



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Switching, Routing and Wireless ACCA6022 Lab Manual

2026-27

BSc (Hons) Computing (Computer Networks and Cyber
Security)
Applied Computing
Wales Institute of Science and Art
University of Wales Trinity Saint David
Swansea

Module Leader
Dr Kapilan Radhakrishnan



Table of content	Page no
Lab 1: Configuring Basic Router Settings with IOS CLI	1
Lab 2: Configuring IPv4 Static and Default Routes	10
Lab 3: Configuring IPv6 Static and Default Routes	16
Lab 4: Troubleshooting IPv4 and IPv6 Static Routes	23
Lab 5: Configuring Basic EIGRP for IPv4	32
Lab 6: Configuring Advanced EIGRP for IPv4 Features	41
Lab 7: Configuring Basic EIGRP for IPv6	51
Lab 8: Troubleshooting Basic EIGRP for IPv4 and IPv6	59
Lab 9: Troubleshooting Advanced EIGRP	70
Lab 10: Configuring Basic Single-Area OSPFv2	78
Lab 11: Configuring OSPFv2 on a Multiaccess Network	99
Lab 12: Configuring OSPFv2 Advanced Features	103
Lab 13: Configuring Basic Single-Area OSPFv3	114
Lab 14: Troubleshooting Basic Single-Area OSPFv2 and OSPFv3	124
Lab 15: Configuring Basic Switch Settings	136
Lab 16: Configuring Switch Security Features Topology	147
Lab 17: Basic VLAN Configuration	156
Lab 18: Configuring VLANs and Trunking	162
Lab 19: Challenge VLAN Configuration	173
Lab 20: Troubleshooting VLAN Configurations	176
Lab 21: Configure Extended VLANs, VTP, and DTP	180
Lab 22: Configuring Per-Interface Inter-VLAN Routing	187
Lab 23: Configuring 802.1Q Trunk-Based Inter-VLAN Routing	192
Lab 24: Building a Switched Network with Redundant Links	198
Lab 25: Configuring Rapid PVST+, PortFast, and BPDU Guard	206
Lab 26: Configuring Basic DHCPv4 on a Router	215
Lab 27: Troubleshooting DHCPv4	221
Lab 28: Configuring EtherChannel	228
Lab 29: Troubleshooting EtherChannel	235
Lab 30: Configuring HSRP	242
Appendix: Configure and Verify Password Recovery	249

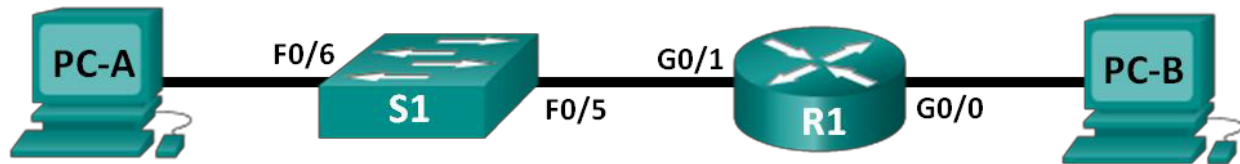
Acknowledgement

The content, learning resources, practical activities, and instructional materials used in this module are sourced wholly or in part from Cisco Networking Academy (Cisco Academy) curriculum materials. We gratefully acknowledge Cisco Networking Academy for the development and provision of these educational resources.



Lab 1: 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
```

- 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.

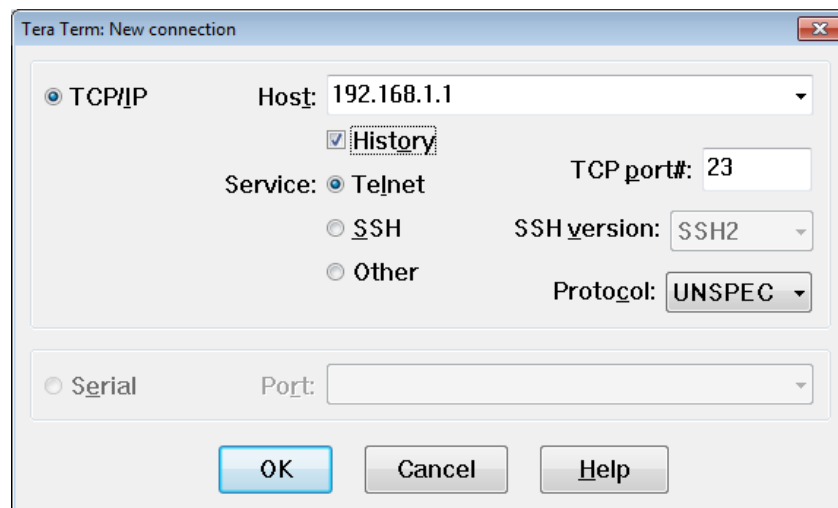
Note: It may be necessary to disable the PCs firewall.

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?

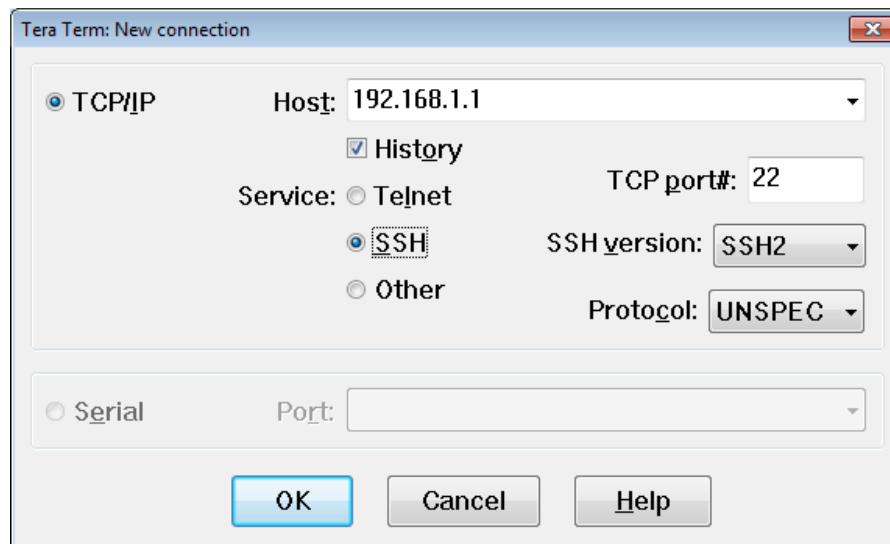
Step 4: Configure the router for SSH access.

- 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

- 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?

- 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?

- 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 1: 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
```

- 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
```

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

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

Step 2: Initialize and reload the switch.

- Console into the switch and enter privileged EXEC mode.

```
Switch> enable
Switch#
```

- 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
```

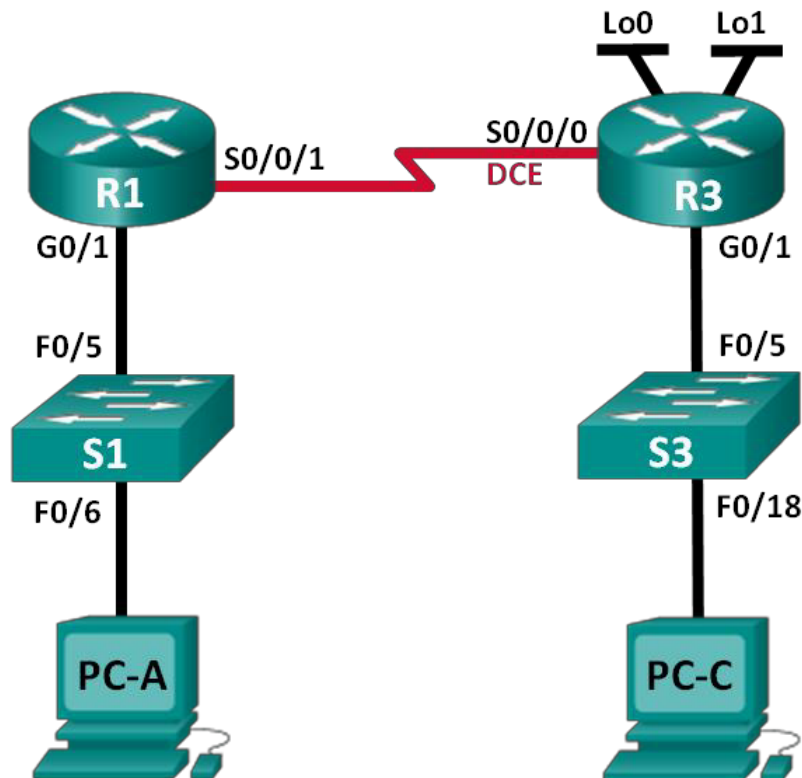
- h. After the switch reloads, you should be prompted to enter the initial configuration dialog. Type **no** and press Enter.

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

```
Switch>
```

Lab 2: 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?
 - 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
```

- 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.

- 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
```

- 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. _____

- 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? _____

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.

- 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?

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.

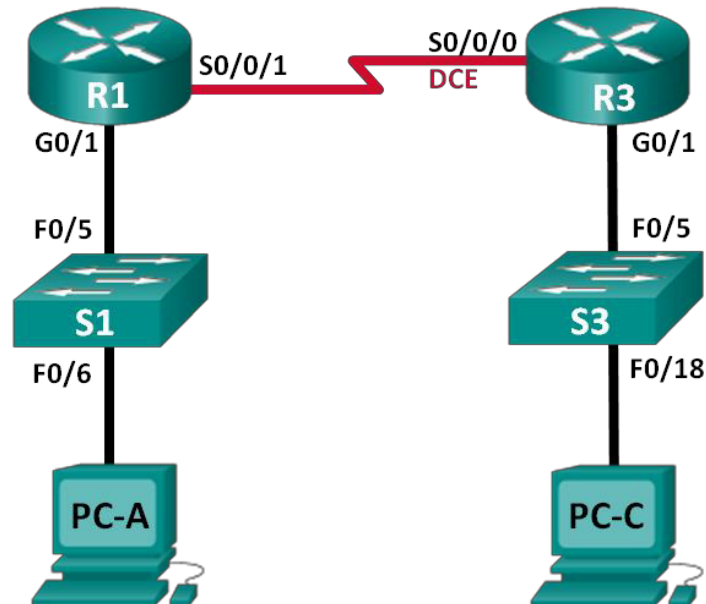
```
R1(config)# no ip route 209.165.200.224 255.255.255.224 serial0/0/1
Or R1(config)# no ip route 209.165.200.224 255.255.255.224 10.1.1.2
Or R1(config)# no ip route 209.165.200.224 255.255.255.224
```

Default Route Configuration

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

Lab 3: 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.
- 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>
```

- a. 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)#
```

- b. 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?

- c. 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.

- d. 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)#
```

- e. 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>
```

- a. 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.

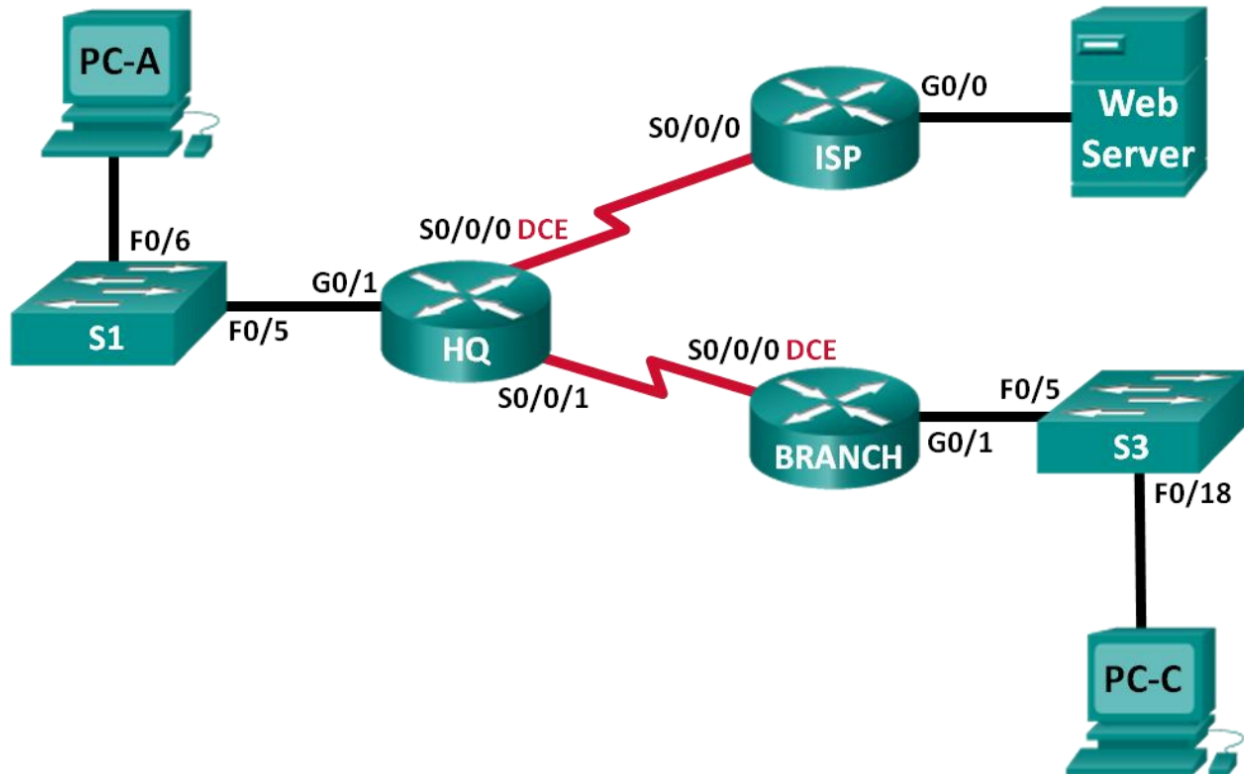
Reflection

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?

Lab 4: Troubleshooting 1Pv4 and 1Pv6 Static Routes

Topology



Addressing Table

Device	Interface	IP Address	Default Gateway
HQ	G0/1	192.168.0.1/25	N/A
		2001:DB8:ACAD::1/64	
		FE80::1 link-local	
	S0/0/0 (DCE)	10.1.1.2/30	N/A
		2001:DB8:ACAD::20:2/64	
	S0/0/1	192.168.0.253/30	N/A
		2001:DB8:ACAD:2::1/30	
ISP	G0/0	172.16.3.1/24	N/A
		2001:DB8:ACAD:30::1/64	
		FE80::1 link-local	
	S0/0/0	10.1.1.1/30	N/A
		2001:DB8:ACAD:20::/64	

BRANCH	G0/1	192.168.1.1/24 2001:DB8:ACAD:1::1/64 FE80::1 link-local	N/A
	S0/0/0 (DCE)	192.168.0.254/30 2001:DB8:ACAD:2::2/64	N/A
S1	VLAN 1	N/A	N/A
S3	VLAN 1	N/A	N/A
PC-A	NIC	192.168.0.3/25 2001:DB8:ACAD::3/64	192.168.0.1 FE80::1
Web Server	NIC	172.16.3.3/24 2001:DB8:ACAD:30::3/64	172.16.3.1 FE80::1
PC-C	NIC	192.168.1.3/24 2001:DB8:ACAD:1::3/64	192.168.1.1 FE80::1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Troubleshoot Static Routes in an IPv4 Network

Part 3: Troubleshoot Static Routes in an IPv6 Network

Background / Scenario

As a network administrator, you must be able to configure routing of traffic using static routes. Understanding how to configure and troubleshoot static routing is a requirement. Static routes are commonly used for stub networks and default routes. Your company's ISP has hired you to troubleshoot connectivity issues on the network. You will have access to the HQ, BRANCH, and the ISP routers.

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, the hosts on the network should be able to communicate with each other.

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

- 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 the routers and switches with some basic settings, such as passwords and IP addresses. Preset configurations are also provided for you for the initial router configurations. You will also configure the IP settings for the PCs in the topology.

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

Attach the devices as shown in the topology diagram and cable, as necessary.

Step 2: Initialize and reload the routers and switches.

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 mode password.
- Assign **cisco** as the console and vty passwords.
- Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 4: Configure hosts and Web Server.

- Configure IP addresses for IPv4 and IPv6.
- Configure IPv4 default gateway.

Step 5: Load router configurations.

Router HQ

```
hostname HQ
ipv6 unicast-routing
interface GigabitEthernet0/1
  ipv6 address 2001:DB8:ACAD::1/64
  ip address 192.168.0.1 255.255.255.128
  ipv6 address FE80::1 link-local
interface Serial0/0/0
  ipv6 address 2001:DB8:ACAD:20::2/64
  ip address 10.1.1.2 255.255.255.252
  clock rate 800000
  no shutdown
interface Serial0/0/1
  ipv6 address 2001:DB8:ACAD:2::3/64
  ip address 192.168.0.253 255.255.255.252
  no shutdown
ip route 172.16.3.0 255.255.255.0 10.1.1.1
ip route 192.168.1.0 255.255.255.0 192.16.0.254 ipv6
route 2001:DB8:ACAD:1::/64 2001:DB8:ACAD:2::2 ipv6
route 2001:DB8:ACAD:30::/64 2001:DB8:ACAD::20:1
```

Router ISP

```
hostname ISP
```

```

ipv6 unicast-routing
interface GigabitEthernet0/0
  ipv6 address 2001:DB8:ACAD:30::1/64
  ip address 172.16.3.11 255.255.255.0
  ipv6 address FE80::1 link-local
  no shutdown
interface Serial0/0/0
  ipv6 address 2001:DB8::ACAD:20:1/64
  ip address 10.1.1.1 255.255.255.252
  no shutdown
ip route 192.168.1.0 255.255.255.0 10.1.1.2
ipv6 route 2001:DB8:ACAD::/62 2001:DB8:ACAD:20::2

```

Router BRANCH

```

hostname BRANCH
ipv6 unicast-routing
interface GigabitEthernet0/1
  ipv6 address 2001:DB8:ACAD:1::1/64
  ip address 192.168.1.1 255.255.255.0
  ipv6 address FE80::1 link-local
  no shutdown
interface Serial0/0/0
  ipv6 address 2001:DB8:ACAD:2::2/64
  clock rate 128000
  ip address 192.168.0.249 255.255.255.252
  clock rate 128000
  no shutdown
ip route 0.0.0.0 0.0.0.0 10.1.1.2
ipv6 route ::/0 2001:DB8:ACAD::1

```

Part 2: Troubleshoot Static Routes in an IPv4 Network

IPv4 Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	G0/1	192.168.0.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A
	S0/0/1	192.168.0.253	255.255.255.252	N/A
ISP	G0/0	172.16.3.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
BRANCH	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.0.254	255.255.255.252	N/A
S1	VLAN 1	192.168.0.11	255.255.255.128	192.168.0.1
S3	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1

PC-A	NIC	192.168.0.3	255.255.255.128	192.168.0.1
Web Server	NIC	172.16.3.3	255.255.255.0	172.16.3.1
PC-C	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Step 1: Troubleshoot the HQ router.

The HQ router is the link between the ISP router and the BRANCH router. The ISP router represents the outside network while the BRANCH router represents the corporate network. The HQ router is configured with static routes to ISP and BRANCH networks.

- a. Display the status of the interfaces on HQ. Enter **show ip interface brief**. Record and resolve any issues as necessary.

- b. Ping from HQ router to BRANCH router (192.168.0.254). Were the pings successful? _____

- c. Ping from HQ router to ISP router (10.1.1.1). Were the pings successful? _____

- d. Ping from PC-A to the default gateway. Were the pings successful? _____

- e. Ping from PC-A to PC-C. Were the pings successful? _____

- f. Ping from PC-A to Web Server. Were the pings successful? _____

- g. Display the routing table on HQ. What non-directly connected routes are shown in the routing table?

- h. Based on the results of the pings, routing table output, and static routes in the running configuration, what can you conclude about network connectivity?

- i. What commands (if any) need to be entered to resolve routing issues? Record the command(s).

- j. Repeat any of the steps from b to f to verify whether the problems have been resolved. Record your observations and possible next steps in troubleshooting connectivity.

Step 2: Troubleshoot the ISP router.

For the ISP router, there should be a route to HQ and BRANCH routers. One static route is configured on ISP router to reach the 192.168.1.0/24, 192.168.0.0/25, and 192.168.0.252/30 networks.

- a. Display the status of interfaces on ISP. Enter **show ip interface brief**. Record and resolve any issues as necessary.

- b. Ping from the ISP router to the HQ router (10.1.1.2). Were the pings successful? _____

- c. Ping from Web Server to the default gateway. Were the pings successful? _____
- d. Ping from Web Server to PC-A. Were the pings successful? _____
- e. Ping from Web Server to PC-C. Were the pings successful? _____
- f. Display the routing table on ISP. What non-directly connected routes are shown in the routing table?

- g. Based on the results of the pings, routing table output, and static routes in the running configuration, what can you conclude about network connectivity?

- h. What commands (if any) need to be entered to resolve routing issues? Record the command(s).
(Hint: ISP only requires one summarized route to the company's networks 192.168.1.0/24, 192.168.0.0/25, and 192.168.0.252/32.)
- i. Repeat any of the steps from b to e to verify whether the problems have been resolved. Record your observations and possible next steps in troubleshooting connectivity.

Step 3: Troubleshoot the BRANCH router.

For the BRANCH router, a default route is set to reach the rest of the network and ISP.

- a. Display the status of the interfaces on BRANCH. Enter **show ip interface brief**. Record and resolve any issues, as necessary.

- b. Ping from the BRANCH router to the HQ router (192.168.0.253). Were the pings successful? _____
- c. Ping from PC-C to the default gateway. Were the pings successful? _____
- d. Ping from PC-C to PC-A. Were the pings successful? _____
- e. Ping from PC-C to Web Server. Were the pings successful? _____
- f. Display the routing table on BRANCH. What non-directly connected routes are shown in the routing table?

- g. Based on the results of the pings, routing table output, and static routes in the running configuration, what can you conclude about network connectivity?

- h. What commands (if any) need to be entered to resolve routing issues? Record the command(s).

- i. Repeat any of the steps from b to e to verify whether the problems have been resolved. Record your observations and possible next steps in troubleshooting connectivity.

Part 3: Troubleshoot Static Routes in an IPv6 Network

Device	Interface	IPv6 Address	Prefix Length	Default Gateway
HQ	G0/1	2001:DB8:ACAD::1	64	N/A
	S0/0/0 (DCE)	2001:DB8:ACAD::20:2	64	N/A
	S0/0/1	2001:DB8:ACAD:2::1	64	N/A
ISP	G0/0	2001:DB8:ACAD:30::1	64	N/A
	S0/0/0	2001:DB8:ACAD:20::1	64	N/A
BRANCH	G0/1	2001:DB8:ACAD:1::1	64	N/A
	S0/0/0 (DCE)	2001:DB8:ACAD:2::2	64	N/A
PC-A	NIC	2001:DB8:ACAD::3	64	FE80::1
Web Server	NIC	2001:DB8:ACAD:30::3	64	FE80::1
PC-C	NIC	2001:DB8:ACAD:1::3	64	FE80::1

Step 1: Troubleshoot the HQ router.

The HQ router is the link between the ISP router and the BRANCH router. The ISP router represents the outside network while the BRANCH router represents the corporate network. The HQ router is configured with static routes to both the ISP and the BRANCH networks.

- a. Display the status of the interfaces on HQ. Enter **show ipv6 interface brief**. Record and resolve any issues, as necessary.

- b. Ping from the HQ router to the BRANCH router (2001:DB8:ACAD:2::2). Were the pings successful? ____ c.
 Ping from the HQ router to the ISP router (2001:DB8:ACAD:20::1). Were the pings successful? ____ d.
 Ping from PC-A to the default gateway. Were the pings successful? _____

- e. Ping from PC-A to Web Server. Were the pings successful? _____

- f. Ping from PC-A to PC-C. Were the pings successful? _____

- g. Display the routing table by issuing a **show ipv6 route** command. What non-directly connected routes are shown in the routing table?

- h. Based on the results of the pings, routing table output, and static routes in the running configuration, what can you conclude about network connectivity?

- i. What commands (if any) need to be entered to resolve routing issues? Record the command(s).

- j. Repeat any of the steps from b to f to verify whether the problems have been resolved. Record your observations and possible next steps in troubleshooting connectivity.

Step 2: Troubleshoot the ISP router.

On the ISP router, one static route is configured to reach all the networks on HQ and BRANCH routers.

- a. Display the status of the interfaces on ISP. Enter **show ipv6 interface brief**. Record and resolve any issues, as necessary.

- b. Ping from the ISP router to the HQ router (2001:DB8:ACAD:20::2). Were the pings successful? _____
- c. Ping from Web Server to the default gateway. Were the pings successful? _____
- d. Ping from Web Server to PC-A. Were the pings successful? _____
- e. Ping from Web Server to PC-C. Were the pings successful? _____
- f. Display the routing table. What non-directly connected routes are shown in the routing table?

- g. Based on the results of the pings, routing table output, and static routes in the running configuration, what can you conclude about network connectivity?

- h. What commands (if any) need to be entered to resolve routing issues? Record the command(s).

- i. Repeat any of the steps from b to e to verify whether the problems have been resolved. Record your observations and possible next steps in troubleshooting connectivity.

Step 3: Troubleshoot the BRANCH router.

For the BRANCH routers, there is a default route to the HQ router. This default route allows the BRANCH network to the ISP router and Web Server.

- a. Display the status of the interfaces on BRANCH. Enter **show ipv6 interface brief**. Record and resolve any issues, as necessary.

- b. Ping from the BRANCH router to the HQ router (2001:DB8:ACAD:2::1). Were the pings successful? _____
- c. Ping from the BRANCH router to the ISP router (2001:DB8:ACAD:20::1). Were the pings successful? _____
- d. Ping from PC-C to the default gateway. Were the pings successful? _____
- e. Ping from PC-C to PC-A. Were the pings successful? _____

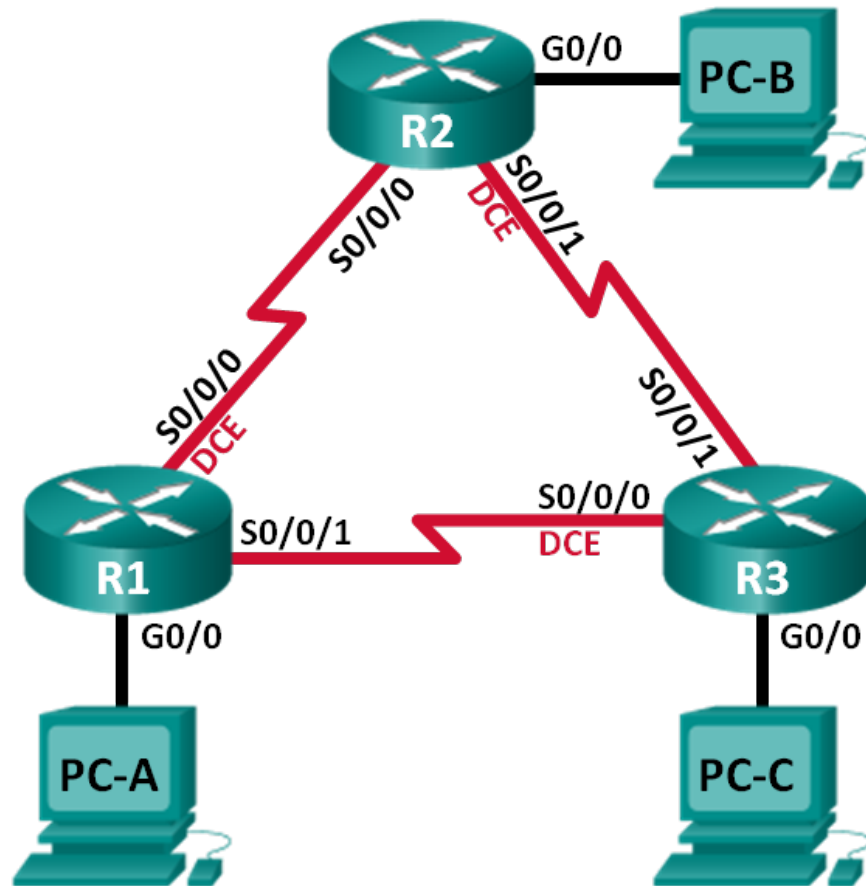
- f. Ping from PC-C to Web Server. Were the pings successful? _____
- g. Display the routing table. What non-directly connected routes are shown in the routing table?
- _____
- _____
- h. Based on the results of the pings, routing table output, and static routes in the running configuration, what can you conclude about network connectivity?
- _____
- _____
- i. What commands (if any) need to be entered to resolve routing issues? Record the command(s).
- _____
- _____
- j. Repeat any of the steps from b to f to verify whether the problems have been resolved. Record your observations and possible next steps in troubleshooting connectivity.
- _____
- _____

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)

Lab 5: Configuring Basic EIGRP for IPv4

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)	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	G0/0	192.168.2.1	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	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	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 Verify Connectivity

Part 2: Configure EIGRP Routing

Part 3: Verify EIGRP Routing

Part 4: Configure Bandwidth and Passive Interfaces

Background / Scenario

Enhanced Interior Gateway Routing Protocol (EIGRP) is a powerful distance vector routing protocol and is relatively easy to configure for basic networks.

In this lab, you will configure EIGRP for the topology and networks shown above. You will modify bandwidth and configure passive interfaces to allow EIGRP to function more efficiently.

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 Verify Connectivity

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords.

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

Task 2: Configure PC hosts.

Task 3: Initialize and reload the routers as necessary.

Task 4: Configure basic settings for each router.

Step 1: Disable DNS lookup.

Step 2: Configure IP addresses for the routers, as listed in the Addressing Table.

Step 3: Configure device name as shown in the topology.

Step 4: Assign **cisco** as the console and vty passwords.

Step 5: Assign **class** as the privileged EXEC password.

Step 6: Configure **logging synchronous** to prevent console and vty messages from interrupting command entry.

Step 7: Configure a message of the day.

Step 8: Copy the running configuration to the startup configuration.

Task 5: Verify connectivity.

The routers should be able to ping one another, and each PC should be able to ping its default gateway. The PCs will not be able to ping other PCs until EIGRP routing is configured. Verify and troubleshoot if necessary.

Part 2: Configure EIGRP Routing

Task 1: Enable EIGRP routing on R1. Use AS number 10.

```
R1(config)# router eigrp 10
```

Task 2: Advertise the directly connected networks on R1 using the wildcard mask.

```
R1(config-router)# network 10.1.1.0 0.0.0.3
```

```
R1(config-router)# network 192.168.1.0 0.0.0.255
```

```
R1(config-router)# network 10.3.3.0 0.0.0.3
```

Why is it a good practice to use wildcard masks when advertising networks? Could the mask have been omitted from any of the network statements above? If so, which one(s)?

Task 3: Enable EIGRP routing and advertise the directly connected networks on R2 and R3.

You will see neighbor adjacency messages as interfaces are added to the EIGRP routing process. The messages on R2 are displayed as an example.

```
*Apr 14 15:24:59.543: %DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 10.1.1.1 (Serial0/0/0) is up: new adjacency
```

Task 4: Verify end-to-end connectivity.

All devices should be able to ping each other if EIGRP is configured correctly.

Note: Depending on the operating system, it may be necessary to disable the firewall for the pings to the host PCs to be successful.

Part 3: Verify EIGRP Routing

Task 1: Examine the EIGRP neighbor table.

On R1, issue the **show ip eigrp neighbors** command to verify that the adjacency has been established with its neighboring routers.

```
R1# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(10)
H   Address                  Interface                Hold Uptime    SRTT   RTO  Q  Seq
                               (sec)           (ms)          Cnt  Num
1   10.3.3.2                   Se0/0/1              13 00:24:58     8   100  0   17
0   10.1.1.2                   Se0/0/0              13 00:29:23     7   100  0   23
```

Task 2: Examine the IP EIGRP routing table.

```
R1# show ip route eigrp
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

```
10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D       10.2.2.0/30 [90/2681856] via 10.3.3.2, 00:29:01, Serial0/0/1
          [90/2681856] via 10.1.1.2, 00:29:01, Serial0/0/0
D       192.168.2.0/24 [90/2172416] via 10.1.1.2, 00:29:01, Serial0/0/0
D       192.168.3.0/24 [90/2172416] via 10.3.3.2, 00:27:56, Serial0/0/1
```

Why does R1 have two paths to the 10.2.2.0/30 network?

Task 3: Examine the EIGRP topology table.

```
R1# show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(10)/ID(192.168.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.3.0/24, 1 successors, FD is 2172416
    via 10.3.3.2 (2172416/28160), Serial0/0/1
P 192.168.2.0/24, 1 successors, FD is 2172416
    via 10.1.1.2 (2172416/28160), Serial0/0/0
P 10.2.2.0/30, 2 successors, FD is 2681856
    via 10.1.1.2 (2681856/2169856), Serial0/0/0
    via 10.3.3.2 (2681856/2169856), Serial0/0/1
P 10.3.3.0/30, 1 successors, FD is 2169856
    via Connected, Serial0/0/1
P 192.168.1.0/24, 1 successors, FD is 2816
    via Connected, GigabitEthernet0/0
P 10.1.1.0/30, 1 successors, FD is 2169856
    via Connected, Serial0/0/0
```

Why are there no feasible successors listed in the R1 topology table?

Task 4: Verify the EIGRP routing parameters and networks advertised.

Issue the **show ip protocols** command to verify the EIGRP routing parameters used.

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 10"
  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-IPv4 Protocol for AS(10)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 192.168.1.1
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    10.1.1.0/30
    10.3.3.0/30
```

192.168.1.0

Routing Information Sources:

Gateway	Distance	Last Update
10.3.3.2	90	02:38:34
10.1.1.2	90	02:38:34

Distance: internal 90 external 170

Based on the output of issuing the **show ip protocols** command, answer the following questions.

What AS number is used? _____

What networks are advertised? _____

What is the administrative distance for EIGRP? _____

How many equal cost paths does EIGRP use by default? _____

Part 4: Configure Bandwidth and Passive Interfaces

EIGRP uses a default bandwidth based on the type of interface in the router. In Part 4, you will modify the bandwidth so that the link between R1 and R3 has a lower bandwidth than the link between R1/R2 and R2/R3. In addition, you will set passive interfaces on each router.

Task 1: Observe the current routing settings.

Step 1: Issue the **show interface s0/0/0** command on R1.

```
R1# show interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.1/30
  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)
  Last input 00:00:01, output 00:00:02, output hang never
  Last clearing of "show interface" counters 03:43:45
  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
    4050 packets input, 270294 bytes, 0 no buffer
    Received 1554 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    1 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 1 abort
    4044 packets output, 271278 bytes, 0 underruns
    0 output errors, 0 collisions, 5 interface resets
    4 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
    12 carrier transitions
  DCD=up DSR=up DTR=up RTS=up CTS=up
```

What is the default bandwidth for this serial interface? _____

Step 2: How many routes are listed in the routing table to reach the 10.2.2.0/30 network? _____

Task 2: Modify the bandwidth on the routers.

Step 1: Modify the bandwidth on R1 for the serial interfaces.

```
R1(config)# interface s0/0/0
R1(config-if)# bandwidth 2000
R1(config-if)# interface s0/0/1
R1(config-if)# bandwidth 64
```

Issue **show ip route** command on R1. Is there a difference in the routing table? If so, what is it?

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

```

      10.0.0.0/8 is variably subnetted, 5 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
D       10.2.2.0/30 [90/2681856] via 10.1.1.2, 00:03:09, Serial0/0/0
C       10.3.3.0/30 is directly connected, Serial0/0/1
L       10.3.3.1/32 is directly connected, Serial0/0/1
      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
D       192.168.2.0/24 [90/1794560] via 10.1.1.2, 00:03:09, Serial0/0/0
D       192.168.3.0/24 [90/2684416] via 10.1.1.2, 00:03:08, Serial0/0/0

```

Step 2: Modify the bandwidth on the R2 and R3 serial interfaces.

```
R2(config)# interface s0/0/0
R2(config-if)# bandwidth 2000
R2(config-if)# interface s0/0/1
R2(config-if)# bandwidth 2000
```

```
R3(config)# interface s0/0/0
R3(config-if)# bandwidth 64
R3(config-if)# interface s0/0/1
R3(config-if)# bandwidth 2000
```

Task 3: Verify the bandwidth modifications.

Step 1: Verify bandwidth modifications. Issue a **show interface serial 0/0/x** command, with x being the appropriate serial interface on all three routers to verify that bandwidth is set correctly. R1 is shown as an example.

```

R1# show interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 2000 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:01, output 00:00:02, output hang never
  Last clearing of "show interface" counters 04:06:06
  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
    4767 packets input, 317155 bytes, 0 no buffer
    Received 1713 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    1 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 1 abort
    4825 packets output, 316451 bytes, 0 underruns
    0 output errors, 0 collisions, 5 interface resets
    4 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
    12 carrier transitions
  DCD=up DSR=up DTR=up RTS=up CTS=up

```

Based on your bandwidth configuration, try and determine what the R2 and R3 routing tables will look like before you issue a **show ip route** command. Are their routing tables the same or different?

Task 4: Configure G0/0 interface as passive on R1, R2, and R3.

A passive interface does not allow outgoing and incoming routing updates over the configured interface. The **passive-interface** *interface* command causes the router to stop sending and receiving Hello packets over an interface; however, the network associated with the interface is still advertised to other routers through the non-passive interfaces. Router interfaces connected to LANs are typically configured as passive.

```

R1(config)# router eigrp 10
R1(config-router)# passive-interface g0/0

R2(config)# router eigrp 10
R2(config-router)# passive-interface g0/0

R3(config)# router eigrp 10
R3(config-router)# passive-interface g0/0

```

Task 5: Verify the passive interface configuration.

Issue a **show ip protocols** command on R1, R2, and R3 and verify that G0/0 has been configured as passive.

```
R1# show ip protocols
```

*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 10"

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-IPv4 Protocol for AS(10)

Metric weight K1=1, K2=0, K3=1, K4=0, K5=0

NSF-aware route hold timer is 240

Router-ID: 192.168.1.1

Topology : 0 (base)

Active Timer: 3 min

Distance: internal 90 external 170

Maximum path: 4

Maximum hopcount 100

Maximum metric variance 1

Automatic Summarization: disabled

Maximum path: 4

Routing for Networks:

10.1.1.0/30

10.3.3.0/30

192.168.1.0

Passive Interface(s):

GigabitEthernet0/0

Routing Information Sources:

Gateway	Distance	Last Update
---------	----------	-------------

10.3.3.2	90	00:48:09
----------	----	----------

10.1.1.2	90	00:48:26
----------	----	----------

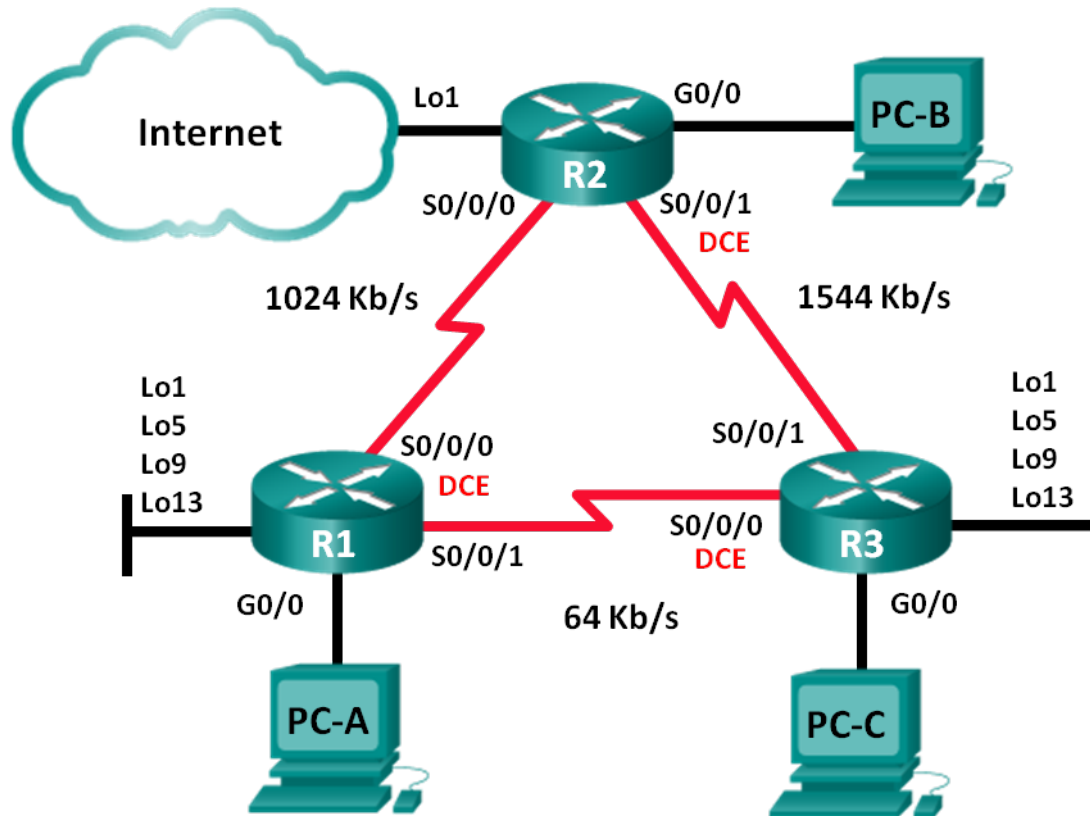
Distance: internal 90 external 170

Reflection

You could have used only static routing for this lab. What is an advantage of using EIGRP?

Lab 6: Configuring Advanced EIGRP for IPv4 Features

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
	Lo1	192.168.11.1	255.255.255.252	N/A
	Lo5	192.168.11.5	255.255.255.252	N/A
	Lo9	192.168.11.9	255.255.255.252	N/A
	Lo13	192.168.11.13	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
	Lo1	192.168.22.1	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
	Lo1	192.168.33.1	255.255.255.252	N/A
	Lo5	192.168.33.5	255.255.255.252	N/A
	Lo9	192.168.33.9	255.255.255.252	N/A
	Lo13	192.168.33.13	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 EIGRP and Verify Connectivity

Part 3: Configure Summarization for EIGRP

- Configure EIGRP for automatic summarization.
- Configure manual summarization for EIGRP.

Part 4: Configure and Propagate a Default Static Route

Part 5: Fine-Tune EIGRP

- Configure bandwidth utilization for EIGRP.
- Configure the hello interval and hold timer for EIGRP.

Part 6: Configure EIGRP Authentication

Background / Scenario

EIGRP has advanced features to allow changes related to summarization, default route propagation, bandwidth utilization, metrics, and security.

In this lab, you will configure automatic and manual summarization for EIGRP, configure EIGRP route propagation, fine-tune EIGRP metrics, and use MD5 authentication to secure EIGRP 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 this end of the lab for the correct interface identifiers.

Note: Ensure 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 will set up the network topology and configure basic settings on the PC hosts and routers.

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

Task 2: Configure PC hosts.

Task 3: Initialize and reload the routers as necessary.

Task 4: Configure basic settings for each router.

Step 1: Disable DNS lookup.

Step 2: Configure device name as shown in the topology.

Step 3: Assign **cisco** as the console and vty passwords.

Step 4: Assign **class** as the privileged EXEC password.

Step 5: Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 6: Configure the IP address listed in the Addressing Table for all interfaces.

Note: Do **NOT** configure the loopback interfaces at this time.

Step 7: Copy the running configuration to the startup configuration.

Part 2: Configure EIGRP and Verify Connectivity

In Part 2, you will configure basic EIGRP for the topology and set bandwidths for the serial interfaces.

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

Task 1: Configure EIGRP.

Step 1: On R1, configure EIGRP routing with an autonomous system (AS) ID of 1 for all directly connected networks. Write the commands used in the space below.

Step 2: For the LAN interface on R1, disable the transmission of EIGRP hello packets. Write the command used in the space below.

Step 3: On R1, configure the bandwidth for S0/0/0 to 1024 Kb/s and the bandwidth for S0/0/1 to 64 Kb/s. Write the commands used in the space below. **Note:** The **bandwidth** command only affects the EIGRP metric calculation, not the actual bandwidth of the serial link.

Step 4: On R2, configure EIGRP routing with an AS ID of 1 for all networks, disable the transmission of EIGRP hello packets for the LAN interface, and configure the bandwidth for S0/0/0 to 1024 Kb/s.

Step 5: On R3, configure EIGRP routing with an AS ID of 1 for all networks, disable the transmission of EIGRP hello packets for the LAN interface, and configure the bandwidth for S0/0/0 to 64 Kb/s.

Task 2: Test connectivity.

All PCs should be able to ping one another. Verify and troubleshoot if necessary.

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

Part 3: Configure Summarization for EIGRP

In Part 3, you will add loopback interfaces to R1, enable EIGRP automatic summarization on R1, and observe the effects on the routing table for R2. You will also add loopback interfaces on R3.

Task 1: Configure EIGRP for automatic summarization.

Step 1: Issue the **show ip protocols** command on R1. What is the default status of automatic summarization in EIGRP?

Step 2: Configure the loopback addresses on R1.

Step 3: Add the appropriate network statements to the EIGRP process on R1. Record the commands used in the space below.

Step 4: On R2, issue the **show ip route eigrp** command. How are the loopback networks represented in the output?

Step 5: On R1, issue the **auto-summary** command inside the EIGRP process.

```
R1(config)# router eigrp 1
R1(config-router)# auto-summary
R1(config-router)#
*Apr 14 01:14:55.463: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.13.2
(Serial0/0/1) is resync: summary configured
*Apr 14 01:14:55.463: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.12.2
(Serial0/0/0) is resync: summary configured
*Apr 14 01:14:55.463: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.13.2
(Serial0/0/1) is resync: summary up, remove components
R1(config-router)#67: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.12.2
(Serial0/0/0) is resync: summary up, remove components
*Apr 14 01:14:55.467: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.12.2
(Serial0/0/0) is resync: summary up, remove components
*Apr 14 01:14:55.467: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.13.2
(Serial0/0/1) is resync: summary up, remove components
```

How does the routing table on R2 change?

Task 2: Configure manual summarization for EIGRP.

Step 1: Configure the loopback addresses on R3.

Step 2: Add the appropriate network statements to the EIGRP process on R3.

Step 3: On R2, issue the **show ip route eigrp** command. How are the loopback networks from R3 represented in the output?

Step 4: Determine the summary EIGRP route for the loopback addresses on R3. Write the summary route in the space below.

Step 5: For the serial interfaces on R3, issue the **ip summary-address eigrp 1 network address subnet mask** command to manually summarize the networks.

```
R3(config)# interface s0/0/0
R3(config-if)# ip summary-address eigrp 1 192.168.33.0 255.255.255.240
R3(config-if)# exit
R3(config)# interface s0/0/1
R3(config-if)# ip summary-address eigrp 1 192.168.33.0 255.255.255.240
*Apr 14 01:33:46.433: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.13.1
(Serial0/0/0) is resync: summary configured
*Apr 14 01:33:46.433: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.23.1
(Serial0/0/1) is resync: summary configured
```

How does the routing table on R2 change?

Part 4: Configure and Propagate a Default Static Route

In Part 4, you will configure a default static route on R2 and propagate the route to all other routers.

Step 1: Configure the loopback address on R2.

Step 2: Configure a default static route with an exit interface of Lo1.

```
R2(config)# ip route 0.0.0.0 0.0.0.0 Lo1
```

Step 3: Use the **redistribute static** command within the EIGRP process to propagate the default static route to other participating routers.

```
R2(config)# router eigrp 1
```

```
R2(config-router)# redistribute static
```

Step 4: Use the **show ip protocols** command on R2 to verify the static route is being distributed.

```
R2# show ip protocols
```

```
*** IP Routing is NSF aware ***
```

```
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
```

```
Redistributing: static
```

```
EIGRP-IPv4 Protocol for AS(1)
```

```
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
```

```
NSF-aware route hold timer is 240
```

```
Router-ID: 192.168.23.1
```

```
Topology : 0 (base)
```

```
Active Timer: 3 min
```

```
Distance: internal 90 external 170
```

```
Maximum path: 4
```

```
Maximum hopcount 100
```

```
Maximum metric variance 1
```

```
Automatic Summarization: disabled
```

```
Maximum path: 4
```

```
Routing for Networks:
```

```
192.168.2.0
```

```
192.168.12.0/30
```

```
192.168.23.0/30
```

```
Passive Interface(s):
```

```
GigabitEthernet0/0
```

```
Routing Information Sources:
```

```
Gateway Distance Last Update
```

```
192.168.12.1 90 00:13:20
```

```
192.168.23.2 90 00:13:20
```

```
Distance: internal 90 external 170
```

Step 5: On R1, issue the **show ip route eigrp | include 0.0.0.0** command to view statements specific to the default route. How is the static default route represented in the output? What is the administrative distance (AD) for the propagated route?

Part 5: Fine-Tune EIGRP

In Part 5, you will configure the percentage of bandwidth that can be used by an EIGRP interface and change the hello interval and hold timers for EIGRP interfaces.

Task 1: Configure bandwidth utilization for EIGRP.

Step 1: Configure the serial link between R1 and R2 to allow only 75 percent of the link bandwidth for EIGRP traffic.

```
R1(config)# interface s0/0/0
R1(config-if)# ip bandwidth-percent eigrp 1 75
R2(config)# interface s0/0/0
R2(config-if)# ip bandwidth-percent eigrp 1 75
```

Step 2: Configure the serial link between R1 and R3 to allow 40 percent of the links bandwidth for EIGRP traffic.

Task 2: Configure the hello interval and hold timer for EIGRP.

Step 1: On R2, use the **show ip eigrp interfaces detail** command to view the hello interval and hold timer for EIGRP.

```
R2# show ip eigrp interfaces detail
```

```
EIGRP-IPv4 Interfaces for AS(1)
```

Interface	Peers	Xmit Queue Un/Reliable	PeerQ Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Se0/0/0	1	0/0	0/0	1	0/15	50	0
Hello-interval is 5, Hold-time is 15							
Split-horizon is enabled							
Next xmit serial <none>							
Packetized sent/expedited: 29/1							
Hello's sent/expedited: 390/2							
Un/reliable mcasts: 0/0 Un/reliable ucasts: 35/39							
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0							
Retransmissions sent: 0 Out-of-sequence rcvd: 0							
Topology-ids on interface - 0							
Interface BW percentage is 75							
Authentication mode is not set							
Se0/0/1	1	0/0	0/0	1	0/16	50	0
Hello-interval is 5, Hold-time is 15							
Split-horizon is enabled							
Next xmit serial <none>							
Packetized sent/expedited: 34/5							
Hello's sent/expedited: 382/2							
Un/reliable mcasts: 0/0 Un/reliable ucasts: 31/42							
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 2							
Retransmissions sent: 0 Out-of-sequence rcvd: 0							
Topology-ids on interface - 0							
Authentication mode is not set							

What is the default value for hello time? _____

What is the default value for hold time? _____

Step 2: Configure S0/0/0 and S0/0/1 interfaces on R1 to use a hello interval of 60 seconds and a hold time of 180 seconds in that specific order.

```
R1(config)# interface s0/0/0
R1(config-if)# ip hello-interval eigrp 1 60
R1(config-if)# ip hold-time eigrp 1 180
R1(config)# interface s0/0/1
R1(config-if)# ip hello-interval eigrp 1 60
R1(config-if)# ip hold-time eigrp 1 180
```

Step 3: Configure the serial interfaces on R2 and R3 to use a hello interval of 60 seconds and a hold time of 180 seconds.

Step 4: Use the **show ip eigrp interfaces detail** command on R2 to verify configuration.

Part 6: Configure EIGRP Authentication

In Part 6, you will create an authentication key on all routers and configure router interfaces to use MD5 authentication for EIGRP message authentication.

Task 1: Configure authentication keys.

Step 1: On R1, use the **key chain name** command in global configuration mode to create a key chain with the label EIGRP-KEYS.

```
R1(config)# key chain EIGRP-KEYS
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string cisco
```

Step 2: Complete the configuration on R2 and R3.

Step 3: Issue the **show key chain** command. You should have the same output on every router.

Task 2: Configure EIGRP link authentication.

Step 1: Apply the following commands to active EIGRP authentication on the serial interfaces on R1.

```
R1# conf t
R1(config)# interface s0/0/0
R1(config-if)# ip authentication key-chain eigrp 1 EIGRP-KEYS
R1(config-if)# ip authentication mode eigrp 1 md5
R1(config-if)# interface s0/0/1
R1(config-if)# ip authentication key-chain eigrp 1 EIGRP-KEYS
R1(config-if)# ip authentication mode eigrp 1 md5
```

Step 2: Activate EIGRP authentication on the serial interfaces on R2 and R3.

Step 3: On R2, use the **show ip eigrp interfaces detail** command to verify authentication.

```
R2# show ip eigrp interfaces detail
```

```
EIGRP-IPv4 Interfaces for AS(1)
```

Interface	Peers	Xmit Queue Un/Reliable	PeerQ Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Se0/0/0	1	0/0	0/0	1	0/23	50	0

Hello-interval is 60, Hold-time is 180
Split-horizon is enabled

```

Next xmit serial <none>
Packetized sent/expedited: 30/5
Hello's sent/expedited: 1163/5
Un/reliable mcasts: 0/0  Un/reliable ucasts: 25/34
Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 0
Retransmissions sent: 0  Out-of-sequence rcvd: 0
Topology-ids on interface - 0
Authentication mode is md5, key-chain is "EIGRP-KEYS"
Se0/0/1          1          0/0          0/0          2          0/15          50          0
Hello-interval is 60, Hold-time is 180
Split-horizon is enabled
Next xmit serial <none>
Packetized sent/expedited: 31/1
Hello's sent/expedited: 1354/3
Un/reliable mcasts: 0/0  Un/reliable ucasts: 28/34
Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 4
Retransmissions sent: 0  Out-of-sequence rcvd: 0
Topology-ids on interface - 0
Authentication mode is md5, key-chain is "EIGRP-KEYS"

```

Reflection

1. What are the benefits of summarizing routes?

2. When setting EIGRP timers, why is it important to make the hold time value equal to or greater than the hello interval?

3. Why is it important to configure authentication for EIGRP?

Appendix A: Configuration Commands

Router R1

```

R1(config)# router eigrp 1
R1(config-router)# network 192.168.1.0
R1(config-router)# network 192.168.12.0 0.0.0.3
R1(config-router)# network 192.168.13.0 0.0.0.3
R1(config-router)# network 192.168.11.0 0.0.0.3
R1(config-router)# network 192.168.11.4 0.0.0.3
R1(config-router)# network 192.168.11.8 0.0.0.3
R1(config-router)# network 192.168.11.12 0.0.0.3
R1(config-router)# passive-interface g0/0
R1(config)# int s0/0/0
R1(config-if)# bandwidth 1024
R1(config-if)# int s0/0/1
R1(config-if)# bandwidth 64

```

Router R2

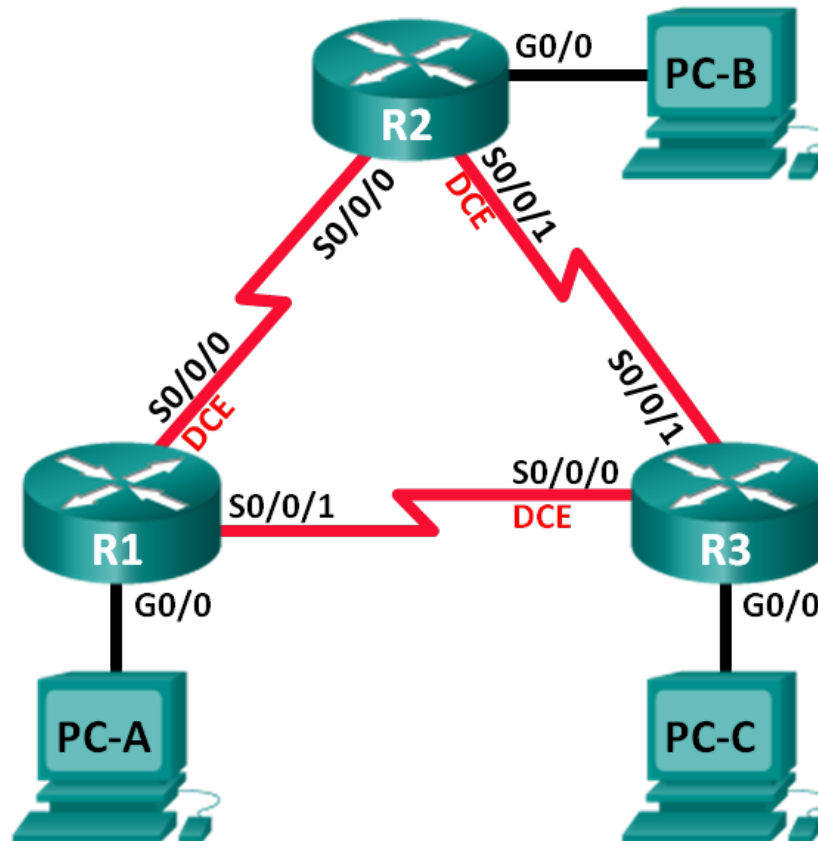
```
R2(config)# router eigrp 1
R2(config-router)# network 192.168.2.0
R2(config-router)# network 192.168.12.0 0.0.0.3
R2(config-router)# network 192.168.23.0 0.0.0.3
R2(config-router)# passive-interface g0/0
R2(config)# int s0/0/0
R2(config-if)# bandwidth 1024
```

Router R3

```
R3(config)# router eigrp 1
R3(config-router)# network 192.168.3.0
R3(config-router)# network 192.168.13.0 0.0.0.3
R3(config-router)# network 192.168.23.0 0.0.0.3
R3(config-router)# network 192.168.33.0 0.0.0.3
R3(config-router)# network 192.168.33.4 0.0.0.3
R3(config-router)# network 192.168.33.8 0.0.0.3
R3(config-router)# network 192.168.33.12 0.0.0.3
R3(config-router)# passive-interface g0/0
R3(config)# int s0/0/0
R3(config-if)# bandwidth 64
```

Lab 7: Configuring Basic EIGRP for IPv6

Topology



Addressing Table

Device	Interface	IP 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::1/64 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::1/64 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::3/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::3/64	FE80::2
PC-C	NIC	2001:DB8:ACAD:C::3/64	FE80::3

Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure EIGRP for IPv6 Routing

Part 3: Verify EIGRP for IPv6 Routing

Part 4: Configure and Verify Passive Interfaces

Background / Scenario

EIGRP for IPv6 has the same overall operation and features as EIGRP for IPv4. However, there are a few major differences between them:

- EIGRP for IPv6 is configured directly on the router interfaces.
- With EIGRP for IPv6, a router ID is required on each router or the routing process does not start.
- The EIGRP for IPv6 routing process uses a shutdown feature.

In this lab, you will configure the network with EIGRP routing for IPv6. You will also assign router IDs, configure passive interfaces, verify the network is fully converged, and display routing information using CLI **show** commands.

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 Verify Connectivity

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords.

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

Task 2: Configure PC hosts.

Task 3: Initialize and reload the routers as necessary.

Task 4: Configure basic settings for each router.

Step 1: Disable DNS lookup.

Step 2: Configure IP addresses for the routers as listed in Addressing Table.

Note: Configure the FE80::x link-local address and the unicast address for each router interface.

Step 3: Configure the device name as shown in the topology.

Step 4: Assign **cisco** as the console and vty passwords.

Step 5: Assign **class** as the privileged EXEC password.

Step 6: Configure **logging synchronous** to prevent console and vty messages from interrupting command entry.

Step 7: Configure a message of the day.

Step 8: Copy the running configuration to the startup configuration.

Task 5: Verify connectivity.

The routers should be able to ping one another, and each PC should be able to ping its default gateway. The PCs will not be able to ping other PCs until EIGRP routing is configured. Verify and troubleshoot if necessary.

Part 2: Configure EIGRP for IPv6 Routing

Task 1: Enable IPv6 routing on the routers.

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

Task 2: Assign a router ID to each router.

Step 1: To begin the EIGRP for IPv6 routing configuration process, issue the **ipv6 router eigrp 1** command, where **1** is the AS number.

```
R1(config)# ipv6 router eigrp 1
```

Step 2: EIGRP for IPv6 requires a 32-bit address for the router ID. Use the **router-id** command to configure the router ID in the router configuration mode.

```
R1(config)# ipv6 router eigrp 1
```

```
R1(config-rtr)# router-id 1.1.1.1
```

```
R2(config)# ipv6 router eigrp 1
```

```
R2(config-rtr)# router-id 2.2.2.2
```

```
R3(config)# ipv6 router eigrp 1
```

```
R3(config-rtr)# router-id 3.3.3.3
```

Task 3: Enable EIGRP for IPv6 routing on each router.

The IPv6 routing process is shut down by default. Issue the **no shutdown** command to enable EIGRP for IPv6 routing on all routers.

```
R1(config)# ipv6 router eigrp 1
```

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

```
R2(config)# ipv6 router eigrp 1
```

```
R2(config-rtr)# no shutdown
```

```
R3(config)# ipv6 router eigrp 1
```

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

Task 4: Configure EIGRP for IPv6 using AS 1 on the Serial and Gigabit Ethernet interfaces on the routers.

Step 1: Issue the **ipv6 eigrp 1** command on the interfaces that participate in the EIGRP routing process. The AS number is 1 as assigned in Step 2. The configuration for R1 is displayed below as an example.

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

```
R1(config-if)# ipv6 eigrp 1
```

```
R1(config-if)# interface s0/0/0
```

```
R1(config-if)# ipv6 eigrp 1
```

```
R1(config-if)# interface s0/0/1
```

```
R1(config-if)# ipv6 eigrp 1
```

Step 2: Assign EIGRP participating interfaces on R2 and R3. You will see neighbor adjacency messages as interfaces are added to the EIGRP routing process. The messages on R1 are displayed below as an example.

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

```
*Apr 12 00:25:49.183: %DUAL-5-NBRCHANGE: EIGRP-IPv6 1: Neighbor FE80::2 (Serial0/0/0) is up: new adjacency
```

```
*Apr 12 00:26:15.583: %DUAL-5-NBRCHANGE: EIGRP-IPv6 1: Neighbor FE80::3 (Serial0/0/1) is up: new adjacency
```

What address is used to indicate the neighbor in the adjacency messages? _____

Task 5: Verify end-to-end connectivity.

Part 3: Verify EIGRP for IPv6 Routing

Task 1: Examine the neighbor adjacencies.

On R1, issue the **show ipv6 eigrp neighbors** command to verify that the adjacency has been established with its neighboring routers. The link-local addresses of the neighboring routers are displayed in the adjacency table.

```
R1# show ipv6 eigrp neighbors
EIGRP-IPv6 Neighbors for AS(1)
H   Address                               Interface      Hold Uptime    SRTT    RTO  Q  Seq
                               (sec)          (ms)          Cnt  Num
 1   Link-local address: Se0/0/1          13 00:02:42    1    100  0   7
    FE80::3
 0   Link-local address: Se0/0/0          13 00:03:09   12    100  0   9
    FE80::2
```

Task 2: Examine the IPv6 EIGRP routing table.

Use the **show ipv6 route eigrp** command to display IPv6 specific EIGRP routes on all the routers.

```
R1# show ipv6 route eigrp
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
D   2001:DB8:ACAD:B::/64 [90/2172416]
    via FE80::2, Serial0/0/0
D   2001:DB8:ACAD:C::/64 [90/2172416]
    via FE80::3, Serial0/0/1
D   2001:DB8:ACAD:23::/64 [90/2681856]
    via FE80::2, Serial0/0/0
    via FE80::3, Serial0/0/1
```

Task 3: Examine the EIGRP topology.

```
R1# show ipv6 eigrp topology
EIGRP-IPv6 Topology Table for AS(1)/ID(1.1.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 2001:DB8:ACAD:A::/64, 1 successors, FD is 28160
   via Connected, GigabitEthernet0/0
P 2001:DB8:ACAD:C::/64, 1 successors, FD is 2172416
   via FE80::3 (2172416/28160), Serial0/0/1
P 2001:DB8:ACAD:12::/64, 1 successors, FD is 2169856
   via Connected, Serial0/0/0
P 2001:DB8:ACAD:B::/64, 1 successors, FD is 2172416
   via FE80::2 (2172416/28160), Serial0/0/0
```

```
P 2001:DB8:ACAD:23::/64, 2 successors, FD is 2681856
    via FE80::2 (2681856/2169856), Serial0/0/0
    via FE80::3 (2681856/2169856), Serial0/0/1
P 2001:DB8:ACAD:13::/64, 1 successors, FD is 2169856
    via Connected, Serial0/0/1
```

Compare the highlighted entries to the routing table. What can you conclude from the comparison?

Task 4: Verify the parameters and current state of the active IPv6 routing protocol processes.

Issue the **show ipv6 protocols** command to verify the configured parameter. From the output, EIGRP is the configured IPv6 routing protocol with 1.1.1.1 as the router ID for R1. This routing protocol is associated with autonomous system 1 with three active interfaces: G0/0, S0/0/0, and S0/0/1.

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "eigrp 1"
EIGRP-IPv6 Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  NSF-aware route hold timer is 240
  Router-ID: 1.1.1.1
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 16
    Maximum hopcount 100
    Maximum metric variance 1

Interfaces:
  GigabitEthernet0/0
  Serial0/0/0
  Serial0/0/1
Redistribution:
  None
```

Part 4: Configure and Verify Passive Interfaces

A passive interface does not allow outgoing and incoming routing updates over the configured interface. The **passive-interface** command causes the router to stop sending and receiving Hello packets over an interface.

Task 1: Configure interface G0/0 as passive on R1 and R2.

```
R1(config)# ipv6 router eigrp 1
R1(config-rtr)# passive-interface g0/0

R2(config)# ipv6 router eigrp 1
```

```
R2(config-rtr)# passive-interface g0/0
```

Task 2: Verify the passive interface configuration.

Issue the **show ipv6 protocols** command on R1 and verify that G0/0 has been configured as passive.

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "eigrp 1"
EIGRP-IPv6 Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  NSF-aware route hold timer is 240
  Router-ID: 1.1.1.1
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 16
    Maximum hopcount 100
    Maximum metric variance 1

Interfaces:
  Serial0/0/0
  Serial0/0/1
  GigabitEthernet0/0 (passive)

Redistribution:
  None
```

Task 3: Configure the G0/0 passive interface on R3.

If a few interfaces are configured as passive, use the **passive-interface default** command to configure all the interfaces on the router as passive. Use the **no passive-interface interface** command to allow EIGRP Hello messages in and out of the router interface.

Step 1: Configure all interfaces as passive on R3.

```
R3(config)# ipv6 router eigrp 1
R3(config-rtr)# passive-interface default
R3(config-rtr)#
*Apr 13 00:07:03.267: %DUAL-5-NBRCHANGE: EIGRP-IPv6 1: Neighbor FE80::1 (Serial0/0/0) is
down: interface passive
*Apr 13 00:07:03.267: %DUAL-5-NBRCHANGE: EIGRP-IPv6 1: Neighbor FE80::2 (Serial0/0/1) is
down: interface passive
```

Step 2: After you have issued the **passive-interface default** command, R3 no longer participates in the routing process. What command can you use to verify it?

Step 3: What command can you use to display the passive interfaces on R3?

Step 4: Configure the serial interfaces to participate in the routing process.

```
R3(config)# ipv6 router eigrp 1
R3(config-rtr)# no passive-interface s0/0/0
R3(config-rtr)# no passive-interface s0/0/1
```

```
R3(config-rtr)#
```

```
*Apr 13 00:21:23.807: %DUAL-5-NBRCHANGE: EIGRP-IPv6 1: Neighbor FE80::1 (Serial0/0/0) is  
up: new adjacency
```

```
*Apr 13 00:21:25.567: %DUAL-5-NBRCHANGE: EIGRP-IPv6 1: Neighbor FE80::2 (Serial0/0/1) is  
up: new adjacency
```

Step 5: The neighbor relationships have been established again with R1 and R2. Verify that only G0/0 has been configured as passive. What command do you use to verify the passive interface?

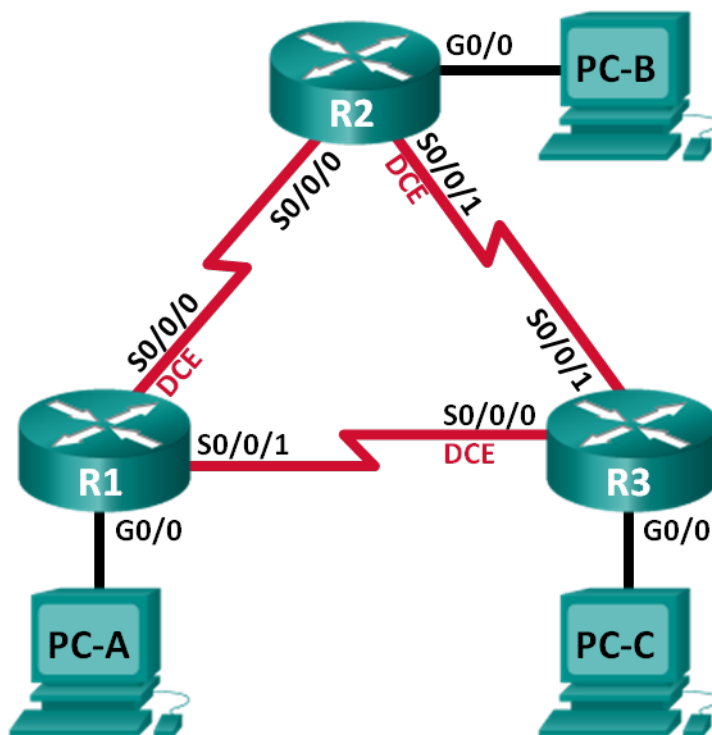
Reflection

1. Where would you configure passive interfaces? Why?

2. What are some advantages with using EIGRP as the routing protocol in your network?

Lab 8: Troubleshooting Basic EIGRP for IPv4 and IPv6

Topology



Addressing Table

Device	EIGRP Router ID	Interface	IP Address	Default Gateway
R1	1.1.1.1	G0/0	192.168.1.1/24 2001:DB8:ACAD:A::1/64 FE80::1 link-local	N/A
		S0/0/0 (DCE)	192.168.12.1/30 2001:DB8:ACAD:12::1/64 FE80::1 link-local	N/A
		S0/0/1	192.18.13.1/30 2001:DB8:ACAD:13::1/64 FE80::1 link-local	N/A
R2	2.2.2.2	G0/0	192.168.2.1/24 2001:DB8:ACAD:B::2/64 FE80::2 link-local	N/A
		S0/0/0	192.168.12.2/30 2001:DB8:ACAD:12::2/64 FE80::2 link-local	N/A
		S0/0/1 (DCE)	192.168.23.1/30 2001:DB8:ACAD:23::2/64 FE80::2 link-local	N/A
R3	3.3.3.3	G0/0	192.168.3.1/24 2001:DB8:ACAD:C::3/64 FE80::3 link-local	N/A
		S0/0/0 (DCE)	192.168.13.2/30 2001:DB8:ACAD:13::3/64 FE80::3 link-local	N/A
		S0/0/1	192.168.23.2/30 2001:DB8:ACAD:23::3/64 FE80::3 link-local	N/A
PC-A		NIC	192.168.1.3/24 2001:DB8:ACAD:A::A/64	192.168.1.1 FE80::1
PC-B		NIC	192.168.2.3/24 2001:DB8:ACAD:B::B/64	192.168.2.1 FE80::2
PC-C		NIC	192.168.3.3/24 2001:DB8:ACAD:C::C/64	192.168.3.1 FE80::3

Objectives

Part 1: Build the Network and Load Device Configurations

Part 2: Troubleshoot Layer 3 Connectivity

Part 3: Troubleshoot EIGRP for IPv4

Part 4: Troubleshoot EIGRP for IPv6

Background / Scenario

The Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance vector routing protocol developed by Cisco Systems. EIGRP routers discover neighbors and establish and maintain adjacencies with neighbor routers using Hello packets. An EIGRP router assumes that as long as it is receiving Hello packets from a neighboring router, that neighbor is up and its routes remain viable.

EIGRP for IPv4 runs over the IPv4 network layer, communicating with other EIGRP IPv4 peers, and advertising only IPv4 routes. EIGRP for IPv6 has the same functionality as EIGRP for IPv4 but uses IPv6 as the network layer protocol, communicating with EIGRP for IPv6 peers and advertising IPv6 routes.

In this lab, you will troubleshoot a network that runs EIGRP for IPv4 and EIGRP for IPv6 routing protocols. This network is experiencing problems and you are tasked with finding the problems and correcting them.

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 Router (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 Load Device Configurations

In Part 1, you will set up the network topology and configure basic settings on the PC hosts and routers.

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

Task 2: Configure PC hosts.

Task 3: Load router configurations.

Load the following configurations into the appropriate router. All routers have the same passwords. The privileged EXEC password is **class**, and the console and vty password is **cisco**.

Router R1 Configuration:

```
conf t
service password-encryption
hostname R1
enable secret class
```

```
no ip domain lookup
ipv6 unicast-routing
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:A::1/64
 ipv6 eigrp 1
 no shutdown
interface Serial0/0/0
 bandwidth 128
 ip address 192.168.21.1 255.255.255.252
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:12::1/64
 ipv6 eigrp 1
 clock rate 128000
 no shutdown
interface Serial0/0/1
 ip address 192.168.13.1 255.255.255.252
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:31::1/64
 ipv6 eigrp 1
 no shutdown
router eigrp 1
 network 192.168.1.0
 network 192.168.12.0 0.0.0.3
 network 192.168.13.0 0.0.0.3
 passive-interface GigabitEthernet0/0
 eigrp router-id 1.1.1.1
ipv6 router eigrp 1
 no shutdown
banner motd @
  Unauthorized Access is Prohibited! @
line con 0
 password cisco
 logging synchronous
line vty 0 4
 password cisco
login
 transport input all
end
```

Router R2 Configuration:

```
conf t
service password-encryption
hostname R2
```

```
enable secret class
no ip domain lookup
ipv6 unicast-routing
interface GigabitEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:ACAD:B::2/64
 ipv6 eigrp 1
interface Serial0/0/0
 ip address 192.168.12.2 255.255.255.252
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:ACAD:12::2/64
 ipv6 eigrp 1
 no shutdown
interface Serial0/0/1
 bandwidth 128
 ip address 192.168.23.1 255.255.255.0
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:ACAD:23::2/64
 ipv6 eigrp 1
 clock rate 128000
 no shutdown
router eigrp 1
 network 192.168.12.0 0.0.0.3
 network 192.168.23.0 0.0.0.3
 passive-interface GigabitEthernet0/0
 eigrp router-id 2.2.2.2
ipv6 router eigrp 1
 no shutdown
 passive-interface GigabitEthernet0/0
banner motd @
  Unauthorized Access is Prohibited! @
line con 0
 password cisco
 login
 logging synchronous
line vty 0 4
 password cisco
 login
 transport input all
end
```

Router R3 Configuration:

```
conf t
service password-encryption
```

```
hostname R3
enable secret class
no ip domain lookup
interface GigabitEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FE80::3 link-local
 ipv6 address 2001:DB8:ACAD:C::3/64
 ipv6 eigrp 1
interface Serial0/0/0
 ip address 192.168.13.2 255.255.255.252
 ipv6 address FE80::3 link-local
 ipv6 address 2001:DB8:ACAD:13::3/64
 ipv6 eigrp 1
 no shutdown
interface Serial0/0/1
 bandwidth 128
 ip address 192.168.23.2 255.255.255.252
 ipv6 address FE80::3 link-local
 ipv6 address 2001:DB8:ACAD:23::3/64
 ipv6 eigrp 1
 no shutdown
router eigrp 1
 network 192.168.3.0
 network 192.168.13.0 0.0.0.3
 passive-interface GigabitEthernet0/0
 eigrp router-id 3.3.3.3
banner motd @
  Unauthorized Access is Prohibited! @
line con 0
 password cisco
 login
 logging synchronous
line vty 0 4
 password cisco
 login
 transport input all
end
```

Task 4: Save the running configuration for all routers.

Part 2: Troubleshoot Layer 3 Connectivity

In Part 2, you will verify that Layer 3 connectivity is established on all interfaces. You will need to test both IPv4 and IPv6 connectivity for all device interfaces.

Note: All serial interfaces should be set with a bandwidth of 128 Kb/s. The clock rate on the DCE interface should be set to 128000.

Task 1: Verify that the interfaces listed in the Addressing Table are active and configured with correct IP address information.

Step 1: Issue the **show ip interface brief** command on all routers to verify that the interfaces are in an up/up state. Record your findings.

Step 2: Issue the **show run interface** command to verify IP address assignments on all router interfaces. Compare the interface IP addresses against the Addressing Table and verify the subnet mask assignments. For IPv6, verify that the link-local address has been assigned. Record your findings.

Step 3: Issue the **show interfaces** *interface-id* command to verify bandwidth setting on the serial interfaces. Record your findings.

Step 4: Issue the **show controllers** *interface-id* command to verify that clock rates have been set to 128 Kb/s on all DCE serial interfaces. Issue the **show interfaces** *interface-id* command to verify bandwidth setting on the serial interfaces. Record your findings.

Step 5: Resolve all problems found. Record the commands used to correct the issues.

[illegible]

Task 2: Verify Layer 3 connectivity.

Use the **ping** command and verify that each router has network connectivity with the serial interfaces on the neighbor routers. Verify that the PCs can ping their default gateways. If problems still exist, continue troubleshooting Layer 3 issues.

Part 3: Troubleshoot EIGRP for IPv4

In Part 3, you will troubleshoot EIGRP for IPv4 problems and make the necessary changes needed to establish EIGRP for IPv4 routes and end-to-end IPv4 connectivity.

Note: LAN (G0/0) interfaces should not advertise EIGRP routing information, but routes to these networks should be contained in the routing tables.

Task 1: Test IPv4 end-to-end connectivity.

From each PC host, ping the other PC hosts in the topology to verify end-to-end connectivity.

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

Step 1: Ping from PC-A to PC-B. Were the pings successful? _____

Step 2: Ping from PC-A to PC-C. Were the pings successful? _____

Step 3: Ping from PC-B to PC-C. Were the pings successful? _____

Task 2: Verify that all interfaces are assigned to EIGRP for IPv4.

Step 1: Issue the **show ip protocols** command to verify that EIGRP is running and that all networks are advertised. This command also allows you to verify that the router ID is set correctly, and that the LAN interfaces are set as passive interfaces. Record your findings.

Step 2: Make the necessary changes based on the output from the **show ip protocols** command. Record the commands that were used to correct the issues.

Step 3: Re-issue the **show ip protocols** command to verify that your changes had the desired effect.

Task 3: Verify EIGRP neighbor information.

Step 1: Issue the **show ip eigrp neighbor** command to verify that EIGRP adjacencies have been established between the neighboring routers.

Step 2: Resolve any outstanding problems that were discovered.

Task 4: Verify EIGRP for IPv4 routing information.

Step 1: Issue the **show ip route eigrp** command to verify that each router has EIGRP for IPv4 routes to all non-adjointing networks.

Are all EIGRP routes available? _____

If any EIGRP for IPv4 routes are missing, what is missing?

Step 2: If any routing information is missing, resolve these issues.

Task 5: Verify IPv4 end-to-end connectivity.

From each PC, verify that IPv4 end-to-end connectivity exists. PCs should be able to ping the other PC hosts in the topology. If IPv4 end-to-end connectivity does not exist, then continue troubleshooting to resolve remaining issues.

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

Part 4: Troubleshoot EIGRP for IPv6

In Part 3, you will troubleshoot EIGRP for IPv6 problems and make the necessary changes needed to establish EIGRP for IPv6 routes and end-to-end IPv6 connectivity.

Note: LAN (G0/0) interfaces should not advertise EIGRP routing information, but routes to these networks should be contained in the routing tables.

Task 1: Test IPv6 end-to-end connectivity.

From each PC host, ping the IPv6 addresses of the other PC hosts in the topology to verify end-to-end connectivity.

Task 2: Verify that IPv6 unicast routing has been enabled on all routers.

Step 1: An easy way to verify that IPv6 routing has been enabled on a router is to use the **show run | section ipv6 unicast** command. By adding this pipe to the **show run** command, the **ipv6 unicast-routing** command is displayed if IPv6 routing has been enabled.

Note: The **show run** command can also be issued without any pipe, and then a manual search for the **ipv6 unicast-routing** command can be done.

Issue the command on each router. Record your findings.

Step 2: If IPv6 unicast routing is not enabled on one or more routers, enable it now. Record the commands that were used to correct the issues.

Task 3: Verify that all interfaces are assigned to EIGRP for IPv6.

Step 1: Issue the **show ipv6 protocols** command and verify that the router ID is correct. This command also allows you to verify that the LAN interfaces are set as passive interfaces.

Note: If no output is generated from this command, then the EIGRP for IPv6 process has not been configured.

Record your findings.

Step 2: Make the necessary configuration changes. Record the commands used to correct the issues.

[illegible]

Step 3: Re-issue the **show ipv6 protocols** command to verify that your changes are correct.

Task 4: Verify that all routers have correct neighbor adjacency information.

Step 1: Issue the **show ipv6 eigrp neighbor** command to verify that adjacencies have formed between neighboring routers.

Step 2: Resolve any EIGRP adjacency issues that still exist.

Task 5: Verify EIGRP for IPv6 routing information.

Step 1: Issue the **show ipv6 route eigrp** command, and verify that EIGRP for IPv6 routes exist to all non-adjointing networks.

Are all EIGRP routes available?

If any EIGRP for IPv6 routes are missing, what is missing?

Step 2: Resolve any routing issues that still exist.

Task 6: Test IPv6 end-to-end connectivity.

From each PC, verify that IPv6 end-to-end connectivity exists. PCs should be able to ping the other PC hosts in the topology. If IPv6 end-to-end connectivity does not exist, then continue troubleshooting to resolve remaining issues.

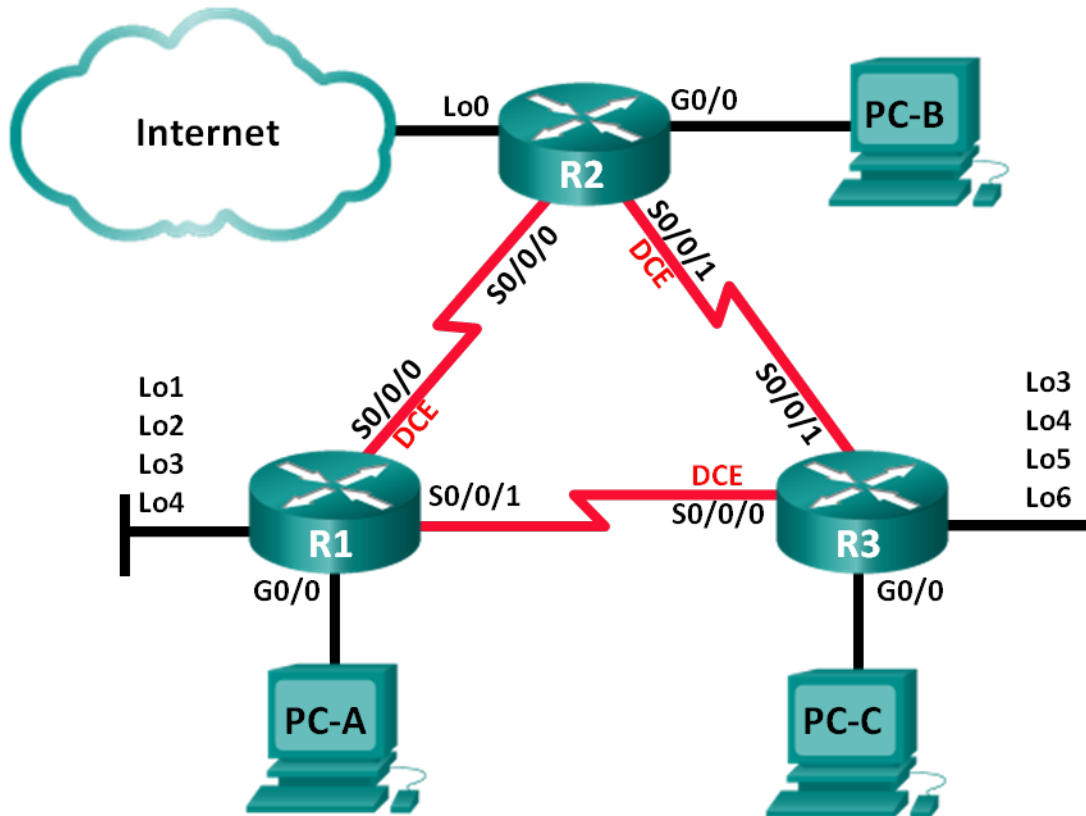
Note: It may be necessary to disable the PCs firewall.

Reflection

Why would you troubleshoot EIGRP for IPv4 and EIGRP for IPv6 separately?

Lab 9: Troubleshooting Advanced EIGRP

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	Lo1	172.16.11.1	255.255.255.0	N/A
	Lo2	172.16.12.1	255.255.255.0	N/A
	Lo3	172.16.13.1	255.255.255.0	N/A
	Lo4	172.16.14.1	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
	Lo0	209.165.200.225	255.255.255.252	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
	Lo3	172.16.33.1	255.255.255.0	N/A
	Lo4	172.16.34.1	255.255.255.0	N/A
	Lo5	172.16.35.1	255.255.255.0	N/A
	Lo6	172.16.36.1	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 Load Device Configurations

Part 2: Troubleshoot EIGRP

Background / Scenario

The Enhanced Interior Gateway Routing Protocol (EIGRP) has advanced features to allow changes related to summarization, default route propagation, bandwidth utilization, metrics, and security.

In this lab, you will troubleshoot a network that is running EIGRP. Advanced EIGRP features have been implemented, but the network is now experiencing problems. You are tasked with finding and correcting the network issues.

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: Ensure 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 cables as shown in the topology

Part 1: Build the Network and Load Device Configurations

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

Task 2: Configure PC hosts.

Task 3: Load router configurations.

Load the following configurations into the appropriate router. All routers have the same passwords. The privileged EXEC password is **class**, and **cisco** is the console and vty password.

Router R1 Configuration:

```
conf t
hostname R1
enable secret class
no ip domain lookup
key chain EIGRP-KEYS
  key 1
    key-string cisco123
line con 0
  password cisco
  login
  logging synchronous
line vty 0 4
  password cisco
  login
banner motd @
  Unauthorized Access is Prohibited! @
interface lo1
  description Connection to Branch 11
  ip add 172.16.11.1 255.255.255.0
interface lo2
  description Connection to Branch 12
  ip add 172.16.12.1 255.255.255.0
interface lo3
  description Connection to Branch 13
  ip add 172.16.13.1 255.255.255.0
interface lo4
  description Connection to Branch 14
```

```
ip add 172.16.14.1 255.255.255.0
interface g0/0
description R1 LAN Connection
ip add 192.168.1.1 255.255.255.0
no shutdown
interface s0/0/0
description Serial Link to R2
clock rate 128000
ip add 192.168.12.1 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP-KEYS
ip hello-interval eigrp 1 30
ip hold-time eigrp 1 90
ip bandwidth-percent eigrp 1 40
no shutdown
interface s0/0/1
description Serial Link to R3
bandwidth 128
ip add 192.168.13.1 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP-KEYS
ip bandwidth-percent eigrp 1 40
no shutdown
router eigrp 1
router-id 1.1.1.1
network 192.168.1.0 0.0.0.255
network 192.168.12.0 0.0.0.3
network 192.168.13.0 0.0.0.3
network 172.16.0.0 0.0.255.255
passive-interface g0/0
auto-summary
end
```

Router R2 Configuration:

```
conf t
hostname R2
enable secret class
no ip domain lookup
key chain EIGRP-KEYS
key 1
key-string Cisco123
line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
```

```
login
banner motd @
    Unauthorized Access is Prohibited! @
interface g0/0
    description R2 LAN Connection
    ip add 192.168.2.1 255.255.255.0
    no shutdown
interface s0/0/0
    description Serial Link to R1
    bandwidth 128
    ip add 192.168.12.2 255.255.255.252
    ip authentication mode eigrp 1 md5
    ip authentication key-chain eigrp 1 EIGRP-KEYS
    ip bandwidth-percent eigrp 1 40
    ip hello-interval eigrp 1 30
    ip hold-time eigrp 1 90
    no shutdown
interface s0/0/1
    description Serial Link to R3
    bandwidth 128
    ip add 192.168.23.1 255.255.255.252
    ip authentication mode eigrp 1 md5
    ip bandwidth-percent eigrp 1 40
    ip hello-interval eigrp 1 30
    ip hold-time eigrp 1 90
    no shutdown
interface lo0
    ip add 209.165.200.225 255.255.255.252
    description Connection to ISP
router eigrp 1
    router-id 2.2.2.2
    network 192.168.2.0 0.0.0.255
    network 192.168.12.0 0.0.0.3
    network 192.168.23.0 0.0.0.3
    passive-interface g0/0
ip route 0.0.0.0 0.0.0.0 lo0
end
```

Router R3 Configuration:

```
conf t
hostname R3
enable secret class
no ip domain lookup
key chain EIGRP-KEYS
    key 1
        key-string Cisco123
line con 0
```

```
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
banner motd @
    Unauthorized Access is Prohibited! @
interface lo3
    description Connection to Branch 33
    ip add 172.16.33.1 255.255.255.0
interface lo4
    description Connection to Branch 34
    ip add 172.16.34.1 255.255.255.0
interface lo5
    description Connection to Branch 35
    ip add 172.16.35.1 255.255.255.0
interface lo6
    description Connection to Branch 36
    ip add 172.16.36.1 255.255.255.0
interface g0/0
    description R3 LAN Connection
    ip add 192.168.3.1 255.255.255.0
    no shutdown
interface s0/0/0
    description Serial Link to R1
    ip add 192.168.13.2 255.255.255.252
    ip authentication mode eigrp 1 md5
    ip authentication key-chain eigrp 1 EIGRP-KEYS
    ip hello-interval eigrp 1 30
    ip hold-time eigrp 1 90
    clock rate 128000
    bandwidth 128
    no shutdown
interface s0/0/1
    description Serial Link to R2
    bandwidth 128
    ip add 192.168.23.2 255.255.255.252
    ip authentication mode eigrp 1 md5
    ip authentication key-chain eigrp 1 eigrp-keys
! ip bandwidth-percent eigrp 1 40
    ip hello-interval eigrp 1 30
    ip hold-time eigrp 1 90
    no shutdown
router eigrp 1
    router-id 3.3.3.3
    network 192.168.3.0 0.0.0.255
```

```

network 192.168.13.0 0.0.0.3
network 192.168.23.0 0.0.0.3
network 172.16.0.0 0.0.255.255
passive-interface g0/0
auto-summary
end

```

Task 4: Verify end-to-end connectivity.

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

Task 5: Save the configuration on all routers.

Part 2: Troubleshoot EIGRP

In Part 2, verify that all routers have established neighbor adjacencies, and that all network routes are available.

Additional EIGRP Requirements:

- All serial interface clock rates should be set at 128 Kb/s and a matching bandwidth setting should be available to allow EIGRP cost metrics to be calculated correctly.
- Manual route summarization of the branch networks, simulated by using Loopback interfaces on R1 and R3, should be utilized. The automatic summarization feature of EIGRP should not be used.
- EIGRP should redistribute the static default route to the Internet. This is simulated by using Loopback interface 0 on R2.
- EIGRP should be configured to use no more than **40** percent of the available bandwidth on the serial interfaces.
- EIGRP Hello/Hold timer intervals should be set to **30/90** on all serial interfaces.
- All serial interfaces should be configured with MD5 authentication, using key chain **EIGRP-KEYS**, with a key-string of **Cisco123**.

List the commands used during your EIGRP troubleshooting process:

List the changes made to resolve the EIGRP issues. If no problems were found on the device, then respond with "no problems were found".

R1 Router:

[illegible][illegible]

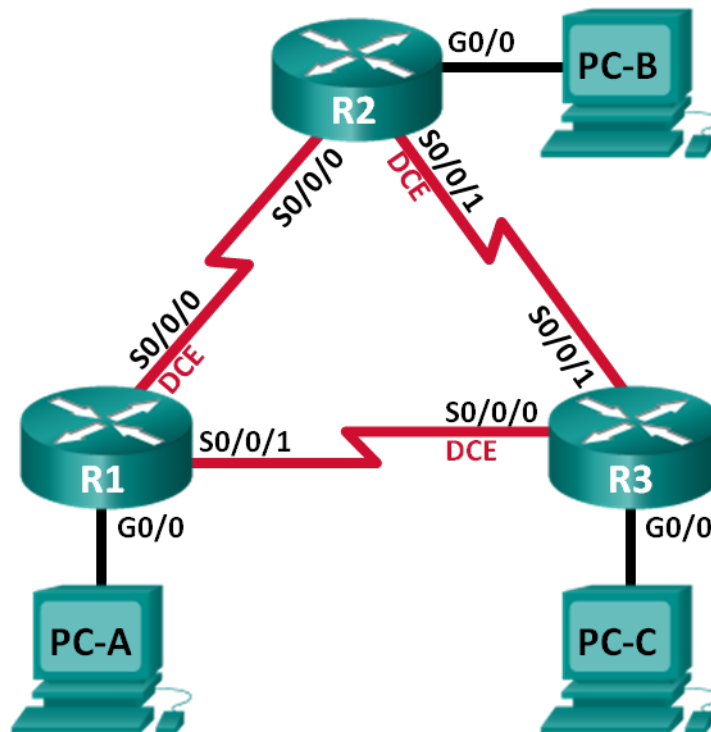
1. How can the **auto-summary** command create routing issues in EIGRP?

-

-

Lab 10: 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.

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

Task 2: Initialize and reload the routers as necessary.

Task 3: Configure basic settings for each router.

Step 1: Disable DNS lookup.

Step 2: Configure device name as shown in the topology.

Step 3: Assign **class** as the privileged EXEC password.

Step 4: Assign **cisco** as the console and vty passwords.

Step 5: Configure a message of the day (MOTD) banner to warn users that unauthorized access is prohibited.

Step 6: Configure **logging synchronous** for the console line.

Step 7: Configure the IP address listed in the Addressing Table for all interfaces.

Step 8: Set the clock rate for all DCE serial interfaces at **128000**.

Step 9: Copy the running configuration to the startup configuration.

Task 4: Configure PC hosts.

Task 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.

Task 1: Configure OSPF on R1.

Step 1: 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.

Step 2: 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
```

Task 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#
```

Task 3: Verify OSPF neighbors and routing information.

Step 1: 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

Step 2: 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?

Task 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)
```

Task 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

```

Task 6: Verify OSPF interface settings.

Step 1: 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	

Step 2: 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)

```

Task 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:

- IP address configured with the OSPF **router-id** command, if present
- Highest IP address of any of the router's loopback addresses, if present
- 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.

Task 1: Change router IDs using loopback addresses.

Step 1: 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
```

Step 2: 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.

Step 3: Save the running configuration to the startup configuration on all three routers.

Step 4: 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.

Step 5: 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)
```

Step 6: 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#
```

Task 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.

Step 1: 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
```

Step 2: 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.

Step 3: 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.

Step 4: 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)
```

Step 5: 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.

Task 1: Configure a passive interface.

Step 1: 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)
```

Step 2: 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
```

Step 3: 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)

```

Step 4: 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

```

Task 2: Set passive interface as the default on a router.

Step 1: 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

Step 2: 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

Step 3: 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

Step 4: 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)

Step 5: 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.

Step 6: 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
```

Step 7: Re-issue the **show ip route** and **show ip 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?

Step 8: Change interface S0/0/1 on R2 to allow it to advertise OSPF routes. Record the commands used below.

Step 9: 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 5, 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.

Task 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.

Step 1: 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.

Step 2: 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      192.168.2.0/24 [110/65] via 192.168.12.2, 00:01:08, Serial0/0/0
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.

Step 3: 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)
```

Step 4: 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.

Step 5: 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.

Step 6: Issue the **auto-cost reference-bandwidth 10000** command on routers R2 and R3.

Step 7: 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)
```

Step 8: 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.

Step 9: 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?

Task 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.

Step 1: 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>

```

Step 2: 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    192.168.2.0/24 [110/65] via 192.168.12.2, 00:00:26, Serial0/0/0
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, 00:00:26, Serial0/0/0

```

Step 3: 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

```

Step 4: 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    192.168.2.0/24 [110/129] via 192.168.12.2, 00:01:47, Serial0/0/0
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

```

Step 5: 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	

Step 6: Change the bandwidth for interface S0/0/1 to the same setting as S0/0/0 on R1.

Step 7: 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    192.168.2.0/24 [110/782] via 192.168.12.2, 00:00:09, Serial0/0/0
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.

Step 8: 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
O    192.168.2.0/24 [110/65] via 192.168.23.1, 00:30:58, Serial0/0/1
  
```

```

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

```

Step 9: 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?

Task 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.

Step 1: 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

```

Step 2: 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)# interface s0/0/1
R1(config-if)# ip ospf cost 1565

```

Step 3: 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

- 192.168.2.0/24 [110/782] via 192.168.12.2, 00:02:06, Serial0/0/0
- 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
- 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

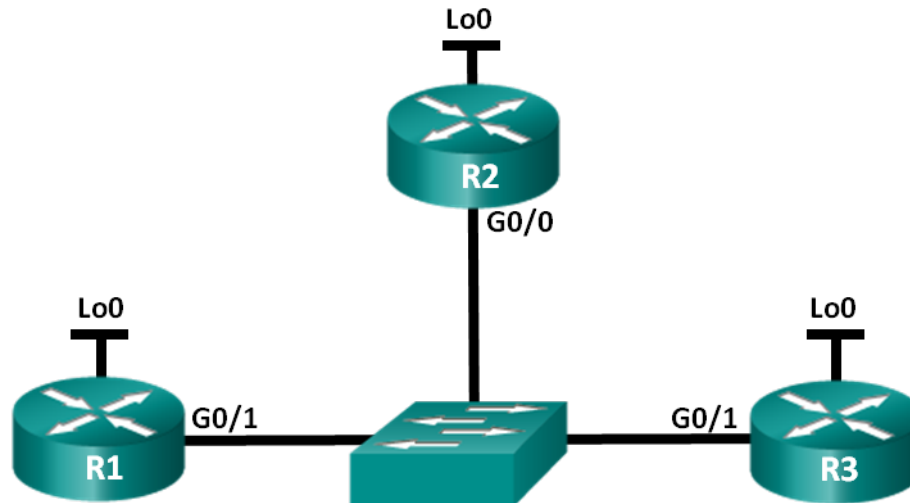
1. Why is it important to control the router ID assignment when using the OSPF protocol?

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?

Lab 11: Configuring OSPFv2 on a Multiaccess Network

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	G0/1	192.168.1.1	255.255.255.0
	Lo0	192.168.31.11	255.255.255.255
R2	G0/0	192.168.1.2	255.255.255.0
	Lo0	192.168.31.22	255.255.255.255
R3	G0/1	192.168.1.3	255.255.255.0
	Lo0	192.168.31.33	255.255.255.255

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure and Verify OSPFv2 on the DR, BDR, and DROther

Part 3: Configure OSPFv2 Interface Priority to Determine the DR and BDR

Background / Scenario

A multiaccess network is a network with more than two devices on the same shared media. Examples include Ethernet and Frame Relay. On multiaccess networks, OSPFv2 elects a Designated Router (DR) to be the collection and distribution point for link-state advertisements (LSAs) that are sent and received. A Backup Designated Router (BDR) is also elected in case the DR fails. All other routers become DROthers as this indicates a router that is neither the DR nor the BDR.

Because the DR acts as a focal point for OSPF routing protocol communication, the router chosen should be capable of supporting a heavier traffic load than other routers in the network. A router with a powerful CPU and adequate DRAM is typically the best choice for the DR.

In this lab, you will configure OSPFv2 on the DR, BDR, and DROther. You will then modify the priority of routers to control the outcome of the DR/BDR election process and ensure that the desired router becomes the DR.

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

- 3 Routers (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)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet 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 on the routers.

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

Attach the devices as shown in the topology diagram, and cable as necessary.

Task 2: Initialize and reload the routers.

Task 3: Configure basic settings for each router.

Step 1: Disable DNS lookup.

Step 2: Configure device names as shown in the topology.

Step 3: Assign **class** as the privileged EXEC password.

Step 4: Assign **cisco** as the console and vty passwords.

Step 5: Encrypt the plain text passwords.

Step 6: Configure a MOTD banner to warn users that unauthorized access is prohibited.

Step 7: Configure **logging synchronous** for the console line.

Step 8: Configure the IP addresses listed in the Addressing Table for all interfaces.

Step 9: Use the **show ip interface brief** command to verify that the IP addressing is correct and that the interfaces are active.

Step 10: Copy the running configuration to the startup configuration.

Part 2: Configure and Verify OSPFv2 on the DR, BDR, and DROther

In Part 2, you will configure OSPFv2 on the DR, BDR, and DROther. 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 does 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.

Task 1: Configure OSPF on R3.

Configure the OSPF process on R3 (the router with the highest router ID) to ensure that this router becomes the DR.

Step 1: Assign 1 as the process ID for the OSPF process. 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.

What factor determined that R3 has the highest router ID?

Step 2: Verify that OSPF has been configured and R3 is the DR.

What command would you use to verify that OSPF has been configured correctly and R3 is the DR?

Task 2: Configure OSPF on R2.

Configure the OSPF process on R2 (the router with the second highest router ID) to ensure that this router becomes the BDR.

Step 1: Assign 1 as the process ID for the OSPF process. 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.

Step 2: Verify that the OSPF has been configured and that R2 is the BDR. Record the command used for verification.

Step 3: Issue the **show ip ospf neighbor** command to view information about the other routers in the OSPF area.

```
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	GigabitEthernet0/0

Notice that R3 is the DR.

Task 3: Configure OSPF on R1.

Configure the OSPF process on R1 (the router with the lowest router ID). This router will be designated as DROther instead of DR or BDR.

Step 1: Assign 1 as the process ID for the OSPF process. 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.

Step 2: Issue **show ip ospf interface brief** command to verify that OSPF has been configured and R1 is the DROther.

```
R1# show ip ospf interface brief
```

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Gi0/1	1	0	192.168.1.1/24	1	DROTH	2/2	

Step 3: Issue the **show ip ospf neighbor** command to view information about the other routers in the OSPF area.

```
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	GigabitEthernet0/1
192.168.31.33	1	FULL/DR	00:00:30	192.168.1.3	GigabitEthernet0/1

What priority are both the DR and BDR routers? _____

Part 3: Configure OSPFv2 Interface Priority to Determine the DR and BDR

In Part 3, you will configure router interface priority to determine the DR/BDR election, reset the OSPFv2 process, and then verify that the DR and BDR routers have changed. OSPF interface priority overrides all other settings in determining which routers become the DR and BDR.

Task 1: Configure R1 G0/1 with OSPF priority 255.

A value of 255 is the highest possible interface priority.

```
R1(config)# interface g0/1
R1(config-if)# ip ospf priority 255
R1(config-if)# end
```

Task 2: Configure R3 G0/1 with OSPF priority 100.

```
R3(config)# interface g0/1
R3(config-if)# ip ospf priority 100
R3(config-if)# end
```

Task 3: Configure R2 G0/0 with OSPF priority 0.

A priority of 0 causes the router to be ineligible to participate in an OSPF election and does not become a DR or BDR.

```
R2(config)# interface g0/0
R2(config-if)# ip ospf priority 0
R2(config-if)# end
```

Task 4: Reset the OSPF process.

Step 1: Issue the **show ip ospf neighbor** command to determine the DR and BDR.

Step 2: Has the DR designation changed? _____ Which router is the DR? _____

Has the BDR designation changed? _____ Which router is the BDR? _____

What is the role of R2 now? _____

Explain the immediate effects caused by the **ip ospf priority** command.

Note: If the DR and BDR designations did not change, issue the **clear ip ospf 1 process** command on all of the routers to reset the OSPF processes and force a new election.

If the **clear ip ospf process** command does not reset the DR and BDR, issue the **reload** command on all routers after saving the running configuration to the startup configuration.

Step 3: Issue the **show ip ospf interface** command on R1 and R3 to confirm the priority settings and DR/BDR status on the routers.

```
R1# show ip ospf interface
GigabitEthernet0/1 is up, line protocol is up
Internet Address 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 DR, Priority 255
```

```

Designated Router (ID) 192.168.31.11, Interface address 192.168.1.1
Backup Designated router (ID) 192.168.31.33, Interface address 192.168.1.3
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:00
Supports Link-local Signaling (LLS)
Index 1/1, flood queue length 0
Next 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 2, Adjacent neighbor count is 2
  Adjacent with neighbor 192.168.31.22
  Adjacent with neighbor 192.168.31.33 (Backup Designated Router)
Suppress hello for 0 neighbor(s)

```

R3# **show ip ospf interface**

```

GigabitEthernet0/1 is up, line protocol is up
Internet Address 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
Backup Designated router (ID) 192.168.31.33, Interface address 192.168.1.3
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:00
Supports Link-local Signaling (LLS)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 2
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 2, Adjacent neighbor count is 2
  Adjacent with neighbor 192.168.31.22
  Adjacent with neighbor 192.168.31.11 (Designated Router)
Suppress hello for 0 neighbor(s)

```

Which router is now the DR? _____

Which router is now the BDR? _____

Did the interface priority override the router ID in determining the DR/BDR? _____

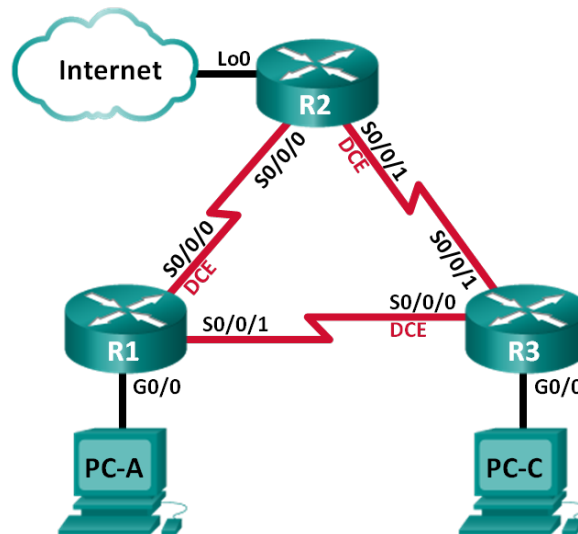
Reflection

1. List the criteria used from highest to lowest for determining the DR on an OSPF network.

2. What is the significance of a 255 interface priority?

Lab 12: Configuring OSPFv2 Advanced Features

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	Lo0	209.165.200.225	255.255.255.252	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-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 OSPF Metrics

Part 4: Configure and Propagate a Static Default Route

Part 5: Configure OSPF Authentication

Background / Scenario

Open Shortest Path First (OSPF) has advanced features to allow changes to be made to control metrics, default route propagation, and security.

In this lab, you will adjust OSPF metrics on the router interfaces, configure OSPF route propagation, and use Message Digest 5 (MD5) authentication to secure 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)
- 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 set up the network topology and configure basic settings on the PC hosts and routers.

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

Task 2: Initialize and reload the routers as necessary.

Task 3: Configure basic settings for each router.

Step 1: Disable DNS lookup.

Step 2: Configure device name as shown in the topology.

Step 3: Assign **class** as the privileged EXEC password.

Step 4: Assign **cisco** as the console and vty passwords.

Step 5: Encrypt the clear text passwords.

Step 6: Configure a MOTD banner to warn users that unauthorized access is prohibited.

Step 7: Configure **logging synchronous** for the console line.

Step 8: Configure the IP addresses listed in the Addressing Table for all interfaces.

Step 9: Set the clock rate for all DCE serial interfaces at 128000.

Step 10: Copy the running configuration to the startup configuration.

Task 4: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

Task 5: Test connectivity.

At this point, the PCs are unable to ping each other. However, the routers should be able to ping the directly connected neighbor interfaces, and the PCs should be able to ping their default gateway. 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.

Task 1: Configure the router ID on all routers.

Assign 1 as the process ID for this OSPF process. Each router should be given the following router ID assignments:

- R1 Router ID: **1.1.1.1**
- R2 Router ID: **2.2.2.2**
- R3 Router ID: **3.3.3.3**

Task 2: Configure OSPF network information on the routers.

Task 3: Verify OSPF routing.

Step 1: Issue the **show ip ospf neighbor** command to verify that each router is listing the other routers in the network.

Step 2: Issue the **show ip route ospf** command to verify that all OSPF networks are present in the routing table on all routers.

Task 4: Test end-to-end connectivity.

Ping PC-C from PC-A to verify end-to-end connectivity. The pings should be successful. If they are not, troubleshoot as necessary.

Note: It may be necessary to disable the PC firewall for the pings to be successful.

Part 3: Change OSPF Metrics

In Part 3, you will change OSPF metrics using the **bandwidth** command, the **auto-cost reference-bandwidth** command, and the **ip ospf cost** command. Making these changes will provide more accurate metrics to OSPF.

Note: All DCE interfaces should have been configured with a clocking rate of 128000 in Part 1.

Task 1: Change the bandwidth on all serial interfaces to 128Kb/s.

Step 1: Issue the **show ip ospf interface brief** command to view the default cost settings on the router 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	

Step 2: Use the **bandwidth 128** interface command on all serial interfaces.

Step 3: Issue the **show ip ospf interface brief** command to view the new cost settings.

```
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	781	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	

Task 2: Change the reference bandwidth on the routers.

Step 1: Issue the **auto-cost reference-bandwidth 1000** command on the routers to change the default reference bandwidth setting to account for Gigabit Ethernet Interfaces.

Step 2: Re-issue the **show ip ospf interface brief** command to view how this command has changed cost values.

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	7812	P2P	0/0	
Se0/0/0	1	0	192.168.12.1/30	7812	P2P	0/0	
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0	

Note: If the router had Fast Ethernet interfaces instead of Gigabit Ethernet interfaces, then the cost would now be 10 on those interfaces.

Task 3: Change the route cost.

Step 1: Issue the **show ip route ospf** command to display the current OSPF routes on R1. Notice that there are currently two routes in the table that use the S0/0/1 interface.

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 [110/7822] via 192.168.13.2, 00:00:12, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O    192.168.23.0 [110/15624] via 192.168.13.2, 00:00:12, Serial0/0/1
    [110/15624] via 192.168.12.2, 00:20:03, Serial0/0/0
```

Step 2: Apply the **ip ospf cost 16000** command to the S0/0/1 interface on R1. A cost of 16,000 is higher than the accumulated cost of the route through R2 which is 15,624.

Step 3: Issue the **show ip ospf interface brief** command on R1 to view the cost change to S0/0/1.

```
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	16000	P2P	1/1	
Se0/0/0	1	0	192.168.12.1/30	7812	P2P	1/1	
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0	

Step 4: 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      192.168.3.0/24 [110/15625] 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 [110/15624] via 192.168.12.2, 01:14:02, Serial0/0/0
```

Explain why the route to the 192.168.3.0/24 network on R1 is now going through R2?

Part 4: Configure and Propagate a Static Default Route

In Part 4, you will use a loopback interface on R2 to simulate an ISP connection to the Internet. You will create a static default route on R2, and then OSPF will propagate that route to the other two routers on the network.

Task 1: Configure a static default route on R2 to loopback 0.

Configure a default route using the loopback interface configured in Part 1, to simulate a connection to an ISP.

Task 2: Have OSPF propagate the default static route.

Issue the **default-information originate** command to include the static default route in the OSPF updates that are sent from R2.

```
R2(config)# router ospf 1
```

```
R2(config-router)# default-information originate
```

Task 3: Verify OSPF static route propagation.

Step 1: Issue the **show ip route static** command on R2.

```
R2# show ip route static
```

```
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 0.0.0.0 to network 0.0.0.0
```

```
S*    0.0.0.0/0 is directly connected, Loopback0
```

Step 2: Issue the **show ip route** command on R1 to verify the propagation of the static route from R2.

```
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
       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 192.168.12.2 to network 0.0.0.0
```

```
O*E2  0.0.0.0/0 [110/1] via 192.168.12.2, 00:02:57, Serial0/0/0
      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      192.168.3.0/24 [110/15634] via 192.168.12.2, 00:03:35, Serial0/0/0
      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 [110/15624] via 192.168.12.2, 00:05:18, Serial0/0/0
```

Step 3: Verify end-to-end connectivity by issuing a ping from PC-A to the ISP interface address 209.165.200.225.

Were the pings successful? _____

Part 5: Configure OSPF Authentication

OSPF authentication can be set up at the link level or the area level. There are three authentication types available for OSPF authentication: Null, plain text, or MD5. In Part 5, you will set up OSPF MD5 authentication, which is the strongest available.

Task 1: Set up MD5 OSPF authentication on a single link.

Step 1: Issue the **debug ip ospf adj** command on R2 to view OSPF adjacency messages.

```
R2# debug ip ospf adj
OSPF adjacency debugging is on
```

Step 2: Assign an MD5 key for OSPF Authentication on R1, interface S0/0/0.

```
R1(config)# interface s0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 MD5KEY
```

Step 3: Activate MD5 authentication on R1, interface S0/0/0.

```
R1(config-if)# ip ospf authentication message-digest
```

OSPF debug messages informing you of a Mismatched Authentication type displays on R2.

```
*Mar 19 00:03:18.187: OSPF-1 ADJ   Se0/0/0: Rcv pkt from 192.168.12.1 : Mismatched
Authentication type. Input packet specified type 2, we use type 0
```

Step 4: Issue the **u all** command, which is the shortest version of the **undebug all** command on R2 to disable debugging.

Step 5: Configure OSPF authentication on R2, interface S0/0/0. Use the same MD5 password you entered for R1.

Step 6: Issue a **show ip ospf interface s0/0/0** command on R2. This command displays the type of authentication at the bottom of the output.

```
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 2.2.2.2, Network Type POINT_TO_POINT, Cost: 7812
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
    0                7812        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 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 1.1.1.1
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
  Youngest key id is 1
```

Task 2: Set up OSPF authentication at the area level.

Step 1: Issue the **area 0 authentication** command to set MD5 authentication for OSPF Area 0 on R1.

```
R1(config)# router ospf 1
R1(config-router)# area 0 authentication message-digest
```

Step 2: This option still requires that you assign the MD5 password at the interface level.

```
R1(config)# interface s0/0/1
R1(config-if)# ip ospf message-digest-key 1 md5 MD5KEY
```

Step 3: Issue the **show ip ospf neighbor** command on R3. R1 no longer has an adjacency with R3.

```
R3# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	0	FULL/ -	00:00:31	192.168.23.1	Serial0/0/1

Step 4: Set up area authentication on R3 and assign the same MD5 password to interface S0/0/0.

```
R3(config)# router ospf 1
R3(config-router)# area 0 authentication message-digest
R3(config-router)# interface s0/0/0
R3(config-if)# ip ospf message-digest-key 1 md5 MD5KEY
```

Step 5: Issue the **show ip ospf neighbor** command on R3. Notice that R1 is now showing as a neighbor, but R2 is missing.

```
R3# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.1	0	FULL/ -	00:00:38	192.168.13.1	Serial0/0/0

Why is R2 no longer showing as an OSPF neighbor?

Step 6: Configure R2 to perform area-level MD5 authentication.

```
R2(config)# router ospf 1
R2(config-router)# area 0 authentication message-digest
```

Step 7: Assign **MD5KEY** as the MD5 password for the link between R2 and R3.

Step 8: Issue the **show ip ospf neighbor** command on all routers to verify that all adjacencies have been re-established.

```
R1# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	0	FULL/ -	00:00:39	192.168.13.2	Serial0/0/1
2.2.2.2	0	FULL/ -	00:00:35	192.168.12.2	Serial0/0/0

```
R2# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	0	FULL/ -	00:00:36	192.168.23.2	Serial0/0/1
1.1.1.1	0	FULL/ -	00:00:32	192.168.12.1	Serial0/0/0

```
R3# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	0	FULL/ -	00:00:33	192.168.23.1	Serial0/0/1
1.1.1.1	0	FULL/ -	00:00:39	192.168.13.1	Serial0/0/0

Reflection

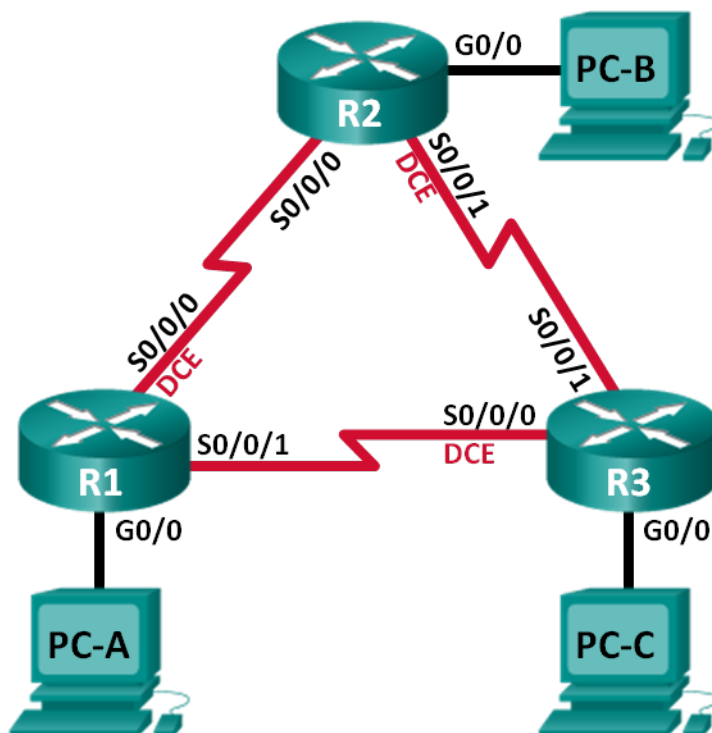
1. What is the easiest and preferred method of manipulating OSPF route costs?

2. What does the **default-information originate** command do for a network using the OSPF routing protocol?

3. Why is it a good idea to use OSPF authentication?

Lab 13: 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 1: 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.

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

Task 2: Initialize and reload the routers as necessary.

Task 3: Configure basic settings for each router.

Step 1: Disable DNS lookup.

Step 2: Configure device name as shown in the topology.

Step 3: Assign **class** as the privileged EXEC password.

Step 4: Assign **cisco** as the vty password.

Step 5: Configure a MOTD banner to warn users that unauthorized access is prohibited.

Step 6: Configure **logging synchronous** for the console line.

Step 7: Encrypt plain text passwords.

Step 8: Configure the IPv6 unicast and link-local addresses listed in the Addressing Table for all interfaces.

Step 9: Enable IPv6 unicast routing on each router.

Step 10: Copy the running configuration to the startup configuration.

Task 4: Configure PC hosts.

Task 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 2: 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.

Task 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.

Step 1: 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.

Step 2: Assign the OSPFv3 router ID **1.1.1.1** to the R1.

```
R1(config-rtr)# router-id 1.1.1.1
```

Step 3: 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.

Step 4: 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>
```

Task 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.

Step 1: 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.

Step 2: 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
```

Task 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

Task 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
```

Task 5: Verify OSPFv3 interfaces.

Step 1: 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)

```

Step 2: 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	

Task 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? _____

Task 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: 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.

Task 1: Configure a passive interface.

Step 1: 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)

```

Step 2: 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

```

Step 3: 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)

```

Step 4: 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

```

Task 2: Set passive interface as the default on the router.

Step 1: 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

```

Step 2: 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

Step 3: 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)

```

Step 4: 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.

Step 5: 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

```

Step 6: 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?

Step 7: On R2, issue the **no passive-interface S0/0/0** command to allow OSPFv3 routing updates to be advertised on that interface.

Step 8: Verify that R1 and R2 are now OSPFv3 neighbors.

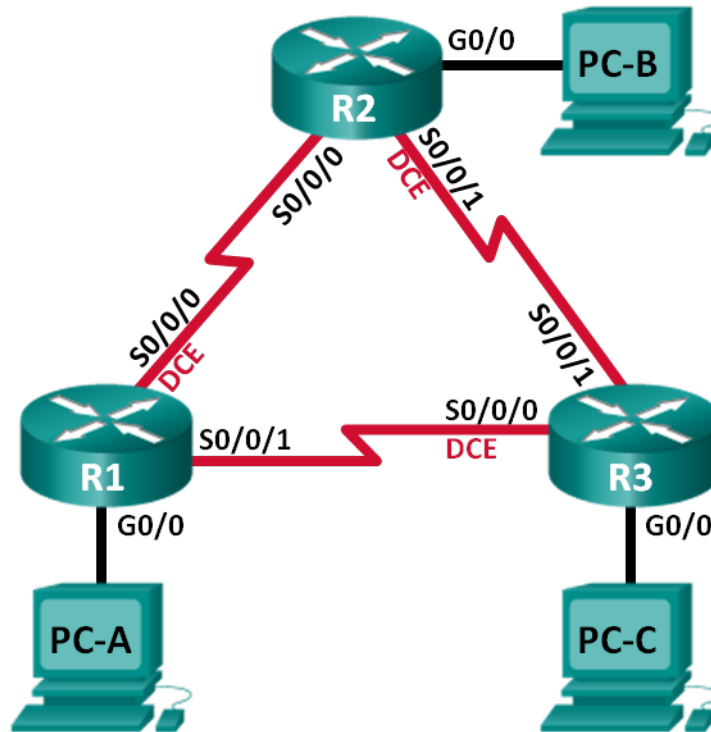
Reflection

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?

Lab 14: Troubleshooting Basic Single-Area OSPFv2 and OSPFv3

Topology



Addressing Table

Device	OSPF Router ID	Interface	IP Address	Default Gateway
R1	1.1.1.1	G0/0	192.168.1.1/24 2001:DB8:ACAD:A::1/64 FE80::1 link-local	N/A
		S0/0/0	192.168.12.1/30 2001:DB8:ACAD:12::1/64 FE80::1 link-local	N/A
		S0/0/1	192.18.13.1/30 2001:DB8:ACAD:13::1/64 FE80::1 link-local	N/A
R2	2.2.2.2	G0/0	192.168.2.1/24 2001:DB8:ACAD:B::2/64 FE80::2 link-local	N/A
		S0/0/0	192.168.12.2/30 2001:DB8:ACAD:12::2/64 FE80::2 link-local	N/A
		S0/0/1	192.168.23.1/30 2001:DB8:ACAD:23::2/64 FE80::2 link-local	N/A
R3	3.3.3.3	G0/0	192.168.3.1/24 2001:DB8:ACAD:C::3/64 FE80::3 link-local	N/A
		S0/0/0	192.168.13.2/30 2001:DB8:ACAD:13::3/64 FE80::3 link-local	N/A
		S0/0/1	192.168.23.2/30 2001:DB8:ACAD:23::3/64 FE80::3 link-local	N/A
PC-A		NIC	192.168.1.3/24 2001:DB8:ACAD:A::A/64	192.168.1.1 FE80::1
PC-B		NIC	192.168.2.3/24 2001:DB8:ACAD:B::B/64	192.168.2.1 FE80::2
PC-C		NIC	192.168.3.3/24 2001:DB8:ACAD:C::C/64	192.168.3.1 FE80::3

Objectives

Part 1: Build the Network and Load Device Configurations

Part 2: Troubleshoot Layer 3 Connectivity

Part 3: Troubleshoot OSPFv2

Part 4: Troubleshoot OSPFv3

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. OSPFv2 and OSPFv3 are completely isolated routing protocols, changes in OSPFv2 do not affect OSPFv3 routing, and vice versa.

In this lab, a single-area OSPF network running OSPFv2 and OSPFv3 is experiencing problems. You have been assigned to find the problems with the network and correct them.

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 Load Device Configurations

In Part 1, you will set up the network topology and configure basic settings on the PC hosts and routers.

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

Task 2: Configure PC hosts.

Task 3: Load router configurations.

Load the following configurations into the appropriate router. All routers have the same passwords. The privileged EXEC password is **cisco**. The password for console and vty access is **class**.

Router R1 Configuration:

```
conf t
service password-encryption
no ip domain lookup
hostname R1
enable secret class
line con 0
logging synchronous
password cisco
```

```
login
line vty 0
password cisco
login
banner motd @Unauthorized Access is Prohibited!@
ipv6 unicast-routing
ipv6 router ospf 1
router-id 1.1.1.1
passive-interface g0/0
interface g0/0
ip address 192.168.1.1 255.255.255.0
ipv6 address 2001:db8:acad:a::1/64
ipv6 address fe80::1 link-local
interface s0/0/0
clock rate 128000
ip address 192.168.12.1 255.255.255.0
ipv6 address 2001:db8:acad:12::1/64
ipv6 address fe80::1 link-local
ipv6 ospf 1 area 0
no shutdown
interface s0/0/1
ip address 192.168.13.1 255.255.255.0
ipv6 address 2001:db8:acad:13::1/64
ipv6 address fe80::1 link-local
ipv6 ospf 1 area 0
no shutdown
router ospf 1
network 192.168.1.0 0.0.0.255 area 0
network 129.168.12.0 0.0.0.3 area 0
network 192.168.13.0 0.0.0.3 area 0
passive-interface g0/0
end
```

Router R2 Configuration:

```
conf t
service password-encryption
no ip domain lookup
hostname R2
enable secret class
line con 0
logging synchronous
password cisco
login
line vty 0
password cisco
login
banner motd @Unauthorized Access is Prohibited!@
```

```
ipv6 unicast-routing
ipv6 router ospf 1
  router-id 2.2.2.2
interface g0/0
ip address 192.168.2.1 255.255.255.0
  ipv6 address 2001:db8:acad:B::2/64
  ipv6 address fe80::1 link-local
  no shutdown
interface s0/0/0
ip address 192.168.12.2 255.255.255.252
  ipv6 address 2001:db8:acad:12::2/64
  ipv6 address fe80::2 link-local
  ipv6 ospf 1 area 0
  no shutdown
interface s0/0/1
  clock rate 128000
  ipv6 address 2001:db8:acad:23::2/64
  ipv6 address fe80::2 link-local
  no shutdown
router ospf 1
  network 192.168.2.0 0.0.0.255 area 0
  network 192.168.12.0 0.0.0.3 area 0
  network 192.168.23.0 0.0.0.3 area 0
end
```

Router R3 Configuration:

```
conf t
service password-encryption
no ip domain lookup
enable secret class
hostname R3
line con 0
  logging synchronous
  password cisco
  login
line vty 0
  password cisco
  login
banner motd @Unauthorized Access is Prohibited!@
interface g0/0
  ipv6 address 2001:db8:acad:c::3/64
  ipv6 address fe80::3 link-local
interface s0/0/0
  clock rate 128000
ip address 192.168.13.1 255.255.255.252
  ipv6 address 2001:db8:acad:13::3/64
  ipv6 address fe80::3 link-local
```

```
no shutdown
interface s0/0/1
  ip address 192.168.23.2 255.255.255.252
  ipv6 address 2001:db8:acad:23::3/64
  ipv6 address fe80::3 link-local
router ospf 1
  network 192.168.3.0 0.0.0.255 area 0
  passive-interface g0/0
end
```

Part 2: Troubleshoot Layer 3 Connectivity

In Part 2, you will verify that Layer 3 connectivity is established on all interfaces. You will need to test both IPv4 and IPv6 connectivity for all device interfaces.

Task 1: Verify that the interfaces listed in the Addressing Table are active and configured with the correct IP address information.

Step 1: Issue the **show ip interface brief** command on all routers to verify that the interfaces are in an up/up state. Record your findings.

Step 2: Issue the **show run interface** command to verify IP address assignments on all router interfaces. Compare the interface IP addresses against the Addressing Table and verify the subnet mask assignments. For IPv6, verify that the link-local address has been assigned. Record your findings.

Step 3: Resolve all problems that are found. Record the commands used to correct the issues.

[illegible]

Step 4: Using the **ping** command, verify that each router has network connectivity with the serial interfaces on the neighbor routers. Verify that the PCs can ping their default gateways. If problems still exist, continue troubleshooting Layer 3 issues.

Part 3: Troubleshoot OSPFv2

In Part 3, you will troubleshoot OSPFv2 problems and make the necessary changes needed to establish OSPFv2 routes and end-to-end IPv4 connectivity.

Note: LAN (G0/0) interfaces should not advertise OSPF routing information, but routes to these networks should be in the routing tables.

Task 1: Test IPv4 end-to-end connectivity.

From each PC host, ping the other PC hosts in the topology to verify end-to-end connectivity.

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

Step 1: Ping from PC-A to PC-B. Were the pings successful? _____

Step 2: Ping from PC-A to PC-C. Were the pings successful? _____

Step 3: Ping from PC-B to PC-C. Were the pings successful? _____

Task 2: Verify that all interfaces are assigned to OSPFv2 area 0 on R1.

Step 1: Issue the **show ip protocols** command to verify that OSPF is running and that all networks are advertised in area 0. Verify that the router ID is set correctly. Record your findings.

Step 2: Make the necessary changes to the configuration on R1 based on the output from the **show ip protocols** command. Record the commands used to correct the issues.

Step 3: Issue the **clear ip ospf process** command if necessary.

Step 4: Re-issue the **show ip protocols** command to verify that your changes had the desired effect.

Step 5: Issue the **show ip ospf interface brief** command to verify that all interfaces are listed as OSPF networks assigned to area 0.

Step 6: Issue the **show ip ospf interface g0/0** command to verify that G0/0 is a passive interface.

Note: This information is also in the **show ip protocols** command.

Step 7: Resolve any problems discovered on R1. List any additional changes made to R1. If no problems were found on the device, then respond with “no problems were found”.

Task 3: Verify that all interfaces are assigned to OSPFv2 area 0 on R2.

Step 1: Issue the **show ip protocols** command to verify that OSPF is running and that all networks are being advertised in area 0. Verify that the router ID is set correctly. Record your findings.

Step 2: Make the necessary changes to the configuration on R2 based on the output from the **show ip protocols** command. Record the commands used to correct the issues.

Step 3: Issue the **clear ip ospf process** command if necessary.

Step 4: Re-issue the **show ip protocols** command to verify that your changes had the desired effect.

Step 5: Issue the **show ip ospf interface brief** command to verify that all interfaces are listed as OSPF networks assigned to area 0.

Step 6: Issue the **show ip ospf interface g0/0** command to verify that G0/0 is a passive interface.

Note: This information is also available from the **show ip protocols** command.

Step 7: Resolve any problems discovered on R2. List any additional changes made to R2. If no problems were found on the device, then respond with “no problems were found”.

Task 4: Verify that all interfaces are assigned to OSPFv2 area 0 on R3.

Step 1: Issue the **show ip protocols** command to verify that OSPF is running and that all networks are being advertised in area 0. Verify that the router ID is set correctly as well. Record your findings.

Step 2: Make the necessary changes to the configuration on R3 based on the output from the **show ip protocols** command. Record the commands used to correct the issues.

Step 3: Issue the **clear ip ospf process** command if necessary.

Step 4: Re-issue the **show ip protocols** command to verify that your changes had the desired effect.

Step 5: Issue the **show ip ospf interface brief** command to verify that all interfaces are listed as OSPF networks assigned to area 0.

Step 6: Issue the **show ip ospf interface g0/0** command to verify that G0/0 is a passive interface.

Note: This information is also in the **show ip protocols** command.

Step 7: Resolve any problems discovered on R3. List any additional changes made to R3. If no problems were found on the device, then respond with “no problems were found”.

Task 5: Verify OSPF neighbor information.

Step 1: Issue the **show ip ospf neighbor** command on all routers to view the OSPF neighbor information.

Task 6: Verify OSPFv2 Routing Information.

Step 1: Issue the **show ip route ospf** command to verify that each router has OSPFv2 routes to all non-adjointing networks.

Are all OSPFv2 routes available? _____

If any OSPFv2 routes are missing, what is missing? _____

Step 2: If any routing information is missing, resolve these issues.

Task 7: Verify IPv4 end-to-end connectivity.

From each PC, verify that IPv4 end-to-end connectivity exists. PCs should be able to ping the other PC hosts in the topology. If IPv4 end-to-end connectivity does not exist, then continue troubleshooting to resolve any remaining issues.

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

Part 4: Troubleshoot OSPFv3

In Part 4, you will troubleshoot OSPFv3 problems and make the necessary changes needed to establish OSPFv3 routes and end-to-end IPv6 connectivity.

Note: LAN (G0/0) interfaces should not advertise OSPFv3 routing information, but routes to these networks should be contained in the routing tables.

Task 1: Test IPv6 end-to-end connectivity.

From each PC host, ping the IPv6 addresses of the other PC hosts in the topology to verify IPv6 end-to-end connectivity.

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

Task 2: Verify that IPv6 unicast routing has been enabled on all routers.

Step 1: An easy way to verify that IPv6 routing has been enabled on a router is to use the **show run | section ipv6 unicast** command. By adding this pipe (|) section to the **show run** command, the **ipv6 unicast-routing** command displays if IPv6 routing has been enabled.

Note: The **show run** command can also be issued without any pipe, and then a manual search for the **ipv6 unicast-routing** command can be done.

Issue the command on each router. Record your findings.

Step 2: If IPv6 unicast routing is not enabled on one or more routers, enable it now. Record the commands used to correct the issues.

Task 3: Verify that all interfaces are assigned to OSPFv3 area 0 on R1.

Step 1: Issue the **show ipv6 protocols** command and verify that the router ID is correct. Also verify that the expected interfaces are displayed under area 0.

Note: If no output is generated from this command, then the OSPFv3 process has not been configured.

Record your findings.

Step 2: Make the necessary configuration changes to R1. Record the commands used to correct the issues.

Step 3: Issue the **clear ipv6 ospf process** command if necessary.

Step 4: Re-issue the **show ipv6 protocols** command to verify that your changes had the desired effect.

Step 5: Issue the **show ipv6 ospf interface brief** command to verify that all interfaces are listed as OSPF networks assigned to area 0.

Step 6: Issue the **show ipv6 ospf interface g0/0** command to verify that this interface is set not to advertise OSPFv3 routes.

Step 7: Resolve any problems discovered on R1. List any additional changes made to R1. If no problems were found on the device, then respond with "no problems were found".

Task 4: Verify that all interfaces are assigned to OSPFv3 area 0 on R2.

Step 1: Issue the **show ipv6 protocols** command and verify the router ID is correct. Also verify that the expected interfaces display under area 0.

Note: If no output is generated from this command, then the OSPFv3 process has not been configured.

Record your findings.

Step 2: Make the necessary configuration changes to R2. Record the commands used to correct the issues.

Step 3: Issue the **clear ipv6 ospf process** command if necessary.

Step 4: Re-issue the **show ipv6 protocols** command to verify that your changes had the desired effect.

Step 5: Issue the **show ipv6 ospf interface brief** command to verify that all interfaces are listed as OSPF networks assigned to area 0.

Step 6: Issue the **show ipv6 ospf interface g0/0** command to verify that this interface is not set to advertise OSPFv3 routes.

Step 7: List any additional changes made to R2. If no problems were found on the device, then respond with “no problems were found”.

Task 5: Verify that all interfaces are assigned to OSPFv3 area 0 on R3.

Step 1: Issue the **show ipv6 protocols** command and verify that the router ID is correct. Also verify that the expected interfaces display under area 0.

Note: If no output is generated from this command, then the OSPFv3 process has not been configured. Record your findings.

Step 2: Make the necessary configuration changes to R3. Record the commands used to correct the issues.

Step 3: Issue the **clear ipv6 ospf process** command if necessary.

Step 4: Re-issue the **show ipv6 protocols** command to verify that your changes had the desired effect.

Step 5: Issue the **show ipv6 ospf interface brief** command to verify that all interfaces are listed as OSPF networks assigned to area 0.

Step 6: Issue the **show ipv6 ospf interface g0/0** command to verify that this interface is set not to advertise OSPFv3 routes.

Step 7: Resolve any problems discovered on R3. List any additional changes made to R3. If no problems were found on the device, then respond with “no problems were found”.

Task 6: Verify that all routers have correct neighbor adjacency information.

Step 1: Issue the **show ipv6 ospf neighbor** command to verify that adjacencies have formed between neighboring routers.

Step 2: Resolve any OSPFv3 adjacency issues that still exist.

Task 7: Verify OSPFv3 routing information.

Step 1: Issue the **show ipv6 route ospf** command, and verify that OSPFv3 routes exist to all non-adjointing networks.

Are all OSPFv3 routes available? _____

If any OSPFv3 routes are missing, what is missing? _____

Step 2: Resolve any routing issues that still exist.

Task 8: Verify IPv6 end-to-end connectivity.

From each PC, verify that IPv6 end-to-end connectivity exists. PCs should be able to ping each interface on the network. If IPv6 end-to-end connectivity does not exist, then continue troubleshooting to resolve remaining issues.

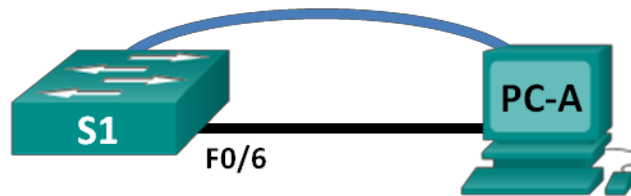
Note: It may be necessary to disable the PC firewall to ping between PCs.

Reflection

Why would you troubleshoot OSPFv2 and OSPFv3 separately?

Lab 6: 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 the switch 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 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, and static MAC address. You will also demonstrate 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 this lab.

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 a switch.

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)
- 1 Console cable to configure the Cisco IOS device via the console port
- 1 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. Connect the console cable as shown in the topology. Do not connect the PC-A Ethernet cable at this time.

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

- b. Connect 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), A console connection using Tera Term or other terminal emulation program will place you 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 that there is a clean default configuration file on the switch by issuing the **show running-config** privileged EXEC mode command. If a configuration file was previously saved, it must be removed.

Depending on the 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 a switch.

- 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 an Ethernet cable from PC-A 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 VLAN 1? _____

Is VLAN 1 active? _____

What type of VLAN is the default VLAN? _____ 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 will configure basic settings for the switch and PC.

Step 1: Configure basic switch settings.

- a. Copy the following basic configuration and paste it into S1 while in global configuration mode.

```
no ip domain-lookup
hostname S1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

- b. 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.

- c. 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.

- d. Issue the **show vlan brief** command to verify that all 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	

- e. Configure the 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. 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)#

```

- f. 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)#
```

- g. Configure the virtual terminal (vty) lines for the switch to allow Telnet access. If you do not configure a vty password, you will not be able 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.

Use the console connection on PC-A to display and verify the 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 is shown 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  
switchport access vlan 99  
!  
interface GigabitEthernet0/2  
switchport access vlan 99  
!  
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 the address of PC-A 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. Check both the physical cabling and logical addressing.

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 command window and type **pkgmgr /iu:"TelnetClient"**. An example is shown below.

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

- With the command 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
```
- After entering the password **cisco**, you will be at the user EXEC mode prompt. Access privileged EXEC mode using the **enable** command and providing the secret password **class**.
- 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 addresses 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.

Open a command prompt on PC-A and issue the **ipconfig /all** command to determine and record the Layer 2 (physical) addresses of the 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 MAC address of PC-A? _____

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

- Display the MAC address table options.

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

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

- 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? _____

- 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.

- Clear the MAC address table.

To remove the existing MAC addresses, use the **clear mac address-table dynamic** command in 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 of 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 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 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 password 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 Switch

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

```
Switch> enable
Switch#
```

- i. 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#
```

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

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

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

- l. You are prompted to confirm deletion of this file. Press Enter to confirm.

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

- m. 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#
```

- n. Reload the switch to remove any old configuration information from memory. You will then receive a prompt to confirm reloading of 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
```

- o. 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
```

Lab 16: 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 strong 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 this lab. 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)

- 1 Console cable to configure the Cisco IOS devices via the console ports
- 2 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 default configurations.

Part 2: Configure Basic Device Settings and Verify Connectivity

In Part 2, you will 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.

Refer to the Addressing Table for the IP Address information.

Step 2: Configure basic settings on R1.

- Console into R1 and enter global configuration mode.
- Copy the following basic configuration and paste it to running-configuration on R1.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
interface g0/1
 ip address 172.16.99.1 255.255.255.0
 no shutdown
end
```

- Save the running configuration to startup configuration.

Step 3: Configure basic settings on S1.

- Console into S1 and enter global configuration mode.
- Copy the following basic configuration and paste it to running-configuration on S1.

```
no ip domain-lookup
```

```
hostname S1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

- c. 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)#
```

- d. 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#
```

- e. Issue the **show vlan** command on S1. What is the status of VLAN 99? _____
- f. 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?

- g. 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
```

- h. Save the running configuration to startup configuration.
- i. 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.

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

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.**

- Enable SSH on S1. From global configuration mode, create a domain name of **CCNA-Lab.com**.
`S1(config)# ip domain-name CCNA-Lab.com`
- 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
```

- 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
```

- 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
```

- Verify the SSH configuration.

```
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? _____ Verify the SSH configuration on S1.

- a. Using the 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 **sshadmin** 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. Change the message of the day (MOTD) banner on S1 to, "Unauthorized access is strictly prohibited. Violators will be prosecuted to the full extent of the law."
- 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 and go to <http://172.16.99.11>. What was your result?
-

- h. From PC-A, open a web browser and go to <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 browser.

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 the next two steps. You will eventually see 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 privileged EXEC mode, ping PC-A. Was the ping successful? Why or why not?

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

```
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. On the switch, 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. The ping should be successful.

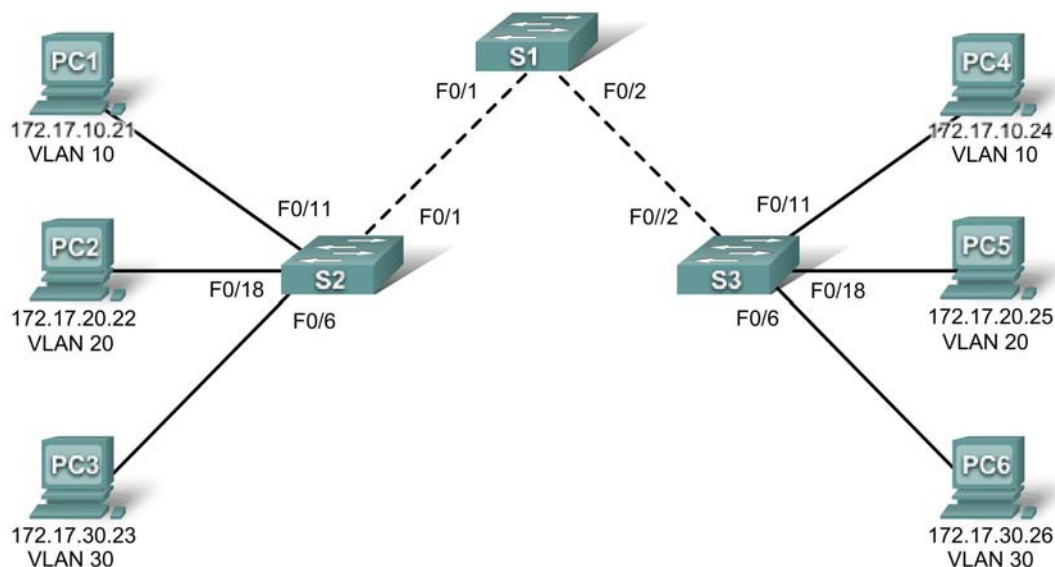
Reflection

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

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

Lab 17: Basic VLAN Configuration

Topology Diagram



Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	N/A
S2	VLAN 99	172.17.99.12	255.255.255.0	N/A
S3	VLAN 99	172.17.99.13	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1
PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1
PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1
PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1

Initial Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
0/5	Trunks (Native VLAN 99)	172.17.99.0 /24
0/10	30 – Guest (Default)	172.17.30.0 /24
1 – 0/17	10 – Faculty/Staff	172.17.10.0 /24
8 – 0/24	20 – Students	172.17.20.0 /24

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 switch to the default state
- Perform basic configuration tasks on a switch
- Create VLANs
- Assign switch ports to a VLAN
- Add, move, and change ports
- Verify VLAN configuration
- Enable trunking on inter-switch connections
- Verify trunk configuration
- Save the VLAN configuration

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 switch in your lab as long as it has the required interfaces shown in the topology. Note:

If you use 2900 or 2950 switches, the outputs may appear different. Also, certain commands may be different or unavailable.

Step 2: Clear any existing configurations on the switches, and initialize all ports in the shutdown state.

If necessary, refer to Lab 2.5.1, Appendix 1, for the procedure to clear switch configurations.

It is a good practice to disable any unused ports on the switches by putting them in shutdown. Disable all ports on the switches:

```
Switch#config term
Switch(config)#interface range fa0/1-24
Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range gi0/1-2
Switch(config-if-range)#shutdown
```

Task 2: Perform Basic Switch Configurations

Step 1: Configure the switches according to the following guidelines.

- Configure the switch hostname.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

Step 2: Re-enable the user ports on S2 and S3.

```
S2(config)#interface range fa0/6, fa0/11, fa0/18
S2(config-if-range)#switchport mode access
```

```
S2(config-if-range)#no shutdown
```

```
S3(config)#interface range fa0/6, fa0/11, fa0/18
S3(config-if-range)#switchport mode access
S3(config-if-range)#no shutdown
```

Task 3: Configure and Activate Ethernet Interfaces

Step 1: Configure the PCs.

You can complete this lab using only two PCs by simply changing the IP addressing for the two PCs specific to a test you want to conduct. For example, if you want to test connectivity between PC1 and PC2, then configure the IP addresses for those PCs by referring to the addressing table at the beginning of the lab. Alternatively, you can configure all six PCs with the IP addresses and default gateways.

Task 4: Configure VLANs on the Switch

Step 1: Create VLANs on switch S1.

Use the **vlan** *vlan-id* command in global configuration mode to add a VLAN to switch S1. There are four VLANs configured for this lab: VLAN 10 (faculty/staff); VLAN 20 (students); VLAN 30 (guest); and VLAN 99 (management). After you create the VLAN, you will be in vlan configuration mode, where you can assign a name to the VLAN with the **name** *vlan name* command.

```
S1(config)#vlan 10
S1(config-vlan)#name faculty/staff
S1(config-vlan)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#end
S1#
```

Step 2: Verify that the VLANs have been created on S1.

Use the **show vlan brief** command to verify that the VLANs have been created.

```
S1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, 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
10	faculty/staff	active	
20	students	active	
30	guest	active	
99	management	active	

Step 3: Configure and name VLANs on switches S2 and S3.

Create and name VLANs 10, 20, 30, and 99 on S2 and S3 using the commands from Step 1. Verify the correct configuration with the **show vlan brief** command.

What ports are currently assigned to the four VLANs you have created?

Step 4: Assign switch ports to VLANs on S2 and S3.

Refer to the port assignment table on page 1. Ports are assigned to VLANs in interface configuration mode, using the **switchport access vlan** *vlan-id* command. You can assign each port individually or you can use the **interface range** command to simplify this task, as shown here. The commands are shown for S3 only, but you should configure both S2 and S3 similarly. Save your configuration when done.

```
S3(config)#interface range fa0/6-10
S3(config-if-range)#switchport access vlan 30
S3(config-if-range)#interface range fa0/11-17
S3(config-if-range)#switchport access vlan 10
S3(config-if-range)#interface range fa0/18-24
S3(config-if-range)#switchport access vlan 20
S3(config-if-range)#end
S3#copy running-config startup-config Destination
filename [startup-config]? [enter] Building
configuration...
[OK]
```

Step 5: Determine which ports have been added.

Use the **show vlan id** *vlan-number* command on S2 to see which ports are assigned to VLAN 10. Which ports are assigned to VLAN 10?

Note: The **show vlan name** *vlan-name* displays the same output.

You can also view VLAN assignment information using the **show interfaces** *interface* **switchport** command.

Step 6: Assign the management VLAN.

A management VLAN is any VLAN that you configure to access the management capabilities of a switch. VLAN 1 serves as the management VLAN if you did not specifically define another VLAN. You assign the management VLAN an IP address and subnet mask. A switch can be managed via HTTP, Telnet, SSH, or SNMP. Because the out-of-the-box configuration of a Cisco switch has VLAN 1 as the default VLAN, VLAN 1 is a bad choice as the management VLAN. You do not want an arbitrary user who is connecting to a switch to default to the management VLAN. Recall that you configured the management VLAN as VLAN 99 earlier in this lab.

From interface configuration mode, use the **ip address** command to assign the management IP address to the switches.

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown

S2(config)#interface vlan 99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown

S3(config)#interface vlan 99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
```

```
S3(config-if)#no shutdown
```

Assigning a management address allows IP communication between the switches, and also allows any host connected to a port assigned to VLAN 99 to connect to the switches. Because VLAN 99 is configured as the management VLAN, any ports assigned to this VLAN are considered management ports and should be secured to control which devices can connect to these ports.

Step 7: Configure trunking and the native VLAN for the trunking ports on all switches.

Trunks are connections between the switches that allow the switches to exchange information for all VLANs.

By default, a trunk port belongs to all VLANs, as opposed to an access port, which can only belong to a single VLAN. If the switch supports both ISL and 802.1Q VLAN encapsulation, the trunks must specify which method is being used. Because the 2960 switch only supports 802.1Q trunking, it is not specified in this lab.

A native VLAN is assigned to an 802.1Q trunk port. In the topology, the native VLAN is VLAN 99. An 802.1Q trunk port supports traffic coming from many VLANs (tagged traffic) as well as traffic that does not come from a VLAN (untagged traffic). The 802.1Q trunk port places untagged traffic on the native VLAN. Untagged traffic is generated by a computer attached to a switch port that is configured with the native VLAN. One of the IEEE 802.1Q specifications for Native VLANs is to maintain backward compatibility with untagged traffic common to legacy LAN scenarios. For the purposes of this lab, a native VLAN serves as a common identifier on opposing ends of a trunk link. It is a best practice to use a VLAN other than VLAN 1 as the native VLAN.

Use the **interface range** command in global configuration mode to simplify configuring trunking.

```
S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end

S2(config)# interface range fa0/1-5
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end

S3(config)# interface range fa0/1-5
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

Verify that the trunks have been configured with the **show interface trunk** command.

```
S1#show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	99
Fa0/2	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Fa0/1	1-4094
Fa0/2	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,30,99
Fa0/2	1,10,20,30,99

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,10,20,30,99
Fa0/2	1,10,20,30,99

Step 8: Verify that the switches can communicate.

From S1, ping the management address on both S2 and S3.

```
S1#ping 172.17.99.12
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms

S1#**ping 172.17.99.13**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.17.99.13, timeout is 2 seconds:

!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

Step 9: Ping several hosts from PC2.

Ping from host PC2 to host PC1 (172.17.10.21). Is the ping attempt successful? _____

Ping from host PC2 to the switch VLAN 99 IP address 172.17.99.12. Is the ping attempt successful?

Because these hosts are on different subnets and in different VLANs, they cannot communicate without a Layer 3 device to route between the separate subnetworks.

Ping from host PC2 to host PC5. Is the ping attempt successful? _____

Because PC2 is in the same VLAN and the same subnet as PC5, the ping is successful

Step 10: Move PC1 into the same VLAN as PC2.

The port connected to PC2 (S2 Fa0/18) is assigned to VLAN 20, and the port connected to PC1 (S2 Fa0/11) is assigned to VLAN 10. Reassign the S2 Fa0/11 port to VLAN 20. You do not need to first remove a port from a VLAN to change its VLAN membership. After you reassign a port to a new VLAN, that port is automatically removed from its previous VLAN.

S2#**configure terminal**

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

S2(config)#**interface fastethernet 0/11**

S2(config-if)#**switchport access vlan 20**

S2(config-if)#**end**

Ping from host PC2 to host PC1. Is the ping attempt successful? _____

Even though the ports used by PC1 and PC2 are in the same VLAN, they are still in different subnetworks, so they cannot communicate directly.

Step 11: Change the IP address and network on PC1.

Change the IP address on PC1 to 172.17.20.21. The subnet mask and default gateway can remain the same. Once again, ping from host PC2 to host PC1, using the newly assigned IP address.

Is the ping attempt successful? _____ Why

was this attempt successful?

Task 5: Document the Switch Configurations

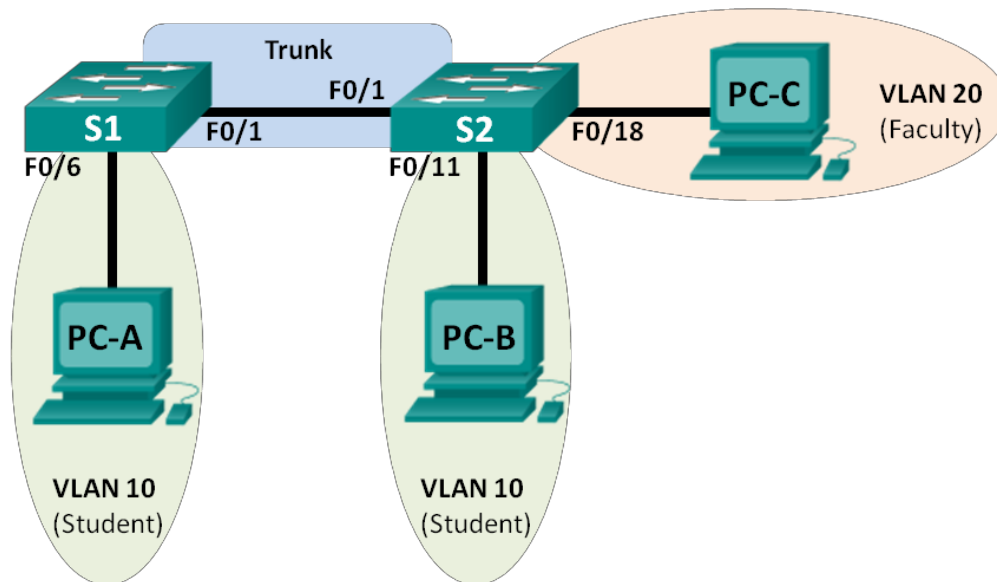
On each switch, capture the running configuration to a text file and save it for future reference.

Task 6: Clean Up

Erase the configurations and reload the switches. 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.

Lab 18: Configuring VLANs and Trunking

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Create VLANs and Assign Switch Ports

Part 3: Maintain VLAN Port Assignments and the VLAN Database

Part 4: Configure an 802.1Q Trunk between the Switches

Part 5: Delete the VLAN Database

Background / Scenario

Modern switches use virtual local-area networks (VLANs) to improve network performance by separating large Layer 2 broadcast domains into smaller ones. VLANs can also be used as a security measure by controlling which hosts can communicate. In general, VLANs make it easier to design a network to support the goals of an organization.

VLAN trunks are used to span VLANs across multiple devices. Trunks allow the traffic from multiple VLANs to travel over a single link, while keeping the VLAN identification and segmentation intact.

In this lab, you will create VLANs on both switches in the topology, assign VLANs to switch access ports,

verify that VLANs are working as expected, and then create a VLAN trunk between the two switches to allow hosts in the same VLAN to communicate through the trunk, regardless of which switch the host is actually attached to.

Note: The switches used are Cisco Catalyst 2960s 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: Ensure that the switches have been erased and have no startup configurations. If you are unsure contact your instructor.

Required Resources

- 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 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 on the PC hosts and switches.

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

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Initialize and reload the switches as necessary.

Step 3: Configure basic settings for each switch.

- a. Console into the switch and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on the switch.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
logging synchronous
login
exit
```

- c. Configure the host name as shown in the topology.
- d. Configure the IP address listed in the Addressing Table for VLAN 1 on the switch.
- e. Administratively deactivate all unused ports on the switch.
- f. 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.

Verify that the PC hosts can ping one another.

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

Can PC-A ping PC-B? _____

Can PC-A ping PC-C? _____

Can PC-A ping S1? _____ Can

PC-B ping PC-C? _____ Can

PC-B ping S2? _____ Can

PC-C ping S2? _____ Can

S1 ping S2? _____

If you answered no to any of the above questions, why were the pings unsuccessful?

Part 2: Create VLANs and Assign Switch Ports

In Part 2, you will create student, faculty, and management VLANs on both switches. You will then assign the VLANs to the appropriate interface. The **show vlan** command is used to verify your configuration settings.

Step 1: Create VLANs on the switches.

- a. Create the VLANs on S1.

```
S1(config)# vlan 10
S1(config-vlan)# name Student
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# end
```

- b. Create the same VLANs on S2.

- c. Issue the **show vlan** command to view the list of VLANs on S1.

```
S1# show vlan
```

VLAN	Name	Status	Ports
1	default	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

10 Student active

20 Faculty active

99 Management active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
99	enet	100099	1500	-	-	-	-	-	0	0

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

Remote SPAN VLANs

Primary Secondary Type Ports

What is the default VLAN? _____

What ports are assigned to the default VLAN?

Step 2: Assign VLANs to the correct switch interfaces.

- a. Assign VLANs to the interfaces on S1.

- 1) Assign PC-A to the Student VLAN.

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

- 2) Move the switch IP address VLAN 99.

```
S1(config)# interface vlan 1
S1(config-if)# no ip address
S1(config-if)# interface vlan 99
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# end
```

- b. Issue the **show vlan brief** command and verify that the VLANs are assigned to the correct interfaces.

S1# **show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, 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
10	Student	active	Fa0/6
20	Faculty	active	
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

- c. Issue the **show ip interface brief** command.

What is the status of VLAN 99? Why?

- d. Use the Topology to assign VLANs to the appropriate ports on S2.
 e. Remove the IP address for VLAN 1 on S2.
 f. Configure an IP address for VLAN 99 on S2 according to the Addressing Table.
 g. Use the **show vlan brief** command to verify that the VLANs are assigned to the correct interfaces.

S2# **show vlan brief**

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

Is PC-A able to ping PC-B? Why?

Is S1 able to ping S2? Why?

Part 3: Maintain VLAN Port Assignments and the VLAN Database

In Part 3, you will change VLAN assignments to ports and remove VLANs from the VLAN database.

Step 1: Assign a VLAN to multiple interfaces.

- On S1, assign interfaces F0/11 – 24 to VLAN 10.

```
S1(config)# interface range f0/11-24
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# end
```
- Issue the **show vlan brief** command to verify VLAN assignments.
- Reassign F0/11 and F0/21 to VLAN 20.
- Verify that VLAN assignments are correct.

Step 2: Remove a VLAN assignment from an interface.

- Use the **no switchport access vlan** command to remove the VLAN 10 assignment to F0/24.

```
S1(config)# interface f0/24
S1(config-if)# no switchport access vlan
S1(config-if)# end
```
- Verify that the VLAN change was made.
 Which VLAN is F0/24 now associated with?

Step 3: Remove a VLAN ID from the VLAN database.

- Add VLAN 30 to interface F0/24 without issuing the VLAN command.

```
S1(config)# interface f0/24
S1(config-if)# switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
```

Note: Current switch technology no longer requires that the **vlan** command be issued to add a VLAN to the database. By assigning an unknown VLAN to a port, the VLAN adds to the VLAN database.

- Verify that the new VLAN is displayed in the VLAN table.

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Gi0/1, Gi0/2
10	Student	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/22, Fa0/23
20	Faculty	active	Fa0/11, Fa0/21
30	VLAN0030	active	Fa0/24
99	Management	active	

```

1002 fddi-default          act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default         act/unsup

```

What is the default name of VLAN 30?

- c. Use the **no vlan 30** command to remove VLAN 30 from the VLAN database.

```

S1(config)# no vlan 30
S1(config)# end

```

- d. Issue the **show vlan brief** command. F0/24 was assigned to VLAN 30.

After deleting VLAN 30, what VLAN is port F0/24 assigned to? What happens to the traffic destined to the host attached to F0/24?

S1# **show vlan brief**

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

- e. Issue the **no switchport access vlan** command on interface F0/24.
- f. Issue the **show vlan brief** command to determine the VLAN assignment for F0/24. To which VLAN is F0/24 assigned?
-

Note: Before removing a VLAN from the database, it is recommended that you reassign all the ports assigned to that VLAN.

Why should you reassign a port to another VLAN before removing the VLAN from the VLAN database?

Part 4: Configure an 802.1Q Trunk Between the Switches

In Part 4, you will configure interface F0/1 to use the Dynamic Trunking Protocol (DTP) to allow it to negotiate the trunk mode. After this has been accomplished and verified, you will disable DTP on interface F0/1 and manually configure it as a trunk.

Step 1: Use DTP to initiate trunking on F0/1.

The default DTP mode of a 2960 switch port is dynamic auto. This allows the interface to convert the link to a

trunk if the neighboring interface is set to trunk or dynamic desirable mode.

- a. Set F0/1 on S1 to negotiate trunk mode.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode dynamic desirable
*Mar 1 05:07:28.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to down
*Mar 1 05:07:29.744: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
S1(config-if)#
*Mar 1 05:07:32.772: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
S1(config-if)#
*Mar 1 05:08:01.789: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
*Mar 1 05:08:01.797: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

You should also receive link status messages on S2.

```
S2#
*Mar 1 05:07:29.794: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
S2#
*Mar 1 05:07:32.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
S2#
*Mar 1 05:08:01.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
*Mar 1 05:08:01.850: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

- b. Issue the **show vlan brief** command on S1 and S2. Interface F0/1 is no longer assigned to VLAN 1. Trunked interfaces are not listed in the VLAN table.

S1# **show vlan brief**

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

- c. Issue the **show interfaces trunk** command to view trunked interfaces. Notice that the mode on S1 is set to desirable, and the mode on S2 is set to auto.

S1# **show interfaces trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	desirable	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,99

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,10,20,99

S2# **show interfaces trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	auto	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,99

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,10,20,99

Note: By default, all VLANs are allowed on a trunk. The **switchport trunk** command allows you to control what VLANs have access to the trunk. For this lab, keep the default settings which allows all VLANs to traverse F0/1.

- d. Verify that VLAN traffic is traveling over trunk interface F0/1.

Can S1 ping S2? _____ Can

PC-A ping PC-B? _____ Can

PC-A ping PC-C? _____ Can

PC-B ping PC-C? _____ Can

PC-A ping S1? _____

Can PC-B ping S2? _____

Can PC-C ping S2? _____

If you answered no to any of the above questions, explain below.

Step 2: Manually configure trunk interface F0/1.

The **switchport mode trunk** command is used to manually configure a port as a trunk. This command should be issued on both ends of the link.

- a. Change the switchport mode on interface F0/1 to force trunking. Make sure to do this on both switches.

S1(config)# **interface f0/1**

```
S1(config-if)# switchport mode trunk
```

- b. Issue the **show interfaces trunk** command to view the trunk mode. Notice that the mode changed from **desirable** to **on**.

```
S2# show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Fa0/1	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,99

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,10,20,99

Why might you want to manually configure an interface to trunk mode instead of using DTP?

Part 5: Delete the VLAN Database

In Part 5, you will delete the VLAN Database from the switch. It is necessary to do this when initializing a switch back to its default settings.

Step 1: Determine if the VLAN database exists.

Issue the **show flash** command to determine if a **vlan.dat** file exists in flash.

```
S1# show flash
```

```
Directory of flash:/
```

2	-rwx	1285	Mar 1 1993 00:01:24 +00:00	config.text
3	-rwx	43032	Mar 1 1993 00:01:24 +00:00	multiple-fs
4	-rwx	5	Mar 1 1993 00:01:24 +00:00	private-config.text
5	-rwx	11607161	Mar 1 1993 02:37:06 +00:00	c2960-lanbasek9-mz.150-2.SE.bin
6	-rwx	736	Mar 1 1993 00:19:41 +00:00	vlan.dat

```
32514048 bytes total (20858880 bytes free)
```

Note: If there is a **vlan.dat** file located in flash, then the VLAN database does not contain its default settings.

Step 2: Delete the VLAN database.

- a. Issue the **delete vlan.dat** command to delete the **vlan.dat** file from flash and reset the VLAN database back to its default settings. You will be prompted twice to confirm that you want to delete the **vlan.dat** file. Press Enter both times.

```
S1# delete vlan.dat
```

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

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

S1#

- b. Issue the **show flash** command to verify that the vlan.dat file has been deleted.

S1# **show flash**

Directory of flash:/

2	-rwx	1285	Mar 1 1993 00:01:24 +00:00	config.text
3	-rwx	43032	Mar 1 1993 00:01:24 +00:00	multiple-fs
4	-rwx	5	Mar 1 1993 00:01:24 +00:00	private-config.text
5	-rwx	11607161	Mar 1 1993 02:37:06 +00:00	c2960-lanbasek9-mz.150-2.SE.bin

32514048 bytes total (20859904 bytes free)

To initialize a switch back to its default settings, what other commands are needed?

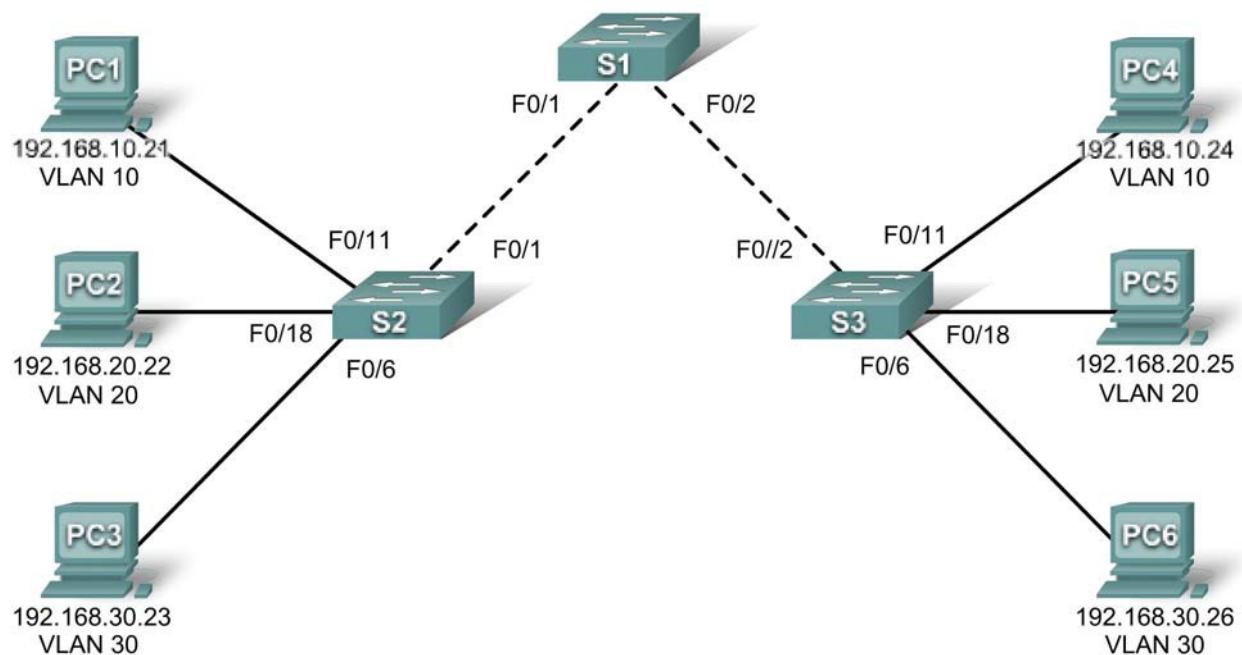
Reflection

1. What is needed to allow hosts on VLAN 10 to communicate to hosts on VLAN 20?

2. What are some primary benefits that an organization can receive through effective use of VLANs?

Lab 19: Challenge VLAN Configuration

Topology Diagram



Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 56	192.168.56.11	255.255.255.0	N/A
S2	VLAN 56	192.168.56.12	255.255.255.0	N/A
S3	VLAN 56	192.168.56.13	255.255.255.0	N/A
PC1	NIC	192.168.10.21	255.255.255.0	192.168.10.1
PC2	NIC	192.168.20.22	255.255.255.0	192.168.20.1
PC3	NIC	192.168.30.23	255.255.255.0	192.168.30.1
PC4	NIC	192.168.10.24	255.255.255.0	192.168.10.1
PC5	NIC	192.168.20.25	255.255.255.0	192.168.20.1
PC6	NIC	192.168.30.26	255.255.255.0	192.168.30.1

Initial Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks (Native VLAN 56)	192.168.56.0 /24
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	192.168.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	192.168.10.0 /24

Fa0/18 – 0/24	VLAN 20 – Students	192.168.20.0 /24
---------------	--------------------	------------------

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 switch to the default state
- Perform basic configuration tasks on a switch
- Create VLANs
- Assign switch ports to a VLAN
- Add, move, and change ports
- Verify VLAN configuration
- Enable trunking on inter-switch connections
- Verify trunk configuration
- Save the VLAN configuration

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear any existing configurations on the switches, and initialize all ports in the shutdown state.

Task 2: Perform Basic Switch Configurations

Step 1: Configure the switches according to the following guidelines.

- Configure the switch hostname.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

Step 2: Re-enable the user ports on S2 and S3.

Task 3: Configure and Activate Ethernet Interfaces

Step 1: Configure the PCs.

Configure the Ethernet interfaces of the six PCs with the IP addresses and default gateways from the addressing table at the beginning of the lab.

Task 4: Configure VLANs on the Switch

Step 1: Create VLANs on switch S1.

Step 2: Verify that the VLANs have been created on S1.

Step 3: Configure, name, and verify VLANs on switches S2 and S3. Step

4: Assign switch ports to VLANs on S2 and S3.

Step 5: Determine which ports have been added to VLAN 10 on S2.

Step 6: Configure management VLAN 56 on each of the switches. Use the IP addresses indicated in the Addressing Table.

Step 7: Configure trunking and the native VLAN for the trunking ports on all three switches. Verify that the trunks have been configured.

Step 8: Verify that S1, S2, and S3 can communicate.

Step 9: Ping several hosts from PC2. What is the result?

Step 10: Move PC1 into the same VLAN as PC2. Can PC1 successfully ping PC2?

Step 11: Change the IP address on PC1 to 192.168.20.21. Can PC1 successfully ping PC2?

Change the IP address on PC1 to 192.168.20.21. The default gateway should be changed to 192.168.20.1. Once again, ping from host PC2 to host PC1, using the newly assigned IP address. Is the ping attempt successful?

Why was this attempt successful?

Task 5: Document the Switch Configurations

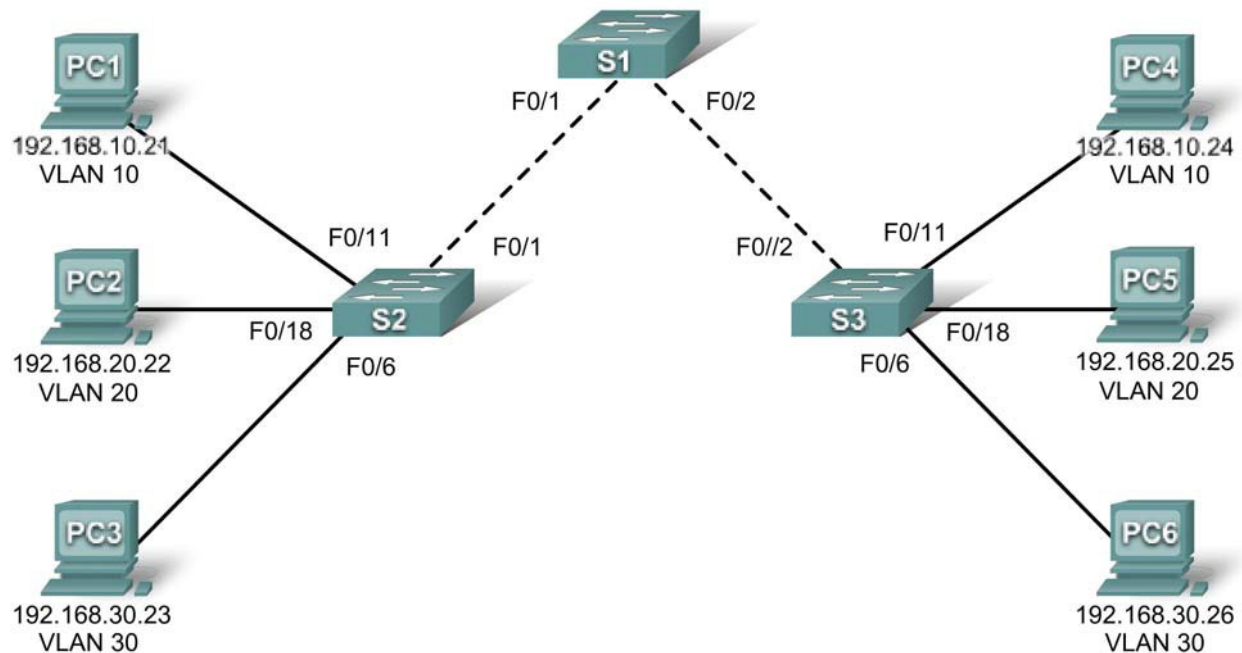
On each switch, capture the running configuration to a text file and save it for future reference.

Task 6: Clean Up

Erase the configurations and reload the switches. 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.

Lab 20: Troubleshooting VLAN Configurations

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN	192.168.56.11	255.255.255.0	N/A
S2	VLAN	192.168.56.12	255.255.255.0	N/A
S3	VLAN	192.168.56.13	255.255.255.0	N/A
PC	NI	192.168.10.21	255.255.255.0	192.168.10.1
PC	NI	192.168.20.22	255.255.255.0	192.168.20.1
PC	NI	192.168.30.23	255.255.255.0	192.168.30.1
PC	NI	192.168.10.24	255.255.255.0	192.168.10.1
PC	NI	192.168.20.25	255.255.255.0	192.168.20.1
PC	NI	192.168.30.26	255.255.255.0	192.168.30.1

Initial Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks (Native VLAN 56)	192.168.56.0 /24
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	192.168.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	192.168.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Students	192.168.20.0 /24

Learning Objective

Practice basic VLAN troubleshooting skills.

Scenario

In this lab, you will practice troubleshooting a misconfigured VLAN environment. Load or have your instructor load the configurations below into your lab gear. Your objective is to locate and correct any and all errors in the configurations and establish end-to-end connectivity. Your final configuration should match the topology diagram and addressing table. All passwords are set to **cisco**, except the enable secret password, which is set to **class**.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear any existing configurations on the switches, and initialize all ports in the shutdown state.

Step 3: Import the configurations below.

Switch 1

```
hostname S1
no ip domain-lookup
enable secret class
!
!
interface range FastEthernet0/1-5
switchport mode trunk
!
interface range FastEthernet0/6-24
shutdown
!
interface Vlan1
no ip address
no ip route-cache
!
interface Vlan56
ip address 192.168.56.11 255.255.255.0
no ip route-cache
!
line con 0
logging synchronous
line vty 0 4
no login
line vty 5 15
password cisco
login
!
end
```

Switch 2

```
hostname S2
no ip domain-lookup
enable secret class
!
vlan 10,20,30,56
```

```
!  
interface range FastEthernet0/1-5  
switchport trunk native vlan 56  
switchport mode access  
!  
interface range FastEthernet0/6-10  
switchport access vlan 30 switchport  
mode access  
!  
interface range FastEthernet0/11-17  
switchport access vlan 10 switchport  
mode access  
!  
interface range FastEthernet0/18-24  
switchport access vlan 20 switchport  
mode access  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
ip address 192.168.56.12 255.255.255.0 no  
ip route-cache  
shutdown  
!  
line con 0  
password cisco  
login  
line vty 0 4  
password cisco  
login  
line vty 5 15  
password cisco  
login  
!  
end
```

Switch 3

```
hostname S3  
no ip domain-lookup  
enable secret class  
!  
vlan 10,20,30  
!  
interface range FastEthernet0/1-5  
switchport trunk native vlan 56  
switchport mode trunk  
!  
interface range FastEthernet0/6-10  
switchport mode access  
!  
interface range FastEthernet0/11-17  
switchport mode access  
!  
interface range FastEthernet0/18-24
```

```
switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
no ip route-cache
shutdown
!
interface Vlan56
no ip route-cache
!
line con 0
password cisco
login
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
end
```

Task 2: Troubleshoot and Repair the VLAN Configuration

Task 3: Document the Switch Configurations

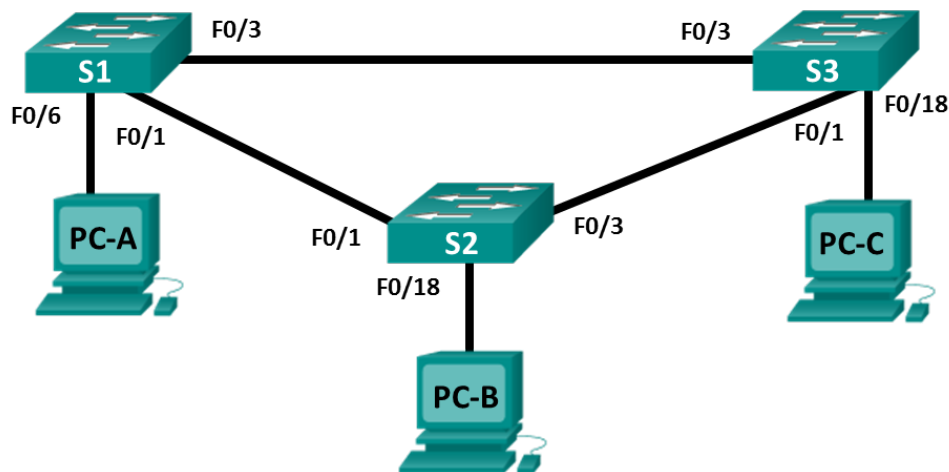
On each switch, capture the running configuration to a text file and save for future reference:

Task 4: Clean Up

Erase the configurations and reload the switches. 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.

Lab 21: Configure Extended VLANs, VTP, and DTP

Topology



Addressing Table

Table Heading	Interface	IP Address	Subnet Mask
S1	VLAN 99	192.168.99.1	255.255.255.0
S2	VLAN 99	192.168.99.2	255.255.255.0
S3	VLAN 99	192.168.99.3	255.255.255.0
PC-A	NIC	192.168.10.1	255.255.255.0
PC-B	NIC	192.168.20.1	255.255.255.0
PC-C	NIC	192.168.10.2	255.255.255.0

Objectives

Part 1: Configure VTP

Part 2: Configure DTP

Part 3: Add VLANs and Assign Ports

Part 4: Configure Extended VLAN

Background / Scenario

It can become challenging to manage VLANs and trunks in a network, as the number of switches increases. VLAN trunking protocol (VTP) allows a network administrator to automate the management of VLANs. Automated trunk negotiation between network devices is managed by the Dynamic Trunking Protocol (DTP). DTP is enabled by default on Catalyst 2960 and Catalyst 3560 switches.

In this lab, you will configure trunk links between the switches. You will also configure a VTP server and VTP clients in the same VTP domain. Furthermore, you will configure an extended VLAN on one of the switches, assign ports to VLANs and verify end-to-end connectivity within the same VLAN.

Note: The switches used are Cisco Catalyst 2960s 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 switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7 or 8 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: Configure VTP

All the switches will be configured to use VTP for VLAN updates. S2 will be configured as the server. Switches S1 and S3 will be configured as clients. They will be in the **CCNA** VTP domain using the password **cisco**.

- a. Configure S2 as a VTP server in the **CCNA** VTP domain using **cisco** as the VTP password.

```
S2(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S2(config)#
*Mar  1 00:03:44.193: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to CCNA.
S2(config)# vtp mode server
Device mode already VTP Server for VLANs.
S2(config)# vtp password cisco
Setting device VTP password to cisco
```

- b. Configure S1 and S3 as VTP clients in the **CCNA** VTP domain using **cisco** as the VTP password. VTP configurations are displayed below.

```
S1(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S1(config)#
*Mar  1 00:03:44.193: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to CCNA.
S1(config)# vtp mode client
Device mode VTP client for VLANs.
S1(config)# vtp password cisco
Setting device VTP password to cisco
```

- c. Verify VTP configurations by entering the **show vtp status** command on all switches. The VTP status for S3 is displayed below.

```
S3# show vtp status
VTP Version capable           : 1 to 3
VTP version running           : 1
VTP Domain Name                : CCNA
VTP Pruning Mode               : Disabled
VTP Traps Generation          : Disabled
Device ID                      : 0cd9.96d2.3580
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:
-----
VTP Operating Mode             : Client
```

```

Maximum VLANs supported locally    : 255
Number of existing VLANs          : 5
Configuration Revision             : 0
MD5 digest                        : 0x8B 0x58 0x3D 0x9D 0x64 0xBE 0xD5 0xF6
                                   0x62 0xCB 0x4B 0x50 0xE5 0x9C 0x6F 0xF6
  
```

Part 2: Configure DTP

Step 1: Configure dynamic trunk links between S1 and S2.

- a. Enter the **show interfaces f0/1 switchport** command on S1 and S2.

What is the administrative and operational mode of switchport f0/1?

- b. In interface configuration mode, configure a dynamic trunk link between S1 and S2. Because the default mode is dynamic auto, only one side of the link needs to be configured as dynamic desirable.

```

S1(config)# interface f0/1
S1(config-if)# switchport mode dynamic desirable
S1(config-if)#
*Mar 1 00:30:45.082: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
*Mar 1 00:30:48.102: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
  
```

- c. Verify trunking link between S1 and S2 using the **show interfaces trunk** command.

S1# **show interfaces trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	desirable	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	none

S2# **show interfaces trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	auto	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	none

Fa0/1 1

Step 2: Configure static trunk link between S1 and S3.

- a. Between S1 and S3, configure a static trunk link using the **switchport mode trunk** command in the interface configuration mode for port F0/3.

```
S1(config)# interface f0/3
S1(config-if)# switchport mode trunk
```

- b. Verify the trunks using **show interfaces trunk** command on S1.

```
S1# show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	desirable	802.1q	trunking	1
Fa0/3	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	1-4094
Fa0/3	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1
Fa0/3	1

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	none
Fa0/3	none

- c. Configure a permanent trunk between S2 and S3.
 d. Record the commands you used to create the static trunk.

Part 3: Add VLANs and Assign Ports

Step 1: Add VLANs on the switches.

- a. On S1, add VLAN 10.

```
S1(config)# vlan 10
```

Were you able to create VLAN 10 on S1? Explain.

- b. On S2, add the following VLANs.

VLAN	Name
10	Red
20	Blue
30	Yellow
99	Management

```
S2(config)# vlan 10
```

```
S2(config-vlan)# name Red
S2(config-vlan)# vlan 20
S2(config-vlan)# name Blue
S2(config-vlan)# vlan 30
S2(config-vlan)# name Yellow
S2(config-vlan)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# end
```

```
S2# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, 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
10	Red	active	
20	Blue	active	
30	Yellow	active	
99	Management	active	

<output omitted>

Step 2: Verify VTP updates on S1 and S3.

Because S2 is configured as a VTP server, and S1 and S3 are configured as VTP clients, S1 and S3 should learn and implement the VLAN information from S2.

What **show** commands did you use to verify the VTP updates on S1 and S3?

Step 3: Assign ports to VLANs.

In this step, you will associate ports to VLANs and configure IP addresses according to the table below.

Port Assignment	VLAN	Attached PC IP Address and Prefix
S1 F0/6	VLAN 10	PC-A: 192.168.10.1 / 24
S2 F0/18	VLAN 20	PC-B: 192.168.20.1 / 24
S3 F0/18	VLAN 10	PC-C: 192.168.10.2 / 24

- a. On S1, configure F0/6 to access mode and assign F0/6 to VLAN 10.

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

- b. Repeat the procedure for switchport F0/18 on S2 and S3. Assign the VLAN according to the table above.
 c. Assign the IP addresses to the PCs according to the table above.

Step 4: Configure IP addresses on the switches.

- a. On S1, assign an IP address to the SVI for VLAN 99 according to the Addressing Table and activate the interface.

```
S1(config)# interface vlan 99
S1(config-if)# ip address 192.168.99.1 255.255.255.0
S1(config-fi)# no shutdown
```

- b. Repeat step a. for S2 and S3.

Step 5: Verify end-to-end connectivity

- a. Ping PC-A from PC-B. Was it successful? Explain.

- b. Ping PC-A from PC-C. Was it successful? Explain.

- c. Ping PC-A from S1. Was it successful? Explain.

- d. Ping S1 from S2. Was it successful? Explain.

Part 4: Configure Extended VLAN

An extended VLAN is a VLAN between 1025 and 4096. Because the extended VLANs cannot be managed with VTP, VTP must be configured in transparent mode. In this part, you will change the VTP mode on S1 to transparent and create an extended VLAN on S1.

Step 1: Configure VTP mode to transparent on S1.

- a. On switch S1, set VTP mode to transparent.

```
S1(config)# vtp mode transparent
Setting device to VTP Transparent mode for VLANs.
S1(config)# exit
```

- b. Verify the VTP mode on S1.

```
S1# show vtp status
VTP Version capable      : 1 to 3
VTP version running      : 1
VTP Domain Name          : CCNA
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0cd9.96e2.3d00
Configuration last modified by 0.0.0.0 at 3-1-93 02:36:11
```

Feature VLAN:

```
VTP Operating Mode       : Transparent
Maximum VLANs supported locally : 255
Number of existing VLANs   : 9
Configuration Revision     : 0
MD5 digest                : 0xB2 0x9A 0x11 0x5B 0xBF 0x2E 0xBF 0xAA
```

0x31 0x18 0xFF 0x2C 0x5E 0x54 0x0A 0xB7

Step 2: Configure an extended VLAN on S1.

- Display the current VLAN configurations on S1.
- Create an extended VLAN 2000.

S1# **conf t**

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

S1(config)# **vlan 2000**S1(config-vlan)# **end**

- Verify the VLAN creation.

S1# **show vlan brief**

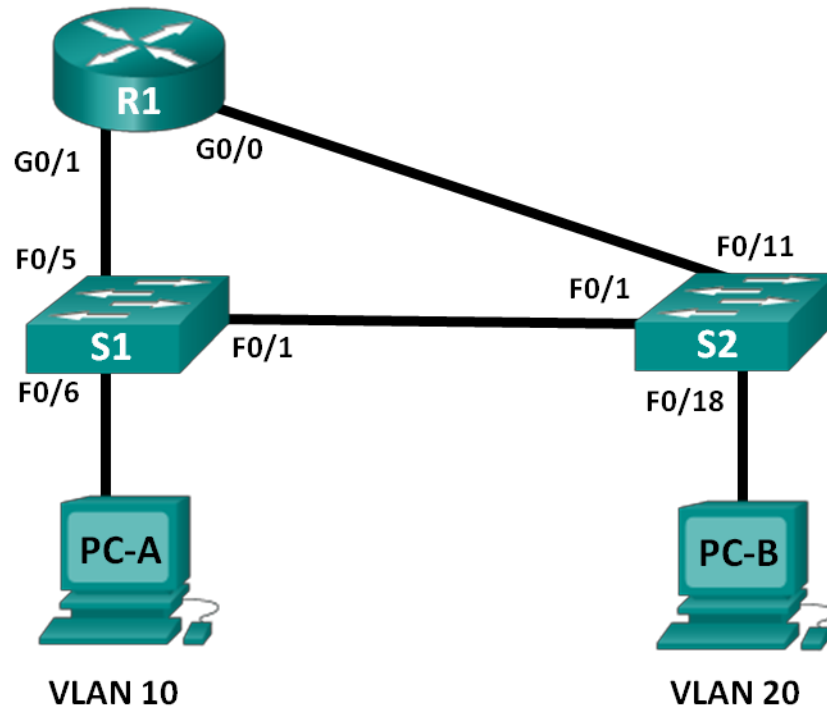
VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/4, Fa0/5, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gi0/1, Gi0/2
10	Red	active	Fa0/6
20	Blue	active	
30	Yellow	active	
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	
2000	VLAN2000	active	

Reflection

What are the advantages and disadvantages of using VTP?

Lab 22: Configuring Per-Interface Inter-VLAN Routing

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.20.1	255.255.255.0	N/A
	G0/1	192.168.10.1	255.255.255.0	N/A
S1	VLAN 10	192.168.10.11	255.255.255.0	192.168.10.1
S2	VLAN 10	192.168.10.12	255.255.255.0	192.168.10.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure Switches with VLANs and Trunking

Part 3: Verify Trunking, VLANs, Routing, and Connectivity

Background / Scenario

Legacy inter-VLAN routing is seldom used in today's networks; however, it is helpful to configure and understand this type of routing before moving on to router-on-a-stick (trunk-based) inter-VLAN routing or configuring Layer-3 switching. Also, you may encounter per-interface inter-VLAN routing in organizations with

very small networks. One of the benefits of legacy inter-VLAN routing is ease of configuration.

In this lab, you will set up one router with two switches attached via the router Gigabit Ethernet interfaces. Two separate VLANs will be configured on the switches, and you will set up routing between the VLANs.

Note: This lab provides minimal assistance with the actual commands necessary to configure the router and switches. The required switch VLAN configuration commands are provided in Appendix A of this lab. 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

- 1 Router (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 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 clear any configurations, if necessary.

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

Step 2: Initialize and reload the router and switches.

Step 3: Configure basic settings for R1.

- a. Console into R1 and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on R1.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

- c. Configure addressing on G0/0 and G0/1 and enable both interfaces.

- d. Copy the running configuration to the startup configuration.

Step 4: Configure basic settings on both switches.

- a. Console into the switch and enter global configuration mode.
- b. Copy the following basic configuration and paste it to running-configuration on the switch.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

- c. Configure the host name as shown in the topology.
- d. Copy the running configuration to the startup configuration.

Step 5: Configure basic settings on PC-A and PC-B.

Configure PC-A and PC-B with IP addresses and a default gateway address according to the Addressing Table.

Part 2: Configure Switches with VLANs and Trunking

In Part 2, you will configure the switches with VLANs and trunking.

Step 1: Configure VLANs on S1.

- a. On S1, create VLAN 10. Assign **Student** as the VLAN name.
- b. Create VLAN 20. Assign **Faculty-Admin** as the VLAN name.
- c. Configure F0/1 as a trunk port.
- d. Assign ports F0/5 and F0/6 to VLAN 10 and configure both F0/5 and F0/6 as access ports.
- e. Assign an IP address to VLAN 10 and enable it. Refer to the Addressing Table.
- f. Configure the default gateway according to the Addressing Table.

Step 2: Configure VLANs on S2.

- a. On S2, create VLAN 10. Assign **Student** as the VLAN name.
- b. Create VLAN 20. Assign **Faculty-Admin** as the VLAN name.
- c. Configure F0/1 as a trunk port.
- d. Assign ports F0/11 and F0/18 to VLAN 20 and configure both F0/11 and F0/18 as access ports.
- e. Assign an IP address to VLAN 10 and enable it. Refer to the Addressing Table.
- f. Configure the default gateway according to the Addressing Table.

Part 3: Verify Trunking, VLANs, Routing, and Connectivity

Step 1: Verify the R1 routing table.

- a. On R1, issue the **show ip route** command. What routes are listed on R1?

- b. On both S1 and S2, issue the **show interface trunk** command. Is the F0/1 port on both switches set to trunk? _____
- c. Issue a **show vlan brief** command on both S1 and S2. Verify that VLANs 10 and 20 are active and that the proper ports on the switches are in the correct VLANs. Why is F0/1 not listed in any of the active VLANs?

- d. Ping from PC-A in VLAN 10 to PC-B in VLAN 20. If Inter-VLAN routing is functioning correctly, the pings between the 192.168.10.0 network and the 192.168.20.0 should be successful.

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

- e. Verify connectivity between devices. You should be able to ping between all devices. Troubleshoot if you are not successful.

Reflection

What is an advantage of using legacy inter-VLAN routing?

Appendix A: Configuration Commands

Switch S1

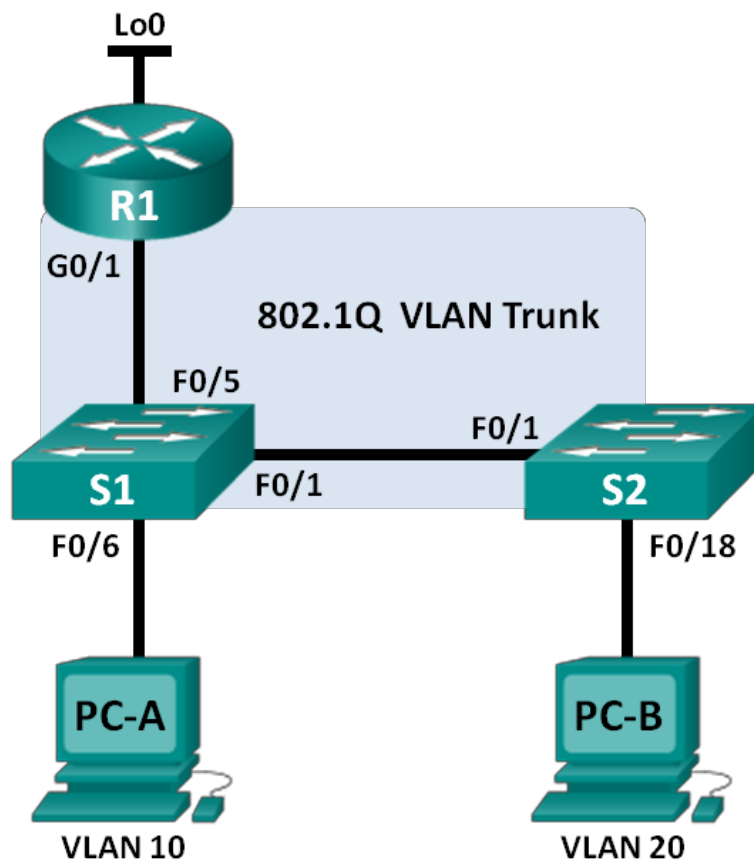
```
S1(config)# vlan 10
S1(config-vlan)# name
Student S1(config-vlan)#
exit S1(config)# vlan 20
S1(config-vlan)# name Faculty-Admin
S1(config-vlan)# exit
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# interface range f0/5 - 6
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# interface vlan 10
S1(config-if)# ip address 192.168.10.11 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.10.1
```

Switch S2

```
S2(config)# vlan 10
S2(config-vlan)# name Student
S2(config-vlan)# exit
S2(config)# vlan 20
S2(config-vlan)# name Faculty-Admin
S2(config-vlan)# exit
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
S2(config-if)# interface f0/11
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if-range)# interface vlan 10
S2(config-if)#ip address 192.168.10.12 255.255.255.0
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.10.1
```

Lab 22: Configuring 802.1Q Trunk-Based Inter-VLAN Routing

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1.1	192.168.1.1	255.255.255.0	N/A
	G0/1.10	192.168.10.1	255.255.255.0	N/A
	G0/1.20	192.168.20.1	255.255.255.0	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Switch Port Assignment Specifications

Ports	Assignment	Network
S1 F0/1	802.1Q Trunk	N/A
S2 F0/1	802.1Q Trunk	N/A
S1 F0/5	802.1Q Trunk	N/A
S1 F0/6	VLAN 10 – Students	192.168.10.0/24
S2 F0/18	VLAN 20 – Faculty	192.168.20.0/24

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure Switches with VLANs and Trunking

Part 3: Configure Trunk-Based Inter-VLAN Routing

Background / Scenario

A second method of providing routing and connectivity for multiple VLANs is through the use of an 802.1Q trunk between one or more switches and a single router interface. This method is also known as router-on-a-stick inter-VLAN routing. In this method, the physical router interface is divided into multiple subinterfaces that provide logical pathways to all VLANs connected.

In this lab, you will configure trunk-based inter-VLAN routing and verify connectivity to hosts on different VLANs as well as with a loopback on the router.

Note: This lab provides minimal assistance with the actual commands necessary to configure trunk-based inter-VLAN routing. However, the required configuration commands are provided in Appendix A of this lab. 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 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

- 1 Router (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 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 on the PC hosts, switches, and router.

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

Step 2: Configure PC hosts.

Step 3: Initialize and reload the router and switches as necessary.

Step 4: Configure basic settings for each switch.

- a. Console into the switch and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on the switch.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```
- c. Configure the device name as shown in the topology.
- d. Configure the IP address listed in the Addressing Table for VLAN 1 on the switch.
- e. Configure the default gateway on the switch.
- f. Administratively deactivate all unused ports on the switch.
- g. Copy the running configuration to the startup configuration.

Step 5: Configure basic settings for the router.

- a. Console into the router and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on the router.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

- c. Configure the Lo0 IP address as shown in the Address Table. Do not configure sub-interfaces at this time. They will be configured in Part 3.
- d. Copy the running configuration to the startup configuration.

Part 2: Configure Switches with VLANs and Trunking

In Part 2, you will configure the switches with VLANs and trunking.

Note: The required commands for Part 2 are provided in Appendix A. Test your knowledge by trying to configure S1 and S2 without referring to the appendix.

Step 1: Configure VLANs on S1.

- a. On S1, configure the VLANs and names listed in the Switch Port Assignment Specifications table. Write the commands you used in the space provided.

- b. On S1, configure the interface connected to R1 as a trunk. Also configure the interface connected to S2 as a trunk. Write the commands you used in the space provided.

- c. On S1, assign the access port for PC-A to VLAN 10. Write the commands you used in the space provided.

Step 2: Configure VLANs on Switch 2.

- a. On S2, configure the VLANs and names listed in the Switch Port Assignment Specifications table.

- b. On S2, verify that the VLAN names and numbers match those on S1. Write the command you used in the space provided.

- c. On S2, assign the access port for PC-B to VLAN 20.

- d. On S2, configure the interface connected to S1 as a trunk.

Part 3: Configure Trunk-Based Inter-VLAN Routing

In Part 3, you will configure R1 to route to multiple VLANs by creating subinterfaces for each VLAN. This method of inter-VLAN routing is called router-on-a-stick.

Note: The required commands for Part 3 are provided in Appendix A. Test your knowledge by trying to configure trunk-based or router-on-a-stick inter-VLAN routing without referring to the appendix.

Step 1: Configure a subinterface for VLAN 1.

- a. Create a subinterface on R1 G0/1 for VLAN 1 using 1 as the subinterface ID. Write the command you used in the space provided.

-
- b. Configure the subinterface to operate on VLAN 1. Write the command you used in the space provided.
-

- c. Configure the subinterface with the IP address from the Address Table. Write the command you used in the space provided.
-

Step 2: Configure a subinterface for VLAN 10.

- Create a subinterface on R1 G0/1 for VLAN 10 using 10 as the subinterface ID.
- Configure the subinterface to operate on VLAN 10.
- Configure the subinterface with the address from the Address Table.

Step 3: Configure a subinterface for VLAN 20.

- Create a subinterface on R1 G0/1 for VLAN 20 using 20 as the subinterface ID.
- Configure the subinterface to operate on VLAN 20.
- Configure the subinterface with the address from the Address Table.

Step 4: Enable the G0/1 interface.

Enable the G0/1 interface. Write the commands you used in the space provided.

Step 5: Verify connectivity.

Enter the command to view the routing table on R1. What networks are listed?

From PC-A, is it possible to ping the default gateway for VLAN 10? _____ From PC-A, is it possible to ping PC-B? _____

From PC-A, is it possible to ping Lo0? _____ From PC-A, is it possible to ping S2? _____

If the answer is **no** to any of these questions, troubleshoot the configurations and correct any errors.

Reflection

What are the advantages of trunk-based or router-on-a-stick inter-VLAN routing?

Appendix A – Configuration Commands**Switch S1**

```
S1(config)# vlan 10
S1(config-vlan)# name Students
S1(config-vlan)# vlan 20
S1(config-vlan)# name
Faculty S1(config-vlan)#
exit S1(config)# interface
f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# interface f0/5
```

```
S1(config-if)# switchport mode trunk
S1(config-if)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

Switch S2

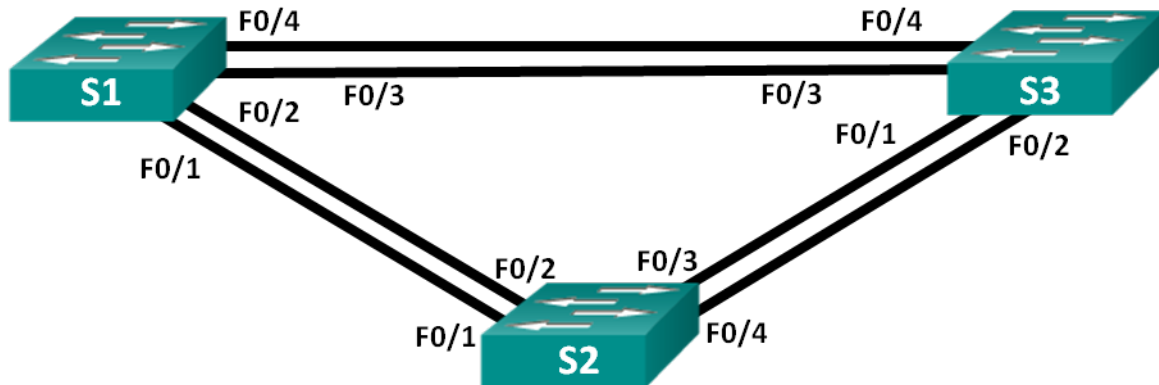
```
S2(config)# vlan 10
S2(config-vlan)# name Students
S2(config-vlan)# vlan 20
S2(config-vlan)# name Faculty
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
S2(config-if)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
```

Router R1

```
R1(config)# interface g0/1.1
R1(config-subif)# encapsulation dot1Q 1
R1(config-subif)# ip address 192.168.1.1 255.255.255.0
R1(config-subif)# interface g0/1.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config-subif)# interface g0/1.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)# interface g0/1
R1(config-if)# no shutdown
```

Lab 24: Building a Switched Network with Redundant Links

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.1	255.255.255.0
S2	VLAN 1	192.168.1.2	255.255.255.0
S3	VLAN 1	192.168.1.3	255.255.255.0

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Determine the Root Bridge

Part 3: Observe STP Port Selection Based on Port Cost

Part 4: Observe STP Port Selection Based on Port Priority

Background / Scenario

Redundancy increases the availability of devices in the network topology by protecting the network from a single point of failure. Redundancy in a switched network is accomplished through the use of multiple switches or multiple links between switches. When physical redundancy is introduced into a network design, loops and duplicate frames can occur.

The Spanning Tree Protocol (STP) was developed as a Layer 2 loop-avoidance mechanism for redundant links in a switched network. STP ensures that there is only one logical path between all destinations on the network by intentionally blocking redundant paths that could cause a loop.

In this lab, you will use the **show spanning-tree** command to observe the STP election process of the root bridge. You will also observe the port selection process based on cost and priority.

Note: The switches used are Cisco Catalyst 2960s 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 switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet 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 on the switches.

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

Attach the devices as shown in the topology diagram, and cable as necessary.

Task 2: Initialize and reload the switches as necessary.

Task 3: Configure basic settings for each switch.

Step 1: Disable DNS lookup.

Step 2: Configure the device name as shown in the topology.

Step 3: Assign **class** as the encrypted privileged EXEC mode password.

Step 4: Assign **cisco** as the console and vty passwords and enable login for console and vty lines.

Step 5: Configure logging synchronous for the console line.

Step 6: Configure a message of the day (MOTD) banner to warn users that unauthorized access is prohibited.

Step 7: Configure the IP address listed in the Addressing Table for VLAN 1 on all switches.

Step 8: Copy the running configuration to the startup configuration.

Task 4: Test connectivity.

Verify that the switches can ping one another.

Can S1 ping S2? _____

Can S1 ping S3? _____

Can S2 ping S3? _____

Troubleshoot until you are able to answer yes to all questions.

Part 2: Determine the Root Bridge

Every spanning-tree instance (switched LAN or broadcast domain) has a switch designated as the root bridge. The root bridge serves as a reference point for all spanning-tree calculations to determine which redundant paths to block.

An election process determines which switch becomes the root bridge. The switch with the lowest bridge identifier (BID) becomes the root bridge. The BID is made up of a bridge priority value, an extended system ID, and the MAC address of the switch. The priority value can range from 0 to 65,535, in increments of 4,096, with a default value of 32,768.

Task 1: Deactivate all ports on the switches.**Task 2: Configure connected ports as trunks.****Task 3: Activate ports F0/2 and F0/4 on all switches.****Task 4: Display spanning tree information.**

Issue the **show spanning-tree** command on all three switches. The Bridge ID Priority is calculated by adding the priority value and the extended system ID. The extended system ID is always the VLAN number. In the example below, all three switches have equal Bridge ID Priority values ($32769 = 32768 + 1$, where default priority = 32768, VLAN number = 1); therefore, the switch with the lowest MAC address becomes the root bridge (S2 in the example).

S1# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID      Priority      32769
             Address      0cd9.96d2.4000
             Cost        19
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

```

```

Bridge ID  Priority      32769 (priority 32768 sys-id-ext 1)
           Address      0cd9.96e8.8a00
           Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time    300 sec

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/2	Root	FWD	19	128.2	P2p
Fa0/4	Altn	BLK	19	128.4	P2p

S2# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID      Priority      32769
             Address      0cd9.96d2.4000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

```

```

Bridge ID  Priority      32769 (priority 32768 sys-id-ext 1)
           Address      0cd9.96d2.4000
           Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time    300 sec

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	----	---	----	-----	-----
Fa0/2	Desg	FWD	19	128.2	P2p
Fa0/4	Desg	FWD	19	128.4	P2p

S3# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID      Priority      32769
              Address      0cd9.96d2.4000
              Cost        19
              Port        2 (FastEthernet0/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

```

```

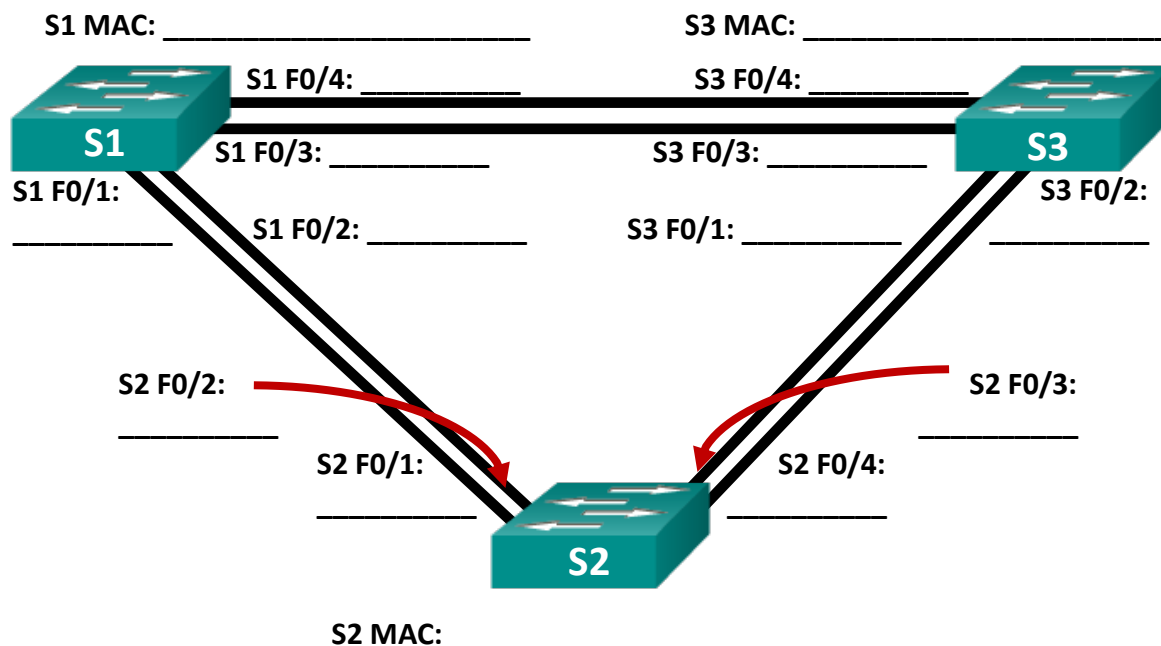
Bridge ID  Priority      32769 (priority 32768 sys-id-ext 1)
           Address      0cd9.96e8.7400
           Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time   300 sec

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	----	---	----	-----	-----
Fa0/2	Root	FWD	19	128.2	P2p
Fa0/4	Desg	FWD	19	128.4	P2p

Note: The default STP mode on the 2960 switch is Per VLAN Spanning Tree (PVST).

In the diagram below, record the Role and Status (Sts) of the active ports on each switch in the Topology.



Based on the output from your switches, answer the following questions.

Which switch is the root bridge? _____

Why did spanning tree select this switch as the root bridge?

Which ports are the root ports on the switches? _____

Which ports are the designated ports on the switches? _____

What port is showing as an alternate port and is currently being blocked? _____

Why did spanning tree select this port as the non-designated (blocked) port?

Part 3: Observe STP Port Selection Based on Port Cost

The spanning tree algorithm (STA) uses the root bridge as the reference point and then determines which ports to block, based on path cost. The port with the lower path cost is preferred. If port costs are equal, then spanning tree compares BIDs. If the BIDs are equal, then the port priorities are used to break the tie. Lower values are always preferred. In Part 3, you will change the port cost to control which port is blocked by spanning tree.

Task 1: Locate the switch with the blocked port.

With the current configuration, only one switch should have a port that is blocked by STP. Issue the **show spanning-tree** command on both non-root switches. In the example below, spanning tree is blocking port F0/4 on the switch with the highest BID (S1).

S1# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID    Priority    32769
           Address    0cd9.96d2.4000
           Cost      19
           Port      2 (FastEthernet0/2)
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

```

```

Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
           Address    0cd9.96e8.8a00
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time 300 sec

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/2	Root	FWD	19	128.2	P2p
Fa0/4	Altn	BLK	19	128.4	P2p

S3# **show spanning-tree**

```

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             Cost        19
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address     0cd9.96e8.7400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time   15 sec

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/2	Root	FWD	19	128.2	P2p
Fa0/4	Desg	FWD	19	128.4	P2p

Note: Root bridge and port selection may differ in your topology.

Task 2: Change port cost.

In addition to the blocked port, the only other active port on this switch is the port designated as the root port. Lower the cost of this root port to 18 by issuing the **spanning-tree cost 18** interface configuration mode command.

```

S1(config)# interface f0/2
S1(config-if)# spanning-tree cost 18

```

Task 3: Observe spanning tree changes.

Re-issue the **show spanning-tree** command on both non-root switches. Observe that the previously blocked port (S1 - F0/4) is now a designated port and spanning tree is now blocking a port on the other non-root switch (S3 - F0/4).

```

S1# show spanning-tree

```

```

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             Cost        18
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address     0cd9.96e8.8a00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time   300 sec

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/2	Root	FWD	18	128.2	P2p
Fa0/4	Desg	FWD	19	128.4	P2p

S3# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID      Priority      32769
             Address      0cd9.96d2.4000
             Cost         19
             Port         2 (FastEthernet0/2)
             Hello Time    2 sec   Max Age 20 sec   Forward Delay 15 sec

```

```

Bridge ID    Priority      32769 (priority 32768 sys-id-ext 1)
             Address      0cd9.96e8.7400
             Hello Time    2 sec   Max Age 20 sec   Forward Delay 15 sec
             Aging Time    300 sec

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/2	Root	FWD	19	128.2	P2p
Fa0/4	Altn	BLK	19	128.4	P2p

Why did spanning tree change the previously blocked port to a designated port, and block the port that was a designated port on the other switch?

Task 4: Remove port cost changes.

Step 1: Issue the **no spanning-tree cost 18** interface configuration mode command to remove the cost statement that you created earlier.

```

S1(config)# interface f0/2
S1(config-if)# no spanning-tree cost 18

```

Step 2: Re-issue the **show spanning-tree** command to verify that STP has reset the port on the non-root switches back to the original port settings. It takes approximately 30 seconds for STP to complete the port transition process.

Part 4: Observe STP Port Selection Based on Port Priority

If port costs are equal, then spanning tree compares BIDs. If the BIDs are equal, then the port priorities are used to break the tie. The default port priority value is 128. STP aggregates the port priority with the port number to break ties. Lower values are always preferred. In Part 4, you will activate redundant paths to each switch to observe how STP selects a port using the port priority.

Step 1: Activate ports F0/1 and F0/3 on all switches.

Step 2: Wait 30 seconds for STP to complete the port transition process, and then issue the **show spanning-tree** command on the non-root switches. Observe that the root port has moved to the lower numbered port linked to the root switch, and blocked the previous root port.

S1# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID      Priority      32769

```

```

      Address      0cd9.96d2.4000
      Cost         19
      Port         1 (FastEthernet0/1)
      Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
      Address      0cd9.96e8.8a00
      Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
      Aging Time   15 sec

Interface          Role Sts Cost      Prio.Nbr Type
-----
Fa0/1              Root FWD 19        128.1    P2p
Fa0/2              Altn BLK 19        128.2    P2p
Fa0/3              Altn BLK 19        128.3    P2p
Fa0/4              Altn BLK 19        128.4    P2p

```

S3# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID      Priority      32769
      Address      0cd9.96d2.4000
      Cost         19
      Port         1 (FastEthernet0/1)
      Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
      Address      0cd9.96e8.7400
      Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
      Aging Time   15 sec

```

```

Interface          Role Sts Cost      Prio.Nbr Type
-----
Fa0/1              Root FWD 19        128.1    P2p
Fa0/2              Altn BLK 19        128.2    P2p
Fa0/3              Desg FWD 19        128.3    P2p
Fa0/4              Desg FWD 19        128.4    P2p

```

What port did STP select as the root port on each non-root switch? _____

Why did STP select these ports as the root port on these switches?

Reflection

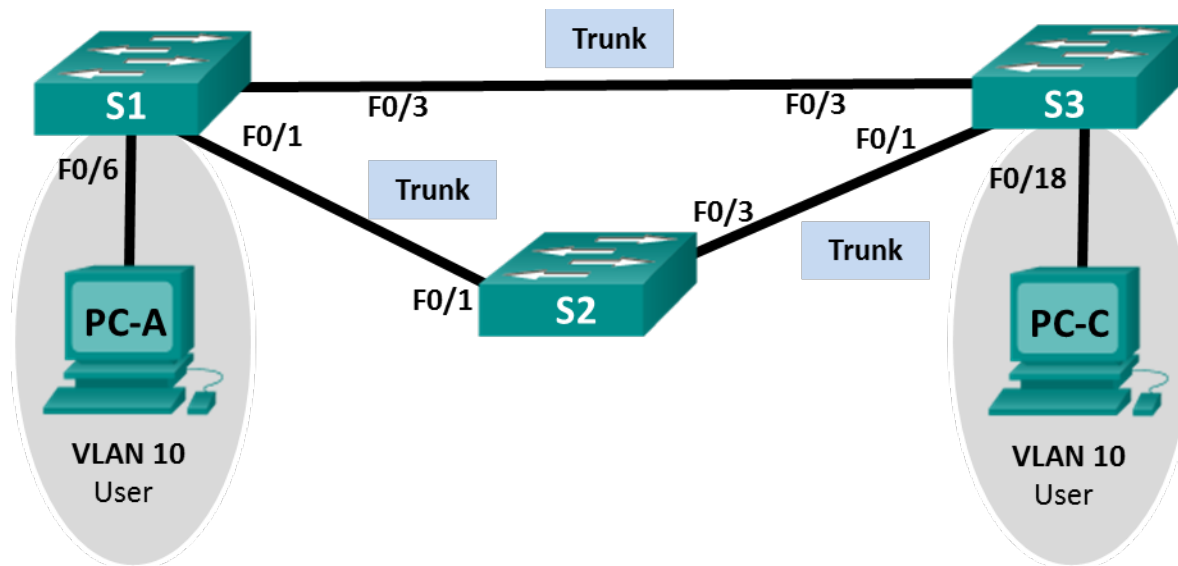
1. After a root bridge has been selected, what is the first value STP uses to determine port selection?

2. If the first value is equal on the two ports, what is the next value that STP uses to determine port selection?

3. If both values are equal on the two ports, what is the next value that STP uses to determine port selection?

Lab 25: Configuring Rapid PVST+, PortFast, and BPDU Guard

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 99	192.168.1.11	255.255.255.0
S2	VLAN 99	192.168.1.12	255.255.255.0
S3	VLAN 99	192.168.1.13	255.255.255.0
PC-A	NIC	192.168.0.2	255.255.255.0
PC-C	NIC	192.168.0.3	255.255.255.0

VLAN Assignments

VLAN	Name
10	User
99	Management

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure VLANs, Native VLAN, and Trunks

Part 3: Configure the Root Bridge and Examine PVST+ Convergence

Part 4: Configure Rapid PVST+, PortFast, BPDU Guard, and Examine Convergence

Background / Scenario

The Per-VLAN Spanning Tree (PVST) protocol is Cisco proprietary. Cisco switches default to PVST. Rapid PVST+ (IEEE 802.1w) is an enhanced version of PVST+ and allows for faster spanning-tree calculations and convergence in response to Layer 2 topology changes. Rapid PVST+ defines three port states: discarding, learning, and forwarding, and provides multiple enhancements to optimize network performance.

In this lab, you will configure the primary and secondary root bridge, examine PVST+ convergence, configure Rapid PVST+ and compare its convergence to PVST+. In addition, you will configure edge ports to transition immediately to a forwarding state using PortFast and prevent the edge ports from forwarding BDPUs using BDPU guard.

Note: This lab provides minimal assistance with the actual commands necessary for configuration. 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 switches used with CCNA hands-on labs are Cisco Catalyst 2960s 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 switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 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 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, such as the interface IP addresses, device access, and passwords.

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

Task 2: Configure PC hosts.

Task 3: Initialize and reload the switches as necessary.

Task 4: Configure basic settings for each switch.

Step 1: Disable DNS lookup.

Step 2: Configure the device name as shown in the Topology.

Step 3: Assign **cisco** as the console and vty passwords and enable login.

Step 4: Assign **class** as the encrypted privileged EXEC mode password.

Step 5: Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 6: Shut down all switch ports.

Step 7: Copy the running configuration to startup configuration.

Part 2: Configure VLANs, Native VLAN, and Trunks

In Part 2, you will create VLANs, assign switch ports to VLANs, configure trunk ports, and change the native VLAN for all switches.

Note: The required commands for Part 2 are provided in Appendix A. Test your knowledge by trying to configure the VLANs, native VLAN, and trunks without referring to the appendix.

Task 1: Create VLANs.

Use the appropriate commands to create VLANs 10 and 99 on all of the switches. Name VLAN 10 as **User** and VLAN 99 as **Management**.

```
S1(config)# vlan 10
S1(config-vlan)# name User
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
```

```
S2(config)# vlan 10
S2(config-vlan)# name User
S2(config-vlan)# vlan 99
S2(config-vlan)# name Management
```

```
S3(config)# vlan 10
S3(config-vlan)# name User
S3(config-vlan)# vlan 99
S3(config-vlan)# name Management
```

Task 2: Enable user ports in access mode and assign VLANs.

For S1 F0/6 and S3 F0/18, enable the ports, configure them as access ports, and assign them to VLAN 10.

Task 3: Configure trunk ports and assign to native VLAN 99.

For ports F0/1 and F0/3 on all switches, enable the ports, configure them as trunk ports, and assign them to native VLAN 99.

Task 4: Configure the management interface on all switches.

Using the Addressing Table, configure the management interface on all switches with the appropriate IP address.

Task 5: Verify configurations and connectivity.

Use the **show vlan brief** command on all switches to verify that all VLANs are registered in the VLAN table and that the correct ports are assigned.

Use the **show interfaces trunk** command on all switches to verify trunk interfaces.

Use the **show running-config** command on all switches to verify all other configurations.

What is the default setting for spanning-tree mode on Cisco switches?

Verify connectivity between PC-A and PC-C. Was your ping successful? _____

If your ping was unsuccessful, troubleshoot the configurations until the issue is resolved.

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

Part 3: Configure the Root Bridge and Examine PVST+ Convergence

In Part 3, you will determine the default root in the network, assign the primary and secondary root, and use the **debug** command to examine convergence of PVST+.

Note: The required commands for Part 3 are provided in Appendix A. Test your knowledge by trying to configure the root bridge without referring to the appendix.

Task 1: Determine the current root bridge.

Which command allows a user to determine the spanning-tree status of a Cisco Catalyst switch for all VLANs? Write the command in the space provided.

Use the command on all three switches to determine the answers to the following questions:

Note: There are three instances of the spanning tree on each switch. The default STP configuration on Cisco switches is PVST+, which creates a separate spanning tree instance for each VLAN (VLAN 1 and any user-configured VLANs).

What is the bridge priority of switch S1 for VLAN 1? _____

What is the bridge priority of switch S2 for VLAN 1? _____

What is the bridge priority of switch S3 for VLAN 1? _____

Which switch is the root bridge? _____

Why was this switch elected as the root bridge?

Task 2: Configure a primary and secondary root bridge for all existing VLANs.

Having a root bridge (switch) elected by MAC address may lead to a suboptimal configuration. In this lab, you will configure switch S2 as the root bridge and S1 as the secondary root bridge.

Step 1: Configure switch S2 to be the primary root bridge for all existing VLANs. Write the command in the space provided.

Step 2: Configure switch S1 to be the secondary root bridge for all existing VLANs. Write the command in the space provided.

Use the **show spanning-tree** command to answer the following questions:

What is the bridge priority of S1 for VLAN 1? _____

What is the bridge priority of S2 for VLAN 1? _____

Which interface in the network is in a blocking state? _____

Task 3: Change the Layer 2 topology and examine convergence.

To examine PVST+ convergence, you will create a Layer 2 topology change while using the **debug** command to monitor spanning-tree events.

Step 1: Enter the **debug spanning-tree events** command in privileged EXEC mode on switch S3.

```
S3# debug spanning-tree events
Spanning Tree event debugging is on
```

Step 2: Create a topology change by disabling interface F0/1 on S3.

```
S3(config)# interface f0/1
S3(config-if)# shutdown
*Mar 1 00:58:56.225: STP: VLAN0001 new root port Fa0/3, cost 38
*Mar 1 00:58:56.225: STP: VLAN0001 Fa0/3 -> listening
*Mar 1 00:58:56.225: STP[1]: Generating TC trap for port FastEthernet0/1
*Mar 1 00:58:56.225: STP: VLAN0010 new root port Fa0/3, cost 38
*Mar 1 00:58:56.225: STP: VLAN0010 Fa0/3 -> listening
*Mar 1 00:58:56.225: STP[10]: Generating TC trap for port FastEthernet0/1
*Mar 1 00:58:56.225: STP: VLAN0099 new root port Fa0/3, cost 38
*Mar 1 00:58:56.225: STP: VLAN0099 Fa0/3 -> listening
*Mar 1 00:58:56.225: STP[99]: Generating TC trap for port FastEthernet0/1
*Mar 1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to down
*Mar 1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to down
*Mar 1 00:58:58.214: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
*Mar 1 00:58:58.230: STP: VLAN0001 sent Topology Change Notice on Fa0/3
*Mar 1 00:58:58.230: STP: VLAN0010 sent Topology Change Notice on Fa0/3
*Mar 1 00:58:58.230: STP: VLAN0099 sent Topology Change Notice on Fa0/3
*Mar 1 00:58:59.220: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
*Mar 1 00:59:11.233: STP: VLAN0001 Fa0/3 -> learning
*Mar 1 00:59:11.233: STP: VLAN0010 Fa0/3 -> learning
*Mar 1 00:59:11.233: STP: VLAN0099 Fa0/3 -> learning
*Mar 1 00:59:26.240: STP[1]: Generating TC trap for port FastEthernet0/3
*Mar 1 00:59:26.240: STP: VLAN0001 Fa0/3 -> forwarding
*Mar 1 00:59:26.240: STP[10]: Generating TC trap for port FastEthernet0/3
*Mar 1 00:59:26.240: STP: VLAN0010 sent Topology Change Notice on Fa0/3
*Mar 1 00:59:26.240: STP: VLAN0010 Fa0/3 -> forwarding
*Mar 1 00:59:26.240: STP[99]: Generating TC trap for port FastEthernet0/3
*Mar 1 00:59:26.240: STP: VLAN0099 Fa0/3 -> forwarding
*Mar 1 00:59:26.248: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
*Mar 1 00:59:26.248: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
```

Note: Before proceeding, use the **debug** output to verify that all VLANs on F0/3 have reached a forwarding state then use the command **no debug spanning-tree events** to stop the **debug** output.

Through which port states do each VLAN on F0/3 proceed during network convergence?

Using the time stamp from the first and last STP debug message, calculate the time (to the nearest second) that it took for the network to converge. **Hint:** The debug timestamp format is date hh.mm.ss:msec.

Part 4: Configure Rapid PVST+, PortFast, BPDU Guard, and Examine Convergence

In Part 4, you will configure Rapid PVST+ on all switches. You will configure PortFast and BPDU guard on all access ports, and then use the **debug** command to examine Rapid PVST+ convergence.

Note: The required commands for Part 4 are provided in Appendix A. Test your knowledge by trying to configure the Rapid PVST+, PortFast, and BPDU guard without referring to the appendix.

Task 1: Configure Rapid PVST+.

Step 1: Configure S1 for Rapid PVST+. Write the command in the space provided.

Step 2: Configure S2 and S3 for Rapid PVST+.

Step 3: Verify configurations with the **show running-config | include spanning-tree mode** command.

```
S1# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
```

```
S2# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
```

```
S3# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
```

Task 2: Configure PortFast and BPDU Guard on access ports.

PortFast is a feature of spanning tree that transitions a port immediately to a forwarding state as soon as it is turned on. This is useful in connecting hosts so that they can start communicating on the VLAN instantly, rather than waiting on spanning tree. To prevent ports that are configured with PortFast from forwarding BPDUs, which could change the spanning tree topology, BPDU guard can be enabled. At the receipt of a BPDU, BPDU guard disables a port configured with PortFast.

Step 1: Configure interface F0/6 on S1 with PortFast. Write the command in the space provided.

Step 2: Configure interface F0/6 on S1 with BPDU guard. Write the command in the space provided.

Step 3: Globally configure all non-trunking ports on switch S3 with PortFast. Write the command in the space provided.

Step 4: Globally configure all non-trunking PortFast ports on switch S3 with BPDU guard. Write the command in the space provided.

Task 3: Examine Rapid PVST+ convergence.

Step 1: Enter the **debug spanning-tree events** command in privileged EXEC mode on switch S3.

Step 2: Create a topology change by enabling interface F0/1 on switch S3.

```
S3(config)# interface f0/1
S3(config-if)# no shutdown
```

```
*Mar  1 01:28:34.946: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
```

```

*Mar 1 01:28:37.588: RSTP(1): initializing port Fa0/1
*Mar 1 01:28:37.588: RSTP(1): Fa0/1 is now designated
*Mar 1 01:28:37.588: RSTP(10): initializing port Fa0/1
*Mar 1 01:28:37.588: RSTP(10): Fa0/1 is now designated
*Mar 1 01:28:37.588: RSTP(99): initializing port Fa0/1
*Mar 1 01:28:37.588: RSTP(99): Fa0/1 is now designated
*Mar 1 01:28:37.597: RSTP(1): transmitting a proposal on Fa0/1
*Mar 1 01:28:37.597: RSTP(10): transmitting a proposal on Fa0/1
*Mar 1 01:28:37.597: RSTP(99): transmitting a proposal on Fa0/1
*Mar 1 01:28:37.597: RSTP(1): updt roles, received superior bpdu on Fa0/1
*Mar 1 01:28:37.597: RSTP(1): Fa0/1 is now root port
*Mar 1 01:28:37.597: RSTP(1): Fa0/3 blocked by re-root
*Mar 1 01:28:37.597: RSTP(1): synced Fa0/1
*Mar 1 01:28:37.597: RSTP(1): Fa0/3 is now alternate
*Mar 1 01:28:37.597: RSTP(10): updt roles, received superior bpdu on Fa0/1
*Mar 1 01:28:37.597: RSTP(10): Fa0/1 is now root port
*Mar 1 01:28:37.597: RSTP(10): Fa0/3 blocked by re-root
*Mar 1 01:28:37.597: RSTP(10): synced Fa0/1
*Mar 1 01:28:37.597: RSTP(10): Fa0/3 is now alternate
*Mar 1 01:28:37.597: RSTP(99): updt roles, received superior bpdu on Fa0/1
*Mar 1 01:28:37.605: RSTP(99): Fa0/1 is now root port
*Mar 1 01:28:37.605: RSTP(99): Fa0/3 blocked by re-root
*Mar 1 01:28:37.605: RSTP(99): synced Fa0/1
*Mar 1 01:28:37.605: RSTP(99): Fa0/3 is now alternate
*Mar 1 01:28:37.605: STP[1]: Generating TC trap for port FastEthernet0/1
*Mar 1 01:28:37.605: STP[10]: Generating TC trap for port FastEthernet0/1
*Mar 1 01:28:37.605: STP[99]: Generating TC trap for port FastEthernet0/1
*Mar 1 01:28:37.622: RSTP(1): transmitting an agreement on Fa0/1 as a response to a
proposal
*Mar 1 01:28:37.622: RSTP(10): transmitting an agreement on Fa0/1 as a response to a
proposal
*Mar 1 01:28:37.622: RSTP(99): transmitting an agreement on Fa0/1 as a response to a
proposal
*Mar 1 01:28:38.595: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up

```

Using the time stamp from the first and last RSTP debug message, calculate the time that it took for the network to converge.

Reflection

1. What is the main benefit of using Rapid PVST+?

2. How does configuring a port with PortFast allow for faster convergence?

3. What protection does BPDU guard provide?

Appendix A – Switch Configuration Commands

Switch S1

```
S1(config)# vlan 10
S1(config-vlan)# name User
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)# interface f0/6
S1(config-if)# no shutdown
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/1
S1(config-if)# no shutdown
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# interface f0/3
S1(config-if)# no shutdown
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# interface vlan 99
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# exit
S1(config)# spanning-tree vlan 1,10,99 root secondary
S1(config)# spanning-tree mode rapid-pvst
S1(config)# interface f0/6
S1(config-if)# spanning-tree portfast
S1(config-if)# spanning-tree bpduguard enable
```

Switch S2

```
S2(config)# vlan 10
S2(config-vlan)# name User
S2(config-vlan)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# exit
S2(config)# interface f0/1
S2(config-if)# no shutdown
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# interface f0/3
S2(config-if)# no shutdown
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# interface vlan 99
S2(config-if)# ip address 192.168.1.12 255.255.255.0
```

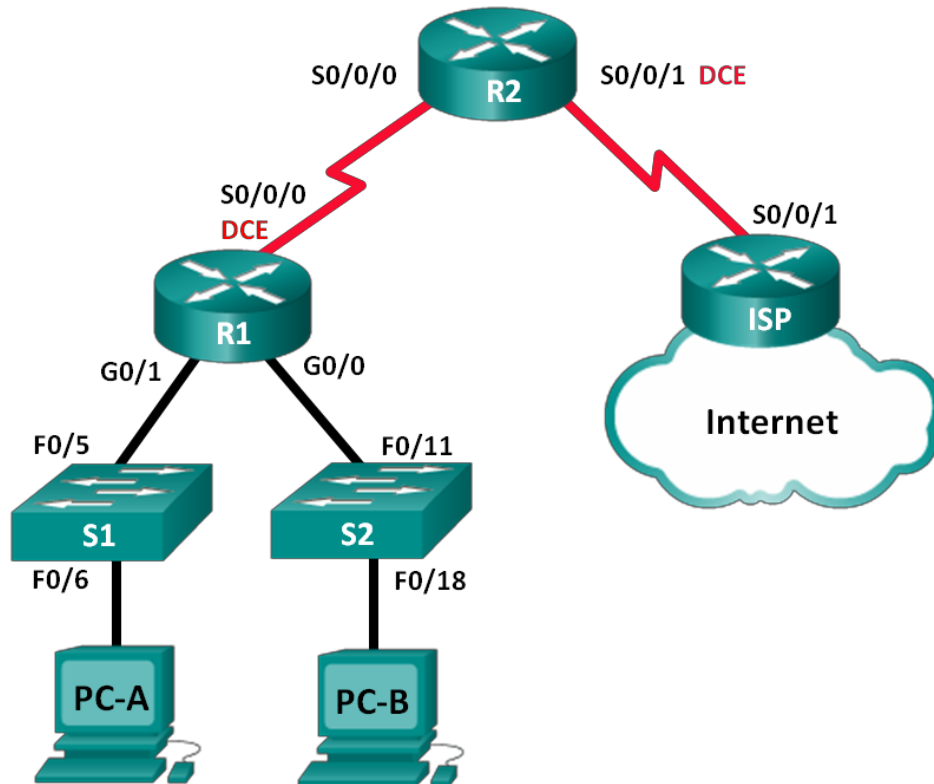
```
S2(config-if)# exit
S2(config)# spanning-tree vlan 1,10,99 root primary
S2(config)# spanning-tree mode rapid-pvst
```

Switch S3

```
S3(config)# vlan 10
S3(config-vlan)# name User
S3(config-vlan)# vlan 99
S3(config-vlan)# name Management
S3(config-vlan)# exit
S3(config)# interface f0/18
S3(config-if)# no shutdown
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 10
S3(config-if)# spanning-tree portfast
S3(config-if)# spanning-tree bpduguard enable
S3(config-if)# interface f0/1
S3(config-if)# no shutdown
S3(config-if)# switchport mode trunk
S3(config-if)# switchport trunk native vlan 99
S3(config-if)# interface f0/3
S3(config-if)# no shutdown
S3(config-if)# switchport mode trunk
S3(config-if)# switchport trunk native vlan 99
S3(config-if)# interface vlan 99
S3(config-if)# ip address 192.168.1.13 255.255.255.0
S3(config-if)# exit
S3(config)# spanning-tree mode rapid-pvst
```

Lab 26: Configuring Basic DHCPv4 on a Router

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
	S0/0/0 (DCE)	192.168.2.253	255.255.255.252	N/A
R2	S0/0/0	192.168.2.254	255.255.255.252	N/A
	S0/0/1 (DCE)	209.165.200.226	255.255.255.224	N/A
ISP	S0/0/1	209.165.200.225	255.255.255.224	N/A
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure a DHCPv4 Server and a DHCP Relay Agent

Background / Scenario

The Dynamic Host Configuration Protocol (DHCP) is a network protocol that lets network administrators

manage and automate the assignment of IP addresses. Without DHCP, the administrator must manually assign and configure IP addresses, preferred DNS servers, and default gateways. As the network grows in size, this becomes an administrative problem when devices are moved from one internal network to another.

In this scenario, the company has grown in size, and the network administrators can no longer assign IP addresses to devices manually. Your job is to configure the R2 router to assign IPv4 addresses on two different subnets connected to router R1.

Note: This lab provides minimal assistance with the actual commands necessary to configure DHCP. 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

- 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)
- 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 set up the network topology and configure the routers and switches with basic settings, such as passwords and IP addresses. You will also configure the IP settings for the PCs in the topology.

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

Step 2: Initialize and reload the routers and switches.

Step 3: Configure basic settings for each router.

- a. Console into the router and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on the router.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco

login
logging synchronous
line vty 0 4
password cisco
```

```
login
```

- c. Configure the host name as shown in the topology.
- d. Configure the IPv4 addresses on the router as shown in the topology.
- e. Set the DCE serial interfaces with a clock rate of 128000.

Step 4: Configure dynamic, default, and static routing on the routers.

- a. Configure RIPv2 for R1.

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.0.0
R1(config-router)# network 192.168.1.0
R1(config-router)# network 192.168.2.252
R1(config-router)# no auto-summary
```

- b. Configure RIPv2 and a default route to the ISP on R2.

```
R2(config)# router rip
R2(config-router)# version 2
R2(config-router)# network 192.168.2.252
R2(config-router)# default-information originate
R2(config-router)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

- c. Configure a summary static route on ISP to reach the networks on the R1 and R2 routers.

```
ISP(config)# ip route 192.168.0.0 255.255.252.0 209.165.200.226
```

- d. Copy the running configuration to the startup configuration.

Step 5: Verify network connectivity between the routers.

If any pings between routers fail, correct the errors before proceeding to the next step. Use **show ip route** and **show ip interface brief** to locate possible issues.

Step 6: Verify the host PCs are configured for DHCP.

Part 2: Configure a DHCPv4 Server and a DHCP Relay Agent

To automatically assign address information on the network, you will configure R2 as a DHCPv4 server and R1 as a DHCP relay agent.

Step 1: Configure DHCPv4 server settings on router R2.

On R2, you will configure a DHCP address pool for each of the R1 LANs. Use the pool name **R1G0** for the G0/0 LAN and **R1G1** for the G0/1 LAN. You will also configure the addresses to be excluded from the address pools. Best practice dictates that excluded addresses be configured first, to guarantee that they are not accidentally leased to other devices.

Exclude the first 9 addresses in each R1 LAN starting with .1. All other addresses should be available in the DHCP address pool. Make sure that each DHCP address pool includes a default gateway, the domain **ccna-lab.com**, a DNS server (209.165.200.225), and a lease time of 2 days.

On the lines below, write the commands necessary for configuring DHCP services on router R2, including the DHCP-excluded addresses and the DHCP address pools.

Note: The required commands for Part 2 are provided in Appendix A. Test your knowledge by trying to

configure DHCP on R1 and R2 without referring to the appendix.

On PC-A or PC-B, open a command prompt and enter the **ipconfig /all** command. Did either of the host PCs receive an IP address from the DHCP server? Why?

Step 2: Configure R1 as a DHCP relay agent.

Configure IP helper addresses on R1 to forward all DHCP requests to the R2 DHCP server.

On the lines below, write the commands necessary to configure R1 as a DHCP relay agent for the R1 LANs.

Step 3: Record IP settings for PC-A and PC-B.

On PC-A and PC-B, issue the **ipconfig /all** command to verify that the PCs have received IP address information from the DHCP server on R2. Record the IP and MAC address for each PC.

Based on the DHCP pool that was configured on R2, what are the first available IP addresses that PC-A and PC-B can lease?

Step 4: Verify DHCP services and address leases on R2.

- a. On R2, enter the **show ip dhcp binding** command to view DHCP address leases.

Along with the IP addresses that were leased, what other piece of useful client identification information is in the output?

- b. On R2, enter the **show ip dhcp server statistics** command to view the DHCP pool statistics and message activity.

How many types of DHCP messages are listed in the output?

- c. On R2, enter the **show ip dhcp pool** command to view the DHCP pool settings.

In the output of the **show ip dhcp pool** command, what does the current index refer to?

- d. On R2, enter the **show run | section dhcp** command to view the DHCP configuration in the running configuration.

- e. On R1, enter the **show run interface** command for interfaces G0/0 and G0/1 to view the DHCP relay configuration in the running configuration.

Reflection

What do you think is the benefit of using DHCP relay agents instead of multiple routers acting as DHCP servers?

Appendix A – DHCP Configuration Commands

Router R1

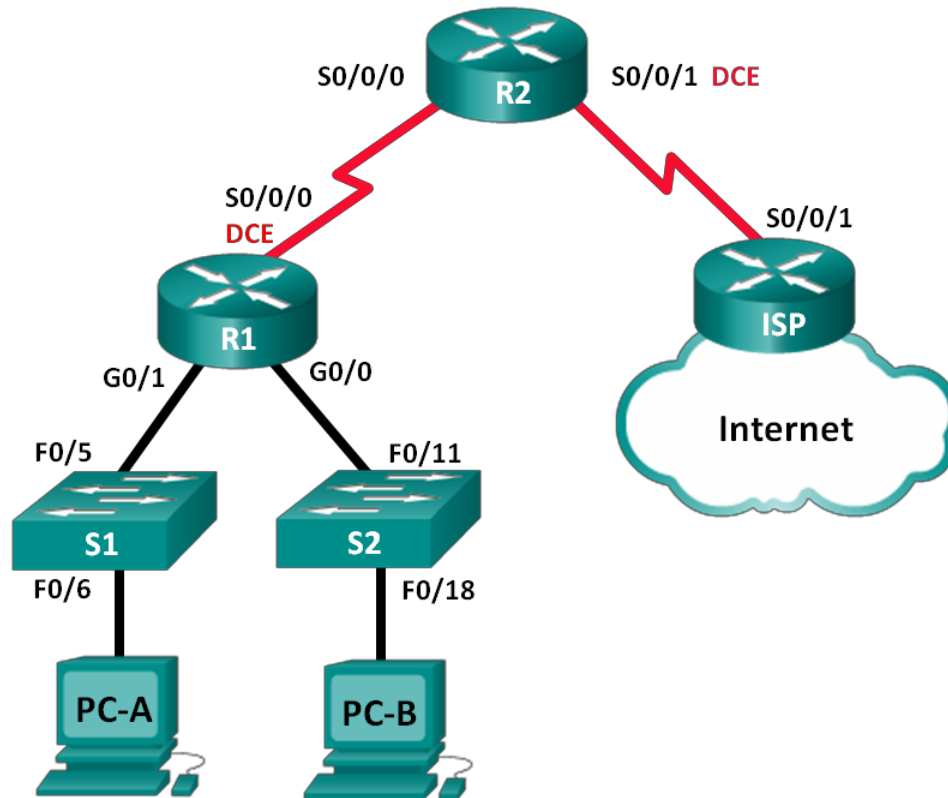
```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.2.254
R1(config-if)# exit
R1(config-if)# interface g0/1
R1(config-if)# ip helper-address 192.168.2.254
```

Router R2

```
R2(config)# ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)# ip dhcp pool R1G1
R2(dhcp-config)# network 192.168.1.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.1.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
R2(config)# ip dhcp pool R1G0
R2(dhcp-config)# network 192.168.0.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.0.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
```


Lab 27: Troubleshooting DHCPv4

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.128	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.0.253	255.255.255.252	N/A
R2	S0/0/0	192.168.0.254	255.255.255.252	N/A
	S0/0/1 (DCE)	209.165.200.226	255.255.255.252	N/A
ISP	S0/0/1	209.165.200.225	255.255.255.252	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.0.2	255.255.255.128	192.168.0.1
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Troubleshoot DHCPv4 Issues

Background / Scenario

The Dynamic Host Configuration Protocol (DHCP) is a network protocol that lets the network administrators manage and automate the assignment of IP addresses. Without DHCP, the administrator must manually assign and configure IP addresses, preferred DNS servers, and the default gateway. As the network grows in size, this becomes an administrative problem when devices are moved from one internal network to another.

In this scenario, the company has grown in size, and the network administrators can no longer assign IP addresses to devices manually. The R2 router has been configured as a DHCP server to assign IP addresses to the host devices on router R1 LANs. Several errors in the configuration have resulted in connectivity issues. You are asked to troubleshoot and correct the configuration errors and document your work.

Ensure that the network supports the following:

- 1) The router R2 should function as the DHCP server for the 192.168.0.0/25 and 192.168.1.0/24 networks connected to R1.
- 2) All PCs connected to S1 and S2 should receive an IP address in the correct network via DHCP.

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

- 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)
- 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 set up the network topology and configure the routers and switches with basic settings, such as passwords and IP addresses. You will also configure the IP settings for the PCs in the topology.

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

Step 2: Initialize and reload the routers and switches.

Step 3: Configure basic settings for each router.

- a. Disable DNS lookup.
- b. Configure device name as shown in the topology.
- c. Assign **class** as the privileged EXEC password.
- d. Assign **cisco** as the console and vty passwords.
- e. Configure **logging synchronous** to prevent console messages from interrupting command entry.
- f. Configure the IP addresses for all the router interfaces.

g. Set clock rate to **128000** for all DCE router interfaces.

h. Configure RIP for R1.

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.0.0
R1(config-router)# network 192.168.1.0
R1(config-router)# no auto-summary
R1(config-router)# exit
```

i. Configure RIP and a static default route on R2.

```
R2(config)# router rip
R2(config-router)# version 2
R2(config-router)# network 192.168.0.0
R2(config-router)# default-information originate
R2(config-router)# no auto-summary
R2(config-router)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

j. Configure a summary static route on ISP to the networks on R1 and R2 routers.

```
ISP(config)# ip route 192.168.0.0 255.255.254.0 209.165.200.226
```

Step 4: Verify network connectivity between the routers.

If any pings between the routers fail, correct the errors before proceeding to the next step. Use **show ip route** and **show ip interface brief** to locate possible issues.

Step 5: Configure basic settings for each switch.

- Disable DNS lookup.
- Configure device name as shown in the topology.
- Configure the IP address for the VLAN 1 interface and the default gateway for each switch.
- Assign **class** as the privileged EXEC mode password.
- Assign **cisco** as the console and vty passwords.
- Configure **logging synchronous** for the console line.

Step 6: Verify the hosts are configured for DHCP.

Step 7: Load the initial DHCP configuration for R1 and R2.

Router R1

```
interface GigabitEthernet0/1
ip helper-address 192.168.0.253
```

Router R2

```
ip dhcp excluded-address 192.168.11.1 192.168.11.9
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp pool R1G1
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
ip dhcp pool R1G0
```

```
network 192.168.0.0 255.255.255.128
default-router 192.168.11.1
```

Part 2: Troubleshoot DHCPv4 Issues

After configuring routers R1 and R2 with DHCPv4 settings, several errors in the DHCP configurations were introduced and resulted in connectivity issues. R2 is configured as a DHCP server. For both pools of DHCP addresses, the first nine addresses are reserved for the routers and switches. R1 relays the DHCP information to all the R1 LANs. Currently, PC-A and PC-B have no access to the network. Use the **show** and **debug** commands to determine and correct the network connectivity issues.

Step 1: Record IP settings for PC-A and PC-B.

- For PC-A and PC-B, at the command prompt, enter **ipconfig /all** to display the IP and MAC addresses.
- Record the IP and MAC addresses in the table below. The MAC address can be used to determine which PC is involved in the debug message.

	IP Address/Subnet Mask	MAC Address
PC-A		
PC-B		

Step 2: Troubleshoot DHCP issues for the 192.168.1.0/24 network on router R1.

Router R1 is a DHCP relay agent for all the R1 LANs. In this step, only the DHCP process for the 192.168.1.0/24 network will be examined. The first nine addresses are reserved for other network devices, such as routers, switches, and servers.

- Use a DHCP **debug** command to observe the DHCP process on R2 router.

```
R2# debug ip dhcp server events
```

- On R1, display the running configuration for the G0/1 interface.

```
R1# show run interface g0/1
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip helper-address 192.168.0.253
 duplex auto
 speed auto
```

If there are any DHCP relay issues, record any commands that are necessary to correct the configurations errors.

- In a command prompt on PC-A, type **ipconfig /renew** to receive an address from the DHCP server. Record the configured IP address, subnet mask, and default gateway for PC-A.
-
- Observe the debug messages on R2 router for the DHCP renewal process for PC-A. The DHCP server attempted to assign 192.168.1.1/24 to PC-A. This address is already in use for G0/1 interface on R1. The same issue occurs with IP address 192.168.1.2/24 because this address has been assigned to S1 in the initial configuration. Therefore, an IP address of 192.168.1.3/24 has been assigned to PC-A. The DHCP assignment conflict indicates there may be an issue with the excluded-address statement on the DHCP

server configuration on R2.

```
*Mar  5 06:32:16.939: DHCPD: Sending notification of DISCOVER:
*Mar  5 06:32:16.939:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:32:16.939:   DHCPD: circuit id 00000000
*Mar  5 06:32:16.939: DHCPD: Seeing if there is an internally specified pool class:
*Mar  5 06:32:16.939:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:32:16.939:   DHCPD: circuit id 00000000
*Mar  5 06:32:16.943: DHCPD: Allocated binding 2944C764
*Mar  5 06:32:16.943: DHCPD: Adding binding to radix tree (192.168.1.1)
*Mar  5 06:32:16.943: DHCPD: Adding binding to hash tree
*Mar  5 06:32:16.943: DHCPD: assigned IP address 192.168.1.1 to client
0100.5056.be76.8c.
*Mar  5 06:32:16.951: %DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged
192.168.1.1.
*Mar  5 06:32:16.951: DHCPD: returned 192.168.1.1 to address pool R1G1.
*Mar  5 06:32:16.951: DHCPD: Sending notification of DISCOVER:
*Mar  5 06:32:16.951:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:32:16.951:   DHCPD: circuit id 00000000
*Mar  5 06:32:1
R2#6.951: DHCPD: Seeing if there is an internally specified pool class:
*Mar  5 06:32:16.951:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:32:16.951:   DHCPD: circuit id 00000000
*Mar  5 06:32:16.951: DHCPD: Allocated binding 31DC93C8
*Mar  5 06:32:16.951: DHCPD: Adding binding to radix tree (192.168.1.2)
*Mar  5 06:32:16.951: DHCPD: Adding binding to hash tree
*Mar  5 06:32:16.951: DHCPD: assigned IP address 192.168.1.2 to client
0100.5056.be76.8c.
*Mar  5 06:32:18.383: %DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged
192.168.1.2.
*Mar  5 06:32:18.383: DHCPD: returned 192.168.1.2 to address pool R1G1.
*Mar  5 06:32:18.383: DHCPD: Sending notification of DISCOVER:
*Mar  5 06:32:18.383:   DHCPD: htype 1 chaddr 0050.56be.6c89
*Mar  5 06:32:18.383:   DHCPD: circuit id 00000000
*Mar  5 06:32:18.383: DHCPD: Seeing if there is an internally specified pool class:
*Mar  5 06:32:18.383:   DHCPD: htype 1 chaddr 0050.56be.6c89
*Mar  5 06:32:18.383:   DHCPD: circuit id 00000000
*Mar  5 06:32:18.383: DHCPD: Allocated binding 2A40E074
*Mar  5 06:32:18.383: DHCPD: Adding binding to radix tree (192.168.1.3)
*Mar  5 06:32:18.383: DHCPD: Adding binding to hash tree
*Mar  5 06:32:18.383: DHCPD: assigned IP address 192.168.1.3 to client
0100.5056.be76.8c.
<output omitted>
```

- e. Display the DHCP server configuration on R2. The first nine addresses for 192.168.1.0/24 network are not excluded from the DHCP pool.

```
R2# show run | section dhcp
ip dhcp excluded-address 192.168.11.1 192.168.11.9
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp pool R1G1
    network 192.168.1.0 255.255.255.0
    default-router 192.168.1.1
ip dhcp pool R1G0
```

```
network 192.168.0.0 255.255.255.128
default-router 192.168.1.1
```

Record the commands to resolve the issue on R2.

- f. At the command prompt on PC-A, type **ipconfig /release** to return the 192.168.1.3 address back to the DHCP pool. The process can be observed in the debug message on R2.

```
*Mar 5 06:49:59.563: DHCPD: Sending notification of TERMINATION:
*Mar 5 06:49:59.563: DHCPD: address 192.168.1.3 mask 255.255.255.0
*Mar 5 06:49:59.563: DHCPD: reason flags: RELEASE
*Mar 5 06:49:59.563: DHCPD: htype 1 chaddr 0050.56be.768c
*Mar 5 06:49:59.563: DHCPD: lease time remaining (secs) = 85340
*Mar 5 06:49:59.563: DHCPD: returned 192.168.1.3 to address pool R1G1.
```

- g. At the command prompt on PC-A, type **ipconfig /renew** to be assigned a new IP address from the DHCP server. Record the assigned IP address and default gateway information.

The process can be observed in the debug message on R2.

```
*Mar 5 06:50:11.863: DHCPD: Sending notification of DISCOVER:
*Mar 5 06:50:11.863: DHCPD: htype 1 chaddr 0050.56be.768c
*Mar 5 06:50:11.863: DHCPD: circuit id 00000000
*Mar 5 06:50:11.863: DHCPD: Seeing if there is an internally specified pool class:
*Mar 5 06:50:11.863: DHCPD: htype 1 chaddr 0050.56be.768c
*Mar 5 06:50:11.863: DHCPD: circuit id 00000000
*Mar 5 06:50:11.863: DHCPD: requested address 192.168.1.3 has already been assigned.
*Mar 5 06:50:11.863: DHCPD: Allocated binding 3003018C
*Mar 5 06:50:11.863: DHCPD: Adding binding to radix tree (192.168.1.10)
*Mar 5 06:50:11.863: DHCPD: Adding binding to hash tree
*Mar 5 06:50:11.863: DHCPD: assigned IP address 192.168.1.10 to client
0100.5056.be76.8c.
<output omitted>
```

- h. Verify network connectivity.

Can PC-A ping the assigned default gateway? _____

Can PC-A ping the R2 router? _____

Can PC-A ping the ISP router? _____

Step 3: Troubleshoot DHCP issues for 192.168.0.0/25 network on R1.

Router R1 is a DHCP relay agent for all the R1 LANs. In this step, only the DHCP process for the 192.168.0.0/25 network is examined. The first nine addresses are reserved for other network devices.

- a. Use a DHCP **debug** command to observe the DHCP process on R2.

```
R2# debug ip dhcp server events
```

- b. Display the running configuration for the G0/0 interface on R1 to identify possible DHCP issues.

```
R1# show run interface g0/0
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.128
 duplex auto
```

```
speed auto
```

Record the issues and any commands that are necessary to correct the configurations errors.

- c. From the command prompt on PC-B, type **ipconfig /renew** to receive an address from the DHCP server. Record the configured IP address, subnet mask, and default gateway for PC-B.
- d. Observe the debug messages on R2 router for the renewal process for PC-A. The DHCP server assigned 192.168.0.10/25 to PC-B.

```
*Mar  5 07:15:09.663: DHCPD: Sending notification of DISCOVER:
*Mar  5 07:15:09.663:   DHCPD: htype 1 chaddr 0050.56be.f6db
*Mar  5 07:15:09.663:   DHCPD: circuit id 00000000
*Mar  5 07:15:09.663: DHCPD: Seeing if there is an internally specified pool class:
*Mar  5 07:15:09.663:   DHCPD: htype 1 chaddr 0050.56be.f6db
*Mar  5 07:15:09.663:   DHCPD: circuit id 00000000
*Mar  5 07:15:09.707: DHCPD: Sending notification of ASSIGNMENT:
*Mar  5 07:15:09.707:   DHCPD: address 192.168.0.10 mask 255.255.255.128
*Mar  5 07:15:09.707:   DHCPD: htype 1 chaddr 0050.56be.f6db
*Mar  5 07:15:09.707:   DHCPD: lease time remaining (secs) = 86400
```

- e. Verify network connectivity.

Can PC-B ping the DHCP assigned default gateway? _____

Can PC-B ping its default gateway (192.168.0.1)? _____

Can PC-B ping the R2 router? _____

Can PC-B ping the ISP router? _____

- f. If any issues failed in Step e, record the problems and any commands to resolve the issues.
-
-

- g. Release and renew the IP configurations on PC-B. Repeat Step e to verify network connectivity.
- h. Discontinue the debug process by using the **undebg all** command.

```
R2# undebg all
```

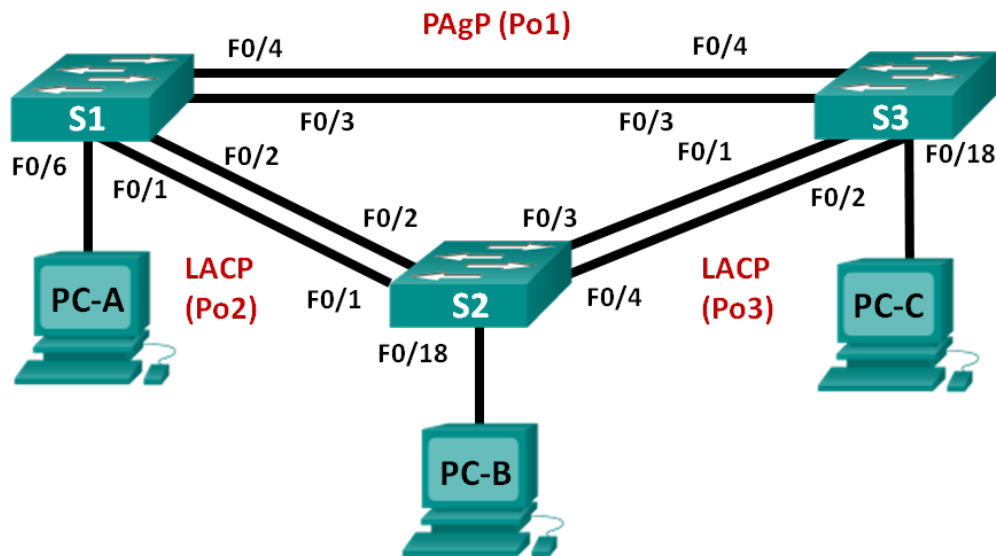
```
All possible debugging has been turned off
```

Reflection

What are the benefits of using DHCP?

Lab 28: Configuring EtherChannel

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 99	192.168.99.11	255.255.255.0
S2	VLAN 99	192.168.99.12	255.255.255.0
S3	VLAN 99	192.168.99.13	255.255.255.0
PC-A	NIC	192.168.10.1	255.255.255.0
PC-B	NIC	192.168.10.2	255.255.255.0
PC-C	NIC	192.168.10.3	255.255.255.0

Objectives

Part 1: Configure Basic Switch Settings

Part 2: Configure PAgP

Part 3: Configure LACP

Background / Scenario

Link aggregation allows the creation of logical links that are comprised of two or more physical links. This provides increased throughput beyond using only one physical link. Link aggregation also provides redundancy if one of the links fails.

In this lab, you will configure EtherChannel, a form of link aggregation used in switched networks. You will configure EtherChannel using Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP).

Note: PAgP is a Cisco-proprietary protocol that you can only run on Cisco switches and on switches that are licensed vendors to support PAgP. LACP is a link aggregation protocol that is defined by IEEE 802.3ad, and it is not associated with any specific vendor.

LACP allows Cisco switches to manage Ethernet channels between switches that conform to the 802.3ad protocol. You can configure up to 16 ports to form a channel. Eight of the ports are in active mode and the other eight are in standby mode. When any of the active ports fail, a standby port becomes active. Standby mode works only for LACP, not for PAgP.

Note: The switches used with CCNA hands-on labs are Cisco Catalyst 2960s 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 switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 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 cables as shown in the topology

Part 1: Configure Basic Switch Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords.

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

Attach the devices as shown in the topology diagram, and cable as necessary.

Task 2: Initialize and reload the switches.

Task 3: Configure basic settings for each switch.

Step 1: Disable DNS lookup.

Step 2: Configure the device name as displayed in the topology.

Step 3: Encrypt plain text passwords.

Step 4: Create a MOTD banner warning users that unauthorized access is prohibited.

Step 5: Assign **class** as the encrypted privileged EXEC mode password.

Step 6: Assign **cisco** as the console and vty password and enable login.

Step 7: Configure logging synchronous to prevent console message from interrupting command entry.

Step 8: Shut down all switchports except the ports connected to PCs.

Step 9: Configure VLAN 99 and name it **Management**.

Step 10: Configure VLAN 10 and name it **Staff**.

Step 11: Configure the switch ports with attached hosts as access ports in VLAN 10.

Step 12: Assign the IP addresses according to the Addressing Table.

Step 13: Copy the running configuration to startup configuration.

Task 4: Configure the PCs.

Assign IP addresses to the PCs according to the Addressing Table.

Part 2: Configure PAgP

PAgP is a Cisco proprietary protocol for link aggregation. In Part 2, a link between S1 and S3 will be configured using PAgP.

Task 1: Configure PAgP on S1 and S3.

For a link between S1 and S3, configure the ports on S1 with PAgP desirable mode and the ports on S3 with PAgP auto mode. Enable the ports after PAgP modes have been configured.

```
S1(config)# interface range f0/3-4
S1(config-if-range)# channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1

S1(config-if-range)# no shutdown

S3(config)# interface range f0/3-4
S3(config-if-range)# channel-group 1 mode auto
Creating a port-channel interface Port-channel 1

S3(config-if-range)# no shutdown
*Mar  1 00:09:12.792: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
*Mar  1 00:09:12.792: %LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to up
S3(config-if-range)#
*Mar  1 00:09:15.384: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up
*Mar  1 00:09:16.265: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4,
changed state to up
S3(config-if-range)#
*Mar  1 00:09:16.357: %LINK-3-UPDOWN: Interface Port-channell1, changed state to up
*Mar  1 00:09:17.364: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channell1,
changed state to up
*Mar  1 00:09:44.383: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

Task 2: Examine the configuration on the ports.

Currently the F0/3, F0/4, and Po1 (Port-channel1) interfaces on both S1 and S3 are in access operational mode with the administrative mode in dynamic auto. Verify the configuration using the **show run interface interface-id** and **show interfaces interface-id switchport** commands, respectively. The example configuration outputs for F0/3 on S1 are as follows:

```
S1# show run interface f0/3
Building configuration...

Current configuration : 103 bytes
!
interface FastEthernet0/3
  channel-group 1 mode desirable

S1# show interfaces f0/3 switchport
```

```

Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access (member of bundle Po1)
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

```

Task 3: Verify that the ports have been aggregated.

```

S1# show etherchannel summary

Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby  (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

```

```

Number of channel-groups in use: 1
Number of aggregators:          1

```

Group	Port-channel	Protocol	Ports
1	Po1 (SU)	PAgP	Fa0/3 (P) Fa0/4 (P)

S3# **show etherchannel summary**

```

Flags:  D - down          P - bundled in port-channel
        I - stand-alone  S - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

```

```

Number of channel-groups in use: 1
Number of aggregators:          1

```

Group	Port-channel	Protocol	Ports
1	Po1 (SU)	PAgP	Fa0/3 (P) Fa0/4 (P)

What do the flags, SU and P, indicate in the Ethernet summary?

Task 4: Configure trunk ports.

After the ports have been aggregated, commands applied at the port channel interface affect all the links that were bundled together. Manually configure the Po1 ports on S1 and S3 as trunk ports and assign them to native VLAN 99.

```

S1(config)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99

```

```

S3(config)# interface port-channel 1
S3(config-if)# switchport mode trunk
S3(config-if)# switchport trunk native vlan 99

```

Task 5: Verify that the ports are configured as trunk ports.

Step 1: Issue the **show run interface interface-id** commands on S1 and S3. What commands are listed for F0/3 and F0/4 on both switches? Compare the results to the running configuration for the Po1 interface? Record your observation.

Step 2: Issue the **show interfaces trunk** and **show spanning-tree** commands on S1 and S3. What trunk port is listed? What is the native VLAN? What is concluding result from the output?

From the **show spanning-tree** output, what is port cost and port priority for the aggregated link?

Part 3: Configure LACP

LACP is an open source protocol for link aggregation developed by the IEEE. In Part 3, the link between S1 and S2, and the link between S2 and S3 will be configured using LACP. Also, the individual links will be configured as trunks before they are bundled together as EtherChannels.

Task 1: Configure LACP between S1 and S2.

```
S1(config)# interface range f0/1-2
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport trunk native vlan 99
S1(config-if-range)# channel-group 2 mode active
Creating a port-channel interface Port-channel 2
```

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

```
S2(config)# interface range f0/1-2
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk native vlan 99
S2(config-if-range)# channel-group 2 mode passive
Creating a port-channel interface Port-channel 2
```

```
S2(config-if-range)# no shutdown
```

Task 2: Verify that the ports have been aggregated.

What protocol is Po2 using for link aggregation? Which ports are aggregated to form Po2? Record the command used to verify.

Task 3: Configure LACP between S2 and S3.

Step 1: Configure the link between S2 and S3 as Po3 and use LACP as the link aggregation protocol.

```
S2(config)# interface range f0/3-4
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk native vlan 99
S2(config-if-range)# channel-group 3 mode active
Creating a port-channel interface Port-channel 3
S2(config-if-range)# no shutdown
```

```
S3(config)# interface range f0/1-2
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# switchport trunk native vlan 99
S3(config-if-range)# channel-group 3 mode passive
Creating a port-channel interface Port-channel 3
```

```
S3(config-if-range)# no shutdown
```

Step 2: Verify that the EtherChannel has formed.

Task 4: Verify end-to-end connectivity.

Verify that all devices can ping each other within the same VLAN. If not, troubleshoot until there is end-to-end connectivity.

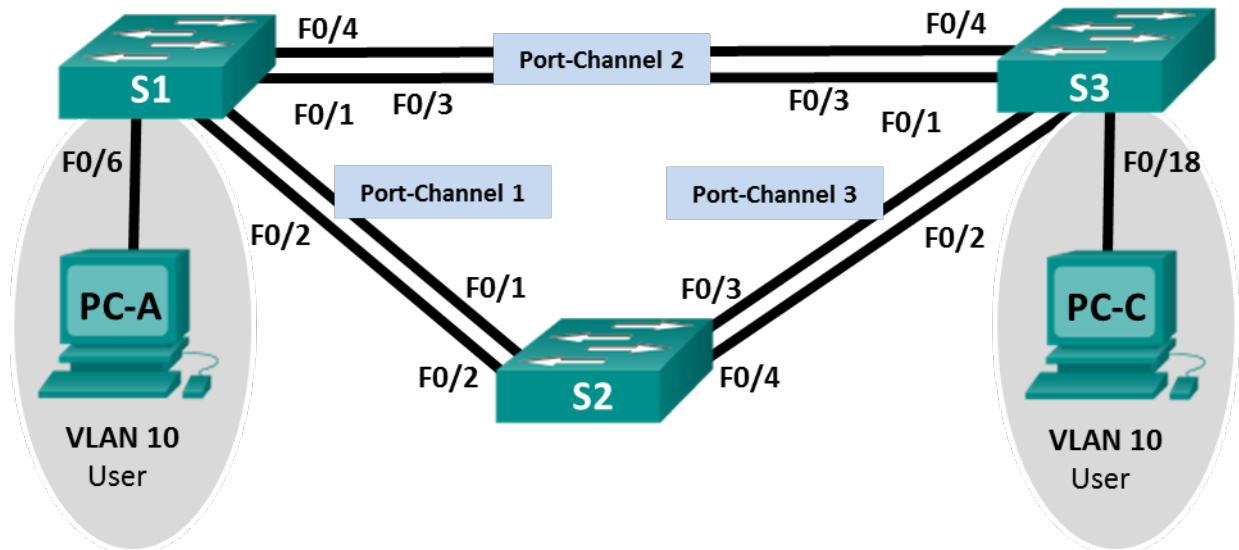
Note: It may be necessary to disable the PC firewall to ping between PCs.

Reflection

What could prevent EtherChannels from forming?

Lab 29: Troubleshooting EtherChannel

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 99	192.168.1.11	255.255.255.0
S2	VLAN 99	192.168.1.12	255.255.255.0
S3	VLAN 99	192.168.1.13	255.255.255.0
PC-A	NIC	192.168.0.2	255.255.255.0
PC-C	NIC	192.168.0.3	255.255.255.0

VLAN Assignments

VLAN	Name
10	User
99	Management

Objectives

Part 1: Build the Network and Load Device Configurations

Part 2: Troubleshoot EtherChannel

Background / Scenario

The switches at your company were configured by an inexperienced network administrator. Several errors in the configuration have resulted in speed and connectivity issues. Your manager has asked you to troubleshoot and correct the configuration errors and document your work. Using your knowledge of EtherChannel and standard

testing methods, find and correct the errors. Ensure that all of the EtherChannels use Port Aggregation Protocol (PAgP), and that all hosts are reachable.

Note: The switches used are Cisco Catalyst 2960s 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 switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with a 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: Build the Network and Load Device Configurations

In Part 1, you will set up the network topology, configure basic settings on the PC hosts, and load configurations on the switches.

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

Task 2: Configure the PC hosts.

Task 3: Erase the startup and VLAN configurations and reload the switches.

Task 4: Load switch configurations.

Load the following configurations into the appropriate switch. All switches have the same passwords. The privileged EXEC password is **class**. The password for console and vty access is **cisco**. As all switches are Cisco devices, the network administrator decided to use Cisco's PAgP on all port channels configured with EtherChannel. Switch S2 is the root bridge for all VLANs in the topology.

Switch S1 Configuration:

```
hostname S1
interface range f0/1-24, g0/1-2
shutdown
exit
enable secret class
no ip domain lookup
line vty 0 15
password cisco
login
line con 0
password cisco
logging synchronous
login
exit
vlan 10
name User
```

```
vlan 99
  Name Management
interface range f0/1-2
  switchport mode trunk
  channel-group 1 mode active
  switchport trunk native vlan 99
  no shutdown
interface range f0/3-4
  channel-group 2 mode desirable
  switchport trunk native vlan 99
  no shutdown
interface f0/6
  switchport mode access
  switchport access vlan 10
  no shutdown
interface vlan 99
  ip address 192.168.1.11 255.255.255.0
interface port-channel 1
  switchport trunk native vlan 99
  switchport mode trunk
interface port-channel 2
  switchport trunk native vlan 99
  switchport mode access
```

Switch S2 Configuration:

```
hostname S2
interface range f0/1-24, g0/1-2
  shutdown
  exit
enable secret class
no ip domain lookup
line vty 0 15
  password cisco
  login
line con 0
  password cisco
  logging synchronous
  login
  exit
vlan 10
  name User
vlan 99
  name Management
spanning-tree vlan 1,10,99 root primary
interface range f0/1-2
  switchport mode trunk
  channel-group 1 mode desirable
```

```
switchport trunk native vlan 99
no shutdown
interface range f0/3-4
switchport mode trunk
channel-group 3 mode desirable
switchport trunk native vlan 99
interface vlan 99
ip address 192.168.1.12 255.255.255.0
interface port-channel 1
switchport trunk native vlan 99
switchport trunk allowed vlan 1,99
interface port-channel 3
switchport trunk native vlan 99
switchport trunk allowed vlan 1,10,99
switchport mode trunk
```

Switch S3 Configuration:

```
hostname S3
interface range f0/1-24, g0/1-2
shutdown
exit
enable secret class
no ip domain lookup
line vty 0 15
password cisco
login
line con 0
password cisco
logging synchronous
login
exit
vlan 10
name User
vlan 99
name Management
interface range f0/1-2
interface range f0/3-4
switchport mode trunk
channel-group 3 mode desirable
switchport trunk native vlan 99
no shutdown
interface f0/18
switchport mode access
switchport access vlan 10
no shutdown
interface vlan 99
ip address 192.168.1.13 255.255.255.0
```

```
interface port-channel 3
  switchport trunk native vlan 99
  switchport mode trunk
```

Task 5: Save your configuration.

Part 2: Troubleshoot EtherChannel

In Part 2, you must examine the configurations on all switches, make corrections if needed, and verify full functionality.

Task 1: Troubleshoot S1.

Step 1: Use the **show interfaces trunk** command to verify that the port channels are functioning as trunk ports.

Do port channels 1 and 2 appear as trunked ports? _____

Step 2: Use the **show etherchannel summary** command to verify that interfaces are configured in the correct port channel, the proper protocol is configured, and the interfaces are in use.

Based on the output, are there any EtherChannel issues? If issues are found, record them in the space provided below.

Step 3: Use the command **show run | begin interface Port-channel** command to view the running configuration beginning with the first port channel interface.

Step 4: Resolve all problems found in the outputs from the previous **show** commands. Record the commands used to correct the configurations.

Step 5: Use the **show interfaces trunk** command to verify trunk settings.

Step 6: Use the **show etherchannel summary** command to verify that the port channels are up and in use.

Task 2: Troubleshoot S2.

Step 1: Issue the command to verify that the port channels are functioning as trunk ports. Record the command used in the space provided below.

Based on the output, are there any issues with the configurations? If issues are found, record them in the space provided below.

Step 2: Issue the command to verify that interfaces are configured in the correct port channel and the proper protocol is configured.

Based on the output, are there any EtherChannel issues? If issues are found, record them in the space provided below.

Step 3: Use the command **show run | begin interface Port-channel** to view the running configuration beginning with the first port-channel interface.

Step 4: Resolve all problems found in the outputs from the previous **show** commands. Record the commands used to correct the configuration.

Step 5: Issue the command to verify trunk settings.

Step 6: Issue the command to verify that the port channels are functioning. Remember that port channel issues can be caused by either end of the link.

Task 3: Troubleshoot S3.

Step 1: Issue the command to verify that the port channels are functioning as trunk ports.

Based on the output, are there any issues with the configurations? If issues are found, record them in the space provided below.

Step 2: Issue the command to verify that the interfaces are configured in the correct port channel and that the proper protocol is configured.

Based on the output, are there any EtherChannel issues? If issues are found, record them in the space provided below.

Step 3: Use the command **show run | begin interface Port-channel** command to view the running configuration beginning with the first port channel interface.

Step 4: Resolve all problems found. Record the commands used to correct the configuration.

Step 5: Issue the command to verify trunk settings. Record the command used in the space provided below.

Step 6: Issue the command to verify that the port channels are functioning. Record the command used in the space provided below.

Task 4: Verify EtherChannel and Connectivity.

Step 1: Use the **show interfaces etherchannel** command to verify full functionality of the port channels.

Step 2: Verify connectivity of the management VLAN.

Can S1 ping S2? _____

Can S1 ping S3? _____

Can S2 ping S3? _____

Step 3: Verify connectivity of PCs.

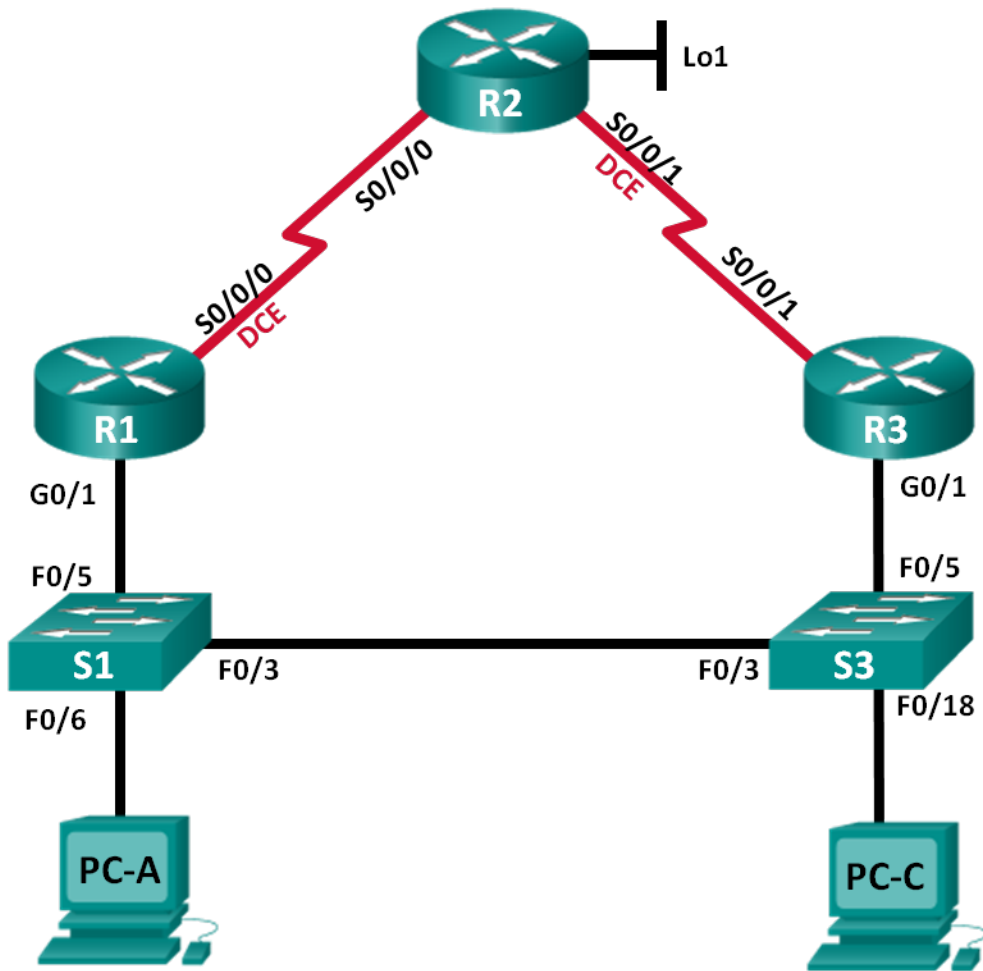
Can PC-A ping PC-C? _____

If EtherChannels are not fully functional, connectivity between switches does not exist, or connectivity between hosts does not exist. Troubleshoot to resolve any remaining issues.

Note: It may be necessary to disable the PC firewall for pings between the PCs to succeed.

Lab 30: Configuring HSRP

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	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
	Lo1	209.165.200.225	255.255.255.224	N/A
R3	G0/1	192.168.1.3	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.13	255.255.255.0	192.168.1.3
PC-A	NIC	192.168.1.31	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.33	255.255.255.0	192.168.1.3

Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure First Hop Redundancy using HSRP

Background / Scenario

Spanning tree provides loop-free redundancy between switches within a LAN. However, it does not provide redundant default gateways for end-user devices within the network if one of the routers fails. First Hop Redundancy Protocols (FHRPs) provide redundant default gateways for end devices with no end-user configuration necessary. In this lab, you will configure Cisco's Hot Standby Routing Protocol (HSRP), a First Hop Redundancy Protocol (FHRP).

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

- 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)
- 2 PCs (Windows 8, 7, or Vista 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 Verify Connectivity

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

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

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Configure PC hosts.

Step 3: Initialize and reload the routers and switches as necessary.

Step 4: Configure basic settings for each router.

Step 5: Disable DNS lookup.

Step 6: Configure the device name as shown in the topology.

Step 7: Configure IP addresses for the routers as listed in the Addressing Table.

Step 8: Set clock rate to **128000** for all DCE serial interfaces.

Step 9: Assign **class** as the encrypted privileged EXEC mode password.

Step 10: Assign **cisco** for the console and vty password and enable login.

Step 11: Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 12: Copy the running configuration to the startup configuration.

Step 13: Configure basic settings for each switch.

Step 14: Disable DNS lookup.

Step 15: Configure the device name as shown in the topology.

Step 16: Assign **class** as the encrypted privileged EXEC mode password.

Step 17: Configure IP addresses for the switches as listed in the Addressing Table.

Step 18: Configure the default gateway on each switch.

Step 19: Assign **cisco** for the console and vty password and enable login.

Step 20: Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 21: Copy the running configuration to the startup configuration.

Step 22: Verify connectivity between PC-A and PC-C.

Ping from PC-A to PC-C. Were the ping results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

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

Step 23: Configure routing.

Step 24: Configure RIP version 2 on all routers. Add all the networks, except 209.165.200.224/27 into the RIP process.

Step 25: Configure a default route on R2 using Lo1 as the exit interface to 209.165.200.224/27 network.

Step 26: On R2, use the following commands to redistribute the default route into the RIP process.

```
R2(config)# router rip
R2(config-router)# default-information originate
```

Step 27: Verify connectivity.

Step 28: From PC-A, you should be able to ping every interface on R1, R2, R3, and PC-C. Were all pings successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 29: From PC-C, you should be able to ping every interface on R1, R2, R3, and PC-A. Were all pings successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Part 2: Configure First Hop Redundancy Using HSRP

Even though the topology has been designed with some redundancy (two routers and two switches on the same LAN network), both PC-A and PC-C are configured with only one gateway address. PC-A is using R1 and PC-C is using R3. If either of these routers or the interfaces on the routers went down, the PC could lose its connection to the Internet.

In Part 2, you will test how the network behaves both before and after configuring HSRP. To do this, you will determine the path that packets take to the loopback address on R2.

Step 1: Determine the path for Internet traffic for PC-A and PC-C.

Step 2: From a command prompt on PC-A, issue a **tracert** command to the 209.165.200.225 loopback address of R2.

```
C:\ tracert 209.165.200.225
Tracing route to 209.165.200.225 over a maximum of 30 hops

  1      1 ms      1 ms      1 ms  192.168.1.1
  2     13 ms     13 ms     13 ms  209.165.200.225
```

Trace complete.

What path did the packets take from PC-A to 209.165.200.225?

Step 3: From a command prompt on PC-C, issue a **tracert** command to the 209.165.200.225 loopback address of R2.

What path did the packets take from PC-C to 209.165.200.225?

Step 4: Start a ping session on PC-A, and break the connection between S1 and R1.

Step 5: From a command prompt on PC-A, issue a **ping -t** command to the 209.165.200.225 address on R2. Make sure you leave the command prompt window open.

Note: The pings continue until you press **Ctrl+C**, or until you close the command prompt window.

```
C:\ ping -t 209.165.200.225
Pinging 209.165.200.225 with 32 bytes of data:
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
<output omitted>
```

Step 6: As the ping continues, disconnect the Ethernet cable from F0/5 on S1. You can also shut down the S1 F0/5 interface, which creates the same result.

What happened to the ping traffic?

Step 7: Would be the results if you repeat Steps 2a and 2b on PC-C and S3?

Step 8: Reconnect the Ethernet cables to F0/5 or enable the F0/5 interface on both S1 and S3, respectively. Re-issue pings to 209.165.200.225 from both PC-A and PC-C to make sure connectivity is re-established.

Step 9: Configure HSRP on R1 and R3.

In this step, you will configure HSRP and change the default gateway address on PC-A, PC-C, S1, and S2 to the virtual IP address for HSRP. R1 becomes the active router via configuration of the HSRP priority command.

Step 10: Configure HSRP on R1.

```
R1(config)# interface g0/1
R1(config-if)# standby version 2
R1(config-if)# standby 1 ip 192.168.1.254
R1(config-if)# standby 1 priority 150
R1(config-if)# standby 1 preempt
```

Step 11: Configure HSRP on R3.

```
R3(config)# interface g0/1
R3(config-if)# standby version 2
R3(config-if)# standby 1 ip 192.168.1.254
```

Step 12: Verify HSRP by issuing the **show standby** command on R1 and R3.

```
R1# show standby
GigabitEthernet0/1 - Group 1 (version 2)
  State is Active
    4 state changes, last state change 00:00:30
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0c9f.f001
    Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.696 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.3, priority 100 (expires in 11.120 sec)
  Priority 150 (configured 150)
  Group name is "hsrp-Gi0/1-1" (default)
```

```
R3# show standby
GigabitEthernet0/1 - Group 1 (version 2)
  State is Standby
    4 state changes, last state change 00:02:29
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0c9f.f001
    Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
```

```

Next hello sent in 0.720 secs
Preemption disabled
Active router is 192.168.1.1, priority 150 (expires in 10.128 sec)
MAC address is d48c.b5ce.a0c1
Standby router is local
Priority 100 (default 100)
Group name is "hsrp-Gi0/1-1" (default)

```

Using the output shown above, answer the following questions:

Which router is the active router? _____

What is the MAC address for the virtual IP address? _____

What is the IP address and priority of the standby router?

Step 13: Use the **show standby brief** command on R1 and R3 to view an HSRP status summary. Sample output is shown below.

R1# **show standby brief**

```

P indicates configured to preempt.
|
Interface  Grp  Pri P State  Active          Standby          Virtual IP
Gi0/1      1    150 P Active  local          192.168.1.3     192.168.1.254

```

R3# **show standby brief**

```

P indicates configured to preempt.
|
Interface  Grp  Pri P State  Active          Standby          Virtual IP
Gi0/1      1    100 Standby 192.168.1.1    local          192.168.1.254

```

Step 14: Change the default gateway address for PC-A, PC-C, S1, and S3. Which address should you use?

Step 15: Verify the new settings. Issue a ping from both PC-A and PC-C to the loopback address of R2. Are the pings successful? _____

Step 16: Start a ping session on PC-A and break the connection between the switch that is connected to the Active HSRP router (R1).

Step 17: From a command prompt on PC-A, issue a **ping -t** command to the 209.165.200.225 address on R2. Ensure that you leave the command prompt window open.

Step 18: As the ping continues, disconnect the Ethernet cable from F0/5 on S1 or shut down the F0/5 interface. What happened to the ping traffic?

Step 19: Verify HSRP settings on R1 and R3.

Step 20: Issue the **show standby brief** command on R1 and R3.

Which router is the active router? _____ Reconnect the cable between the switch and the router or enable interface F0/5. Now which router is the active router? Explain.

Step 21: Change HSRP priorities.

Step 22: Change the HSRP priority to 200 on R3. Which is the active router? _____

Step 23: Issue the command to change the active router to R3 without changing the priority. What command did you use?

Step 24: Use a **show** command to verify that R3 is the active router.

Reflection

Why would there be a need for redundancy in a LAN?

Appendix – Configure and Verify Password Recovery

Topology



Objectives

Part 1: Configure Basic Device Settings

Part 2: Reboot Router and Enter ROMMON

Part 3: Reset Password and Save New Configuration

Part 4: Verify the Router is Loading Correctly

Background / Scenario

The purpose of this lab is to reset the enable password on a specific Cisco router. The enable password protects access to privileged EXEC and configuration mode on Cisco devices. The enable password can be recovered, but the enable secret password is encrypted and will need to be replaced with a new password.

In order to bypass a password, a user must be familiar with the ROM monitor (ROMMON) mode, as well as the configuration register setting for Cisco routers. ROMMON is basic CLI software stored in ROM that can be used to troubleshoot boot errors and recover a router when an IOS is not found.

In this lab, you will change the configuration register in order to reset the enable password on a Cisco router.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cable to connect to the Cisco IOS device via the console port

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and copy the basic configuration into R1. The password is encrypted to setup the scenario of needing to recover from an unknown enabled password.

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

Step 2: Initialize and reload the routers as necessary.

Step 3: Configure basic settings on the router.

- Console into the router and enter global configuration mode.
- Copy the following basic configuration and paste it to the running-configuration on the router.

```
no ip domain-lookup
service password-encryption
hostname R1
enable secret 5 $1$SBb4$n.EuL28kPTzxMLFiyMLl5/
```

```

banner motd #
Unauthorized access is strictly prohibited. #
line con 0
logging sync
end
write
exit

```

- c. Press **Enter** and try to enable Privileged Exec mode.

As you can see, access to a Cisco IOS device is very limited if the enable password is unknown. It is important for a network engineer to be able to recover from an unknown enable password issue on a Cisco IOS device.

Part 2: Reboot Router and Enter ROMMON

Step 1: Reboot the router.

- a. While still consoled into R1, remove the power cord from the back of R1.
- Note:** If you are working in a NETLAB pod, ask your instructor how to power cycle the router.
- b. From the console session on PC-A, issue a hard break to interrupt the routers normal boot process and enter ROMMON mode.

Note: To issue a hard break in Tera Term, press the **Alt** and the **B** keys simultaneously.

Step 2: Reset the configuration register.

- a. From the ROMMON prompt, type a **?**, then press **Enter**. This will display a list of available ROMMON commands. Look for the **confreg** command in this list.

```

rommon 1 > ?
alias                set and display aliases command
boot                 boot up an external process
break                set/show/clear the breakpoint
confreg              configuration register utility
cont                 continue executing a downloaded image
context              display the context of a loaded image
cookie               display contents of motherboard cookie PROM in hex
dev                  list the device table
dir                  list files in file system
frame                print out a selected stack frame
help                 monitor builtin command help
history              monitor command history
iomemset              set IO memory percent
meminfo              main memory information
repeat               repeat a monitor command
reset                system reset
rommon-pref           Select ROMMON
set                  display the monitor variables
showmon              display currently selected ROM monitor
stack                produce a stack trace
sync                 write monitor environment to NVRAM
sysret               print out info from last system return
tftpdnld              tftp image download

```

```

unalias          unset an alias
unset            unset a monitor variable
hwpart           Read HW resources partition
rommon 2 >

```

Note: The number at the end of the ROMMON prompt will increment by one each time a command is entered.

- b. Type **confreg 0x2142** and press **Enter**. Changing the register to Hex 2142 tells the router not to automatically load the startup configuration when booting. The router will need to be rebooted for the configuration register change to take effect.

```
rommon 2 > confreg 0x2142
```

You must reset or power cycle for new config to take effect

```
rommon 3 >
```

- c. Issue the **reset** ROMON command to reboot the router.

```
rommon 3 > reset
```

System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 2011 by cisco Systems, Inc.

```
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled
```

```

Readonly ROMMON initialized
program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

```

IOS Image Load Test

[illegible]

- d. When asked if you would like to enter the initial configuration dialog, type **no** and press **Enter**.
Would you like to enter the initial configuration dialog? [yes/no]: **no**
- e. The router will complete its boot process and display the User Exec prompt. Enter Privileged Exec mode.
Router> **enable**

Router#

Part 3: Reset Password and Save New Configuration

- a. While in Privileged Exec mode, copy the startup configuration to the running configuration.

```
Router# copy startup-config running-config
Destination filename [running-config]?
1478 bytes copied in 0.272 secs (5434 bytes/sec)
```

R1#

- b. Enter global configuration mode.
- c. Reset the enable secret password to **cisco**.
- d. Reset the configuration register back to 0x2102 to allow the startup configuration to automatically load the next time the router is rebooted.

```
R1(config)# config-register 0x2102
```

- e. Exit global configuration mode.
- f. Copy the running configuration to the startup configuration.

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

You have successfully reset the enable password on a router.

Part 4: Verify the Router is Loading Correctly

Step 1: Reboot R1.

Step 2: Verify that the startup configuration loaded automatically.

Step 3: Enter Privileged Exec mode.

The new enable secret password should be cisco. If you are able to enter Privileged Exec mode, then you have successfully completed this lab.

Reflection

Why is it of critical importance that a router be physically secured to prevent unauthorized access?
