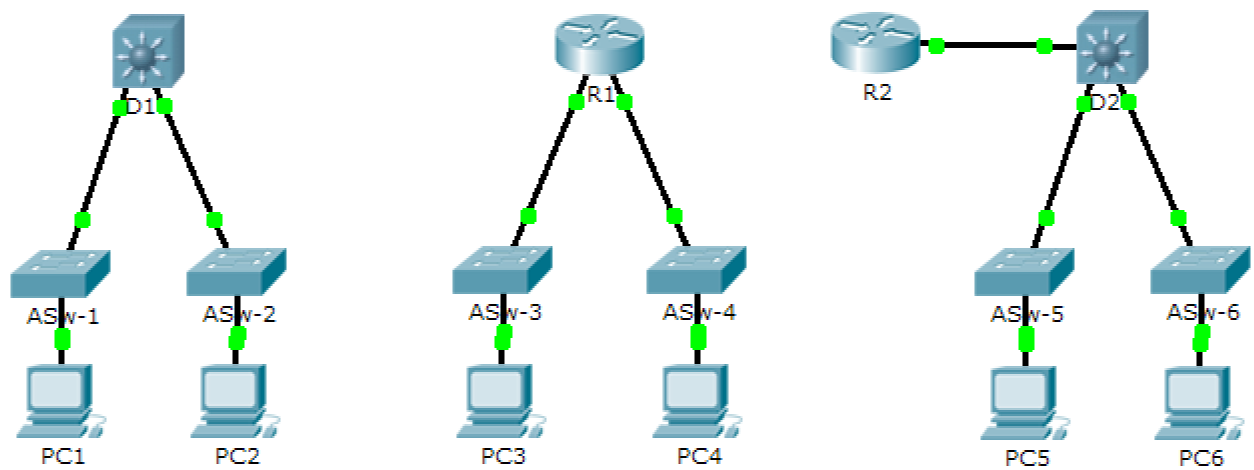
1.2.1.7 Packet Tracer - Comparing 2960 and 3560 Switches

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? _______________
- How many Fast Ethernet and Gigabit Ethernet interfaces does each switch have?

  ____
- List the transmission speed of the Fast Ethernet and Gigabit Ethernet interfaces on each switch.

  ____

  ____
- Are either of the two switches modular in design? _______________

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?

  ____

  ____

- What is the difference between a switch's physical interface and the VLAN interface?

  ____

  ____

  ____

- On which layer does a 2960 and 3560 operate?

  ____

- Which command allows a technician to assign an IP address and subnet mask to the Fast Ethernet interface on a 2960?

  ____

  ____

- Issue the **show run** command to examine the configurations of the **D1** and **ASw-1** switches. Do you notice any differences between them?

  ____

  ____

- 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**?

  ____

  ____

  ____

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?

  ____

  ____

  ____

  ____

- Issue the **show run** command and examine the configurations of R1 and D1. What differences do you see between the two?

  ____

  ____

  ____

- Which command allows D1 to configure an IP address on one of its physical interfaces?

  ____

- Use the **show ip route** command on both devices. Do you see any similarities or differences between the two tables?
- Now, analyze the routing table of R2 and D2. What is evident now that was not in the configuration of R1 and D1.

b. Verify that each topology has full connectivity be 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?

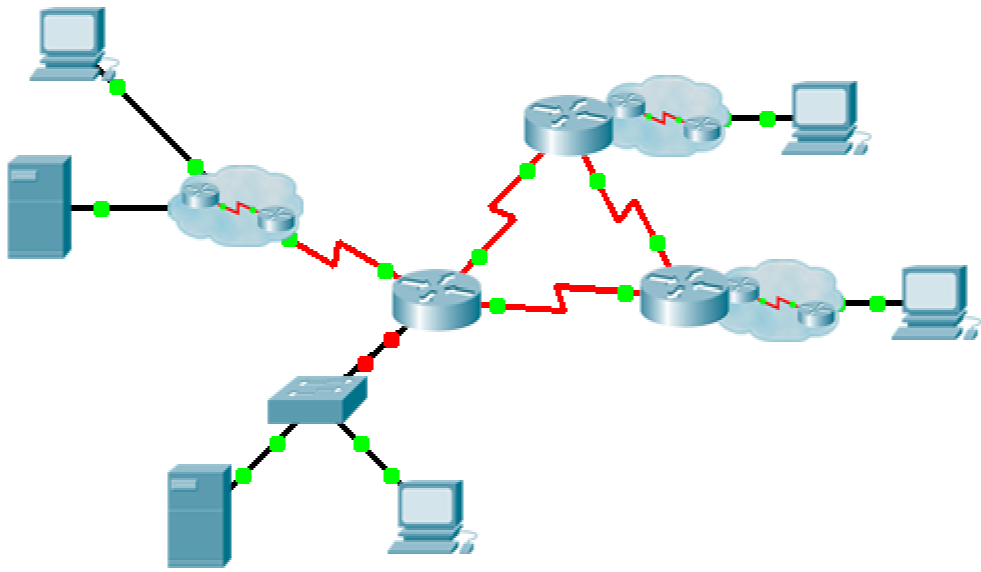
Why were we able to ping across networks without there being a router?

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**	

1.3.1.3 Packet Tracer – Skills Integration Challenge

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
	G0/0.15			N/A
	G0/0.30			N/A
	G0/0.45			N/A
	G0/0.60			N/A
	S0/0/0		255.255.255.252	N/A
	S0/0/1		255.255.255.252	N/A
	S0/1/0		255.255.255.252	N/A
	G0/0			N/A
	S0/0/0		255.255.255.252	N/A
	S0/0/1		255.255.255.252	N/A
	G0/0			N/A
	S0/0/0		255.255.255.252	N/A
	S0/0/1		255.255.255.252	N/A
	VLAN 60			
	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned

VLANs and Port Assignments Table

VLAN Number - Name	Port assignment	Network
15 - Servers	F0/11 - F0/20	
30 - PCs	F0/1 - F0/10	
45 - Native	G1/1	
60 - Management	VLAN 60	

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 ______________, ______________, and ______________ 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:

____

- Configure remote management access including IP addressing and SSH:
  - Domain is cisco.com
  - User ______________ with password ______________
  - 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.

____

- 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 ______________ 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 ______________ 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:

    ____

____

Verify ______________ has received full addressing information from ______________.

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 _______________ 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

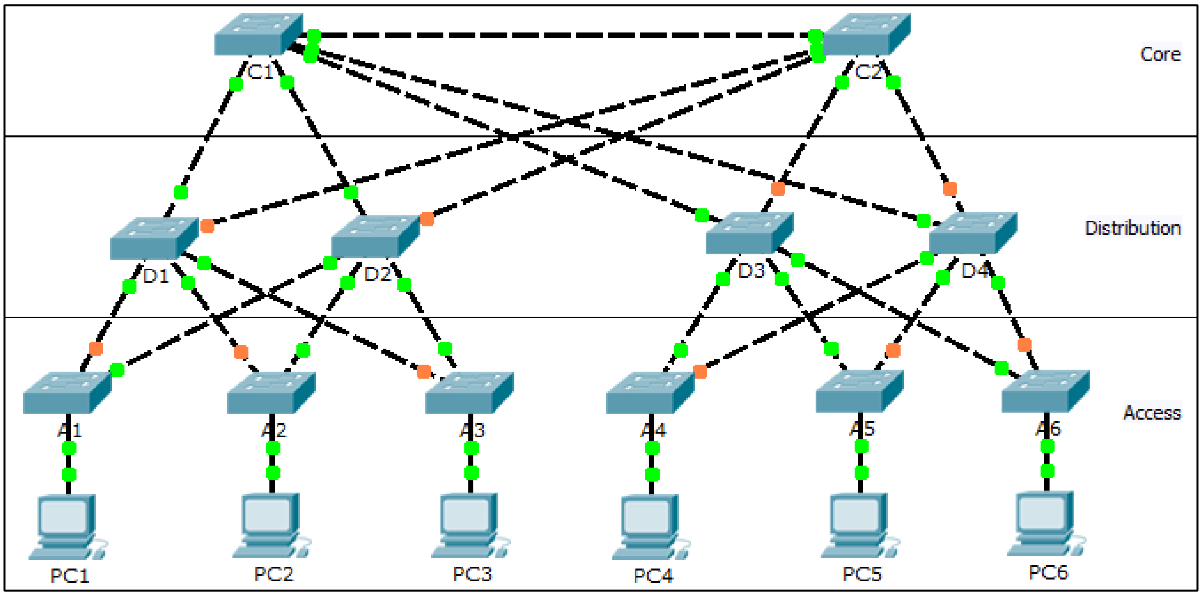
Problem	Solution

Suggested Scoring Rubric

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

2.1.1.5 Packet Tracer – Examining a Redundant Design

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.

a. 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.

b. Notice that the ARP reply from **PC6** travels back along one path. Why?

____

c. Record the loop-free path between **PC1** and **PC6**. ____

Step 3: Examine the ARP process again.

a. Below the **Scenario 0** drop-down list, click **New** to create **Scenario 1**. Examine the ARP process again by pinging between two different PCs.

b. What part of the path changed from the last set of pings? ______________________________________

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.

a. 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.

b. Record the new loop-free path. ____

Step 3: Delete link between C1 and D3.

a. 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.

b. Which link is now the active link to **C2**? ____

Step 4: Ping between PC1 and PC6.

a. Switch to **Simulation** mode and create **Scenario 3**. Ping between **PC1** and **PC6**.

b. Record the new loop-free path. ____

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.

a. Switch to **Simulation** mode and create **Scenario 4**. Ping between **PC1** and **PC6**.

b. Record the new loop-free path. ____

c. What is unique about the new path that you have not seen before?

____

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.

a. Switch to **Simulation** mode and create **Scenario 5**. Ping between **PC1** and **PC6**.

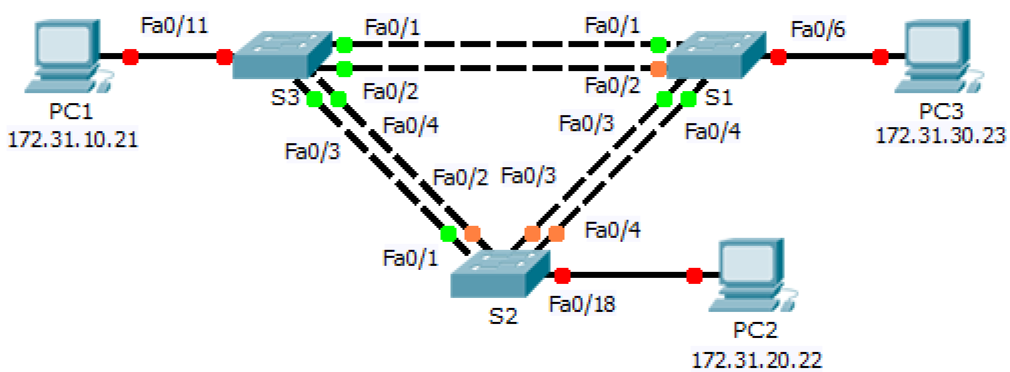
b. Record the new loop-free path. ____

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	
	Part 2 Total	**25**	
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	
	Part 3 Total	**75**	
	Total Score	**100**	

2.3.1.5 Packet Tracer – Configuring PVST+

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.

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.

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.

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.

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

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.

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.

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.

Step 2: Configure BPDU guard on the switches.

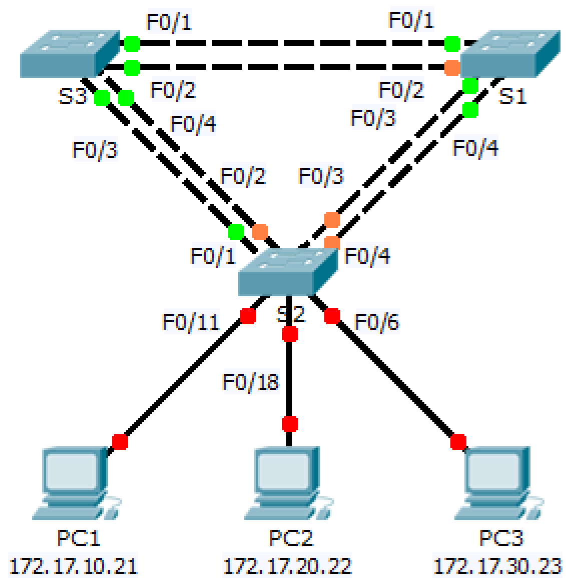
The STP PortFast BPDU guard enhancement allows network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports that have STP PortFast enabled are unable to influence the STP topology. At the reception of BPDUs, the BPDU guard operation disables 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.

Step 3: Verify your configuration.

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

2.3.2.2 Packet Tracer – Configuring Rapid PVST+

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.

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.

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.

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.

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

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.

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.

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.

Step 2: Configuring BPDU Guard on S2.

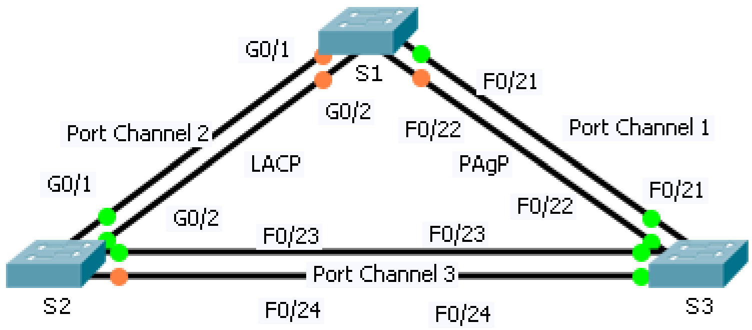
The STP PortFast BPDU Guard enhancement allows network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports that have STP PortFast enabled are not able to influence the STP topology. At the reception of BPDUs, the BPDU Guard operation disables 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.

Step 3: Verify your configuration.

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

3.2.1.3 Packet Tracer – Configuring EtherChannel

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.

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

b. 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.

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.

a. 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.

b. 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.

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.

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.

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.

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.

Step 2: Verify Port Channel 2 status.

a. 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.

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.

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.

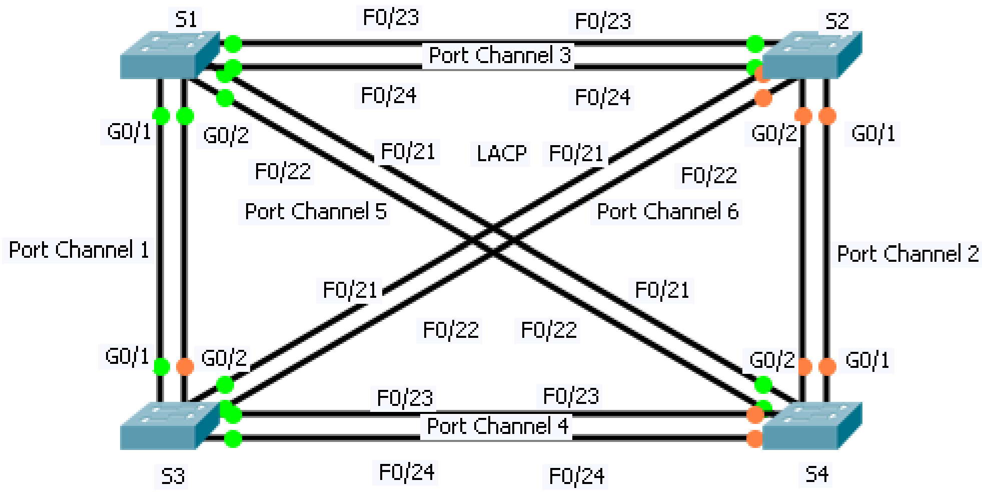
Step 2: Verify Port Channel 3 status.

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.

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**.

3.2.2.3 Packet Tracer – Troubleshooting EtherChannel

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.

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

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

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.

Step 2: Correct port channel assignments.

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

Part 3: Identify and Correct Port Channel Protocol Issues

Step 1: Identify protocol issues.

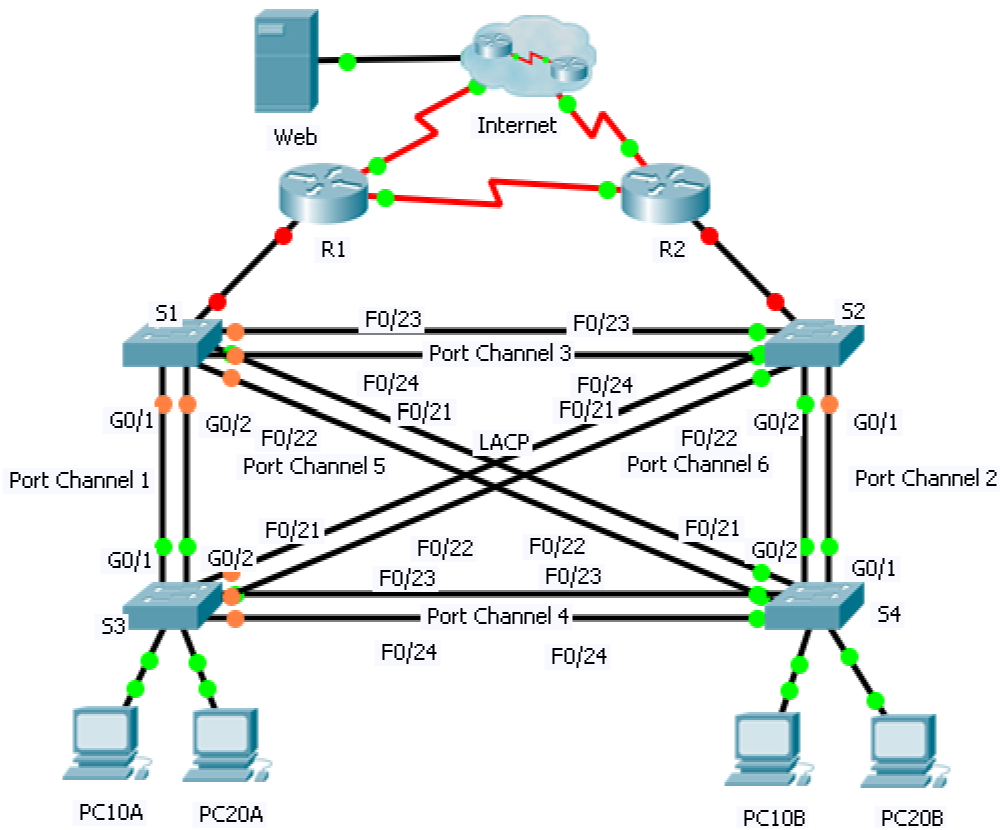
In 2000, the IEEE released 802.3ad (LACP), which is an open standard version of EtherChannel. For compatibility reasons, the network design team chose to use LACP across the network. All ports that participate in EtherChannel need to actively negotiate the link as LACP, as opposed to PAgP. Verify that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

Step 2: Correct Protocol issues.

Correct any switch ports that are not negotiating using LACP.

3.3.1.2 Packet Tracer – Skills Integration Challenge

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 – 1/2 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 – 1/2 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:

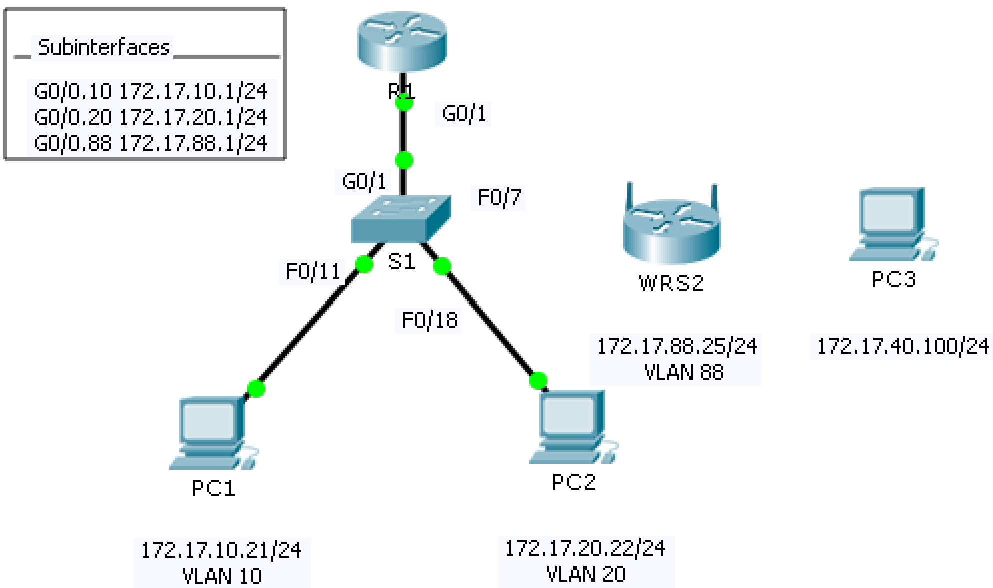
Device	VLAN 10 Priority	VLAN 20 Priority
S1	4096	8192
S2	8192	4096
S3	32768	32768
S4	32768	32768

Connectivity

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

4.4.2.2 Packet Tracer – Configuring Wireless LAN Access

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.

a. Click **WRS2 > GUI** tab.

b. Set the **Internet Connection type** to **Static IP**.

c. Configure the IP addressing according to the Addressing Table.

Step 3: Configure the network setup.

a. 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**.

b. Enable the DHCP server.

c. Scroll to the bottom of the page and click **Save Settings**.

Step 4: Configure wireless access and security.

a. At the top of the window, click **Wireless**. Set the **Network Mode** to **Wireless-N Only** and change the SSID to **WRS_LAN**.

b. Disable **SSID Broadcast** and click **Save Settings**.

c. Click the **Wireless Security** option.

d. Change the **Security Mode** from **Disabled** to **WPA2 Personal**.

e. Configure **cisco123** as the passphrase.

f. 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.

a. Click **PC3** > **Desktop** > **PC Wireless**.

b. Click the **Profiles** tab.

c. Click **New**.

d. Name the new profile **Wireless Access**.

e. On the next screen, click **Advanced Setup**. Then manually enter the SSID of **WRS_LAN** on **Wireless Network Name**. Click **Next**.

f. 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.

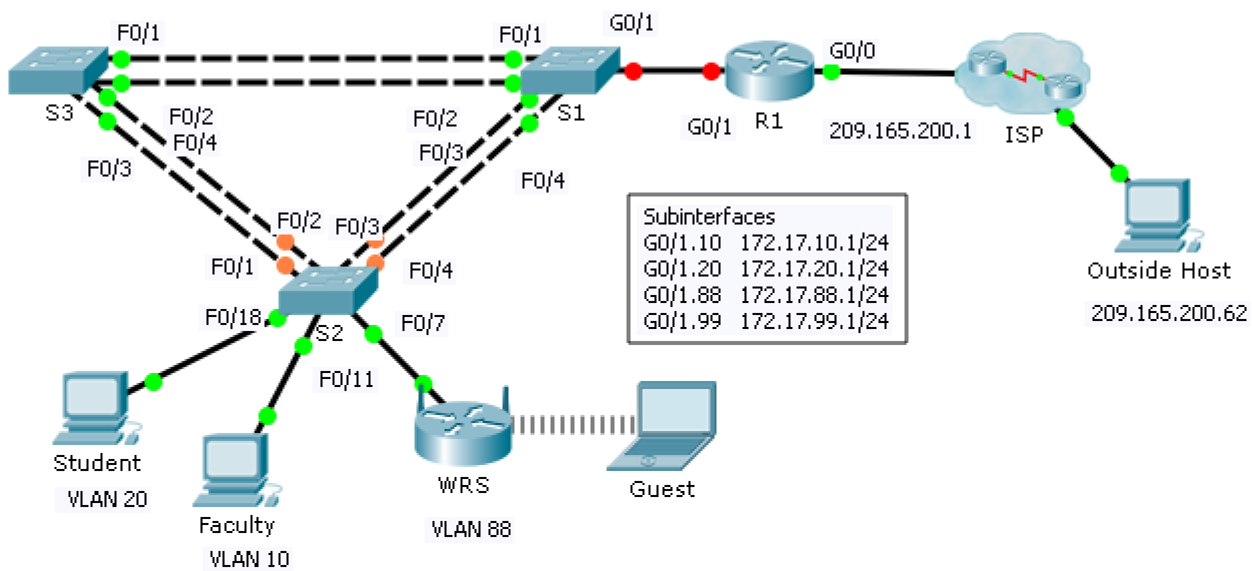
Close the **PC Wireless** configuration window.

Part 3: Verify Connectivity

All the PCs should have connectivity with one another.

4.5.1.2 Packet Tracer – Skills Integration Challenge

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

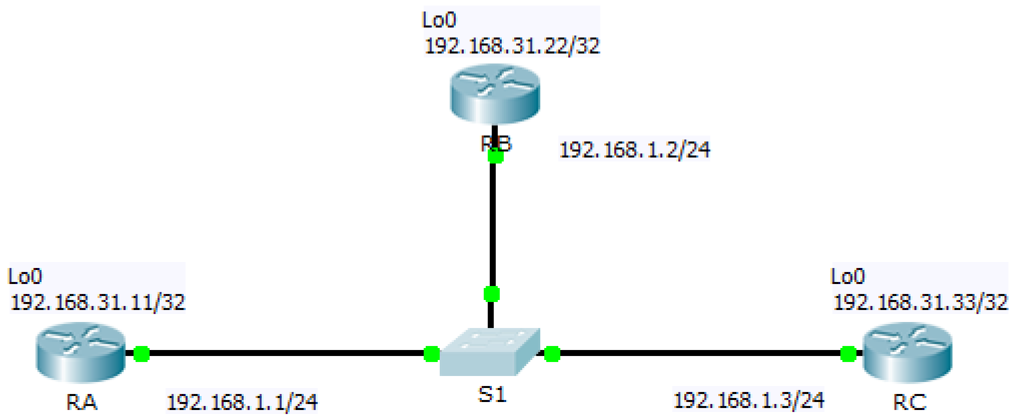
- Set **Internet Setup** to receive IP addressing from R1. You may need to go to the **Status** tab to release and renew the IP addressing. Ensure that **WRS** receives full IP addressing.
- Configure **Network Setup** according to the Addressing Table so that the guest devices receive IP addressing.
- 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.

5.1.1.12 Packet Tracer - Determining the DR and BDR

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.

a. Use the appropriate command on each router to examine the current DR and BDR.

b. Which router is the DR? ______________

c. Which router is the BDR? ______________

Step 3: Turn on IP OSPF adjacency debugging.

a. 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.

a. Disable the link between **RC** and the switch to cause roles to change.

b. 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?

____

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

a. Re-enable the link between **RC** and the switch.

b. Wait for the new DR/BDR elections to occur. Did DR and BDR roles change? Why or why not?

____

____

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

a. Disable the link between **RB** and the switch to cause roles to change.

b. 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?

____

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

a. Re-enable the link between **RB** and the switch.

b. Wait for the new DR/BDR elections to occur. Did DR and BDR roles change? Why or why not?

____

____

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.

a. 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.

b. According to output from an appropriate command, which router is now DR and which router is now BDR?

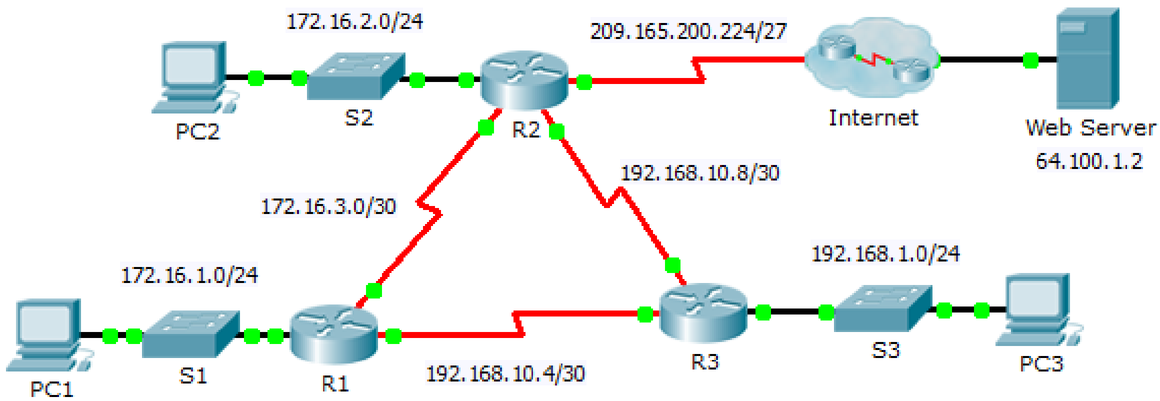
____

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	
Part 1 Total		**60**	
Part 2: Modify OSPF Priority and Force Elections	Step 3b	10	
Part 2 Total		**10**	
Packet Tracer Score		**30**	
Total Score		**100**	

5.1.3.5 Packet Tracer - Propagating a Default Route in OSPFv2

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.

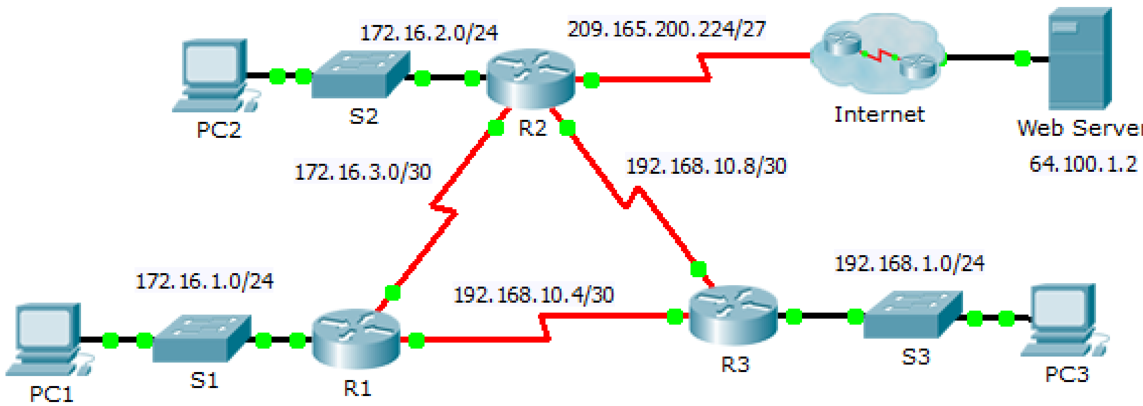
```
R1> show ip route
<output omitted>
O*E2 0.0.0.0/0 [110/1] via 172.16.3.2, 00:00:08, Serial0/0/0
!-------------------
R3> show ip route
<output omitted>
O*E2 0.0.0.0/0 [110/1] via 192.168.10.9, 00:08:15, Serial0/0/1
```

Part 2: Verify Connectivity

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

5.1.5.7 Packet Tracer - Configuring OSPF Advanced Features

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: 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.

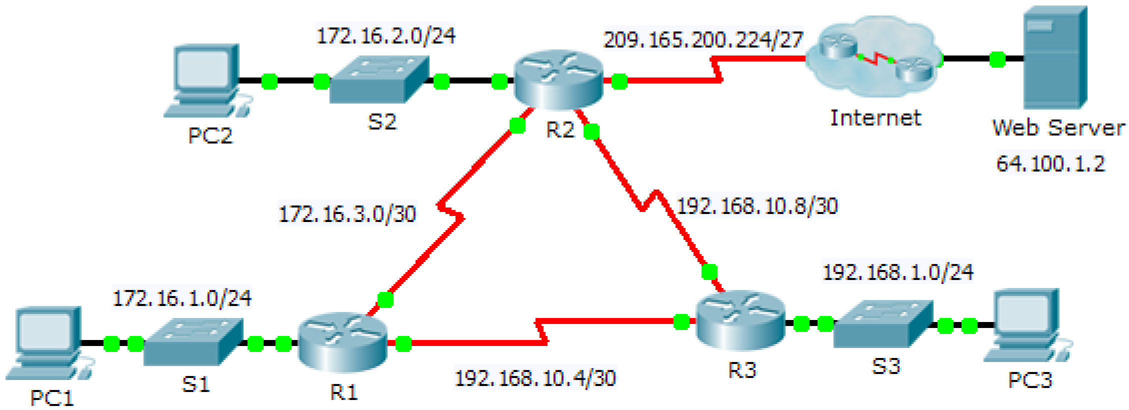
```
R1# show ip ospf interface
Message digest authentication enabled
```

Part 2: Verify Connectivity

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

5.2.2.3 Packet Tracer – Troubleshooting Single-Area OSPFv2

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
	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

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

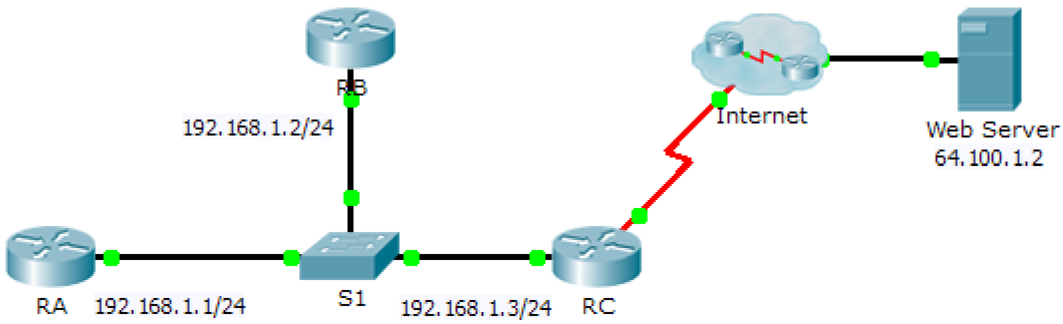
1. Use testing commands to discover connectivity problems in the network and document the problem in the Documentation Table.
2. Use verification commands to discover the source of the problem and devise an appropriate solution to implement. Document the proposed solution in the Documentation Table.
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?

5.3.1.2 Packet Tracer – Skills Integration Challenge

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

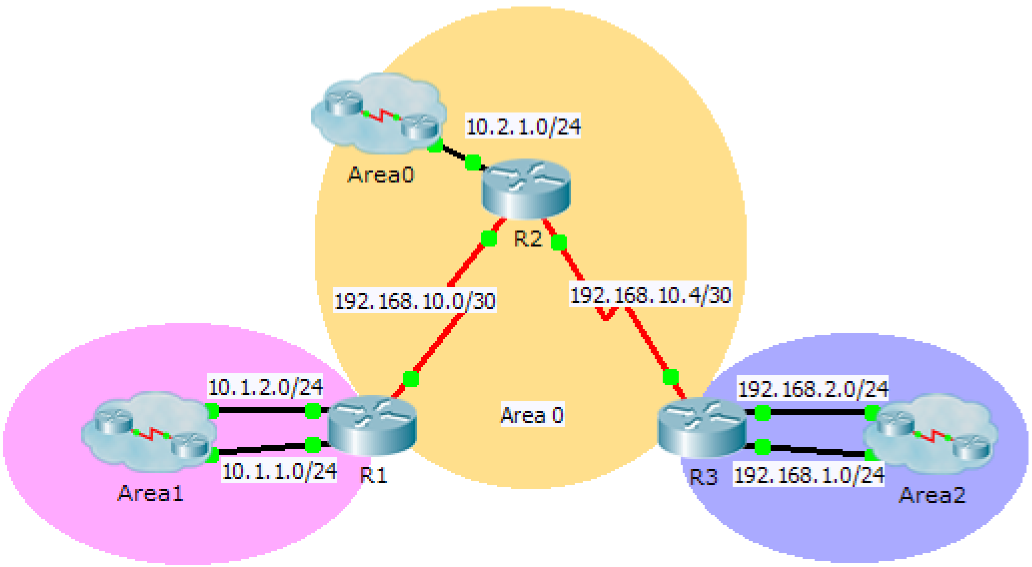
- Configure a directly attached default route to the Internet
- OSPF priority set to 50 on the LAN interface
- OSPF MD5 authentication key ID of 1 and MD5 key "cisco" on the LAN interface of **RC**
- Set the hello interval to 5
- Set the dead interval to 20

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.

6.2.3.6 Packet Tracer – Configuring Multiarea OSPFv2

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.

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.

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? ____
2. Which router(s) are backbone routers? ____
3. Which router(s) are area border routers? ____
4. Which router(s) are autonomous system routers? ____
5. Which routers are generating Type 1 LSAs? ____
6. Which routers are generating Type 2 LSAs? ____
7. Which routers are generating Type 3 LSAs? ____
8. Which routers are generating Type 4 and 5 LSAs? ____
9. How many inter area routes does each router have? ____

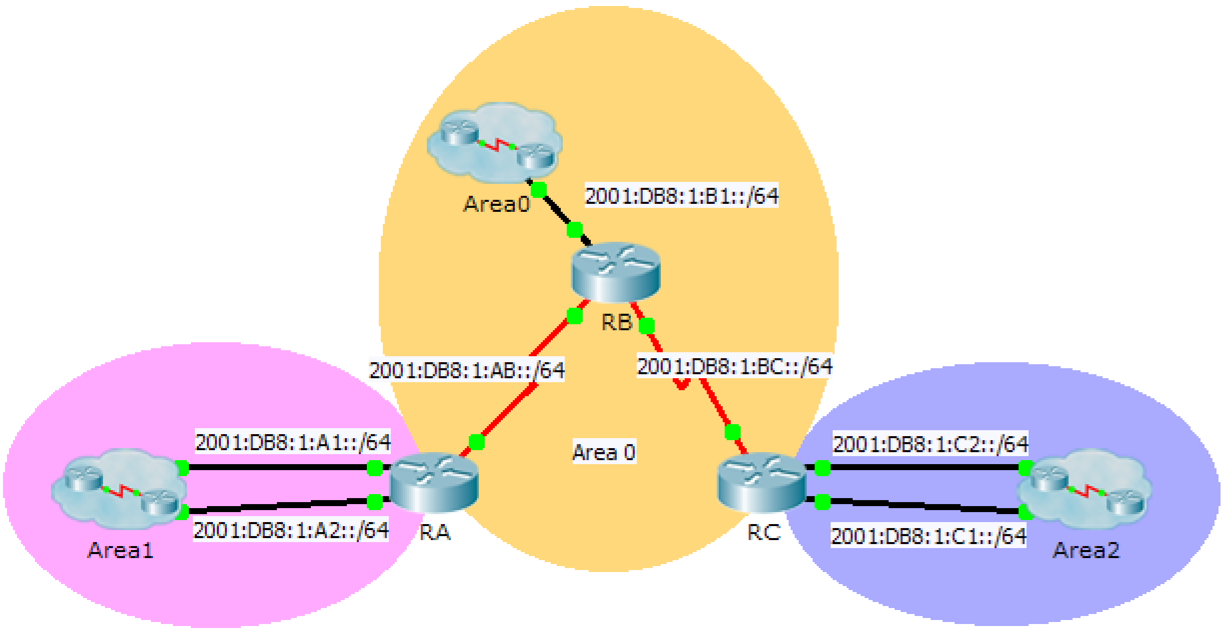
10. Why would there usually be an ASBR in this type of network? ______________________________________

Suggested Scoring Rubric

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

6.2.3.7 Packet Tracer – Configuring Multiarea OSPFv3

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.

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

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.

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.

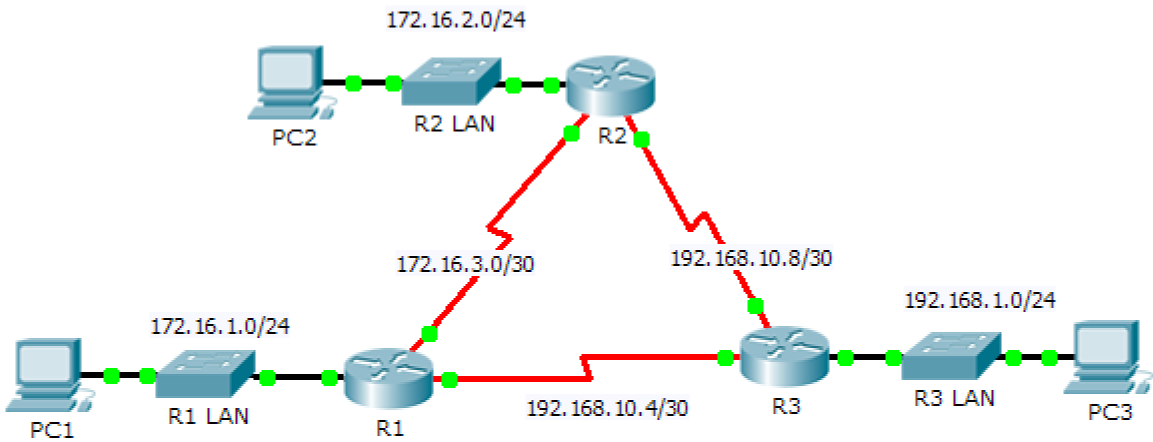
Use the following commands to gather information about your OSPFv3 multiarea implementation.

```
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.

7.2.2.4 Packet Tracer – Configuring Basic EIGRP with IPv4

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
```

What is the range of numbers that can be used for AS numbers? ______________________________

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

Step 2: Advertise directly connected networks.

a. 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?

____

b. 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
```

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
```

Step 4: Disable automatic summarization.

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

```
R1(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.

a. Which command displays the neighbors discovered by EIGRP? ______________________________

b. 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 Uptime    SRTT   RTO   Q   Seq
```



```
                                        (sec)          (ms)         Cnt  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.

a. What command displays the parameters and other information about the current state of any active IPv4 routing protocol processes configured on the router? ________________________________

b. On **R2**, enter the command you listed for 2a and answer the following questions:

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

   Where is this information located under? ________________________________

   What is the maximum hop count? __________

Step 3: Verify end-to-end connectivity

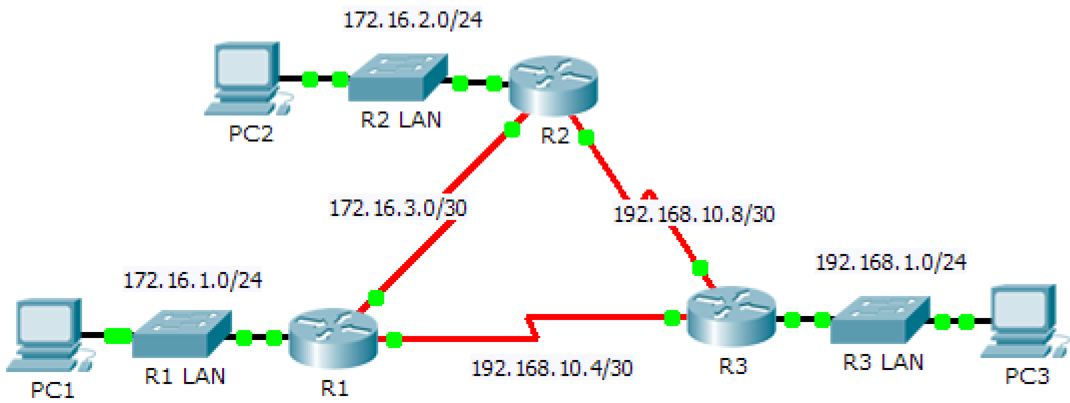
PC1, PC2 and PC3 should now be able to ping each other. If not, troubleshoot your EIGRP configurations.

Suggested Scoring Rubric

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

7.3.4.4 Packet Tracer – Investigating DUAL FSM

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? ______________________________

Are any of the routers load balancing between any network?

____

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

What command displays the neighbor table? ______________________________

How many neighbors does each router have? ______________________________

Step 3: Analyze the topology table of each router.

a. What command displays the topology table? ______________________________

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

Why are there more successor paths than networks?

____

____

b. Copy the output for **R1**'s topology table to a text editor or the space below 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? ______________________________

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?

____

____

____

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? ____

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?

____

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?

____

Step 6: Restore connectivity between R1 and R2.

a. 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.

b. 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?

____

____

How did the DUAL FSM handle the change in topology when the route to **R1** came back up?

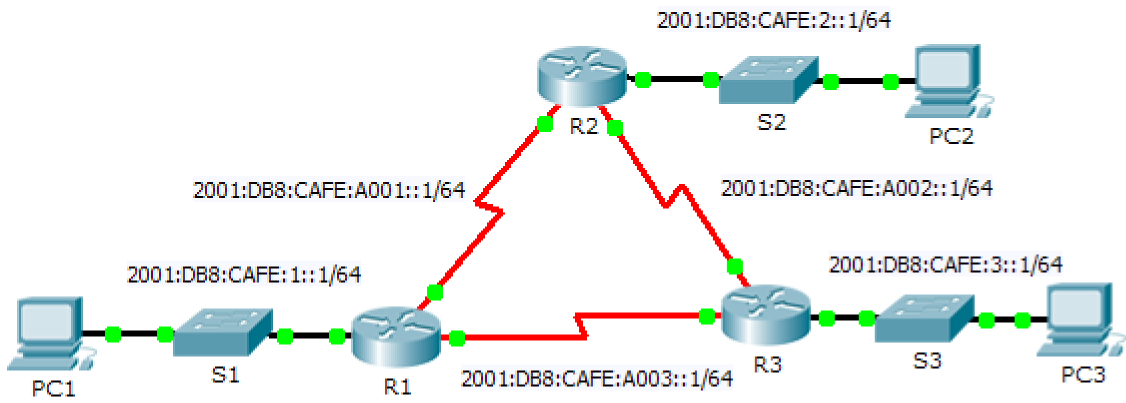
____

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	
	Part 1 Total	**36**	
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	
	Part 2 Total	**64**	
	Total Score	**100**	

7.4.3.4 Packet Tracer – Configuring Basic EIGRP with IPv6

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.

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.

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

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

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.

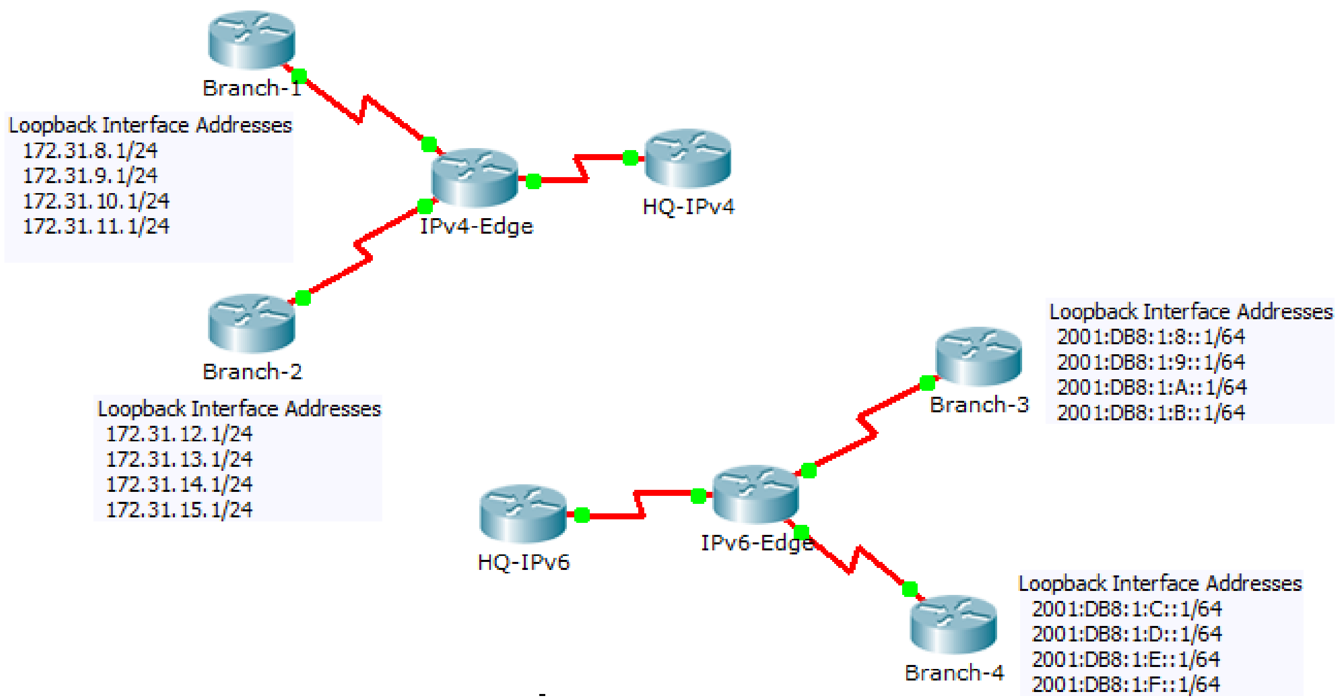
Use the command **show ipv6 protocols** to verify the configured parameter.

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.

8.1.2.5 Packet Tracer – Configuring EIGRP Manual Summary Routes for IPv4 and IPv6

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.

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

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

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

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

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

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.

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

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**.

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**.

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

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**.

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**.

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

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.

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.

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

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**.

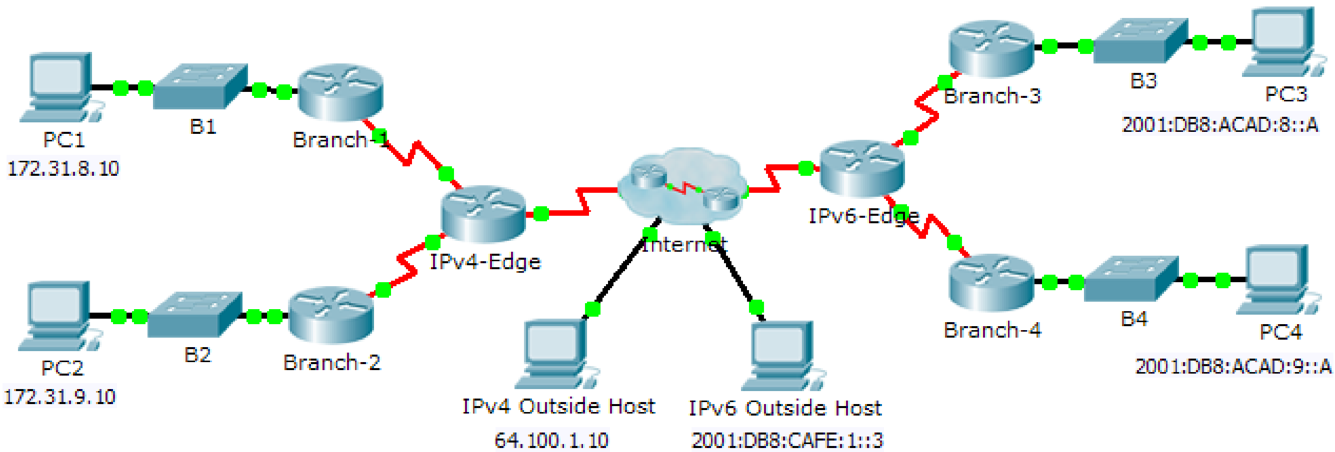
d. You should be able to ping all the IPv6 loopback interfaces from **HQ-IPv6**.

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**	

8.1.3.4 Packet Tracer – Propagating a Default Route in EIGRP for IPv4 and IPv6

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**.

Step 3: Propagate the default route in EIGRP.

Configure the EIGRP routing process to propagate the default route.

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.

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**.

Step 3: Propagate the default route in EIGRP.

Configure the EIGRP routing process to propagate the default route.

Step 4: Verify IPv6 default route is propagating.

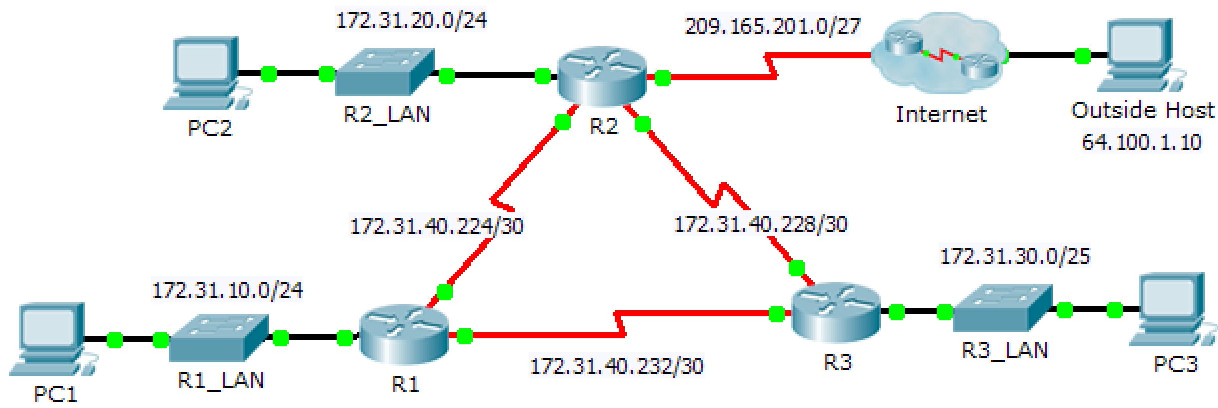
Display the routing tables for **Branch-3** and **Branch-4** to verify the default route is now installed.

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**.

8.2.3.5 Packet Tracer – Troubleshooting EIGRP for IPv4

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	172.30.20.1	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
	S0/1/0	209.165.201.1	255.255.255.224	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

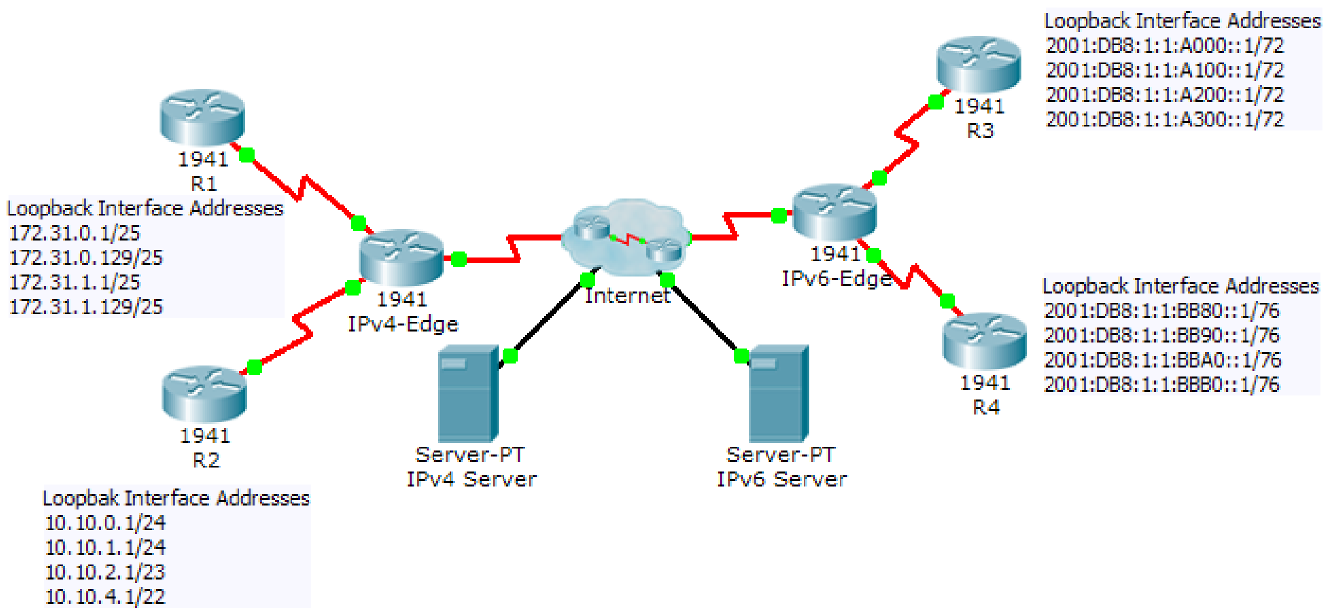
1. Use testing commands to discover connectivity problems in the network and document the problem in the Documentation Table.
2. Use verification commands to discover the source of the problem and devise an appropriate solution to implement. Document the proposed solution in the Documentation Table.
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?

8.3.1.2 Packet Tracer - Skills Integration Challenge

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.
- Configure a directly attached default route on **IPv4-Edge** and propagate it in EIGRP updates.
- Configure the serial interfaces between **R1**, **R2** and **IPv4-Edge** to send hellos every 10 seconds.
- 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:	Summary:

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

- **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**	

9.1.1.9 Packet Tracer – Decoding IOS Image Names

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						
c1841-ipbasek9-mz.124-12.bin						
c2800nm-advipservicesk9-mz.124-15.T9.bin						
c2801-ipbasek9-mz.124-25f.bin						
c2801-advsecurityk9-mz.124-18e.bin						

What do the letters “mz” in the file name tell you about the file?

____

____

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							
c1900-universalk9-mz.SPA.152-4.M2.bin							
c2900-universalk9-mz.SPA.151-4.M4.bin							
c2900-universalk9-mz.SPA.152-3.T3.bin							

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.

IOS 12.4 Image	Hardware	Feature Set	Train No.	Maintenance Release	Train Identifier	Rebuild Identifier

IOS 15 Image	Hardware	Feature Set	Major Release	Minor Release	New Feature Release	Maintenance Release	Maintenance Rebuild

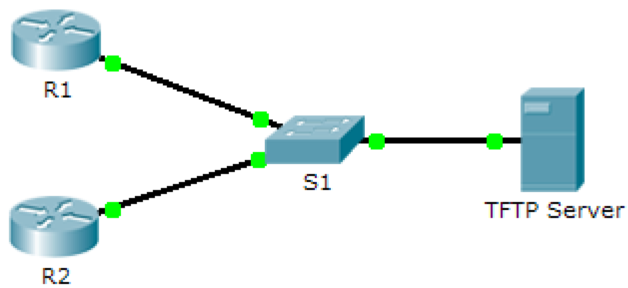
Suggested Scoring Rubric

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**	
Total Score	**100**	

Cisco Networking Academy® Mind Wide Open™

9.1.2.5 Packet Tracer – Using a TFTP Server to Upgrade a Cisco IOS Image

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.

a. Access the TFTP server and enable the TFTP service.

b. Note the IOS images that are available on the TFTP server.

Which IOS images stored on the server are compatible with 1841?

____

c. From **R1**, issue the **show flash:** command and record the available flash memory. ____________________

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:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[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:? ____

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**.

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.

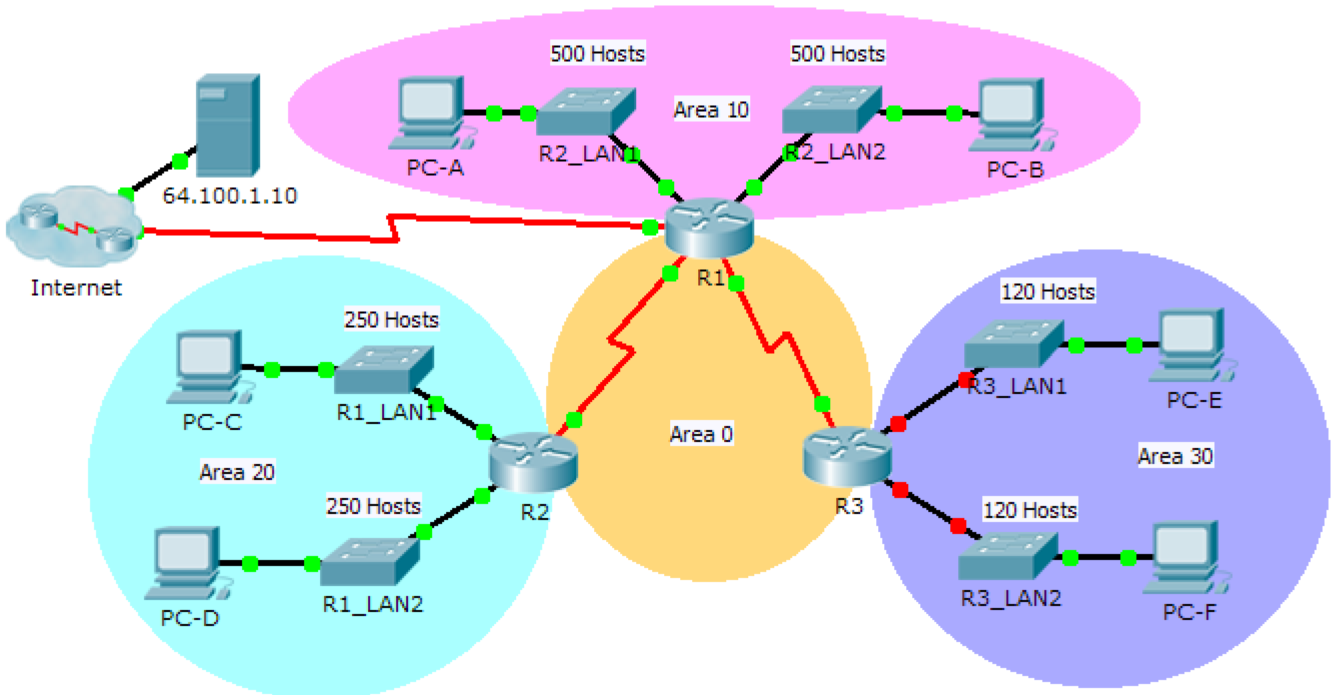
____

b. Use the **copy** command to backup the IOS image in flash memory on **R2** to a TFTP server.

c. Access the TFTP server and verify that the IOS image has been copied to the TFTP server.

9.3.1.4 Packet Tracer – Skills Integration Challenge

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			N/A
	G0/1			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			
PC-F	NIC			

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.
  1) Assign the first subnet for 120 hosts to **R3** LAN1.
  2) 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**.