1.3.1.3 Packet Tracer - Skills Integration Challenge

Topology

Note: You can use this document to record the random values (router names, addressing, etc.) that you will receive when launching the Packet Tracer activity.

Addressing Table

Device	Interface	IP Address	Subnet Mask
	VLAN 1		255.255.255.0
	VLAN 1		255.255.255.0
	NIC		255.255.255.0
	NIC		255.255.255.0

Objectives

- Configure hostnames and IP addresses on two Cisco Internetwork Operating System (IOS) switches using the command-line interface (CLI).
- Use Cisco IOS commands to specify or limit access to the device configurations.
- Use IOS commands to save the running configuration.
- Configure two host devices with IP addresses.
- Verify connectivity between the two PC end devices.

Scenario

As a recently hired LAN technician, your network manager has asked you to demonstrate your ability to configure a small LAN. Your tasks include configuring initial settings on two switches using the Cisco IOS and configuring IP address parameters on host devices to provide end-to-end connectivity. You are to use two switches and two hosts/PCs on a cabled and powered network.

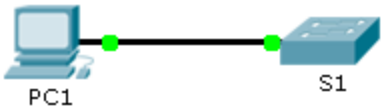
Requirements

- Use a console connection to access each switch.
- Name _____ and _____ switches.
- Use the _____ password for all lines.
- Use the _____ secret password.
- Encrypt all clear text passwords.
- Include the word **warning** in the message-of-the-day (MOTD) Banner.
- Configure addressing for all devices according to the Addressing Table.
- Save your configurations.
- Verify connectivity between all devices.

Note: Click **Check Results** to see your progress. Click **Reset Activity** to generate a new set of requirements. If you click on this before you complete the activity, all configurations will be lost.

2.2.1.4 Packet Tracer - Configuring SSH

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

Objectives

Part 1: Secure Passwords

Part 2: Encrypt Communications

Part 3: Verify SSH Implementation

Background

SSH should replace Telnet for management connections. Telnet uses insecure plain text communications. SSH provides security for remote connections by providing strong encryption of all transmitted data between devices. In this activity, you will secure a remote switch with password encryption and SSH.

Part 1: Secure Passwords

a. Using the command prompt on **PC1**, Telnet to **S1**. The user EXEC and privileged EXEC password is **cisco**.

b. Save the current configuration so that any mistakes you might make can be reversed by toggling the power for **S1**.

c. Show the current configuration and note that the passwords are in plain text. Enter the command that encrypts plain text passwords.

_____

d. Verify that the passwords are encrypted.

Part 2: Encrypt Communications

Step 1: Set the IP domain name and generate secure keys.

It is generally not safe to use Telnet, because data is transferred in plain text. Therefore, use SSH whenever it is available.

a. Configure the domain name to be **netacad.pka**.

_____

b. Secure keys are needed to encrypt the data. Generate the RSA keys using a 1024 key length.

_____

Step 2: Create an SSH user and reconfigure the VTY lines for SSH-only access.

a. Create an **administrator** user with **cisco** as the secret password.

_____

b. Configure the VTY lines to check the local username database for login credentials and to only allow SSH for remote access. Remove the existing vty line password.

_____

_____

_____

Part 3: Verify SSH Implementation

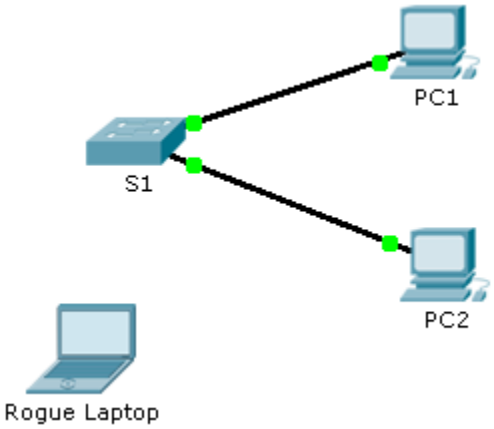
a. Exit the Telnet session and attempt to log back in using Telnet. The attempt should fail.

b. Attempt to log in using SSH. Type **ssh** and press **Enter** without any parameters to reveal the command usage instructions. Hint: The `-l` option is the letter “L”, not the number 1.

c. Upon successful login, enter privileged EXEC mode and save the configuration. If you were unable to successfully access **S1**, toggle the power and begin again at Part 1.

2.2.4.9 Packet Tracer - Configuring Switch Port Security

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0
PC2	NIC	10.10.10.11	255.255.255.0
Rogue Laptop	NIC	10.10.10.12	255.255.255.0

Objective

Part 1: Configure Port Security

Part 2: Verify Port Security

Background

In this activity, you will configure and verify port security on a switch. Port security allows you to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port.

Part 1: Configure Port Security

a. Access the command line for **S1** and enable port security on Fast Ethernet ports 0/1 and 0/2.

b. Set the maximum so that only one device can access the Fast Ethernet ports 0/1 and 0/2.

c. Secure the ports so that the MAC address of a device is dynamically learned and added to the running configuration.

d. Set the violation so that the Fast Ethernet ports 0/1 and 0/2 are not disabled when a violation occurs, but packets are dropped from an unknown source.

e. Disable all the remaining unused ports. Hint: Use the **range** keyword to apply this configuration to all the ports simultaneously.

Part 2: Verify Port Security

a. From **PC1**, ping **PC2**.

b. Verify port security is enabled and the MAC addresses of **PC1** and **PC2** were added to the running configuration.

c. Attach **Rogue Laptop** to any unused switch port and notice that the link lights are red.

d. Enable the port and verify that **Rogue Laptop** can ping **PC1** and **PC2**. After verification, shut down the port connected to **Rogue Laptop.**

e. Disconnect **PC2** and connect **Rogue Laptop** to **PC2's** port. Verify that **Rogue Laptop** is unable to ping **PC1**.

f. Display the port security violations for the port **Rogue Laptop** is connected to.

g. Disconnect **Rouge Laptop** and reconnect **PC2**. Verify **PC2** can ping **PC1**.

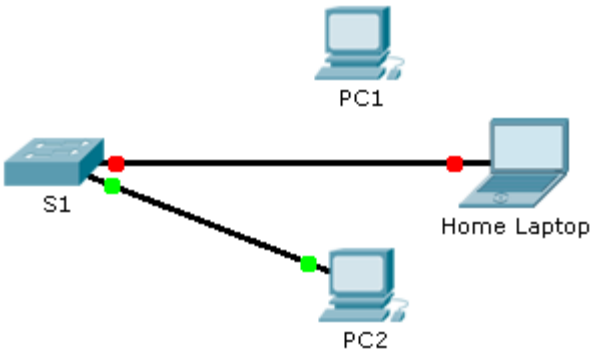
h. Why is **PC2** able to ping **PC1**, but the **Rouge Laptop** is not?

_____

_____

2.2.4.10 Packet Tracer - Troubleshooting Switch Port Security

Topology



Scenario

The employee who normally uses PC1 brought his laptop from home, disconnected PC1 and connected the laptop to the telecommunication outlet. After reminding him of the security policy that does not allow personal devices on the network, you now must reconnect PC1 and re-enable the port.

Requirements

- Disconnect **Home Laptop** and reconnect **PC1** to the appropriate port.
  - When **PC1** was reconnected to the switch port, did the port status change? _____
  - Enter the command to view the port status. What is the state of the port?

    _____
  - Which port security command enabled this feature?

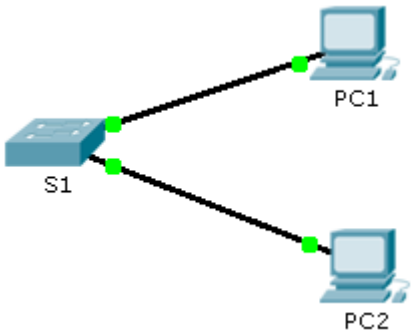
    _____
- Enable the port using the necessary command.
- Verify connectivity. **PC1** should now be able to ping **PC2**.

Suggested Scoring Rubric

Packet Tracer scores 90 points. Answers to the questions are worth 10 points.

2.3.1.2 Packet Tracer - Skills Integration Challenge

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0
PC2	NIC	10.10.10.11	255.255.255.0

Scenario

The network administrator asked you to configure a new switch. In this activity, you will use a list of requirements to configure the new switch with initial settings, SSH, and port security.

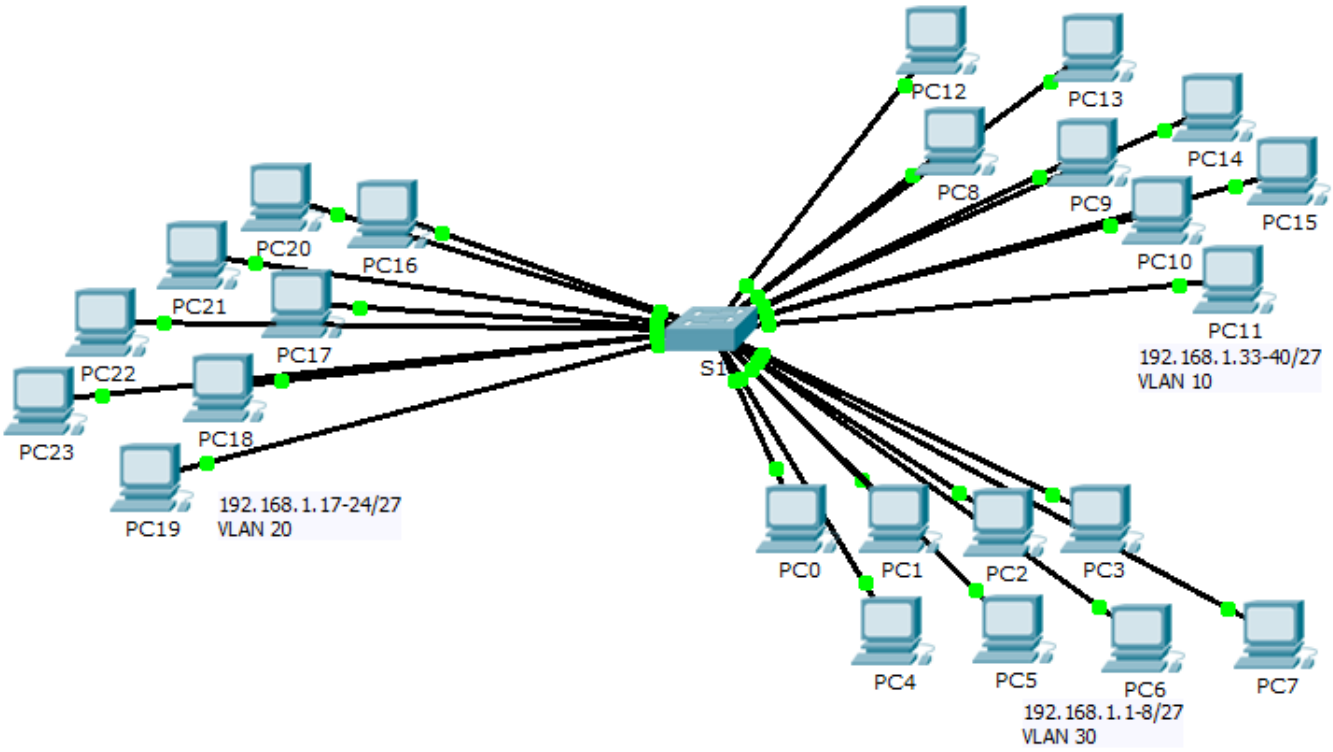
Requirements

- Configure **S1** with the following initial settings:
  - Hostname
  - Banner that includes the word **warning**
  - Console port login and password **cisco**
  - Encrypted enable password of **class**
  - Encrypt plain text passwords
  - Management interface addressing
- Configure SSH to secure remote access with the following settings:
  - Domain name of **cisco.com**
  - RSA key-pair parameters to support SSH version 2
  - Set SSH version 2
  - User **admin** with secret password **ccna**
  - VTY lines only accept SSH connections and use local login for authentication
- Configure the port security feature to restrict network access:
  - Disable all unused ports.

- Set the interface mode to access.
- Enable port security to allow only two hosts per port.
- Record the MAC address in the running configuration.
- Ensure that port violations disable ports.

3.1.1.5 Packet Tracer – Who Hears the Broadcast?

Topology



Objectives

Part 1: Observe Broadcast Traffic in a VLAN Implementation

Part 2: Complete Review Questions

Scenario

In this activity, a 24-port Catalyst 2960 switch is fully populated. All ports are in use. You will observe broadcast traffic in a VLAN implementation and answer some reflection questions.

Part 1: Observe Broadcast Traffic in a VLAN Implementation

Step 1: Use ping to generate traffic.

a. Click **PC0** and click the **Desktop** tab> **Command Prompt**.

b. Enter the **ping 192.168.1.8** command. The ping should succeed.

Unlike a LAN, a VLAN is a broadcast domain created by switches. Using Packet Tracer **Simulation** mode, ping the end devices within their own VLAN. Based on your observation, answer the questions in Step 2.

Step 2: Generate and examine broadcast traffic.

a. Switch to **Simulation** mode.

b. Click **Edit Filters** in the Simulation Panel. Uncheck the **Show All/None** checkbox. Check the **ICMP** checkbox.

c. Click the **Add Complex PDU** tool, this is the open envelope icon on the right toolbar.

d. Float the mouse cursor over the topology and the pointer changes to an envelope with a plus (+) sign.

e. Click **PC0** to serve as the source for this test message and the **Create Complex PDU** dialog window opens. Enter the following values:

- Destination IP Address: 255.255.255.255 (broadcast address)
- Sequence Number: 1
- One Shot Time: 0

Within the PDU settings, the default for **Select Application:** is PING. What are at least 3 other applications available for use?

_____

f. Click **Create PDU**. This test broadcast packet now appears in the **Simulation Panel Event List.** It also appears in the PDU List window. It is the first PDU for Scenario 0.

g. Click **Capture/Forward** twice. What happened to the packet?

_____

_____

h. Repeat this process for **PC8** and **PC16**.

Part 2: Complete Review Questions

1. If a PC in VLAN 10 sends a broadcast message, which devices receive it? _____
2. If a PC in VLAN 20 sends a broadcast message devices receive it? _____
3. If a PC in VLAN 30 sends a broadcast message devices receive it? _____
4. What happens to a frame sent from a PC in VLAN 10 to a PC in VLAN 30?

   _____
5. Which ports on the switch light up if a PC connected to port 11 sends a unicast message to a PC connected to port 13? _____
6. Which ports on the switch light if a PC connected to port 2 sends a unicast message to a PC connected to port 23? _____
7. In terms of ports, what are the collision domains on the switch?

   _____
8. In terms of ports, what are the broadcast domains on the switch?

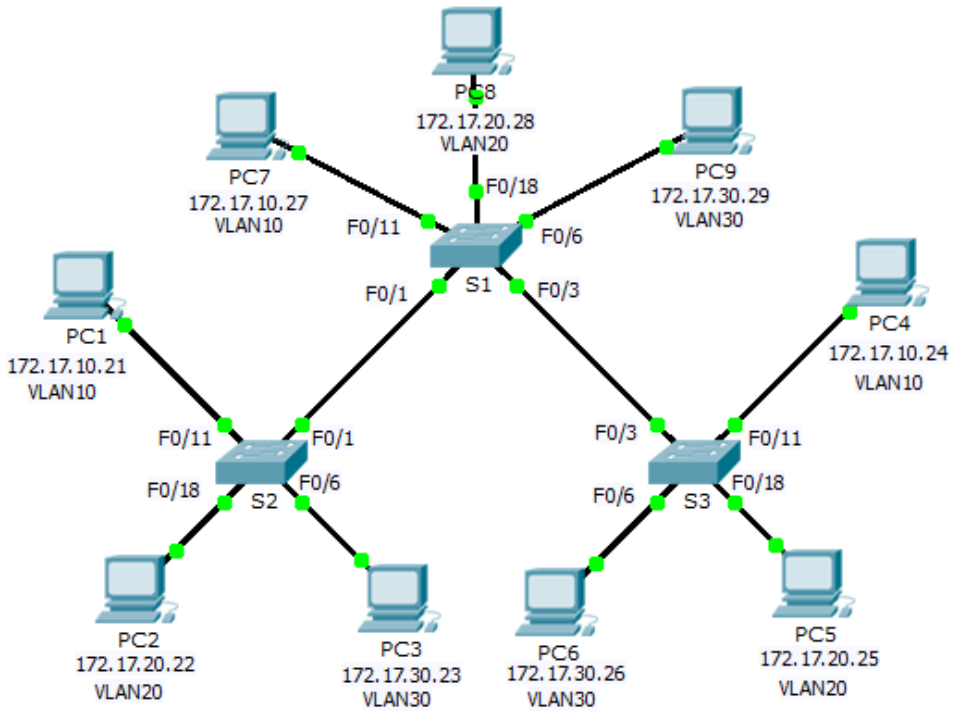
   _____

Suggested Scoring Rubric

There are 10 questions worth 10 points each.

3.1.2.7 Packet Tracer – Investigating a VLAN Implementation

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.31	255.255.255.0	N/A
S2	VLAN 99	172.17.99.32	255.255.255.0	N/A
S3	VLAN 99	172.17.99.33	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1
PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1
PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1
PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1
PC7	NIC	172.17.10.27	255.255.255.0	172.17.10.1
PC8	NIC	172.17.20.28	255.255.255.0	172.17.20.1
PC9	NIC	172.17.30.29	255.255.255.0	172.17.30.1

Objectives

Part 1: Observe Broadcast Traffic in a VLAN Implementation

Part 2: Observe Broadcast Traffic without VLANs

Part 3: Complete Reflection Questions

Background

In this activity, you will observe how broadcast traffic is forwarded by the switches when VLANs are configured and when VLANs are not configured.

Part 1: Observe Broadcast Traffic in a VLAN Implementation

Step 1: Ping from PC1 to PC6.

a. Wait for all the link lights to turn to green. To accelerate this process, click **Fast Forward Time** located in the bottom yellow tool bar.

b. Click the **Simulation** tab and use the **Add Simple PDU** tool. Click on **PC1**, and then click on **PC6**.

c. Click the **Capture/Forward** button to step through the process. Observe the ARP requests as they traverse the network. When the Buffer Full window appears, click the **View Previous Events** button.

d. Were the pings successful? Why?

_____

_____

e. Look at the Simulation Panel, where did **S3** send the packet after receiving it?

_____

In normal operation, when a switch receives a broadcast frame on one of its ports, it forwards the frame out all other ports. Notice that **S2** only sends the ARP request out Fa0/1 to **S1**. Also notice that **S3** only sends the ARP request out F0/11 to **PC4**. **PC1** and **PC4** both belong to VLAN 10. **PC6** belongs to VLAN 30. Because broadcast traffic is contained within the VLAN, **PC6** never receives the ARP request from **PC1**. Because **PC4** is not the destination, it discards the ARP request. The ping from **PC1** fails because **PC1** never receives an ARP reply.

Step 2: Ping from PC1 to PC4.

a. Click the **New** button under the Scenario 0 dropdown tab. Now click on the **Add Simple PDU** icon on the right side of Packet Tracer and ping from **PC1** to **PC4**.

b. Click the **Capture/Forward** button to step through the process. Observe the ARP requests as they traverse the network. When the Buffer Full window appears, click the **View Previous Events** button.

c. Were the pings successful? Why?

_____

_____

_____

d. Examine the Simulation Panel. When the packet reached **S1**, why does it also forward the packet to **PC7**?

_____

_____

Part 2: Observe Broadcasts Traffic without VLANs

Step 1: Clear the configurations on all three switches and delete the VLAN database.

a. Return to **Realtime** mode.

b. Delete the startup configuration on all 3 switches. What command is used to delete the startup configuration of the switches? _____

c. Where is the VLAN file stored in the switches? _____

d. Delete the VLAN file on all 3 switches. What command deletes the VLAN file stored in the switches?

_____

Step 2: Reload the switches.

Use the r**eload** command in privileged EXEC mode to reset all the switches. Wait for the entire link to turn green. To accelerate this process, click **Fast Forward Time** located in the bottom yellow tool bar.

Step 3: Click Capture/Forward to send ARP requests and pings.

a. After the switches reload and the link lights return to green, the network is ready to forward your ARP and ping traffic.

b. Select **Scenario 0** from the drop down tab to return to Scenario 0.

c. From **Simulation** mode, click the **Capture/Forward** button to step through the process. Notice that the switches now forward the ARP requests out all ports, except the port on which the ARP request was received. This default action of switches is why VLANs can improve network performance. Broadcast traffic is contained within each VLAN. When the **Buffer Full** window appears, click the **View Previous Events** button.

Part 3: Complete Reflection Questions

1. If a PC in VLAN 10 sends a broadcast message, which devices receive it?

   _____

2. If a PC in VLAN 20 sends a broadcast message, which devices receive it?

   _____

3. If a PC in VLAN 30 sends a broadcast message, which devices receive it?

   _____

4. What happens to a frame sent from a PC in VLAN 10 to a PC in VLAN 30?

   _____

5. In terms of ports, what are the collision domains on the switch?

   _____

6. In terms of ports, what are the broadcast domains on the switch?

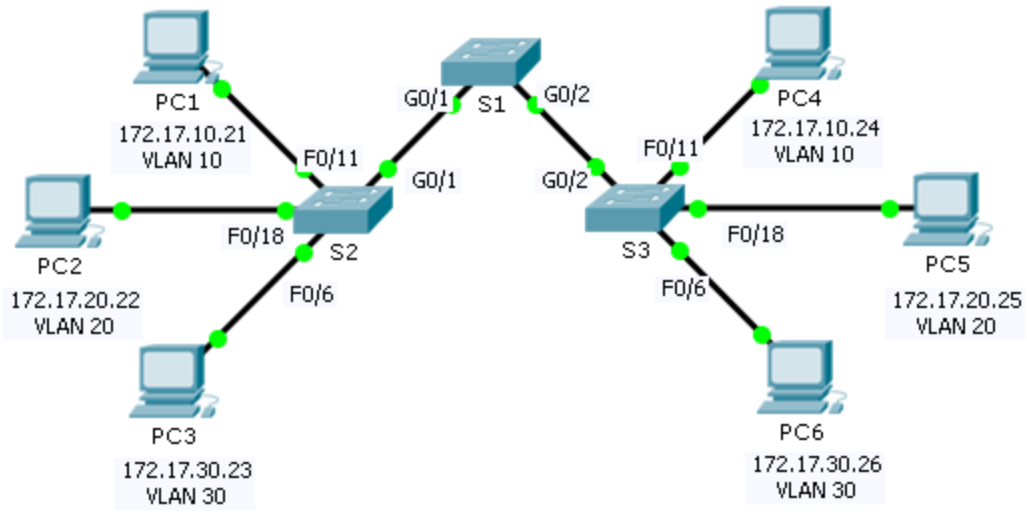
   _____

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Observe Broadcast Traffic in a VLAN Implementation	Step 1d	6	
	Step 1e	5	
	Step 2c	6	
	Step 2d	5	
	Part 1 Total	**22**	
Part 2: Observe Broadcast Traffic without VLANs	Step 1b	6	
	Step 1c	6	
	Step 1d	6	
	Part 2 Total	**18**	
Part 3: Complete Reflection Questions	1	10	
	2	10	
	3	10	
	4	10	
	5	10	
	6	10	
	Part 3 Total	**60**	
	Total Score	**100**	

3.2.1.7 Packet Tracer – Configuring VLANs

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	10
PC2	NIC	172.17.20.22	255.255.255.0	20
PC3	NIC	172.17.30.23	255.255.255.0	30
PC4	NIC	172.17.10.24	255.255.255.0	10
PC5	NIC	172.17.20.25	255.255.255.0	20
PC6	NIC	172.17.30.26	255.255.255.0	30

Objectives

Part 1: Verify the Default VLAN Configuration

Part 2: Configure VLANs

Part 3: Assign VLANs to Ports

Background

VLANs are helpful in the administration of logical groups, allowing members of a group to be easily moved, changed, or added. This activity focuses on creating and naming VLANs, and assigning access ports to specific VLANs.

Part 1: View the Default VLAN Configuration

Step 1: Display the current VLANs.

On S1, issue the command that displays all VLANs configured. By default, all interfaces are assigned to VLAN 1.

Step 2: Verify connectivity between PCs on the same network.

Notice that each PC can ping the other PC that shares the same network.

- PC1 can ping PC4
- PC2 can ping PC5
- PC3 can ping PC6

Pings to PCs in other networks fail.

What benefit will configuring VLANs provide to the current configuration?

_____

_____

Part 2: Configure VLANs

Step 1: Create and name VLANs on S1.

Create the following VLANs. Names are case-sensitive:

- VLAN 10: Faculty/Staff
- VLAN 20: Students
- VLAN 30: Guest(Default)
- VLAN 99: Management&Native

Step 2: Verify the VLAN configuration.

Which command will only display the VLAN name, status, and associated ports on a switch?

_____

Step 3: Create the VLANs on S2 and S3.

Using the same commands from Step 1, create and name the same VLANs on S2 and S3.

Step 4: Verify the VLAN configuration.

Part 3: Assign VLANs to Ports

Step 1: Assign VLANs to the active ports on S2.

Assign the VLANs to the following ports:

- VLAN 10: Fast Ethernet 0/11
- VLAN 20: Fast Ethernet 0/18
- VLAN 30: Fast Ethernet 0/6

Step 2: Assign VLANs to the active ports on S3.

S3 uses the same VLAN access port assignments as S2.

Step 3: Verify loss of connectivity.

Previously, PCs that shared the same network could ping each other successfully. Try pinging between PC1 and PC4. Although the access ports are assigned to the appropriate VLANs, were the pings successful? Why?

_____

_____

What could be done to resolve this issue?

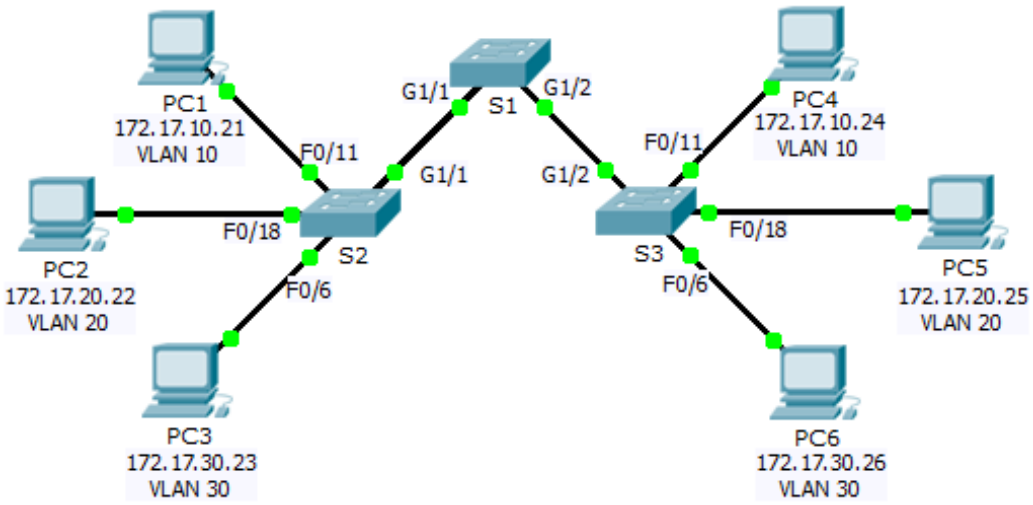
_____

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Verify the Default VLAN Configuration	Step 2	**4**	
Part 2: Configure VLANs	Step 2	**2**	
Part 3: Assign VLANs to Ports	Step 3	**4**	
	Packet Tracer Score	**90**	
	Total Score	**100**	

3.2.2.4 Packet Tracer – Configuring Trunks

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Switch Port	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	S2 F0/11	10
PC2	NIC	172.17.20.22	255.255.255.0	S2 F0/18	20
PC3	NIC	172.17.30.23	255.255.255.0	S2 F0/6	30
PC4	NIC	172.17.10.24	255.255.255.0	S3 F0/11	10
PC5	NIC	172.17.20.25	255.255.255.0	S3 F0/18	20
PC6	NIC	172.17.30.26	255.255.255.0	S3 F0/6	30

Objectives

Part 1: Verify VLANs

Part 2: Configure Trunks

Background

Trunks are required to pass VLAN information between switches. A port on a switch is either an access port or a trunk port. Access ports carry traffic from a specific VLAN assigned to the port. A trunk port by default is a member of all VLANs; therefore, it carries traffic for all VLANs. This activity focuses on creating trunk ports, and assigning them to a native VLAN other than the default.

Part 1: Verify VLANs

Step 1: Display the current VLANs.

a. On **S1**, issue the command that will display all VLANs configured. There should be 9 VLANs in total. Notice how all 26 ports on the switch are assigned to one port or another.

b. On **S2** and **S3**, display and verify all the VLANs are configure and assigned to the correct switchports according to the **Addressing Table**.

Step 2: Verify loss of connectivity between PCs on the same network.

Although **PC1** and **PC4** are on the same network, they cannot ping one another. This is because the ports connecting the switches are assigned to VLAN 1 by default. In order to provide connectivity between the PCs on the same network and VLAN, trunks must be configured.

Part 2: Configure Trunks

Step 1: Configure trunking on S1 and use VLAN 99 as the native VLAN.

a. Configure G1/1 and G1/2 interfaces on S1 for trunking.

b. Configure VLAN 99 as the native VLAN for G1/1 and G1/2 interfaces on **S1**.

The trunk port takes about a minute to become active due to Spanning Tree which you will learn in the proceeding chapters. Click **Fast Forward Time** to speed the process. After the ports become active, you will periodically receive the following syslog messages:

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/2
(99), with S3 GigabitEthernet1/2 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/1
(99), with S2 GigabitEthernet1/1 (1).
```

You configured VLAN 99 as the native VLAN on S1. However, the S2 and S3 are using VLAN 1 as the default native VLAN as indicated by the syslog message.

Although you have a native VLAN mismatch, pings between PCs on the same VLAN are now successful. Why?

_____

_____

_____

Verify trunking is enabled on S2 and S3.

On **S2** and **S3**, issue the **show interface trunk** command to confirm that DTP has successfully negotiated trunking with S1 on S2 and S3. The output also displays information about the trunk interfaces on S2 and S3.

Which active VLANs are allowed to across the trunk?

_____

Step 2: Correct the native VLAN mismatch on S2 and S3.

a. Configure VLAN 99 as the native VLAN for the appropriate interfaces on S2 and S3.

b. Issue **show interface trunk** command to verify the correct native VLAN configuration.

Step 3: Verify configurations on S2 and S3.

a. Issue the **show interface** *interface* **switchport** command to verify that the native VLAN is now 99.

b. Use the **show vlan** command to display information regarding configured VLANs. Why is port G1/1 on S2 no longer assigned to VLAN 1?

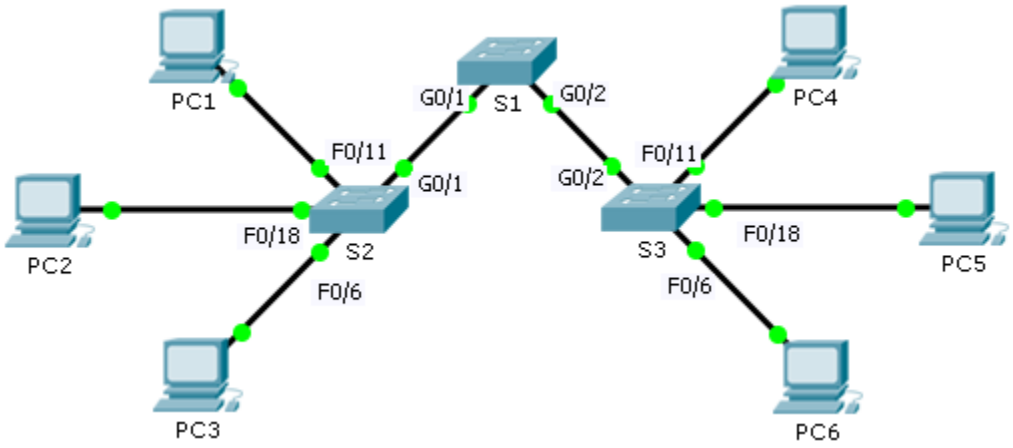
_____

Suggested Scoring Rubric

Packet Tracer scores 80 points. The three questions in Step 1, 2 and 4 are worth 20 points.

3.2.4.7 Packet Tracer - Troubleshooting a VLAN Implementation Scenario 1

Topology



Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Switch Port	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	S1 F0/11	10
PC2	NIC	172.17.20.22	255.255.255.0	S1 F0/18	20
PC3	NIC	172.17.30.23	255.255.255.0	S1 F0/6	30
PC4	NIC	172.17.10.24	255.255.255.0	S2 F0/11	10
PC5	NIC	172.17.20.25	255.255.255.0	S2 F0/18	20
PC6	NIC	172.17.30.26	255.255.255.0	S2 F0/6	30

Objectives

Part 1: Test Connectivity between PCs on the Same VLAN

Part 2: Investigate Connectivity Problems by Gathering Data

Part 3: Implement the Solution and Test Connectivity

Scenario

In this activity, you will troubleshoot connectivity problems between PCs on the same VLAN. The activity is complete when PCs on the same VLAN can ping each other. Any solution you implement must conform to the Addressing Table.

Part 1: Test Connectivity between PCs on the Same VLAN

From the command prompt on each PC, ping between PCs on the same VLAN.

a. Can PC1 ping PC4? _____

b. Can PC2 ping PC5? _____

c. Can PC3 ping PC6? _____

Part 2: Investigate Connectivity Problems by Gathering Data

Step 1: Verify configuration on the PCs.

Verify if the following configurations for each PC is correct.

- IP address
- Subnet mask

Step 2: Verify the configuration on the switches.

Verify if the following configurations on the switches are correct.

- Ports assigned to the correct VLANs.
- Ports configured for the correct mode.
- Ports connected to the correct devices.

Step 3: Document the problem and the solutions.

List the problems and the solutions that will allow these PCs to ping each other. Keep in mind that there could be more than one problem or more than one solution.

PC1 to PC4

a. Explain the connectivity issues between PC1 and PC4.

_____

b. Record the necessary actions to correct the issues.

_____

_____

PC2 to PC5

c. Explain the connectivity issues between PC2 and PC5.

_____

d. Record the necessary actions to correct the issues.

_____

_____

PC3 to PC6

e. What are the reasons why connectivity failed between the PCs?

_____

_____

f. Record the necessary actions to correct the issues.

_____

_____

Part 3: Implement the Solution and Test Connectivity

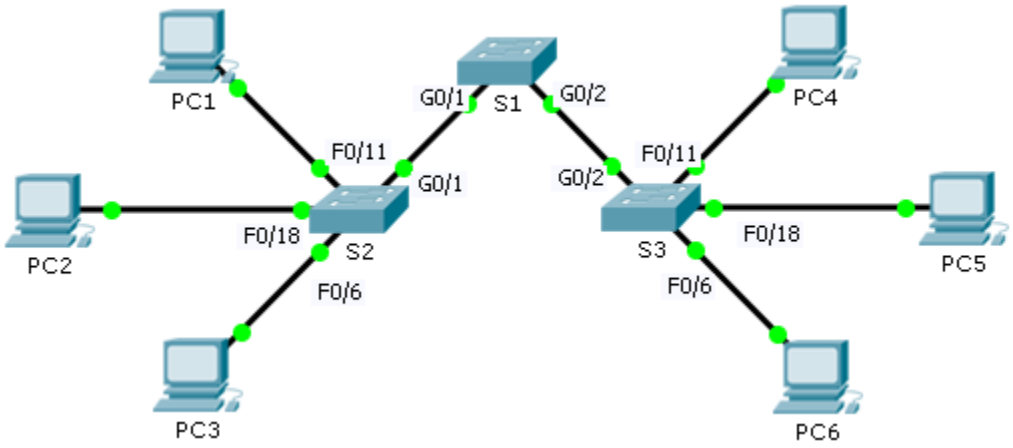
Verify PCs on the same VLAN can now ping each other. If not, continue to troubleshoot.

Suggested Scoring Rubric

Packet Tracer scores 70 points. Documentation in Part 2, Step 3 is worth 30 points.

3.2.4.8 Packet Tracer – Troubleshooting a VLAN Implementation Scenario 2

Topology



Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
S1	VLAN 56	192.168.56.11	255.255.255.0	N/A
S2	VLAN 56	192.168.56.12	255.255.255.0	N/A
S3	VLAN 56	192.168.56.13	255.255.255.0	N/A
PC1	NIC	192.168.10.21	255.255.255.0	192.168.10.1
PC2	NIC	192.168.20.22	255.255.255.0	192.168.20.1
PC3	NIC	192.168.30.23	255.255.255.0	192.168.30.1
PC4	NIC	192.168.10.24	255.255.255.0	192.168.10.1
PC5	NIC	192.168.20.25	255.255.255.0	192.168.20.1
PC6	NIC	192.168.30.26	255.255.255.0	192.168.30.1

VLAN and Port Assignments

Ports	VLAN Number - Name	Network
F0/1 – F0/5	VLAN 56 – Management&Native	192.168.56.0/24
F0/6 – F0/10	VLAN 30 – Guest(Default)	192.168.30.0/24
F0/11 – F0/17	VLAN 10 – Faculty/Staff	192.168.10.0/24
F0/18 – F0/24	VLAN 20 – Students	192.168.20.0/24

Objectives

Part 1: Find and Correct the Network Errors

Part 2: Document the Corrections to the Network

Part 3: Implement Solutions and Test Connectivity

Background

In this activity, you will troubleshoot a misconfigured VLAN environment. The initial network has errors. Your objective is to locate and correct the errors in the configurations and establish end-to-end connectivity. Your final configuration should match the Topology diagram and Addressing Table. The native VLAN for this topology is VLAN 56.

Part 1: Discover and Document Issues in the Network

Use the Topology, Addressing Table, VLAN and Port Assignments table and your knowledge of VLANs and trunking to discover issues in the network. Complete the **Documentation** table listing the problems you discovered and potential solutions.

Documentation

Problems	Solutions

Part 2: Implement the Solution and Test Connectivity

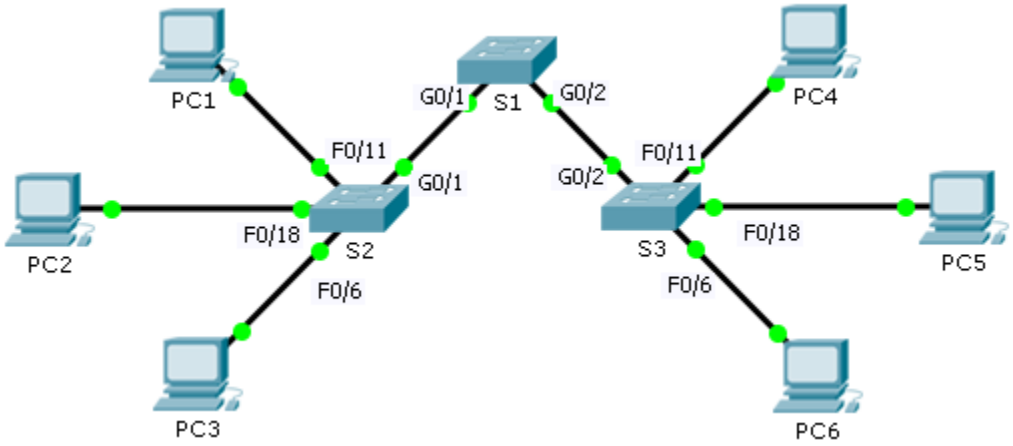
Verify PCs on the same VLAN can now ping each other. If not, continue to troubleshoot.

Suggested Scoring Rubric

Packet Tracer scores 70 points. Documentation in Part 2, Step 3 is worth 30 points.

3.4.1.2 Packet Tracer – Skills Integration Challenge

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 88	172.31.88.2	255.255.255.0	172.31.88.1
S2	VLAN 88	172.31.88.3	255.255.255.0	172.31.88.1
S3	VLAN 88	172.31.88.4	255.255.255.0	172.31.88.1
PC1	NIC	172.31.10.21	255.255.255.0	172.31.10.1
PC2	NIC	172.31.20.22	255.255.255.0	172.31.20.1
PC3	NIC	172.31.30.23	255.255.255.0	172.31.30.1
PC4	NIC	172.31.10.24	255.255.255.0	172.31.10.1
PC5	NIC	172.31.20.25	255.255.255.0	172.31.20.1
PC6	NIC	172.31.30.26	255.255.255.0	172.31.30.1

VLANs and Port Assignment Table

Ports	Assignment	Network
F0/7 - 12	VLAN 10 - Sales	172.31.10.0/24
F0/13 -20	VLAN 20 - Production	172.31.20.0/24
F0/1 - 6	VLAN 30 - Marketing	172.31.30.0/24
Interface VLAN 88	VLAN 88 - Management	172.31.88.0/24
Trunks	VLAN 99 - Native	N/A

Scenario

In this activity, two switches are completely configured. On a third switch, you are responsible for assigning IP addressing to the Switch Virtual Interface, configuring VLANs, assigning VLANs to interfaces, configuring trunking, and performing basic switch security.

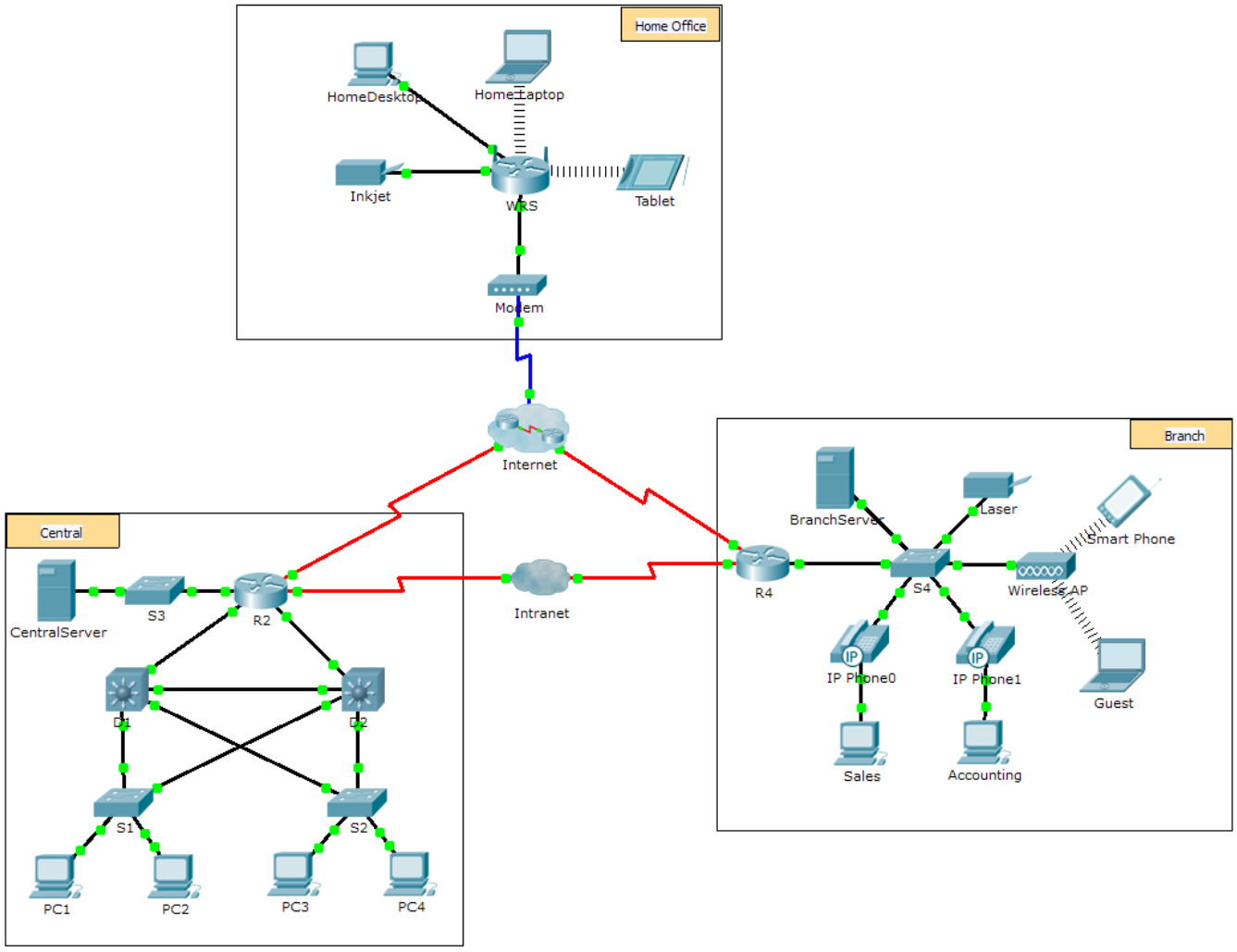
Requirements

S1 and **S2** are fully configured. You cannot access these switches. You are responsible for configuring **S3** with the following requirements:

- IP addressing and default gateway configuration, according to the **Addressing Table**.
- Create, name, and assign VLANs according to the **VLANs and Port Assignment Table**.
- Assign the native VLAN 99 to the trunk port and disable DTP.
- Restrict the trunk to only allow VLANs 10, 20, 30, 88, and 99.
- Use VLAN 99 as the native VLAN on the trunk ports.
- Configure basic switch security on S3.
  - Encrypted secret password of **itsasecret**
  - Console password of **letmein**
  - VTY password of **c1$c0** (where 0 is the number zero)
  - Encrypted plain text passwords
  - MOTD banner with the message **Authorized Access Only!!**
  - Disable unused ports.
- Configure port security on **F0/6**.
  - Only two unique devices are allowed to access the port.
  - Learned MACs are added to the running configuration.
  - Secure the interface so that a notification is sent when there is a violation, but the port is not disabled.
- Verify the PCs in the same VLAN can now ping each other.

4.1.1.8 Packet Tracer - Using Traceroute to Discover the Network

Topology



Scenario

The company you work for has acquired a new branch location. You asked for a topology map of the new location, but apparently one does not exist. However, you have username and password information for the new branch's networking devices and you know the web address for the new branch's server. Therefore, you will verify connectivity and use the **tracert** command to determine the path to the location. You will connect to the edge router of the new location to determine the devices and networks attached. As a part of this process, you will use various show commands to gather the necessary information to finish documenting the IP addressing scheme and create a diagram of the topology.

Note: The user EXEC password is **cisco**. The privileged EXEC password is **class**.

Trace and Document a Remote Location

Note: As you complete the following steps, copy command output into a text file for easy reference and record the missing information in the **Addressing Scheme Documentation** table.

Refer to the **Hints** page for a review of the commands used. In Packet Tracer, click the right arrow (>) on the bottom right side of the instruction window. If you have a printed version of the instructions, the **Hints** page is the last page.

a. Click **Sales** and the **Desktop** tab > **Command Prompt**. Use the **ipconfig** command to check the IP address configuration for **Sales**.

b. The new server web address is **b2server.pt.pka.** Enter the following **nslookup** command to discover the IP address for **b2server**:

```
PC> nslookup b2server.pt.pka
```

What address did the command return for **b2server**? _____

c. Enter the **tracert** command to determine the path from **Sales** to **b2server.pt.pka**.

```
PC> tracert b2server.pt.pka
```

d. Telnet to the first IP address in the **tracert** output and log in.

```
PC> telnet 172.16.0.1
```

e. You are connected to the **R4** router. Issue the **traceroute** command on the router using the address for b2server determined in step b. What is different about the **traceroute** command on the router compared to **tracert** on the PC?

_____

_____

What is the significance of **R4** to **Sales**?

_____

f. Use the **show ip interface brief** command to display the status of the interfaces on **R4**. Based on the output of the command, which interface is used to reach the next device in the list output from the **tracert** command?

_____

Hint: Use **show running-config** to view the subnet mask values for the interfaces.

g. Telnet to the second IP address in the **tracert** list and log in. You can use the number in the far left column of the **tracert** output to track where you are in the list. What is the name of the device to which you are connected? _____

h. Issue the **show ip route** command and study the output. Referring to the list of codes at the beginning of the output, what are the different types of routes displayed in the routing table?

_____

i. Based on the **show ip route** command output, which interface is the exit interface for the next IP address listed in your original **tracert** output? _____

j. Telnet to the third IP address in the **tracert** list and log in. What is the hostname of the current device?

_____

Issue the **show ip route connected** command. What networks are connected directly to this router?

_____

Refer to the **Addressing Scheme Documentation** table. Which interfaces connect the devices between trace route 2 and trace route 3?

_____

k. Telnet to the fourth IP address in the **tracert** list and log in. What is the name of the device?

_____

l. Issue a command to determine to what interface **b2server.pt.pka** is connected

_____

m. If you have used the **Addressing Scheme Documentation** table as you completed the previous steps, the table should now be complete. If not, finish the table now.

n. With a complete documentation of the addressing scheme and knowledge of the path from **Sales** to **branch2.pt.pka**, you should be able to now draw the new branch location in the **Topology Documentation** space below.

Addressing Scheme Documentation

Trace Route ID	Device	Interface	Address	Subnet Mask
-	Sales	NIC	172.16.0.x (DHCP)	255.255.255.0
1				
		S0/0/1.1	64.100.200.1	255.255.255.252
2				
		G0/1	64.104.223.1	255.255.255.252
		S0/0/0	64.100.100.2	
3				
		G0/2		255.255.255.0
		F0/1	128.107.46.1	
4		G0/0		
5	b2server.pt.pka	NIC	128.107.64.254	255.255.255.0

Topology Documentation

Use the space below to draw the topology for the new branch location.

Suggested Scoring Rubric

Activity Section	Possible Points	Earned Points
Questions (2 points each)	20	
Addressing Scheme Documentation	60	
Topology Documentation	20	
Total Point	**100**	

Hints - Command Summary Reference

DOS Commands

ipconfig - The output of the default command contains the IP address, network mask and gateway for all physical and virtual network adapters.

ipconfig /all - This option displays the same IP addressing information for each adapter as the default option. Additionally, it displays DNS and WINS settings for each adapter.

Nslookup - Displays information that you can use to diagnose Domain Name System (DNS) infrastructure.

Syntax:

nslookup dns.name

Tracert - Determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination with incrementally increasing Time to Live (TTL) field values. The path displayed is the list of near-side router interfaces of the routers in the path between a source host and a destination. The near-side interface is the interface of the router that is closest to the sending host in the path. Used without parameters, tracert displays help.

Syntax:

tracert [TargetName/IP Address]

IOS Commands

show ip interface – Displays the IP interface status and configuration

show ip interface brief – Displays a brief summary of IP status and configuration

show ip route – Displays the full IP routing table

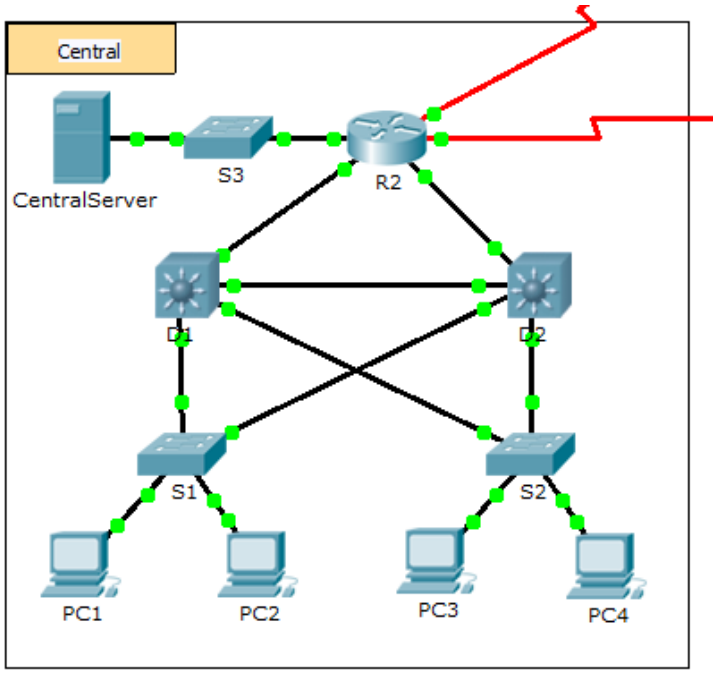
show ip route connected – Displays a list of active directly connected networks

show running-config – Displays the current operating configuration

traceroute – Trace route to destination

4.1.2.9 Packet Tracer - Documenting the Network

Topology



Background

In this activity, your job is to document the addressing scheme and connections used in the Central portion of the network. You must use a variety of commands to gather the required information.

Note: The user EXEC password is **cisco**. The privileged EXEC password is **class**.

Requirements

- Access the command line of the various devices in Central.
- Use commands to gather the information required in the **Addressing Scheme and Device Connection Documentation** table.
- If you do not remember the necessary commands, you can use the IOS built-in help system.
- If you still need additional hints, refer to the **Hints** page. In Packet Tracer, click the right arrow (>) on the bottom right side of the instruction window. If you have a printed version of the instructions, the **Hints** page is the last page.

Addressing Scheme and Device Connection Documentation

Device Name	Interface	Address	Subnet Mask	Connecting Device	
				Device Name	Interface
R2	G0/0				
	G0/1				
	G0/2				
	S0/0/0	64.100.100.1	255.255.255.252	Internet	N/A
	S0/0/1.1	64.100.200.2	255.255.255.252	Intranet	N/A
S3	VLAN 1	10.10.10.254	255.255.255.0	N/A	N/A
	F0/1	N/A	N/A	CentralServer	NIC
	G0/1	N/A	N/A		
CentralServer	NIC				
D1	VLAN2	10.2.0.1	255.255.255.0	N/A	N/A
	G0/1				
	G0/2				
	F0/23	N/A	N/A		
	F0/24	N/A	N/A		
S1	VLAN 2	10.2.0.2	255.255.255.0	N/A	N/A
	F0/23	N/A	N/A		
	G0/1	N/A	N/A		
D2	F0/23	N/A	N/A	S1	F0/23
	F0/24				
	G0/1				
	G0/2				
S2	VLAN 1	10.3.0.2	255.255.255.0	N/A	N/A
	F0/23	N/A	N/A		
	G0/1	N/A	N/A		

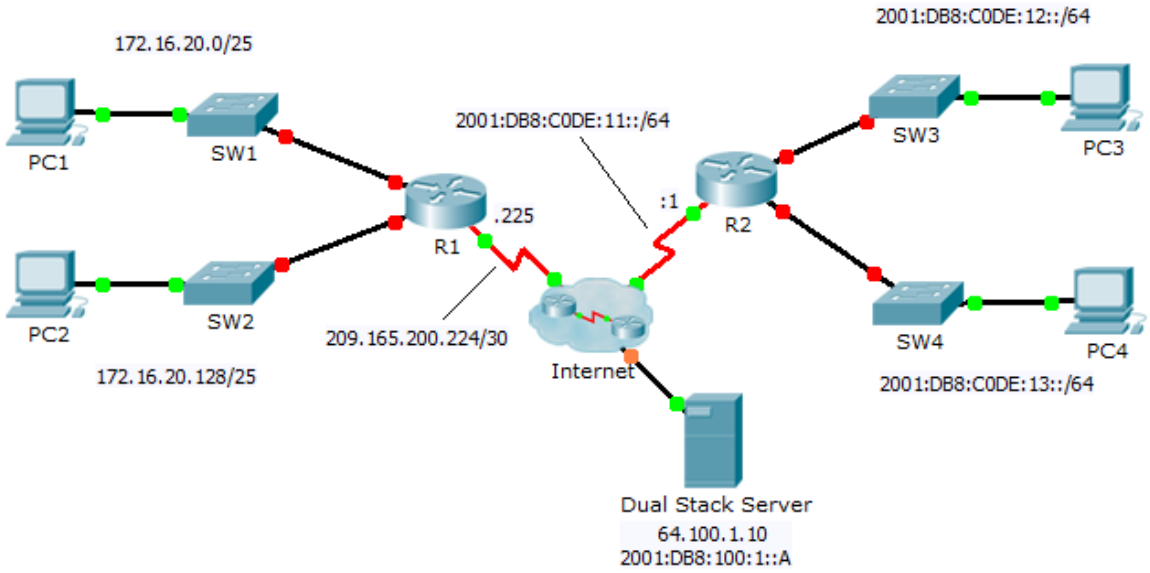
Hints

Use the following commands to gather the information you need to document the network:

```
show ip interface brief
show interfaces
show running-config
ipconfig
```

4.1.3.5 Packet Tracer - Configuring IPv4 and IPv6 Interfaces

Topology



Addressing Table

Device	Interface	IPv4 Address / IPv6 Address/Prefix	Subnet Mask	Default Gateway
R1	G0/0	172.16.20.1	255.255.255.128	N/A
	G0/1	172.16.20.129	255.255.255.128	N/A
	S0/0/0	209.165.200.225	255.255.255.252	N/A
PC1	NIC	172.16.20.10	255.255.255.128	172.16.20.1
PC2	NIC	172.16.20.138	255.255.255.128	172.16.20.129
R2	G0/0	2001:DB8:C0DE:12::1/64		N/A
	G0/1	2001:DB8:C0DE:13::1/64		N/A
	S0/0/1	2001:DB8:C0DE:11::1/64		N/A
	Link-local	FE80::2		N/A
PC3	NIC	2001:DB8:C0DE:12::A/64		FE80::2
PC4	NIC	2001:DB8:C0DE:13::A/64		FE80::2

Objectives

Part 1: Configure IPv4 Addressing and Verify Connectivity

Part 2: Configure IPv6 Addressing and Verify Connectivity

Background

Routers R1 and R2 each have two LANs. Your task is to configure the appropriate addressing on each device and verify connectivity between the LANs.

Note: The user EXEC password is **cisco**. The privileged EXEC password is **class**.

Part 1: Configure IPv4 Addressing and Verify Connectivity

Step 1: Assign IPv4 addresses to R1 and LAN devices.

Referring to the **Addressing Table**, configure IP addressing for **R1** LAN interfaces, **PC1** and **PC2**. The serial interface has already configured.

Step 2: Verify connectivity.

PC1 and **PC2** should be able to ping each other and the **Dual Stack Server**.

Part 2: Configure IPv6 Addressing and Verify Connectivity

Step 1: Assign IPv6 addresses to R2 and LAN devices.

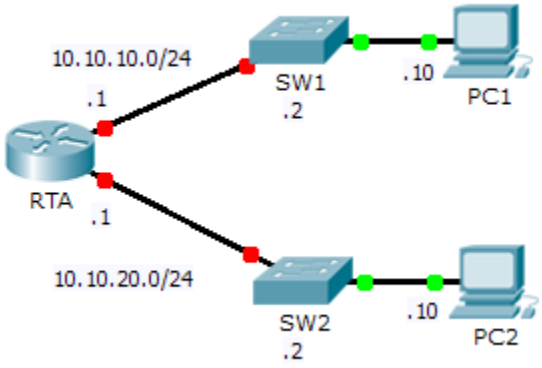
Referring to the **Addressing Table**, configure IP addressing for **R2 LAN interfaces**, **PC3** and **PC4**. The serial interface is already configured.

Step 2: Verify connectivity.

PC3 and **PC4** should be able to ping each other and the **Dual Stack Server**.

4.1.4.5 Packet Tracer - Configuring and Verifying a Small Network

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	G0/0	10.10.10.1	255.255.255.0	N/A
	G0/1	10.10.20.1	255.255.255.0	N/A
SW1	VLAN1	10.10.10.2	255.255.255.0	10.10.10.1
SW2	VLAN1	10.10.20.2	255.255.255.0	10.10.20.1
PC1	NIC	10.10.10.10	255.255.255.0	10.10.10.1
PC2	NIC	10.10.20.10	255.255.255.0	10.10.20.1

Objectives

Part 1: Configure Devices and Verify Connectivity

Part 2: Gather Information with Show Commands

Background

In this activity, you will configure **RTA** with basic settings, including IP addressing. You will also configure SW1 for remote management and configure the PCs. Once you have successfully verified connectivity, you will use **show** commands to gather information about the network.

Note: The user EXEC password is **cisco**. The privileged EXEC password is **class**.

Part 1: Configure Devices and Verify Connectivity

Step 1: Apply basic configurations to RTA.

a. Using the following information and the **Addressing Table**, configure RTA:

- Hostname and banner

- Line passwords set to **cisco**; encrypted password set to **class**
- IP addressing and descriptions on LAN interfaces

b. Save the configuration.

Step 2: Configure addressing on PC1 and PC2.

a. Using the **Addressing Table**, configure IP addressing for PC1 and PC2.

b. Test connectivity between **PC1** and **PC2**. Troubleshoot as necessary.

Step 3: Configure SW1 for remote management.

a. Using the **Addressing Table**, configure the management interface for SW1.

b. Configure the default gateway address.

c. Save the configuration.

Part 2: Gather Information with Show Commands

Step 1: Gather information from show interface command output.

Issue each of the following commands and then answer the related questions:

```
show ip interface brief
show interfaces
show ip interface
```

Which commands display the status of the port?

_____

Which command shows only the IP address (no subnet mask or prefix)? _____

Which command displays the description configured on the interface? _____

Which command displays the IP broadcast address? _____

Which command displays the MAC address of the interface? _____

Step 2: Gather information from show ip route command output.

Issue each of the following commands and then answer the related questions:

```
show ip route
show ip route connected
```

How many networks are known by the router based on the output of the **show ip route** command?

_____

What does the **L** at the beginning of the lines within the routing table represent? _____

What does the /32 prefix listed in the route table indicate? _____

Step 3: Gather information after an interface state is changed.

a. On **RTA**, shut down the Gigabit Ethernet 0/0 interface and issue the **show ip route** command. How many networks are displayed in the routing table now? _____

b. Attempt to ping PC1. Was the ping successful? _____

c. Issue the **show ip interface brief** command. What is the status of the Gigabit Ethernet 0/0 interface?

_____

d. Reactivate the Gigabit Ethernet 0/0 interface. Issue the **show ip route** command. Did the routing table repopulate? _____

What can be inferred about the interface status of routes that appear in the routing table?

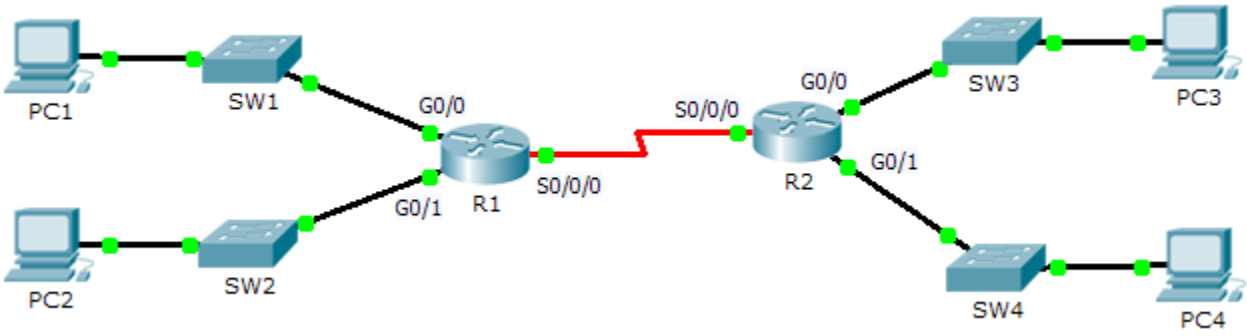
_____

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 2: Gather Information with Show Commands	Step 1	15	
	Step 2	10	
	Step 3	15	
	Part 2 Total	**40**	
	Packet Tracer Score	**60**	
	Total Score	**100**	

4.3.2.5 Packet Tracer - Investigating Directly Connected Routes

Topology



Objectives

Part 1: Investigate IPv4 Directly Connected Routes

Part 2: Investigate IPv6 Directly Connected Routes

Background

The network in the activity is already configured. You will log in to the routers and use **show** commands to discover and answer the questions below about the directly connected routes.

Note: The user EXEC password is **cisco** and the privileged exec password is **class.**

Part 1: Investigate IPv4 Directly Connected Routes

Step 1: Use show commands to gather information about the IPv4 directly connected networks.

Enter the following command on **R1**:

```
R1> show ip route ?
```

a. What option would be most beneficial in determining the networks assigned to the interfaces of the router? _____

b. Which networks are directly connected on **R1**? Hint: Use the option determined above.

_____

_____

_____

c. Which IP addresses are assigned to the LAN interfaces on **R1**?

_____

_____

_____

d. Which networks are directly connected on **R2**?

_____

_____

_____

e. Which IP addresses are assigned to the LAN interfaces on **R2**?

_____

_____

_____

Step 2: Verify PC addressing and test connectivity.

a. Open a command prompt on **PC1**. Issue the command to display the IP settings. Based on the output, would you expect **PC1** to be able to communicate with all interfaces on the router? Provide a short answer describing your expectations.

_____

b. Open a command prompt on **PC2**. Issue the command to display the IP settings. Based on the output, would you expect **PC2** to be able to communicate with **PC1**? Verify your expectations. _____

c. Determine the IP addresses of **PC3** and **PC4**. Record the results and determine if **PC3** and **PC4** are able to communicate.

_____

d. Test connectivity from **PC1** to **PC3**. Was the test successful? _____

e. **Bonus**: Looking at the outputs of the routing tables on **R1** and **R2**, what might indicate a reason for the success or failure of communication between **PC1** and **PC3**? _____

Part 2: Investigate IPv6 Directly Connected Routes

Step 1: Use show commands to gather information about the IPv6 directly connected networks.

a. Which IPv6 networks are available on **R1**?

_____

_____

_____

_____

_____

_____

b. Which IPv6 unicast addresses are assigned to the LAN interfaces on **R1**?

_____

_____

_____

_____

c. Which IPv6 networks are available on R2?

_____

_____

_____

_____

_____

_____

d. Which IPv6 addresses are assigned to the LAN interfaces on **R2**?

_____

_____

Step 2: Verify PC settings and connectivity.

a. Open a command prompt on **PC1**. Issue the command to display the IPv6 settings. Based on the output, would you expect **PC1** to be able to communicate with all interfaces on the router? Provide a short answer describing your expectations

_____

_____

b. Open a command prompt on **PC2**. Issue the command to display the IPv6 settings. Based on the output, would you expect **PC2** to be able to communicate with **PC1**? Verify your expectations. _____

c. Determine the IPv6 addresses of **PC3** and **PC4**. Record the results and determine if **PC3** and **PC4** are able to communicate.

_____

d. Test connectivity from **PC1** to **PC3**. Was the test successful? _____

e. **Bonus**: What might indicate a reason for the success or failure of communication between **PC1** and **PC3** after looking at the outputs of the IPv6 routing tables on **R1** and **R2**?

_____

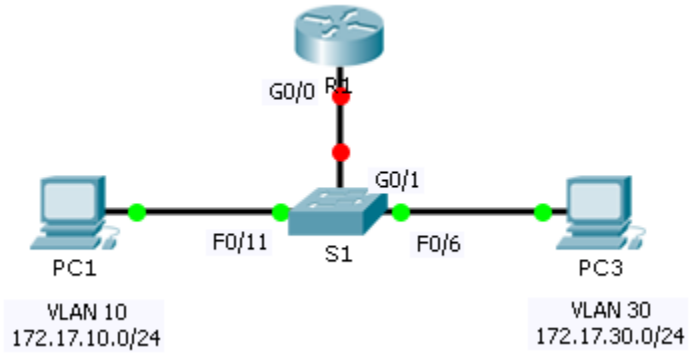
_____

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Investigate IPv4 Directly Connected Routes	Step 1	25	
	Step 2	25	
Part 2: Investigate IPv6 Directly Connected Routes	Step 1	25	
	Step 2	25	
	Total Score	**100**	

5.1.3.6 Packet Tracer – Configuring Router-on-a-Stick Inter-VLAN Routing

Topology



Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0.10	172.17.10.1	255.255.255.0	N/A
	G0/0.30	172.17.30.1	255.255.255.0	N/A
PC1	NIC	172.17.10.10	255.255.255.0	172.17.10.1
PC2	NIC	172.17.30.10	255.255.255.0	172.17.30.1

Objectives

Part 1: Test Connectivity without Inter-VLAN Routing

Part 2: Add VLANs to a Switch

Part 3: Configure Subinterfaces

Part 4: Test Connectivity with Inter-VLAN Routing

Scenario

In this activity, you will check for connectivity prior to implementing inter-VLAN routing. You will then configure VLANs and inter-VLAN routing. Finally, you will enable trunking and verify connectivity between VLANs.

Part 1: Test Connectivity Without Inter-VLAN Routing

Step 1: Ping between PC1 and PC3.

Wait for switch convergence or click **Fast Forward Time** a few times. When the link lights are green for **PC1** and **PC3**, ping between **PC1** and **PC3**. Because the two PCs are on separate networks and **R1** is not configured, the ping fails.

Step 2: Switch to Simulation mode to monitor pings.

a. Switch to Simulation mode by clicking the **Simulation** tab or pressing **Shift+S**.

b. Click **Capture/Forward** to see the steps the ping takes between **PC1** and **PC3**. Notice how the ping never leaves **PC1**. What process failed and why?

_____

_____

_____

Part 2: Add VLANs to a Switch

Step 1: Create VLANs on S1.

Return to **Realtime** mode and create VLAN 10 and VLAN 30 on **S1**.

Step 2: Assign VLANs to ports.

a. Configure interface F0/6 and F0/11 as access ports and assign VLANs.

- Assign **PC1** to VLAN 10.
- Assign **PC3** to VLAN 30.

b. Issue the **show vlan brief** command to verify VLAN configuration.

```
S1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   VLAN0010                          active    Fa0/11
30   VLAN0030                          active    Fa0/6
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Step 3: Test connectivity between PC1 and PC3.

From **PC1**, ping **PC3**. The pings should still fail. Why were the pings unsuccessful?

_____

_____

Part 3: Configure Subinterfaces

Step 1: Configure subinterfaces on R1 using the 802.1Q encapsulation.

a. Create the subinterface G0/0.10.

- Set the encapsulation type to 802.1Q and assign VLAN 10 to the subinterface.
- Refer to the **Address Table** and assign the correct IP address to the subinterface.

b. Repeat for the G0/0.30 subinterface.

Step 2: Verify Configuration.

a. Use the **show ip interface brief** command to verify subinterface configuration. Both subinterfaces are down. Subinterfaces are virtual interfaces that are associated with a physical interface. Therefore, in order to enable subinterfaces, you must enable the physical interface that they are associated with.

b. Enable the G0/0 interface. Verify that the subinterfaces are now active.

Part 4: Test Connectivity with Inter-VLAN Routing

Step 1: Ping between PC1 and PC3.

From **PC1**, ping **PC3**. The pings should still fail.

Step 2: Enable trunking.

a. On **S1**, issue the **show vlan** command. What VLAN is G0/1 assigned to? _____

b. Because the router was configured with multiple subinterfaces assigned to different VLANs, the switch port connecting to the router must be configured as a trunk. Enable trunking on interface G0/1.

c. How can you determine that the interface is a trunk port using the **show vlan** command?

_____

d. Issue the **show interface trunk** command to verify the interface is configured as a trunk.

Step 3: Switch to Simulation mode to monitor pings.

a. Switch to **Simulation** mode by clicking the **Simulation** tab or pressing **Shift+S**.

b. Click **Capture/Forward** to see the steps the ping takes between **PC1** and **PC3**.

c. You should see ARP requests and replies between **S1** and **R1**. Then ARP requests and replies between **R1** and **S3**. Then **PC1** can encapsulate an ICMP echo request with the proper data-link layer information and R1 will route the request to **PC3**.

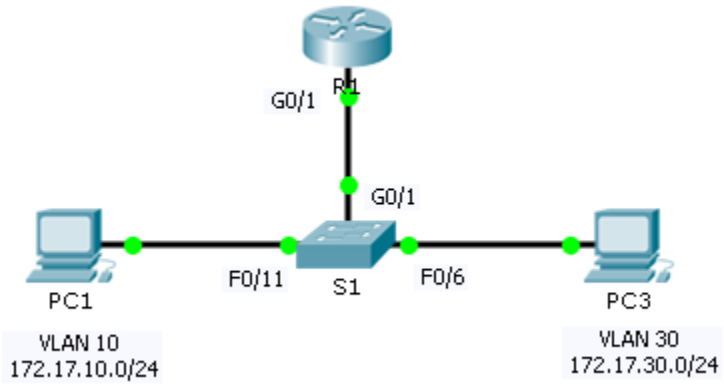
Note: After the ARP process finishes, you may need to click Reset Simulation to see the ICMP process complete.

Suggested Scoring Rubric

Packet Tracer scores 60 points. The four questions are worth 10 points each.

5.2.2.4 Packet Tracer – Troubleshooting Inter-VLAN Routing

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	VLAN
R1	G0/1.10	172.17.10.1	255.255.255.0	N/A	VLAN 10
	G0/1.30	172.17.30.1	255.255.255.0	N/A	VLAN 30
PC1	NIC	172.17.10.10	255.255.255.0	172.17.10.1	VLAN 10
PC3	NIC	172.17.30.10	255.255.255.0	172.17.30.1	VLAN 30

Objectives

Part 1: Locate Network Problems

Part 2: Implement the Solution

Part 3: Verify Network Connectivity

Scenario

In this activity, you will troubleshoot connectivity problems caused by improper configurations related to VLANs and inter-VLAN routing.

Part 1: Locate the Network Problems

Examine the network and locate the source of any connectivity issues.

- Test connectivity and use the necessary **show** commands on to verify configurations.
- List all of the problems and possible solutions in the **Documentation Table**.

Documentation Table

Problems	Solutions

Part 2: Implement the Solutions

Make changes according to your recommended solutions.

Part 3: Verify Network Connectivity

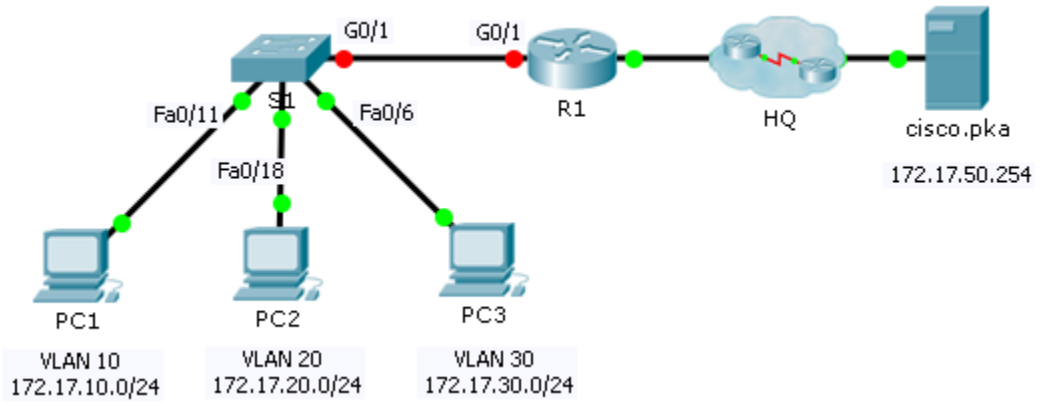
Verify the PCs can ping other PCs and R1. If not, continue to troubleshoot until the pings are successful.

Suggested Scoring Rubric

Packet Tracer scores 60 points. Completing the **Documentation Table** is worth 40 points.

5.4.1.2 Packet Tracer – Skills Integration Challenge

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.17.25.2	255.255.255.252	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
	G0/1.30	172.17.30.1	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
S1	VLAN 99	172.17.99.10	255.255.255.0	172.17.99.1
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1

VLAN and Port Assignments Table

VLAN	Name	Interface
10	Faculty/Staff	Fa0/11-17
20	Students	Fa0/18-24
30	Guest(Default)	Fa0/6-10
88	Native	G0/1
99	Management	VLAN 99

Scenario

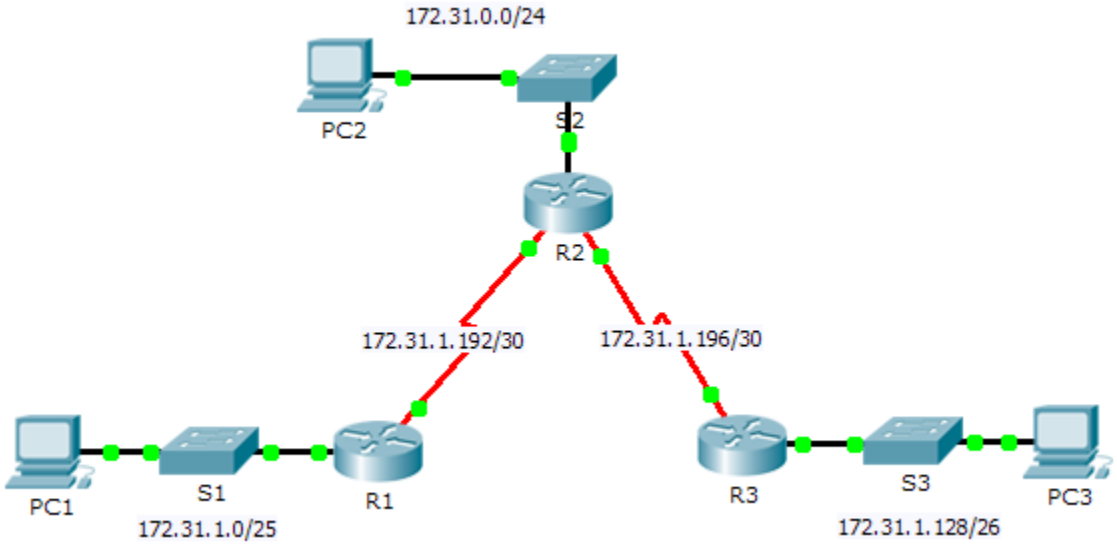
In this activity, you will demonstrate and reinforce your ability to implement inter-VLAN routing, including configuring IP addresses, VLANs, trunking and subinterfaces.

Requirements

- Assign IP addressing to **R1** and **S1** based on the **Addressing Table**.
- Create, name and assign VLANs on **S1** based on the **VLAN and Port Assignments Table**. Ports should be in access mode.
- Configure **S1** to trunk, allow only the VLANs in the **VLAN and Port Assignments Table**.
- Configure the default gateway on **S1.**
- All ports not assigned to a VLAN should be disabled.
- Configure inter-VLAN routing on **R1** based on the **Addressing Table**.
- Verify connectivity. **R1**, **S1**, and all PCs should be able to ping each other and the **cisco.pka** server.

6.2.2.4 Packet Tracer - Configuring IPv4 Static and Default Routes

Topology



Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0	172.31.1.1	255.255.255.128	N/A
	S0/0/0	172.31.1.194	255.255.255.252	N/A
R2	G0/0	172.31.0.1	255.255.255.0	N/A
	S0/0/0	172.31.1.193	255.255.255.252	N/A
	S0/0/1	172.31.1.197	255.255.255.252	N/A
R3	G0/0	172.31.1.129	255.255.255.192	N/A
	S0/0/1	172.31.1.198	255.255.255.252	N/A
PC1	NIC	172.31.1.126	255.255.255.128	172.31.1.1
PC2	NIC	172.31.0.254	255.255.255.0	172.31.0.1
PC3	NIC	172.31.1.190	255.255.255.192	172.31.1.129

Objectives

Part 1: Examine the Network and Evaluate the Need for Static Routing

Part 2: Configure Static and Default Routes

Part 3: Verify Connectivity

Background

In this activity, you will configure static and default routes. A static route is a route that is entered manually by the network administrator to create a reliable and safe route. There are four different static routes that are used in this activity: a recursive static route, a directly attached static route, a fully specified static route, and a default route.

Part 1: Examine the Network and Evaluate the Need for Static Routing

a. Looking at the topology diagram, how many networks are there in total? _____

b. How many networks are directly connected to R1, R2, and R3? _____

c. How many static routes are required by each router to reach networks that are not directly connected?

_____

d. Test connectivity to the R2 and R3 LANs by pinging PC2 and PC3 from PC1.

Why were you unsuccessful? _____

Part 2: Configure Static and Default Routes

Step 1: Configure recursive static routes on R1.

a. What is recursive static route?

_____

_____

b. Why does a recursive static route require two routing table lookups?

_____

_____

c. Configure a recursive static route to every network not directly connected to R1, including the WAN link between R2 and R3.

d. Test connectivity to the R2 LAN and ping the IP addresses of PC2 and PC3.

Why were you unsuccessful?

_____

Step 2: Configure directly attached static routes on R2.

a. How does a directly attached static route differ from a recursive static route?

_____

_____

b. Configure a directly attached static route from R2 to every network not directly connected.

c. Which command only displays directly connected networks? _____

d. Which command only displays the static routes listed in the routing table? _____

e. When viewing the entire routing table, how can you distinguish between a directly attached static route and a directly connected network?

_____

Step 3: Configure a default route on R3.

a. How does a default route differ from a regular static route?

_____

_____

_____

b. Configure a default route on R3 so that every network not directly connected is reachable.

c. How is a static route displayed in the routing table? _____

Step 4: Document the commands for fully specified routes.

Note: Packet Tracer does not currently support configuring fully specified static routes. Therefore, in this step, document the configuration for fully specified routes.

a. Explain a fully specified route.

_____

_____

b. Which command provides a fully specified static route from R3 to the R2 LAN?

_____

c. Write a fully specified route from R3 to the network between R2 and R1. Do not configure the route; just calculate it.

_____

d. Write a fully specified static route from R3 to the R1 LAN. Do not configure the route; just calculate it.

_____

Step 5: Verify static route configurations.

Use the appropriate **show** commands to verify correct configurations.

Which **show** commands can you use to verify that the static routes are configured correctly?

_____

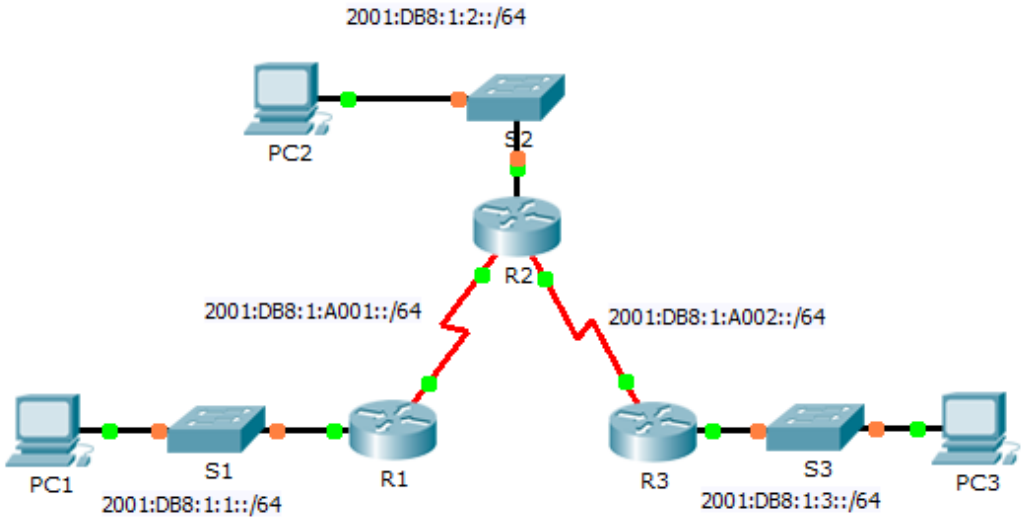
Part 3: Verify Connectivity

Every device should now be able to ping every other device. If not, review your static and default route configurations.

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Examine the Network and Evaluate the Need for Static Routing	a - d	10	
	Part 1 Total	**10**	
Part 2: Configure Static and Default Routes	Step 1	7	
	Step 2	7	
	Step 3	3	
	Step 4	10	
	Step 5	3	
	Part 2 Total	**30**	
	Packet Tracer Score	**60**	
	Total Score	**100**	

6.2.4.4 Packet Tracer - Configuring IPv6 Static and Default Routes



IPv6 Addressing Table

Device	Interface	IPv6 Address/Prefix	Default Gateway
R1	G0/0	2001:DB8:1:1::1/64	N/A
	S0/0/0	2001:DB8:1:A001::1/64	N/A
R2	G0/0	2001:DB8:1:2::1/64	N/A
	S0/0/0	2001:DB8:1:A001::2/64	N/A
	S0/0/1	2001:DB8:1:A002::1/64	N/A
R3	G0/0	2001:DB8:1:3::1/64	N/A
	S0/0/1	2001:DB8:1:A002::2/64	N/A
PC1	NIC	2001:DB8:1:1::F/64	FE80::1
PC2	NIC	2001:DB8:1:2::F/64	FE80::2
PC3	NIC	2001:DB8:1:3::F/64	FE80::3

Objectives

Part 1: Examine the Network and Evaluate the Need for Static Routing

Part 2: Configure IPv6 Static and Default Routes

Part 3: Verify Connectivity

Background

In this activity, you will configure IPv6 static and default routes. A static route is a route that is entered manually by the network administrator in order to create a route that is reliable and safe. There are four

different static routes used in this activity: a recursive static route; a directly attached static route; a fully specified static route; and a default route.

Part 1: Examine the Network and Evaluate the Need for Static Routing

a. Looking at the topology diagram, how many networks are there in total? _____

b. How many networks are directly connected to R1, R2, and R3? _____

c. How many static routes are required by each router to reach networks that are not directly connected?

_____

_____

d. Which command is used to configure IPv6 static routes?

_____

Part 2: Configure IPv6 Static and Default Routes

Step 1: Enable IPv6 routing on all routers.

Before configuring static routes, we must configure the router to forward IPv6 packets

Which command accomplishes this? _____

Enter this command on each router.

Step 2: Configure recursive static routes on R1.

Configure an IPv6 recursive static route to every network not directly connected to R1.

Step 3: Configure a directly attached and a fully specified static route on R2.

a. Configure a directly attached static route from R2 to the R1 LAN.

b. Configure a fully specific route from R2 to the R3 LAN.
Note: Packet Tracer v6.0.1 only checks for directly attached and recursive static routes. Your instructor may ask to review your configuration of a fully specified IPv6 static route.

Step 4: Configure a default route on R3.

Configure a recursive default route on R3 to reach all networks not directly connected.

Step 5: Verify static route configurations.

a. Which command is used to verify the IPv6 configuration of a PC from the command prompt?

_____

b. Which command displays the IPv6 addresses configured on a router's interface?

_____

c. Which command displays the contents of the IPv6 routing table? _____

Part 3: Verify Network Connectivity

Every device should now be able to ping every other device. If not, review your static and default route configurations.

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Exam the Network and Evaluate the Need for Static Routing	a - d	20	
	Part 1 Total	**20**	
Part 2: Configure IPv6 Static and Default Routes	Step 1	5	
	Step 5	15	
	Part 2 Total	**20**	
	Packet Tracer Score	**60**	
	Total Score	**100**	

6.3.3.6 Packet Tracer - Designing and Implementing a VLSM Addressing Scheme

Topology

You will receive one of three possible topologies.

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
	G0/0			N/A
	G0/1			N/A
	S0/0/0			N/A
	G0/0			N/A
	G0/1			N/A
	S0/0/0			N/A
	VLAN 1			
	VLAN 1			
	VLAN 1			
	VLAN 1			
	NIC			
	NIC			
	NIC			
	NIC			

Objectives

Part 1: Examine the Network Requirements

Part 2: Design the VLSM Addressing Scheme

Part 3: Assign IP Addresses to Devices and Verify Connectivity

Background

In this activity, you are given a /24 network address to use to design a VLSM addressing scheme. Based on a set of requirements, you will assign subnets and addressing, configure devices and verify connectivity.

Part 1: Examine the Network Requirements

Step 1: Determine the number of subnets needed.

You will subnet the network address _____. The network has the following requirements:

- _____ LAN will require _____ host IP addresses
- _____ LAN will require _____ host IP addresses
- _____ LAN will require _____ host IP addresses
- _____ LAN will require _____ host IP addresses

How many subnets are needed in the network topology? _____

Step 2: Determine the subnet mask information for each subnet.

a. Which subnet mask will accommodate the number of IP addresses required for _____?

   How many usable host addresses will this subnet support? _____

b. Which subnet mask will accommodate the number of IP addresses required for _____?

   How many usable host addresses will this subnet support? _____

c. Which subnet mask will accommodate the number of IP addresses required for _____?

   How many usable host addresses will this subnet support? _____

d. Which subnet mask will accommodate the number of IP addresses required for _____?

   How many usable host addresses will this subnet support? _____

e. Which subnet mask will accommodate the number of IP addresses required for the connection between _____ and _____?

Part 2: Design the VLSM Addressing Scheme

Step 1: Divide the _____. network based on the number of hosts per subnet.

a. Use the first subnet to accommodate the largest LAN.

b. Use the second subnet to accommodate the second largest LAN.

c. Use the third subnet to accommodate the third largest LAN.

d. Use the fourth subnet to accommodate the fourth largest LAN.

e. Use the fifth subnet to accommodate the connection between _____ and _____.

Step 2: Document the VLSM subnets.

Complete the **Subnet Table**, listing the subnet descriptions (e.g. _____ LAN), number of hosts needed, then network address for the subnet, the first usable host address, and the broadcast address. Repeat until all addresses are listed.

Subnet Table

Subnet Description	Number of Hosts Needed	Network Address/CIDR	First Usable Host Address	Broadcast Address

Step 3: Document the addressing scheme.

a. Assign the first usable IP addresses to _____ for the two LAN links and the WAN link.

b. Assign the first usable IP addresses to _____ for the two LANs links. Assign the last usable IP address for the WAN link.

c. Assign the second usable IP addresses to the switches.

d. Assign the last usable IP addresses to the hosts.

Part 3: Assign IP Addresses to Devices and Verify Connectivity

Most of the IP addressing is already configured on this network. Implement the following steps to complete the addressing configuration.

Step 1: Configure IP addressing on _____ LAN interfaces.

Step 2: Configure IP addressing on _____, including the default gateway.

Step 3: Configure IP addressing on _____, including the default gateway.

Step 4: Verify connectivity.

You can only verify connectivity from _____, _____, and _____. However, you should be able to ping every IP address listed in the **Addressing Table**.

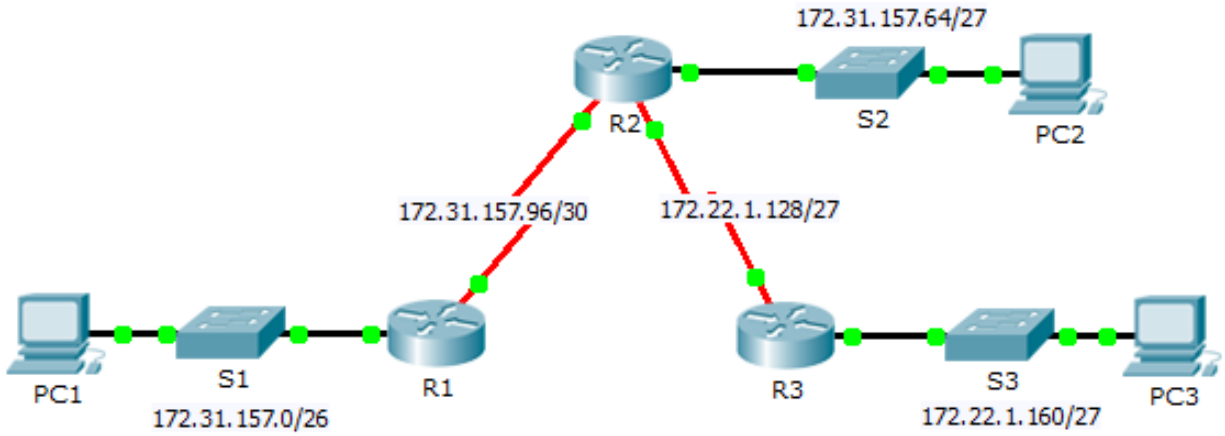
Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Examine the Network Requirements	Step 1	1	
	Step 2	4	
	Part 1 Total	**5**	
Part 2: Design the VLSM Addressing Scheme			
	Complete Subnet Table	25	
	Document Addressing	40	
	Part 2 Total	**65**	
	Packet Tracer Score	**30**	
	Total Score	**100**	

ID: _____

6.4.1.5 Packet Tracer - Configuring IPv4 Route Summarization - Scenario 1

Topology



Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0	172.31.157.1	255.255.255.192	N/A
	S0/0/0	172.31.157.97	255.255.255.252	N/A
R2	G0/0	172.31.157.65	255.255.255.224	N/A
	S0/0/0	172.31.157.98	255.255.255.252	N/A
	S0/0/1	172.22.1.129	255.255.255.224	N/A
R3	G0/0	172.22.1.161	255.255.255.224	N/A
	S0/0/1	172.22.1.158	255.255.255.224	N/A
PC1	NIC	172.31.157.62	255.255.255.192	172.31.157.1
PC2	NIC	172.31.157.94	255.255.255.224	172.31.157.65
PC3	NIC	172.22.1.190	255.255.255.224	172.22.1.161

Objectives

Part 1: Calculate Summary Routes

Part 2: Configure Summary Routes

Part 3: Verify Connectivity

Background

In this activity, you will calculate and configure summary routes. Router summarization, also known as route aggregation, is the process of advertising a contiguous set of addresses as a single address.

Part 1: Calculate Summary Routes

Step 1: Calculate a summary route on R1 to reach LANs on R3.

a. List the 172.22.1.128/27 and 172.22.1.160/27 networks in binary format.

```
172.22.1.128: 10101100.00010110.00000001.10000000
172.22.1.160: 10101100.00010110.00000001.10100000
```

b. Count the left-most matching bits to determine the mask for the summary route. They have 26 left-most bits in common.

```
172.22.1.128: 10101100.00010110.00000001.10000000
172.22.1.160: 10101100.00010110.00000001.10100000
```

c. Copy the matching bits and fill in the remaining bits with zeros to determine the summarized network address.

```
10101100.00010110.00000001.10000000
```

d. What is the summarized network address and subnet mask? _____

Step 2: Calculate a summary route on R3 to reach LANs on R1 and R2.

a. Calculate the summary route for the 172.31.157.0/26, 172.31.157.64/27, and 172.31.157.96/30 networks. List the networks in binary format. Then, count the left-most matching bits to determine the mask for the summary route.

_____

_____

_____

b. What is the summarized network address and subnet mask? _____

Part 2: Configure Summary Routes

Step 1: Configure a summary route for R1.

Configure the recursive summary route that you calculated in Part 1, Step 1.

Step 2: Configure a summary route for R3.

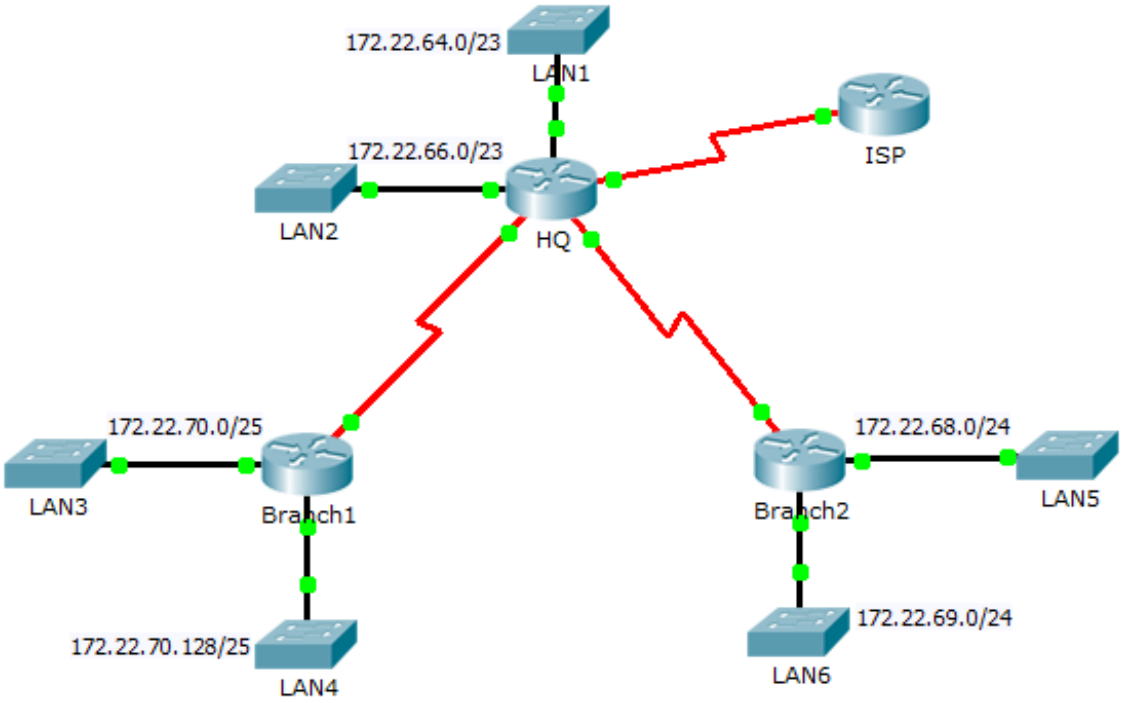
Configure the directly attached summary route that you calculated in Part 1, Step 2.

Part 3: Verify Connectivity

Verify that all PC hosts and routers can ping other PC hosts and routers in the topology. If not, troubleshoot and correct the issues.

6.4.1.6 Packet Tracer - Configuring IPv4 Route Summarization - Scenario 2

Topology



Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
ISP	S0/0/1	198.0.0.1	255.255.255.252	N/A
HQ	G0/0	172.22.64.1	255.255.254.0	N/A
	G0/1	172.22.66.1	255.255.254.0	N/A
	S0/0/0	172.22.71.1	255.255.255.252	N/A
	S0/0/1	172.22.71.5	255.255.255.252	N/A
	S0/1/0	198.0.0.2	255.255.255.252	N/A
Branch1	G0/0	172.22.70.1	255.255.255.128	N/A
	G0/1	172.22.70.129	255.255.255.128	N/A
	S0/0/0	172.22.71.2	255.255.255.252	N/A
Branch2	G0/0	172.22.68.1	255.255.255.0	N/A
	G0/1	172.22.69.1	255.255.255.0	N/A
	S0/0/1	172.22.71.6	255.255.255.252	N/A
LAN1	VLAN 1	172.22.64.2	255.255.254.0	172.22.64.1
LAN2	VLAN 1	172.22.66.2	255.255.254.0	172.22.66.1
LAN3	VLAN 1	172.22.70.2	255.255.255.128	172.22.70.1
LAN4	VLAN 1	172.22.70.130	255.255.255.128	172.22.70.129
LAN5	VLAN 1	172.22.68.2	255.255.255.0	172.22.68.1
LAN6	VLAN 1	172.22.69.2	255.255.255.0	172.22.69.1

Objectives

Part 1: Calculate Summary Routes

Part 2: Configure Summary Routes

Part 3: Verify Connectivity

Background

In this activity, you will calculate and configure summary routes. Route summarization, also known as route aggregation is the process of advertising a contiguous set of addresses as a single address. After calculating summary routes for each LAN, you must summarize a route that includes all networks in the topology for the ISP to reach each LAN.

Part 1: Calculate Summary Routes

a. What is the summary route to reach HQ LANs? _____

b. What is the summary route to reach Branch1 LANs? _____

c. What is the summary route to reach Branch2 LANs? _____

d. What is the summary route from the ISP router to reach all LANs? _____

Part 2: Configure Summary Routes

Step 1: Configure the summary routes on the HQ router to other networks.

a. Configure a directly attached summary route on **HQ** to reach the **Branch1** LANs.

b. Configure a recursive summary route on **HQ** to reach the **Branch2** LANs.

Step 2: Configure the summary routes on the Branch1 router to other networks.

a. Configure a recursive summary route on **Branch1** to reach the **HQ** LANs.

b. Configure a recursive summary route on **Branch1** to reach the **Branch2** LANs.

Step 3: Configure the summary routes on the Branch2 router to other networks.

a. Configure a directly attached summary route on **Branch2** to reach the **Branch1** LANs.

b. Configure a recursive summary route on **Branch2** to reach the **HQ** LANs.

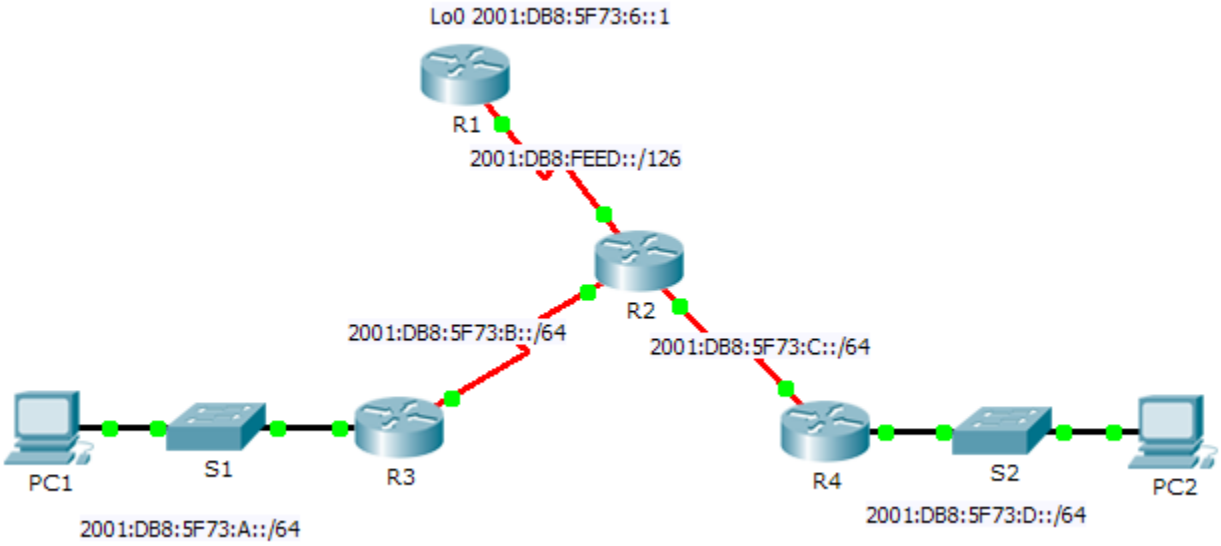
Step 4: Configure a summary route on ISP to reach all networks.

Part 3: Verify Connectivity

Verify that all switches and routers can ping other devices in the topology. If not, troubleshoot your summary routes to correct any issues.

6.4.2.4 Packet Tracer – Calculating and Configuring IPv6 Route Summarization

Topology



Addressing Table

Device	Interface	IPv6 Address/Prefix
R1	S0/0/0	2001:DB8:FEED::1/126
	Lo0	2001:DB8:5F73:6::1/64
R2	S0/0/0	2001:DB8:FEED::2/126
	S0/0/1	2001:DB8:5F73:B::1/64
	S0/1/0	2001:DB8:5F73:C::1/64
R3	G0/1	2001:DB8:5F73:A::1/64
	S0/0/0	2001:DB8:5F73:B::2/64
R4	G0/1	2001:DB8:5F73:D::1/64
	S0/0/1	2001:DB8:5F73:C::2/64

Objectives

Part 1: Calculate a Summary Route for R1

Part 2: Configure the Summary Route and Verify Connectivity

Background

In this activity, you will calculate, configure and verify a summary route for all the networks R1 can access through R2. R1 is configured with a loopback interface. Instead of adding a LAN or another network to R1, use a loopback interface to simplify testing when verifying routing.

Part 1: Calculate a Summary Route for R1

When summarizing an IPv6 address, look at the prefix to determine where the address ends. In this case, a /64 ends at the fourth segment.

a. List the first four segments of each of the networks. Because the first three segments have the identical hexadecimal digits, there is no need to write them in binary. The fourth segment is different (:A, :B, :C, and :D); therefore, write the 16 bits for each in binary. Count the left-most matching bits to determine the prefix for the summary route.

2001:DB8:5F73:0000000000001010

2001:DB8:5F73:0000000000001011

2001:DB8:5F73:0000000000001100

2001:DB8:5F73:0000000000001101

b. In the fourth segment, the network addresses have the first 13 bits in common. Therefore, the summarized prefix is the 48 bits from the first three segments, plus the 13 bit from the fourth segment (or /61).

c. Copy the matching bits and fill in the remaining bits with zeros to determine that the summarized network address is 2001:0DB8:5F73:8::/61.

Part 2: Configure the Summary Route and Verify Connectivity

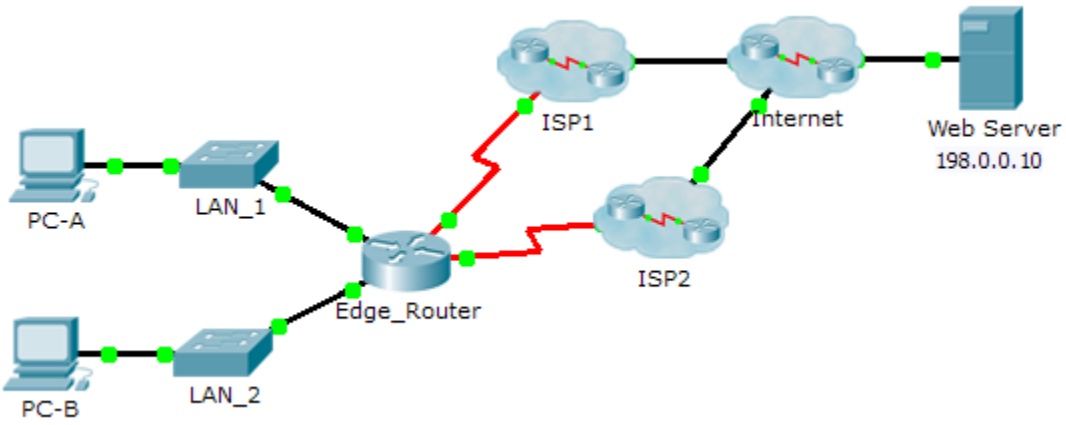
a. Configure a directly attached summary route on R1.

b. PC1 should be able to ping PC2.

c. PC1 and PC2 should both be able to ping the Loopback 0 interface on R1.

6.4.3.4 Packet Tracer - Configuring a Floating Static Route

Topology



Objectives

Part 1: Configure a Floating Static Route

Part 2: Test Failover to the Backup Route

Background

In this activity, you will configure a floating static route which is used as a backup route. This route has a manually configured administrative distance greater than that of the primary route and, therefore, would not be in the routing table until the primary route fails. You will test failover to the backup route, and then restore connectivity to the primary route.

Part 1: Configuring a Floating Static Route

Step 1: Configure a directly attached static default route.

a. Configure a directly attached static default route from **Edge_Router** to the Internet. The primary default route should be through **ISP1**.

b. Display the contents of the routing table. Verify that the default route is visible in the routing table.

c. What command is used to trace a path from a PC to a destination? _____

From **PC-A**, trace the route to the **Web Server**. The route should start at the default gateway 192.168.10.1 and go through the 10.10.10.1 address. If not, check your static default route configuration.

Step 2: Configure a floating static route.

a. What is the administrative distance of a static route? _____

b. Configure a directly attached floating static default route with an administrative distance of 5. The route should point to **ISP2**.

c. View the running configuration and verify that the floating static default route is there, as well as the static default route.

d. Display the contents of the routing table. Is the floating static route visible in the routing table? Why or why not?

_____

_____

_____

Part 2: Test Failover to the Backup Route

a. On **Edge_Router**, administratively disable the exit interface of the primary route.

b. Verify that the backup route is now in the routing table.

c. Trace the route from **PC-A** to the **Web Server**.

Did the backup route work? If not, wait a few more seconds for convergence and then re-test. If the backup route is still not working, investigate your floating static route configuration.

d. Restore connectivity to the primary route.

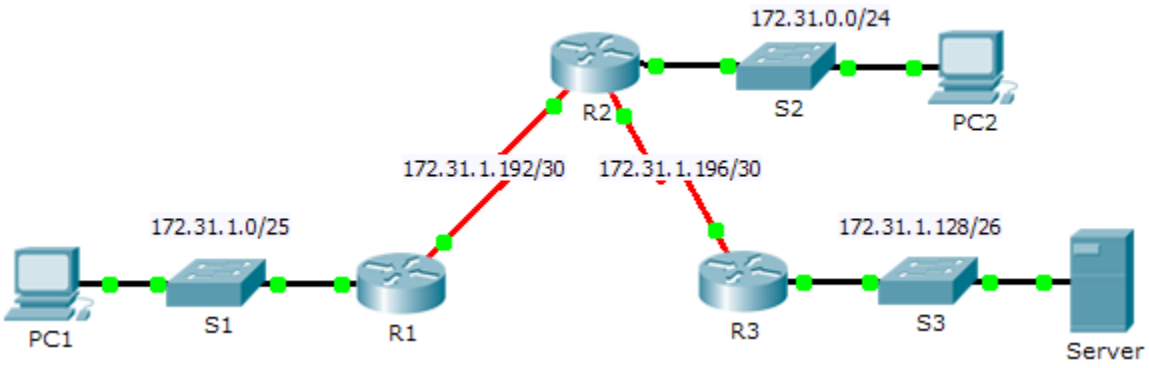
e. Trace the route from **PC-A** to the **Web Server** to verify that the primary route is restored.

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Configuring a Floating Static Route	Step 1c	2	
	Step 2a	3	
	Step 2d	5	
	Part 1 Total	**10**	
	Packet Tracer Score	**90**	
	Total Score	**100**	

6.5.2.3 Packet Tracer - Troubleshooting Static Routes

Topology



Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0	172.31.1.1	255.255.255.128	N/A
	S0/0/0	172.31.1.194	255.255.255.252	N/A
R2	G0/0	172.31.0.1	255.255.255.0	N/A
	S0/0/0	172.31.1.193	255.255.255.252	N/A
	S0/0/1	172.31.1.197	255.255.255.252	N/A
R3	G0/0	172.31.1.129	255.255.255.192	N/A
	S0/0/1	172.31.1.198	255.255.255.252	N/A
PC1	NIC	172.31.1.126	255.255.255.128	172.31.1.1
PC2	NIC	172.31.0.254	255.255.255.0	172.31.0.1
Server	NIC	172.31.1.190	255.255.255.192	172.31.1.129

Objectives

Part 1: Locate the Problem

Part 2: Determine the Solution

Part 3: Implement the Solution

Part 4: Verify That the Issue Is Resolved

Background

In this activity, PC1 reports that they cannot access resources on the server. Locate the problem, decide on an appropriate solution and resolve the issue.

Part 1: Locate the Problem

PC1 cannot access files on the server. Locate the problem using the appropriate **show** commands on all routers and any troubleshooting commands on the PCs that you have learned from previous chapters.

What are some of the troubleshooting commands on routers and PCs that can be used to identify the source of the problem?

_____

Part 2: Determine the Solution

After you have located the problem that is preventing PC1 from accessing files on the server, fill in the table below.

Problem	Solution

Part 3: Implement the Solution

a. If there are any misconfigured static routes, you must remove them before the correct ones can be added to the configuration.

b. Add any missing static routes by configuring directly attached routes.

Part 4: Verify That the Issue Is Resolved

a. Ping from PC1 to the server.

b. Open a web connection to the server. After you correctly identify and implement the correct solution to the problem, you will receive a message in the web browser when you connect to the server.

Suggested Scoring Rubric

Activity Section	Possible Points	Earned Points
Part 1: Locate the Problem	**2**	
Part 2: Determine the Solution	**8**	
Packet Tracer Score	**90**	
Total Score	**100**	

6.5.2.4 Packet Tracer - Troubleshooting VLSM and Route Summarization

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	G0/0			
	G0/1			
	S0/0/0			
	S0/0/1			
EAST	G0/0			
	G0/1			
	S0/0/0			
WEST	G0/0			
	G0/1			
	S0/0/0			
	S0/0/1			
HQ_LAN1	VLAN 1			
HQ_LAN2	VLAN 1			
EAST_LAN1	VLAN 1			
EAST_LAN2	VLAN 1			
WEST_LAN1	VLAN 1			
WEST_LAN2	VLAN 1			

Objectives

Part 1: Locate the Problem

Part 2: Determine the Solution

Part 3: Implement the Solution

Part4: Verify That the Issues Are Resolved

Background / Scenario

In this activity, the network is already addressed using VLSM and configured with static routes but there is a problem. Locate the issues, determine the best solution, implement the solution, and verify the issues are resolved.

Part 1: Locate the Problem

a. Investigate the device and document the current addressing scheme in the Addressing Table.

b. Using the Host Chart below, determine if the addressing on each LAN interface has the appropriate subnet mask based on the number of hosts required for that LAN.

Host Chart

LAN	Interface	Number of Hosts
HQ LAN 1	G0/1	1500
HQ LAN 2	G0/0	1000
EAST LAN 1	G0/1	900
EAST LAN 2	G0/0	900
WEST LAN 1	G0/0	250
WEST LAN 2	G0/1	500

Part 2: Determine the Solution

a. Determine the solution to the addressing errors and correct the documentation in the Addressing Table.

b. After the addressing scheme is corrected, analyze the summary routes to see if any errors exist. There should be one summary route for both LANs of each router.

c. Document the errors and the solution to each problem found in the Troubleshooting Documentation table below.

Troubleshooting Documentation

Problem	Solution

Part 3: Implement the Solution

a. Correct addressing errors.

b. Correct summary route errors.

Note: It is possible to configure a summary route that restores connectivity, but it is still incorrect because it includes addresses that are not part of the topology.

Part 4: Verify That the Issues Are Resolved

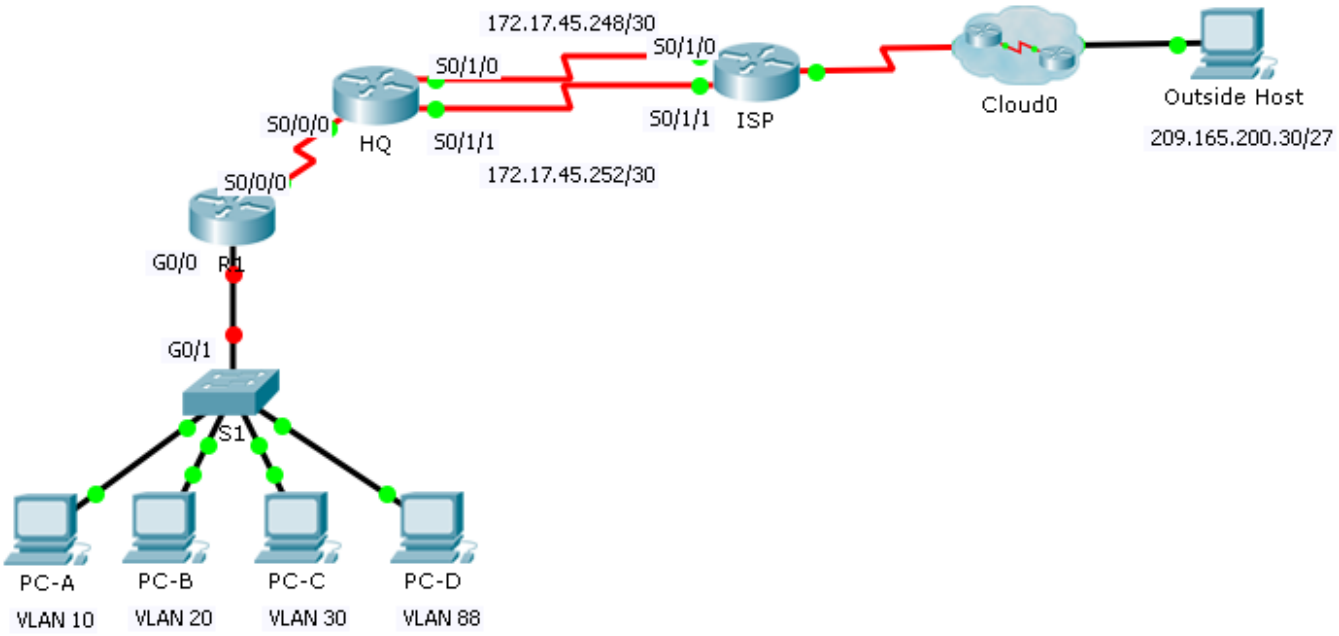
Ping each switch from EAST_LAN1. If you are unsuccessful, recheck your addressing scheme and summary route configurations.

Suggested Scoring Rubric

Activity Section	Possible Points	Earned Points
Addressing Table	**25**	
Troubleshooting Documentation	**25**	
Packet Tracer Score	**50**	
Total Score	**100**	

6.6.1.2 Packet Tracer – Skills Integration Challenge

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	VLAN
R1	S0/0/0	172.31.1.2	255.255.255.0	N/A	N/A
	G0/0.10	172.31.10.1	255.255.255.0	N/A	10
	G0/0.20	172.31.20.1	255.255.255.0	N/A	20
	G0/0.30	172.31.30.1	255.255.255.0	N/A	30
	G0/0.88	172.31.88.1	255.255.255.0	N/A	88
	G0/0.99	172.31.99.1	255.255.255.0	N/A	99
S1	VLAN 88	172.31.88.33	255.255.255.0	172.31.88.1	88
PC-A	NIC	172.31.10.21	255.255.255.0	172.31.10.1	10
PC-B	NIC	172.31.20.22	255.255.255.0	172.31.20.1	20
PC-C	NIC	172.31.30.23	255.255.255.0	172.31.30.1	30
PC-D	NIC	172.31.88.24	255.255.255.0	172.31.88.1	88

VLAN Table

VLAN	Name	Interfaces
10	Sales	F0/11-15
20	Production	F0/16-20
30	Marketing	F0/5-10
88	Management	F0/21-24
99	Native	G0/1

Scenario

In this activity, you will demonstrate and reinforce your ability to configure routers for inter-VLAN communication and configure static routes to reach destinations outside of your network. Among the skills you will demonstrate are configuring inter-VLAN routing, static and default routes.

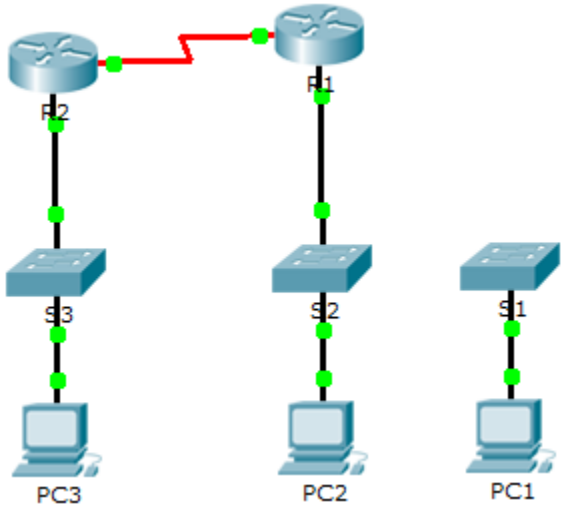
Requirements

- Configure inter-VLAN routing on **R1** based on the **Addressing Table**.
- Configure trunking on **S1**.
- Configure four directly attached static route on **HQ** to each VLANs 10, 20, 30 and 88.
- Configure directly attached static routes on **HQ** to reach **Outside Host**.
  - Configure the primary path through the Serial 0/1/0 interface.
  - Configure the backup route through the Serial 0/1/1 interface with a 10 AD.
- Configure directly attached primary and backup summary routes on **ISP** for the entire 172.31.0.0/17 address space.

  - Configure the primary path through the Serial 0/1/1 interface.
  - Configure the backup route through the Serial 0/1/0 interface with 25 AD.
- Configure a directly attached default route on **R1**.
- Verify connectivity by making sure all the PCs can ping **Outside Host**.

7.1.3.6 Packet Tracer – Investigating Convergence

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	209.165.0.1	255.255.255.0	N/A
	G0/1	64.100.0.1	255.0.0.0	N/A
	S0/0/0	192.168.1.2	255.255.255.0	N/A
R2	G0/0	10.0.0.1	255.0.0.0	N/A
	S0/0/0	192.168.1.1	255.255.255.0	N/A
PC1	NIC	64.100.0.2	255.0.0.0	64.100.0.1
PC2	NIC	209.165.0.2	255.255.255.0	209.165.0.1
PC3	NIC	10.0.0.2	255.0.0.0	10.0.0.1

Objectives

Part 1: View the Routing Table of a Converged Network

Part 2: Add a New LAN to the Topology

Part 3: Watch the Network Converge

Background

This activity will help you identify important information in routing tables and witness the process of network convergence.

Part 1: View the Routing Table of a Converged Network

Step 1: Use show commands and interpret the output.

a. Show the directly connected networks of **R1**. How many routes are connected to **R1**? _____

```
R1# show ip route connected
```

b. Show the running configuration of **R1**. What routing protocol is in use? _____

c. Are the IP addresses in the configuration advertised by RIP the same as those that are connected? ____

d. Are these IP addresses assignable, network, or broadcast? _____

e. Show the networks of **R1** learned through RIP. How many routes are there? _____

```
R1# show ip route rip
```

f. Show all of the networks that **R1** has in its routing table. What do the leading letters represent?

_____

```
R1# show ip route
```

g. Repeat step 1, a to f on **R2**. Compare the output of the two routers.

Step 2: Verify the state of the topology.

a. Ping **PC3** from **PC2**. The ping should be successful.

b. Show the interface status on **R2**. Two interfaces should have assigned addresses. Each address corresponds to a connected network.

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

c. Show the interface status on **R1**. How many interfaces have assigned addresses? _____

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

Part 2: Add a New LAN to the Topology

Step 1: Add an Ethernet cable.

a. Connect the correct Ethernet cable from **S1** to the appropriate port on **R1**.

b. Ping from **PC1** to **PC2** after the affected **S1** port turns green. Was the ping successful? _____

c. Ping from **PC1** to **PC3**. Was the ping successful? Why?

_____

Step 2: Configure a route.

a. Switch from Realtime mode to Simulation mode.

b. Enter a new route on **R1** for the 64.0.0.0 network.

```
R1(config)# router rip
R1(config-router)# network 64.0.0.0
```

c. Examine the PDUs leaving **R1**. What type are they? _____

Part 3: Watch the Network Converge

Step 1: Use debug commands.

a. Enable debugging on **R2**.

```
R2# debug ip rip
R2# debug ip routing
```

b. For reference, show the routing table of **R2** as in step 1f.

c. Click **Capture / Forward** from simulation mode. What notification appeared in the terminal of **R2**?

_____

d. According to the debugging output, how many hops away from R2 is 64.0.0.0? _____

e. What interface does **R2** send packets destined for the 64.0.0.0 network? _____

f. Show the routing table of **R2**. Record the new entry.

_____

Step 2: Verify the state of the topology.

Ping from **PC1** to **PC3**. Was the ping successful? Why?

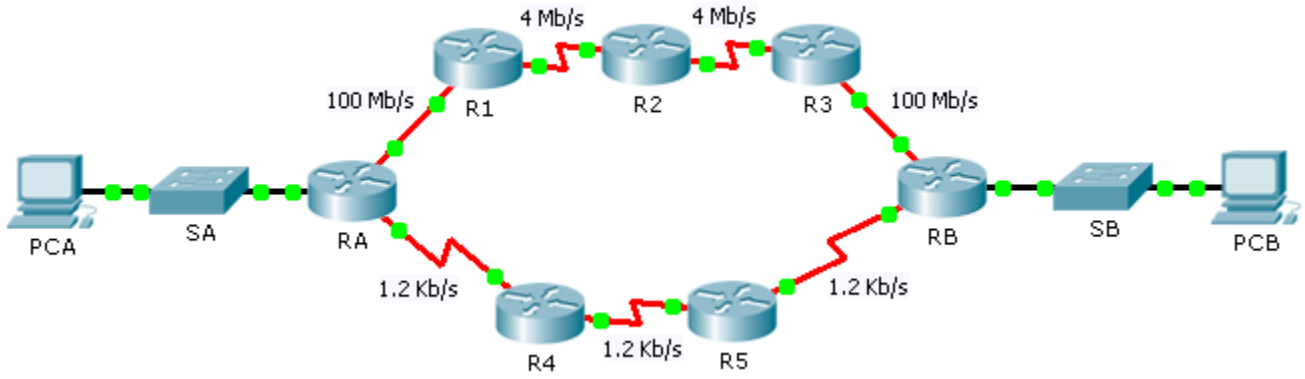
_____

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: View the Routing Table of a Converged Network.	Step 1-a	6	
	Step 1-b	6	
	Step 1-c	6	
	Step 1-d	6	
	Step 1-e	6	
	Step 1-f	6	
	Step 2-c	6	
	Part 1 Total	**42**	
Part 2: Add a New LAN to the Topology	Step 1-b	6	
	Step 1-c	6	
	Step 2-c	6	
	Part 2 Total	**18**	
Part 3: Watch the Network Converge	Step 1-c	6	
	Step 1-d	6	
	Step 1-e	6	
	Step 1-f	6	
	Step 2-a	6	
	Part 3 Total	**30**	
	Packet Tracer Score	**10**	
	Total Score	**100**	

7.2.2.4 Packet Tracer – Comparing RIP and EIGRP Path Selection

Topology



Objectives

Part 1: Predict the Path

Part 2: Trace the Route

Part 3: Reflection Questions

Scenario

PCA and **PCB** need to communicate. The path that the data takes between these end devices can travel through **R1**, **R2**, and **R3,** or it can travel through **R4** and **R5**. The process by which routers select the best path depends on the routing protocol. We will examine the behavior of two distance vector routing protocols, Enhanced Interior Gateway Routing Protocol (EIGRP) and Routing Information Protocol version 2 (RIPv2).

Part 1: Predict the Path

Metrics are factors that can be measured. Routing protocols are each designed to consider various metrics when considering which route is the best to send data along. These metrics include, hop count, bandwidth, delay, reliability, path cost, and more.

Step 1: Consider EIGRP Metrics.

a. EIGRP can consider many metrics. By default, however, bandwidth and delay are used to determine best path selection.

b. Based on the metrics, what path would you predict data would take from **PCA** to **PCB**?

_____

Step 2: Consider RIP Metrics.

a. What metric(s) are used by RIP? _____

b. Based on the metrics, what path would you predict data would take from **PCA** to **PCB**?

_____

Part 2: Trace the Route

Step 1: Examine the EIGRP Path.

a. On **RA**, view the routing table using the appropriate command. Which protocol codes are listed in the table and what protocols do they represent? _____

b. Trace the route from **PCA** to **PCB**.

What path does the data take? _____

How many hops away is the destination? _____

What is the minimum bandwidth on the path? _____

Step 2: Examine the RIPv2 Path.

You may have noticed that, while RIPv2 is configured, the routers ignore the routes that it generates, because they prefer EIGRP. Cisco routers use a scale called administrative distance and we need to change that number for RIPv2 in **RA** to make the router prefer the protocol.

a. For reference purposes, show the routing table of **RA** using the appropriate command. What is the first number between the brackets in each EIGRP route entry? _____

b. Set the administrative distance for RIPv2 using the following commands. This forces **RA** to choose RIP routes over EIGRP routes.

```
RA(config)# router rip
RA(config-router)# distance 89
```

c. Wait a minute and show the routing table again. Which protocol codes are listed in the table and what protocols do they represent? _____

d. Trace the route from **PCA** to **PCB**.

What path does the data take? _____

How many hops away is the destination? _____

What is the minimum bandwidth on the path? _____

e. What is the first number between the brackets in each RIP entry? _____

Part 3: Reflection Questions

1. What metrics does the RIPv2 routing protocol ignore? _____

   How could this affect its performance? _____

2. What metrics does the EIGRP routing protocol ignore? _____

   How could this affect its performance?

   _____

3. Which do you prefer for your own Internet access, lower hops or more bandwidth? _____

4. Is one routing protocol suitable for all applications? Why?

   _____

   _____

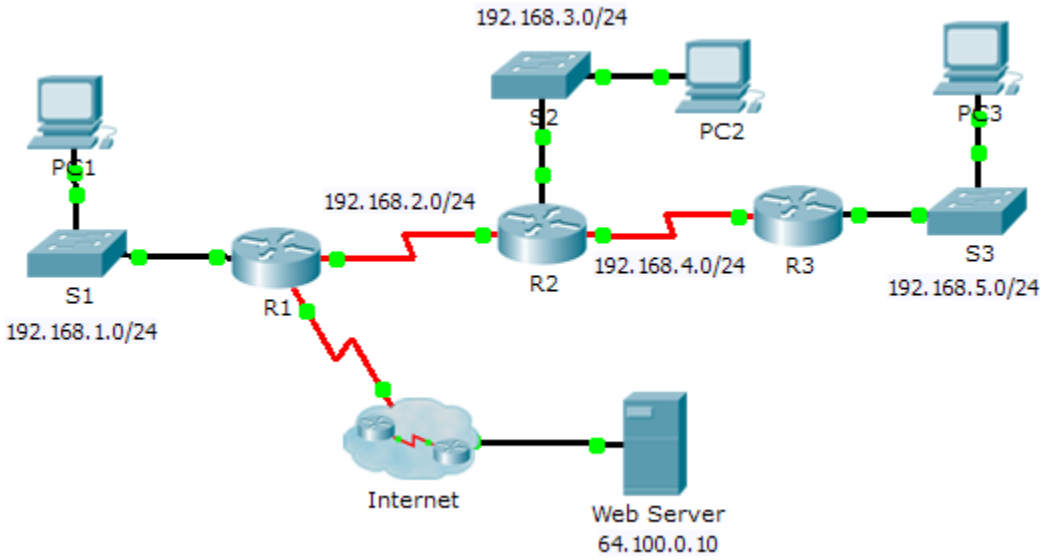
   _____

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Predict the Path	Step 1-b	8	
	Step 2-a	8	
	Step 2-b	8	
	Part 1 Total	**24**	
Part 2: Trace the Route	Step 1-a	8	
	Step 1-b	8	
	Step 2-a	8	
	Step 2-c	8	
	Step 2-d	8	
	Step 2-e	8	
	Part 2 Total	**48**	
Part 3: Reflection Questions	1	7	
	2	7	
	3	7	
	4	7	
	Part 3 Total	**28**	
	Total Score	**100**	

7.3.1.8 Packet Tracer – Configuring RIPv2

Topology



Objectives

Part 1: Configure RIPv2

Part 2: Verify Configurations

Background

Although RIP is rarely used in modern networks, it is useful as a foundation for understanding basic network routing. In this activity, you will configure a default route, RIP version 2, with appropriate network statements and passive interfaces, and verify full connectivity.

Part 1: Configure RIPv2

Step 1: Configure RIPv2 on R1.

a. Use the appropriate command to create a default route on **R1** for all Internet traffic to exit the network through S0/0/1.

b. Enter RIP protocol configuration mode.

c. Use version 2 of the RIP protocol and disable the summarization of networks.

d. Configure RIP for the networks that connect to **R1**.

e. Configure the LAN port that contains no routers so that it does not send out any routing information.

f. Advertise the default route configured in step 1a with other RIP routers.

g. Save the configuration.

Step 2: Configure RIPv2 on R2.

a. Enter RIP protocol configuration mode.

b. Use version 2 of the RIP protocol and disable the summarization of networks.

c. Configure RIP for the networks directly connected to **R2**.

d. Configure the interface that contains no routers so that it does not send out routing information.

e. Save the configuration.

Step 3: Configure RIPv2 on R3

Repeat Step 2 on **R3**.

Part 2: Verify Configurations

Step 1: View routing tables of R1, R2, and R3.

a. Use the appropriate command to show the routing table of **R1**. RIP (R) now appears with connected (C) and local (L) routes in the routing table. All networks have an entry. You also see a default route listed.

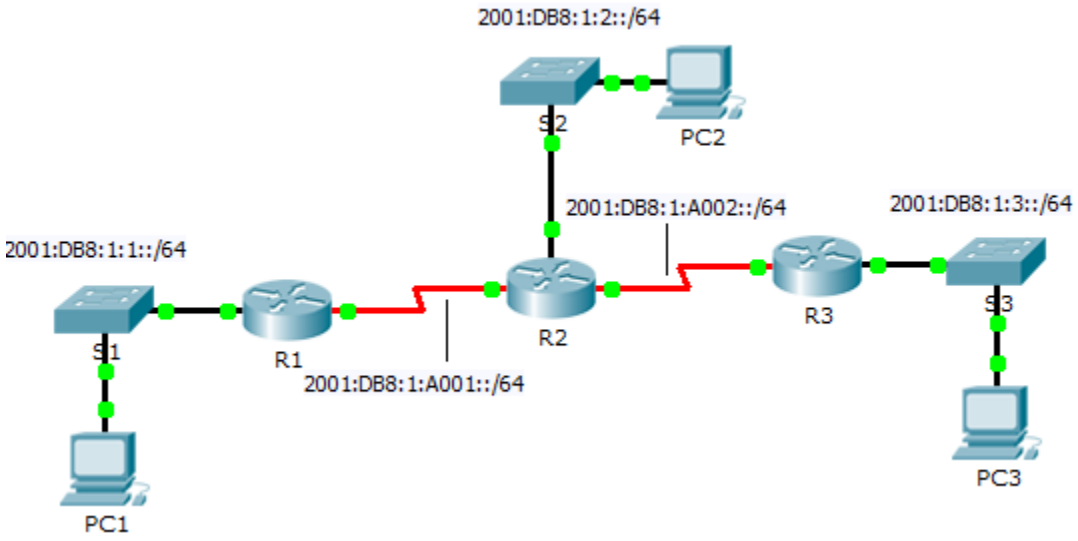
b. View the routing tables for **R2** and **R3**. Notice that each router has a full listing of all the 192.168.x.0 networks and a default route.

Step 2: Verify full connectivity to all destinations.

Every device should now be able to ping every other device inside the network. In addition, all devices should be able to ping the **Web Server**.

7.3.2.3 Packet Tracer – Configuring RIPng

Topology



Addressing Table

Device	Interface	IPv6 Address/Prefix
R1	G0/0	2001:DB8:1:1::1/64
	S0/0/0	2001:DB8:1:A001::1/64
R2	G0/0	2001:DB8:1:2::1/64
	S0/0/0	2001:DB8:1:A001::2/64
	S0/0/1	2001:DB8:1:A002::1/64
R3	G0/0	2001:DB8:1:3::1/64
	S0/0/1	2001:DB8:1:A002::2/64

Objectives

Part 1: Configure RIPng

Part 2: Verify Configurations and Connectivity

Background

RIPng (RIP Next Generation) is a distance vector routing protocol for routing IPv6 addresses. RIPng is based on RIPv2 and has the same administrative distance and 15 hop limitation. This activity will help you become more familiar with RIPng.

Part 1: Configure RIPng

Step 1: Configure RIPng on R1.

a. Enable IPv6 routing on **R1**.

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

b. Enter RIPng protocol configuration mode.

```
R1(config)# ipv6 router rip CISCO
```

c. Enable RIPng for the networks that connect to **R1**.

```
R1(config-rtr)# int g0/0
R1(config-if)# ipv6 rip CISCO enable
R1(config-if)# int s0/0/0
R1(config-if)# ipv6 rip CISCO enable
```

d. Save the configuration.

Step 2: Configure RIPng on R2 and R3

Repeat Step 1a to Step 1d on **R2** and **R3**.

Part 2: Verify Configurations and Connectivity

Step 1: View routing tables of R1, R2, and R3.

a. Use the appropriate command to view the routing table for **R1**. RIPng (R) now appear with connected (C) and local (L) routes in the routing table. All networks have an entry.

b. Verify that the appropriate interfaces are using RIPng.

```
R1# show ipv6 protocols
```

c. View the running configuration of **R1**. RIPng entries are present.

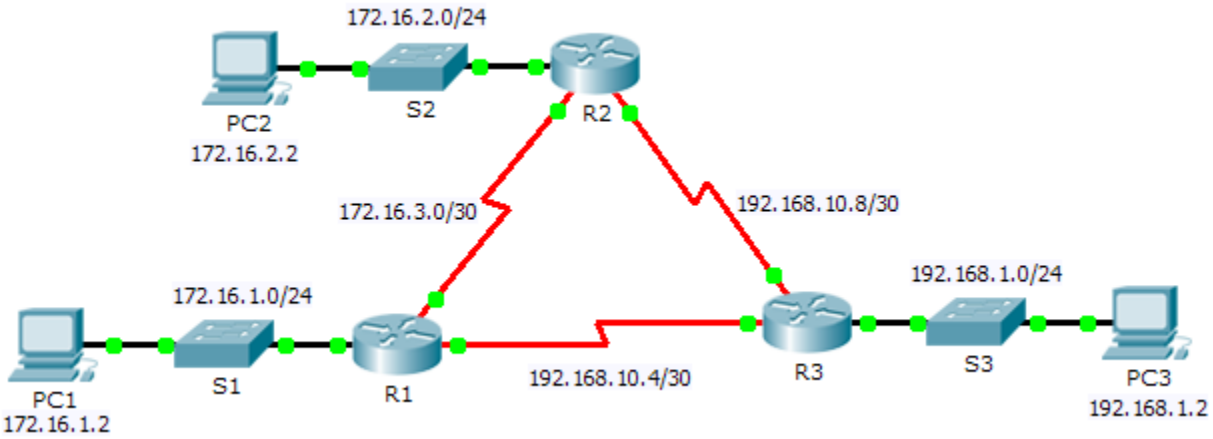
d. Repeat Step 1a to Step 1c with **R2** and **R3** to verify that they were properly configured.

Step 2: Verify full connectivity.

Every device should now be able to ping every other device. If not, review your configurations for errors and implement appropriate solutions.

8.2.2.7 Packet Tracer – Configuring OSPFv2 in a Single Area

Topology



Addressing Table

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

Objectives

Part 1: Configure OSPFv2 Routing

Part 2: Verify the Configurations

Background

In this activity, the IP addressing is already configured. You are responsible for configuring the three router topology with basic single area OSPFv2 and then verifying connectivity between end devices.

Part 1: Configure OSPFv2 Routing

Step 1: Configure OSPF on the R1, R2 and R3.

Use the following requirements to configure OSPF routing on all three routers:

- Process ID 10
- Router ID for each router: R1 = 1.1.1.1; R2 = 2.2.2.2; R3 = 3.3.3.3
- Network address for each interface
- LAN interface set to passive (do not use the **default** keyword)

Step 2: Verify OSPF routing is operational.

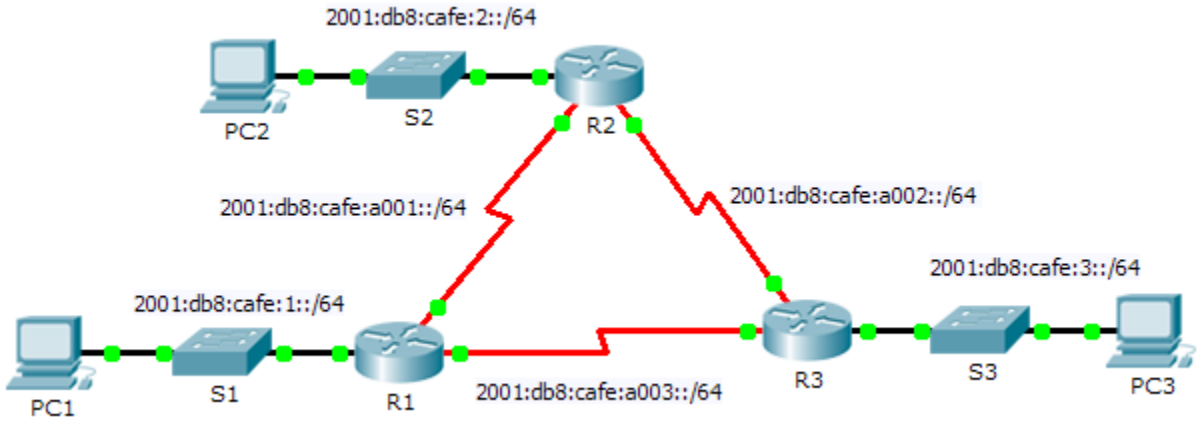
On each router, the routing table should now have a route to every network in the topology.

Part 2: Verify the Configurations

Each PC should be able to ping the other two PCs. If not, check your configurations.

8.3.3.5 Packet Tracer – Configuring Basic OSPFv3 in a Single Area

Topology



Addressing Table

Device	Interface	IPv6 Address/Prefix	Default Gateway
R1	F0/0	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
R2	F0/0	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
R3	F0/0	2001:db8:cafe:3::1/64	N/A
	S0/0/0	2001:db8:cafe:a003::264	N/A
	S0/0/1	2001:db8:cafe:a002::2/64	N/A
PC1	NIC	2001:db8:cafe:1::10/64	fe80::1
PC2	NIC	2001:db8:cafe:2::10/64	fe80::2
PC3	NIC	2001:db8:cafe:3::10/64	fe80::3

Objectives

Part 1: Configure OSPFv3 Routing

Part 2: Verify Connectivity

Background

In this activity, the IPv6 addressing is already configured. You are responsible for configuring the three router topology with basic single area OSPFv3 and then verifying connectivity between end devices.

Part 1: Configure OSPFv3 Routing

Step 1: Configure OSPFv3 on R1, R2 and R3.

Use the following requirements to configure OSPF routing on all three routers:

- Enable IPv6 routing
- Process ID 10
- Router ID for each router: R1 = 1.1.1.1; R2 = 2.2.2.2; R3 = 3.3.3.3
- Enable OSPFv3 on each interface

Note: Packet Trace version 6.0.1 does not support the **auto-cost reference-bandwidth** command, so you will not be adjust bandwidth costs in this activity.

Step 2: Verify OSPF routing is operational.

Verify each router has established adjacency with the other two routers. Verify the routing table has a route to every network in the topology.

Part 2: Verify Connectivity

Each PC should be able to ping the other two PCs. If not, check your configurations.

Note: This activity is graded using only connectivity tests. The instructions window will not show your score. To see your score, click **Check Results** > **Assessment Items**. To see the results of a specific connectivity test, click **Check Results** > **Connectivity Tests**.

8.4.1.2 Packet Tracer – Skills Integration Challenge

Addressing Table

Device	Interface	IPv4 Address / IPv6 Address/Prefix	Subnet Mask	Default Gateway
RA	G0/0	172.31.0.1	255.255.254.0	N/A
	S0/1/0	172.31.4.1	255.255.255.252	N/A
RB	G0/0	172.31.2.1	255.255.254.0	N/A
		2001:DB8:1::1/64		N/A
	S0/0/0	172.31.4.2	255.255.255.252	N/A
	S0/0/1	2001:DB8:2::1/64		N/A
RC	G0/0	2001:DB8:3::1/64		N/A
	S0/0/0	2001:DB8:2::2/64		N/A
PC-A	NIC			
PC-B	NIC			
PC-C	NIC			

Background

In this Skills Integration Challenge, your focus is OSPFv2 and OSPFv3 configurations. You will configure IP addressing for all devices. Then you will configure OSPFv2 routing for the IPv4 portion of the network and OSPFv3 routing for the IPv6 portion of the network. One router will be configured with both IPv4 and IPv6 configurations. Finally, you will verify your configurations and test connectivity between end devices.

Note: This activity is graded using a combination of assessment items and connectivity tests. The instructions window will not show your score. To see your score, click **Check Results** > **Assessment Items**. To see the results of a specific connectivity test, click **Check Results** > **Connectivity Tests**.

Requirements

- Use the following requirements to configure **RA** addressing and OSPFv2 routing:
  - IPv4 addressing according to the Addressing Table
  - Process ID 1
  - Router ID 1.1.1.1
  - Network address for each interface
  - LAN interface set to passive (do not use the **default** keyword)
- Use the following requirements to configure **RB** addressing, OSPFv2 routing and OSPFv3 routing:
  - IPv4 and IPv6 addressing according to the Addressing Table

    Set the Gigabit Ethernet 0/0 Link Local address to FE80::1

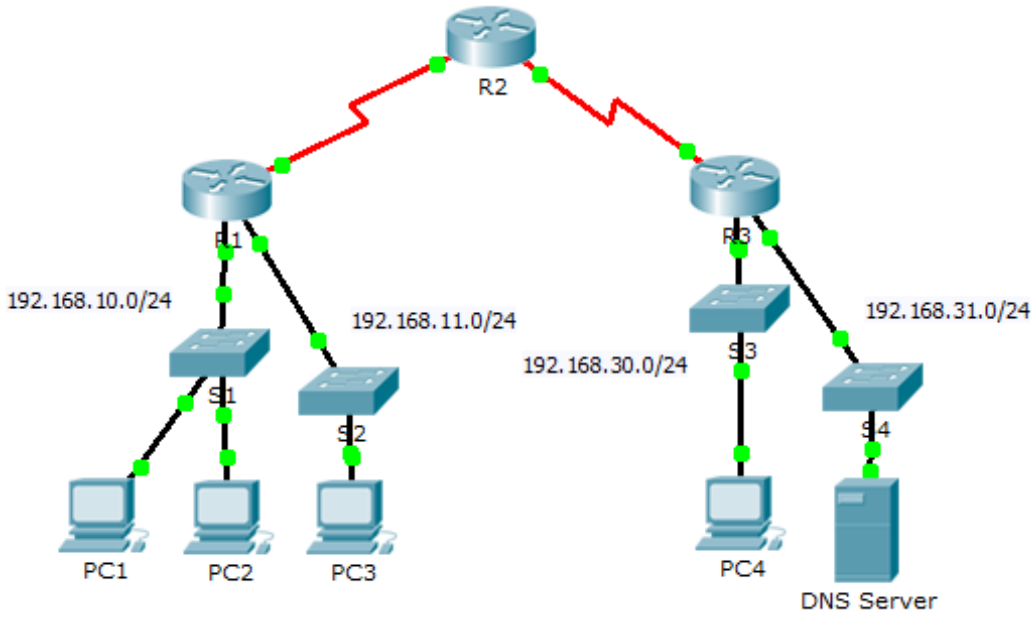
- OSPFv2 routing requirements:
  - Process ID 1
  - Router ID 2.2.2.2
  - Network address for each interface
  - LAN interface set to passive (do not use the **default** keyword)
- OSPFv3 routing requirements:
  - Enable IPv6 routing
  - Process ID 1
  - Router ID 2.2.2.2
  - Enable OSPFv3 on each interface

- Use the following requirements to configure **RC** addressing and OSPFv3 routing:
  - IPv6 addressing according to the Addressing Table
    - Set the Gigabit Ethernet 0/0 Link Local address to FE80::3
  - OSPFv3 routing requirements:
    - Enable IPv6 routing
    - Process ID 1
    - Router ID 3.3.3.3
    - Enable OSPFv3 on each interface
- Configure PCs with appropriate addressing.
  - **PCA** and **PCB** IPv4 addressing must use the last assignable address in the IPv4 subnet.
  - **PCB** and **PCC** IPv6 addressing must use the second assignable address in the IPv6 network and the link-local FE80 address as the default gateway.
  - Finish the Addressing Table documentation
- Verify your configurations and test connectivity
  - OSPF neighbors should be established and routing tables should be complete
  - Pings between PCA and PCB should be successful
  - Pings between PCB and PCC should be successful

    Note: If OSPFv3 has not converged, check the status of interfaces using the **show ip ospf interface** command. Sometimes, the OSPFv3 process needs to be removed and reapplied to force convergence.

9.1.1.6 Packet Tracer – Access Control List Demonstration

Topology



Objectives

Part 1: Verify Local Connectivity and Test Access Control List

Part 2: Remove Access Control List and Repeat Test

Background

In this activity, you will observe how an access control list (ACL) can be used to prevent a ping from reaching hosts on remote networks. After removing the ACL from the configuration, the pings will be successful.

Part 1: Verify Local Connectivity and Test Access Control List

Step 1: Ping devices on the local network to verify connectivity.

a. From the command prompt of **PC1**, ping **PC2**.

b. From the command prompt of **PC1**, ping **PC3**.

Why were the pings successful? _____

_____

Step 2: Ping devices on remote networks to test ACL functionality.

a. From the command prompt of **PC1**, ping **PC4**.

b. From the command prompt of **PC1**, ping the **DNS Server**.

Why did the pings fail? (Hint: Use simulation mode or view the router configurations to investigate.)

_____

Part 2: Remove ACL and Repeat Test

Step 1: Use show commands to investigate the ACL configuration.

a. Use the **show run** and **show access-lists** commands to view the currently configured ACLs. To quickly view the current ACLs, use **show access-lists**. Enter the **show access-lists** command, followed by a space and a question mark (?) to view the available options:

```
R1#show access-lists ?
  <1-199>  ACL number
  WORD     ACL name
  <cr>
```

If you know the ACL number or name, you can filter the **show** output further. However, **R1** only has one ACL; therefore, the **show access-lists** command will suffice.

```
R1#show access-lists
Extended IP access list 101
    deny icmp any any echo
    permit ip any any
```

The first line of the ACL prevents Internet Control Message Protocol (ICMP) echos (ping requests) from **any** source to **any** destination. The second line of the ACL allows all other **ip** traffic from **any** source to **any** destination.

b. For an ACL to impact router operation, it must be applied somewhere. In this scenario, the ACL is used to filter traffic on an interface. Although you can view IP information with the **show ip interface** command, it may be more efficient in some situations to simply use the **show run** command. Using one or both of these commands, to which interface is the ACL applied to? _____

Step 2: Remove access list 101 from the configuration

You can remove ACLs from the configuration by issuing the **no access list** [*number of the ACL*] command. The **no access-list** command deletes all ACLs configured on the router; the **no access-list** [*number of the ACL*] command removes only a specific ACL.

a. In global configuration mode, remove the ACL by entering the following command:

```
R1(config)# no access-list 101
```

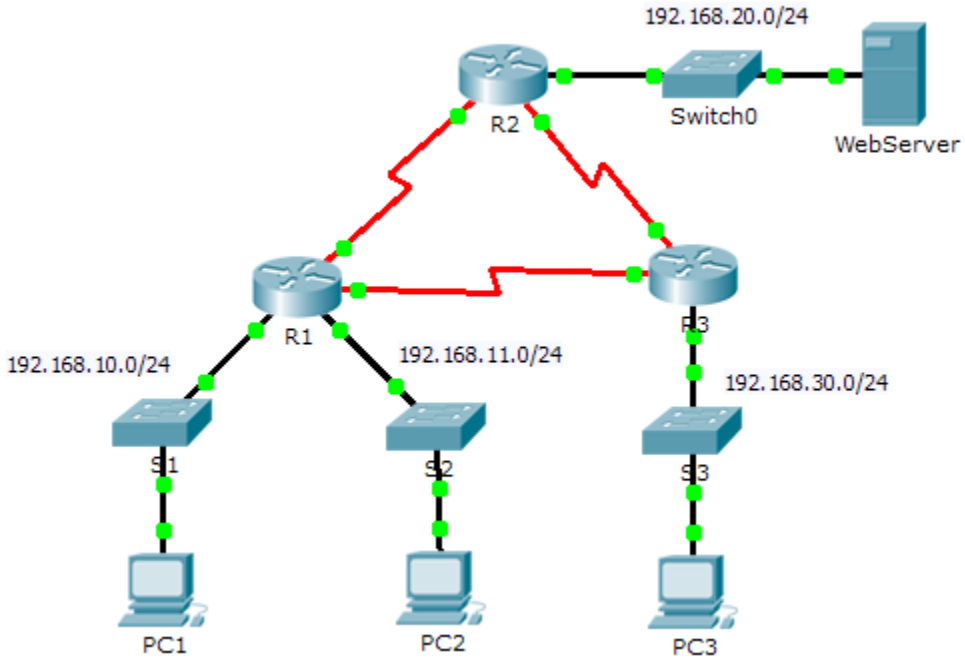
b. Verify that **PC1** can now ping the **DNS Server**.

Suggested Scoring Rubric

Question Location	Possible Points	Earned Points
Part 1, Step 1 b.	50	
Part 1, Step 2 b.	40	
Part 2, Step 2 b.	10	
Total Score	**100**	

9.2.1.10 Packet Tracer - Configuring Standard ACLs

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	F0/0	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	F0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Objectives

Part 1: Plan an ACL Implementation

Part 2: Configure, Apply, and Verify a Standard ACL

Background / Scenario

Standard access control lists (ACLs) are router configuration scripts that control whether a router permits or denies packets based on the source address. This activity focuses on defining filtering criteria, configuring standard ACLs, applying ACLs to router interfaces, and verifying and testing the ACL implementation. The routers are already configured, including IP addresses and Enhanced Interior Gateway Routing Protocol (EIGRP) routing.

Part 1: Plan an ACL Implementation

Step 1: Investigate the current network configuration.

Before applying any ACLs to a network, it is important to confirm that you have full connectivity. Verify that the network has full connectivity by choosing a PC and pinging other devices on the network. You should be able to successfully ping every device.

Step 2: Evaluate two network policies and plan ACL implementations.

a. The following network policies are implemented on **R2**:

- The 192.168.11.0/24 network is not allowed access to the **WebServer** on the 192.168.20.0/24 network.
- All other access is permitted.

To restrict access from the 192.168.11.0/24 network to the **WebServer** at 192.168.20.254 without interfering with other traffic, an ACL must be created on **R2**. The access list must be placed on the outbound interface to the **WebServer**. A second rule must be created on **R2** to permit all other traffic.

b. The following network policies are implemented on **R3**:

- The 192.168.10.0/24 network is not allowed to communicate to the 192.168.30.0/24 network.
- All other access is permitted.

To restrict access from the 192.168.10.0/24 network to the 192.168.30/24 network without interfering with other traffic, an access list will need to be created on **R3**. The ACL must placed on the outbound interface to **PC3**. A second rule must be created on **R3** to permit all other traffic.

Part 2: Configure, Apply, and Verify a Standard ACL

Step 1: Configure and apply a numbered standard ACL on R2.

a. Create an ACL using the number 1 on **R2** with a statement that denies access to the 192.168.20.0/24 network from the 192.168.11.0/24 network.

```
R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255
```

b. By default, an access list denies all traffic that does not match a rule. To permit all other traffic, configure the following statement:

```
R2(config)# access-list 1 permit any
```

c. For the ACL to actually filter traffic, it must be applied to some router operation. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# ip access-group 1 out
```

Step 2: Configure and apply a numbered standard ACL on R3.

a. Create an ACL using the number 1 on **R3** with a statement that denies access to the 192.168.30.0/24 network from the **PC1** (192.168.10.0/24) network.

```
R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255
```

b. By default, an ACL denies all traffic that does not match a rule. To permit all other traffic, create a second rule for ACL 1.

```
R3(config)# access-list 1 permit any
```

c. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.

```
R3(config)# interface GigabitEthernet0/0
R3(config-if)# ip access-group 1 out
```

Step 3: Verify ACL configuration and functionality.

a. On **R2** and **R3**, enter the **show access-list** command to verify the ACL configurations. Enter the **show run** or **show ip interface gigabitethernet 0/0** command to verify the ACL placements.

b. With the two ACLs in place, network traffic is restricted according to the policies detailed in Part 1. Use the following tests to verify the ACL implementations:

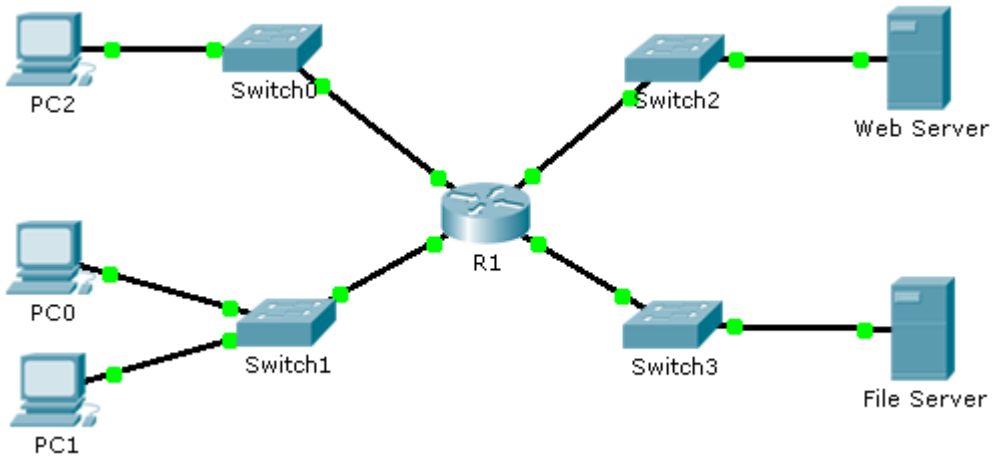
- A ping from 192.168.10.10 to 192.168.11.10 succeeds.
- A ping from 192.168.10.10 to 192.168.20.254 succeeds.
- A ping from 192.168.11.10 to 192.168.20.254 fails.

- A ping from 192.168.10.10 to 192.168.30.10 fails.
- A ping from 192.168.11.10 to 192.168.30.10 succeeds.
- A ping from 192.168.30.10 to 192.168.20.254 succeeds.

9.2.1.11

Packet Tracer - Configuring Named Standard ACLs

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.20.1	255.255.255.0	N/A
	E0/0/0	192.168.100.1	255.255.255.0	N/A
	E0/1/0	192.168.200.1	255.255.255.0	N/A
File Server	NIC	192.168.200.100	255.255.255.0	192.168.200.1
Web Server	NIC	192.168.100.100	255.255.255.0	192.168.100.1
PC0	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC1	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC2	NIC	192.168.10.3	255.255.255.0	192.168.10.1

Objectives

Part 1: Configure and Apply a Named Standard ACL

Part 2: Verify the ACL Implementation

Background / Scenario

The senior network administrator has tasked you to create a standard named ACL to prevent access to a file server. All clients from one network and one specific workstation from a different network should be denied access.

Part 1: Configure and Apply a Named Standard ACL

Step 1: Verify connectivity before the ACL is configured and applied.

All three workstations should be able to ping both the **Web Server** and **File Server**.

Step 2: Configure a named standard ACL.

Configure the following named ACL on **R1**.

```
R1(config)# ip access-list standard File_Server_Restrictions
R1(config-std-nacl)# permit host 192.168.20.4
R1(config-std-nacl)# deny any
```

Note: For scoring purposes, the ACL name is case-sensitive.

Step 3: Apply the named ACL.

a. Apply the ACL outbound on the interface Fast Ethernet 0/1.

```
R1(config-if)# ip access-group File_Server_Restrictions out
```

b. Save the configuration.

Part 2: Verify the ACL Implementation

Step 1: Verify the ACL configuration and application to the interface.

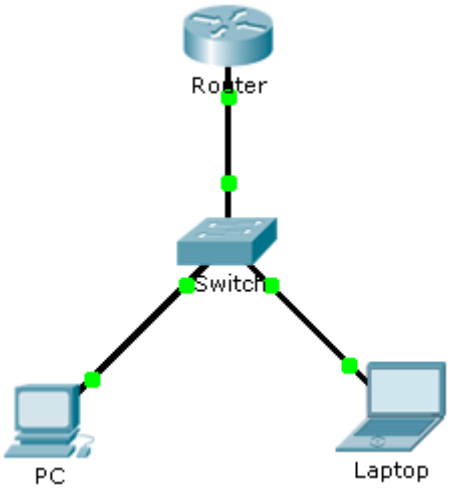
Use the **show access-lists** command to verify the ACL configuration. Use the **show run** or **show ip interface fastethernet 0/1** command to verify that the ACL is applied correctly to the interface.

Step 2: Verify that the ACL is working properly.

All three workstations should be able to ping the **Web Server**, but only **PC1** should be able to ping the **File Server**.

9.2.3.3 Packet Tracer - Configuring an ACL on VTY Lines

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router	F0/0	10.0.0.254	255.0.0.0	N/A
PC	NIC	10.0.0.1	255.0.0.0	10.0.0.254
Laptop	NIC	10.0.0.2	255.0.0.0	10.0.0.254

Objectives

Part 1: Configure and Apply an ACL to VTY Lines

Part 2: Verify the ACL Implementation

Background

As network administrator, you must have remote access to your router. This access should not be available to other users of the network. Therefore, you will configure and apply an access control list (ACL) that allows **PC** access to the Telnet lines, but denies all other source IP addresses.

Part 1: Configure and Apply an ACL to VTY Lines

Step 1: Verify Telnet access before the ACL is configured.

Both computers should be able to Telnet to the **Router**. The password is **cisco**.

Step 2: Configure a numbered standard ACL.

Configure the following numbered ACL on **Router**.

```
Router(config)# access-list 99 permit host 10.0.0.1
```

Because we do not want to permit access from any other computers, the implicit deny property of the access list satisfies our requirements.

Step 3: Place a named standard ACL on the router.

Access to the **Router** interfaces must be allowed, while Telnet access must be restricted. Therefore, we must place the ACL on Telnet lines 0 through 4. From the configuration prompt of **Router**, enter line configuration mode for lines 0 – 4 and use the **access-class** command to apply the ACL to all the VTY lines:

```
Router(config)# line vty 0 15
Router(config-line)# access-class 99 in
```

Part 2: Verify the ACL Implementation

Step 1: Verify the ACL configuration and application to the VTY lines.

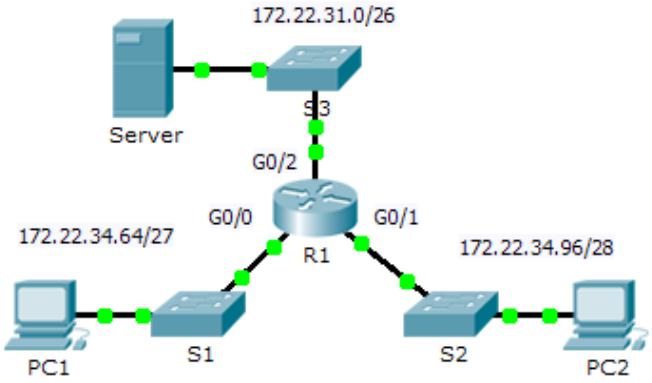
Use the **show access-lists** to verify the ACL configuration. Use the **show run** command to verify the ACL is applied to the VTY lines.

Step 2: Verify that the ACL is working properly.

Both computers should be able to ping the **Router**, but only **PC** should be able to Telnet to it.

9.3.2.10 Packet Tracer - Configuring Extended ACLs - Scenario 1

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.22.34.65	255.255.255.224	N/A
	G0/1	172.22.34.97	255.255.255.240	N/A
	G0/2	172.22.34.1	255.255.255.192	N/A
Server	NIC	172.22.34.62	255.255.255.192	172.22.34.1
PC1	NIC	172.22.34.66	255.255.255.224	172.22.34.65
PC2	NIC	172.22.34.98	255.255.255.240	172.22.34.97

Objectives

Part 1: Configure, Apply and Verify an Extended Numbered ACL

Part 2: Configure, Apply and Verify an Extended Named ACL

Background / Scenario

Two employees need access to services provided by the server. **PC1** only needs FTP access while **PC2** only needs web access. Both computers are able to ping the server, but not each other.

Part 1: Configure, Apply and Verify an Extended Numbered ACL

Step 1: Configure an ACL to permit FTP and ICMP.

a. From global configuration mode on **R1**, enter the following command to determine the first valid number for an extended access list.

```
R1(config)# access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
```

b. Add **100** to the command, followed by a question mark.

```
R1(config)# access-list 100 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
```

c. To permit FTP traffic, enter **permit,** followed by a question mark.

```
R1(config)# access-list 100 permit ?
  ahp    Authentication Header Protocol
  eigrp  Cisco's EIGRP routing protocol
  esp    Encapsulation Security Payload
  gre    Cisco's GRE tunneling
  icmp   Internet Control Message Protocol
  ip     Any Internet Protocol
  ospf   OSPF routing protocol
  tcp    Transmission Control Protocol
  udp    User Datagram Protocol
```

d. This ACL permits FTP and ICMP. ICMP is listed above, but FTP is not, because FTP uses TCP. So you enter TCP. Enter **tcp** to further refine the ACL help.

```
R1(config)# access-list 100 permit tcp ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
```

e. Notice that we could filter just for **PC1** by using the **host** keyword or we could allow **any** host. In this case, any device is allowed that has an address belonging to the 172.22.34.64/27 network. Enter the network address, followed by a question mark.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 ?
  A.B.C.D  Source wildcard bits
```

f. Calculate the wildcard mask determining the binary opposite of a subnet mask.

11111111.11111111.11111111.11100000 = 255.255.255.224
00000000.00000000.00000000.000**11111** = 0.0.0.31

g. Enter the wildcard mask, followed by a question mark.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?
  A.B.C.D  Destination address
  any      Any destination host
  eq       Match only packets on a given port number
  gt       Match only packets with a greater port number
  host     A single destination host
  lt       Match only packets with a lower port number
  neq      Match only packets not on a given port number
  range    Match only packets in the range of port numbers
```

h. Configure the destination address. In this scenario, we are filtering traffic for a single destination, the server. Enter the **host** keyword followed by the server's IP address.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 ?
  dscp         Match packets with given dscp value
  eq           Match only packets on a given port number
  established  established
  gt           Match only packets with a greater port number
  lt           Match only packets with a lower port number
  neq          Match only packets not on a given port number
  precedence   Match packets with given precedence value
  range        Match only packets in the range of port numbers
  <cr>
```

i. Notice that one of the options is **<cr>** (carriage return). In other words, you can press **Enter** and the statement would permit all TCP traffic. However, we are only permitting FTP traffic; therefore, enter the **eq** keyword, followed by a question mark to display the available options. Then, enter **ftp** and press **Enter**.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ?
  <0-65535>  Port number
  ftp        File Transfer Protocol (21)
  pop3       Post Office Protocol v3 (110)
  smtp       Simple Mail Transport Protocol (25)
  telnet     Telnet (23)
  www        World Wide Web (HTTP, 80)
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ftp
```

j. Create a second access list statement to permit ICMP (ping, etc.) traffic from **PC1** to **Server**. Note that the access list number remains the same and a specific type of ICMP traffic does not need to be specified.

```
R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host
172.22.34.62
```

k. All other traffic is denied, by default.

Step 2: Apply the ACL on the correct interface to filter traffic.

From **R1**'s perspective, the traffic that ACL 100 applies to is inbound from the network connected to Gigabit Ethernet 0/0 interface. Enter interface configuration mode and apply the ACL.

```
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip access-group 100 in
```

Step 3: Verify the ACL implementation.

a. Ping from **PC1** to **Server**. If the pings are unsuccessful, verify the IP addresses before continuing.

b. FTP from **PC1** to **Server**. The username and password are both **cisco**.

```
PC> ftp 172.22.34.62
```

c. Exit the FTP service of the **Server**.

```
ftp> quit
```

d. Ping from **PC1** to **PC2**. The destination host should be unreachable, because the traffic was not explicitly permitted.

Part 2: Configure, Apply and Verify an Extended Named ACL

Step 1: Configure an ACL to permit HTTP access and ICMP.

a. Named ACLs start with the **ip** keyword. From global configuration mode of **R1**, enter the following command, followed by a question mark.

```
R1(config)# ip access-list ?
  extended  Extended Access List
  standard  Standard Access List
```

b. You can configure named standard and extended ACLs. This access list filters both source and destination IP addresses; therefore, it must be extended. Enter **HTTP_ONLY** as the name. (For Packet Tracer scoring, the name is case-sensitive.)

```
R1(config)# ip access-list extended HTTP_ONLY
```

c. The prompt changes. You are now in extended named ACL configuration mode. All devices on the **PC2** LAN need TCP access. Enter the network address, followed by a question mark.

```
R1(config-ext-nacl)# permit tcp 172.22.34.96 ?
  A.B.C.D  Source wildcard bits
```

d. An alternative way to calculate a wildcard is to subtract the subnet mask from 255.255.255.255.

```
  255.255.255.255
- 255.255.255.240
-----------------
=   0.  0.  0. 15
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 ?
```

e. Finish the statement by specifying the server address as you did in Part 1 and filtering **www** traffic.

```
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
```

f. Create a second access list statement to permit ICMP (ping, etc.) traffic from **PC2** to **Server**. Note: The prompt remains the same and a specific type of ICMP traffic does not need to be specified.

```
R1(config-ext-nacl)# permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
```

g. All other traffic is denied, by default. Exit out of extended named ACL configuration mode.

Step 2: Apply the ACL on the correct interface to filter traffic.

From **R1**'s perspective, the traffic that access list **HTTP_ONLY** applies to is inbound from the network connected to Gigabit Ethernet 0/1 interface. Enter the interface configuration mode and apply the ACL.

```
R1(config)# interface gigabitEthernet 0/1
R1(config-if)# ip access-group HTTP_ONLY in
```

Step 3: Verify the ACL implementation.

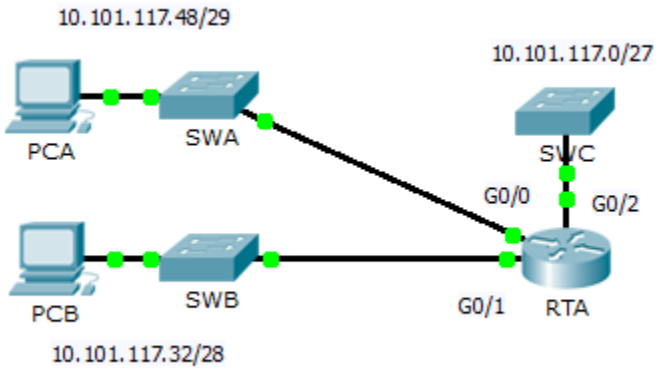
a. Ping from **PC2** to **Server**. If the pings unsuccessful, verify the IP addresses before continuing.

b. FTP from **PC2** to **Server**. The connection should fail.

c. Open the web browser on **PC2** and enter the IP address of **Server** as the URL. The connection should be successful.

9.3.2.11 Packet Tracer - Configuring Extended ACLs - Scenario 2

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	G0/0	10.101.117.49	255.255.255.248	N/A
	G0/1	10.101.117.33	255.255.255.240	N/A
	G0/2	10.101.117.1	255.255.255.224	N/A
PCA	NIC	10.101.117.51	255.255.255.248	10.101.117.49
PCB	NIC	10.101.117.35	255.255.255.240	10.101.117.33
SWC	VLAN1	10.101.117.2	255.255.255.224	10.101.117.1

Objectives

Part 1: Configure, Apply and Verify an Extended Numbered ACL

Part 2: Reflection Questions

Background / Scenario

In this scenario, devices on one LAN are allowed to remotely access devices in another LAN using the Telnet protocol. Besides ICMP, all traffic from other networks is denied.

Part 1: Configure, Apply and Verify an Extended Numbered ACL

Configure, apply and verify an ACL to satisfy the following policy:

- Telnet traffic from devices on the 10.101.117.32/28 network is allowed to devices on the 10.100.117.0/27 networks.
- ICMP traffic is allowed from any source to any destination
- All other traffic is blocked.

Step 1: Configure the extended ACL.

a. From the appropriate configuration mode on **RTA**, use the last valid extended access list number to configure the ACL. Use the following steps to construct the first ACL statement:

1) The last extended list number is 199.

2) The protocol is TCP.

3) The source network is 10.101.117.32.

4) The wildcard can be determined by subtracting 255.255.255.240 from 255.255.255.255.

5) The destination network is 10.101.117.0.

6) The wildcard can be determined by subtracting 255.255.255.224 from 255.255.255.255.

7) The protocol is Telnet.

What is the first ACL statement?

_____

_____

b. ICMP is allowed, and a second ACL statement is needed. Use the same access list number to permit all ICMP traffic, regardless of the source or destination address. What is the second ACL statement? (Hint: Use the any keywords)

_____

c. All other IP traffic is denied, by default.

Step 2: Apply the extended ACL.

The general rule is to place extended ACLs close to the source. However, since access list 199 affects traffic originating from both networks 10.101.117.48/29 and 10.101.117.32/28, the best placement for this ACL might be on interface Gigabit Ethernet 0/2 in the outbound direction. What is the command to apply ACL 199 to the Gigabit Ethernet 0/2 interface?

_____

Step 3: Verify the extended ACL implementation.

a. Ping from **PCB** to all of the other IP addresses in the network. If the pings are unsuccessful, verify the IP addresses before continuing.

b. Telnet from **PCB** to **SWC**. The password is **cisco**.

c. Exit the Telnet service of the **SWC**.

d. Ping from **PCA** to all of the other IP addresses in the network. If the pings are unsuccessful, verify the IP addresses before continuing.

e. Telnet from **PCA** to **SWC**. The access list causes the router to reject the connection.

f. Telnet from **PCA** to **SWB**. The access list is placed on **G0/2** and does not affect this connection.

g. After logging into **SWB,** do not log out. Telnet to **SWC**.

Part 2: Reflection Questions

1. How was PCA able to bypass access list 199 and Telnet to SWC?

_____

2. What could have been done to prevent PCA from accessing SWC indirectly, while allowing PCB Telnet access to SWC?

_____

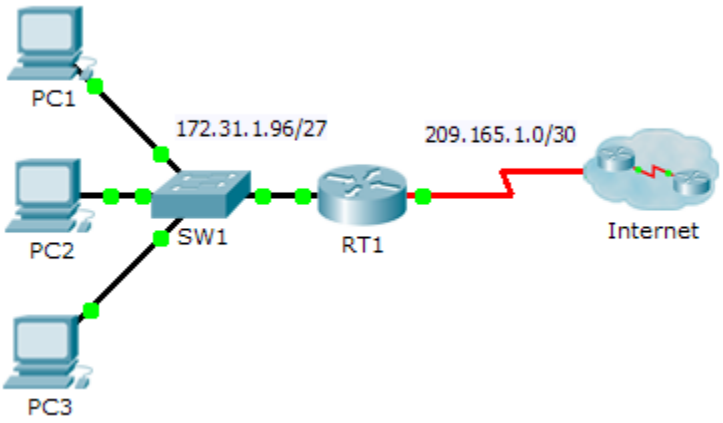
_____

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Configure, Apply and Verify an Extended Numbered ACL	Step 1a	4	
	Step 1b	4	
	Step 2	4	
	Part 1 Total	**12**	
Part 2: Reflection Questions	Question 1	4	
	Question 2	4	
	Part 2 Total	**8**	
	Packet Tracer Score	**80**	
	Total Score	**100**	

9.3.2.12 Packet Tracer - Configuring Extended ACLs - Scenario 3

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
RT1	G0/0	172.31.1.126	255.255.255.224	N/A
	S0/0/0	209.165.1.2	255.255.255.252	N/A
PC1	NIC	172.31.1.101	255.255.255.224	172.31.1.126
PC2	NIC	172.31.1.102	255.255.255.224	172.31.1.126
PC3	NIC	172.31.1.103	255.255.255.224	172.31.1.126
Server1	NIC	64.101.255.254		
Server2	NIC	64.103.255.254		

Objectives

Part 1: Configure a Named Extended ACL

Part 2: Apply and Verify the Extended ACL

Background / Scenario

In this scenario, specific devices on the LAN are allowed to various services on servers located on the Internet.

Part 1: Configure a Named Extended ACL

Use one named ACL to implement the following policy:

- Block HTTP and HTTPS access from **PC1** to **Server1** and **Server2.** The servers are inside the cloud and you only know their IP addresses.
- Block FTP access from **PC2** to **Server1** and **Server2**.

- Block ICMP access from **PC3** to **Server1** and **Server2**.

Note: For scoring purposes, you must configure the statements in the order specified in the following steps.

Step 1: Deny PC1 to access HTTP and HTTPS services on Server1 and Server2.

a. Create an extended IP access list named ACL which will deny **PC1** access to the HTTP and HTTPS services of **Server1** and **Server2**. Because it is impossible to directly observe the subnet of servers on the Internet, four rules are required.

What is the command to begin the named ACL? _____

b. Record the statement that denies access from **PC1** to **Server1**, only for HTTP (port 80).

_____

c. Record the statement that denies access from **PC1** to **Server1**, only for HTTPS (port 443).

_____

d. Record the statement that denies access from **PC1** to **Server2**, only for HTTP.

_____

e. Record the statement that denies access from **PC1** to **Server2**, only for HTTPS.

_____

Step 2: Deny PC2 to access FTP services on Server1 and Server2.

a. Record the statement that denies access from **PC2** to **Server1**, only for FTP (port 21 only).

_____

b. Record the statement that denies access from **PC2** to **Server2**, only for FTP (port 21 only).

_____

Step 3: Deny PC3 to ping Server1 and Server2.

a. Record the statement that denies ICMP access from **PC3** to **Server1**.

_____

b. Record the statement that denies ICMP access from **PC3** to **Server2**.

_____

Step 4: Permit all other IP traffic.

By default, an access list denies all traffic that does not match any rule in the list. What command permits all other traffic? _____

Part 2: Apply and Verify the Extended ACL

The traffic to be filtered is coming from the 172.31.1.96/27 network and is destined for remote networks. Appropriate ACL placement also depends on the relationship of the traffic with respect to **RT1**.

Step 1: Apply the ACL to the correct interface and in the correct direction.

a. What are the commands you need to apply the ACL to the correct interface and in the correct direction?

_____

_____

Step 2: Test access for each PC.

a. Access the websites of **Server1** and **Server2** using the Web Browser of **PC1** and using both HTTP and HTTPS protocols.

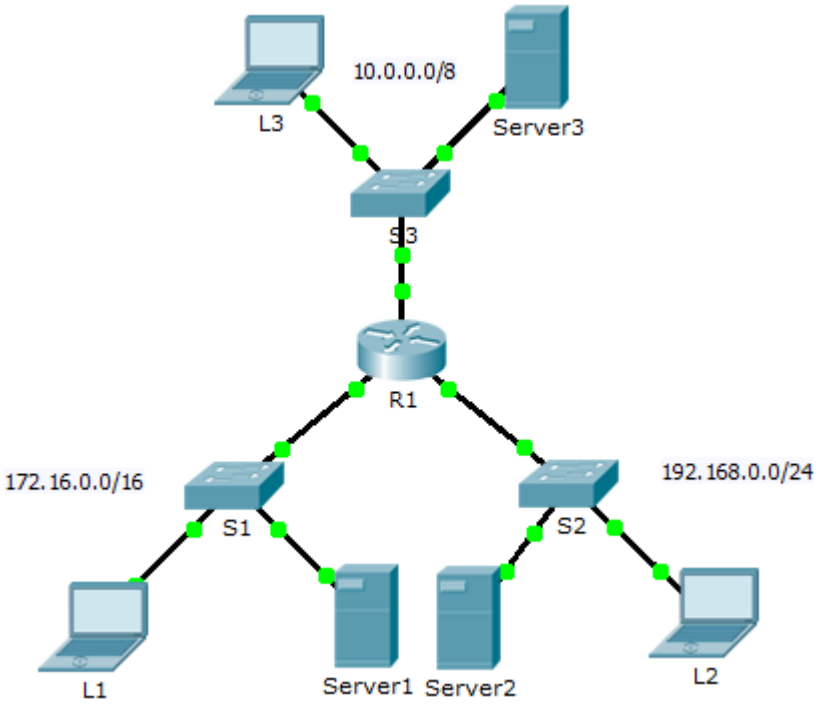
b. Access FTP of **Server1** and **Server2** using **PC1**. The username and password is "**cisco**".

c. Ping **Server1** and **Server2** from **PC1**.

d. Repeat Step 2a to Step 2c with **PC2** and **PC3** to verify proper access list operation.

9.4.2.6 Packet Tracer - Troubleshooting ACLs

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	10.0.0.1	255.0.0.0	N/A
	G0/1	172.16.0.1	255.255.0.0	N/A
	G0/2	192.168.0.1	255.255.255.0	N/A
Server1	NIC	172.16.255.254	255.255.0.0	172.16.0.1
Server2	NIC	192.168.0.254	255.255.255.0	192.168.0.1
Server3	NIC	10.255.255.254	255.0.0.0	10.0.0.1
L1	NIC	172.16.0.2	255.255.0.0	172.16.0.1
L2	NIC	192.168.0.2	255.255.255.0	192.168.0.1
L3	NIC	10.0.0.2	255.0.0.0	10.0.0.1

Objectives

Part 1: Troubleshoot ACL Issue 1

Part 2: Troubleshoot ACL Issue 2

Part 3: Troubleshoot ACL Issue 3

Scenario

This network is meant to have the following three policies implemented:

- Hosts from the 192.168.0.0/24 network are unable to access any TCP service of **Server3**.
- Hosts from the 10.0.0.0/8 network are unable to access the HTTP service of **Server1**.
- Hosts from the 172.16.0.0/16 network are unable to access the FTP service of **Server2**.

Note: All FTP usernames and passwords are "**cisco**".

No other restrictions should be in place. Unfortunately, the rules that have been implemented are not working correctly. Your task is to find and fix the errors related to the access lists on **R1**.

Part 1: Troubleshoot ACL Issue 1

Hosts from the 192.168.0.0/24 network are intentionally unable to access any TCP service of **Server3**, but should not be otherwise restricted.

Step 1: Determine the ACL problem.

As you perform the following tasks, compare the results to what you would expect from the ACL.

a. Using **L2**, attempt to access FTP and HTTP services of **Server1**, **Server2**, and **Server3**.

b. Using **L2**, ping **Server1**, **Server2**, and **Server3**.

c. Using **L2**, ping **G0/2** of **R1**.

d. View the running configuration on **R1**. Examine access list **192_to_10** and its placement on the interfaces. Is the access list placed on the correct interface and in the correct direction? Is there any statement in the list that permits or denies traffic to other networks? Are the statements in the correct order?

e. Perform other tests, as necessary.

Step 2: Implement a solution.

Make an adjustment to access list **192_to_10** to fix the problem.

Step 3: Verify that the problem is resolved and document the solution.

If the problem is resolved, document the solution: otherwise return to Step 1.

_____

_____

Part 2: Troubleshoot ACL Issue 2

Hosts from the 10.0.0.0/8 network are intentionally unable to access the HTTP service of **Server1**, but should not be otherwise restricted.

Step 1: Determine the ACL problem.

As you perform the following tasks, compare the results to what you would expect from the ACL.

a. Using **L3**, attempt to access FTP and HTTP services of **Server1**, **Server2**, and **Server3**.

b. Using **L3**, ping **Server1**, **Server2**, and **Server3**.

c. View the running configuration on **R1**. Examine access list **10_to_172** and its placement on the interfaces. Is the access list placed on the correct interface and in the correct direction? Is there any statement in the list that permits or denies traffic to other networks? Are the statements in the correct order?

d. Run other tests as necessary.

Step 2: Implement a solution.

Make an adjustment to access list **10_to_172** to fix the problem.

Step 3: Verify the problem is resolved and document the solution.

If the problem is resolved, document the solution; otherwise return to Step 1.

_____

Part 3: Troubleshoot ACL Issue 3

Hosts from the 172.16.0.0/16 network are intentionally unable to access the FTP service of **Server2**, but should not be otherwise restricted.

Step 1: Determine the ACL problem.

As you perform the following tasks, compare the results to the expectations of the ACL.

a. Using **L1**, attempt to access FTP and HTTP services of **Server1**, **Server2**, and **Server3**.

b. Using **L1**, ping **Server1**, **Server2**, and **Server3**.

c. View the running configuration on **R1**. Examine access list **172_to_192** and its placement on the interfaces. Is the access list placed on the correct port in the correct direction? Is there any statement in the list that permits or denies traffic to other networks? Are the statements in the correct order?

d. Run other tests as necessary.

Step 2: Implement a solution.

Make an adjustment to access list **172_to_192** to fix the problem.

Step 3: Verify the problem is resolved and document the solution.

If the problem is resolved, document the solution; otherwise return to Step 1.

_____

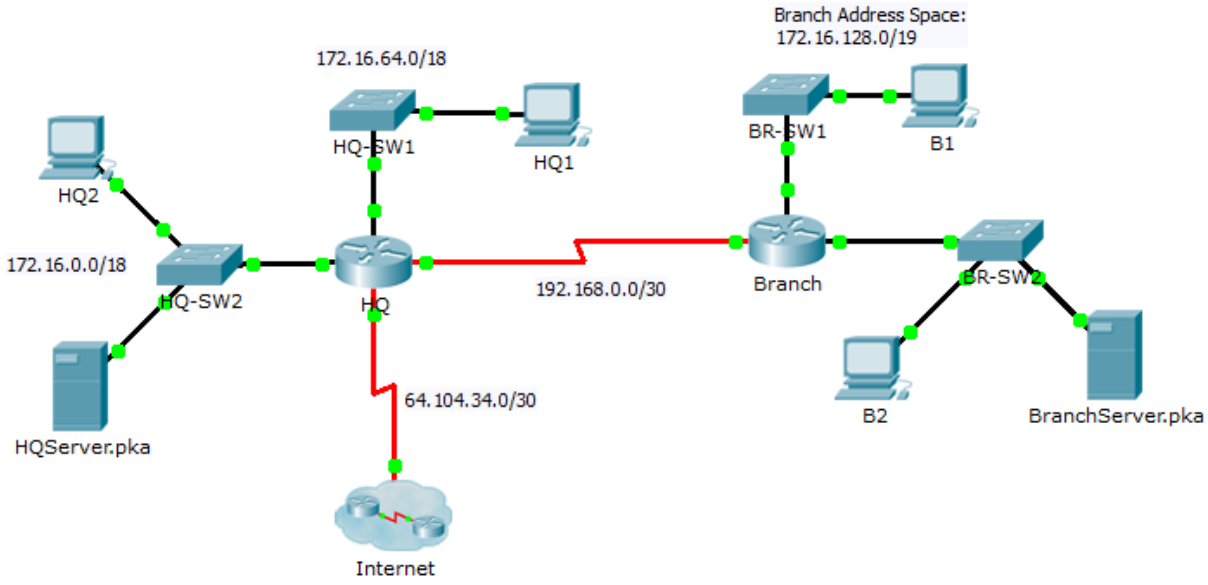
_____

Suggested Scoring Rubric

Question Location	Possible Points	Earned Points
Documentation Score	**10**	
Packet Tracer Score	**90**	
Total Score	**100**	

9.4.2.8 Packet Tracer - Skills Integration Challenge

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	G0/0	172.16.127.254	255.255.192.0	N/A
	G0/1	172.16.63.254	255.255.192.0	N/A
	S0/0/0	192.168.0.1	255.255.255.252	N/A
	S0/0/1	64.104.34.2	255.255.255.252	64.104.34.1
Branch	G0/0			N/A
	G0/1			N/A
	S0/0/0	192.168.0.2	255.255.255.252	N/A
HQ1	NIC	172.16.64.1	255.255.192.0	172.16.127.254
HQ2	NIC	172.16.0.2	255.255.192.0	172.16.63.254
HQServer.pka	NIC	172.16.0.1	255.255.192.0	172.16.63.254
B1	NIC			
B2	NIC	172.16.128.2	255.255.240.0	172.16.143.254
BranchServer.pka	NIC	172.16.128.1	255.255.240.0	172.16.143.254

Scenario

In this challenge activity, you will finish the addressing scheme, configure routing, and implement named access control lists.

Requirements

a. Divide 172.16.128.0/19 into two equal subnets for use on **Branch**.

   1) Assign the last usable address of the second subnet to the Gigabit Ethernet 0/0 interface.

   2) Assign the last usable address of the first subnet to the Gigabit Ethernet 0/1 interface.

   3) Document the addressing in the Addressing Table.

   4) Configure **Branch** with appropriate addressing

b. Configure **B1** with appropriate addressing using the first available address of the network to which it is attached. Document the addressing in the Addressing Table.

c. Configure **HQ** and **Branch** with OSPF routing according to the following criteria:

   - Assign the process ID 1.
   - Advertise all three attached networks. Do not advertise the link to the Internet.
   - Configure appropriate interfaces as passive.

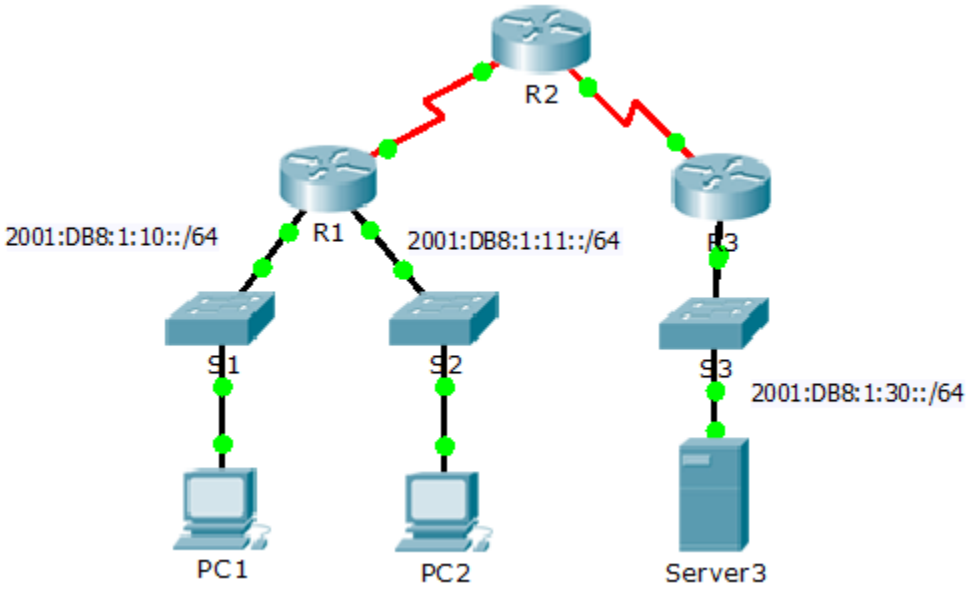
d. Set a default route on **HQ** which directs traffic to S0/0/1 interface. Redistribute the route to **Branch**.

e. Design a named access list **HQServer** to prevent any computers attached to the Gigabit Ethernet 0/0 interface of the **Branch** router from accessing **HQServer.pka**. All other traffic is permitted. Configure the access list on the appropriate router, apply it to the appropriate interface and in the appropriate direction.

f. Design a named access list **BranchServer** to prevent any computers attached to the Gigabit Ethernet 0/0 interface of the **HQ** router from accessing the HTTP and HTTPS service of the **Branch** server. All other traffic is permitted. Configure the access list on the appropriate router, apply it to the appropriate interface and in the appropriate direction.

9.5.2.6 Packet Tracer - Configuring IPv6 ACLs

Topology



Addressing Table

Device	Interface	IPv6 Address/Prefix	Default Gateway
Server3	NIC	2001:DB8:1:30::30/64	FE80::30

Objectives

Part 1: Configure, Apply, and Verify an IPv6 ACL

Part 2: Configure, Apply, and Verify a Second IPv6 ACL

Part 1: Configure, Apply, and Verify an IPv6 ACL

Logs indicate that a computer on the 2001:DB8:1:11::0/64 network is repeatedly refreshing their web page causing a Denial-of-Service (DoS) attack against **Server3**. Until the client can be identified and cleaned, you must block HTTP and HTTPS access to that network with an access list.

Step 1: Configure an ACL that will block HTTP and HTTPS access.

Configure an ACL named **BLOCK_HTTP** on **R1** with the following statements.

a. Block HTTP and HTTPS traffic from reaching **Server3**.

```
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq www
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq 443
```

b. Allow all other IPv6 traffic to pass.

Step 2: Apply the ACL to the correct interface.

Apply the ACL on the interface closest the source of the traffic to be blocked.

```
R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in
```

Step 3: Verify the ACL implementation.

Verify the ACL is operating as intended by conducting the following tests:

- Open the **web browser** of **PC1** to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should appear.
- Open the **web browser** of **PC2** to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should be blocked
- Ping from **PC2** to 2001:DB8:1:30::30. The ping should be successful.

Part 2: Configure, Apply, and Verify a Second IPv6 ACL

The logs now indicate that your server is receiving pings from many different IPv6 addresses in a Distributed Denial of Service (DDoS) attack. You must filter ICMP ping requests to your server.

Step 1: Create an access list to block ICMP.

Configure an ACL named **BLOCK_ICMP** on **R3** with the following statements:

a. Block all ICMP traffic from any hosts to any destination.

b. Allow all other IPv6 traffic to pass.

Step 2: Apply the ACL to the correct interface.

In this case, ICMP traffic can come from any source. To ensure that ICMP traffic is blocked regardless of its source or changes that occur to the network topology, apply the ACL closest to the destination.

Step 3: Verify that the proper access list functions.

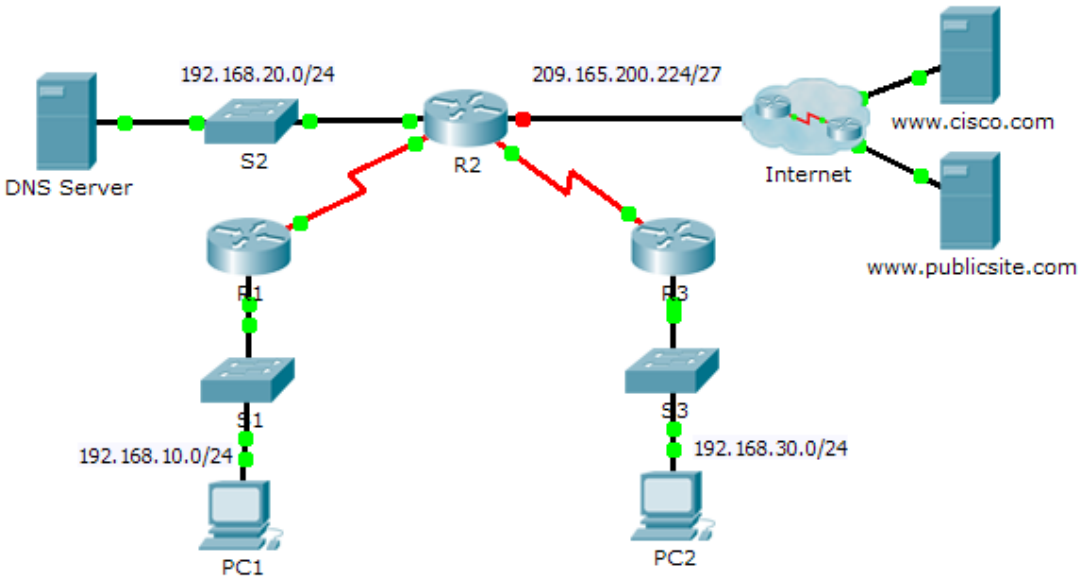
a. Ping from **PC2** to 2001:DB8:1:30::30. The ping should fail.

b. Ping from **PC1** to 2001:DB8:1:30::30. The ping should fail.

Open the **web browser** of **PC1** to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should display.

10.1.3.3 Packet Tracer - Configuring DHCP Using Cisco IOS

Topology



Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	G0/0	192.168.20.1	255.255.255.0	N/A
	G0/1	DHCP Assigned	DHCP Assigned	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
R3	G0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.0	N/A
PC1	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned
PC2	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned
DNS Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Objectives

Part 1: Configure a Router as a DHCP Server

Part 2: Configure DHCP Relay

Part 3: Configure a Router as a DHCP Client

Part 4: Verify DHCP and Connectivity

Scenario

A dedicated DHCP server is scalable and relatively easy to manage, but can be costly to have one at every location in a network. However, a Cisco router can be configured to provide DHCP services without the need for a dedicated server. Cisco routers use the Cisco IOS feature set, Easy IP, as an optional, full-featured DHCP server. Easy IP leases configurations for 24 hours by default. As the network technician for your company, you are tasked with configuring a Cisco router as a DHCP server to provide dynamic allocation of addresses to clients on the network. You are also required to configure the edge router as a DHCP client so that it receives an IP address from the ISP network.

Part 1: Configure a Router as a DHCP Server

Step 1: Configure the excluded IPv4 addresses.

Configure **R2** to exclude the first 10 addresses from the R1 and R3 LANs. All other addresses should be available in the DHCP address pool.

Step 2: Create a DHCP pool on R2 for the R1 LAN.

a. Create a DHCP pool named **`R1-LAN`** (case-sensitive).

b. Configure the DHCP pool to include the network address, the default gateway, and the IP address of the DNS server.

Step 3: Create a DHCP pool on R2 for the R3 LAN.

a. Create a DHCP pool named **`R3-LAN`** (case-sensitive).

b. Configure the DHCP pool to include the network address, the default gateway, and the IP address of the DNS server.

Part 2: Configure DHCP Relay

Step 1: Configure R1 and R3 as a DHCP relay agent.

Step 2: Set PC1 and PC2 to receive IP addressing information from DHCP.

Part 3: Configure R2 as a DHCP Client

a. Configure the Gigabit Ethernet 0/1 interface on R2 to receive IP addressing from DHCP and activate the interface.

Note: Use Packet Tracer's **Fast Forward Time** feature to speed up the process or wait until R2 forms an EIGRP adjacency with the ISP router.

b. Use the **show ip interface brief** command to verify that R2 received an IP address from DHCP.

Part 4: Verify DHCP and Connectivity

Step 1: Verify DHCP bindings.

```
R2# show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.10.11    0002.4AA5.1470           --                     Automatic
```

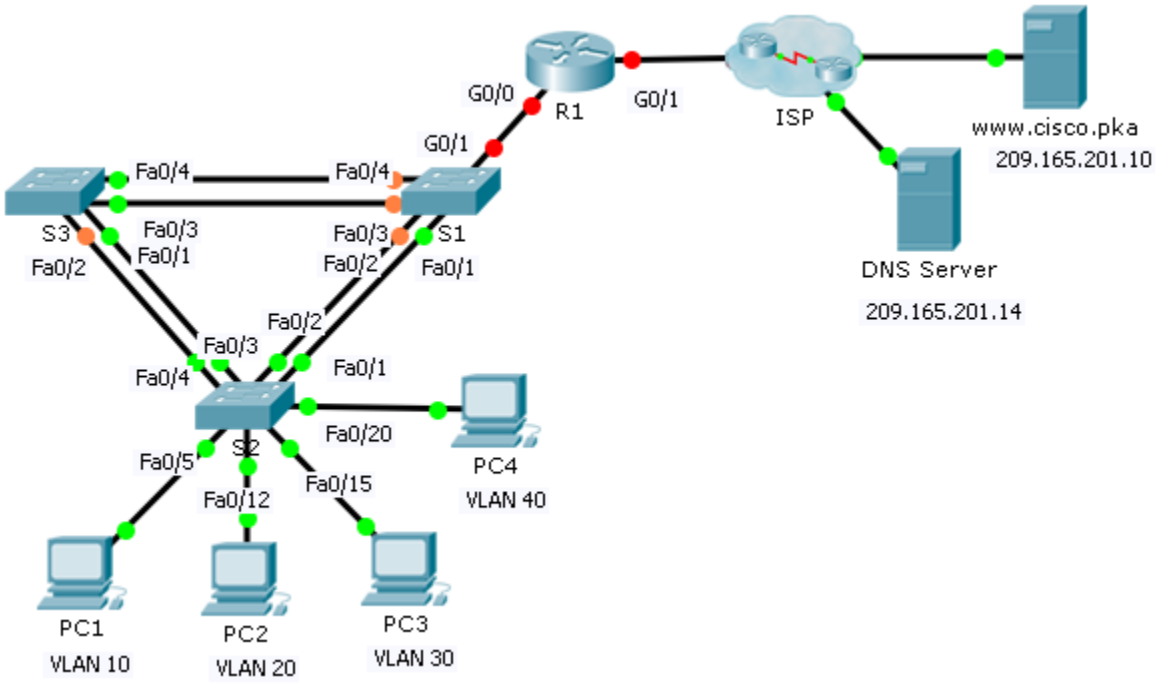
```
  192.168.30.11    0004.9A97.2535          --                    Automatic
```

Step 2: Verify configurations.

Verify that **PC1** and **PC2** can now ping each other and all other devices.

10.3.1.2 Packet Tracer – Skills Integration Challenge

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0.10	172.31.10.1	255.255.255.224	N/A
	G0/0.20	172.31.20.1	255.255.255.240	N/A
	G0/0.30	172.31.30.1	255.255.255.128	N/A
	G0/0.40	172.31.40.1	255.255.255.192	N/A
	G0/1	DHCP Assigned	DHCP Assigned	N/A
PC1	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned
PC2	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned
PC3	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned
PC4	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned

VLAN Port Assignments and DHCP Information

Ports	VLAN Number - Name	DHCP Pool Name	Network
Fa0/5 – 0/9	VLAN 10 - Sales	VLAN_10	172.31.10.0/27
Fa0/10 – Fa0/14	VLAN 20 - Production	VLAN_20	172.31.20.0/28
Fa0/15 – Fa0/19	VLAN 30 - Marketing	VLAN_30	172.31.30.0/25
Fa0/20 - Fa0/24	VLAN 40 - HR	VLAN_40	172.31.40.0/26

Scenario

In this culminating activity, you will configure VLANs, trunks, DHCP Easy IP, DHCP relay agents, and configure a router as a DHCP client.

Requirements

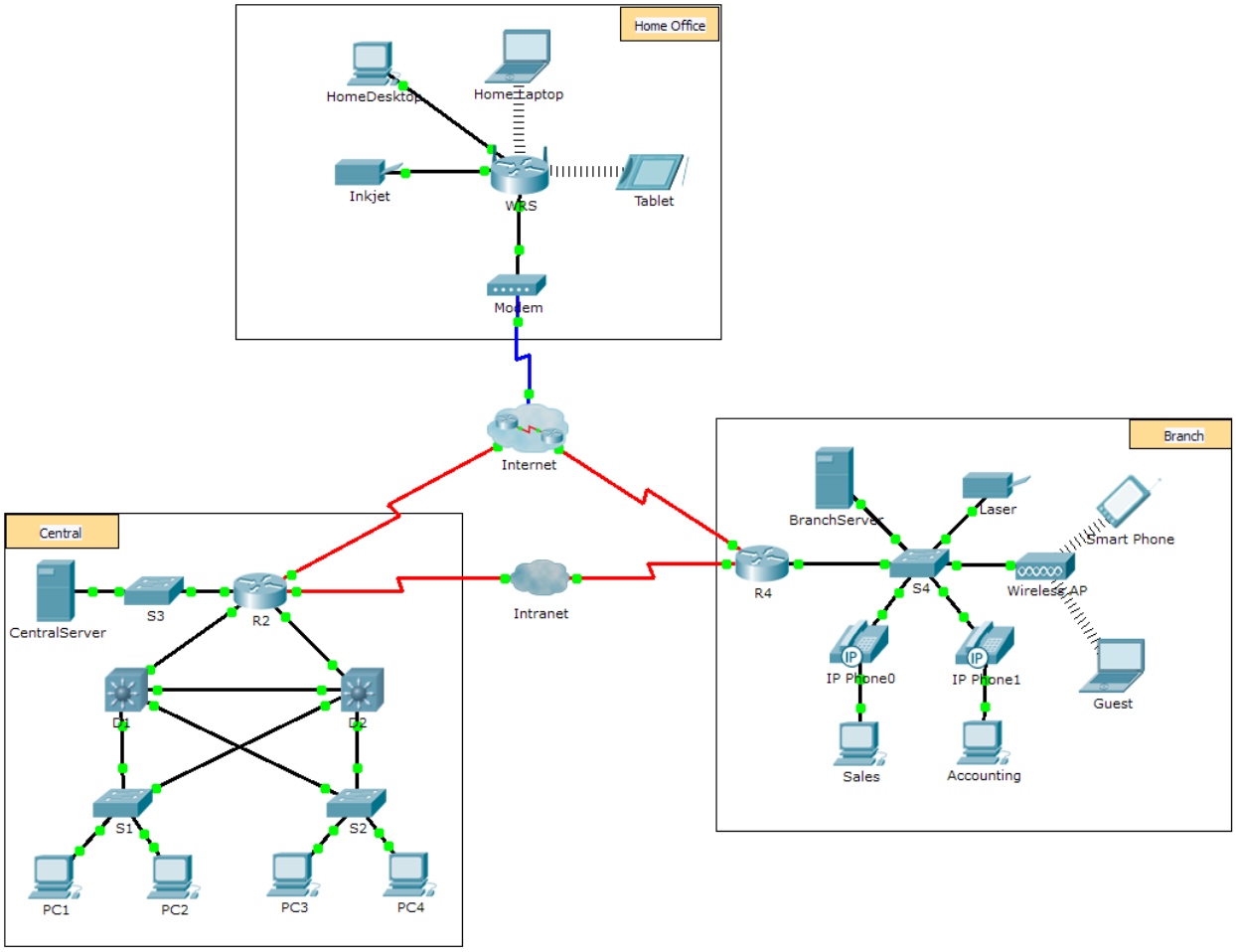
Using the information in the tables above, implement the following requirements:

- Create VLANs on **S2** and assign VLANs to appropriate ports. Names are case-sensitive
- Configure **S2** ports for trunking.
- Configure all non-trunk ports on **S2** as access ports.
- Configure **R1** to route between VLANs. Subinterface names should match the VLAN number.
- Configure **R1** to act as a DHCP server for the VLANs attached to S2.
  - Create a DHCP pool for each VLAN. Names are case-sensitive.
  - Assign the appropriate addresses to each pool.
  - Configure DHCP to provide the default gateway address
  - Configure the DNS server 209.165.201.14 for each pool.
  - Prevent the first 10 addresses from each pool from being distributed to end devices.
- Verify that each PC has an address assigned from the correct DHCP pool.

  Note: DHCP address assignments may take some time. Click **Fast Forward Time** to speed up the process.
- Configure **R1** as a DHCP client so that it receives an IP address from the ISP network.
- Verify all devices can now ping each other and **www.cisco.pka**.

11.1.26 Packet Tracer – Investigating NAT Operation

Topology



Objectives

Part 1: Investigate NAT Operation Across the Intranet

Part 2: Investigate NAT Operation Across the Internet

Part 3: Conduct Further Investigations

Scenario

As a frame travels across a network, the MAC addresses may change. IP addresses can also change when a packet is forwarded by a device configured with NAT. In this activity, we will investigate what happens to IP addresses during the NAT process.

Part 1: Investigate NAT Operation Across the Intranet

Step 1: Wait for the network to converge.

It might take a few minutes for everything in the network to converge. You can speed the process up by clicking on Fast Forward Time.

Step 2: Generate an HTTP request from any PC in the Central domain.

a. Open the Web Browser of any PC in the **Central** domain and type the following without pressing enter or clicking **Go**: **http://branchserver.pka**.

b. Switch to **Simulation** mode and edit the filters to show only HTTP requests.

c. Click **Go** in the browser, a PDU envelope will appear.

d. Click **Capture / Forward** until the PDU is over **D1** or **D2**. Record the source and destination IP addresses. To what devices do those addresses belong?

_____

_____

e. Click **Capture / Forward** until the PDU is over **R2**. Record the source and destination IP addresses in the outbound packet. To what devices do those addresses belong?

_____

_____

f. Login to R2 using '**class**' to enter privileged EXEC and show the running configuration. The address came from the following address pool:

```
ip nat pool R2Pool 64.100.100.3 64.100.100.31 netmask 255.255.255.224
```

g. Click **Capture / Forward** until the PDU is over **R4**. Record the source and destination IP addresses in the outbound packet. To what devices do those addresses belong?

_____

_____

h. Click **Capture / Forward** until the PDU is over **Branserver.pka**. Record the source and destination TCP port addresses in the outbound segment.

i. On both **R2** and **R4**, run the following command and match the IP addresses and ports recorded above to the correct line of output:

```
R2# show ip nat translations
R4# show ip nat translations
```

j. What do the inside local IP addresses have in common? _____

k. Did any private addresses cross the Intranet? _____

l. Return to **Realtime** mode.

Part 2: Investigate NAT Operation Across the Internet

Step 1: Generate an HTTP request from any computer in the home office.

a. Open the Web Browser of any computer in the home office and type the following without pressing enter or clicking **Go**: **http://centralserver.pka**.

b. Switch to **Simulation** mode. The filters should already be set to show only HTTP requests.

c. Click **Go** in the browser, a PDU envelope will appear.

d. Click **Capture / Forward** until the PDU is over **WRS**. Record the inbound source and destination IP addresses and the outbound source and destination addresses. To what devices do those addresses belong?

_____

_____

e. Click **Capture / Forward** until the PDU is over **R2**. Record the source and destination IP addresses in the outbound packet. To what devices do those addresses belong?

_____

f. On **R2**, run the following command and match the IP addresses and ports recorded above to the correct line of output:

```
R2# show ip nat translations
```

g. Return to **Realtime** mode. Did all of the web pages appear in the browsers? _____

Part 3: Conduct Further Investigations

a. Experiment with more packets, both HTTP and HTTPS. There are many questions to consider such as:

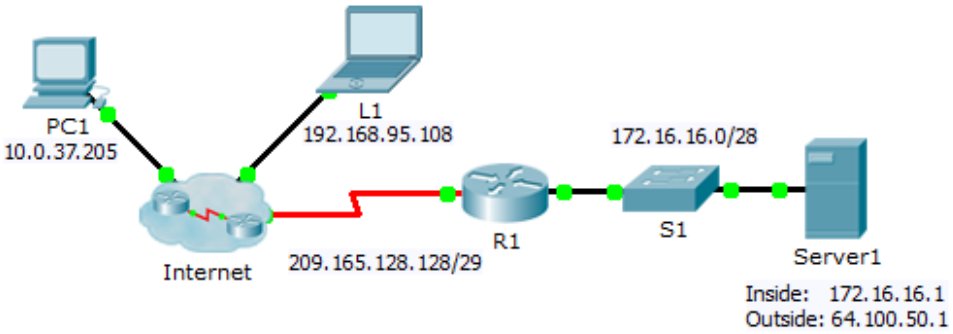
- Do the NAT translation tables grow?
- Does WRS have a pool of addresses?
- Is this how the computers in the classroom connect to the Internet?
- Why does NAT use four columns of addresses and ports?

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Request a Web Page Across the Intranet	Step 2d	12	
	Step 2e	12	
	Step 2g	13	
	Step 2j	12	
	Step 2k	12	
	Part 1 Total	61	
Part 2: Request a Web Page Across the Internet	Step 1d	13	
	Step 1e	13	
	Step 1g	13	
	Part 2 Total	**39**	
	Total Score	**100**	

11.2.1.4 Packet Tracer – Configuring Static NAT

Topology



Objectives

Part 1: Test Access without NAT

Part 2: Configure Static NAT

Part 3: Test Access with NAT

Scenario

In IPv4 configured networks, clients and servers use private addressing. Before packets with private addressing can cross then Internet, they need to be translated to public addressing. Servers that are accessed from outside the organization are usually assigned both a public and a private static IP address. In this activity, you will configure static NAT so that outside devices can access and inside server at its public address.

Part 1: Test Access without NAT

Step 1: Attempt to connect to Server1 using Simulation Mode.

a. From **PC1** or **L1**, attempt to connect to the **Server1** web page at 172.16.16.1. Use the Web Browser to browse **Server1** at 172.16.16.1. The attempts should fail.

b. From **PC1**, ping the **R1** S0/0/0 interface. The ping should succeed.

Step 2: View R1 routing table and running-config.

a. View the running configuration of **R1**. Note that there are no commands referring to NAT.

b. Verify that the routing table does not contain entries referring to the IP addresses used by **PC1** and **L1**.

c. Verify that NAT is not being used by **R1**.

```
R1# show ip nat translations
```

Part 2: Configure Static NAT

Step 1: Configure static NAT statements.

Refer to the Topology. Create a static NAT translation to map the **Server1** inside address to its outside address.

Step 2: Configure interfaces.

Configure the correct inside and outside interfaces.

Part 3: Test Access with NAT

Step 1: Verify connectivity to the Server1 web page.

a. Open the command prompt on **PC1** or **L1**, attempt to ping the public address for **Server1**. Pings should succeed.

b. Verify that both **PC1** and **L1** can now access the **Server1** web page.

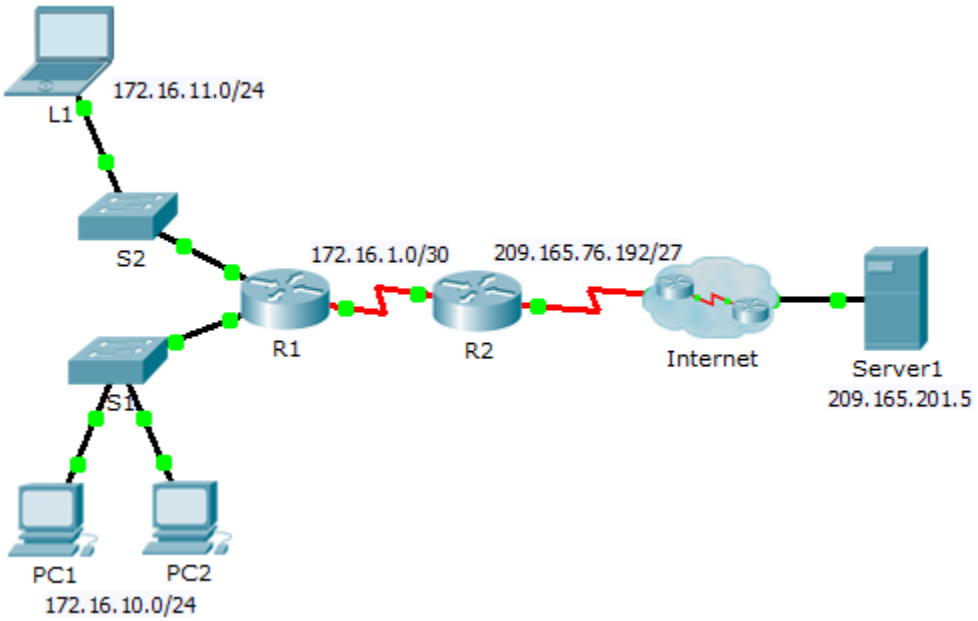
Step 2: View NAT translations.

Use the following commands to verify the static NAT configuration:

```
show running-config
show ip nat translations
show ip nat statistics
```

11.2.2.5 Packet Tracer – Configuring Dynamic NAT

Topology



Objectives

Part 1: Configure Dynamic NAT

Part 2: Verify NAT Implementation

Part 1: Configure Dynamic NAT

Step 1: Configure traffic that will be permitted.

On **R2**, configure one statement for ACL 1 to permit any address belonging to 172.16.0.0/16.

Step 2: Configure a pool of address for NAT.

Configure **R2** with a NAT pool that uses all four addresses in the 209.165.76.196/30 address space.

Notice in the topology there are 3 network ranges that would be translated based on the ACL created. What will happen if more than 2 devices attempt to access the Internet?

_____

_____

Step 3: Associate ACL1 with the NAT pool.

Step 4: Configure the NAT interfaces.

Configure **R2** interfaces with the appropriate inside and outside NAT commands.

Part 2: Verify NAT Implementation

Step 1: Access services across the Internet.

From the web browser of **L1**, **PC1**, or **PC2**, access the web page for **Server1**.

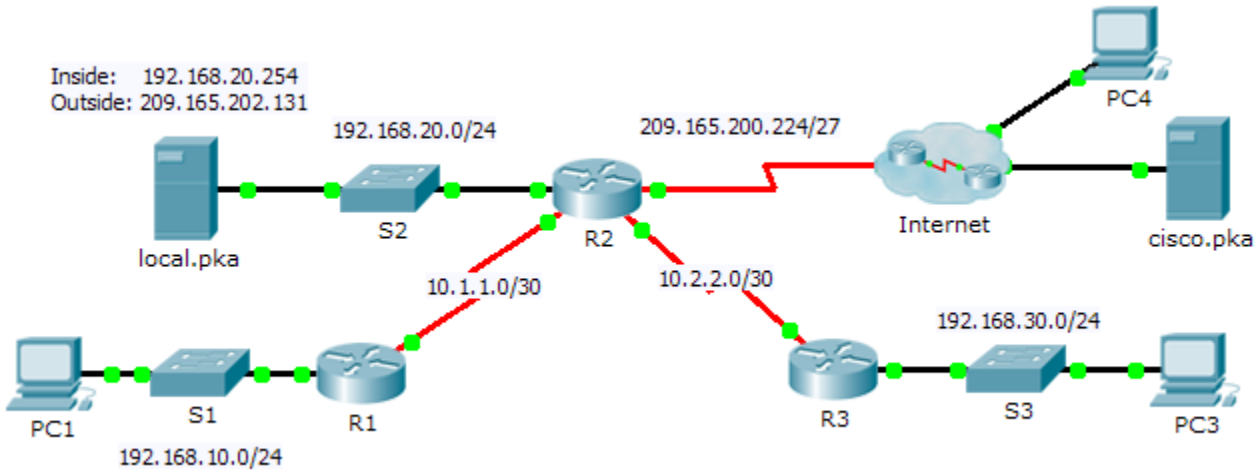
Step 2: View NAT translations.

View the NAT translations on **R2**.

```
R2# show ip nat translations
```

11.2.3.6 Packet Tracer – Implementing Static and Dynamic NAT

Topology



Objectives

Part 1: Configure Dynamic NAT with PAT

Part 2: Configure Static NAT

Part 3: Verify NAT Implementation

Part 1: Configure Dynamic NAT with PAT

Step 1: Configure traffic that will be permitted for NAT translations.

On **R2**, configure a standard ACL named **R2NAT** that uses three statements to permit, in order, the following private address spaces:192.168.10.0/24, 192.168.20.0/24, and 192.168.30.0/24.

Step 2: Configure a pool of addresses for NAT.

Configure **R2** with a NAT pool named **R2POOL** that uses the first three addresses in the 209.165.202.128/30 address space. The fourth address is used for static NAT later in Part 2.

Step 3: Associate the named ACL with the NAT pool and enable PAT.

Step 4: Configure the NAT interfaces.

Configure **R2** interfaces with the appropriate inside and outside NAT commands.

Part 2: Configure Static NAT

Refer to the Topology. Create a static NAT translation to map the **local.pka** inside address to its outside address.

Part 3: Verify NAT Implementation

Step 1: Access services across the Internet.

a. From the web browser of **PC1**, or **PC3**, access the web page for **cisco.pka**.

b. From the web browser for **PC4**, access the web page for **local.pka**.

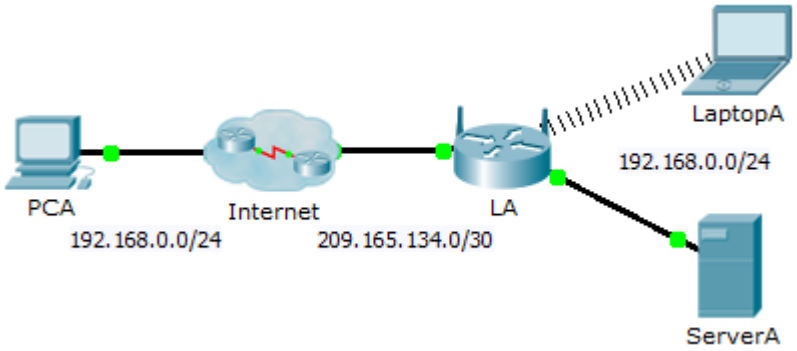
Step 2: View NAT translations.

View the NAT translations on **R2**.

```
R2# show ip nat translations
```

11.2.4.4 Packet Tracer – Configuring Port Forwarding on a Linksys Router

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
LA	Internet	209.165.134.1	255.255.255.252
	LAN	192.168.0.1	255.255.255.0

Objectives

Part 1: Configure Port Forwarding

Part 2: Verify Remote Connectivity to ServerA

Scenario

Your friend wants to play a game with you on your server. Both of you are at your respective homes, connected to the Internet. You need to configure your SOHO (Small Office, Home Office) router to port forward HTTP requests to your server so that your friend can access the game lobby web page.

Part 1: Configure Port Forwarding

a. From the web browser on **LaptopA**, access **LA** by entering the LAN IP address, 192.168.0.1. The username is **admin** and the password is **cisco123**.

b. Click **Applications & Gaming**. In the first dropdown on the left, choose **HTTP** and then enter 192.168.0.2 in the "To IP Address" column. This configures **LA** to forward port 80 to 192.168.0.2. Check the **Enabled** box next to the address column.

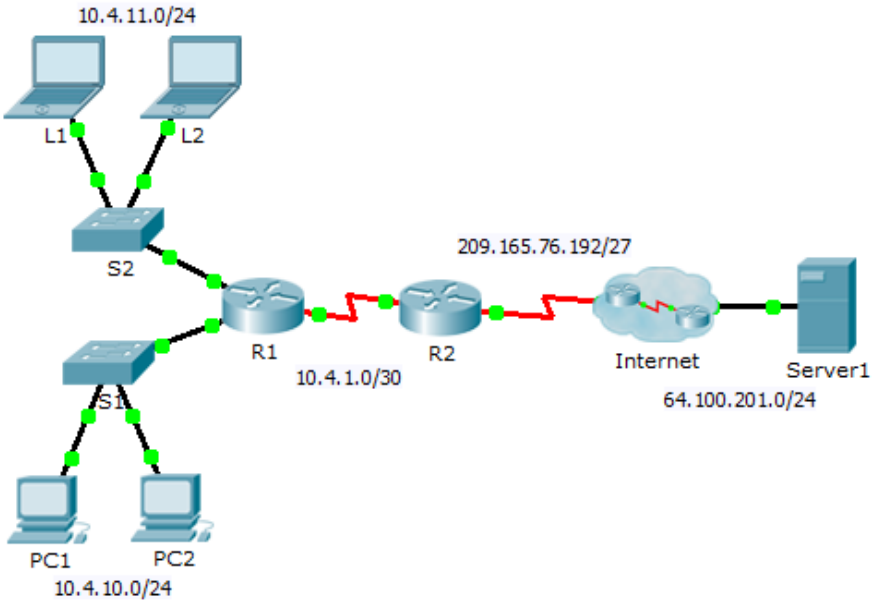
c. Scroll to the bottom and click **Save Settings**.

Part 2: Verify Remote Connectivity to ServerA

From the web browser on **PCA**, enter the Internet IP address for **LA**. The game server web page should appear.

11.3.1.4 Packet Tracer – Verifying and Troubleshooting NAT Configurations

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	10.4.10.254	255.255.255.0	N/A
	G0/1	10.4.11.254	255.255.255.0	N/A
	S0/0/1	10.4.1.2	255.255.255.252	N/A
R2	S0/0/0	209.165.76.194	255.255.255.224	N/A
	S0/0/1	10.4.1.1	255.255.255.252	N/A
Server1	NIC	64.100.201.5	255.255.255.0	64.100.201.1
PC1	NIC	10.4.10.1	255.255.255.0	10.4.10.254
PC2	NIC	10.4.10.2	255.255.255.0	10.4.10.254
L1	NIC	10.4.11.1	255.255.255.0	10.4.11.254
L2	NIC	10.4.11.2	255.255.255.0	10.4.11.254

Objectives

Part 1: Isolate Problems

Part 2: Troubleshoot NAT Configuration

Part 3: Verify Connectivity

Scenario

A contractor restored an old configuration to a new router running NAT. But, the network has changed and a new subnet was added after the old configuration was backed up. It is your job to get the network working again.

Part 1: Isolate Problems

Ping **Server1** from **PC1**, **PC2**, **L1**, **L2**, and **R2**. Record the success of each ping. Ping any other machines as needed.

Part 2: Troubleshoot NAT Configuration

Step 1: View the NAT translations on R2.

If NAT is working, there should be table entries.

Step 2: Show the running configuration of R2.

The NAT inside port should align with the private address, while the NAT outside port should align with the public address.

Step 3: Correct the Interfaces.

Assign the **ip nat inside** and **ip nat outside** commands to the correct ports.

Step 4: Ping Server1 from PC1, PC2, L1, L2, and R2.

Record the success of each ping. Ping any other machines as needed.

Step 5: View the NAT translations on R2.

If NAT is working, there should be table entries.

Step 6: Show Access-list 101 on R2.

The wildcard mask should encompass both the 10.4.10.0 network and the 10.4.11.0 network.

Step 7: Correct the Access-list.

Delete access-list 101 and replace it with a similar list that is also one statement in length. The only difference should be the wildcard.

Part 3: Verify Connectivity

Step 1: Verify connectivity to Server1.

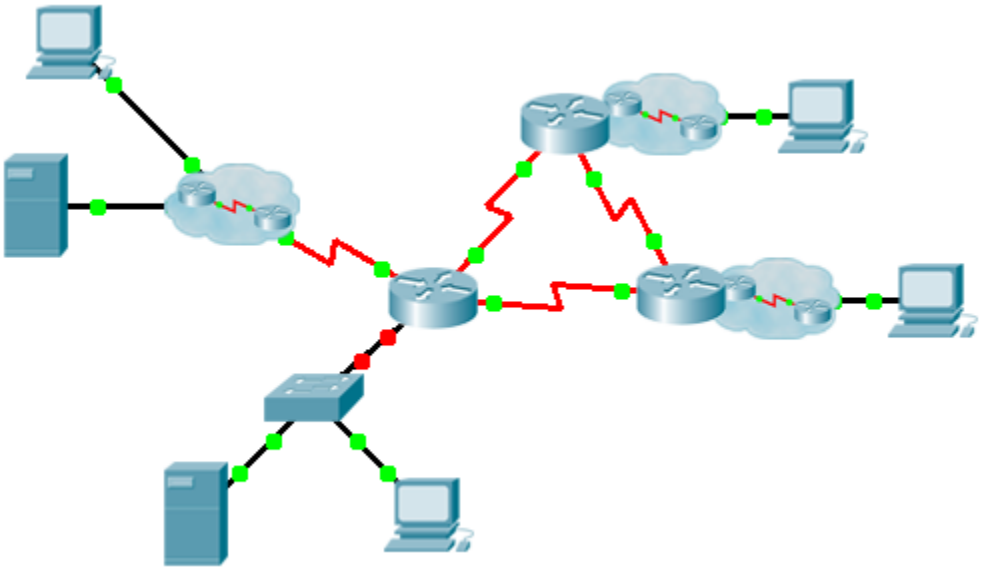
Record the success of each ping. All hosts should be able to ping **Server1**, **R1**, and **R2**. Troubleshoot if the pings are not successful.

Step 2: View the NAT translations on R2.

NAT should display many table entries.

11.4.1.2 Packet Tracer – Skills Integration Challenge

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
[[R1Name]]	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
[[R2Name]]	G0/0			N/A
	S0/0/0		255.255.255.252	N/A
	S0/0/1		255.255.255.252	N/A
[[R3Name]]	G0/0			N/A
	S0/0/0		255.255.255.252	N/A
	S0/0/1		255.255.255.252	N/A
[[S1Name]]	VLAN 60			
[[PC1Name]]	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned

VLANs and Port Assignments Table

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

Scenario

This culminating activity includes many of the skills that you have acquired during this course. 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.