configuration for R2, because no updates will be sent between R2 and R3 and we don't want to advertise the 192.168.4.0 network to R1.

```
R2(config)#router rip
```

Step 2: Completely remove RIP routing from R3.

```
R3(config)#no router rip
```

Task 2: Configure the Static Route on R3 for the 172.30.0.0/16 network.

Because R3 and R2 are not exchanging RIP updates, we need to configure a static route on R3 for the 172.30.0.0/16 network. This will send all 172.30.0.0/16 traffic to R2.

```
R3(config)#ip route 172.30.0.0 255.255.252.0 serial0/0/1
```

Task 3: Configure a Default Static Route on R2.

Step 1: Configure R2 to send default traffic to R3.

Configure a default static route on R2 that will send all default traffic—packets with destination IP addresses that do not match a specific route in the routing table—to R3.

```
R2(config)# ip route 0.0.0.0 0.0.0.0 serial 0/0/1
```

Step 2: Configure R2 to send default static route information to R1.

The **default-information originate** command is used to configure R2 to include the default static route with its RIP updates. Configure this command on R2 so that the default static route information is sent to R1.

```
R2(config)#router rip  
R2(config-router)#default-information originate  
R2(config-router)#
```

Note: Sometimes it is necessary to clear the RIP routing process before the **default-information originate** command will work. First, try the command **clear ip route *** on both R1 and R2. This command will cause the routers to immediately flush routes in the routing table and request updates from each other. Sometimes this does not work with RIP. If the default route information is still not sent to R1, save the configuration on R1 and R2 and then reload both routers. Doing this will reset the hardware and both routers will restart the RIP routing process.

Task 4: Verify RIP Routing.

Step 1: Use the `show ip route` command to view the routing table on R2 and R1.

R2#`show ip route`

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

```
172.30.0.0/24 is subnetted, 3 subnets
C      172.30.2.0 is directly connected, Serial0/0/0
C      172.30.3.0 is directly connected, FastEthernet0/0
      192.168.4.0/30 is subnetted, 1 subnets
C      192.168.4.8 is directly connected, Serial0/0/1
S* 0.0.0.0/0 is directly connected, Serial0/0/1
```

Notice that R2 now has a static route tagged as a **candidate default**.

R1#`show ip route`

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 172.30.2.2 to network 0.0.0.0

```
172.30.0.0/24 is subnetted, 3 subnets
C      172.30.2.0 is directly connected, Serial0/0/0
R      172.30.3.0 [120/1] via 172.30.2.2, 00:00:05, Serial0/0/0
C      172.30.1.0 is directly connected, FastEthernet0/0
R* 0.0.0.0/0 [120/1] via 172.30.2.2, 00:00:19, Serial0/0/0
```

Notice that R1 now has a RIP route tagged as a **candidate default** route. The route is the “quad-zero” default route sent by R2. R1 will now send default traffic to the **Gateway of last resort** at 172.30.2.2, which is the IP address of R2.

Step 2: View the RIP updates that are sent and received on R1 with the `debug ip rip` command.

```
R1#debug ip rip
RIP protocol debugging is on
R1#RIP: sending v1 update to 255.255.255.255 via Serial0/0/0
(172.30.2.1) RIP: build update entries
    network 172.30.1.0 metric 1
RIP: received v1 update from 172.30.2.2 on Serial0/0/0
    0.0.0.0 in 1 hops
    172.30.3.0 in 1 hops
```

Notice that R1 is receiving the default route from R2.

Step 3: Discontinue the debug output with the `undebug all` command.

```
R1#undebug all
All possible debugging has been turned off
```

Step 4: Use the `show ip route` command to view the routing table on R3.

```
R3#show ip route

<Output omitted>

S    172.30.0.0/16 is directly connected, Serial0/0/1
    192.168.4.0/30 is subnetted, 1 subnets
C      192.168.4.8 is directly connected, Serial0/0/1
C    192.168.5.0/24 is directly connected, FastEthernet0/0
```

Notice that RIP is not being used on R3. The only route that is not directly connected is the static route.

Task 5: Document the Router Configurations

On each router, capture the following command output to a text file and save for future reference:

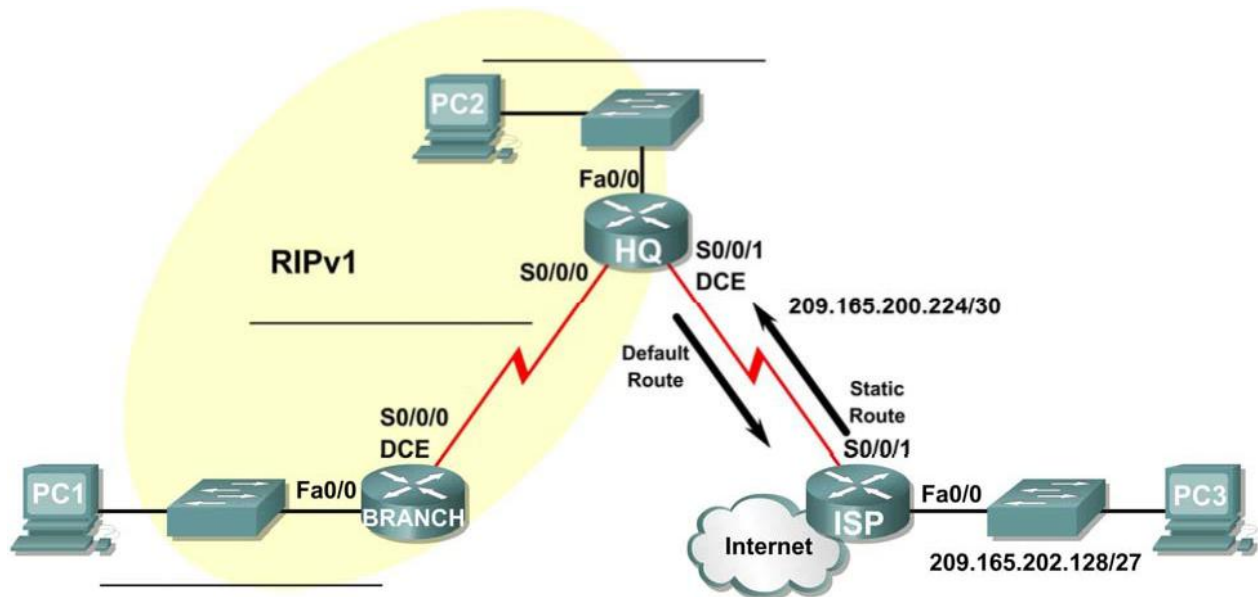
- Running configuration
- Routing table
- Interface summarization
- Output from `show ip protocols`

Task 6: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

12 - Challenge RIP Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
BRANCH	Fa0/0			N/A
	S0/0/0			N/A
HQ	Fa0/0			N/A
	S0/0/0			N/A
	S0/0/1			N/A
ISP	Fa0/0			N/A
	S0/0/1			N/A
PC1	NIC			
PC2	NIC			
PC3	NIC			

Learning Objectives

Upon completion of this lab, you will be able to:

- Subnet an address space given requirements.
- Assign appropriate addresses to interfaces and document them in the Addressing Table.
- Cable a network according to the Topology Diagram.

- Erase the startup configuration and reload a router to the default state.
- Configure RIPv1 routing on all routers.
- Configure and propagate a static default route.
- Verify RIPv1 operation.
- Test and verify full connectivity.
- Reflect upon and document the network implementation.

Scenario

In this lab activity, you will be given a network address that must be subnetted to complete the addressing of the network shown in the Topology Diagram. A combination of RIPv1 and static routing will be required so that hosts on networks that are not directly connected will be able to communicate with each other.

Task 1: Subnet the Address Space.

Step 1: Examine the network requirements.

The addressing for the network has the following requirements:

- The ISP LAN will use the 209.165.202.128/27 network.
- The link between the ISP router and the HQ router will use the 209.165.200.224/30 network.
- The 192.168.1.0/24 network must be subnetted for use in the HQ LAN and the link between the HQ and BRANCH routers. The HQ LAN will require 50 host IP addresses.
- The BRANCH LAN will use the 10.10.2.0/23 network.

(**Note:** Remember that the interfaces of network devices are also host IP addresses and are included in the above addressing requirements.)

Step 2: Consider the following questions when creating your network design:

How many subnets need to be created from the 192.168.1.0/24 network? _____

What is the subnet mask for this network in dotted decimal format? _____ What is the subnet

What are the network addresses of the

subnets? Subnet 0: _____

Subnet 1: _____

Subnet 2: _____

Subnet 3: _____

How many usable host IP addresses are there per subnet? _____

How many usable hosts IP addresses are available in the BRANCH LAN? _____

Step 3: Assign subnetwork addresses to the Topology Diagram.

1. Assign subnet 1 in the 192.168.1.0 network to the WAN link between the HQ and BRANCH routers.

2. Assign subnet 2 in the 192.168.1.0 network to the LAN attached to the HQ router.

Task 2: Determine Interface Addresses.

Step 1: Assign appropriate addresses to the device interfaces.

1. Assign the first valid host address in the 209.165.202.128/27 network to the LAN interface on the ISP router.
2. Assign the last valid host address in the 209.165.202.128/27 network to PC3.
3. Assign the first valid host address in the 209.165.200.224/30 network to the WAN interface of the ISP router.
4. Assign the last valid host address in the 209.165.200.224/30 network to the Serial 0/0/1 interface of the HQ router.
5. Assign the first valid host address in the HQ LAN network to the LAN interface of the HQ router.
6. Assign the last valid host address in the HQ LAN network to PC 2.
7. Assign the first valid host address in the HQ/BRANCH WAN link to the Serial 0/0/0 interface of the HQ router.
8. Assign the last valid host address in the HQ/BRANCH WAN link to the Serial 0/0/0 interface of the BRANCH router.
9. Assign the first valid host address in the 10.10.2.0/23 network to the LAN interface on the BRANCH router.
10. Assign the last valid host address in the 10.10.2.0/23 network to PC1.

Step 2: Document the addresses to be used in the table provided under the Topology Diagram.

Task 3: Prepare the Network.

Step 1: Cable a network that is similar to the one in the Topology Diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

Note: If you use 1700, 2500, or 2600 routers, the router outputs and interface descriptions will appear different.

Step 2: Clear any existing configurations on the routers.

Task 4: Perform Basic Router Configurations.

Perform basic configuration in the BRANCH, HQ, and ISP routers according to the following guidelines:

1. Configure the router hostname.
2. Disable DNS lookup.
3. Configure an EXEC mode password.
4. Configure a message-of-the-day banner.

5. Configure a password for console connections.
6. Configure a password for VTY connections.
7. Synchronize unsolicited messages and debug output with solicited output and prompts for the console and virtual terminal lines.
8. Configure an EXEC timeout of 15 minutes.

Task 5: Configure and Activate Serial and Ethernet Addresses.

Step 1: Configure the BRANCH, HQ, and ISP routers.

Configure the interfaces on the BRANCH, HQ, and ISP routers with the IP addresses from the Addressing Table provided under the Topology Diagram.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 2: Configure the Ethernet interfaces of PC1, PC2, and PC3.

Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses from the Addressing Table provided under the Topology Diagram.

Task 6: Verify Connectivity to Next-Hop Device.

You should *not* have connectivity between end devices yet. However, you can test connectivity between two routers and between an end device and its default gateway.

Step 1: Verify BRANCH connectivity.

Verify that BRANCH can ping across the WAN link to HQ and that HQ can ping across the WAN link it shares with ISP.

Step 2: Verify Ethernet interface connectivity.

Verify that PC1, PC2, and PC3 can ping their respective default gateways.

Task 7: Configure RIP Routing on the BRANCH Router.

Consider the networks that need to be included in the RIP updates that are sent out by the BRANCH router.

What networks are currently present in the BRANCH routing table before RIP is configured? List the networks with slash notation.

What commands are required to enable RIP version 1 and include these networks in the routing updates?

Are there any router interfaces that do not need to have RIP updates sent out? _____

What command is used to disable RIP updates on this interface?

Task 8: Configure RIP and Static Routing on the HQ Router

Consider the type of static routing that is needed on HQ.

What networks are present in the HQ routing table? List the networks with slash notation.

A static default route will need to be configured to send all packets with destination addresses that are not in the routing table to the ISP router. What command is needed to accomplish this? Use the appropriate exit interface on the HQ router in the command.

What commands are required to enable RIPv1 and include the LAN network in the routing updates?

Are there any router interfaces that do not need to have RIP updates sent out? _____

What command is used to disable RIP updates on this interface?

The HQ router needs to send the default route information to the BRANCH router in the RIP updates. What command is used to configure this?

Task 9: Configure Static Routing on the ISP Router

Static routes will need to be configured on the ISP router for all traffic that is destined for the RFC 1918 addresses that are used on the BRANCH LAN, HQ LAN, and the link between the BRANCH and HQ routers.

What are the commands that will need to be configured on the ISP router to accomplish this?

ISP(config) # _____

ISP(config) # _____

Task 10: Verify the Configurations

Answer the following questions to verify that the network is operating as expected. From PC2, is it possible to ping PC1? _____

From PC2, is it possible to ping PC3? _____

From PC1, is it possible to ping PC3? _____

The answer to the above questions should be **yes**. If any of the above pings failed, check your physical connections and configurations. Refer to the basic troubleshooting techniques used in the Chapter 1 labs.

What routes are present in the routing table of the BRANCH router?

What is the gateway of last resort in the routing table of the BRANCH router?

What routes are present in the routing table of the HQ router?

What networks are present in the routing table of the ISP router?

What networks, including the metric, are present in the RIP updates sent from the HQ router?

What networks, including the metric, are present in the RIP updates sent from the BRANCH router?

Task 11: Reflection

If static routing were used instead of RIP on the BRANCH router, how many individual static routes would be needed for hosts on the BRANCH LAN to communicate with all of the networks in the Topology Diagram? _____

Task 12: Document the Router Configurations

On each router, capture the following command output to a text file and save for future reference:

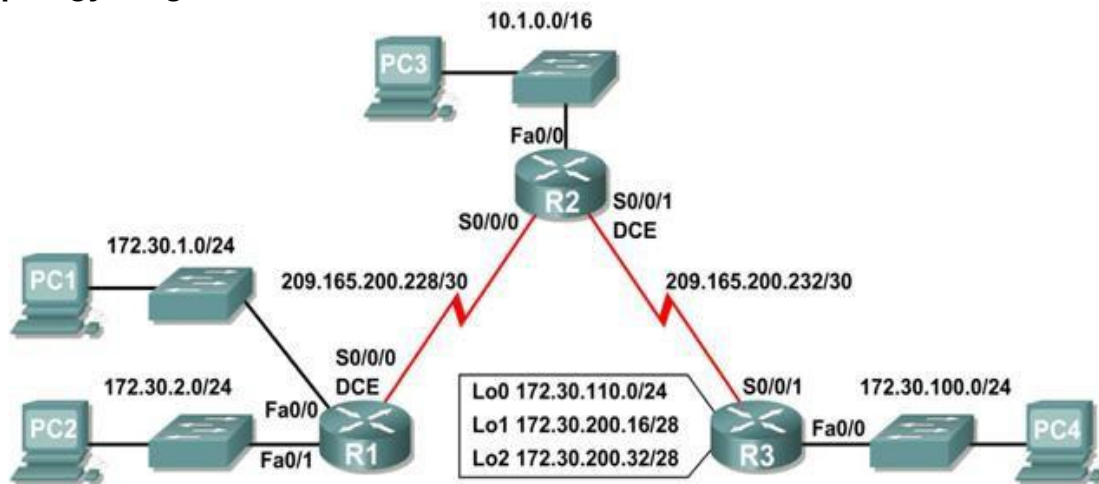
- Running configuration
- Routing table
- Interface summarization

Task 13: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

13 - RIPv2 Basic Configuration Lab

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.30.1.1	255.255.255.0	N/A
	Fa0/1	172.30.2.1	255.255.255.0	N/A
	S0/0/0	209.165.200.230	255.255.255.252	N/A
R2	Fa0/0	10.1.0.1	255.255.0.0	N/A
	S0/0/0	209.165.200.229	255.255.255.252	N/A
	S0/0/1	209.165.200.233	255.255.255.252	N/A
R3	Fa0/0	172.30.100.1	255.255.255.0	N/A
	S0/0/1	209.165.200.234	255.255.255.252	N/A
	Lo0	172.30.110.1	255.255.255.0	N/A
	Lo1	172.30.200.17	255.255.255.240	N/A
	Lo2	172.30.200.33	255.255.255.240	N/A
PC1	NIC	172.30.1.10	255.255.255.0	172.30.1.1
PC2	NIC	172.30.2.10	255.255.255.0	172.30.2.1
PC3	NIC	10.1.0.10	255.255.0.0	10.1.0.1
PC4	NIC	172.30.100.10	255.255.255.0	172.30.100.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the Topology Diagram.
- Load provided scripts onto the routers.
- Examine the current status of the network.
- Configure RIPv2 on all routers.
- Examine the automatic summarization of routes.
- Examine routing updates with **debug ip rip**.
- Disable automatic summarization.
- Examine the routing tables. Verify network connectivity. Document the RIPv2 configuration.

Scenario

The network shown in the Topology Diagram contains a discontinuous network, 172.30.0.0. This network has been subnetted using VLSM. The 172.30.0.0 subnets are physically and logically divided by at least one other classful or major network, in this case the two serial networks 209.165.200.228/30 and 209.165.200.232/30. This can be an issue when the routing protocol used does not include enough information to distinguish the individual subnets. RIPv2 is a classless routing protocol that can be used to provide subnet mask information in the routing updates. This will allow VLSM subnet information to be propagated throughout the network.

Task 1: Cable, Erase, and Reload the Routers.

Step 1: Cable a network.

Cable a network that is similar to the one in the Topology Diagram.

Step 2: Clear the configuration on each router.

Clear the configuration on each of routers using the **erase startup-config** command and then **reload** the routers. Answer **no** if asked to save changes.

Task 2: Load Routers with the Supplied Scripts.

Step 1: Load the following script onto R1.

```
!  
hostname R1  
!  
!  
!  
interface FastEthernet0/0  
ip address 172.30.1.1 255.255.255.0  
duplex auto
```

```

    speed auto
    no shutdown
!
interface FastEthernet0/1
    ip address 172.30.2.1 255.255.255.0
    duplex auto
    speed auto
    no shutdown
!
interface Serial0/0/0
    ip address 209.165.200.230 255.255.255.252
    clock rate 64000
    no shutdown
!
router rip
    passive-interface FastEthernet0/0
    passive-interface FastEthernet0/1
    network 172.30.0.0
    network 209.165.200.0
!
line con 0
line vty 0 4
    login
!
end

```

Step 2: Load the following script onto R2.

```

hostname R2
!
!
!
interface FastEthernet0/0
    ip address 10.1.0.1 255.255.0.0
    duplex auto
    speed auto
    no shutdown
!
interface Serial0/0/0
    ip address 209.165.200.229 255.255.255.252
    no shutdown
!
interface Serial0/0/1
    ip address 209.165.200.233 255.255.255.252
    clock rate 64000
    no shutdown
!
router rip
    passive-interface FastEthernet0/0
    network 10.0.0.0
    network 209.165.200.0
!

```

```
line con 0
line vty 0 4
  login
!
end
```

Step 3: Load the following script onto R3.

```
hostname R3
!
!
!
interface FastEthernet0/0
  ip address 172.30.100.1 255.255.255.0
  duplex
  auto
  speed
  auto no
  shutdown
!
interface Serial0/0/1
  ip address 209.165.200.234
  255.255.255.252 no shutdown
!
interface Loopback0
  ip address 172.30.110.1 255.255.255.0
!
interface Loopback1
  ip address 172.30.200.17 255.255.255.240
!
interface Loopback2
  ip address 172.30.200.33 255.255.255.240
!
router rip
  passive-interface FastEthernet0/0
  network 172.30.0.0
  network 209.165.200.0
!
line con
0 line
vty 0 4
  login
!
end
```

Task 3: Examine the Current Status of the Network.

Step 1: Verify that both serial links are up.

The two serial links can quickly be verified using the **show ip interface brief** command on R2.

R2#**show ip interface brief**

Interface	IP-Address	OK?	Method	Status
	Protocol FastEthernet0/0			
	10.1.0.1	YES	manual	up
FastEthernet0/1	unassigned	YES	manual	administratively down
Serial0/0/0	209.165.200.229	YES	manual	up
Serial0/0/1	209.165.200.233	YES	manual	up
Vlan1	unassigned	YES	manual	administratively down

Step 2: Check the connectivity from R2 to the hosts on the R1 and R3 LANs.

Note: For the 1841 router, you will need to disable IP CEF to obtain the correct output from the **ping** command. Although a discussion of IP CEF is beyond the scope of this course, you may disable IP CEF by using the following command in global configuration mode:

R2(config)#**no ip cef**

From the R2 router, how many ICMP messages are successful when pinging PC1?

From the R2 router, how many ICMP messages are successful when pinging PC4?

Step 3: Check the connectivity between the PCs.

From the PC1, is it possible to ping PC2? _____

What is the success rate? _____

From the PC1, is it possible to ping PC3? _____

What is the success rate? _____

From the PC1, is it possible to ping PC4? _____

What is the success rate? _____

From the PC4, is it possible to ping PC2? _____

What is the success rate? _____

From the PC4, is it possible to ping PC3? _____

What is the success rate? _____

Step 4: View the routing table on R2.

Both the R1 and R3 are advertising routes to the 172.30.0.0/16 network; therefore, there are two entries for this network in the R2 routing table. The R2 routing table only shows the major classful network address of 172.30.0.0—it does not show any of the subnets for this network that are used on the LANs attached to R1 and R3. Because the routing metric is the same for both entries, the router alternates the routes that are used when forwarding packets that are destined for the 172.30.0.0/16 network.

```
R2#show ip route
```

Output omitted

```
10.0.0.0/16 is subnetted, 1 subnets
C    10.1.0.0 is directly connected, FastEthernet0/0
R    172.30.0.0/16 [120/1] via 209.165.200.230, 00:00:24, Serial0/0/0
    [120/1] via 209.165.200.234, 00:00:15, Serial0/0/1
209.165.200.0/30 is subnetted, 2 subnets
C    209.165.200.228 is directly connected, Serial0/0/0
C    209.165.200.232 is directly connected, Serial0/0/1
```

Step 5: Examine the routing table on the R1 router.

Both R1 and R3 are configured with interfaces on a discontinuous network, 172.30.0.0. The 172.30.0.0 subnets are physically and logically divided by at least one other classful or major network—in this case, the two serial networks 209.165.200.228/30 and 209.165.200.232/30. Classful routing protocols like RIPv1 summarize networks at major network boundaries. Both R1 and R3 will be summarizing 172.30.0.0/24 subnets to 172.30.0.0/16. Because the route to 172.30.0.0/16 is directly connected, and because R1 does not have any specific routes for the 172.30.0.0 subnets on R3, packets destined for the R3 LANs will not be forwarded properly.

```
R1#show ip route
```

Output omitted

```
R    10.0.0.0/8 [120/1] via 209.165.200.229, 00:00:02, Serial0/0/0
    172.30.0.0/24 is subnetted, 2 subnets
C    172.30.1.0 is directly connected, FastEthernet0/0
C    172.30.2.0 is directly connected, FastEthernet0/1
209.165.200.0/30 is subnetted, 2 subnets
C    209.165.200.228 is directly connected, Serial0/0/0
R    209.165.200.232 [120/1] via 209.165.200.229, 00:00:02, Serial0/0/0
```

Step 6: Examine the routing table on the R3 router.

R3 only shows its own subnets for 172.30.0.0 network: 172.30.100/24, 172.30.110/24, 172.30.200.16/28, and 172.30.200.32/28. R3 does not have any routes for the 172.30.0.0 subnets on R1.

```
R3#show ip route
```

Output omitted

```
R    10.0.0.0/8 [120/1] via 209.165.200.233, 00:00:19, Serial0/0/1
    172.30.0.0/16 is variably subnetted, 4 subnets, 2 masks
C    172.30.100.0/24 is directly connected, FastEthernet0/0
C    172.30.110.0/24 is directly connected, Loopback0
C    172.30.200.16/28 is directly connected, Loopback1
C    172.30.200.32/28 is directly connected, Loopback2
209.165.200.0/30 is subnetted, 2 subnets
R    209.165.200.228 [120/1] via 209.165.200.233, 00:00:19, Serial0/0/1
```

C 209.165.200.232 is directly connected, Serial0/0/1

Step 7: Examine the RIPv1 packets that are being received by R2.

Use the **debug ip rip** command to display RIP routing updates.

R2 is receiving the route 172.30.0.0, with 1 hop, from both R1 and R3. Because these are equal cost metrics, both routes are added to the R2 routing table. Because RIPv1 is a classful routing protocol, no subnet mask information is sent in the update.

```
R2#debug ip rip
RIP protocol debugging is on
RIP: received v1 update from 209.165.200.234 on Serial0/0/1
    172.30.0.0 in 1 hops
RIP: received v1 update from 209.165.200.230 on Serial0/0/0
    172.30.0.0 in 1 hops
```

R2 is sending only the routes for the 10.0.0.0 LAN and the two serial connections to R1 and R3. R1 and R3 are not receiving any information about the 172.30.0.0 subnet routes.

```
RIP: sending v1 update to 255.255.255.255 via Serial0/0/1
(209.165.200.233)
RIP: build update entries
    network 10.0.0.0 metric 1
    network 209.165.200.228 metric 1
RIP: sending v1 update to 255.255.255.255 via Serial0/0/0
(209.165.200.229)
RIP: build update entries
    network 10.0.0.0 metric 1
    network 209.165.200.232 metric 1
```

When you are finished, turn off the debugging.

```
R2#undebug all
```

Task 4: Configure RIP Version 2.

Step 1: Use the `version 2` command to enable RIP version 2 on each of the routers.

```
R2(config)#router rip
R2(config-router)#version 2

R1(config)#router rip
R1(config-router)#version 2

R3(config)#router rip
R3(config-router)#version 2
```

RIPv2 messages include the subnet mask in a field in the routing updates. This allows subnets and their masks to be included in the routing updates. However, by default RIPv2 summarizes networks at major network boundaries, just like RIPv1, except that the subnet mask is included in the update.

Step 2: Verify that RIPv2 is running on the routers.

The **debug ip rip**, **show ip protocols**, and **show run** commands can all be used to confirm that RIPv2 is running. The output of the **show ip protocols** command for R1 is shown below.

```
R1# show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 7 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2

  Interface          Send  Recv  Triggered RIP  Key-chain
FastEthernet0/0      2      2
FastEthernet0/1      2      2
Serial0/0/0          2      2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  172.30.0.0
  209.165.200.0
Passive Interface(s):
  FastEthernet0/0
  FastEthernet0/1
Routing Information Sources:
  Gateway         Distance      Last Update
  209.165.200.229    120
Distance: (default is 120)
```

Task 5: Examine the Automatic Summarization of Routes.

The LANs connected to R1 and R3 are still composed of discontinuous networks. R2 still shows two equal cost paths to the 172.30.0.0/16 network in the routing table. R2 still shows only the major classful network address of 172.30.0.0 and does not show any of the subnets for this network.

```
R2#show ip route
```

Output omitted

```
    10.0.0.0/16 is subnetted, 1 subnets
C       10.1.0.0 is directly connected, FastEthernet0/0
R       172.30.0.0/16 [120/1] via 209.165.200.230, 00:00:07, Serial0/0/0
                    [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
    209.165.200.0/30 is subnetted, 2 subnets
C       209.165.200.228 is directly connected, Serial0/0/0
C       209.165.200.232 is directly connected, Serial0/0/1
```

R1 still shows only its own subnets for the 172.30.0.0 network. R1 still does not have any routes for the 172.30.0.0 subnets on R3.

```
R1#show ip route
```

Output omitted

```
R    10.0.0.0/8 [120/1] via 209.165.200.229, 00:00:09, Serial0/0/0
    172.30.0.0/24 is subnetted, 2 subnets
C    172.30.1.0 is directly connected, FastEthernet0/0
C    172.30.2.0 is directly connected, FastEthernet0/1
    209.165.200.0/30 is subnetted, 2 subnets
C    209.165.200.228 is directly connected, Serial0/0/0
R    209.165.200.232 [120/1] via 209.165.200.229, 00:00:09, Serial0/0/0
```

R3 still only shows its own subnets for the 172.30.0.0 network. R3 still does not have any routes for the 172.30.0.0 subnets on R1.

```
R3#show ip route
```

Output omitted

```
R    10.0.0.0/8 [120/1] via 209.165.200.233, 00:00:16, Serial0/0/1
    172.30.0.0/16 is variably subnetted, 4 subnets, 2 masks
C    172.30.100.0/24 is directly connected, FastEthernet0/0
C    172.30.110.0/24 is directly connected, Loopback0
C    172.30.200.16/28 is directly connected, Loopback1
C    172.30.200.32/28 is directly connected, Loopback2
    209.165.200.0/30 is subnetted, 2 subnets
R    209.165.200.228 [120/1] via 209.165.200.233, 00:00:16, Serial0/0/1
C    209.165.200.232 is directly connected, Serial0/0/1
```

Use the output of the **debug ip rip** command to answer the following questions:

What entries are included in the RIP updates sent out from R3?

On R2, what routes are in the RIP updates that are received from R3?

R3 is not sending any of the 172.30.0.0 subnets—only the summarized route of 172.30.0.0/16, including the subnet mask. This is why R2 and R1 are not seeing the 172.30.0.0 subnets on R3.

Task 6: Disable Automatic Summarization.

The **no auto-summary** command is used to turn off automatic summarization in RIPv2. Disable auto summarization on all routers. The routers will no longer summarize routes at major network boundaries.

```
R2 (config)#router rip
R2 (config-router)#no auto-summary

R1 (config)#router rip
R1 (config-router)#no auto-summary

R3 (config)#router rip
R3 (config-router)#no auto-summary
```

The **show ip route** and **ping** commands can be used to verify that automatic summarization is off.

Task 7: Examine the Routing Tables.

The LANs connected to R1 and R3 should now be included in all three routing tables.

```
R2#show ip route
```

Output omitted

```
10.0.0.0/16 is subnetted, 1 subnets
C    10.1.0.0 is directly connected, FastEthernet0/0
    172.30.0.0/16 is variably subnetted, 7 subnets, 3 masks
R    172.30.0.0/16 [120/1] via 209.165.200.230, 00:01:28, Serial0/0/0
    [120/1] via 209.165.200.234, 00:01:56, Serial0/0/1
R    172.30.1.0/24 [120/1] via 209.165.200.230, 00:00:08, Serial0/0/0
    172.30.2.0/24 [120/1] via 209.165.200.230, 00:00:08, Serial0/0/0
R    172.30.100.0/24 [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
R    172.30.110.0/24 [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
R    172.30.200.16/28 [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
R    172.30.200.32/28 [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
    209.165.200.0/30 is subnetted, 2 subnets
C    209.165.200.228 is directly connected, Serial0/0/0
C    209.165.200.232 is directly connected, Serial0/0/1
```

```
R1#show ip route
```

Output omitted

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R    10.0.0.0/8 [120/1] via 209.165.200.229, 00:02:13, Serial0/0/0
R    10.1.0.0/16 [120/1] via 209.165.200.229, 00:00:21, Serial0/0/0
    172.30.0.0/16 is variably subnetted, 6 subnets, 2 masks
C    172.30.1.0/24 is directly connected, FastEthernet0/0
```

```

C      172.30.2.0/24 is directly connected, FastEthernet0/1
R      172.30.100.0/24 [120/2] via 209.165.200.229, 00:00:21, Serial0/0/0
R      172.30.110.0/24 [120/2] via 209.165.200.229, 00:00:21, Serial0/0/0
R      172.30.200.16/28 [120/2] via 209.165.200.229, 00:00:21, Serial0/0/0
R      172.30.200.32/28 [120/2] via 209.165.200.229, 00:00:21, Serial0/0/0
      209.165.200.0/30 is subnetted, 2 subnets
C      209.165.200.228 is directly connected, Serial0/0/0
R      209.165.200.232 [120/1] via 209.165.200.229, 00:00:21, Serial0/0/0

```

R3#**show ip route**

Output omitted

```

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R      10.0.0.0/8 [120/1] via 209.165.200.233, 00:02:28, Serial0/0/1
R      10.1.0.0/16 [120/1] via 209.165.200.233, 00:00:08, Serial0/0/1
      172.30.0.0/16 is variably subnetted, 6 subnets, 2 masks
R      172.30.1.0/24 [120/2] via 209.165.200.233, 00:00:08, Serial0/0/1
R      172.30.2.0/24 [120/2] via 209.165.200.233, 00:00:08, Serial0/0/1
C      172.30.100.0/24 is directly connected, FastEthernet0/0
C      172.30.110.0/24 is directly connected, Loopback0
C      172.30.200.16/28 is directly connected, Loopback1
C      172.30.200.32/28 is directly connected, Loopback2
      209.165.200.0/30 is subnetted, 2 subnets
R      209.165.200.228 [120/1] via 209.165.200.233, 00:00:08, Serial0/0/1
C      209.165.200.232 is directly connected, Serial0/0/1

```

Use the output of the **debug ip rip** command to answer the following questions:

What entries are included in the RIP updates sent out from R1?

On R2, what routes are in the RIP updates that are received from R1?

Are the subnet masks now included in the routing updates? _____

Task 8: Verify Network Connectivity.

Step 1: Check connectivity between R2 router and PCs.

From R2, how many ICMP messages are successful when pinging PC1?

From R2, how many ICMP messages are successful when pinging PC4?

Step 2: Check the connectivity between the PCs.

From PC1, is it possible to ping PC2? _____

What is the success rate? _____

From PC1, is it possible to ping PC3? _____

What is the success rate? _____

From PC1, is it possible to ping PC4? _____

What is the success rate? _____

From PC4, is it possible to ping PC2? _____

What is the success rate? _____

From PC4, is it possible to ping PC3? _____

What is the success rate? _____

Task 9: Documentation

On each router, capture the following command output to a text (.txt) file and save for future reference.

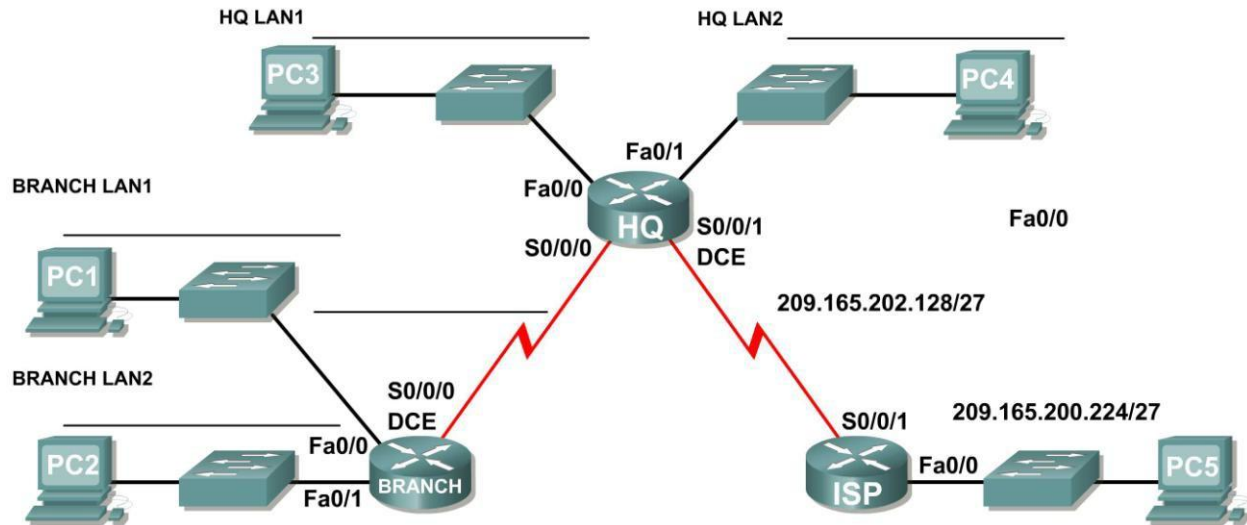
```
show running-config
show ip route
show ip interface brief
show ip protocols
```

Task 10: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

14 - RIPv2 Challenge Configuration Lab

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
BRANCH	Fa0/0			N/A
	Fa0/1			N/A
	S0/0/0			N/A
HQ	Fa0/0			N/A
	Fa0/1			N/A
	S0/0/0			N/A
	S0/0/1			N/A
ISP	Fa0/0			N/A
	S0/0/1			N/A
PC1	NIC			
PC2	NIC			
PC3	NIC			
PC4	NIC			
PC5	NIC			

Learning Objectives

Upon completion of this lab, you will be able to:

- Create an efficient VLSM design given the requirements.
- Assign appropriate addresses to interfaces and document the addresses.
- Cable a network according to the Topology Diagram.
- Erase the startup configuration and reload a router to the default state.
- Configure routers including RIP version 2.
- Configure and propagate a static default route.
- Verify RIP version 2 operation.
- Test and verify full connectivity.
- Reflect upon and document the network implementation.

Scenario

In this lab activity, you will be given a network address that must be subnetted using VLSM to complete the addressing of the network shown in the Topology Diagram. A combination of RIP version 2 and static routing will be required so that hosts on networks that are not directly connected will be able to communicate with each other.

Task 1: Subnet the Address Space.

Step 1: Examine the network requirements.

The addressing for the network has the following requirements:

- The ISP LAN will use the 209.165.200.224/27 network.
 - The link between ISP and HQ will use the 209.165.202.128/27 network.
 - The 192.168.40.0/24 network must be subnetted using VLSM for all other addresses in the network.
 - The HQ LAN1 will require 50 host IP addresses.
 - The HQ LAN2 will require 50 host IP addresses.
 - The BRANCH LAN1 will require 30 host IP addresses.
 - The BRANCH LAN2 will require 12 host IP addresses.
 - The link between HQ and BRANCH will require an IP address at each end.
- (Note: Remember that the interfaces of network devices are also host IP addresses and are included in the above addressing requirements.)

Step 2: Consider the following questions when creating your network design:

- How many subnets need to be created from the 192.168.40.0/24 network? _____
- How many total IP addresses are required from the 192.168.40.0/24 network? _____
- What subnet mask will be used for the HQ LAN1 subnet? _____
- What is the maximum number of host addresses that could be used on this subnet? _____
- What subnet mask will be used for the HQ LAN2 subnet? _____
- What is the maximum number of host addresses that could be used on this subnet? _____
- What subnet mask will be used for the BRANCH LAN1 subnet? _____

What is the maximum number of host addresses that could be used on this subnet? _____

What subnet mask will be used for the BRANCH LAN2 subnet? _____

What is the maximum number of host addresses that could be used on this subnet? _____

What subnet mask will be used for the link between the HQ and BRANCH routers?

What is the maximum number of host addresses that could be used on this subnet? _____

Step 3: Assign subnetwork addresses to the Topology Diagram.

1. Assign subnet 0 of the 192.168.40.0 network to the HQ LAN1 subnet.
What is the network address of this subnet? _____
2. Assign subnet 1 of the 192.168.40.0 network to the HQ LAN2 subnet.
What is the network address of this subnet? _____
3. Assign subnet 2 of the 192.168.40.0 network to the BRANCH LAN1 subnet.
What is the network address of this subnet? _____
4. Assign subnet 3 of the 192.168.40.0 network to the BRANCH LAN2 subnet.
What is the network address of this subnet? _____
5. Assign subnet 4 of the 192.168.40.0 network to the link between the HQ and BRANCH routers.
What is the network address of this subnet? _____

Task 2: Determine Interface Addresses.

Step 1: Assign appropriate addresses to the device interfaces.

1. Assign the first valid host address in the 209.165.200.224/27 network to the LAN interface on the ISP router.
2. Assign the last valid host address in 209.165.200.224/27 network to PC5.
3. Assign the first valid host address in the 209.165.202.128/27 network to the WAN interface of ISP.
4. Assign the last valid host address in the 209.165.202.128/27 network to the Serial 0/0/1 interface of HQ.
5. Assign the first valid host address in the HQ LAN1 network to the LAN1 interface of HQ.
6. Assign the last valid host address in the HQ LAN1 network to PC 3.
7. Assign the first valid host address in the HQ LAN2 network to the LAN2 interface of HQ.
8. Assign the last valid host address in the HQ LAN2 network to PC 4.
9. Assign the first valid host address in the HQ/BRANCH WAN link to the Serial 0/0/0 interface of HQ.
10. Assign the last valid host address in the HQ/BRANCH WAN link to the Serial 0/0/0 interface of BRANCH.

11. Assign the first valid host address in the BRANCH LAN1 network to the LAN1 interface of BRANCH.
12. Assign the last valid host address in the BRANCH LAN1 network to PC 1.
13. Assign the first valid host address in the BRANCH LAN2 network to the LAN2 interface of BRANCH.
14. Assign the last valid host address in the BRANCH LAN2 network to PC 2.

Step 2: Document the addresses to be used in the table provided under the Topology Diagram.

Task 3: Prepare the Network.

Step 1: Cable a network that is similar to the one in the Topology Diagram.

You can use any current router in your lab as long as it has the required interfaces as shown in the topology.

Note: If you use 1700, 2500, or 2600 routers, the router outputs and interface descriptions will appear different.

Step 2: Clear any existing configurations on the routers.

Task 4: Perform Basic Router Configurations.

Perform basic configuration of the BRANCH, HQ, and ISP routers according to the following guidelines:

1. Configure the router hostname.
2. Disable DNS lookup.
3. Configure an EXEC mode password.
4. Configure a message-of-the-day banner.
5. Configure a password for console connections.
6. Configure a password for VTY connections.
7. Synchronize unsolicited messages and debug output with solicited output and prompts for the console and virtual terminal lines.
8. Configure an EXEC timeout of 15 minutes.

Task 5: Configure and Activate Serial and Ethernet Addresses

Step 1: Configure the BRANCH, HQ, and ISP routers.

Configure the interfaces on BRANCH, HQ, and ISP with the IP addresses from the Addressing Table provided under the Topology Diagram.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 2: Configure the Ethernet interfaces of PC1, PC2, PC3, PC4, and PC5.

Configure the Ethernet interfaces of PC1, PC2, PC3, PC4, and PC5 with the IP addresses from the Addressing Table provided under the Topology Diagram.

Task 6: Verify Connectivity to Next-Hop Device.

You should *not* have connectivity between end devices yet. However, you can test connectivity between two routers and between an end device and its default gateway.

Step 1: Verify BRANCH connectivity.

Verify that BRANCH can ping across the WAN link to HQ and that HQ can ping across the WAN link it shares with ISP.

Step 2: Verify that PC1, PC2, PC3, PC4, and PC5 can ping their respective default gateways.

Task 7: Configure RIPv2 Routing on the BRANCH Router.

Consider the networks that need to be included in the RIP updates that are sent out by BRANCH. What networks are present in the BRANCH routing table? List the networks with slash notation.

What commands are required to enable RIP version 2 and include the connected networks in the routing updates?

Are there any router interfaces that do not need to have RIP updates sent out? _____

What command is used to disable RIP updates on these interfaces?

Task 8: Configure RIPv2 and Static Routing on HQ.

Consider the type of static routing that is needed on HQ.

What networks are present in the HQ routing table? List the networks with slash notation.

Static default route will need to be configured to send all packets with destination addresses that are not in the routing table to ISP. What command is needed to accomplish this? Use the appropriate exit interface on HQ in the command.

What commands are required to enable RIP version 2 and include the LAN1 and LAN2 networks as well as the link between HQ and BRANCH in the routing updates?

Are there any router interfaces that do not need to have RIP updates sent out? _____

What command is used to disable RIP updates on these interfaces?

HQ needs to send the default route information to BRANCH in the RIP updates. What command is used to configure this?

Task 9: Configure Static Routing on the ISP Router.

Note: In a real-world implementation of this topology, you would not be configuring the ISP router. However, your service provider is an active partner in solving your connectivity needs. Service provider administrators are human, too, and make mistakes. Therefore, it is important that you understand the types of errors an ISP could make that would cause your networks to lose connectivity.

Static routes will need to be configured on ISP for all traffic that is destined for the RFC 1918 addresses that are used on the BRANCH LANs, HQ LANs, and the link between the BRANCH and HQ routers.

What are the commands that will need to be configured on the ISP router to accomplish this?

Task 10: Verify the Configurations.

Answer the following questions to verify that the network is operating as expected:

From PC1, is it possible to ping PC3? _____

From PC1, is it possible to ping the PC5? _____

From PC4, is it possible to ping the PC5? _____

The answer to the above questions should be **yes**. If any of the above pings failed, check your physical connections and configurations. Refer to your basic troubleshooting techniques used in the Chapter 1 labs.

What routes are present in the routing table of the BRANCH router?

What is the gateway of last resort in the routing table of BRANCH?

What routes are present in the routing table of the HQ router?

What networks are present in the routing table of ISP?

What networks are present in the RIP updates sent from HQ?

What networks are present in the RIP updates sent from BRANCH?

Task 11: Reflection

Why is it necessary to use RIPv2 instead of RIPv1 with this network design?

Task 12: Document the Router Configurations

On each router, capture the following command output to a text (.txt) file and save for future reference.

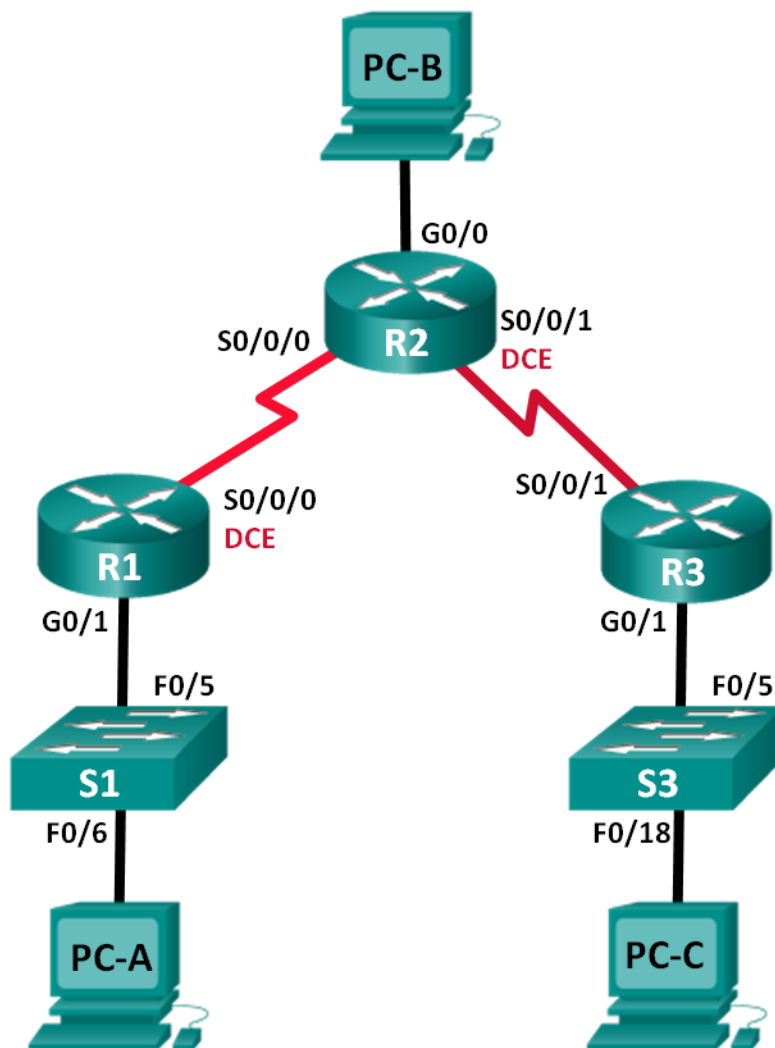
- Running configuration
- Routing table
- Interface summarization

Task 13: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

15 – Configuring Basic RIPv2 and RIPvng

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	172.30.10.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	G0/0	209.165.201.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	172.30.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	N/A	VLAN 1	N/A	N/A
S3	N/A	VLAN 1	N/A	N/A
PC-A	NIC	172.30.10.3	255.255.255.0	172.30.10.1
PC-B	NIC	209.165.201.2	255.255.255.0	209.165.201.1
PC-C	NIC	172.30.30.3	255.255.255.0	172.30.30.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure and Verify RIPv2 Routing

- Configure and verify RIPv2 is running on routers.
- Configure a passive interface.
- Examine routing tables.
- Disable automatic summarization.
- Configure a default route.
- Verify end-to-end connectivity.

Part 3: Configure IPv6 on Devices

Part 4: Configure and Verify RIPvng Routing

- Configure and verify RIPvng is running on routers.
- Examine routing tables.
- Configure a default route.
- Verify end-to-end connectivity.

Background / Scenario

RIP version 2 (RIPv2) is used for routing of IPv4 addresses in small networks. RIPv2 is a classless, distance-vector routing protocol, as defined by RFC 1723. Because RIPv2 is a classless routing protocol, subnet masks are included in the routing updates. By default, RIPv2 automatically summarizes networks at major network boundaries. When automatic summarization has been disabled, RIPv2 no longer summarizes networks to their classful address at boundary routers.

RIPng (RIP Next Generation) is a distance-vector routing protocol for routing IPv6 addresses, as defined by RFC 2080. RIPng is based on RIPv2 and has the same administrative distance and 15-hop limitation.

In this lab, you will configure the network topology with RIPv2 routing, disable automatic summarization, propagate a default route, and use CLI commands to display and verify RIP routing information. You will then configure the network topology with IPv6 addresses, configure RIPng, propagate a default route, and use CLI commands to display and verify RIPng routing information.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and Serial cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the router and switch.

Step 3: Configure basic settings for each router and switch.

- Disable DNS lookup.
- Configure device names as shown in the topology.
- Configure password encryption.
- Assign **class** as the privileged EXEC password.
- Assign **cisco** as the console and vty passwords.
- Configure a MOTD banner to warn users that unauthorized access is prohibited.
- Configure **logging synchronous** for the console line.
- Configure the IP address listed in the Addressing Table for all interfaces.
- Configure a description to each interface with an IP address.
- Configure the clock rate if applicable to the DCE serial interface.
- Copy the running-configuration to the startup-configuration.

Step 4: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

Step 5: Test connectivity.

At this point, the PCs are unable to ping each other.

- Each workstation should be able to ping the attached router. Verify and troubleshoot if necessary.
- The routers should be able to ping one another. Verify and troubleshoot if necessary.

Part 2: Configure and Verify RIPv2 Routing

In Part 2, you will configure RIPv2 routing on all routers in the network and then verify that routing tables are updated correctly. After RIPv2 has been verified, you will disable automatic summarization, configure a default route, and verify end-to-end connectivity.

Step 1: Configure RIPv2 routing.

- On R1, configure RIPv2 as the routing protocol and advertise the appropriate networks.

```
R1# config t
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# passive-interface g0/1
R1(config-router)# network 172.30.0.0
R1(config-router)# network 10.0.0.0
```

The **passive-interface** command stops routing updates out the specified interface. This process prevents unnecessary routing traffic on the LAN. However, the network that the specified interface belongs to is still advertised in routing updates that are sent out across other interfaces.

- Configure RIPv2 on R3 and use the **network** statement to add appropriate networks and prevent routing updates on the LAN interface.
- Configure RIPv2 on R2. Do not advertise the 209.165.201.0 network.

Note: It is not necessary to make the G0/0 interface passive on R2 because the network associated with this interface is not being advertised.

Step 2: Examine current state of network.

- The status of the two serial links can quickly be verified using the **show ip interface brief** command on R2.

```
R2# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	209.165.201.1	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/0/0	10.1.1.2	YES	manual	up	up
Serial0/0/1	10.2.2.2	YES	manual	up	up

- Check connectivity between PCs.

From PC-A, is it possible to ping PC-B? _____ Why? _____

From PC-A, is it possible to ping PC-C? _____ Why? _____

From PC-C, is it possible to ping PC-B? _____ Why? _____

From PC-C, is it possible to ping PC-A? _____ Why? _____

- c. Verify that RIPv2 is running on the routers.

You can use the **debug ip rip**, **show ip protocols**, and **show run** commands to confirm that RIPv2 is running. The **show ip protocols** command output for R1 is shown below.

```
R1# show ip protocols
Routing Protocol is "rip"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Sending updates every 30 seconds, next due in 7 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv Triggered RIP Key-chain
  Serial0/0/0         2      2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.30.0.0
Passive Interface(s):
  GigabitEthernet0/1
Routing Information Sources:
  Gateway         Distance    Last Update
  10.1.1.2         120
Distance: (default is 120)
```

When issuing the **debug ip rip** command on R2, what information is provided that confirms RIPv2 is running?

When you are finished observing the debugging outputs, issue the **undebug all** command at the privileged EXEC prompt.

When issuing the **show run** command on R3, what information is provided that confirms RIPv2 is running?

- d. Examine the automatic summarization of routes.

The LANs connected to R1 and R3 are composed of discontinuous networks. R2 displays two equal-cost paths to the 172.30.0.0/16 network in the routing table. R2 displays only the major classful network address of 172.30.0.0 and does not display any of the subnets for this network.

```
R2# show ip route
<Output omitted>
  10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
```

```

R      172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:23, Serial0/0/1
      [120/1] via 10.1.1.1, 00:00:09, Serial0/0/0
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C      209.165.201.0/24 is directly connected, GigabitEthernet0/0
L      209.165.201.1/32 is directly connected, GigabitEthernet0/0

```

R1 displays only its own subnets for the 172.30.0.0 network. R1 does not have any routes for the 172.30.0.0 subnets on R3.

R1# **show ip route**

<Output omitted>

```

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C      10.1.1.0/30 is directly connected, Serial0/0/0
L      10.1.1.1/32 is directly connected, Serial0/0/0
R      10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:21, Serial0/0/0
      172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.30.10.0/24 is directly connected, GigabitEthernet0/1
L      172.30.10.1/32 is directly connected, GigabitEthernet0/1

```

R3 only displays its own subnets for the 172.30.0.0 network. R3 does not have any routes for the 172.30.0.0 subnets on R1.

R3# **show ip route**

<Output omitted>

```

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C      10.2.2.0/30 is directly connected, Serial0/0/1
L      10.2.2.1/32 is directly connected, Serial0/0/1
R      10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:23, Serial0/0/1
      172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.30.30.0/24 is directly connected, GigabitEthernet0/1
L      172.30.30.1/32 is directly connected, GigabitEthernet0/1

```

Use the **debug ip rip** command on R2 to determine the routes received in the RIP updates from R3 and list them here.

R3 is not sending any of the 172.30.0.0 subnets, only the summarized route of 172.30.0.0/16, including the subnet mask. Therefore, the routing tables on R1 and R2 do not display the 172.30.0.0 subnets on R3.

Step 3: Disable automatic summarization.

- The **no auto-summary** command is used to turn off automatic summarization in RIPv2. Disable auto summarization on all routers. The routers will no longer summarize routes at major classful network boundaries. R1 is shown here as an example.

```

R1(config)# router rip
R1(config-router)# no auto-summary

```

- Issue the **clear ip route *** command to clear the routing table.

```

R1(config-router)# end
R1# clear ip route *

```

- Examine the routing tables. Remember will it take some time to converge the routing tables after clearing them.

The LAN subnets connected to R1 and R3 should now be included in all three routing tables.

R2# **show ip route**

<Output omitted>

Gateway of last resort is not set

```

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
      172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
R       172.30.0.0/16 [120/1] via 10.2.2.1, 00:01:01, Serial0/0/1
          [120/1] via 10.1.1.1, 00:01:15, Serial0/0/0
R       172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:21, Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:04, Serial0/0/1
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.0/24 is directly connected, GigabitEthernet0/0
L       209.165.201.1/32 is directly connected, GigabitEthernet0/0
```

R1# **show ip route**

<Output omitted>

Gateway of last resort is not set

```

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
R       10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:12, Serial0/0/0
      172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.30.10.0/24 is directly connected, GigabitEthernet0/1
L       172.30.10.1/32 is directly connected, GigabitEthernet0/1
R       172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:12, Serial0/0/0
```

R3# **show ip route**

<Output omitted>

```

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:23, Serial0/0/1
      172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.30.30.0/24 is directly connected, GigabitEthernet0/1
L       172.30.30.1/32 is directly connected, GigabitEthernet0/1
R       172.30.10.0 [120/2] via 10.2.2.2, 00:00:16, Serial0/0/1
```

- d. Use the **debug ip rip** command on R2 to exam the RIP updates.

R2# **debug ip rip**

After 60 seconds, issue the **no debug ip rip** command.

What routes are in the RIP updates that are received from R3? _____

Are the subnet masks now included in the routing updates? _____

Step 4: Configure and redistribute a default route for Internet access.

- From R2, create a static route to network 0.0.0.0 0.0.0.0, using the **ip route** command. This forwards any unknown destination address traffic to the R2 G0/0 toward PC-B, simulating the Internet by setting a Gateway of Last Resort on the R2 router.

```
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.2
```

- R2 will advertise a route to the other routers if the **default-information originate** command is added to its RIP configuration.

```
R2(config)# router rip
```

```
R2(config-router)# default-information originate
```

Step 5: Verify the routing configuration.

- View the routing table on R1.

```
R1# show ip route
```

<Output omitted>

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

R* 0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks

C 10.1.1.0/30 is directly connected, Serial0/0/0

L 10.1.1.1/32 is directly connected, Serial0/0/0

R 10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0

172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks

C 172.30.10.0/24 is directly connected, GigabitEthernet0/1

L 172.30.10.1/32 is directly connected, GigabitEthernet0/1

R 172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:13, Serial0/0/0

How can you tell from the routing table that the subnetted network shared by R1 and R3 has a pathway for Internet traffic?

- View the routing table on R2.

How is the pathway for Internet traffic provided in its routing table?

Step 6: Verify connectivity.

- Simulate sending traffic to the Internet by pinging from PC-A and PC-C to 209.165.201.2.

Were the pings successful? _____

- Verify that hosts within the subnetted network can reach each other by pinging between PC-A and PC-C.

Were the pings successful? _____

Note: It may be necessary to disable the PCs firewall.

Part 3: Configure IPv6 on Devices

In Part 3, you will configure all interfaces with IPv6 addresses and verify connectivity.

Addressing Table

Device	Interface	IPv6 Address / Prefix Length	Default Gateway
R1	G0/1	2001:DB8:ACAD:A::1/64 FE80::1 link-local	N/A
	S0/0/0	2001:DB8:ACAD:12::1/64 FE80::1 link-local	N/A
R2	G0/0	2001:DB8:ACAD:B::2/64 FE80::2 link-local	N/A
	S0/0/0	2001:DB8:ACAD:12::2/64 FE80::2 link-local	N/A
	S0/0/1	2001:DB8:ACAD:23::2/64 FE80::2 link-local	N/A
R3	G0/1	2001:DB8:ACAD:C::3/64 FE80::3 link-local	N/A
	S0/0/1	2001:DB8:ACAD:23::3/64 FE80::3 link-local	N/A
PC-A	NIC	2001:DB8:ACAD:A::A/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::B/64	FE80::2
PC-C	NIC	2001:DB8:ACAD:C::C/64	FE80::3

Step 1: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

Step 2: Configure IPv6 on routers.

Note: Assigning an IPv6 address in addition to an IPv4 address on an interface is known as dual stacking. This is because both IPv4 and IPv6 protocol stacks are active.

- For each router interface, assign the global and link local address from the Addressing Table.
- Enable IPv6 routing on each router.
- Enter the appropriate command to verify IPv6 addresses and link status. Write the command in the space below.

- Each workstation should be able to ping the attached router. Verify and troubleshoot if necessary.
- The routers should be able to ping one another. Verify and troubleshoot if necessary.

Part 4: Configure and Verify RIPng Routing

In Part 4, you will configure RIPng routing on all routers, verify that routing tables are updated correctly, configure and distribute a default route, and verify end-to-end connectivity.

Step 1: Configure RIPng routing.

With IPv6, it is common to have multiple IPv6 addresses configured on an interface. The network statement has been eliminated in RIPng. RIPng routing is enabled at the interface level instead, and is identified by a locally significant process name as multiple processes can be created with RIPng.

- a. Issue the **ipv6 rip Test1 enable** command for each interface on R1 that is to participate in RIPng routing, where **Test1** is the locally significant process name.

```
R1(config)# interface g0/1
R1(config)# ipv6 rip Test1 enable
R1(config)# interface s0/0/0
R1(config)# ipv6 rip Test1 enable
```

- b. Configure RIPng for the serial interfaces on R2 with **Test2** as the process name. Do not configure for the G0/0 interface.
- c. Configure RIPng for each interface on R3 with **Test3** as the process name.
- d. Verify that RIPng is running on the routers.

The **show ipv6 protocols**, **show run**, **show ipv6 rip database**, and **show ipv6 rip process name** commands can all be used to confirm that RIPng is running. On R1, issue the **show ipv6 protocols** command.

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip Test1"
  Interfaces:
    Serial0/0/0
    GigabitEthernet0/1
  Redistribution:
    None
```

How is the RIPng listed in the output? _____

- e. Issue the **show ipv6 rip Test1** command.

```
R1# show ipv6 rip Test1
RIP process "Test1", port 521, multicast-group FF02::9, pid 314
  Administrative distance is 120. Maximum paths is 16
  Updates every 30 seconds, expire after 180
  Holddown lasts 0 seconds, garbage collect after 120
  Split horizon is on; poison reverse is off
  Default routes are not generated
  Periodic updates 1, trigger updates 0
  Full Advertisement 0, Delayed Events 0
  Interfaces:
    GigabitEthernet0/1
    Serial0/0/0
  Redistribution:
```

None

How are RIPv2 and RIPv6 similar?

- f. Inspect the IPv6 routing table on each router. Write the appropriate command used to view the routing table in the space below.
-

On R1, how many routes have been learned by RIPv6? _____

On R2, how many routes have been learned by RIPv6? _____

On R3, how many routes have been learned by RIPv6? _____

- g. Check connectivity between PCs.

From PC-A, is it possible to ping PC-B? _____

From PC-A, is it possible to ping PC-C? _____

From PC-C, is it possible to ping PC-B? _____

From PC-C, is it possible to ping PC-A? _____

Why are some pings successful and others not?

Step 2: Configure and redistribute a default route.

- a. From R2, create a static default route to network ::0/64 using the **ipv6 route** command, and the IP address of exit interface G0/0. This forwards any unknown destination address traffic to the R2 G0/0 interface toward PC-Bs, simulating the Internet. Write the command used in the space below.
-

- b. Static routes can be included in RIPv6 updates by using the **ipv6 rip process name default-information originate** command in interface configuration mode. Configure the serial links on R2 to send the default route in RIPv6 updates.

```
R2(config)# int s0/0/0
```

```
R2(config-rtr)# ipv6 rip Test2 default-information originate
```

```
R2(config)# int s0/0/1
```

```
R2(config-rtr)# ipv6 rip Test2 default-information originate
```

Step 3: Verify the routing configuration.

- a. View the IPv6 routing table on R2.

```
R2# show ipv6 route
```

```
IPv6 Routing Table - 10 entries
```

```
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
```

```
U - Per-user Static route, M - MIPv6
```

```
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
```

```
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
```

```
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
```

```
D - EIGRP, EX - EIGRP external
```

```
S    ::/64 [1/0]
```

```

        via 2001:DB8:ACAD:B::B
R   2001:DB8:ACAD:A::/64 [120/2]
    via FE80::1, Serial0/0/0
C   2001:DB8:ACAD:B::/64 [0/0]
    via ::, GigabitEthernet0/1
L   2001:DB8:ACAD:B::2/128 [0/0]
    via ::, GigabitEthernet0/1
R   2001:DB8:ACAD:C::/64 [120/2]
    via FE80::3, Serial0/0/1
C   2001:DB8:ACAD:12::/64 [0/0]
    via ::, Serial0/0/0
L   2001:DB8:ACAD:12::2/128 [0/0]
    via ::, Serial0/0/0
C   2001:DB8:ACAD:23::/64 [0/0]
    via ::, Serial0/0/1
L   2001:DB8:ACAD:23::2/128 [0/0]
    via ::, Serial0/0/1
L   FF00::/8 [0/0]
    via ::, Null0

```

How can you tell from the routing table that R2 has a pathway for Internet traffic?

- b. View the routing tables on R1 and R3.

How is the pathway for Internet traffic provided in their routing tables?

Step 4: Verify connectivity.

Simulate sending traffic to the Internet by pinging from PC-A and PC-C to 2001:DB8:ACAD:B::B/64.

Were the pings successful? _____

Reflection

1. Why would you turn off automatic summarization for RIPv2?

2. In both scenarios, how did R1 and R3 learn the pathway to the Internet?

3. How are configuring RIPv2 and RIPv6 different?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

16 - Basic OSPF Configuration Lab

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the Topology Diagram
- Erase the startup configuration and reload a router to the default state
- Perform basic configuration tasks on a router
- Configure and activate interfaces Configure OSPF routing on all routers Configure OSPF router IDs
- Verify OSPF routing using show commands
- Configure a static default route
- Propagate default route to OSPF neighbors Configure OSPF Hello and Dead Timers Configure OSPF on a Multi-access network Configure OSPF priority
- Understand the OSPF election process
- Document the OSPF configuration

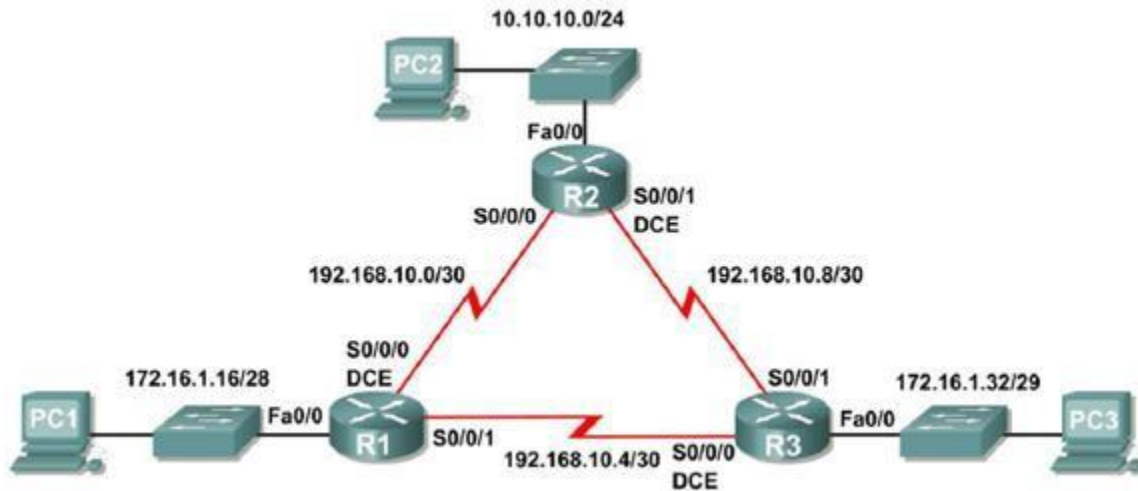
Scenarios

In this lab activity, there are two separate scenarios. In the first scenario, you will learn how to configure the routing protocol OSPF using the network shown in the Topology Diagram in Scenario A. The segments of the network have been subnetted using VLSM. OSPF is a classless routing protocol that can be used to provide subnet mask information in the routing updates. This will allow VLSM subnet information to be propagated throughout the network.

In the second scenario, you will learn to configure OSPF on a multi-access network. You will also learn to use the OSPF election process to determine the designated router (DR), backup designated router (BDR), and DROther states.

Scenario A: Basic OSPF Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.16.1.17	255.255.255.240	N/A
	S0/0/0	192.168.10.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	Fa0/0	10.10.10.1	255.255.255.0	N/A
	S0/0/0	192.168.10.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
R3	Fa0/0	172.16.1.33	255.255.255.248	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	NIC	172.16.1.20	255.255.255.240	172.16.1.17
PC2	NIC	10.10.10.10	255.255.255.0	10.10.10.1
PC3	NIC	172.16.1.35	255.255.255.248	172.16.1.33

Task 1: Prepare the Network.

Step 1: Cable a network that is similar to the one in the Topology Diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

Note: If you use 1700, 2500, or 2600 routers, the router outputs and interface descriptions will appear different.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations.

Perform basic configuration of the R1, R2, and R3 routers according to the following guidelines:

1. Configure the router hostname.
2. Disable DNS lookup.
3. Configure a privileged EXEC mode password.
4. Configure a message-of-the-day banner.
5. Configure a password for console connections.
6. Configure a password for VTY connections.

Task 3: Configure and Activate Serial and Ethernet Addresses.

Step 1: Configure interfaces on R1, R2, and R3.

Configure the interfaces on the R1, R2, and R3 routers with the IP addresses from the table under the Topology Diagram.

Step 2: Verify IP addressing and interfaces.

Use the `show ip interface brief` command to verify that the IP addressing is correct and that the interfaces are active.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 3: Configure Ethernet interfaces of PC1, PC2, and PC3.

Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses and default gateways from the table under the Topology Diagram.

Step 4: Test the PC configuration by pinging the default gateway from the PC.

Task 4: Configure OSPF on the R1 Router

Step 1: Use the router ospf command in global configuration mode to enable OSPF on the

R1 router. Enter a process ID of 1 for the *process-ID* parameter.

```
R1(config)#router ospf 1  
R1(config-router)#
```

Step 2: Configure the `network` statement for the LAN network.

Once you are in the Router OSPF configuration sub-mode, configure the LAN network 172.16.1.16/28 to be included in the OSPF updates that are sent out of R1.

The OSPF **network** command uses a combination of *network-address* and *wildcard-mask* similar to that which can be used by EIGRP. Unlike EIGRP, the wildcard mask in OSPF is required.

Use an area ID of 0 for the OSPF *area-id* parameter. 0 will be used for the OSPF area ID in all of the **network** statements in this topology.

```
R1(config-router)#network 172.16.1.16 0.0.0.15 area 0  
R1(config-router)#
```

Step 3: Configure the router to advertise the 192.168.10.0/30 network attached to the Serial0/0/0 interface.

```
R1(config-router)# network 192.168.10.0 0.0.0.3 area 0  
R1(config-router)#
```

Step 4: Configure the router to advertise the 192.168.10.4/30 network attached to the Serial0/0/1 interface.

```
R1(config-router)# network 192.168.10.4 0.0.0.3 area 0  
R1(config-router)#
```

Step 5: When you are finished with the OSPF configuration for R1, return to privileged EXEC mode.

```
R1(config-router)#end  
%SYS-5-CONFIG_I: Configured from console by console  
R1#
```

Task 5: Configure OSPF on the R2 and R3 Routers

Step 1: Enable OSPF routing on the R2 router using the `router ospf` command. Use a process ID of 1.

```
R2(config)#router ospf 1  
R2(config-router)#
```

Step 2: Configure the router to advertise the LAN network 10.10.10.0/24 in the OSPF updates.

```
R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
```

```
R2(config-router)#
```

Step 3: Configure the router to advertise the 192.168.10.0/30 network attached to the Serial0/0/0 interface.

```
R2(config-router)#network 192.168.10.0 0.0.0.3 area 0
R2(config-router)#
00:07:27: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.5 on Serial0/0/0
from EXCHANGE to FULL, Exchange Done
```

Notice that when the network for the serial link from R1 to R2 is added to the OSPF configuration, the router sends a notification message to the console stating that a neighbor relationship with another OSPF router has been established.

Step 4: Configure the router to advertise the 192.168.10.8/30 network attached to the Serial0/0/1 interface.

When you are finished, return to privileged EXEC mode.

```
R2(config-router)#network 192.168.10.8 0.0.0.3 area 0
R2(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R2#
```

Step 5: Configure OSPF on the R3 router using the `router ospf` and `network` commands.

Use a process ID of 1. Configure the router to advertise the three directly connected networks. When you are finished, return to privileged EXEC mode.

```
R3(config)#router ospf 1
R3(config-router)#network 172.16.1.32 0.0.0.7 area 0
R3(config-router)#network 192.168.10.4 0.0.0.3 area 0
R3(config-router)#
00:17:46: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.5 on Serial0/0/0
from LOADING to FULL, Loading Done
R3(config-router)#network 192.168.10.8 0.0.0.3 area 0
R3(config-router)#
00:18:01: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.9 on Serial0/0/1
from EXCHANGE to FULL, Exchange Done
R3(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R3#
```

Notice that when the networks for the serial links from R3 to R1 and R3 to R2 are added to the OSPF configuration, the router sends a notification message to the console stating that a neighbor relationship with another OSPF router has been established.

Task 6: Configure OSPF Router IDs

The OSPF router ID is used to uniquely identify the router in the OSPF routing domain. A router ID is an IP address. Cisco routers derive the Router ID in one of three ways and with the following precedence:

1. IP address configured with the OSPF **router-id** command.
2. Highest IP address of any of the router's loopback addresses.
3. Highest active IP address on any of the router's physical interfaces.

Step 1: Examine the current router IDs in the topology.

Since no router IDs or loopback interfaces have been configured on the three routers, the router ID for each router is determined by the highest IP address of any active interface.

What is the router ID for R1? _____

What is the router ID for R2? _____

What is the router ID for R3? _____

The router ID can also be seen in the output of the **show ip protocols**, **show ip ospf**, and **show ip ospf interfaces** commands.

R3#**show ip protocols**

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 192.168.10.10

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

<output omitted>

R3#**show ip ospf**

Routing Process "ospf 1" with ID 192.168.10.10

Supports only single TOS(TOS0) routes

Supports opaque LSA

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

<output omitted>

R3#**show ip ospf interface**

FastEthernet0/0 is up, line protocol is up

Internet address is 172.16.1.33/29, Area 0

Process ID 1, Router ID 192.168.10.10, Network Type BROADCAST, Cost:

1

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 192.168.10.10, Interface address 172.16.1.33

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:00

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

```
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

<output omitted>

R3#

Step 2: Use loopback addresses to change the router IDs of the routers in the topology.

```
R1(config)#interface loopback 0
R1(config-if)#ip address 10.1.1.1 255.255.255.255
```

```
R2(config)#interface loopback 0
R2(config-if)#ip address 10.2.2.2 255.255.255.255
```

```
R3(config)#interface loopback 0
R3(config-if)#ip address 10.3.3.3 255.255.255.255
```

Step 3: Reload the routers to force the new Router IDs to be used.

When a new Router ID is configured, it will not be used until the OSPF process is restarted. Make sure that the current configuration is saved to NRAM, and then use the **reload** command to restart each of the routers..

When the router is reloaded, what is the router ID for R1?
When the router is reloaded, what is the router ID for R2?
When the router is reloaded, what is the router ID for R3?

Step 4: Use the **show ip ospf neighbors** command to verify that the router IDs have changed.

R1#**show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address
Interface				
10.3.3.3	0	FULL/ -	00:00:30	192.168.10.6
Serial0/0/1				
10.2.2.2	0	FULL/ -	00:00:33	192.168.10.2
Serial0/0/0				

R2#**show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address
Interface				
10.3.3.3	0	FULL/ -	00:00:36	192.168.10.10
Serial0/0/1				
10.1.1.1	0	FULL/ -	00:00:37	192.168.10.1
Serial0/0/0				

R3#**show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address
Interface				

10.2.2.2	0	FULL/	-	00:00:34	192.168.10.9
Serial0/0/1					
10.1.1.1	0	FULL/	-	00:00:38	192.168.10.5
Serial0/0/0					

Step 5: Use the `router-id` command to change the router ID on the R1 router.

Note: Some IOS versions do not support the `router-id` command. If this command is not available, continue to Task 7.

```
R1(config)#router ospf 1
R1(config-router)#router-id 10.4.4.4
Reload or use "clear ip ospf process" command, for this to take effect
```

If this command is used on an OSPF router process which is already active (has neighbors), the new router-ID is used at the next reload or at a manual OSPF process restart. To manually restart the OSPF process, use the `clear ip ospf process` command.

```
R1#(config-router)#end
R1# clear ip ospf process
Reset ALL OSPF processes? [no]:yes
R1#
```

Step 6: Use the `show ip ospf neighbor` command on router R2 to verify that the router ID of R1 has been changed.

```
R2#show ip ospf neighbor
```

Neighbor ID	Pri	State		Dead Time	Address
Interface					
10.3.3.3	0	FULL/	-	00:00:36	192.168.10.10
Serial0/0/1					
10.4.4.4	0	FULL/	-	00:00:37	192.168.10.1
Serial0/0/0					

Step 7: Remove the configured router ID with the `no` form of the `router-id` command.

```
R1(config)#router ospf 1
R1(config-router)#no router-id 10.4.4.4
Reload or use "clear ip ospf process" command, for this to take effect
```

Step 8: Restart the OSPF process using the `clear ip ospf process` command.

Restarting the OSPF process forces the router to use the IP address configured on the Loopback 0 interface as the Router ID.

```
R1(config-router)#end
R1# clear ip ospf process
Reset ALL OSPF processes? [no]:yes
R1#
```

Task 7: Verify OSPF Operation

Step 1: On the R1 router, Use the `show ip ospf neighbor` command to view the information about the OSPF neighbor routers R2 and R3. You should be able to see the neighbor ID and IP address of each adjacent router, and the interface that R1 uses to reach that OSPF neighbor.

```
R1#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address
Interface
10.2.2.2        0    FULL/-          00:00:32    192.168.10.2
Serial0/0/0
10.3.3.3        0    FULL/-          00:00:32    192.168.10.6
Serial0/0/1
```

R1#

Step 2: On the R1 router, use the `show ip protocols` command to view information about the routing protocol operation.

Notice that the information that was configured in the previous Tasks, such as protocol, process ID, neighbor ID, and networks, is shown in the output. The IP addresses of the adjacent neighbors are also shown.

```
R1#show ip protocols
```

```
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.16 0.0.0.15 area 0
    192.168.10.0 0.0.0.3 area 0
    192.168.10.4 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.2.2.2         110          00:11:43
    10.3.3.3         110          00:11:43
  Distance: (default is 110)
```

R1#

Notice that the output specifies the process ID used by OSPF. Remember, the process ID must be the same on all routers for OSPF to establish neighbor adjacencies and share routing information.

Task8: Examine OSPF Routes in the Routing Tables

View the routing table on the R1 router. OSPF routes are denoted in the routing table with an "O".

```
R1#show ip route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
 inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is not set

```

    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.1/32 is directly connected, Loopback0
O       10.10.10.0/24 [110/65] via 192.168.10.2, 00:01:02, Serial0/0/0
    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.16/28 is directly connected, FastEthernet0/0
O       172.16.1.32/29 [110/65] via 192.168.10.6, 00:01:12, Serial0/0/1
    192.168.10.0/30 is subnetted, 3 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/1
O       192.168.10.8 [110/128] via 192.168.10.6, 00:01:12, Serial0/0/1
        [110/128] via 192.168.10.2, 00:01:02, Serial0/0/0
R1#

```

Notice that unlike RIPv2 and EIGRP, OSPF does not automatically summarize at major network boundaries.

Task 9: Configure OSPF Cost

Step 1: Use the show ip route command on the R1 router to view the OSPF cost to reach the 10.10.10.0/24 network.

R1#**show ip route**

<output omitted>

```

    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.1/32 is directly connected, Loopback0
O       10.10.10.0/24 [110/65] via 192.168.10.2, 00:16:56, Serial0/0/0
    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.16/28 is directly connected, FastEthernet0/0
O       172.16.1.32/29 [110/65] via 192.168.10.6, 00:17:06, Serial0/0/1
    192.168.10.0/30 is subnetted, 3 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/1
O       192.168.10.8 [110/128] via 192.168.10.6, 00:17:06, Serial0/0/1
        [110/128] via 192.168.10.2, 00:16:56, Serial0/0/0
R1#

```

Step 2: Use the show interfaces serial0/0/0 command on the R1 router to view the bandwidth of the Serial 0/0/0 interface.

```

R1#show interfaces serial0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 192.168.10.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load
1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0

```

<output omitted>

On most serial links, the bandwidth metric will default to 1544 Kbits. If this is not the actual bandwidth of the serial link, the bandwidth will need to be changed so that the OSPF cost can be calculated correctly.

Step 3: Use the bandwidth command to change the bandwidth of the serial interfaces of the R1 and R2 routers to the actual bandwidth, 64 kbps.

```

R1 router:
R1(config)#interface serial0/0/0
R1(config-if)#bandwidth 64
R1(config-if)#interface serial0/0/1
R1(config-if)#bandwidth 64

```

```

R2 router:
R2(config)#interface serial0/0/0
R2(config-if)#bandwidth 64
R2(config)#interface serial0/0/1
R2(config-if)#bandwidth 64

```

Step 4: Use the show ip ospf interface command on the R1 router to verify the cost of the serial links.

The cost of each of the Serial links is now 1562, the result of the calculation: $10^8/64,000$ bps.

```

R1#show ip ospf interface

```

<output omitted>

```

Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.10.1/30, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type POINT-TO-POINT, Cost:
1562
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1

```

```

    Adjacent with neighbor 10.2.2.2
    Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
    Internet address is 192.168.10.5/30, Area 0
    Process ID 1, Router ID 10.1.1.1, Network Type POINT-TO-POINT, Cost:
1562
    Transmit Delay is 1 sec, State POINT-TO-POINT,

<output omitted>

```

Step 5: Use the `ip ospf cost` command to configure the OSPF cost on the R3 router. An alternative method to using the `bandwidth` command is to use the `ip ospf cost` command, which allows you to directly configure the cost. Use the `ip ospf cost` command to change the bandwidth of the serial interfaces of the R3 router to 1562.

```

R3(config)#interface serial0/0/0
R3(config-if)#ip ospf cost 1562
R3(config-if)#interface serial0/0/1
R3(config-if)#ip ospf cost 1562

```

Step 6: Use the `show ip ospf interface` command on the R3 router to verify that the cost of the link the cost of each of the Serial links is now 1562.

```

R3#show ip ospf interface

```

```

<output omitted>
Serial0/0/1 is up, line protocol is up
    Internet address is 192.168.10.10/30, Area 0
    Process ID 1, Router ID 10.3.3.3, Network Type POINT-TO-POINT, Cost:
1562
    Transmit Delay is 1 sec, State POINT-TO-POINT,
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
    Index 2/2, flood queue length 0
    Next 0x0(0)/0x0(0)
    Last flood scan length is 1, maximum is 1
    Last flood scan time is 0 msec, maximum is 0 msec
    Neighbor Count is 1 , Adjacent neighbor count is 1
        Adjacent with neighbor 10.2.2.2
        Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
    Internet address is 192.168.10.6/30, Area 0
    Process ID 1, Router ID 10.3.3.3, Network Type POINT-TO-POINT, Cost:
1562
    Transmit Delay is 1 sec, State POINT-TO-POINT,

<output omitted>

```

Task 10: Redistribute an OSPF Default Route

Step 1: Configure a loopback address on the R1 router to simulate a link to an ISP.

```
R1(config)#interface loopback1
```

```
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed
state to up
```

```
R1(config-if)#ip address 172.30.1.1 255.255.255.252
```

Step 2: Configure a static default route on the R1 router.

Use the loopback address that has been configured to simulate a link to an ISP as the exit interface.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback1
R1(config)#
```

Step 3: Use the default-information originate command to include the static route in the OSPF updates that are sent from the R1 router.

```
R1(config)#router ospf 1
R1(config-router)#default-information originate
R1(config-router)#
```

Step 4: View the routing table on the R2 router to verify that the static default route is being redistributed via OSPF.

```
R2#show ip route
```

<output omitted>

Gateway of last resort is 192.168.10.1 to network 0.0.0.0

```

    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.2.2.2/32 is directly connected, Loopback0
C       10.10.10.0/24 is directly connected, FastEthernet0/0
    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O       172.16.1.16/28 [110/1563] via 192.168.10.1, 00:29:28,
Serial0/0/0
O       172.16.1.32/29 [110/1563] via 192.168.10.10, 00:29:28,
Serial0/0/1
    192.168.10.0/30 is subnetted, 3 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
O       192.168.10.4 [110/3124] via 192.168.10.10, 00:25:56,
Serial0/0/1
                                [110/3124] via 192.168.10.1, 00:25:56, Serial0/0/0
C       192.168.10.8 is directly connected, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 192.168.10.1, 00:01:11, Serial0/0/0
R2#
```

Task 11: Configure Additional OSPF Features

Step 1: Use the `auto-cost reference-bandwidth` command to adjust the reference bandwidth value.

Increase the reference bandwidth to 10000 to simulate 10GigE speeds. Configure this command on all routers in the OSPF routing domain.

```
R1(config-router)#auto-cost reference-bandwidth 10000
```

```
% OSPF: Reference bandwidth is changed.
```

```
    Please ensure reference bandwidth is consistent across all  
routers.
```

```
R2(config-router)#auto-cost reference-bandwidth 10000
```

```
% OSPF: Reference bandwidth is changed.
```

```
    Please ensure reference bandwidth is consistent across all  
routers.
```

```
R3(config-router)#auto-cost reference-bandwidth 10000
```

```
% OSPF: Reference bandwidth is changed.
```

```
    Please ensure reference bandwidth is consistent across all  
routers.
```

Step 2: Examine the routing table on the R1 router to verify the change in the OSPF cost metric.

Notice that the values are much larger cost values for OSPF routes.

```
R1#show ip route
```

```
<output omitted>
```

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
```

```
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks  
C       10.1.1.1/32 is directly connected, Loopback0  
O       10.10.10.0/24 [110/65635] via 192.168.10.2, 00:01:01,  
Serial0/0/0  
    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks  
C       172.16.1.16/28 is directly connected, FastEthernet0/0  
O       172.16.1.32/29 [110/65635] via 192.168.10.6, 00:00:51,  
Serial0/0/1  
    172.30.0.0/30 is subnetted, 1 subnets  
C       172.30.1.0 is directly connected, Loopback1  
    192.168.10.0/30 is subnetted, 3 subnets  
C       192.168.10.0 is directly connected, Serial0/0/0  
C       192.168.10.4 is directly connected, Serial0/0/1  
O       192.168.10.8 [110/67097] via 192.168.10.2, 00:01:01,  
Serial0/0/0  
S*    0.0.0.0/0 is directly connected, Loopback1  
R1#
```

Step 3: Use the `show ip ospf neighbor` command on R1 to view the Dead Time counter.

The Dead Time counter is counting down from the default interval of 40 seconds.

```

R1#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address
Interface
10.2.2.2          0    FULL/-          00:00:34    192.168.10.2
Serial0/0/0
10.3.3.3          0    FULL/-          00:00:34    192.168.10.6
Serial0/0/1

```

Step 4: Configure the OSPF Hello and Dead intervals.

The OSPF Hello and Dead intervals can be modified manually using the **ip ospf hello-interval** and **ip ospf dead-interval** interface commands. Use these commands to change the hello interval to 5 seconds and the dead interval to 20 seconds on the Serial 0/0/0 interface of the R1 router.

```

R1(config)#interface serial0/0/0
R1(config-if)#ip ospf hello-interval 5
R1(config-if)#ip ospf dead-interval 20
R1(config-if)#
01:09:04: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/0/0 from
FULL to DOWN, Neighbor Down: Dead timer expired
01:09:04: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/0/0 from
FULL to Down: Interface down or detached

```

After 20 seconds the Dead Timer on R1 expires. R1 and R2 loose adjacency because the Dead Timer and Hello Timers must be configured identically on each side of the serial link between R1 and R2.

Step 5: Modify the Dead Timer and Hello Timer intervals.

Modify the Dead Timer and Hello Timer intervals on the Serial 0/0/0 interface in the R2 router to match the intervals configured on the Serial 0/0/0 interface of the R1 router.

```

R2(config)#interface serial0/0/0
R2(config-if)#ip ospf hello-interval 5
R2(config-if)#ip ospf dead-interval 20
R2(config-if)#
01:12:10: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.1 on Serial0/0/0 from
EXCHANGE to FULL, Exchange Done

```

Notice that the IOS displays a message when adjacency has been established with a state of Full.

Step 5: Use the show ip ospf interface serial0/0/0 command to verify that the Hello Timer and Dead Timer intervals have been modified.

```

R2#show ip ospf interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.10.2/30, Area 0
  Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT, Cost:
1562
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
    Hello due in 00:00:00
  Index 3/3, flood queue length 0

```

```

Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
  Adjacent with neighbor 10.1.1.1
Suppress hello for 0 neighbor(s)
R2#

```

Step 6: Use the `show ip ospf neighbor` command on R1 to verify that the neighbor adjacency with R2 has been restored.

Notice that the Dead Time for Serial 0/0/0 is now much lower since it is counting down from 20 seconds instead of the default 40 seconds. Serial 0/0/1 is still operating with default timers.

```

R1#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address
Interface
10.2.2.2         0    FULL/-         00:00:19   192.168.10.2
Serial0/0/0
10.3.3.3         0    FULL/-         00:00:34   192.168.10.6
Serial0/0/1
R1#

```

Task 12: Document the Router Configurations.

On each router, capture the following command output to a text file and save for future reference:

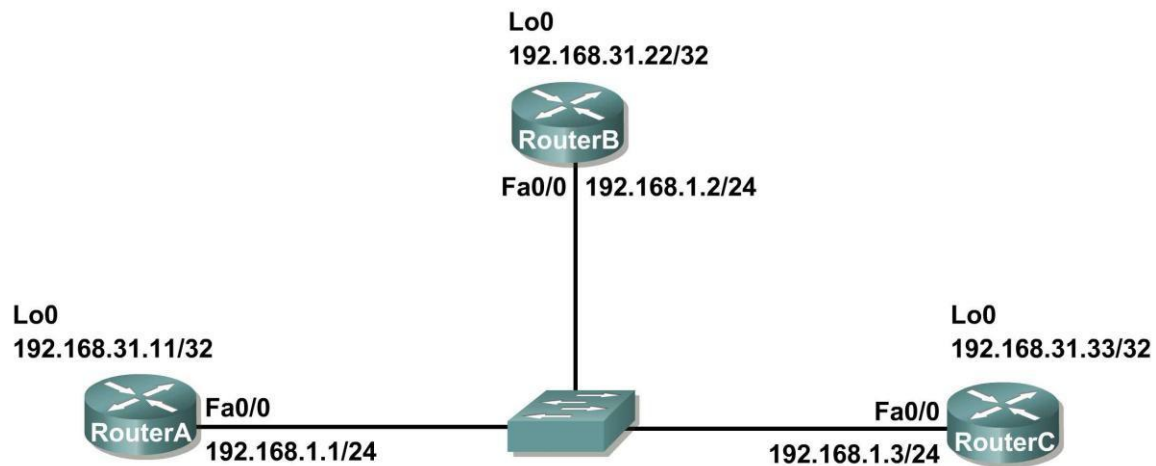
- Running configuration
- Routing table
- Interface summarization
- Output from `show ip protocols`

Task 11: Clean Up.

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Scenario B: Configure OSPF on a Multi-access Network

Topology Diagram



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	Loopback1	192.168.31.11	255.255.255.255	N/A
R2	Fa0/0	192.168.1.2	255.255.255.0	N/A
	Loopback1	192.168.31.22	255.255.255.255	N/A
R3	Fa0/0	192.168.1.3	255.255.255.0	N/A
	Loopback1	192.168.31.33	255.255.255.255	N/A

Task 1: Prepare the Network.

Step 1: Cable a network that is similar to the one in the Topology Diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

Note: If you use 1700, 2500, or 2600 routers, the router outputs and interface descriptions will appear different.

In this topology we have three routers sharing a common Ethernet multiaccess network, 192.168.1.0/24. Each router will be configured with an IP address on the Fast Ethernet interface and a loopback address for the router ID.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations.

Perform basic configuration of the R1, R2, and R3 routers according to the following guidelines:

1. Configure the router hostname.
2. Disable DNS lookup.
3. Configure a privileged EXEC mode password.
4. Configure a message-of-the-day banner.
5. Configure a password for console connections.
6. Configure a password for VTY connections

Task 3: Configure and Activate Ethernet and Loopback Addresses

Step 1: Configure interfaces on R1, R2, and R3.

Configure the Ethernet and Loopback interfaces on the R1, R2, and R3 routers with the IP addresses from the table under the Topology Diagram. Use the **show ip interface brief** command to verify that the IP addressing is correct. When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 2: Verify IP addressing and interfaces.

Use the **show ip interface brief** command to verify that the IP addressing is correct and that the interfaces are active.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

Task 4: Configure OSPF on the DR Router

The DR and BDR election process takes place as soon as the first router has its interface enabled on the multiaccess network. This can happen as the routers are powered-on or when the OSPF **network** command for that interface is configured. If a new router enters the network after the DR and BDR have already been elected, it will not become the DR or BDR even if it has a higher OSPF interface priority or router ID than the current DR or BDR. Configure the OSPF process on the router with the highest router ID first to ensure that this router becomes the DR.

Step 1: Use the **router ospf** command in global configuration mode to enable OSPF on the R3 router.

Enter a process ID of 1 for the *process-ID* parameter. Configure the router to advertise the 192.168.1.0/24 network. Use an area ID of 0 for the OSPF *area-id* parameter in the **network** statement.

```
R3(config)#router ospf 1
R3(config-router)#network 192.168.1.0 0.0.0.255 area 0
R3(config-router)#end
R3#
```

Step 2: Use the `show ip ospf interface` command to verify that the OSPF has been configured correctly and that R3 is the DR.

```
R3#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.3/24, Area 0
  Process ID 1, Router ID 192.168.31.33, Network Type BROADCAST, Cost:
1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.31.33, Interface address 192.168.1.3
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R3#
```

Task 5: Configure OSPF on the BDR Router

Configure the OSPF process on the router with the second highest router ID next to ensure that this router becomes the BDR.

Step 1: Use the `router ospf` command in global configuration mode to enable OSPF on the R2 router.

Enter a process ID of 1 for the *process-ID* parameter. Configure the router to advertise the 192.168.1.0/24 network. Use an area ID of 0 for the OSPF *area-id* parameter in the **network** statement.

```
R2(config)#router ospf 1
R2(config-router)#network 192.168.1.0 0.0.0.255 area 0
R2(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R2#
00:08:51: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.33 on
FastEthernet0/0 from LOADING to FULL, Loading Done
```

Notice that an adjacency is formed with the R3 router. It may take up to 40 seconds for the R3 router to send a hello packet. When this packet is received, the neighbor relationship is formed.

Step 2: Use the `show ip ospf interface` command to verify that the OSPF has been configured correctly and that R2 is the BDR.

```
R2#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.2/24, Area 0
  Process ID 1, Router ID 192.168.31.22, Network Type BROADCAST, Cost:
1
  Transmit Delay is 1 sec, State BDR, Priority 1
```

```

Designated Router (ID) 192.168.31.33, Interface address 192.168.1.3
Backup Designated Router (ID) 192.168.31.22, Interface address
192.168.1.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:03
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.1.3    (Designated Router)
Suppress hello for 0 neighbor(s)
R2#

```

Step 3: Use the `show ip ospf neighbors` command in global configuration mode to view information about the other routers in the OSPF area.

Notice that R3 is the DR.

```

R2#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address
Interface
192.168.31.33    1    FULL/DR         00:00:33    192.168.1.3
FastEthernet0/0

```

Task 6: Configure OSPF on the DRother Router

Configure the OSPF process on the router with the lowest router ID last. This router will be designated as DRother instead of DR or BDR.

Step 1: Use the `router ospf` command in global configuration mode to enable OSPF on the R1 router.

Enter a process ID of 1 for the *process-ID* parameter. Configure the router to advertise the 192.168.1.0/24 network. Use an area ID of 0 for the OSPF *area-id* parameter in the **network** statement.

```

R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#
00:16:08: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.22 on
FastEthernet0/0 from LOADING to FULL, Loading Done
00:16:12: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.33 on
FastEthernet0/0 from EXCHANGE to FULL, Exchange Done

```

Notice that an adjacency is formed with the R2 and R3 routers. It may take up to 40 seconds for both the R2 and R3 routers to each send a hello packet.

Step 2: Use the `show ip ospf interface` command to verify that the OSPF has been configured correctly and that R1 is a DRother.

```

R1#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.31.11, Network Type BROADCAST, Cost:
  1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.31.33, Interface address 192.168.1.3
  Backup Designated Router (ID) 192.168.31.22, Interface address
  192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 192.168.31.33 (Designated Router)
    Adjacent with neighbor 192.168.31.22 (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
R1#

```

Step 3: Use the `show ip ospf neighbors` command in global configuration mode to view information about the other routers in the OSPF area.

Notice that R3 is the DR and R2 is the BDR.

```

R1#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address
Interface
192.168.31.22    1    FULL/BDR        00:00:35    192.168.1.2
FastEthernet0/0
192.168.31.33    1    FULL/DR         00:00:30    192.168.1.3
FastEthernet0/0

```

Task 7: Use the OSPF Priority to Determine the DR and BDR

Step 1: Use the `ip ospf priority interface` command to change the OSPF priority of the R1 router to 255.

This is the highest possible priority.

```

R1(config)#interface fastEthernet0/0
R1(config-if)#ip ospf priority 255
R1(config-if)#end

```

Step 2: Use the `ip ospf priority interface` command to change the OSPF priority of the R3 router to 100.

```

R3(config)#interface fastEthernet0/0
R3(config-if)#ip ospf priority 100
R3(config-if)#end

```

Step 3: Use the `ip ospf priority interface` command to change the OSPF priority of the R2 router to 0. A priority of 0 causes the router to be ineligible to participate in an OSPF election and become a DR or BDR.

```
R2(config)#interface fastEthernet0/0
R2(config-if)#ip ospf priority 0
R2(config-if)#end
```

Step 4: Shut down and re-enable the FastEthernet0/0 interfaces to force an OSPF election. The FastEthernet0/0 interfaces of each of the routers can be shut down and re-enabled to force an OSPF election. Shut down the FastEthernet0/0 interface on each of the three routers. Notice that as the interfaces are shut down the OSPF adjacencies are lost.

R1:

```
R1(config)#interface fastethernet0/0
R1(config-if)#shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to down
02:17:22: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.22 on
FastEthernet0/0 from FULL to Down: Interface down or detached
02:17:22: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.33 on
FastEthernet0/0 from FULL to Down: Interface down or detached
```

R2:

```
R2(config)#interface fastethernet0/0
R2(config-if)#shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to down
02:17:06: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.33 on
FastEthernet0/0 from FULL to Down: Interface down or detached
02:17:06: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.11 on
FastEthernet0/0 from FULL to Down: Interface down or detached
```

R3:

```
R3(config)#interface fastethernet0/0
R3(config-if)#shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to down
02:17:22: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.22 on
FastEthernet0/0 from FULL to Down: Interface down or detached
02:17:22: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.11 on
FastEthernet0/0 from FULL to Down: Interface down or detached
```

Step 5: Re-enable the FastEthernet0/0 interface on the R2 router.

```
R2(config-if)#no shut
R2(config-if)#end
```

```
%SYS-5-CONFIG_I: Configured from console by console
R2#
```

Step 6: Re-enable the FastEthernet0/0 interface on the R1 router.

Notice that an adjacency is formed with the R2 router. It may take up to 40 seconds for the R2 router to send a hello packet.

```
R1(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
R1(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#
02:31:43: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.22 on
FastEthernet0/0 from EXCHANGE to FULL, Exchange Done
```

Step 7: Use the `show ip ospf neighbor` command on the R1 router to view the OSPF neighbor information for that router.

Notice that even though the R2 router has a higher router ID than R1, the R2 router has been set to a state of DROTHER because the OSPF priority has been set to 0.

```
R1#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address
Interface
192.168.31.22    0    FULL/DROTHER    00:00:33    192.168.1.2
FastEthernet0/0
R1#
```

Step 8: Re-enable the FastEthernet0/0 interface on the R3 router.

Notice that an adjacency is formed with the R1 and R2 routers. It may take up to 40 seconds for both the R1 and R2 routers to each send a hello packet.

```
R3(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
R3(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
02:37:32: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.11 on
FastEthernet0/0 from LOADING to FULL, Loading Done
02:37:36: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.22 on
FastEthernet0/0 from EXCHANGE to FULL, Exchange Done
```

Step 9: Use the `show ip ospf interface` command on the R3 router to verify that R3 has become the BDR.

```
R3#show ip ospf interface
```

```
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.3/24, Area 0
  Process ID 1, Router ID 192.168.31.33, Network Type BROADCAST, Cost:
1
  Transmit Delay is 1 sec, State BDR, Priority 100
  Designated Router (ID) 192.168.31.11, Interface address 192.168.1.1

<output omitted>
```

Task 8: Document the Router Configurations.

On each router, capture the following command output to a text file and save for future reference:

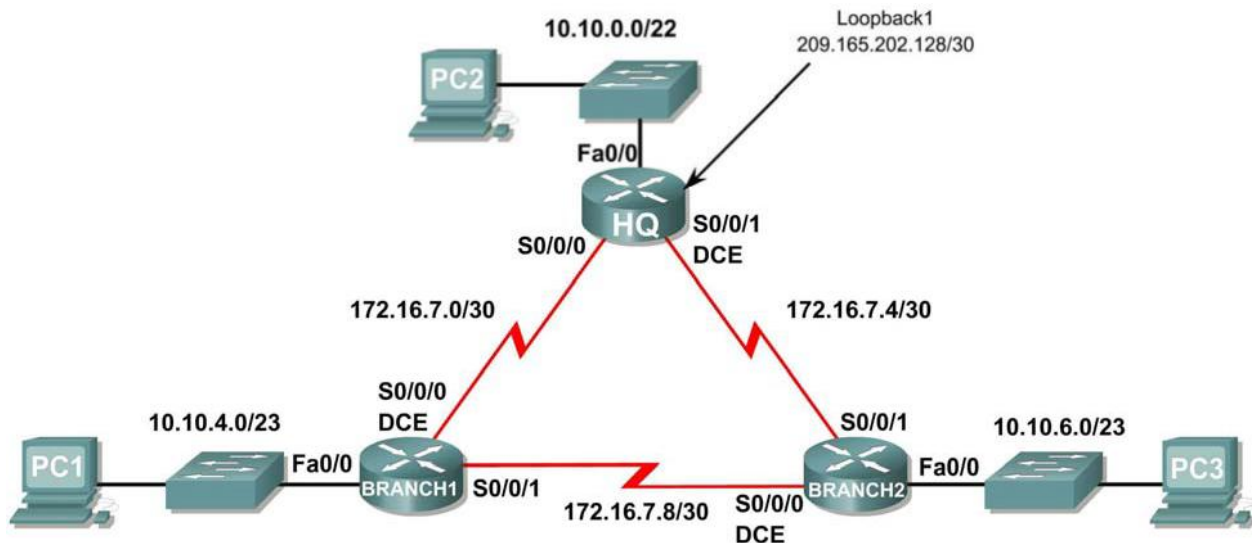
- Running configuration
- Routing table
- Interface summarization
- Output from **show ip protocols**

Task 9: Clean Up.

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

17 - OSPF Troubleshooting Lab

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	Fa0/0	10.10.0.1	255.255.252.0	N/A
	S0/0/0	172.16.7.1	255.255.255.252	N/A
	S0/0/1	172.16.7.5	255.255.255.252	N/A
	Lo1	209.165.202.129	255.255.255.252	N/A
Branch1	Fa0/0	10.10.4.1	255.255.254.0	N/A
	S0/0/0	172.16.7.2	255.255.255.252	N/A
	S0/0/1	172.16.7.9	255.255.255.252	N/A
Branch2	Fa0/0	10.10.6.1	255.255.254.0	N/A
	S0/0/0	172.16.7.10	255.255.255.252	N/A
	S0/0/1	172.16.7.6	255.255.255.252	N/A
PC1	NIC	10.10.5.254	255.255.254.0	10.10.4.1
PC2	NIC	10.10.3.254	255.255.252.0	10.10.0.1
PC3	NIC	10.10.7.254	255.255.254.0	10.10.6.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the Topology Diagram.
- Erase the startup configuration and reload a router to the default state.
- Load the routers with supplied scripts.
- Discover where communication is not possible.
- Gather information about the misconfigured portion of the network along with any other errors.
- Analyze information to determine why communication is not possible.
- Propose solutions to network errors.
- Implement solutions to network errors.
- Document the corrected network.

Scenario

In this lab, you will begin by loading configuration scripts on each of the routers. These scripts contain errors that will prevent end-to-end communication across the network. You will need to troubleshoot each router to determine the configuration errors, and then use the appropriate commands to correct the configurations. When you have corrected all of the configuration errors, all of the hosts on the network should be able to communicate with each other.

The network should also have the following requirements met:

- OSPF routing is configured on the Branch1 router.
- OSPF routing is configured on the Branch2 router.
- OSPF routing is configured on the HQ router.
- OSPF updates must be disabled on the LAN and Loopback interfaces.
- The HQ router must redistribute the default route to the Loopback interface in the routing updates.
- All OSPF routers must use a process ID of 1.
- All OSPF routers must be in area 0.

Task 1: Cable, Erase, and Reload the routers.

Step 1: Cable a network.

Cable a network that is similar to the one in the Topology Diagram.

Step 2: Clear the configuration on each router.

Clear the configuration on each of the routers using the `erase startup-config` command and then `reload` the routers. Answer **no** if asked to save changes.

Task 2: Load Routers with the Supplied Scripts

Step 1: Load the following script onto the Branch1 router:

```

hostname Branch1
!
no ip domain-lookup
!
interface FastEthernet0/0
ip address 10.10.4.1 255.255.254.0
duplex auto
speed auto no
shutdown
!
interface Serial0/0/0
ip address 172.16.7.2 255.255.255.252 no
shutdown
!
interface Serial0/0/1
ip address 172.16.7.9 255.255.255.252
no shutdown
!
router ospf 1
passive-interface FastEthernet0/0
network 10.10.4.0 0.0.1.255 area 0
network 172.16.7.0 0.0.0.3 area 0
network 172.16.7.8 0.0.0.3 area 0
!
ip classless
!
line con 0 line
vty 0 4
login
!
end

```

Step 2: Load the following script onto the Branch2 router.

```

hostname Branch2
!
interface FastEthernet0/0
ip address 10.10.6.1 255.255.254.0
duplex auto
speed auto no
shutdown
!
interface Serial0/0/0
ip address 172.16.7.10 255.255.255.252
clock rate 64000

```

```

no shutdown
!
interface Serial0/0/1
ip address 172.16.7.6 255.255.255.252
!
router ospf 1
log-adjacency-changes
passive-interface Serial0/0/1 network
172.16.7.4 0.0.0.3 area 0 network
172.16.7.8 0.0.0.3 area 0 network
10.10.6.0 0.0.3.255 area 0
!
ip classless
!
line con 0
line vty 0 4
login
!
end

```

Step 3: Load the following script onto the HQ router.

```

hostname HQ
!
no ip domain-lookup
!
interface FastEthernet0/0
ip address 10.10.10.1 255.255.252.0
duplex auto
speed auto no
shutdown
!
interface Serial0/0/0
ip address 172.16.7.1 255.255.255.252 no
shutdown
!
interface Serial0/0/1
ip address 172.16.7.5 255.255.255.252
clock rate 64000
no shutdown
!
interface Loopback1
ip address 209.165.202.129 255.255.255.252
!
router ospf 1
log-adjacency-changes

```

```

passive-interface FastEthernet0/0
passive-interface Loopback1 network
172.16.7.0 0.0.0.3 area 0 network
172.16.7.4 0.0.0.3 area 0 network
10.10.0.0 0.0.7.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 loopback1
!
line con 0 line
vty 0 4
  login
!
end

```

Task 3: Troubleshoot the Branch1 Router

Step 1: Begin troubleshooting at the Host connected to the Branch1 router.

From the host PC1, is it possible to ping PC2? _____ From

the host PC1, is it possible to ping PC3? _____

From the host PC1, is it possible to ping the default gateway? _____

Step 2: Examine the Branch1 router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router. Are there any problems with the status of the interfaces?

If there are any problems with the configuration of the interfaces, record any commands that will be necessary to correct the configuration errors.

Step 3: If you have recorded any commands above, apply them to the router configuration now.

Step 4: View summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors on the Branch1 router? _____

If the answer is **yes**, troubleshoot the interface status of the interfaces again.

Step 5: Troubleshoot the routing configuration on the Branch1 router.

What routes are shown in the routing table?

Are there any problems with the routing table?

Does the information in routing table indicate any configuration errors on the Branch1 router, or will it be necessary to troubleshoot the configurations on the other two routers to correct the errors?

Step 6: Attempt to ping between the hosts again.

From the host PC1, is it possible to ping PC2? _____

From the host PC1, is it possible to ping PC3? _____

From the host PC1, is it possible to ping the Serial 0/0/0 interface of the HQ router? _____

From the host PC1, is it possible to ping the Serial 0/0/1 interface of the HQ router? _____

Task 4: Troubleshoot the HQ Router

Step 1: Begin troubleshooting at the host PC2.

From the host PC2, is it possible to ping PC1? _____

From the host PC2, is it possible to ping PC3? _____

From the host PC2, is it possible to ping the default gateway? _____

Step 2: Examine the HQ router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router. Are there any problems with the status of the interfaces?

If there are any problems with the configuration of the interfaces, record any commands that will be necessary to correct the configuration errors.

Are there any problems with the interface status that could be due to errors on other parts of the network?

Step 3: If you have recorded any commands above, apply them to the router configuration now.

Step 4: View summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors on the HQ router?

If the answer is **yes**, troubleshoot the interface status of the interfaces again.

Step 5: Troubleshoot the routing configuration on the HQ router.

What routes are shown in the routing table?

Are there any problems with the routing table?

Use the **show running-configuration**, **show ip protocols**, and **show ip ospf neighbor** commands to view information about the OSPF configuration on the HQ router. Are there any additional problems with the OSPF configuration?

If there are any problems with the OSPF configuration, record any commands that will be necessary to correct the configuration errors.

Are there any problems on the HQ router that could be due to errors on other parts of the network?

Step 6: If you have recorded any commands above; apply them to the router configuration now.

Step 7: View the routing information.

If any changes were made to the configuration in the previous steps, view the routing information again. Does the information in routing table indicate any configuration errors on the HQ router? _____

If the answer to either of this is **yes**, troubleshoot the routing configuration again.

Step 8: Attempt to ping between the hosts again.

From the host PC2, is it possible to ping PC1? _____ From

the host PC2, is it possible to ping PC3? _____

From the host PC2, is it possible to ping the Serial 0/0/0 interface of the Branch2 router? _____

From the host PC2, is it possible to ping the Serial 0/0/1 interface of the Branch2 router? _____

Task 5: Troubleshoot the Branch2 Router

Step 1: Begin troubleshooting at the Host PC3.

From the host PC3, is it possible to ping PC1? _____ From

the host PC3, is it possible to ping PC2? _____

From the host PC3, is it possible to ping the default gateway? _____

From the host PC3, is it possible to ping the Serial0/0/1 interface of the Branch 2 router? _____

Step 2: Examine the Branch2 router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router. Are there any problems with the status of the interfaces?

If there are any problems with the configuration of the interfaces, record any commands that will be necessary to correct the configuration errors.

Step 3: If you have recorded any commands above, apply them to the router configuration now.

Step 4: View summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors on the Branch router? _____

If the answer is **yes**, troubleshoot the interface status of the interfaces again.

Step 5: Troubleshoot the routing configuration on the Branch2 router.

What routes are shown in the routing table?

Are there any problems with the routing table?

Use the **show running-configuration**, **show ip protocols**, and **show ip ospf neighbor** commands to view information about the OSPF configuration on the Branch2 router. Are there any problems with the OSPF configuration?

If there are any problems with the OSPF configuration, record any commands that will be necessary to correct the configuration errors.

Step 6: If you have recorded any commands above; apply them to the router configuration now.

Step 7: View the routing information.

If any changes were made to the configuration in the previous steps, view the routing information again. Does the information in routing table indicate any configuration errors on the Branch2 router? _____ If the answer to this question is **yes**, troubleshoot the routing configuration again.

What routes are shown in the routing table?

Step 8: Attempt to ping between the hosts again.

From the host PC3, is it possible to ping PC1? _____ From
the host PC3, is it possible to ping PC2? _____

From the host PC3, is it possible to ping the Serial 0/0/0 interface of the Branch1 router? _____

From the host PC3, is it possible to ping the Serial 0/0/1 interface of the Branch1 router? _____

Task 6: Reflection

There were a number of configuration errors in the scripts that were provided for this lab. Use the space below to write a brief description of the errors that you found.

Task 7: Documentation

On each router, capture the following command output to a text (.txt) file and save for future reference.

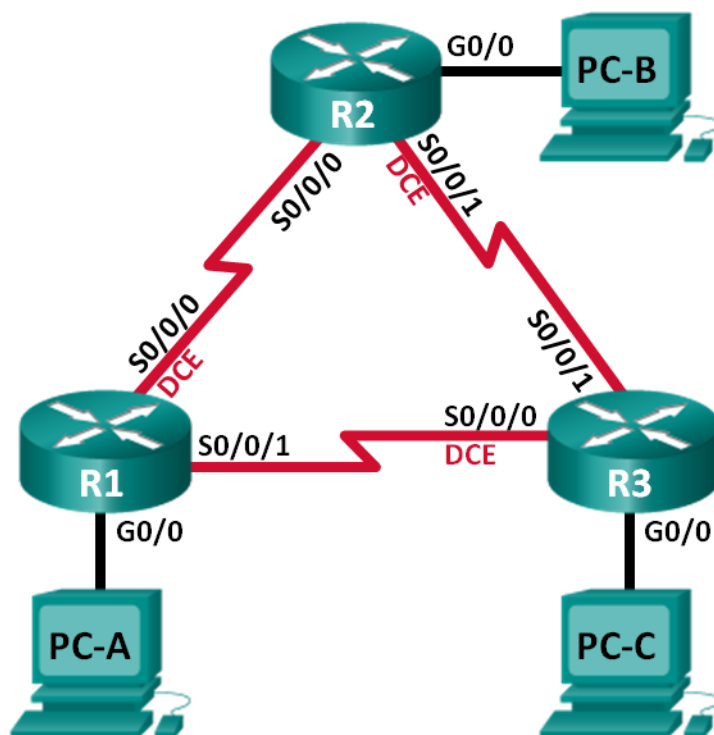
- `show running-config`
- `show ip route`
- `show ip interface brief`
- `show ip protocols`

Task 8: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

18 - Configuring Basic Single-Area OSPFv2

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	N/A
	S0/0/1	192.168.13.1	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	192.168.12.2	255.255.255.252	N/A
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	N/A
	S0/0/1	192.168.23.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure and Verify OSPF Routing

Part 3: Change Router ID Assignments

Part 4: Configure OSPF Passive Interfaces

Part 5: Change OSPF Metrics

Background / Scenario

Open Shortest Path First (OSPF) is a link-state routing protocol for IP networks. OSPFv2 is defined for IPv4 networks, and OSPFv3 is defined for IPv6 networks. OSPF detects changes in the topology, such as link failures, and converges on a new loop-free routing structure very quickly. It computes each route using Dijkstra's algorithm, a shortest path first algorithm.

In this lab, you will configure the network topology with OSPFv2 routing, change the router ID assignments, configure passive interfaces, adjust OSPF metrics, and use a number of CLI commands to display and verify OSPF routing information.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). Other routers and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)

- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you set up the network topology and configure basic settings on the PC hosts and routers.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the routers as necessary.

Step 3: Configure basic settings for each router.

- Disable DNS lookup.
- Configure device name as shown in the topology.
- Assign **class** as the privileged EXEC password.
- Assign **cisco** as the console and vty passwords.
- Configure a message of the day (MOTD) banner to warn users that unauthorized access is prohibited.
- Configure **logging synchronous** for the console line.
- Configure the IP address listed in the Addressing Table for all interfaces.
- Set the clock rate for all DCE serial interfaces at **128000**.
- Copy the running configuration to the startup configuration.

Step 4: Configure PC hosts.

Step 5: Test connectivity.

The routers should be able to ping one another, and each PC should be able to ping its default gateway. The PCs are unable to ping other PCs until OSPF routing is configured. Verify and troubleshoot if necessary.

Part 2: Configure and Verify OSPF Routing

In Part 2, you will configure OSPFv2 routing on all routers in the network and then verify that routing tables are updated correctly. After OSPF has been verified, you will configure OSPF authentication on the links for added security.

Step 1: Configure OSPF on R1.

- Use the **router ospf** command in global configuration mode to enable OSPF on R1.

```
R1(config)# router ospf 1
```

Note: The OSPF process id is kept locally and has no meaning to other routers on the network.

- Configure the **network** statements for the networks on R1. Use an area ID of 0.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

```
R1(config-router)# network 192.168.12.0 0.0.0.3 area 0
```

```
R1(config-router)# network 192.168.13.0 0.0.0.3 area 0
```

Step 2: Configure OSPF on R2 and R3.

Use the **router ospf** command and add the **network** statements for the networks on R2 and R3. Neighbor adjacency messages display on R1 when OSPF routing is configured on R2 and R3.

```
R1#
00:22:29: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on Serial0/0/0 from LOADING to FULL, Loading Done
R1#
00:23:14: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.2 on Serial0/0/1 from LOADING to FULL, Loading Done
R1#
```

Step 3: Verify OSPF neighbors and routing information.

- a. Issue the **show ip ospf neighbor** command to verify that each router lists the other routers in the network as neighbors.

```
R1# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.23.2	0	FULL/ -	00:00:33	192.168.13.2	Serial0/0/1
192.168.23.1	0	FULL/ -	00:00:30	192.168.12.2	Serial0/0/0

- b. Issue the **show ip route** command to verify that all networks display in the routing table on all routers.

```
R1# show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O       192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0
O       192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.12.2, 00:31:38, Serial0/0/0
        [110/128] via 192.168.13.2, 00:31:38, Serial0/0/1
```

What command would you use to only see the OSPF routes in the routing table?

Step 4: Verify OSPF protocol settings.

The **show ip protocols** command is a quick way to verify vital OSPF configuration information. This information includes the OSPF process ID, the router ID, networks the router is advertising, the neighbors the router is receiving updates from, and the default administrative distance, which is 110 for OSPF.

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.13.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.23.2     110          00:19:16
    192.168.23.1     110          00:20:03
  Distance: (default is 110)
```

Step 5: Verify OSPF process information.

Use the **show ip ospf** command to examine the OSPF process ID and router ID. This command displays the OSPF area information, as well as the last time the SPF algorithm was calculated.

```
R1# show ip ospf
Routing Process "ospf 1" with ID 192.168.13.1
  Start time: 00:20:23.260, Time elapsed: 00:25:08.296
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  Supports Link-local Signaling (LLS)
  Supports area transit capability
  Supports NSSA (compatible with RFC 3101)
  Event-log enabled, Maximum number of events: 1000, Mode: cyclic
  Router is not originating router-LSAs with maximum metric
  Initial SPF schedule delay 5000 msecs
  Minimum hold time between two consecutive SPF's 10000 msecs
  Maximum wait time between two consecutive SPF's 10000 msecs
  Incremental-SPF disabled
  Minimum LSA interval 5 secs
  Minimum LSA arrival 1000 msecs
  LSA group pacing timer 240 secs
  Interface flood pacing timer 33 msecs
  Retransmission pacing timer 66 msecs
  Number of external LSA 0. Checksum Sum 0x000000
  Number of opaque AS LSA 0. Checksum Sum 0x000000
  Number of DCbitless external and opaque AS LSA 0
```

```

Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps

```

Area BACKBONE (0)

```

Number of interfaces in this area is 3
Area has no authentication
SPF algorithm last executed 00:22:53.756 ago
SPF algorithm executed 7 times
Area ranges are
Number of LSA 3. Checksum Sum 0x019A61
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

```

Step 6: Verify OSPF interface settings.

- a. Issue the **show ip ospf interface brief** command to display a summary of OSPF-enabled interfaces.

```
R1# show ip ospf interface brief
```

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Se0/0/1	1	0	192.168.13.1/30	64	P2P	1/1	
Se0/0/0	1	0	192.168.12.1/30	64	P2P	1/1	
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0	

- b. For a more detailed list of every OSPF-enabled interface, issue the **show ip ospf interface** command.

```
R1# show ip ospf interface
```

```

Serial0/0/1 is up, line protocol is up
Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost: 64
Topology-MTID      Cost      Disabled      Shutdown      Topology Name
    0              64         no           no           Base
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:01
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.23.2
Suppress hello for 0 neighbor(s)

```

```

Serial0/0/0 is up, line protocol is up
  Internet Address 192.168.12.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
      0              64         no           no           Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.23.1
  Suppress hello for 0 neighbor(s)
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost: 1
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
      0              1         no           no           Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.13.1, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)

```

Step 7: Verify end-to-end connectivity.

Each PC should be able to ping the other PCs in the topology. Verify and troubleshoot if necessary.

Note: It may be necessary to disable the PC firewall to ping between PCs.

Part 3: Change Router ID Assignments

The OSPF router ID is used to uniquely identify the router in the OSPF routing domain. Cisco routers derive the router ID in one of three ways and with the following precedence:

- 1) IP address configured with the OSPF **router-id** command, if present
- 2) Highest IP address of any of the router's loopback addresses, if present
- 3) Highest active IP address on any of the router's physical interfaces

Because no router IDs or loopback interfaces have been configured on the three routers, the router ID for each router is determined by the highest IP address of any active interface.

In Part 3, you will change the OSPF router ID assignment using loopback addresses. You will also use the **router-id** command to change the router ID.

Step 1: Change router IDs using loopback addresses.

- a. Assign an IP address to loopback 0 on R1.

```
R1(config)# interface lo0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# end
```

- b. Assign IP addresses to Loopback 0 on R2 and R3. Use IP address 2.2.2.2/32 for R2 and 3.3.3.3/32 for R3.
- c. Save the running configuration to the startup configuration on all three routers.
- d. You must reload the routers in order to reset the router ID to the loopback address. Issue the **reload** command on all three routers. Press Enter to confirm the reload.
- e. After the router completes the reload process, issue the **show ip protocols** command to view the new router ID.

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3          110          00:01:00
    2.2.2.2          110          00:01:14
  Distance: (default is 110)
```

- f. Issue the **show ip ospf neighbor** command to display the router ID changes for the neighboring routers.

```
R1# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	0	FULL/ -	00:00:35	192.168.13.2	Serial0/0/1
2.2.2.2	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0

```
R1#
```

Step 2: Change the router ID on R1 using the router-id command.

The preferred method for setting the router ID is with the **router-id** command.

- Issue the **router-id 11.11.11.11** command on R1 to reassign the router ID. Notice the informational message that appears when issuing the **router-id** command.

```
R1(config)# router ospf 1
R1(config-router)# router-id 11.11.11.11
Reload or use "clear ip ospf process" command, for this to take effect
R1(config)# end
```

- You will receive an informational message telling you that you must either reload the router or use the **clear ip ospf process** command for the change to take effect. Issue the **clear ip ospf process** command on all three routers. Type **yes** to reply to the reset verification message, and press ENTER.
- Set the router ID for R2 to **22.22.22.22** and the router ID for R3 to **33.33.33.33**. Then use **clear ip ospf process** command to reset ospf routing process.
- Issue the **show ip protocols** command to verify that the router ID changed on R1.

```
R1# show ip protocols
*** IP Routing is NSF aware ***
```

```
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 11.11.11.11
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    33.33.33.33      110          00:00:19
    22.22.22.22      110          00:00:31
    3.3.3.3          110          00:00:41
    2.2.2.2          110          00:00:41
  Distance: (default is 110)
```

- Issue the **show ip ospf neighbor** command on R1 to verify that new router ID for R2 and R3 is listed.

```
R1# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:36	192.168.13.2	Serial0/0/1
22.22.22.22	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0

Part 4: Configure OSPF Passive Interfaces

The **passive-interface** command prevents routing updates from being sent through the specified router interface. This is commonly done to reduce traffic on the LANs as they do not need to receive dynamic routing protocol communication. In Part 4, you will use the **passive-interface** command to configure a single interface as passive. You will also configure OSPF so that all interfaces on the router are passive by default, and then enable OSPF routing advertisements on selected interfaces.

Step 1: Configure a passive interface.

- a. Issue the **show ip ospf interface g0/0** command on R1. Notice the timer indicating when the next Hello packet is expected. Hello packets are sent every 10 seconds and are used between OSPF routers to verify that their neighbors are up.

```
R1# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
    0                1          no            no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

- b. Issue the **passive-interface** command to change the G0/0 interface on R1 to passive.

```
R1(config)# router ospf 1
R1(config-router)# passive-interface g0/0
```

- c. Re-issue the **show ip ospf interface g0/0** command to verify that G0/0 is now passive.

```
R1# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
    0                1          no            no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
```

No Hellos (Passive interface)

```
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

- d. Issue the **show ip route** command on R2 and R3 to verify that a route to the 192.168.1.0/24 network is still available.

R2# **show ip route**

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
```

Gateway of last resort is not set

```
      2.0.0.0/32 is subnetted, 1 subnets
C      2.2.2.2 is directly connected, Loopback0
O      192.168.1.0/24 [110/65] via 192.168.12.1, 00:58:32, Serial0/0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.2.0/24 is directly connected, GigabitEthernet0/0
L      192.168.2.1/32 is directly connected, GigabitEthernet0/0
O      192.168.3.0/24 [110/65] via 192.168.23.2, 00:58:19, Serial0/0/1
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.12.0/30 is directly connected, Serial0/0/0
L      192.168.12.2/32 is directly connected, Serial0/0/0
      192.168.13.0/30 is subnetted, 1 subnets
O      192.168.13.0 [110/128] via 192.168.23.2, 00:58:19, Serial0/0/1
           [110/128] via 192.168.12.1, 00:58:32, Serial0/0/0
      192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.23.0/30 is directly connected, Serial0/0/1
L      192.168.23.1/32 is directly connected, Serial0/0/1
```

Step 2: Set passive interface as the default on a router.

- a. Issue the **show ip ospf neighbor** command on R1 to verify that R2 is listed as an OSPF neighbor.

R1# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:31	192.168.13.2	Serial0/0/1
22.22.22.22	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0

- b. Issue the **passive-interface default** command on R2 to set the default for all OSPF interfaces as passive.

```
R2(config)# router ospf 1
```

```
R2(config-router)# passive-interface default
```

```
R2(config-router)#
```

```
*Apr  3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
```

```
*Apr  3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
```

- c. Re-issue the **show ip ospf neighbor** command on R1. After the dead timer expires, R2 will no longer be listed as an OSPF neighbor.

```
R1# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:34	192.168.13.2	Serial0/0/1

- d. Issue the **show ip ospf interface S0/0/0** command on R2 to view the OSPF status of interface S0/0/0.

```
R2# show ip ospf interface s0/0/0
```

```
Serial0/0/0 is up, line protocol is up
```

```
Internet Address 192.168.12.2/30, Area 0, Attached via Network Statement
```

```
Process ID 1, Router ID 22.22.22.22, Network Type POINT_TO_POINT, Cost: 64
```

Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0	64	no	no	Base

```
Transmit Delay is 1 sec, State POINT_TO_POINT
```

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
oob-resync timeout 40
```

```
No Hellos (Passive interface)
```

```
Supports Link-local Signaling (LLS)
```

```
Cisco NSF helper support enabled
```

```
IETF NSF helper support enabled
```

```
Index 2/2, flood queue length 0
```

```
Next 0x0(0)/0x0(0)
```

```
Last flood scan length is 0, maximum is 0
```

```
Last flood scan time is 0 msec, maximum is 0 msec
```

```
Neighbor Count is 0, Adjacent neighbor count is 0
```

```
Suppress hello for 0 neighbor(s)
```

- e. If all interfaces on R2 are passive, then no routing information is being advertised. In this case, R1 and R3 should no longer have a route to the 192.168.2.0/24 network. You can verify this by using the **show ip route** command.

- f. On R2, issue the **no passive-interface** command so the router will send and receive OSPF routing updates. After entering this command, you will see an informational message that a neighbor adjacency has been established with R1.

```
R2(config)# router ospf 1
```

```
R2(config-router)# no passive-interface s0/0/0
```

```
R2(config-router)#
```

```
*Apr  3 00:18:03.463: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from LOADING to FULL, Loading Done
```

- g. Re-issue the **show ip route** and **show ipv6 ospf neighbor** commands on R1 and R3, and look for a route to the 192.168.2.0/24 network.

What interface is R3 using to route to the 192.168.2.0/24 network? _____

What is the accumulated cost metric for the 192.168.2.0/24 network on R3? _____

Does R2 show up as an OSPF neighbor on R1? _____

Does R2 show up as an OSPF neighbor on R3? _____

What does this information tell you?

- h. Change interface S0/0/1 on R2 to allow it to advertise OSPF routes. Record the commands used below.

- i. Re-issue the **show ip route** command on R3.

What interface is R3 using to route to the 192.168.2.0/24 network? _____

What is the accumulated cost metric for the 192.168.2.0/24 network on R3 now and how is this calculated?

Is R2 listed as an OSPF neighbor to R3? _____

Part 5: Change OSPF Metrics

In Part 3, you will change OSPF metrics using the **auto-cost reference-bandwidth** command, the **bandwidth** command, and the **ip ospf cost** command.

Note: All DCE interfaces should have been configured with a clocking rate of 128000 in Part 1.

Step 1: Change the reference bandwidth on the routers.

The default reference-bandwidth for OSPF is 100Mb/s (Fast Ethernet speed). However, most modern infrastructure devices have links that are faster than 100Mb/s. Because the OSPF cost metric must be an integer, all links with transmission speeds of 100Mb/s or higher have a cost of 1. This results in Fast Ethernet, Gigabit Ethernet and 10G Ethernet interfaces all having the same cost. Therefore, the reference-bandwidth must be changed to a higher value to accommodate networks with links faster than 100Mb/s.

- a. Issue the **show interface** command on R1 to view the default bandwidth setting for the G0/0 interface.

```
R1# show interface g0/0
```

```
GigabitEthernet0/0 is up, line protocol is up
```

```
Hardware is CN Gigabit Ethernet, address is c471.fe45.7520 (bia c471.fe45.7520)
```

```
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 100 usec,
```

```
reliability 255/255, txload 1/255, rxload 1/255
```

```
Encapsulation ARPA, loopback not set
```

```
Keepalive set (10 sec)
```

```

Full Duplex, 100Mbps, media type is RJ45
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 00:17:31, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts (0 IP multicasts)
  0 runs, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 0 multicast, 0 pause input
  279 packets output, 89865 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 unknown protocol drops
  0 babbles, 0 late collision, 0 deferred
  1 lost carrier, 0 no carrier, 0 pause output
  0 output buffer failures, 0 output buffers swapped out

```

Note: The bandwidth setting on G0/0 may differ from what is shown above if the PC host interface can only support Fast Ethernet speed. If the PC host interface is not capable of supporting gigabit speed, then the bandwidth will most likely be displayed as 100000 Kbit/sec.

- b. Issue the **show ip route ospf** command on R1 to determine the route to the 192.168.3.0/24 network.

```
R1# show ip route ospf
```

```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

```

```
Gateway of last resort is not set
```

```

O      192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:57, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O      192.168.23.0 [110/128] via 192.168.13.2, 00:00:57, Serial0/0/1
      [110/128] via 192.168.12.2, 00:01:08, Serial0/0/0

```

Note: The accumulated cost to the 192.168.3.0/24 network from R1 is 65.

- c. Issue the **show ip ospf interface** command on R3 to determine the routing cost for G0/0.

```
R3# show ip ospf interface g0/0
```

```

GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1

```

```

Topology-MTID      Cost      Disabled      Shutdown      Topology Name
      0              1          no          no          Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:05
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

```

- d. Issue the **show ip ospf interface s0/0/1** command on R1 to view the routing cost for S0/0/1.

```

R1# show ip ospf interface s0/0/1
Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 64
Topology-MTID      Cost      Disabled      Shutdown      Topology Name
      0             64          no          no          Base
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:04
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.23.2
Suppress hello for 0 neighbor(s)

```

The sum of the costs of these two interfaces is the accumulated cost for the route to the 192.168.3.0/24 network on R3 (1 + 64 = 65), as can be seen in the output from the **show ip route** command.

- e. Issue the **auto-cost reference-bandwidth 10000** command on R1 to change the default reference bandwidth setting. With this setting, 10Gb/s interfaces will have a cost of 1, 1 Gb/s interfaces will have a cost of 10, and 100Mb/s interfaces will have a cost of 100.

```

R1(config)# router ospf 1
R1(config-router)# auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
  Please ensure reference bandwidth is consistent across all routers.

```

- f. Issue the **auto-cost reference-bandwidth 10000** command on routers R2 and R3.
- g. Re-issue the **show ip ospf interface** command to view the new cost of G0/0 on R3, and S0/0/1 on R1.

R3# **show ip ospf interface g0/0**

```
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 10
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
        0             10         no            no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Note: If the device connected to the G0/0 interface does not support Gigabit Ethernet speed, the cost will be different than the output display. For example, the cost will be 100 for Fast Ethernet speed (100Mb/s).

R1# **show ip ospf interface s0/0/1**

```
Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 6476
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
        0             6476         no            no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:05
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.23.2
  Suppress hello for 0 neighbor(s)
```

- h. Re-issue the **show ip route ospf** command to view the new accumulated cost for the 192.168.3.0/24 route (10 + 6476 = 6486).

Note: If the device connected to the G0/0 interface does not support Gigabit Ethernet speed, the total cost will be different than the output display. For example, the accumulated cost will be 6576 if G0/0 is operating at Fast Ethernet speed (100Mb/s).

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

```
O      192.168.2.0/24 [110/6486] via 192.168.12.2, 00:05:40, Serial0/0/0
O      192.168.3.0/24 [110/6486] via 192.168.13.2, 00:01:08, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O          192.168.23.0 [110/12952] via 192.168.13.2, 00:05:17, Serial0/0/1
                  [110/12952] via 192.168.12.2, 00:05:17, Serial0/0/
```

Note: Changing the default reference-bandwidth on the routers from 100 to 10,000 in effect changed the accumulated costs of all routes by a factor of 100, but the cost of each interface link and route is now more accurately reflected.

- i. To reset the reference-bandwidth back to its default value, issue the **auto-cost reference-bandwidth 100** command on all three routers.

R1(config)# **router ospf 1**

R1(config-router)# **auto-cost reference-bandwidth 100**

% OSPF: Reference bandwidth is changed.

Please ensure reference bandwidth is consistent across all routers.

Why would you want to change the OSPF default reference-bandwidth?

Step 2: Change the bandwidth for an interface.

On most serial links, the bandwidth metric will default to 1544 Kbits (that of a T1). If this is not the actual speed of the serial link, the bandwidth setting will need to be changed to match the actual speed to allow the route cost to be calculated correctly in OSPF. Use the **bandwidth** command to adjust the bandwidth setting on an interface.

Note: A common misconception is to assume that the **bandwidth** command will change the physical bandwidth, or speed, of the link. The command modifies the bandwidth metric used by OSPF to calculate routing costs, and does not modify the actual bandwidth (speed) of the link.

- a. Issue the **show interface s0/0/0** command on R1 to view the current bandwidth setting on S0/0/0. Even though the clock rate, link speed on this interface was set to 128Kb/s, the bandwidth is still showing 1544Kb/s.

R1# **show interface s0/0/0**

Serial0/0/0 is up, line protocol is up

Hardware is WIC MBRD **Serial**

```

Internet address is 192.168.12.1/30
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
<Output omitted>

```

- b. Issue the **show ip route ospf** command on R1 to view the accumulated cost for the route to network 192.168.23.0/24 using S0/0/0. Note that there are two equal-cost (128) routes to the 192.168.23.0/24 network, one via S0/0/0 and one via S0/0/1.

```
R1# show ip route ospf
```

```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

```

```
Gateway of last resort is not set
```

```

O      192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:26, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O      192.168.23.0 [110/128] via 192.168.13.2, 00:00:26, Serial0/0/1
      [110/128] via 192.168.12.2, 00:00:42, Serial0/0/0

```

- c. Issue the **bandwidth 128** command to set the bandwidth on S0/0/0 to 128Kb/s.

```
R1(config)# interface s0/0/0
```

```
R1(config-if)# bandwidth 128
```

- d. Re-issue the **show ip route ospf** command. The routing table no longer displays the route to the 192.168.23.0/24 network over the S0/0/0 interface. This is because the best route, the one with the lowest cost, is now via S0/0/1.

```
R1# show ip route ospf
```

```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

```

```
Gateway of last resort is not set
```

```

O      192.168.3.0/24 [110/65] via 192.168.13.2, 00:04:51, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O      192.168.23.0 [110/128] via 192.168.13.2, 00:04:51, Serial0/0/1

```

- e. Issue the **show ip ospf interface brief** command. The cost for S0/0/0 has changed from 64 to 781 which is an accurate cost representation of the link speed.

R1# **show ip ospf interface brief**

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Se0/0/1	1	0	192.168.13.1/30	64	P2P	1/1	
Se0/0/0	1	0	192.168.12.1/30	781	P2P	1/1	
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0	

- f. Change the bandwidth for interface S0/0/1 to the same setting as S0/0/0 on R1.
- g. Re-issue the **show ip route ospf** command to view the accumulated cost of both routes to the 192.168.23.0/24 network. Note that there are again two equal-cost (845) routes to the 192.168.23.0/24 network, one via S0/0/0 and one via S0/0/1.

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
 + - replicated route, % - next hop override

Gateway of last resort is not set

```
O      192.168.3.0/24 [110/782] via 192.168.13.2, 00:00:09, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O      192.168.23.0 [110/845] via 192.168.13.2, 00:00:09, Serial0/0/1
      [110/845] via 192.168.12.2, 00:00:09, Serial0/0/0
```

Explain how the costs to the 192.168.3.0/24 and 192.168.23.0/30 networks from R1 were calculated.

- h. Issue the **show ip route ospf** command on R3. The accumulated cost of the 192.168.1.0/24 is still showing as 65. Unlike the **clock rate** command, the **bandwidth** command needs to be applied on each side of a serial link.

R3# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
 + - replicated route, % - next hop override

Gateway of last resort is not set

```

O      192.168.1.0/24 [110/65] via 192.168.13.1, 00:30:58, Serial0/0/0
      192.168.12.0/30 is subnetted, 1 subnets
O      192.168.12.0 [110/128] via 192.168.23.1, 00:30:58, Serial0/0/1
      [110/128] via 192.168.13.1, 00:30:58, Serial0/0/0

```

- i. Issue the **bandwidth 128** command on all remaining serial interfaces in the topology.

What is the new accumulated cost to the 192.168.23.0/24 network on R1? Why?

Step 3: Change the route cost.

OSPF uses the bandwidth setting to calculate the cost for a link by default. However, you can override this calculation by manually setting the cost of a link using the **ip ospf cost** command. Like the **bandwidth** command, the **ip ospf cost** command only affects the side of the link where it was applied.

- a. Issue the **show ip route ospf** on R1.

```

R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

```

Gateway of last resort is not set

```

O      192.168.2.0/24 [110/782] via 192.168.12.2, 00:00:26, Serial0/0/0
O      192.168.3.0/24 [110/782] via 192.168.13.2, 00:02:50, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O      192.168.23.0 [110/1562] via 192.168.13.2, 00:02:40, Serial0/0/1
      [110/1562] via 192.168.12.2, 00:02:40, Serial0/0/0

```

- b. Apply the **ip ospf cost 1565** command to the S0/0/1 interface on R1. A cost of 1565 is higher than the accumulated cost of the route through R2 which is 1562.

```

R1(config)# int s0/0/1
R1(config-if)# ip ospf cost 1565

```

- c. Re-issue the **show ip route ospf** command on R1 to display the effect this change has made on the routing table. All OSPF routes for R1 are now being routed through R2.

```

R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

```

Gateway of last resort is not set

- O 192.168.2.0/24 [110/782] via 192.168.12.2, 00:02:06, Serial0/0/0
- O 192.168.3.0/24 [110/1563] via 192.168.12.2, 00:05:31, Serial0/0/0
- 192.168.23.0/30 is subnetted, 1 subnets
- O 192.168.23.0 [110/1562] via 192.168.12.2, 01:14:02, Serial0/0/0

Note: Manipulating link costs using the **ip ospf cost** command is the easiest and preferred method for changing OSPF route costs. In addition to changing the cost based on bandwidth, a network administrator may have other reasons for changing the cost of a route, such as preference for a particular service provider or the actual monetary cost of a link or route.

Explain why the route to the 192.168.3.0/24 network on R1 is now going through R2?

Reflection

1. Why is it important to control the router ID assignment when using the OSPF protocol?

2. Why is the DR/BDR election process not a concern in this lab?

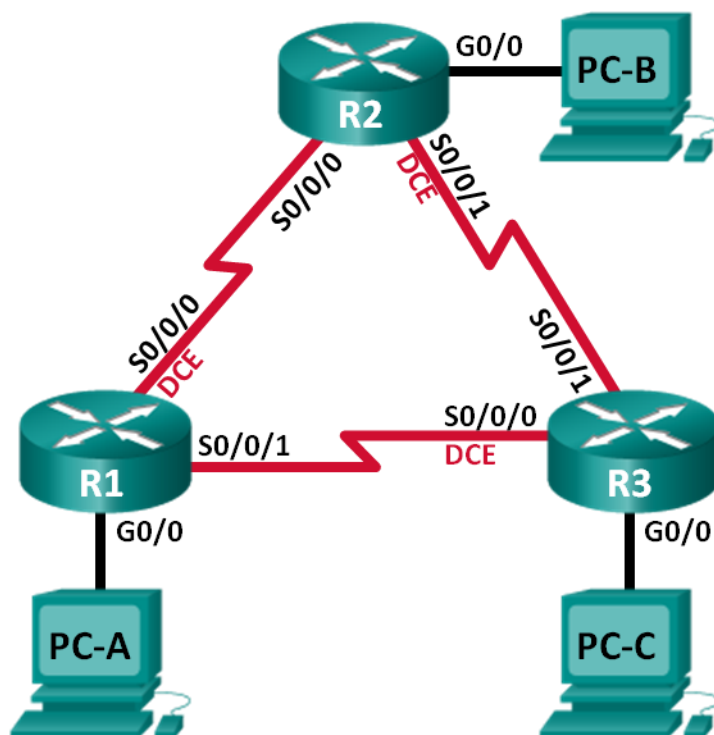
3. Why would you want to set an OSPF interface to passive?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

19 - Configuring Basic Single-Area OSPFv3

Topology



Addressing Table

Device	Interface	IPv6 Address	Default Gateway
R1	G0/0	2001:DB8:ACAD:A::1/64 FE80::1 link-local	N/A
	S0/0/0 (DCE)	2001:DB8:ACAD:12::1/64 FE80::1 link-local	N/A
	S0/0/1	2001:DB8:ACAD:13::1/64 FE80::1 link-local	N/A
R2	G0/0	2001:DB8:ACAD:B::2/64 FE80::2 link-local	N/A
	S0/0/0	2001:DB8:ACAD:12::2/64 FE80::2 link-local	N/A
	S0/0/1 (DCE)	2001:DB8:ACAD:23::2/64 FE80::2 link-local	N/A
R3	G0/0	2001:DB8:ACAD:C::3/64 FE80::3 link-local	N/A
	S0/0/0 (DCE)	2001:DB8:ACAD:13::3/64 FE80::3 link-local	N/A
	S0/0/1	2001:DB8:ACAD:23::3/64 FE80::3 link-local	N/A
PC-A	NIC	2001:DB8:ACAD:A::A/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::B/64	FE80::2
PC-C	NIC	2001:DB8:ACAD:C::C/64	FE80::3

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure and Verify OSPFv3 Routing

Part 3: Configure OSPFv3 Passive Interfaces

Background / Scenario

Open Shortest Path First (OSPF) is a link-state routing protocol for IP networks. OSPFv2 is defined for IPv4 networks, and OSPFv3 is defined for IPv6 networks.

In this lab, you will configure the network topology with OSPFv3 routing, assign router IDs, configure passive interfaces, and use a number of CLI commands to display and verify OSPFv3 routing information.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). Other routers and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 6: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the PC hosts and routers.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the routers as necessary.

Step 3: Configure basic settings for each router.

- Disable DNS lookup.
- Configure device name as shown in the topology.
- Assign **class** as the privileged EXEC password.
- Assign **cisco** as the vty password.
- Configure a MOTD banner to warn users that unauthorized access is prohibited.
- Configure **logging synchronous** for the console line.
- Encrypt plain text passwords.
- Configure the IPv6 unicast and link-local addresses listed in the Addressing Table for all interfaces.
- Enable IPv6 unicast routing on each router.
- Copy the running configuration to the startup configuration.

Step 4: Configure PC hosts.

Step 5: Test connectivity.

The routers should be able to ping one another, and each PC should be able to ping its default gateway. The PCs are unable to ping other PCs until OSPFv3 routing is configured. Verify and troubleshoot if necessary.

Part 7: Configure OSPFv3 Routing

In Part 2, you will configure OSPFv3 routing on all routers in the network and then verify that routing tables are updated correctly.

Step 1: Assign router IDs.

OSPFv3 continues to use a 32 bit address for the router ID. Because there are no IPv4 addresses configured on the routers, you will manually assign the router ID using the **router-id** command.

- a. Issue the **ipv6 router ospf** command to start an OSPFv3 process to the router.

```
R1(config)# ipv6 router ospf 1
```

Note: The OSPF process ID is kept locally and has no meaning to other routers on the network.

- b. Assign the OSPFv3 router ID **1.1.1.1** to the R1.

```
R1(config-rtr)# router-id 1.1.1.1
```

- c. Start the OSPFv3 routing process and assign a router ID of **2.2.2.2** to R2 and a router ID of **3.3.3.3** to R3.

- d. Issue the **show ipv6 ospf** command to verify the router IDs on all routers.

```
R2# show ipv6 ospf
```

```
Routing Process "ospfv3 1" with ID 2.2.2.2
```

```
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
```

```
Router is not originating router-LSAs with maximum metric
```

```
<output omitted>
```

Step 2: Configure OSPFv6 on R1.

With IPv6, it is common to have multiple IPv6 addresses configured on an interface. The network statement has been eliminated in OSPFv3. OSPFv3 routing is enabled at the interface level instead.

- a. Issue the **ipv6 ospf 1 area 0** command for each interface on R1 that is to participate in OSPFv3 routing.

```
R1(config)# interface g0/0
```

```
R1(config-if)# ipv6 ospf 1 area 0
```

```
R1(config-if)# interface s0/0/0
```

```
R1(config-if)# ipv6 ospf 1 area 0
```

```
R1(config-if)# interface s0/0/1
```

```
R1(config-if)# ipv6 ospf 1 area 0
```

Note: The process ID must match the process ID you used in Step1a.

- b. Assign the interfaces on R2 and R3 to OSPFv3 area 0. You should see neighbor adjacency messages display when adding the interfaces to area 0.

```
R1#
```

```
*Mar 19 22:14:43.251: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from  
LOADING to FULL, Loading Done
```

```
R1#
```

```
*Mar 19 22:14:46.763: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from  
LOADING to FULL, Loading Done
```

Step 3: Verify OSPFv3 neighbors.

Issue the **show ipv6 ospf neighbor** command to verify that the router has formed an adjacency with its neighboring routers. If the router ID of the neighboring router is not displayed, or if its state does not show as FULL, the two routers have not formed an OSPF adjacency.

```
R1# show ipv6 ospf neighbor
```

```
OSPFv3 Router with ID (1.1.1.1) (Process ID 1)
```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	0	FULL/ -	00:00:39	6	Serial0/0/1
2.2.2.2	0	FULL/ -	00:00:36	6	Serial0/0/0

Step 4: Verify OSPFv3 protocol settings.

The **show ipv6 protocols** command is a quick way to verify vital OSPFv3 configuration information, including the OSPF process ID, the router ID, and the interfaces enabled for OSPFv3.

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Router ID 1.1.1.1
  Number of areas: 1 normal, 0 stub, 0 nssa
  Interfaces (Area 0):
    Serial0/0/1
    Serial0/0/0
    GigabitEthernet0/0
  Redistribution:
    None
```

Step 5: Verify OSPFv3 interfaces.

- a. Issue the **show ipv6 ospf interface** command to display a detailed list for every OSPF-enabled interface.

```
R1# show ipv6 ospf interface
Serial0/0/1 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 7
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Graceful restart helper support enabled
  Index 1/3/3, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 3.3.3.3
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 6
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Graceful restart helper support enabled
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
```

```

    Adjacent with neighbor 2.2.2.2
    Suppress hello for 0 neighbor(s)
    GigabitEthernet0/0 is up, line protocol is up
    Link Local Address FE80::1, Interface ID 3
    Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
    Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State DR, Priority 1
    Designated Router (ID) 1.1.1.1, local address FE80::1
    No backup designated router on this network
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
    Graceful restart helper support enabled
    Index 1/1/1, flood queue length 0
    Next 0x0(0)/0x0(0)/0x0(0)
    Last flood scan length is 0, maximum is 0
    Last flood scan time is 0 msec, maximum is 0 msec
    Neighbor Count is 0, Adjacent neighbor count is 0
    Suppress hello for 0 neighbor(s)

```

- b. To display a summary of OSPFv3-enabled interfaces, issue the **show ipv6 ospf interface brief** command.

```

R1# show ipv6 ospf interface brief

```

Interface	PID	Area	Intf ID	Cost	State	Nbrs	F/C
Se0/0/1	1	0	7	64	P2P	1/1	
Se0/0/0	1	0	6	64	P2P	1/1	
Gi0/0	1	0	3	1	DR	0/0	

Step 6: Verify the IPv6 routing table.

Issue the **show ipv6 route** command to verify that all networks are appearing in the routing table.

```

R2# show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001:DB8:ACAD:A::/64 [110/65]
    via FE80::1, Serial0/0/0
C   2001:DB8:ACAD:B::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:B::2/128 [0/0]
    via GigabitEthernet0/0, receive
O   2001:DB8:ACAD:C::/64 [110/65]
    via FE80::3, Serial0/0/1
C   2001:DB8:ACAD:12::/64 [0/0]
    via Serial0/0/0, directly connected
L   2001:DB8:ACAD:12::2/128 [0/0]
    via Serial0/0/0, receive

```

```

O  2001:DB8:ACAD:13::/64 [110/128]
    via FE80::3, Serial0/0/1
    via FE80::1, Serial0/0/0
C  2001:DB8:ACAD:23::/64 [0/0]
    via Serial0/0/1, directly connected
L  2001:DB8:ACAD:23::2/128 [0/0]
    via Serial0/0/1, receive
L  FF00::/8 [0/0]
    via Null0, receive

```

What command would you use to only see the OSPF routes in the routing table? _____

Step 7: Verify end-to-end connectivity.

Each PC should be able to ping the other PCs in the topology. Verify and troubleshoot if necessary.

Note: It may be necessary to disable the PC firewall to ping between PCs.

Part 8: Configure OSPFv3 Passive Interfaces

The **passive-interface** command prevents routing updates from being sent through the specified router interface. This is commonly done to reduce traffic on the LANs as they do not need to receive dynamic routing protocol communication. In Part 3, you will use the **passive-interface** command to configure a single interface as passive. You will also configure OSPFv3 so that all interfaces on the router are passive by default, and then enable OSPF routing advertisements on selected interfaces.

Step 1: Configure a passive interface.

- Issue the **show ipv6 ospf interface g0/0** command on R1. Notice the timer indicating when the next Hello packet is expected. Hello packets are sent every 10 seconds and are used between OSPF routers to verify that their neighbors are up.

```

R1# show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, local address FE80::1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Graceful restart helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)

```

- Issue the **passive-interface** command to change the G0/0 interface on R1 to passive.

```

R1(config)# ipv6 router ospf 1
R1(config-rtr)# passive-interface g0/0

```

- c. Re-issue the **show ipv6 ospf interface g0/0** command to verify that G0/0 is now passive.

```
R1# show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
  Wait time before Designated router selection 00:00:34
  Graceful restart helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

- d. Issue the **show ipv6 route ospf** command on R2 and R3 to verify that a route to the 2001:DB8:ACAD:A::/64 network is still available.

```
R2# show ipv6 route ospf
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O    2001:DB8:ACAD:A::/64 [110/65]
    via FE80::1, Serial0/0/0
O    2001:DB8:ACAD:C::/64 [110/65]
    via FE80::3, Serial0/0/1
O    2001:DB8:ACAD:13::/64 [110/128]
    via FE80::3, Serial0/0/1
    via FE80::1, Serial0/0/0
```

Step 2: Set passive interface as the default on the router.

- a. Issue the **passive-interface default** command on R2 to set the default for all OSPFv3 interfaces as passive.

```
R2(config)# ipv6 router ospf 1
R2(config-rtr)# passive-interface default
```

- b. Issue the **show ipv6 ospf neighbor** command on R1. After the dead timer expires, R2 is no longer listed as an OSPF neighbor.

```
R1# show ipv6 ospf neighbor
```

```
OSPFv3 Router with ID (1.1.1.1) (Process ID 1)
```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	0	FULL/ -	00:00:37	6	Serial0/0/1

- c. On R2, issue the **show ipv6 ospf interface s0/0/0** command to view the OSPF status of interface S0/0/0.

```
R2# show ipv6 ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Link Local Address FE80::2, Interface ID 6
  Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
  Graceful restart helper support enabled
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 3
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

- d. If all OSPFv3 interfaces on R2 are passive, then no routing information is being advertised. If this is the case, then R1 and R3 should no longer have a route to the 2001:DB8:ACAD:B::/64 network. You can verify this by using the **show ipv6 route** command.
- e. Change S0/0/1 on R2 by issuing the **no passive-interface** command, so that it sends and receives OSPFv3 routing updates. After entering this command, an informational message displays stating that a neighbor adjacency has been established with R3.

```
R2(config)# ipv6 router ospf 1
R2(config-rtr)# no passive-interface s0/0/1
*Apr  8 19:21:57.939: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from LOADING to FULL, Loading Done
```

- f. Re-issue the **show ipv6 route** and **show ipv6 ospf neighbor** commands on R1 and R3, and look for a route to the 2001:DB8:ACAD:B::/64 network.

What interface is R1 using to route to the 2001:DB8:ACAD:B::/64 network? _____

What is the accumulated cost metric for the 2001:DB8:ACAD:B::/64 network on R1? _____

Does R2 show up as an OSPFv3 neighbor on R1? _____

Does R2 show up as an OSPFv3 neighbor on R3? _____

What does this information tell you?

- g. On R2, issue the **no passive-interface S0/0/0** command to allow OSPFv3 routing updates to be advertised on that interface.
- h. Verify that R1 and R2 are now OSPFv3 neighbors.

Reflection

1. If the OSPFv6 configuration for R1 had a process ID of 1, and the OSPFv3 configuration for R2 had a process ID of 2, can routing information be exchanged between the two routers? Why?

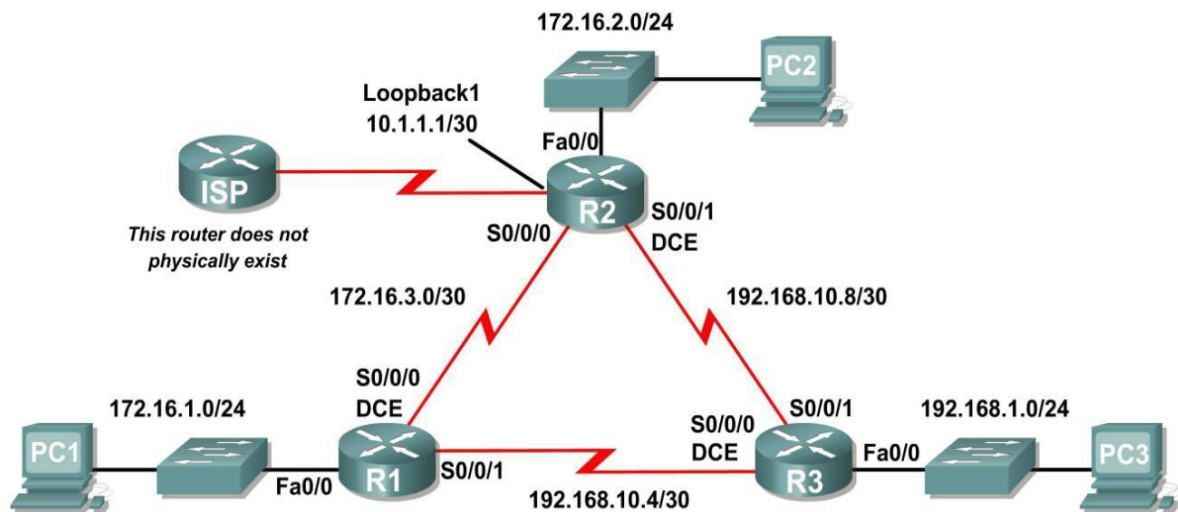
2. What may have been the reasoning for removing the **network** command in OSPFv3?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

20 - Basic EIGRP Configuration Lab

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.3.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	Fa0/0	172.16.2.1	255.255.255.0	N/A
	S0/0/0	172.16.3.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
	Lo1	10.1.1.1	255.255.255.252	N/A
R3	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	NIC	172.16.1.10	255.255.255.0	172.16.1.1
PC2	NIC	172.16.2.10	255.255.255.0	172.16.2.1
PC3	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the Topology Diagram.
- Erase the startup configuration and reload a router to the default state.
- Perform basic configuration tasks on a router.
- Configure and activate interfaces.
- Configure EIGRP routing on all routers.
- Verify EIGRP routing using **show** commands.
- Disable automatic summarization.
- Configure manual summarization. Configure a static default route.
- Propagate default route to EIGRP neighbors.
- Document the EIGRP configuration.

Scenario

In this lab activity, you will learn how to configure the routing protocol EIGRP using the network shown in the Topology Diagram. A loopback address will be used on the R2 router to simulate a connection to an ISP, where all traffic that is not destined for the local network will be sent. Some segments of the network have been subnetted using VLSM. EIGRP is a classless routing protocol that can be used to provide subnet mask information in the routing updates. This will allow VLSM subnet information to be propagated throughout the network.

Task 1: Prepare the Network.

Step 1: Cable a network that is similar to the one in the Topology Diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations,

Perform basic configuration of the R1, R2, and R3 routers according to the following guidelines:

1. Configure the router hostname.
2. Disable DNS lookup.
3. Configure an EXEC mode password.
4. Configure a message-of-the-day banner.
5. Configure a password for console connections.
6. Configure a password for VTY connections.

Task 3: Configure and Activate Serial and Ethernet Addresses.

Step 1: Configure the interfaces on the R1, R2, and R3 routers.

Configure the interfaces on the R1, R2, and R3 routers with the IP addresses from the table under the Topology Diagram.

Step 2: Verify IP addressing and interfaces.

Use the **show ip interface brief** command to verify that the IP addressing is correct and that the interfaces are active.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 3: Configure Ethernet interfaces of PC1, PC2, and PC3.

Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses and default gateways from the table under the Topology Diagram.

Task 4: Configure EIGRP on the R1 Router.

Step 1: Enable EIGRP.

Use the **router eigrp** command in global configuration mode to enable EIGRP on the R1 router. Enter a process ID of 1 for the *autonomous-system* parameter.

```
R1(config)#router eigrp 1
R1(config-router)#
```

Step 2: Configure classful network 172.16.0.0.

Once you are in the Router EIGRP configuration sub-mode, configure the classful network 172.16.0.0 to be included in the EIGRP updates that are sent out of R1.

```
R1(config-router)#network 172.16.0.0
R1(config-router)#
```

The router will begin to send EIGRP update messages out each interface belonging to the 172.16.0.0 network. EIGRP updates will be sent out of the FastEthernet0/0 and Serial0/0/0 interfaces because they are both on subnets of the 172.16.0.0 network.

Step 3: Configure the router to advertise the 192.168.10.4/30 network attached to the Serial0/0/1 interface.

Use the *wildcard-mask* option with the **network** command to advertise only the subnet and not the entire 192.168.10.0 classful network.

Note: Think of a wildcard mask as the inverse of a subnet mask. The inverse of the subnet mask 255.255.255.252 is 0.0.0.3. To calculate the inverse of the subnet mask, subtract the subnet mask from 255.255.255.255:

255.255.255.255	
- 255.255.255.252	Subtract the subnet mask

0. 0. 0. 3	Wildcard mask

```
R1(config-router)# network 192.168.10.4 0.0.0.3  
R1(config-router)#
```

When you are finished with the EIGRP configuration for R1, return to privileged EXEC mode and save the current configuration to NVRAM.

```
R1(config-router)#end  
%SYS-5-CONFIG_I: Configured from console by console  
R1#
```

Task 5: Configure EIGRP on the R2 and R3 Routers.

Step 1: Enable EIGRP routing on the R2 router using the `router eigrp` command.

Use a process ID of 1.

```
R2(config)#router eigrp 1  
R2(config-router)#
```

Step 2: Use the classful address 172.16.0.0 to include the network for the FastEthernet0/0 interface.

```
R2(config-router)#network 172.16.0.0  
R2(config-router)#  
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.3.1 (Serial0/0/0) is up:  
new adjacency
```

Notice that DUAL sends a notification message to the console stating that a neighbor relationship with another EIGRP router has been established.

What is the IP address of the EIGRP neighbor router?

What interface on the R2 router is the neighbor adjacent to?

Step 3: Configure the R2 router to advertise the 192.168.10.8/30 network attached to the Serial0/0/1 interface.

1. Use the *wildcard-mask* option with the **network** command to advertise only the subnet and not the entire 192.168.10.0 classful network.
2. When you are finished, return to privileged EXEC mode.

```
R2(config-router)#network 192.168.10.8 0.0.0.3  
R2(config-router)#end  
%SYS-5-CONFIG_I: Configured from console by console  
R2#
```

Step 4: Configure EIGRP on the R3 router using the `router eigrp` and `network` commands.

1. Use a process ID of 1.

2. Use the classful network address for the network attached to the FastEthernet0/0 interface.
3. Include the wildcard masks for the subnets attached to the Serial0/0/0 and Serial 0/0/1 interfaces.
4. When you are finished, return to privileged EXEC mode.

```
R3(config)#router eigrp 1
R3(config-router)#network 192.168.1.0
R3(config-router)#network 192.168.10.4 0.0.0.3
R3(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.5 (Serial0/0/0) is up:
new adjacency
R3(config-router)#network 192.168.10.8 0.0.0.3
R3(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.9 (Serial0/0/1) is up:
new adjacency
R3(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R3#
```

Notice that when the networks for the serial links from R3 to R1 and R3 to R2 are added to the EIGRP configuration, DUAL sends a notification message to the console stating that a neighbor relationship with another EIGRP router has been established.

Task 6: Verify EIGRP Operation.

Step 1: View neighbors.

On the R1 router, use the **show ip eigrp neighbors** command to view the neighbor table and verify that EIGRP has established an adjacency with the R2 and R3 routers. You should be able to see the IP address of each adjacent router and the interface that R1 uses to reach that EIGRP neighbor.

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address           Interface           Hold Uptime        SRTT   RTO   Q   Seq
                               (sec)              (ms)                Cnt   Num
0   172.16.3.2          Ser0/0/0            10    00:36:51    40     500   0   13
1   192.168.10.6         Ser0/0/1            11    00:26:51    40     500   0   4
R1#
```

Step 2: View routing protocol information.

On the R1 router, use the **show ip protocols** command to view information about the routing protocol operation. Notice that the information that was configured in Task 5, such as protocol, process ID, and networks, is shown in the output. The IP addresses of the adjacent neighbors are also shown.

```
R1#show ip protocols

Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
```

```

EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
Redistributing: eigrp 1
Automatic network summarization is in effect
Automatic address summarization:
Maximum path: 4
Routing for Networks:
  172.16.0.0
  192.168.10.4/30
Routing Information Sources:
  Gateway         Distance      Last Update
  172.16.3.2       90            4811399
  192.168.10.6     90            5411677
Distance: internal 90 external 170

```

Notice that the output specifies the process ID used by EIGRP. Remember, the process ID must be the same on all routers for EIGRP to establish neighbor adjacencies and share routing information.

Task7: Examine EIGRP Routes in the Routing Tables.

Step1: View the routing table on the R1 router.

EIGRP routes are denoted in the routing table with a **D**, which stands for DUAL (Diffusing Update Algorithm), which is the routing algorithm used by EIGRP.

R1#**show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is not set

```

      172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 01:16:19, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/2172416] via 172.16.3.2, 01:16:20, Serial0/0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
D       192.168.1.0/24 [90/2172416] via 192.168.10.6, 01:06:18, Serial0/0/1
      192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 01:06:07, Null0
C       192.168.10.4/30 is directly connected, Serial0/0/1
D       192.168.10.8/30 [90/2681856] via 192.168.10.6, 01:06:07, Serial0/0/1
R1#

```

Notice that the 172.16.0.0/16 parent network is variably subnetted with three child routes using either a /24 or /30 mask. Also notice that EIGRP has automatically included a summary route to Null0 for the 172.16.0.0/16 network. The 172.16.0.0/16 route does not actually represent a path to reach the parent network, 172.16.0.0/16. If a packet destined for 172.16.0.0/16 does not match one of the level 2 child routes, it is sent to the Null0 interface.

172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks

```
D    172.16.0.0/16 is a summary, 01:16:19, Null0
C    172.16.1.0/24 is directly connected, FastEthernet0/0
D    172.16.2.0/24 [90/2172416] via 172.16.3.2, 01:16:20, Serial0/0/0
C    172.16.3.0/30 is directly connected, Serial0/0/0
```

The 192.168.10.0/24 Network is also variably subnetted and includes a Null0 route.

192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks

```
D    192.168.10.0/24 is a summary, 01:06:07, Null0
C    192.168.10.4/30 is directly connected, Serial0/0/1
D    192.168.10.8/30 [90/2681856] via 192.168.10.6, 01:06:07,
Serial0/0/1
```

Step 2: View the routing table on the R3 router.

The routing table for R3 shows that both R1 and R2 are automatically summarizing the 172.16.0.0/16 network and sending it as a single routing update. Because of automatic summarization, R1 and R2 are not propagating the individual subnets. Because R3 is getting two equal cost routes for 172.16.0.0/16 from both R1 and R2, both routes are included in the routing table.

```
R3#show ip route
```

<output omitted>

```
D    172.16.0.0/16 [90/2172416] via 192.168.10.5, 01:15:35, Serial0/0/0
      [90/2172416] via 192.168.10.9, 01:15:22, Serial0/0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
      192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D    192.168.10.0/24 is a summary, 01:15:22, Null0
C    192.168.10.4/30 is directly connected, Serial0/0/0
C    192.168.10.8/30 is directly connected, Serial0/0/1
R3#
```

Task 8: Configure EIGRP Metrics.

Step 1: View the EIGRP metric information.

Use the `show interface serial0/0/0` command to view the EIGRP metric information for the Serial0/0/0 interface on the R1 router. Notice the values that are shown for the bandwidth, delay, reliability, and load.

```
R1#show interface serial0/0/0
```

```
Serial0/0/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 172.16.3.1/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

<output omitted>

Step 2: Modify the bandwidth of the Serial interfaces.

On most serial links, the bandwidth metric will default to 1544 Kbits. If this is not the actual bandwidth of the serial link, the bandwidth will need to be changed so that the EIGRP metric can be calculated correctly.

For this lab, the link between R1 and R2 will be configured with a bandwidth of 64 kbps, and the link between R2 and R3 will be configured with a bandwidth of 1024 kbps. Use the **bandwidth** command to modify the bandwidth of the Serial interfaces of each router.

R1 router:

```
R1(config)#interface serial0/0/0
R1(config-if)#bandwidth 64
```

R2 router:

```
R2(config)#interface serial0/0/0
R2(config-if)#bandwidth 64
R2(config)#interface serial0/0/1
R2(config-if)#bandwidth 1024
```

R3 router:

```
R3(config)#interface serial0/0/1
R3(config-if)#bandwidth 1024
```

Note: The **bandwidth** command only modifies the bandwidth metric used by routing protocols, not the physical bandwidth of the link.

Step 3: Verify the bandwidth modifications.

Use the **show ip interface** command to verify that the bandwidth value of each link has been changed.

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 172.16.3.1/30
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

<output omitted>

```
R2#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 172.16.3.2/30
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

<output omitted>

```
R3#show interface serial0/0/1
```

Serial0/0/1 is up, line protocol is up (connected)

Hardware is HD64570

Internet address is 192.168.10.10/30

MTU 1500 bytes, BW 1024 Kbit, DLY 20000 usec, rely 255/255, load 1/255

Encapsulation HDLC, loopback not set, keepalive set (10 sec)

<output omitted>

Note: Use the interface configuration command **no bandwidth** to return the bandwidth to its default value.

Task 9: Examine Successors and Feasible Distances.

Step 1: Examine the successors and feasible distances in the routing table on R2.

```
R2#show ip route
```

<output omitted>

```
10.0.0.0/30 is subnetted, 1 subnets
C    10.1.1.0 is directly connected, Loopback1
172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D    172.16.0.0/16 is a summary, 00:00:52, Null0
D    172.16.1.0/24 [90/40514560] via 172.16.3.1, 00:00:52, Serial0/0/0
C    172.16.2.0/24 is directly connected, FastEthernet0/0
C    172.16.3.0/30 is directly connected, Serial0/0/0
D    192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:00:11, Serial0/0/1
192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D    192.168.10.0/24 is a summary, 00:00:11, Null0
D    192.168.10.4/30 [90/3523840] via 192.168.10.10, 00:00:11,
Serial0/0/1
C    192.168.10.8/30 is directly connected, Serial0/0/1
R2#
```

Step 2: Answer the following questions:

What is the best path to PC1?

A successor is a neighboring router that is currently being used for packet forwarding. A successor is the least-cost route to the destination network. The IP address of a successor is shown in a routing table entry right after the word “via”.

What is the IP address and name of the successor router in this route?

Feasible distance (FD) is the lowest calculated metric to reach that destination. FD is the metric listed in the routing table entry as the second number inside the brackets.

What is the feasible distance to the network that PC1 is on?

Task 10: Determine if R1 is a Feasible Successor for the Route from R2 to the 192.168.1.0 Network.

A feasible successor is a neighbor who has a viable backup path to the same network as the successor. In order to be a feasible successor, R1 must satisfy the feasibility condition. The feasibility condition (FC) is met when a neighbor's reported distance (RD) to a network is less than the local router's feasible distance to the same destination network.

Step 1: Examine the routing table on R1.

```
R1#show ip route
```

```
<output omitted>
```

```
    172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:42:59, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/40514560] via 172.16.3.2, 00:43:00, Serial0/0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
D       192.168.1.0/24 [90/2172416] via 192.168.10.6, 00:42:26, Serial0/0/1
    192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:42:20, Null0
C       192.168.10.4/30 is directly connected, Serial0/0/1
D       192.168.10.8/30 [90/3523840] via 192.168.10.6, 00:42:20,
Serial0/0/1
R1#
```

What is the reported distance to the 192.168.1.0 network?

Step 2: Examine the routing table on R2.

```
R2#show ip route
```

```
<output omitted>
```

```
    10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback1
    172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:00:52, Null0
D       172.16.1.0/24 [90/40514560] via 172.16.3.1, 00:00:52, Serial0/0/0
C       172.16.2.0/24 is directly connected, FastEthernet0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
D       192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:00:11, Serial0/0/1
    192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:00:11, Null0
D       192.168.10.4/30 [90/3523840] via 192.168.10.10, 00:00:11,
Serial0/0/1
C       192.168.10.8/30 is directly connected, Serial0/0/1
R2#
```

What is the feasible distance to the 192.168.1.0 network?

Would R2 consider R1 to be a feasible successor to the 192.168.1.0 network? _____

Task 11: Examine the EIGRP Topology Table.

Step 1: View the EIGRP topology table.

Use the **show ip eigrp topology** command to view the EIGRP topology table on R2.

```
R2#show ip eigrp topology
IP-EIGRP Topology Table for AS 1

Codes: P - Passive, A - Active, U - Update, Q - Query, R -
       Reply, r - Reply status

P 172.16.2.0/24, 1 successors, FD is
    28160 via Connected,
    FastEthernet0/0
P 172.16.3.0/30, 1 successors, FD is
    40512000 via Connected,
    Serial0/0/0
P 192.168.10.8/30, 1 successors, FD is 3011840
    via Connected, Serial0/0/1
P 172.16.0.0/16, 1 successors, FD is 28160
    via Summary (28160/0), Null0
P 192.168.10.0/24, 1 successors, FD is
    3011840 via Summary (3011840/0),
    Null0
P 172.16.1.0/24, 1 successors, FD is 40514560
    via 172.16.3.1 (40514560/28160), Serial0/0/0
P 192.168.1.0/24, 1 successors, FD is 3014400
    via 192.168.10.10 (3014400/28160),
    Serial0/0/1 via 172.16.3.1
    (41026560/2172416), Serial0/0/0
P 192.168.10.4/30, 1 successors, FD is 3523840
    via 192.168.10.10 (3523840/2169856), Serial0/0/1
R2#
```

Step 2: View detailed EIGRP topology information.

Use the `[network]` parameter of the **show ip eigrp topology** command to view detailed EIGRP topology information for the 192.16.0.0 network.

```
R2#show ip eigrp topology 192.168.1.0
IP-EIGRP (AS 1): Topology entry for 192.168.1.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 3014400
  Routing Descriptor Blocks:
    192.168.10.10 (Serial0/0/1), from 192.168.10.10, Send flag is 0x0
      Composite metric is (3014400/28160), Route is Internal
```

```

Vector metric:
  Minimum bandwidth is 1024 Kbit
  Total delay is 20100 microseconds
  Reliability is 255/255
  Load is 1/255
  Minimum MTU is 1500
  Hop count is 1
172.16.3.1 (Serial0/0/0), from 172.16.3.1, Send flag is 0x0
Composite metric is (41026560/2172416), Route is Internal
Vector metric:
  Minimum bandwidth is 64 Kbit
  Total delay is 40100 microseconds
  Reliability is 255/255
  Load is 1/255
  Minimum MTU is 1500
  Hop count is 2
R2#

```

How many successors are there for this network?

What is the feasible distance to this network?

What is the IP address of the feasible successor?

What is the reported distance for 192.168.1.0 from the feasible successor?

What would be the feasible distance to 192.168.1.0 if R1 became the successor?

Task 12: Disable EIGRP Automatic Summarization.

Step 1: Examine the routing table of the R3 router.

Notice that R3 is not receiving individual routes for the 172.16.1.0/24, 172.16.2.0/24, and 172.16.3.0/24 subnets. Instead, the routing table only has a summary route to the classful network address of 172.16.0.0/16 through the R1 router. This will cause packets that are destined for the 172.16.2.0/24 network to be sent through the R1 router instead of being sent straight to the R2 router.

```
R3#show ip route
```

```
<output omitted>
```

```

D    172.16.0.0/16 [90/2172416] via 192.168.10.5, 01:21:54, Serial0/0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D    192.168.10.0/24 is a summary, 01:21:47, Null0

```

```
C      192.168.10.4/30 is directly connected, Serial0/0/0
C      192.168.10.8/30 is directly connected, Serial0/0/1
R3#
```

Why is the R1 router (192.168.10.5) the only successor for the route to the 172.16.0.0/16 network?

Notice that the reported distance from R2 is higher than the feasible distance from R1.

```
R3#show ip eigrp topology
IP-EIGRP Topology Table for AS 1

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.1.0/24, 1 successors, FD is 28160
   via Connected, FastEthernet0/0
P 192.168.10.4/30, 1 successors, FD is 2169856
   via Connected, Serial0/0/0
P 192.168.10.0/24, 1 successors, FD is 2169856
   via Summary (2169856/0), Null0
P 172.16.0.0/16, 1 successors, FD is 2172416
   via 192.168.10.5 (2172416/28160), Serial0/0/0
   via 192.168.10.9 (3014400/28160), Serial0/0/1
P 192.168.10.8/30, 1 successors, FD is 3011840
   via Connected, Serial0/0/1
```

Step 3: Disable automatic summarization on all three routers with the `no auto-summary` command.

```
R1(config)#router eigrp 1
R1(config-router)#no auto-summary

R2(config)#router eigrp 1
R2(config-router)#no auto-summary

R3(config)#router eigrp 1
R3(config-router)#no auto-summary
```

Step 4: View the routing table on R1 again.

Notice that individual routes for the 172.16.1.0/24, 172.16.2.0/24, and 172.16.3.0/24 subnets are now present and the summary Null route is no longer listed.

```
R3#show ip route
```

<output omitted>

```
172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D    172.16.1.0/24 [90/2172416] via 192.168.10.5, 00:02:37, Serial0/0/0
```

```

D      172.16.2.0/24 [90/3014400] via 192.168.10.9, 00:02:39, Serial0/0/1
D      172.16.3.0/30 [90/41024000] via 192.168.10.9, 00:02:39,
      Serial0/0/1 [90/41024000] via 192.168.10.5,
      00:02:37, Serial0/0/0
C      192.168.1.0/24 is directly connected, FastEthernet0/0
      192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C      192.168.10.4/30 is directly connected, Serial0/0/0
C      192.168.10.8/30 is directly connected, Serial0/0/1
R3#

```

Task 13: Configure Manual Summarization.

Step 1: Add loopback addresses to R3 router.

Add two loopback addresses, 192.168.2.1/24 and 192.168.3.1/24, to the R3 router. These virtual interfaces will be used to represent networks to be manually summarized along with the 192.168.1.0/24

LAN.

```

R3(config)#interface loopback1

%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed
state to upR3(config-if)#ip address 192.168.2.1 255.255.255.0
R3(config-if)#interface loopback2

%LINK-5-CHANGED: Interface Loopback2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2, changed state
to up
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#

```

Step 2: Add the 192.168.2.0 and 192.168.3.0 networks to the EIGRP configuration on R3.

```

R3(config)#router eigrp 1
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.3.0

```

Step 3: Verify new routes.

View the routing table on the R1 router to verify that the new routes are being sent out in the EIGRP updates sent by R3.

```

R1#show ip route

<output omitted>

      172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C      172.16.1.0/24 is directly connected, FastEthernet0/0
D      172.16.2.0/24 [90/3526400] via 192.168.10.6, 00:15:07, Serial0/0/1
C      172.16.3.0/30 is directly connected, Serial0/0/0
D      192.168.1.0/24 [90/2172416] via 192.168.10.6, 00:15:07, Serial0/0/1

```

```

D    192.168.2.0/24 [90/2297856] via 192.168.10.6, 00:01:07, Serial0/0/1
D    192.168.3.0/24 [90/2297856] via 192.168.10.6, 00:00:57, Serial0/0/1
    192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C        192.168.10.4/30 is directly connected, Serial0/0/1
D        192.168.10.8/30 [90/3523840] via 192.168.10.6, 00:15:07,
Serial0/0/1
R1#

```

Step 4: Apply manual summarization to outbound interfaces.

The routes to the 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24 networks can be summarized in the single network 192.168.0.0/22. Use the **ip summary-address eigrp *as-number* network- address subnet-mask** command to configure manual summarization on each of the outbound interfaces connected to EIGRP neighbors.

```

R3(config)#interface serial0/0/0
R3(config-if)#ip summary-address eigrp 1 192.168.0.0 255.255.252.0
R3(config-if)#interface serial0/0/1
R3(config-if)#ip summary-address eigrp 1 192.168.0.0 255.255.252.0
R3(config-if)#

```

Step 5: Verify the summary route.

View the routing table on the R1 router to verify that the summary route is being sent out in the EIGRP updates sent by R3.

```

R1#show ip route

<output omitted>

    172.16.0.0/16 is variably subnetted, 4 subnets, 3
                        masks
C        172.16.1.0/24 is directly connected, FastEthernet0/0
D        172.16.2.0/24 [90/3526400] via 192.168.10.6, 00:15:07, Serial0/0/1
C        172.16.3.0/30 is directly connected, Serial0/0/0
D    192.168.0.0/22 [90/2172416] via 192.168.10.6, 00:01:11, Serial0/0/1
    192.168.10.0/24 is variably subnetted, 3 subnets, 2
                        masks
C        192.168.10.4/30 is directly connected, Serial0/0/1
D        192.168.10.8/30 [90/3523840] via 192.168.10.6, 00:15:07,
Serial0/0/1
R1#

```

Task 14: Configure and Distribute a Static Default Route.

Step 1: Configure a static default route on the R2 router.

Use the loopback address that has been configured to simulate a link to an ISP as the exit interface.

```

R2(config)#ip route 0.0.0.0 0.0.0.0 loopback1
R2(config)#

```

Step 2: Include the static route in EIGRP updates.

Use the **redistribute static** command to include the static route in the EIGRP updates that are sent from the R2 router.

```
R2(config)#router eigrp 1
R2(config-router)#redistribute static
R2(config-router)#
```

Step 3: Verify the static default route.

View the routing table on the R1 router to verify that the static default route is being redistributed via EIGRP.

```
R1#show ip route
```

<output omitted>

Gateway of last resort is 192.168.10.6 to network 0.0.0.0

```
192.168.10.0/30 is subnetted, 2 subnets
C      192.168.10.4 is directly connected, Serial0/0/1
D      192.168.10.8 [90/3523840] via 192.168.10.6, 01:06:01, Serial0/0/1
172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C      172.16.1.0/24 is directly connected, FastEthernet0/0
D      172.16.2.0/24 [90/3526400] via 192.168.10.6, 01:05:39, Serial0/0/1
C      172.16.3.0/30 is directly connected, Serial0/0/0
D*EX 0.0.0.0/0 [170/3651840] via 192.168.10.6, 00:02:14, Serial0/0/1
D      192.168.0.0/22 [90/2172416] via 192.168.10.6, 01:05:38, Serial0/0/1
```

Task 15: Documentation

On each router, capture the following command output to a text (.txt) file and save for future reference.

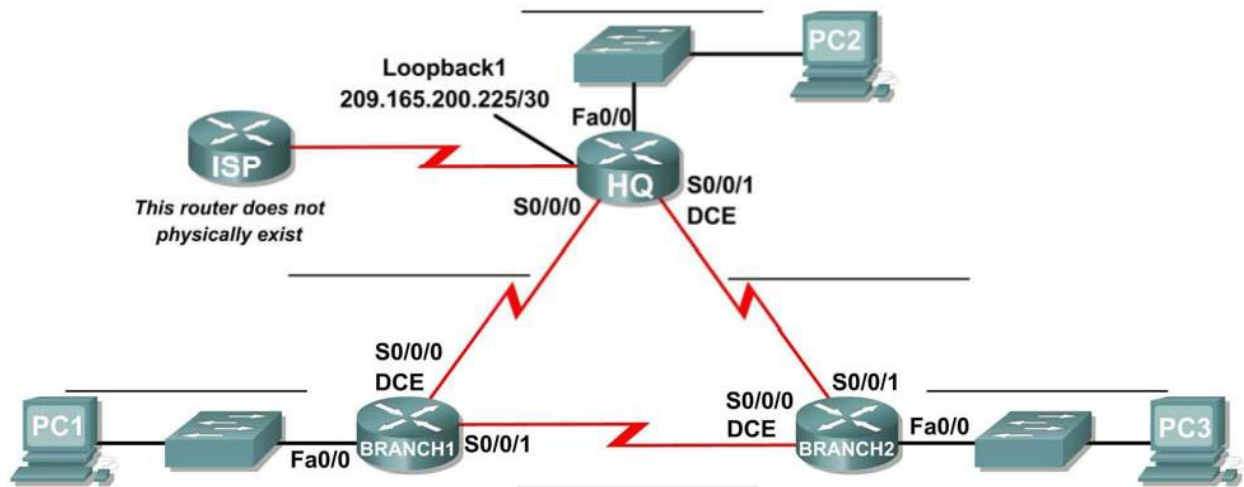
```
show running-config
show ip route
show ip interface brief
show ip protocols
```

Task 16: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

21 - Challenge EIGRP Configuration Lab

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	Fa0/0			N/A
	S0/0/0			N/A
	S0/0/1			N/A
	Lo1			N/A
BRANCH1	Fa0/0			N/A
	S0/0/0			N/A
	S0/0/1			N/A
BRANCH2	Fa0/0			N/A
	S0/0/0			N/A
	S0/0/1			N/A
PC1	NIC			
PC2	NIC			
PC3	NIC			

Learning Objectives

Upon completion of this lab, you will be able to:

- Create an efficient VLSM design given requirements.
- Assign appropriate addresses to interfaces and document.
- Cable a network according to the Topology Diagram.
- Erase the startup configuration and reload a router to the default state.
- Configure routers including EIGRP.
- Configure and propagate a static default route.
- Verify EIGRP operation.
- Test and verify full connectivity.
- Reflect upon and document the network implementation.

Scenario

In this lab activity, you will be given a network address that must be subnetted using VLSM to complete the addressing of the network shown in the Topology Diagram. A combination of EIGRP routing and static routing will be required so that hosts on networks that are not directly connected will be able to communicate with each other. EIGRP must be configured so that all IP traffic takes the shortest path to the destination address.

Task 1: Subnet the Address Space.

Step 1: Examine the network requirements.

The addressing for the network has the following requirements:

- The 172.16.0.0/16 network must be subnetted to provide addresses for the three LANs.
 - The HQ LAN will require 500 addresses.
 - The BRANCH1 LAN will require 200 addresses.
 - The Branch 2 LAN will require 100 addresses.
- The loopback address representing the link between the HQ router and the ISP will use the 209.165.200.224/30 network.
- The 192.168.1.16/28 address space must be subnetted to obtain the addresses for the links between the three routers.

Step 2: Consider the following questions when creating your network design:

How many subnets need to be created from the 172.16.0.0/16 network? _____

How many total IP addresses are required from the 172.16.0.0/16 network? _____

What subnet mask will be used for the HQ LAN subnet? _____

What is the maximum number of host addresses that could be used on this subnet? _____

What subnet mask will be used for the BRANCH1 LAN subnet?

What is the maximum number of host addresses that could be used on this subnet? _____

What subnet mask will be used for the BRANCH2 LAN subnet?

What is the maximum number of host addresses that could be used on this subnet? _____

What subnet mask will be used for the links between the three routers? _____

What is the maximum number of host addresses that could be used on each of these subnets? _____

Step 3: Assign subnetwork addresses to the Topology Diagram.

1. Assign subnet 0 of the 172.16.0.0/16 network to the HQ LAN subnet.
What is the network address of this subnet? _____
2. Assign subnet 1 of the 172.16.0.0/16 network to the BRANCH1 LAN subnet.
What is the network address of this subnet? _____
3. Assign subnet 2 of the 172.16.0.0/16 network to the BRANCH2 LAN subnet.
What is the network address of this subnet? _____
4. Assign subnet 0 of the 192.168.1.16/28 network to the link between the HQ and BRANCH1 routers.
What is the network address of this subnet? _____
5. Assign subnet 1 of the 192.168.1.16/28 network to the link between the HQ and BRANCH2 routers.
What is the network address of this subnet? _____
6. Assign subnet 2 of the 192.168.1.16/28 network to the link between the BRANCH1 and BRANCH2 routers. What is the network address of this subnet?

Task 2: Determine Interface Addresses.

Step 1: Assign appropriate addresses to the device interfaces.

1. Assign the first valid host address of the 209.165.200.224/30 network to the Loopback interface on the HQ router.
2. Assign the first valid IP address of the HQ LAN network to the LAN interface of the HQ router.
3. Assign the last valid IP address of the HQ LAN network to PC2.
4. Assign the first valid IP address of the BRANCH1 LAN network to the LAN interface of the BRANCH1 router.
5. Assign the last valid IP address of the BRANCH1 LAN network to PC1.
6. Assign the first valid IP address of the BRANCH2 LAN network to the LAN interface of the BRANCH2 router.
7. Assign the last valid IP address of the BRANCH2 LAN network to PC3.
8. Assign the first valid IP address of the HQ to BRANCH1 link network to the Serial 0/0/0 interface of the HQ router.
9. Assign the last valid IP address of the HQ to BRANCH1 link network to the Serial 0/0/0 interface of the Branch router.
10. Assign the first valid IP address of the HQ to BRANCH2 link network to the Serial 0/0/1 interface of the HQ router.

11. Assign the last valid IP address of the HQ to BRANCH2 link network to the Serial0/0/1 interface of the Branch router.
12. Assign the first valid IP address of the BRANCH1 to BRANCH2 link network to the Serial 0/0/1 interface of the BRANCH1 router.
13. Assign the last valid IP address of the BRANCH1 to BRANCH2 link network to the Serial0/0/0 interface of the BRANCH2 router.

Step 2: Document the addresses to be used in the table provided under the Topology Diagram.

Task 3: Prepare the Network.

Step 1 Cable a network that is similar to the one in the Topology Diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

Step 2 Clear any existing configurations on the routers.

Task 4: Perform Basic Router Configurations.

Perform basic configuration of the BRANCH1, BRANCH2, HQ, and ISP routers according to the following guidelines:

1. Configure the router hostname.
2. Disable DNS lookup.
3. Configure an EXEC mode password.
4. Configure a message-of-the-day banner.
5. Configure a password for console connections.
6. Configure a password for VTY connections.
7. Synchronize unsolicited messages and debug output with solicited output and prompts for the console and virtual terminal lines.
8. Configure an EXEC timeout of 15 minutes.

Task 5: Configure and Activate Serial and Ethernet Addresses.

Step 1: Configure the interfaces on the HQ, BRANCH1, and BRANCH2 routers.

Configure the interfaces on the HQ, BRANCH1, and BRANCH2 routers with the IP addresses from the table provided under the Topology Diagram.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 2: Configure the Ethernet interfaces.

Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses from the Addressing Table provided under the Topology Diagram.

Task 6: Verify Connectivity to Next-Hop Device.

You should *not* have connectivity between end devices yet. However, you can test connectivity between two routers and between an end device and its default gateway.

Step 1: Verify connectivity of routers.

Verify that the HQ, BRANCH1, and BRANCH2 routers can ping each of the neighboring routers across the WAN links.

Step 2: Verify connectivity of PCs.

Verify that PC1, PC2, and PC3 can ping their respective default gateways.

Task 7: Configure EIGRP Routing on the BRANCH1 Router.

Consider the networks that need to be included in the EIGRP updates that are sent out by the BRANCH1 router.

What directly connected networks are present in the BRANCH1 routing table?

Will these networks need to have the subnet mask information included in the network statements?

What commands are required to enable EIGRP and include the connected networks in the routing updates?

What command is required to enable EIGRP to include the VLSM information instead of summarizing routes at the classful boundary?

Are there any router interfaces that do not need to have EIGRP updates sent out? _____

What command is used to disable EIGRP updates on these interfaces?

Task 8: Configure EIGRP and Static Routing on the HQ Router.

Consider the type of static routing that is needed on HQ.

A static default route will need to be configured to send all packets with destination addresses that are not in the routing table to the loopback address representing the link between the HQ router and the ISP. What command is needed to accomplish this?

What directly connected networks are present in the HQ routing table?

Will the networks of the HQ LAN and the links between the BRANCH1 and BRANCH2 routers need to have the subnet mask information included in the network statements? _____

What commands are required to enable EIGRP and include the appropriate networks in the routing updates?

What command is required to enable EIGRP to include the VLSM information instead of summarizing routes at the classful boundary?

Are there any router interfaces that do not need to have EIGRP updates sent out? _____

What command is used to disable EIGRP updates on this interface?

The HQ router needs to send the default route information to the BRANCH1 and BRANCH2 routers in the EIGRP updates. What command is used to configure this?

Task 9: Configure EIGRP Routing on the BRANCH2 Router.

Consider the networks that need to be included in the EIGRP updates that are sent out by the BRANCH2 router.

What directly connected networks are present in the BRANCH2 routing table?

Will these networks need to have the subnet mask information included in the network statements?

What commands are required to enable EIGRP and include the connected networks in the routing updates?

What command is required to enable EIGRP to include the VLSM information instead of summarizing routes at the classful boundary?

Are there any router interfaces that do not need to have EIGRP updates sent out? _____

What command is used to disable EIGRP updates on these interfaces?

Task 10: Verify the Configurations.

Answer the following questions to verify that the network is operating as expected:

From PC1, is it possible to ping PC2? _____

From PC1, is it possible to ping the PC3? _____

The answer to the above questions should be **yes**. If any of the above pings failed, check your physical connections and configurations. Refer to your basic troubleshooting techniques used in the Chapter 1 labs.

What EIGRP routes are present in the routing table of the BRANCH1 router?

What is the gateway of last resort in the routing table of the BRANCH1 router?

What EIGRP routes are present in the routing table of the HQ router?

What is the gateway of last resort in the routing table of the HQ router?

What EIGRP routes are present in the routing table of the BRANCH2 router?

What is the gateway of last resort in the routing table of the BRANCH2 router?

Task 11: Reflection

Why is it necessary to use disable automatic summarization with this network design?

If the routes in the routing table are summarized at the classful network boundary 17.16.0.0, the paths between the three routers will all have an equal cost and packets may not be sent using the route with the least hops.

Task 12: Document the Router Configurations.

On each router, capture the following command output to a text (.txt) file and save for future reference.

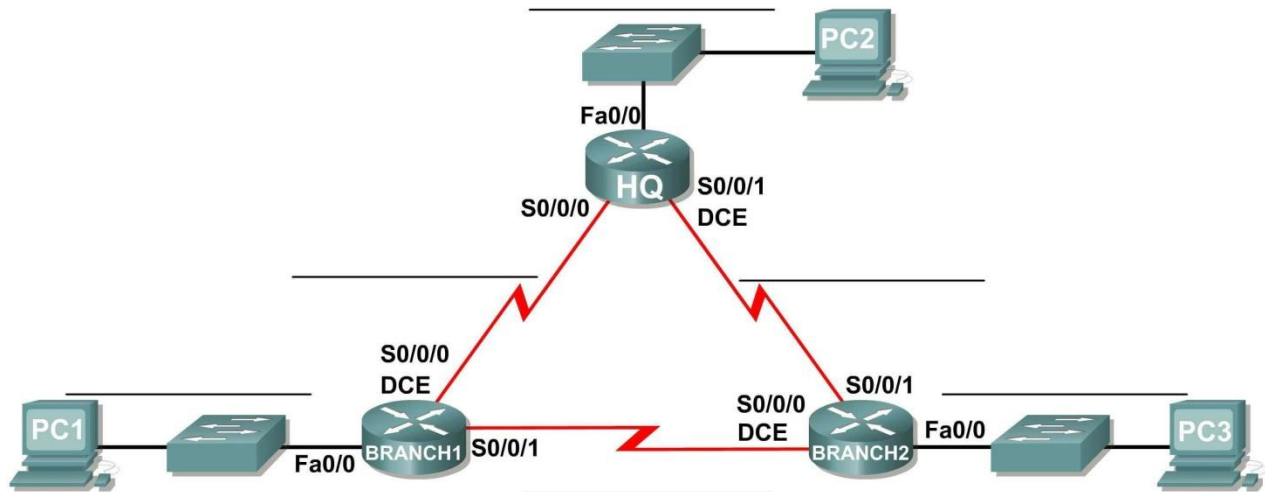
- **Running configuration**
- **Routing table**
- **Interface summarization**

Task 13: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

22 - EIGRP Troubleshooting Lab

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	Fa0/0	172.18.64.1	255.255.192.0	N/A
	S0/0/0	209.165.202.129	255.255.255.252	N/A
	S0/0/1	209.165.202.133	255.255.255.252	N/A
BRANCH1	Fa0/0	172.18.129.1	255.255.255.240	N/A
	S0/0/0	209.165.202.130	255.255.255.252	N/A
	S0/0/1	209.165.202.137	255.255.255.252	N/A
BRANCH2	Fa0/0	172.18.128.1	255.255.255.0	N/A
	S0/0/0	209.165.202.138	255.255.255.252	N/A
	S0/0/1	209.165.202.134	255.255.255.252	N/A
PC1	NIC	172.18.129.14	255.255.255.240	172.18.129.1
PC2	NIC	172.18.100.100	255.255.192.0	172.18.64.1
PC3	NIC	172.18.128.10	255.255.255.0	172.18.128.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the Topology Diagram.
- Erase the startup configuration and reload a router to the default state.
- Load the routers with supplied scripts.
- Discover where communication is not possible.
- Gather information about the misconfigured portion of the network along with any other errors.
- Analyze information to determine why communication is not possible.
- Propose solutions to network errors.
- Implement solutions to network errors.
- Document the corrected network.

Scenario

In this lab, you will begin by loading configuration scripts on each of the routers. These scripts contain errors that will prevent end-to-end communication across the network. You will need to troubleshoot each router to determine the configuration errors, and then use the appropriate commands to correct the configurations. When you have corrected all of the configuration errors, all of the hosts on the network should be able to communicate with each other.

The network should also have the following requirements met:

- EIGRP routing is configured on the BRANCH1 router.
- EIGRP routing is configured on the BRANCH2 router.
- EIGRP routing is configured on the HQ router.
- EIGRP updates must be disabled on the BRANCH1, BRANCH2, and HQ LAN interfaces.
- All EIGRP routers must use a process ID of 1.

Task 1: Cable, Erase, and Reload the Routers.

Step 1: Cable a network.

Cable a network that is similar to the one in the Topology Diagram.

Step 2: Clear the configuration on each router.

Clear the configuration on each of the routers using the `erase startup-config` command and then `reload` the routers. Answer **no** if asked to save changes.

Task 2: Load Routers with the Supplied Scripts.

Step 1: Load the following script onto the BRANCH1 router:

```
hostname BRANCH1
!  
no ip domain-lookup
```

```

!
interface FastEthernet0/0
 ip address 172.18.129.1 255.255.255.240
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 209.165.202.130 255.255.255.252
 clock rate 64000 no
 shutdown
!
interface Serial0/0/1
 ip address 209.165.202.137 255.255.255.252
 no shutdown
!
router eigrp 2
 passive-interface FastEthernet0/0
 network 209.165.202.128 0.0.0.3 network
 209.165.202.136 0.0.0.3 network
 172.18.129.0 0.0.0.7
 no auto-summary
!
ip classless
!
line con 0 line
 vty 0 4
 login
!
end

```

Step 2: Load the following script onto the BRANCH2 router:

```

hostname BRANCH2
!
no ip domain-lookup
!
interface FastEthernet0/0
 ip address 172.18.128.1 255.255.255.0
 duplex auto
 speed auto no
 shutdown
!
interface Serial0/0/0
 ip address 209.165.202.138 255.255.255.252
 clock rate 64000
 no shutdown

```

```

!
interface Serial0/0/1
 ip address 209.165.202.134 255.255.255.252 no
 shutdown
!
router eigrp 1
 passive-interface FastEthernet0/0
 network 172.18.128.0 0.0.0.255
 network 209.165.202.132 0.0.0.3
 network 209.165.202.136 0.0.0.3
!
ip classless
!
line con 0 line
 vty 0 4
  login
!
end

```

Step 3: Load the following script onto the HQ router:

```

hostname HQ
!
no ip domain-lookup
!
interface FastEthernet0/0
 ip address 172.18.64.1 255.255.192.0
 duplex auto
 speed auto no
 shutdown
!
interface Serial0/0/0
 ip address 209.165.202.129 255.255.255.252 no
 shutdown
!
interface Serial0/0/1
 ip address 209.165.202.133 255.255.255.252
 clock rate 64000 no
 shutdown
!
router eigrp 1
 passive-interface Serial0/0/0
 network 172.18.64.0
 network 209.165.202.128 0.0.0.3
 network 209.165.202.132 0.0.0.3 no
 auto-summary

```

```
!  
ip classless  
!  
line con 0 line  
vty 0 4  
  login  
!  
end
```

Task 3: Troubleshoot the BRANCH1 Router.

Step 1: Begin troubleshooting at the Host connected to the BRANCH1 router.

From the host PC1, is it possible to ping PC2? _____ From

the host PC1, is it possible to ping PC3? _____

From the host PC1, is it possible to ping the default gateway? _____

Step 2: Examine the BRANCH1 router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the configuration of the interfaces?

If there are any problems with the configuration of the interfaces, record any commands that will be necessary to correct the configuration errors.

Step 3: If you have recorded any commands above, apply them to the router configuration now.

Step 4: View summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors on the BRANCH1 router? _____

If the answer is **yes**, troubleshoot the interface status of the interfaces again.

Step 5: Troubleshoot the routing configuration on the BRANCH1 router.

What routes are shown in the routing table?

Are there any problems with the routing table or the EIGRP configuration?

If there are any problems with the EIGRP configuration, record any commands that will be necessary to correct the configuration errors.

Are there any connectivity problems that could be due to errors on other parts of the network?

What connected networks are shown in the EIGRP topology table of the BRANCH1 router?

Are there any problems with the connected networks in the EIGRP topology table?

Step 6: If you have recorded any commands above, apply them to the router configuration now.

Step 7: View the routing information.

If any changes were made to the configuration in the previous steps, view the routing information again. Does the information in routing table indicate any configuration errors on the BRANCH1 router? _____

Does the information in the EIGRP topology table indicate any configuration errors on the BRANCH1 router? _____

If the answer to either of these questions is **yes**, troubleshoot the routing configuration again.

What routes are shown in the routing table?

Step 8: Attempt to ping between the hosts again. From

the host PC1, is it possible to ping PC2? _____

From the host PC1, is it possible to ping PC3? _____

From the host PC1, is it possible to ping the Serial 0/0/0 interface of the HQ router? _____

From the host PC1, is it possible to ping the Serial 0/0/1 interface of the HQ router? _____

Task 4: Troubleshoot the HQ Router

Step 1: Begin troubleshooting at the host PC2.

From the host PC2, is it possible to ping PC1? _____

From the host PC2, is it possible to ping PC3? _____

From the host PC2, is it possible to ping the default gateway? _____

Step 2: Examine the HQ router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router. Are there any problems with the configuration of the interfaces?

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the configuration of the interfaces?

If there are any problems with the configuration of the interfaces, record any commands that will be necessary to correct the configuration errors.

Step 3: If you have recorded any commands above, apply them to the router configuration now.

Step 4: View summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors on the HQ router?

If the answer is **yes**, troubleshoot the interface status of the interfaces again.

Step 5: Troubleshoot the routing configuration on the HQ router.

What routes are shown in the routing table?

Are there any problems with the routing table or the EIGRP configuration?

If there are any problems with the EIGRP configuration, record any commands that will be necessary to correct the configuration errors.

Are there any connectivity problems that could be due to errors on other parts of the network?

What connected networks are shown in the EIGRP topology table of the HQ router?

Are there any problems with the connected networks in the EIGRP topology table?

Step 6: If you have recorded any commands above, apply them to the router configuration now.

Step 7: View the routing information.

If any changes were made to the configuration in the previous steps, view the routing information again. Does the information in routing table indicate any configuration errors on the HQ router? _____

Does the information in the EIGRP topology table indicate any configuration errors on the HQ router?

If the answer to either of these questions is **yes**, troubleshoot the routing configuration again.

Step 8: Attempt to ping between the hosts again. From

the host PC2, is it possible to ping PC1? _____ From

the host PC2, is it possible to ping PC3? _____

From the host PC2, is it possible to ping the Serial 0/0/0 interface of the BRANCH2 router? _____

From the host PC2, is it possible to ping the Serial 0/0/1 interface of the BRANCH2 router? _____

Task 5: Troubleshoot the BRANCH2 Router

Step 1: Begin troubleshooting at the Host PC3.

From the host PC3, is it possible to ping PC1? _____

From the host PC3, is it possible to ping PC2? _____

From the host PC3, is it possible to ping the default gateway? _____

Step 2: Examine the BRANCH2 router to find possible configuration errors.

Are there any problems with the configuration of the interfaces?

If there are any problems with the configuration of the interfaces, record any commands that will be necessary to correct the configuration errors.

Step 3: If you have recorded any commands above, apply them to the router configuration now.

Step 4: View summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors on the BRANCH2 router? _____

If the answer is **yes**, troubleshoot the interface status of the interfaces again.

Step 5: Troubleshoot the routing configuration on the BRANCH2 router.

What routes are shown in the routing table?

Are there any problems with the routing table or the EIGRP configuration?

If there are any problems with the EIGRP configuration, record any commands that will be necessary to correct the configuration errors.

Are there any connectivity problems that could be due to errors on other parts of the network?

What connected networks are shown in the EIGRP topology table of the BRANCH2 router?

Are there any problems with the connected networks in the EIGRP topology table?

Step 6: If you have recorded any commands above, apply them to the router configuration now.

Step 7: View the routing information.

If any changes were made to the configuration in the previous steps, view the routing information again. Does the information in routing table indicate any configuration errors on the BRANCH2 router? _____

Does the information in the EIGRP topology table indicate any configuration errors on the BRANCH2 router? _____

If the answer to either of these questions is **yes**, troubleshoot the routing configuration again.

What routes are shown in the routing table?

Step 8: Attempt to ping between the hosts again. From

the host PC3, is it possible to ping PC1? _____

From the host PC3, is it possible to ping PC2? _____

From the host PC3, is it possible to ping the Serial 0/0/0 interface of the BRANCH1 router? _____

From the host PC3, is it possible to ping the Serial 0/0/1 interface of the BRANCH1 router? _____

Task 6: Reflection

There were a number of configuration errors in the scripts that were provided for this lab. Use the space below to write a brief description of the errors that you found.

Task 7: Documentation

On each router, capture the following command output to a text (.txt) file and save for future reference.

- `show running-config`
- `show ip route`
- `show ip interface brief`
- `show ip protocols`

If you need to review the procedures for capturing command output, refer to Lab 1.5.1

Task 8: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.