Cisco | Networking Academy®
Mind Wide Open™

CCNA Routing and Switching: Introduction to Networks

Instructor Packet Tracer Manual

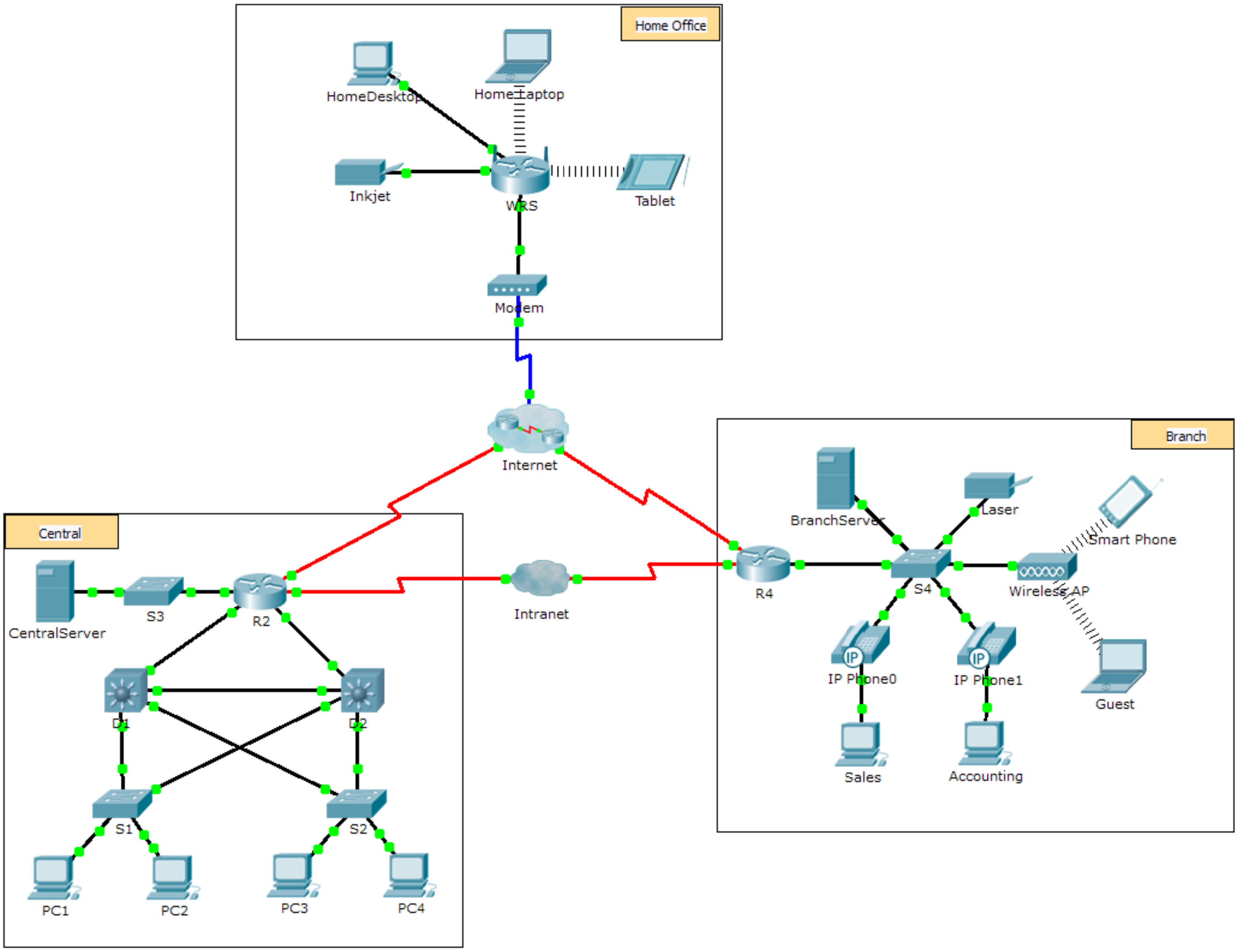
Packet Tracer - Network Representation (Instructor Version)

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

All clients have full connectivity to the servers. For the sake of frame diversity, the environment is not entirely realistic. For instance:

- NAT and PAT overload are both being used on the Branch network, but the Central 10.X.X.X network is being shared publicly.
- There is a separate DNS server in the 172 network due to the inability of computers to use the file server's public address. The simulated DNS server, unlike BIND, is basic and does not forward requests that it does not know to a root server - so the A records are duplicated.
- EIGRP is running in the cloud, as opposed to BGP.
- The Branch switch is actually providing DHCP, just because it can. It makes that side of the simulation different than the Central side.
- The cloud includes two servers, one of which uses the correct IP of netacad.com, and the other uses the correct IP of Google's DNS.
- The router passwords are "cisco" and "class", but there is a "banner motd" and "banner login" which readily give the passwords to the curious.
- The S1 and S2 switches have spanning tree PVST enabled. Each has a different blocking port, so all connections are green.

Topology



Objectives

Part 1: Overview of the Packet Tracer Program

Part 2: Exploring LANs, WANs, and Internets

Background

Packet Tracer is a fun, take-home, flexible software program which will help you with your Cisco Certified Network Associate (CCNA) studies. Packet Tracer allows you to experiment with network behavior, build network models, and ask "what if" questions. In this activity, you will explore a relatively complex network that highlights a few of Packet Tracer's features. While doing so, you will learn how to access Help and the tutorials. You will also learn how to switch between various modes and workspaces. Finally, you will explore how Packet Tracer serves as a modeling tool for network representations.

Note: It is not important that you understand everything you see and do in this activity. Feel free to explore the network on your own. If you wish to proceed more systematically, follow the steps below. Answer the questions to the best of your ability.

Part 1: Overview of the Packet Tracer Program

The network size is larger than most of the networks you will experience in this course (although you will see this topology often in your Networking Academy studies). You may need to adjust the window size of Packet Tracer to see the full network. If necessary, you can use the zoom in and out tools to adjust the size of the Packet Tracer window.

Step 1: Access the Packet Tracer Help pages, tutorial videos, and online resources

a. Access the Packet Tracer Help pages in two ways:

   1) Click the question mark icon in the top, right-hand corner of the menu toolbar.

   2) Click the **Help** menu, and then choose **Contents**.

b. Access the Packet Tracer tutorial videos by clicking **Help** > **Tutorials**. These videos are a visual demonstration of the information found in the **Help** pages and various aspects of the Packet Tracer software program. Before proceeding with this activity, you should gain some familiarity with the Packet Tracer interface and Simulation mode.

   1) View the **Interface Overview** video in the **Getting Started** section of Tutorials.

   2) View the **Simulation Environment** video in the **Realtime and Simulation Modes** section of **Tutorials**.

c. Find the “Configuring Devices Using the Desktop Tab” tutorial. Watch the first part to answer the following question: What information can you configure in the IP Configuration window? You can choose DHCP or Static and configure the IP address, Subnet Mask, Default Gateway, and DNS Server.

Step 2: Toggle between Realtime and Simulation modes.

a. Find the **Realtime** word in the bottom right corner of the Packet Tracer interface. In Realtime mode, your network is always running like a real network, whether you are working on the network or not. Your configurations are done in real time, and the network responds in near real time.

b. Click the tab directly behind the **Realtime** tab to switch to **Simulation** mode. In Simulation mode, you can watch your network run at a slower pace, observing the paths that data takes and inspecting the data packets in detail.

c. In the Simulation Panel, click **Auto Capture / Play**. You should now see data packets, represented as envelopes of various colors, traveling between the devices.

d. Click **Auto Capture / Play** again to pause the simulation.

e. Click **Capture / Forward** to step through the simulation. Click the button a few more times to see the effect.

f. In the network topology on the left, click one of the envelopes on an intermediate device and investigate what is inside. Over the course of your CCNA studies, you will learn the meaning of most everything inside these envelopes. For now, see if you can answer the following questions:

   - Under the **OSI Model tab**, how many **In Layers** and **Out Layers** have information? Answers will vary depending on the layer of the device.
   - Under the **Inbound PDU Details** and **Outbound PDU Details** tabs, what are the headings of the major sections? Answers will vary, but some likely answers will be Ethernet 802.3, LLC, STP BPDU, etc.
   - Click back and forth between the **Inbound PDU Details** and **Outbound PDU Details** tabs. Do you see information changing? If so, what? Answers will vary, but the source and/or destination addresses in the data link layer are changing. Other data may be changing as well depending on which packet the student chose to open.

g. Click the toggle button above **Simulation** in the bottom right corner to return to **Realtime** mode.

Step 3: Toggle between Logical and Physical views.

a. Find the **Logical** word in the top left corner of the Packet Tracer interface. You are currently in the **Logical** workspace where you will spend the majority of your time building, configuring, investigating, and troubleshooting networks.

   Note: Although you can add a geographical map as the background image for the **Logical** workspace, it does not usually have any relationship to the actual physical location of devices.

b. Click the tab below **Logical** to switch to the **Physical** workspace. The purpose of the **Physical** workspace is to give a physical dimension to your Logical network topology. It gives you a sense of scale and placement (how your network might look in a real environment).

c. During your CCNA studies, you will use this workspace on occasion. For now, just know that it is here and available for you to use. To learn more about the Physical workspace, refer to the Help files and tutorial videos.

d. Click the toggle button below **Physical** in the top right corner to return to the **Logical** workspace.

Part 2: Exploring LANs, WANs, and Internets

The network model in this activity incorporates many of the technologies that you will master in your CCNA studies. It represents a simplified version of how a small to medium-sized business network might look. Feel free to explore the network on your own. When ready, proceed through the following steps and answer the questions.

Step 1: Identify common components of a network as represented in Packet Tracer.

a. The Icon toolbar has various categories of networking components. You should see categories that correspond to intermediate devices, end devices, and media. The **Connections** category (with the lightning bolt icon) represents the networking media supported by Packet Tracer. There is also an **End Devices** category and two categories specific to Packet Tracer: **Custom Made Devices** and **Multiuser Connection**.

b. List the intermediate device categories. Routers, Switches, Hubs, Wireless Devices, and WAN Emulation

c. Without entering into the Internet cloud or Intranet cloud, how many icons in the topology represent endpoint devices (only one connection leading to them)? 13

d. Without counting the two clouds, how many icons in the topology represent intermediate devices (multiple connections leading to them)? 11

e. How many intermediate devices are routers? Note: The Linksys device is a router. 5

f. How many end devices are **not** desktop computers? 8

g. How many different types of media connections are used in this network topology? 4

h. Why isn't there a connection icon for wireless in the Connections category? Wireless connections are not physically made by the network technician. Instead, the devices are responsible for negotiating the connection and bringing up the physical link.

Step 2: Explain the purpose of the devices.

a. In Packet Tracer, the Server-PT device can act as a server. The desktop and laptop PCs cannot act as a server. Is that true in the real world? No.
   Based on your studies so far, explain the client-server model. In modern networks, a host can act as a client, a server, or both. Software installed on the host determines which role it plays on the network. Servers are hosts that have software installed that enables them to provide information and services, like

email or web pages, to other hosts on the network. Clients are hosts that have software installed that enables them to request and display the information obtained from the server. But a client could also be configured as a server simply by installing server software.

b. List at least two functions of intermediary devices. Regenerate and retransmit data signals; maintain information about what pathways exist through the network and internetwork; Notify other devices of errors and communication failures; Direct data along alternate pathways when there is a link failure; Classify and direct messages according to QoS priorities; Permit or deny the flow of data, based on security settings.

c. List at least two criteria for choosing a network media type. The distance the media can successfully carry a signal. The environment in which the media is to be installed. The amount of data and the speed at which it must be transmitted. The cost of the media and installation.

Step 3: Compare and contrast LANs and WANs.

a. Explain the difference between a LAN and a WAN. Give examples of each. LANs provide access to end users in a small geographical area. A home office or school campus are examples of LANs. WANs provide access to users in a wide geographical area over long distances spanning a few miles to thousands of miles. A Metropolitan Area Network and the Internet are examples of WANs. A company's intranet may also connect multiple remote sites using a WAN.

b. In the Packet Tracer network, how many WANs do you see? There are two: the Internet and the Intranet WANs.

c. How many LANs do you see? There are three, easily identifiable because each has a border and label.

d. The Internet in this Packet Tracer network is overly simplified and does not represent the structure and form of the real Internet. Briefly describe the Internet. The Internet is mostly used when we need to communicate with a resource on another network. The Internet is a global mesh of interconnected networks (internetworks).

e. What are some of the common ways a home user connects to the Internet? Cable, DSL, dial-up, cellular, and satellite.

f. What are some common methods that businesses use to connect to the Internet in your area? Dedicated leased line, Metro-E, DSL, Cable, Satellite

Challenge

Now that you have had an opportunity to explore the network represented in this Packet Tracer activity, you may have picked up a few skills that you would like to try out. Or maybe you would like the opportunity to explore this network in more detail. Realizing that most of what you see and experience in Packet Tracer is currently beyond your skill level, here are some challenges you might want to attempt. Do not worry if you cannot do them all. You will be a Packet Tracer master user and network designer soon enough.

- Add an end device to the topology and connect it to one of the LANs with a media connection. What else does this device need to send data to other end users? Can you provide the information? Is there a way to verify that you correctly connected the device?
- Add a new intermediary device to one of the networks and connect it to one of the LANs or WANs with a media connection. What else does this device need to serve as an intermediary to other devices in the network?
- Open a new instance of Packet Tracer. Create a new network with at least two LANs connected by a WAN. Connect all the devices. Investigate the original Packet Tracer activity to see what else you might need to do to make your new network functional. Record your thoughts and save your Packet Tracer file. You may want to revisit your network later after you have mastered a few more skills.

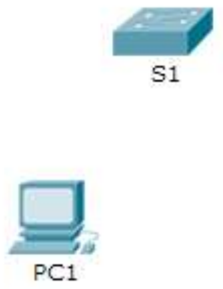
Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Overview of the Packet Tracer Program	Step 1c	4	
	Step 2f	6	
	Part 1 Total	**10**	
Part 2: Exploring LANs, WANs, and Internets	Step 1b	5	
	Step 1c	5	
	Step 1d	5	
	Step 1e	5	
	Step 1f	5	
	Step 1g	5	
	Step 1h	6	
	Step 2a	6	
	Step 2b	6	
	Step 2c	6	
	Step 3a	6	
	Step 3b	6	
	Step 3c	6	
	Step 3d	6	
	Step 3e	6	
	Step 3f	6	
	Part 2 Total	**90**	
	Total Score	**100**	

Packet Tracer - Navigating the IOS (Instructor Version)

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

Topology



Objectives

Part 1: Basic Connections, Accessing the CLI and Exploring Help

Part 2: Exploring EXEC Modes

Part 3: Setting the Clock

Background

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

Part 1: Basic Connections, Accessing the CLI and Exploring Help

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

Step 1: Connect PC1 to S1 using a console cable.

a. Click the **Connections** icon (the one that looks like a lightning bolt) in the lower left corner of the Packet Tracer window.

b. 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 off of it.

c. Click **PC1**; a window displays an option for an RS-232 connection.

d. Drag the other end of the console connection to the S1 switch and click the switch to bring up the connection list.

e. Select the Console port to complete the connection.

Step 2: Establish a terminal session with S1.

a. Click **PC1** and then select the **Desktop** tab.

b. Click the **Terminal** application icon; verify that the Port Configuration default settings are correct.

What is the setting for bits per second? 9600

c. Click **OK**.

d. The screen that appears may have several messages displayed. Somewhere on the display there should be a `Press RETURN to get started!` message. Press **ENTER**.

What is the prompt displayed on the screen? S1>

Step 3: Explore the IOS Help.

a. The IOS can provide help for commands depending on the level being accessed. The prompt currently being 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

b. At the prompt, type **t**, followed by a question mark (**?**).

```
S1> t?
```

Which commands are displayed? telnet terminal traceroute

c. At the prompt, type **te**, followed by a question mark (**?**).

```
S1> te?
```

Which commands are displayed? telnet terminal

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

Part 2: Exploring EXEC Modes

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

Step 1: Enter privileged EXEC mode.

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

```
S1> ?
```

What information is displayed that describes the **enable** command? Turn on privileged commands

b. 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 with the **enable** command, the remaining portion is displayed.

What would happen if you were to type **te<Tab>** at the prompt?

'te' does not provide enough characters to make the command unique so the characters will continue to display prompting the user for additional characters to make the command unique. There is more than one command that begins with the letters 'te'.

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

It changes from S1> to S1# indicating Privileged EXEC mode.

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

```
S1# ?
```

Previously there was one command that started 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’.)

5 - clear clock configure connect copy

Step 2: Enter Global Configuration mode.

a. One of the commands starting with the letter ‘C’ is **configure** when in Privileged EXEC mode. Type either the full command or enough of the command to make it unique along with 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]?

b. Press the **<ENTER>** key to accept the default parameter enclosed in brackets **[terminal]**.

How does the prompt change? S1(config)#

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

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

Part 3:   Setting the Clock

Step 1: Use the clock command.

a. 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?

UTC Mon Mar 1 1993 preceded by the hours, minutes, and seconds since the device started. The year is 1993.

b. 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.

c. The `% Incomplete command` message is returned by the IOS indicating that the **clock** command needs further 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

d. Set the clock using the **clock set** command. Continue proceeding 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

e. 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 further parameters are needed.

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

The output returns the request for more information:

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

f. 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
```

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

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

Step 2: Explore additional command messages.

a. The IOS provides various outputs for incorrect or incomplete commands as experienced in earlier sections. Continue to use the **clock** command to explore additional messages that may be encountered as you learn to use the IOS.

b. 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.
```

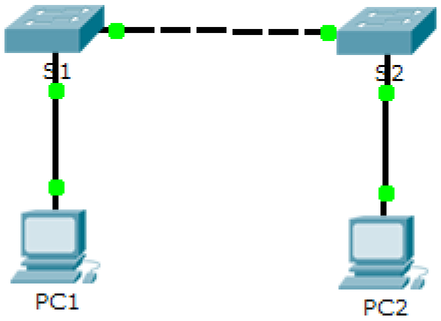
Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Basic Connections, Accessing the CLI and Exploring Help	Step 2a	5	
	Step 2c	5	
	Step 3a	5	
	Step 3b	5	
	Step 3c	5	
	Part 1 Total	**25**	
Part 2: Exploring 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: Setting 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**	

Packet Tracer - Configuring Initial Switch Settings (Instructor Version)

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

Topology



Objectives

Part 1: Verify the Default Switch Configuration

Part 2: Configure a Basic Switch Configuration

Part 3: Configure a MOTD Banner

Part 4: Save Configuration Files to NVRAM

Part 5: Configure S2

Background

In this activity, you will perform basic switch configurations. You will secure access to the command-line interface (CLI) and console ports using encrypted and plain text passwords. You will also learn how to configure messages for users logging into the switch. These banners are also used to warn unauthorized users that access is prohibited.

Part 1: Verify the Default Switch Configuration

Step 1: Enter privileged mode.

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

The privileged EXEC command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes are gained.

a. Click **S1** and then the **CLI** tab. Press **<Enter>**.

b. Enter privileged EXEC mode by entering the **enable** command:

```
Switch> enable
Switch#
```

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

Step 2: Examine the current switch configuration.

a. Enter the **show running-config** command.

```
Switch# show running-config
```

b. Answer the following questions:

How many FastEthernet interfaces does the switch have? 24

How many Gigabit Ethernet interfaces does the switch have? 2

What is the range of values shown for the vty lines? 0 -15

Which command will display the current contents of non-volatile random-access memory (NVRAM)? show startup-configuration

Why does the switch respond with `startup-config is not present`? It displays this message because the configuration file was not saved to NVRAM. Currently it is only located in RAM.

Part 2: Create a Basic Switch Configuration

Step 1: Assign a name to a switch.

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

```
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# exit
S1#
```

Step 2: Secure access to the console line.

To secure access to the console line, access config-line mode and set the console password to **letmein**.

```
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# line console 0
S1(config-line)# password letmein
S1(config-line)# login
S1(config-line)# exit
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Why is the **login** command required? In order for the password checking process to work, it requires both the **login** and **password** commands.

Step 3: Verify that console access is secured.

Exit privileged mode to verify that the console port password is in effect.

```
S1# exit
Switch con0 is now available
Press RETURN to get started.
```

```
User Access Verification
Password:
S1>
```

Note: If the switch did not prompt you for a password, then you did not configure the **login** parameter in Step 2.

Step 4: Secure privileged mode access.

Set the **enable** password to **c1$c0**. This password protects access to privileged mode.

Note: The **0** in **c1$c0** is a zero, not a capital O. This password will not grade as correct until after you encrypt it in Step 8.

```
S1> enable
S1# configure terminal
S1(config)# enable password c1$c0
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Step 5: Verify that privileged mode access is secure.

a. Enter the **exit** command again to log out of the switch.

b. Press **<Enter>** and you will now be asked for a password:

```
User Access Verification
Password:
```

c. The first password is the console password you configured for **line con 0**. Enter this password to return to user EXEC mode.

d. Enter the command to access privileged mode.

e. Enter the second password you configured to protect privileged EXEC mode.

f. Verify your configurations by examining the contents of the running-configuration file:

```
S1# show running-config
```

Notice how the console and enable passwords are both in plain text. This could pose a security risk if someone is looking over your shoulder.

Step 6: Configure an encrypted password to secure access to privileged mode.

The **enable password** should be replaced with the newer encrypted secret password using the **enable secret** command. Set the enable secret password to **itsasecret**.

```
S1# config t
S1(config)# enable secret itsasecret
S1(config)# exit
S1#
```

Note: The **enable secret** password overrides the **enable** password. If both are configured on the switch, you must enter the **enable secret** password to enter privileged EXEC mode.

Step 7: Verify that the enable secret password is added to the configuration file.

a. Enter the **show running-config** command again to verify the new **enable secret** password is configured.

   Note: You can abbreviate **show running-config** as

   ```
   S1# show run
   ```

b. What is displayed for the **enable secret** password? $1$mERr$ILwq/b7kc.7X/ejA4Aosn0

c. Why is the **enable secret** password displayed differently from what we configured? The enable secret is shown in encrypted form, whereas the enable password is in plain text.

Step 8: Encrypt the enable and console passwords.

As you noticed in Step 7, the **enable secret** password was encrypted, but the **enable** and **console** passwords were still in plain text. We will now encrypt these plain text passwords using the **service password-encryption** command.

```
S1# config t
S1(config)# service password-encryption
S1(config)# exit
```

If you configure any more passwords on the switch, will they be displayed in the configuration file as plain text or in encrypted form? Explain why? The service password-encryption command encrypts all current and future passwords.

Part 3: Configure a MOTD Banner

Step 1: Configure a message of the day (MOTD) banner.

The Cisco IOS command set includes a feature that allows you to configure messages that anyone logging onto the switch sees. These messages are called message of the day, or MOTD banners. Enclose the banner text in quotations or use a delimiter different from any character appearing in the MOTD string.

```
S1# config t
S1(config)# banner motd "This is a secure system. Authorized Access Only!"

S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

When will this banner be displayed? The message will be displayed when someone enters the switch through the console port.

Why should every switch have a MOTD banner? Every switch should have a banner to warn unauthorized users that access is prohibited but can also be used for sending messages to network personnel/technicians (such as impending system shutdowns or who to contact for access).

Part 4: Save Configuration Files to NVRAM

Step 1: Verify that the configuration is accurate using the show run command.

Step 2: Save the configuration file.

You have completed the basic configuration of the switch. 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.

```
S1# copy running-config startup-config
```

```
Destination filename [startup-config]?[Enter]
Building configuration...
[OK]
```

What is the shortest, abbreviated version of the **copy running-config startup-config** command? **cop r s**

Step 3: Examine the startup configuration file.

Which command will display the contents of NVRAM? **show startup-config**

Are all the changes that were entered recorded in the file? Yes, it is the same as the running-configuration

Part 5: Configure S2

You have completed the configuration on S1. You will now configure S2. If you cannot remember the commands, refer to Parts 1 to 4 for assistance.

Configure S2 with the following parameters:

a. Name device: **S2**

b. Protect access to the console using the **letmein** password.

c. Configure an enable password of **c1$c0** and an enable secret password of **itsasecret**.

d. Configure a message to those logging into the switch with the following message:

```
Authorized access only. Unauthorized access is prohibited and violators
will be prosecuted to the full extent of the law.
```

e. Encrypt all plain text passwords.

f. Ensure that the configuration is correct.

g. Save the configuration file to avoid loss if the switch is powered down.

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#line console 0
S2(config-line)#password letmein
S2(config-line)#login
S2(config-line)#enable password c1$c0
S2(config)#enable secret itsasecret
S2(config)#banner motd $any text here$
S2(config)#service password-encryption
S2(config)#do wr
```

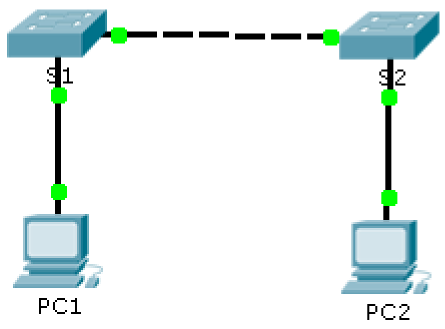
Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Verify the Default Switch Configuration	Step 2b, q1	2	
	Step 2b, q2	2	
	Step 2b, q3	2	
	Step 2b, q4	2	
	Step 2b, q5	2	
	Part 1 Total	**10**	
Part 2: Create a Basic Switch Configuration	Step 2	2	
	Step 7b	2	
	Step 7c	2	
	Step 8	2	
	Part 2 Total	**8**	
Part 3: Configure a MOTD Banner	Step 1, q1	2	
	Step 1, q2	2	
	Part 3 Total	**4**	
Part 4: Save Configuration Files to NVRAM	Step 2	2	
	Step 3, q1	2	
	Step 3, q2	2	
	Part 4 Total	**6**	
	Packet Tracer Score	**72**	
	Total Score	**100**	

Packet Tracer - Implement Basic Connectivity (Instructor Version)

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

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
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.

Part 1: Perform a Basic Configuration on S1 and S2

Complete the following steps on S1 and S2.

Step 1: Configure S1 with a hostname.

a. Click **S1**, and then click the **CLI** tab.

b. Enter the correct command to configure the hostname as **S1**.

Step 2: Configure the console and privileged EXEC mode passwords.

a. Use **cisco** for the console password.

b. Use **class** for the privileged EXEC mode password.

Step 3: Verify the password configurations for S1.

How can you verify that both passwords were configured correctly?

After you exit out of user exec mode, the switch will prompt you for a password to access the console interface and will prompt you a second time when accessing the privileged exec mode. You can also use the **show run** command to view the passwords..

Step 4: Configure a message of the day (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.

Step 5: Save the configuration file to NVRAM.

Which command do you issue to accomplish this step?

```
S1(config)#exit (or end)
S1#copy run start
```

Step 6: Repeat Steps 1 to 5 for S2.

Part 2: Configure the PCs

Configure PC1 and PC2 with IP addresses.

Step 1: Configure both PCs with IP addresses.

a. Click **PC1**, and then click the **Desktop** tab.

b. 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.

c. Repeat steps 1a and 1b for PC2.

Step 2: Test connectivity to switches.

a. Click **PC1**. Close the **IP Configuration** window if it is still open. In the **Desktop** tab, click **Command Prompt**. .

b. 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? Why or why not?

You should not have been successful because the switches have not been configured with an IP address.

Part 3: Configure the Switch Management Interface

Configure S1 and S2 with an IP address.

Step 1: Configure S1 with an IP address.

Switches can be used as a plug-and-play device, meaning they do not need to be configured for them to work. Switches forward information from one port to another based on Media Access Control (MAC) addresses. If this is the case, why would we configure it with an IP address?

In order for you to connect remotely to a switch, you need to assign it an IP address. The default configuration on the switch is to have the management of the switch controlled through VLAN 1.

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 need to enter the **no shutdown** command? The **no shutdown** command administratively enables the interface to an active state.

Step 2: Configure S2 with an IP addresses.

Use the information in the addressing table to configure S2 with an IP address.

Step 3: Verify the IP address configuration on S1 and S2.

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

Step 4: Save configurations for S1 and S2 to NVRAM.

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

Step 5: 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’s and S2's IP address from PC1 and PC2.

a. Click **PC1**, and then click the **Desktop** tab.

b. Click **Command Prompt**.

c. Ping the IP address for PC2.

d. Ping the IP address for S1.

e. Ping the IP address for S2.

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

All pings should be successful. If your first ping result is 80%, retry; it should now be 100%. You will learn why a ping may 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**	

Packet Tracer - Skills Integration Challenge (Instructor Version)

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

Addressing Table

Device	Interface	IP Address	Subnet Mask
[[S1Name]]	VLAN 1	[[S1Add]]	255.255.255.0
[[S2Name]]	VLAN 1	[[S2Add]]	255.255.255.0
[[PC1Name]]	NIC	[[PC1Add]]	255.255.255.0
[[PC2Name]]	NIC	[[PC2Add]]	255.255.255.0

Objectives

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

Scenario

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

Requirements

- Use a console connection to access each switch.
- Name **[[S1Name]]** and **[[S2Name]]** switches.
- Use the **[[LinePW]]** password for all lines.
- Use the **[[SecretPW]]** secret password.
- Encrypt all clear text passwords.
- Include the word **warning** in the message-of-the-day (MOTD) Banner.
- Configure addressing for all devices according to the Addressing Table.
- Save your configurations.
- Verify connectivity between all devices.

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

Isomorph Index: [[indexNames]][[indexPWs]][[indexAdds]][[indexTopos]]

Instructor Notes

The following information is for the Instructor version only.

This activity uses variables that are randomly generated each time the activity is open or the “Rest Activity” button is clicked. Although the tables below show device names mapping to specific address schemes, the names and addresses are not bound together. For example, a student could get the device names shown in Scenario 1 with the addressing shown in Scenario 2. In addition, one of three versions of the topology will be presented to the student.

Scenario 1

Device	Interface	Address	Subnet Mask
Class-A	VLAN 1	128.107.20.10	255.255.255.0
Class-B	VLAN1	128.107.20.15	255.255.255.0
Student-1	NIC	128.107.20.25	255.255.255.0
Student-2	NIC	128.107.20.30	255.255.255.0

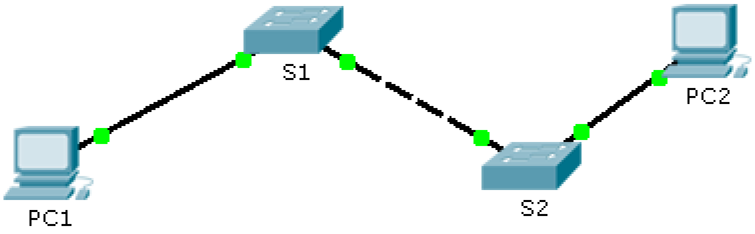
Scenario 2

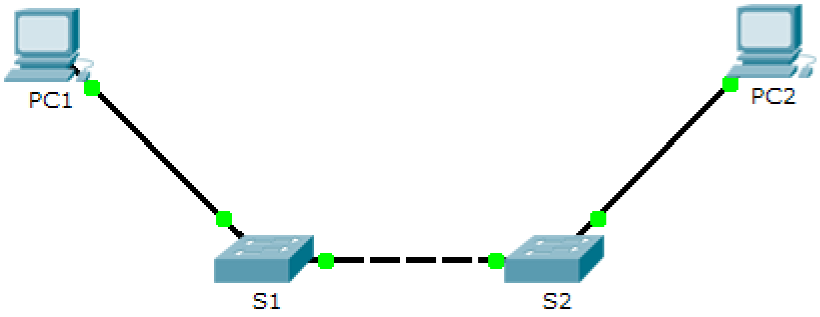
Device	Interface	Address	Subnet Mask
Room-145	VLAN 1	172.16.5.35	255.255.255.0
Room-146	VLAN 1	172.16.5.40	255.255.255.0
Manager	NIC	172.16.5.50	255.255.255.0
Reception	NIC	172.16.5.60	255.255.255.0

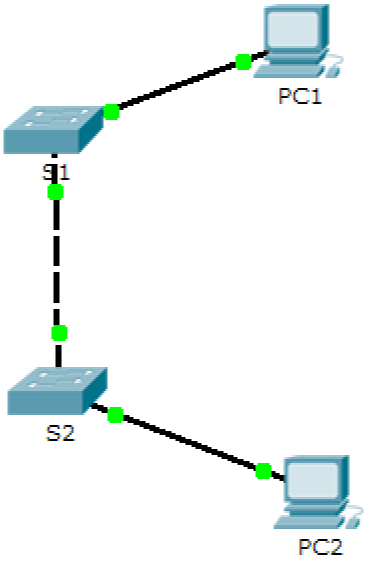
Scenario 3

Device	Interface	Address	Subnet Mask
ASw-1	VLAN 1	10.10.10.100	255.255.255.0
ASw-2	VLAN 1	10.10.10.150	255.255.255.0
User-01	NIC	10.10.10.4	255.255.255.0
User-02	NIC	10.10.10.5	255.255.255.0

Topology Isomorphs



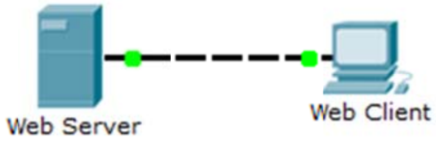




Packet Tracer - Investigating the TCP/IP and OSI Models in Action (Instructor Version)

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

Topology



Objectives

Part 1: Examine HTTP Web Traffic

Part 2: Display Elements of the TCP/IP Protocol Suite

Background

This simulation activity is intended to provide a foundation for understanding the TCP/IP protocol suite and the relationship to the OSI model. Simulation mode allows you to view the data contents being sent across the network at each layer.

As data moves through the network, it is broken down into smaller pieces and identified so that the pieces can be put back together when they arrive at the destination. Each piece is assigned a specific name (protocol data unit [PDU]) and associated with a specific layer of the TCP/IP and OSI models. Packet Tracer simulation mode enables you to view each of the layers and the associated PDU. The following steps lead the user through the process of requesting a web page from a web server by using the web browser application available on a client PC.

Even though much of the information displayed will be discussed in more detail later, this is an opportunity to explore the functionality of Packet Tracer and be able to visualize the encapsulation process.

Part 1: Examine HTTP Web Traffic

In Part 1 of this activity, you will use Packet Tracer (PT) Simulation mode to generate web traffic and examine HTTP.

Step 1: Switch from Realtime to Simulation mode.

In the lower right corner of the Packet Tracer interface are tabs to toggle between **Realtime** and **Simulation** mode. PT always starts in **Realtime** mode, in which networking protocols operate with realistic timings. However, a powerful feature of Packet Tracer allows the user to “stop time” by switching to Simulation mode. In Simulation mode, packets are displayed as animated envelopes, time is event driven, and the user can step through networking events.

a. Click the **Simulation** mode icon to switch from **Realtime** mode to **Simulation** mode.

b. Select **HTTP** from the **Event List Filters**.

1) HTTP may already be the only visible event. Click **Edit Filters** to display the available visible events. Toggle the **Show All/None** check box and notice how the check boxes switch from unchecked to checked or checked to unchecked, depending on the current state.

2) Click the **Show All/None** check box until all boxes are cleared and then select **HTTP**. Click anywhere outside of the **Edit Filters** box to hide it. The Visible Events should now only display HTTP.

Step 2: Generate web (HTTP) traffic.

Currently the Simulation Panel is empty. There are six columns listed across the top of the Event List within the Simulation Panel. As traffic is generated and stepped through, events appear in the list. The **Info** column is used to inspect the contents of a particular event.

Note: The Web Server and Web Client are displayed in the left pane. The panels can be adjusted in size by hovering next to the scroll bar and dragging left or right when the double-headed arrow appears.

a. Click **Web Client** in the far left pane.

b. Click the **Desktop** tab and click the **Web Browser** icon to open it.

c. In the URL field, enter **www.osi.local** and click **Go**.

Because time in Simulation mode is event-driven, you must use the **Capture/Forward** button to display network events.

d. Click **Capture/Forward** four times. There should be four events in the Event List.

Look at the Web Client web browser page. Did anything change?

The web page was returned from the web server.

Step 3: Explore the contents of the HTTP packet.

a. Click the first colored square box under the **Event List** > **Info** column. It may be necessary to expand the **Simulation Panel** or use the scrollbar directly below the **Event List**.

The **PDU Information at Device: Web Client** window displays. In this window, there are only two tabs (**OSI Model** and **Outbound PDU Details**) because this is the start of the transmission. As more events are examined, there will be three tabs displayed, adding a tab for **Inbound PDU Details**. When an event is the last event in the stream of traffic, only the **OSI Model** and **Inbound PDU Details** tabs are displayed.

b. Ensure that the **OSI Model** tab is selected. Under the **Out Layers** column, ensure that the **Layer 7** box is highlighted.

What is the text displayed next to the **Layer 7** label? HTTP

What information is listed in the numbered steps directly below the **In Layers** and **Out Layers** boxes?

“1. The HTTP client sends a HTTP request to the server.”

c. Clic k **Next Layer**. Layer 4 should be highlighted. What is the **Dst Port** value? 80

d. Click **Next Layer**. Layer 3 should be highlighted. What is the **Dest. IP** value? 192.168.1.254

e. Click **Next Layer**. What information is displayed at this layer? Layer 2 Ethernet II Header and inbound and outbound MAC addresses.

f. Click the **Outbound PDU Details** tab.

Information listed under the **PDU Details** is reflective of the layers within the TCP/IP model.

Note: The information listed under the **Ethernet II** section provides even more detailed information than is listed under Layer 2 on the **OSI Model** tab. The **Outbound PDU Details** provides more descriptive and detailed information. The values under **DEST MAC** and **SRC MAC** within the **Ethernet II** section of the **PDU Details** appear on the **OSI Model** tab under Layer 2, but are not identified as such.

What is the common information listed under the **IP** section of **PDU Details** as compared to the information listed under the **OSI Model** tab? With which layer is it associated? SRC IP and DST IP at Layer 3

What is the common information listed under the **TCP** section of **PDU Details**, as compared to the information listed under the **OSI Model** tab, and with which layer is it associated? SRC PORT and DEST PORT at Layer 4

What is the **Host** listed under the **HTTP** section of the **PDU Details**? What layer would this information be associated with under the **OSI Model** tab? www.osi.local, Layer 7

g. Click the next colored square box under the **Event List** > **Info** column. Only Layer 1 is active (not grayed out). The device is moving the frame from the buffer and placing it on to the network.

h. Advance to the next HTTP **Info** box within the **Event List** and click the colored square box. This window contains both **In Layers** and **Out Layers**. Notice the direction of the arrow directly under the **In Layers** column; it is pointing upward, indicating the direction the information is travelling. Scroll through these layers making note of the items previously viewed. At the top of the column the arrow points to the right. This denotes that the server is now sending the information back to the client.

Comparing the information displayed in the **In Layers** column with that of the **Out Layers** column, what are the major differences? The Src and Dst Ports, Src and Dst IPs and MAC addresses have been swapped.

i. Click the **Outbound PDU Details** tab. Scroll down to the **HTTP** section.

What is the first line in the HTTP message that displays? HTTP/1.1 200 OK – this means that the request was successful and the page delivered from the server.

j. Click the last colored square box under the **Info** column. How many tabs are displayed with this event and why?

Just 2, one for the OSI Model and one for Inbound PDU Details because this is the receiving device.

Part 2: Display Elements of the TCP/IP Protocol Suite

In Part 2 of this activity, you will use the Packet Tracer Simulation mode to view and examine some of the other protocols comprising of the TCP/IP suite.

Step 1: View Additional Events

a. Close any open PDU information windows.

b. In the Event List Filters > Visible Events section, click **Show All**.

What additional Event Types are displayed? Depending on whether any communications has occurred prior to starting the original simulation, there should now be entries for ARP, DNS, TCP and HTTP. It is possible that the ARP entries may not show, depending on what a student may have done prior to going to simulation mode. If the activity is started from scratch all of those will be listed.

These extra entries play various roles within the TCP/IP suite. If the Address Resolution Protocol (ARP) is listed, it searches MAC addresses. DNS is responsible for converting a name (for example, **www.osi.local**) to an IP address. The additional TCP events are responsible for connecting, agreeing on communication parameters, and disconnecting the communications sessions between the devices. These protocols have been mentioned previously and will be further discussed as the course progresses. Currently there are over 35 possible protocols (event types) available for capture within Packet Tracer.

c. Click the first DNS event in the **Info** column. Explore the **OSI Model** and **PDU Detail** tabs and note the encapsulation process. As you look at the **OSI Model** tab with **Layer 7** highlighted, a description of what is occurring is listed directly below the **In Layers** and **Out Layers** (“1. The DNS client sends a DNS query to the DNS server.”). This is very useful information to help understand what is occurring during the communication process.

d. Click the **Outbound PDU Details** tab. What information is listed in the **NAME**: in the DNS QUERY section?

www.osi.local

e. Click the last DNS **Info** colored square box in the event list. Which device is displayed?

The Web Client

What is the value listed next to **ADDRESS**: in the DNS ANSWER section of the **Inbound PDU Details**?

192.168.1.254 – the address of the Web Server

f. Find the first **HTTP** event in the list and click the colored square box of the **TCP** event immediately following this event. Highlight **Layer 4** in the **OSI Model** tab. In the numbered list directly below the **In Layers** and **Out Layers**, what is the information displayed under items 4 and 5?

4. The TCP connection is successful. 5. The device sets the connection state to ESTABLISHED.

TCP manages the connecting and disconnecting of the communications channel along with other responsibilities. This particular event shows that the communication channel has been ESTABLISHED.

g. Click the last TCP event. Highlight Layer 4 in the **OSI Model** tab. Examine the steps listed directly below **In Layers** and **Out Layers**. What is the purpose of this event, based on the information provided in the last item in the list (should be item 4)? CLOSING the connection.

Challenge

This simulation provided an example of a web session between a client and a server on a local area network (LAN). The client makes requests to specific services running on the server. The server must be set up to listen on specific ports for a client request. (Hint: Look at Layer 4 in the **OSI Model** tab for port information.)

Based on the information that was inspected during the Packet Tracer capture, what port number is the **Web Server** listening on for the web request? The first HTTP PDU being requested by the Web Client shows port 80 under the layer 4 DST port.

What port is the **Web Server** listening on for a DNS request? The first DNS PDU being requested by the Web Client shows a layer 4 destination of port 53.

Suggested Scoring Rubric

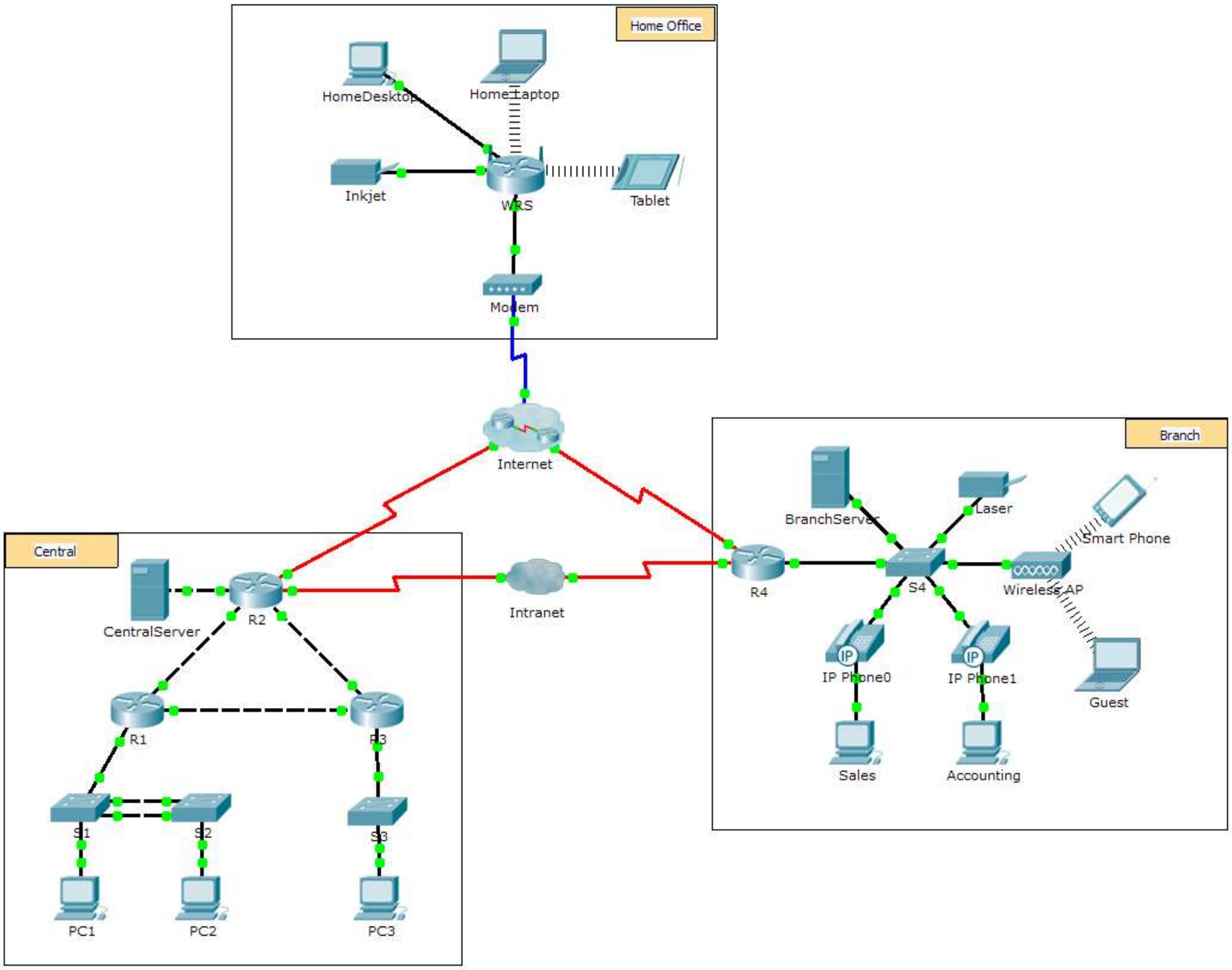
Activity Section	Question Location	Possible Points	Earned Points
Part 1: Examine HTTP Web Traffic	Step 2d	5	
	Step 3b-1	5	
	Step 3b-2	5	
	Step 3c	5	
	Step 3d	5	
	Step 3e	5	
	Step 3f-1	5	
	Step 3f-2	5	
	Step 3f-3	5	
	Step 3h	5	
	Step 3i	5	
	Step 3j	5	
	Part 1 Total	**60**	
Part 2: Display Elements of the TCP/IP Protocol Suite	Step 1b	5	
	Step 1d	5	
	Step 1e-1	5	
	Step 1e-2	5	
	Step 1f	5	
	Step 1g	5	
	Part 2 Total	**30**	
Challenge 1		5	
	2 5		
	Part 3 Total	**10**	
	Total Score	**100**	

Packet Tracer - Explore a Network (Instructor Version)

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

This activity uses a complex topology and a fictitious top level domain (.pta) to avoid conflicts with Internet naming. Because PT does not forward DNS requests, the same entries have been made on each DNS server so that DNS traffic can remain local when it is relevant to do so. In order to deal with the use of RFC 1918 private addressing, NAT is used both at the Home Office and Branch Office to help avoid any misconceptions.

Topology



Objectives

Part 1: Examine Internetwork Traffic at Branch

Part 2: Examine Internetwork Traffic to Central

Part 3: Examine Internet Traffic from Branch

Background

This simulation activity is intended to help you understand the flow of traffic and the contents of data packets as they traverse a complex network. Communications will be examined at three different locations simulating typical business and home networks.

Take a few moments to study the topology displayed. The Central location has three routers and multiple networks possibly representing different buildings within a campus. The Branch location has only one router with a connection to both the Internet and a dedicated wide-area network (WAN) connection to the Central location. The Home Office makes use of a cable modem broadband connection to provide access to both the Internet and to corporate resources over the Internet.

The devices at each location use a combination of static and dynamic addressing. The devices are configured with default gateways and Domain Name System (DNS) information, as appropriate.

Part 1: Examine Internetwork Traffic at Branch

In Part 1 of this activity, you will use Simulation mode to generate web traffic and examine the HTTP protocol along with other protocols necessary for communications.

Step 1: Switching from Realtime to Simulation mode.

a. Click the **Simulation** mode icon to switch from **Realtime** mode to **Simulation** mode.

b. Verify that **ARP, DNS, HTTP**, and **TCP** are selected from the **Event List Filters**.

c. Move the slider located below the **Play Controls** buttons (**Back**, **Auto Capture**/**Play**, **Capture**/**Forward**) all the way to the right.

Step 2: Generate traffic using a web browser.

Currently the Simulation Panel is empty. In the Event List at the top of the Simulation Panel there are six columns listed across the heading. As traffic is generated and stepped through, events display in the list. The **Info** column is used to inspect the contents of a particular event.

Note: The panel to the left of the Simulation Panel displays the topology. Use the scrollbars to bring the Branch location into the panel, if necessary. The panels can be adjusted in size by hovering next to the scrollbar and dragging left or right.

a. Click the **Sales PC** in the far left pane.

b. Click the **Desktop** tab and click the **Web Browser** icon to open it.

c. In the URL field, enter **http://branchserver.pt.pta** and click **Go**. Look in the Event List in the Simulation Panel. What is the first type of event listed?

The DNS request for the IP address of branchserver.pt.pta.

d. Click the **DNS** info box. In the **Out Layers**, DNS is listed for Layer 7. Layer 4 is using UDP to contact the DNS server on port 53 (**Dst Port:**). Both the source and destination IP addresses are listed. What information is missing to communicate with the DNS server?

The Layer 2 information, specifically the destination MAC address.

e. Click **Auto Capture/Play**. In approximately 30 to 40 seconds, a window displays, indicating the completion of the current simulation. (Or a window may display indicating that the buffer is full.) Click the **View Previous Events** button. Scroll back to the top of the list and note the number of **ARP** events. Looking at the Device column in Event list, how many of the devices in the Branch location does the **ARP** request pass through?

Each device received an ARP request.

f. Scroll down the events in the list to the series of **DNS** events. Select the **DNS** event that has the “At Device” listed as **BranchServer**. Click the square box in the **Info** column. What can be determined by selecting Layer 7 in the **OSI Model**? (Look at the results displayed directly below **In Layers.**)

   The DNS server receives a DNS query. The name queried resolved locally.

g. Click the **Outbound PDU Details** tab. Scroll to the bottom of the window and locate the DNS Answer section. What is the address displayed?

   172.16.0.3, the address of Branchserver.

h. The next several events are **TCP** events enabling a communications channel to be established. Select the last **TCP** event at device **Sales** just prior to the **HTTP** event. Click the colored square Info box to display the PDU information. Highlight Layer 4 in the **In Layers** column. Looking at item 6 in the list directly below the **In Layers** column, what is the connection state?

   Established

i. The next several events are **HTTP** events. Select any one of the **HTTP** events at an intermediary device (IP Phone or Switch). How many layers are active at one of these devices, and why?

   Two layers, because these are Layer 2 devices.

j. Select the last **HTTP** event at the Sales PC. Select the uppermost layer from the **OSI Model** tab. What is the result listed below the **In Layers** column?

   The HTTP client receives a HTTP reply from the server. It displays the page in the web browser.

Part 2: Examine Internetwork Traffic to Central

In Part 2 of this activity, you will use Packet Tracer (PT) Simulation mode to view and examine how traffic leaving the local network is handled.

Step 1: Set up for traffic capture to the Central web server.

a. Close any open PDU Information windows.

b. Click **Reset Simulation** (located near the middle of the Simulation Panel).

c. Type **http://centralserver.pt.pta** in the web browser of the Sales PC.

d. Click **Auto Capture/Play**; in approximately 75 seconds, a window displays, indicating the completion of the current simulation. Click **View Previous Events**. Scroll back to the top of the list; note that the first series of events are **DNS** and there are no **ARP** entries prior to contacting the **BranchServer**. Based on what you have learned so far, why is this the case?

   The Sales PC already knows the MAC address of the DNS server.

e. Click the last DNS event in the **Info** column. Select **Layer 7** in the **OSI Model** tab.

   By looking at the information provided, what can be determined about the DNS results? The DNS server was able to resolve the domain name for centralserver.pt.pta.

f. Click the **Inbound PDU Details** tab. Scroll down to the **DNS ANSWER** section. What is the address listed for centralserver.pt.pta? 10.10.10.2

g. The next several events are **ARP** events. Click the colored square Info box of the last **ARP** event. Click the **Inbound PDU Details** tab and note the MAC address. Based on the information in the ARP section, what device is providing the ARP reply? The R4 Router, the gateway device.

h. The next several events are **TCP** events, once again preparing to set up a communications channel. Find the first **HTTP** event in the Event List. Click the colored square box of the **HTTP** event. Highlight Layer 2 in the **OSI Model** tab. What can be determined about the destination MAC address?

   It is the MAC Address of the R4 router.

i. Click the **HTTP** event at device **R4**. Notice that Layer 2 contains an Ethernet II header. Click the **HTTP** event at device **Intranet**. What is the Layer 2 listed at this device? Frame Relay FRAME RELAY.

Notice that there are only two active layers, as opposed to three active layers when moving through the router. This is a WAN connection, which will be discussed in a later course.

Part 3: Examine Internet Traffic from Branch

In Part 3 of this activity, you will clear the events and start a new web request that will make use of the Internet.

Step 1: Set up for traffic capture to an Internet web server.

a. Close any open PDU information windows.

b. Click **Reset Simulation** near the middle of the Simulation Panel. Type **http://www.netacad.pta** in the web browser of the Sales PC.

c. Click **Auto Capture/Play**; in approximately 75 seconds, a window displays, indicating the completion of the current simulation. Click **View Previous Events**. Scroll back to the top of the list; notice that the first series of events are **DNS**. What do you notice about the number of **DNS** events?

There are considerably more DNS events. Because the DNS entry is not local it is forwarded to a server on the Internet.

d. Observe some of the devices that the **DNS** events travel through on the way to a DNS server. Where are these devices located? In the Internet Cloud, students should be shown that those devices can be displayed by clicking the cloud and then clicking the Back link to go back.

e. Click the last **DNS** event. Click the **Inbound PDU Details** tab and scroll down to the last DNS Answer section. What is the address listed for **www.netacad.pta**? 216.146.46.11

f. When routers move the **HTTP** event through the network, there are three layers active in both the **In Layers** and **Out Layers** in the **OSI Model** tab. Based on that information, how many routers are passed through?

There are 3 routers (ISP-Tier3a, ISP-Tier3b and R4), however there are 4 HTTP events travelling through the routers.

g. Click the **TCP** event just prior to the last **HTTP** event. Based on the information displayed, what is the purpose of this event? To close the TCP connection to 216.146.46.11.

h. There are several more **TCP** events listed. Locate the **TCP** event where the *Last Device* is **IP Phone** and the *Device At* is **Sales**. Click the colored square Info box and select **Layer 4** in the **OSI Model** tab. Based on the information from the output, what is the connection state set to? Closing

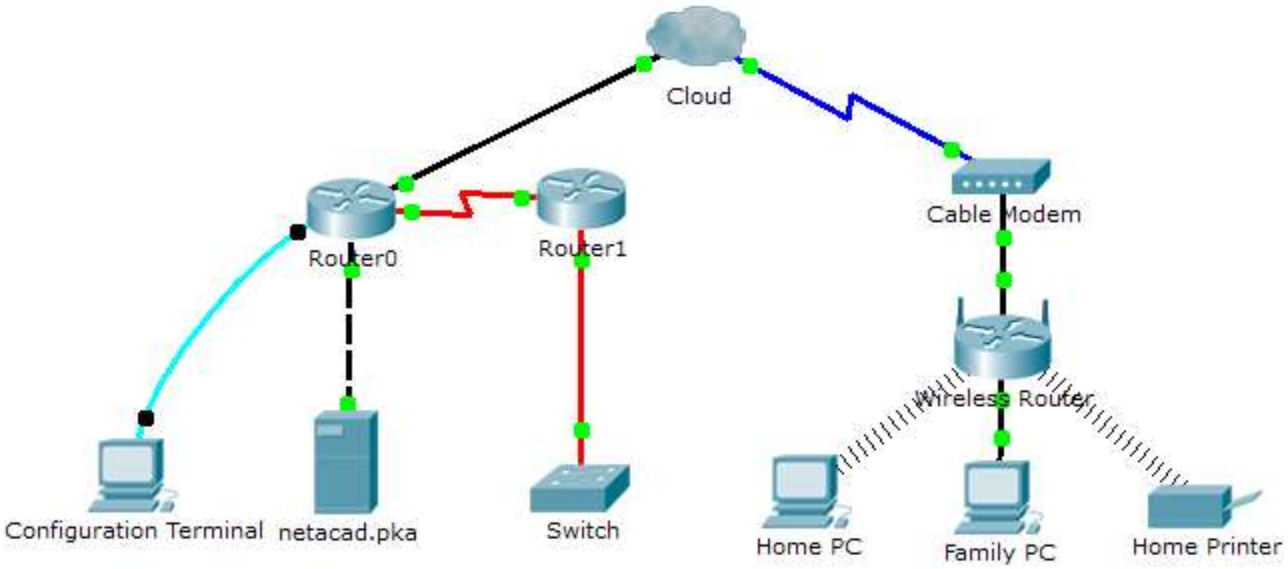
Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Examine Internetwork Traffic at Branch	Step 2c	5	
	Step 2d	5	
	Step 2e	5	
	Step 2f	5	
	Step 2g	5	
	Step 2h	5	
	Step 2i	5	
	Step 2j	5	
	Part 1 Total	**40**	
Part 2: Examine Internetwork Traffic to Central	Step 1c	5	
	Step 1d	5	
	Step 1e	5	
	Step 1f	5	
	Step 1g	5	
	Step 1h	5	
	Part 2 Total	**30**	
Part 3: Examine Internet Traffic from Branch	Step 1c	5	
	Step 1d	5	
	Step 1e	5	
	Step 1f	5	
	Step 1g	5	
	Step 1h	5	
	Part 3 Total	**30**	
	Total Score	**100**	

Packet Tracer - Connecting a Wired and Wireless LAN (Instructor Version)

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

Topology



Addressing Table

Device	Interface	IP Address	Connects To
Cloud	Eth6	N/A	Fa0/0
	Coax7	N/A	Port0
Cable Modem	Port0	N/A	Coax7
	Port1	N/A	Internet
Router0	Console	N/A	RS232
	Fa0/0	192.168.2.1/24	Eth6
	Fa0/1	10.0.0.1/24	Fa0
	Ser0/0/0	172.31.0.1/24	Ser0/0
Router1	Ser0/0	172.31.0.2/24	Ser0/0/0
	Fa1/0	172.16.0.1/24	Fa0/1
WirelessRouter	Internet	192.168.2.2/24	Port 1
	Eth1	192.168.1.1	Fa0
Family PC	Fa0	192.168.1.102	Eth1
Switch	Fa0/1	172.16.0.2	Fa1/0
Netacad.pka	Fa0	10.0.0.254	Fa0/1
Configuration Terminal	RS232	N/A	Console

Objectives

Part 1: Connect to the Cloud

Part 2: Connect Router0

Part 3: Connect Remaining Devices

Part 4: Verify Connections

Part 5: Examine the Physical Topology

Background

When working in Packet Tracer (a lab environment or a corporate setting), you should know how to select the appropriate cable and how to properly connect devices. This activity will examine device configurations in Packet Tracer, selecting the proper cable based on the configuration, and connecting the devices. This activity will also explore the physical view of the network in Packet Tracer.

Part 1: Connect to the Cloud

Step 1: Connect the cloud to Router0.

a. At the bottom left, click the orange lightning icon to open the available **Connections**.

b. Choose the correct cable to connect **Router0 Fa0/0** to **Cloud Eth6**. **Cloud** is a type of switch, so use a **Copper Straight-Through** connection. If you attached the correct cable, the link lights on the cable turn green.

Step 2: Connect the cloud to Cable Modem.

Choose the correct cable to connect **Cloud Coax7** to **Modem Port0**.

If you attached the correct cable, the link lights on the cable turn green.

Part 2: Connect Router0

Step 1: Connect Router0 to Router1.

Choose the correct cable to connect **Router0 Ser0/0/0** to **Router1 Ser0/0**. Use one of the available **Serial** cables.

If you attached the correct cable, the link lights on the cable turn green.

Step 2: Connect Router0 to netacad.pka.

Choose the correct cable to connect **Router0 Fa0/1** to **netacad.pka Fa0**. Routers and computers traditionally use the same wires to transmit (1 and 2) and receive (3 and 6). The correct cable to choose consists of these crossed wires. Although many NICs can now autosense which pair is used to transmit and receive, **Router0** and **netacad.pka** do not have autosensing NICs.

If you attached the correct cable, the link lights on the cable turn green.

Step 3: Connect Router0 to the Configuration Terminal.

Choose the correct cable to connect **Router0 Console** to **Configuration Terminal RS232**. This cable does not provide network access to **Configuration Terminal**, but allows you to configure **Router0** through its terminal.

If you attached the correct cable, the link lights on the cable turn black.

Part 3: Connect Remaining Devices

Step 1: Connect Router1 to Switch.

Choose the correct cable to connect **Router1 Fa1/0** to **Switch Fa0/1**.

If you attached the correct cable, the link lights on the cable turn green. Allow a few seconds for the light to transition from amber to green.

Step 2: Connect Cable Modem to Wireless Router.

Choose the correct cable to connect **Modem Port1** to **Wireless Router Internet** port.

If you attached the correct cable, the link lights on the cable will turn green.

Step 3: Connect Wireless Router to Family PC.

Choose the correct cable to connect **Wireless Router Ethernet 1** to **Family PC**.

If you attached the correct cable, the link lights on the cable turn green.

Part 4: Verify Connections

Step 1: Test the connection from Family PC to netacad.pka.

a. Open the **Family PC** command prompt and ping **netacad.pka**.

b. Open the **Web Browser** and the web address **http://netacad.pka**.

Step 2: Ping the Switch from Home PC.

Open the **Home PC** command prompt and ping the **Switch** IP address of to verify the connection.

Step 3: Open Router0 from Configuration Terminal.

a. Open the **Terminal** of **Configuration Terminal** and accept the default settings.

b. Press **Enter** to view the **Router0** command prompt.

c. Type **show ip interface brief** to view interface statuses.

Part 5: Examine the Physical Topology

Step 1: Examine the Cloud.

a. Click the **Physical Workspace** tab or press **Shift**+**P** and **Shift**+**L** to toggle between the logical and physical workspaces.

b. Click the **Home City** icon.

c. Click the **Cloud** icon. How many wires are connected to the switch in the blue rack? 2

d. Click **Back** to return to **Home City**.

Step 2: Examine the Primary Network.

a. Click the **Primary Network** icon. Hold the mouse pointer over the various cables. What is located on the table to the right of the blue rack? Configuration Terminal

b. Click **Back** to return to **Home City**.

Step 3: Examine the Secondary Network.

a. Click the **Secondary Network** icon. Hold the mouse pointer over the various cables. Why are there two orange cables connected to each device? Fiber cables come in pairs, one for transmit, the other for receive.

b. Click **Back** to return to **Home City**.

Step 4: Examine the Home Network.

a. Why is there an oval mesh covering the home network? It represents the range of the wireless network.

b. Click the **Home Network** icon. Why is there no rack to hold the equipment? Home networks typically do not have racks.

c. Click the **Logical Workspace** tab to return to the logical topology.

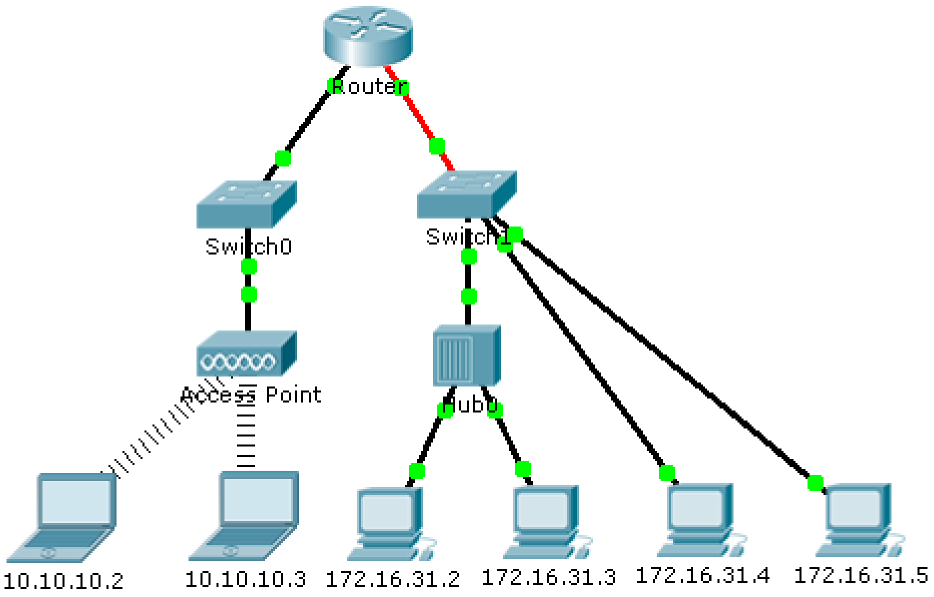
Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 5: Examine the Physical Topology	Step 1c	4	
	Step 2a	4	
	Step 3a	4	
	Step 4a	4	
	Step 4b	4	
Part 5 Total		**20**	
Packet Tracer Score		**80**	
Total Score		**100**	

Packet Tracer - Identify MAC and IP Addresses (Instructor Version)

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

Topology



Objectives

Part 1: Gather PDU Information

Part 2: Reflection Questions

Background

This activity is optimized for viewing PDUs. The devices are already configured. You will gather PDU information in simulation mode and answer a series of questions about the data you collect.

Part 1: Gather PDU Information

Note: Review the Reflection Questions in Part 2 before proceeding with Part 1. It will give you an idea of the types of information you will need to gather.

Step 1: Gather PDU information as a packet travels from 172.16.31.2 to 10.10.10.3.

a. Click **172.16.31.2** and open the **Command Prompt**.

b. Enter the **ping 10.10.10.3** command.

c. Switch to simulation mode and repeat the **ping 10.10.10.3** command. A PDU appears next to **172.16.31.2**.

d. Click the PDU and note the following information from the **Outbound PDU Layer** tab:

- Destination MAC Address: 00D0:BA8E:741A
- Source MAC Address: 000C:85CC:1DA7
- Source IP Address: 172.16.31.2

- Destination IP Address: 10.10.10.3
- At Device: Computer

e. Click **Capture / Forward** to move the PDU to the next device. Gather the same information from Step 1d. Repeat this process until the PDU reaches its destination. Record the PDU information you gathered into a spreadsheet using a format like the table shown below:

Example Spreadsheet Format

Test	At Device	Dest. MAC	Src MAC	Src IPv4	Dest IPv4
Ping from 172.16.31.2 to 10.10.10.3	172.16.31.2	00D0:BA8E:741A	000C:85CC:1DA7	172.16.31.2	10.10.10.3
	Hub	--	--	--	--
	Switch1	00D0:BA8E:741A	000C:85CC:1DA7	--	--
	Router	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3
	Switch0	0060:4706:572B	00D0:588C:2401	--	--
	Access Point	--	--	--	--
	10.10.10.3	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3

Step 2: Gather additional PDU information from other pings.

Repeat the process in Step 1 and gather the information for the following tests:

- Ping 10.10.10.2 from 10.10.10.3.
- Ping 172.16.31.2 from 172.16.31.3.
- Ping 172.16.31.4 from 172.16.31.5.
- Ping 172.16.31.4 from 10.10.10.2.
- Ping 172.16.31.3 from 10.10.10.2.

Part 2: Reflection Questions

Answer the following questions regarding the captured data:

1. Were there different types of wires used to connect devices? Yes, copper and fiber
2. Did the wires change the handling of the PDU in any way? No
3. Did the **Hub** lose any of the information given to it? No
4. What does the **Hub** do with MAC addresses and IP addresses? Nothing
5. Did the wireless **Access Point** do anything with the information given to it? Yes. It repackaged it as wireless 802.11
6. Was any MAC or IP address lost during the wireless transfer? No
7. What was the highest OSI layer that the **Hub** and **Access Point** used? Layer 1
8. Did the **Hub** or **Access Point** ever replicate a PDU that was rejected with a red “X”? Yes
9. When examining the **PDU Details** tab, which MAC address appeared first, the source or the destination? Destination

10. Why would the MAC addresses appear in this order? A switch can begin forwarding a frame to a known MAC address more quickly if the destination is listed first
11. Was there a pattern to the MAC addressing in the simulation? No
12. Did the switches ever replicate a PDU that was rejected with a red “X”? No
13. Every time that the PDU was sent between the 10 network and the 172 network, there was a point where the MAC addresses suddenly changed. Where did that occur? It occurred at the Router
14. Which device uses MAC addresses starting with 00D0? The Router
15. To what devices did the other MAC addresses belong? To the sender and receiver
16. Did the sending and receiving IPv4 addresses switch in any of the PDUs? No
17. If you follow the reply to a ping, sometimes called a *pong*, do the sending and receiving IPv4 addresses switch? Yes
18. What is the pattern to the IPv4 addressing in this simulation? Each port of a router requires a set of non-overlapping addresses
19. Why do different IP networks need to be assigned to different ports of a router? The function of a router is to inter-connect different IP networks.
20. If this simulation was configured with IPv6 instead of IPv4, what would be different? The IPv4 addresses would be replaced with IPv6 addresses, but everything else would be the same.

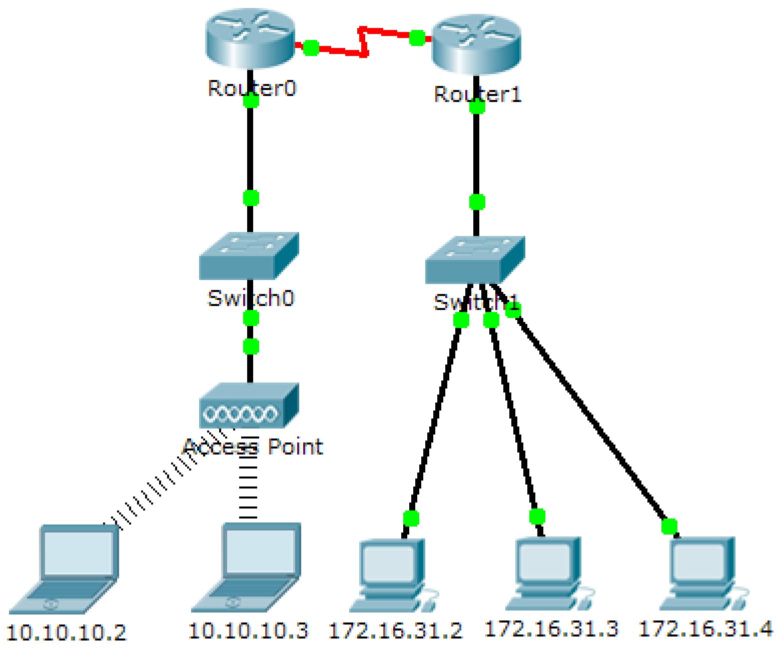
Suggested Scoring Rubric

There are 20 questions worth 5 points each for a possible score of 100.

Packet Tracer - Examine the ARP Table (Instructor Version)

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

Topology



Addressing Table

Device	Interface	MAC Address	Switch Interface
Router0	Gig0/0	0001.6458.2501	Gig0/1
	Se0/0/0	N/A	N/A
Router1	Gig0/0	00E0.F7B1.8901	Gig0/1
	Se0/0/0	N/A	N/A
10.10.10.2	Wireless	0060.2F84.4AB6	Fa0/2
10.10.10.3	Wireless	0060.4706.572B	Fa0/2
172.16.31.2	Fa0	000C.85CC.1DA7	Fa0/1
172.16.31.3	Fa0	0060.7036.2849	Fa0/2
172.16.31.4	Gig0	0002.1640.8D75	Fa0/3

Objectives

Part 1: Examine an ARP Request

Part 2: Examine a Switch MAC Address Table

Part 3: Examine the ARP Process in Remote Communications

Background

This activity is optimized for viewing PDUs. The devices are already configured. You will gather PDU information in simulation mode and answer a series of questions about the data you collect.

Part 1: Examine an ARP Request

Step 1: Generate ARP requests by pinging 172.16.31.3 from 172.16.31.2.

a. Click **172.16.31.2** and open the **Command Prompt**.

b. Enter the **arp -d** command to clear the ARP table.

c. Enter **Simulation** mode and enter the command **ping 172.16.31.3**. Two PDUs will be generated. The **ping** command cannot complete the ICMP packet without knowing the MAC address of the destination. So the computer sends an ARP broadcast frame to find the MAC address of the destination.

d. Click **Capture/Forward** once. The ARP PDU moves **Switch1** while the ICMP PDU disappears, waiting for the ARP reply. Open the PDU and record the destination MAC address. Is this address listed in the table above? No

e. Click **Capture/Forward** to move the PDU to the next device. How many copies of the PDU did **Switch1** make? 3

f. What is the IP address of the device that accepted the PDU? 172.16.31.3

g. Open the PDU and examine Layer 2. What happened to the source and destination MAC addresses? Source became destination, FFFF.FFFF.FFFF turned into MAC address of 172.16.31.3

h. Click **Capture/Forward** until the PDU returns to **172.16.31.2**. How many copies of the PDU did the switch make during the ARP reply? 1

Step 2: Examine the ARP table.

a. Note that the ICMP packet reappears. Open the PDU and examine the MAC addresses. Do the MAC addresses of the source and destination align with their IP addresses? Yes

b. Switch back to **Realtime** and the ping completes.

c. Click **172.16.31.2** and enter the **arp –a** command. To what IP address does the MAC address entry correspond? 172.16.31.3

d. In general, when does an end device issue an ARP request? When it does not know the receiver's MAC address.

Part 2: Examine a Switch MAC Address Table

Step 1: Generate additional traffic to populate the switch MAC address table.

a. From **172.16.31.2**, enter the **ping 172.16.31.4** command.

b. Click **10.10.10.2** and open the **Command Prompt**.

c. Enter the **ping 10.10.10.3** command. How many replies were sent and received? 4 sent, 4 received.

Step 2: Examine the MAC address table on the switches.

a. Click **Switch1**and then the **CLI** tab. Enter the **show mac-address-table** command. Do the entries correspond to those in the table above? Yes

b. Click **Switch0**, then the **CLI** tab. Enter the **show mac-address-table** command. Do the entries correspond to those in the table above? Yes

c. Why are two MAC addresses associated with one port? Because both devices connect to one port through the Access Point.

Part 3: Examine the ARP Process in Remote Communications

Step 1: Generate traffic to produce ARP traffic.

a. Click **172.16.31.2** and open the **Command Prompt**.

b. Enter the **ping 10.10.10.1** command.

c. Type **arp –a**. What is the IP address of the new ARP table entry? 172.16.31.1

d. Enter **arp -d** to clear the ARP table and switch to **Simulation** mode.

e. Repeat the ping to 10.10.10.1. How many PDUs appear? 2

f. Click **Capture/Forward**. Click the PDU that is now at **Switch1**. What is the target destination IP destination address of the ARP request? 172.16.31.1

g. The destination IP address is not 10.10.10.1. Why? The gateway address of the router interface is stored in the IPv4 configuration of the hosts. If the receiving host is not on the same network, the source uses the ARP process to determine a MAC address for the router interface serving as the gateway.

Step 2: Examine the ARP table on Router1.

a. Switch to **Realtime** mode. Click **Router1** and then the **CLI** tab.

b. Enter privileged EXEC mode and then the **show mac-address-table** command. How many MAC addresses are in the table? Why? Zero, This command means something completely different than the switch command show mac address-table.

c. Enter the **show arp** command. Is there an entry for **172.16.31.2**? Yes

d. What happens to the first ping in a situation where the router responds to the ARP request? It times out.

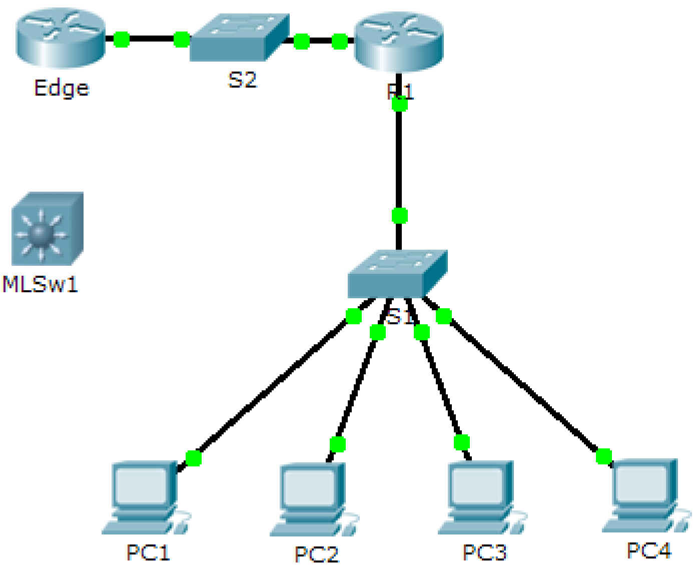
Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Examine an ARP Request	Step 1	10	
	Step 2	15	
	Part 1 Total	**25**	
Part 2: Examine a Switch MAC Address Table	Step 1	5	
	Step 2	20	
	Part 2 Total	**25**	
Part 3: Examine the ARP Process in Remote Communications	Step 1	25	
	Step 2	25	
	Part 3 Total	**50**	
	Total Score	**100**	

Packet Tracer - Configure Layer 3 Switches (Instructor Version)

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

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	G0/0	172.16.31.1	255.255.255.0
	G0/1	192.168.0.2	255.255.255.0
MLSw1	G0/1	192.168.0.2	255.255.255.0
	VLAN 1	172.16.31.1	255.255.255.0

Objectives

Part 1: Document the Current Network Configurations

Part 2: Configure, Deploy, and Test the New Multilayer Switch

Scenario

The Network Administrator is replacing the current router and switch with a new Layer 3 switch. As the Network Technician, it is your job to configure the switch and place it into service. You will be working after hours to minimize disruption to the business.

Note: This activity begins with a score of 8/100, because the device connections for the PCs are scored. You will delete and restore these connections in Part 2. The scoring is there to verify that you correctly restored the connections.

Part 1: Document the Current Network Configurations

Note: Normally a production router would have many more configurations than just interface IP addressing. However, to expedite this activity, only interface IP addressing is configured on **R1**.

a. Click **R1** and then the **CLI** tab.

b. Use the available commands to gather interface addressing information.

c. Document the information in the **Addressing Table**.

Part 2: Configure, Deploy, and Test the New Multilayer Switch

Step 1: Configure MLSw1 to use the addressing scheme from R1.

a. Click **MLSw1** and then the **CLI** tab.

b. Enter interface configuration mode for **GigabitEthernet 0/1**.

c. Change the port to routing mode by entering the **no switchport** command.

d. Configure the IP address to be the same as the address for **R1 GigabitEthernet 0/1** and activate the port.

e. Enter interface configuration mode for **interface VLAN1**.

f. Configure the IP address to be the same as the address for **R1 GigabitEthernet 0/0** and activate the port.

g. Save the configuration.

Step 2: Deploy the new multilayer switch and verify that connectivity is restored.

Note: The following steps would normally be done after hours or when traffic on the production network is at its lowest volume. To minimize downtime, the new equipment should be fully configured and ready to deploy.

a. Click an empty area of the screen to unselect all devices.

b. Use the **Delete** tool to remove all the connections, or simply delete **R1**, **S1**, and **S2**.

c. Select the appropriate cables to complete the following:

- Connect **MLSw1 GigabitEthernet 0/1** to the **Edge GigabitEthernet 0/0**.
- Connect the PCs to Fast Ethernet ports on **MLSw1**.

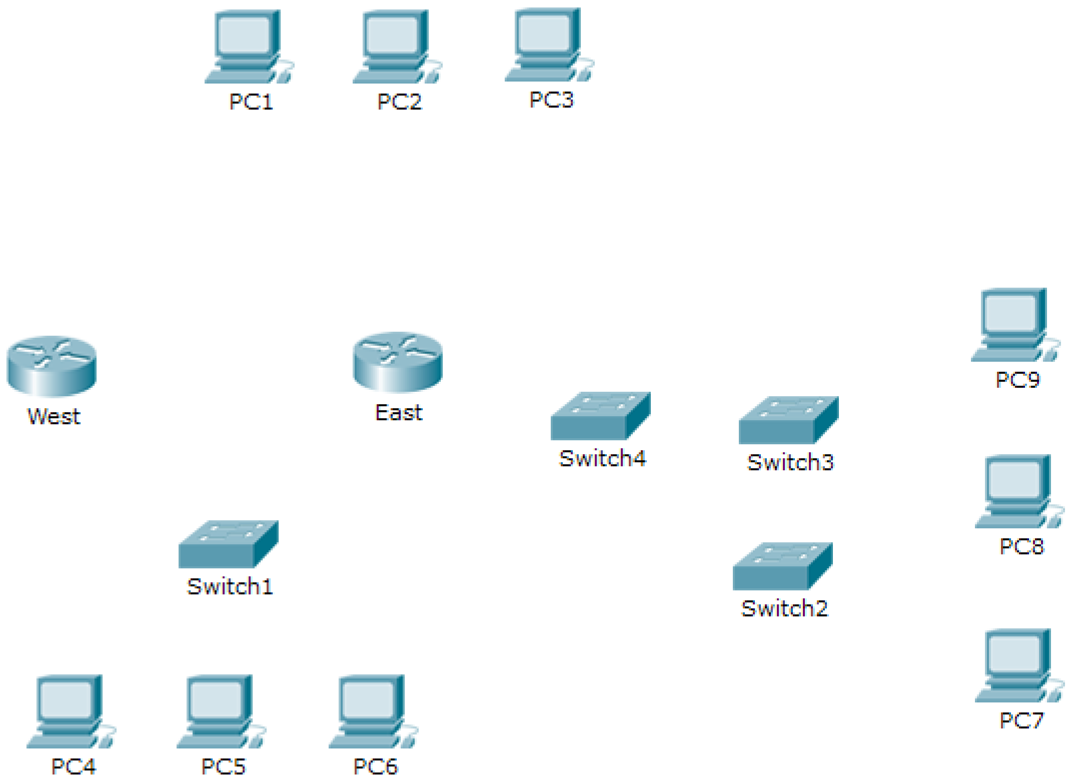
d. Verify the PCs can all ping **Edge** at 192.168.0.1.

Note: Wait until orange link lights turn green.

Packet Tracer - Exploring Internetworking Devices (Instructor Version)

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

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.

Part 1: Identify Physical Characteristics of Internetworking Devices

Step 1: Identify the management ports of a Cisco router.

a. Click the **East** router. The **Physical** tab should be active.

b. Zoom in and expand the window to see the entire router.

c. Which management ports are available? AUX and Console ports

Step 2: Identify the LAN and WAN interfaces of a Cisco router

a. Which LAN and WAN interfaces are available on the **East** router and how many are there? There are 2 WAN interfaces and 2 Gigabit Ethernet interfaces.

b. 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

c. Enter the following commands:

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

What is the default bandwidth of this interface? 1000000 Kbit

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

What is the default bandwidth of this interface? 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.

Step 3: Identify module expansion slots on switches.

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

b. Click **Switch2** or **Switch3.** How many expansion slots are available? They each have 5 slots available

Part 2: Select Correct Modules for Connectivity

Step 1: Determine which modules provide the required connectivity.

a. 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.

   1) 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 module

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

b. Click **Switch2**. Which module can you insert to provide a Gigabit optical connection to **Switch3**? PT-SWITCH-NM-1FGE

Step 2: Add the correct modules and power up devices.

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

b. 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.

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

d. 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

e. 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).

f. Use the appropriate command to verify that the new serial interfaces are installed.

Part 3: 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:

a. Select the appropriate cable type.

b. Click the first device and select the specified interface.

c. Click the second device and select the specified interface.

d. 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**	
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**	
	Packet Tracer Score	**52**	
	Total Score	**100**	

Packet Tracer - Configure Initial Router Settings (Instructor Version)

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

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.

Part 1: Verify the Default Router Configuration

Step 1: Establish a console connection to R1.

a. Choose a **Console** cable from the available connections.

b. Click **PCA** and select **RS 232.**

c. Click **R1** and select **Console.**

d. Click **PCA** > **Desktop** tab > **Terminal**.

e. Click **OK** and press **ENTER**. You are now able to configure **R1**.

Step 2: 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.

a. 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.

b. Enter the **show running-config** command:

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

c. 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

d. 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? It displays this message because the configuration file was not saved to NVRAM. Currently it is only located in RAM.

Part 2: 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.

Step 1: 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.

a. **R1** as the hostname.

b. Use the following passwords:

1) Console: **letmein**

2) Privileged EXEC, unencrypted: **cisco**

3) Privileged EXEC, encrypted: **itsasecret**

c. Encrypt all plain text passwords.

d. Message of the day text: `Unauthorized access is strictly prohibited.`

Note: The activity is configured with a regular expression to only check for the word "access" in the student's **banner motd** command.

Step 2: Verify the initial settings on R1.

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

b. Exit the current console session until you see the following message:

```
R1 con0 is now available


Press RETURN to get started.
```

c. 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? Every router should have a banner to warn unauthorized users that access is prohibited but can also be used for sending messages to network personnel/technicians (such as impending system shutdowns or who to contact for access).

If you are not prompted for a password, what console line command did you forget to configure? `R1(config-line)# login`

d. 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? The **enable secret** password overrides the enable password. If both are configured on the Router, you must enter the **enable secret** password to enter privileged EXEC mode.

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 command encrypts all current and future passwords.

Part 3: Save the Running Configuration File

Step 1: Save the configuration file to NVRAM.

a. 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? `copy running-config startup-config`

What is the shortest, unambiguous version of this command? `copy r s`

Which command displays the contents of the NVRAM? `show startup-configuration or show start`

b. 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.

Step 2: 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.

a. 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? Answers may vary, but two clues are the file length compared to the others and the .bin at the end of the file name

b. 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**.

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

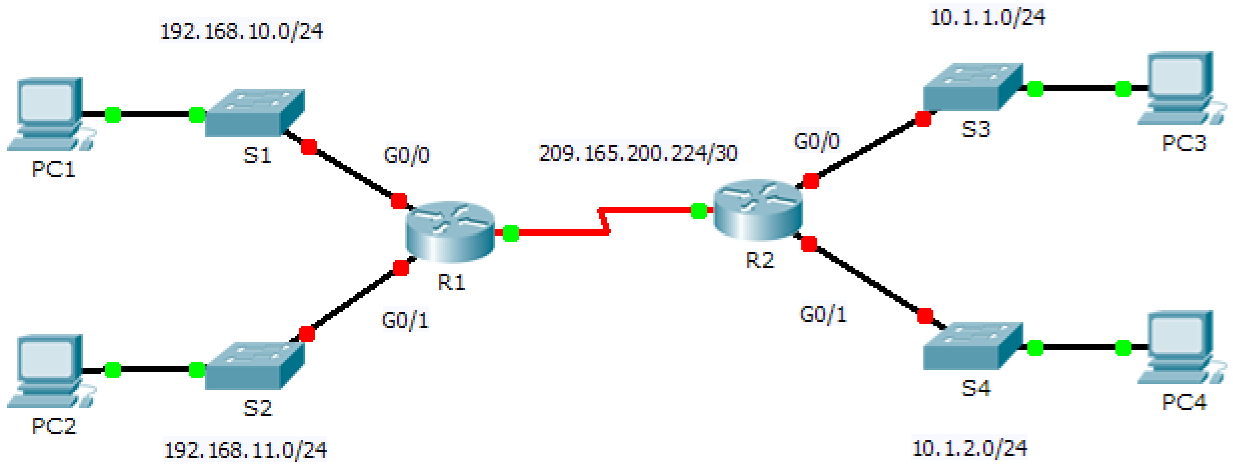
Suggested Scoring Rubric

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**	

Packet Tracer - Connect a Router to a LAN (Instructor Version)

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

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	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.

Note: The serial interfaces are already configured and active. In addition, routing is configured using EIGRP. This is done so that this activity is (1) consistent with examples shown in the chapter, (2) ready to provide complete output from **show** commands when the student configures and activates the Ethernet interfaces.

Part 1: Display Router Information

Step 1: 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**.

a. Which command displays the statistics for all interfaces configured on a router? `show` interfaces

b. Which command displays the information about the Serial 0/0/0 interface only? show interface serial 0/0/0

c. Enter the command to display the statistics for the Serial 0/0/0 interface on R1 and answer the following questions:

1) What is the IP address configured on **R1**? 209.165.200.225/30

2) What is the bandwidth on the Serial 0/0/0 interface? 1544 kbits

d. Enter the command to display the statistics for the GigabitEthernet 0/0 interface and answer the following questions:

1) What is the IP address on **R1**? There is no IP address configured on the GigabitEthernet 0/0 interface.

2) What is the MAC address of the GigabitEthernet 0/0 interface? 000d.bd6c.7d01

3) What is the bandwidth on the GigabitEthernet 0/0 interface? 1000000 kbits

Step 2: Display a summary list of the interfaces on R1.

a. Which command displays a brief summary of the current interfaces, statuses, and IP addresses assigned to them? show ip interface brief

b. Enter the command on each router and answer the following questions:

1) How many serial interfaces are there on **R1** and **R2**? Each router has 2 serial interfaces.

2) How many Ethernet interfaces are there on **R1** and **R2**? R1 has 6 Ethernet interfaces and R2 has 2 Ethernet interfaces.

3) Are all the Ethernet interfaces on **R1** the same? If no, explain the difference(s). No they are not. There are two Gigabit Ethernet interfaces and 4 Fast Ethernet interfaces. Gigabit Ethernet interfaces support speeds of up to 1,000,000,000 bits and Fast Ethernet interfaces support speeds of up to 1,000,000 bits.

Step 3: Display the routing table on R1.

a. What command displays the content of the routing table? show ip route

b. Enter the command on **R1** and answer the following questions:

1) How many connected routes are there (uses the C code)? 1

2) Which route is listed? 209.165.200.224/30

3) How does a router handle a packet destined for a network that is not listed in the routing table? A router will only send packets to a network listed in the routing table. If a network is not listed, the packet will be dropped.

Part 2: Configure Router Interfaces

Step 1: Configure the GigabitEthernet 0/0 interface on R1.

a. 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
```

b. 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
```

c. **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
```

Step 2: Configure the remaining Gigabit Ethernet Interfaces on R1 and R2.

a. Use the information in the Addressing Table to finish the interface configurations for **R1** and **R2**. For each interface, do the following:

1) Enter the IP address and activate the interface.

2) Configure an appropriate description.

b. Verify interface configurations.

Step 3: Back up the configurations to NVRAM.

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

Part 3: Verify the Configuration

Step 1: Use verification commands to check your interface configurations.

a. 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? 3 on each router

   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 run, show interfaces, show ip protocols`

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

   1) How many connected routes (uses the **C** code) do you see on each router? 3

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

   3) 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

   4) 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.

Step 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.
- From the command line on R2, ping PC2.

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

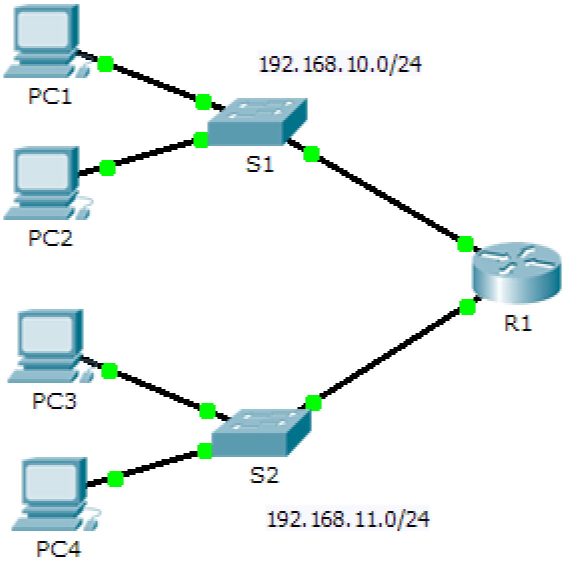
Suggested Scoring Rubric

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**	

Packet Tracer - Troubleshooting Default Gateway Issues
(Instructor Version)

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

Topology



Addressing Table

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

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:

1) Verify the network documentation and use tests to isolate problems.
2) Determine an appropriate solution for a given problem.
3) Implement the solution.
4) Test to verify the problem is resolved.
5) 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.

Part 1: 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.

Step 1: Verify the network documentation and isolate any problems.

a. 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.

b. 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.

c. 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.

Step 2: Determine an appropriate solution for the problem.

a. 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.

b. 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.

c. 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.

Part 2: 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.

Step 1: 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.

Step 2: Verify that the problem is now resolved.

a. Verify your solution has solved the problem by performing the test you used to identify the problem. For example, can PC1 now ping PC2?.

b. 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.

Step 3: Verify that all issues are resolved.

a. If you still have an outstanding issue with a solution that has not yet been implemented, return to Part 2, Step 1.

b. 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.

Issues

- PC1 cannot ping PC2 because PC1 has an IP address that does not belong to the network PC1 is attached to.
- Devices cannot ping S2 and S2 cannot ping any device because S2 is missing an IP address.
- Remote devices cannot ping PC4 because PC4 has the wrong default gateway configured.
- Remote devices cannot ping S1 because S1 is missing a default gateway configuration.

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**	

Cisco Networking Academy® Mind Wide Open™

Packet Tracer - Skills Integration Challenge

(Instructor Version)

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

Topology

You will receive one of three possible topologies.

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
[[R1Name]]	G0/0	[[R1G0Add]]	255.255.255.0 N/A	
	G0/1	[[R1G1Add]]	255.255.255.0 N/A	
[[S1Name]]	VLAN 1	[[S1Add]]	255.255.255.0	[[R1G0Add]]
[[S2Name]]	VLAN 1	[[S2Add]]	255.255.255.0	[[R1G1Add]]
[[PC1Name]]	NIC	[[PC1Add]]	255.255.255.0	[[R1G0Add]]
[[PC2Name]]	NIC	[[PC2Add]]	255.255.255.0	[[R1G0Add]]
[[PC3Name]]	NIC	[[PC3Add]]	255.255.255.0	[[R1G1Add]]
[[PC4Name]]	NIC	[[PC4Add]]	255.255.255.0	[[R1G1Add]]

Objectives

- Finish the network documentation.
- Perform basic device configurations on a router and a switch.
- Verify connectivity and troubleshoot any issues.

Scenario

Your network manager is impressed with your performance in your job as a LAN technician. She would like you to now demonstrate your ability to configure a router connecting two LANs. Your tasks include configuring basic settings on a router and a switch using the Cisco IOS. You will then verify your configurations, as well as configurations on existing devices by testing end-to-end connectivity.

Note: After completing this activity, you can choose to click the **Reset Activity** button to generate a new set of requirements. Variable aspects include device names, IP addressing schemes, and the topology.

Requirements

- Provide the missing information in the Addressing Table.
- Name the router **[[R1Name]]** and the second switch **[[S2Name]]**. You will not be able to access **[[S1Name]]**.
- Use **cisco** as the user EXEC password for all lines.
- Use **class** as the privileged EXEC password.
- Encrypt all plain text passwords.
- Configure an appropriate banner.

- Configure addressing for all devices according to the Addressing Table.
- Document interfaces with descriptions, including the **[[S2Name]]** VLAN 1 interface.
- Save your configurations.
- Verify connectivity between all devices. All devices should be able to ping any other device.
- Troubleshoot and document any issues.
- Implement the solutions necessary to enable and verify full end-to-end connectivity.

Note: Click **Check Results** button to see your progress. Click the **Reset Activity** button to generate a new set of requirements.

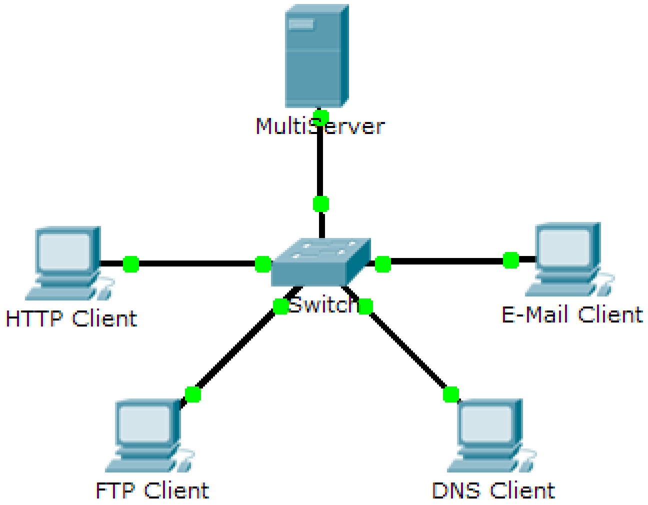
ID: [[indexNames]][[indexAdds]][[indexTopos]]

This activity is configured with an error that the student must correct before receiving full credit. The IP address on [[PC4Name]] is in the wrong subnet and does not match the IP address in the Addressing Table. The correct answers depend on the scenario the student received. The password to access Activity Wizard is **PT_ccna5**.

Packet Tracer Simulation - TCP and UDP Communications (Instructor Version)

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

Topology



Objectives

Part 1: Generate Network Traffic in Simulation Mode

Part 2: Examine the Functionality of the TCP and UDP Protocols

Background

This simulation activity is intended to provide a foundation for understanding the TCP and UDP in detail. Simulation mode provides the ability to view the functionality of the different protocols.

As data moves through the network, it is broken down into smaller pieces and identified in some fashion so that the pieces can be put back together. Each of these pieces is assigned a specific name (protocol data unit [PDU]) and associated with a specific layer. Packet Tracer Simulation mode enables the user to view each of the protocols and the associated PDU. The steps outlined below lead the user through the process of requesting services using various applications available on a client PC.

This activity provides an opportunity to explore the functionality of the TCP and UDP protocols, multiplexing and the function of port numbers in determining which local application requested the data or is sending the data.

Part 1: Generate Network Traffic in Simulation Mode

Step 1: Generate traffic to populate Address Resolution Protocol (ARP) tables.

Perform the following tasks task to reduce the amount of network traffic viewed in the simulation.

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

b. Enter the **ping 192.168.1.255** command. This will take a few seconds as every device on the network responds to **MultiServer**.

c. Close the **MultiServer** window.

Step 2: Generate web (HTTP) traffic.

a. Switch to Simulation mode.

b. Click **HTTP Client** and click the **Desktop** tab > **Web Browser**.

c. In the URL field, enter **192.168.1.254** and click **Go**. Envelopes (PDUs) will appear in the simulation window.

d. Minimize, but do not close, the **HTTP Client** configuration window.

Step 3: Generate FTP traffic.

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

b. Enter the **ftp 192.168.1.254** command. PDUs will appear in the simulation window.

c. Minimize, but do not close, the **FTP Client** configuration window.

Step 4: Generate DNS traffic.

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

b. Enter the **nslookup multiserver.pt.ptu** command. A PDU will appear in the simulation window.

c. Minimize, but do not close, the **DNS Client** configuration window.

Step 5: Generate Email traffic.

a. Click **E-Mail Client** and click the **Desktop** tab > **E Mail** tool.

b. Click **Compose** and enter the following information:

1) **To:** user@multiserver.pt.ptu

2) **Subject:** Personalize the subject line

3) **E-Mail Body:** Personalize the Email

c. Click **Send**.

d. Minimize, but do not close, the **E-Mail Client** configuration window.

Step 6: Verify that the traffic is generated and ready for simulation.

Every client computer should have PDUs listed in the Simulation Panel.

Part 2: Examine Functionality of the TCP and UDP Protocols

Step 1: Examine multiplexing as all of the traffic crosses the network.

You will now use the **Capture/Forward button** and the **Back** button in the Simulation Panel.

a. Click **Capture/Forward** once. All of the PDUs are transferred to the switch.

b. Click **Capture/Forward** again. Some of the PDUs disappear. What do you think happened to them?

They are stored in the switch.

c. Click **Capture/Forward** six times. All clients should have received a reply. Note that only one PDU can cross a wire in each direction at any given time. What is this called?

Multiplexing.

d. A variety of PDUs appears in the event list in the upper right pane of the simulation window. Why are they so many different colors?

They represent different protocols.

e. Click **Back** eight times. This should reset the simulation.

NOTE: Do not click **Reset Simulation** any time during this activity; if you do, you will need to repeat the steps in Part 1.

Step 2: Examine HTTP traffic as the clients communicate with the server.

a. Filter the traffic that is currently displayed to display only **HTTP** and **TCP** PDUs filter the traffic that is currently displayed:

1) Click **Edit Filters** and toggle the **Show All/None** check box.

2) Select **HTTP** and **TCP**. Click anywhere outside of the Edit Filters box to hide it. The Visible Events should now display only **HTTP** and **TCP** PDUs.

b. Click **Capture/Forward**. Hold your mouse above each PDU until you find one that originates from **HTTP Client**. Click the PDU envelope to open it.

c. Click the **Inbound PDU Details** tab and scroll down to the last section. What is the section labeled?

TCP

Are these communications considered to be reliable?

Yes.

d. Record the **SRC PORT**, **DEST PORT**, **SEQUENCE NUM**, and **ACK NUM** values. What is written in the field to the left of the **WINDOW** field?

1025 (could be different), 80, 0, 0 SYN

e. Close the PDU and click **Capture/Forward** until a PDU returns to the **HTTP Client** with a checkmark.

f. Click the PDU envelope and select **Inbound PDU Details**. How are the port and sequence numbers different than before?

80, 1025, 0, 1. SYN+ACK. The source and destination ports are reversed, and the acknowledgement number is 1. The SYN has changed to SYN+ACK.

g. There is a second **PDU** of a different color, which **HTTP Client** has prepared to send to **MultiServer**. This is the beginning of the HTTP communication. Click this second PDU envelope and select **Outbound PDU Details.**

h. What information is now listed in the TCP section? How are the port and sequence numbers different from the previous two PDUs?

1025, 80, 1, 1. PSH+ACK The source and destination ports are reversed, and both sequence and acknowledgement numbers are 1.

i. Click **Back** until the simulation is reset.

Step 3: Examine FTP traffic as the clients communicate with the server.

a. In the Simulation Panel, change **Edit Filters** to display only **FTP** and **TCP**.

b. Click **Capture/Forward**. Hold your cursor above each PDU until you find one that originates from **FTP Client**. Click that PDU envelope to open it.

c. Click the **Inbound PDU Details** tab and scroll down to the last section. What is the section labeled?

TCP

Are these communications considered to be reliable?

Yes.

d. Record the **SRC PORT**, **DEST PORT**, **SEQUENCE NUM**, and **ACK NUM** values. What is written in the field to the left of the **WINDOW** field?

1025, 21, 0, 0. SYN

e. Close the PDU and click **Capture/Forward** until a PDU returns to the **FTP Client** with a checkmark.

f. Click the PDU envelope and select **Inbound PDU Details**. How are the port and sequence numbers different than before?

21, 1025, 0, 1. SYN+ACK. The source and destination ports are reversed, and the acknowledgement number is 1.

g. Click the **Outbound PDU Details** tab. How are the port and sequence numbers different from the previous two results?

1025, 21, 1, 1. ACK. The source and destination ports are reversed, and both sequence and acknowledgement numbers are 1.

h. Close the PDU and click **Capture/Forward** until a second PDU returns to the **FTP Client**. The PDU is a different color.

i. Open the PDU and select **Inbound PDU Details**. Scroll down past the TCP section. What is the message from the server?

May say either “Username ok, need password” or “Welcome to PT Ftp server”

j. Click **Back** until the simulation is reset.

Step 4: Examine DNS traffic as the clients communicate with the server.

a. In the Simulation Panel, change **Edit Filters** to display only **DNS** and **UDP**.

b. Click the PDU envelope to open it.

c. Click the **Inbound PDU Details** tab and scroll down to the last section. What is the section labeled?

UDP

Are these communications considered to be reliable?

No

d. Record the **SRC PORT** and **DEST PORT** values. Why is there no sequence and acknowledgement number?

1025, 53. Because UDP does not need to establish a reliable connection.

e. Close the **PDU** and click **Capture/Forward** until a PDU returns to the **DNS Client** with a checkmark.

f. Click the PDU envelope and select **Inbound PDU Details**. How are the port and sequence numbers different than before?

53, 1025. The source and destination ports are reversed.

g. What is the last section of the **PDU** called?

DNS ANSWER.

h. Click **Back** until the simulation is reset.

Step 5: Examine email traffic as the clients communicate with the server.

a. In the Simulation Panel, change **Edit Filters** to display only **POP3, SMTP** and **TCP**.

b. Click **Capture/Forward**. Hold your cursor above each PDU until you find one that originates from **E-mail Client**. Click that PDU envelope to open it.

c. Click the **Inbound PDU Details** tab and scroll down to the last section. What transport layer protocol does email traffic use?

TCP

Are these communications considered to be reliable?

Yes.

d. Record the **SRC PORT**, **DEST PORT**, **SEQUENCE NUM**, and **ACK NUM** values. What is written in the field to the left of the **WINDOW** field?

1025, 25, 0, 0. SYN

e. Close the **PDU** and click **Capture/Forward** until a PDU returns to the **E-Mail Client** with a checkmark.

f. Click the PDU envelope and select **Inbound PDU Details**. How are the port and sequence numbers different than before?

25, 1025, 0, 1. SYN+ACK. The source and destination ports are reversed, and the acknowledgement number is 1.

g. Click the **Outbound PDU Details** tab. How are the port and sequence numbers different from the previous two results?

1025, 25, 1, 1. ACK. The source and destination ports are reversed, and both sequence and acknowledgement numbers are 1. ACK

h. There is a second **PDU** of a different color that **HTTP Client** has prepared to send to **MultiServer**. This is the beginning of the email communication. Click this second PDU envelope and select **Outbound PDU Details.**

i. How are the port and sequence numbers different from the previous two **PDU**s?

1025, 25, 1, 1. PSH+ACK. The source and destination ports are reversed, and both sequence and acknowledgement numbers are 1.

j. What email protocol is associated with TCP port 25? What protocol is associated with TCP port 110?

SMTP. POP3.

k. Click **Back** until the simulation is reset.

Step 6: Examine the use of port numbers from the server.

a. To see TCP active sessions, perform the following steps in quick succession:

1) Switch back to **Realtime** mode.

2) Click **MultiServer** and click the **Desktop** tab > **Command Prompt**.

b. Enter the **netstat** command. What protocols are listed in the left column? TCP

What port numbers are being used by the server? Answers will vary, but students may see all three: 21, 25, 80. They should certainly see 21

c. What states are the sessions in?

Answer will vary. Possible states include CLOSED, ESTABLISHED, LAST_ACK

d. Repeat the **netstat** command several times until you see only one session still ESTABLISHED. For which service is this connection still open? FTP

Why doesn’t this session close like the other three? (Hint: Check the minimized clients)

The server is waiting for a password from the client.

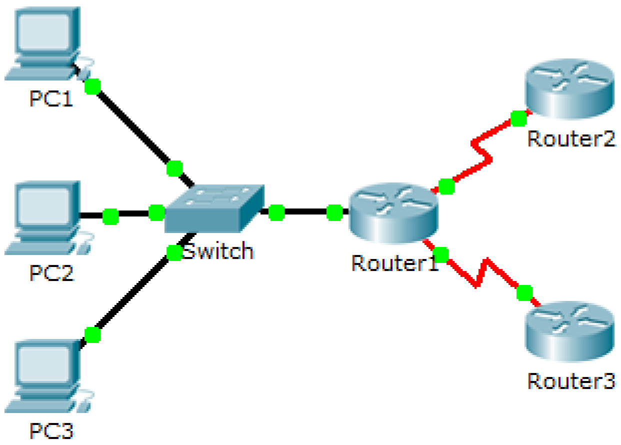
Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 2: Examine Functionality of the TCP and UDP Protocols	Step 1	15	
	Step 2	15	
	Step 3	15	
	Step 4	15	
	Step 5	15	
	Step 6	25	
	Total Score	**100**	

Packet Tracer - Investigate Unicast, Broadcast, and Multicast Traffic (Instructor Version)

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

Topology



Objectives

Part 1: Generate Unicast Traffic

Part 2: Generate Broadcast Traffic

Part 3: Investigate Multicast Traffic

Background/Scenario

This activity will examine unicast, broadcast, and multicast behavior. Most traffic in a network is unicast. When a PC sends an ICMP echo request to a remote router, the source address in the IP packet header is the IP address of the sending PC. The destination address in the IP packet header is the IP address of the interface on the remote router. The packet is sent only to the intended destination.

Using the **ping** command or the Add Complex PDU feature of Packet Tracer, you can directly ping broadcast addresses to view broadcast traffic.

For multicast traffic, you will view EIGRP traffic. EIGRP is used by Cisco routers to exchange routing information between routers. Routers using EIGRP send packets to multicast address 224.0.0.10, which represents the group of EIGRP routers. Although these packets are received by other devices, they are dropped at Layer 3 by all devices except EIGRP routers, with no other processing required.

Part 1: Generate Unicast Traffic

Step 1: Use ping to generate traffic.

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

b. Enter the **ping 10.0.3.2** command. The ping should succeed.

Step 2: Enter Simulation mode.

a. Click the **Simulation** tab to enter Simulation mode.

b. Click **Edit Filters** and verify that only ICMP and EIGRP events are selected.

c. Click **PC1** and enter the **ping 10.0.3.2** command.

Step 3: Examine unicast traffic.

The PDU at **PC1** is an ICMP echo request intended for the serial interface on **Router3**.

a. Click **Capture/Forward** repeatedly and watch while the echo request is sent to **Router3** and the echo reply is sent back to **PC1**. Stop when the first echo reply reaches PC1.

Which devices did the packet travel through with the unicast transmission?

From PC1 to Switch1 to Router1 to Router3 and back.

b. In the Simulation Panel Event List section, the last column contains a colored box that provides access to detailed information about an event. Click the colored box in the last column for the first event. The PDU Information window opens.

What layer does this transmission start at and why?

Layer 3, because it is dealing specifically with IP and ICMP

c. Examine the Layer 3 information for all of the events. Notice that both the source and destination IP addresses are unicast addresses that refer to PC1 and the serial interface on Router3.

What two changes take place at Layer 3 when the packet arrives at Router3?

The source and destination IP addresses are flipped and the ICMP message type is now 0.

d. Click **Reset Simulation**.

Part 2: Generate Broadcast Traffic

Step 1: Add a complex PDU.

a. Click **Add Complex PDU**. The icon for this is in the right toolbar and shows an open envelope.

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

c. Click **PC1** to serve as the source for this test message and the **Create Complex PDU** dialog window opens. Enter the following values:

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

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

DNS, FINGER, FTP, HTTP, HTTPS, IMAP, NETBIOS, PING, POP3, SFTP, SMTP, SNMP, SSH, TELNET, TFTP and OTHER

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

e. Click **Capture/Forward** twice. This packet is sent to the switch and then broadcasted to **PC2**, **PC3**, and **Router1**. Examine the Layer 3 information for all of the events. Notice that the destination IP address is 255.255.255.255, which is the IP broadcast address you configured when you created the complex PDU.

Analyzing the OSI Model information, what changes occur in the Layer 3 information of the Out Layers column at Router1, PC2, and PC3?

The PDU becomes a unicast replying back to PC1.

f. Click **Capture/Forward** again. Does the broadcast PDU ever forward on to Router2 or Router3? Why?

No. The limited broadcast should remain within the local network unless the router is set to forward.

g. After you are done examining the broadcast behavior, delete the test packet by clicking **Delete** below **Scenario 0**.

Part 3: Investigate Multicast Traffic

Step 1: Examine the traffic generated by routing protocols.

a. Click **Capture/Forward**. EIGRP packets are at Router1 waiting to be multicast out of each interface.

b. Examine the contents of these packets by opening the PDU Information window and click **Capture/Forward** again. The packets are sent to the two other routers and the switch. The routers accept and process the packets, because they are part of the multicast group. The switch will forward the packets to the PCs.

c. Click **Capture/Forward** until you see the EIGRP packet arrive at the PCs.

What do the hosts do with the packets?

The hosts reject and drop the packets.

Examine the Layer 3 and Layer 4 information for all of the EIGRP events.

What is the destination address of each of the packets?

224.0.0.10, the IP multicast address for the EIGRP routing protocol.

d. Click one of the packets delivered to one of the PCs. What happens to those packets?

The packets are dropped and no additional processing is done.

Based on the traffic generated by the three types of IP packets, what are the major differences in delivery?

The unicast packet moves through the network destined for a specific device, the broadcast gets sent to every device in the local area network and the multicast is sent to all devices but only processed by those that are part of the multicast group.

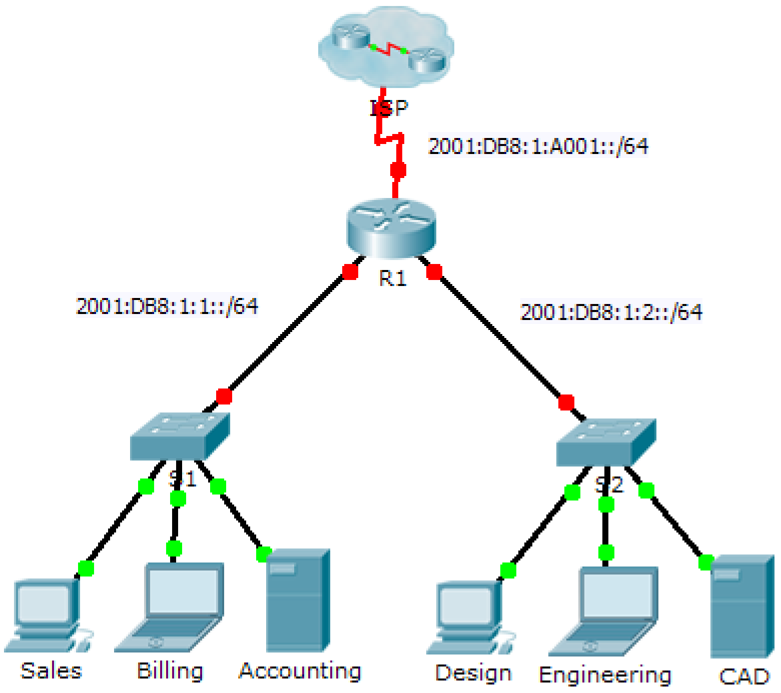
Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Unicast Traffic	Step 3a	10	
	Step 3b	10	
	Step 3c	10	
	Part 1 Total	**30**	
Part 2: Broadcast traffic	Step 1c	10	
	Step 1e	10	
	Step 1f	10	
	Part 2 Total	**30**	
Part 3: Multicast traffic	Step 1c,q1	10	
	Step 1c, q2	10	
	Step 1d, q1	10	
	Step 1d, q2	10	
	Part 3 Total	**40**	
	Total Score	**100**	

Packet Tracer - Configuring IPv6 Addressing (Instructor Version)

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

Topology



Addressing Table

Device	Interface	IPv6 Address/Prefix	Default Gateway
R1	G0/0	2001:DB8:1:1::1/64	N/A
	G0/1	2001:DB8:1:2::1/64	N/A
	S0/0/0	2001:DB8:1:A001::2/64	N/A
	Link-local	FE80::1	N/A
Sales	NIC	2001:DB8:1:1::2/64	FE80::1
Billing	NIC	2001:DB8:1:1::3/64	FE80::1
Accounting	NIC	2001:DB8:1:1::4/64	FE80::1
Design	NIC	2001:DB8:1:2::2/64	FE80::1
Engineering	NIC	2001:DB8:1:2::3/64	FE80::1
CAD	NIC	2001:DB8:1:2::4/64	FE80::1

Objectives

Part 1: Configure IPv6 Addressing on the Router

Part 2: Configure IPv6 Addressing on Servers

Part 3: Configure IPv6 Addressing on Clients

Part 4: Test and Verify Network Connectivity

Background

In this activity, you will practice configuring IPv6 addresses on a router, servers, and clients. You will also practice verifying your IPv6 addressing implementation.

Part 1: Configure IPv6 Addressing on the Router

Step 1: Enable the router to forward IPv6 packets.

a. Enter the ipv6 unicast-routing global configuration command. This command must be configured to enable the router to forward IPv6 packets. This command will be discussed in a later semester.

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

Step 2: Configure IPv6 addressing on GigabitEthernet0/0.

a. Click **R1** and then the **CLI** tab. Press **Enter**.

b. Enter privileged EXEC mode.

c. Enter the commands necessary to transition to interface configuration mode for GigabitEthernet0/0.

d. Configure the IPv6 address with the following command:

```
R1(config-if)# ipv6 address 2001:DB8:1:1::1/64
```

e. Configure the link-local IPv6 address with the following command:

```
R1(config-if)# ipv6 address FE80::1 link-local
```

f. Activate the interface.

Step 3: Configure IPv6 addressing on GigabitEthernet0/1.

a. Enter the commands necessary to transition to interface configuration mode for GigabitEthernet0/1.

b. Refer to the **Addressing Table** to obtain the correct IPv6 address.

c. Configure the IPv6 address, the link-local address and activate the interface.

Step 4: Configure IPv6 addressing on Serial0/0/0.

a. Enter the commands necessary to transition to interface configuration mode for Serial0/0/0.

b. Refer to the **Addressing Table** to obtain the correct IPv6 address.

c. Configure the IPv6 address, the link-local and activate the interface.

Part 2: Configure IPv6 Addressing on the Servers

Step 1: Configure IPv6 addressing on the Accounting Server.

a. Click **Accounting** and click the **Desktop** tab > **IP Configuration**.

b. Set the **IPv6 Address** to **2001:DB8:1:1::4** with a prefix of **/64**.

c. Set the **IPv6 Gateway** to the link-local address, **FE80::1**.

Step 2: Configure IPv6 addressing on the CAD Server.

Repeat Steps 1a to 1c for the **CAD** server. Refer to the **Addressing Table** for the IPv6 address.

Part 3: Configure IPv6 Addressing on the Clients

Step 1: Configure IPv6 addressing on the Sales and Billing Clients.

a. Click **Billing** and then select the **Desktop** tab followed by **IP Configuration**.

b. Set the **IPv6 Address** to **2001:DB8:1:1::3** with a prefix of **/64**.

c. Set the **IPv6 Gateway** to the link-local address, **FE80::1**.

d. Repeat Steps 1a through 1c for **Sales**. Refer to the **Addressing Table** for the IPv6 address.

Step 2: Configure IPv6 Addressing on the Engineering and Design Clients.

a. Click **Engineering** and then select the **Desktop** tab followed by **IP Configuration**.

b. Set the **IPv6 Address** to **2001:DB8:1:2::3** with a prefix of **/64**.

c. Set the **IPv6 Gateway** to the link-local address, **FE80::1**.

d. Repeat Steps 1a through 1c for **Design**. Refer to the **Addressing Table** for the IPv6 address.

Part 4: Test and Verify Network Connectivity

Step 1: Open the server web pages from the clients.

a. Click **Sales** and click the **Desktop** tab. Close the **IP Configuration** window, if necessary.

b. Click **Web Browser**. Enter **2001:DB8:1:1::4** in the URL box and click **Go**. The **Accounting** website should appear.

c. Enter **2001:DB8:1:2::4** in the URL box and click **Go**. The **CAD** website should appear.

d. Repeat steps 1a through 1d for the rest of the clients.

Step 2: Ping the ISP.

a. Open any client computer configuration window by clicking the icon.

b. Click the **Desktop** tab > **Command Prompt**.

c. Test connectivity to the ISP by entering the following command:

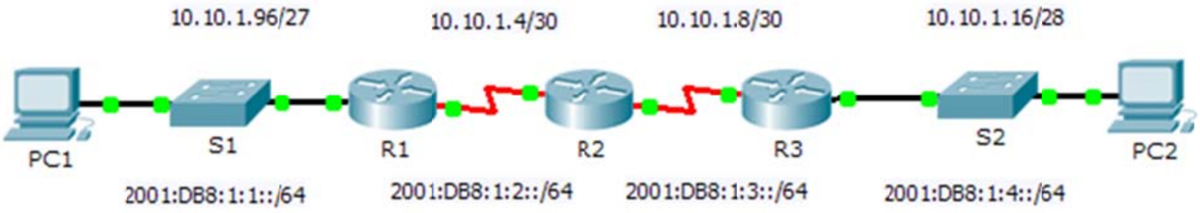
```
PC> ping 2001:DB8:1:A001::1
```

d. Repeat the **ping** command with other clients until full connectivity is verified.

Packet Tracer - Verifying IPv4 and IPv6 Addressing (Instructor Version)

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

Topology



Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
		IPv6 Address/Prefix		
R1	G0/0	10.10.1.97	255.255.255.224	N/A
		2001:DB8:1:1::1/64 N/A		
	S0/0/1	10.10.1.6 255.25	5.255.252	N/A
		2001:DB8:1:2::2/64 N/A		
	Link-local FE80::1			N/A
R2	S0/0/0	10.10.1.5 255.25	5.255.252	N/A
		2001:DB8:1:2::1/64 N/A		
	S0/0/1	10.10.1.9 255.25	5.255.252	N/A
		2001:DB8:1:3::1/64 N/A		
	Link-local FE80::2			N/A
R3	G0/0	10.10.1.17 255.25	5.255.240	N/A
		2001:DB8:1:4::1/64		N/A
	S0/0/1	10.10.1.10 255.25	5.255.252	N/A
		2001:DB8:1:3::2/64 N/A		
	Link-local FE80::3			N/A
PC1 NIC		10.10.1.100 255.25	5.255.224	10.10.1.97
		2001:DB8:1:1::A/64 FE80::1		
PC2 NIC		10.10.1.20 255.25	5.255.240	10.10.1.17
		2001:DB8:1:4::A/64 FE80::3		

Objectives

Part 1: Complete the Addressing Table Documentation

Part 2: Test Connectivity Using Ping

Part 3: Discover the Path by Tracing the Route

Background

Dual-stack allows IPv4 and IPv6 to coexist on the same network. In this activity, you will investigate a dual-stack implementation including documenting the IPv4 and IPv6 configuration for end devices, testing connectivity for both IPv4 and IPv6 using **ping**, and tracing the path from end to end for IPv4 and IPv6.

Part 1: Complete the Addressing Table Documentation

Step 1: Use ipconfig to verify IPv4 addressing.

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

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

c. Clic k **PC2** and click the **Desktop** tab > **Command Prompt.**

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

Step 2: Use ipv6config to verify IPv6 addressing.

a. On **PC1**, enter the **ipv6config /all** command to collect the IPv6 information. Fill in the **Addressing Table** with the IPv6 address, subnet prefix, and default gateway.

b. On **PC2**, enter the **ipv6config /all** command to collect the IPv6 information. Fill in the **Addressing Table** with the IPv6 address, subnet prefix, and default gateway.

Part 2: Test Connectivity Using Ping

Step 1: Use ping to verify IPv4 connectivity.

a. From **PC1**, ping the IPv4 address for **PC2**. Was the result successful? Yes

b. From **PC2**, ping the IPv4 address for **PC1**. Was the result successful? Yes

Step 2: Use ping to verify IPv6 connectivity.

a. From **PC1**, ping the IPv6 address for **PC2**. Was the result successful? Yes

b. From **PC2**, ping the IPv6 address of **PC1**. Was the result successful? Yes

Part 3: Discover the Path by Tracing the Route

Step 1: Use tracert to discover the IPv4 path.

a. From **PC1**, trace the route to **PC2**.

```
PC> tracert 10.10.1.20
```

What addresses were encountered along the path? 10.10.1.97, 10.10.1.5, 10.10.1.10, 10.10.1.20

With which interfaces are the four addresses associated? G0/0 of R1, S0/0/0 on R2, S0/0/01 on R3, NIC of PC2

b. From **PC2**, trace the route to **PC1**.

What addresses were encountered along the path? 10.10.1.17, 10.10.1.9, 10.10.1.6, 10.10.1.100

With which interfaces are the four addresses associated? G0/0 of R3, S0/0/1 of R2, S0/0/1 of R1, NIC of PC1

Step 2: Use tracert to discover the IPv6 path.

a. From **PC1**, trace the route to the IPv6 address for **PC2**.

```
PC> tracert 2001:DB8:1:4::A
```

What addresses were encountered along the path? 2001:DB8:1:1::1, 2001:DB8:1:2::1, 2001:DB8:1:3::2, 2001:DB8:1:4::A

With which interfaces are the four addresses associated? g0/0 of R1, S0/0/0 of r2, S0/0/1 of R3, NIC of PC2

b. From **PC2**, trace the route to the IPv6 address for **PC1**.

What addresses were encountered along the path? 2001:DB8:1:4::1, 2001:DB8:1:3::1, 2001:DB8:1:2::2, 2001:DB8:1:1::A

With which interfaces are the four addresses associated? Ga0/0 of R3, S0/0/1 of R2, S0/0/1 of R1, NIC of PC1

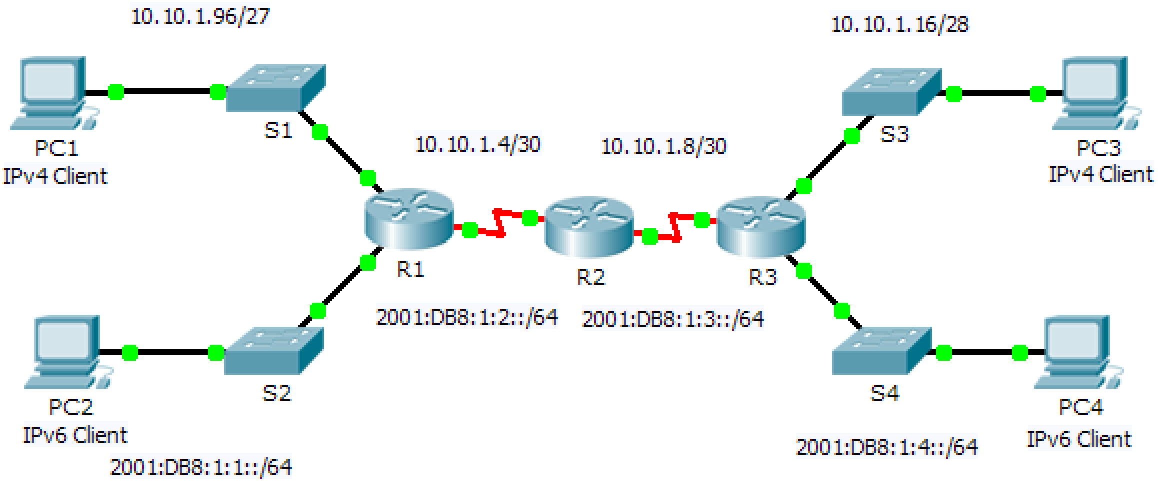
Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Complete the Addressing Table Documentation	Step 1b	10	
	Step 1d	10	
	Step 2a	10	
	Step 2b	10	
	Part 1 Total	**40**	
Part 2: Test Connectivity Using Ping	Step 1a	7	
	Step 1b	7	
	Step 2a	7	
	Step 2b	7	
	Part 2 Total	**28**	
Part 3: Discover the Path by Tracing the Route	Step 1a	8	
	Step 1b	8	
	Step 2a	8	
	Step 2b	8	
	Part 3 Total	**32**	
	Total Score	**100**	

Packet Tracer - Pinging and Tracing to Test the Path (Instructor Version)

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

Topology



Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
		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::2/64		FE80::1
PC3	NIC	10.10.1.18	255.255.255.240	10.10.1.17
PC4	NIC	2001:DB8:1:4::2/64		FE80::1

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**.

Part 1: Test and Restore IPv4 Connectivity

Step 1: 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.

Step 2: 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? 10.10.1.6/32, 10.10.1.4/30

h. Repeat step 2e to 2g with **R3** and 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.

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

Step 3: 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's Serial 0/0/0 interface is configured with the wrong IP address.

b. What solution would you propose to correct the problem? Configure the correct IP address on R2's Serial 0/0/0 interface (10.10.1.5)

Step 4: Implement the plan.

Implement the solution you proposed in Step 3b.

Step 5: Verify that connectivity is restored.

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

b. From **PC3** test connectivity to **PC1**. Is the problem resolved? Yes

Step 6: Document the solution.

Part 2: Test and Restore IPv6 Connectivity

Step 1: 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.

Step 2: 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 IPv6 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.

Step 3: 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 is using the wrong default gateway configuration.

b. What solution would you propose to correct the problem? Configure PC4 with the correct default gateway address: FE80::3.

Step 4: Implement the plan.

Implement the solution you proposed in Step 3b.

Step 5: Verify that connectivity is restored.

a. From **PC2** test connectivity to **PC4**.

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

Step 6: Document the solution.

Suggested Scoring Rubric

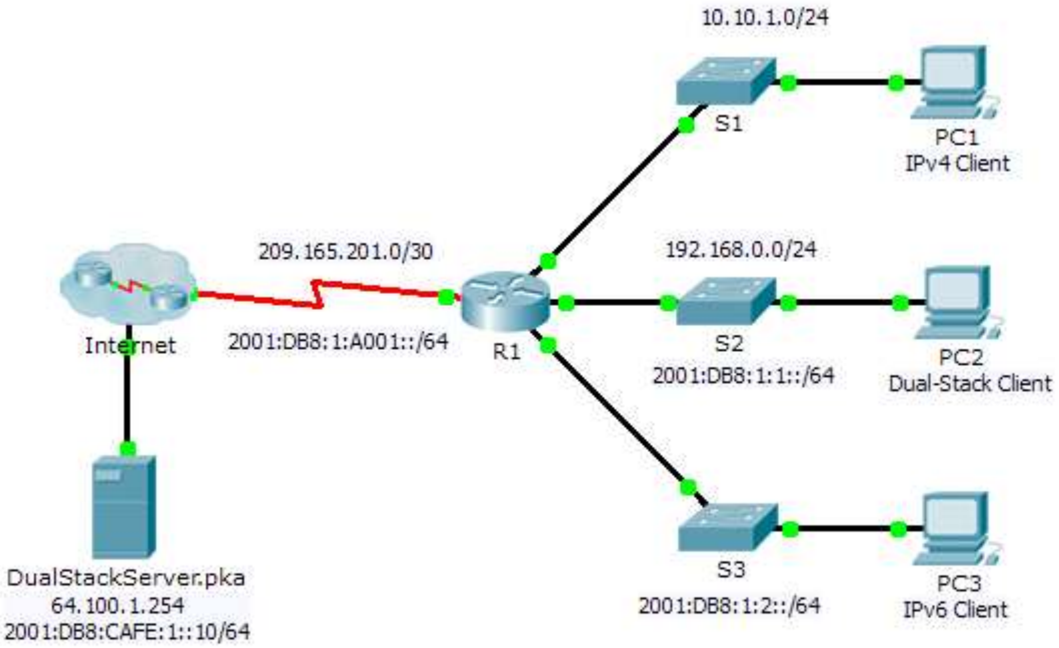
Activity Section	Question Location	Possible Points	Earned Points
Part 1: Test and Restore Connectivity Between PC1 and PC3	Step 1b	5	
	Step 1d	5	
	Step 2a	5	
	Step 2c	5	
	Step 2f	5	
	Step 2g	5	
	Step 2h	5	
	Step 3a	5	
	Step 3b	5	
	Part 1 Total	**45**	
Part 2: Test and Restore Connectivity Between PC2 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**	

Packet Tracer - Troubleshooting IPv4 and IPv6 Addressing

(Instructor Version)

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

Topology



Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
		IPv6 Address/Prefix		
R1	G0/0	10.10.1.1	255.255.255.0	N/A
	Ga0/1	192.168.0.1	255.255.255.0	N/A
		2001:DB8:1:1::1/64		N/A
	G0/2	2001:DB8:1:2::1/64		N/A
	S0/0/0	209.165.201.2	255.255.255.252	N/A
		2001:DB8:1:A001::2/64		N/A
	Link-local	FE80::1		N/A
Dual Stack Server	NIC	64.100.1.254	255.255.255.0	64.100.1.1
		2001:DB8:CAFE:1::10/64		FE80::A
DNS Server	NIC	64.100.1.254	255.255.255.0	64.100.1.1
		2001:DB8:CAFE:1::10/64		FE80::A
PC1	NIC	10.10.1.2	255.255.255.0	10.10.1.1
PC2	NIC	192.168.0.2	255.255.255.0	192.168.0.1
		2001:DB8:1:1::2/64		FE80::1
PC3	NIC	2001:DB8:1:2::2/64		FE80::1

Objectives

Part 1: Troubleshoot First Issue

Part 2: Troubleshoot Second Issue

Part 3: Troubleshoot Third Issue

Scenario

You are a network technician working for a company that has decided to migrate from IPv4 to IPv6. In the interim, they must support both protocols (dual-stack). Three co-workers have called the help desk with problems and have received limited assistance. The help desk has escalated the matter to you, a Level 2 support technician. Your job is to locate the source of the problems and implement appropriate solutions.

Part 1: Troubleshoot First Issue

A customer using **PC1** complains that she cannot access the **dualstackserver.pka** web page.

Step 1: Verify a detailed help desk ticket.

The help desk collected the following information from the customer, over the phone. Verify that it is correct.

Help Desk Ticket	
Client Identifier: PC1	
Issue: Unable to access the dualstackserver.pka web page.	
Detailed information about the issue	
Test: Does the computer have an IP address using **ipconfig**?	Yes
Test: Can the computer contact its gateway using **ping**?	Yes
Test: Can the computer contact the server using **tracert**?	Yes
Test: Can the computer contact the server using **nslookup**?	No
Resolution: Escalate to Level 2 support.	

Step 2: Consider probable causes for the failure.

a. Note the tests that have been conducted. If possible, discuss possible scenarios that would create this situation with your fellow network technicians (classmates).

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

Step 3: Propose a solution to solve the problem.

Make a list of things that could be changed to solve this problem. Start with the solution that is most likely to work.

Step 4: Implement the plan.

Try the most likely solution from the list. If it has already been tried, move on to the next solution.

Step 5: Verify the solution resolved the problem.

a. Repeat the tests from the help desk ticket. Did it solve the problem?

b. If the problem still exists, reverse the change if you are not sure it is correct and return to Step 4.

Step 6: Document the solution.

Record the solution to the problem. If you ever encounter the same problem again, your notes will be very valuable. PC1 IPv4 DNS address is incorrect.

Part 2: Troubleshoot Second Issue

A customer using PC2 complains that he cannot access files on the **DualStackServer.pka** at 2001:DB8:CAFE:1::10.

Step 1: Verify a detailed help desk ticket.

The help desk collected the following information from the customer, over the phone. Verify that it is correct.

Help Desk Ticket	
Client Identifier: PC2	
Issue: Unable to access the FTP service of 2001:DB8:CAFE:1:10.	
Detail information about the Issue	
Test: Does the computer have an IPv6 address using **ipv6config**?	Yes
Test: Can the computer contact its gateway using **ping**?	Yes
Test: Can the computer contact the server using **tracert**?	No
Resolution: Escalate to Level 2 support.	

Step 2: Complete Steps 2 to 5 from Part 1 for this problem.

Step 3: Document the solution.

Record the solution to the problem. If you ever encounter the same problem again, your notes will be very valuable. DualStackServer.pka IPv6 gateway address is incorrect

Part 3: Troubleshoot Third Issue

A customer using **PC3** complains that he cannot communicate with **PC2.**

Step 1: Verify a detailed help desk ticket.

The help desk collected the following information from the user over the phone. Verify that it is correct.

Help Desk Ticket	
Client Identifier: PC3	
Issue: Unable to communicate with PC2.	
Detail information about the Issue	
Test: Does the computer have an IP address using **ipconfig**?	Yes
Test: Does computer have an IPv6 address using **ipv6config**?	Yes
Test: Can the computer contact its IPv4 gateway using **ping**?	No
Test: Can the computer contact its IPv6 gateway using **ping**?	Yes
Test: Can the computer contact the IPv4 client using **tracert**?	No
Test: Can the computer contact the IPv6 client using **tracert**?	Yes
Resolution: Escalate to Level 2 support.	

Step 2: Complete Steps 2 to 5 from Part 1 for this problem.

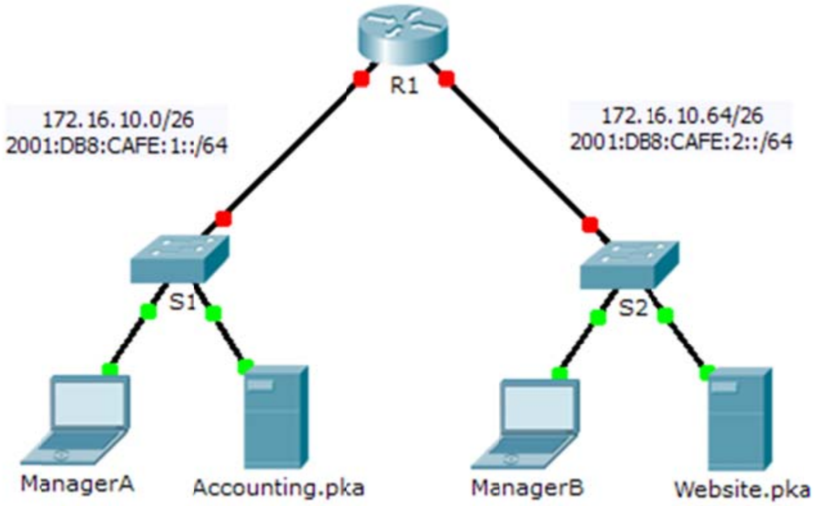
Step 3: Document the solution.

Record the solution to the problem. If you ever encounter the same problem again, your notes will be very valuable. PC2 IPv4 gateway address is incorrect

Packet Tracer - Skills Integration Challenge (Instructor Version)

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

Topology



Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
		IPv6 Address/Prefix		
R1	G0/0	172.16.10.1 255.25	5.255.192	N/A
		2001:DB8:CAFE:1::1/64 N/A		
	G0/1	172.16.10.65 255.	25 5.255.192	N/A
		2001:DB8:CAFE:2::1/64 N/A		
	Link-local	FE80::1		N/A
S1 VLAN1		172.16.10.62	255.255.255.192	172.16.10.1
S2 VLAN1		172.16.10.126	255.255.255.192	172.16.10.65
ManagerA NIC		172.16.10.3 255.25	5.255.192	172.16.10.1
		2001:DB8:CAFE:1::3/64		FE80::1
Accounting.pka NIC		172.16.10.2 255.25	5.255.192	172.16.10.1
		2001:DB8:CAFE:1::2/64		FE80::1
ManagerB NIC		172.16.10.67 255.	25 5.255.192	172.16.10.65
		2001:DB8:CAFE:2::3/64		FE80::1
Website.pka N	IC	172.16.10.66 255.	25 5.255.192	172.16.10.65
		2001:DB8:CAFE:2::2/64		FE80::1

Scenario

Your company has won a contract to set up a small network for a restaurant owner. There are two restaurants near each other, and they all share one connection. The equipment and cabling is installed and the network administrator has designed the implementation plan. Your job is to implement the rest of the addressing scheme according to the abbreviated Addressing Table and verify connectivity.

Requirements

- Complete the **Addressing Table** documentation.
- Configure **R1** with IPv4 and IPv6 addressing.
- Configure **S1** with IPv4 addressing. **S2** is already configured.
- Configure **ManagerA** with IPv4 and IPv6 addressing. The rest of the clients are already configured.
- Verify connectivity. All clients should be able to ping each other and access the websites on **Accounting.pka** and **Website.pka**.

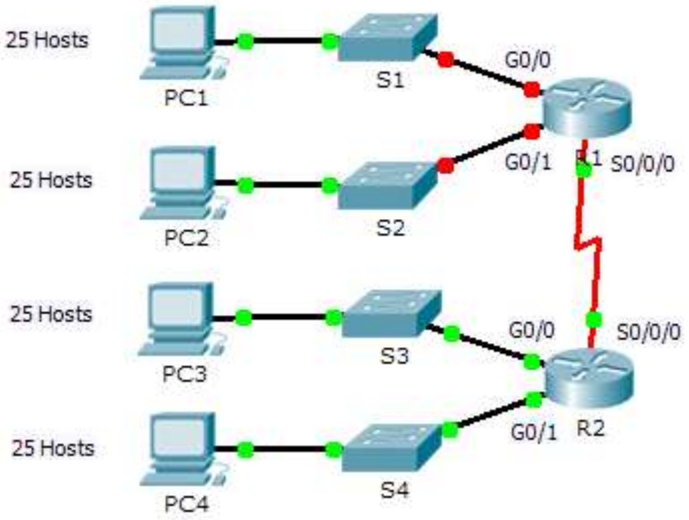
Suggested Scoring Rubric

Packet Tracer scores 80 points. Completing the **Addressing Table** is worth 20 points.

Packet Tracer - Subnetting Scenario 1 (Instructor Version)

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

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.100.1	255.255.255.224	N/A
	G0/1	192.168.100.33	255.255.255.224	N/A
	S0/0/0	192.168.100.129	255.255.255.224	N/A
R2	G0/0	192.168.100.65	255.255.255.224	N/A
	G0/1	192.168.100.97	255.255.255.224	N/A
	S0/0/0	192.168.100.158	255.255.255.224	N/A
S1	VLAN 1	192.168.100.2	255.255.255.224	192.168.100.1
S2	VLAN 1	192.168.100.34	255.255.255.224	192.168.100.33
S3	VLAN 1	192.168.100.66	255.255.255.224	192.168.100.65
S4	VLAN 1	192.168.100.98	255.255.255.224	192.168.100.97
PC1	NIC	192.168.100.30	255.255.255.224	192.168.100.1
PC2	NIC	192.168.100.62	255.255.255.224	192.168.100.33
PC3	NIC	192.168.100.94	255.255.255.224	192.168.100.65
PC4	NIC	192.168.100.126	255.255.255.224	192.168.100.97

Objectives

Part 1: Design an IP Addressing Scheme

Part 2: Assign IP Addresses to Network Devices and Verify Connectivity

Scenario

In this activity, you are given the network address of 192.168.100.0/24 to subnet and provide the IP addressing for the network shown in the topology. Each LAN in the network requires enough space for, at least, 25 addresses for end devices, the switch and the router. The connection between R1 to R2 will require an IP address for each end of the link.

Part 1: Design an IP Addressing Scheme

Step 1: Subnet the 192.168.100.0/24 network into the appropriate number of subnets.

a. Based on the topology, how many subnets are needed? 5

b. How many bits must be borrowed to support the number of subnets in the topology table? 3

c. How many subnets does this create? 8

d. How many usable hosts does this create per subnet? 30

Note: If your answer is less than the 25 hosts required, then you borrowed too many bits.

e. Calculate the binary value for the first five subnets. The first subnet is already shown.

```
Net 0: 192 . 168 . 100 .  0   0   0   0   0   0   0   0
Net 1: 192 . 168 . 100 . ___ ___ ___ ___ ___ ___ ___ ___
Net 1: 192 . 168 . 100 .  0   0   1   0   0   0   0   0

Net 2: 192 . 168 . 100 . ___ ___ ___ ___ ___ ___ ___ ___
Net 2: 192 . 168 . 100 .  0   1   0   0   0   0   0   0

Net 3: 192 . 168 . 100 . ___ ___ ___ ___ ___ ___ ___ ___
Net 3: 192 . 168 . 100 .  0   1   1   0   0   0   0   0

Net 4: 192 . 168 . 100 . ___ ___ ___ ___ ___ ___ ___ ___
Net 4: 192 . 168 . 100 .  1   0   0   0   0   0   0   0
```

f. Calculate the binary and decimal value of the new subnet mask.

```
11111111.11111111.11111111. ___ ___ ___ ___ ___ ___ ___ ___
11111111.11111111.111111111. 1   1   1   0   0   0   0   0
   255   .   255   .   255   . ______
   255   .   255   .   255   .  224
```

g. Fill in the **Subnet Table**, listing the decimal value of all available subnets, the first and last usable host address, and the broadcast address. Repeat until all addresses are listed.

Note: You may not need to use all rows.

Subnet Table

Subnet Number	Subnet Address	First Usable Host Address	Last Usable Host Address	Broadcast Address
0	192.168.100.0	192.168.100.1	192.168.100.30	192.168.100.31
1	192.168.100.32	192.168.100.33	192.168.100.62	192.168.100.63
2	192.168.100.64	192.168.100.65	192.168.100.94	192.168.100.95
3	192.168.100.96	192.168.100.97	192.168.100.126	192.168.100.127
4	192.168.100.128	192.168.100.129	192.168.100.158	192.168.100.159
5	192.168.100.160	192.168.100.161	192.168.100.190	192.168.100.191
6	192.168.100.192	192.168.100.193	192.168.100.222	192.168.100.223
7	192.168.100.224	192.168.100.225	192.168.100.254	192.168.100.255
8				
9				
10				

Step 2: Assign the subnets to the network shown in the topology.

a. Assign Subnet 0 to the LAN connected to the GigabitEthernet 0/0 interface of R1: 192.168.100.0 /27

b. Assign Subnet 1 to the LAN connected to the GigabitEthernet 0/1 interface of R1: 192.168.100.32 /27

c. Assign Subnet 2 to the LAN connected to the GigabitEthernet 0/0 interface of R2: 192.168.100.64 /27

d. Assign Subnet 3 to the LAN connected to the GigabitEthernet 0/1 interface of R2: 192.168.100.96 /27

e. Assign Subnet 4 to the WAN link between R1 to R2: 192.168.100.128 /27

Step 3: Document the addressing scheme.

Fill in the **Subnet Table** using the following guidelines:

a. Assign the first usable IP addresses to R1 for the two LAN links and the WAN link.

b. Assign the first usable IP addresses to R2 for the LANs links. Assign the last usable IP address for the WAN link.

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

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

Part 2: Assign IP Addresses to Network Devices and Verify Connectivity

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

Step 1: Configure IP addressing on R1 LAN interfaces.

Step 2: Configure IP addressing on S3, including the default gateway.

Step 3: Configure IP addressing on PC4, including the default gateway.

Step 4: Verify connectivity.

You can only verify connectivity from R1, S3, and PC4. However, you should be able to ping every IP address listed in the **Addressing Table**.

Suggested Scoring Rubric

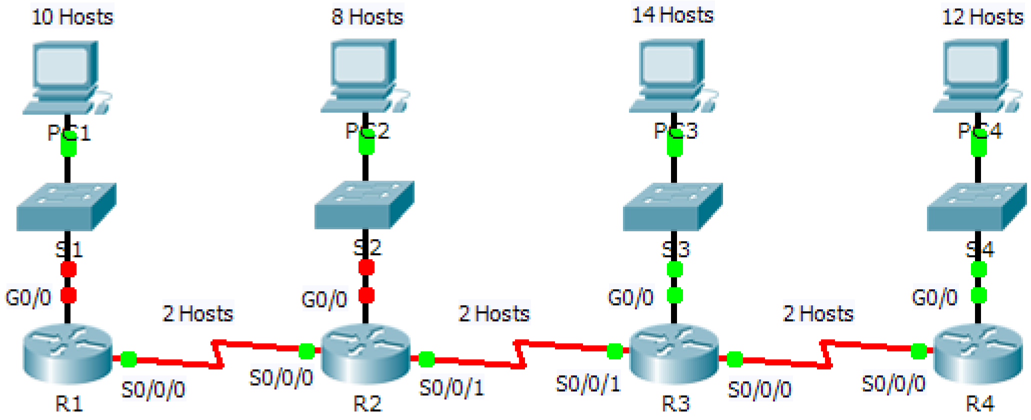
Note: The majority of points are allocated to designing and documenting the addressing scheme. Implementation of the addresses in Packet Tracer is of minimal consideration.

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Design an IP Addressing Scheme	Step 1a	1	
	Step 1b	1	
	Step 1c	1	
	Step 1d	1	
	Step 1e	4	
	Step 1f	2	
Complete Subnet Table	Step 1g	10	
Assign Subnets	Step 2	10	
Document Addressing	Step 3	40	
Part 1 Total		**70**	
Packet Tracer Score		**30**	
Total Score		**100**	

Packet Tracer - Subnet Scenario 2 (Instructor Version)

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

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.31.1.1	255.255.255.240	N/A
	S0/0/0	172.31.1.65	255.255.255.240	N/A
R2	G0/0	172.31.1.17	255.255.255.240	N/A
	S0/0/0	172.31.1.78	255.255.255.240	N/A
	S0/0/1	172.31.1.81	255.255.255.240	N/A
R3	G0/0	172.31.1.33	255.255.255.240	N/A
	S0/0/0	172.31.1.97	255.255.255.240	N/A
	S0/0/1	172.31.1.94	255.255.255.240	N/A
R4	G0/0	172.31.1.49	255.255.255.240	N/A
	S0/0/0	172.31.1.110	255.255.255.240	N/A
S1	VLAN 1	172.31.1.2	255.255.255.240	172.31.1.1
S2	VLAN 1	172.31.1.18	255.255.255.240	172.31.1.17
S3	VLAN 1	172.31.1.34	255.255.255.240	172.31.1.33
S4	VLAN 1	172.31.1.50	255.255.255.240	172.31.1.49
PC1	NIC	172.31.1.14	255.255.255.240	172.31.1.1
PC2	NIC	172.31.1.30	255.255.255.240	172.31.1.17
PC3	NIC	172.31.1.46	255.255.255.240	172.31.1.33
PC4	NIC	172.31.1.62	255.255.255.240	172.31.1.49

Objectives

Part 1: Design an IP Addressing Scheme

Part 2: Assign IP Addresses to Network Devices and Verify Connectivity

Scenario

In this activity, you are given the network address of 172.31.1.0 /24 to subnet and provide the IP addressing for the network shown in the Topology. The required host addresses for each WAN and LAN link are labeled in the topology.

Part 1: Design an IP Addressing Scheme

Step 1: Subnet the 172.31.1.0/24 network based on the maximum number of hosts required by the largest subnet.

a. Based on the topology, how many subnets are needed? 7

b. How many bits must be borrowed to support the number of subnets in the topology table? 4

c. How many subnets does this create? 16

d. How many usable host addresses does this create per subnet? 14

Note: If your answer is less than the 14 maximum hosts required for the R3 LAN, then you borrowed too many bits.

e. Calculate the binary value for the first five subnets. Subnet zero is already shown.

```
Net 0: 172 . 31 . 1 .  0   0   0   0   0   0   0   0

Net 1: 172 . 31 . 1 . ___ ___ ___ ___ ___ ___ ___ ___
Net 1: 172 . 31 . 1 .  0   0   0   1   0   0   0   0

Net 2: 172 . 31 . 1 . ___ ___ ___ ___ ___ ___ ___ ___
Net 2: 172 . 31 . 1 .  0   0   1   0   0   0   0   0

Net 3: 172 . 31 . 1 . ___ ___ ___ ___ ___ ___ ___ ___
Net 3: 172 . 31 . 1 .  0   0   1   1   0   0   0   0

Net 4: 172 . 31 . 1 . ___ ___ ___ ___ ___ ___ ___ ___
Net 4: 172 . 31 . 1 .  0   1   0   0   0   0   0   0
```

f. Calculate the binary and decimal value of the new subnet mask.

```
11111111.11111111.11111111. ___ ___ ___ ___ ___ ___ ___ ___
11111111.11111111.111111111. 1   1   1   1   0   0   0   0
   255   .   255   .   255   . ______
   255   .   255   .   255   .  240
```

g. Complete the **Subnet Table**, listing all available subnets, the first and last usable host address, and the broadcast address. The first subnet is done for you. Repeat until all addresses are listed.

Note: You may not need to use all rows.

Subnet Table

Subnet Number	Subnet IP	First Usable Host IP	Last Usable Host IP	Broadcast Address
0	172.31.1.0	172.31.1.1	172.31.1.14	172.31.1.15
1	172.31.1.16	172.31.1.17	172.31.1.30	172.31.1.31
2	172.31.1.32	172.31.1.33	172.31.1.46	172.31.1.47
3	172.31.1.48	172.31.1.49	172.31.1.62	172.31.1.63
4	172.31.1.64	172.31.1.65	172.31.1.78	172.31.1.79
5	172.31.1.80	172.31.1.81	172.31.1.94	172.31.1.95
6	172.31.1.96	172.31.1.97	172.31.1.110	172.31.1.111
7	172.31.1.112	172.31.1.113	172.31.1.126	172.31.1.127
8	172.31.1.128	172.31.1.129	172.31.1.142	172.31.1.143
9	172.31.1.144	172.31.1.145	172.31.1.158	172.31.1.159
10	172.31.1.160	172.31.1.161	172.31.1.174	172.31.1.175
11	172.31.1.176	172.31.1.177	172.31.1.190	172.31.1.191
12	172.31.1.192	172.31.1.193	172.31.1.206	172.31.1.207
13	172.31.1.208	172.31.1.209	172.31.1.222	172.31.1.223
14	172.31.1.224	172.31.1.225	172.31.1.238	172.31.1.239
15	172.31.1.240	172.31.1.241	172.31.1.254	172.31.1.255

Step 2: Assign the subnets to the network shown in the topology.

When assigning the subnets, keep in mind that routing is necessary to allow information to be sent throughout the network.

a. Assign Subnet 0 to the R1 LAN: 172.31.1.0 /28

b. Assign Subnet 1 to the R2 LAN: 172.31.1.16/28

c. Assign Subnet 2 to the R3 LAN: 172.31.1.32/28

d. Assign Subnet 3 to the R4 LAN: 172.31.1.48/28

e. Assign Subnet 4 to the link between R1 and R2. 172.31.1.64/28

f. Assign Subnet 5 to the link between R2 and R3. 172.31.1.80/28

g. Assign Subnet 6 to the link between R3 and R4. 172.31.1.96/28

Step 3: Document the addressing scheme.

Complete the **Addressing Table** using the following guidelines:

a. Assign the first usable IP addresses to routers for each of the LAN links.

b. Use the following method to assign WAN link IP addresses:

- For the WAN link between R1 and R2, assign the first usable IP address to R1 and last usable IP address R2.
- For the WAN link between R2 and R3, assign the first usable IP address to R2 and last usable IP address R3.
- For the WAN link between R3 and R4, assign the first usable IP address to R3 and last usable IP address R4.

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

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

Part 2: Assign IP Addresses to Network Devices and Verify Connectivity

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

Step 1: Configure IP addressing on R1 and R2 LAN interfaces.

Step 2: Configure IP addressing on S3, including the default gateway.

Step 3: Configure IP addressing on PC4, including the default gateway.

Step 4: Verify connectivity.

You can only verify connectivity from R1, R2, S3, and PC4. However, you should be able to ping every IP address listed in the **Addressing Table**.

Suggested Scoring Rubric

Note: The majority of points are allocated to designing and documenting the addressing scheme. Implementation of the addresses in Packet Tracer is of minimal consideration.

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Design an IP Addressing Scheme	Step 1a	1	
	Step 1b	1	
	Step 1c	1	
	Step 1d	1	
	Step 1e	4	
	Step 1f	2	
Complete Subnet Table	Step 1g	10	
Assign Subnets	Step 2	10	
Document Addressing	Step 3	40	
Part 1 Total		**70**	
Packet Tracer Score		**30**	
Total Score		**100**	

Packet Tracer - Designing and Implementing a VLSM Addressing Scheme (Instructor Version)

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

Topology

You will receive one of three possible topologies.

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
[[R1Name]]	G0/0	[[R1G0Add]]	[[R1G0Sub]] N/A	
	G0/1	[[R1G1Add]]	[[R1G1Sub]] N/A	
	S0/0/0	[[R1S0Add]]	[[R1S0Sub]] N/A	
[[R2Name]]	G0/0	[[R2G0Add]]	[[R2G0Sub]] N/A	
	G0/1	[[R2G1Add]]	[[R2G1Sub]] N/A	
	S0/0/0	[[R2S0Add]]	[[R2S0Sub]] N/A	
[[S1Name]] VLAN	1	[[S1Add]]	[[S1Sub]]	[[R1G0Add]]
[[S2Name]] VLAN	1	[[S2Add]]	[[S2Sub]]	[[R1G1Add]]
[[S3Name]] VLAN	1	[[S3Add]]	[[S3Sub]]	[[R2G0Add]]
[[S4Name]] VLAN	1	[[S4Add]]	[[S4Sub]]	[[R2G1Add]]
[[PC1Name]] NIC		[[PC1Add]]	[[PC1Sub]]	[[R1G0Add]]
[[PC2Name]] NIC		[[PC2Add]]	[[PC2Sub]]	[[R1G1Add]]
[[PC3Name]] NIC		[[PC3Add]]	[[PC3Sub]]	[[R2G0Add]]
[[PC4Name]] NIC		[[PC4Add]]	[[PC4Sub]]	[[R2G1Add]]

Objectives

Part 1: Examine the Network Requirements

Part 2: Design the VLSM Addressing Scheme

Part 3: Assign IP Addresses to Devices and Verify Connectivity

Background

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

Part 1: Examine the Network Requirements

Step 1: Determine the number of subnets needed.

You will subnet the network address [[DisplayNet]]. The network has the following requirements:

- **[[S1Name]]** LAN will require **[[HostReg1]]** host IP addresses
- **[[S2Name]]** LAN will require **[[HostReg2]]** host IP addresses
- **[[S3Name]]** LAN will require **[[HostReg3]]** host IP addresses
- **[[S4Name]]** LAN will require **[[HostReg4]]** host IP addresses

How many subnets are needed in the network topology? 5

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

a. Which subnet mask will accommodate the number of IP addresses required for **[[S1Name]]**?

How many usable host addresses will this subnet support?

b. Which subnet mask will accommodate the number of IP addresses required for **[[S2Name]]**?

How many usable host addresses will this subnet support?

c. Which subnet mask will accommodate the number of IP addresses required for **[[S3Name]]**?

How many usable host addresses will this subnet support?

d. Which subnet mask will accommodate the number of IP addresses required for **[[S4Name]]**?

How many usable host addresses will this subnet support?

e. Which subnet mask will accommodate the number of IP addresses required for the connection between **[[R1Name]]** and **[[R2Name]]**?

Part 2: Design the VLSM Addressing Scheme

Step 1: Divide the [[DisplayNet]] network based on the number of hosts per subnet.

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

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

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

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

e. Use the fifth subnet to accommodate the connection between **[[R1Name]]** and **[[R2Name]]**.

Step 2: Document the VLSM subnets.

Complete the **Subnet Table**, listing the subnet descriptions (e.g. [[S1Name]] LAN), number of hosts needed, then network address for the subnet, the first usable host address, and the broadcast address. Repeat until all addresses are listed.

Subnet Table

Note: The correct answers for this table are variable depending on the scenario received. Refer to the Instructor Notes at the end of these instructions for further information. The format here follows what the student used in **Designing and Implementing a VLSM Addressing Scheme**.

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

Step 3: Document the addressing scheme.

a. Assign the first usable IP addresses to **[[R1Name]]** for the two LAN links and the WAN link.

b. Assign the first usable IP addresses to **[[R2Name]]** for the two LANs links. Assign the last usable IP address for the WAN link.

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

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

Part 3: Assign IP Addresses to Devices and Verify Connectivity

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

Step 1: Configure IP addressing on [[R1Name]] LAN interfaces.

Step 2: Configure IP addressing on [[S3Name]], including the default gateway.

Step 3: Configure IP addressing on [[PC4Name]], including the default gateway.

Step 4: Verify connectivity.

You can only verify connectivity from [[R1Name]], [[S3Name]], and [[PC4Name]]. However, you should be able to ping every IP address listed in the **Addressing Table**.

Suggested Scoring Rubric

Note: The majority of points are allocated to designing and documenting the addressing scheme. Implementation of the addresses in Packet Tracer is of minimal consideration.

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

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

Instructor Notes:

The following addressing tables represent the three possible addressing scenarios the student may get. Note that the Device column is independent of the addressing scheme. For example, a student could receive the device names from Scenario 1 and the addressing scheme from Scenario 3. In addition, the three possible topologies are also independent of the device names and the addressing scheme (click reset in the activity to see the different topologies). Therefore, this activity uses three independent variables with three possible values each for a total of 27 possible combinations (3 device names x 3 addressing schemes x 3 topologies = 27 isomorphs).

Scenario 1 - Network Address: 10.11.48.0/24

Subnet Table

Subnet Description	Number of Hosts Needed	Network Address/CIDR	First Usable Host Address	Last Usable Host Address	Broadcast Address
Host-D LAN	60	10.11.48.0/26	10.11.48.1 10.11.48.6	2	10.11.48.63
Host-B LAN	30	10.11.48.64/27 10.11.48.6	5	10.11.48.94	10.11.48.95
Host-A LAN	14	10.11.48.96/28	10.11.48.97 10.11.48.1	10	10.11.48.111
Host-C LAN	6	10.11.48.112/29	10.11.48.113 10.11.48.1	18	10.11.48.119
WAN Link	2	10.11.48.120/30	10.11.48.121 10.11.48.1	22	10.11.48.123

Device	Interface	Address	Subnet Mask	Default Gateway
Building1	G0/0 10.11.48.9	7	255.255.255.240	N/A
	G0/1 10.11.48.6	5	255.255.255.224	N/A
	S0/0/0	10.11.48.121	255.255.255.252 N/A	
Building2	G0/0	10.11.48.113	255.255.255.248	N/A
	G0/1	10.11.48.1	255.255.255.192	N/A
	S0/0/0	10.11.48.122	255.255.255.252	N/A
ASW1 VLAN	1	10.11.48.98 255.25	5.255.240	10.11.48.97
ASW2 VLAN	1	10.11.48.66 255.25	5.255.224	10.11.48.65
ASW3 VLAN	1	10.11.48.114 255.25	5.255.248	10.11.48.113
ASW4 VLAN	1	10.11.48.2 255.25	5.255.192	10.11.48.1
Host-A NIC		10.11.48.110 255.25	5.255.240	10.11.48.97
Host-B NIC		10.11.48.94 255.25	5.255.224	10.11.48.65
Host-C NIC		10.11.48.118 255.25	5.255.248	10.11.48.113
Host-D NIC		10.11.48.62 255.25	5.255.192	10.11.48.1

Building 1

```
en
conf t
int g0/0
ip add 10.11.48.97 255.255.255.240
no shut
int g0/1
ip add 10.11.48.65 255.255.255.224
no shut
```

ASW3

```
en
conf t
int vlan 1
ip add 10.11.48.114 255.255.255.248
no shut
ip def 10.11.48.113
```

Scenario 2 - Network Address: 172.31.103.0/24

Subnet Table

Subnet Description	Number of Hosts Needed	Network Address/CIDR	First Usable Host Address	Last Usable Host Address	Broadcast Address
PC-A LAN	27	172.31.103.0/27	172.31.103.1 172.31.1	03.30	172.31.103.31
PC-B LAN	25	172.31.103.32/27	172.31.103.33 172.31.1	03.62	172.31.103.63
PC-C LAN	14	172.31.103.64/28	172.31.103.65 172.31.1	03.78	172.31.103.79
PC-D LAN	8	172.31.103.80/28	172.31.103.81 172.31.1	03.94	172.31.103.95
WAN Link	2	172.31.103.96/30	172.31.103.97 172.31.1	03.98	172.31.103.99

Device	Interface	Address	Subnet Mask	Default Gateway
Branch1	G0/0 172.31.1	03.1	255.255.255.224	N/A
	G0/1 172.31.1	03.33	255.255.255.224	N/A
	S0/0/0	172.31.103.97	255.255.255.252 N/A	
Branch2	G0/0	172.31.103.65	255.255.255.240	N/A
	G0/1	172.31.103.81	255.255.255.240	N/A
	S0/0/0	172.31.103.98	255.255.255.252	N/A
Room-114 VLAN	1	172.31.103.2 255.25	5.255.224	172.31.103.1
Room-279 VLAN	1	172.31.103.34 255.25	5.255.224	172.31.103.33
Room-312 VLAN	1	172.31.103.66 255.25	5.255.240	172.31.103.65
Room-407 VLAN	1	172.31.103.82 255.25	5.255.240	172.31.103.81
PC-A NIC		172.31.103.30 255.25	5.255.224	172.31.103.1
PC-B NIC		172.31.103.62 255.25	5.255.224	172.31.103.33
PC-C NIC		172.31.103.78 255.25	5.255.240	172.31.103.65
PC-D NIC		172.31.103.94 255.25	5.255.240	172.31.103.81

Branch 1

```
en
conf t
int g0/0
ip add 172.31.103.1 255.255.255.224
no shut
int g0/1
```

```
      ip add 172.31.103.33 255.255.255.224
      no shut
```

Room-312

```
      en
      conf t
      int vlan 1
      ip add 172.31.103.66 255.255.255.240
      no shut
      ip def 172.31.103.65
```

Scenario 3 - Network Address: 192.168.72.0/24

Subnet Table

Subnet Description	Number of Hosts Needed	Network Address/CIDR	First Usable Host Address	Last Usable Host Address	Broadcast Address
User-4 LAN	58	192.168.72.0/26	192.168.72.1	192.168.72.62	192.168.72.63
User-3 LAN	29	192.168.72.64/27	192.168.72.65	192.168.72.94	192.168.72.95
User-2 LAN	15	192.168.72.96/27	192.168.72.97	192.168.72.126	192.168.72.127
User-1 LAN	7	192.168.72.128/28	192.168.72.129	192.168.72.142	192.168.72.143
WAN Link	2	192.168.72.144/30	192.168.72.145	192.168.72.146	192.168.72.147

Device	Interface	Address	Subnet Mask	Default Gateway
Remote-Site1	G0/0	192.168.72.129	255.255.255.240	N/A
	G0/1	192.168.72.97	255.255.255.224	N/A
	S0/0/0	192.168.72.145	255.255.255.252	N/A
Remote-Site2	G0/0	192.168.72.65	255.255.255.224	N/A
	G0/1	192.168.72.1	255.255.255.192	N/A
	S0/0/0	192.168.72.146	255.255.255.252	N/A
Sw1 VLAN	1	192.168.72.130	255.255.255.240	192.168.72.129
Sw2 VLAN	1	192.168.72.98	255.255.255.224	192.168.72.97
Sw3 VLAN	1	192.168.72.66	255.255.255.224	192.168.72.65
Sw4 VLAN	1	192.168.72.2	255.255.255.192	192.168.72.1
User-1 NIC		192.168.72.142	255.255.255.240	192.168.72.129
User-2 NIC		192.168.72.126	255.255.255.224	192.168.72.97
User-3 NIC		192.168.72.94	255.255.255.224	192.168.72.65
User-4 NIC		192.168.72.62	255.255.255.192	192.168.72.1

Remote-Site1

```
en
conf t
int g0/0
ip add 192.168.72.129 255.255.255.240
no shut
int g0/1
```

```
      ip add 192.168.72.97 255.255.255.224
      no shut
```

Sw-3

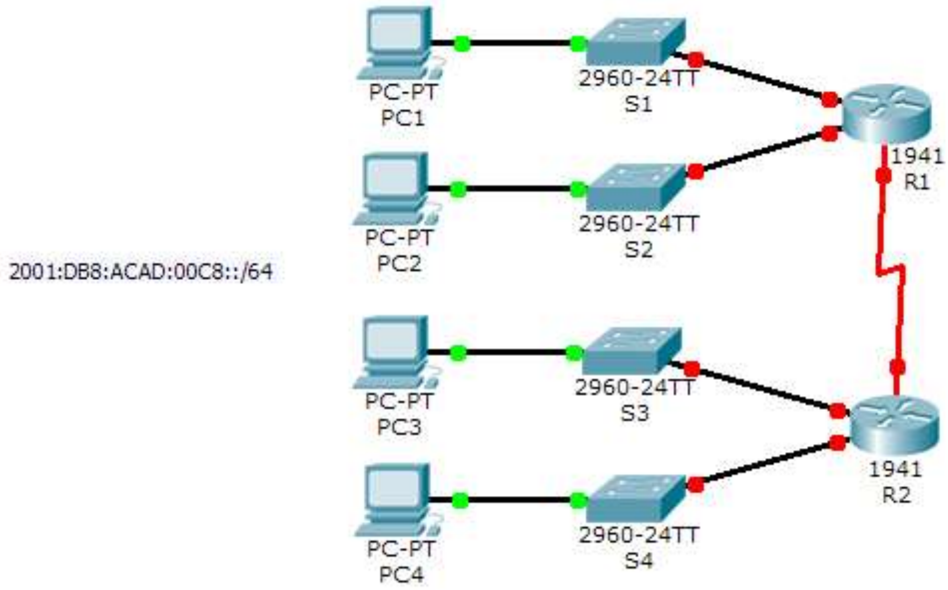
```
      en
      conf t
      int vlan 1
      ip add 192.168.72.66 255.255.255.224
      no shut
      ip def 192.168.72.65
```

Cisco Networking Academy® Mind Wide Open™

Packet Tracer - Implementing a Subnetted IPv6 Addressing Scheme (Instructor Version)

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

Topology



Addressing Table

Device	Interface	IPv6 Address	Link-Local
R1	G0/0	2001:DB8:ACAD:00C8::1/64	FE80::1
	G0/1	2001:DB8:ACAD:00C9::1/64	FE80::1
	S0/0/0	2001:DB8:ACAD:00CC::1/64	FE80::1
R2	G0/0	2001:DB8:ACAD:00CA::1/64	FE80::2
	G0/1	2001:DB8:ACAD:00CB::1/64	FE80::2
	S0/0/0	2001:DB8:ACAD:00CC::2/64	FE80::2
PC1	NIC	Auto Config	
PC2	NIC	Auto Config	
PC3	NIC	Auto Config	
PC4	NIC	Auto Config	

Objectives

Part 1: Determine the IPv6 Subnets and Addressing Scheme

Part 2: Configure the IPv6 Addressing on Routers and PCs and Verify Connectivity

Scenario

Your network administrator wants you to assign five /64 IPv6 subnets to the network shown in the topology. Your job is to determine the IPv6 subnets, assign IPv6 addresses to the routers, and set the PCs to automatically receive IPv6 addressing. Your final step is to verify connectivity between IPv6 hosts.

Part 1: Determine the IPv6 Subnets and Addressing Scheme

Step 1: Determine the number of subnets needed.

Start with the IPv6 subnet 2001:DB8:ACAD:00C8::/64 and assign it to the R1 LAN attached to GigabitEthernet 0/0, as shown in the **Subnet Table**. For the rest of the IPv6 subnets, increment the 2001:DB8:ACAD:00C8::/64 subnet address by 1 and complete the **Subnet Table** with the IPv6 subnet addresses.

Subnet Table

Subnet Description	Subnet Address
R1 G0/0 LAN	2001:DB8:ACAD:00C8::0/64
R1 G0/1 LAN	2001:DB8:ACAD:00C9::0/64
R2 G0/0 LAN	2001:DB8:ACAD:00CA::0/64
R2 G0/1 LAN	2001:DB8:ACAD:00CB::0/64
WAN Link	2001:DB8:ACAD:00CC::0/64

Step 2: Assign IPv6 addressing to the routers.

a. Assign the first IPv6 addresses to R1 for the two LAN links and the WAN link.

b. Assign the first IPv6 addresses to R2 for the two LANs. Assign the second IPv6 address for the WAN link.

c. Document the IPv6 addressing scheme in the **Addressing Table**.

Part 2: Configure the IPv6 Addressing on Routers and PCs and Verify Connectivity

Step 1: Configure the routers with IPv6 addressing.

Note: This network is already configured with some IPv6 commands that are covered in a later course. At this point in your studies, you only need to know how to configure IPv6 address on an interface.

Configure R1 and R2 with the IPv6 addresses you specified in the **Addressing Table** and activate the interfaces.

```
Router(config-if)# ipv6 address ipv6-address/prefix
Router(config-if)# ipv6 address ipv6-link-local link-local
```

Step 2: Configure the PCs to automatically receive IPv6 addressing.

Configure the four PCs for autoconfiguration. Each should then automatically receive full IPv6 addresses from the routers.

Step 3: Verify connectivity between the PCs.

Each PC should be able to ping the other PCs and the routers.

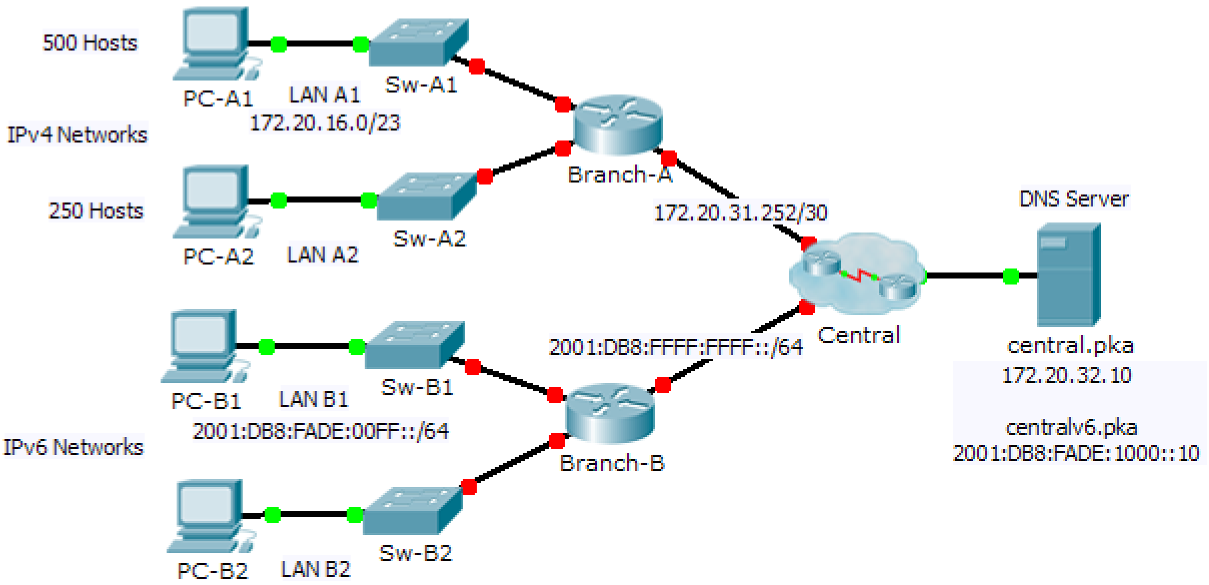
Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Determine IPv6 Subnets and Addressing Scheme	Subnet Table	30	
	Addressing Table	30	
Part 1 Total		**60**	
Packet Tracer Score		**40**	
Total Score		**100**	

Packet Tracer - Skills Integration Challenge (Instructor Version)

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

Topology



Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
		IPv6 Address/Prefix		
Branch-A	G0/0	172.20.16.1	255.255.254.0	N/A
	G0/1	172.20.18.1	255.255.255.0	N/A
	G0/2	172.20.31.254	255.255.255.252	N/A
Branch-B	G0/0	2001:DB8:FADE:00FF::1/64		N/A
	G0/1	2001:DB8:FADE:0100::1/64		N/A
	G0/2	2001:DB8:FFFF:FFFF::2/64		N/A
PC-A1	NIC	172.20.17.254	255.255.254.0	172.20.16.1
PC-A2	NIC	172.20.18.254	255.255.255.0	172.20.18.1
PC-B1	NIC	2001:DB8:FADE:00FF::10/64		FE80::B
PC-B2	NIC	2001:DB8:FADE:0100::10/64		FE80::B

Scenario

As a network technician familiar with IPv4 and IPv6 addressing implementations, you are now ready to take an existing network infrastructure and apply your knowledge and skills to finalize the configuration. In this activity, the network administrator has already configured some commands on the routers. **Do not erase or**

modify those configurations. Your task is to complete the IPv4 and IPv6 addressing scheme, implement IPv4 and IPv6 addressing, and verify connectivity.

Requirements

- Configure the initial settings on **Branch-A** and **Branch-B**, including the hostname, banner, lines, and passwords. Use **cisco** as the user EXEC password and **class** as the privileged EXEC password. Encrypt all passwords.
- LAN A1 is using the subnet 172.20.16.0/23. Assign the next available subnet to LAN A2 for a maximum of 250 hosts.
- LAN B1 is using the subnet 2001:DB8:FADE:00FF::/64. Assign the next available subnet to LAN B2.
- Finish documenting the addressing scheme in the **Addressing Table** using the following guidelines:
  - Assign the first IP address for LAN A1, LAN A2, LAN B1, and LAN B2 to the router interface.
  - For the IPv4 networks, assign the last IPv4 address to the PCs.
  - For the IPv6 networks, assign the 16th IPv6 address to the PCs.
- Configure the routers addressing according to your documentation. Include an appropriate description for each router interface. **Branch-B** uses FE80::B as the link-local address.
- Configure PCs with addressing according to your documentation. The DNS Server addresses for IPv4 and IPv6 are shown in the topology.
- Verify connectivity between the IPv4 PCs and between the IPv6 PCs.
- Verify the IPv4 PCs can access the web page at **central.pka**.
- Verify the IPv6 PCs can access the web page at **centralv6.pka**.

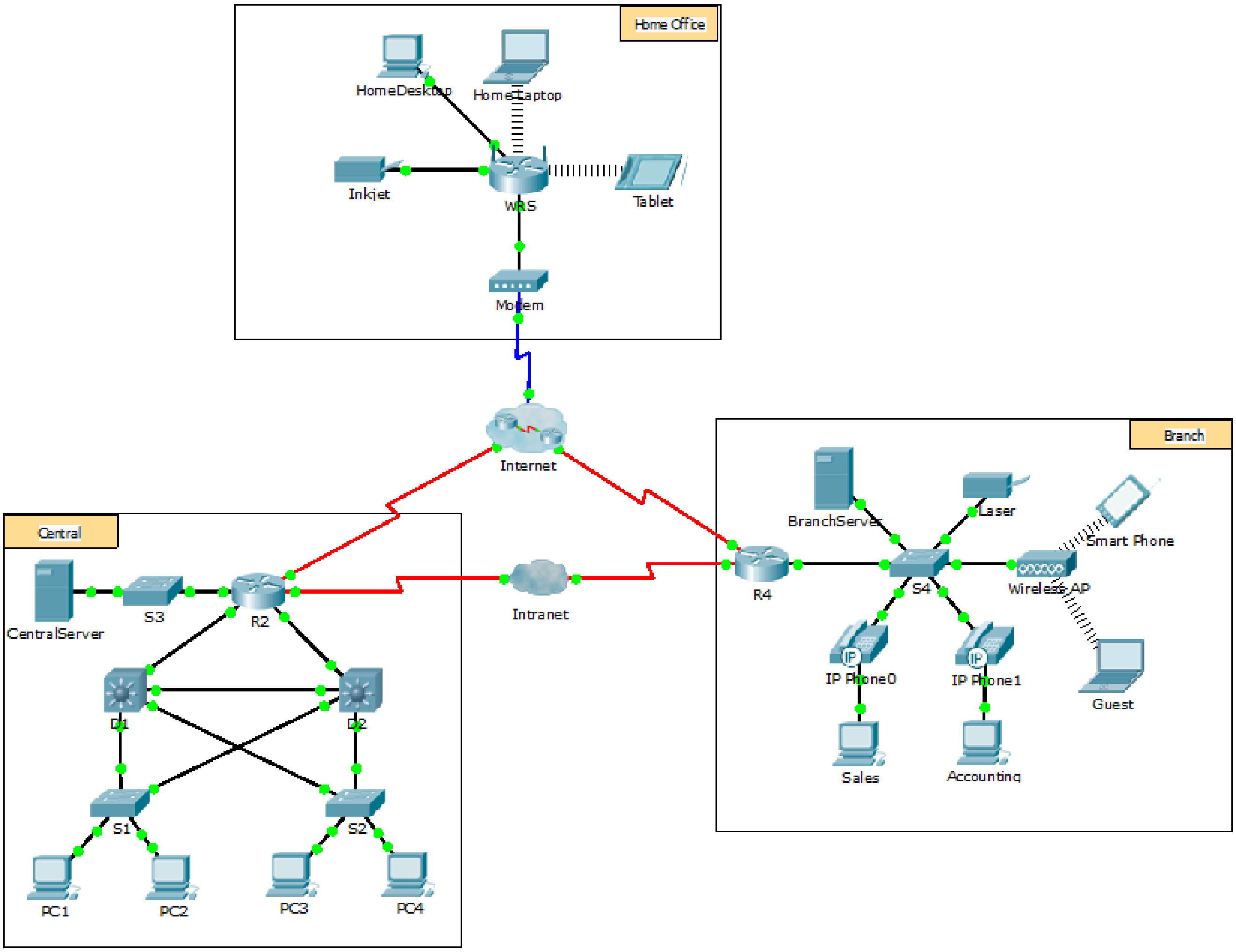
Suggested Scoring Rubric

Activity Section	Possible Points	Earned Points
Addressing Table Documentation	**25**	
Packet Tracer Score	**75**	
Total Score	**100**	

Packet Tracer - Web and Email Servers (Instructor Version)

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

Topology



Objectives

Part 1: Configure and Verify Web Services

Part 2: Configure and Verify Email Services

Background

In this activity, you will configure HTTP and email services using the simulated server in Packet Tracer. You will then configure clients to access the HTTP and email services.

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

Part 1: Configure and Verify Web Services

Step 1: Configure web services on CentralServer and BranchServer.

a. Click **CentralServer** and click the **Services** tab > **HTTP**.

b. Click **On** to enable HTTP and HTTP Secure (HTTPS).

c. Optional. Personalize the HTML code.

d. Repeat Step1a – 1c on **BranchServer**.

Step 2: Verify the web servers by accessing the web pages.

There are many endpoint devices in this network, but for the purposes of this step, use **PC3**.

a. Click **PC3** and click the **Desktop** tab > **Web Browser**.

b. In the URL box, enter **10.10.10.2** as the IP address and click **Go**. The **CentralServer** website displays.

c. In the URL box, enter **64.100.200.1** as the IP address and click **Go**. The **BranchServer** website displays.

d. In the URL box, enter **centralserver.pt.pka** and click **Go**. The **CentralServer** website displays.

e. In the URL box, enter **branchserver.pt.pka** and click **Go**. The **BranchServer** website displays.

f. What protocol is translating the **centralserver.pt.pka** and **branchserver.pt.pka** names to IP addresses?

____

Domain Name Service (DNS)

Part 2: Configure and Verify Email Services on Servers

Step 1: Configure CentralServer to send (SMTP) and receive (POP3) Email.

a. Click **CentralServer**, and then select the **Services** tab followed by the **EMAIL** button.

b. Click **On** to enable the SMTP and POP3.

c. Set the domain name to **centralserver.pt.pka** and click **Set**.

d. Create a user named **central-user** with password **cisco**. Click **+** to add the user.

Step 2: Configure BranchServer to send (SMTP) and receive (POP3) Email.

a. Click **BranchServer** and click the **Services** tab > **EMAIL**.

b. Click **On** to enable SMTP and POP3.

c. Set the domain name to **branchserver.pt.pka** and click **Set**.

d. Create a user named **branch-user** with password **cisco**. Click **+** to add the user.

Step 3: Configure PC3 to use the CentralServer email service.

a. Click **PC3** and click the **Desktop** tab > **E Mail**.

b. Enter the following values into their respective fields:

1) Your Name: **Central User**

2) Email Address: **central-user@centralserver.pt.pka**

3) Incoming Mail Server: **10.10.10.2**

4) Outgoing Mail Server: **10.10.10.2**

5) User Name: **central-user**

6) Password: **cisco**

c. Click **Save**. The Mail Browser window displays.

d. Click **Receive**. If everything has been set up correctly on both the client and server, the Mail Browser window displays the `Receive Mail Success` message confirmation.

Step 4: Configure Sales to use the Email service of BranchServer.

a. Click **Sales** and click the **Desktop** tab > **E Mail**.

b. Enter the following values into their respective fields:

1) Your Name: **Branch User**

2) Email Address: **branch-user@branchserver.pt.pka**

3) Incoming Mail Server: **172.16.0.3**

4) Outgoing Mail Server: **172.16.0.3**

5) User Name: **branch-user**

6) Password: **cisco**

c. Click **Save**. The Mail Browser window displays.

d. Click **Receive**. If everything has been set up correctly on both the client and server, the Mail Browser window displays the `Receive Mail Success` message confirmation.

e. The activity should be 100% complete. Do not close the Sales configuration window or the Mail Browser window.

Step 5: Send an Email from the Sales client and the PC3 client.

a. From the **Sales Mail Browser** window, click **Compose**.

b. Enter the following values into their respective fields:

1) To: **central-user@centralserver.pt.pka**

2) Subject: *Personalize the subject line*.

3) **Email** Body: *Personalize the email*.

c. Click **Send**.

d. Verify that **PC3** received the email. Click **PC3**. If the Mail Browser window is closed, click **E Mail**.

e. Click **Receive**. An email from Sales displays. Double-click the email.

f. Click **Reply**, personalize a response, and click **Send**.

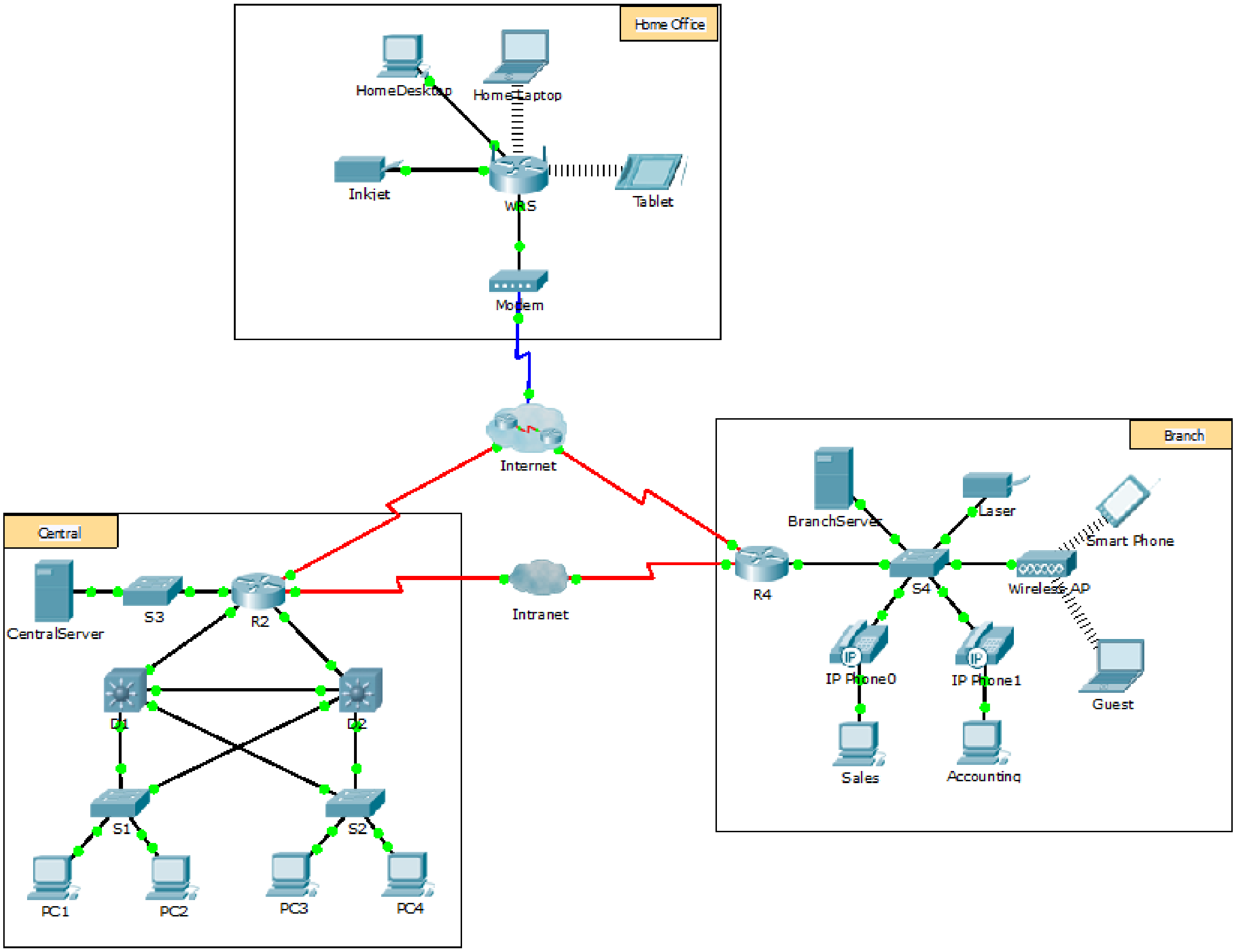
g. Verify that **Sales** received the reply.

Cisco Networking Academy® Mind Wide Open™

Packet Tracer - DHCP and DNS Servers (Instructor Version)

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

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.

Part 1: Configure Static IPv4 Addressing

Step 1: 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.

a. Click **Inkjet** and click the **Config** tab, which displays the Global Settings.

b. Statically assign the Gateway address as **192.168.0.1** and the DNS Server address as **64.100.8.8**.

c. Click **FastEthernet0** and statically assign the IP address as **192.168.0.2** and the Subnet Mask address as **255.255.255.0**.

d. Close the Inkjet window.

Step 2: Configure WRS to provide DHCP services.

a. Click **WRS** and click the **GUI** tab, and maximize the window.

b. The Basic Setup window displays, by default. Configure the following settings in the Network Setup section:

1) Change the IP Address to **192.168.0.1**.

2) Set the Subnet Mask to **255.255.255.0**.

3) Enable the DHCP Server.

4) Set the Static DNS 1 address to **64.100.8.8**.

5) Scroll to the bottom and click **Save**.

c. Close the **WRS** window.

Step 3: 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**.

a. Click **Home Laptop** and click the **Desktop** tab > **IP Configuration**.

b. Click **DHCP** and wait until the DHCP request is successful.

c. **Home Laptop** should now have a full IP configuration. If not, return to Step 2 and verify your configurations on **WRS**.

d. Close the IP Configuration window and then close the **Home Laptop** window.

Step 4: Request DHCP addressing for the tablet.

a. Click **Tablet** and click the **Desktop** tab > **IP Configuration**.

b. Click **DHCP** and wait until the DHCP request is successful.

c. **Tablet** should now have a full IP configuration. If not, return to Step 2 and verify your configurations on **WRS**.

Step 5: Test access to websites.

a. Close the **IP Configuration** window, and then click Web Browser.

b. 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.

c. 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.

Part 2: Configure Records on the DNS Server

Step 1: 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.

a. Click the **Internet** cloud. A new network displays.

b. Click **famous.dns.pka** and click the **Services** tab > **DNS**.

c. Add the following resource records:

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

d. Close the famous.dns.pka window.

e. Click **Back** to exit the **Internet** cloud.

Step 2: 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.

a. Click **Home Laptop** or **Tablet**.

b. 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.

c. 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.

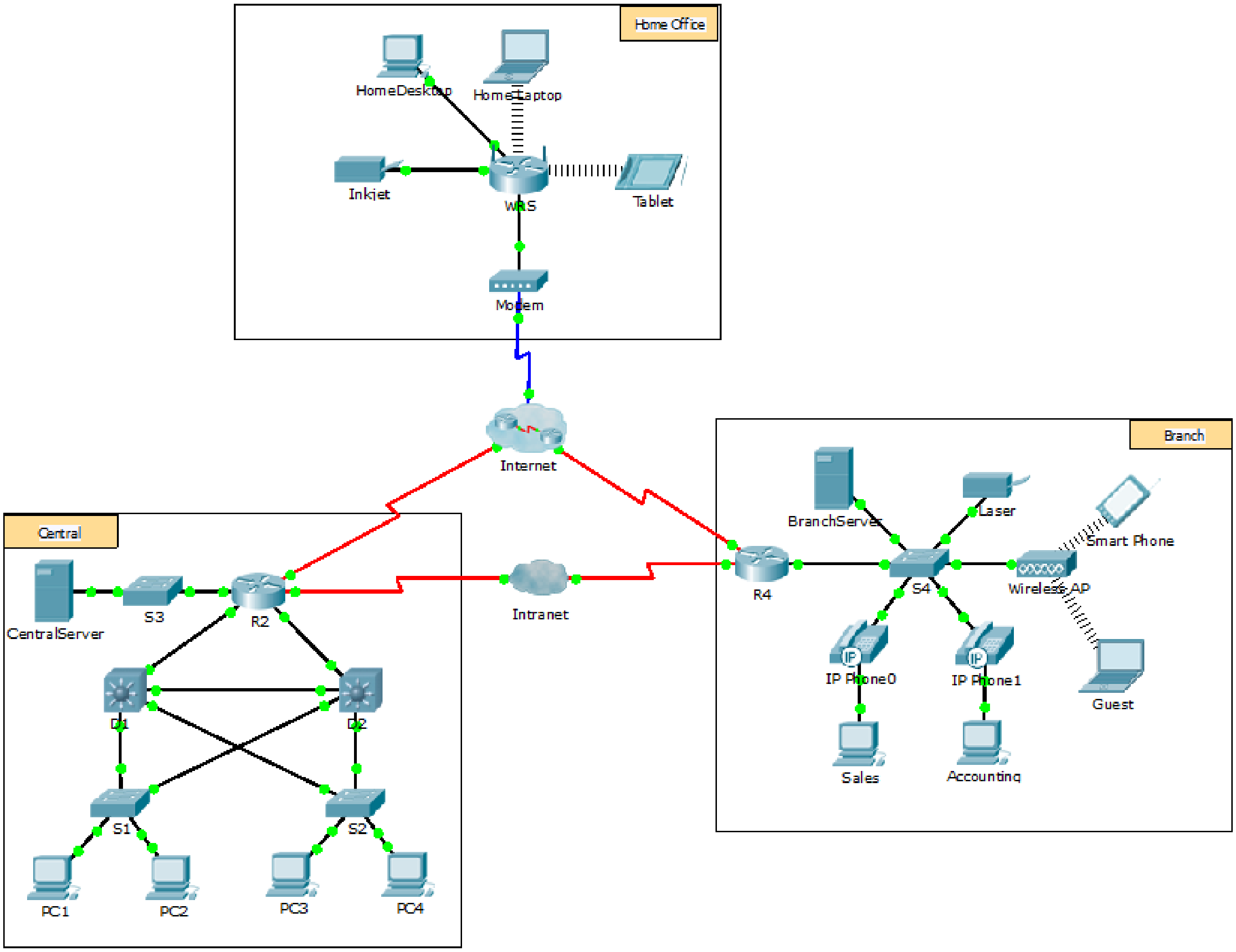
Test the functionality of the DNS server by entering the commands **nslookup centralserver.pt.pka** and **nslookup branchserver.pt.pka**. You should get a name resolution showing the IP address for each.

d. 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**.

Packet Tracer - FTP Servers (Instructor Version)

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

Topology



Objectives

Part 1: Configure FTP Services on Servers

Part 2: Upload a File to the FTP Server

Part 3: Download a File from the FTP Server

Background

In this activity, you will configure FTP services. You will then use the FTP services to transfer files between clients and the server.

Note: Packet Tracer only simulates the process for configuring these services. FTP server and client software packages each have their own unique installation and configuration instructions. The first time you attempt to connect to a web address, Packet Tracer takes several seconds to simulate the DNS name resolution process.

Part 1: Configure FTP Services on Servers

Step 1: Configure the FTP service on CentralServer.

a. Click **CentralServer** > **Services** tab > **FTP**.

b. Click **On** to enable FTP service.

c. In **User Setup**, create the following user accounts. Click **Add** to add the account:

Username	Password	Permissions
anonymous	anonymous	limited to **Read** and **List**
administrator	cisco	full permission

d. Click the default **cisco** user account and click **Remove** to delete it. Close the CentralServer configuration window.

Step 2: Configure the FTP service on BranchServer.

Repeat Step 1 on **BranchServer**.

Part 2: Upload a File to the FTP Server

Step 1: Transfer the README.txt file from the home laptop to CentralServer.

As network administrator, you must place a notice on the FTP servers. The document has been created on the home laptop and must be uploaded to the FTP servers.

a. Click **Home Laptop** and click the **Desktop** tab > **Text Editor**.

b. Open the **README.txt** file and review it. Close the **Text Editor** when done.

Note: Do not change the file because this affects scoring.

c. In the **Desktop** tab, open the Command Prompt window and perform the following steps:

1) Type **ftp centralserver.pt.pka**. Wait several seconds while the client connects.

   Note: Because Packet Tracer is a simulation, it can take up to 30 seconds for FTP to connect the first time.

2) The server prompts for a username and password. Use the credentials for the **administrator** account.

3) The prompt changes to `ftp>`. List the contents of the directory by typing **dir**. The file directory on **CentralServer** displays.

4) Transfer the README.txt file: at the `ftp>` prompt, type **put README.txt**. The README.txt file is transferred from the home laptop to **CentralServer**.

5) Verify the transfer of the file by typing **dir**. The README.txt file is now listed in the file directory.

6) Close the FTP client by typing **quit**. The prompt will return to `PC>`.

Step 2: Transfer the README.txt file from the home laptop to BranchServer.

a. Repeat Step 1c to transfer the README.txt file to **branchserver.pt.pka**.

b. Close the Command Prompt and Home Laptop windows, respectively.

Part 3: Download a File from the FTP Server

Step 1: Transfer README.txt from CentralServer to PC2.

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

1) Type **ftp centralserver.pt.pka**.

2) The server prompts for a username and password. Use the credentials for the **anonymous** account.

3) The prompt changes to `ftp>`. List the contents of the directory by typing **dir**. The README.txt file is listed at the top of the directory list.

4) Download the README.txt file: at the ftp> prompt, type **get README.txt**. The README.txt file is transferred to **PC2**.

5) Verify that the **anonymous** account does not have the permission to write files to **CentralServer** by typing **put sampleFile.txt**. The following error message displays:

```
Writing file sampleFile.txt to centralserver.pt.pka:
File transfer in progress...

%Error ftp://centralserver.pt.pka/sampleFile.txt (No such file or directory Or
Permission denied)
550-Requested action not taken. permission denied).
```

6) Close the FTP client by typing **quit**. The prompt returns to the `PC>` prompt.

7) Verify the transfer of the file to PC2 by typing **dir**. README.txt is listed in the directory.

8) Close the command line window.

b. In the **Desktop** tab, open the **Text Editor** and then the **README.txt** file to verify the integrity of the file.

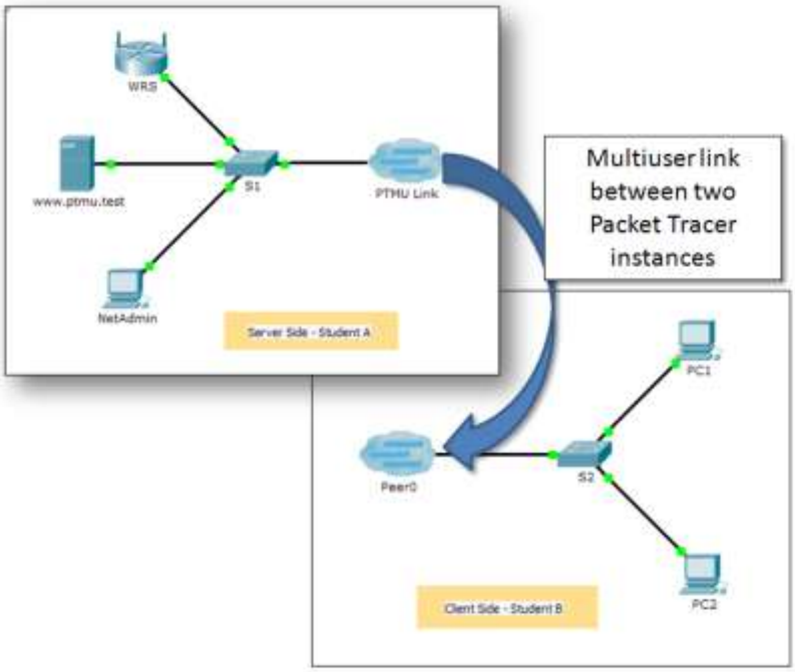
c. Close the **Text Editor** and then the PC2 configuration window.

Step 2: Transfer the README.txt file from BranchServer to the Smart Phone.

Repeat Step 1 for **Smart Phone**, except download the README.txt file from **branchserver.pt.pka**.

Packet Tracer Multiuser - Tutorial (Instructor Version)

Topology



Addressing Table

Device	IP Address	Subnet Mask	DNS Server
www.ptmu.test	10.10.10.1	255.0.0.0	10.10.10.1
PC	10.10.10.10	255.0.0.0	10.10.10.1

Objectives

Part 1: Establish a Local Multiuser Connection to another Instance of Packet Tracer

Part 2: Verify Connectivity across a Local Multiuser Connection

Background

The multiuser feature in Packet Tracer allows multiple point-to-point connections between multiple instances of Packet Tracer. This first Packet Tracer Multiuser (PTMU) activity is a quick tutorial demonstrating the steps to establish and verify a multiuser connection to another instance of Packet Tracer within the same LAN. Ideally, this activity is meant for two students. However, it can also be completed as a solo activity simply by opening the two separate files to create two separate instances of Packet Tracer on your local machine.

Part 1: Establish a Local Multiuser Connection to Another Instance of Packet Tracer

Step 1: Select a partner and determine the role for each student.

a. Find a fellow classmate with whom you will cooperate to complete this activity. Your computers must both be connected to the same LAN.

b. Determine which of you will play the server side and which of you will play the client side in this activity.

- The server side player opens **Packet Tracer Multiuser - Tutorial - Server Side.pka**.
- The client side player opens **Packet Tracer Multiuser - Tutorial - Client Side.pka**.

Note: Solo players can open both files and complete the steps for both sides.

Step 2: Server Side Player - Configure the server side of the PTMU link.

The client side player must have the IP address, port number, and password used by the server side player before the client side player can create a connection to the server side player.

a. Configure Packet Tracer to be ready for an incoming connection by completing the following steps:

1) Click the **Extensions** menu, then **Multiuser**, then **Listen**.
2) You have two Local Listening Addresses. If there are more than two listed, refer to the first two only. The first one is the real IP address of the server side player's local machine. It is the IP address your computer uses to send and receive data. The other IP address (127.0.0.1) can only be used for communications within your own computer's environment.
3) The port number is listed next to your IP addresses and in the Port Number field. If this is the first instance of Packet Tracer you opened on your computer, then the port number will be 38000. However, if you have multiple instances open, it will increment by 1 for each instance (38001, 38002, etc.). The port number is required by the client side player to configure the multiuser connection.
4) The password is set to **cisco**, by default. You can change it, but it is not necessary for this activity.
5) Tell the client side player your IP address, port number, and password. The client side player will need these three pieces of information to connect to your Packet Tracer instance in Step 3.
6) In the **Existing Remote Networks** section, you must click **Always Accept** or **Prompt** radio button for the client side player to successfully connect.
7) In the **New Remote Networks** section, confirm that the **Always Deny** radio button is enabled. This will prevent the client side player from creating a new link that is not specified in this activity.
8) Click **OK**.

b. Click the **Multiuser Connection** icon (represented as a cloud with three lines). Then click the **Remote Network** icon and add a **Remote Network** to the topology.

c. Click the **Peer0** name and change it to **PTMU Link** (it is case-sensitive).

d. Click the **PTMU Link** cloud and verify that the Connection Type is **Incoming** and that the **Use Global Multiuser Password** check box is enabled.

e. Click the **Connections** icon and choose the solid-black **Copper Straight-Through** connection.

f. Click **S1** and choose the GigabitEthernet0/1 connection. Then click **PTMU Link** > **Create New Link**.

Step 3: Client Side Player - Configure the client side of the PTMU link.

a. Record the following information supplied to you by the server side player:

IP Address: ____

Port Number: ____

Password (**cisco**, by default) ___________________________

b. The client side player must add a **Remote Network** to the topology using the following directions: Click the **Multiuser Connection** icon (represented as a cloud with three lines). Then click the **Remote Network** icon and add a **Remote Network** to the topology.

c. Click the **Peer0** cloud and change the Connection Type to **Outgoing**.

1) In the Peer Address field, enter the server side IP address you recorded in Step 3a.

2) In the Peer Port Number field, enter the server side port number you recorded in Step 3a.

3) In the Peer Network Name field, enter **PTMU Link**. This is case-sensitive.

4) In the Password field, enter **cisco** or the password configured by the server side player.

5) Click **Connect**.

d. The **Peer0** cloud should now be yellow, indicating that the two instances of Packet Tracer are connected.

e. Click the **Connections** icon and choose the solid-black **Copper Straight-Through** connection.

f. Click **S2** and choose the **GigabitEthernet0/1** connection. Then click **Peer0** > **Link 0 (S1 GigabitEthernet 0/1)**.

The **Peer0** cloud on the client side player and the **PTMU Link** cloud on the server side player should now both be blue. After a short period, the link light between the switch and the cloud will transition from amber to green.

The multiuser link is now established and ready for testing.

Part 2: Verify Connectivity Across a Local Multiuser Connection

Step 1: Configure IP addressing.

a. The server side player configures the **www.ptmu.test** server with the IP address **10.10.10.1**, the subnet mask **255.0.0.0**, and the DNS server address **10.10.10.1**.

b. The client side player configures the PC with the IP address **10.10.10.10**, the subnet mask **255.0.0.0**, and the DNS server address **10.10.10.1**.

Step 2: Verify connectivity and access a web page on the server side.

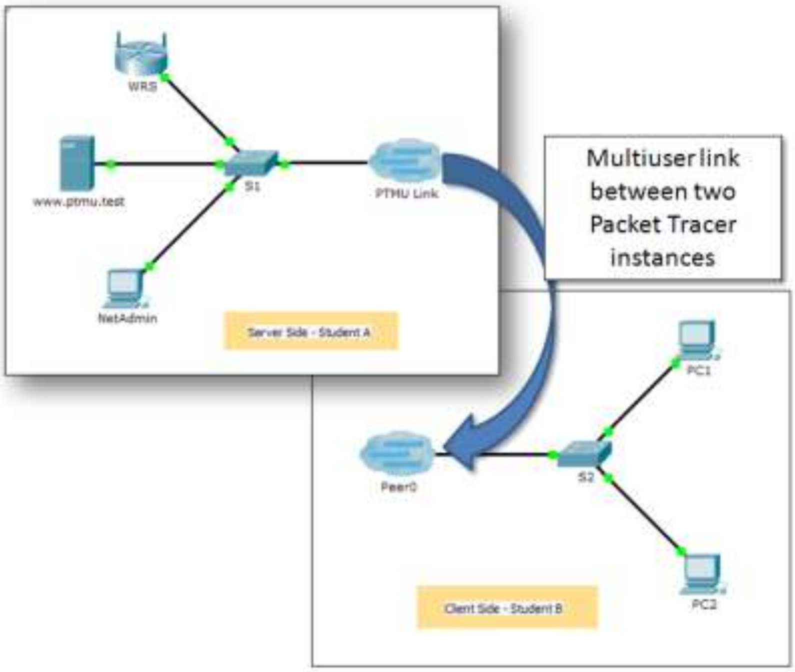
a. The server side player should now be able to ping the PC in the client side player instance of Packet Tracer.

b. The client side player should now be able to ping the **www.ptmu.test** server.

c. The client side player should also be able to open the web browser and access the web page at **www.ptmu.test**. What is displayed on the web page? Congratulations! You successfully verified a Packet Tracer multiuser connection.

Packet Tracer Multiuser - Implement Services (Instructor Version)

Topology



Addressing Table

Device	IP Address	Subnet Mask
Server Side Player		
WRS	172.16.1.254	255.255.255.0
S1	172.16.1.1	255.255.255.0
www.ptmu.test	172.16.1.5	255.255.255.0
NetAdmin	DHCP Assigned	DHCP Assigned
Client Side Player		
S2	172.16.1.2	255.255.255.0
PC1	DHCP Assigned	DHCP Assigned
PC2	DHCP Assigned	DHCP Assigned

Objectives

Part 1: Establish a Local Multiuser Connection to another Instance of Packet Tracer

Part 2: Server Side Player - Implement and Verify Services

Part 3: Client Side Player - Configure and Verify Access to Services

Background

Note: Completing the prior activities in this chapter, including the **Packet Tracer Multiuser - Tutorial**, are prerequisites to completing this activity.

In this multiuser activity, two students (players) cooperate to implement and verify services including DHCP, HTTP, Email, DNS, and FTP. The server side player will implement and verify services on one server. The client side player will configure two clients and verify access to services.

Part 1: Establish a Local Multiuser Connection to Another Instance of Packet Tracer

Step 1: Select a partner and determine the role for each student.

a. Find a fellow classmate with whom you will cooperate to complete this activity. Your computers must both be connected to the same LAN.

b. Determine which of you will play the server side and which of you will play the client side in this activity.

- The server side player opens **Packet Tracer Multiuser - Implement Services - Server Side.pka**.
- The client side player opens **Packet Tracer Multiuser - Implement Services - Client Side.pka**.

Note: Solo players can open both files and complete the steps for both sides.

Step 2: Configure the switches with initial configurations.

Each player: configure your respective switch with the following:

a. Hostname using the name in the addressing tables. (**S1** for the switch in the Server Side Player or **S2** for the switch in the Client Side Player). Change the Display Name of each switch to match the new hostname using the **Config** tab.

b. An appropriate message-of-the-day (MOTD) banner.

c. Privileged EXEC mode and line passwords.

d. Correct IP addressing, according to the Addressing Table.

e. Scoring should be 8/33 for the client side player and 8/44 for the server side player.

Step 3: Server Side Player - Configure the PTMU link and communicate addressing.

a. Complete the steps necessary to verify that the **PTMU Link** is ready to receive an incoming connection.

b. Communicate the necessary configuration information to the client side player.

Step 4: Client Side Player - Configure the outgoing multiuser connection.

a. Client side player: Record the following information supplied to you by the server side player:

IP Address: ____

Port Number: ____

Password (**cisco**, by default) ___________________________

b. Configure **Peer0** to connect to the server side player's **PTMU Link**.

c. Connect the **S2 GigabitEthernet0/1** to **Link0** on **Peer0**.

Step 5: Verify connectivity across the local multiuser connection.

a. The server side player should be able to ping S2 in the client side player's instance of Packet Tracer.

b. The client side player should be able to ping S1 in the server side player's instance of Packet Tracer.

c. Scoring should be 11/33 for the client side player and 9/44 for the server side player.

Part 2: Server Side Player - Implement and Verify Services

Step 1: Configure WRS as the DHCP server.

WRS provides DHCP services. Configure DHCP Server Settings with the following:

a. Starting IP address is **172.16.1.11**.

b. Maximum number of users is **100**.

c. **Static DNS 1** is **172.16.1.5**.

d. Verify **NetAdmin** received IP addressing through DHCP.

e. From **NetAdmin**, access the User Account Information web page at **172.16.1.5**. You will use this information to configure user accounts in Step 2.

f. Scoring should be 17/44 for the server side player.

Step 2: Configure services on www.ptmu.test.

The **www.ptmu.test** server provides the rest of the services and should be configured with the following:

a. Enable the DNS service and create a DNS record associating the IP address for **www.ptmu.test** server to the name www.ptmu.test.

b. Enable the Email services and create user accounts using the user list from Part 2 Step 1e. The Domain Name is **ptmu.test**.

c. Enable the FTP service and create user accounts using the user list from Part 2 Step 1e. Give each user permission to write, read, and list.

d. Scoring should be 38/44 for the server side player.

Step 3: Verify that all services are implemented according to the requirements.

From **NetAdmin**, complete the following:

a. Configure the email client for the NetAdmin user account. (Hint: Use www.ptmu.test for both the incoming and outgoing mail server.)

b. Send an email to the user at **PC1**.

c. Upload the **secret.txt** file to the FTP server. Do not change the file.

Note: The score for the server side player will be **43/44** until the client side player successfully downloads the **secret.txt** file, modifies the file, and then uploads it to the **www.ptmu.test** FTP server.

Part 3: Client Side Player - Configure and Verify Access to Services

Step 1: Configure and verify PC addressing.

a. Configure **PC1** and **PC2** to automatically obtain addressing.

b. PC1 and PC2 should be able to access the web page using the IP address, **http://172.16.1.5**, as well as the domain name, **http://www.ptmu.test**.

c. The score for the client side player should be 21/33.

Step 2: Configure and verify PC email accounts.

a. Configure email accounts according to the requirements at **www.ptmu.test/user.html**.

b. Verify that PC1 received an email from NetAdmin and send a reply.

c. Send an email from PC1 to PC2. **Note:** Scoring will not change.

d. Verify that PC2 received an email from PC1.

e. The score for the client side player should be 31/33.

Step 3: Upload and download a file from the FTP server.

a. From PC2, access the FTP server and download the **secret.txt** file.

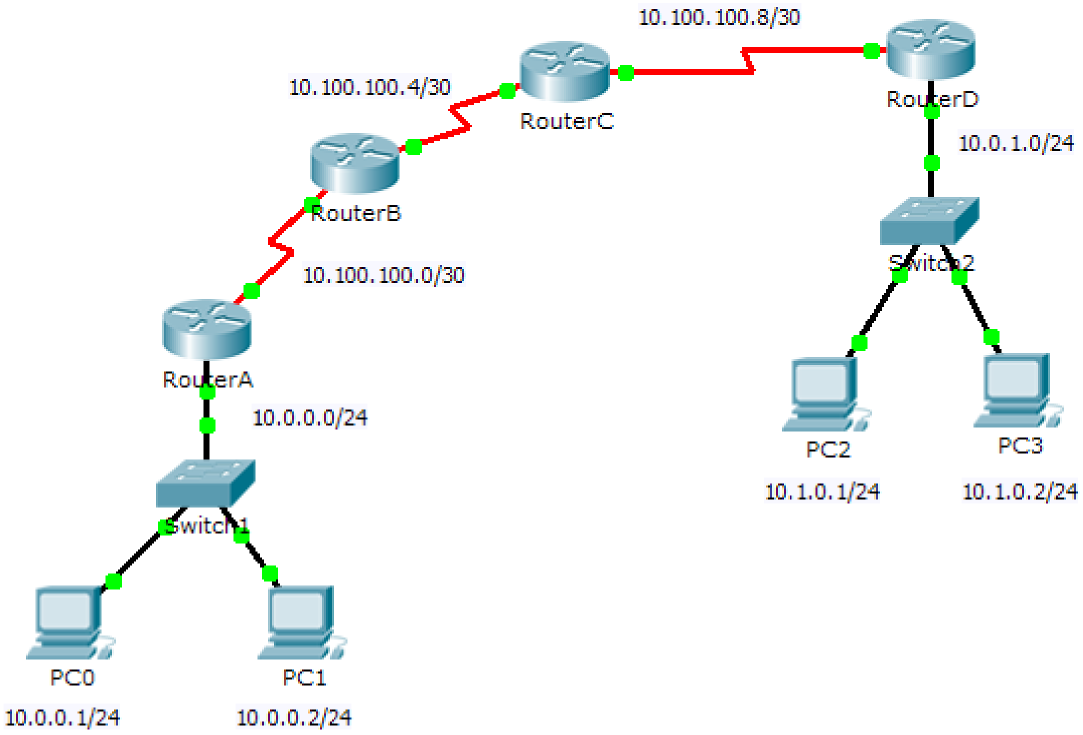
b. Open the **secret.txt** file, change only the secret word to **apple**, and upload the file.

c. The server side player score should be **44/44** and the client side player score should be **33/33**.

Packet Tracer - Testing Connectivity with Traceroute (Instructor Version)

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

Topology



Objectives

Part 1: Test End-to-End Connectivity with the tracert Command

Part 2: Compare to the traceroute Command on a Router

Background

This activity is designed to help you troubleshoot network connectivity issues using commands to trace the route from source to destination. You are required to examine the output of **tracert** (the Windows command) and **traceroute** (the IOS command) as packets traverse the network and determine the cause of a network issue. After the issue is corrected, use the **tracert** and **traceroute** commands to verify the completion.

Part 1: Test End-to-End Connectivity with the tracert Command

Step 1: Send a ping from one end of the network to the other end.

Click **PC1** and open the **Command Prompt**. Ping **PC3** at **10.1.0.2**. What message is displayed as a result of the ping? Destination host unreachable

Step 2: Trace the route from PC1 to determine where in the path connectivity fails.

a. From the **Command Prompt** of **PC1**, enter the **tracert 10.1.0.2** command.

b. When you receive the **Request timed out** message, press **Ctrl**+**C**. What was the first IP address listed in the **tracert** output? 10.0.0.254—the gateway address of the PC

c. Observe the results of the **tracert** command. What is the last address reached with the **tracert** command? 10.100.100.6

Step 3: Correct the network problem.

a. Compare the last address reached with the **tracert** command with the network addresses listed on the topology. The furthest device from the host 10.0.0.2 with an address in the network range found is the point of failure. What devices have addresses configured for the network where the failure occurred? RouterB and RouterC

b. Click **RouterC** and then the **CLI** tab.

c. What is the status of the interfaces? They appear to be up and active.

d. Compare the IP addresses on the interfaces with the network addresses on the topology. Does there appear to be anything extraordinary? The Serial 0/0/0 interface has an incorrect IP address based on the topology.

e. Make the necessary changes to restore connectivity; however, do not change the subnets. What is solution? Change the IP address on S0/0/0 to 10.100.100.9/30

Step 4: Verify that end-to-end connectivity is established.

a. From the **PC1 Command Prompt**, enter the **tracert 10.1.0.2** command.

b. Observe the output from the **tracert** command. Was the command successful? Yes

Part 2: Compare to the traceroute Command on a Router

a. Click **RouterA** and then the **CLI** tab.

b. Enter the **traceroute 10.1.0.2** command. Did the command complete successfully? Yes

c. Compare the output from the router **traceroute** command with the PC **tracert** command. What is noticeably different about the list of addresses returned? The router has one less IP address because it will be using RouterB as the next device along the path.

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Test End-to-End Connectivity with the **tracert** Command	Step 1	10	
	Step 2b	10	
	Step 2c	10	
	Step 3a	10	
	Step 3c	10	
	Step 3d	10	
	Step 3e	10	
	Step 4b	10	
	Part 1 Total	**80**	
Part 2: Compare to the **traceroute** Command on a Router	a	10	
	b	10	
	Part 2 Total	**20**	
	Total Score	**100**	

Packet Tracer - Using Show Commands (Instructor Version)

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

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.

Part 1: Analyze Show Command Output

Step 1: 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
```

Part 2: Reflection Questions

1. Which commands would provide the IP address, network prefix, and interface? show ip route, show interfaces, show protocols (before IOS 15, the show ip route command did not display the IP address of the interfaces)
2. Which commands provide the IP address and interface assignment, but not the network prefix? show ip interface brief
3. Which commands provide the status of the interfaces? show interfaces, show ip interface brief
4. Which commands provide information about the IOS loaded on the router? show flash, show version
5. Which commands provide information about the addresses of the router interfaces? show arp, show interfaces
6. Which commands provide information about the amount of and Flash memory available? show version
7. Which commands provide information about the lines being used for configuration or device monitoring? show users
8. Which commands provide traffic statistics of router interfaces? show interfaces
9. Which commands provide information about paths available for network traffic? show ip route
10. Which interfaces are currently active on the router? GigabitEthernet 0/0, Serial 0/0/1

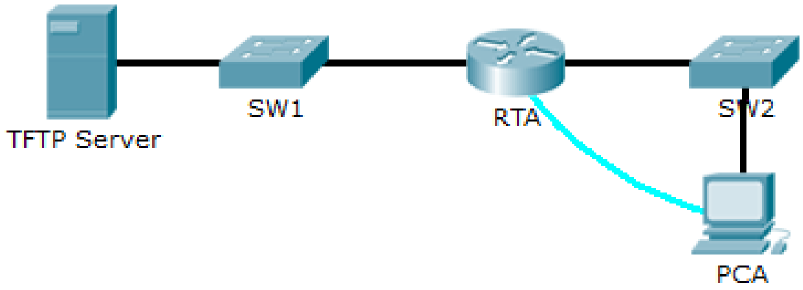
Suggested Scoring Rubric

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

Packet Tracer - Backing Up Configuration Files (Instructor Version)

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

Topology



Objectives

Part 1: Establish Connectivity to TFTP Server

Part 2: Transfer Configuration from TFTP Server

Part 3: Backup Configuration and IOS to TFTP Server

Background / Scenario

This activity is designed to show how to restore a configuration from a backup and then perform a new backup. Due to an equipment failure, a new router has been put in place. Fortunately backup configuration files have been saved to a Trivial File Transfer Protocol (TFTP) Server. You are required to restore the files from the TFTP Server to get the router back online with as little down time as possible.

Part 1: Establish Connectivity to the TFTP Server

Note: Because this is a new router, initial configuration will be performed using a console connection to the router.

a. Click **PCA**, then the **Desktop** tab, followed by **Terminal** to access the **RTA** command line.

b. Configure and activate the **Gigabit Ethernet 0/0** interface. The IP address should match the default gateway for the **TFTP Server**.

c. Test connectivity to **TFTP Server**. Troubleshoot, if necessary.

Part 2: Transfer Configuration from the TFTP Server

a. From privileged EXEC mode, issue the following command:

```
Router# copy tftp running-config
Address or name of remote host []? 172.16.1.2
Source filename []? RTA-confg
Destination filename [running-config]? <cr>
```

The router should return the following:

```
Accessing tftp://172.16.1.2/RTA-confg...
```

```
Loading RTA-confg from 172.16.1.2: !
[OK - 785 bytes]
785 bytes copied in 0 secs
RTA#
%SYS-5-CONFIG_I: Configured from console by console
RTA#
```

b. Issue the command to display the current configuration. What changes were made? The configuration stored on the TFTP Server was loaded into the router.

c. Issue the appropriate **show** command to display the interface status. Are all interfaces active? No, Gi0/1 is administratively down. All router interfaces are shutdown by default.

d. Correct any issues related to interface problems and test connectivity.

Part 3: Backup Configuration and IOS to TFTP Server

a. Change the hostname of **RTA** to **RTA-1**.

b. Save the configuration to NVRAM.

c. Copy the configuration to the **TFTP Server** using the **copy** command:

```
RTA-1# copy running-config tftp:
Address or name of remote host []? 172.16.1.2
Destination filename [RTA-1-confg]? <cr>
```

d. Issue the command to display the files in flash.

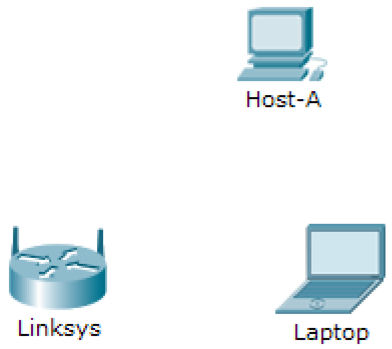
e. Copy the IOS in flash to the **TFTP Server** using the following command:

```
RTA-1# copy flash tftp:
Source filename []? c1900-universalk9-mz.SPA.151-4.M4.bin
Address or name of remote host []? 172.16.1.2
Destination filename [c1900-universalk9-mz.SPA.151-4.M4.bin]? <cr>
```

Packet Tracer - Configuring a Linksys Router (Instructor Version)

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

Topology



Objectives

Part 1: Connect to Linksys router

Part 2: Enable Wireless Connectivity

Part 3: Configure and Verify Wireless Client Access

Background

In this activity, you will configure a Linksys wireless router, allowing remote access to wireless clients as well as connectivity with WPA security.

Part 1: Connect to Linksys Router

Step 1: Establish and verify connectivity to the Linksys router.

a. Connect the appropriate cable from **Host-A** to the Ethernet 1 port on **Linksys**.

b. Wait for the link light to turn green. Then open the command prompt for **Host-A**. Use the **ipconfig** command to verify **Host-received** IP addressing information.

c. Enter the command **ping 192.168.0.1** to verify **Host-A** can access the default gateway.

Step 2: Access the Linksys graphical user interface (GUI) using a web browser.

a. To configure the **Linksys** router using the GUI, you will need to access it using the **Host-A** web browser. Open the web browser and access **Linksys** by entering the default gateway address in the URL field.

b. Enter **admin** as the default username and password to access the **Linksys** router.

Note: You will not see your score change when configuring the **Linksys** router until you click **Save Settings**.

Part 2: Enable Wireless Connectivity

Step 1: Configure the Linksys router for Internet connectivity.

There is no Internet connectivity in this scenario, but you will still configure the settings for the Internet-facing interface. For **Internet Connection Type**, choose **Static IP** from the drop down list. Then enter the following static IP information:

- Internet IP Address - **198.133.219.1**
- Subnet Mask - **255.255.255.0**
- Default Gateway - **198.133.219.254**
- DNS 1 - **198.133.219.10**

Step 2: Configure the inside network parameters.

Scroll down to the **Network Setup** section and configure the following information:

- IP Address - **172.31.1.1**
- Subnet Mask - **255.255.255.224**
- Starting IP Address - Enter **5** for the last octet.
- Maximum number of Users – **25**

Note: The IP address range of the DHCP pool will only reflect the changes once you click '**Save Settings**'

Step 3: Save the settings and reconnect to the Linksys router.

a. Scroll to the bottom of the page and click **Save Settings**. If you move from one tab to another without saving, your configurations will be lost.

b. You lose your connection when you click **Save Settings**. This occurred because you changed the IP address of the router.

c. Return to the command prompt of **Host-A**. Enter the command **ipconfig /renew** to renew the IP address.

d. Use the **Host-A** web browser to reconnect to the **Linksys**. You will need to use the new default gateway address. Verify the **Internet Connection** settings in the **Status** tab. The settings should match the values you configured in Part 2, Step 1. If not, repeat Part 2, Step 1 and Step 2.

Step 4: Configure wireless connectivity for wireless devices.

a. Click the **Wireless** tab and investigate the options in the dropdown list for **Network Mode**.

When would you choose to the **Disable** option? When you do not have wireless devices.

When would you choose the **Mixed** option? When you have wireless devices that consist of B, G or N.

b. Set the network mode for **Wireless-N Only**.

c. Change the SSID to **MyHomeNetwork.**

What are two characteristics of the SSID? It is case sensitive and the name cannot exceed 32-characters

d. When a wireless client surveys the area searching for wireless networks, it detects any SSID broadcasts. SSID broadcasts are enabled by default.

If the SSID of an access point is not being broadcast, how will devices connect to it? The client must be configured with the name and correct spelling in order to make a connection.

e. For best performance in a network using Wireless-N, set the radio band to **Wide-40MHz.**

f. Click **Save Settings** and then click **Continue**.

Step 5: Configure wireless sercurity so that clients must authenticate to connect to the wireless network.

a. Click the **Wireless Security** option under the **Wireless** tab.

b. Set the **Security Mode** to **WPA2 Personal**.

What is the difference between personal and enterprise? Enterprise uses a Radius server to authenticate users, whereas personal mode uses the Linksys router to authenticate users.

c. Leave the encryption mode to AES and set the passphrase to **itsasecret.**

d. Click **Save Settings** and then click **Continue**.

Step 6: Change the default password to access the Linksys for configuration.

a. You should always change the default password. Click the **Administration** tab and change the **Router Access** password to **letmein.**

b. Click **Save Settings**. Enter the username **admin** and the new password.

Part 3: Configure and Verify Wireless Client Access

Step 1: Configure Laptop to access the wireless network.

a. Click **Laptop** and click **Desktop** > **PC Wireless**. The window that opens in the client Linksys GUI.

b. Click the **Connect** tab and click **Refresh**, if necessary. You should see **MyHomeNetwork** listed under Wireless Network Name.

c. Click **MyHomeNetwork** and click **Connect**.

d. You should now see **MyHomeNetwork**. Click it and then **Connect**.

e. The **Pre-shared Key** is the password you configured in Part 2, Step 5c. Enter the password and click **Connect**.

f. Close the Linksys GUI and click **Command Prompt**. Enter the command **ipconfig** to verify **Laptop** received IP addressing.

Step 2: Verify connectivity between Laptop and Host-A.

a. Ping the **Linksys** router from the **Laptop**.

b. Ping **Host-A** from the **Laptop.**

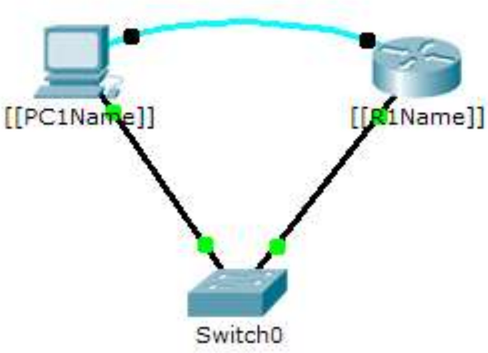
Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 2: Enable Wireless Connectivity	Step 4	4	
	Step 5	1	
	Part 2 Total	**5**	
	Packet Tracer Score	**95**	
	Total Score	**100**	

Packet Tracer - Skills Integration Challenge (Instructor Version)

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

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
[[R1Name]]	G0/0	[[R1Add]]	255.255.255.0
[[PC1Name]]	NIC	[[PC1Add]]	255.255.255.0

Scenario

The network administrator has asked you to prepare a router for deployment. Before it can be connected to the network, security measures must be enabled. In this activity, you will encrypt and configure strong passwords. You will then configure SSH for remote access and demonstrate that you can access the router from a PC.

Requirements

- Configure IP addressing on **[[PC1Name]]** and **[[R1Name]]**.
- Configure the hostname as **[[R1Name]]** and encrypt all plain text passwords.
- Set a strong secret password of your choosing.
- Set the domain name to **[[R1Name]]** (case-sensitive).

```
[[R1Name]](config)# ip domain-name [[R1Name]]
```

- Create a user of your choosing with a strong password.

```
[[R1Name]](config)# user any_user password any_password
```

- Generate 1024-bit RSA keys.

Note: In Packet Tracer, enter the **crypto key generate rsa** command, and press **Enter** to continue.

```
[[R1Name]](config)# crypto key generate rsa
The name for the keys will be: [[R1Name]].[[R1Name]]
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

- Block anyone for three minutes who fails to log in after four attempts within a two-minute period.

```
[[R1Name]](config)# login block-for 180 attempts 4 within 120
```

- Configure the vty lines for SSH access and require the local user profiles.

```
[[R1Name]](config-line)# transport input ssh
[[R1Name]](config-line)# login local
```

- Save the configuration to NVRAM.
- Be prepared to demonstrate to your instructor that you have established SSH access from **[[PC1Name]]** to **[[R1Name]]**.

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