Liityntäverkot Labrat

CCNA 1-3

Juuso Leppänen, TTV22S3

Laboratorio harjoitukset
Liityntäverkot, Jussi Ahonen
10.12.2024
Tietoverkot moduuli

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

Kuvaotsikkoluettelon hakusanoja ei löytynyt.**Taulukot**

Kuvaotsikkoluettelon hakusanoja ei löytynyt.

1 Kuvaotsikkoluettelon hakusanoja ei löytynyt.**Johdanto**

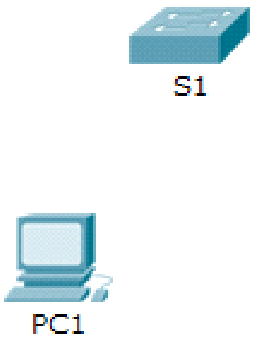
Opintojaksolla perehdyttiin liityntäverkkojen rakenteeseen, teknologioihin ja protokolliin sekä niiden käytännön soveltamiseen. Tavoitteena oli oppia suunnittelemaan, konfiguroimaan ja hallitsemaan liityntäverkkoja hyödyntäen teknologioita kuten 5G, DSL, FTTH/PON, VPN-ratkaisut ja ohjelmoitavat verkot (SD-WAN, SASE). Lisäksi harjoiteltiin tiedonhakua alan standardeista ja laitevalmistajien dokumentaatiosta ongelmanratkaisun tueksi.

Opintojaksoon sisältyi kolme Cisco Packet Tracer -laboratoriotehtäväsarjaa, joissa syvennyttiin liityntäverkkoteknologioiden suunnitteluun, konfigurointiin ja vianetsintään. Harjoitukset tarjosivat käytännön osaamista ICT-ammattilaisen tarpeisiin.

2 CCNA 1

2.1 Packet Tracer - Navigating the IOS

- **Topology**



- **Objectives**

Part 1: Establish Basic Connections, Access the CLI, and Explore Help

Part 2: Explore EXEC Modes

Part 3: Set the Clock

- **Background**

In this activity, you will practice skills necessary for navigating the Cisco IOS, such as different user access modes, various configuration modes, and common commands used on a regular basis. You will also practice accessing the context-sensitive Help by configuring the **clock** command.

Establish Basic Connections, Access the CLI, and Explore Help

In Part 1 of this activity, you will connect a PC to a switch using a console connection and explore various command modes and Help features.

Connect PC1 to S1 using a console cable.

- Click the **Connections** icon (the one that looks like a lightning bolt) in the lower left corner of the Packet Tracer window.
- Select the light blue Console cable by clicking it. The mouse pointer will change to what appears to be a connector with a cable dangling from it.
- Click **PC1**. A window displays an option for an RS-232 connection.
- Drag the other end of the console connection to the S1 switch and click the switch to access the connection list.
- Select the **Console** port to complete the connection.

Establish a terminal session with S1.

- Click **PC1** and then select the **Desktop** tab.
- Click the **Terminal** application icon. Verify that the Port Configuration default settings are correct.

  What is the setting for bits per second? 9600
- Click **OK**.
- The screen that appears may have several messages displayed. Somewhere on the screen there should be a `Press RETURN to get started!` message. Press ENTER.

  What is the prompt displayed on the screen? S1

Explore the IOS Help.

- The IOS can provide help for commands depending on the level accessed. The prompt currently displayed is called **User EXEC**, and the device is waiting for a command. The most basic form of help is to type a question mark (?) at the prompt to display a list of commands.

  ```
  S1> ?
  ```

  Which command begins with the letter ‘C’? connect
- At the prompt, type **t** and then a question mark (**?**).

  ```
  S1> t?
  ```

  Which commands are displayed? telnet, terminal and traceroute
- At the prompt, type **te** and then a question mark (**?**).

  ```
  S1> te?
  ```

  Which commands are displayed? telnet and terminal

  This type of help is known as **context-sensitive** Help. It provides more information as the commands are expanded.

Explore EXEC Modes

In Part 2 of this activity, you will switch to privileged EXEC mode and issue additional commands.

Enter privileged EXEC mode.

- At the prompt, type the question mark (**?**).

  ```
  S1> ?
  ```

  What information is displayed that describes the **enable** command? Turn on privileged commands
- Type **en** and press the **Tab** key.

```
S1> en<Tab>
```

What displays after pressing the **Tab** key? enable

This is called command completion (or tab completion). When part of a command is typed, the **Tab** key can be used to complete the partial command. If the characters typed are enough to make the command unique, as in the case of the **enable** command, the remaining portion of the command is displayed.

What would happen if you typed **te<Tab>** at the prompt?

It will do nothing, since there are more than one command that could be filled in

- Enter the **enable** command and press ENTER. How does the prompt change?

  it has > instead of #

  When prompted, type the question mark (**?**).

```
S1# ?
```

One command starts with the letter 'C' in user EXEC mode. How many commands are displayed now that privileged EXEC mode is active? (**Hint**: you could type c? to list just the commands beginning with 'C'.)

clear, clock, configure, connect and copy

Enter Global Configuration mode.

When in privileged EXEC mode, one of the commands starting with the letter 'C' is **configure**. Type either the full command or enough of the command to make it unique. Press the <**Tab**> key to issue the command and press ENTER.

```
S1# configure
```

What is the message that is displayed?

Configuring from terminal, memory, or network [terminal]?

- Press Enter to accept the default parameter that is enclosed in brackets **[terminal]**.

  How does the prompt change? it gets (config)

- This is called global configuration mode. This mode will be explored further in upcoming activities and labs. For now, return to privileged EXEC mode by typing **end**, **exit**, or **Ctrl-Z**.

```
S1(config)# exit
S1#
```

Set the Clock

Use the clock command.

- Use the **clock** command to further explore Help and command syntax. Type **show clock** at the privileged EXEC prompt.

```
S1# show clock
```

What information is displayed? What is the year that is displayed?

*0:13:10.608 UTC Mon Mar 1 1993

- Use the context-sensitive Help and the **clock** command to set the time on the switch to the current time. Enter the command **clock** and press ENTER.

```
S1# clock<ENTER>
```

What information is displayed? % Incomplete command.

The "% Incomplete command" message is returned by the IOS. This indicates that the **clock** command needs more parameters. Any time more information is needed, help can be provided by typing a space after the command and the question mark (?).

```
S1# clock ?
```

What information is displayed? set Set the time and date

- Set the clock using the **clock set** command. Proceed through the command one step at a time.

```
S1# clock set ?
```

What information is being requested? hh:mm:ss Current Time

What would have been displayed if only the **clock set** command had been entered, and no request for help was made by using the question mark? % Incomplete command.

- Based on the information requested by issuing the **clock set ?** command, enter a time of 3:00 p.m. by using the 24-hour format of 15:00:00. Check to see if more parameters are needed.

```
S1# clock set 15:00:00 ?
```

The output returns a request for more information:

```
<1-31>   Day of the month
MONTH    Month of the year
```

- Attempt to set the date to 01/31/2035 using the format requested. It may be necessary to request additional help using the context-sensitive Help to complete the process. When finished, issue the **show clock** command to display the clock setting. The resulting command output should display as:

```
S1# show clock
*15:0:4.869 UTC Tue Jan 31 2035
```

- If you were not successful, try the following command to obtain the output above:

```
S1# clock set 15:00:00 31 Jan 2035
```

Explore additional command messages.

- The IOS provides various outputs for incorrect or incomplete commands. Continue to use the **clock** command to explore additional messages that may be encountered as you learn to use the IOS.
- Issue the following command and record the messages:

```
S1# cl
```

What information was returned? % Ambiguous command: "cl"

```
S1# clock
```

What information was returned? % Incomplete command.

```
S1# clock set 25:00:00
```

What information was returned?

```
S1#clock set 25:00:00
               ^
% Invalid input detected at '^' marker
```

```
S1# clock set 15:00:00 32
```

What information was returned?

```
S1#clock set 15:00:00 32
                      ^
% Invalid input detected at '^' marker.
```

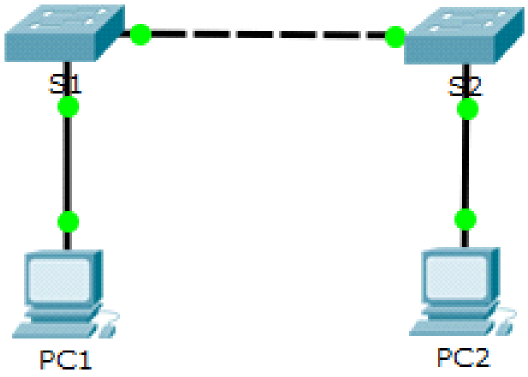
Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
	Step 2b	5	
	Step 2d	5	

Part 1: Establish Basic Connections, Access the CLI, and Explore Help	Step 3a	5	
	Step 3b	5	
	Step 3c	5	
	Part 1 Total	**25**	
Part 2: Explore EXEC Modes	Step 1a	5	
	Step 1b	5	
	Step 1c	5	
	Step 1d	5	
	Step 2a	5	
	Step 2b	5	
	Part 2 Total	**30**	
Part 3: Set the Clock	Step 1a	5	
	Step 1b	5	
	Step 1c	5	
	Step 1d	5	
	Step 2b	5	
	Part 3 Total	**25**	
	Packet Tracer Score	**20**	
	Total Score	**100**	100

2.2 Packet Tracer - Implementing Basic Connectivity

- **Topology**



- **Addressing Table**

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC1	NIC	192.168.1.1	255.255.255.0

PC2	NIC	192.168.1.2	255.255.255.0

- ## Objectives

Part 1: Perform a Basic Configuration on S1 and S2

Part 2: Configure the PCs

Part 3: Configure the Switch Management Interface

- ## Background

In this activity, you will first perform basic switch configurations. Then, you will implement basic connectivity by configuring IP addressing on switches and PCs. When the IP addressing configuration is complete, you will use various **show** commands to verify configurations and use the **ping** command to verify basic connectivity between devices.

- # Perform a Basic Configuration on S1 and S2

Complete the following steps on S1 and S2.

- ### Configure S1 with a hostname.

- Click S1 and then click the **CLI** tab.
- Enter the correct command to configure the hostname as **S1**.

- ### Configure the console and privileged EXEC mode passwords.

- Use **cisco** for the console password.
- Use **class** for the privileged EXEC mode password.

- ### Verify the password configurations for S1.

How can you verify that both passwords were configured correctly?

exit until you are at the startup screen, then press enter to get password prompt. Next enter enable and there should be another password prompt

Configure an MOTD banner.

Use an appropriate banner text to warn unauthorized access. The following text is an example:

Authorized access only. Violators will be prosecuted to the full extent of the law.

- ### Save the configuration file to NVRAM.

Which command do you issue to accomplish this step?

configure

banner motd "Authorized access only. Violators will be prosecuted to the full extent of the law."

exit

write memory

- ### Repeat Steps 1 to 5 for S2.

- # Configure the PCs

Configure PC1 and PC2 with IP addresses.

- ### Configure both PCs with IP addresses.

  - Click PC1 and then click the **Desktop** tab.

- Click **IP Configuration**. In the Addressing Table above, you can see that the IP address for PC1 is 192.168.1.1 and the subnet mask is 255.255.255.0. Enter this information for PC1 in the **IP Configuration** window.
- Repeat steps 1a and 1b for PC2.

- **Test connectivity to switches.**

  - Click PC1. Close the **IP Configuration** window if it is still open. In the **Desktop** tab, click **Command Prompt**.
  - Type the **ping** command and the IP address for S1 and press Enter.

```
Packet Tracer PC Command Line 1.0
PC> ping 192.168.1.253
```

Were you successful? Explain.

yes. I configured switches too early in exercise

Configure the Switch Management Interface

Configure S1 and S2 with an IP address.

Configure S1 with an IP address.

Switches can be used as plug-and-play devices. This means that they do not need to be configured for them to work. Switches forward information from one port to another based on MAC addresses. If this is the case, why would we configure it with an IP address?

While switches can operate without configuration for basic connectivity, configuring an IP address is crucial for management, troubleshooting, and advanced functionality in a more complex network environment. It enhances the switch's capabilities and integrates it into a larger, managed network effectively.

Use the following commands to configure S1 with an IP address.

```
S1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.253 255.255.255.0
S1(config-if)# no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S1(config-if)#
S1(config-if)# exit
S1#
```

Why do you enter the **no shutdown** command?

so the machine doesn't shut down when applying configuration

Configure S2 with an IP address.

Use the information in the Addressing Table to configure S2 with an IP address.

Verify the IP address configuration on S1 and S2.

Use the **show ip interface brief** command to display the IP address and status of all the switch ports and interfaces. You can also use the **show running-config** command.

Save configurations for S1 and S2 to NVRAM.

Which command is used to save the configuration file in RAM to NVRAM?

write memory

Verify network connectivity.

Network connectivity can be verified using the **ping** command. It is very important that connectivity exists throughout the network. Corrective action must be taken if there is a failure. Ping S1 and S2 from PC1 and PC2.

- Click PC1 and then click the **Desktop** tab.
- Click **Command Prompt**.
- Ping the IP address for PC2.
- Ping the IP address for S1.
- Ping the IP address for S2.

Note: You can also use the **ping** command on the switch CLI and on PC2.

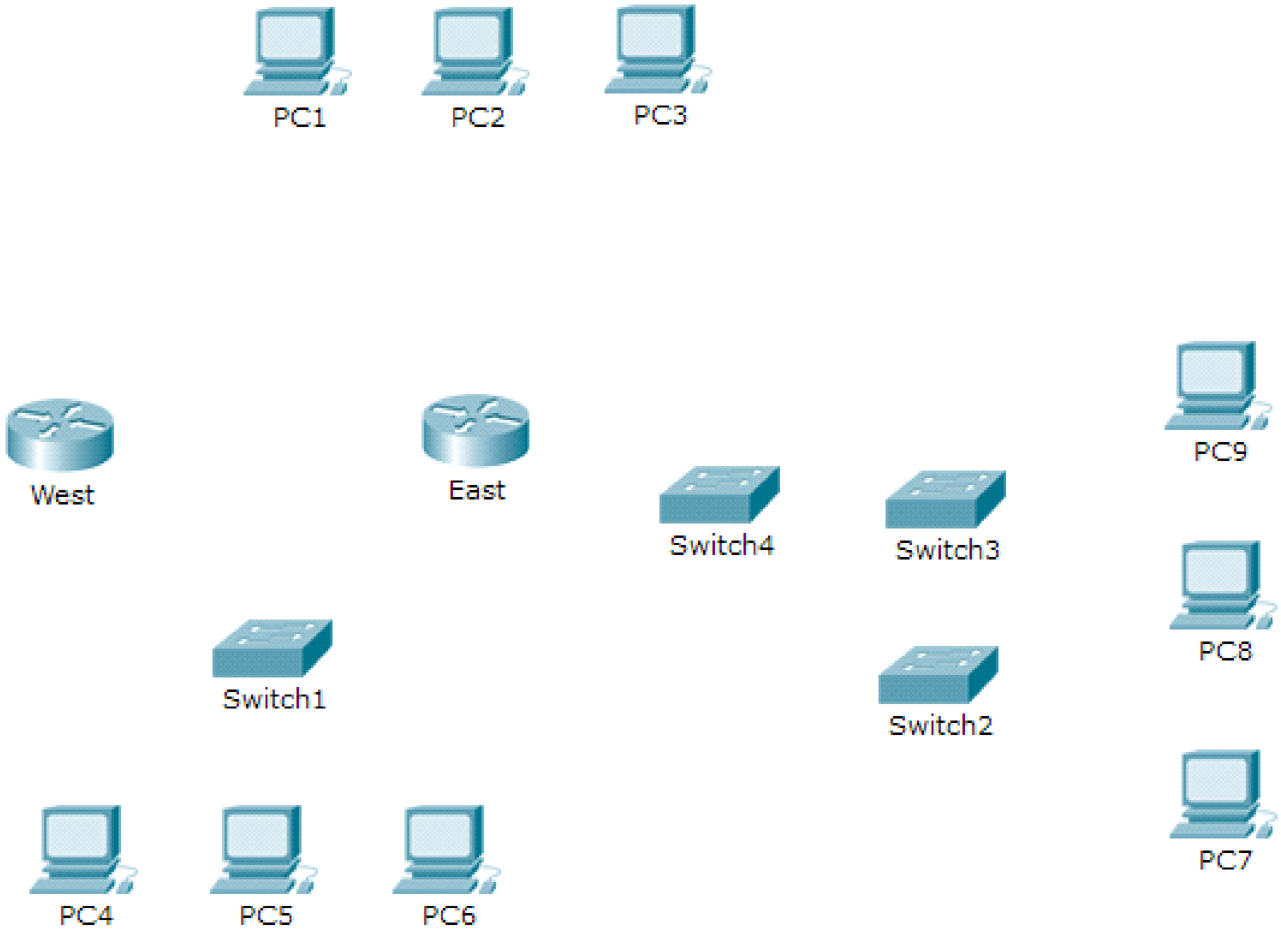
All pings should be successful. If your first ping result is 80%, try again. It should now be 100%. You will learn why a ping may sometimes fail the first time later in your studies. If you are unable to ping any of the devices, recheck your configuration for errors.

- **Suggested Scoring Rubric**

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Perform a Basic Configuration on S1 and S2	Step 3	2	
	Step 5	2	
Part 2: Configure the PCs	Step 2b	2	
Part 3: Configure the Switch Management Interface	Step 1, q1	2	
	Step 1, q2	2	
	Step 4	2	
	Questions	**12**	
	Packet Tracer Score	**88**	
	Total Score	**100**	100

2.3 Packet Tracer - Exploring Internetworking Devices

- ### Topology



- ### Objectives

Part 1: Identify Physical Characteristics of Internetworking Devices

Part 2: Select Correct Modules for Connectivity

Part 3: Connect Devices

- ### Background

In this activity, you will explore the different options available on internetworking devices. You will also be required to determine which options provide the necessary connectivity when connecting multiple devices. Finally, you will add the correct modules and connect the devices.

Note: Scoring for this activity is a combination of Packet Tracer-automated scoring and your recorded answers to the questions posed in the instructions. See the Suggested Scoring Rubric at the end of this activity, and consult with your instructor to determine your final score.

- ## Identify Physical Characteristics of Internetworking Devices

- ### Identify the management ports of a Cisco router.

- Click the **East** router. The **Physical** tab should be active.
- Zoom in and expand the window to see the entire router.

- Which management ports are available? The Cisco 1941 router, along with its modules, offers three management ports in total, allowing for both local and remote management capabilities

- ### Identify the LAN and WAN interfaces of a Cisco router

- Which LAN and WAN interfaces are available on the **East** router and how many are there?

  Total LAN Interfaces: 5

  Total WAN Interfaces: 2

- Click the **CLI** tab and enter the following commands:

  ```
  East> show ip interface brief
  ```

  The output verifies the correct number of interfaces and their designation. The vlan1 interface is a virtual interface that only exists in software. How many physical interfaces are listed? 4

- Enter the following commands:

  ```
  East> show interface gigabitethernet 0/0
  ```

  What is the default bandwidth of this interface? BW 1000000 Kbit

  ```
  East> show interface serial 0/0/0
  ```

  What is the default bandwidth of this interface? BW 1544 Kbit

  Note: Bandwidth on serial interfaces is used by routing processes to determine the best path to a destination. It does not indicate the actual bandwidth of the interface. Actual bandwidth is negotiated with a service provider.

- ### Identify module expansion slots on switches.

- How many expansion slots are available to add additional modules to the **East** router? 1

- Click **Switch2** or **Switch3.** How many expansion slots are available? 5

- ## Select Correct Modules for Connectivity

- ### Determine which modules provide the required connectivity.

- Click **East** and then click the **Physical** tab. On the left, beneath the **Modules** label, you see the available options to expand the capabilities of the router. Click each module. A picture and a description displays at the bottom. Familiarize yourself with these options.

- You need to connect PCs 1, 2, and 3 to the **East** router, but you do not have the necessary funds to purchase a new switch. Which module can you use to connect the three PCs to the **East** router?

  HWIC-4ESW

- How many hosts can you connect to the router using this module? 4

- Click **Switch2**. Which module can you insert to provide a Gigabit optical connection to **Switch3**?

  PT-SWITCH-NM-1FGE

- ### Add the correct modules and power up devices.

- Click **East** and attempt to insert the appropriate module from Step 1a.

- The `Cannot add a module when the power is on` message should display. Interfaces for this router model are not hot-swappable. The device must be turned off. Click the power switch located to the right of the Cisco logo to turn off **East**. Insert the appropriate module from Step 1a. When done, click the power switch to power up **East**.

  Note: If you insert the wrong module and need to remove it, drag the module down to its picture in the bottom right corner, and release the mouse button.

- Using the same procedure, insert the appropriate modules from Step 1b in the empty slot farthest to the right in both **Switch2** and **Switch3**.

- Use the **show ip interface brief** command to identify the slot in which the module was placed.

Into which slot was it inserted? GigabitEthernet5/1

- Click the **West** router. The **Physical** tab should be active. Install the appropriate module that will add a serial interface to the enhanced high-speed WAN interface card (**eHWIC 0**) slot on the right. You can cover any unused slots to prevent dust from entering the router (optional).
- Use the appropriate command to verify that the new serial interfaces are installed.

Connect Devices

This may be the first activity you have done where you are required to connect devices. Although you may not know the purpose of the different cable types, use the table below and follow these guidelines to successfully connect all the devices:

- Select the appropriate cable type.
- Click the first device and select the specified interface.
- Click the second device and select the specified interface.
- If you correctly connected two devices, you will see your score increase.

Example: To connect **East** to **Switch1**, select the **Copper Straight-Through** cable type. Click **East** and choose **GigabitEthernet0/0**. Then, click **Switch1** and choose **GigabitEthernet0/1**. Your score should now be 4/52.

Note: For the purposes of this activity, link lights are disabled. The devices are not configured with any IP addressing, so you are unable to test connectivity.

Device	Interface	Cable Type	Device	Interface
East	GigabitEthernet0/0	Copper Straight-Through	Switch1	GigabitEthernet0/1
East	GigabitEthernet0/1	Copper Straight-Through	Switch4	GigabitEthernet0/1
East	FastEthernet0/1/0	Copper Straight-Through	PC1	FastEthernet0
East	FastEthernet0/1/1	Copper Straight-Through	PC2	FastEthernet0
East	FastEthernet0/1/2	Copper Straight-Through	PC3	FastEthernet0
Switch1	FastEthernet0/1	Copper Straight-Through	PC4	FastEthernet0
Switch1	FastEthernet0/2	Copper Straight-Through	PC5	FastEthernet0
Switch1	FastEthernet0/3	Copper Straight-Through	PC6	FastEthernet0
Switch4	GigabitEthernet0/2	Copper Cross-Over	Switch3	GigabitEthernet3/1
Switch3	GigabitEthernet5/1	Fiber	Switch2	GigabitEthernet5/1
Switch2	FastEthernet0/1	Copper Straight-Through	PC7	FastEthernet0
Switch2	FastEthernet1/1	Copper Straight-Through	PC8	FastEthernet0
Switch2	FastEthernet2/1	Copper Straight-Through	PC9	FastEthernet0
East	Serial0/0/0	Serial DCE (connect to East first)	West	Serial0/0/0

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Identify Physical Characteristics of Internetworking Devices	Step 1c	4	
	Step 2a	4	
	Step 2b	4	
	Step 2c, q1	4	

	Step 2c, q2	4	
	Step 3a	4	
	Step 3b	4	
Part 1 Total		**28**	28
Part 2: Select Correct Modules for Connectivity	Step 1a, q1	5	
	Step 1a, q2	5	
	Step 1b	5	
	Step 2d	5	
Part 2 Total		**20**	20
Packet Tracer Score		**52**	52
Total Score		**100**	100

2.4 Packet Tracer - Configure Initial Router Settings

- ### Topology

- ### Objectives

Part 1: Verify the Default Router Configuration

Part 2: Configure and Verify the Initial Router Configuration

Part 3: Save the Running Configuration File

- ### Background

In this activity, you will perform basic router configurations. You will secure access to the CLI and console port using encrypted and plain text passwords. You will also configure messages for users logging into the router. These banners also warn unauthorized users that access is prohibited. Finally, you will verify and save your running configuration.

- ## Verify the Default Router Configuration

- ### Establish a console connection to R1.

- Choose a **Console** cable from the available connections.
- Click **PCA** and select **RS 232**.
- Click **R1** and select **Console**.
- Click **PCA** > **Desktop** tab > **Terminal**.
- Click **OK** and press **ENTER**. You are now able to configure **R1**.

Enter privileged mode and examine the current configuration.

You can access all the router commands from privileged EXEC mode. However, because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use.

- Enter privileged EXEC mode by entering the **enable** command.

  ```
  Router> enable
  Router#
  ```

  Notice that the prompt changed in the configuration to reflect privileged EXEC mode.

- Enter the `show running-config` command:

  ```
  Router# show running-config
  ```

- Answer the following questions:

  What is the router's hostname? Router

  How many Fast Ethernet interfaces does the Router have? 4

  How many Gigabit Ethernet interfaces does the Router have? 2

  How many Serial interfaces does the router have? 2

  What is the range of values shown for the vty lines? 0-4

- Display the current contents of NVRAM.

  ```
  Router# show startup-config
  startup-config is not present
  ```

  Why does the router respond with the `startup-config is not present` message?

  because configuration file is saved on RAM and not NVRAM

Configure and Verify the Initial Router Configuration

To configure parameters on a router, you may be required to move between various configuration modes. Notice how the prompt changes as you navigate through the router.

Configure the initial settings on R1.

Note: If you have difficulty remembering the commands, refer to the content for this topic. The commands are the same as you configured on a switch.

- **R1** as the hostname.
- Use the following passwords:
- Console: **letmein**
- Privileged EXEC, unencrypted: **cisco**
- Privileged EXEC, encrypted: **itsasecret**
- Encrypt all plain text passwords.
- Message of the day text: `Unauthorized access is strictly prohibited.`

Verify the initial settings on R1.

- Verify the initial settings by viewing the configuration for R1. What command do you use?

  show running-config

- Exit the current console session until you see the following message:

  ```
  R1 con0 is now available

  Press RETURN to get started.
  ```

- Press **ENTER**; you should see the following message:

  ```
  Unauthorized access is strictly prohibited.

  User Access Verification

  Password:
  ```

  Why should every router have a message-of-the-day (MOTD) banner?

  you can warn about unauthorized access but can also be used to message technicians

  If you are not prompted for a password, what console line command did you forget to configure?

  R1(config-line)# login

- Enter the passwords necessary to return to privileged EXEC mode.

  Why would the **enable secret** password allow access to the privileged EXEC mode and **the enable password** no longer be valid?

  enable secret password overrides the enable password

  If you configure any more passwords on the router, are they displayed in the configuration file as plain text or in encrypted form? Explain.

  the service password-encryption encrypts all passwords

• Save the Running Configuration File

• Save the configuration file to NVRAM.

- You have configured the initial settings for **R1**. Now back up the running configuration file to NVRAM to ensure that the changes made are not lost if the system is rebooted or loses power.

  What command did you enter to save the configuration to NVRAM?

  write memory

  What is the shortest, unambiguous version of this command? wr

  Which command displays the contents of the NVRAM?

  show startup-configuration

- Verify that all of the parameters configured are recorded. If not, analyze the output and determine which commands were not done or were entered incorrectly. You can also click **Check Results** in the instruction window.

• Optional bonus: Save the startup configuration file to flash.

Although you will be learning more about managing the flash storage in a router in later chapters, you may be interested to know now that —, as an added backup procedure —, you can save your startup configuration file to flash. By default, the router still loads the startup configuration from NVRAM, but if NVRAM becomes corrupt, you can restore the startup configuration by copying it over from flash.

Complete the following steps to save the startup configuration to flash.

- Examine the contents of flash using the **show flash** command:

  ```
  R1# show flash
  ```

  How many files are currently stored in flash? 3

  Which of these files would you guess is the IOS image? c1900-universalk9-mz.SPA.151-4.M4.bin

  Why do you think this file is the IOS image?

  the bin is a giveaway in the file extension

- Save the startup configuration file to flash using the following commands:

```
R1# copy startup-config flash
Destination filename [startup-config]
```

The router prompts to store the file in flash using the name in brackets. If the answer is yes, then press **ENTER**; if not, type an appropriate name and press **ENTER**.

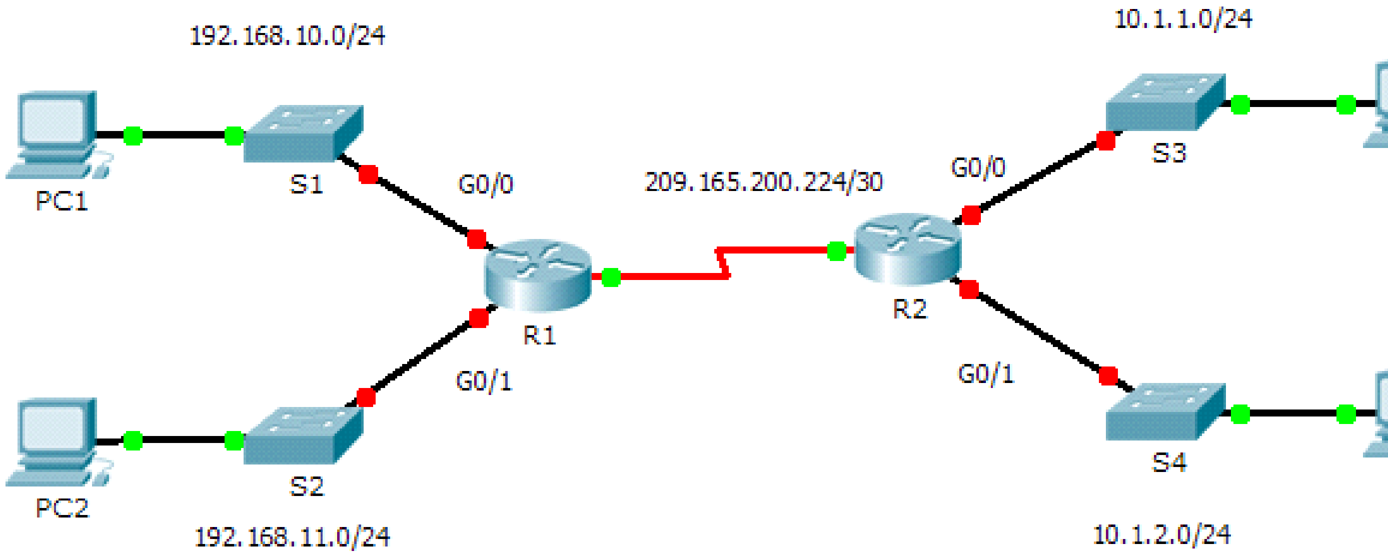
- Use the **show flash** command to verify the startup configuration file is now stored in flash.

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Verify the Default Router Configuration	Step 2c	10	
	Step 2d	2	
	Part 1 Total	**12**	
Part 2: Configure and Verify the Initial Router Configuration	Step 2a	2	
	Step 2c	5	
	Step 2d	6	
	Part 2 Total	**13**	
Part 3: Save the Running Configuration File	Step 1a	5	
	Step 2a (bonus)	5	
	Part 3 Total	**10**	
	Packet Tracer Score	**80**	
	Total Score (with bonus)	**105**	

2.5 Packet Tracer - Connect a Router to a LAN

- ### Topology



- ### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0 (DCE)	209.165.200.225	255.255.255.252	N/A
R2	G0/0	10.1.1.1	255.255.255.0	N/A
	G0/1	10.1.2.1	255.255.255.0	N/A
	S0/0/0	209.165.200.226	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	10.1.1.10	255.255.255.0	10.1.1.1
PC4	NIC	10.1.2.10	255.255.255.0	10.1.2.1

- ### Objectives

Part 1: Display Router Information

Part 2: Configure Router Interfaces

Part 3: Verify the Configuration

- ### Background

In this activity, you will use various **show** commands to display the current state of the router. You will then use the Addressing Table to configure router Ethernet interfaces. Finally, you will use commands to verify and test your configurations.

Note: The routers in this activity are partially configured. Some of the configurations are not covered in this course, but are provided to assist you in using verification commands.

- ## Display Router Information

- ### Display interface information on R1.

Note: Click a device and then click the **CLI** tab to access the command line directly. The console password is **cisco**. The privileged EXEC password is **class**.

- Which command displays the statistics for all interfaces configured on a router? show interfaces
- Which command displays the information about the Serial 0/0/0 interface only?show interfaces serial 0/0/0
- Enter the command to display the statistics for the Serial 0/0/0 interface on R1 and answer the following questions:
- What is the IP address configured on **R1**? 209.165.200.255/30
- What is the bandwidth on the Serial 0/0/0 interface? 1544 Kbit
- Enter the command to display the statistics for the GigabitEthernet 0/0 interface and answer the following questions:
- What is the IP address on **R1**? The ip address has not been configured on the interface
- What is the MAC address of the GigabitEthernet 0/0 interface? 000d.bd6c.7d01
- What is the bandwidth on the GigabitEthernet 0/0 interface? 1000000 Kbit

- ### Display a summary list of the interfaces on R1.

- Which command displays a brief summary of the current interfaces, statuses, and IP addresses assigned to them?

  show ip interface brief
- Enter the command on each router and answer the following questions:
- How many serial interfaces are there on **R1** and **R2**? 2 on each
- How many Ethernet interfaces are there on **R1** and **R2**?

  R1=2 R2=6

  Are all the Ethernet interfaces on **R1** the same? If no, explain the difference(s).

  no, because GigabitEthernet(2 ports) supports much faster speeds than FastEthernet(6 ports)

- ### Display the routing table on R1.

- What command displays the content of the routing table? show ip route
- Enter the command on **R1** and answer the following questions:
- How many connected routes are there (uses the C code)? 1

  Which route is listed? 209.165.200.224/30 is directly connected, Serial0/0/0
- How does a router handle a packet destined for a network that is not listed in the routing table?

  If the router has no route on routing table, the package will be dropped

- ## Configure Router Interfaces

- ### Configure the GigabitEthernet 0/0 interface on R1.

- Enter the following commands to address and activate the GigabitEthernet 0/0 interface on **R1**:

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
```

- It is good practice to configure a description for each interface to help document the network information. Configure an interface description indicating to which device it is connected.

```
R1(config-if)# description LAN connection to S1
```

- **R1** should now be able to ping PC1.

```
R1(config-if)# end
%SYS-5-CONFIG_I: Configured from console by console
R1# ping 192.168.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms
```

- **Configure the remaining Gigabit Ethernet Interfaces on R1 and R2.**

- Use the information in the Addressing Table to finish the interface configurations for **R1** and **R2**. For each interface, do the following:
- Enter the IP address and activate the interface.
- Configure an appropriate description.
- Verify interface configurations.

- **Back up the configurations to NVRAM.**

Save the configuration files on both routers to NVRAM. What command did you use?

copy running-config startup-config

• Verify the Configuration

- **Use verification commands to check your interface configurations.**

- Use the **show ip interface brief** command on both **R1** and **R2** to quickly verify that the interfaces are configured with the correct IP address and active.

How many interfaces on **R1** and **R2** are configured with IP addresses and in the “up” and “up” state?

R1=3, R2=3

What part of the interface configuration is NOT displayed in the command output? the subnet mask

What commands can you use to verify this part of the configuration?

show interfaces, show running-config

se the **show ip route** command on both **R1** and **R2** to view the current routing tables and answer the following questions:

How many connected routes (uses the **C** code) do you see on each router? R1=3, R2=3

How many EIGRP routes (uses the **D** code) do you see on each router? 2

If the router knows all the routes in the network, then the number of connected routes and dynamically learned routes (EIGRP) should equal the total number of LANs and WANs. How many LANs and WANs are in the topology? 5

Does this number match the number of C and D routes shown in the routing table? yes

Note: If your answer is “no”, then you are missing a required configuration. Review the steps in Part 2.

- ### Test end-to-end connectivity across the network.

You should now be able to ping from any PC to any other PC on the network. In addition, you should be able to ping the active interfaces on the routers. For example, the following should tests should be successful:

- From the command line on PC1, ping PC4. ping 10.1.2.10
- From the command line on R2, ping PC2. ping 192.168.11.10

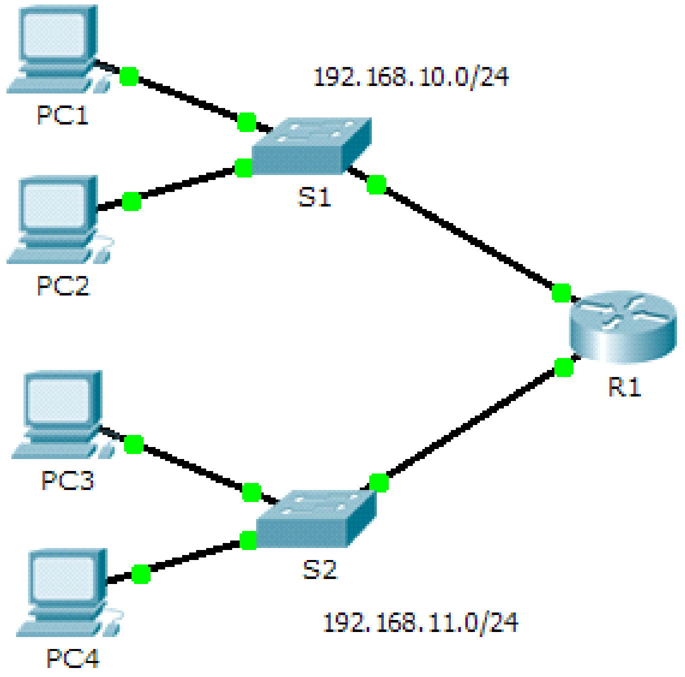
Note: For simplicity in this activity, the switches are not configured; you will not be able to ping them.

- ## Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Display Router Information	Step 1a	2	
	Step 1b	2	
	Step 1c	4	
	Step 1d	6	
	Step 2a	2	
	Step 2b	6	
	Step 3a	2	
	Step 3b	6	
	Part 1 Total	**30**	
Part 2: Configure Router Interfaces	Step 3	2	
	Part 2 Total	**2**	
Part 3: Verify the Configuration	Step 1a	6	
	Step 1b	8	
	Part 3 Total	**14**	
	Packet Tracer Score	**54**	
	Total Score (with bonus)	**100**	

2.6 Packet Tracer - Troubleshooting Default Gateway Issues

- ### Topology



- ### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	192.168.11.1	255.255.255.0	N/A
S1	VLAN 1	192.168.10.2	255.255.255.0	
S2	VLAN 1	192.168.11.2	255.255.255.0	
PC1	NIC	192.168.10.10	255.255.255.0	
PC2	NIC	192.168.10.11	255.255.255.0	
PC3	NIC	192.168.11.10	255.255.255.0	
PC4	NIC	192.168.11.11	255.255.255.0	

- ### Objectives

Part 1: Verify Network Documentation and Isolate Problems

Part 2: Implement, Verify, and Document Solutions

- ### Background

For a device to communicate across multiple networks, it must be configured with an IP address, subnet mask, and a default gateway. The default gateway is used when the host wants to send a packet to a device on another network. The default gateway address is generally the router interface address attached to the local network to which the host is connected. In this activity, you will finish documenting the network. You will then verify the network documentation by testing end-to-end connectivity and troubleshooting issues. The troubleshooting method you will use consists of the following steps:

- Verify the network documentation and use tests to isolate problems.
- Determine an appropriate solution for a given problem.
- Implement the solution.
- Test to verify the problem is resolved.
- Document the solution.

Throughout your CCNA studies, you will encounter different descriptions of the troubleshooting method, as well as different ways to test and document issues and solutions. This is intentional. There is no set standard or template for troubleshooting. Each organization develops unique processes and documentation standards (even if that process is “we don’t have one”). However, all effective troubleshooting methodologies generally include the above steps.

Note: If you are proficient with default gateway configurations, this activity might seem more involved than it should be. You can, most likely, quickly discover and solve all the connectivity issues faster than following these procedures. However, as you proceed in your studies, the networks and problems you encounter will become increasingly more complex. In such situations, the only effective way to isolate and solve issues is to use a methodical approach such as the one used in this activity.

• Verify Network Documentation and Isolate Problems

In Part 1 of this activity, complete the documentation and perform connectivity tests to discover issues. In addition, you will determine an appropriate solution for implementation in Part 2.

• Verify the network documentation and isolate any problems.

- Before you can effectively test a network, you must have complete documentation. Notice in the **Addressing Table** that some information is missing. Complete the **Addressing Table** by filling in the missing default gateway information for the switches and the PCs.
- Test connectivity to devices on the same network. By isolating and correcting any local access issues, you can better test remote connectivity with the confidence that local connectivity is operational.

  A verification plan can be as simple as a list of connectivity tests. Use the following tests to verify local connectivity and isolate any access issues. The first issue is already documented, but you must implement and verify the solution during Part 2.

• Testing and Verification Documentation

Test	Successful?	Issues	Solution	Verified
PC1 to PC2	**No**	**IP address on PC1**	**Change PC1 IP address**	
PC1 to S1				
PC1 to R1				

Note: The table is an example; you must create your own document. You can use paper and pencil to draw a table, or you can use a text editor or spreadsheet. Consult your instructor if you need further guidance.

- Test connectivity to remote devices (such as from PC1 to PC4) and document any problems. This is frequently referred to as *end-to-end connectivity*. This means that all devices in a network have the full connectivity allowed by the network policy.

  Note: Remote connectivity testing may not be possible yet, because you must first resolve local connectivity issues. After you have solved those issues, return to this step and test connectivity between networks.

Determine an appropriate solution for the problem.

- Using your knowledge of the way networks operate and your device configuration skills, search for the cause of the problem. For example, S1 is not the cause of the connectivity issue between PC1 and PC2. The link lights are green and no configuration on S1 would cause traffic to not pass between PC1 and PC2. So the problem must be with PC1, PC2, or both.
- Verify the device addressing to ensure it matches the network documentation. For example, the IP address for PC1 is incorrect as verified with the **ipconfig** command.
- Suggest a solution that you think will resolve the problem and document it. For example, change the IP address for PC1 to match the documentation.

  Note: Often there is more than one solution. However, it is a troubleshooting best practice to implement one solution at a time. Implementing more than one solution could introduce additional issues in a more complex scenario.

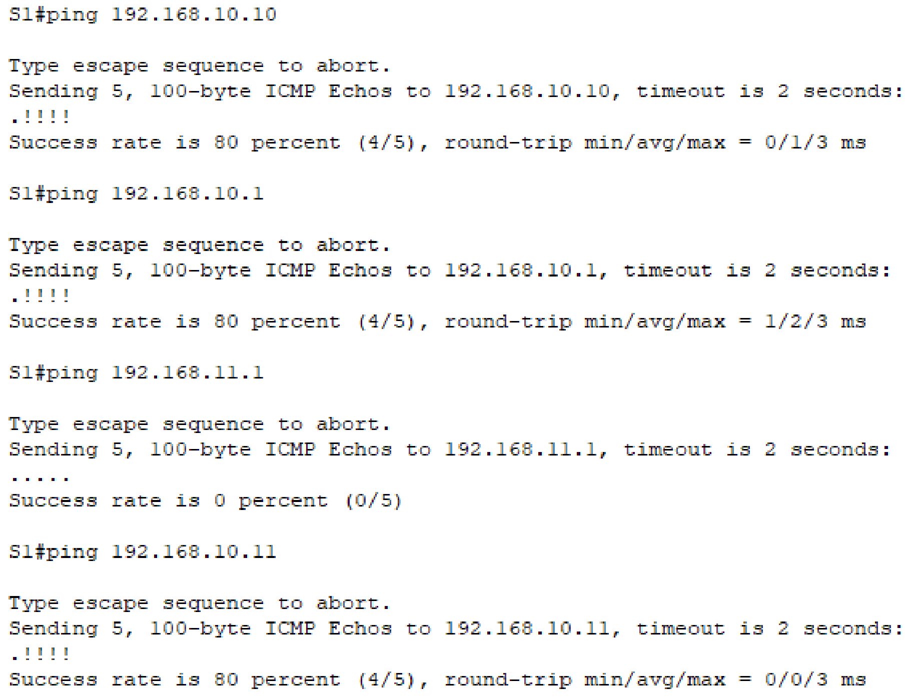
Implement, Verify, and Document Solutions

In Part 2 of this activity, you will implement the solutions you identified in Part 1. You will then verify the solution worked. You may need to return to Part 1 to finish isolating all the problems.

Implement solutions to connectivity problems.

Refer to your documentation in Part 1. Choose the first issue and implement your suggested solution. For example, correct the IP address on PC1.

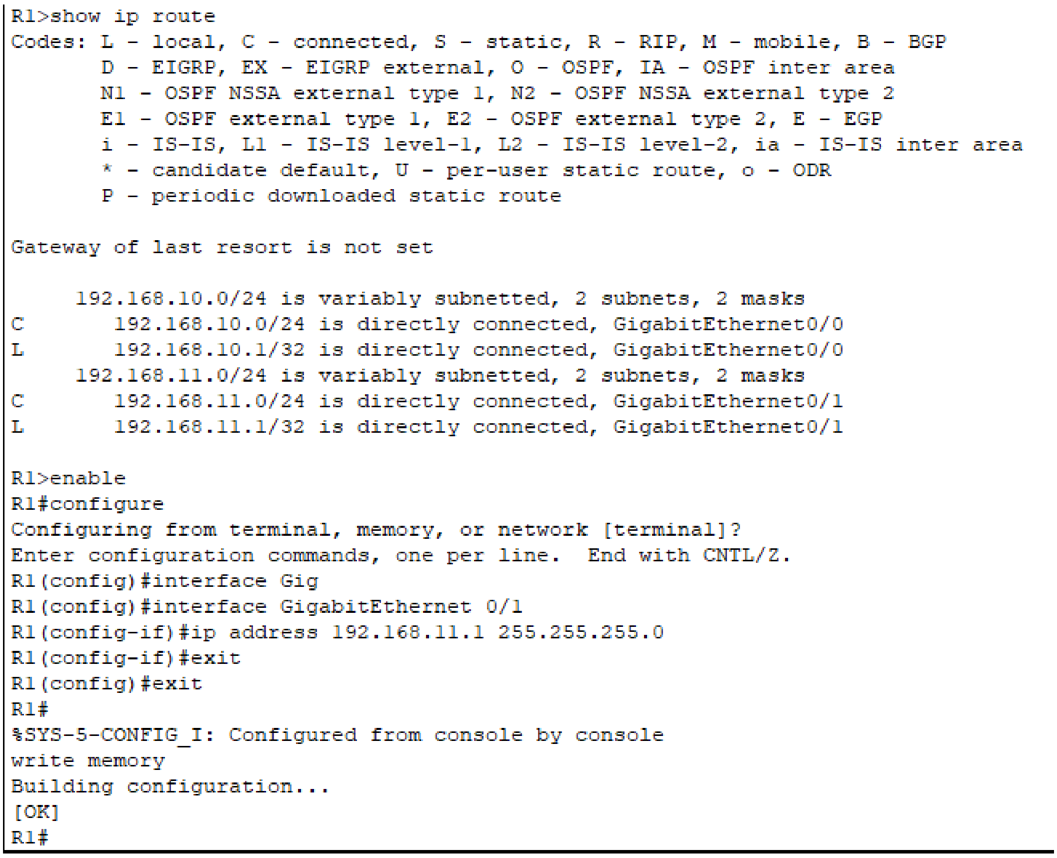
PC1 had wrong ip. It should be 192.168.10.10.



```
S1#ping 192.168.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/3 ms

S1#ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/3 ms

S1#ping 192.168.11.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

S1#ping 192.168.10.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.11, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/3 ms
```

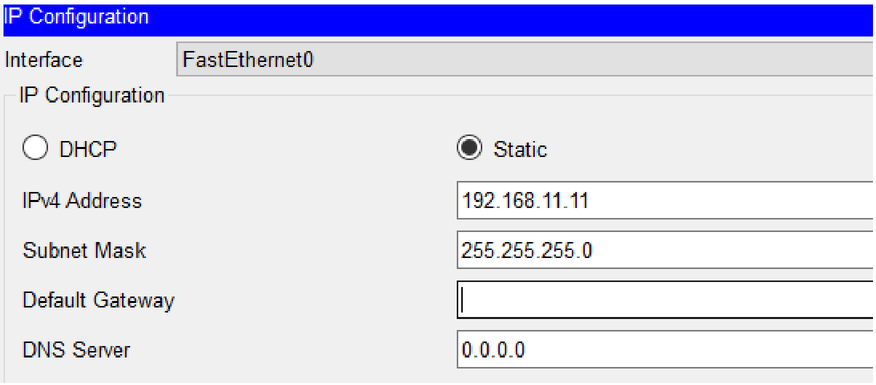
S1 vlan was setup incorrectly

ping S1 -> R1 G0/1. S1 has been configured properly



```
R1>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/1
L       192.168.11.1/32 is directly connected, GigabitEthernet0/1

R1>enable
R1#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface Gig
R1(config)#interface GigabitEthernet 0/1
R1(config-if)#ip address 192.168.11.1 255.255.255.0
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
R1#
```

PC4 had wrong gateway



IP Configuration

Interface	FastEthernet0

IP Configuration

○ DHCP ● Static

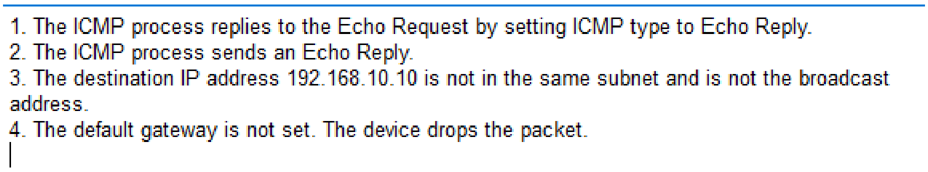
IPv4 Address	192.168.11.11
Subnet Mask	255.255.255.0
Default Gateway	
DNS Server	0.0.0.0

```
Vlan1                  unassigned      YES manual up                    up
```

S2 had no ip address assigned

R1 -> can ping everyone

PC1 -> can ping PC3



1. The ICMP process replies to the Echo Request by setting ICMP type to Echo Reply.
2. The ICMP process sends an Echo Reply.
3. The destination IP address 192.168.10.10 is not in the same subnet and is not the broadcast address.
4. The default gateway is not set. The device drops the packet.

PC4 has been assigned a default gateway. now ping is going through

PC4 was missing default gateway

S1 vlan 1 was not setup and missing default gateway

S2 was missing an ip address

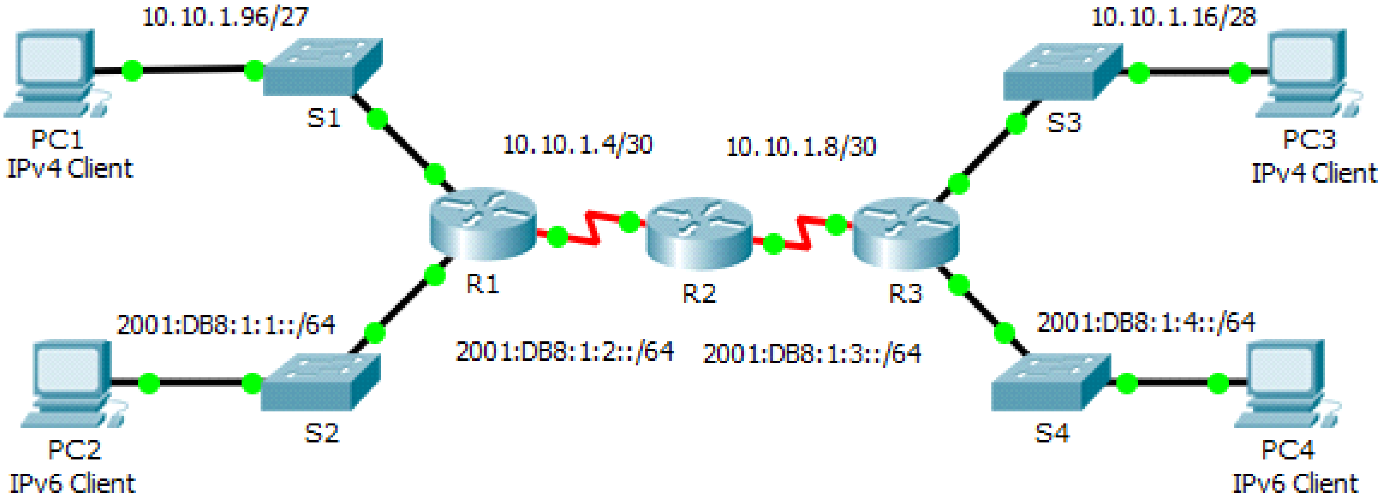
PC1 had wrong ip address

- **Verify that the problem is now resolved.**
  - Verify your solution has solved the problem by performing the test you used to identify the problem. For example, can PC1 now ping PC2?
  - If the problem is resolved, indicate so in your documentation. For example, in the table above, a simple checkmark would suffice in the “Verified” column.
- **Verify that all issues are resolved.**
  - If you still have an outstanding issue with a solution that has not yet been implemented, return to Part 2, Step 1.
  - If all your current issues are resolved, have you also resolved any remote connectivity issues (such as can PC1 ping PC4)? If the answer is no, return to Part 1, Step 1c to test remote connectivity.
- **Suggested Scoring Rubric**

Task	Possible Points	Earned Points
Complete Network Documentation	**20**	
Document Issues and Solutions	**45**	
Packet Tracer Score (Issues Resolved)	**35**	
Total Score	**100**	

2.7 Packet Tracer - Pinging and Tracing to Test the Path

- **Topology**



- **Addressing Table**

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
		IPv6 Address/Prefix		
R1	G0/0	2001:DB8:1:1::1/64		N/A
	G0/1	10.10.1.97	255.255.255.224	N/A
	S0/0/1	10.10.1.6	255.255.255.252	N/A
		2001:DB8:1:2::2/64		N/A
	Link-local	FE80::1		N/A
R2	S0/0/0	10.10.1.5	255.255.255.252	N/A
		2001:DB8:1:2::1/64		N/A
	S0/0/1	10.10.1.9	255.255.255.252	N/A
		2001:DB8:1:3::1/64		N/A
	Link-local	FE80::2		N/A
R3	G0/0	2001:DB8:1:4::1/64		N/A
	G0/1	10.10.1.17	255.255.255.240	N/A
	S0/0/1	10.10.1.10	255.255.255.252	N/A
		2001:DB8:1:3::2/64		N/A
	Link-local	FE80::3		N/A
PC1	NIC	10.10.1.98	255.255.255.224	10.10.1.97
PC2	NIC	2001:DB8:1:1::2		FE80::1
PC3	NIC	10.10.1.18	255.255.255.240	10.10.1.17
PC4	NIC	2001::206:2AFF:FEBC:7CD4		FE80::2

- **Objectives**

Part 1: Test and Restore IPv4 Connectivity

Part 2: Test and Restore IPv6 Connectivity

- ## Scenario

There are connectivity issues in this activity. In addition to gathering and documenting information about the network, you will locate the problems and implement acceptable solutions to restore connectivity.

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

- ## Test and Restore IPv4 Connectivity

- ### Use ipconfig and ping to verify connectivity.

a. Click **PC1** and click the **Desktop** tab > **Command Prompt**.

b. Enter the **ipconfig /all** command to collect the IPv4 information. Complete the **Addressing Table** with the IPv4 address, subnet mask, and default gateway.

c. Click **PC3** and click the **Desktop** tab > **Command Prompt**.

d. Enter the **ipconfig /all** command to collect the IPv4 information. Complete the **Addressing Table** with the IPv4 address, subnet mask, and default gateway.

e. Test connectivity between **PC1** and **PC3**. The ping should fail.

- ### Locate the source of connectivity failure.

a. From **PC1**, enter the necessary command to trace the route to **PC3**. What is the last successful IPv4 address that was reached? 10.10.1.97

b. The trace will eventually end after 30 attempts. Enter **Ctrl**+**C** to stop the trace before 30 attempts.

c. From **PC3**, enter the necessary command to trace the route to **PC1**. What is the last successful IPv4 address that was reached? 10.10.1.17

d. Enter **Ctrl**+**C** to stop the trace.

e. Click **R1** and then the **CLI** tab. Press **ENTER** and log in to the router.

f. Enter the **show ip interface brief** command to list the interfaces and their status. There are two IPv4 addresses on the router. One should have been recorded in Step 2a. What is the other? 10.10.1.6

g. Enter the **show ip route** command to list the networks to which the router is connected. Note that there are two networks connected to the **Serial0/0/1** interface. What are they? 10.10.1.4/30, 10.10.1.6/32

h. Repeat step 2e to 2g with **R3** and record the answers here. 10.10.1.10, 10.10.1.8/30, 10.10.1.10/32

Notice how the serial interface for R3 changes.

a. Run more tests if it helps visualize the problem. Simulation mode is available.

- ### Propose a solution to solve the problem.

a. Compare your answers in Step 2 to the documentation you have available for the network. What is the error?

R2 serial 0/0/0 interface has the wrong ip address

a. What solution would you propose to correct the problem?

configure the correct ip address(10.10.1.5) on serial 0/0/0 interface

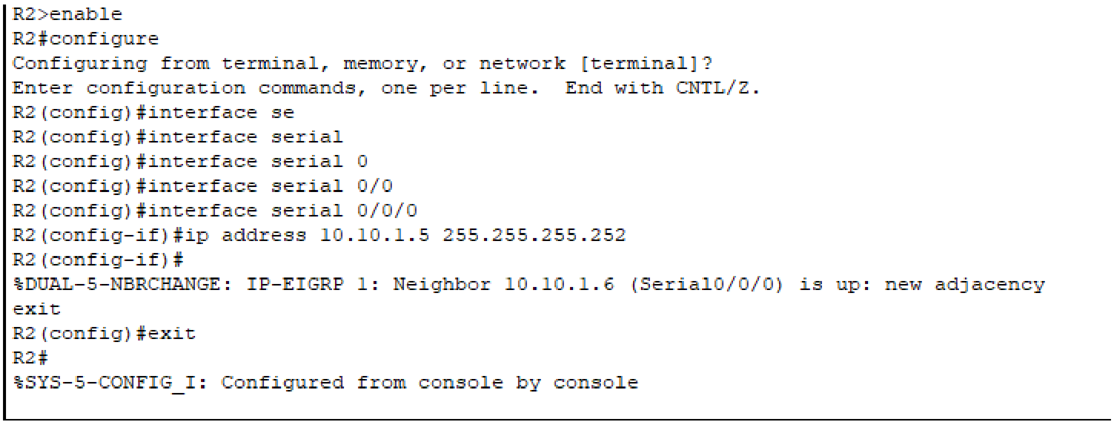
- ### Implement the plan.

Implement the solution you proposed in Step 3b.

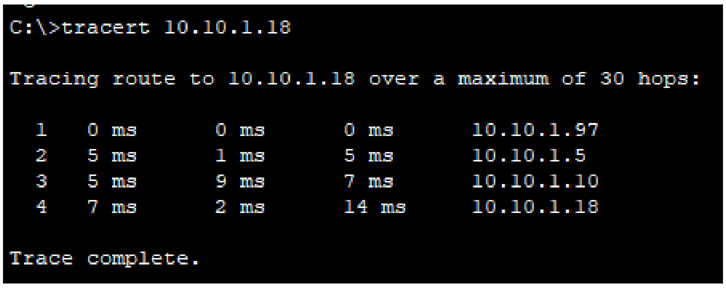
- ### Verify that connectivity is restored.

- From **PC1** test connectivity to **PC3**.

- From **PC3** test connectivity to **PC1**. Is the problem resolved? yes



```
R2>enable
R2#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface se
R2(config)#interface serial
R2(config)#interface serial 0
R2(config)#interface serial 0/0
R2(config)#interface serial 0/0/0
R2(config-if)#ip address 10.10.1.5 255.255.255.252
R2(config-if)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.10.1.6 (Serial0/0/0) is up: new adjacency
exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
```



```
C:\>tracert 10.10.1.18

Tracing route to 10.10.1.18 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      10.10.1.97
  2   5 ms      1 ms      5 ms      10.10.1.5
  3   5 ms      9 ms      7 ms      10.10.1.10
  4   7 ms      2 ms      14 ms     10.10.1.18

Trace complete.
```

- **Document the solution.**

- ## Test and Restore IPv6 Connectivity

- ### Use ipv6config and ping to verify connectivity.

a. Click **PC2** and click the **Desktop** tab > **Command Prompt**.

b. Enter the **ipv6config /all** command to collect the IPv6 information. Complete the **Addressing Table** with the IPv6 address, subnet prefix, and default gateway.

c. Click **PC4** and click the **Desktop** tab > **Command Prompt**.

d. Enter the **ipv6config /all** command to collect the IPv6 information. Complete the **Addressing Table** with the IPv6 address, subnet prefix, and default gateway.

e. Test connectivity between **PC2** and **PC4**. The ping should fail.

- ### Locate the source of connectivity failure.

a. From **PC2**, enter the necessary command to trace the route to **PC4**. What is the last successful IPv6 address that was reached? 2001:DB8:1:3::2

b. The trace will eventually end after 30 attempts. Enter **Ctrl**+**C** to stop the trace before 30 attempts.

c. From **PC4**, enter the necessary command to trace the route to **PC2**. What is the last successful IPv6 address that was reached? No ip address was reached

d. Enter **Ctrl**+**C** to stop the trace.

e. Click **R3** and then the **CLI** tab. Press **ENTER** and log in to the router.

f. Enter the **show ipv6 interface brief** command to list the interfaces and their status. There are two IPv6 addresses on the router. One should match the gateway address recorded in Step 1d. Is there a discrepancy? Yes

g. Run more tests if it helps visualize the problem. Simulation mode is available.

- **Propose a solution to solve the problem.**

a. Compare your answers in Step 2 to the documentation you have available for the network. What is the error?

PC4 has wrong default gateway

a. What solution would you propose to correct the problem?

Configure default gateway to FE80::3

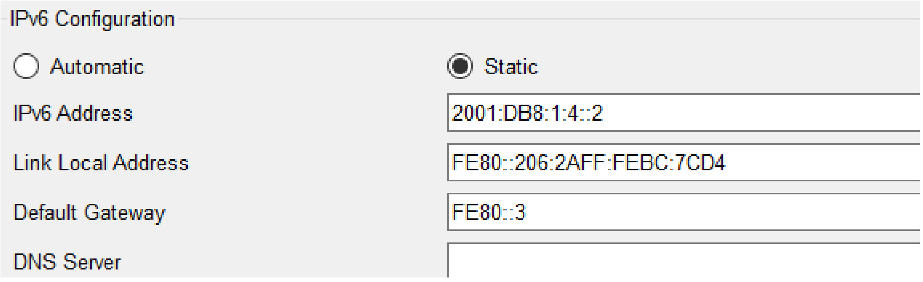
- **Implement the plan.**

Implement the solution you proposed in Step 3b.

- **Verify that connectivity is restored.**

  - From **PC2** test connectivity to **PC4**.
  - From **PC4** test connectivity to **PC2**. Is the problem resolved? Yes

- **Document the solution.**



IPv6 Configuration

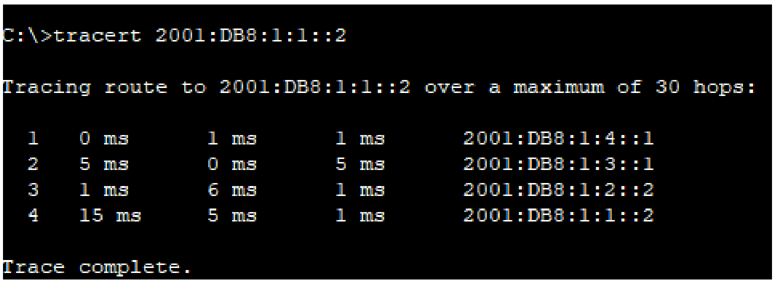
○ Automatic ● Static

IPv6 Address: 2001:DB8:1:4::2

Link Local Address: FE80::206:2AFF:FEBC:7CD4

Default Gateway: FE80::3

DNS Server:



```
C:\>tracert 2001:DB8:1:1::2

Tracing route to 2001:DB8:1:1::2 over a maximum of 30 hops:

  1   0 ms      1 ms      1 ms      2001:DB8:1:4::1
  2   5 ms      0 ms      5 ms      2001:DB8:1:3::1
  3   1 ms      6 ms      1 ms      2001:DB8:1:2::2
  4   15 ms     5 ms      1 ms      2001:DB8:1:1::2

Trace complete.
```

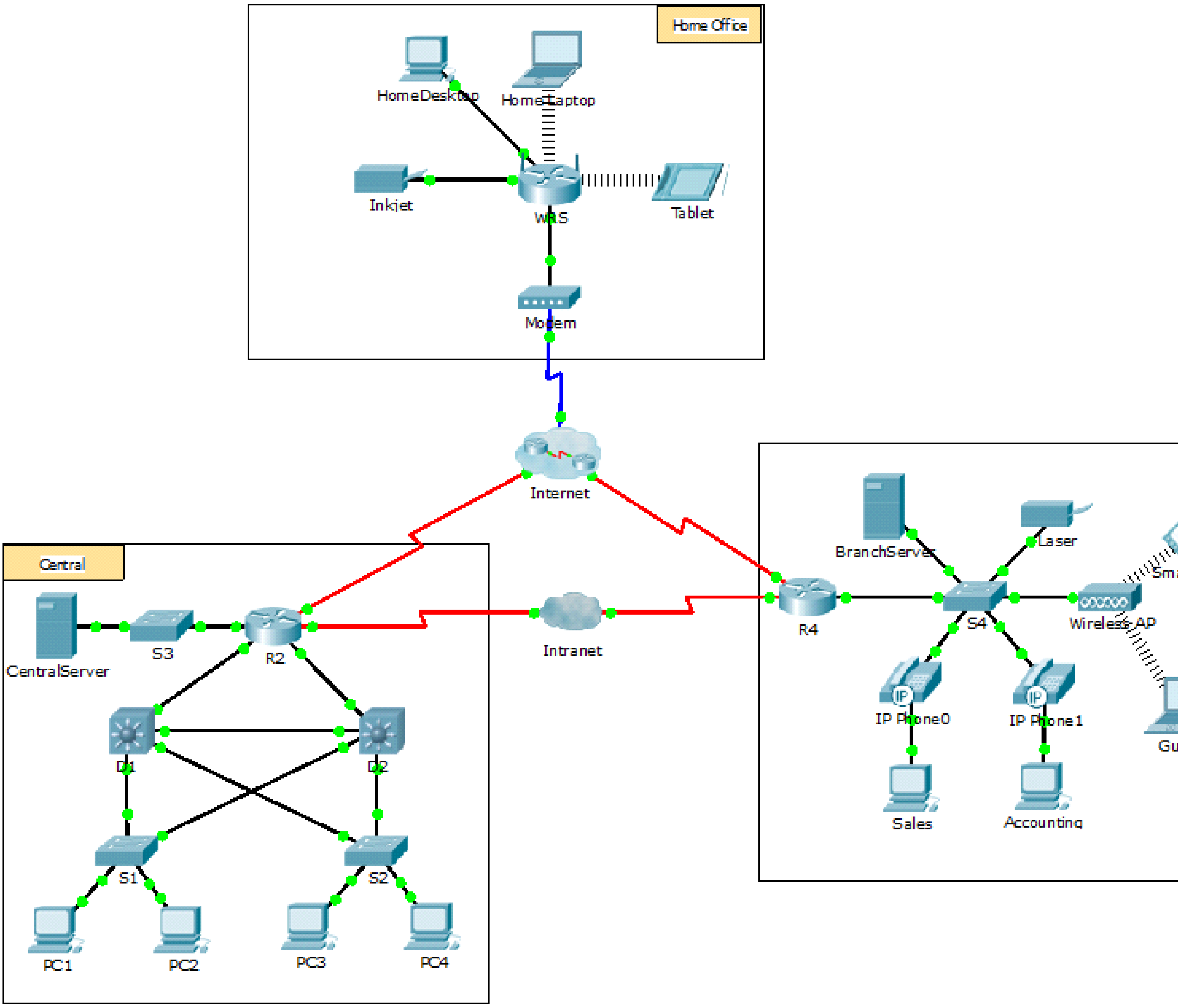
- **Suggested Scoring Rubric**

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Test and Restore Connectivity Between PC1 and PC3	Step 1b	5	
	Step 1d	5	
	Step 2a	5	
	Step 2c	5	

	Step 2f	5	
	Step 2g	5	
	Step 2h	5	
	Step 3a	5	
	Step 3b	5	
	Part 1 Total	**45**	
Part 2: Test and Restore Connectivity Between PC2 and PC4	Step 1b	5	
	Step 1d	5	
	Step 2a	5	
	Step 2c	5	
	Step 2f	5	
	Step 3a	5	
	Step 3b	5	
	Part 2 Total	**35**	
	Packet Tracer Score	**20**	
	Total Score	**100**	

2.8 Packet Tracer - DHCP and DNS Servers

- ### Topology



- ### Objectives

Part 1: Configure Static IPv4 Addressing

Part 2: Configure and Verify DNS Records

- ### Background

In this activity, you will configure and verify static IP addressing and DHCP addressing. You will then configure a DNS server to map IP addresses to the website names.

Note: Packet Tracer only simulates the process for configuring these services. DHCP and DNS software packages each have their own unique installation and configuration instructions.

Configure Static IPv4 Addressing

Configure the Inkjet printer with static IPv4 addressing.

The home office computers need to know the printer's IPv4 address to send information to it. The printer, therefore, must use a static (unchanging) IPv4 address.

- Click **Inkjet** and click the **Config** tab, which displays the Global Settings.
- Statically assign the Gateway address as **192.168.0.1** and the DNS Server address as **64.100.8.8**.
- Click **FastEthernet0** and statically assign the IP address as **192.168.0.2** and the Subnet Mask address as **255.255.255.0**.
- Close the Inkjet window.

Configure WRS to provide DHCP services.

- Click **WRS** and click the **GUI** tab, and maximize the window.
- The Basic Setup window displays, by default. Configure the following settings in the Network Setup section:
- Change the IP Address to **192.168.0.1**.
- Set the Subnet Mask to **255.255.255.0**.
- Enable the DHCP Server.
- Set the Static DNS 1 address to **64.100.8.8**.
- Scroll to the bottom and click **Save**.
- Close the **WRS** window.

Request DHCP addressing for the home laptop.

This activity focuses on the home office. The clients that you will configure with DHCP are **Home Laptop** and **Tablet**.

- Click **Home Laptop** and click the **Desktop** tab > **IP Configuration**.
- Click **DHCP** and wait until the DHCP request is successful.
- **Home Laptop** should now have a full IP configuration. If not, return to Step 2 and verify your configurations on **WRS**.
- Close the IP Configuration window and then close the **Home Laptop** window.

Request DHCP addressing for the tablet.

- Click **Tablet** and click the **Desktop** tab > **IP Configuration**.
- Click **DHCP** and wait until the DHCP request is successful.
- **Tablet** should now have a full IP configuration. If not, return to Step 2 and verify your configurations on **WRS**.

Test access to websites.

- Close the **IP Configuration** window, and then click Web Browser.
- In the URL box, type **10.10.10.2** (for the **CentralServer** website) or **64.100.200.1** (for the **BranchServer** website) and click **Go**. Both websites should appear.
- Reopen the web browser. Test the names for those same websites by entering **centralserver.pt.pka** and **branchserver.pt.pka**. Click on **Fast Forward Time** on the yellow bar below the topology to speed the process.

• Configure Records on the DNS Server

• Configure famous.dns.pka with records for CentralServer and BranchServer.

Typically, DNS records are registered with companies, but for the purposes of this activity you control the **famous.dns.pka** server on the Internet.

- Click the **Internet** cloud. A new network displays.
- Click **famous.dns.pka** and click the **Services** tab > **DNS**.
- Add the following resource records:

Resource Record Name	Address
centralserver.pt.pka	10.10.10.2
branchserver.pt.pka	64.100.200.1

- Close the famous.dns.pka window.
- Click **Back** to exit the **Internet** cloud.

• Verify the ability of client computers to use DNS.

Now that you have configured DNS records, **Home Laptop** and **Tablet** should be able to access the websites by using the names instead of the IP addresses. First, check that the DNS client is working properly and then verify access to the website.

- Click **Home Laptop** or **Tablet**.
- If the web browser is open, close it and select **Command Prompt**.

  Verify the IPv4 addressing by entering the command **ipconfig /all**. You should see the IP address for the DNS server.
- Ping the DNS server at **64.100.8.8** to verify connectivity.

  Note: The first two or three pings may fail as Packet Tracer simulates all the various processes that must occur for successful connectivity to a remote resource.

  Test the functionality of the DNS server by entering the commands **nslookup centralserver.pt.pka** and **nslookup branchserver.pt.pka**. You should get a name resolution showing the IP address for each.
- Close the Command Prompt window and click **Web Browser**. Verify that **Home Laptop** or **Tablet** can now access the web pages for **CentralServer** and **BranchServer**.

2.9 Packet Tracer - Using Show Commands

• Objectives

Part 1: Analyze Show Command Output

Part 2: Reflection Questions

• Background

This activity is designed to reinforce the use of router **show** commands. You are not required to configure, but rather examine the output of several **show** commands.

Analyze Show Command Output

Connect to ISPRouter

a. Click **ISP PC**, then the **Desktop** tab, followed by **Terminal**.

b. Enter privileged EXEC mode.

c. Use the following **show** commands to answer the Reflection Questions in Part 2:

```
show arp
show flash:
show ip route
show interfaces
show ip interface brief
show protocols
show users
show version
```

Reflection Questions

- Which commands would provide the IP address, network prefix, and interface?

  show ip route, show protocols

- Which commands provide the IP address and interface assignment, but not the network prefix?

  show ip interface brief

- Which commands provide the status of the interfaces?

  show interfaces, show ip interface brief

- Which commands provide information about the IOS loaded on the router?

show version

- Which commands provide information about the addresses of the router interfaces?

show arp, show interfaces

- Which commands provide information about the amount of and Flash memory available?

show flash, show version

- Which commands provide information about the lines being used for configuration or device monitoring?

show users

- Which commands provide traffic statistics of router interfaces?

show interfaces

- Which commands provide information about paths available for network traffic?

show ip route

- Which interfaces are currently active on the router?

GigabitEthernet 0/0, Serial 0/0/1

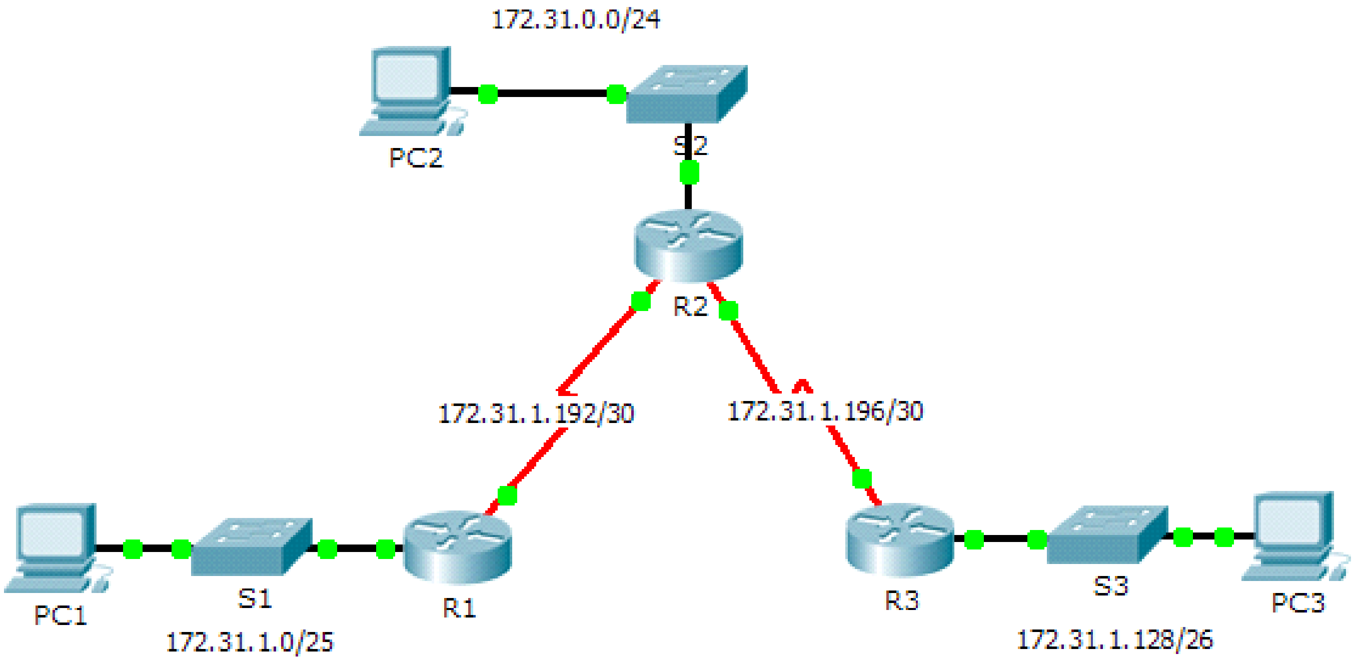
Suggested Scoring Rubric

Each question is worth 10 points for a total score of 100.

3 CCNA 2

3.1 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.

Examine the Network and Evaluate the Need for Static Routing

- Looking at the topology diagram, how many networks are there in total? 5
- How many networks are directly connected to R1, R2, and R3? R1=2, R2=3, R3=2
- How many static routes are required by each router to reach networks that are not directly connected? R1=3 static routes, R2=2 static routes, R3=3 static routes
- Test connectivity to the R2 and R3 LANs by pinging PC2 and PC3 from PC1.

  Why were you unsuccessful? Because the ping won't go through from R1

Configure Static and Default Routes

Configure recursive static routes on R1.

- What is recursive static route?
- A recursive static route is a route where the next-hop IP address is not directly connected to the router. The router must perform a recursive lookup in its routing table to determine how to reach the next-hop address. The router first identifies how to get to the next-hop IP, then forwards the packet using the appropriate outgoing interface.
- Why does a recursive static route require two routing table lookups?
- First Lookup: The router looks up the destination network to find the next-hop IP address.
- Second Lookup: The router performs a second lookup to find how to reach that next-hop IP address and the outgoing interface associated with it.
- Configure a recursive static route to every network not directly connected to R1, including the WAN link between R2 and R3.
- R1(config)# ip route 172.31.1.128 255.255.255.192 172.31.1.193, R1(config)# ip route 172.31.0.0 255.255.255.0 172.31.1.193, R1(config)# ip route 172.31.1.196 255.255.255.252 172.31.1.193
- Test connectivity to the R2 LAN and ping the IP addresses of PC2 and PC3.

  Why were you unsuccessful?

  R2 and R3 may not have static routes configured back to the networks connected to R1 (such as 172.31.1.0/25). If R2 and R3 do not know how to return traffic to R1, pings will fail.

Configure directly attached static routes on R2.

- How does a directly attached static route differ from a recursive static route?
- A directly attached static route specifies the outgoing interface directly, rather than the next-hop IP address. This eliminates the need for a second routing table lookup, as the router already knows which interface to forward the packet out of.
- A recursive static route specifies a next-hop IP address rather than an outgoing interface. The router must perform a second lookup to resolve how to reach the next-hop IP, determining which interface to use.
- Configure a directly attached static route from R2 to every network not directly connected.
- ip route 172.31.1.0 255.255.255.128 Serial0/0/0
- ip route 172.31.1.128 255.255.255.192 Serial0/0/1

- Which command only displays directly connected networks? R2# show ip route connected
- Which command only displays the static routes listed in the routing table? R2# show ip route static
- When viewing the entire routing table, how can you distinguish between a directly attached static route and a directly connected network?
- The C indicates the network is directly connected, while the S indicates a static route. You can easily distinguish between them based on these codes.

- **Configure a default route on R3.**

- How does a default route differ from a regular static route?
- A default route is a special type of static route that is used to direct traffic for any destination that is not explicitly listed in the routing table. It acts as a "catch-all" for unknown networks. The default route is defined with the destination network set to 0.0.0.0/0.
- A regular static route specifies a specific destination network along with its subnet mask. This route is only used for traffic that matches the specified network and will not be used for any other destinations that are not explicitly configured.
- In summary, while a regular static route provides a specific path for defined networks, a default route provides a path for all unspecified networks.
- Configure a default route on R3 so that every network not directly connected is reachable.
- R3(config)# ip route 0.0.0.0 0.0.0.0 172.31.1.193
- How is a static route displayed in the routing table? show ip route static

- **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.

- Explain a fully specified route.
- A fully specified route is a type of static route that explicitly defines both:
- The destination network (including its subnet mask).
- The next-hop IP address or the outgoing interface through which the destination can be reached.Which command provides a fully specified static route from R3 to the R2 LAN?

- Write a fully specified route from R3 to the network between R2 and R1. Do not configure the route; just calculate it.
- To create a fully specified static route from R3 to the R2 LAN (assuming R2's LAN is 172.31.0.0/24), the command would be:
- R3(config)# ip route 172.31.0.0 255.255.255.0 172.31.1.193
- 172.31.0.0 255.255.255.0: Destination network and subnet mask for R2's LAN.
- 172.31.1.193: Next-hop IP address (R2's interface IP connected to R3).
- Write a fully specified static route from R3 to the R1 LAN. Do not configure the route; just calculate it.

  Assuming the network between R2 and R1 is 172.31.1.192/30 (with R2 having 172.31.1.193 and R1 having 172.31.1.194), the fully specified route would be:

  bash

  ```
  ip route 172.31.1.192 255.255.255.252 172.31.1.193
  ```

  This specifies that traffic to 172.31.1.192/30 should be sent to the next-hop 172.31.1.193.

- **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?

show ip route, show ip route static

- ## Verify Connectivity

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

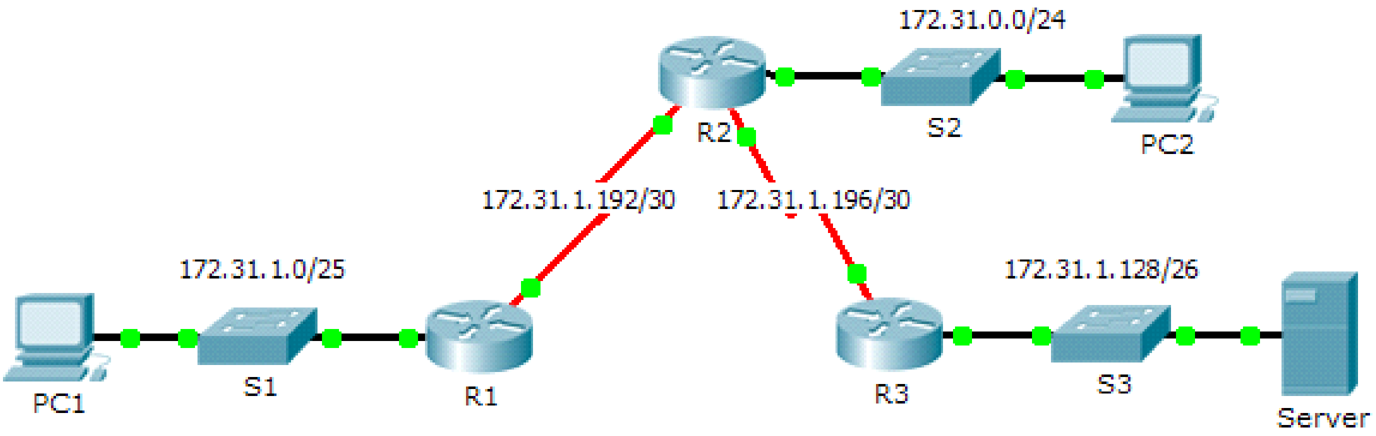
- ### Suggested Scoring Rubric

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**	

-
-

3.2 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.

• 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?

show ip route, show run, traceroute, tracert, ping

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
Static routes next-hop addresses are incorrect on R2	Remove static routes and add correct next-hop adresses
There is no route in R3 for R1 lan	Add a static route to R1 LAN

Implement the Solution

- If there are any misconfigured static routes, you must remove them before the correct ones can be added to the configuration.
- Add any missing static routes by configuring directly attached routes.

```
R2(config)#no ip route 172.31.1.0 255.255.255.128 172.31.1.198
R2(config)#no ip route 172.31.1.128 255.255.255.192 172.31.1.194
R2(config)#ip route 172.31.1.0 255.255.255.128 172.31.1.194
R2(config)#ip route 172.31.1.128 255.255.255.192 172.31.1.198
```

remember exit and wr commands

```
R3(config)#ip route 172.31.1.0 255.255.255.128 s0/0/1
%Default route without gateway, if not a point-to-point interface, may impact performance
R3(config)#exit
```

Verify That the Issue Is Resolved

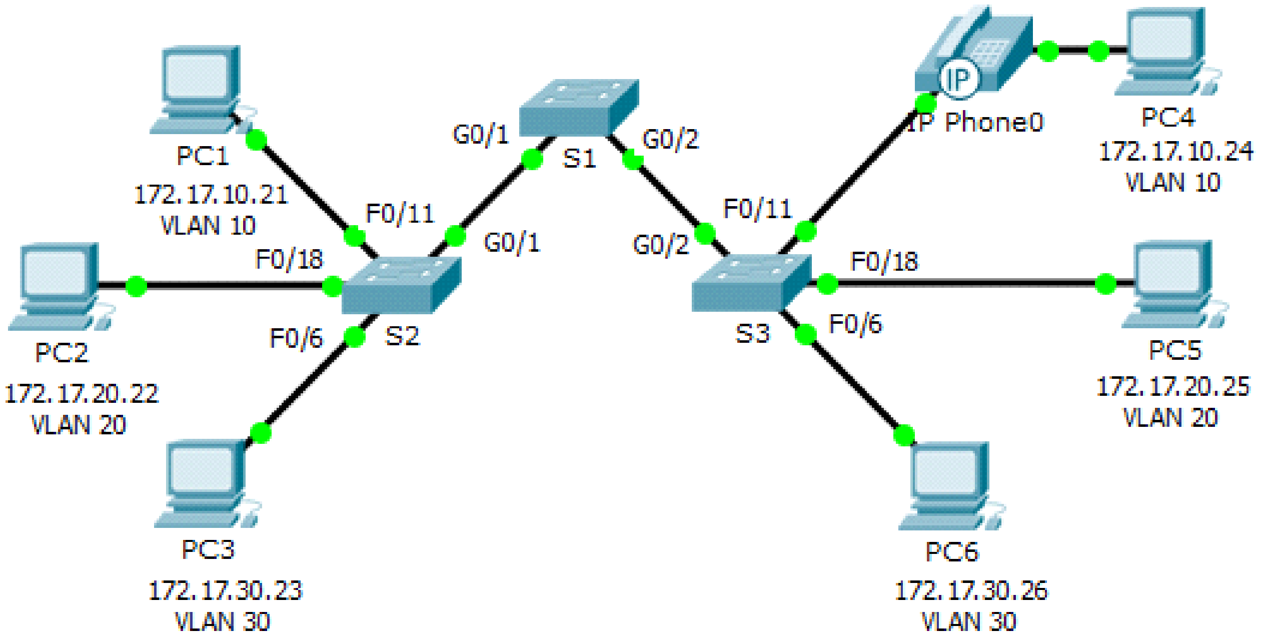
- Ping from PC1 to the server.
- Open a web connection to the server. After you correctly identify and implement the correct solution to the problem, you will receive a message in the web browser when you connect to the server.

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**	

3.3 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.

View the Default VLAN Configuration

Display the current VLANs.

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

```
show vlan brief
```

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?

Improved Security, Broadcast Domain Control, Efficient Network Management, Traffic Segmentation, Scalability

Configure VLANs

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
- VLAN 150: VOICE

```
S1(config)#vlan 10
S1(config-vlan)#name Faculty/Staff
S1(config-vlan)#vlan 20
S1(config-vlan)#name Students
S1(config-vlan)#vlan 30
S1(config-vlan)#name Guest/Default
S1(config-vlan)#vlan 99
S1(config-vlan)#name Management&Native
S1(config-vlan)#vlan 150
S1(config-vlan)#name VOICE
```

Verify the VLAN configuration.

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

```
S1#show vlan brief
```

Create the VLANs on S2 and S3.

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

- **Verify the VLAN configuration.**

Assign VLANs to Ports

- **Assign VLANs to the active ports on S2.**

Configure the interfaces as access ports and assign the VLANs as follows:

- VLAN 10: FastEthernet 0/11
- VLAN 20: FastEthernet 0/18
- VLAN 30: FastEthernet 0/6

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

- **Assign VLANs to the active ports on S3.**

S3 uses the same VLAN access port assignments as S2. Configure the interfaces as access ports and assign the VLANs as follows:

- VLAN 10: FastEthernet 0/11
- VLAN 20: FastEthernet 0/18
- VLAN 30: FastEthernet 0/6

```
S3(config)#interface f0/11
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 10
S3(config-if)#interface f0/18
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 20
S3(config-if)#interface f0/6
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 30
```

- **Assign the VOICE VLAN to FastEthernet 0/11 on S3.**

As shown in the topology, the S3 FastEthernet 0/11 interface connects to a Cisco IP Phone and PC4. The IP phone contains an integrated three-port 10/100 switch. One port on the phone is labeled Switch and connects to F0/4. Another port on the phone is labeled PC and connects to PC4. The IP phone also has an internal port that connects to the IP phone functions.

The S3 F0/11 interface must be configured to support user traffic to PC4 using VLAN 10 and voice traffic to the IP phone using VLAN 150. The interface must also enable QoS and trust the Class of Service (CoS) values assigned by the IP phone.

```
S3(config)#interface f0/11
S3(config-if)#mls qos trust cos
```

```
S3(config-if)#switchport voice vlan 150
```

- **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?

No, ping failed because the ports on switches are in VLAN 1 and PC1 AND PC4 are in VLAN 10

What could be done to resolve this issue?

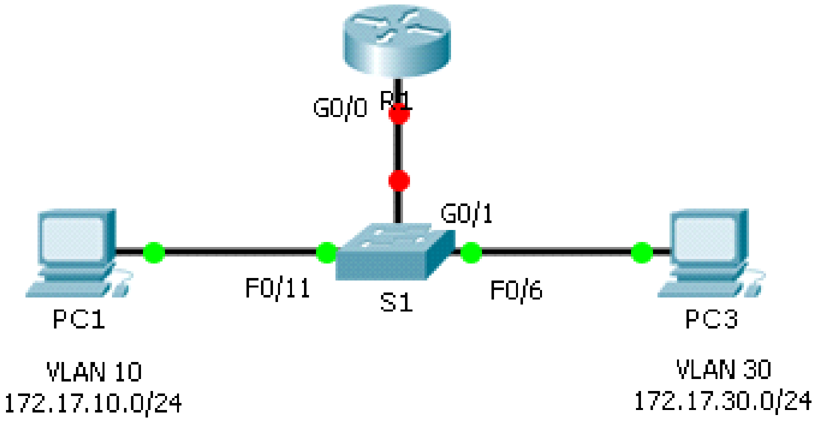
Configuring trunk ports between switches

- **Suggested Scoring Rubric**

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Verify the Default VLAN Configuration	Step 2	**2**	
Part 2: Configure VLANs	Step 2	**2**	
Part 3: Assign VLANs to Ports	Step 3	**2**	
Packet Tracer Score		**94**	
Total Score		**100**	

3.4 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.

- # Test Connectivity Without Inter-VLAN Routing

- ### 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.

- ### Switch to Simulation mode to monitor pings.

- Switch to Simulation mode by clicking the **Simulation** tab or pressing **Shift+S**.
- 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?
- PC1 and PC3 are not in the same network so S1 does not forward PC1 ARP request to VLAN30

- # Add VLANs to a Switch

- ### Create VLANs on S1.

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

```
S1(config)#vlan 10
S1(config-vlan)#vlan 30
```

- ### Assign VLANs to ports.

- Configure interface F0/6 and F0/11 as access ports and assign VLANs.
  - Assign **PC1** to VLAN 10.
  - Assign **PC3** to VLAN 30.

```
S1(config-vlan)#int fa0/11
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#int fa0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
```

- 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
```

Test connectivity between PC1 and PC3.

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

Each VLAN is diffferent network. Router would be needed to next-hop to a different VLAN

Configure Subinterfaces

Configure subinterfaces on R1 using the 802.1Q encapsulation.

- 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.
- Repeat for the G0/0.30 subinterface.

```
R1(config)#int g0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-subif)#int g0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
```

Verify Configuration.

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

Test Connectivity with Inter-VLAN Routing

Ping between PC1 and PC3.

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

Enable trunking.

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

- Default
- 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.
- S1(config)#int g0/1
- S1(config-if)#switchport mode trunk
- How can you determine that the interface is a trunk port using the **show vlan** command?
- I cannot, so instead I used switchport command
- S1#show interfaces g0/1 switchport
- Issue the **show interface trunk** command to verify the interface is configured as a trunk.

- **Switch to Simulation mode to monitor pings.**

- Switch to **Simulation** mode by clicking the **Simulation** tab or pressing **Shift+S**.
- Click **Capture/Forward** to see the steps the ping takes between **PC1** and **PC3**.
- 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.

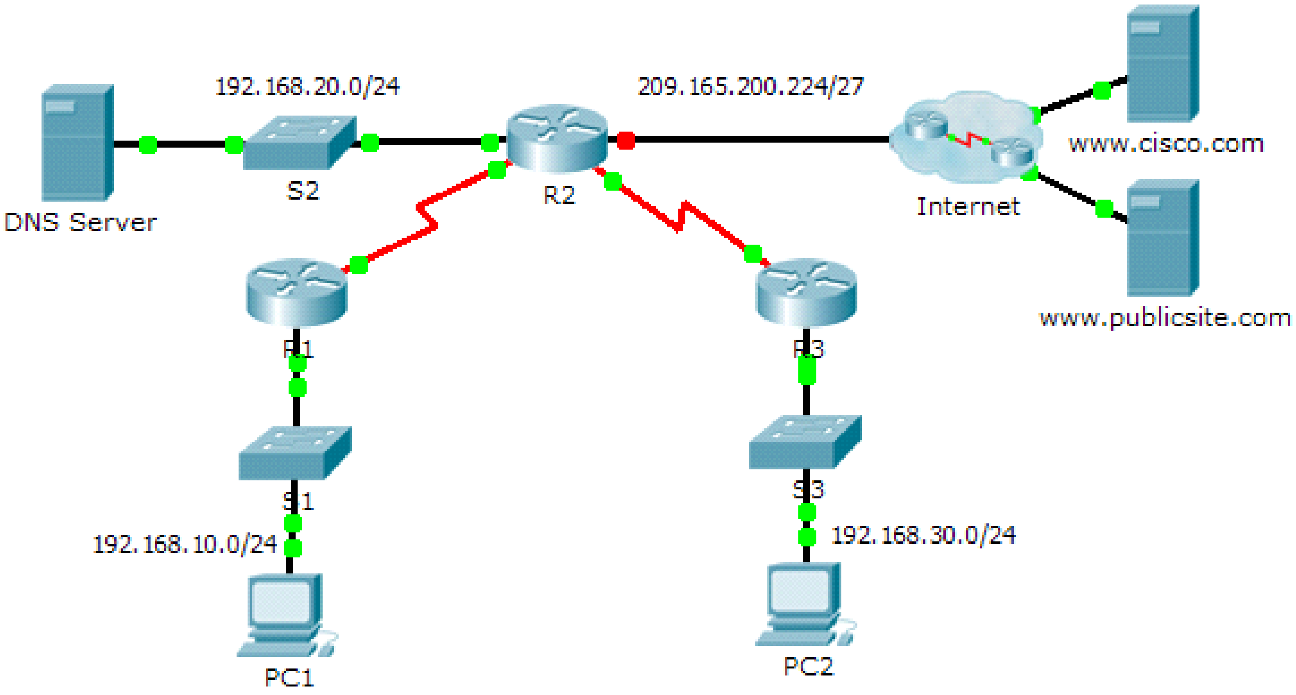
  took me way too long to realize that I did not write no shutdown when configuring R1 interfaces so the ARP and ping did not go through

- **Suggested Scoring Rubric**

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

3.5 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. 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.

Configure a Router as a DHCP Server

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.

```
R2(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R2(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.10
```

Create a DHCP pool on R2 for the R1 LAN.

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

```
R2(config)#ip dhcp pool R1-LAN
```

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

```
R2(dhcp-config)#network 192.168.10.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.10.1
R2(dhcp-config)#dns-server 192.168.20.254
```

Create a DHCP pool on R2 for the R3 LAN.

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

```
R2(config)#ip dh pool R3-LAN
```

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

```
R2(dhcp-config)#network 192.168.30.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.30.1
R2(dhcp-config)#dns-server 192.168.20.254
```

Configure DHCP Relay

Configure R1 and R3 as a DHCP relay agent.

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

R1(config-if)#ip helper-address 10.1.1.2

R1(config-if)#no shutdown

R1(config-if)#exit

R3(config)#interface g0/0

R3(config-if)#ip helper-address 10.2.2.2

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

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

Configure R2 as a DHCP Client

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

```
R2(config)#interface g0/1
R2(config-if)#ip address dhcp
R2(config-if)#no shutdown
```

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

```
GigabitEthernet0/1     209.165.200.231 YES DHCP   up                up
```

Verify DHCP and Connectivity

Verify DHCP bindings.

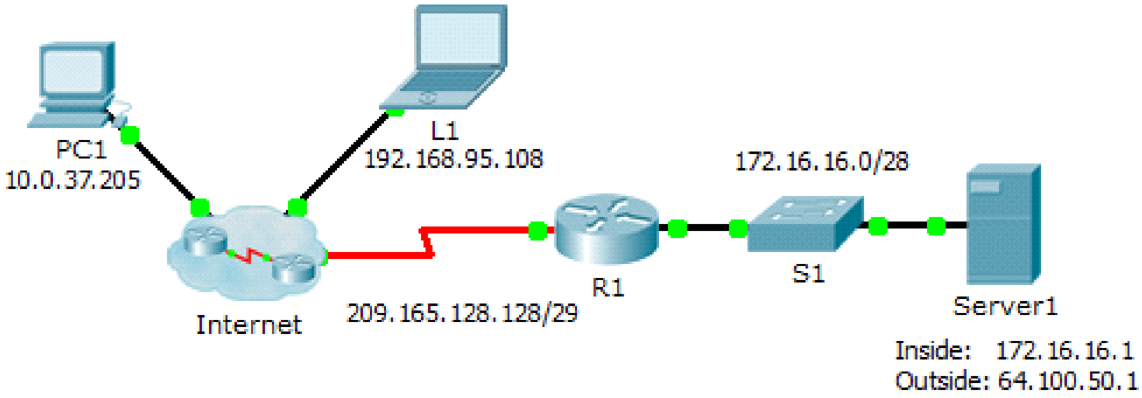
```
R2# show ip dhcp binding
IP address        Client-ID/              Lease expiration        Type
                  Hardware address
192.168.10.11     0002.4AA5.1470           --                     Automatic
192.168.30.11     0004.9A97.2535           --                     Automatic
```

Verify configurations.

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

3.6 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.

- ## Test Access without NAT

- ### Attempt to connect to Server1 using Simulation Mode.

  - 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.
  - From **PC1**, ping the **R1** S0/0/0 interface. The ping should succeed.

- ### View R1 routing table and running-config.

  - View the running configuration of **R1**. Note that there are no commands referring to NAT.
  - Verify that the routing table does not contain entries referring to the IP addresses used by **PC1** and **L1**.
  - Verify that NAT is not being used by **R1**.

```
R1# show ip nat translations
```

- ## Configure Static NAT

- ### Configure static NAT statements.

Refer to the Topology. Create a static NAT translation to map the **Server1** inside address to its outside address.

```
R1(config)#ip nat inside source static 172.16.16.1 64.100.50.1
```

- **Configure interfaces.**

Configure the correct inside and outside interfaces.

```
R1(config)#interface g0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface s0/0/0
R1(config-if)#ip nat outside
```

- ### Test Access with NAT

- **Verify connectivity to the Server1 web page.**
  - Open the command prompt on **PC1** or **L1**, attempt to ping the public address for **Server1**. Pings should succeed.
  - Verify that both **PC1** and **L1** can now access the **Server1** web page.

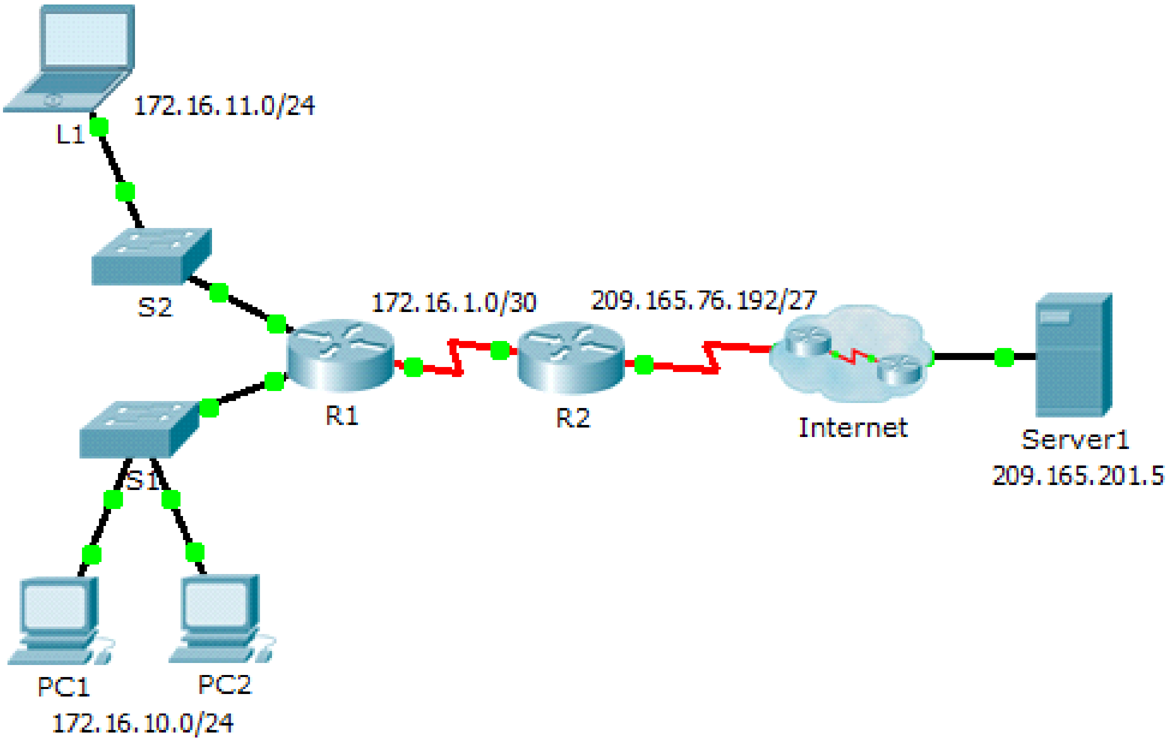
- **View NAT translations.**

Use the following commands to verify the static NAT configuration:

```
show running-config
show ip nat translations
show ip nat statistics
```

3.7 Packet Tracer – Configuring Dynamic NAT

- ### Topology



- ### Objectives

Part 1: Configure Dynamic NAT

Part 2: Verify NAT Implementation

- ## Configure Dynamic NAT

- **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.

```
R2(config)#access-list 1 permit 172.16.0.0 0.0.255.255
```

- **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.

```
R2(config)#ip nat pool pool_name 209.165.76.196 209.165.76.199 netmask 255.255.255.252
```

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?

- the extra devices would be denied until the current translation is timed out. freeing the address for next device

- **Associate ACL1 with the NAT pool.**

```
R2(config)#ip nat inside source list 1 pool pool_name
```

- **Configure the NAT interfaces.**

Configure **R2** interfaces with the appropriate inside and outside NAT commands.

```
R2(config)#interface s0/0/0
R2(config-if)#ip nat outside
R2(config-if)#interface s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#no shutdown
```

- ## Verify NAT Implementation

- **Access services across the Internet.**

From the web browser of **L1**, **PC1**, or **PC2**, access the web page for **Server1**.

- **View NAT translations.**

View the NAT translations on **R2**.

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

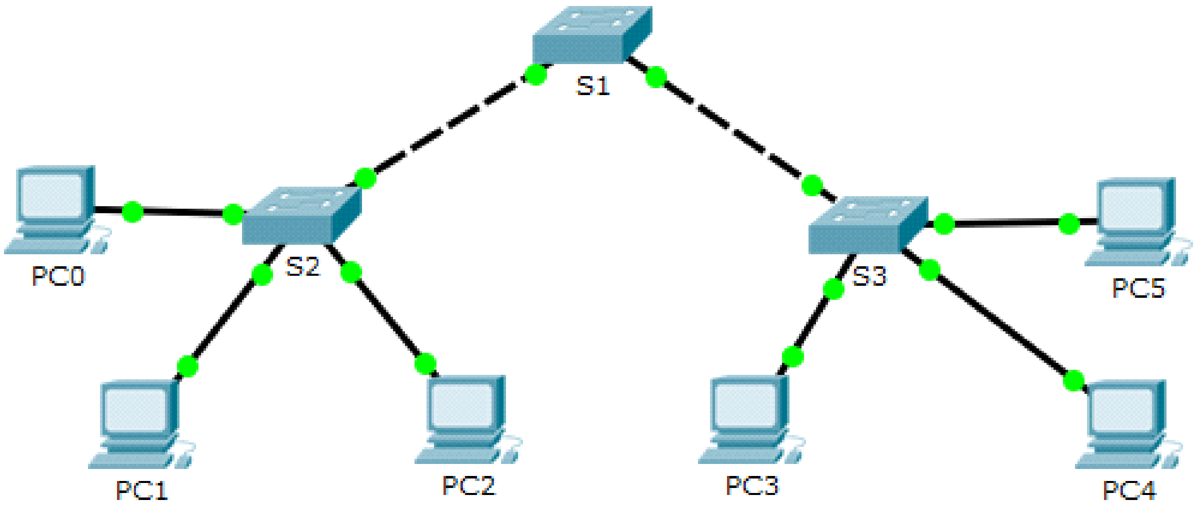
```
R2#show ip nat translations
Pro  Inside global      Inside local        Outside local       Outside
global
icmp 209.165.76.197:5   172.16.10.1:5       209.165.201.5:5
209.165.201.5:5
icmp 209.165.76.197:6   172.16.10.1:6       209.165.201.5:6
209.165.201.5:6
icmp 209.165.76.197:7   172.16.10.1:7       209.165.201.5:7
209.165.201.5:7
```

```
icmp 209.165.76.197:8  172.16.10.1:8      209.165.201.5:8
209.165.201.5:8
tcp 209.165.76.197:1029172.16.10.1:1029   209.165.201.5:80
209.165.201.5:80
```

4 CCNA 3

4.1 Packet Tracer – Configure VLANs, VTP and DTP

- **Topology**



- **Addressing Table**

Device	Interface	IP Address	Subnet Mask
PC0	NIC	192.168.10.1	255.255.255.0
PC1	NIC	192.168.20.1	255.255.255.0
PC2	NIC	192.168.30.1	255.255.255.0
PC3	NIC	192.168.30.2	255.255.255.0
PC4	NIC	192.168.20.2	255.255.255.0
PC5	NIC	192.168.10.2	255.255.255.0
S1	VLAN 99	192.168.99.1	255.255.255.0
S2	VLAN 99	192.168.99.2	255.255.255.0
S3	VLAN 99	192.168.99.3	255.255.255.0

- **Objectives**

Part 1: Configure and Verify DTP

Part 2: Configure and Verify VTP

• Background / Scenario

As the number of switches in a network increases, the administration necessary to manage the VLANs and trunks can be challenging. To ease some of the VLAN and trunking configurations, VLAN trunking protocol (VTP) allows a network administration to automate the management of VLANs. Trunk negotiation between network devices is managed by the Dynamic Trunking Protocol (DTP), and is automatically enabled on Catalyst 2960 and Catalyst 3560 switches.

In this activity, you will configure trunk links between the switches. You will configure a VTP server and VTP clients in the same VTP domain. You will also observe the VTP behavior when a switch is in VTP transparent mode. You will assign ports to VLANs and verify end-to-end connectivity with the same VLAN.

1. Configure and Verify DTP

In Part 1, you will configure trunk links among the switches, and you will configure VLAN 999 as the native VLAN.

1. Verify VLAN configuration.

Verify the configured VLANs on the switches.

a. On S1, click the **CLI** tab. At the prompt, enter **enable** and enter the **show vlan brief** command to verify the configured VLANs on S1.

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
99   Management                       active
999  VLAN0999                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

a. Repeat step a. on S2 and S3. What VLANs are configured on the switches?

Vlan 99 and VLAN 999 on all switches

1. Configure Trunks on S1, S2, and S3.

Dynamic trunking protocol (DTP) manages the trunk links between Cisco switches. Currently all the switchports are in the default trunking mode, which is dynamic auto. In this step, you will change the trunking mode to dynamic desirable for the link between switches S1 and S2. For the link between switches S1 and S3, the link will be set as a static trunk. Use VLAN 999 as the native VLAN in this topology.

a. On switch S1 and switch S2, configure the trunk link to dynamic desirable on the GigabitEthernet 0/1 interface. The configuration of S1 is shown below.

```
S1(config)# interface g0/1
S1(config-if)# switchport mode dynamic desirable
```

a. For the trunk link between S1 and S3, configure a static trunk link on the GigabitEthernet 0/2 interface.

```
S1(config)# interface g0/2
S1(config-if)# switchport mode trunk
S3(config)# interface g0/2
S3(config-if)# switchport mode trunk
```

a. Verify trunking is enabled on all the switches using the **show interfaces trunk** command.

```
S1# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      desirable    n-802.1q       trunking      1
Gig0/2      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,99,999
Gig0/2      1,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      none
Gig0/2      none
```

What is the native VLAN for these trunks currently? VLAN 1

a. Configure VLAN 999 as the native VLAN for the trunk links on S1.

```
S1(config)# interface range g0/1 - 2
S1(config-if-range)# switchport trunk native vlan 999
```

What messages did you receive on S1? How would you correct it?

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (999), with S3 GigabitEthernet0/2 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (999), with S2 GigabitEthernet0/1 (1).

Correcting the issue requires VLAN 999 to be native VLAN on S2 and S3

a. On S2 and S3, configure VLAN 999 as the native VLAN.

b. Verify trunking is successfully configured on all the switches. You should be able ping one switch from another switch in the topology using the IP addresses configured on the SVI.

1. Configure and Verify VTP

S1 will be configured as the VTP server and S2 will be configured as a VTP client. All the switches will be configured to be in the VTP domain **CCNA** and use the VTP password **cisco**.

VLANs can be created on the VTP server and distributed to other switches in the VTP domain. In this part, you will create 3 new VLANs on the VTP server, S1. These VLANs will be distributed to S2 using VTP. Observe how the transparent VTP mode behaves.

1. Configure S1 as VTP server.

Configure S1 as the VTP server in the **CCNA** domain with the password **cisco**.

a. Configure S1 as a VTP server.

```
S1(config)# vtp mode server
Setting device to VTP SERVER mode.
```

a. Configure **CCNA** as the VTP domain name.

```
S1(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
```

a. Configure **cisco** as the VTP password.

```
S1(config)# vtp password cisco
Setting device VLAN database password to cisco
```

1. Verify VTP on S1.

a. Use the **show vtp status** command on the switches to confirm that the VTP mode and domain are configured correctly.

```
S1# show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 7
VTP Operating Mode              : Server
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63 0x17
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 192.168.99.1 on interface Vl99 (lowest numbered VLAN interface
found)
```

a. To verify the VTP password, use the **show vtp password** command.

```
S1# show vtp password
VTP Password: cisco
```

1. Add S2 and S3 to the VTP domain.

Before S2 and S3 will accept VTP advertisements from S1, they must belong to the same VTP domain. Configure S2 as a VTP client with **CCNA** as the VTP domain name and **cisco** as the VTP password. Remember that VTP domain names are case sensitive.

a. Configure S2 as a VTP client in the **CCNA** VTP domain with the VTP password **cisco**.

```
S2(config)# vtp mode client
Setting device to VTP CLIENT mode.
S2(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S2(config)# vtp password cisco
Setting device VLAN database password to cisco
```

a. To verify the VTP password, use the **show vtp password** command.

```
S2# show vtp password
VTP Password: cisco
```

a. Configure S3 to be in the **CCNA** VTP domain with the VTP password **cisco**. Switch S3 will be set in VTP transparent mode.

```
S3(config)# vtp mode Transparent
S3(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S3(config)# vtp password cisco
Setting device VLAN database password to cisco
```

a. Enter **show vtp status** command on all the switches to answer the following question.

Notice that the configuration revision number is 0 on all three switches. Explain.

configuration number increases by one every time VLAN is added, deleted or modified. indicates that no additional VLAN changes have been made

1. Create more VLANs on S1.

a. On S1, create VLAN 10 and name it Red.

```
S1(config)# vlan 10
S1(config-vlan)# name Red
```

a. Create VLANs 20 and 30 according to the table below.

VLAN Number	VLAN Name
10	Red
20	Blue
30	Yellow

a. Verify the addition of the new VLANs. Enter **show vlan brief** at the privileged EXEC mode.

Which VLANs are configured on S1?

VLAN 1, 10, 20, 30, 99, 999

a. Confirm configuration changes using the **show vtp status** command on S1 and S2 to confirm that the VTP mode and domain are configured correctly. Output for S2 is shown here:

```
S2# show vtp status
VTP Version                     : 2
Configuration Revision          : 6
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xE6 0x56 0x05 0xE0 0x7A 0x63 0xFB 0x33
Configuration last modified by 192.168.99.1 at 3-1-93 00:21:07
```

How many VLANs are configured on S2? Does S2 have the same VLANs as S1? Explain.

S1 and S2 has 10 VLANS but S2 has VTP client mode, so it does not create VLAN itself and learns VLAN information from VTP server which is S1.

1. Observe VTP transparent mode.

S3 is currently configured as VTP transparent mode.

a. Use **show vtp status** command to answer the following question.

How many VLANs are configured on S3 currently? What is the configuration revision number? Explain your answer.

S3 has 7 VLANs, and the configuration number is 0 because it is in transparent mode, meaning VLAN configurations are not synchronized through VTP and haven’t been modified since startup.

How would you change the number of VLANs on S3?

In transparent mode, S3 does not apply VLAN updates from the VTP server. VLANs must either be configured manually or S3 must be changed to client mode to receive VLAN information from the VTP server.

a. Change VTP mode to client on S3.

Use show commands to verify the changes on VTP mode. How many VLANs exists on S3 now?

10

Note: VTP advertisements are flooded throughout the management domain every five minutes, or whenever a change occurs in VLAN configurations. To accelerate this process, you can switch between Realtime mode and Simulation mode until the next round of updates. However, you may have to do this multiple times because this will only forward Packet Tracer's clock by 10 seconds each time. Alternatively, you can change one of the client switches to transparent mode and then back to client mode.

1. Assign VLANs to Ports

Use the **switchport mode access** command to set access mode for the access links. Use the **switchport access vlan** *vlan-id* command to assign a VLAN to an access port.

Ports	Assignments	Network
S2 F0/1 – 8 S3 F0/1 – 8	VLAN 10 (Red)	192.168.10.0 /24
S2 F0/9 – 16 S3 F0/9 – 16	VLAN 20 (Blue)	192.168.20.0 /24
S2 F0/17 – 24 S3 F0/17 – 24	VLAN 30 (Yellow)	192.168.30.0 /24

a. Assign VLANs to ports on S2 using assignments from the table above.

```
S2(config-if)# interface range f0/1 - 8
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 10
S2(config-if-range)# interface range f0/9 -16
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 20
S2(config-if-range)# interface range f0/17 - 24
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 30
```

a. Assign VLANs to ports on S3 using assignment from the table above.

1. Verify end to end connectivity.

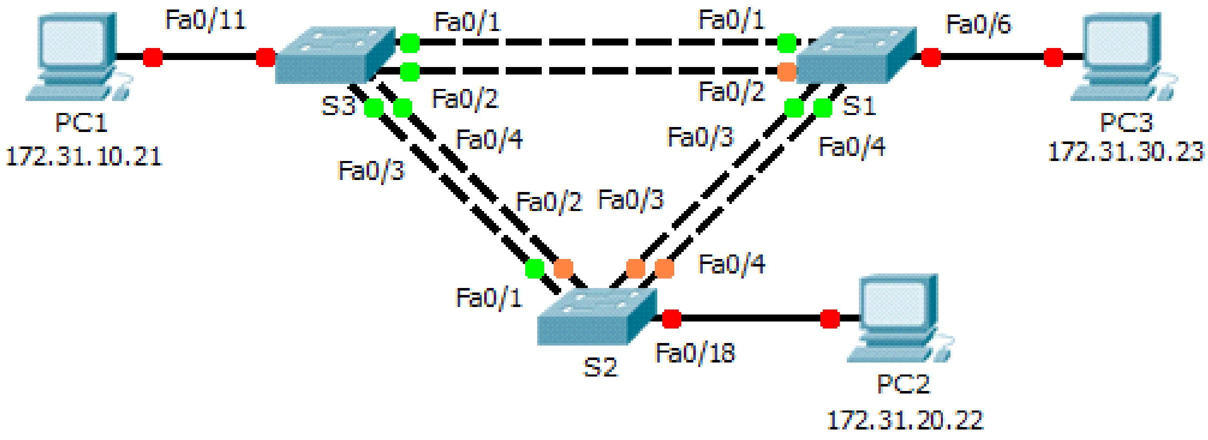
a. From PC0 ping PC5.

b. From PC1 ping PC4.

c. From PC2 ping PC3.

4.2 Packet Tracer – Configuring PVST+

- ### Topology



- ### Addressing Table

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

- ### Switch Port Assignment Specifications

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

- ### Objectives

Part 1: Configure VLANs

Part 2: Configure Spanning Tree PVST+ and Load Balancing

Part 3: Configure PortFast and BPDU Guard

- ### Background

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

Configure VLANs

Enable the user ports on S1, S2, and S3 in access mode.

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

```
S1(config)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#no shutdown
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S3(config)#interface f0/11
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
```

Create VLANs.

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

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

Assign VLANs to switch ports.

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

```
S1(config-vlan)#interface f0/6
S1(config-if)#switchport access vlan 30
S2(config-vlan)#interface f0/18
S2(config-if)#switchport access vlan 20
S3(config-vlan)#interface f0/11
S3(config-if)#switchport access vlan 10
```

Verify the VLANs.

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

```
S3#show vlan brief
```

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
10   VLAN0010                         active    Fa0/11
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active
50   VLAN0050                         active
60   VLAN0060                         active
70   VLAN0070                         active
80   VLAN0080                         active
99   VLAN0099                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
```

- **Assign the trunks to native VLAN 99.**

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

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



S1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down

%LINEPROTO-5-UPDOWN: Line protoco
```

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

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

```
S3(config-if-range)#interface vlan99
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S3(config-if)#ip address 172.31.99.3 255.255.255.0
S2(config-if)#ip address 172.31.99.2 255.255.255.0
S1(config-if)#ip address 172.31.99.1 255.255.255.0
```

Configure Spanning Tree PVST+ and Load Balancing

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

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

Configure STP mode.

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

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

use the command on all switches

Configure Spanning Tree PVST+ load balancing.

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

```
S1(config)#spanning-tree vlan 1,10,30,50,70 root primary
S2(config)#spanning-tree vlan 1,10,20,30,40,50,60,70,80,99 root secondary
S3(config)#spanning-tree vlan 20,40,60,80,99 root primary
```

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

Configure PortFast and BPDU Guard

Configure PortFast on the switches.

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

```
S1(config)#interface f0/6

S1(config-if)#spanning-tree portfast

S2(config)#interface f0/18

S2(config-if)#spanning-tree portfast

S3(config)#interface f0/11

S3(config-if)#spanning-tree portfast
```

Configure BPDU guard on the switches.

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

```
S1(config)#interface f0/6

S1(config-if)#spanning-tree bpduguard enable

S2(config)#interface f0/18

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

S3(config)#interface f0/11

S3(config-if)#spanning-tree bpduguard enable
```

Verify your configuration.

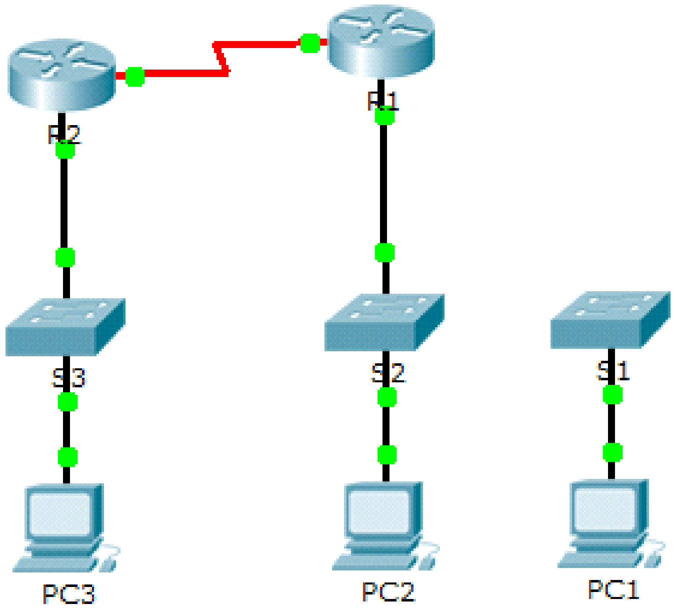
Use the **show running-configuration** command to verify your configuration.

```
spanning-tree mode pvst

spanning-tree extend system-id

spanning-tree vlan 1,10,30,50,70 priority 24576

!

vlan 10

!

vlan 20

!

vlan 30

!

vlan 40

!

vlan 50

!
```

```
vlan 60
!
vlan 70
!
vlan 80
!
vlan 99
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
!
interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
```

4.3 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.

- ## View the Routing Table of a Converged Network

- ### Use show commands and interpret the output.

- Show the directly connected networks of **R1**. How many routes are connected to **R1**? 2

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

- Show the running configuration of **R1**. What routing protocol is in use? Routing Information Protocol (RIP)
- Are the IP addresses in the configuration advertised by RIP the same as those that are connected? yes
- Are these IP addresses assignable, network, or broadcast? network
- Show the networks of **R1** learned through RIP. How many routes are there? 1

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

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

  C is connected and R is RIP and L is local

```
R1# show ip route
```

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

Verify the state of the topology.

- Ping **PC3** from **PC2**. The ping should be successful.
- Show the interface status on **R2**. Two interfaces should have assigned addresses. Each address corresponds to a connected network.

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

- Show the interface status on **R1**. How many interfaces have assigned addresses? 3

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

Add a New LAN to the Topology

Add an Ethernet cable.

- Connect the correct Ethernet cable from **S1** to the appropriate port on **R1**.
- Ping from **PC1** to **PC2** after the affected **S1** port turns green. Was the ping successful? Yes
- Ping from **PC1** to **PC3**. Was the ping successful? Why?

  R1 is not advertising 64.0.0.0 address to R2

Configure a route.

- Switch from Realtime mode to Simulation mode.
- 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
```

- Examine the PDUs leaving **R1**. What type are they? RIPv1

Watch the Network Converge

Use debug commands.

- Enable debugging on **R2**.

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

- For reference, show the routing table of **R2** as in step 1f.
- Click **Capture / Forward** from simulation mode. What notification appeared in the terminal of **R2**?

  RT: add 64.0.0.0/8 via 192.168.1.2, rip metric [120/1]

- According to the debugging output, how many hops away from R2 is 64.0.0.0? 1
- What interface does **R2** send packets destined for the 64.0.0.0 network? S0/0/0
- Show the routing table of **R2**. Record the new entry.

  R   64.0.0.0/8 [120/1] via 192.168.1.2, 00:00:10, Serial0/0/0

- **Verify the state of the topology.**

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

yes. because R1 advertised the packages

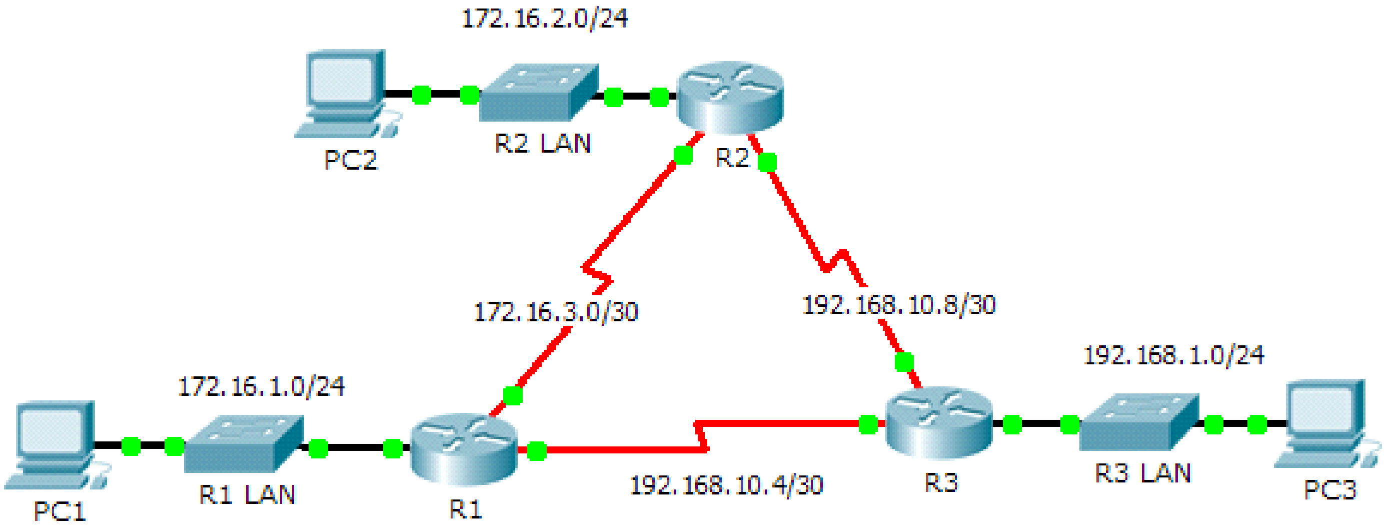
- **Suggested Scoring Rubric**

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**	

-

4.4 Packet Tracer – Configuring Basic EIGRP with IPv4

- ### Topology



- ### Addressing Table

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

- ### Objectives

Part 1: Configure EIGRP

Part 2: Verify EIGRP Routing

- ### Background

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

Configure EIGRP

Enable the EIGRP routing process.

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

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

What is the range of numbers that can be used for AS numbers? 1-65535

Advertise directly connected networks.

- Use the **show ip route** command to display the directly connected networks on each router.
- How can you tell the difference between subnet addresses and interface addresses?
- Subnets are identified with a "C" and link addresses are identified with an "L".
- On each router, configure EIGRP to advertise the specific directly connected subnets. The configuration for **R1** is shown.

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

Configure passive interfaces.

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

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

Disable automatic summarization.

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

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

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

Save the configurations.

Verify EIGRP Routing

Examine neighbor adjacencies.

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

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

Display the EIGRP routing protocol parameters.

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

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

Where is this information located under? Routing Information Sources

What is the maximum hop count? 100

- **Verify end-to-end connectivity**

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

- **Suggested Scoring Rubric**

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

-

5 Pohdinta

Opintojakso syvensi merkittävästi ymmärrystäni liityntäverkoista, erityisesti laboratorioharjoitusten kautta. Cisco Packet Tracerin avulla tehdyt tehtävät auttoivat yhdistämään teorian käytäntöön ja paransivat taitoja liityntäverkkoratkaisujen suunnittelussa, konfiguroinnissa ja ongelmanratkaisussa. Harjoitusten myötä ymmärrys verkkojen toiminnasta sekä työkalun käyttötaidot kehittyivät huomattavasti. Opintojakso loi vahvan perustan jatkokehitykselle ja valmiuksia toimia itsenäisesti alan tehtävissä. (Cisco Learning Network, N.d.).

Lähteet

Cisco Learning Network. N.d. Tietoverkot. Oppimateriaali. Viitattu 6.12.2024. https://learning-network.cisco.com/

Liitteet

Liite 1. Liitteen otsikko

Liite 2. Liitteen otsikko