



## CCNA Routing and Switching: Scaling Networks

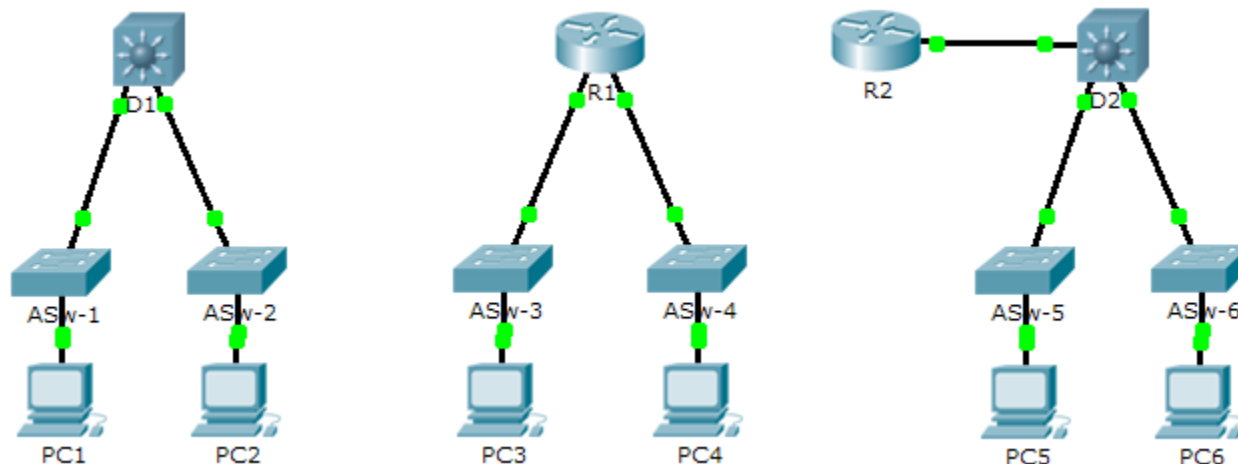
Instructor Packet Tracer Manual

This document is exclusive property of Cisco Systems, Inc. Permission is granted to print and copy this document for non-commercial distribution and exclusive use by instructors in the CCNA Routing and Switching: Scaling Networks course as part of an official Cisco Networking Academy Program.

# Packet Tracer - Comparing 2960 and 3560 Switches (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



## Objective

Part 1: Compare Layer 2 and Layer 3 Switches

Part 2: Compare a Layer 3 Switch and a Router

## Background

In this activity, you will use various commands to examine three different switching topologies and compare the similarities and differences between the 2960 and 3560 switches. You will also compare the routing table of a 1941 router with a 3560 switch.

## Part 1: Compare Layer 2 and Layer 3 Switches

- a. Examine the physical aspects of **D1** and **ASw-1**.
  - How many physical interfaces does each switch have in total? **26**
  - How many Fast Ethernet and Gigabit Ethernet interfaces does each switch have? **24 Fast Ethernet and 2 Gigabit Ethernet interfaces.**
  - List the transmission speed of the Fast Ethernet and Gigabit Ethernet interfaces on each switch. **The Fast Ethernet interfaces support speeds of 10/100mbps and the Gigabit Ethernet interfaces support speeds of up to 1000mbps.**
  - Are either of the two switches modular in design? **No**
- b. The interface of a 3560 switch can be configured as a Layer 3 interface by entering the **no switchport** command in interface configuration mode. This allows technicians to assign an IP address and subnet mask to the interface the same way it is configured on a router's interface.
  - What is the difference between a Layer 2 switch and a Layer 3 switch? **A Layer 2 switch makes forwarding decisions based on L2 (MAC) addresses. Interfaces on Layer 3 switches can be**

configured with IP addresses. The switches can also be configured with routing protocols just like a router.

- What is the difference between a switch's physical interface and the VLAN interface? A switch's physical interface is used to physically connect end devices to the network. A switched virtual interface (SVI or VLAN) is used to configure the switch with an IP address so that it can be managed remotely.
- On which layer does a 2960 and 3560 operate? The 2960 operates at Layer 2, and the 3560 operates on Layers 2 and 3.
- Which command allows a technician to assign an IP address and subnet mask to the Fast Ethernet interface on a 2960? Fast Ethernet interfaces on 2960 switches cannot be configured with an IP address and subnet mask.
- Issue the **show run** command to examine the configurations of the **D1** and **ASw-1** switches. Do you notice any differences between them? Yes, D1's G0/1 and the G0/2 interfaces are configured with the **no switchport** command and show an IP address and mask configured on both Gigabit Ethernet interfaces. D1 has IP routing enabled.
- Display the routing table on both switches using the **show ip route** command. Why do you think the command does not work on **ASW-1**, but works on the **D1**? It works on D1 because it functions on Layers 2 and 3, which allows it to function as a Layer 2 switch but at the same time, allows it to route packets and make forwarding decisions based on Layer 3 information (IP addresses) that conventional switches cannot.

## Part 2: Compare a Layer 3 Switch and a Router

- a. Up until recently, switches and routers have been separate and distinct devices. The term switch was set aside for hardware based devices that function at Layer 2. Routers, on the other hand, are devices that make forwarding decisions based on Layer 3 information and use routing protocols to share routing information and to communicate with other routers. Layer 3 switches, such as the 3560, can be configured to forward Layer 3 packets. Entering the **ip routing** command in global configuration mode allows Layer 3 switches to be configured with routing protocols, thereby possessing some of the same capabilities as a router. However, although similar in some forms, they are different in many other aspects.
  - Open the Physical tab on D1 and R1. Do you notice any similarities and differences between the two? They both have a console port and both two Gigabit Ethernet interfaces. R1 is modular and can add various interfaces while D1 has only fixed interfaces. R1 has Serial and Asynchronous interfaces while D1 only has Ethernet interfaces. In retrospect, D1 can only use copper cables while R1 can use various connection types.
  - Issue the **show run** command and examine the configurations of R1 and D1. What differences do you see between the two? R1 and D1 have the same IP addresses configured on them but on different interfaces. In order for the switch port to be assigned an IP address technicians will have to issue the **no switchport** command.
  - Which command allows D1 to configure an IP address on one of its physical interfaces? The **no switchport** command.
  - Use the **show ip route** command on both devices. Do you see any similarities or differences between the two tables? The codes are the same except the router has an L code for local. This is a link that is configured on the physical interface of R1, while the switch does not have it. Both devices display the same networks in their routing tables.

- Now, analyze the routing table of R2 and D2. What is evident now that was not in the configuration of R1 and D1? They both have EIGRP configured and both are learning networks from one another.
- b. Verify that each topology has full connectivity by completing the following tests:
- Ping from **PC1** to **PC2**
  - Ping from **PC3** to **PC4**
  - Ping from **PC5** to **PC6**

In all three examples, each PC is on a different network. Which device is used to provide communication between networks? Router or multilayer switch.

Why were we able to ping across networks without there being a router? A multilayer switch can route between networks as long as it is configured with an IP address and has IP routing enabled. It must also be enabled if you plan to run routing protocols such as EIGRP on the switch. Don't forget the **no switchport** command must be enabled on the interface in order to assign an IP address and subnet mask on the switch's physical interface.

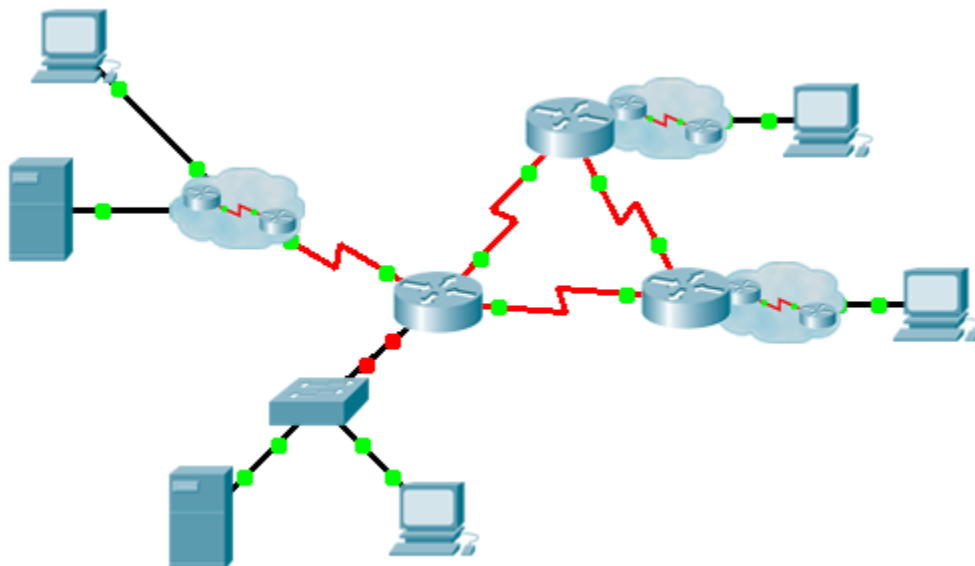
### Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Compare Layer 2 and Layer 3 Switches	a	20	
	b	40	
Part 1 Total		60	
Part 2: Compare a Layer 3 Switch and a Router	a	30	
	b	10	
Part 2 Total		40	
Total Score		100	

## Packet Tracer – Skills Integration Challenge (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

### Topology



## Addressing Table

**Instructor Note:** The student version has blanks in place of all variables shown in double brackets.

Device	Interface	IP Address	Subnet Mask	Default Gateway
[[R1Name]]	G0/0.15	[[R1G0sub15Add]]	[[R1G0sub15SM]]	N/A
	G0/0.30	[[R1G0sub30Add]]	[[R1G0sub30SM]]	N/A
	G0/0.45	[[R1G0sub45Add]]	[[R1G0sub45SM]]	N/A
	G0/0.60	[[R1G0sub60Add]]	[[R1G0sub60SM]]	N/A
	S0/0/0	[[R1S000Add]]	255.255.255.252	N/A
	S0/0/1	[[R1S001Add]]	255.255.255.252	N/A
	S0/1/0	[[R1S010Add]]	255.255.255.252	N/A
[[R2Name]]	G0/0	[[R2G00Add]]	[[R2R3LanSM]]	N/A
	S0/0/0	[[R2S000Add]]	255.255.255.252	N/A
	S0/0/1	[[R2S001Add]]	255.255.255.252	N/A
[[R3Name]]	G0/0	[[R3G00Add]]	[[R2R3LanSM]]	N/A
	S0/0/0	[[R3S000Add]]	255.255.255.252	N/A
	S0/0/1	[[R3S001Add]]	255.255.255.252	N/A
[[S1Name]]	VLAN 60	[[S1VLAN60Add]]	[[R1G0sub60SM]]	[[R1G0sub60Add]]
[[PC1Name]]	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned

## VLANs and Port Assignments Table

VLAN Number - Name	Port assignment	Network
15 - Servers	F0/11 - F0/20	[[R1-VLANsrvNet]]
30 - PCs	F0/1 - F0/10	[[R1-VLANpcNet]]
45 - Native	G1/1	[[R1-VLANntvNet]]
60 - Management	VLAN 60	[[R1-VLANmanNet]]

## Scenario

This activity includes many of the skills that you have acquired during your CCNA studies. First, you will complete the documentation for the network. So make sure you have a printed version of the instructions. During implementation, you will configure VLANs, trunking, port security and SSH remote access on a switch. Then, you will implement inter-VLAN routing and NAT on a router. Finally, you will use your documentation to verify your implementation by testing end-to-end connectivity.

## Documentation

You are required to fully document the network. You will need a print out of this instruction set, which will include an unlabeled topology diagram:

- Label all the device names, network addresses and other important information that Packet Tracer generated.
- Complete the **Addressing Table** and **VLANs and Port Assignments Table**.
- Fill in any blanks in the **Implementation** and **Verification** steps. The information is supplied when you launch the Packet Tracer activity.

### Implementation

Note: All devices in the topology except **[[R1Name]]**, **[[S1Name]]**, and **[[PC1Name]]** are fully configured. You do not have access to the other routers. You can access all the servers and PCs for testing purposes.

Implement to following requirements using your documentation:

#### **[[S1Name]]**

- Configure remote management access including IP addressing and SSH:
  - Domain is cisco.com
  - User **[[UserText]]** with password **[[UserPass]]**
  - Crypto key length of 1024
  - SSH version 2, limited to 2 authentication attempts and a 60 second timeout
  - Clear text passwords should be encrypted.
- Configure, name and assign VLANs. Ports should be manually configured as access ports.
- Configure trunking.
- Implement port security:
  - On Fa0/1, allow 2 MAC addresses that are automatically added to the configuration file when detected. The port should not be disabled, but a syslog message should be captured if a violation occurs.
  - Disable all other unused ports.

#### **[[R1Name]]**

- Configure inter-VLAN routing.
- Configure DHCP services for VLAN 30. Use **LAN** as the case-sensitive name for the pool.
- Implement routing:
  - Use OSPF process ID 1 and router ID 1.1.1.1
  - Configure one network statement for the entire **[[DisplayNet]]** address space
  - Disable interfaces that should not send OSPF messages.
  - Configure a default route to the Internet.
- Implement NAT:
  - Configure a standard, one statement ACL number 1. All IP addresses belonging to the **[[DisplayNet]]** address space are allowed.
  - Refer to your documentation and configure static NAT for the File Server.
  - Configure dynamic NAT with PAT using a pool name of your choice, a /30 mask, and these two public addresses:

**[[NATPoolText]]**

#### **[[PC1Name]]**

Verify **[[PC1Name]]** has received full addressing information from **[[R1Name]]**.

### Verification

All devices should now be able to ping all other devices. If not, troubleshoot your configurations to isolate and solve problems. A few tests include:

- Verify remote access to **[[S1Name]]** by using SSH from a PC.
- Verify VLANs are assigned to appropriate ports and port security is in force.
- Verify OSPF neighbors and a complete routing table.
- Verify NAT translations and statics.
  - **Outside Host** should be able to access **File Server** at the public address.
  - Inside PCs should be able to access **Web Server**.
- Document any problems you encountered and the solutions in the **Troubleshooting Documentation** table below.

### Troubleshooting Documentation

Problem	Solution

### Suggested Scoring Rubric

Packet Tracer scores 70 points. Documentation is worth 30 points.

ID:[[indexAdds]][[indexNames]]

\*\*\*\*\*

ISOMORPH ID KEY:

ID = XY where;

X = indexAdds for /24 private address space

Y = indexNAMES for device names

Note: Each seed contains variables that are independent of the other seeds. You do not need to test all the



```
various combinations.
=====
ISOMORPH ID = 00
=====
!HQ!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
ip dhcp pool LAN
  network 172.16.15.32 255.255.255.224
  default-router 172.16.15.33
interface GigabitEthernet0/0
  no shutdown
interface GigabitEthernet0/0.15
  encapsulation dot1Q 15
  ip address 172.16.15.17 255.255.255.240
  ip nat inside
interface GigabitEthernet0/0.30
  encapsulation dot1Q 30
  ip address 172.16.15.33 255.255.255.224
  ip nat inside
interface GigabitEthernet0/0.45
  encapsulation dot1Q 45 native
  ip address 172.16.15.1 255.255.255.248
interface GigabitEthernet0/0.60
  encapsulation dot1Q 60
  ip address 172.16.15.9 255.255.255.248
router ospf 1
  router-id 1.1.1.1
  passive-interface GigabitEthernet0/0
network 172.16.15.0 0.0.0.255 area 0
!
ip nat pool TEST 209.165.200.225 209.165.200.226 netmask 255.255.255.252
ip nat inside source list 1 pool TEST overload
ip nat inside source static 172.16.15.18 209.165.200.227
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
access-list 1 permit 172.16.15.0 0.0.0.255
interface s0/0/0
  ip nat inside
interface s0/0/1
  ip nat inside
interface s0/1/0
  ip nat outside
end
wr
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!HQ-Sw!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!
en
conf t
int vlan 60
ip add 172.16.15.10 255.255.255.248
no shut
ip default-gateway 172.16.15.9
vlan 15
name Servers
vlan 30
name PCs
vlan 45
name Native
vlan 60
name Management
interface range fa0/1 - 10
switchport mode access
switchport access vlan 30
interface fa0/1
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
interface range fa0/11 - 20
switchport mode access
switchport access vlan 15
interface g1/1
switchport mode trunk
switchport trunk native vlan 45
interface range fa0/21 - 24 , g1/2
shutdown
ip domain-name cisco.com
crypto key gen rsa
1024

user HQadmin pass ciscoclass
service password-encryption
ip ssh version 2
ip ssh auth 2
ip ssh time 60
line vty 0 15
login local
transport input ssh
```

```
=====
ISOMORPH ID = 11
=====
!Admin!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
ip dhcp pool LAN
  network 10.10.10.192 255.255.255.192
  default-router 10.10.10.193
interface GigabitEthernet0/0
  no shutdown
interface GigabitEthernet0/0.15
  encapsulation dot1Q 15
  ip address 10.10.10.161 255.255.255.224
  ip nat inside
interface GigabitEthernet0/0.30
  encapsulation dot1Q 30
  ip address 10.10.10.193 255.255.255.192
  ip nat inside
interface GigabitEthernet0/0.45
  encapsulation dot1Q 45 native
  ip address 10.10.10.129 255.255.255.240
interface GigabitEthernet0/0.60
  encapsulation dot1Q 60
  ip address 10.10.10.145 255.255.255.240
router ospf 1
  router-id 1.1.1.1
  passive-interface GigabitEthernet0/0
network 10.10.10.0 0.0.0.255 area 0
interface s0/0/0
  ip nat inside
interface s0/0/1
  ip nat inside
interface s0/1/0
  ip nat outside
!
ip nat pool TEST 198.133.219.128 198.133.219.129 netmask 255.255.255.252
ip nat inside source list 1 pool TEST overload
ip nat inside source static 10.10.10.162 198.133.219.130
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
access-list 1 permit 10.10.10.0 0.0.0.255
end
wr
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!Admin-Sw!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
en
conf t
int vlan 60
ip add 10.10.10.146 255.255.255.240
no shut
ip default-gateway 10.10.10.145
vlan 15
name Servers
vlan 30
name PCs
vlan 45
name Native
vlan 60
name Management
interface range fa0/1 - 10
switchport mode access
switchport access vlan 30
interface fa0/1
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
interface range fa0/11 - 20
switchport mode access
switchport access vlan 15
interface g1/1
switchport mode trunk
switchport trunk native vlan 45
interface range fa0/21 - 24 , g1/2
shutdown
ip domain-name cisco.com
crypto key gen rsa
1024

user Admin pass letmein
service password-encryption
ip ssh version 2
ip ssh auth 2
ip ssh time 60
line vty 0 15
login local
transport input ssh
```

```
=====
ISOMORPH ID: 22
```

```
=====
!Central!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
ip dhcp pool LAN
  network 192.168.45.128 255.255.255.192
  default-router 192.168.45.129
interface GigabitEthernet0/0
  no shutdown
interface GigabitEthernet0/0.15
  encapsulation dot1Q 15
  ip address 192.168.45.65 255.255.255.192
  ip nat inside
interface GigabitEthernet0/0.30
  encapsulation dot1Q 30
  ip address 192.168.45.129 255.255.255.192
  ip nat inside
interface GigabitEthernet0/0.45
  encapsulation dot1Q 45 native
  ip address 192.168.45.17 255.255.255.240
interface GigabitEthernet0/0.60
  encapsulation dot1Q 60
  ip address 192.168.45.33 255.255.255.240
router ospf 1
  router-id 1.1.1.1
  passive-interface GigabitEthernet0/0
network 192.168.45.0 0.0.0.255 area 0
interface s0/0/0
  ip nat inside
interface s0/0/1
  ip nat inside
interface s0/1/0
  ip nat outside
!
ip nat pool TEST 64.100.32.56 64.100.32.57 netmask 255.255.255.252
ip nat inside source list 1 pool TEST overload
ip nat inside source static 192.168.45.66 64.100.32.58
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
access-list 1 permit 192.168.45.0 0.0.0.255
end
wr
!!!!!!!!!!!!!!!!!!!!!!
!Cnt-Sw!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
```

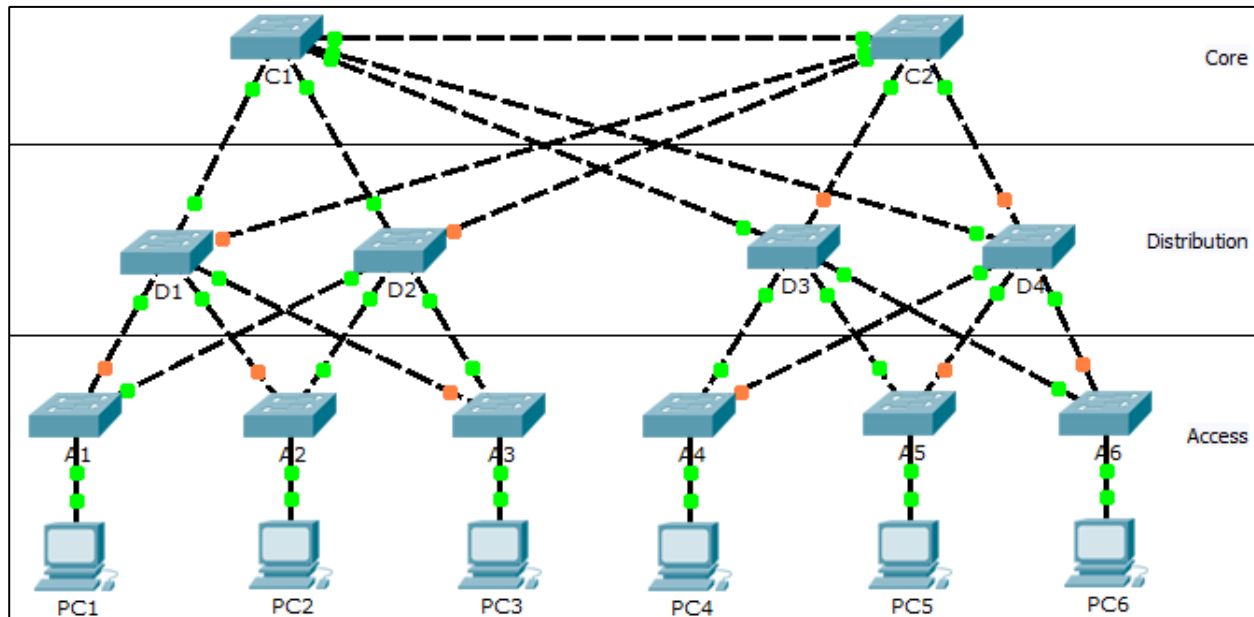
```
int vlan 60
ip add 192.168.45.34 255.255.255.240
no shut
ip default-gateway 192.168.45.33
vlan 15
name Servers
vlan 30
name PCs
vlan 45
name Native
vlan 60
name Management
interface range fa0/1 - 10
switchport mode access
switchport access vlan 30
interface fa0/1
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
interface range fa0/11 - 20
switchport mode access
switchport access vlan 15
interface g1/1
switchport mode trunk
switchport trunk native vlan 45
interface range fa0/21 - 24 , g1/2
shutdown
ip domain-name cisco.com
crypto key gen rsa
1024

user CAdmin pass itsasecret
service password-encryption
ip ssh version 2
ip ssh auth 2
ip ssh time 60
line vty 0 15
login local
transport input ssh
```

# Packet Tracer – Examining a Redundant Design (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



## Objectives

**Part 1: Check for STP Convergence**

**Part 2: Examine the ARP Process**

**Part 3: Test Redundancy in a Switched Network**

## Background

In this activity, you will observe how STP operates, by default, and how it reacts when faults occur. Switches have been added to the network “out of the box”. Cisco switches can be connected to a network without any additional action required by the network administrator. For the purpose of this activity, the bridge priority was modified.

## Part 1: Check for STP Convergence

When STP is fully converged, the following conditions exist:

- All PCs have green link lights on the switched ports.
- Access layer switches have one forwarding uplink (green link) to a distribution layer switch and a blocking uplink (amber link) to a second distribution layer switch.
- Distribution layer switches have one forwarding uplink (green link) to a core layer switch and a blocking uplink (amber link) to another core layer switch.

## Part 2: Examine the ARP Process

### Step 1: Switch to Simulation mode.

### Step 2: Ping from PC1 to PC6.

- Use the **Add Simple PDU** tool to create a PDU from **PC1** to **PC6**. Verify that ARP and ICMP are selected in the **Event List Filters**. Click **Capture/Forward** to examine the ARP process as the switched network learns the MAC addresses of **PC1** and **PC6**. Notice that all possible loops are stopped by blocking ports. For example, the ARP request from **PC1** travels from **A1** to **D2** to **C1** to **D1** and then back to **A1**. However, because STP is blocking the link between **A1** and **D1**, no loop occurs.
- Notice that the ARP reply from **PC6** travels back along one path. Why? **It is the only valid path when STP is blocking the redundant links.**
- Record the loop-free path between **PC1** and **PC6**. **PC1 > A1 > D2 > C1 > D3 > A6 > PC6**

### Step 3: Examine the ARP process again.

- Below the **Scenario 0** drop-down list, click **New** to create **Scenario 1**. Examine the ARP process again by pinging between two different PCs.
- What part of the path changed from the last set of pings? **Answers may vary depending on which PC students ping from.**

## Part 3: Test Redundancy in a Switched Network

### Step 1: Delete the link between A1 and D2.

Switch to **Realtime** mode. Delete the link between **A1** and **D2**. It takes some time for STP to converge and establish a new, loop-free path. Because only **A1** is affected, watch for the amber light on the link between **A1** and **D1** to change to green. You can click **Fast Forward Time** to accelerate the STP convergence process.

### Step 2: Ping between PC1 and PC6.

- After the link between **A1** and **D1** is active (indicated by a green light), switch to **Simulation** mode and create **Scenario 2**. Ping between **PC1** and **PC6** again.
- Record the new loop-free path. **PC1 > A1 > D1 > C1 > D3 > A6 > PC6**

### Step 3: Delete link between C1 and D3.

- Switch to **Realtime** mode. Notice that the links between **D3** and **D4** to **C2** are amber. Delete the link between **C1** and **D3**. It takes some time for STP to converge and establish a new, loop-free path. Watch the amber links on **D3** and **D4**. You can click **Fast Forward Time** to accelerate the STP convergence process.
- Which link is now the active link to **C2**? **Link between D3 F0/1 to C2 F0/2**

### Step 4: Ping between PC1 and PC6.

- Switch to **Simulation** mode and create **Scenario 3**. Ping between **PC1** and **PC6**.
- Record the new loop-free path. **PC1 > A1 > D1 > C1 > D4 > A6 > PC6**



### Step 5: Delete D4.

Switch to **Realtime** mode. Notice that **A4**, **A5**, and **A6** are all forwarding traffic to **D4**. Delete **D4**. It takes some time for STP to converge and establish a new, loop-free path. Watch for the links between **A4**, **A5**, and **A6** to **D3** transition to forwarding (green). All three switches should now be forwarding to **D3**.

### Step 6: Ping between PC1 and PC6.

- Switch to **Simulation** mode and create **Scenario 4**. Ping between **PC1** and **PC6**.
- Record the new loop-free path. **PC1 > A1 > D1 > C1 > C2 > D3 > A6 > PC6**
- What is unique about the new path that you have not seen before? **D3** is now the designated switch for packet forwarding if **PC1** would like to ping **PC6**, no redundant path below **C2**.

### Step 7: Delete C1.

Switch to **Realtime** mode. Notice that **D1** and **D2** are both forwarding traffic to **C1**. Delete **C1**. It takes some time for STP to converge and establish a new, loop-free path. Watch for the links between **D1** and **D2** to **C2** to transition to forwarding (green). Once converged, both switches should now be forwarding to **C2**.

### Step 8: Ping between PC1 and PC6.

- Switch to **Simulation** mode and create **Scenario 5**. Ping between **PC1** and **PC6**.
- Record the new loop-free path. **PC1 > A1 > D1 > C2 > D3 > A6 > PC6**

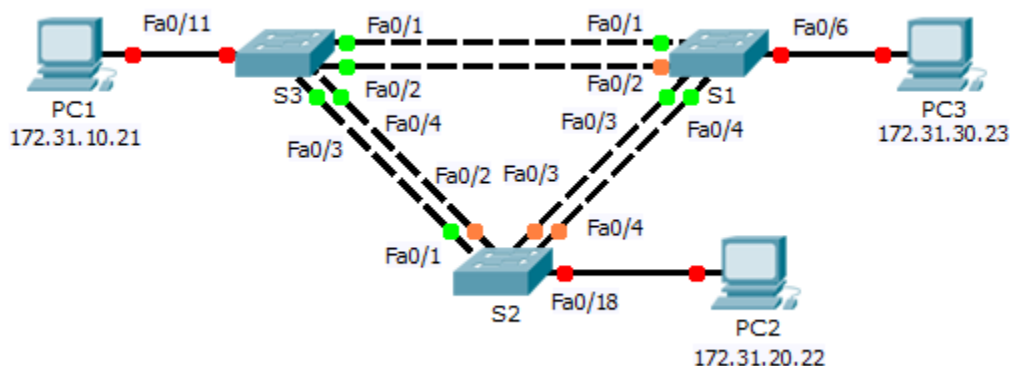
### Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 2: Examine the ARP Process	Step 2b	5	
	Step 2c	15	
	Step 3	5	
<b>Part 2 Total</b>		<b>25</b>	
Part 3: Test Redundancy in a Switched Network	Step 2	15	
	Step 3	5	
	Step 4	15	
	Step 6b	15	
	Step 6c	10	
	Step 8	15	
<b>Part 3 Total</b>		<b>75</b>	
<b>Total Score</b>		<b>100</b>	

## Packet Tracer – Configuring PVST+ (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

### Topology



### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.31.99.1	255.255.255.0	N/A
S2	VLAN 99	172.31.99.2	255.255.255.0	N/A
S3	VLAN 99	172.31.99.3	255.255.255.0	N/A
PC1	NIC	172.31.10.21	255.255.255.0	172.31.10.254
PC2	NIC	172.31.20.22	255.255.255.0	172.31.20.254
PC3	NIC	172.31.30.23	255.255.255.0	172.31.30.254

### Switch Port Assignment Specifications

Ports	Assignments	Network
S1 F0/6	VLAN 30	172.17.30.0/24
S2 F0/18	VLAN 20	172.17.20.0/24
S3 F0/11	VLAN 10	172.17.10.0/24

### Objectives

**Part 1: Configure VLANs**

**Part 2: Configure Spanning Tree PVST+ and Load Balancing**

**Part 3: Configure PortFast and BPDU Guard**

### Background

In this activity, you will configure VLANs and trunks, and examine and configure the Spanning Tree Protocol primary and secondary root bridges. You will also optimize the switched topology using PVST+, PortFast, and BPDU guard.

### Part 1: Configure VLANs

#### Step 1: Enable the user ports on S1, S2, and S3 in access mode.

Refer to the topology diagram to determine which switch ports (**S1**, **S2**, and **S3**) are activated for end-user device access. These three ports will be configured for access mode and enabled with the **no shutdown** command.

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# no shutdown
```

```
S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# no shutdown
```

```
S3(config)# interface f0/11
S3(config-if)# switchport mode access
S3(config-if)# no shutdown
```

#### Step 2: Create VLANs.

Using the appropriate command, create VLANs 10, 20, 30, 40, 50, 60, 70, 80, and 99 on all of the switches.

```
S1(config)# vlan 10
S1(config-vlan)# vlan 20
S1(config-vlan)# vlan 30
S1(config-vlan)# vlan 40
S1(config-vlan)# vlan 50
S1(config-vlan)# vlan 60
S1(config-vlan)# vlan 70
S1(config-vlan)# vlan 80
S1(config-vlan)# vlan 99
```

```
S2(config)# vlan 10
S2(config-vlan)# vlan 20
S2(config-vlan)# vlan 30
S2(config-vlan)# vlan 40
S2(config-vlan)# vlan 50
S2(config-vlan)# vlan 60
S2(config-vlan)# vlan 70
S2(config-vlan)# vlan 80
S2(config-vlan)# vlan 99
```

```
S3(config)# vlan 10
S3(config-vlan)# vlan 20
S3(config-vlan)# vlan 30
S3(config-vlan)# vlan 40
S3(config-vlan)# vlan 50
S3(config-vlan)# vlan 60
S3(config-vlan)# vlan 70
S3(config-vlan)# vlan 80
S3(config-vlan)# vlan 99
```

### Step 3: Assign VLANs to switch ports.

Port assignments are listed in the table at the beginning of the activity. Save your configurations after assigning switch ports to the VLANs.

```
S1(config)# interface f0/6
S1(config-if)# switchport access vlan 30

S2(config)# interface f0/18
S2(config-if)# switchport access vlan 20

S3(config)# interface f0/11
S3(config-if)# switchport access vlan 10
```

### Step 4: Verify the VLANs.

Use the **show vlan brief** command on all switches to verify that all VLANs are registered in the VLAN table.

### Step 5: Assign the trunks to native VLAN 99.

Use the appropriate command to configure ports F0/1 to F0/4 on each switch as trunk ports, and assign these trunk ports to native VLAN 99.

```
S1(config)# interface range f0/1-4
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport trunk native vlan 99

S2(config)# interface range f0/1-4
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk native vlan 99

S3(config)# interface range f0/1-4
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# switchport trunk native vlan 99
```

### Step 6: Configure the management interface on all three switches with an address.

```
S1(config)# interface vlan99
S1(config-if)# ip address 172.31.99.1 255.255.255.0

S2(config)# interface vlan99
```

```
S2(config-if)# ip address 172.31.99.2 255.255.255.0
```

```
S3(config)# interface vlan99
```

```
S3(config-if)# ip address 172.31.99.3 255.255.255.0
```

Verify that the switches are correctly configured by pinging between them.

## Part 2: Configure Spanning Tree PVST+ and Load Balancing

Because there is a separate instance of the spanning tree for every active VLAN, a separate root election is conducted for each instance. If the default switch priorities are used in root selection, the same root is elected for every spanning tree instance, as we have seen. This could lead to an inferior design. Some reasons to control the selection of the root switch include:

- The root switch is responsible for generating BPDUs for STP 802.1D and is the focal point for spanning tree to control traffic. The root switch must be capable of handling this additional load.
- The placement of the root defines the active switched paths in the network. Random placement is likely to lead to suboptimal paths. Ideally the root is in the distribution layer.
- Consider the topology used in this activity. Of the six trunks configured, only three are carrying traffic. While this prevents loops, it is a waste of resources. Because the root can be defined on the basis of the VLAN, you can have some ports blocking for one VLAN and forwarding for another. This is demonstrated below.

### Step 1: Configure STP mode.

Use the **spanning-tree mode** command to configure the switches so they use PVST as the STP mode.

```
S1(config)# spanning-tree mode pvst
```

```
S2(config)# spanning-tree mode pvst
```

```
S3(config)# spanning-tree mode pvst
```

### Step 2: Configure Spanning Tree PVST+ load balancing.

- a. Configure **S1** to be the primary root for VLANs 1, 10, 30, 50, and 70. Configure **S3** to be the primary root for VLANs 20, 40, 60, 80, and 99. Configure **S2** to be the secondary root for all VLANs.

```
S1(config)# spanning-tree vlan 1,10,30,50,70 root primary
```

```
S2(config)# spanning-tree vlan 1,10,20,30,40,50,60,70,80,99 root secondary
```

```
S3(config)# spanning-tree vlan 20,40,60,80,99 root primary
```

- b. Verify your configurations using the **show spanning-tree** command.

## Part 3: Configure PortFast and BPDU Guard

### Step 1: Configure PortFast on the switches.

PortFast causes a port to enter the forwarding state almost immediately by dramatically decreasing the time of the listening and learning states. PortFast minimizes the time it takes for the server or workstation to come online. Configure PortFast on the switch interfaces that are connected to PCs.

```
S1(config)# interface f0/6
S1(config-if-range)# spanning-tree portfast

S2(config)# interface f0/18
S2(config-if-range)# spanning-tree portfast

S3(config)# interface f0/11
S3(config-if-range)# spanning-tree portfast
```

### Step 2: Configure BPDU guard on the switches.

The STP PortFast BPDU guard enhancement allows network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports that have STP PortFast enabled are unable to influence the STP topology. At the reception of BPDUs, the BPDU guard operation disables the port that has PortFast configured. The BPDU guard transitions the port into the err-disable state, and a message appears on the console. Configure BPDU guard on switch interfaces that are connected to PCs.

```
S1(config)# interface f0/6
S1(config-if)# spanning-tree bpduguard enable

S2(config)# interface f0/18
S2(config-if)# spanning-tree bpduguard enable

S3(config)# interface f0/11
S3(config-if)# spanning-tree bpduguard enable
```

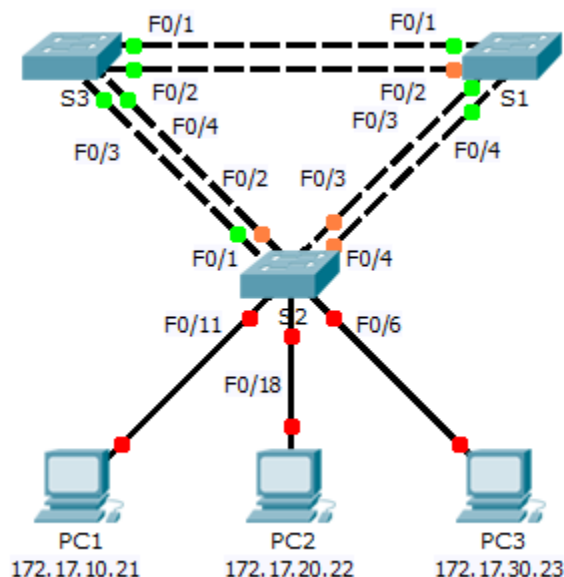
### Step 3: Verify your configuration.

Use the **show running-configuration** command to verify your configuration.

# Packet Tracer – Configuring Rapid PVST+ (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



## Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	N/A
S2	VLAN 99	172.17.99.12	255.255.255.0	N/A
S3	VLAN 99	172.17.99.13	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.254
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.254
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.254

## Switch Port Assignment Specifications

Ports	Assignments	Network
S2 F0/6	VLAN 30	172.17.30.0/24
S2 F0/18	VLAN 20	172.17.20.0/24
S2 F0/11	VLAN 10	172.17.10.0/24

## Objectives

### Part 1: Configure VLANs

### Part 2: Configure Rapid Spanning Tree PVST+ Load balancing

### Part 3: Configure PortFast and BPDU Guard

## Background

In this activity, you will configure VLANs and trunks, Rapid Spanning Tree PVST+, primary and secondary root bridges, and examine the configuration results. You will also optimize the network by configuring PortFast, and BPDU Guard on edge ports.

## Part 1: Configure VLANs

### Step 1: Enable the user ports on S2 in access mode.

Refer to the topology diagram to determine which switch ports on **S2** are activated for end-user device access. These three ports will be configured for access mode and enabled with the **no shutdown** command.

```
S2(config)# interface range f0/6,f0/11,f0/18
S2(config-if-range)# switchport mode access
S2(config-fi-range)# no shutdown
```

### Step 2: Create VLANs.

Using the appropriate command, create VLANs 10, 20, 30, 40, 50, 60, 70, 80, and 99 on all of the switches.

```
S1(config)# vlan 10
S1(config-vlan)# vlan 20
S1(config-vlan)# vlan 30
S1(config-vlan)# vlan 40
S1(config-vlan)# vlan 50
S1(config-vlan)# vlan 60
S1(config-vlan)# vlan 70
S1(config-vlan)# vlan 80
S1(config-vlan)# vlan 99
```

```
S2(config)# vlan 10
S2(config-vlan)# vlan 20
S2(config-vlan)# vlan 30
S2(config-vlan)# vlan 40
S2(config-vlan)# vlan 50
S2(config-vlan)# vlan 60
S2(config-vlan)# vlan 70
S2(config-vlan)# vlan 80
S2(config-vlan)# vlan 99
```

```
S3(config)# vlan 10
S3(config-vlan)# vlan 20
S3(config-vlan)# vlan 30
S3(config-vlan)# vlan 40
S3(config-vlan)# vlan 50
S3(config-vlan)# vlan 60
```



```
S3(config-vlan)# vlan 70
S3(config-vlan)# vlan 80
S3(config-vlan)# vlan 99
```

### Step 3: Assign VLANs to switch ports.

Port assignments are listed in the table at the beginning of the activity. Save your configurations after assigning switch ports to the VLANs.

```
S2(config)# interface f0/6
S2(config-if)# switchport access vlan 30
S2(config-if)# interface f0/11
S2(config-if)# switchport access vlan 10
S2(config-if)# interface f0/18
S2(config-if)# switchport access vlan 20
```

### Step 4: Verify the VLANs.

Use the **show vlan brief** command on all switches to verify that all VLANs are registered in the VLAN table.

### Step 5: Assign the trunks to native VLAN 99.

Use the appropriate command to configure ports F0/1 to F0/4 on each switch as trunk ports and assign these trunk ports to native VLAN 99.

```
S1(config)# interface range f0/1-4
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport trunk native vlan 99

S2(config)# interface range f0/1-4
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk native vlan 99

S3(config)# interface range f0/1-4
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# switchport trunk native vlan 99
```

### Step 6: Configure the management interface on all three switches with an address.

```
S1(config)# interface vlan99
S1(config-if)# ip address 172.17.99.11 255.255.255.0

S2(config)# interface vlan99
S2(config-if)# ip address 172.17.99.12 255.255.255.0

S3(config)# interface vlan99
S3(config-if)# ip address 172.17.99.13 255.255.255.0
```

Verify that the switches are correctly configured by pinging between them.

## Part 2: Configure Rapid Spanning Tree PVST+ Load Balancing

The Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) can be seen as an evolution of the 802.1D standard more so than a revolution. The 802.1D terminology remains primarily the same. Most parameters have been left unchanged so users familiar with 802.1D can rapidly configure the new protocol comfortably. In most cases, RSTP performs better than proprietary extensions of Cisco without any additional configuration. 802.1w can also revert back to 802.1D in order to interoperate with legacy bridges on a per-port basis.

### Step 1: Configure STP mode.

Use the **spanning-tree mode** command to configure the switches to use rapid PVST as the STP mode.

```
S1(config)# spanning-tree mode rapid-pvst
```

```
S2(config)# spanning-tree mode rapid-pvst
```

```
S3(config)# spanning-tree mode rapid-pvst
```

### Step 2: Configure Rapid Spanning Tree PVST+ load balancing.

Configure **S1** to be the primary root for VLANs 1, 10, 30, 50, and 70. Configure **S3** to be the primary root for VLANs 20, 40, 60, 80, and 99. Configure **S2** to be the secondary root for all of the VLANs.

```
S1(config)# spanning-tree vlan 1,10,30,50,70 root primary
```

```
S2(config)# spanning-tree vlan 1,10,20,30,40,50,60,70,80,99 root secondary
```

```
S3(config)# spanning-tree vlan 20,40,60,80,99 root primary
```

Verify your configurations by using the **show spanning-tree** command.

## Part 3: Configure PortFast and BPDU Guard

### Step 1: Configuring PortFast on S2.

PortFast causes a port to enter the forwarding state almost immediately by dramatically decreasing the time of the listening and learning states. PortFast minimizes the time it takes for the server or workstation to come online. Configure PortFast on **S2** interfaces that are connected to PCs.

```
S2(config)# interface range f0/6 , f0/11 , f0/18
```

```
S2(config-if-range)# spanning-tree portfast
```

### Step 2: Configuring BPDU Guard on S2.

The STP PortFast BPDU Guard enhancement allows network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports that have STP PortFast enabled are not able to influence the STP topology. At the reception of BPDUs, the BPDU Guard operation disables the port that has PortFast configured. The BPDU Guard transitions the port into err-disable state, and a message appears on the console. Configure BPDU Guard on **S2** interfaces that are connected to PCs.

```
S2(config)# interface range f0/6 , f0/11 , f0/18
```

```
S2(config-if-range)# spanning-tree bpduguard enable
```

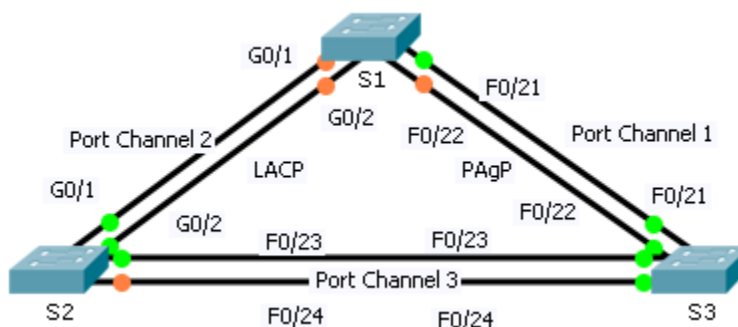
### Step 3: Verify your configuration.

Use the **show run** command to verify your configuration.

# Packet Tracer – Configuring EtherChannel (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



## Objectives

**Part 1: Configure Basic Switch Settings**

**Part 2: Configure an EtherChannel with Cisco PAgP**

**Part 3: Configure an 802.3ad LACP EtherChannel**

**Part 4: Configure a Redundant EtherChannel Link**

## Background

Three switches have just been installed. There are redundant uplinks between the switches. Usually, only one of these links could be used; otherwise, a bridging loop might occur. However, using only one link utilizes only half of the available bandwidth. EtherChannel allows up to eight redundant links to be bundled together into one logical link. In this lab, you will configure Port Aggregation Protocol (PAgP), a Cisco EtherChannel protocol, and Link Aggregation Control Protocol (LACP), an IEEE 802.3ad open standard version of EtherChannel.

## Part 1: Configure Basic Switch Settings

### Step 1: Configure basic switch parameters.

- Assign each switch a hostname according to the topology diagram.

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

```
Switch(config)# hostname S2
```

```
Switch(config)# hostname S3
```

- Configure all required ports as trunks, depending on the connections between devices.

**Note:** If the ports are configured with dynamic auto mode, and you do not set the mode of the ports to trunk, the links do not form trunks and remain access ports. The default mode on a 2960 switch is dynamic auto.

```
S1(config)# interface range g0/1 - 2
```

```
S1(config-if-range)# switchport mode trunk
```

```
S1(config-if-range)# interface range f0/21 - 22
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# end
```

```
S2(config)# interface range g0/1 - 2
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# interface range f0/23 - 24
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# end
```

```
S3(config)# interface range f0/21 - 24
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# end
```

## Part 2: Configure an EtherChannel with Cisco PAgP

**Note:** When configuring EtherChannels, it is recommended to shut down the physical ports being grouped on both devices before configuring them into channel groups. Otherwise, the EtherChannel Misconfig Guard may place these ports into err-disabled state. The ports and port channels can be re-enabled after EtherChannel is configured.

### Step 1: Configure Port Channel 1.

- The first EtherChannel created for this activity aggregates ports F0/22 and F0/21 between **S1** and **S3**. Use the **show interfaces trunk** command to ensure that you have an active trunk link for those two links.

```
S1# show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
F0/21	on	802.1q	trunking	1
F0/22	on	802.1q	trunking	1
G0/1	on	802.1q	trunking	1
G0/2	on	802.1q	trunking	1

<output omitted>

- On both switches, add ports F0/21 and F0/22 to Port Channel 1 with the **channel-group 1 mode desirable** command. The **mode desirable** option enables the switch to actively negotiate to form a PAgP link.

```
S1(config)# interface range f0/21 - 22
S1(config-if-range)# shutdown
S1(config-if-range)# channel-group 1 mode desirable
S1(config-if-range)# no shutdown
```

```
S3(config)# interface range f0/21 - 22
S3(config-if-range)# shutdown
S3(config-if-range)# channel-group 1 mode desirable
S3(config-if-range)# no shutdown
```

- c. Configure the logical interface to become a trunk by first entering the **interface port-channel number** command and then the **switchport mode trunk** command. Add this configuration to both switches.

**Instructor Note:** Packet Tracer 6.0.1 does not grade the **switchport mode trunk** command in port-channel interfaces.

```
S1(config)# interface port-channel 1
S1(config-if)# switchport mode trunk
```

**Instructor Note:** Packet Tracer 6.0.1 does not grade the **switchport mode trunk** command in port-channel interfaces.

```
S3(config)# interface port-channel 1
S3(config-if)# switchport mode trunk
```

### Step 2: Verify Port Channel 1 status.

- a. Issue the **show etherchannel summary** command to verify that EtherChannel is working on both switches. This command displays the type of EtherChannel, the ports utilized, and port states.

```
S1# show etherchannel summary
Flags:  D - down          P - 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
        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	F0/21 (P) F0/22 (P)

```
S3# show etherchannel summary
Flags:  D - down          P - 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
        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      F0/21 (P)      F0/22 (P)
```

- b. If the EtherChannel does not come up, shut down the physical interfaces on both ends of the EtherChannel and then bring them back up again. This involves using the **shutdown** command on those interfaces, followed by a **no shutdown** command a few seconds later.

The **show interfaces trunk** and **show spanning-tree** commands also show the port channel as one logical link.

```
S1# show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gig0/1	on	802.1q	trunking	1
Gig0/2	on	802.1q	trunking	1
Po1	on	802.1q	trunking	1

```
<output omitted>
```

```
S1# show spanning-tree
```

```
VLAN0001
```

```
Spanning tree enabled protocol ieee
  Root ID    Priority    32769
              Address    0001.436E.8494
              Cost        9
              Port        27 (Port-channel 1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Bridge ID    Priority    32769 (priority 32768 sys-id-ext 1)
              Address    000A.F313.2395
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	---	---	-----	-----	-----
Gi0/1	Desg	FWD	4	128.25	P2p
Gi0/2	Desg	FWD	4	128.26	P2p
Po1	Root	FWD	9	128.27	Shr

## Part 3: Configure an 802.3ad LACP EtherChannel

### Step 1: Configure Port Channel 2.

- a. In 2000, the IEEE released 802.3ad, which is an open standard version of EtherChannel. Using the previous commands, configure the link between **S1** and **S2** on ports G0/1 and G0/2 as an LACP EtherChannel. You must use a different port channel number on **S1** than 1, because you already used that in the previous step. To configure a port channel as LACP, use the interface configuration mode **channel-group number mode active** command. Active mode indicates that the switch actively tries to negotiate that link as LACP, as opposed to PAgP.

**Instructor Note:** Packet Tracer 6.0.1 does not grade the **switchport mode trunk** command in port-channel interfaces.

```
S1(config)# interface range g0/1 - 2
```

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

```
S1(config-if-range)# channel-group 2 mode active
S1(config-if-range)# no shutdown
S1(config-if-range)# interface port-channel 2
S1(config-if)# switchport mode trunk
```

```
S2(config)# interface range g0/1 - 2
S2(config-if-range)# shutdown
S2(config-if-range)# channel-group 2 mode active
S2(config-if-range)# no shutdown
S2(config-if-range)# interface port-channel 2
S2(config-if)# switchport mode trunk
```

### Step 2: Verify Port Channel 2 status.

- Use the **show** commands from Part 1 Step 2 to verify the status of Port Channel 2. Look for the protocol used by each port.

```
S1# show etherchannel summary
Flags:  D - down          P - 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
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
```

```
Number of channel-groups in use: 2
Number of aggregators:          2
```

Group	Port-channel	Protocol	Ports
1	Po1 (SU)	PAgP	Fa0/21 (P) Fa0/22 (P)
2	Po2 (SU)	LACP	Gig0/1 (P) Gig0/2 (P)

## Part 4: Configure a Redundant EtherChannel Link

### Step 1: Configure Port Channel 3.

There are various ways to enter the **channel-group number mode** command:

```
S2(config)# interface range f0/23 - 24
S2(config-if-range)# channel-group 3 mode ?
active      Enable LACP unconditionally
auto        Enable PAgP only if a PAgP device is detected
desirable   Enable PAgP unconditionally
on          Enable Etherchannel only
passive     Enable LACP only if a LACP device is detected
```

- a. On switch **S2**, add ports F0/23 and F0/24 to Port Channel 3 with the **channel-group 3 mode passive** command. The **passive** option indicates that you want the switch to use LACP only if another LACP device is detected. Statically configure Port Channel 3 as a trunk interface.

**Instructor Note:** Packet Tracer 6.0.1 does not grade the **switchport mode trunk** command in port-channel interfaces.

```
S2(config)# interface range f0/23 - 24
S2(config-if-range)# shutdown
S2(config-if-range)# channel-group 3 mode passive
S2(config-if-range)# no shutdown
S2(config-if-range)# interface port-channel 3
S2(config-if)# switchport mode trunk
```

- b. On switch **S3**, add ports F0/23 and F0/24 to Port Channel 3 with the **channel-group 3 mode active** command. The **active** option indicates that you want the switch to use LACP unconditionally. Statically configure Port Channel 3 as a trunk interface.

**Instructor Note:** Packet Tracer 6.0.1 does not grade the **switchport mode trunk** command in port-channel interfaces.

```
S3(config)# interface range f0/23 - 24
S3(config-if-range)# shutdown
S3(config-if-range)# channel-group 3 mode active
S3(config-if-range)# no shutdown
S3(config-if-range)# interface port-channel 3
S3(config-if)# switchport mode trunk
```

### Step 2: Verify Port Channel 3 status.

- a. Use the **show** commands from Part 1 Step 2 to verify the status of Port Channel 3. Look for the protocol used by each port.

```
S2# show etherchannel summary
<output omitted>
Number of channel-groups in use: 2
Number of aggregators:          2
Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
2      Po2 (SU)          LACP    Gig0/1 (P) Gig0/2 (P)
3      Po3 (SU)          LACP    Fa0/23 (P) Fa0/24 (P)
```

- b. Port Channel 2 is not operative because spanning tree protocol placed some ports into blocking mode. Unfortunately, those ports were Gigabit ports. To restore these ports, configure **S1** to be **primary** root for VLAN 1 or set the priority to **24576**.

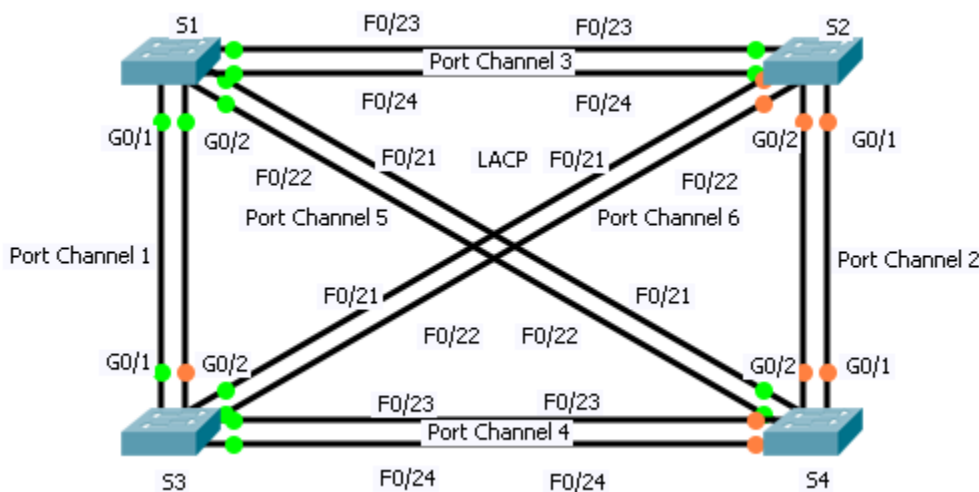
```
S1(config)# spanning-tree vlan 1 root primary
or
S1(config)# spanning-tree vlan 1 priority 24576
```



# Packet Tracer – Troubleshooting EtherChannel (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



## Objectives

**Part 1: Examine the Physical Layer and Correct Switch Port Mode Issues**

**Part 2: Identify and Correct Port Channel Assignment Issues**

**Part 3: Identify and Correct Port Channel Protocol Issues**

## Background

Four switches were recently configured by a junior technician. Users are complaining that the network is running slow and would like you to investigate.

## Part 1: Examine the Physical Layer and Correct Switch Port Mode Issues

### Step 1: Look for access ports.

Examine the switches. When physical ports are assigned to an EtherChannel port, they behave as one. Each pair will either be operational or down. They will not be mixed with one port green and the other port orange.

### Step 2: Set ports to trunking mode.

- Verify that all physical ports in the topology are set to trunking. Correct any that are in access mode.

```
S2(config)# interface range f0/21 - 24
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# interface range g0/1-2
S2(config-if-range)# switchport mode trunk
```

- Correct any EtherChannel ports that are not set to trunking mode.

**Instructor Note:** Packet Tracer 6.0.1 does not grade the **switchport mode trunk** command in port-channel interfaces.

```
S1(config)# interface port-channel 1
S1(config-if)# switchport mode trunk

S2(config)# interface port-channel 2
S2(config-if)# switchport mode trunk
S2(config-if)# interface port-channel 3
S2(config-if)# switchport mode trunk
S2(config-if)# interface Port-channel 6
S2(config-if)# switchport mode trunk
```

## Part 2: Identify and Correct Port Channel Assignment Issues

### Step 1: Examine port channel assignments.

The topology illustrates physical ports and their EtherChannel assignments. Verify that the switches are configured as indicated.

```
S1# show etherchannel summary
```

```
<output omitted>
```

1	Po1 (SD)	LACP	Gig0/1 (I)	Gig0/2 (I)
3	Po3 (SU)	LACP	Fa0/23 (P)	Fa0/24 (P)
5	Po5 (SU)	LACP	Fa0/21 (P)	Fa0/22 (P)

```
S2# show etherchannel summary
```

```
<output omitted>
```

2	Po2 (SU)	LACP	Gig0/1 (P)	Gig0/2 (P)
3	Po3 (SU)	LACP	Fa0/23 (P)	Fa0/24 (P)
6	Po6 (SD)	LACP	Fa0/21 (I)	Fa0/22 (I)

```
S3# show etherchannel summary
```

```
<output omitted>
```

1	Po1 (SD)	PAgP	Gig0/1 (I)	Gig0/2 (I)
4	Po4 (SD)	PAgP	Fa0/23 (I)	Fa0/24 (I)
6	Po6 (SD)	PAgP	Fa0/21 (I)	Fa0/22 (I)

```
S4# show etherchannel summary
```

```
<output omitted>
```

2	Po2 (SU)	LACP	Gig0/1 (P)	Gig0/2 (P)		
4	Po4 (SU)	LACP	Fa0/21 (P)	Fa0/22 (P)	Fa0/23 (I)	Fa0/24 (I)
5	Po5 (SD)	-				

### Step 2: Correct port channel assignments.

Correct any switch ports that are not assigned to the correct EtherChannel port.

```
S4(config)# interface range f0/21 - 22
S4(config-if-range)# channel-group 5 mode active
```

## Part 3: Identify and Correct Port Channel Protocol Issues

### Step 1: Identify protocol issues.

In 2000, the IEEE released 802.3ad (LACP), which is an open standard version of EtherChannel. For compatibility reasons, the network design team chose to use LACP across the network. All ports that participate in EtherChannel need to actively negotiate the link as LACP, as opposed to PAgP. Verify that the physical ports are configured as indicated.

```
S3# show etherchannel summary
<output omitted>
1      Po1 (SD)          PAgP    Gig0/1 (I) Gig0/2 (I)
4      Po4 (SD)          PAgP    Fa0/23 (I) Fa0/24 (I)
6      Po6 (SD)          PAgP    Fa0/21 (I) Fa0/22 (I)
```

### Step 2: Correct Protocol issues.

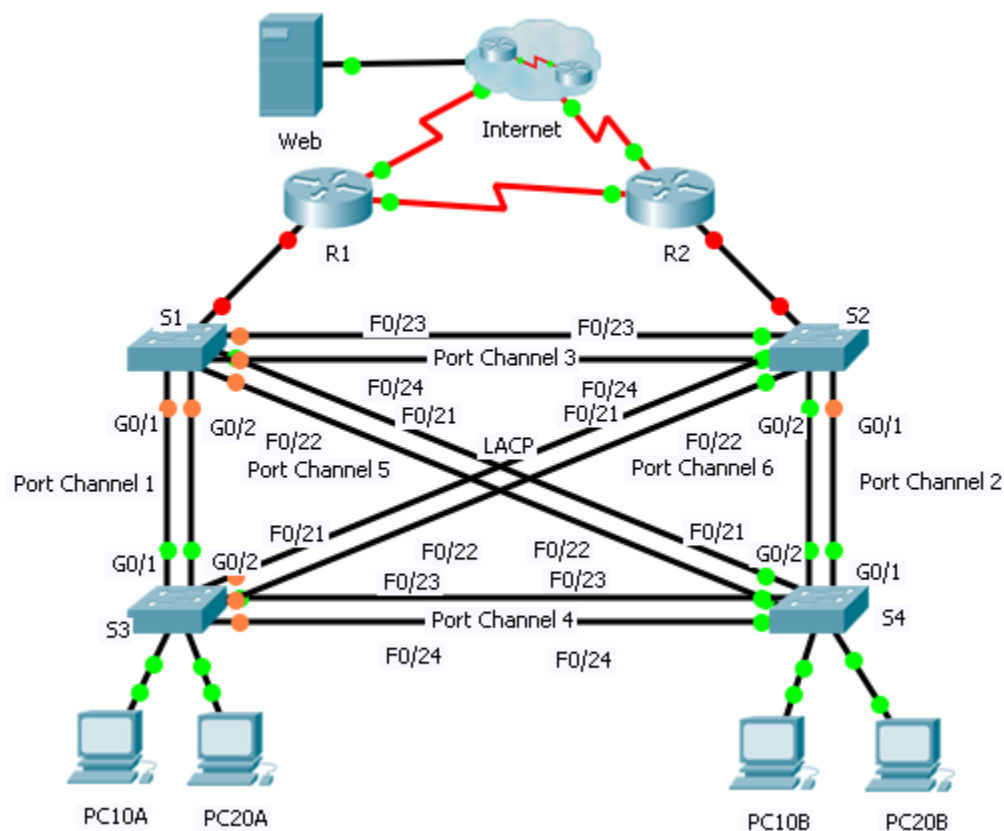
Correct any switch ports that are not negotiating using LACP.

```
S3(config)# interface range g0/1 - 2
S3(config-if-range)# no channel-group
S3(config-if-range)# channel-group 1 mode active
S3(config-if-range)# interface range f0/21 - 22
S3(config-if-range)# no channel-group
S3(config-if-range)# channel-group 6 mode active
S3(config-if-range)# interface range f0/23 - 24
S3(config-if-range)# no channel-group
S3(config-if-range)# channel-group 4 mode active
```

## Packet Tracer – Skills Integration Challenge (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

### Topology



## Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	VLAN Association
R1	G0/0.1	192.168.99.1	255.255.255.0	N/A	VLAN 99
	G0/0.10	192.168.10.1	255.255.255.0	N/A	VLAN 10
	G0/0.20	192.168.20.1	255.255.255.0	N/A	VLAN 20
	S0/0/0	209.165.22.222	255.255.255.224	N/A	N/A
	S0/0/1	192.168.1.1	255.255.255.0	N/A	N/A
R2	G0/0.1	192.168.99.2	255.255.255.0	N/A	VLAN 99
	G0/0.10	192.168.10.2	255.255.255.0	N/A	VLAN 10
	G0/0.20	192.168.20.2	255.255.255.0	N/A	VLAN 20
	S0/0/0	192.168.1.2	255.255.255.0	N/A	N/A
	S0/0/1	209.165.22.190	255.255.255.224	N/A	N/A
ISP	S0/0/0	209.165.22.193	255.255.255.224	N/A	N/A
	S0/0/1	209.165.22.161	255.255.255.224	N/A	N/A
Web	NIC	64.104.13.130	255.255.255.252	64.104.13.129	N/A
PC10A	NIC	192.168.10.101	255.255.255.0	192.168.10.1	VLAN 10
PC10B	NIC	192.168.10.102	255.255.255.0	192.168.10.1	VLAN 10
PC20A	NIC	192.168.20.101	255.255.255.0	192.168.20.1	VLAN 20
PC20B	NIC	192.168.20.102	255.255.255.0	192.168.20.1	VLAN 20

## Scenario

In this activity, two routers are configured to communicate with each other. You are responsible for configuring subinterfaces to communicate with the switches. You will configure VLANs, trunking, and EtherChannel with PVST. The Internet devices are all preconfigured.

## Requirements

You are responsible for configuring routers **R1** and **R2** and switches **S1**, **S2**, **S3**, and **S4**.

**Note:** Packet Tracer does not allow assigning point values less than 1. Since this activity is checking 154 items, not all configurations are assigned a point value. Click **Check Results > Assessment Items** to verify you correctly configured all 154 items.

### Inter-VLAN Routing

On **R1** and **R2**, enable and configure the subinterfaces with the following requirement:

- Configure the appropriate dot1Q encapsulation.
- Configure VLAN 99 as the native VLAN.
- Configure the IP address for the subinterface according to the Addressing Table.

### Routing

Configure OSPFv2 using the following requirements:

- User process ID 1.
- Advertise the network for each subinterface.
- Disable OSPF updates for each subinterface.

### VLANs

- For all switches, create VLAN 10, 20, and 99.
- Configure the following static ports for **S1** and **S2**:
  - F0/1 – 9 as access ports in VLAN 10.
  - F0/10 – 19 as access ports in VLAN 20.
  - F0/20 – F24 and G0/1 – 0/2 as the native trunk for VLAN 99.
- Configure the following static ports for **S3** and **S4**:
  - F0/1 – 9 as access ports in VLAN 10.
  - F0/10 – 20 as access ports in VLAN 20.
  - F0/21 – F24 and G0/1 – 0/2 as the native trunk for VLAN 99.

### EtherChannels

- All EtherChannels are configured as LACP.
- All EtherChannels are statically configured as the native trunk for VLAN 99.
- Use the following table to configure the appropriate switch ports to form EtherChannels:

Port Channel	Device: Ports	Device: Ports
1	S1: G0/1 – 2	S3: G0/1 – 2
2	S2: G0/1 – 2	S4: G0/1 – 2
3	S1: F0/23 – 24	S2: F0/23 – 24
4	S3: F0/23 – 24	S4: F0/23 – 24
5	S1: F0/21 – 22	S4: F0/21 – 22
6	S2: F0/21 – 22	S3: F0/21 - 22

### Spanning Tree

- Configure per-VLAN rapid spanning tree mode for all switches.
- Configure spanning tree priorities according to the table below:

Device	VLAN 10 Priority	VLAN 20 Priority
S1	4096	8192
S2	8192	4096
S3	32768	32768
S4	32768	32768

**Instructor Note:** Packet Tracer 6.0.1 does not grade the **switchport mode trunk** command or the **switchport trunk native vlan** command in port-channel interfaces.

### Connectivity

- All PCs should be able to ping the **Web** and other PCs.

### Scripts

#### Router R1

```
!R1
enable
configure t
interface GigabitEthernet0/0
  no shut
!
interface GigabitEthernet0/0.1
  encapsulation dot1Q 99 native
  ip address 192.168.99.1 255.255.255.0
!
interface GigabitEthernet0/0.10
  encapsulation dot1Q 10
  ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/0.20
  encapsulation dot1Q 20
  ip address 192.168.20.1 255.255.255.0
!
router ospf 1
  passive-interface GigabitEthernet0/0.1
  passive-interface GigabitEthernet0/0.10
  passive-interface GigabitEthernet0/0.20
  network 192.168.99.0 0.0.0.255 area 0
  network 192.168.10.0 0.0.0.255 area 0
  network 192.168.20.0 0.0.0.255 area 0
end
copy run start
```

#### Router R2

```
!R2
enable
configure t
!
interface GigabitEthernet0/0
  no shut
!
interface GigabitEthernet0/0.1
  encapsulation dot1Q 99 native
  ip address 192.168.99.2 255.255.255.0
!
interface GigabitEthernet0/0.10
  encapsulation dot1Q 10
  ip address 192.168.10.2 255.255.255.0
```

```
!  
interface GigabitEthernet0/0.20  
  encapsulation dot1Q 20  
  ip address 192.168.20.2 255.255.255.0  
!  
router ospf 1  
  passive-interface GigabitEthernet0/0.1  
  passive-interface GigabitEthernet0/0.10  
  passive-interface GigabitEthernet0/0.20  
  network 192.168.99.0 0.0.0.255 area 0  
  network 192.168.10.0 0.0.0.255 area 0  
  network 192.168.20.0 0.0.0.255 area 0  
end  
copy run start
```

### Switch S1

```
!S1  
enable  
configure t  
vlan 10  
vlan 20  
vlan 99  
interface range f0/1 - 9  
  switchport mode access  
  switchport access vlan 10  
inte range f0/10 - 19  
  switchport mode access  
  switchport access vlan 20  
interface range f0/20 - 24, g0/1-2  
  switchport mode trunk  
  switchport trunk native vlan 99  
!  
interface range g0/1 - 2  
  channel-group 1 mode active  
interface range f0/21 - 22  
  channel-group 5 mode active  
interface range f0/23 - 24  
  channel-group 3 mode active  
!  
interface po 1  
  switchport mode trunk  
  switchport trunk native vlan 99  
interface po 3  
  switchport mode trunk  
  switchport trunk native vlan 99  
interface po 5  
  switchport mode trunk  
  switchport trunk native vlan 99  
!
```



```
spanning-tree mode rapid-pvst
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 8192
end
copy run start
```

### Switch S2

```
!S2
enable
configure t
vlan 10
vlan 20
vlan 99
interface range f0/1 - 9
    switchport mode access
    switchport access vlan 10
inte range f0/10 - 19
    switchport mode access
    switchport access vlan 20
inte range f0/20 - 24, g0/1-2
    switchport mode trunk
    switchport trunk native vlan 99
!
interface range g0/1 - 2
    channel-group 2 mode active
interface range f0/21 - 22
    channel-group 6 mode active
interface range f0/23 - 24
    channel-group 3 mode active
!
interface po 2
    switchport mode trunk
    switchport trunk native vlan 99
interface po 3
    switchport mode trunk
    switchport trunk native vlan 99
interface po 6
    switchport mode trunk
    switchport trunk native vlan 99
!
spanning-tree mode rapid-pvst
spanning-tree vlan 10 priority 8192
spanning-tree vlan 20 priority 4096
end
copy run start
```

### Switch S3

```
!S3
```

```
enable
configure t
vlan 10
vlan 20
vlan 99
interface range f0/1 - 9
    switchport mode access
    switchport access vlan 10
inte range f0/10 - 20
    switchport mode access
    switchport access vlan 20
inte range f0/21 - 24, g0/1-2
    switchport mode trunk
    switchport trunk native vlan 99
!
interface range g0/1 - 2
    channel-group 1 mode active
interface range f0/21 - 22
    channel-group 6 mode active
interface range f0/23 - 24
    channel-group 4 mode active
!
interface po 1
    switchport mode trunk
    switchport trunk native vlan 99
interface po 4
    switchport mode trunk
    switchport trunk native vlan 99
interface po 6
    switchport mode trunk
    switchport trunk native vlan 99
!
spanning-tree mode rapid-pvst
spanning-tree vlan 10 priority 32768
spanning-tree vlan 20 priority 32768
end
copy run start
```

### Switch S4

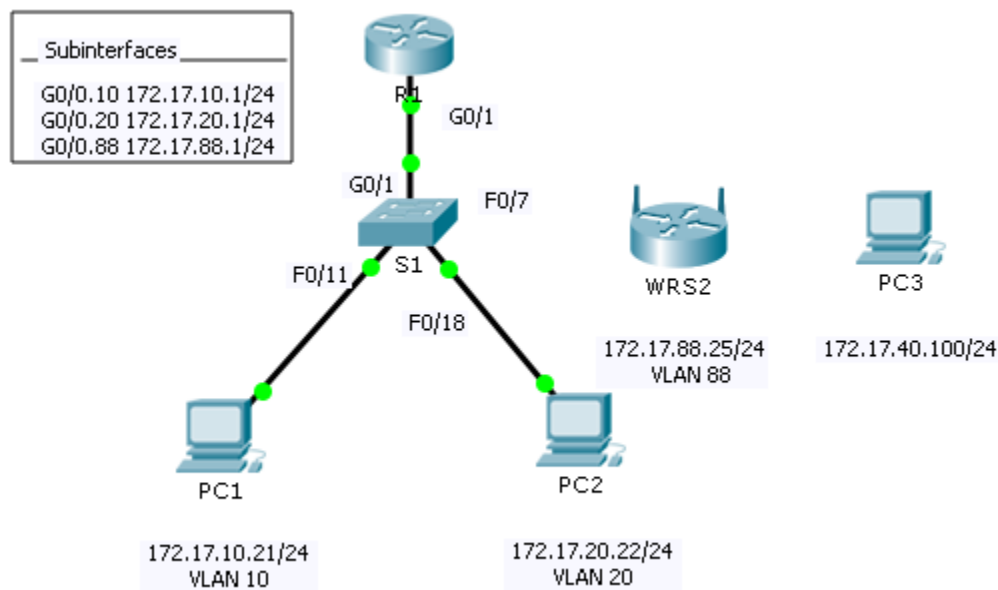
```
!S4
enable
configure t
vlan 10
vlan 20
vlan 99
interface range f0/1 - 9
    switchport mode access
    switchport access vlan 10
inte range f0/10 - 20
```

```
switchport mode access
switchport access vlan 20
inte range f0/21 - 24, g0/1-2
switchport mode trunk
switchport trunk native vlan 99
!
interface range g0/1 - 2
channel-group 2 mode active
interface range f0/21 - 22
channel-group 5 mode active
interface range f0/23 - 24
channel-group 4 mode active
interface po 2
switchport mode trunk
switchport trunk native vlan 99
interface po 4
switchport mode trunk
switchport trunk native vlan 99
interface po 5
switchport mode trunk
switchport trunk native vlan 99
!
spanning-tree mode rapid-pvst
spanning-tree vlan 10 priority 32768
spanning-tree vlan 20 priority 32768
end
copy run start
```

# Packet Tracer – Configuring Wireless LAN Access (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



## Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0.10	172.17.10.1	255.255.255.0	N/A
	G0/0.20	172.17.20.1	255.255.255.0	N/A
	G0/0.88	172.17.88.1	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned
WRS2	NIC	172.17.88.25	255.255.255.0	172.17.88.1

## Objectives

**Part 1: Configure a Wireless Router**

**Part 2: Configure a Wireless Client**

**Part 3: Verify Connectivity**

### Scenario

In this activity, you will configure a Linksys wireless router, allowing for remote access from PCs as well as wireless connectivity with WPA2 security. You will manually configure PC wireless connectivity by entering the Linksys router SSID and password.

## Part 1: Configure a Wireless Router

### Step 1: Connect the Internet interface of WRS2 to S1.

Connect the **WRS2** Internet interface to the **S1** F0/7 interface.

### Step 2: Configure the Internet connection type.

- Click **WRS2 > GUI** tab.
- Set the **Internet Connection type** to **Static IP**.
- Configure the IP addressing according to the Addressing Table.

### Step 3: Configure the network setup.

- Scroll down to **Network Setup**. For the **Router IP** option, set the IP address to **172.17.40.1** and the subnet mask to **255.255.255.0**.
- Enable the DHCP server.
- Scroll to the bottom of the page and click **Save Settings**.

### Step 4: Configure wireless access and security.

- At the top of the window, click **Wireless**. Set the **Network Mode** to **Wireless-N Only** and change the SSID to **WRS\_LAN**.
- Disable **SSID Broadcast** and click **Save Settings**.
- Click the **Wireless Security** option.
- Change the **Security Mode** from **Disabled** to **WPA2 Personal**.
- Configure **cisco123** as the passphrase.
- Scroll to the bottom of the page and click **Save Settings**.

## Part 2: Configure a Wireless Client

### Step 1: Configure PC3 for wireless connectivity.

Because SSID broadcast is disabled, you must manually configure **PC3** with the correct SSID and passphrase to establish a connection with the router.

- Click **PC3 > Desktop > PC Wireless**.
- Click the **Profiles** tab.
- Click **New**.
- Name the new profile **Wireless Access**.
- On the next screen, click **Advanced Setup**. Then manually enter the SSID of **WRS\_LAN** on **Wireless Network Name**. Click **Next**.
- Choose **Obtain network settings automatically (DHCP)** as the network settings, and then click **Next**.

- g. On **Wireless Security**, choose **WPA2-Personal** as the method of encryption and click **Next**.
- h. Enter the passphrase **cisco123** and click **Next**.
- i. Click **Save** and then click **Connect to Network**.

### Step 2: Verify PC3 wireless connectivity and IP addressing configuration.

The **Signal Strength** and **Link Quality** indicators should show that you have a strong signal.

Click **More Information** to see details of the connection including IP addressing information.

Close the **PC Wireless** configuration window.

### Part 3: Verify Connectivity

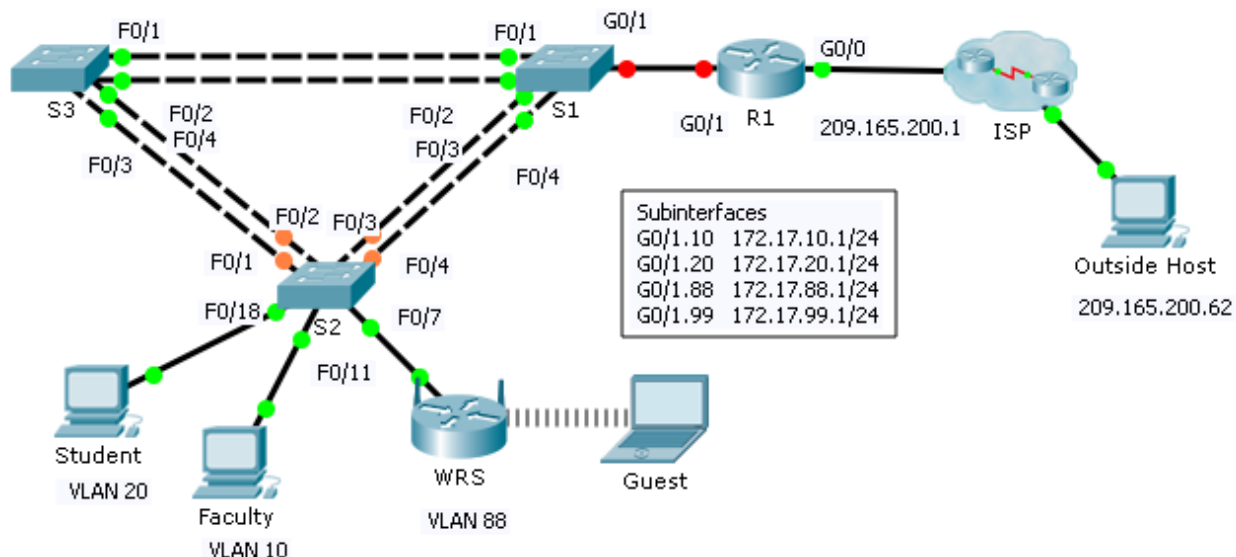
All the PCs should have connectivity with one another.

**Instructor Note:** There are no IOS configurations for this activity. Use the password **PT\_ccna5** to access Activity Wizard and view the answer network.

## Packet Tracer – Skills Integration Challenge (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

### Topology



### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	209.165.200.1	255.255.255.224	N/A
	G0/1.10	172.17.10.1	255.255.255.0	N/A
	G0/1.20	172.17.20.1	255.255.255.0	N/A
	G0/1.88	172.17.88.1	255.255.255.0	N/A
	G0/1.99	172.17.99.1	255.255.255.0	N/A
S2	VLAN 99	172.17.99.32	255.255.255.0	172.17.99.1
WRS	Internet	DHCP Assigned	DHCP Assigned	DHCP Assigned
	LAN	172.17.40.1	255.255.255.0	N/A

### Scenario

In this challenge activity, you will configure VLANs and inter-VLAN routing, DHCP, and Rapid PVST+. You will also be required to configure a Linksys router for wireless connectivity with wireless security. At the end of the activity, the PCs will not be able to ping each other but should be able to ping the outside host.

### Requirements

#### R1 Configurations

- Enable and configure the subinterfaces with the following requirements:
  - Configure IP addressing for the subinterfaces according to the Addressing Table.

- Configure the appropriate dot1Q encapsulation.
- Configure VLAN 99 as the native VLAN.
- Configure DHCP pools for VLAN 10, 20 and 88 with the following requirements:
  - Name the DHCP pools **VLAN10**, **VLAN20**, and **VLAN88**.
  - Set the default-router within each pool as the subinterface address.
  - Exclude the first 20 addresses for VLAN 10.
  - Exclude the first 20 addresses for VLAN 20.
  - Exclude the first 10 addresses for VLAN 88.

### Switch Configurations

- Configure Rapid PVST+ on all switches.
- Configure the IP addressing according to the Addressing Table on **S2**.
- Configure the default gateway on **S2**.
- Most of the VLANs are already configured. Create a new VLAN 999 on **S2** and name it **Blackhole**.
- Configure the following static ports for **S2**:
  - F0/1 – 4 as trunk ports as the native trunk for VLAN 99.
  - F0/7 as access ports in VLAN 88.
  - F0/18 as access port in VLAN 20.
  - F0/11 as access port in VLAN 10.
  - Shut down all unused ports and assign them as access ports in VLAN 999.

### WRS Configurations

- Set **Internet Setup** to receive IP addressing from R1. You may need to go to the **Status** tab to release and renew the IP addressing. Ensure that **WRS** receives full IP addressing.
- Configure **Network Setup** according to the Addressing Table so that the guest devices receive IP addressing.
- Configure wireless settings.
  - Set the network mode to **Wireless N-only**.
  - Rename the SSID **WRS\_Guest** and disable SSID broadcast.
- Configure wireless security. Set the authentication type to **WPA2 Personal** and configure **guestuser** as the passphrase.

### PC Configurations

- Verify that **Student** and **Faculty** PCs received full addressing from **R1**.
- Configure **Guest** to access the wireless LAN.
- Verify **Guest** received full addressing.
- Verify connectivity.

### Scripts

```
!!!!!!R1
enable
config t
interface g0/1
```



```
no shutdown
interface g0/1.10
  encapsulation dot 10
  ip address 172.17.10.1 255.255.255.0
interface g0/1.20
  encapsulation dot 20
  ip address 172.17.20.1 255.255.255.0
interface g0/1.88
  encapsulation dot 88
  ip address 172.17.88.1 255.255.255.0
interface g0/1.99
  encapsulation dot 99 native
  ip address 172.17.99.1 255.255.255.0
ip dhcp excluded 172.17.10.1 172.17.10.20
ip dhcp pool VLAN10
  network 172.17.10.0 255.255.255.0
  default-router 172.17.10.1
ip dhcp excluded 172.17.20.1 172.17.20.20
ip dhcp pool VLAN20
  network 172.17.20.0 255.255.255.0
  default-router 172.17.20.1
ip dhcp excluded 172.17.88.1 172.17.88.10
ip dhcp pool VLAN88
  network 172.17.88.0 255.255.255.0
  default-router 172.17.88.1
end
copy run start
```

```
!!!!!!S2
enable
configure t
interface vlan 99
  ip address 172.17.99.32 255.255.255.0
ip default-gateway 172.17.99.1
spanning-tree mode rapid-pvst
vlan 999
  name Blackhole
interface range f0/1-4
  switchport mode trunk
  switchport trunk native vlan 99
interface range f0/5-24,g0/1-2
  switchport mode access
  switchport access vlan 999
shutdown
interface f0/7
  no shutdown
  switchport access vlan 88
interface f0/18
  no shutdown
```

## Packet Tracer – Skills Integration Challenge

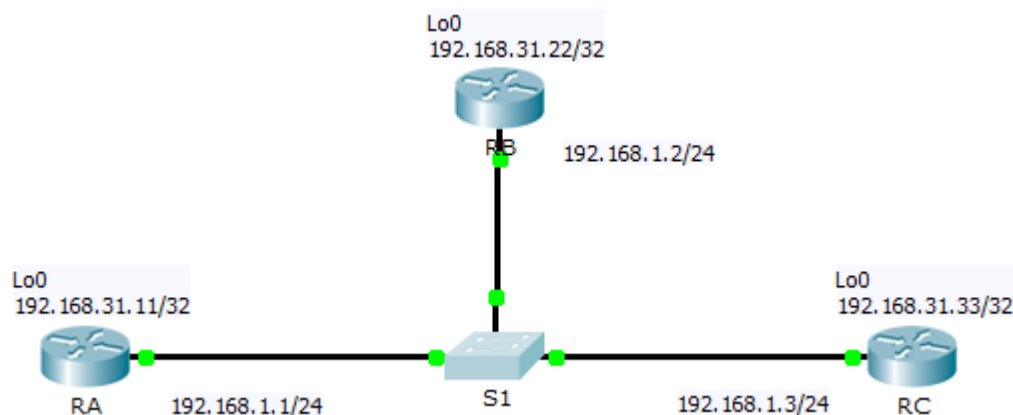
---

```
switchport access vlan 20
interface f0/11
  no shutdown
  switchport access vlan 10
end
copy run start
```

## Packet Tracer - Determining the DR and BDR (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

### Topology



### Addressing Table

Device	Interface	IP Address	Subnet Mask
RA	G0/0	192.168.1.1	255.255.255.0
	Lo0	192.168.31.11	255.255.255.255
RB	G0/0	192.168.1.2	255.255.255.0
	Lo0	192.168.31.22	255.255.255.255
RC	G0/0	192.168.1.3	255.255.255.0
	Lo0	192.168.31.33	255.255.255.255

### Objectives

**Part 1: Examine DR and BDR Changing Roles**

**Part 2: Modify OSPF Priority and Force Elections**

### Scenario

In this activity, you will examine DR and BDR roles and watch the roles change when there is a change in the network. You will then modify the priority to control the roles and force a new election. Finally, you will verify routers are filling the desired roles.

## Part 1: Examine DR and BDR Changing Roles

### Step 1: Wait until the amber link lights turn green.

When you first open the file in Packet Tracer, you may notice that the link lights for the switch are amber. These link lights will stay amber for 50 seconds while the switch makes sure that one of the routers is not another switch. Alternatively, you can click **Fast Forward Time** to bypass this process.

### Step 2: Verify the current OSPF neighbor states.

- Use the appropriate command on each router to examine the current DR and BDR.
- Which router is the DR? **RC**
- Which router is the BDR? **RB**

### Step 3: Turn on IP OSPF adjacency debugging.

- You can monitor the DR and BDR election process with a **debug** command. On **RA** and **RB**, enter the following command.

```
RA# debug ip ospf adj
```

```
RB# debug ip ospf adj
```

### Step 4: Disable the Gigabit Ethernet 0/0 interface on RC.

- Disable the link between **RC** and the switch to cause roles to change.
- Wait about 30 seconds for the dead timers to expire on **RA** and **RB**. According to the debug output, which router was elected DR and which router was elected BDR? **RB is now DR and RA is now BDR.**

### Step 5: Restore the Gigabit Ethernet 0/0 interface on RC.

- Re-enable the link between **RC** and the switch.
- Wait for the new DR/BDR elections to occur. Did DR and BDR roles change? Why or why not? **No, roles did not change because the current DR and BDR are still active. A router that comes online with a higher router ID will not assume the DR role until the DR fails.**

### Step 6: Disable the Gigabit Ethernet 0/0 interface on RB.

- Disable the link between **RB** and the switch to cause roles to change.
- Wait about 30 seconds for the holddown timers to expire on **RA** and **RC**. According to the debug output on **RA**, which router was elected DR and which router was elected BDR? **RA is now DR and RC is now BDR.**

### Step 7: Restore the Gigabit Ethernet 0/0 interface on RB.

- Re-enable the link between **RB** and the switch.
- Wait for the new DR/BDR elections to occur. Did DR and BDR roles change? Why or why not? **No, roles did not change because the current DR and BDR are still active. A router that comes online with a higher router ID will not assume the DR role until the DR fails.**

### Step 8: Turn off Debugging.

Enter the command **undebug all** on **RA** and **RB** to disable debugging.

## Part 2: Modify OSPF Priority and Force Elections

### Step 1: Configure OSPF priorities on each router.

To change the DR and BDR, configure the Gigabit Ethernet 0/0 port of each router with the following OSPF interface priorities:

- RA: 200**
- RB: 100**

- **RC:** 1 (This is the default priority)

### Step 2: Force an election by reloading the switch.

**Note:** The command **clear ip ospf process** can also be used on the routers to reset the OSPF process.

### Step 3: Verify DR and BDR elections were successful.

- Wait long enough for OSPF to converge and for the DR/BDR election to occur. This should take a few minutes. You can click **Fast Forward Time** to speed up the process.
- According to output from an appropriate command, which router is now DR and which router is now BDR? **RA is now DR and RB is now BDR.**

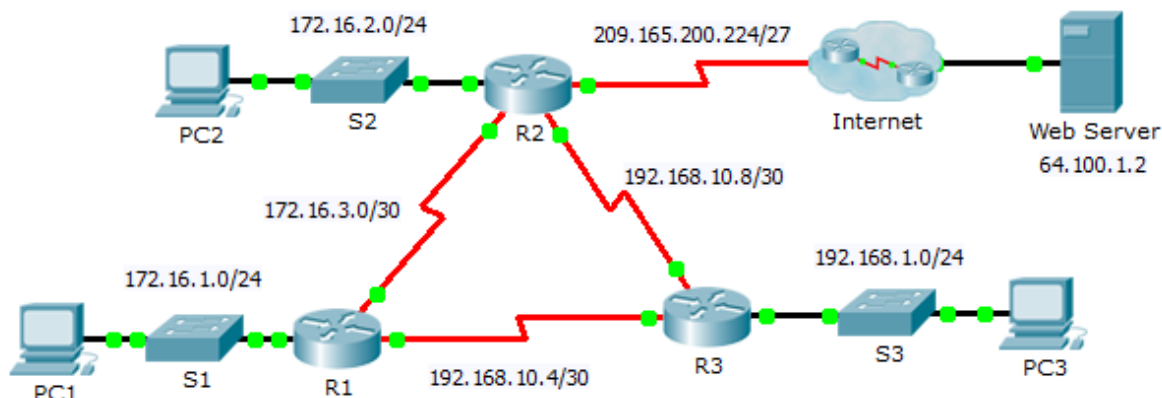
### Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Examine DR and BDR Changing Roles	Step 2b	10	
	Step 2c	10	
	Step 4b	10	
	Step 5b	10	
	Step 6b	10	
	Step 7b	10	
<b>Part 1 Total</b>		<b>60</b>	
Part 2: Modify OSPF Priority and Force Elections	Step 3b	10	
<b>Part 2 Total</b>		<b>10</b>	
<b>Packet Tracer Score</b>		<b>30</b>	
<b>Total Score</b>		<b>100</b>	

# Packet Tracer - Propagating a Default Route in OSPFv2 (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



## Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.3.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	G0/0	172.16.2.1	255.255.255.0	N/A
	S0/0/0	172.16.3.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
	S0/1/0	209.165.200.225	255.255.255.224	N/A
R3	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	NIC	172.16.1.2	255.255.255.0	172.16.1.1
PC2	NIC	172.16.2.2	255.255.255.0	172.16.2.1
PC3	NIC	192.168.1.2	255.255.255.0	192.168.1.1

## Objectives

**Part 1: Propagate a Default Route**

**Part 2: Verify Connectivity**

### Background

In this activity, you will configure an IPv4 default route to the Internet and propagate that default route to other OSPF routers. You will then verify the default route is in downstream routing tables and that hosts can now access a web server on the Internet.

### Part 1: Propagate a Default Route

#### Step 1: Configure a default route on R2.

Configure R2 with a directly attached default route to the Internet.

```
R2(config)# ip route 0.0.0.0 0.0.0.0 Serial0/1/0
```

#### Step 2: Propagate the route in OSPF.

Configure OSPF to propagate the default route in OSPF routing updates.

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

#### Step 3: Examine the routing tables on R1 and R3.

Examine the routing tables of R1 and R3 to verify that the route has been propagated.

```
R1> show ip route
<output omitted>
O*E2 0.0.0.0/0 [110/1] via 172.16.3.2, 00:00:08, Serial0/0/0
!-----
R3> show ip route
<output omitted>
O*E2 0.0.0.0/0 [110/1] via 192.168.10.9, 00:08:15, Serial0/0/1
```

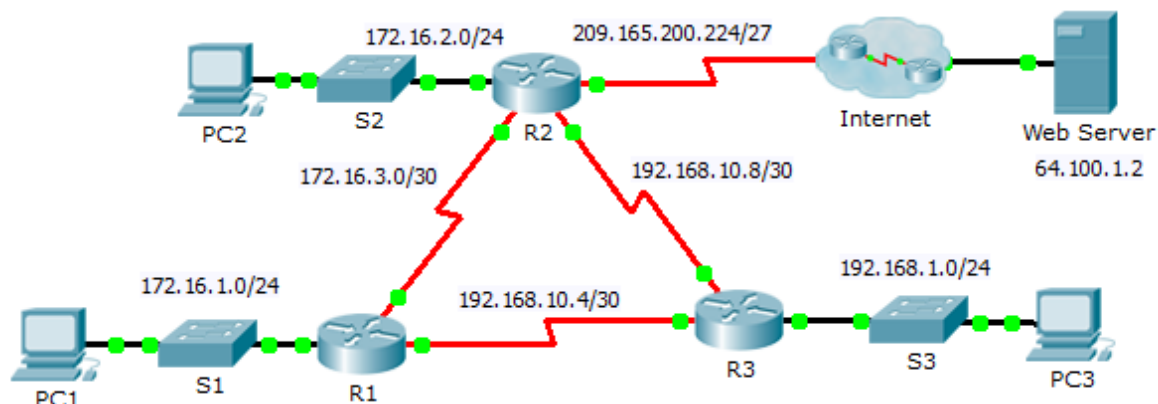
### Part 2: Verify Connectivity

Verify that PC1, PC2, and PC3 can ping the web server.

# Packet Tracer - Configuring OSPF Advanced Features (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



## Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.3.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	G0/0	172.16.2.1	255.255.255.0	N/A
	S0/0/0	172.16.3.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
R3	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	NIC	172.16.1.2	255.255.255.0	172.16.1.1
PC2	NIC	172.16.2.2	255.255.255.0	172.16.2.1
PC3	NIC	192.168.1.2	255.255.255.0	192.168.1.1

## Objectives

**Part 1: Modify OSPF Default Settings**

**Part 2: Verify Connectivity**



### Scenario

In this activity, OSPF is already configured and all end devices currently have full connectivity. You will modify the default OSPF routing configuration by changing the hello and dead timers, adjusting the bandwidth of a link, and enabling OSPF authentication. Then you will verify that full connectivity is restored for all end devices.

### Part 1: Modify OSPF Default Settings

#### Step 1: Test connectivity between all end devices.

Before modifying the OSPF settings, verify that all PCs can ping the web server and each other.

#### Step 2: Adjust the hello and dead timers between R1 and R2.

- a. Enter the following commands on **R1**.

```
R1(config)# interface s0/0/0
R1(config-if)# ip ospf hello-interval 15
R1(config-if)# ip ospf dead-interval 60
```

- b. After a short period of time, the OSPF connection with **R2** will fail. Both sides of the connection need to have the same timers in order for the adjacency to be maintained. Adjust the timers on **R2**.

#### Step 3: Adjust the bandwidth setting on R1.

- a. Trace the path between **PC1** and the web server located at 64.100.1.2. Notice that the path from **PC1** to 64.100.1.2 is routed through **R2**. OSPF prefers the lower cost path.
- b. On the **R1** Serial 0/0/0 interface, set the bandwidth to 64 Kb/s. This does not change the actual port speed, only the metric that the OSPF process on **R1** will use to calculate best routes.  

```
R1(config-if)# bandwidth 64
```
- c. Trace the path between **PC1** and the web server located at 64.100.1.2. Notice that the path from **PC1** to 64.100.1.2 is redirected through **R3**. OSPF prefers the lower cost path.

#### Step 4: Enable OSPF authentication on all serial interfaces.

- a. Use the following commands to configure authentication between **R1** and **R2**.

**Note:** The key text **R1-R2** is case-sensitive.

```
R1(config-router)# area 0 authentication message-digest
R1(config)# interface serial 0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 R1-R2
```

- b. After the dead interval expires, neighbor adjacency between **R1** and **R2** will be lost. Repeat the authentication commands on **R2**.
- c. Use the following command to configure authentication on **R1** for the link it shares with **R3**.

```
R1(config-if)# ip ospf message-digest-key 1 md5 R1-R3
```

- d. Finish the authentication configurations necessary to restore full connectivity. The password for the link between **R2** and **R3** is **R2-R3**.
- e. Verify that authentication is working between each router.

```
R1# show ip ospf interface
Message digest authentication enabled
```

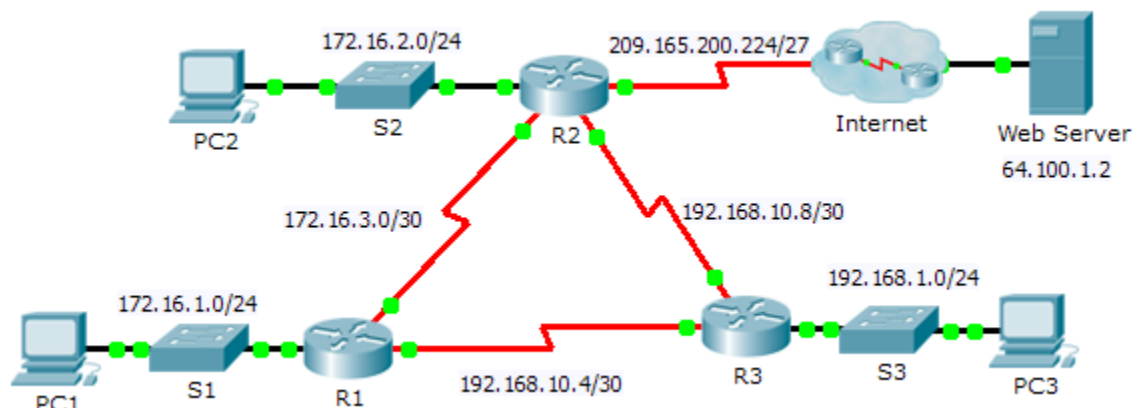
## Part 2: Verify Connectivity

Verify all PCs can ping the web server and each other.

# Packet Tracer – Troubleshooting Single-Area OSPFv2 (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



## Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.3.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	G0/0	172.16.2.1	255.255.255.0	N/A
	S0/0/0	172.16.3.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
R3	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	NIC	172.16.1.2	255.255.255.0	172.16.1.1
PC2	NIC	172.16.2.2	255.255.255.0	172.16.2.1
PC3	NIC	192.168.1.2	255.255.255.0	192.168.1.1

## Scenario

In this activity, you will troubleshoot OSPF routing issues using **ping** and **show** commands to identify errors in the network configuration. Then, you will document the errors you discover and implement an appropriate solution. Finally, you will verify end-to-end connectivity is restored.

## Troubleshooting Process

1. Use testing commands to discover connectivity problems in the network and document the problem in the Documentation Table.
2. Use verification commands to discover the source of the problem and devise an appropriate solution to implement. Document the proposed solution in the Documentation Table.
3. Implement each solution one at a time and verify if the problem is resolved. Indicate the resolution status in the Documentation Table.
4. If the problem is not resolved, it may be necessary to first remove the implemented solution before returning to Step 2.
5. Once all identified problems are resolved, test for end-to-end connectivity.

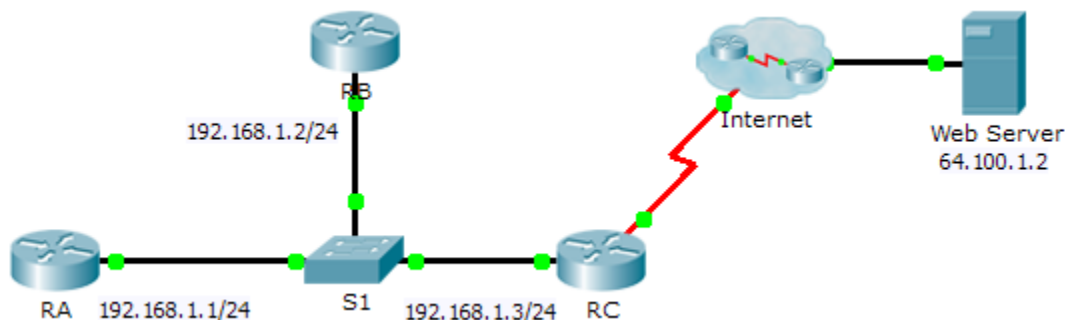
## Documentation Table

Device	Identified Problem	Proposed Solution	Resolved?
R1	Is not forming neighborship with R3	Remove the network 172.16.10.4 0.0.0.3 area 0 statement and replace it with netowrk 192.168.10.4 0.0.0.3 area 0	
R2	Is not propagating the default route	Configure OSPF with the <b>default-information originate</b> command	
R3	Is not forming neighborship with R2	Remove the hello-interval command on the R3 S0/0/1 interface.	

# Packet Tracer – Skills Integration Challenge (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



## Addressing Table

Device	Interface	IP Address	Subnet Mask
RA	G0/0	192.168.1.1	255.255.255.0
RB	G0/0	192.168.1.2	255.255.255.0
RC	G0/0	192.168.1.3	255.255.255.0
	S0/0/0	209.165.200.225	255.255.255.252

## Scenario

In this Skills Integration Challenge, your focus is OSPFv2 advanced configurations. IP addressing has been configured for all devices. You will configure OSPFv2 routing with passive interfaces and default route propagation. You will modify the OSPFv2 configuration by adjusting timers and establishing MD5 authentication. Finally, you will verify your configurations and test connectivity between end devices.

## Requirements

- Use the following requirements to configure OSPFv2 routing on **RA** and **RB**:
  - OSPFv2 routing requirements:
    - Process ID 1
    - Network address for each interface
    - Enable authentication for area 0
  - OSPF priority set to 150 on the LAN interface of **RA**
  - OSPF priority set to 100 on the LAN interface of **RB**
  - OSPF MD5 authentication key ID of 1 and MD5 key "cisco" on the LAN interfaces of RA and RB
  - Set the hello interval to 5
  - Set the dead interval to 20
- Use the following requirements to configure **RC** OSPFv2 routing:
  - OSPFv2 routing requirements:

Process ID 1

Network address for the LAN interface

Enable authentication for area 0

Set all interfaces to passive by default, allow OSPF updates on the active LAN

Set the router to distribute default routes

- Configure a directly attached default route to the Internet
- OSPF priority set to 50 on the LAN interface
- OSPF MD5 authentication key ID of 1 and MD5 key “cisco” on the LAN interface of **RC**
- Set the hello interval to 5
- Set the dead interval to 20

**Note:** Issue the **clear ip ospf process** command on **RC** if the default route does not propagate.

- Verify your configurations and test connectivity
  - OSPF neighbors should be established and routing tables should be complete.
  - **RA** should be the DR, **RB** should be the BDR.
  - All three routers should be able to ping the web server.

### Answer Scripts

```
!-----  
Router RA  
!-----  
en  
conf t  
interface GigabitEthernet0/0  
ip ospf message-digest 1 md5 cisco  
ip ospf hello-interval 5  
ip ospf dead-interval 20  
ip ospf priority 150  
router ospf 1  
area 0 authentication message-digest  
network 192.168.1.0 0.0.0.255 area 0  
end
```

```
!-----  
Router RB  
!-----  
en  
conf t  
interface GigabitEthernet0/0
```

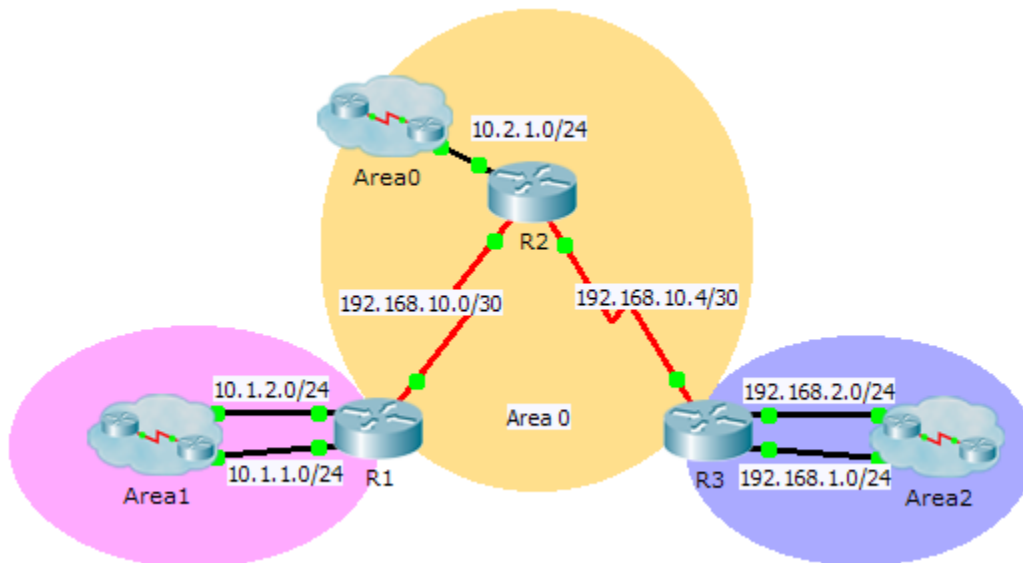
```
ip ospf message-digest 1 md5 cisco
ip ospf hello-interval 5
ip ospf dead-interval 20
ip ospf priority 100
router ospf 1
  area 0 authentication message-digest
  network 192.168.1.0 0.0.0.255 area 0
end
```

```
!-----
Router RC
!-----
en
conf t
interface GigabitEthernet0/0
  ip ospf message-digest 1 md5 cisco
  ip ospf hello-interval 5
  ip ospf dead-interval 20
  ip ospf priority 50
router ospf 1
  passive-interface default
no passive-interface GigabitEthernet0/0
  area 0 authentication message-digest
  network 192.168.1.0 0.0.0.255 area 0
  default-information originate
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
end
```

# Packet Tracer – Configuring Multiarea OSPFv2 (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



## Addressing Table

Device	Interface	IP Address	Subnet Mask	OSPFv2 Area
R1	G0/0	10.1.1.1	255.255.255.0	1
	G0/1	10.1.2.1	255.255.255.0	1
	S0/0/0	192.168.10.2	255.255.255.252	0
R2	G0/0	10.2.1.1	255.255.255.0	0
	S0/0/0	192.168.10.1	255.255.255.252	0
	S0/0/1	192.168.10.5	255.255.255.252	0
R3	G0/0	192.168.2.1	255.255.255.0	2
	G0/1	192.168.1.1	255.255.255.0	2
	S0/0/1	192.168.10.6	255.255.255.252	0

## Objectives

**Part 1: Configure Multiarea OSPFv2**

**Part 2: Verify and Examine Multiarea OSPFv2**



### Background

In this activity, you will configure multiarea OSPFv2. The network is already connected and interfaces are configured with IPv4 addressing. Your job is to enable multiarea OSPFv2, verify connectivity, and examine the operation of multiarea OSPFv2.

### Part 1: Configure OSPFv2

#### Step 1: Configure OSPFv2 on R1.

Configure OSPFv2 on R1 with a process ID of 1 and a router ID of 1.1.1.1.

```
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
```

#### Step 2: Advertise each directly connected network in OSPFv2 on R1.

Configure each network in OSPFv2 assigning areas according to the **Addressing Table**.

```
R1(config-router)# network 10.1.1.0 0.0.0.255 area 1
R1(config-router)# network 10.1.2.0 0.0.0.255 area 1
R1(config-router)# network 192.168.10.0 0.0.0.3 area 0
```

#### Step 3: Configure OSPFv2 on R2 and R3.

Repeat the steps above for R2 and R3 using a router ID of 2.2.2.2 and 3.3.3.3, respectively.

```
R2(config)# router ospf 1
R2(config-router)# router-id 2.2.2.2
R2(config-router)# network 10.2.1.0 0.0.0.255 area 0
R2(config-router)# network 192.168.10.0 0.0.0.3 area 0
R2(config-router)# network 192.168.10.4 0.0.0.3 area 0
!
R3(config)# router ospf 1
R3(config-router)# router-id 3.3.3.3
R3(config-router)# network 192.168.2.0 0.0.0.255 area 2
R3(config-router)# network 192.168.1.0 0.0.0.255 area 2
R3(config-router)# network 192.168.10.4 0.0.0.3 area 0
```

### Part 2: Verify and Examine Multiarea OSPFv2

#### Step 1: Verify connectivity to each of the OSPFv2 areas.

From R1, ping each of the following remote devices in area 0 and area 2: 192.168.1.2, 192.168.2.2, and 10.2.1.2.

#### Step 2: Use show commands to examine the current OSPFv2 operations.

Use the following commands to gather information about your OSPFv2 multiarea implementation.

```
show ip protocols
show ip route
```

```
show ip ospf database
show ip ospf interface
show ip ospf neighbor
```

### Reflection Questions

1. Which router(s) are internal routers? **R2**
2. Which router(s) are backbone routers? **R1, R2, and R3 are all backbone routers.**
3. Which router(s) are area border routers? **R1 and R3**
4. Which router(s) are autonomous system routers? **None, all active interfaces on all three routers connect to an OSPF area.**
5. Which routers are generating Type 1 LSAs? **All OSPF routers generate Type 1 LSAs.**
6. Which routers are generating Type 2 LSAs? **Hidden routers in each of the areas that are DRs are. Router IDs 4.4.4.4, 5.5.5.5, 6.6.6.6, 9.9.9.9**
7. Which routers are generating Type 3 LSAs? **R1 and R3 because each is an ABR and needs to flood area information from one area to the other.**
8. Which routers are generating Type 4 and 5 LSAs? **None, because there is not an ASBR in the network.**
9. How many inter area routes does each router have? **R1 and R3 have two IAs and R2 has 4 IAs.**
10. Why would there usually be an ASBR in this type of network? **ASBR is used to connect external routing domains.**

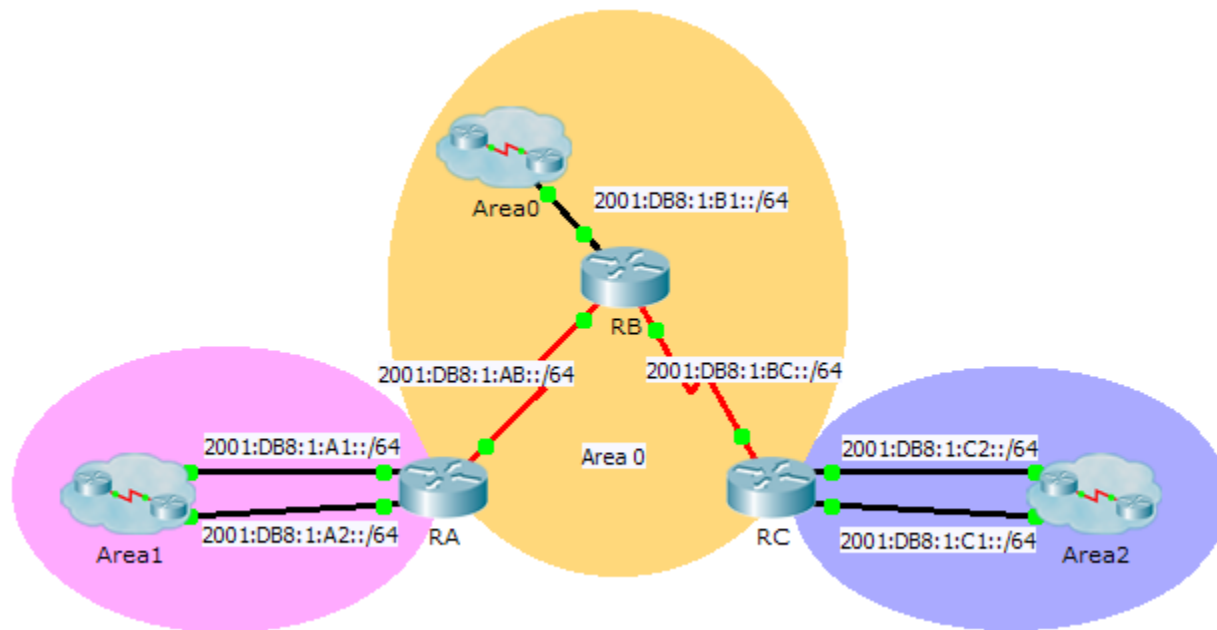
### Suggested Scoring Rubric

Packet Tracer scores 80 points. Each of the Reflection Questions is worth 2 points.

# Packet Tracer – Configuring Multiarea OSPFv3 (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



## Addressing Table

Device	Interface	IPv6 Address	OSPF Area
RA	G0/0	2001:DB8:1:A1::1/64	1
	G0/1	2001:DB8:1:A2::1/64	1
	S0/0/0	2001:DB8:1:AB::2/64	0
	Link-Local	FE80::A	N/A
RB	G0/0	2001:DB8:1:B1::1/64	0
	S0/0/0	2001:DB8:1:AB::1/64	0
	S0/0/1	2001:DB8:1:BC::1/64	0
	Link-Local	FE80::B	N/A
RC	G0/0	2001:DB8:1:C1::1/64	2
	G0/1	2001:DB8:1:C2::1/64	2
	S0/0/1	2001:DB8:1:BC::2/64	0
	Link-Local	FE80::C	N/A

### Objectives

#### Part 1: Configure OSPFv3

#### Part 2: Verify Multiarea OSPFv3 Operations

### Background

In this activity, you will configure multiarea OSPFv3. The network is already connected and interfaces are configured with IPv6 addressing. Your job is to enable multiarea OSPFv3, verify connectivity and examine the operation of multiarea OSPFv3.

### Part 1: Configure OSPFv3

#### Step 1: Enable IPv6 routing and configure OSPFv3 on RA.

- a. Enable IPv6 routing.

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

- b. Configure OSPFv3 on RA with a process ID of 1 and a router ID of 1.1.1.1.

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

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

#### Step 2: Advertise each directly connected network in OSPFv3 on RA.

Configure each active IPv6 interface with OSPFv3 assigning each to the area listed in the **Addressing Table**.

```
RA(config)# interface GigabitEthernet 0/0
```

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

```
RA(config-if)# interface GigabitEthernet 0/1
```

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

```
RA(config-if)# interface Serial 0/0/0
```

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

#### Step 3: Configure OSPFv3 on RB and RC

Repeat the Steps 1 and 2 for **RB** and **RC**, changing the router ID to 2.2.2.2 and 3.3.3.3 respectively.

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

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

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

```
RB(config-rtr)# interface GigabitEthernet0/0
```

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

```
RB(config-if)# interface Serial0/0/0
```

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

```
RB(config-if)# interface Serial0/0/1
```

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

```
!
```

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

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

```
RC(config-rtr)# router-id 3.3.3.3
RC(config-rtr)# interface GigabitEthernet 0/0
RC(config-if)# ipv6 ospf 1 area 2
RC(config-if)# interface GigabitEthernet 0/1
RC(config-if)# ipv6 ospf 1 area 2
RC(config-if)# interface Serial 0/0/1
RC(config-if)# ipv6 ospf 1 area 0
```

## Part 2: Verify Multiarea OSPFv3 Operations

### Step 1: Verify connectivity to each of the OSPFv3 areas.

From RA, ping each of the following remote devices in area 0 and area 2: 2001:DB8:1:B1::2, 2001:DB8:1:A1::2, 2001:DB8:1:A2::2, 2001:DB8:1:C1::2, and 2001:DB8:1:C2::2.

### Step 2: Use show commands to examine the current OSPFv3 operations.

Use the following commands to gather information about your OSPFv3 multiarea implementation.

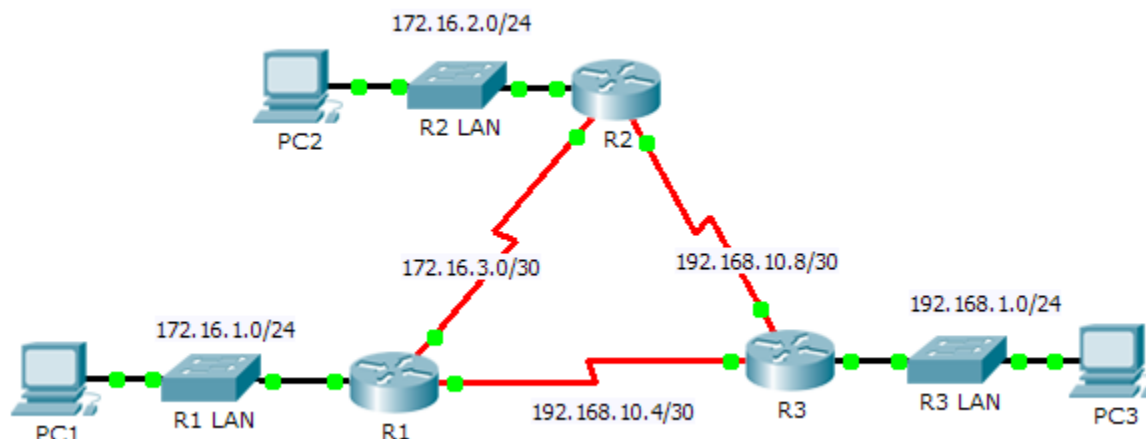
```
show ipv6 ospf
show ipv6 route
show ipv6 ospf database
show ipv6 ospf interface
show ipv6 ospf neighbor
```

**Note:** Packet Tracer output for **show ipv6 protocols** is currently not aligned with IOS 15 output. Refer to the real equipment labs for correct **show** command output.

# Packet Tracer – Configuring Basic EIGRP with IPv4 (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



## Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.3.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	G0/0	172.16.2.1	255.255.255.0	N/A
	S0/0/0	172.16.3.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
R3	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	NIC	172.16.1.10	255.255.255.0	172.16.1.1
PC2	NIC	172.16.2.10	255.255.255.0	172.16.2.1
PC3	NIC	192.168.1.10	255.255.255.0	192.168.1.1

## Objectives

**Part 1: Configure EIGRP**

**Part 2: Verify EIGRP Routing**

### Background

In this activity, you will implement basic EIGRP configurations including network commands, passive interfaces and disabling automatic summarization. You will then verify your EIGRP configuration using a variety of show commands and testing end-to-end connectivity.

### Part 1: Configure EIGRP

#### Step 1: Enable the EIGRP routing process.

Enable the EIGRP routing process on each router using AS number 1. The configuration for **R1** is shown.

```
R1(config)# router eigrp 1
R2(config)# router eigrp 1
R3(config)# router eigrp 1
```

What is the range of numbers that can be used for AS numbers? **1 – 65,535**

**Note:** Packet Tracer currently does not support the configuration of an EIGRP router ID.

#### Step 2: Advertise directly connected networks.

- Use the **show ip route** command to display the directly connected networks on each router.

How can you tell the difference between subnet addresses and interface addresses? **Subnets are identified with a "C" and link addresses are identified with an "L".**

- On each router, configure EIGRP to advertise the specific directly connected subnets. The configuration for **R1** is shown.

```
R1(config-router)# network 172.16.1.0 0.0.0.255
R1(config-router)# network 172.16.3.0 0.0.0.3
R1(config-router)# network 192.168.10.4 0.0.0.3
```

```
R2(config-router)# network 172.16.2.0 0.0.0.255
R2(config-router)# network 172.16.3.0 0.0.0.3
R2(config-router)# network 192.168.10.8 0.0.0.3
```

```
R3(config-router)# network 192.168.1.0 0.0.0.255
R3(config-router)# network 192.168.10.4 0.0.0.3
R3(config-router)# network 192.168.10.8 0.0.0.3
```

#### Step 3: Configure passive interfaces.

Configure the LAN interfaces to not advertise EIGRP updates. The configuration for **R1** is shown.

```
R1(config-router)# passive-interface g0/0
R2(config-router)# passive-interface g0/0
R3(config-router)# passive-interface g0/0
```

#### Step 4: Disable automatic summarization.

The topology contains discontinuous networks. Therefore, disable automatic summarization on each router. The configuration for **R1** is shown.

```
R1(config-router)# no auto-summary
```

```
R2(config-router)# no auto-summary
```

```
R3(config-router)# no auto-summary
```

**Note:** Prior to IOS 15 auto-summary had to be manually disabled.

**Step 5: Save the configurations.**

## Part 2: Verify EIGRP Routing

**Step 1: Examine neighbor adjacencies.**

- Which command displays the neighbors discovered by EIGRP? **show ip eigrp neighbors**
- All three routers should have two neighbors listed. The output for **R1** should look similar to the following:

IP-EIGRP neighbors for process 1

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
0	172.16.3.2	Se0/0/0	14	00:25:05	40	1000	0	28
1	192.168.10.6	Se0/0/1	12	00:13:29	40	1000	0	31

**Step 2: Display the EIGRP routing protocol parameters.**

- What command displays the parameters and other information about the current state of any active IPv4 routing protocol processes configured on the router? **show ip protocols**
- On **R2**, enter the command you listed for 2a and answer the following questions:

How many routers are sharing routing information with **R2**? **2**

Where is this information located under? **Routing Information Sources**

What is the maximum hop count? **100**

**Step 3: Verify end-to-end connectivity**

PC1, PC2 and PC3 should now be able to ping each other. If not, troubleshoot your EIGRP configurations.



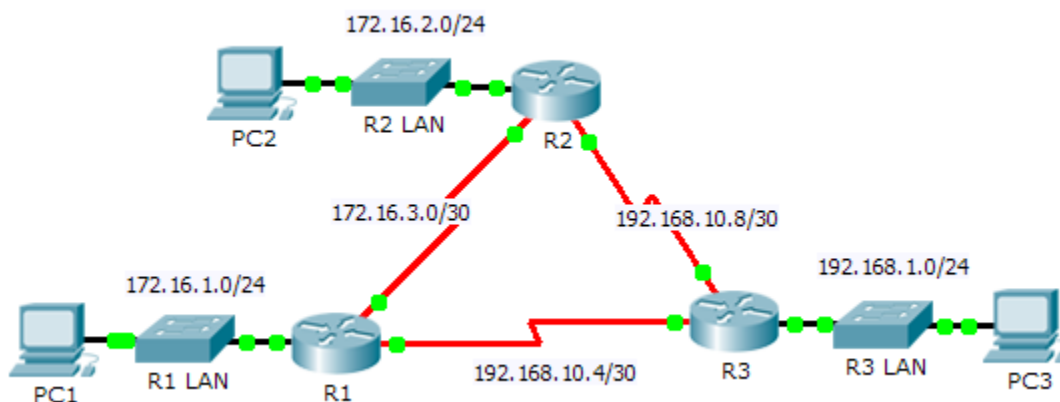
### Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Configure EIGRP	Step 1	2	
	Step 2a	2	
<b>Part 1 Total</b>		<b>4</b>	
Part 2: Verify EIGRP Routing	Step 1a	5	
	Step 2a	5	
	Step 2b	6	
<b>Part 2 Total</b>		<b>16</b>	
<b>Packet Tracer Score</b>		<b>80</b>	
<b>Total Score</b>		<b>100</b>	

# Packet Tracer – Investigating DUAL FSM (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



## Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.16.1.254	255.255.255.0	N/A
	S0/0/0	172.16.3.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	G0/0	172.16.2.254	255.255.255.0	N/A
	S0/0/0	172.16.3.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
R3	G0/0	192.168.1.254	255.255.255.0	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	NIC	172.16.1.1	255.255.255.0	172.16.1.254
PC2	NIC	192.168.1.1	255.255.255.0	192.168.1.254
PC3	NIC	192.168.2.1	255.255.255.0	192.168.2.254

## Objectives

**Part 1: Verify the EIGRP Configuration**

**Part 2: Observe the EIGRP DUAL FSM**

## Background

In this activity, you will modify the EIGRP metric formula to cause a change in the topology. This will allow you to see how EIGRP reacts when a neighbor goes down due to unforeseen circumstances. You will then use the

**debug** command to view topology changes and how the DUAL Finite State Machine determines successor and feasible successor paths to re-converge the network.

### Part 1: Verify EIGRP Configuration

#### Step 1: Examine the routing tables of each router and verify that there is a path to every network in the topology.

What command displays the routing table? **show ip route**

Are any of the routers load balancing between any network? Yes, R1 to the 192.168.10.8 network, R2 to the 192.168.10.4 network, and R3 to the 172.16.3.0 network.

#### Step 2: Verify that each router has entries in its neighbor table.

What command displays the neighbor table? **show ip eigrp neighbors**

How many neighbors does each router have? All routers have two neighbors.

#### Step 3: Analyze the topology table of each router.

- a. What command displays the topology table? **show ip eigrp topology**

Based on the output in the topology table, how many successor paths does each router have? **7**

Why are there more successor paths than networks? There are 6 networks in the topology but each router has two successor paths to one network (R1 has 2 successor paths to 192.168.10.8).

- b. Copy the output for R1's topology table to a text editor so that you can refer to it later.

### Part 2: Observe the EIGRP DUAL FSM

#### Step 1: On R1, turn on the debugging feature that will display DUAL FSM notifications.

What command enables debugging for the EIGRP DUAL FSM? **debug eigrp fsm**

#### Step 2: Force a DUAL FSM update to generate debug output.

- a. Place the R1 and R3 windows side by side so that you can observe the debug output. Then on R3, disable the serial 0/0/0 interface.

```
R3(config)# interface s0/0/0
```

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

- b. Do not disable debugging yet. What debug output indicated changes to the routing table?

<output omitted>

```
DUAL: Dest 192.168.10.4/30 (No peers) not entering active state.
```

```
DUAL: Removing dest 192.168.10.4/30, nexthop 0.0.0.0
```

```
DUAL: No routes. Flushing dest 192.168.10.4/30
```

#### Step 3: Display the routing table of R1.

Verify that 192.168.10.4/30 network is no longer in R1's routing table.

Describe any other changes to the R1 routing table? The 192.168.10.8 only has one route instead of two.

### Step 4: Determine the difference in the topology table.

Examine the topology table of **R1** and compare it to the previous output from Part 1.

Are there any other changes to the **R1**'s topology table? Yes, The 192.168.10.4/30 is no longer in the topology table and there is only one successor to the 192.168.10.8/30.

### Step 5: Document changes in each router's neighbor table.

Examine the neighbor table of each router and compare it to the previous one from Part 1.

Are there any changes to the neighbor table? Yes, R1 192.168.10.6 no longer has R3 192.168.10.5 as a neighbor.

### Step 6: Restore connectivity between R1 and R2.

- With the R1 and R3 windows side by side, on R3 activate the serial 0/0/0 interface and observe the debug output on R1.
- Disable debugging by entering the **no** form of the debug command or simply enter **undebug** all. What debug output indicated changes to the routing table?

```
DUAL: Find FS for dest: 192.168.1.0/24. FD is 2682112, RD is 2170112
```

```
DUAL: RT installed 192.168.1.0/24 via 192.168.10.6
```

How did the DUAL FSM handle the change in topology when the route to **R1** came back up? The route between R1 and R3 on network 192.167.10.4/30 came back up and adjacencies were formed.

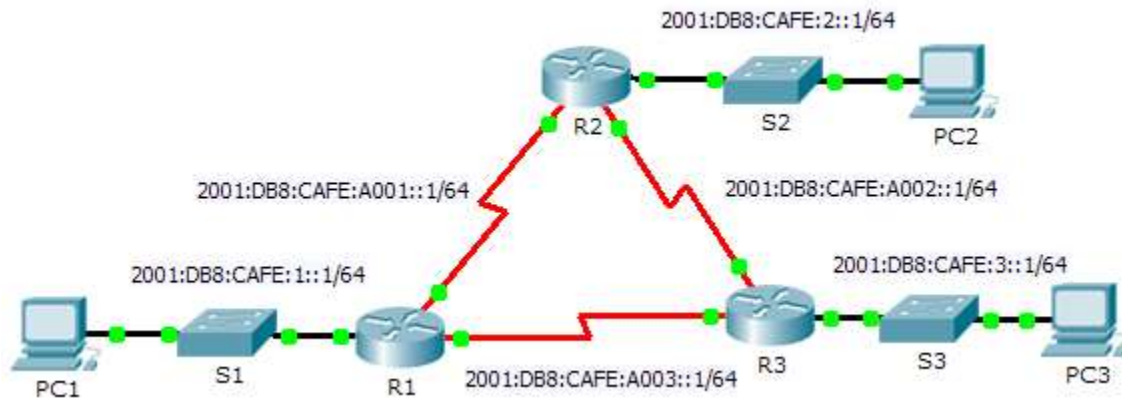
## Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Verify EIGRP Configuration	Step 1	12	
	Step 2	12	
	Step 3	12	
<b>Part 1 Total</b>		<b>36</b>	
Part 2: Observe the EIGRP DUAL FSM	Step 1	10	
	Step 2	12	
	Step 3	10	
	Step 4	10	
	Step 5	10	
	Step 6	12	
<b>Part 2 Total</b>		<b>64</b>	
<b>Total Score</b>		<b>100</b>	

# Packet Tracer – Configuring Basic EIGRP with IPv6 (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



## Addressing Table

Device	Interface	IPv6 Address	Default Gateway
R1	G0/0	2001:DB8:CAFE:1::1/64	N/A
	S0/0/0	2001:DB8:CAFE:A001::1/64	N/A
	S0/0/1	2001:DB8:CAFE:A003::1/64	N/A
	Link-local	FE80::1	N/A
R2	G0/0	2001:DB8:CAFE:2::1/64	N/A
	S0/0/0	2001:DB8:CAFE:A001::2/64	N/A
	S0/0/1	2001:DB8:CAFE:A002::1/64	N/A
	Link-local	FE80::2	N/A
R3	G0/0	2001:DB8:CAFE:3::1/64	N/A
	S0/0/0	2001:DB8:CAFE:A003::2/64	N/A
	S0/0/1	2001:DB8:CAFE:A002::2/64	N/A
	Link-local	FE80::3	N/A
PC1	NIC	2001:DB8:CAFE:1::3/64	Fe80::1
PC2	NIC	2001:DB8:CAFE:2::3/64	Fe80::2
PC3	NIC	2001:DB8:CAFE:3::3/64	Fe80::3

## Objectives

### Part 1: Configure EIGRP for IPv6 Routing

### Part 2: Verify IPv6 EIGRP for IPv6 Routing

#### Scenario

In this activity, 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 **show** commands.

EIGRP for IPv6 has the same overall operation and features as EIGRP for IPv4. 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 will not start.
- The EIGRP for IPv6 routing process uses a “shutdown” feature.

### Part 1: Configure EIGRP for IPv6 Routing

#### Step 1: Enable IPv6 routing on each router.

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

```
R2(config)# ipv6 unicast-routing
```

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

#### Step 2: Enable EIGRP for IPv6 routing on each router.

The IPv6 routing process is shutdown by default. Issue a command that will enable EIGRP for IPv6 routing in R1, R2 and R3.

Enable the EIGRP process on all routers and use **1** as the Autonomous System number.

```
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 3: Assign a router ID to each router.

The router IDs are as follows:

- R1: 1.1.1.1
- R2: 2.2.2.2
- R3: 3.3.3.3

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

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

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

### Step 4: Using AS 1, configure EIGRP for IPv6 on each interface.

```
R1(config)# int g0/0
R1(config-if)# ipv6 eigrp 1
R1(config)# int s0/0/0
R1(config-if)# ipv6 eigrp 1
R1(config)# int s0/0/1
R1(config-if)# ipv6 eigrp 1
```

```
R2(config)# int g0/0
R2(config-if)# ipv6 eigrp 1
R2(config)# int s0/0/0
R2(config-if)# ipv6 eigrp 1
R2(config)# int s0/0/1
R2(config-if)# ipv6 eigrp 1
```

```
R3(config)# int g0/0
R3(config-if)# ipv6 eigrp 1
R3(config)# int s0/0/0
R3(config-if)# ipv6 eigrp 1
R3(config)# int s0/0/1
R3(config-if)# ipv6 eigrp 1
```

## Part 2: Verify EIGRP for IPv6 Routing

### Step 1: Examine neighbor adjacencies.

Use the command **show ipv6 eigrp neighbors** 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.

### Step 2: Examine the IPv6 EIGRP routing table.

Use the **show ipv6 route** command to display the IPv6 routing table on all routers. EIGRP for IPv6 routes are denoted in the routing table with a **D**.

### Step 3: Verify the parameters and current state of the active IPv6 routing protocol processes.

Use the command **show ipv6 protocols** to verify the configured parameter.

### Step 4: Verify end-to-end connectivity.

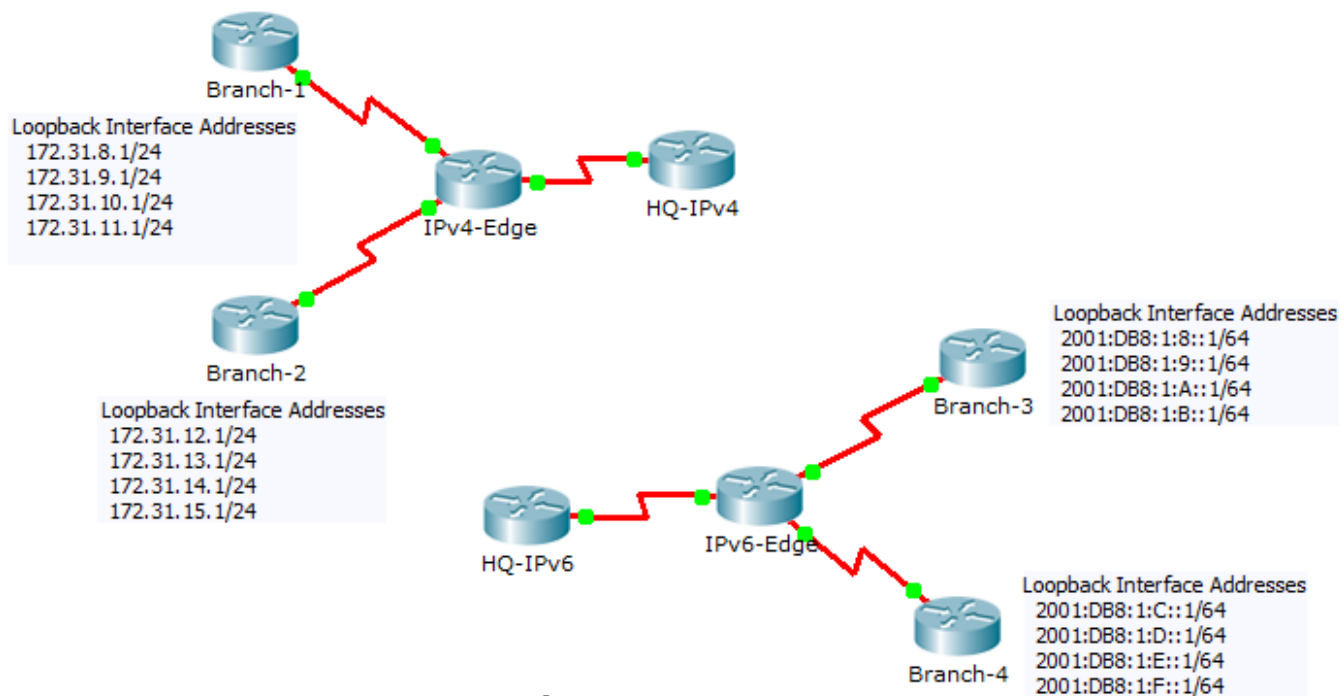
PC1, PC2, and PC3 should now be able to ping each other. If not, troubleshoot your EIGRP configurations.



## Packet Tracer – Configuring EIGRP Manual Summary Routes for IPv4 and IPv6 (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

### Topology



## Addressing Table

Device	Interface	IPv4 Address	Subnet Mask
		IPv6 Address/Prefix	
HQ-IPv4	S0/0/1	10.10.10.1	255.255.255.0
IPv4-Edge	S0/0/0	172.31.6.1	255.255.255.0
	S0/0/1	172.31.7.1	255.255.255.0
	S0/1/0	10.10.10.2	255.255.255.0
Branch-1	S0/0/0	172.31.6.2	255.255.255.0
Branch-2	S0/0/1	172.31.7.2	255.255.255.0
HQ-IPv6	S0/0/1	2001:DB8:1:A001::1/64	
IPv6-Edge	S0/0/0	2001:DB8:1:7::1/64	
	S0/0/1	2001:DB8:1:6::1/64	
	S0/1/0	2001:DB8:1:A001::2/164	
Branch-3	S0/0/0	2001:DB8:1:7::2/64	
Branch-4	S0/0/1	2001:DB8:1:6::2/64	

## Objectives

**Part 1: Configure EIGRP Manual Summary Routes for IPv4**

**Part 2: Configure EIGRP Manual Summary Routes for IPv6**

## Scenario

In this activity, you will calculate and configure summary routes for the IPv4 and IPv6 networks. EIGRP is already configured; however, you are required to configure IPv4 and IPv6 summary routes on the specified interfaces. EIGRP will replace the current routes with a more specific summary route thereby reducing the size of the routing tables.

## Part 1: Configure EIGRP Manual Summary Routes for IPv4

### Step 1: Verify EIGRP configuration on each IPv4 enabled router.

Display the routing table on each IPv4 enabled router and verify that all IPv4 routes are visible. Ping the loopback interfaces from **HQ-IPv4** to verify connectivity.

### Step 2: Calculate, configure and verify a summary route on Branch-1.

By looking at the routing table on **IPv4-Edge**, verify that **Branch-1** is advertising all four networks represented by the loopback interfaces.

- Calculate a summary address for the four loopback interfaces on **Branch-1**.

**172.31.8.0/22**

- Configure **Branch-1** to advertise an EIGRP summary route to **IPv4-Edge**.

```
Branch-1(config)# interface Serial0/0/0
```

```
Branch-1(config-if)# ip summary-address eigrp 1 172.31.8.0 255.255.252.0
```

- c. Verify that **IPv4-Edge** now only has one summary route for all four loopback networks on **Branch-1**.

```
IPv4-Edge# show ip route
```

```
<output omitted>
```

```
D 172.31.8.0/22 [90/2297856] via 172.31.6.2, 00:00:40, Serial0/0/0
```

```
D 172.31.12.1/32 [90/2297856] via 172.31.7.2, 00:01:25, Serial0/0/1
```

```
D 172.31.13.1/32 [90/2297856] via 172.31.7.2, 00:01:25, Serial0/0/1
```

```
D 172.31.14.1/32 [90/2297856] via 172.31.7.2, 00:01:25, Serial0/0/1
```

```
D 172.31.15.1/32 [90/2297856] via 172.31.7.2, 00:01:25, Serial0/0/1
```

### Step 3: Calculate, configure and verify a summary route on Branch-2.

By looking at the routing table on **IPv4-Edge**, verify that **Branch-2** is advertising all four networks represented by the loopback interfaces.

- a. Calculate a summary address for the four loopback interfaces on **Branch-2**.

```
172.31.12.0/22
```

- b. Configure **Branch-2** to advertise an EIGRP summary route to **IPv4-Edge**.

```
Branch-2(config)# interface Serial0/0/1
```

```
Branch-2(config-if)# ip summary-address eigrp 1 172.31.12.0 255.255.252.0
```

- c. Verify that **IPv4-Edge** now only has one summary route for all four loopback networks on **Branch-2**.

```
IPv4-Edge# show ip route
```

```
<output omitted>
```

```
D 172.31.8.0/22 [90/2297856] via 172.31.6.2, 00:02:55, Serial0/0/0
```

```
D 172.31.12.0/22 [90/2297856] via 172.31.7.2, 00:00:07, Serial0/0/1
```

### Step 4: Calculate, configure and verify a summary route on IPv4-Edge.

Although **HQ-IPv4** has two routes that represent the eight loopback networks, these two routes can be summarized into one route.

- a. Calculate a summary address for the two summary routes in **IPv4-Edge's** routing table.

```
172.31.8.0/21
```

- b. Configure **IPv4-Edge** to advertise an EIGRP summary route to **HQ-IPv4**.

```
IPv4-Edge(config)# interface Serial0/1/0
```

```
IPv4-Edge(config-if)# ip summary-address eigrp 1 172.31.8.0 255.255.248.0
```

- c. Verify that **HQ-IPv4** now has only one summary route representing the eight loopback networks on Branch-1 and Branch-2.

**Note:** It may be necessary to reset the interface linking **HQ-IPv4** to **IPv4-Edge**.

```
HQ-IPv4# show ip route
```

```
<output omitted>
```

```
D 172.31.8.0/21 [90/2681856] via 10.10.10.2, 00:06:42, Serial0/0/1
```

- d. You should be able to ping all the IPv4 loopback interfaces from **HQ-IPv4**.

## Part 2: Configure EIGRP Manual Summary Routes for IPv6

### Step 1: Verify EIGRP configuration on each IPv6 enabled router.

Display the routing table on each IPv6 enabled router and verify that all IPv6 routes are visible. Ping the loopback interfaces from **HQ-IPv6** to verify connectivity.

### Step 2: Calculate, configure and verify a summary route on Branch-3.

By looking at the routing table on **IPv6-Edge**, verify that **Branch-3** is advertising all four networks represented by the loopback interfaces.

- a. Calculate a summary address for the four loopback interfaces on **Branch-3**.

```
2001:DB8:1:8::/62
```

- b. Configure **Branch-3** to advertise an EIGRP summary route to **IPv6-Edge**.

```
Branch-3(config)# interface Serial0/0/0
```

```
Branch-3(config-if)# ipv6 summary-address eigrp 1 2001:DB8:1:8::/62
```

- c. Verify that **IPv6-Edge** now only has one summary route for all four loopback networks on **Branch-3**.

**Note:** Packet Tracer does not currently grade EIGRP for IPv6 summary routes. However, the **IPv6-Edge** router should now only have five EIGRP routes, one of which is the summary you configured on **Branch-3**.

```
IPv6-Edge# show ipv6 route
```

```
<output omitted>
```

```
D 2001:DB8:1:8::/62 [90/2297856]
```

```
via FE80::3, Serial0/0/0
```

```
D 2001:DB8:1:C::/64 [90/2297856]
```

```
via FE80::4, Serial0/0/1
```

```
D 2001:DB8:1:D::/64 [90/2297856]
```

```
via FE80::4, Serial0/0/1
```

```
D 2001:DB8:1:E::/64 [90/2297856]
```

```
via FE80::4, Serial0/0/1
```

```
D 2001:DB8:1:F::/64 [90/2297856]
```

```
via FE80::4, Serial0/0/1
```

### Step 3: Calculate, configure and verify a summary route on Branch-4.

By looking at the routing table on **IPv6-Edge**, verify that **Branch-4** is advertising all four networks represented by the loopback interfaces.

- a. Calculate a summary address for the four loopback interfaces on **Branch-4**.

```
2001:DB8:1:C::/62
```

- b. Configure **Branch-4** to advertise an EIGRP summary route to **IPv6-Edge**.

```
Branch-4(config)# interface Serial0/0/1
```

```
Branch-4(config-if)# ipv6 summary-address eigrp 1 2001:DB8:1:C::/62
```

- c. Verify that **IPv6-Edge** now only has one summary route for all four loopback networks on **Branch-4**.

**Note:** Packet Tracer does not currently grade EIGRP for IPv6 summary routes. However, the **IPv6-Edge** router should now only have two EIGRP routes, one summary route from each of the IPv6 branch routers.

```
IPv6-Edge# show ipv6 route
```

```
<output omitted>
```

```
D    2001:DB8:1:8::/62 [90/2297856]
```

```
    via FE80::3, Serial0/0/0
```

```
D    2001:DB8:1:C::/62 [90/2297856]
```

```
    via FE80::4, Serial0/0/1
```

### Step 4: Calculate, configure and verify a summary route on IPv6-Edge.

Although **HQ-IPv6** has two routes that represent the eight loopback networks, these two routes can be summarized into one route.

- a. Calculate a summary address for the two summary routes in **IPv6-Edge's** routing table.

```
2001:DB8:1:8::/61
```

- b. Configure **IPv6-Edge** to advertise an EIGRP summary route to **HQ-IPv6**.

```
IPv6-Edge(config)# interface Serial0/1/0
```

```
IPv6-Edge(config-if)# ipv6 summary-address eigrp 1 2001:DB8:1:8::/61
```

- c. Verify that **HQ-IPv6** now only has one summary route representing the eight loopback networks on **Branch-3** and **Branch-4**.

**Note:** It may be necessary to reset the interface linking **HQ-IPv6** to **IPv6-Edge**.

```
HQ-IPv6# show ipv6 route
```

```
<output omitted>
```

```
D    2001:DB8:1:8::/61 [90/2681856]
```

```
    via FE80::2, Serial0/0/1
```

- d. You should be able to ping all the IPv6 loopback interfaces from **HQ-IPv6**.

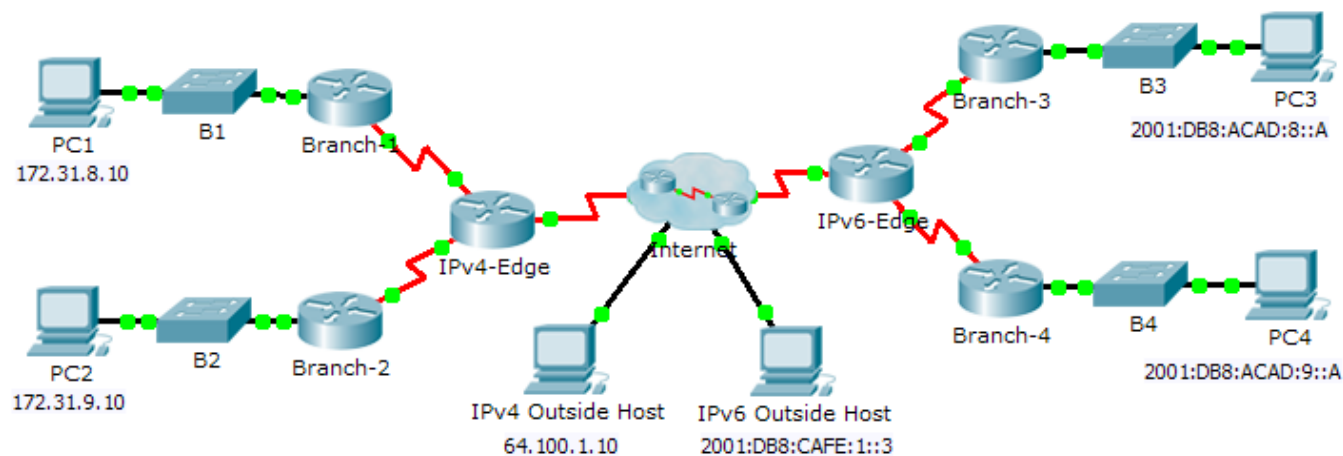
### Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 2: Configure EIGRP Manual Summary Routes for IPv6	Step 2	20	
	Step 3	20	
	Step 4	10	
Part 2 Total		50	
Packet Tracer Score		50	
Total Score		100	

## Packet Tracer – Propagating a Default Route in EIGRP for IPv4 and IPv6 (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

### Topology



## Addressing Table

Device	Interface	IPv4 Address	Subnet Mask
		IPv6 Address/Prefix	
IPv4-Edge	S0/0/0	172.31.6.1	255.255.255.0
	S0/0/1	172.31.7.1	255.255.255.0
	S0/1/0	209.165.200.226	255.255.255.224
Branch-1	G0/0	172.31.8.1	255.255.255.0
	S0/0/0	172.31.6.2	255.255.255.0
Branch-2	G0/0	172.31.9.1	255.255.255.0
	S0/0/1	172.31.7.2	255.255.255.0
IPv6-Edge	S0/0/0	2001:DB8:ACAD:7::1/64	
	S0/0/1	2001:DB8:ACAD:6::1/64	
	S0/1/0	2001:DB8:CAFE:ABCD::2/164	
Branch-3	G0/0	2001:DB8:ACAD:8::1/64	
	S0/0/0	2001:DB8:ACAD:7::2/64	
Branch-4	G0/0	2001:DB8:ACAD:9::1/64	
	S0/0/1	2001:DB8:ACAD:6:::2/64	

## Objectives

**Part 1: Propagate an IPv4 Default Route**

**Part 2: Propagate an IPv6 Default Route**

**Part 3: Verify Connectivity to Outside Hosts**

## Scenario

In this activity, you will configure and propagate a default route in EIGRP for IPv4 and IPv6 networks. EIGRP is already configured. However, you are required to configure an IPv4 and an IPv6 default route. Then, you will configure the EIGRP routing process to propagate the default route to downstream EIGRP neighbors. Finally, you will verify the default routes by pinging hosts outside the EIGRP routing domain.

## Part 1: Propagate a Default Route in EIGRP for IPv4

### Step 1: Verify EIGRP configuration on each IPv4 enabled router.

Display the routing table of each IPv4 enabled router and verify that all IPv4 routes are visible.

### Step 2: Configure an IPv4 default route.

Configure a directly connected IPv4 default route on **IPv4-Edge**.

```
IPv4-Edge(config)# ip route 0.0.0.0 0.0.0.0 Serial0/1/0
```



### Step 3: Propagate the default route in EIGRP.

Configure the EIGRP routing process to propagate the default route.

```
IPv4-Edge(config)# router eigrp 1
IPv4-Edge(config-router)# redistribute static
```

### Step 4: Verify IPv4 default route is propagating.

Display the routing tables for **Branch-1** and **Branch-2** to verify the default route is now installed.

```
Branch-1# show ip route
<output omitted>
D*EX 0.0.0.0/0 [170/7289856] via 172.31.6.1, 00:01:24, Serial0/0/0

Branch-2# show ip route
<output omitted>
D*EX 0.0.0.0/0 [170/7289856] via 172.31.7.1, 00:01:45, Serial0/0/1
```

## Part 2: Propagate a Default Route in EIGRP for IPv6

### Step 1: Verify EIGRP configuration on each IPv6 enabled router.

Display the routing table of each IPv6 enabled router and verify that all IPv6 routes are visible.

### Step 2: Configure an IPv6 default route.

Configure a directly connected IPv6 default route on **IPv6-Edge**.

```
IPv6-Edge(config)# ipv6 route ::/0 Serial0/1/0
```

### Step 3: Propagate the default route in EIGRP.

Configure the EIGRP routing process to propagate the default route.

```
IPv6-Edge(config)# ipv6 router eigrp 1
IPv6-Edge(config-rtr)# redistribute static
```

### Step 4: Verify IPv6 default route is propagating.

Display the routing tables for **Branch-3** and **Branch-4** to verify the default route is now installed.

```
Branch-3> en
Branch-3# show ipv6 route
<output omitted>
EX ::/0 [170/7289856]
    via FE80::1, Serial0/0/0

Branch-4# show ipv6 route
<output omitted>
EX ::/0 [170/7289856]
```

```
via FE80::1, Serial0/0/1
```

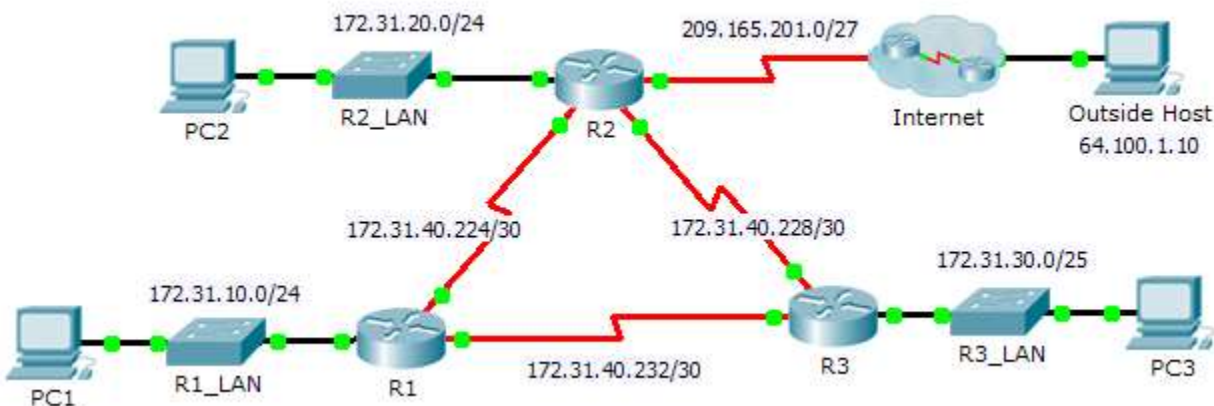
### Part 3: Verify Connectivity to Outside Hosts

- **PC1** and **PC2** should now be able to ping **IPv4 Outside Host**.
- **PC3** and **PC4** should now be able to ping **IPv6 Outside Host**.

## Packet Tracer – Troubleshooting EIGRP for IPv4 (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

### Topology



### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.31.10.1	255.255.255.0	N/A
	S0/0/0	172.31.40.225	255.255.255.252	N/A
	S0/0/1	172.31.40.233	255.255.255.252	N/A
R2	G0/0	172.31.20.1	255.255.255.0	N/A
	S0/0/0	172.31.40.226	255.255.255.252	N/A
	S0/0/1	172.31.40.229	255.255.255.252	N/A
R3	G0/0	172.31.30.1	255.255.255.0	N/A
	S0/0/0	172.31.40.234	255.255.255.252	N/A
	S0/0/1	172.31.40.230	255.255.255.252	N/A
PC1	NIC	172.31.10.10	255.255.255.0	172.31.10.1
PC2	NIC	172.31.20.10	255.255.255.0	172.31.20.1
PC3	NIC	172.31.30.10	255.255.255.0	172.31.30.1

### Scenario

In this activity, you will troubleshoot EIGRP neighbor issues. Use show commands to identify errors in the network configuration. Then, you will document the errors you discover and implement an appropriate solution. Finally, you will verify full end-to-end connectivity is restored.

### Troubleshooting Process

1. Use testing commands to discover connectivity problems in the network and document the problem in the Documentation Table.
2. Use verification commands to discover the source of the problem and devise an appropriate solution to implement. Document the proposed solution in the Documentation Table.
3. Implement each solution one at a time and verify if the problem is resolved. Indicate the resolution status in the Documentation Table.
4. If the problem is not resolved, it may be necessary to first remove the implemented solution before returning to Step 2.
5. Once all identified problems are resolved, test for full end-to-end connectivity.

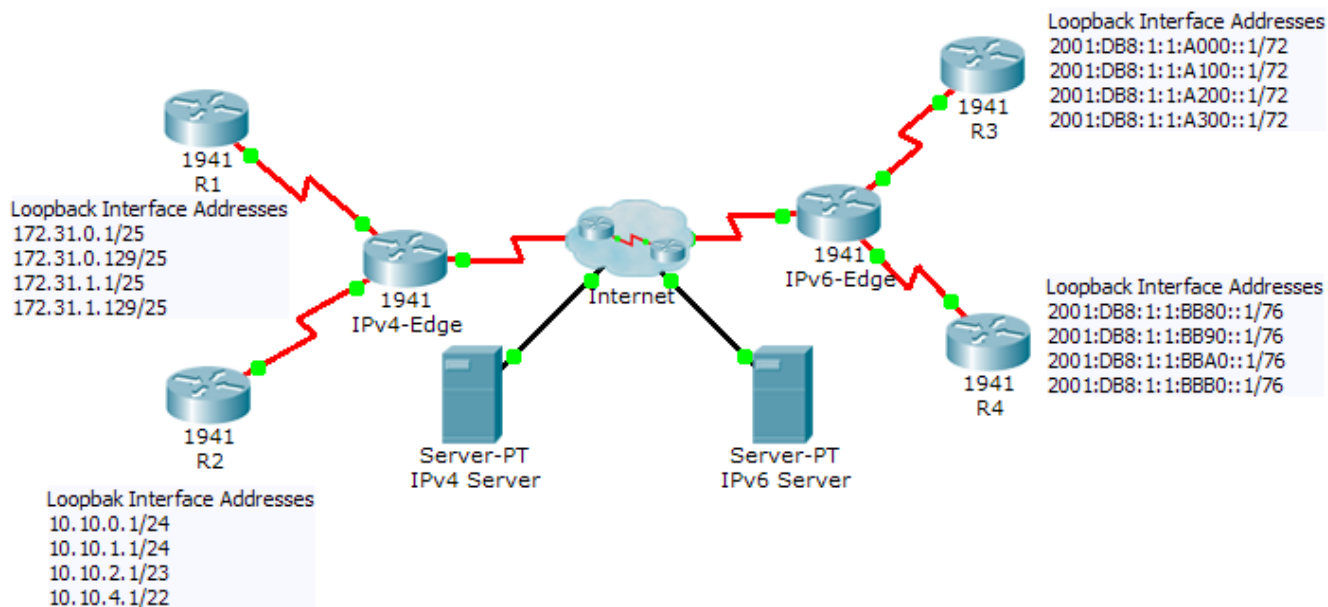
### Documentation Table

Device	Identified Problem	Proposed Solution	Resolved?
R1	Has not established any adjacencies	Remove EIGRP 11 and configure EIGRP 1, advertise the directly connected networks and passive-interface g0/0 and disable automatic summarization.	
R2	Is not forming an adjacency with R3.	Advertise the 172.31.40.228/30 network	
R3	Is performing automatic summarization	Disable automatic summarization using the no auto-summary EIGRP subcommand	

## Packet Tracer - Skills Integration Challenge (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

### Topology



## Addressing Table

Device	Interface	IPv4 Address	Subnet Mask
		IPv6 Address/Prefix	
IPv4-Edge	S0/0/0	172.31.6.1	255.255.255.252
	S0/0/1	10.10.8.1	255.255.255.252
	S0/1/0	209.165.200.226	255.255.255.224
R1	S0/0/0	172.31.6.2	255.255.255.252
R2	S0/0/1	10.10.8.2	255.255.255.252
IPv6-Edge	S0/0/0	2001:DB8:A001:6::1/64	
	S0/0/1	2001:DB8:A001:7::1/64	
	S0/1/0	2001:DB8:CAFE:1::2/64	
R3	S0/0/0	2001:DB8:A001:7::2/64	
R4	S0/0/1	2001:DB8:A001:6::2/64	

## Scenario

In this activity, you are tasked with implementing EIGRP for IPv4 and IPv6 on two separate networks. Your task includes enabling EIGRP, assigning router-IDs, changing the hello timers, configuring EIGRP summary routes and limiting EIGRP advertisements.

## Requirements

### EIGRP for IPv4

- Implement EIGRP on IPv4 enabled routers using Autonomous System 1.
  - Use the classful network address for the loopback interfaces.
  - Use the wildcard mask to advertise the /30 networks between **R1**, **R2** and **IPv4-Edge**.
  - Use the **default** method to only allow EIGRP updates out the active EIGRP serial interfaces.
  - Advertisements should not be summarized.

```
R1(config)# router eigrp 1
R1(config-router)# passive-interface default
R1(config-router)# no passive-interface Serial0/0/0
R1(config-router)# network 172.31.0.0
R1(config-router)# no auto-summary
```

```
R2(config)# router eigrp 1
R2(config-router)# passive-interface default
R2(config-router)# no passive-interface Serial0/0/1
R2(config-router)# network 10.0.0.0
```

```
R2(config-router)# no auto-summary
```

```
IPv4-Edge(config)# router eigrp 1
```

```
IPv4-Edge(config-router)# passive-interface default
```

```
IPv4-Edge(config-router)# no passive-interface Serial0/0/0
```

```
IPv4-Edge(config-router)# no passive-interface Serial0/0/1
```

```
IPv4-Edge(config-router)# network 172.31.6.0 0.0.0.3
```

```
IPv4-Edge(config-router)# network 10.10.8.0 0.0.0.3
```

```
IPv4-Edge(config-router)# no auto-summary
```

- Configure a directly attached default route on **IPv4-Edge** and propagate it in EIGRP updates.

```
IPv4-Edge(config)# ip route 0.0.0.0 0.0.0.0 Serial0/1/0
```

```
IPv4-Edge(config)# router eigrp 1
```

```
IPv4-Edge(config-router)# redistribute static
```

- Configure the serial interfaces between **R1**, **R2** and **IPv4-Edge** to send hellos every 10 seconds.

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

```
R1(config-if)# ip hello-interval eigrp 1 10
```

```
R2(config)# interface s0/0/1
```

```
R2(config-if)# ip hello-interval eigrp 1 10
```

```
IPv4-Edge(config)# interface s0/0/0
```

```
IPv4-Edge(config-if)# ip hello-interval eigrp 1 10
```

```
IPv4-Edge(config-if)# interface s0/0/1
```

```
IPv4-Edge(config-if)# ip hello-interval eigrp 1 10
```

- On **R1** and **R2**, configure an EIGRP summary route for the loopback networks.

R1 Loopback Networks	R2 Loopback Networks
172.31.0.0/25	10.10.0.0/24
172.31.0.128/25	10.10.1.0/24
172.31.1.0/25	10.10.2.0/23
172.31.1.128/25	10.10.4.0/22
Summary: 172.31.0.0/23	Summary: 10.10.0.0/21

```
R1(config)# interface Serial0/0/0
```

```
R1(config-if)# ip summary-address eigrp 1 172.31.0.0 255.255.254.0
```

```
R2(config)# interface Serial0/0/1
```

```
R2(config-if)# ip summary-address eigrp 1 10.10.0.0 255.255.248.0
```

- **R1** and **R2** should only have four EIGRP routes in the routing table, one of which is the default route (D\*EX). **IPv4-Edge** should only have two EIGRP routes in the routing table.
- Verify **R1** and **R2** can ping the **IPv4 Server**. **IPv4 Server** should also be able to ping every loopback address on **R1** and **R2**.

### EIGRP for IPv6

- Implement EIGRP on IPv6 enabled routers using Autonomous System 1.
  - Assign **IPv6-Edge** with the router-ID of 1.1.1.1
  - Assign **R3** with the router-ID of 3.3.3.3
  - Assign **R4** with the router-ID of 4.4.4.4

```
IPv6-Edge(config)# ipv6 unicast-routing
IPv6-Edge(config)# ipv6 router eigrp 1
IPv6-Edge(config-rtr)# eigrp router-id 1.1.1.1
IPv6-Edge(config-rtr)# no shutdown
IPv6-Edge(config-rtr)# interface Serial0/0/0
IPv6-Edge(config-if)# ipv6 eigrp 1
IPv6-Edge(config-if)# interface Serial0/0/1
IPv6-Edge(config-if)# ipv6 eigrp 1
```

```
R3(config)# ipv6 unicast-routing
R3(config)# ipv6 router eigrp 1
R3(config-rtr)# eigrp router-id 3.3.3.3
R3(config-rtr)# no shutdown
R3(config-rtr)# interface Loopback0
R3(config-if)# ipv6 eigrp 1
R3(config-if)# interface Loopback1
R3(config-if)# ipv6 eigrp 1
R3(config-if)# interface Loopback2
R3(config-if)# ipv6 eigrp 1
R3(config-if)# interface Loopback3
R3(config-if)# ipv6 eigrp 1
R3(config-if)# interface Serial0/0/0
R3(config-if)# ipv6 eigrp 1
```

```
R4(config)# ipv6 unicast-routing
R4(config)# ipv6 router eigrp 1
R4(config-rtr)# eigrp router-id 4.4.4.4
R4(config-rtr)# no shutdown
R4(config-rtr)# interface Loopback8
```



```
R4(config-if)# ipv6 eigrp 1
R4(config-if)# interface Loopback9
R4(config-if)# ipv6 eigrp 1
R4(config-if)# interface Loopback10
R4(config-if)# ipv6 eigrp 1
R4(config-if)# interface Loopback11
R4(config-if)# ipv6 eigrp 1
R4(config-if)# interface Serial0/0/1
R4(config-if)# ipv6 eigrp 1
```

- Configure a directly attached default route on **IPv6-Edge** and propagate it in EIGRP updates.

```
IPv6-Edge(config)# ipv6 route ::/0 Serial0/1/0
IPv6-Edge(config)# ipv6 router eigrp 1
IPv6-Edge(config-rtr)# redistribute static
```

- On **R3** and **R4**, configure an EIGRP summary route for the loopback networks.

R3 Loopback Networks	R4 Loopback Networks
2001:DB8:1:1:A000::1/72	2001:DB8:1:1:BB80::1/76
2001:DB8:1:1:A100::1/72	2001:DB8:1:1:BB90::1/76
2001:DB8:1:1:A200::1/72	2001:DB8:1:1:BBA0::1/76
2001:DB8:1:1:A300::1/72	2001:DB8:1:1:BBB0::1/76
Summary: 2001:DB8:1:1:A000::/70	Summary: 2001:DB8:1:1:BB80::/74

```
R3(config)# interface Serial0/0/0
R3(config-if)# ipv6 summary-address eigrp 1 2001:DB8:1:1:A000::/70
```

```
R4(config)# interface Serial0/0/1
R4(config-if)# ipv6 summary-address eigrp 1 2001:DB8:1:1:BB80::/74
```

- R3** and **R4** should only have four EIGRP routes in the routing table, counting the default external route. **IPv6-Edge** should only have two EIGRP routes in the routing table.
- Verify **R3** and **R4** can ping the **IPv6 Server**. **IPv6 Server** should also be able to ping every loopback address on **R3** and **R4**.

### Suggested Scoring Rubric

**Note:** Packet Tracer does not currently grade EIGRP for IPv6 summary routes. Therefore, part of your grade depends on routing table verification by your instructor.

Scored Work	Possible Points	Earned Points
IPv6-Edge Routing Table	10	
Packet Tracer Score	90	
Total Score	100	

The **IPv6-Edge** router should show the following summary routes and no other **D** routes:

```
IPv6-Edge# show ipv6 route
```

```
<output omitted>
```

```
D    2001:DB8:1:1:A000::/70 [90/2297856]
```

```
    via FE80::2E0:F7FF:FE41:B901, Serial0/0/1
```

```
D    2001:DB8:1:1:BB80::/74 [90/2297856]
```

```
    via FE80::20A:41FF:FE80:4002, Serial0/0/0
```

# Packet Tracer – Decoding IOS Image Names (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



## Objectives

**Part 1: Naming Convention for IOS 12.4 Images**

**Part 2: Naming Convention for IOS 15 Images**

**Part 3: Use show version Command to Find IOS Images**

## Scenario

As a network technician, it is important that you are familiar with the IOS image naming convention so that you can, at a glance, determine important information about operating systems currently running on a device. In this scenario, Company A has merged with Company B. Company A has inherited network equipment from Company B. You have been assigned to document the features for the IOS images on these devices.

## Part 1: Naming Convention for 12.4 Images

In the table below, you will find a list IOS 12.4 images. Decode the IOS image name by entering the appropriate information in each column.

IOS Images	Hardware	Feature Set	Train No.	Maintenance Release	Train Identifier	Rebuild Identifier
c1841-advipservicesk9-mz.124-24.T6.bin	1841	Advipservicesk9 (Advanced IP Services with strong encryption)	12.4	24	T	6
c1841-ipbasek9-mz.124-12.bin	1841	Ipbasek9 (Base IP Services with strong encryption)	12.4	12	M	
c2800nm-advipservicesk9-mz.124-15.T9.bin	2811	advipservicesk9	12.4	15	T	9
c2801-ipbasek9-mz.124-25f.bin	2801	ipbasek9	12.4	25	M	f
c2801-advsecurityk9-mz.124-18e.bin	2801	advsecurityk9 (Advanced Security with strong encryption)	12.4	18	M	e

What do the letters “mz” in the file name tell you about the file? The letter “m” indicates that the image is executed in Random Access Memory (RAM). The letter “z” indicates that the file is in a compressed format.

## Part 2: Naming Convention for IOS 15 Images

In the table below, you will find a list IOS 15 images. Decode the IOS image name by entering the appropriate information in each column.

IOS Images	Hardware	Feature Set	Major Release	Minor Release	New Feature Release	Maintenance Release	Maintenance Rebuild
c1900-universalk9-mz.SPA.153-2.T.bin	1900	universal	15	3	2	T	
c1900-universalk9-mz.SPA.152-4.M2.bin	1900	universal	15	2	4	M	2
c2900-universalk9-mz.SPA.151-4.M4.bin	2900	universal	15	1	4	M	4
c2900-universalk9-mz.SPA.152-3.T3.bin	2900	universal	15	2	3	T	3

## Part 3: Use show version Command to Find IOS Images

Access the routers in the topology. At the command prompt, issue the **show version** command on both routers and list the IOS image of each router in the table. Decode the IOS image name by entering the appropriate information in each column.

## Packet Tracer – Decoding IOS Images Names

IOS 12.4 Image	Hardware	Feature Set	Train No.	Maintenance Release	Train Identifier	Rebuild Identifier
c1841-advipservicesk9-mz.124-15.T1.bin	1841	Advipservicesk9	12.4	15	T	1

IOS 15 Image	Hardware	Feature Set	Major Release	Minor Release	New Feature Release	Maintenance Release	Maintenance Rebuild
c1900-universalk9-mz.SPA.151-1.M4.bin	1941	universal	15	1	1	M	4

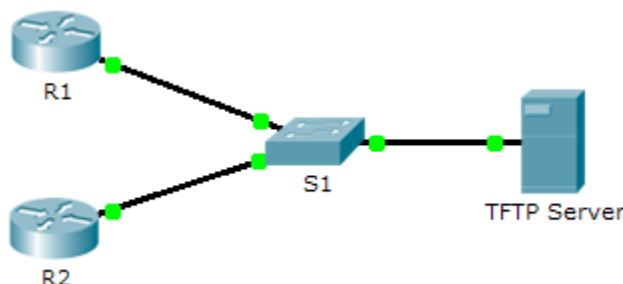
### Suggested Scoring Rubric

Activity Section	Possible Points	Earned Points
Part 1: Naming Convention for IOS 12.4 Images	30	
Part 2: Naming Convention for IOS 15 Images	20	
Part 3: Use show version Command to Find IOS Images	50	
<b>Total Score</b>	<b>100</b>	

# Packet Tracer – Using a TFTP Server to Upgrade a Cisco IOS Image (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



## Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.2.1	255.255.255.0	N/A
R2	G0/0	192.168.2.2	255.255.255.0	N/A
S1	VLAN 1	192.168.2.3	255.255.255.0	192.168.2.1
TFTP Server	NIC	192.168.2.254	255.255.255.0	192.168.2.1

## Objectives

**Part 1: Upgrade an IOS Image on a Cisco Device**

**Part 2: Backup an IOS Image on a TFTP Server**

## Scenario

A TFTP server can help manage the storage of IOS images and revisions to IOS images. For any network, it is good practice to keep a backup copy of the Cisco IOS Software image in case the system image in the router becomes corrupted or accidentally erased. A TFTP server can also be used to store new upgrades to the IOS and then deployed throughout the network where it is needed. In this activity, you will upgrade the IOS images on Cisco devices by using a TFTP server. You will also backup an IOS image with the use of a TFTP server.

## Part 1: Upgrade an IOS Image on a Cisco Device

### Step 1: Upgrade an IOS image on a router.

- Access the TFTP server and enable the TFTP service.
- Note the IOS images that are available on the TFTP server.

Which IOS images stored on the server are compatible with 1841? c1841-ipbase-mz.123-14.T7.bin, c1841-ipbasek9-mz.124-12.bin, and c1841-advipservicesk9-mz.124-15.T1.bin

- From **R1**, issue the **show flash:** command and record the available flash memory. 49928533 bytes

- d. Copy the IPBase with strong encryption IOS image (ipbasek9) for the 1841 router from the TFTP Server to **R1**.

```
R1# copy tftp: flash:
```

```
Address or name of remote host []? 192.168.2.254
```

```
Source filename []? c1841-ipbasek9-mz.124-12.bin
```

Destination filename [c1841-ipbasek9-mz.124-12.bin]?

```
Accessing tftp://192.168.2.254/c1841-ipbasek9-mz.124-12.bin...
```

Loading c1841-ipbasek9-mz.124-12.bin from 192.168.2.254:

[illegible]

```
[OK - 16599160 bytes]
```

16599160 bytes copied in 3.44 secs (1079726 bytes/sec)

- e. Verify that the IOS image has been copied to flash. How many IOS images are located in the flash? 2

- f. Use the **boot system** command to load the IPBase image on the next reload.

```
R1(config)# boot system flash c1841-ipbasek9-mz.124-12.bin
```

- g. Save the configuration and reload **R1**.

- h. Verify the upgraded IOS image is loaded after **R1** reboots.

## Step 2: Upgrade an IOS image on a switch.

- a. Access the TFTP server and copy the c2960-lanbase-mz.122-25.FX.bin image to **S1**.

```
S1# copy tftp: flash:
```

- b. Verify that this new image is listed first in the **show flash:** output.

**Note:** The first image listed the **show flash:** output is loaded by default.

- c. Reload S1 and verify the new image has been loaded into memory.

## Part 2: Backup an IOS Image to a TFTP Server

- a. On R2, display the contents of flash and record the IOS image. `c1900-universalk9-mz.SPA.151-4.M4.bin`

```
R2# show flash:
```

- b. Use the **copy** command to backup the IOS image in flash memory on **R2** to a TFTP server.

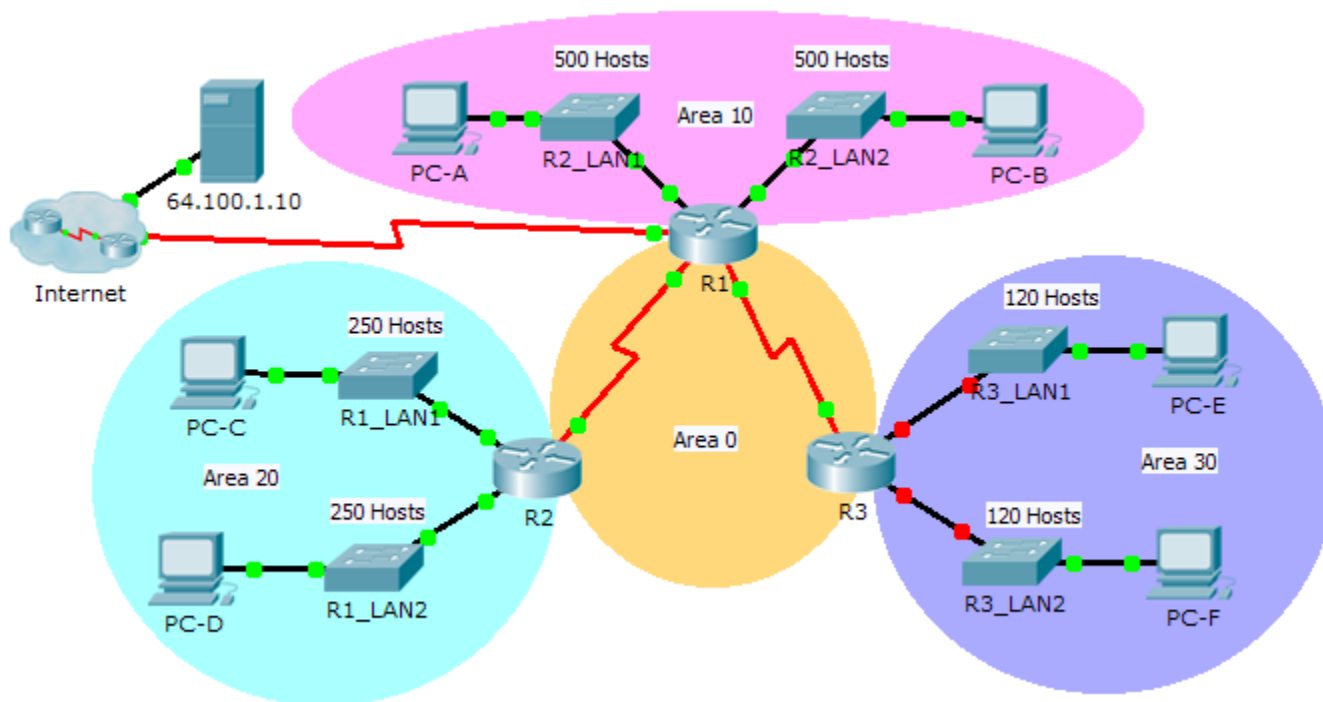
```
R2# copy flash: tftp:
```

- c. Access the TFTP server and verify that the IOS image has been copied to the TFTP server.

## Packet Tracer – Skills Integration Challenge (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

### Topology





## Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.31.25.254	255.255.254.0	N/A
	G0/1	172.31.27.254	255.255.254.0	N/A
	S0/0/0	172.31.31.249	255.255.255.252	N/A
	S0/0/1	172.31.31.253	255.255.255.252	N/A
	S0/1/0	209.165.201.2	255.255.255.252	N/A
R2	G0/0	172.31.28.254	255.255.255.0	N/A
	G0/1	172.31.29.254	255.255.255.0	N/A
	S0/0/0	172.31.31.250	255.255.255.252	N/A
R3	G0/0	172.31.30.126	255.255.255.128	N/A
	G0/1	172.31.30.254	255.255.255.128	N/A
	S0/0/1	172.31.31.254	255.255.255.252	N/A
PC-A	NIC	172.31.24.1	255.255.254.0	172.31.25.254
PC-B	NIC	172.31.26.1	255.255.254.0	172.31.27.254
PC-C	NIC	172.31.28.1	255.255.255.0	172.31.28.254
PC-D	NIC	172.31.29.1	255.255.255.0	172.31.29.254
PC-E	NIC	172.31.30.1	255.255.255.128	172.31.30.126
PC-F	NIC	172.31.30.129	255.255.255.128	172.31.30.254

## Scenario

As network technician familiar with IPv4 addressing, routing and network security, you are now ready to apply your knowledge and skills to a network infrastructure. Your task is to finish designing the VLSM IPv4 addressing scheme, implement multi-area OSPF and secure access to the VTY lines using access control lists.

## Requirements

- The **R3** LANs need addressing. Complete the VLSM design using the next available subnets in the remaining **172.31.30.0/23** address space.
  - Assign the first subnet for 120 hosts to **R3** LAN1.
  - Assign the second subnet for 120 hosts to **R3** LAN2.
- Document your addressing scheme by completing the **Addressing Table**.
  - Assign the last IP address in the subnet to the appropriate **R3** interface.
  - Assign the first IP address in the subnet to the PC.
- Configure addressing for **R3**, **PC-E** and **PC-F**.
- Implement multiarea OSPF using 1 as the process ID.
  - Assign the serial links to OSPF Area 0.

- Configure the router ID as **x.x.x.x** where **x** is the number of the router. For example, the router ID for **R1** is 1.1.1.1.
- Summarize the LANs in each area and advertise them using one network statement.
  - 1) Assign the R1 LANs to OSPF Area 10.
  - 2) Assign the R2 LANs to OSPF Area 20.
  - 3) Assign the R3 LANs to OSPF Area 30.
- Prevent routing updates from being sent out LAN interfaces. Do not use the **default** argument.
- Implement default routing to the Internet.
  - Configure **R1** with a directly attached default route.
  - Advertise the default route to **R2** and **R3**.
- Configure MD5 authentication on the serial interfaces
  - Use **1** as the key.
  - Use **cisco123** as the key string.
- Limit VTY access to **R1**.
  - Configure an ACL number 1.
  - Only **PC-A** is allowed to telnet into **R1**.

```
!-----
!R1
!-----
en
conf t
!
interface Serial0/0/0
 ip ospf message-digest-key 1 md5 cisco123
!
interface Serial0/0/1
 ip ospf message-digest-key 1 md5 cisco123
!
router ospf 1
 router-id 1.1.1.1
 area 0 authentication message-digest
 passive-interface GigabitEthernet0/0
 passive-interface GigabitEthernet0/1
 network 172.31.31.248 0.0.0.3 area 0
 network 172.31.31.252 0.0.0.3 area 0
 network 172.31.24.0 0.0.3.255 area 10
 default-info orig
!
access-list 1 permit host 172.31.24.1
```

```
access-list 1 deny any
!or without the implicit deny is also acceptable
!access-list 1 permit host 172.31.24.1
!
ip route 0.0.0.0 0.0.0.0 s0/1/0
!
line vty 0 15
  access-class 1 in
!
end

!-----
!R2
!-----
!
en
conf t
!
interface Serial0/0/0
  ip ospf message-digest-key 1 md5 cisco123
!
router ospf 1
  router-id 2.2.2.2
  area 0 authentication message-digest
  passive-interface GigabitEthernet0/0
  passive-interface GigabitEthernet0/1
  network 172.31.31.248 0.0.0.3 area 0
  network 172.31.28.0 0.0.1.255 area 20
!
!
end

!-----
!R3
!-----
!
en
conf t
!
interface GigabitEthernet0/0
```

```
ip address 172.31.30.126 255.255.255.128
no shut
!
interface GigabitEthernet0/1
ip address 172.31.30.254 255.255.255.128
no shut
!
interface Serial0/0/1
ip ospf message-digest-key 1 md5 cisco123
!
router ospf 1
router-id 3.3.3.3
area 0 authentication message-digest
passive-interface GigabitEthernet0/0
passive-interface GigabitEthernet0/1
network 172.31.31.252 0.0.0.3 area 0
network 172.31.30.0 0.0.0.255 area 30
!
end
```