



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

Advanced Routing and Switching Lab Manual

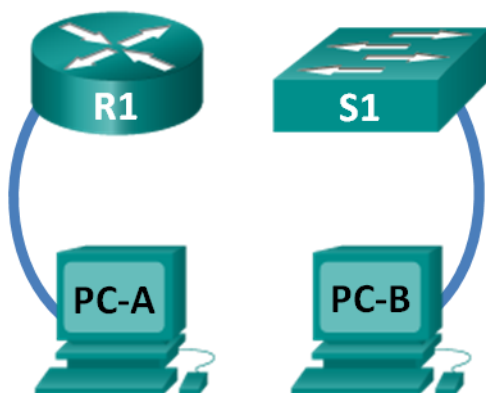
ACCA6010

Computer Networks and Cyber Security
Applied Computing Portfolio
Wales Institute of Science and Art
University of Wales Trinity Saint David
Swansea.

Module Leader
Dr Kapilan Radhakrishnan

Lab 1 - Initializing and Reloading a Router and Switch

Topology



Objectives

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

Part 2: Initialize the Router and Reload

Part 3: Initialize the Switch and Reload

Background / Scenario

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

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

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS software, Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports

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

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

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

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

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

Part 2: Initialize the Router and Reload

Step 1: Connect to the router.

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

```
Router> enable
Router#
```

Step 2: Erase the startup configuration file from NVRAM.

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

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

Step 3: Reload the router.

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

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

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

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

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

Step 4: Bypass the initial configuration dialog.

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

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

Step 5: Terminate the autoinstall program.

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

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

Part 3: Initialize the Switch and Reload

Step 1: Connect to the switch.

Console into the switch and enter privileged EXEC mode.

```
Switch> enable
Switch#
```

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

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

```
Switch# show flash
```

```
Directory of flash:/
```

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

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

```
Switch#
```

Step 3: Delete the VLAN file.

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

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

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

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

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

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

```
Switch#
```

Step 4: Erase the startup configuration file.

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

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

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

```
[OK]
```

```
Erase of nvram: complete
```

```
Switch#
```

Step 5: Reload the switch.

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

```
Switch# reload
```

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

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

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

Step 6: Bypass the initial configuration dialog.

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

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

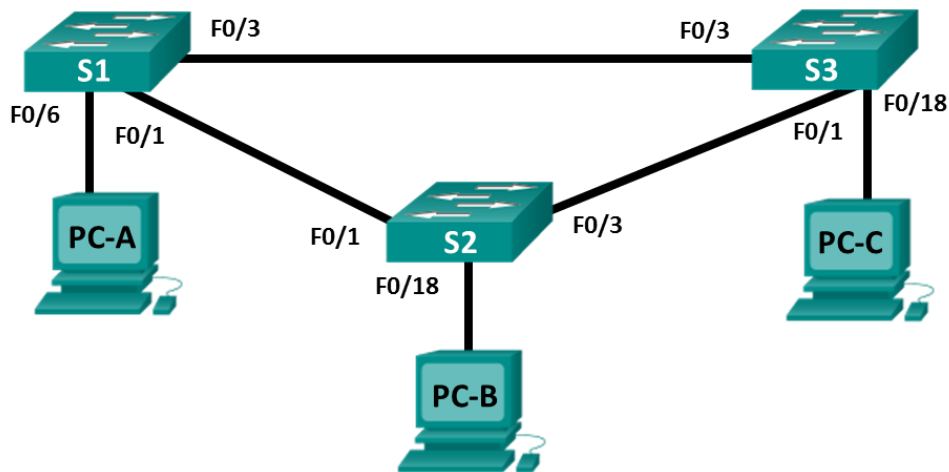
Reflection

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

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

Lab 2 – 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**.

- 1) 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
```

- 2) 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
```

- 3) 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

a. Configure dynamic trunk links between S1 and S2.

1) Enter the **show interfaces f0/1 switchport** command on S1 and S2.

What is the administrative and operational mode of switchport f0/1?

2) 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
```

3) 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     1
```

b. Configure static trunk link between S1 and S3.

- 1) 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
```

- 2) 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
```

- 3) Configure a permanent trunk between S2 and S3.
- 4) Record the commands you used to create the static trunk.

Part 3: Add VLANs and Assign Ports

a. Add VLANs on the switches.

- 1) On S1, add VLAN 10.

```
S1(config)# vlan 10
```

Were you able to create VLAN 10 on S1? Explain.

- 2) 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>

b. 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?

c. 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

- 1) 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
```

- 2) Repeat the procedure for switchport F0/18 on S2 and S3. Assign the VLAN according to the table above.
- 3) Assign the IP addresses to the PCs according to the table above.

d. Configure IP addresses on the switches.

- 1) 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
```

- 2) Repeat step a. for S2 and S3.

e. Verify end-to-end connectivity

- 1) Ping PC-A from PC-B. Was it successful? Explain.

-
- 2) Ping PC-A from PC-C. Was it successful? Explain.

-
- 3) Ping PC-A from S1. Was it successful? Explain.

-
- 4) 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.

a. Configure VTP mode to transparent on S1.

- 1) On switch S1, set VTP mode to transparent.

```
S1(config)# vtp mode transparent
Setting device to VTP Transparent mode for VLANs.
S1(config)# exit
```

2) 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
```

b. Configure an extended VLAN on S1.

1) Display the current VLAN configurations on S1.

2) 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**

3) 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

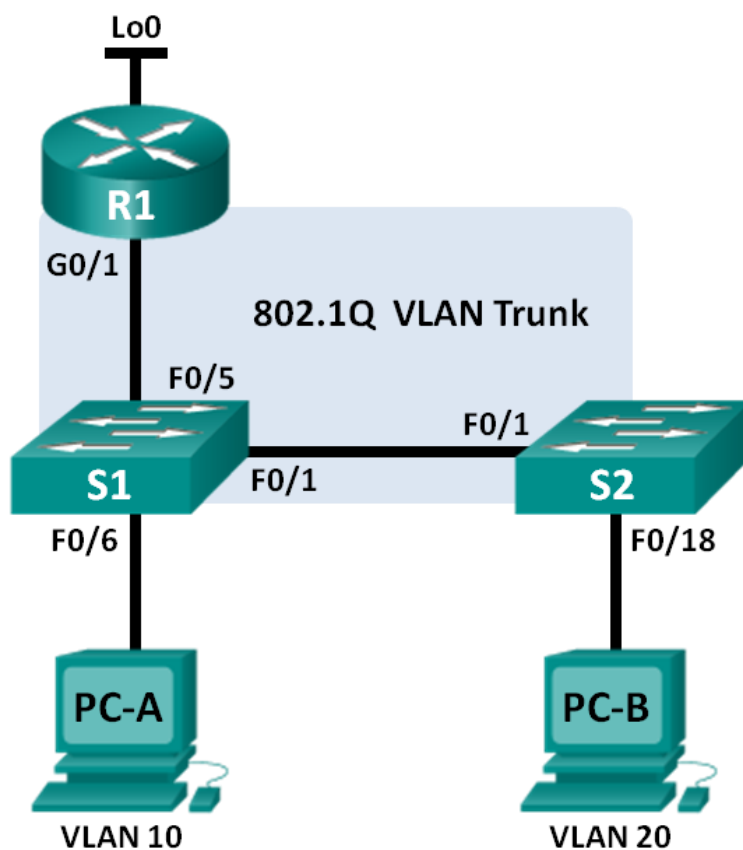
What are the advantages and disadvantages of using VTP?

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.				

Lab 3 – Troubleshooting 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 – R&D	192.168.10.0/24
S2 F0/18	VLAN 20 – Engineering	192.168.20.0/24

Objectives

Part 1: Build the Network and Load Device Configurations

Part 2: Troubleshoot the Inter-VLAN Routing Configuration

Part 3: Verify VLAN Configuration, Port Assignment, and Trunking

Part 4: Test Layer 3 Connectivity

Background / Scenario

The network has been designed and configured to support three VLANs. Inter-VLAN routing is provided by an external router using an 802.1Q trunk, also known as router-on-a-stick. Routing to a remote web server, which is simulated by Lo0, is also provided by R1. However, it is not working as designed, and user complaints have not given much insight into the source of the problems.

In this lab, you must first define what is not working as expected, and then analyze the existing configurations to determine and correct the source of the problems. This lab is complete when you can demonstrate IP connectivity between each of the user VLANs and the external web server network, and between the switch management VLAN and the web server network.

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 (Microsoft Windows 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

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.

Refer to the Addressing Table for PC host address information.

Step 3: Load router and switch configurations.

Load the following configurations into the appropriate router or switch. All devices have the same passwords; the enable password is **class**, and the line password is **cisco**.

Router R1 Configuration:

```
hostname R1
enable secret class
no ip domain lookup
line con 0
  password cisco
  login
  logging synchronous
line vty 0 4
  password cisco
  login
interface loopback0
  ip address 209.165.200.225 255.255.255.224
interface gigabitEthernet0/1
  no ip address
interface gigabitEthernet0/1.1
  encapsulation dot1q 11
  ip address 192.168.1.1 255.255.255.0
interface gigabitEthernet0/1.10
  encapsulation dot1q 10
```

```
ip address 192.168.11.1 255.255.255.0
interface gigabitEthernet0/1.20
encapsulation dot1q 20
ip address 192.168.20.1 255.255.255.0
end
```

Switch S1 Configuration:

```
hostname S1
enable secret class
no ip domain-lookup
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
vlan 10
name R&D
exit
interface fastethernet0/1
switchport mode access
interface fastethernet0/5
switchport mode trunk
interface vlan1
ip address 192.168.1.11 255.255.255.0
ip default-gateway 192.168.1.1
end
```

Switch S2 Configuration:

```
hostname S2
enable secret class
no ip domain-lookup
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
vlan 20
name Engineering
exit
interface fastethernet0/1
switchport mode trunk
interface fastethernet0/18
```

```
switchport access vlan 10
switchport mode access
interface vlan1
ip address 192.168.1.12 255.255.255.0
ip default-gateway 192.168.1.1
end
```

Step 4: Save the running configuration to the startup configuration.

Part 2: Troubleshoot the Inter-VLAN Routing Configuration

In Part 2, you will verify the inter-VLAN routing configuration.

- a. On R1, enter the **show ip route** command to view the routing table.

Which networks are listed? _____

Are there any networks missing in the routing table? If so, which networks?

What is one possible reason that a route would be missing from the routing table?

- b. On R1, issue the **show ip interface brief** command.

Based on the output, are there any interface issues on the router? If so, what commands would resolve the issues?

- c. On R1, re-issue the **show ip route** command.

Verify that all networks are available in the routing table. If not, continue to troubleshoot until all networks are present.

Part 3: Verify VLAN Configuration, Port Assignment, and Trunking

In Part 3, you will verify that the correct VLANs exist on both S1 and S2 and that trunking is configured correctly.

Step 1: Verify VLAN configuration and port assignments.

- a. On S1, enter the **show vlan brief** command to view the VLAN database.

Which VLANs are listed? Ignore VLANs 1002 to 1005.

Are there any VLANs numbers or names missing in the output? If so, list them.

Are the access ports assigned to the correct VLANs? If not, list the missing or incorrect assignments.

If required, what commands would resolve the VLAN issues?

- b. On S1, re-issue the **show vlan brief** command to verify configuration.
- c. On S2, enter the **show vlan brief** command to view the VLAN database.
Which VLANs are listed? Ignore VLANs 1002 to 1005.

Are there any VLANs numbers or names missing in the output? If so, list them.

Are the access ports assigned to the correct VLANs? If not, list the missing or incorrect assignments.

If required, what commands would resolve the VLAN issues?

- d. On S2, re-issue the **show vlan brief** command to verify any configuration changes.

Step 2: Verify trunking interfaces.

- a. On S1, enter the **show interface trunk** command to view the trunking interfaces.

Which ports are in trunking mode? _____

Are there any ports missing in the output? If so, list them. _____

If required, what commands would resolve the port trunking issues?

- b. On S1, re-issue the **show interface trunk** command to verify any configuration changes.

- c. On S2, enter the **show interface trunk** command to view the trunking interfaces.

Which ports are in trunking mode? _____

Are there any ports missing in the output? If so, list them. _____

If required, what commands would resolve the port trunking issues?

Part 4: Test Layer 3 Connectivity

- a. Now that you have corrected multiple configuration issues, let's test connectivity.

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? _____

If the answer is **no** to any of these questions, troubleshoot the configurations and correct the error.

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

From PC-A, is it possible to ping S1? _____

From PC-A, is it possible to ping S2? _____

List some of the issues that could still be preventing successful pings to the switches.

- b. One way to help resolve where the error is occurring is to do a **tracert** from PC-A to S1.

```
C:\Users\User1> tracert 192.168.1.11
```

```
Tracing route to 192.168.1.11 over a maximum of 30 hops
```

```
 1    <1 ms    <1 ms    <1 ms    192.168.10.1
 2      *        *        *        Request timed out.
 3      *        *        *        Request timed out.
```

```
<output omitted>
```

This output shows that the request from PC-A is reaching the default gateway on R1 g0/1.10, but the packet stops at the router.

- c. You have already verified the routing table entries for R1, now execute the **show run | section interface** command to verify VLAN configuration. List any configuration errors.

What commands would resolve any issues found?

- d. Verify that that pings from PC-A now reach both S1 and S2.

From PC-A, is it possible to ping S1? _____

From PC-A, is it possible to ping S2? _____

Reflection

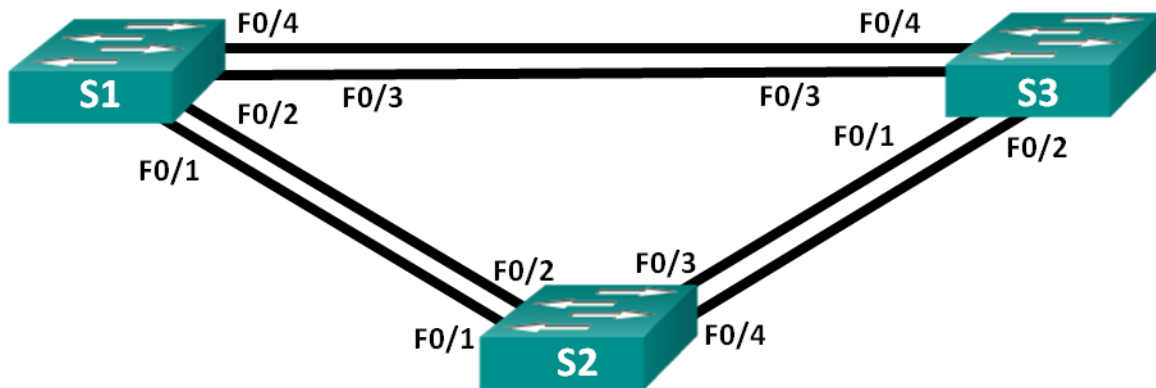
What are the advantages of viewing the routing table for troubleshooting purposes?

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.				

Lab 4 – 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.

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.

- Disable DNS lookup.
- Configure the device name as shown in the topology.
- Assign **class** as the encrypted privileged EXEC mode password.
- Assign **cisco** as the console and vty passwords and enable login for console and vty lines.
- Configure logging synchronous for the console line.
- Configure a message of the day (MOTD) banner to warn users that unauthorized access is prohibited.
- Configure the IP address listed in the Addressing Table for VLAN 1 on all switches.
- Copy the running configuration to the startup configuration.

Step 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.

Step 1: Deactivate all ports on the switches.

Step 2: Configure connected ports as trunks.

Step 3: Activate ports F0/2 and F0/4 on all switches.

Step 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

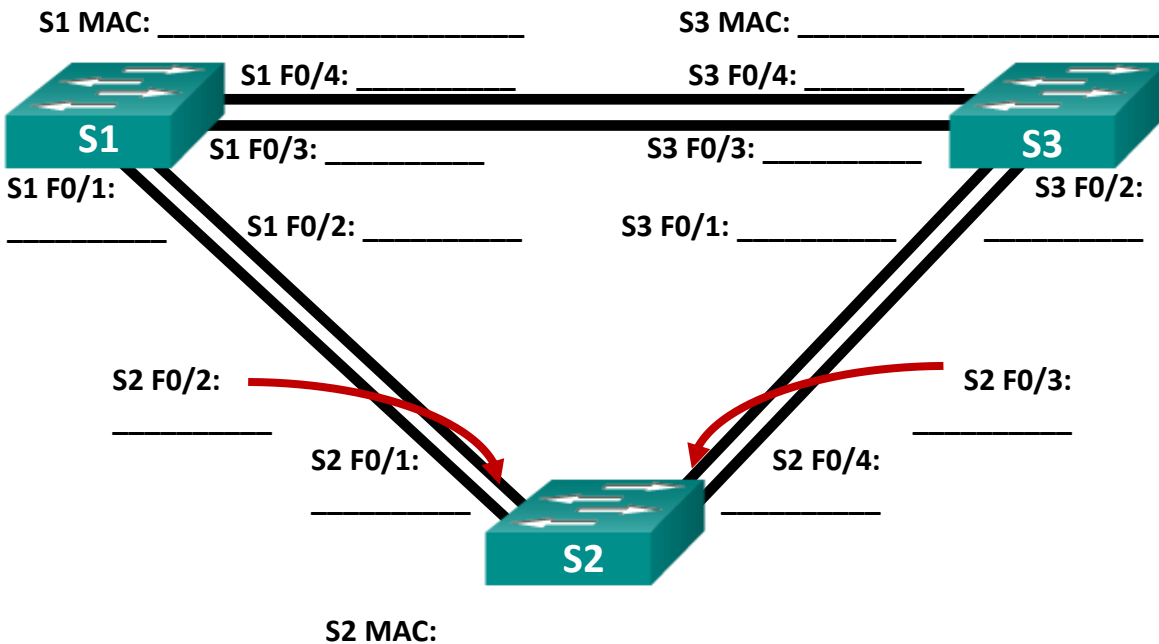
Root ID Priority 32769
 Address 0cd9.96d2.4000
 Cost 19
 Port 2 (FastEthernet0/2)
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

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.

Step 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.

Step 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
```

Step 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?

Step 4: Remove port cost changes.

- 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

```
- 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.

- Activate ports F0/1 and F0/3 on all switches.
- 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

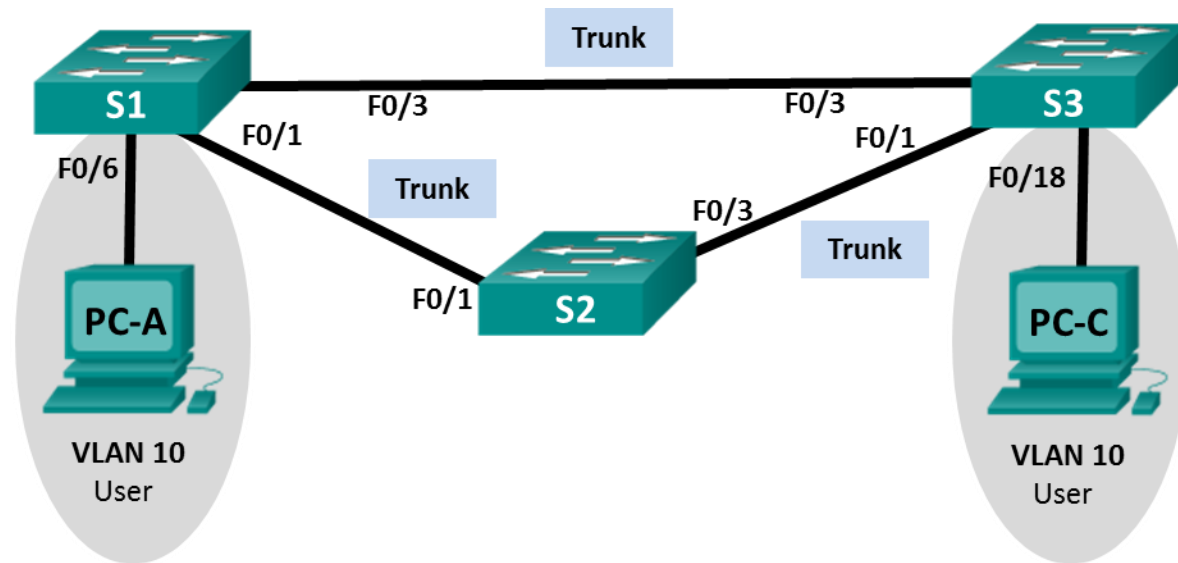
1. After a root bridge has been selected, what is the first value STP uses to determine port selection?

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 5 – 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.

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

Step 2: Configure PC hosts.

Step 3: Initialize and reload the switches as necessary.

Step 4: Configure basic settings for each switch.

- Disable DNS lookup.
- Configure the device name as shown in the Topology.
- Assign **cisco** as the console and vty passwords and enable login.
- Assign **class** as the encrypted privileged EXEC mode password.
- Configure **logging synchronous** to prevent console messages from interrupting command entry.
- Shut down all switch ports.
- 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.

Step 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
```

Step 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.

Step 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.

Step 4: Configure the management interface on all switches.

Using the Addressing Table, configure the management interface on all switches with the appropriate IP address.

Step 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.

Step 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?

Step 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.

- a. Configure switch S2 to be the primary root bridge for all existing VLANs. Write the command in the space provided.
-

- b. 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? _____

Step 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.

- a. 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
```

- b. 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.

Step 1: Configure Rapid PVST+.

- a. Configure S1 for Rapid PVST+. Write the command in the space provided.

- b. Configure S2 and S3 for Rapid PVST+.

- c. 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
```

Step 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.

- a. Configure interface F0/6 on S1 with PortFast. Write the command in the space provided.

- b. Configure interface F0/6 on S1 with BPDU guard. Write the command in the space provided.

- c. Globally configure all non-trunking ports on switch S3 with PortFast. Write the command in the space provided.

- d. Globally configure all non-trunking PortFast ports on switch S3 with BPDU guard. Write the command in the space provided.

Step 3: Examine Rapid PVST+ convergence.

- Enter the **debug spanning-tree events** command in privileged EXEC mode on switch S3.
- 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

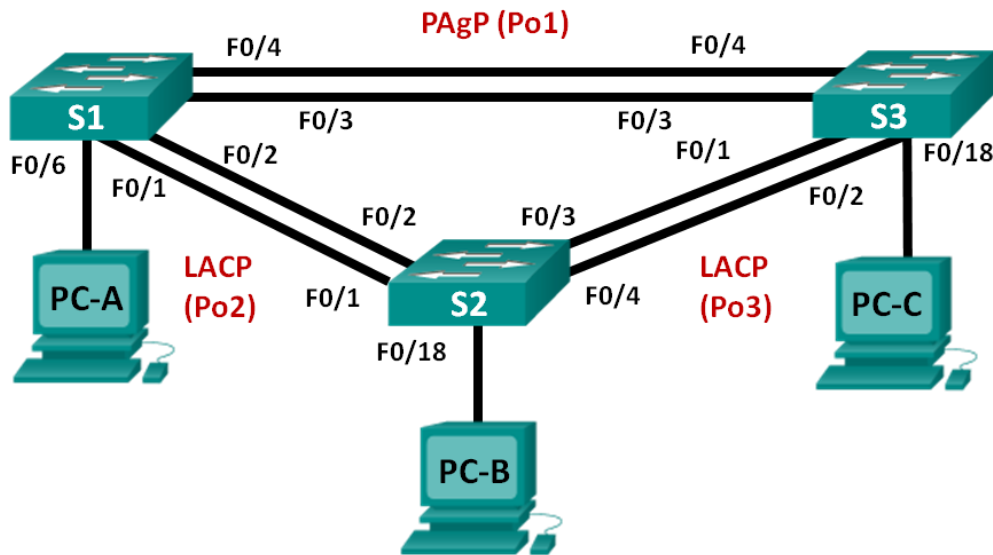
```

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 6 – 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.

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.

Step 3: Configure basic settings for each switch.

- Disable DNS lookup.
- Configure the device name as displayed in the topology.
- Encrypt plain text passwords.
- Create a MOTD banner warning users that unauthorized access is prohibited.
- Assign **class** as the encrypted privileged EXEC mode password.
- Assign **cisco** as the console and vty password and enable login.
- Configure logging synchronous to prevent console message from interrupting command entry.
- Shut down all switchports except the ports connected to PCs.
- Configure VLAN 99 and name it **Management**.
- Configure VLAN 10 and name it **Staff**.
- Configure the switch ports with attached hosts as access ports in VLAN 10.
- Assign the IP addresses according to the Addressing Table.
- Copy the running configuration to startup configuration.

Step 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.

Step 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-channel1, changed state to up
*Mar  1 00:09:17.364: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1,
changed state to up
*Mar  1 00:09:44.383: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

Step 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
```

Step 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?

Step 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

```

Step 5: Verify that the ports are configured as trunk ports.

- 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.
-
-

- b. 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.

Step 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
```

Step 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.

Step 3: Configure LACP between S2 and S3.

- a. 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
```

- b. Verify that the EtherChannel has formed.

Step 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.

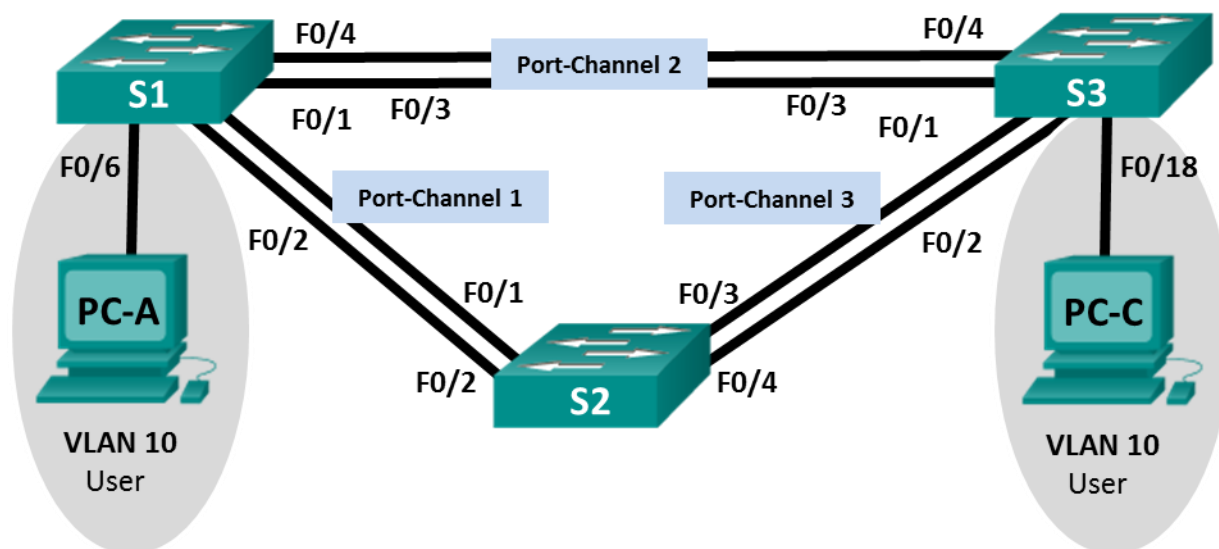
Note: It may be necessary to disable the PC firewall to ping between PCs.

Reflection

What could prevent EtherChannels from forming?

Lab 7 – 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.

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

Step 2: Configure the PC hosts.

Step 3: Erase the startup and VLAN configurations and reload the switches.

Step 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
```

Step 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.

Step 1: Troubleshoot S1.

- 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? _____
- 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.

- Use the command **show run | begin interface Port-channel** command to view the running configuration beginning with the first port channel interface.
- Resolve all problems found in the outputs from the previous **show** commands. Record the commands used to correct the configurations.

- Use the **show interfaces trunk** command to verify trunk settings.
- Use the **show etherchannel summary** command to verify that the port channels are up and in use.

Step 2: Troubleshoot S2.

- 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.

- b. 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.

- c. Use the command **show run | begin interface Port-channel** to view the running configuration beginning with the first port-channel interface.
- d. Resolve all problems found in the outputs from the previous **show** commands. Record the commands used to correct the configuration.

- e. Issue the command to verify trunk settings.
- f. 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.

Step 3: Troubleshoot S3.

- a. 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.

- b. 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.

- c. Use the command **show run | begin interface Port-channel** command to view the running configuration beginning with the first port channel interface.

- d. Resolve all problems found. Record the commands used to correct the configuration.

- e. Issue the command to verify trunk settings. Record the command used in the space provided below.

- f. Issue the command to verify that the port channels are functioning. Record the command used in the space provided below.

Step 4: Verify EtherChannel and Connectivity.

- a. Use the **show interfaces etherchannel** command to verify full functionality of the port channels.
- b. Verify connectivity of the management VLAN.

Can S1 ping S2? _____

Can S1 ping S3? _____

Can S2 ping S3? _____

- c. Verify connectivity of PCs.

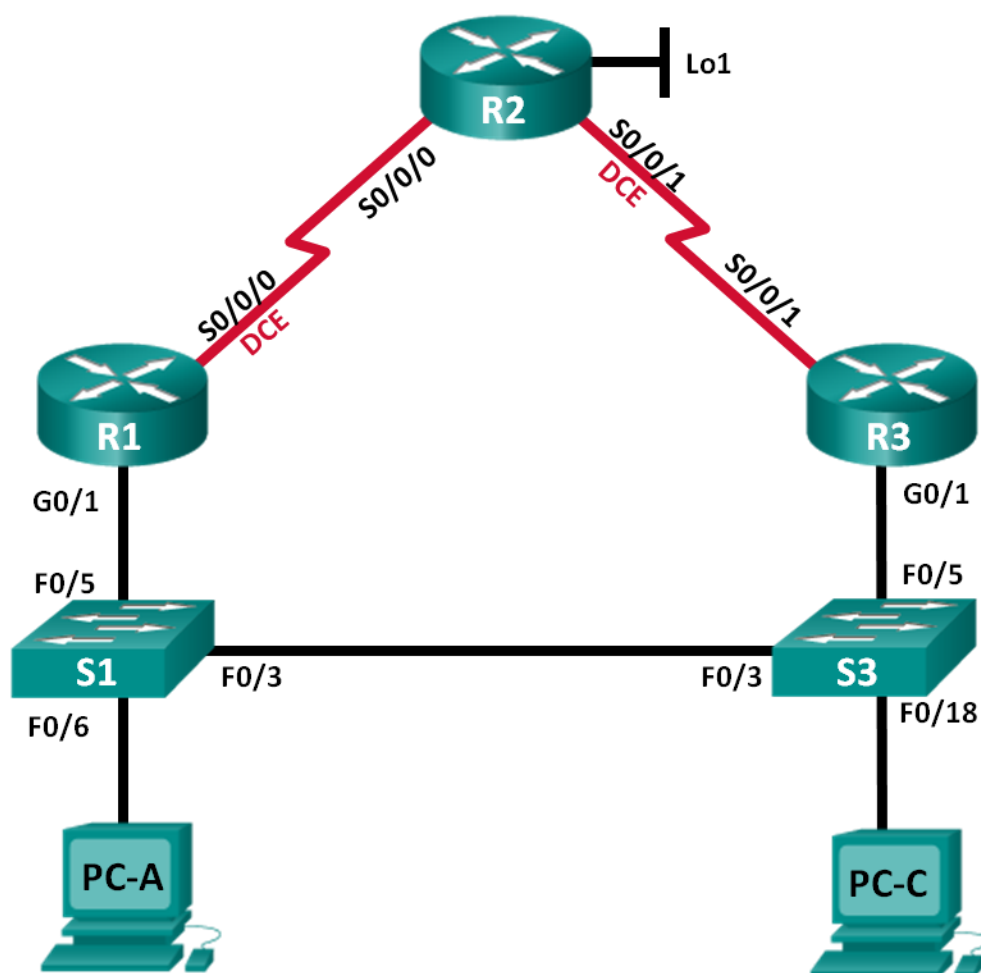
Can PC-A ping PC-C? _____

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 8 - 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.

- a. Disable DNS lookup.
- b. Configure the device name as shown in the topology.
- c. Configure IP addresses for the routers as listed in the Addressing Table.
- d. Set clock rate to **128000** for all DCE serial interfaces.
- e. Assign **class** as the encrypted privileged EXEC mode password.
- f. Assign **cisco** for the console and vty password and enable login.
- g. Configure **logging synchronous** to prevent console messages from interrupting command entry.
- h. Copy the running configuration to the startup configuration.

Step 5: Configure basic settings for each switch.

- a. Disable DNS lookup.
- b. Configure the device name as shown in the topology.
- c. Assign **class** as the encrypted privileged EXEC mode password.
- d. Configure IP addresses for the switches as listed in the Addressing Table.
- e. Configure the default gateway on each switch.
- f. Assign **cisco** for the console and vty password and enable login.
- g. Configure **logging synchronous** to prevent console messages from interrupting command entry.
- h. Copy the running configuration to the startup configuration.

Step 6: 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 7: Configure routing.

- a. Configure RIP version 2 on all routers. Add all the networks, except 209.165.200.224/27 into the RIP process.
- b. Configure a default route on R2 using Lo1 as the exit interface to 209.165.200.224/27 network.
- c. 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 8: Verify connectivity.

- a. 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.

- b. 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.

- a. 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?

- b. 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 2: Start a ping session on PC-A, and break the connection between S1 and R1.

- a. 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>

- b. 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?

-
- c. Would be the results if you repeat Steps 2a and 2b on PC-C and S3?

-
- d. 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 3: 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.

- a. 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
```

- b. 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
```

- c. 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?

- d. 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

```

- e. Change the default gateway address for PC-A, PC-C, S1, and S3. Which address should you use?

- f. 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 4: Start a ping session on PC-A and break the connection between the switch that is connected to the Active HSRP router (R1).

- 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.
- 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 5: Verify HSRP settings on R1 and R3.

- a. 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 6: Change HSRP priorities.

- a. Change the HSRP priority to 200 on R3. Which is the active router? _____
- b. Issue the command to change the active router to R3 without changing the priority. What command did you use?
-

- c. Use a **show** command to verify that R3 is the active router.
-

Reflection

Why would there be a need for redundancy in a LAN?

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.				

Lab 9 - Classless EIGRP

Objectives

Describe the basic features of EIGRP.

Scenario

EIGRP was introduced as a distance vector routing protocol in 1992. It was originally designed to work as a proprietary protocol on Cisco devices only. In 2013, EIGRP became a multi-vendor routing protocol, meaning that it can be used by other device vendors in addition to Cisco devices.

View the *Fundamental Configuration and Verification of EIGRP* video located at http://www.cisco.com/E-Learning/bulk/subscribed/tac/netbits/iprouting/eigrp/01_fundamental_eigrp/start.htm. In order to view the video you must have a cisco.com account. If you do not have a cisco.com account, please register to create one.

While viewing the video, pay close attention to the following concepts and terms:

- Subnet mask reporting to routing tables for classful and classless networks
- Auto-summarization of networks in routing tables
- Autonomous system numbers
- Wildcard masks
- Passive interfaces
- EIGRP configuration commands
- EIGRP verification commands

Complete the reflection questions which accompany the PDF file for this activity. Save your work and be prepared to share your answers with the class.

Resources

Internet access

Reflection

1. Explain classful routing protocols.

2. Explain classless routing protocols.

3. What is network auto-summarization?

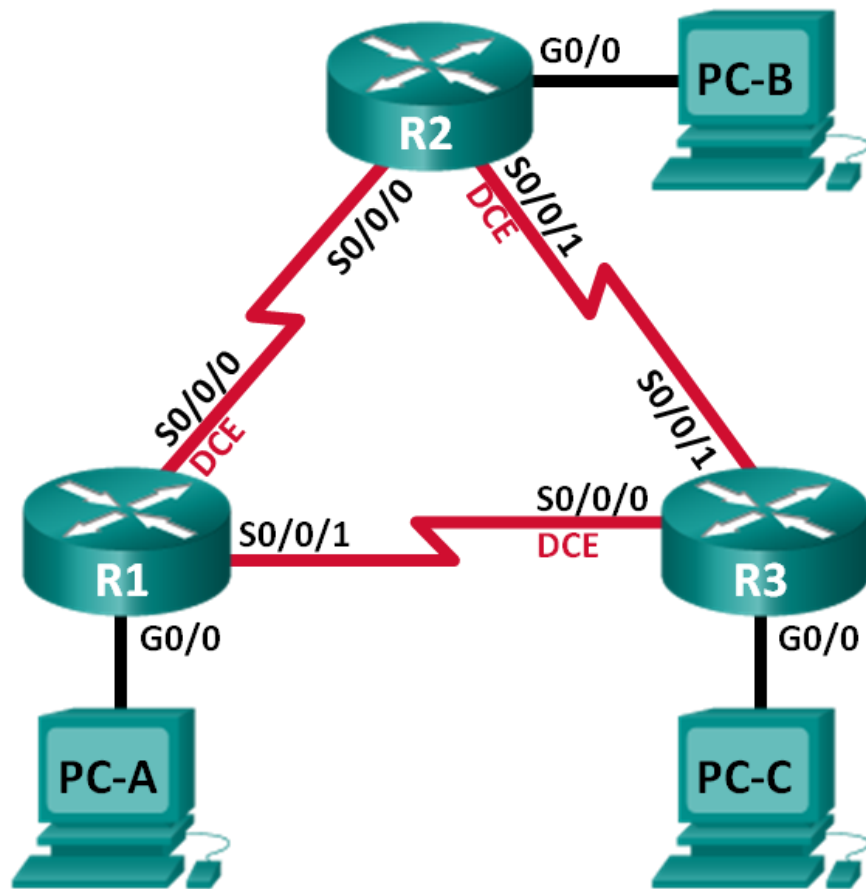
4. What is an autonomous system number?

5. What are wildcard masks?

6. What is a passive interface?

Lab 10 – 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.

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

Step 2: Configure PC hosts.

Step 3: Initialize and reload the routers as necessary.

Step 4: Configure basic settings for each router.

- a. Disable DNS lookup.
- b. Configure IP addresses for the routers, as listed in the Addressing Table.
- c. Configure device name as shown in the topology.
- d. Assign **cisco** as the console and vty passwords.
- e. Assign **class** as the privileged EXEC password.
- f. Configure **logging synchronous** to prevent console and vty messages from interrupting command entry.
- g. Configure a message of the day.
- h. Copy the running configuration to the startup configuration.

Step 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

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

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

Step 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)?

Step 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
```

Step 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

Step 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
```

Step 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?

Step 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?

Step 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.

Step 1: Observe the current routing settings.

- a. 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? _____

- b. How many routes are listed in the routing table to reach the 10.2.2.0/30 network? _____

Step 2: Modify the bandwidth on the routers.

- a. 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
```

-
- b. 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
```

Step 3: Verify the bandwidth modifications.

- a. 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?

Step 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
```

Step 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

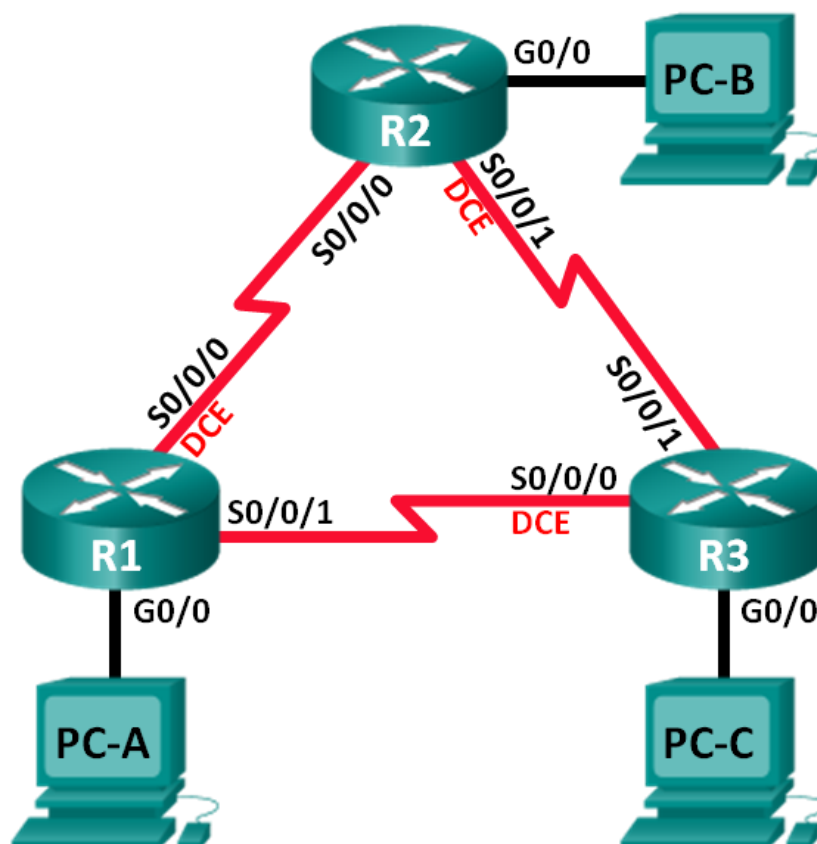
You could have used only static routing for this lab. What is an advantage of using EIGRP?

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.				

Lab 11 - 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.

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

Step 2: Configure PC hosts.

Step 3: Initialize and reload the routers as necessary.

Step 4: Configure basic settings for each router.

- Disable DNS lookup.
- 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.
- Configure the device name as shown in the topology.
- Assign **cisco** as the console and vty passwords.
- Assign **class** as the privileged EXEC password.
- Configure **logging synchronous** to prevent console and vty messages from interrupting command entry.
- Configure a message of the day.
- Copy the running configuration to the startup configuration.

Step 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

Step 1: Enable IPv6 routing on the routers.

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

Step 2: Assign a router ID to each router.

- 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
```

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

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

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

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

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

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

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

Step 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
```

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

- 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
```

- b. 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? _____

Step 5: Verify end-to-end connectivity.

Part 3: Verify EIGRP for IPv6 Routing

Step 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 (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
1	Link-local address: FE80::3	Se0/0/1	13	00:02:42	1	100	0	7
0	Link-local address: FE80::2	Se0/0/0	13	00:03:09	12	100	0	9

Step 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
```

Step 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?

Step 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** *interface* command causes the router to stop sending and receiving Hello packets over an interface.

Step 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
```

Step 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
```

Step 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.

a. 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
```

- b. 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?
-

- c. What command can you use to display the passive interfaces on R3?
-

- d. 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
```

- e. 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?

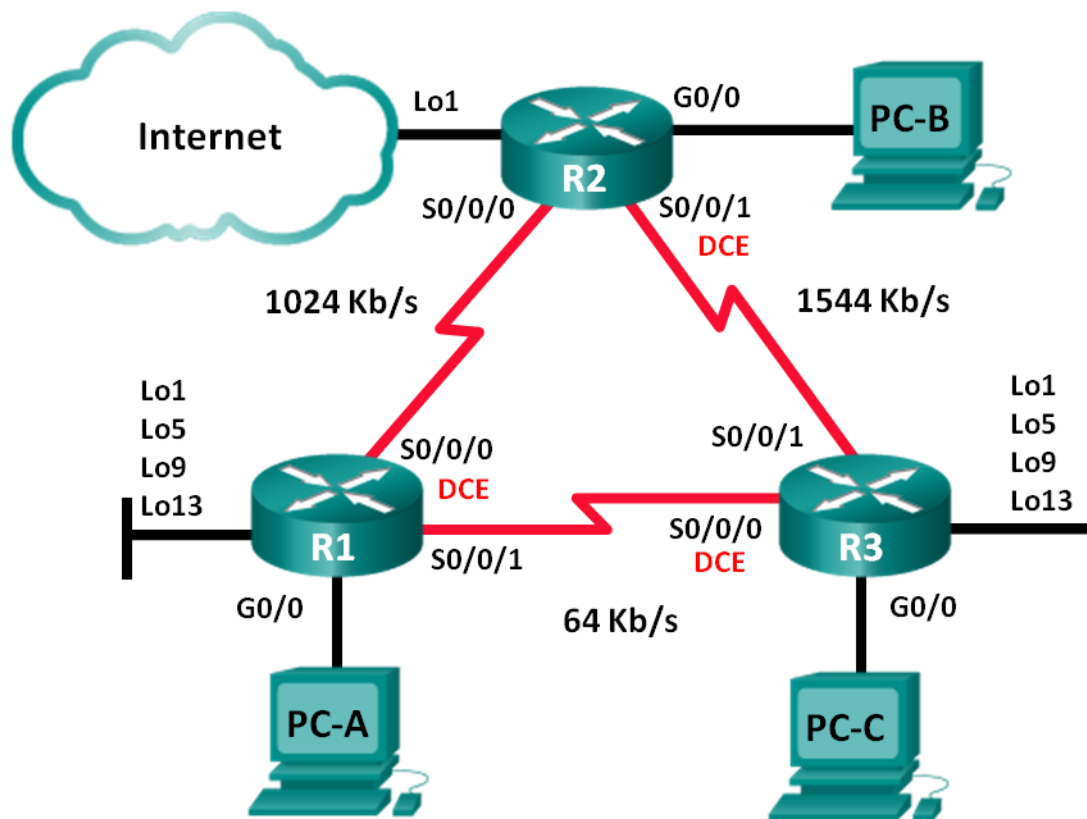
2. What are some advantages with using EIGRP as the routing protocol in your network?

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.				

Lab 12 – 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 EIGRP for Automatic Summarization

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.

Background / Scenario

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

In this lab, you will configure automatic summarization for EIGRP, configure EIGRP route propagation, and fine-tune EIGRP metrics.

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 with a 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.

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

Step 2: Configure PC hosts.

Step 3: Initialize and reload the routers as necessary.

Step 4: Configure basic settings for each router.

- Disable DNS lookup.
- Configure device name as shown in the topology.
- Assign **cisco** as the console and vty passwords.
- Assign **class** as the privileged EXEC password.
- Configure **logging synchronous** to prevent console messages from interrupting command entry.
- Configure the IP address listed in the Addressing Table for all interfaces.

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

- 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.

Step 1: Configure EIGRP.

- a. 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.

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

- c. 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.

- d. 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.
- e. 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.

Step 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 EIGRP for Automatic Summarization

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

Step 1: Configure EIGRP for automatic summarization.

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

- b. Configure the loopback addresses on R1.
- c. Add the appropriate network statements to the EIGRP process on R1. Record the commands used in the space below.

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

- e. 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?

- f. Repeat substeps b through e by adding loopback interfaces, adding EIGRP process networks and auto-summary on R3.

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.

- a. Configure the loopback address on R2.
b. Configure a default static route with an exit interface of Lo1.

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

- c. 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
```

- d. 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 ***
<output omitted>
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

```

- e. 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 for EIGRP traffic on an interface and change the hello interval and hold timers for EIGRP interfaces.

Step 1: Configure bandwidth utilization for EIGRP.

- a. 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

```
- b. Configure the serial link between R1 and R3 to allow 40 percent of the links bandwidth for EIGRP traffic.

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

- a. 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? _____

- b. 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

```

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

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?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Appendix A: Configuration Commands

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-router)# auto-summary
R1(config)# int s0/0/0
R1(config-if)# bandwidth 1024
R1(config-if)# ip bandwidth-percent eigrp 1 75
R1(config-if)# ip hello-interval eigrp 1 60
R1(config-if)# ip hold-time eigrp 1 180
R1(config-if)# int s0/0/1
R1(config-if)# bandwidth 64
R1(config-if)# ip bandwidth-percent eigrp 1 40
R1(config-if)# ip hello-interval eigrp 1 60
R1(config-if)# ip hold-time eigrp 1 180

```

Router R2

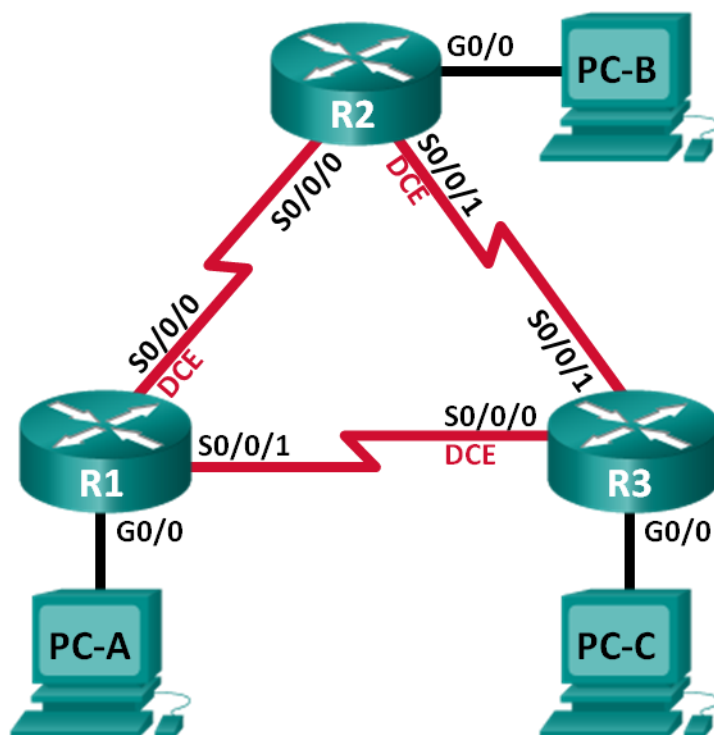
```
R2(config)# router eigrp 1
R2(config-router)# network 192.168.2.0
R2(config-router)# network 192.168.12.0 0.0.0.3
R2(config-router)# network 192.168.23.0 0.0.0.3
R2(config-router)# passive-interface g0/0
R2(config-router)# redistribute static
R2(config)# int s0/0/0
R2(config-if)# bandwidth 1024
R2(config-if)# ip bandwidth-percent eigrp 1 75
R2(config-if)# ip hello-interval eigrp 1 60
R2(config-if)# ip hold-time eigrp 1 180
R2(config-if)# int s0/0/1
R2(config-if)# ip hello-interval eigrp 1 60
R2(config-if)# ip hold-time eigrp 1 180
```

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-router)# auto-summary
R3(config)# int s0/0/0
R3(config-if)# bandwidth 64
R3(config-if)# ip bandwidth-percent eigrp 1 40
R3(config-if)# ip hello-interval eigrp 1 60
R3(config-if)# ip hold-time eigrp 1 180
R3(config-if)# int s0/0/1
R3(config-if)# ip hello-interval eigrp 1 60
R3(config-if)# ip hold-time eigrp 1 180
```

Lab 13 – 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.

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

Step 2: Configure PC hosts.

Step 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
```

Step 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.

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

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

- b. 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.

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

- d. 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.

- e. Resolve all problems found. Record the commands used to correct the issues.

Step 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.

Step 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.

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

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

- 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.

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

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

Step 3: Verify EIGRP neighbor information.

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

- b. Resolve any outstanding problems that were discovered.

Step 4: Verify EIGRP for IPv4 routing information.

- a. 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?

- b. If any routing information is missing, resolve these issues.

Step 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.

Step 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.

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

- a. 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.

- b. 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.
-

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

- a. 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.

-
-
-

-
- This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

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

- Issue the **show ipv6 eigrp neighbor** command to verify that adjacencies have formed between neighboring routers.
- Resolve any EIGRP adjacency issues that still exist.

Step 5: Verify EIGRP for IPv6 routing information.

- a. 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?

- b. Resolve any routing issues that still exist.

Step 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

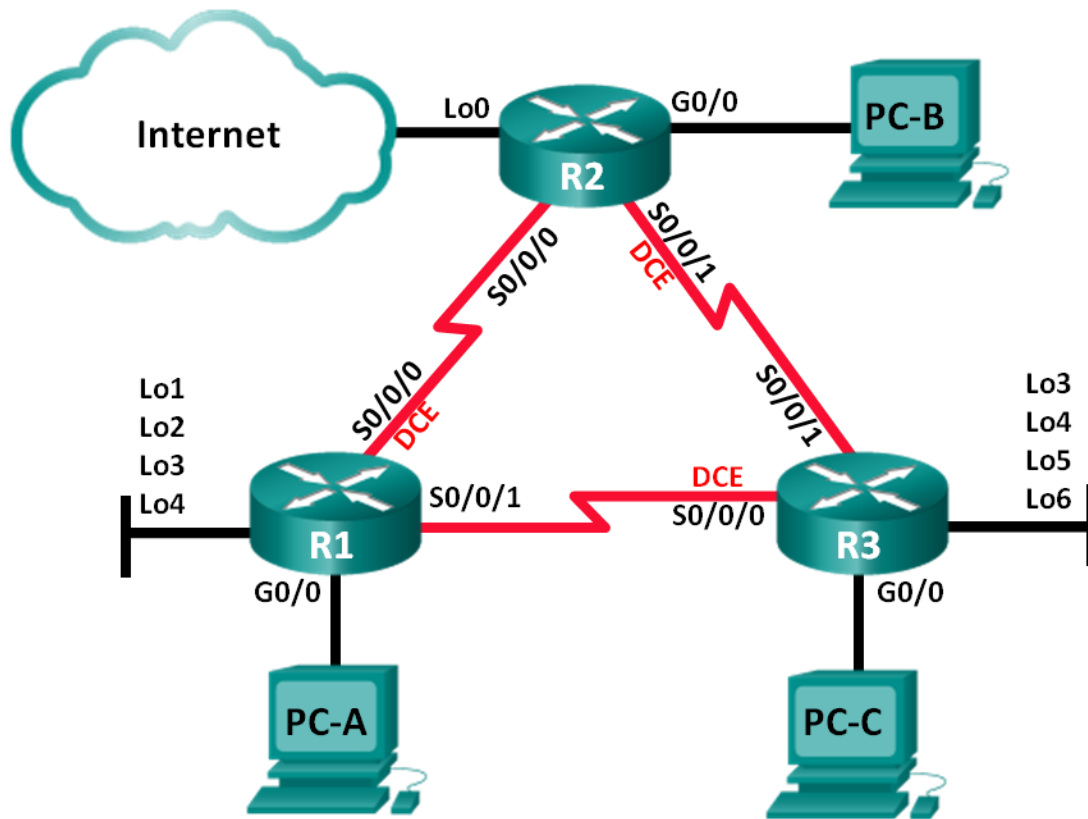
Why would you troubleshoot EIGRP for IPv4 and EIGRP for IPv6 separately?

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.				

Lab 14 – 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, and metrics.

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 must find and correct 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 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

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

Step 2: Configure PC hosts.

Step 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
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
ip add 192.168.12.1 255.255.255.252
no shutdown
interface s0/0/1
    description Serial Link to R3
    ip add 192.168.13.1 255.255.255.252
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 172.16.11.0 0.0.0.255
    network 172.16.12.0 0.0.0.255
    network 172.16.13.0 0.0.0.255
    network 172.16.14.0 0.0.0.255
    passive-interface g0/0
end

```

Router R2 Configuration:

```

conf t
hostname R2
enable secret class
no ip domain lookup
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

```

```

    ip add 192.168.12.2 255.255.255.252
no shutdown
interface s0/0/1
    description Serial Link to R3
ip add 192.168.23.1 255.255.255.252
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
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
no shutdown
interface s0/0/1
description Serial Link to R2
ip add 192.168.23.2 255.255.255.252
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 172.16.33.0 0.0.0.255
network 172.16.34.0 0.0.0.255
network 172.16.35.0 0.0.0.255
network 172.16.36.0 0.0.0.255
passive-interface g0/0
end

```

Step 4: Verify end-to-end connectivity.

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

Step 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.
- Automatic route summarization of the branch networks.
- EIGRP should redistribute the static default route to the Internet. This is simulated by using Loopback 0 interface 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.

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:

2 Router:

R3 Router:

Reflection

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

2. Why would you want to change the EIGRP Hello and Hold time intervals on an interface?

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.				

Class Activity - Tuning EIGRP

Objectives

Implement advanced EIGRP features to enhance operation in a small- to medium-sized business network.

This chapter will focus on some advanced methods to tune EIGRP network configurations. This modeling activity will prove your mastery of some of these concepts.

Scenario

The purpose of this activity is to review EIGRP routing protocol tuning concepts.

You will work with a partner to design one EIGRP topology. This topology will be the basis for two parts of the activity. The first will use default settings for all configurations and the second will incorporate at least three of the following EIGRP tuning options:

- Default routes
- Default routes propagation
- Hello interval timer settings
- EIGRP bandwidth percent utilization

Refer to the labs, Packet Tracer activities, and interactive activities to help you as you progress through this modeling activity.

Directions are listed on the PDF file for this activity. Share your completed work with another group. You may wish to save a copy of this activity to a portfolio.

Resources

- Packet Tracer software or physical network lab equipment
- Word processing program

Directions

Step 1: Design a WAN and LAN topology.

- a. Use Packet Tracer to design a network with two routers (1941 model, suggested). If necessary, add NICs to the routers to provide connectivity to the routers for at least two LANs for each router. Add at least one PC to each LAN.
- b. Address the networks using either an IPv4 or IPv6 addressing scheme. VLSM may be used per group discretion. A fully VLSM-addressed network will work with EIGRP because auto-summarization is turned off by default.
- c. Configure the topology using basic EIGRP default settings.
- d. Make sure all PCs can ping each other, to prove connectivity.
- e. Save your work.

Step 2: Copy the topology.

- a. Using your cursor, highlight the entire EIGRP-configured topology.
- b. Press **Ctrl+C** to copy the highlighted topology.
- c. Use **Ctrl+V** to paste a full copy of the topology to the Packet Tracer desktop. There should be two EIGRP-configured topologies displayed. You will use the topology copy to tune the network.
- d. While highlighted, move the copied topology to a different location on the Packet Tracer desktop to create room between the two for configuration purposes.

Step 3: Configure tuning features on the copied topology.

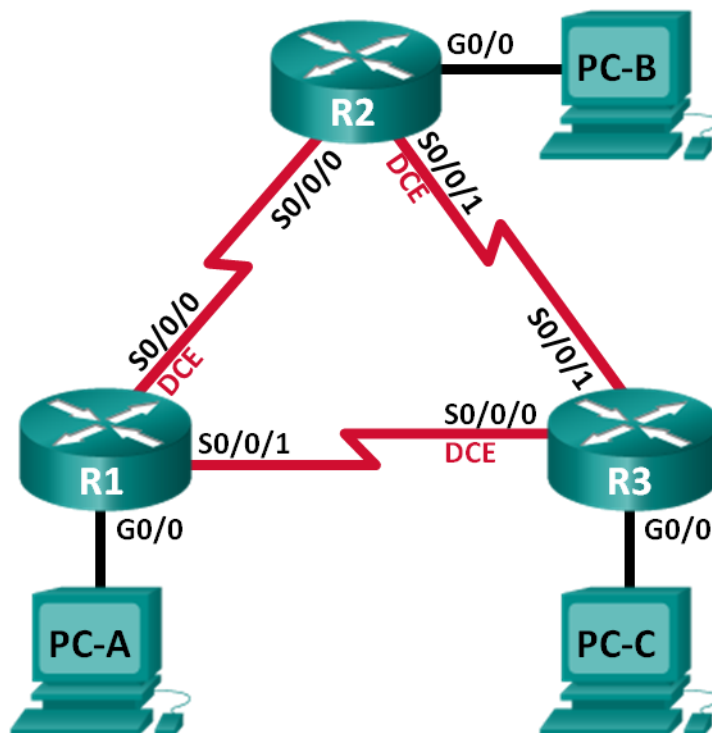
- a. Choose three of the bulleted items from the Scenario section of this activity. Configure your changes on the copied topology.
Note: By changing the Hello interval times, network instability may occur, however you should be able to troubleshoot it. Make sure to notice adjacency status changes if you choose the Hello interval configuration option.
- b. Save your work to avoid losing your configuration.

Step 4: Use verification commands to compare and contrast the default configuration and the tuned configuration.

- a. Use at least three output commands to compare and contrast the two topologies, and copy them to a word processing software program. For example, some useful commands include:
 - `show ip route`
 - `show running-configuration`
 - `show ip protocols, show ip eigrp neighbors`
- b. Share your work with another group. Explain how you changed the second topology from the first configured example. Justify what happened when you configured the three EIGRP tuning options.

Lab 16 - 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 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

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

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

Step 2: Initialize and reload the routers as necessary.

Step 3: Configure basic settings for each router.

- Disable DNS lookup.
- Configure device name as shown in the topology.
- Assign **class** as the privileged EXEC password.
- Assign **cisco** as the console and vty passwords.
- Configure a message of the day (MOTD) banner to warn users that unauthorized access is prohibited.
- Configure **logging synchronous** for the console line.

- g. Configure the IP address listed in the Addressing Table for all interfaces.
- h. Set the clock rate for all DCE serial interfaces at **128000**.
- i. Copy the running configuration to the startup configuration.

Step 4: Configure PC hosts.

Step 5: Test connectivity.

The routers should be able to ping one another, and each PC should be able to ping its default gateway. The PCs are unable to ping other PCs until OSPF routing is configured. Verify and troubleshoot if necessary.

Part 2: Configure and Verify OSPF Routing

In Part 2, you will configure OSPFv2 routing on all routers in the network and then verify that routing tables are updated correctly.

Step 1: Configure OSPF on R1.

- a. 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.

- b. Configure the **network** statements for the networks on R1. Use an area ID of 0.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

```
R1(config-router)# network 192.168.12.0 0.0.0.3 area 0
```

```
R1(config-router)# network 192.168.13.0 0.0.0.3 area 0
```

Step 2: Configure OSPF on R2 and R3.

Use the **router ospf** command and add the **network** statements for the networks on R2 and R3. Neighbor adjacency messages display on R1 when OSPF routing is configured on R2 and R3.

```
R1#
```

```
00:22:29: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on Serial0/0/0 from LOADING to FULL, Loading Done
```

```
R1#
```

```
00:23:14: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.2 on Serial0/0/1 from LOADING to FULL, Loading Done
```

```
R1#
```

Step 3: Verify OSPF neighbors and routing information.

- a. Issue the **show ip ospf neighbor** command to verify that each router lists the other routers in the network as neighbors.

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

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.23.2	0	FULL/ -	00:00:33	192.168.13.2	Serial0/0/1
192.168.23.1	0	FULL/ -	00:00:30	192.168.12.2	Serial0/0/0

- b. Issue the **show ip route** command to verify that all networks display in the routing table on all routers.

```
R1# show ip route
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is not set

```

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O       192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0
O       192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1
    192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
    192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.12.2, 00:31:38, Serial0/0/0
        [110/128] via 192.168.13.2, 00:31:38, Serial0/0/1

```

What command would you use to only see the OSPF routes in the routing table?

Step 4: Verify OSPF protocol settings.

The **show ip protocols** command is a quick way to verify vital OSPF configuration information. This information includes the OSPF process ID, the router ID, networks the router is advertising, the neighbors the router is receiving updates from, and the default administrative distance, which is 110 for OSPF.

```

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

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.13.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.23.2     110          00:19:16
    192.168.23.1     110          00:20:03

```

Distance: (default is 110)

Step 5: Verify OSPF process information.

Use the **show ip ospf** command to examine the OSPF process ID and router ID. This command displays the OSPF area information, as well as the last time the SPF algorithm was calculated.

```
R1# show ip ospf
Routing Process "ospf 1" with ID 192.168.13.1
Start time: 00:20:23.260, Time elapsed: 00:25:08.296
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPF's 10000 msecs
Maximum wait time between two consecutive SPF's 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
Area BACKBONE(0)
  Number of interfaces in this area is 3
  Area has no authentication
  SPF algorithm last executed 00:22:53.756 ago
  SPF algorithm executed 7 times
  Area ranges are
  Number of LSA 3. Checksum Sum 0x019A61
  Number of opaque link LSA 0. Checksum Sum 0x000000
  Number of DCbitless LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0
```

Step 6: Verify OSPF interface settings.

- a. Issue the **show ip ospf interface brief** command to display a summary of OSPF-enabled interfaces.

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

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Se0/0/1	1	0	192.168.13.1/30	64	P2P	1/1	
Se0/0/0	1	0	192.168.12.1/30	64	P2P	1/1	
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0	

- b. For a more detailed list of every OSPF-enabled interface, issue the **show ip ospf interface** command.

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

```
Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID      Cost      Disabled    Shutdown    Topology Name
        0             64         no          no          Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.23.2
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet Address 192.168.12.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID      Cost      Disabled    Shutdown    Topology Name
        0             64         no          no          Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.23.1
  Suppress hello for 0 neighbor(s)
```

```
GigabitEthernet0/0 is up, line protocol is up
Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost: 1
Topology-MTID      Cost      Disabled      Shutdown      Topology Name
      0              1          no            no            Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.13.1, Interface address 192.168.1.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:01
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

Step 7: Verify end-to-end connectivity.

Each PC should be able to ping the other PCs in the topology. Verify and troubleshoot if necessary.

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

Part 3: Change Router ID Assignments

The OSPF router ID is used to uniquely identify the router in the OSPF routing domain. Cisco routers derive the router ID in one of three ways and with the following precedence:

- 1) IP address configured with the OSPF **router-id** command, if present
- 2) Highest IP address of any of the router's loopback addresses, if present
- 3) Highest active IP address on any of the router's physical interfaces

Because no router IDs or loopback interfaces have been configured on the three routers, the router ID for each router is determined by the highest IP address of any active interface.

In Part 3, you will change the OSPF router ID assignment using loopback addresses. You will also use the **router-id** command to change the router ID.

Step 2: Change router IDs using loopback addresses.

- a. Assign an IP address to loopback 0 on R1.

```
R1(config)# interface lo0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# end
```

- b. Assign IP addresses to Loopback 0 on R2 and R3. Use IP address 2.2.2.2/32 for R2 and 3.3.3.3/32 for R3.
- c. Save the running configuration to the startup configuration on all three routers.

- d. You must reload the routers in order to reset the router ID to the loopback address. Issue the **reload** command on all three routers. Press Enter to confirm the reload.
- e. After the router completes the reload process, issue the **show ip protocols** command to view the new router ID.

```
R1# show ip protocols
```

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

```
Routing Protocol is "ospf 1"
```

```
Outgoing update filter list for all interfaces is not set
```

```
Incoming update filter list for all interfaces is not set
```

```
Router ID 1.1.1.1
```

```
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
```

```
Maximum path: 4
```

```
Routing for Networks:
```

```
192.168.1.0 0.0.0.255 area 0
```

```
192.168.12.0 0.0.0.3 area 0
```

```
192.168.13.0 0.0.0.3 area 0
```

```
Routing Information Sources:
```

Gateway	Distance	Last Update
3.3.3.3	110	00:01:00
2.2.2.2	110	00:01:14

```
Distance: (default is 110)
```

- f. Issue the **show ip ospf neighbor** command to display the router ID changes for the neighboring routers.

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

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	0	FULL/ -	00:00:35	192.168.13.2	Serial0/0/1
2.2.2.2	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0

```
R1#
```

Step 3: 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.

- a. 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
```

- b. 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.
- c. 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.
- d. 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)

```

- e. Issue the **show ip ospf neighbor** command on R1 to verify that new router ID for R2 and R3 is listed.

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

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:36	192.168.13.2	Serial0/0/1
22.22.22.22	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0

Part 4: Configure OSPF Passive Interfaces

The **passive-interface** command prevents routing updates from being sent through the specified router interface. This is commonly done to reduce traffic on the LANs as they do not need to receive dynamic routing protocol communication. In Part 4, you will use the **passive-interface** command to configure a single interface as passive. You will also configure OSPF so that all interfaces on the router are passive by default, and then enable OSPF routing advertisements on selected interfaces.

Step 1: Configure a passive interface.

- a. Issue the **show ip ospf interface g0/0** command on R1. Notice the timer indicating when the next Hello packet is expected. Hello packets are sent every 10 seconds and are used between OSPF routers to verify that their neighbors are up.

```
R1# show ip ospf interface g0/0
```

```

GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
    0                1         no            no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

```

```

oob-resync timeout 40
Hello due in 00:00:02
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

```

- b. Issue the **passive-interface** command to change the G0/0 interface on R1 to passive.

```

R1(config)# router ospf 1
R1(config-router)# passive-interface g0/0

```

- c. Re-issue the **show ip ospf interface g0/0** command to verify that G0/0 is now passive.

```

R1# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
    0                1          no            no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
  No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)

```

- d. Issue the **show ip route** command on R2 and R3 to verify that a route to the 192.168.1.0/24 network is still available.

```

R2# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

```

Gateway of last resort is not set

```
2.0.0.0/32 is subnetted, 1 subnets
C      2.2.2.2 is directly connected, Loopback0
O      192.168.1.0/24 [110/65] via 192.168.12.1, 00:58:32, Serial0/0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.2.0/24 is directly connected, GigabitEthernet0/0
L      192.168.2.1/32 is directly connected, GigabitEthernet0/0
O      192.168.3.0/24 [110/65] via 192.168.23.2, 00:58:19, Serial0/0/1
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.12.0/30 is directly connected, Serial0/0/0
L      192.168.12.2/32 is directly connected, Serial0/0/0
      192.168.13.0/30 is subnetted, 1 subnets
O      192.168.13.0 [110/128] via 192.168.23.2, 00:58:19, Serial0/0/1
      [110/128] via 192.168.12.1, 00:58:32, Serial0/0/0
      192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.23.0/30 is directly connected, Serial0/0/1
L      192.168.23.1/32 is directly connected, Serial0/0/1
```

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

- a. Issue the **show ip ospf neighbor** command on R1 to verify that R2 is listed as an OSPF neighbor.

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

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:31	192.168.13.2	Serial0/0/1
22.22.22.22	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0

- b. Issue the **passive-interface default** command on R2 to set the default for all OSPF interfaces as passive.

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

```
R2(config-router)# passive-interface default
```

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

```
*Apr  3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
```

```
*Apr  3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
```

- c. Re-issue the **show ip ospf neighbor** command on R1. After the dead timer expires, R2 will no longer be listed as an OSPF neighbor.

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

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:34	192.168.13.2	Serial0/0/1

- d. Issue the **show ip ospf interface S0/0/0** command on R2 to view the OSPF status of interface S0/0/0.

```
R2# show ip ospf interface s0/0/0
```

```
Serial0/0/0 is up, line protocol is up
```

```
Internet Address 192.168.12.2/30, Area 0, Attached via Network Statement
```

```
Process ID 1, Router ID 22.22.22.22, Network Type POINT_TO_POINT, Cost: 64
```

```

Topology-MTID      Cost      Disabled      Shutdown      Topology Name
    0              64         no           no           Base
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  No Hellos (Passive interface)
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

```

- e. If all interfaces on R2 are passive, then no routing information is being advertised. In this case, R1 and R3 should no longer have a route to the 192.168.2.0/24 network. You can verify this by using the **show ip route** command.
- f. On R2, issue the **no passive-interface** command so the router will send and receive OSPF routing updates. After entering this command, you will see an informational message that a neighbor adjacency has been established with R1.

```

R2(config)# router ospf 1
R2(config-router)# no passive-interface s0/0/0
R2(config-router)#
*Apr  3 00:18:03.463: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from
LOADING to FULL, Loading Done

```

- g. Re-issue the **show ip route** and **show 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?

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

- i. Re-issue the **show ip route** command on R3.

What interface is R3 using to route to the 192.168.2.0/24 network? _____

What is the accumulated cost metric for the 192.168.2.0/24 network on R3 now and how is this calculated?

Is R2 listed as an OSPF neighbor to R3? _____

Part 5: Change OSPF Metrics

In Part 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.

Step 1: Change the reference bandwidth on the routers.

The default reference-bandwidth for OSPF is 100Mb/s (Fast Ethernet speed). However, most modern infrastructure devices have links that are faster than 100Mb/s. Because the OSPF cost metric must be an integer, all links with transmission speeds of 100Mb/s or higher have a cost of 1. This results in Fast Ethernet, Gigabit Ethernet, and 10G Ethernet interfaces all having the same cost. Therefore, the reference-bandwidth must be changed to a higher value to accommodate networks with links faster than 100Mb/s.

- a. Issue the **show interface** command on R1 to view the default bandwidth setting for the G0/0 interface.

```
R1# show interface g0/0
```

```
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is c471.fe45.7520 (bia c471.fe45.7520)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:17:31, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    279 packets output, 89865 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    1 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out
```

Note: The bandwidth setting on G0/0 may differ from what is shown above if the PC host interface can only support Fast Ethernet speed. If the PC host interface is not capable of supporting gigabit speed, then the bandwidth will most likely be displayed as 100000 Kbit/sec.

- b. Issue the **show ip route ospf** command on R1 to determine the route to the 192.168.3.0/24 network.

```
R1# show ip route ospf
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
```

```
Gateway of last resort is not set
```

```
O      192.168.2.0/24 [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.

- c. Issue the **show ip ospf interface** command on R3 to determine the routing cost for G0/0.

```
R3# show ip ospf interface g0/0
```

```
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
    0                  1          no            no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:05
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

- d. Issue the **show ip ospf interface s0/0/1** command on R1 to view the routing cost for S0/0/1.

```
R1# show ip ospf interface s0/0/1
```

```
Serial0/0/1 is up, line protocol is up
```

```

Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 64
Topology-MTID      Cost      Disabled      Shutdown      Topology Name
      0              64          no            no            Base
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:04
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.23.2
Suppress hello for 0 neighbor(s)

```

The sum of the costs of these two interfaces is the accumulated cost for the route to the 192.168.3.0/24 network on R3 ($1 + 64 = 65$), as can be seen in the output from the **show ip route** command.

- e. Issue the **auto-cost reference-bandwidth 10000** command on R1 to change the default reference bandwidth setting. With this setting, 10Gb/s interfaces will have a cost of 1, 1 Gb/s interfaces will have a cost of 10, and 100Mb/s interfaces will have a cost of 100.

```

R1(config)# router ospf 1
R1(config-router)# auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.

```

- f. Issue the **auto-cost reference-bandwidth 10000** command on routers R2 and R3.
- g. Re-issue the **show ip ospf interface** command to view the new cost of G0/0 on R3, and S0/0/1 on R1.

```

R3# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement
Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 10
Topology-MTID      Cost      Disabled      Shutdown      Topology Name
      0              10          no            no            Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:02
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0

```

```
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

Note: If the device connected to the G0/0 interface does not support Gigabit Ethernet speed, the cost will be different than the output display. For example, the cost will be 100 for Fast Ethernet speed (100Mb/s).

R1# **show ip ospf interface s0/0/1**

```
Serial0/0/1 is up, line protocol is up
Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 6476
Topology-MTID      Cost      Disabled      Shutdown      Topology Name
      0             6476         no             no             Base
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:05
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.23.2
Suppress hello for 0 neighbor(s)
```

- h. Re-issue the **show ip route ospf** command to view the new accumulated cost for the 192.168.3.0/24 route (10 + 6476 = 6486).

Note: If the device connected to the G0/0 interface does not support Gigabit Ethernet speed, the total cost will be different than the output display. For example, the accumulated cost will be 6576 if G0/0 is operating at Fast Ethernet speed (100Mb/s).

R1# **show ip route ospf**

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
```

```
Gateway of last resort is not set
```

```
O      192.168.2.0/24 [110/6486] via 192.168.12.2, 00:05:40, Serial0/0/0
O      192.168.3.0/24 [110/6486] via 192.168.13.2, 00:01:08, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O          192.168.23.0 [110/12952] via 192.168.13.2, 00:05:17, Serial0/0/1
          [110/12952] via 192.168.12.2, 00:05:17, Serial0/0/
```

Note: Changing the default reference-bandwidth on the routers from 100 to 10,000 in effect changed the accumulated costs of all routes by a factor of 100, but the cost of each interface link and route is now more accurately reflected.

- i. To reset the reference-bandwidth back to its default value, issue the **auto-cost reference-bandwidth 100** command on all three routers.

```
R1(config)# router ospf 1
```

```
R1(config-router)# auto-cost reference-bandwidth 100
```

```
% OSPF: Reference bandwidth is changed.
```

```
Please ensure reference bandwidth is consistent across all routers.
```

Why would you want to change the OSPF default reference-bandwidth?

Step 2: Change the bandwidth for an interface.

On most serial links, the bandwidth metric will default to 1544 Kbits (that of a T1). If this is not the actual speed of the serial link, the bandwidth setting will need to be changed to match the actual speed to allow the route cost to be calculated correctly in OSPF. Use the **bandwidth** command to adjust the bandwidth setting on an interface.

Note: A common misconception is to assume that the **bandwidth** command will change the physical bandwidth, or speed, of the link. The command modifies the bandwidth metric used by OSPF to calculate routing costs, and does not modify the actual bandwidth (speed) of the link.

- a. Issue the **show interface s0/0/0** command on R1 to view the current bandwidth setting on S0/0/0. Even though the clock rate, link speed on this interface was set to 128Kb/s, the bandwidth is still showing 1544Kb/s.

```
R1# show interface s0/0/0
```

```
Serial0/0/0 is up, line protocol is up
```

```
Hardware is WIC MBRD Serial
```

```
Internet address is 192.168.12.1/30
```

```
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
```

```
reliability 255/255, txload 1/255, rxload 1/255
```

```
Encapsulation HDLC, loopback not set
```

```
Keepalive set (10 sec)
```

```
<Output omitted>
```

- b. Issue the **show ip route ospf** command on R1 to view the accumulated cost for the route to network 192.168.23.0/24 using S0/0/0. Note that there are two equal-cost (128) routes to the 192.168.23.0/24 network, one via S0/0/0 and one via S0/0/1.

```
R1# show ip route ospf
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
```

```
+ - replicated route, % - next hop override
```

```
Gateway of last resort is not set
```

```

O      192.168.2.0/24 [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

```

- c. Issue the **bandwidth 128** command to set the bandwidth on S0/0/0 to 128Kb/s.

```

R1(config)# interface s0/0/0
R1(config-if)# bandwidth 128

```

- d. Re-issue the **show ip route ospf** command. The routing table no longer displays the route to the 192.168.23.0/24 network over the S0/0/0 interface. This is because the best route, the one with the lowest cost, is now via S0/0/1.

```
R1# show ip route ospf
```

```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

```

Gateway of last resort is not set

```

O      192.168.2.0/24 [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

```

- e. Issue the **show ip ospf interface brief** command. The cost for S0/0/0 has changed from 64 to 781 which is an accurate cost representation of the link speed.

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

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Se0/0/1	1	0	192.168.13.1/30	64	P2P	1/1	
Se0/0/0	1	0	192.168.12.1/30	781	P2P	1/1	
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0	

- f. Change the bandwidth for interface S0/0/1 to the same setting as S0/0/0 on R1.

- g. Re-issue the **show ip route ospf** command to view the accumulated cost of both routes to the 192.168.23.0/24 network. Note that there are again two equal-cost (845) routes to the 192.168.23.0/24 network, one via S0/0/0 and one via S0/0/1.

```
R1# show ip route ospf
```

```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

```

+ - replicated route, % - next hop override

Gateway of last resort is not set

```
O    192.168.2.0/24 [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.

- h. Issue the **show ip route ospf** command on R3. The accumulated cost of the 192.168.1.0/24 is still showing as 65. Unlike the **clock rate** command, the **bandwidth** command needs to be applied on each side of a serial link.

R3# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

```
O    192.168.1.0/24 [110/65] via 192.168.13.1, 00:30:58, Serial0/0/0
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
```

- i. Issue the **bandwidth 128** command on all remaining serial interfaces in the topology.

What is the new accumulated cost to the 192.168.23.0/24 network on R1? Why?

Step 3: Change the route cost.

OSPF uses the bandwidth setting to calculate the cost for a link by default. However, you can override this calculation by manually setting the cost of a link using the **ip ospf cost** command. Like the **bandwidth** command, the **ip ospf cost** command only affects the side of the link where it was applied.

- a. Issue the **show ip route ospf** on R1.

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
 + - replicated route, % - next hop override

Gateway of last resort is not set

```
O    192.168.2.0/24 [110/782] via 192.168.12.2, 00:00:26, Serial0/0/0
O    192.168.3.0/24 [110/782] via 192.168.13.2, 00:02:50, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/1562] via 192.168.13.2, 00:02:40, Serial0/0/1
        [110/1562] via 192.168.12.2, 00:02:40, Serial0/0/0
```

- b. Apply the **ip ospf cost 1565** command to the S0/0/1 interface on R1. A cost of 1565 is higher than the accumulated cost of the route through R2 which is 1562.

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

- c. Re-issue the **show ip route ospf** command on R1 to display the effect this change has made on the routing table. All OSPF routes for R1 are now being routed through R2.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
```

Gateway of last resort is not set

```
O    192.168.2.0/24 [110/782] via 192.168.12.2, 00:02:06, Serial0/0/0
O    192.168.3.0/24 [110/1563] via 192.168.12.2, 00:05:31, Serial0/0/0
    192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/1562] via 192.168.12.2, 01:14:02, Serial0/0/0
```

Note: Manipulating link costs using the **ip ospf cost** command is the easiest and preferred method for changing OSPF route costs. In addition to changing the cost based on bandwidth, a network administrator may have other reasons for changing the cost of a route, such as preference for a particular service provider or the actual monetary cost of a link or route.

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

Reflection

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

2. Why is the DR/BDR election process not a concern in this lab?

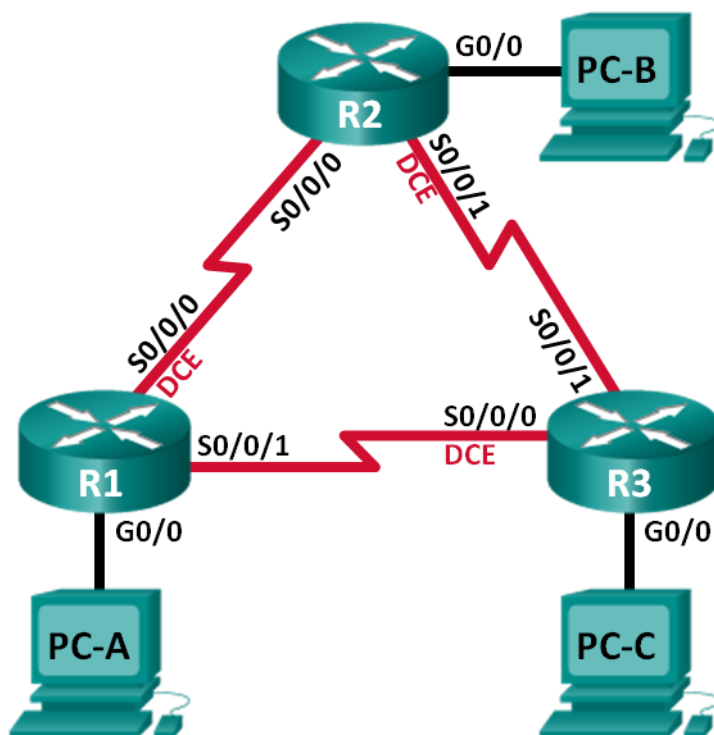
3. Why would you want to set an OSPF interface to passive?

Router Interface Summary Table

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

Lab 17 - 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 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.

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

Step 2: Initialize and reload the routers as necessary.

Step 3: Configure basic settings for each router.

- Disable DNS lookup.
- Configure device name as shown in the topology.
- Assign **class** as the privileged EXEC password.
- Assign **cisco** as the vty password.
- Configure a MOTD banner to warn users that unauthorized access is prohibited.
- Configure **logging synchronous** for the console line.
- Encrypt plain text passwords.
- Configure the IPv6 unicast and link-local addresses listed in the Addressing Table for all interfaces.
- Enable IPv6 unicast routing on each router.
- Copy the running configuration to the startup configuration.

Step 4: Configure PC hosts.

Step 5: Test connectivity.

The routers should be able to ping one another, and each PC should be able to ping its default gateway. The PCs are unable to ping other PCs until OSPFv3 routing is configured. Verify and troubleshoot if necessary.

Part 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.

Step 1: Assign router IDs.

OSPFv3 continues to use a 32 bit address for the router ID. Because there are no IPv4 addresses configured on the routers, you will manually assign the router ID using the **router-id** command.

- Issue the **ipv6 router ospf** command to start an OSPFv3 process to the router.

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

Note: The OSPF process ID is kept locally and has no meaning to other routers on the network.

- b. Assign the OSPFv3 router ID **1.1.1.1** to the R1.

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

- c. Start the OSPFv3 routing process and assign a router ID of **2.2.2.2** to R2 and a router ID of **3.3.3.3** to R3.

- d. Issue the **show ipv6 ospf** command to verify the router IDs on all routers.

```
R2# show ipv6 ospf
```

```
Routing Process "ospfv3 1" with ID 2.2.2.2
```

```
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
```

```
Router is not originating router-LSAs with maximum metric
```

```
<output omitted>
```

Step 2: Configure OSPFv6 on R1.

With IPv6, it is common to have multiple IPv6 addresses configured on an interface. The network statement has been eliminated in OSPFv3. OSPFv3 routing is enabled at the interface level instead.

- a. Issue the **ipv6 ospf 1 area 0** command for each interface on R1 that is to participate in OSPFv3 routing.

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

```
R1(config-if)# ipv6 ospf 1 area 0
```

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

```
R1(config-if)# ipv6 ospf 1 area 0
```

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

```
R1(config-if)# ipv6 ospf 1 area 0
```

Note: The process ID must match the process ID you used in Step1a.

- b. Assign the interfaces on R2 and R3 to OSPFv3 area 0. You should see neighbor adjacency messages display when adding the interfaces to area 0.

```
R1#
```

```
*Mar 19 22:14:43.251: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from  
LOADING to FULL, Loading Done
```

```
R1#
```

```
*Mar 19 22:14:46.763: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from  
LOADING to FULL, Loading Done
```

Step 3: Verify OSPFv3 neighbors.

Issue the **show ipv6 ospf neighbor** command to verify that the router has formed an adjacency with its neighboring routers. If the router ID of the neighboring router is not displayed, or if its state does not show as FULL, the two routers have not formed an OSPF adjacency.

```
R1# show ipv6 ospf neighbor
```

```
OSPFv3 Router with ID (1.1.1.1) (Process ID 1)
```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	0	FULL/ -	00:00:39	6	Serial0/0/1
2.2.2.2	0	FULL/ -	00:00:36	6	Serial0/0/0

Step 4: Verify OSPFv3 protocol settings.

The **show ipv6 protocols** command is a quick way to verify vital OSPFv3 configuration information, including the OSPF process ID, the router ID, and the interfaces enabled for OSPFv3.

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Router ID 1.1.1.1
  Number of areas: 1 normal, 0 stub, 0 nssa
  Interfaces (Area 0):
    Serial0/0/1
    Serial0/0/0
    GigabitEthernet0/0
  Redistribution:
    None
```

Step 5: Verify OSPFv3 interfaces.

- a. Issue the **show ipv6 ospf interface** command to display a detailed list for every OSPF-enabled interface.

```
R1# show ipv6 ospf interface
Serial0/0/1 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 7
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Graceful restart helper support enabled
  Index 1/3/3, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 3.3.3.3
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 6
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Graceful restart helper support enabled
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
```

```

    Adjacent with neighbor 2.2.2.2
    Suppress hello for 0 neighbor(s)
    GigabitEthernet0/0 is up, line protocol is up
    Link Local Address FE80::1, Interface ID 3
    Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
    Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State DR, Priority 1
    Designated Router (ID) 1.1.1.1, local address FE80::1
    No backup designated router on this network
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
    Graceful restart helper support enabled
    Index 1/1/1, flood queue length 0
    Next 0x0(0)/0x0(0)/0x0(0)
    Last flood scan length is 0, maximum is 0
    Last flood scan time is 0 msec, maximum is 0 msec
    Neighbor Count is 0, Adjacent neighbor count is 0
    Suppress hello for 0 neighbor(s)

```

- b. To display a summary of OSPFv3-enabled interfaces, issue the **show ipv6 ospf interface brief** command.

```

R1# show ipv6 ospf interface brief

```

Interface	PID	Area	Intf ID	Cost	State	Nbrs	F/C
Se0/0/1	1	0	7	64	P2P	1/1	
Se0/0/0	1	0	6	64	P2P	1/1	
Gi0/0	1	0	3	1	DR	0/0	

Step 6: Verify the IPv6 routing table.

Issue the **show ipv6 route** command to verify that all networks are appearing in the routing table.

```

R2# show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001:DB8:ACAD:A::/64 [110/65]
    via FE80::1, Serial0/0/0
C   2001:DB8:ACAD:B::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:B::2/128 [0/0]
    via GigabitEthernet0/0, receive
O   2001:DB8:ACAD:C::/64 [110/65]
    via FE80::3, Serial0/0/1
C   2001:DB8:ACAD:12::/64 [0/0]
    via Serial0/0/0, directly connected
L   2001:DB8:ACAD:12::2/128 [0/0]
    via Serial0/0/0, receive

```

```

O  2001:DB8:ACAD:13::/64 [110/128]
    via FE80::3, Serial0/0/1
    via FE80::1, Serial0/0/0
C  2001:DB8:ACAD:23::/64 [0/0]
    via Serial0/0/1, directly connected
L  2001:DB8:ACAD:23::2/128 [0/0]
    via Serial0/0/1, receive
L  FF00::/8 [0/0]
    via Null0, receive

```

What command would you use to only see the OSPF routes in the routing table?

Step 7: Verify end-to-end connectivity.

Each PC should be able to ping the other PCs in the topology. Verify and troubleshoot if necessary.

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

Part 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.

Step 1: Configure a passive interface.

- Issue the **show ipv6 ospf interface g0/0** command on R1. Notice the timer indicating when the next Hello packet is expected. Hello packets are sent every 10 seconds and are used between OSPF routers to verify that their neighbors are up.

```

R1# show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, local address FE80::1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Graceful restart helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)

```

- Issue the **passive-interface** command to change the G0/0 interface on R1 to passive.

```

R1(config)# ipv6 router ospf 1

```

```
R1(config-rtr)# passive-interface g0/0
```

- c. Re-issue the **show ipv6 ospf interface g0/0** command to verify that G0/0 is now passive.

```
R1# show ipv6 ospf interface g0/0
```

```
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
  Wait time before Designated router selection 00:00:34
  Graceful restart helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

- d. Issue the **show ipv6 route ospf** command on R2 and R3 to verify that a route to the 2001:DB8:ACAD:A::/64 network is still available.

```
R2# show ipv6 route ospf
```

```
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O    2001:DB8:ACAD:A::/64 [110/65]
    via FE80::1, Serial0/0/0
O    2001:DB8:ACAD:C::/64 [110/65]
    via FE80::3, Serial0/0/1
O    2001:DB8:ACAD:13::/64 [110/128]
    via FE80::3, Serial0/0/1
    via FE80::1, Serial0/0/0
```

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

- a. Issue the **passive-interface default** command on R2 to set the default for all OSPFv3 interfaces as passive.

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

```
R2(config-rtr)# passive-interface default
```

- b. Issue the **show ipv6 ospf neighbor** command on R1. After the dead timer expires, R2 is no longer listed as an OSPF neighbor.

```
R1# show ipv6 ospf neighbor
```

OSPFv3 Router with ID (1.1.1.1) (Process ID 1)

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	0	FULL/ -	00:00:37	6	Serial0/0/1

- c. On R2, issue the **show ipv6 ospf interface s0/0/0** command to view the OSPF status of interface S0/0/0.

```
R2# show ipv6 ospf interface s0/0/0
```

```
Serial0/0/0 is up, line protocol is up
```

```
Link Local Address FE80::2, Interface ID 6
```

```
Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
```

```
Network Type POINT_TO_POINT, Cost: 64
```

```
Transmit Delay is 1 sec, State POINT_TO_POINT
```

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
No Hellos (Passive interface)
```

```
Graceful restart helper support enabled
```

```
Index 1/2/2, flood queue length 0
```

```
Next 0x0(0)/0x0(0)/0x0(0)
```

```
Last flood scan length is 2, maximum is 3
```

```
Last flood scan time is 0 msec, maximum is 0 msec
```

```
Neighbor Count is 0, Adjacent neighbor count is 0
```

```
Suppress hello for 0 neighbor(s)
```

- d. If all OSPFv3 interfaces on R2 are passive, then no routing information is being advertised. If this is the case, then R1 and R3 should no longer have a route to the 2001:DB8:ACAD:B::/64 network. You can verify this by using the **show ipv6 route** command.
- e. Change S0/0/1 on R2 by issuing the **no passive-interface** command, so that it sends and receives OSPFv3 routing updates. After entering this command, an informational message displays stating that a neighbor adjacency has been established with R3.

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

```
R2(config-rtr)# no passive-interface s0/0/1
```

```
*Apr  8 19:21:57.939: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1  
from LOADING to FULL, Loading Done
```

- f. Re-issue the **show ipv6 route** and **show ipv6 ospf neighbor** commands on R1 and R3, and look for a route to the 2001:DB8:ACAD:B::/64 network.

```
O    2001:DB8:ACAD:B::/64 [110/129]  
    via FE80::3, Serial0/0/1
```

What interface is R1 using to route to the 2001:DB8:ACAD:B::/64 network? _____

What is the accumulated cost metric for the 2001:DB8:ACAD:B::/64 network on R1? _____

Does R2 show up as an OSPFv3 neighbor on R1? _____

Does R2 show up as an OSPFv3 neighbor on R3? _____

What does this information tell you?

- g. On R2, issue the **no passive-interface S0/0/0** command to allow OSPFv3 routing updates to be advertised on that interface.
- h. Verify that R1 and R2 are now OSPFv3 neighbors.

Reflection

1. If the OSPFv6 configuration for R1 had a process ID of 1, and the OSPFv3 configuration for R2 had a process ID of 2, can routing information be exchanged between the two routers? Why?

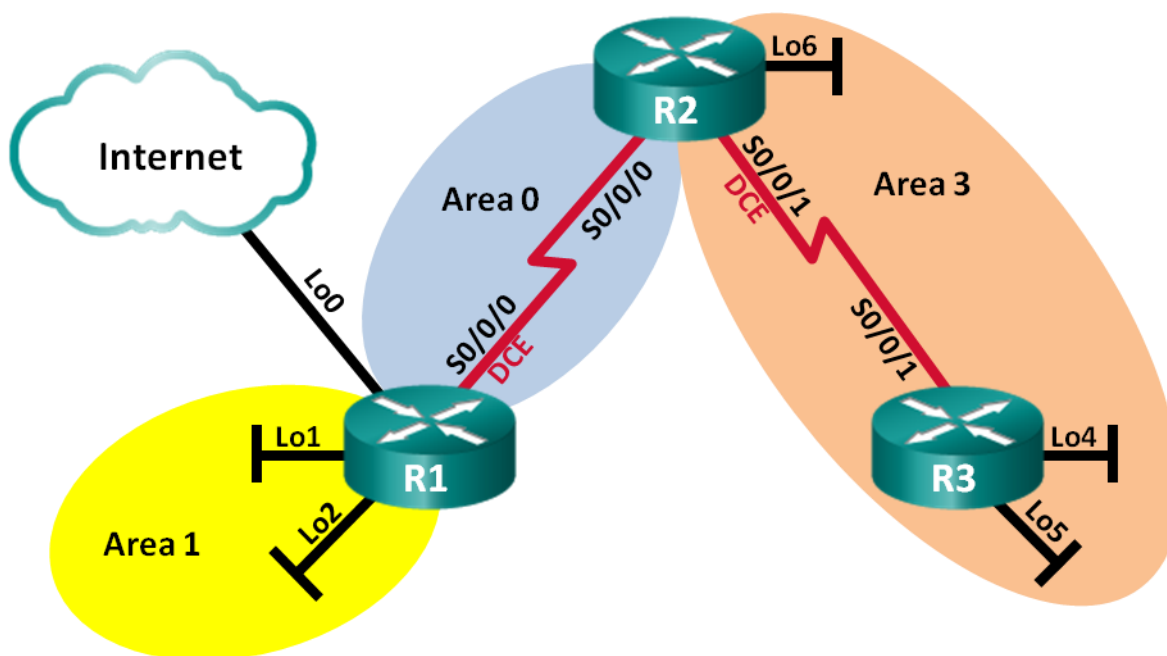
2. What may have been the reasoning for removing the **network** command in OSPFv3?

Router Interface Summary Table

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

Lab 18 - Configuring Multi-area OSPFv2

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	Lo0	209.165.200.225	255.255.255.252
	Lo1	192.168.1.1	255.255.255.0
	Lo2	192.168.2.1	255.255.255.0
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252
R2	Lo6	192.168.6.1	255.255.255.0
	S0/0/0	192.168.12.2	255.255.255.252
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252
R3	Lo4	192.168.4.1	255.255.255.0
	Lo5	192.168.5.1	255.255.255.0
	S0/0/1	192.168.23.2	255.255.255.252

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure a Multi-area OSPFv2 Network

Background / Scenario

To make OSPF more efficient and scalable, OSPF supports hierarchical routing using the concept of areas. An OSPF area is a group of routers that share the same link-state information in their link-state databases (LSDBs). When a large OSPF area is divided into smaller areas, it is called multi-area OSPF. Multi-area OSPF is useful in larger network deployments to reduce processing and memory overhead.

In the lab, you will configure a multi-area OSPFv2 network.

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)
- Console cables to configure the Cisco IOS devices via the console ports
- 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 routers.

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

Step 2: Initialize and reload the routers as necessary.

Step 3: Configure basic settings for each router.

- Disable DNS lookup.
- Configure device name, as shown in the topology.
- Assign **class** as the privileged EXEC password.
- Assign **cisco** as the console and vty passwords.
- Configure **logging synchronous** for the console line.
- Configure an MOTD banner to warn users that unauthorized access is prohibited.
- Configure the IP addresses listed in the Addressing Table for all interfaces. DCE interfaces should be configured with a clock rate of 128000. Bandwidth should be set to 128 Kb/s on all serial interfaces.
- Copy the running configuration to the startup configuration.

Step 4: Verify Layer 3 connectivity.

Use the **show ip interface brief** command to verify that the IP addressing is correct and that the interfaces are active. Verify that each router can ping their neighbor's serial interface.

Part 2: Configure a Multi-area OSPFv2 Network

In Part 2, you will configure a multi-area OSPFv2 network with a process ID of 1. All LAN loopback interfaces should be passive.

Step 1: Identify the OSPF router types in the topology.

Identify the Backbone router(s): _____

Identify the Autonomous System Boundary Router(s) (ASBR): _____

Identify the Area Border Router(s) (ABR): _____

Identify the Internal router(s): _____

Step 2: Configure OSPF on R1.

a. Configure a router ID of 1.1.1.1 with OSPF process ID of 1.

b. Add the networks for R1 to OSPF.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 1
```

```
R1(config-router)# network 192.168.2.0 0.0.0.255 area 1
```

```
R1(config-router)# network 192.168.12.0 0.0.0.3 area 0
```

c. Set LAN loopback interfaces, Lo1 and Lo2, as passive.

d. Create a default route to the Internet using exit interface Lo0.

Note: You may see the “%Default route without gateway, if not a point-to-point interface, may impact performance” message. This is normal behavior if using a Loopback interface to simulate a default route.

e. Configure OSPF to propagate the routes throughout the OSPF areas.

Step 3: Configure OSPF on R2.

a. Configure a router ID of 2.2.2.2 with OSPF process ID of 1.

b. Add the networks for R2 to OSPF. Add the networks to the correct area. Write the commands used in the space below.

c. Set all LAN loopback interfaces as passive.

Step 4: Configure OSPF on R3.

a. Configure a router ID of 3.3.3.3 with OSPF process ID of 1.

b. Add the networks for R3 to OSPF. Write the commands used in the space below.

c. Set all LAN loopback interfaces as passive.

Step 5: Verify that OSPF settings are correct and adjacencies have been established between routers.

- Issue the **show ip protocols** command to verify OSPF settings on each router. Use this command to identify the OSPF router types and to determine the networks assigned to each area.

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

It is an area border and autonomous system boundary router

Redistributing External Routes from,

Number of areas in this router is 2. 2 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

192.168.1.0 0.0.0.255 area 1

192.168.2.0 0.0.0.255 area 1

192.168.12.0 0.0.0.3 area 0

Passive Interface(s):

Loopback1

Loopback2

Routing Information Sources:

Gateway	Distance	Last Update
2.2.2.2	110	00:01:45

Distance: (default is 110)

R2# **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 2.2.2.2

It is an area border router

Number of areas in this router is 2. 2 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

192.168.6.0 0.0.0.255 area 3

192.168.12.0 0.0.0.3 area 0

192.168.23.0 0.0.0.3 area 3

Passive Interface(s):

Loopback6

Routing Information Sources:

Gateway	Distance	Last Update
3.3.3.3	110	00:01:20
1.1.1.1	110	00:10:12

Distance: (default is 110)

R3# **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 3.3.3.3

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

192.168.4.0 0.0.0.255 area 3

192.168.5.0 0.0.0.255 area 3

192.168.23.0 0.0.0.3 area 3

Passive Interface(s):

Loopback4

Loopback5

Routing Information Sources:

Gateway	Distance	Last Update
1.1.1.1	110	00:07:46
2.2.2.2	110	00:07:46

Distance: (default is 110)

What is the OSPF router type for each router?

R1: _____

R2: _____

R3: _____

- b. Issue the **show ip ospf neighbor** command to verify that OSPF adjacencies have been established between routers.

R1# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	0	FULL/ -	00:00:34	192.168.12.2	Serial0/0/0

R2# **show ip ospf neighbor**

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

R3# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	0	FULL/ -	00:00:38	192.168.23.1	Serial0/0/1

- c. Issue the **show ip ospf interface brief** command to display a summary of interface route costs.

R1# **show ip ospf interface brief**

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Se0/0/0	1	0	192.168.12.1/30	781	P2P	1/1	
Lo1	1	1	192.168.1.1/24	1	LOOP	0/0	

```
Lo2          1      1          192.168.2.1/24      1      LOOP  0/0
```

```
R2# show ip ospf interface brief
```

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Se0/0/0	1	0	192.168.12.2/30	781	P2P	1/1	
Lo6	1	3	192.168.6.1/24	1	LOOP	0/0	
Se0/0/1	1	3	192.168.23.1/30	781	P2P	1/1	

```
R3# show ip ospf interface brief
```

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Lo4	1	3	192.168.4.1/24	1	LOOP	0/0	
Lo5	1	3	192.168.5.1/24	1	LOOP	0/0	
Se0/0/1	1	3	192.168.23.2/30	781	P2P	1/1	

Reflection

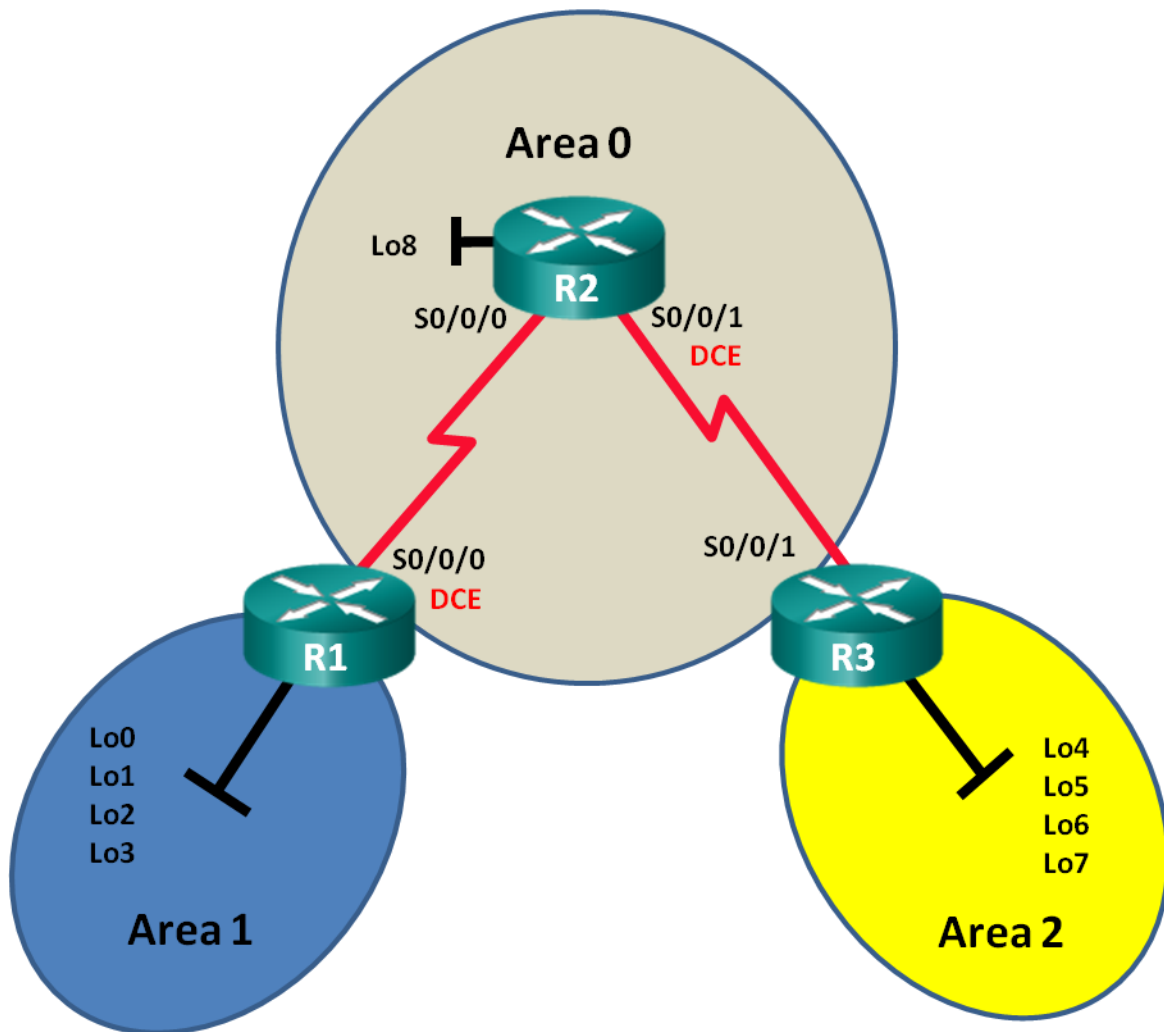
What are three advantages for designing a network with multi-area OSPF?

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.				

Lab 19 - Configuring Multi-area OSPFv3

Topology



Addressing Table

Device	Interface	IPv6 Address
R1	S0/0/0 (DCE)	2001:DB8:ACAD:12::1/64 FE80::1 link-local
	Lo0	2001:DB8:ACAD::1/64
	Lo1	2001:DB8:ACAD:1::1/64
	Lo2	2001:DB8:ACAD:2::1/64
	Lo3	2001:DB8:ACAD:3::1/64
R2	S0/0/0	2001:DB8:ACAD:12::2/64 FE80::2 link-local
	S0/0/1 (DCE)	2001:DB8:ACAD:23::2/64 FE80::2 link-local
	Lo8	2001:DB8:ACAD:8::1/64
R3	S0/0/1	2001:DB8:ACAD:23::3/64 FE80::3 link-local
	Lo4	2001:DB8:ACAD:4::1/64
	Lo5	2001:DB8:ACAD:5::1/64
	Lo6	2001:DB8:ACAD:6::1/64
	Lo7	2001:DB8:ACAD:7::1/64

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure Multi-area OSPFv3 Routing

Background / Scenario

Using multi-area OSPFv3 in large IPv6 network deployments can reduce router processing cycles by creating smaller routing tables and requiring less memory overhead. In multi-area OSPFv3, all areas are connected to the backbone area (area 0) through area border routers (ABRs).

In this lab, you will implement OSPFv3 routing for multiple areas. You will also use a number of **show** commands to display and verify OSPFv3 routing information. This lab uses loopback addresses to simulate networks in multiple OSPFv3 areas.

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 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 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- 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 routers.

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

Step 2: Initialize and reload the routers as necessary.

Step 3: Configure basic settings for each router.

- Disable DNS lookup.
- Configure device name as shown in the topology.
- Assign **class** as the privileged EXEC password.
- Assign **cisco** as the vty password.
- Configure a MOTD banner to warn users that unauthorized access is prohibited.
- Configure **logging synchronous** for the console line.
- Encrypt plaintext passwords.
- Configure the IPv6 unicast and link-local addresses listed in the Addressing Table for all interfaces.
- Enable IPv6 unicast routing on each router.
- Copy the running configuration to the startup configuration.

Step 4: Test connectivity.

The routers should be able to ping one another. The routers are unable to ping distant loopbacks until OSPFv3 routing is configured. Verify and troubleshoot if necessary.

Part 2: Configure Multi-area OSPFv3 Routing

In Part 2, you will configure OSPFv3 routing on all routers to separate the network domain into three distinct areas, and then verify that routing tables are updated correctly.

Step 1: Assign router IDs.

- On R1, issue the **ipv6 router ospf** command to start an OSPFv3 process on 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.
- Assign the OSPFv3 router ID **1.1.1.1** to R1.

```
R1(config-rtr)# router-id 1.1.1.1
```
- Start an OSPFv3 process on R2 and R3 and assign a router ID of **2.2.2.2** to R2 and a router ID of **3.3.3.3** to R3.

- d. Issue the **show ipv6 ospf** command to verify the router IDs on all routers.

```
R2# show ipv6 ospf
```

```
Routing Process "ospfv3 1" with ID 2.2.2.2
```

```
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
```

```
Router is not originating router-LSAs with maximum metric
```

```
<output omitted>
```

Step 2: Configure multi-area OSPFv3.

- a. Issue the **ipv6 ospf 1 area area-id** command for each interface on R1 that is to participate in OSPFv3 routing. The loopback interfaces are assigned to area 1 and the serial interface is assigned to area 0. You will change the network type on the loopback interfaces to ensure that the correct subnet is advertised.

```
R1(config)# interface lo0
```

```
R1(config-if)# ipv6 ospf 1 area 1
```

```
R1(config-if)# ipv6 ospf network point-to-point
```

```
R1(config-if)# interface lo1
```

```
R1(config-if)# ipv6 ospf 1 area 1
```

```
R1(config-if)# ipv6 ospf network point-to-point
```

```
R1(config-if)# interface lo2
```

```
R1(config-if)# ipv6 ospf 1 area 1
```

```
R1(config-if)# ipv6 ospf network point-to-point
```

```
R1(config-if)# interface lo3
```

```
R1(config-if)# ipv6 ospf 1 area 1
```

```
R1(config-if)# ipv6 ospf network point-to-point
```

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

```
R1(config-if)# ipv6 ospf 1 area 0
```

- b. Use the **show ipv6 protocols** command to verify multi-area OSPFv3 status.

```
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
```

```
Area border router
```

```
Number of areas: 2 normal, 0 stub, 0 nssa
```

```
Interfaces (Area 0):
```

```
Serial0/0/0
```

```
Interfaces (Area 1):
```

```
Loopback0
```

```
Loopback1
```

```
Loopback2
```

```
Loopback3
```

```
Redistribution:
```

```
None
```

- c. Assign all interfaces on R2 to participate in OSPFv3 area 0. For the loopback interface, change the network type to point-to-point. Write the commands used in the space below.

- d. Use the **show ipv6 ospf interface brief** command to view OSPFv3-enabled interfaces.

R2# **show ipv6 ospf interface brief**

Interface	PID	Area	Intf ID	Cost	State	Nbrs	F/C
Lo8	1	0	13	1	P2P	0/0	
Se0/0/1	1	0	7	64	P2P	1/1	
Se0/0/0	1	0	6	64	P2P	1/1	

- e. Assign the loopback interfaces on R3 to participate in OSPFv3 area 2 and change the network type to point-to-point. Assign the serial interface to participate in OSPFv3 area 0. Write the commands used in the space below.

- f. Use the **show ipv6 ospf** command to verify configurations.

R3# **show ipv6 ospf**

Routing Process "ospfv3 1" with ID 3.3.3.3

Event-log enabled, Maximum number of events: 1000, Mode: cyclic

It is an area border router

Router is not originating router-LSAs with maximum metric

Initial SPF schedule delay 5000 msec

Minimum hold time between two consecutive SPF's 10000 msec

Maximum wait time between two consecutive SPF's 10000 msec

Minimum LSA interval 5 sec

Minimum LSA arrival 1000 msec

LSA group pacing timer 240 sec

Interface flood pacing timer 33 msec

Retransmission pacing timer 66 msec

Number of external LSA 0. Checksum Sum 0x000000

Number of areas in this router is 2. 2 normal 0 stub 0 nssa

Graceful restart helper support enabled

Reference bandwidth unit is 100 mbps
RFC1583 compatibility enabled

Area BACKBONE (0)

Number of interfaces in this area is 1
SPF algorithm executed 2 times
Number of LSA 16. Checksum Sum 0x0929F8
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

Area 2

Number of interfaces in this area is 4
SPF algorithm executed 2 times
Number of LSA 13. Checksum Sum 0x048E3C
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

Step 3: Verify OSPFv3 neighbors and routing information.

- a. Issue the **show ipv6 ospf neighbor** command on all routers to verify that each router is listing the correct routers as neighbors.

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
2.2.2.2	0	FULL/ -	00:00:39	6	Serial0/0/0

- b. Issue the **show ipv6 route ospf** command on all routers to verify that each router has learned routes to all networks in the Addressing Table.

R1# **show ipv6 route ospf**

IPv6 Routing Table - default - 16 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, R - RIP, H - NHRP, 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

OI 2001:DB8:ACAD:4::/64 [110/129]

via FE80::2, Serial0/0/0

OI 2001:DB8:ACAD:5::/64 [110/129]

via FE80::2, Serial0/0/0

OI 2001:DB8:ACAD:6::/64 [110/129]

via FE80::2, Serial0/0/0

OI 2001:DB8:ACAD:7::/64 [110/129]

via FE80::2, Serial0/0/0

O 2001:DB8:ACAD:8::/64 [110/65]

via FE80::2, Serial0/0/0

```
O    2001:DB8:ACAD:23::/64 [110/128]
```

```
via FE80::2, Serial0/0/0
```

What does OI stand for? How was the OI route learned?

-
- c. Issue the **show ipv6 ospf database** command on all routers.

```
R1# show ipv6 ospf database
```

```
OSPFv3 Router with ID (1.1.1.1) (Process ID 1)
```

Router Link States (Area 0)

ADV Router	Age	Seq#	Fragment ID	Link count	Bits
1.1.1.1	908	0x80000001	0	1	B
2.2.2.2	898	0x80000003	0	2	None
3.3.3.3	899	0x80000001	0	1	B

Inter Area Prefix Link States (Area 0)

ADV Router	Age	Seq#	Prefix
1.1.1.1	907	0x80000001	2001:DB8:ACAD::/62
3.3.3.3	898	0x80000001	2001:DB8:ACAD:4::/62

Link (Type-8) Link States (Area 0)

ADV Router	Age	Seq#	Link ID	Interface
1.1.1.1	908	0x80000001	6	Se0/0/0
2.2.2.2	909	0x80000002	6	Se0/0/0

Intra Area Prefix Link States (Area 0)

ADV Router	Age	Seq#	Link ID	Ref-lstype	Ref-LSID
1.1.1.1	908	0x80000001	0	0x2001	0
2.2.2.2	898	0x80000003	0	0x2001	0
3.3.3.3	899	0x80000001	0	0x2001	0

Router Link States (Area 1)

ADV Router	Age	Seq#	Fragment ID	Link count	Bits
1.1.1.1	908	0x80000001	0	0	B

Inter Area Prefix Link States (Area 1)

ADV Router	Age	Seq#	Prefix
1.1.1.1	907	0x80000001	2001:DB8:ACAD:12::/64
1.1.1.1	907	0x80000001	2001:DB8:ACAD:8::/64
1.1.1.1	888	0x80000001	2001:DB8:ACAD:23::/64
1.1.1.1	888	0x80000001	2001:DB8:ACAD:4::/62

Link (Type-8) Link States (Area 1)

ADV Router	Age	Seq#	Link ID	Interface
1.1.1.1	908	0x80000001	13	Lo0
1.1.1.1	908	0x80000001	14	Lo1
1.1.1.1	908	0x80000001	15	Lo2
1.1.1.1	908	0x80000001	16	Lo3

Intra Area Prefix Link States (Area 1)

ADV Router	Age	Seq#	Link ID	Ref-lsttype	Ref-LSID
1.1.1.1	908	0x80000001	0	0x2001	0

How many link state databases are found on R1? _____

How many link state databases are found on R2? _____

How many link state databases are found on R3? _____

Reflection

1. Why would multi-area OSPFv3 be used?

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.				

DR and BDR Elections

Objectives

Modify the OSPF interface priority to influence the Designated Router (DR) and Backup Designated Router (BDR) election.

Scenario

You are trying to decide how to influence the selection of the designated router and backup designated router for your OSPF network. This activity simulates that process.

Three separate designated-router election scenarios will be presented. The focus is on electing a DR and BDR for your group. Refer to the PDF for this activity for the remaining instructions.

If additional time is available, two groups can be combined to simulate DR and BDR elections.

Required Resources

- Router priorities paper sign example (student developed)
- Router ID paper sign example (student developed)

Directions

This is a group activity with four classmates comprising each group. Before reporting to the group, each student will prepare router priority and router ID signs to bring to the group.

Step 4: Decide the router priority.

- a. Prior to joining your group, use a clean sheet of paper. On one side of the paper, write DEFAULT ROUTER PRIORITY = 1.
- b. On the other side of the same sheet of paper, write ROUTER PRIORITY = (choose a number between 0 and 255).

Step 5: Decide the router ID.

- a. On a second clean sheet of paper, on one side, write ROUTER ID = (any IPv4 number).
- b. On the other side, write ROUTER ID = Loopback (any IPv4) number.

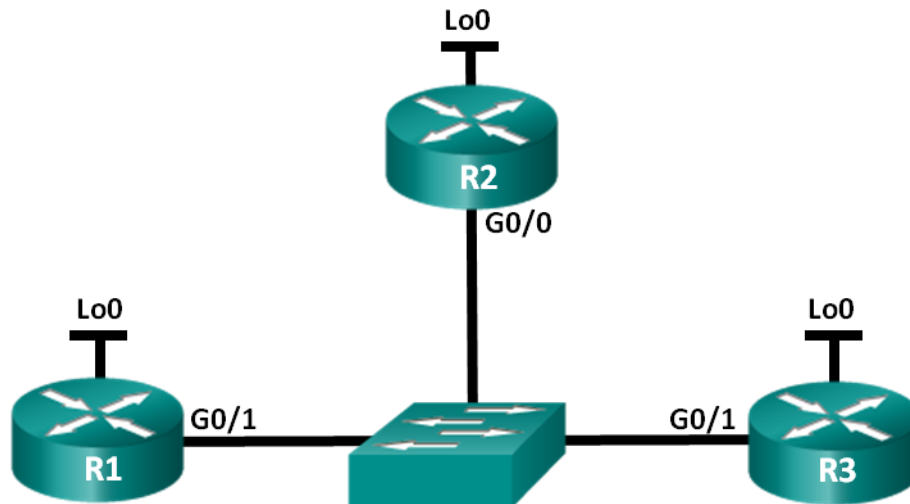
Step 6: Begin DR and BDR elections.

- a. Start the first election process.
 - 1) Students within the group will show each other the router priority numbers they selected for Step 1b.
 - 2) After comparing their priority numbers, the student with the highest priority number is elected the DR and the student with the second-highest priority number is elected the BDR. Any student, who wrote 0 as their priority number, cannot participate in the election.
 - 3) The elected DR student will announce the elections by saying "I am the DR for all of you in this group. Please send me any changes to your networks or interfaces to IP address 224.0.0.6. I will then forward those changes to all of you at IP address 224.0.0.5. Stay tuned for future updates."

- 4) The BDR's elected student will say, "I am your BDR. Please send all changes to your router interfaces or networks to the DR. If the DR does not announce your changes, I will step in and do that from that point onward."
- b. Start the second election process.
- 1) Students will hold up their DEFAULT ROUTER PRIORITY = 1 sign first. When it is agreed that all of the students have the same router priority, they will put that paper down.
 - 2) Next, students will display their ROUTER ID = Loopback (IPv4) address signs.
 - 3) The student with the highest loopback IPv4 address wins the election and repeats "I am the DR for all of you in this group. Our priorities are the same, but I have the highest loopback address on my router as compared to all of you; therefore, you have elected me as your DR. Please send all changes to your network addresses or interfaces to 224.0.0.6. I will then report any changes to all of you via 224.0.0.5."
 - 4) The BDR will repeat his/her respective phrase from Step 3a,4).
- c. Start the third election process, but this time, all students can choose which sides of their papers to display. The DR/BDR election process uses the highest router priority first, highest loopback router ID second, and highest IPv4 router ID third, and elects a DR and BDR.
- 1) Elect a DR and BDR.
 - 2) Justify your elections.
 - 3) If you have time, get together with another group and go through the scenario processes again to solidify DR and BDR elections.

Lab 20 - 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.

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.

Step 3: Configure basic settings for each router.

- Disable DNS lookup.
- Configure device names as shown in the topology.
- Assign **class** as the privileged EXEC password.
- Assign **cisco** as the console and vty passwords.
- Encrypt the plain text passwords.
- Configure a MOTD banner to warn users that unauthorized access is prohibited.
- Configure **logging synchronous** for the console line.
- Configure the IP addresses listed in the Addressing Table for all interfaces.
- Use the **show ip interface brief** command to verify that the IP addressing is correct and that the interfaces are active.
- 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.

Step 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.

- a. 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?

- b. 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?

Step 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.

- a. 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.
 - b. Verify that the OSPF has been configured and that R2 is the BDR. Record the command used for verification.
-

- c. 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.

Step 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.

- a. 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.
- b. 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	

- c. 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.

Step 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
```

Step 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
```

Step 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
```

Step 4: Reset the OSPF process.

- Issue the **show ip ospf neighbor** command to determine the DR and BDR.
- 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.

- 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.

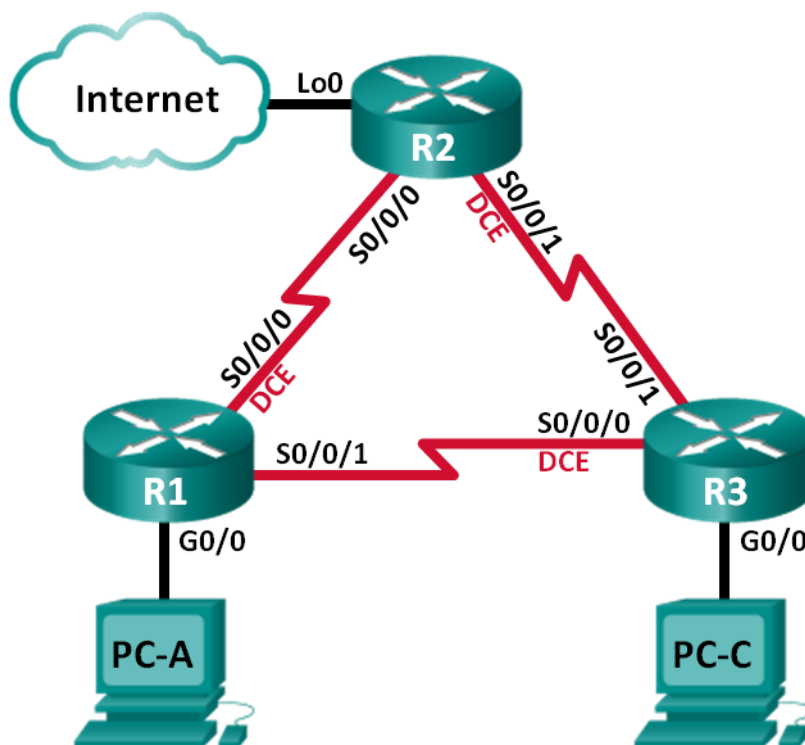
2. What is the significance of a 255 interface priority?

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.				

Lab 22 - 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

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 and configure OSPF route propagation.

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 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.

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

Step 2: Initialize and reload the routers as necessary.

Step 3: Configure basic settings for each router.

- Disable DNS lookup.
- Configure device name as shown in the topology.
- Assign **class** as the privileged EXEC password.
- Assign **cisco** as the console and vty passwords.
- Encrypt the plaintext passwords.
- Configure a MOTD banner to warn users that unauthorized access is prohibited.
- Configure **logging synchronous** for the console line.
- Configure the IP addresses listed in the Addressing Table for all interfaces.
- Set the clock rate for all DCE serial interfaces at 128000.
- Copy the running configuration to the startup configuration.

Step 4: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

Step 5: Test connectivity.

At this point, the PCs are unable to ping each other. 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.

Step 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**

Step 2: Configure OSPF network information on the routers.

Step 3: Verify OSPF routing.

- Issue the **show ip ospf neighbor** command to verify that each router is listing the other routers in the network.
- Issue the **show ip route ospf** command to verify that all OSPF networks are present in the routing tables on all routers.

Step 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, Step 3., substep i.

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

- 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

- Use the **bandwidth 128** interface command on all serial interfaces.
- 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

Step 2: Change the reference bandwidth on the routers.

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

Step 3: Change the route cost.

- 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
```

- 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.
- 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	

- d. 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.

Step 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.

Step 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
```

Step 3: Verify OSPF static route propagation.

- a. 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

- b. 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

- c. 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? _____

Reflection

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

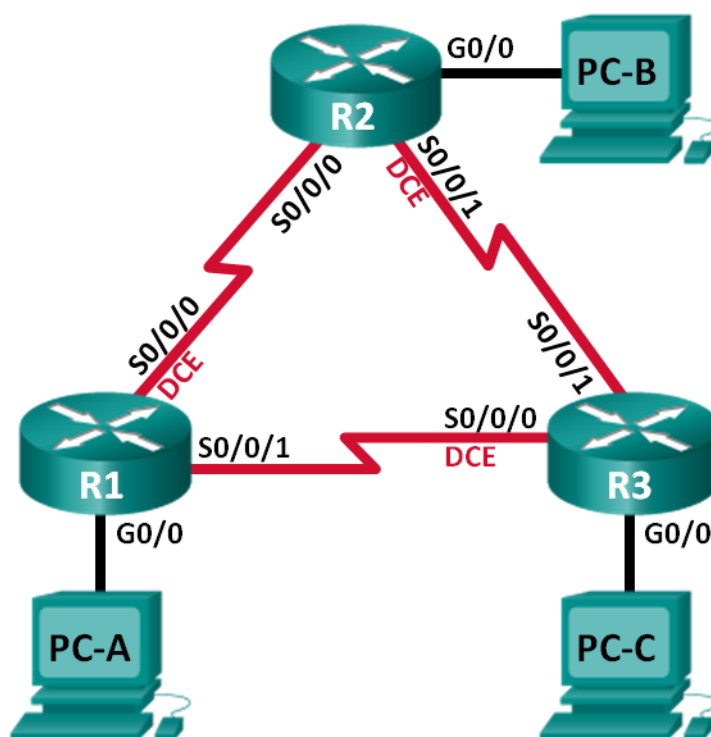
2. What does the **default-information originate** command do for a network using the OSPF routing protocol?
-

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.				

Lab 23 – 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.

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

Step 2: Configure PC hosts.

Step 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.

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

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

- b. 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.

- c. Resolve all problems that are found. Record the commands used to correct the issues.

- d. 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.

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

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

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

- Step 2: Verify that all interfaces are assigned to OSPFv2 area 0 on R1.**

-
-
-

- b. 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.

- c. Issue the **clear ip ospf process** command if necessary.
- d. Re-issue the **show ip protocols** command to verify that your changes had the desired effect.
- e. Issue the **show ip ospf interface brief** command to verify that all interfaces are listed as OSPF networks assigned to area 0.
- f. 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.
- g. 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”.

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

- a. 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.

- b. 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.

- c. Issue the **clear ip ospf process** command if necessary.
- d. Re-issue the **show ip protocols** command to verify that your changes had the desired effect.
- e. Issue the **show ip ospf interface brief** command to verify that all interfaces are listed as OSPF networks assigned to area 0.
- f. 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.
- g. 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”.

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

- a. 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.

- b. 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.

- c. Issue the **clear ip ospf process** command if necessary.
- d. Re-issue the **show ip protocols** command to verify that your changes had the desired effect.
- e. Issue the **show ip ospf interface brief** command to verify that all interfaces are listed as OSPF networks assigned to area 0.
- f. 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.
- g. 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".

Step 5: Verify OSPF neighbor information.

- a. Issue the **show ip ospf neighbor** command on all routers to view the OSPF neighbor information.

Step 6: Verify OSPFv2 Routing Information.

- a. 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? _____
- b. If any routing information is missing, resolve these issues.

Step 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.

Step 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.

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

- a. 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.

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

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

- a. 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.

- b. Make the necessary configuration changes to R1. Record the commands used to correct the issues.

- c. Issue the **clear ipv6 ospf process** command if necessary.
- d. Re-issue the **show ipv6 protocols** command to verify that your changes had the desired effect.
- e. Issue the **show ipv6 ospf interface brief** command to verify that all interfaces are listed as OSPF networks assigned to area 0.
- f. Issue the **show ipv6 ospf interface g0/0** command to verify that this interface is set not to advertise OSPFv3 routes.
- g. 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".

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

- a. 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.

- b. Make the necessary configuration changes to R2. Record the commands used to correct the issues.

- c. Issue the **clear ipv6 ospf process** command if necessary.
- d. Re-issue the **show ipv6 protocols** command to verify that your changes had the desired effect.
- e. Issue the **show ipv6 ospf interface brief** command to verify that all interfaces are listed as OSPF networks assigned to area 0.
- f. Issue the **show ipv6 ospf interface g0/0** command to verify that this interface is not set to advertise OSPFv3 routes.
- g. List any additional changes made to R2. If no problems were found on the device, then respond with “no problems were found”.

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

- a. 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.

- b. Make the necessary configuration changes to R3. Record the commands used to correct the issues.

- c. Issue the **clear ipv6 ospf process** command if necessary.
 - d. Re-issue the **show ipv6 protocols** command to verify that your changes had the desired effect.
 - e. Issue the **show ipv6 ospf interface brief** command to verify that all interfaces are listed as OSPF networks assigned to area 0.
 - f. Issue the **show ipv6 ospf interface g0/0** command to verify that this interface is set not to advertise OSPFv3 routes.
 - g. 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”.
-

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

- a. Issue the **show ipv6 ospf neighbor** command to verify that adjacencies have formed between neighboring routers.
- b. Resolve any OSPFv3 adjacency issues that still exist.

Step 7: Verify OSPFv3 routing information.

- a. 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? _____

- b. Resolve any routing issues that still exist.

Step 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

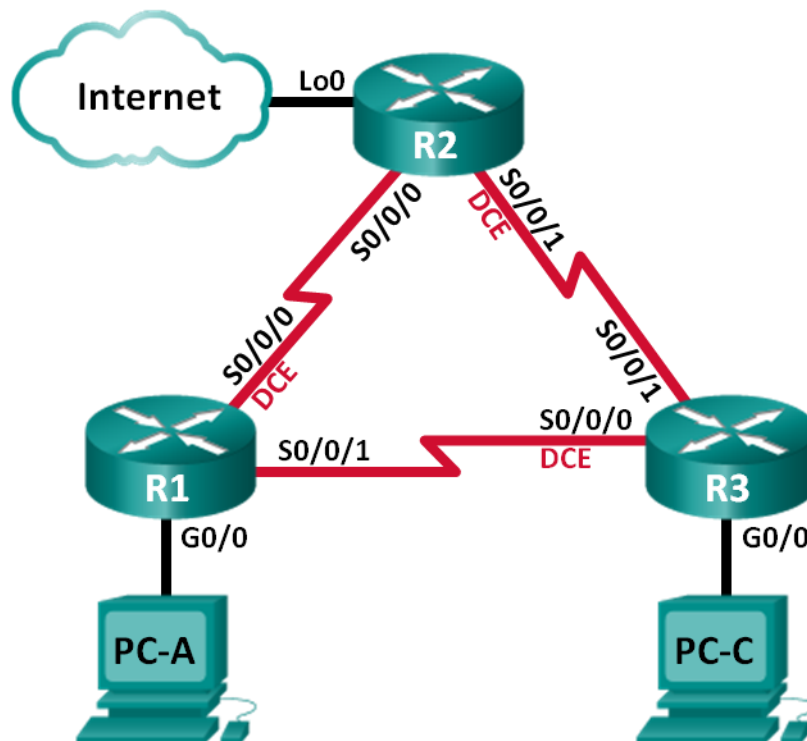
Why would you troubleshoot OSPFv2 and OSPFv3 separately?

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.				

Lab 25 – Troubleshooting Advanced 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	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 Load Device Configurations

Part 2: Troubleshoot OSPF

Background / Scenario

OSPF is a popular routing protocol used by businesses worldwide. A network administrator should be able to isolate OSPF issues and resolve those issues in a timely manner.

In this lab, you will troubleshoot a single-area OSPFv2 network and resolve all issues that exist.

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 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.

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

Step 2: Configure PC hosts.

Step 3: Load router configurations.

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

Router R1 Configuration:

```
conf t
hostname R1
enable secret class
no ip domain lookup
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
no shut
interface Serial0/0/0
bandwidth 128
```

```

ip address 192.168.12.1 255.255.255.252
clock rate 128000
no shut
interface Serial0/0/1
bandwidth 64
ip address 192.168.13.1 255.255.255.252
no shut
router ospf 1
auto-cost reference-bandwidth 1000
passive-interface g0/0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.12.0 0.0.0.3 area 0
network 192.168.13.0 0.0.0.3 area 0
banner motd ^
    Unauthorized Access is Prohibited!
^
line con 0
password cisco
logging synchronous
login
line vty 0 4
password cisco
login
transport input all
end

```

Router R2 Configuration:

```

conf t
hostname R2
enable secret class
no ip domain lookup
interface Loopback0
ip address 209.165.200.225 255.255.255.252
interface Serial0/0/0
bandwidth 182
ip address 192.168.12.2 255.255.255.252
no shut
interface Serial0/0/1
bandwidth 128
ip address 192.168.23.1 255.255.255.252
clock rate 128000
no shut
router ospf 1
router-id 2.2.2.2
auto-cost reference-bandwidth 1000
passive-interface g0/0

```

```

network 192.168.12.0 0.0.0.3 area 0
network 192.168.23.0 0.0.0.3 area 0
ip route 0.0.0.0 0.0.0.0 Loopback0
banner motd ^
    Unauthorized Access is Prohibited!
^
line con 0
    password cisco
    logging synchronous
    login
line vty 0 4
    password cisco
    login
    transport input all
end

```

Router R3 Configuration:

```

conf t
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
    no shut
interface Serial0/0/0
    bandwidth 128
    ip address 192.168.13.2 255.255.255.252
    clock rate 128000
    no shut
interface Serial0/0/1
    bandwidth 128
    ip address 192.168.23.2 255.255.255.252
    no shut
router ospf 1
    router-id 3.3.3.3
passive-interface g0/0
    network 192.168.3.0 0.0.0.255 area 0
    network 192.168.13.0 0.0.0.3 area 0
    network 192.168.23.0 0.0.0.3 area 0
banner motd ^
    Unauthorized Access is Prohibited!
^
line con 0
    password cisco

```

```

logging synchronous
login
line vty 0 4
password cisco
login
transport input all
end

```

Step 4: Test end-to-end connectivity.

All interfaces should be up and the PCs should be able to ping the default gateway.

Part 2: Troubleshoot OSPF

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

Additional OSPF Requirements:

- Each router should have 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**
- All serial interface clocking rates should be set at 128 Kb/s and a matching bandwidth setting should be available to allow OSPF cost metrics to be calculated correctly.
- The 1941 routers have Gigabit interfaces, so the default OSPF reference bandwidth should be adjusted to allow cost metrics to reflect appropriate costs for all interfaces.
- OSPF should propagate a default route to the Internet. This is simulated by using Loopback interface 0 on R2.

List the commands used during your OSPF troubleshooting process:

List the changes made to resolve the OSPF issues. If no problems were found on the device, then respond with “no problems were found”.

R1 Router:

R2 Router:

R3 Router:

Reflection

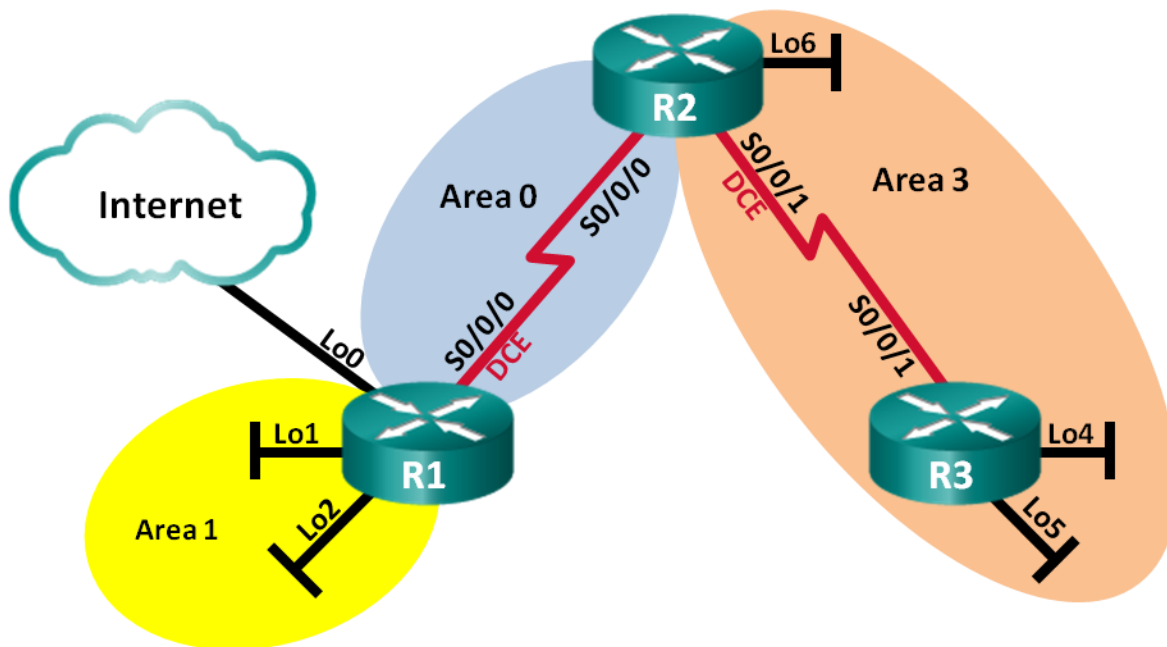
How would you change the network in this lab so that all LAN traffic was routed through R2?

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.				

Lab 26 – Troubleshooting Multiarea OSPFv2 and OSPFv3

Topology



Addressing Table

Device	Interface	IP Address
R1	Lo0	209.165.200.225/30
	Lo1	192.168.1.1/24 2001:DB8:ACAD:1::1/64 FE80::1 link-local
	Lo2	192.168.2.1/24 2001:DB8:ACAD:2::1/64 FE80::1 link-local
	S0/0/0 (DCE)	192.168.12.1/30 2001:DB8:ACAD:12::1/64 FE80::1 link-local
R2	S0/0/0	192.168.12.2/30 2001:DB8:ACAD:12::2/64 FE80::2 link-local
	S0/0/1 (DCE)	192.168.23.2/30 2001:DB8:ACAD:23::2/64 FE80::2 link-local
	Lo6	192.168.6.1/24 2001:DB8:ACAD:6::1/64 FE80::2 link-local
R3	Lo4	192.168.4.1/24 2001:DB8:ACAD:4::1/64 FE80::3 link-local
	Lo5	192.168.5.1/24 2001:DB8:ACAD:5::1/64 FE80::3 link-local
	S0/0/1	192.168.23.1/30 2001:DB8:ACAD:23::1/64 FE80::3 link-local

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 an open-standard link-state routing protocol for IP networks. OSPFv2 is defined for IPv4 networks, while OSPFv3 is defined for IPv6 networks. OSPFv2 and OSPFv3 are completely isolated routing protocols, meaning changes in OSPFv2 do not affect OSPFv3 routing, and vice versa.

In this lab, a multiarea 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)
- Console cables to configure the Cisco IOS devices via the console ports
- Serial cables as shown in the topology

Part 1: Build the Network and Load Device Configurations

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

Step 2: Load router configuration files.

Load the following configurations into the appropriate router. All routers have the same passwords. The enable password is **class**, and the line password is **cisco**.

Router R1 Configuration:

```
enable
conf t
hostname R1
enable secret class
ipv6 unicast-routing
no ip domain lookup
interface Loopback0
 ip address 209.165.200.225 255.255.255.252
interface Loopback1
 ip address 192.168.1.1 255.255.255.0
 ipv6 address 2001:DB80:ACAD:1::1/64
 ipv6 ospf network point-to-point
interface Loopback2
 ip address 192.168.2.1 255.255.255.0
 ipv6 address 2001:DB8:ACAD:2::1/64
 ipv6 ospf 1 area 1
 ipv6 ospf network point-to-point
interface Serial0/0/0
```

```

    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 ospf 1 area 0
    clock rate 128000
    shutdown
router ospf 1
    router-id 1.1.1.1
    passive-interface Loopback1
    passive-interface Loopback2
network 192.168.2.0 0.0.0.255 area 1
    network 192.168.12.0 0.0.0.3 area 0
    default-information originate
ipv6 router ospf 1
ip route 0.0.0.0 0.0.0.0 Loopback0
banner motd @
    Unauthorized Access is Prohibited! @
line con 0
    password cisco
    logging synchronous
    login
line vty 0 4
    password cisco
    logging synchronous
    login
    transport input all
end

```

Router R2 Configuration:

```

enable
conf t
hostname R2
ipv6 unicast-routing
no ip domain lookup
enable secret class
interface Loopback6
    ip address 192.168.6.1 255.255.255.0
    ipv6 address 2001:DB8:CAD:6::1/64
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 ospf 1 area 0
    no shutdown
interface Serial0/0/1
    ip address 192.168.23.2 255.255.255.252

```

```

ipv6 address FE80::2 link-local
ipv6 address 2001:DB8:ACAD:23::2/64
ipv6 ospf 1 area 3
clock rate 128000
no shutdown
router ospf 1
  router-id 2.2.2.2
  passive-interface Loopback6
  network 192.168.6.0 0.0.0.255 area 3
  network 192.168.12.0 0.0.0.3 area 0
  network 192.168.23.0 0.0.0.3 area 3
ipv6 router ospf 1
  router-id 2.2.2.2
banner motd @
  Unauthorized Access is Prohibited! @
line con 0
  password cisco
  logging synchronous
  login
line vty 0 4
  password cisco
  logging synchronous
  login
  transport input all
end

```

Router R3 Configuration:

```

enable
conf t
hostname R3
no ip domain lookup
ipv6 unicast-routing
enable secret class
interface Loopback4
  ip address 192.168.4.1 255.255.255.0
  ipv6 address 2001:DB8:ACAD:4::1/64
  ipv6 ospf 1 area 3
interface Loopback5
  ip address 192.168.5.1 255.255.255.0
  ipv6 address 2001:DB8:ACAD:5::1/64
  ipv6 ospf 1 area 3
interface Serial0/0/1
  ip address 192.168.23.1 255.255.255.252
  ipv6 address FE80::3 link-local
  ipv6 address 2001:DB8:ACAD:23::1/64
  ipv6 ospf 1 area 3

```

```

no shutdown
router ospf 1
  router-id 3.3.3.3
  passive-interface Loopback4
  passive-interface Loopback5
  network 192.168.4.0 0.0.0.255 area 3
  network 192.168.5.0 0.0.0.255 area 3
ipv6 router ospf 1
  router-id 3.3.3.3
banner motd @
  Unauthorized Access is Prohibited! @
line con 0
  password cisco
  logging synchronous
  login
line vty 0 4
  password cisco
  logging synchronous
  login
  transport input all
end

```

Step 3: Save your configuration.

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.

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

- Issue the **show ip interface brief** command on all three routers to verify that the interfaces are in an up/up state.
- Issue the **show run | section interface** command to view all the commands related to interfaces.
- Resolve all problems found. Record the commands used to correct the configuration.

- d. Using the **ping** command, verify that IPv4 and IPv6 connectivity has been established on all directly connected router interfaces. If problems still exist, continue troubleshooting Layer 3 issues.

Part 3: Troubleshoot OSPFv2

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

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

From each router, ping all interfaces on the other routers. Record your results below as IPv4 OSPFv2 connectivity problems do exist.

Step 2: Verify that all interfaces are assigned to the proper OSPFv2 areas on R1.

- a. Issue the **show ip protocols** command to verify that OSPF is running and that all networks are being advertised in the correct areas. Verify that the router ID is set correctly, as well for OSPF.
- b. If required, make the necessary changes needed to the configuration on R1 based on the output from the **show ip protocols** command. Record the commands used to correct the configuration.

- c. If required, re-issue the **show ip protocols** command to verify that your changes had the desired effect.
- d. Issue the **show ip ospf interface brief** command to verify that the serial interface and loopback interfaces 1 and 2 are listed as OSPF networks assigned to their respective areas.
- e. Resolve any problems discovered on R1 for OSPFv2.

Step 3: Verify that all interfaces are assigned to the proper OSPFv2 areas on R2.

- a. Issue the **show ip protocols** command to verify that OSPF is running and that all networks are being advertised in their proper respective areas. Verify that the router ID is also set correctly.
- b. If required, make any necessary changes to the configuration on R2 based on the output from the **show ip protocols** command. Record the commands used to correct the configuration.

- c. If required, re-issue the **show ip protocols** command to verify that your changes had the desired effect.
- d. Issue the **show ip ospf interface brief** command to verify that all interfaces are listed as OSPF networks assigned to their proper respective areas.
- e. Resolve any problems discovered on R2 for OSPFv2.

Step 4: Verify that all interfaces are assigned to the proper OSPFv2 areas on R3.

- a. Issue the **show ip protocols** command to verify that OSPF is running and that all networks are being advertised in their respective areas. Verify that the router ID is also set correctly.
- b. If required, 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 configuration.

- c. If required, re-issue the **show ip protocols** command to verify that your changes had the desired effect.
- d. Issue the **show ip ospf interface brief** command to verify that all interfaces are listed as OSPF networks assigned to their proper areas.
- e. Resolve any problems discovered on R3 for OSPFv2.

Step 5: Verify OSPFv2 neighbor information.

Issue the **show ip ospf neighbor** command to verify that each router has all OSPFv2 neighbors listed.

Step 6: Verify OSPFv2 routing information.

- a. Issue the **show ip route ospf** command to verify that each router has all OSPFv2 routes in their respective routing tables.
- b. If any OSPFv2 routes are missing, troubleshoot and resolve the problems.

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

From each router, ping all interfaces on other routers. If IPv4 end-to-end connectivity does not exist, then continue troubleshooting to resolve any remaining issues.

Part 4: Troubleshoot OSPFv3

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

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

From each router, ping all interfaces on the other routers. Record your results as IPv6 connectivity problems do exist.

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

- a. 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 the pipe section to the **show run** command, the **ipv6 unicast-routing** command is displayed if IPv6 routing has been enabled.

- b. If IPv6 unicast routing is not enabled on one or more routers, enable it now. If required, record the commands used to correct the configuration.

Step 3: Verify that all interfaces are assigned to the proper OSPFv3 areas on R1.

- a. Issue the **show ipv6 protocols** command to verify that the router ID is correct and the expected interfaces display in their proper areas.
- b. If required, make any necessary changes to the configuration on R1 based on the output from the **show ipv6 protocols** command. Record the commands used to correct the configuration. It may be necessary to reset OSPF process by issuing the **clear ipv6 ospf process** command.

- c. Re-issue the **show ipv6 protocols** command on R1 to make sure changes took effect.
- d. Enter the **show ipv6 route ospf** command on R1 to verify that the routes are configured correctly.

```
R1# 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
OI  2001:DB8:ACAD:4::1/128 [110/128]
    via FE80::2, Serial0/0/0
OI  2001:DB8:ACAD:5::1/128 [110/128]
    via FE80::2, Serial0/0/0
OI  2001:DB8:ACAD:23::/64 [110/128]
    via FE80::2, Serial0/0/0
```

Step 4: Verify that all interfaces are assigned to the proper OSPFv3 areas on R2.

- a. Issue the **show ipv6 protocols** command and verify that the router ID is correct and that the expected interfaces are showing up under their proper areas.
- b. If required, make any necessary changes to the configuration on R2 based on the output from the **show ipv6 protocols** command. Record the commands used to correct the configuration. It may be necessary to reset OSPF process by issuing the **clear ipv6 ospf process** command.

- c. Verify that the configuration change has the desired effect.

Step 5: Verify that all interfaces are assigned to the proper OSPFv3 areas on R3.

- a. Issue the **show ipv6 protocols** command to verify that the router ID is correct and the expected interfaces display under their respective areas.
- b. If required, make any necessary changes to the configuration on R3 based on the output from the **show ipv6 protocols** command. Record the commands used to correct the configuration. It may be necessary to reset OSPF process by issuing the **clear ipv6 ospf process** command.

- c. Verify that the configuration changes have the desired effect.

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

- a. Issue the **show ipv6 ospf neighbor** command to verify that adjacencies have formed between neighboring routers.

Step 7: Verify OSPFv3 routing information.

- a. Issue the **show ipv6 route ospf** command, and verify that OSPFv3 routes exist to all networks.
- b. Resolve any routing issues that still exist.

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

From each router, ping all of the IPv6 interfaces on the other routers. If IPv6 end-to-end issues still exist, continue troubleshooting to resolve any remaining issues.

Reflection

Why not just use the **show running-config** command to resolve all issues?

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.				

OSPF Troubleshooting Mastery

Objective

Explain the process and tools used to troubleshoot a single-area OSPF network.

Scenario

You have decided to change your routing protocol from RIPv2 to OSPFv2. Your small- to medium-sized business network topology will not change from its original physical settings. Use the diagram on the PDF for this activity as your company's small- to medium- business network design.

Your addressing design is complete and you then configure your routers with IPv4 and VLSM. OSPF has been applied as the routing protocol. However, some routers are sharing routing information with each other and some are not.

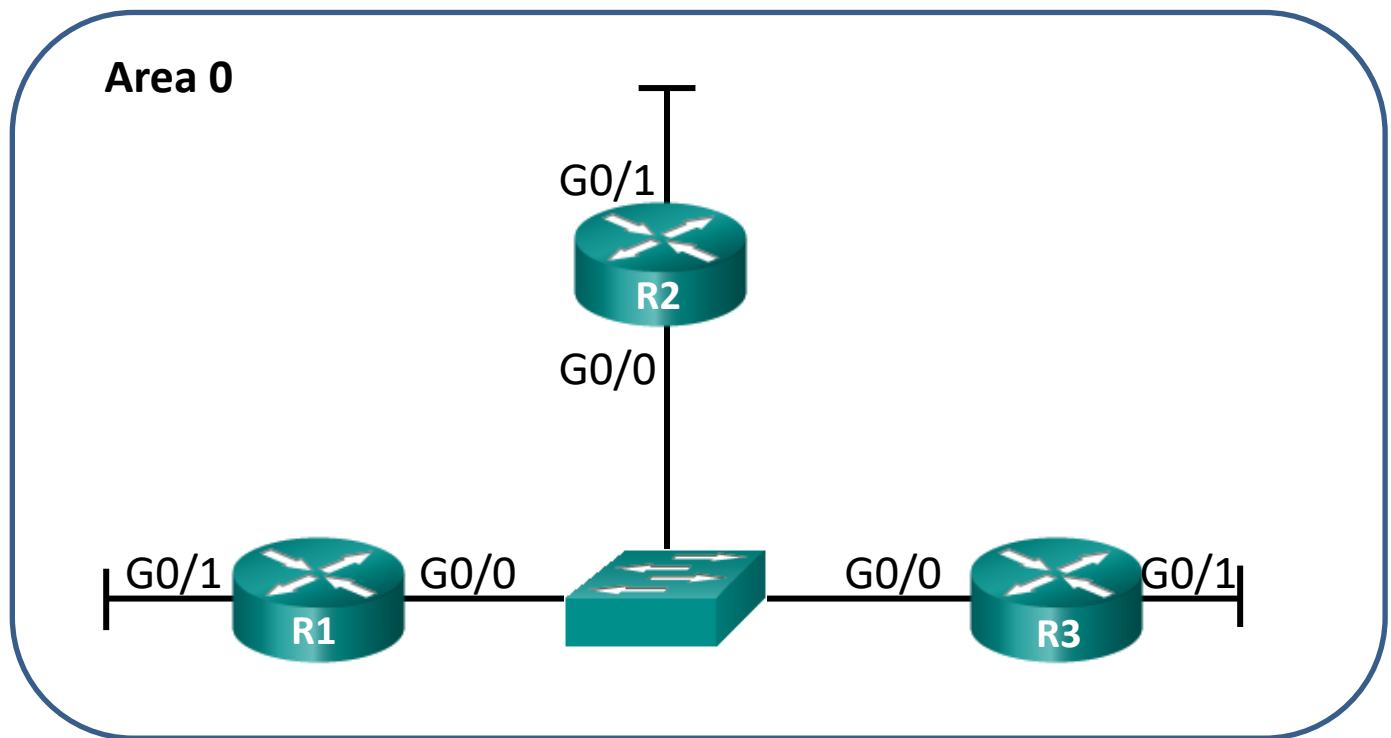
Open the PDF file that accompanies this modeling activity and follow the directions to complete the activity.

When the steps in the directions are complete, regroup as a class and compare recorded activity correction times. The group taking the shortest time to find and fix the configuration error will be declared the winner only after successfully explaining how they found the error, fixed it, and proved that the topology is now working.

Required Resources

- Topology diagram
- Packet Tracer software
- Timer

Topology Diagram



Directions

Choose a partner from the class with whom to work on this activity. Use Packet Tracer to create the topology diagram shown for this activity.

Step 1: Build the topology based on the modeling activity page for this scenario.

Step 2: Configure the routers.

- Use IPv4 for all interfaces.
- Incorporate VLSM into the addressing scheme.
- Make one intentional configuration error.
- Verify that the network does not work based upon the intentional error.
- Save your file to be used with Step 3.

Step 3: Exchange your Packet Tracer file with another group.

- Find the configuration error on the Packet Tracer network file you received from another group.
- Fix the OSPF configuration error so that the network operates fully.

- Record the time it took to find and fix the OSPF network error. _____
- When complete, meet with your class to determine the Master Troubleshooter for the day.