Experiment 1

Aim: To construct and understand RJ45 connectors.

Theory:

T568A and T568B are standards for wiring twisted-pair network cabling using 8P8C connectors, commonly known as RJ45. They define the pinout, or the order of wire connections, for Ethernet cables. T568A and T568B differ in the arrangement of pairs 2 and 3, affecting compatibility with certain networking equipment.

Tools and Materials:

a. Twisted-pair cable (Cat5, Cat5e, Cat6)
b. RJ45 connectors
c. Cable stripper
d. Crimping tool
e. Cable tester (optional but recommended)

Procedure:

1. Cut the Cable:
   Use a crimping tool to cut the cable to the desired length.

2. Strip the Cable:
   Remove about 1 inch (2.5 cm) of the outer jacket from the cable end using a cable stripper.

3. Untwist and Arrange Wires:
   Untwist the wire pairs and arrange them according to the T568A or T568B standard. Flatten them between your fingers to maintain the order.

4. Trim the Wires:
   Trim the wires evenly, leaving about 0.5 inches (1.3 cm) exposed beyond the jacket.

5. Insert Wires into Connector:
   With the RJ45 connector clip facing down, carefully insert the wires into the connector slots.

Safaan Shawl
A2305222148

6. Crimp the Connector:
   Place the RJ45 connector into the crimping tool and squeeze firmly to secure it onto the cable.

7. Test the Cable:
   Use a cable tester to verify the wiring and ensure the cable functions properly.

Pinout for T568A:

1. White/Green
2. Green
3. White/Orange
4. Blue
5. White/Blue
6. Orange
7. White/Brown
8. Brown

Pinout for T568B:

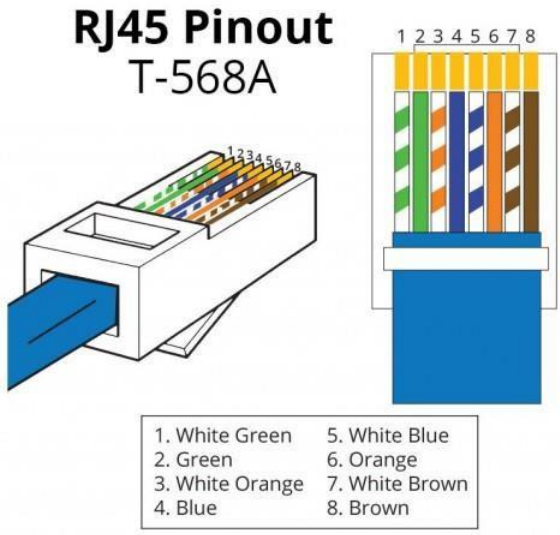
1. White/Orange
2. Orange
3. White/Green
4. Blue
5. White/Blue
6. Green
7. White/Brown
8. Brown

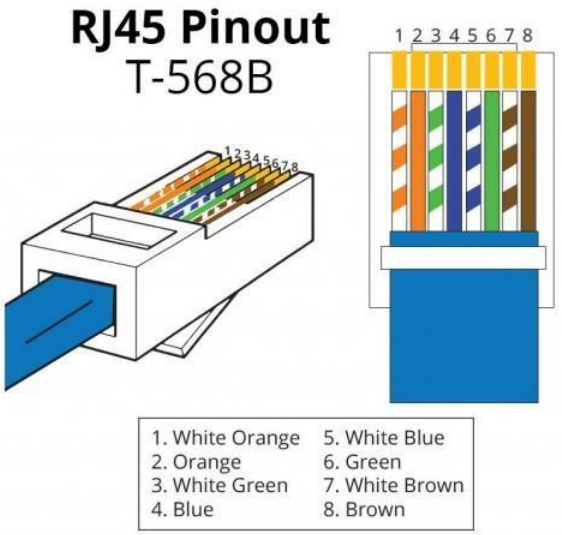
Building a Straight-Through Cable:

Use the same wiring standard (either T568A or T568B) on both ends of the cable.

Building a Crossover Cable:

Use the T568A wiring standard on one end and the T568B wiring standard on the other end.





Safaan Shawl
A2305222148

Experiment 2

Aim: Navigate the IOS (Packet Tracer 2.3.7)

Theory:

In this exercise, the objective is to familiarize yourself with the Cisco IOS by learning to access and navigate the Command Line Interface (CLI). This includes establishing basic connections, exploring different EXEC modes (User and Privileged), and using the Help system to understand commands. Additionally, the exercise involves practical tasks such as setting the system clock and demonstrating how to apply basic configuration commands.

Instructions:

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

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 from it.

c. Click **PC1**. A window displays an option for an RS-232 connection. Connect the cable to the RS-232 port.

d. Drag the other end of the console connection to the S1 switch and click the switch to access 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?

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

What is the prompt displayed on the screen?

Step 3: Explore the IOS Help.

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

S1> **?**

Which command begins with the letter ‘C’?

Safaan Shawl
A2305222148

b. At the prompt, type t and then a question mark (?).

S1> **t?**

Which commands are displayed?

At the prompt, type te and then a question mark (?).

S1> **te?**

Which commands are displayed?

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

Part 2: Explore EXEC Modes

In Part 2 of this activity, you will 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 for the **enable** command?

b. Type **en** and press the **Tab** key.

S1> **en<Tab>**

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

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

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

c. Enter the **enable** command and press ENTER.

How does the prompt change?

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

S1# **?**

One command starts with the letter 'C' in user EXEC mode.

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

Step 2: Enter Global Configuration mode

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

S1# **configure**

What is the message that is displayed?

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

How does the prompt change?

c. This is called global configuration mode. This mode will be explored further in upcoming activities and labs.

Safaan Shawl
A2305222148

For now, return to privileged EXEC mode by typing **end**, **exit**, or **Ctrl-Z**.

S1(config)# **exit**
S1#

Part 3: Set 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?

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?

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

S1# **clock ?**

What information is displayed?

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

S1# **clock set ?**

What information is being requested?

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?

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 more parameters are needed.

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

The output returns a request for more information:

<1-31> Day of the month

MONTH Month of the year

f. Attempt to set the date to 01/31/2035 using the format requested. It may be necessary to request additional help using 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. 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 commands and record the messages:

Safaan Shawl
A2305222148

S1# **cl<tab>**

What information was returned?

S1# **clock**

What information was returned?

S1# **clock set 25:00:00**

What information was returned?

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

What information was returned?

Commands:

```
S1>?
Exec commands:
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  ssh         Open a secure shell client connection
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
S1>t?
telnet  terminal  traceroute
S1>tte?
% Unrecognized command
S1>en
S1>enable
S1# configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show clock
*10:36:22.372 UTC Mon Mar 1 1993
S1#clock ?
  set  Set the time and date
S1#clock ?
  set  Set the time and date
S1#clock set?
```

```
set
S1#clock set 15:00:00
% Incomplete command.
S1#clock set 15:00:00?
hh:mm:ss
S1#clock set 15:00:00 15 Jan 2004
S1#cl
S1#clclo
S1#clo
S1#show clock
15:1:43.273 UTC Thu Jan 15 2004
S1#?
Exec commands:
  clear       Reset functions
  clock       Manage the system clock
  configure   Enter configuration mode
  connect     Open a terminal connection
  copy        Copy from one file to another
  debug       Debugging functions (see also 'undebug')
  delete      Delete a file
  dir         List files on a filesystem
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  erase       Erase a filesystem
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  more        Display the contents of a file
  no          Disable debugging informations
  ping        Send echo messages
  reload      Halt and perform a cold restart
  resume      Resume an active network connection
  setup       Run the SETUP command facility
  show        Show running system information
 --More--
```

Safaan Shawl
A2305222148

Results:

File Edit Options View Tools Extensions Window Help

Activity Results

Congratulations Safaan You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All | Show Incorrect Items

Assessment Items	Status	Points	Component(s)	Feedback
Network	Correct	0	Other	

Safaan Shawl
A2305222148

Experiment 3

Aim: Configure Initial Switch Settings (Packet Tracer 2.5.5)

Theory:

In this exercise, the goal is to understand and apply basic configurations to a network switch. The exercise begins with verifying the default switch settings to establish a baseline. Next, it involves configuring fundamental settings such as hostname, passwords, and VLANs, which are essential for securing and managing the network environment. A Message of the Day (MOTD) banner is configured to provide important information or warnings to users accessing the switch. The final steps include saving the configuration changes to NVRAM to ensure they persist after a reboot and configuring an additional switch, S2, to replicate the setup and ensure network consistency.

Instructions:

Part 1: Verify the Default Switch Configuration

Step 1: Enter privileged EXEC mode.

You can access all switch 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.

The privileged EXEC command set includes the commands available in user EXEC mode, many additional commands, and the **configure** command through which access to the configuration modes is 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 to reflect privileged EXEC mode.

Step 2: Examine the current switch configuration.

Enter the show running-config command.

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

Answer the following questions:

How many Fast Ethernet interfaces does the switch have?

How many Gigabit Ethernet interfaces does the switch have?

What is the range of values shown for the vty lines?

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

Why does the switch respond with “startup-config is not present?”

Part 2: Create a Basic Switch Configuration

Safaan Shawl
A2305222148

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?

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.

Safaan Shawl
A2305222148

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 configuration by examining the contents of the running-configuration file:

S1# **show running-config**

Notice that the console and enable passwords are both in plain text. This could pose a security risk if someone is looking over your shoulder or obtains access to config files stored in a backup location.

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.

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**

What is displayed for the enable secret password?

Why is the enable secret password displayed differently from what we configured?

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.

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.

Safaan Shawl
A2305222148

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?

Why should every switch have a MOTD banner?

Part 4: Save and Verify Configuration Files to NVRAM

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

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?

Examine the startup configuration file.

Which command will display the contents of NVRAM?

Are all the changes that were entered recorded in the file?

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. Device name: **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 an appropriate message to those logging into the switch.

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.

Safaan Shawl
A2305222148

Commands:

```
Press RETURN to get started.
```

```
User Access Verification

Password:
% Password:  timeout expired!
```

```
Press RETURN to get started!
```

```
User Access Verification

Password:

S1>enable
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#enable password c1$c0
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
exit
User Access Verification

Password:
Password:

S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#service password-encryption
S1(config)#banner motd "This is a secure system"
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

```
S1 con0 is now available

Press RETURN to get started.
```

```
This is a secure system

User Access Verification

Password:

S1>enable
Password:
Password:
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

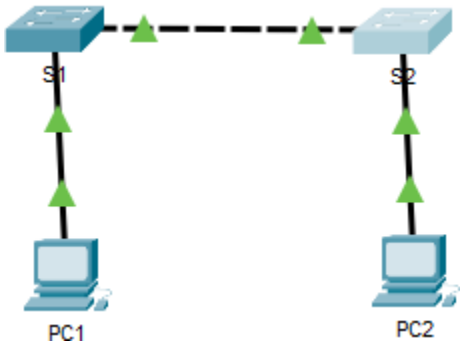
```
S1 con0 is now available

Press RETURN to get started.
```

```
User Access Verification

Password:

S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#enable secret itsasecret
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

```
S1 con0 is now available

Press RETURN to get started.
```

Safaan Shawl
A2305222148

Results:



Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All | Show Incorrect Items

Assessment Items	Status	Points	Component(s)	Feedback
Network				
S1				
Banner MOTD	Correct	6	Basic Security C...	
Console Line				
Login	Correct	4	Basic Security C...	
Password	Correct	4	Basic Security C...	
Enable Password	Correct	4	Basic Security C...	
Enable Secret	Correct	4	Basic Security C...	
Host Name	Correct	5	Hostname Config...	
Service Password Encryption	Correct	4	Basic Security C...	
Startup Config	Correct	5	Configuration Ma...	
S2				
Banner MOTD	Correct	6	Basic Security C...	
Console Line				
Login	Correct	4	Basic Security C...	
Password	Correct	4	Basic Security C...	
Enable Password	Correct	4	Basic Security C...	
Enable Secret	Correct	4	Basic Security C...	
Host Name	Correct	5	Hostname Config...	
Service Password Encryption	Correct	4	Basic Security C...	
Startup Config	Correct	5	Configuration Ma...	

Safaan Shawl
A2305222148

Experiment 4

Aim: - Implement Basic Connectivity

Theory: In this practical, we configured basic network settings for two switches, S1 and S2, and two PCs. We assigned hostnames, set console and privileged EXEC mode passwords, and saved configurations to NVRAM. The switches were configured with IP addresses to enable remote management. Connectivity between devices was verified using the ping command, ensuring proper communication within the network. This setup is foundational for managing and securing network infrastructure.

Instructions:

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 encrypted 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.

Question:
How can you verify that both passwords were configured correctly?
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 4: Save the configuration file to NVRAM.

Question:
Which command do you issue to accomplish this step?

Step 5: 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.

Safaan Shawl
A2305222148

Packet Tracer PC Command Line 1.0
PC> **ping 192.168.1.253**
Question:
Were you successful? Explain.

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 plug-and-play devices. This means that they do not need to be configured for them to work. Switches forward information from one port to another based on MAC addresses.
Question:
If this is the case, why would we configure it with an IP address?
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#
Question:
Why do you enter the **no shutdown** command?

Step 2: Configure S2 with an IP address.

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 all the switch ports and interfaces. You can also use the **show running-config** command.

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

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

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 and S2 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.

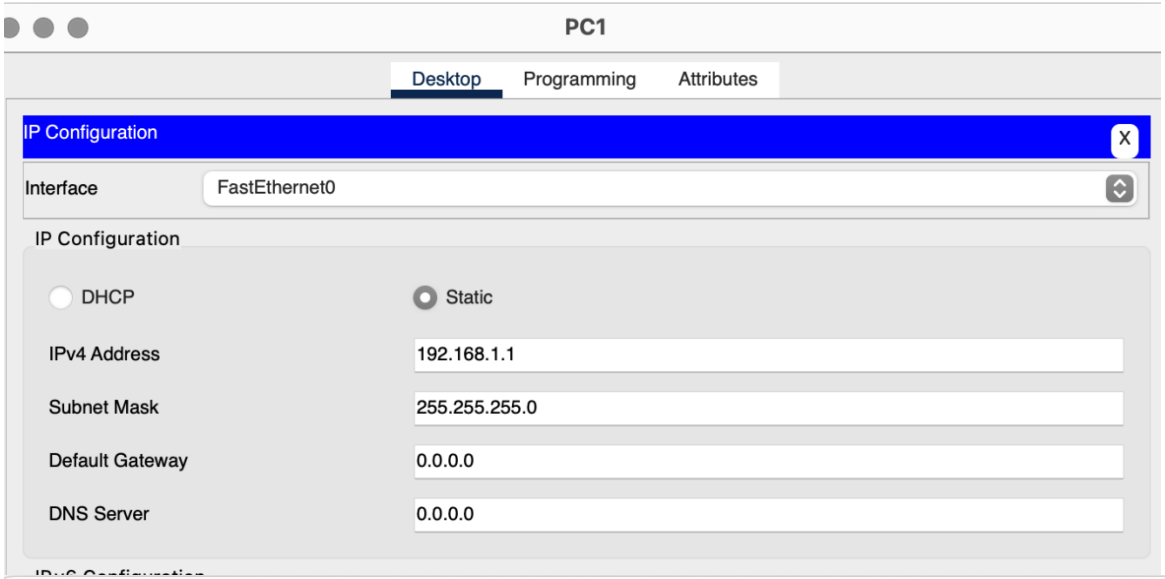
Note: You can also use the **ping** command on the switch CLI and on PC2.
All pings should be successful. If your first ping result is 80%, try again. It should now be 100%. You will learn why a ping may sometimes fail the first time later in your studies. If you are unable to ping any of the devices, recheck your configuration for errors.

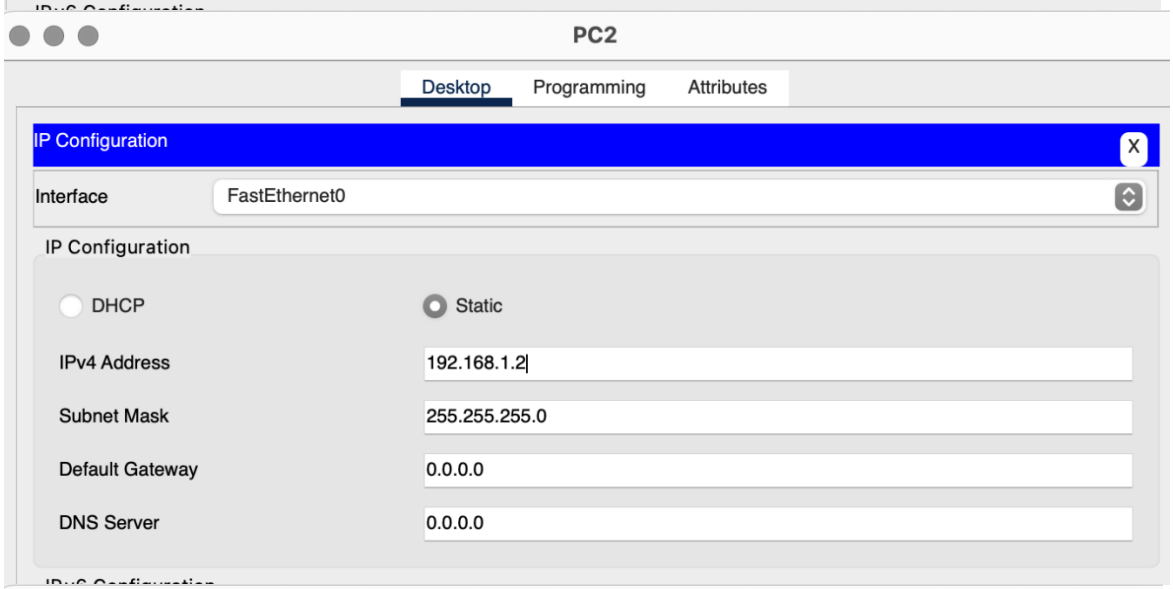
Safaan Shawl
A2305222148

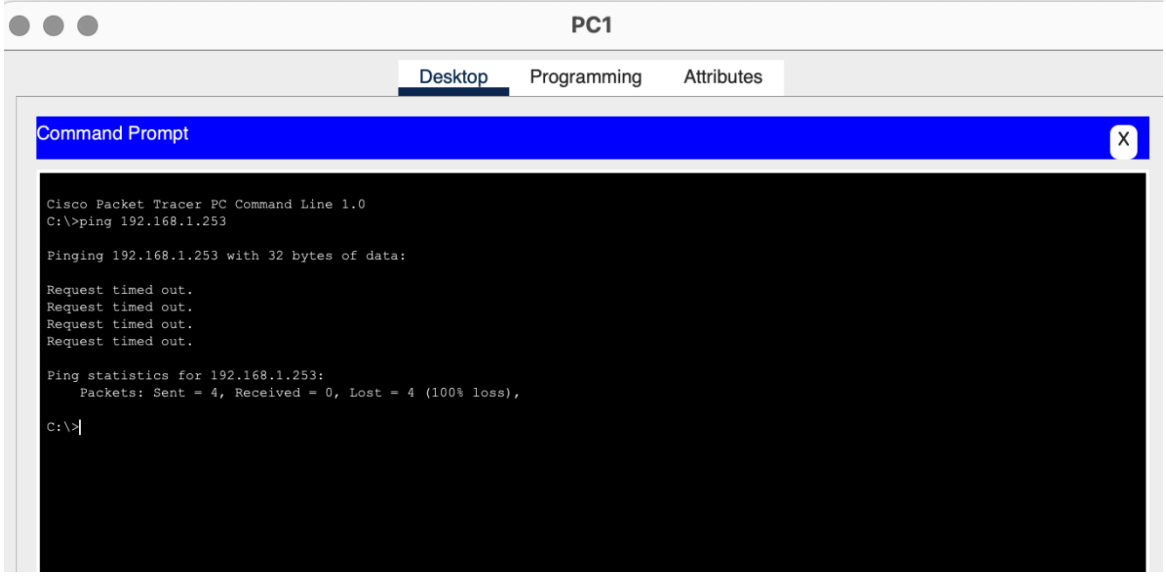
Commands:

```
Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

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

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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


Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
exit

User Access Verification

Password:
Password:

S1>enable
S1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#secret class
             ^
% Invalid input detected at '^' marker.

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

S1#exit


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 cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#enable secret class
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#banner motd "Authorized access only. Violators will be presecuted to the full extent of the law."
S2(config)#
?Bad filename
%Error parsing filename (Bad file number)
S2(config)#
```

Safaan Shawl
A2305222148





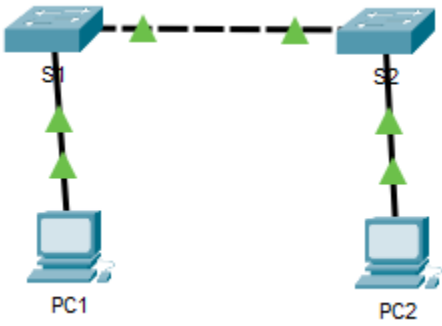


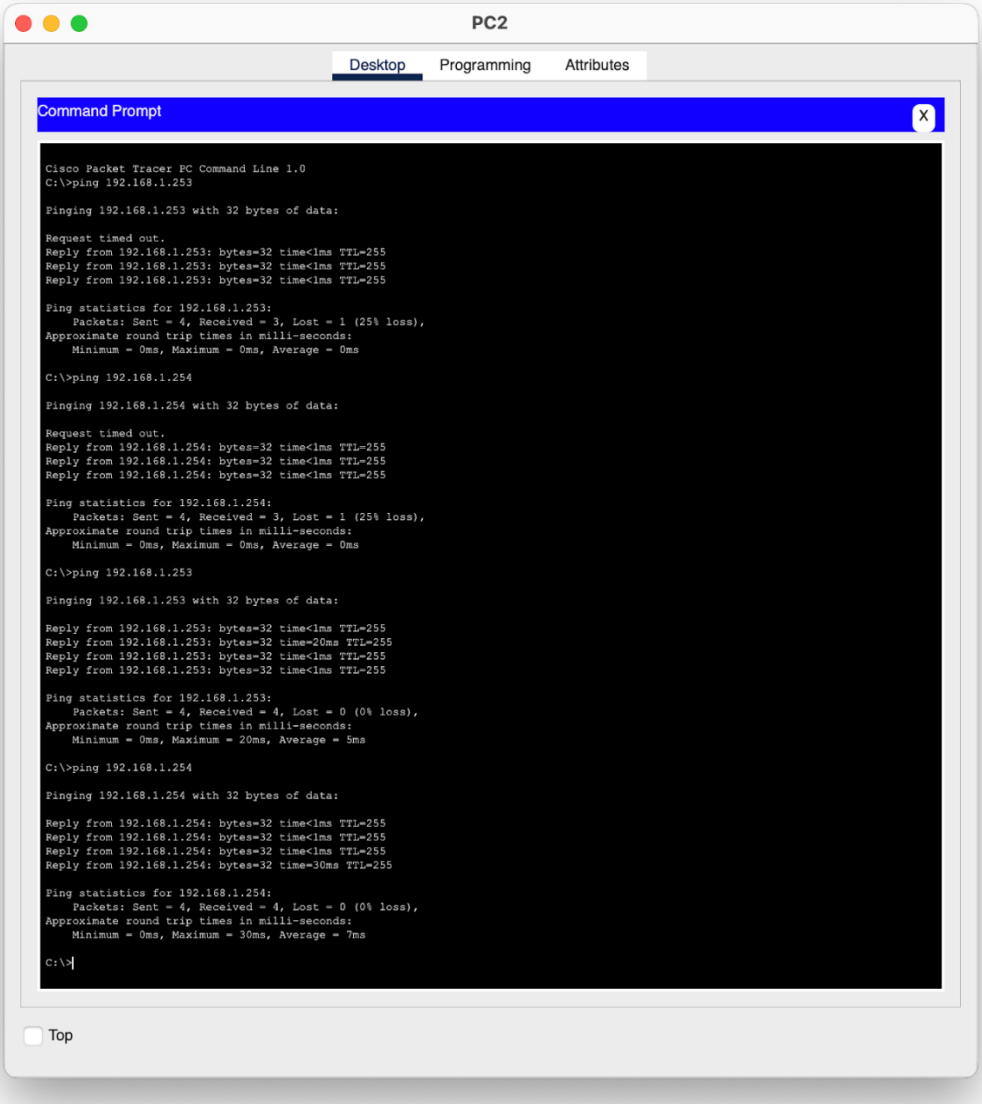
Safaan Shawl
A2305222148

```
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

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#exit
S1(config)#
S2(config)#interface vlan1
S2(config-if)#ip address 192.168.1.254 255.255.255.0
S2(config-if)#no shutdown

S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S2(config-if)#exit
S2(config)#
```

Safaan Shawl
A2305222148

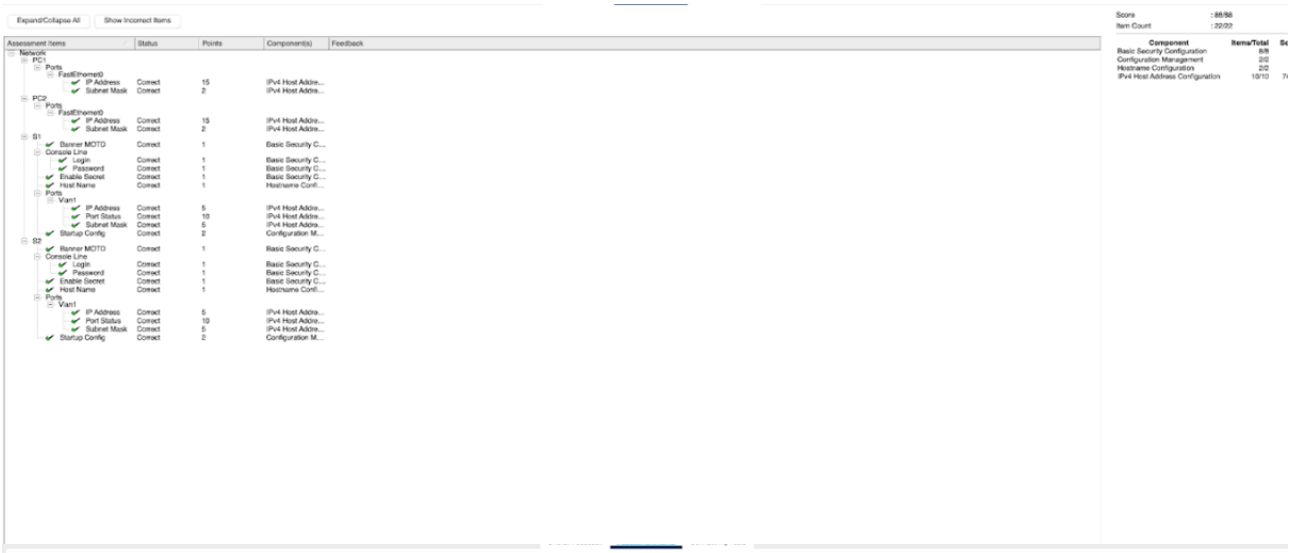
Results:

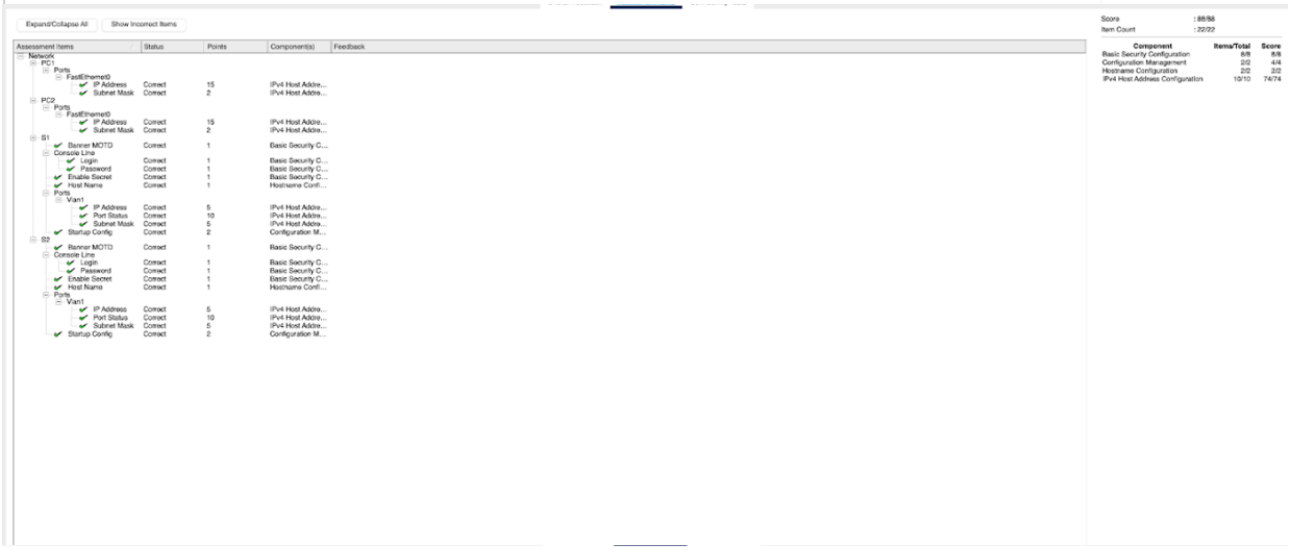




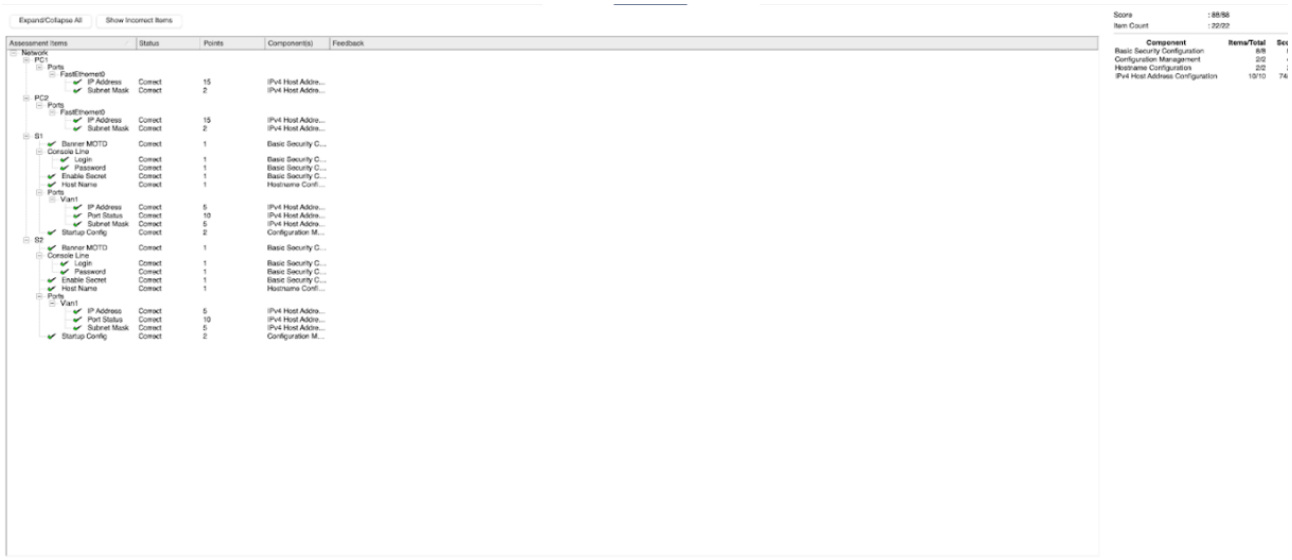
Safaan Shawl
A2305222148

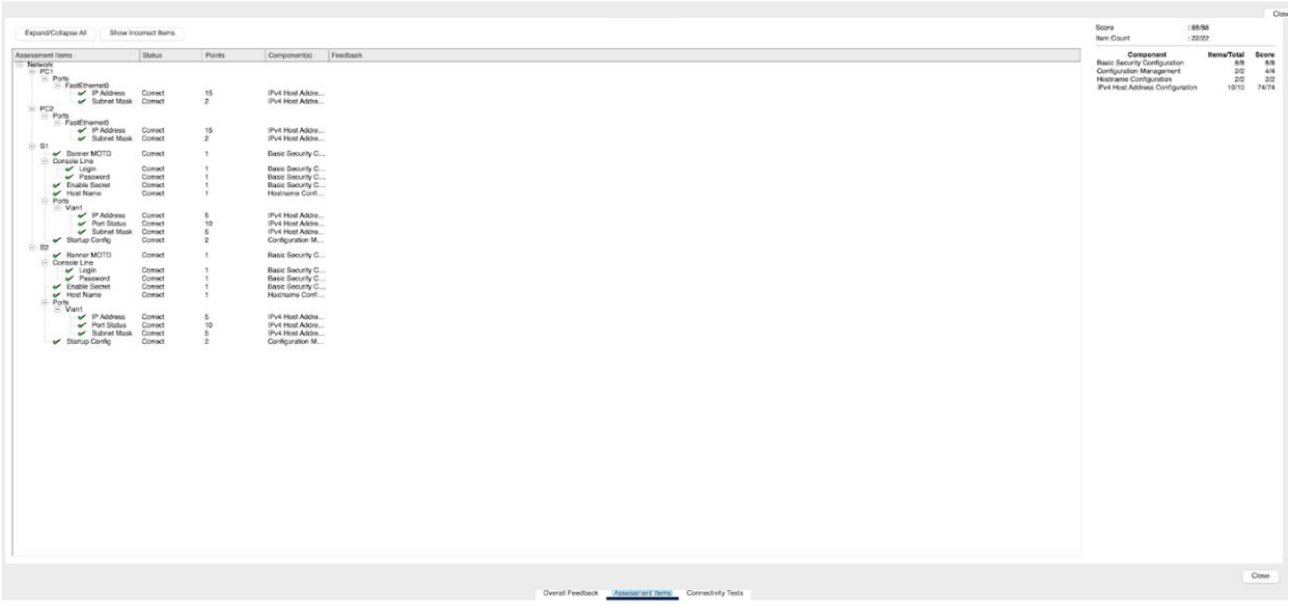
Safaan Shawl
A2305222148

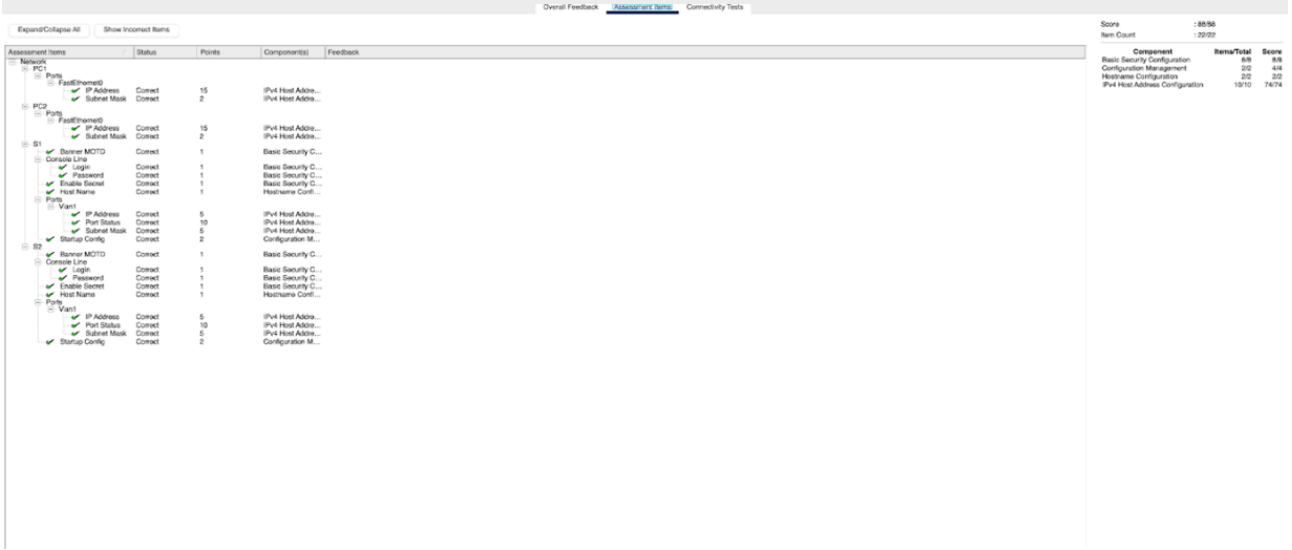




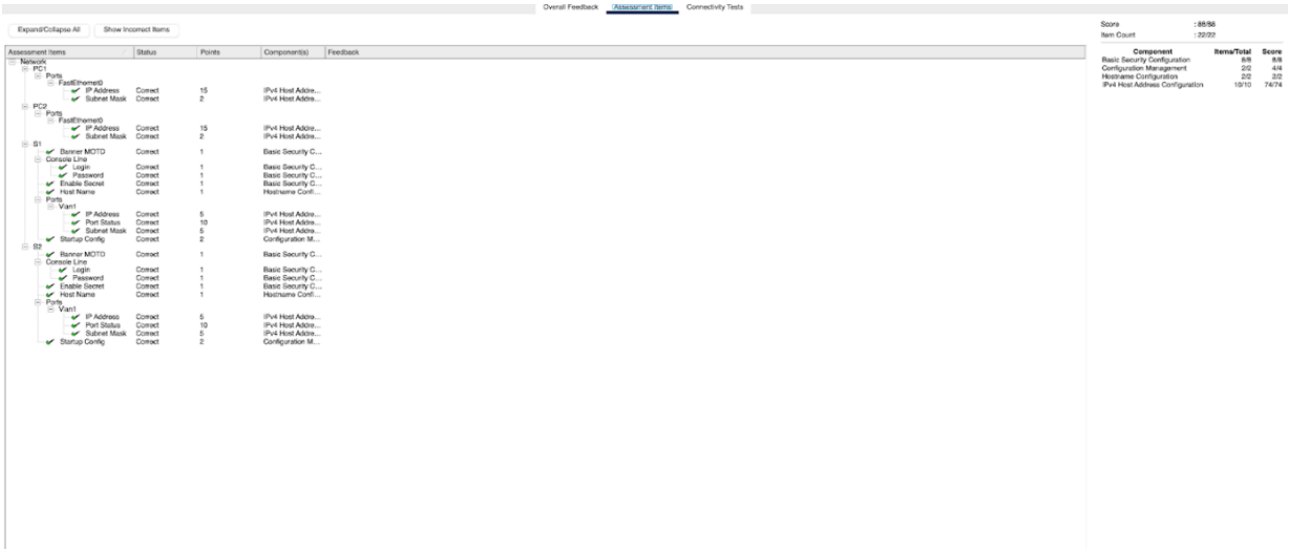
Safaan Shawl
A2305222148







Safaan Shawl
A2305222148



Safaan Shawl
A2305222148

Experiment 5

Aim: - Connect a Wired and Wireless LAN (Packet Tracer 4.6.5)

Theory: This experiment focuses on setting up and connecting a basic network using routers, switches, a cloud, a modem, and a wireless router. It involves selecting the correct cables, such as Copper Straight-Through, Coaxial, and Serial, to link devices like Router0 to a cloud switch, another router, and a configuration terminal. The experiment also covers connecting a Wireless Router to a Family PC and testing the network through pings and web access. Finally, the physical topology is examined, highlighting the connections and device placements in different network segments, reinforcing the importance of proper network design and verification.

Instructions:

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 F0/0 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 F0/1 to netacad.pka F0. 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.

Safaan Shawl
A2305222148

Part 3: Connect Remaining Devices

Step 1: Connect Router1 to Switch.

Choose the correct cable to connect Router1 F1/0 to Switch F0/1.

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 Cable 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?

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?

b. Click Back to return to Home City.

Safaan Shawl
A2305222148

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?

b. Click Back to return to Home City.

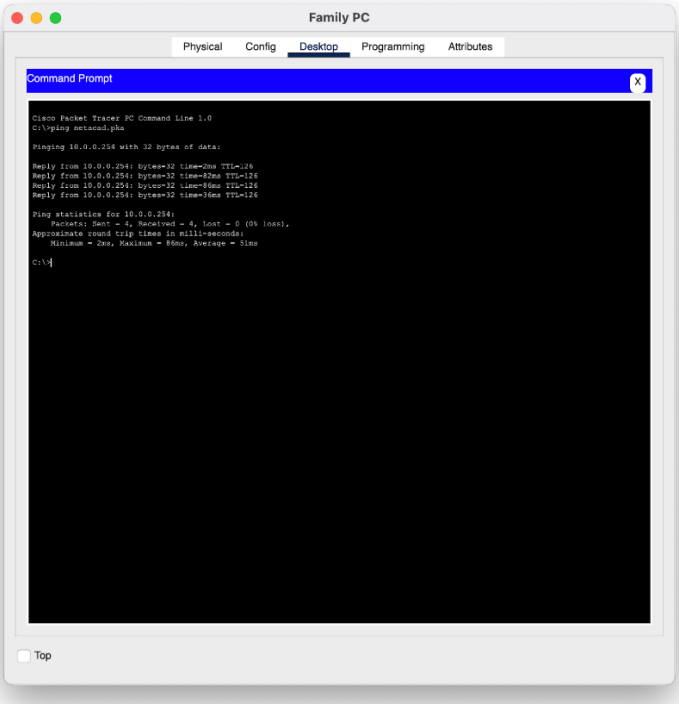
Step 4: Examine the Home Network.

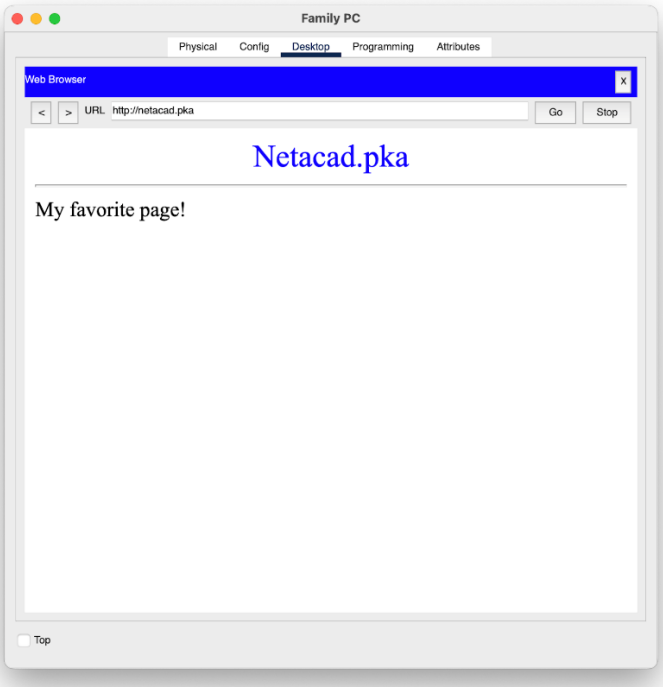
a. Click the Home Network icon.

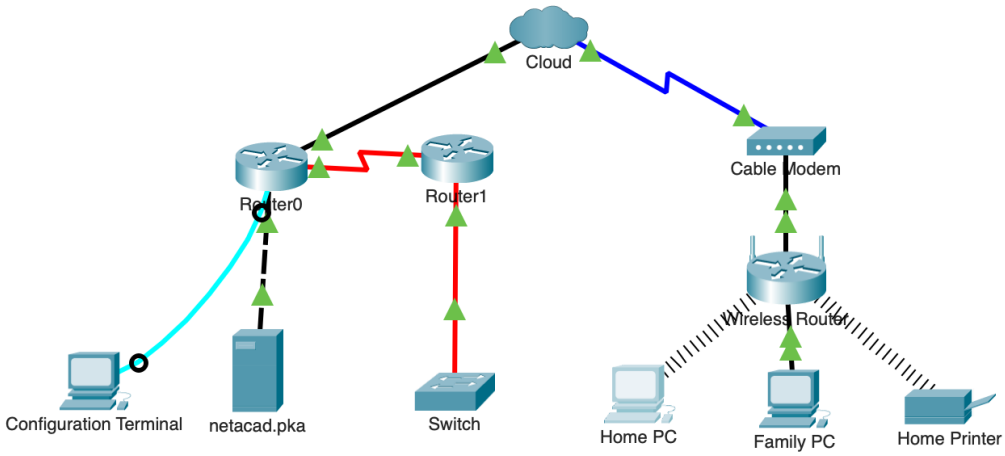
Why is there no rack to hold the equipment?

b. Click the Logical Workspace tab to return to the logical topology.

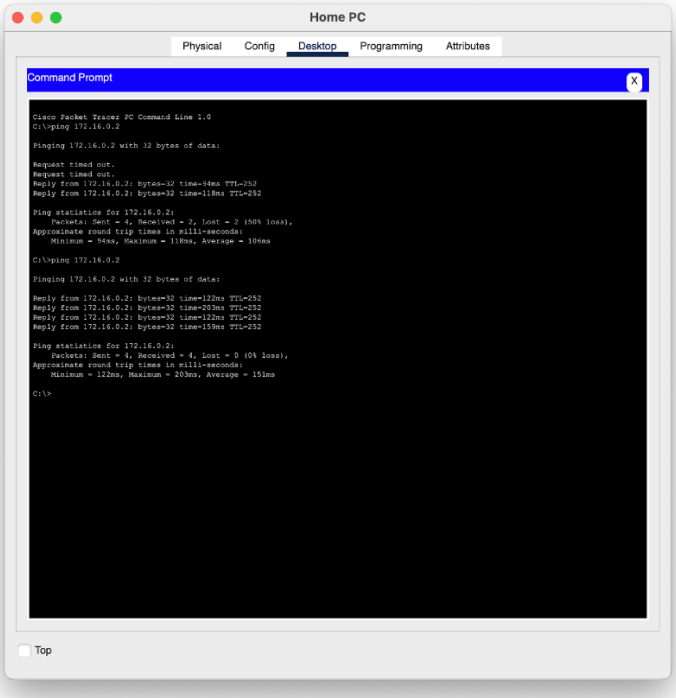
Commands/Results:

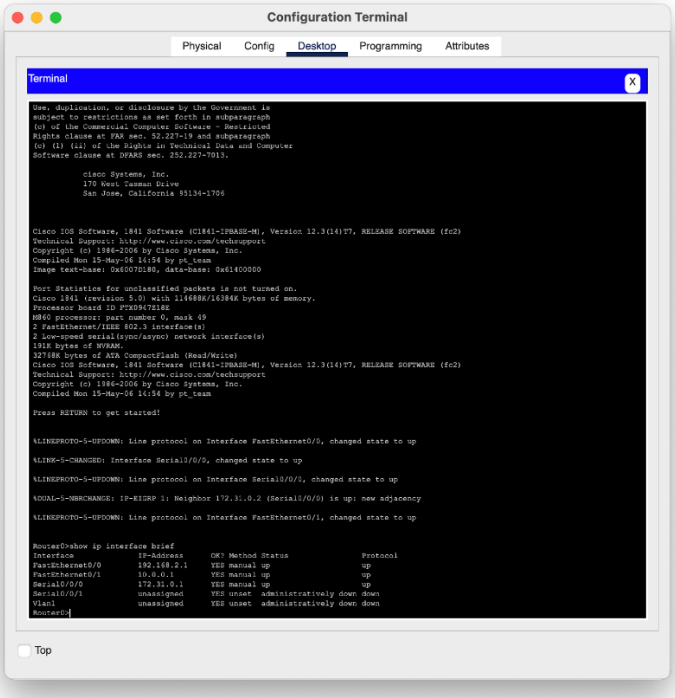


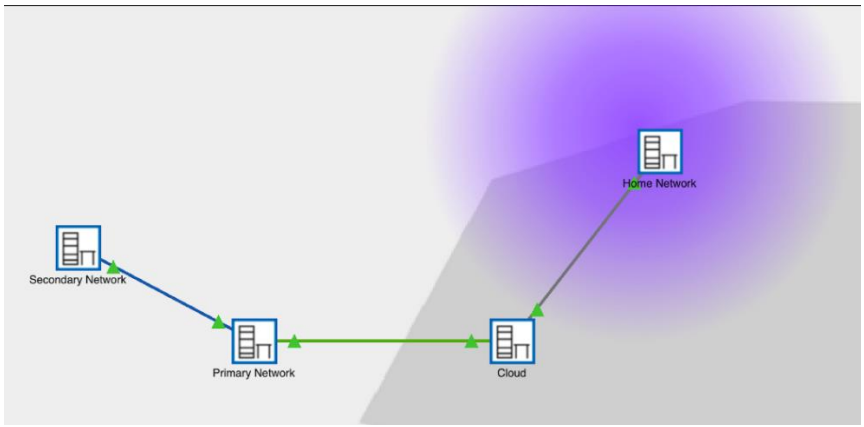


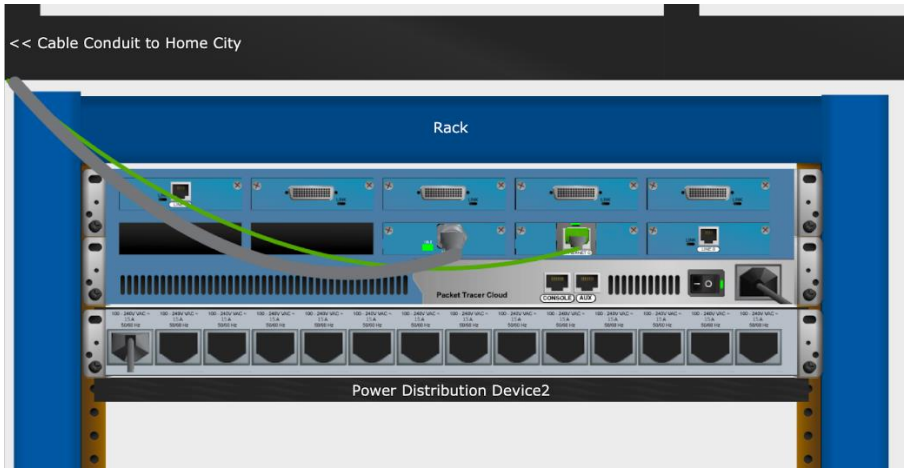


Safaan Shawl
A2305222148

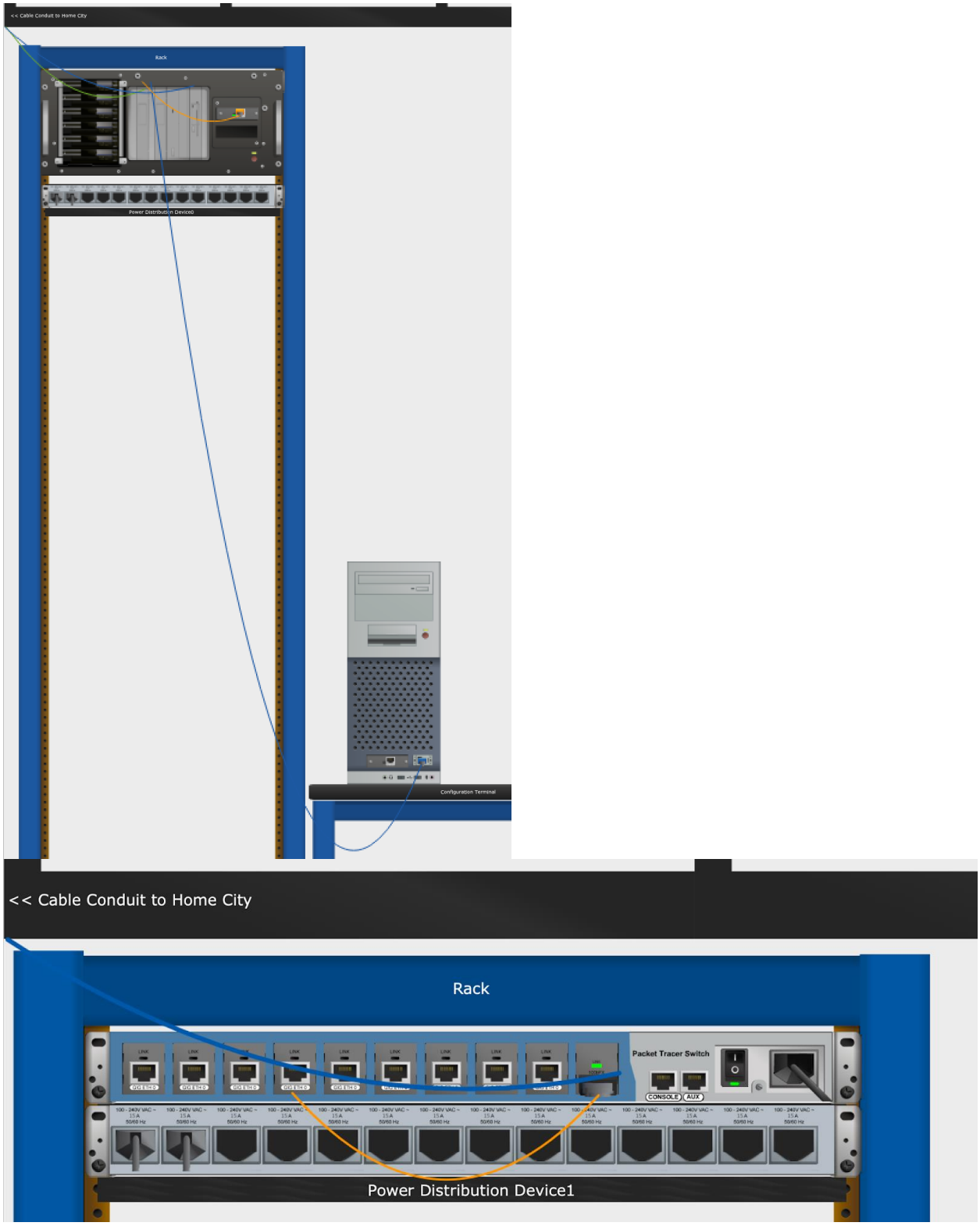




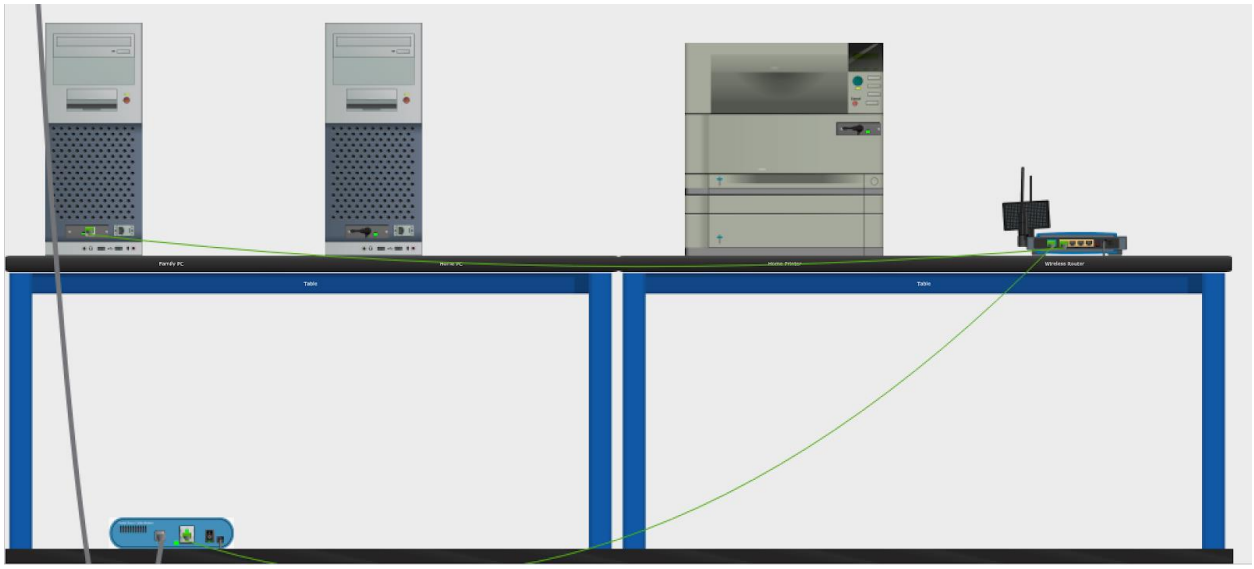




Safaan Shawl
A2305222148



Safaan Shawl
A2305222148



Expand/Collapse All | Show Incorrect Items

Assessment Items	Status	Points	Component(s)	Feedback
Network				
Cable Modem				
Ports				
Port 0		0	Other	
Link to Cloud		0	Other	
✔ Connects to Coaxial7	Correct	5	Device Connection	
Port 1		0	Other	
Link to Wireless Router		0	Other	
✔ Connects to Internet	Correct	5	Device Connection	
Cloud				
Ports				
Coaxial7		0	Other	
Link to Cable Modem		0	Other	
✔ Connects to Port 0	Correct	5	Device Connection	

Safaan Shawl
A2305222148

Experiment 6

Aim: - Packet Tracer - Physical Layer Exploration - Physical Mode (Packet Tracer 4.7.1)

Theory: In a home network, devices use private IPv4 addresses, like 192.168.0.75, to communicate locally. The router, often at 192.168.0.1, acts as the gateway between the local network and the internet, translating private IPs to a public IPv4 address. Tools like `ipconfig` and `tracert` allow users to identify their device's IP, the default gateway, and trace the path data takes to external servers. This process, called NAT (Network Address Translation), ensures efficient IP address management, while traceroute provides insights into each "hop" or router the data passes through on its journey to the destination server.

Instructions:

Part 1: Examine Local IP Addressing Information
Step 1: What is my IPv4 address?
Your IP address identifies your computer when sending and receiving packets, similar to how your home address is used to send and receive mail. Use the ipconfig command on Windows or the ifconfig command on macOS and Linux to find your IP address.

- IPv4 Address Example: 192.168.0.75 (Private IPv4 address)

Private IPv4 addresses are used to conserve the limited number of globally routable public IPv4 addresses.
Question:

- What is the IPv4 address and default gateway for your device?

Step 2: What is the IPv4 address for my router?
The ipconfig command shows the IPv4 address of your local router, also known as the default gateway.

- Example Router IPv4 Address: 192.168.0.1

This router connects your local home network to your Internet Service Provider's (ISP) network and provides internet access.
Question:

- What is the IPv4 address for your router?

Step 3: What is my public IPv4 address?
Private IPv4 addresses are not routable on the internet. When IP packets leave your network, they need to have their private IPv4 address replaced with a public IPv4 address.
Your local router performs this translation between private and public IPv4 addresses.
To find your public IPv4 address, search for "what is my IP" on the internet.
Question:

- List your public IPv4 address, location, and ISP.

Step 4: Examine the connections in your network.
Questions:

1. What does the connection look like between your device and your router? Is it wired or wireless?
2. Where is the router that your device uses to access the internet?
3. What does the connection look like between your router and the internet? Does it use a cable from the cable company, phone company, or is it wireless?
4. Can you find the cable as it leaves your house or see the remote tower if it is a wireless connection?

Search YouTube for "Tour of Home Network 2020 8-bit guy" to explore more.

Part 2: Trace the Path Between Source and Destination
Step 1: Use traceroute to display the path from Monterey to Hawaii.
Instructions:

1. In Packet Tracer, use the tracert www.hawaii.edu command to simulate a traceroute from Monterey, California, to the University of Hawaii.
2. On your own device, open a terminal and use the appropriate traceroute command for your operating system.

- Note: Real traceroute output will vary based on your location.

Safaan Shawl
A2305222148

Questions:

1. What is the IP address for your ISP's POP (Point of Presence)?

Step 2: Investigate the second hop in the traceroute output.
The second hop represents the first router outside your local network, typically belonging to your ISP.
Questions:

1. What is the IP address for your ISP's POP?
2. What is the technology for the local loop you are using (e.g., Cable, DSL, Satellite, Cellular)?

Step 3: Attempt to discover the physical location of the IP address for your ISP POP.
Use an "IP lookup" tool to gather information about your ISP's POP.

- Note: Geolocation information for IP addresses may not always be accurate.

Step 4: Investigate why geolocation information is not always accurate.
Search the internet for "600 million IP addresses Kansas" to explore the issue of incorrect geolocation data.
Step 5: Investigate the local ISP network.
Identify how many hops in your traceroute output belong to your local ISP.
Questions:

1. What is the IPv4 address of the 3rd hop in the Packet Tracer traceroute output?
2. Which router and interface in the Monterey building is configured with this IPv4 address?
3. What is the IPv4 address of the 4th hop in the Packet Tracer traceroute output?
4. Which router and interface in the Monterey building is configured with this IPv4 address?
5. Why do you think the IP addresses for the other interfaces are not shown in the traceroute output?
6. List the hops in your own traceroute output that belong to your local ISP.

Step 6: Investigate the domain names in the output to discover more clues about the location of routers at each hop.
Domain names in traceroute outputs can provide clues about the location of routers.
Questions:

1. What information, if any, can you decipher from the domain names for your local ISP?

Step 7: Investigate the link between Comcast and Internet2.
Traceroute output will often show the final hop within your ISP's network before packets are forwarded to another ISP, often occurring at an Internet Exchange Point (IXP).
Question:

1. What is the interface for the 10th hop in the traceroute?

Step 8: Investigate Internet2.

- Internet2 is a non-profit ISP focused on research and education. Learn more by searching the web for additional resources on this organization.

Question:

1. What speed is the Internet backbone that provides connections between Internet2 members?

Step 9: Investigate the link to Los Angeles.
The traceroute output may provide information about the next hop in the network, such as a router located in Los Angeles.
Question:

1. What is the interface used for the 11th hop in the traceroute output?

Step 10: Investigate the link across the Pacific Ocean.
The increase in roundtrip time indicates that packets are traveling a much greater distance. For example, packets traveling from Los Angeles to Hawaii might show a noticeable jump in time.
Questions:

1. How many submarine cables terminate at Hermosa Beach?
2. What is the name of the submarine cable that runs from Hermosa Beach to Hawaii?
3. What is the name of the landing point in Hawaii?
4. How many submarine cables terminate at this landing point in Hawaii?

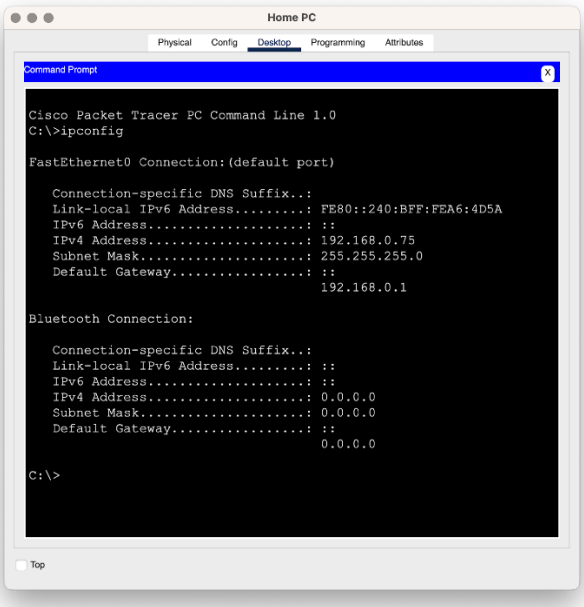
Step 11: Investigate the link between Internet2 and the University of Hawaii network.
The domain name in the traceroute output may indicate the router is part of the University of Hawaii network.
Question:

1. What interface is assigned to the 13th hop?

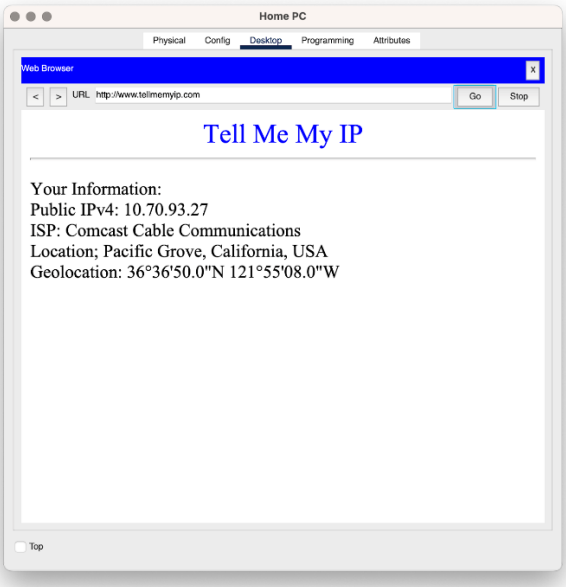
Step 12: Investigate the last known IP address in the traceroute output.
The traceroute may begin timing out after a certain point, as routers or firewalls might block traceroute messages. In this case, the route was traced from Monterey, California, all the way to the University of Hawaii in Honolulu.

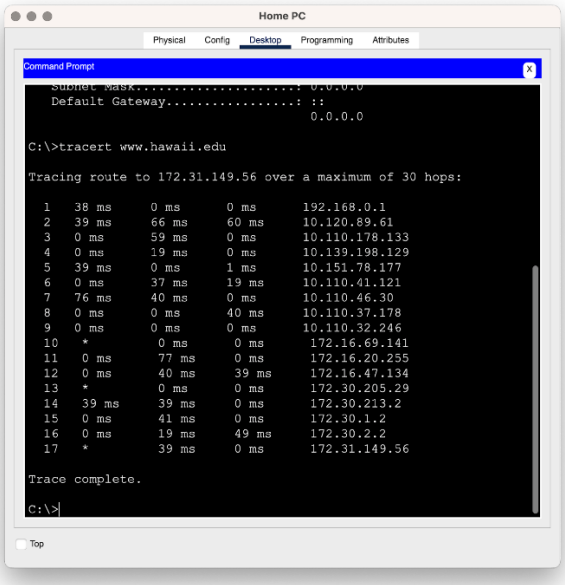
Safaan Shawl
A2305222148

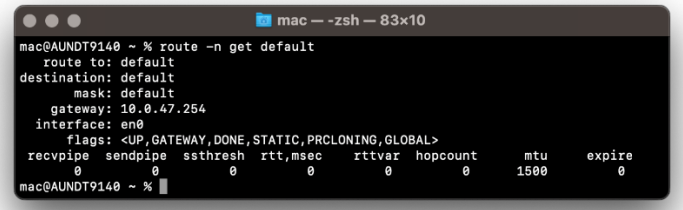
Commands/Results:

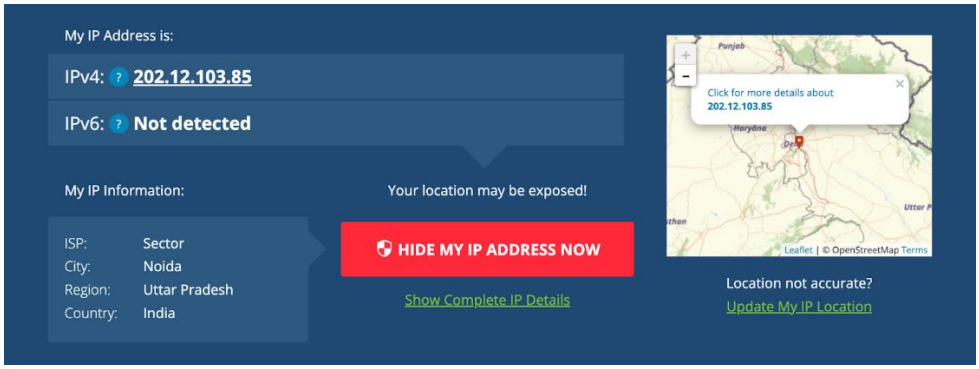


Safaan Shawl
A2305222148



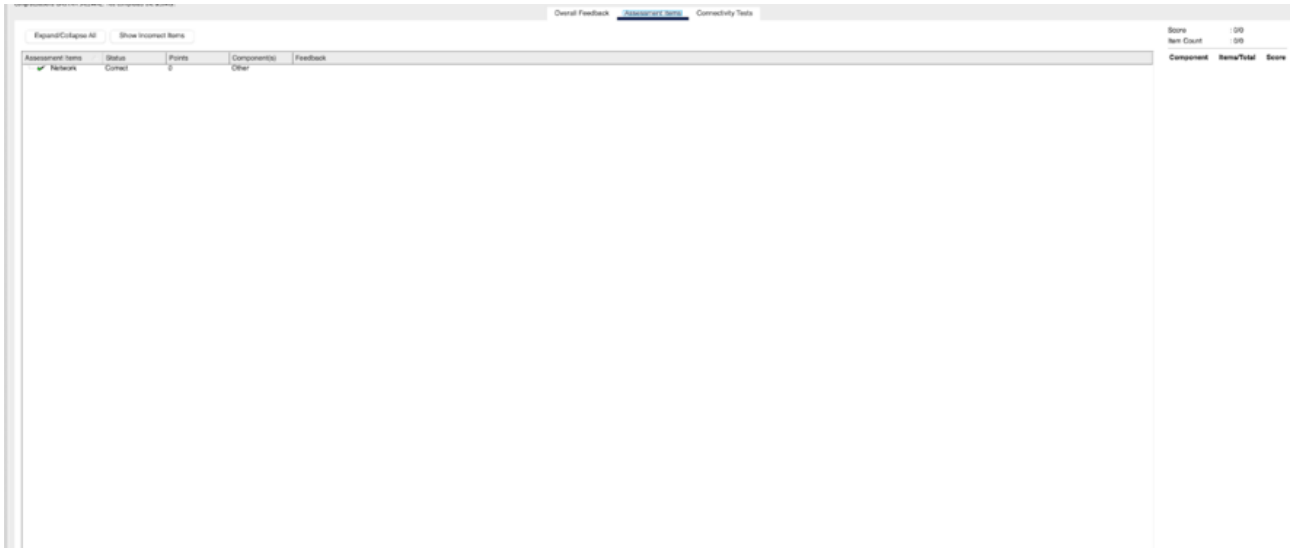






Safaan Shawl
A2305222148

Congratulations on completing this activity!



Safaan Shawl
A2305222148

Experiment 7

Aim: - Packet Tracer - Physical Layer Exploration - Physical Mode (Packet Tracer 4.7.1)

Theory: This experiment focuses on identifying and configuring the physical characteristics of internetworking devices, specifically Cisco routers and switches. It involves exploring management ports, LAN and WAN interfaces, and verifying their configuration using CLI commands. The experiment also covers the identification and insertion of appropriate expansion modules to enhance connectivity. Additionally, it guides connecting devices using suitable cables, checking interface statuses, and ensuring successful communication between devices. Wireless connections on laptops and tablets are established and verified, demonstrating the setup of both wired and wireless networks. The experiment concludes with verifying web connectivity across the networked devices..

Instructions:

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.

Question:

Which management ports are available?

Question:

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

d. Click the **CLI** tab, press the **Enter** key to access the user mode prompt, and enter the following commands:

Open a configuration window

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.

Question:

How many physical interfaces are listed?

e. Enter the following commands:

East> **show interface gigabitethernet 0/0**

Question:

What is the default bandwidth of this interface?

East> **show interface serial 0/0/0**

Question:

What is the default bandwidth of this interface?

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 2: Identify module expansion slots.

Questions:

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

Click **Switch2**. How many expansion slots are available?

Safaan Shawl
A2305222148

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 display at the bottom. Familiarize yourself with these options.

Questions:

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?

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

b. Click **Switch2**.

Question:

Which module can you insert to provide a Gigabit optical connection to **Switch3**?

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

a. Click **East** and attempt to insert the appropriate module from Step 1a. Modules are added by clicking the module and dragging it to the empty slot on the device.

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 before adding or removing modules. 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.

b. Using the same procedure, insert the module that you identified in Step 1b into the empty slot farthest to the right in **Switch2**.

c. Use the **show ip interface brief** command on **Switch2** to identify the slot in which the module was placed.

Question:

Into which slot was it inserted?

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 have 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 4/55.

Note: For the purposes of this activity, link lights are disabled.

Safaan Shawl
A2305222148

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
Switch2	Gigabit3/1	Copper Straight-Through	AccessPoint	Port 0
East	Serial0/0/0	Serial DCE (connect to East first)	West	Serial0/0/0

Part 4: Check Connectivity

Step 1: Check the interface status on East.

a. Click the **CLI** tab and enter the following commands:

East> **show ip interface brief**

Compare the output to the following:

Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 172.30.1.1 YES manual up up
GigabitEthernet0/1 172.31.1.1 YES manual up up
Serial0/0/0 10.10.10.1 YES manual up up
Serial0/0/1 unassigned YES unset down down
FastEthernet0/1/0 unassigned YES unset up up
FastEthernet0/1/1 unassigned YES unset up up
FastEthernet0/1/2 unassigned YES unset up up
FastEthernet0/1/3 unassigned YES unset up down
Vlan1 172.29.1.1 YES manual up up

If all of the cabling is correct the outputs should match.

Close the configuration window

Step 2: Connect wireless devices, Laptop and TabletPC.

a. Click the Laptop and select the **Config** Tab. Select the **Wireless0** interface. Put a check in the box labeled **On** next to Port Status. Within a few seconds the wireless connection should appear.

b. Click the **Desktop** tab of the **Laptop**. Click on the **Web Browser** icon to launch the web browser. Enter **www.cisco.pka** in the URL box and click **Go**. The page should display **Cisco Packet Tracer**.

c. Click the TabletPC and select the **Config** Tab. Select the **Wireless0** interface. Put a check in the box labeled **On** next to Port Status. Within a few seconds the wireless connection should appear.

d. Repeat the steps in Step 2b to verify the page displays.

Safaan Shawl
A2305222148

Step 3: Change the access method of the TabletPC.

a. Click the TabletPC and select the **Config** Tab. Select the **Wireless0** interface. Uncheck the box labeled **On** next to Port Status. It should now be clear and the wireless connection will drop.

b. Click the **3G/4G Cell1** interface. Put a check in the box labeled **On** next to Port Status. Within a few seconds the cellular connection should appear.

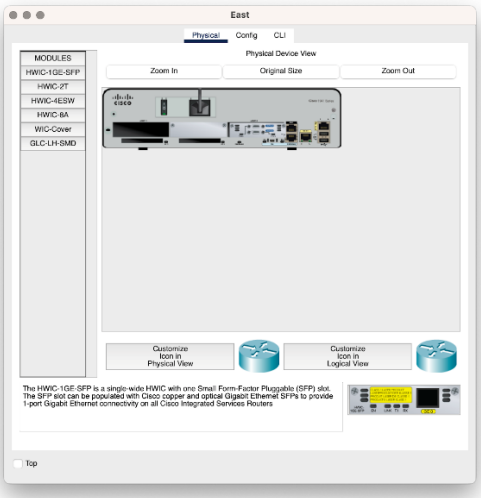
c. Repeat the process of verifying web access.

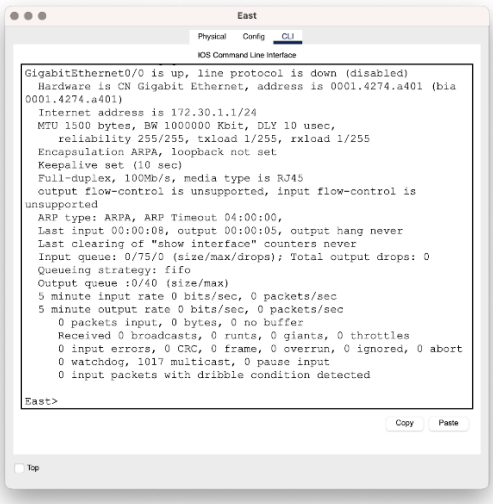
Note: You should not have both the wireless0 interface and 3G/4G Cell1 interfaces active at the same time. This may cause confusion to the device when attempting to connect to some resources.

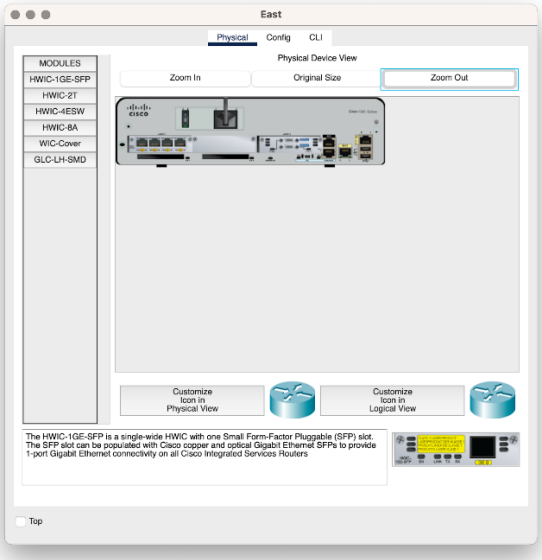
Step 4: Check connectivity of the other PCs.

All of the PCs should have connectivity to the web site and each other. You will learn to use connectivity testing in many upcoming labs.

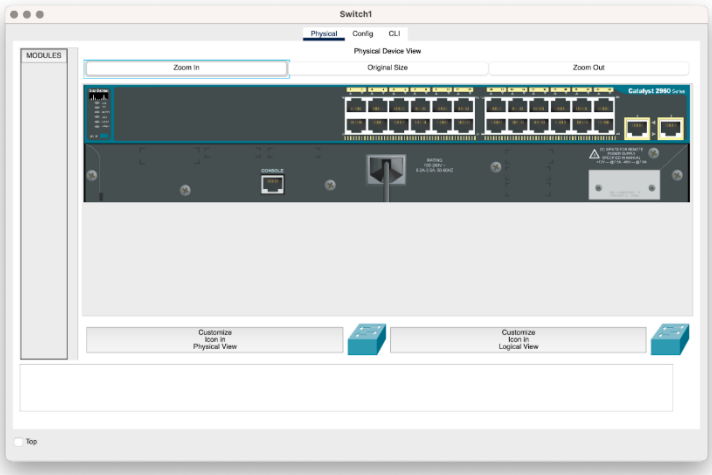
Commands/Results:

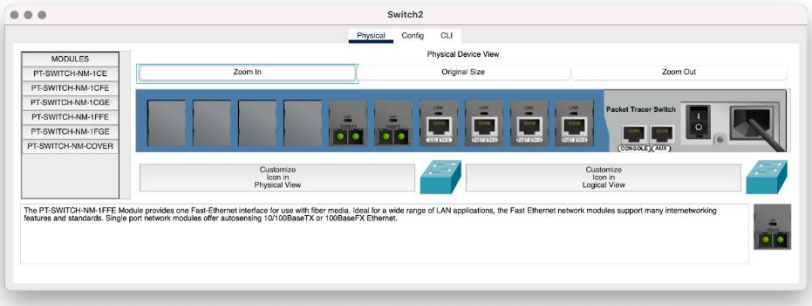


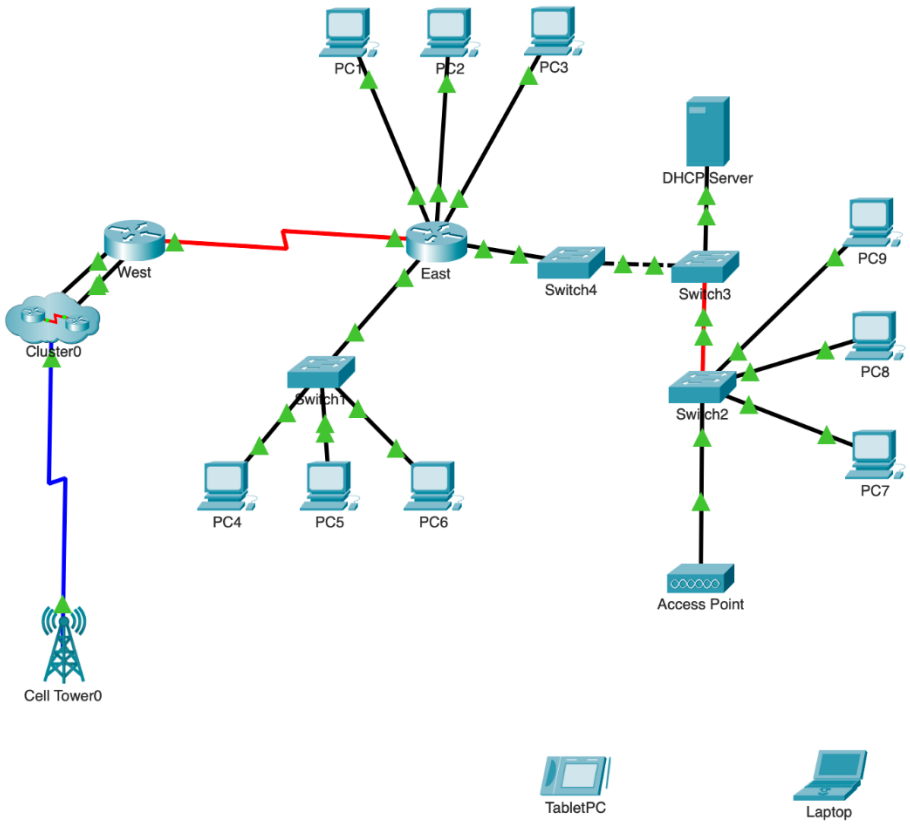




Safaan Shawl
A2305222148

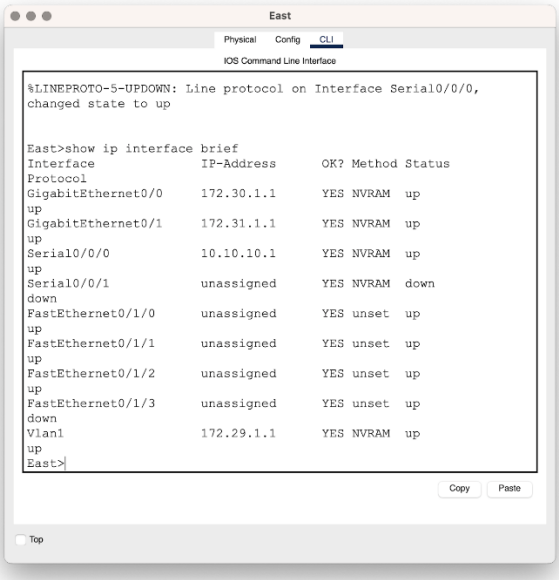


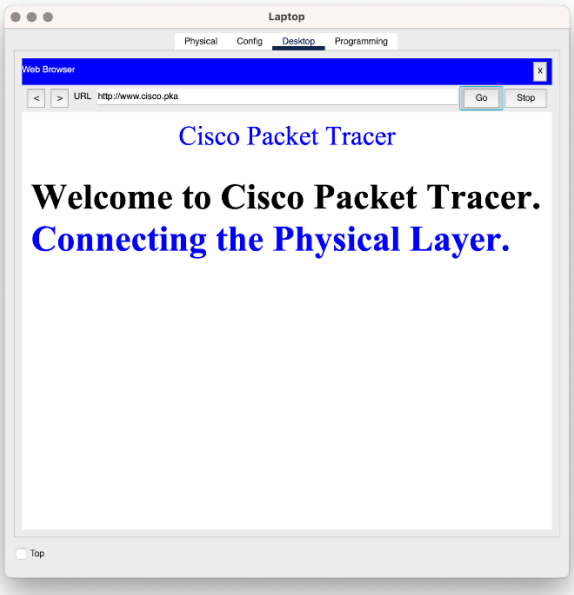


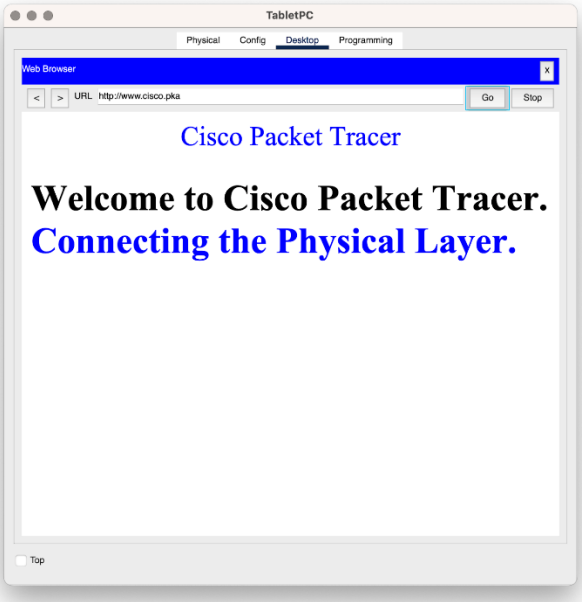


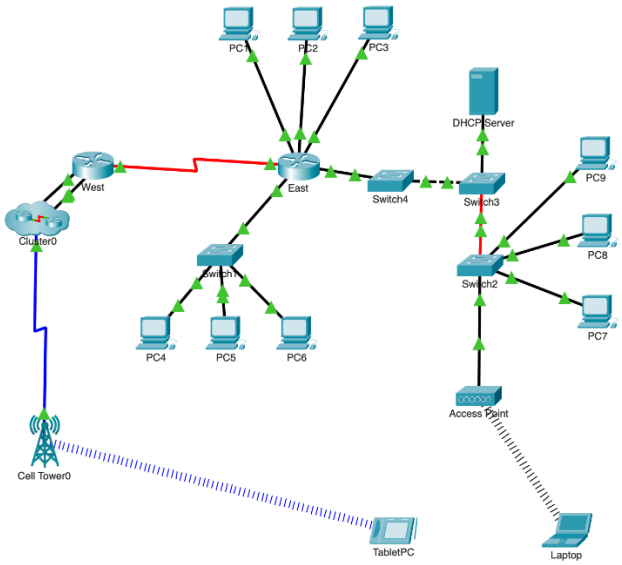
Safaan Shawl
A2305222148

Safaan Shawl
A2305222148









Safaan Shawl
A2305222148

Experiment 8

Aim: - Use Wireshark to Examine Ethernet Frames Topology

Theory: In this lab, we explore the structure of an Ethernet II frame using a Wireshark capture. The Ethernet II frame consists of several key components: the preamble, destination address, source address, frame type, data, and frame check sequence (FCS).

Instructions:

Part 1: Examine the Header Fields in an Ethernet II Frame

Step 1: Review the Ethernet II header field descriptions and lengths. The Ethernet II header consists of the following fields:

Preamble: 8 bytes
Destination Address: 6 bytes
Source Address: 6 bytes
Frame Type: 2 bytes
Data: 46 – 1500 bytes
Frame Check Sequence (FCS): 4 bytes

Step 2: Examine the network configuration of the PC. In this example, the PC has an IPv4 address of 192.168.1.147 and the default gateway is 192.168.1.1. To review the PC's network configuration, you can use the ipconfig /all command, which provides details such as:

IPv4 Address: 192.168.1.147
Default Gateway: 192.168.1.1
MAC Address: F0-1F-AF-50-FD-C8

Step 3: Examine Ethernet frames in a Wireshark capture. Wireshark captures network traffic and displays it for analysis. In this example, ARP (Address Resolution Protocol) and ICMP (Internet Control Message Protocol) traffic is filtered and analyzed. ARP is used to resolve the MAC address associated with an IP address. The capture shows an ARP query and reply to determine the MAC address of the gateway, followed by four ping requests and replies between the PC and the default gateway.

Step 4: Examine the Ethernet II header contents of an ARP request. The ARP request contains the following Ethernet II header fields:

Destination Address: ff:ff:ff:ff:ff:ff (broadcast)
Source Address: f0:1f:af:50:fd:c8 (unicast)
Frame Type: 0x0806 (indicating ARP)
Data: Contains ARP protocol information
FCS: Used for error checking, not shown in the Wireshark capture.

Safaan Shawl
A2305222148

Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

Step 1: Default Gateway IP

Open a command prompt and run ipconfig to find the default gateway's IP address.
Default Gateway IP: 192.168.1.1

Step 2: Start Traffic Capture

Open Wireshark and start capturing on the NIC.

Step 3: Filter for ICMP Traffic

In the Wireshark Filter box, type icmp to display only ICMP traffic. Apply the filter.

Step 4: Ping Default Gateway

Open a command prompt and ping the default gateway using the IP address from Step 1.

Step 5: Stop Capture

Stop the packet capture in Wireshark.

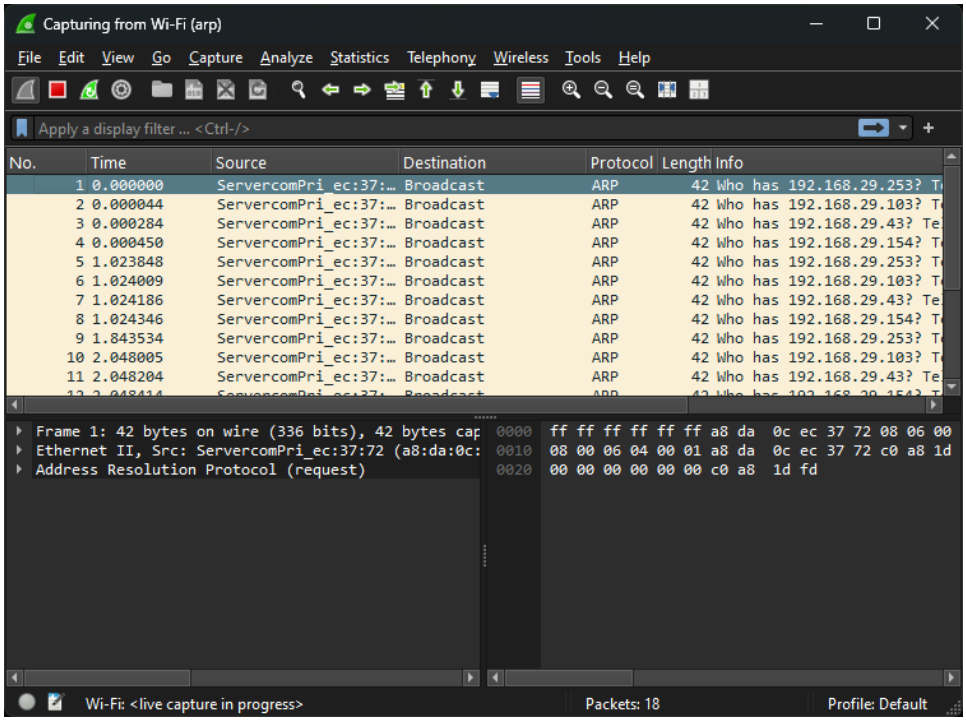
Step 6: Examine First Echo Request

a. In Wireshark's packet list pane, click the first Echo (ping) request.
b. Frame length is displayed in the details pane: 74 bytes
c. Source and destination MAC addresses are shown under Ethernet II.
PC NIC MAC Address: 00:1A:2B:3C:4D:5E
Default Gateway MAC Address: 00:1A:2B:3C:4D:5F
d. Type of frame displayed: Ethernet II
e. Source and destination IP addresses:
Source IP Address: 192.168.1.100
Destination IP Address: 192.168.1.1
f. Last two highlighted octets in the bytes pane: FA DE
g. In the Echo reply frame, notice the reversal of source and destination MAC addresses:
Destination MAC Address: 00:1A:2B:3C:4D:5E

Step 7: Capture Remote Host Packets

a. Start a new capture and ping www.cisco.com.
b. Stop capture and examine the first Echo request.
Source MAC Address: 00:1A:2B:3C:4D:5E
Destination MAC Address: 00:1A:2B:3C:4D:5F
Source IP Address: 192.168.1.100
Destination IP Address: 72.163.4.161

Safaan Shawl
A2305222148




```
C:\Users\gauta>ping www.google.com

Pinging www.google.com [2404:6800:4002:81f::2004] with 32 bytes of data:
Reply from 2404:6800:4002:81f::2004: time=9ms
Reply from 2404:6800:4002:81f::2004: time=7ms
Reply from 2404:6800:4002:81f::2004: time=6ms
Reply from 2404:6800:4002:81f::2004: time=5ms

Ping statistics for 2404:6800:4002:81f::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 9ms, Average = 6ms

C:\Users\gauta>ping www.google.com

Pinging www.google.com [2404:6800:4002:81f::2004] with 32 bytes of data:
Reply from 2404:6800:4002:81f::2004: time=10ms
Reply from 2404:6800:4002:81f::2004: time=9ms
Reply from 2404:6800:4002:81f::2004: time=5ms
Reply from 2404:6800:4002:81f::2004: time=6ms

Ping statistics for 2404:6800:4002:81f::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 10ms, Average = 7ms

C:\Users\gauta>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Gloid
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : auup.amity.edu.in
   Description . . . . . . . . . . . : Killer E2600 Gigabit Ethernet Controller
   Physical Address. . . . . . . . . : 08-8F-C3-06-2A-2D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 76-4C-A1-48-CE-2B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

Safaan Shawl
A2305222148

Experiment 9

Aim: Identify MAC and IP Addresses (Packet Tracer 9.1.3)

Theory: This Packet Tracer simulation demonstrates how data is transferred across networks by capturing and analyzing Protocol Data Units (PDUs). Each device involved in the process, such as switches, routers, and access points, interacts with both MAC and IP addresses at various OSI layers. The simulation reveals key insights, such as how hubs forward packets without altering MAC/IP addresses, while switches and routers adjust MAC addresses for correct routing. IPv4 addressing follows a distinct pattern in local and remote communications, with MAC addresses changing as data moves across network segments. IPv6, if used, would alter addressing formats and potentially impact packet routing processes.

Instructions:

Part 1: Gather PDU Information for Local Network Communication

Note: Review the Reflection Questions in Part 3 before proceeding with Part 1. It will give you an idea of the type of information you will need to gather.Gather PDU information as a packet travels from 172.16.31.5 to 172.16.31.2.

a. Click **172.16.31.5** and open the **Command Prompt**.

b. Enter the **ping 172.16.31.2** command.

c. Switch to simulation mode and repeat the **ping 172.16.31.2** command. A PDU appears next to **172.16.31.5**.

d. Click the PDU and note the following information from the **OSI Model** and **Outbound PDU Layer** tabs:

- Destination MAC Address: **000C:85CC:1DA7**
- Source MAC Address: **00D0:D311:C788**
- Source IP Address: **172.16.31.5**
- Destination IP Address: **172.16.31.2**
- At Device: **172.16.31.5**

e. Click **Capture / Forward (the right arrow followed by a vertical bar)** 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

At Device	Dest. MAC	Src MAC	Src IPv4	Dest IPv4
172.16.31.5	000C:85CC:1DA7	00D0:D311:C788	172.16.31.5	172.16.31.2
Switch1	000C:85CC:1DA7	00D0:D311:C788	N/A	N/A
Hub	N/A	N/A	N/A	N/A
172.16.31.2	00D0:D311:C788	000C:85CC:1DA7	172.16.31.2	172.16.31.5

Step 2: Gather additional PDU information from other pings.

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

- Ping 172.16.31.2 from 172.16.31.3.

Safaan Shawl
A2305222148

- Ping 172.16.31.4 from 172.16.31.5.

Return to Realtime mode.

Part 2: Gather PDU Information for Remote Network Communication

In order to communicate with remote networks, a gateway device is necessary. Study the process that takes place to communicate with devices on the remote network. Pay close attention to the MAC addresses used.

Step 1: Gather PDU information as a packet travels from 172.16.31.5 to 10.10.10.2.

a. Click **172.16.31.5** and open the **Command Prompt**.

b. Enter the **ping 10.10.10.2** command.

c. Switch to simulation mode and repeat the **ping 10.10.10.2** command. A PDU appears next to **172.16.31.5**.

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

- Destination MAC Address: 00D0:BA8E:741A
- Source MAC Address: 00D0:D311:C788
- Source IP Address: 172.16.31.5
- Destination IP Address: 10.10.10.2
- At Device: 172.16.31.5

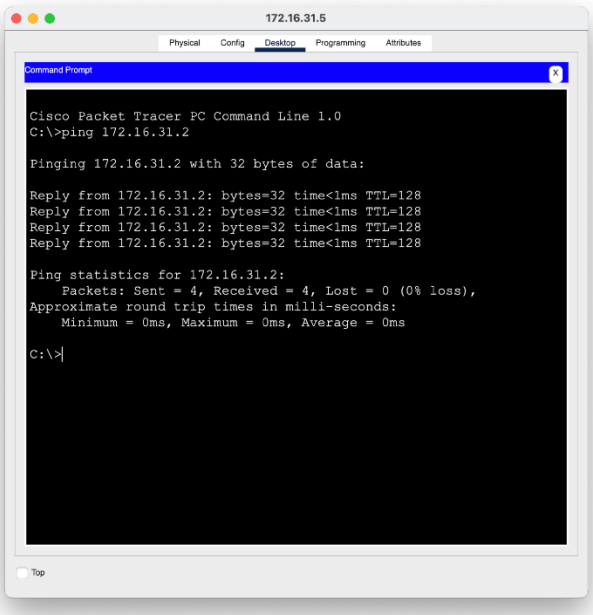
What device has the destination MAC that is shown?

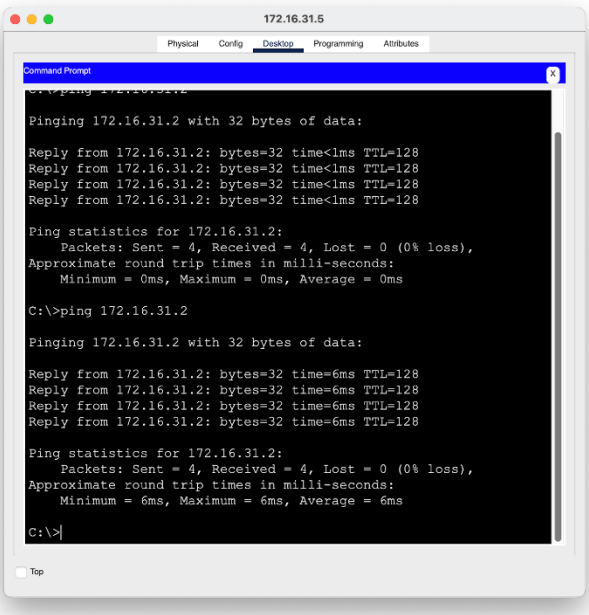
e. Click **Capture / Forward (the right arrow followed by a vertical bar)** to move the PDU to the next device. Gather the same information from Step 1d. Repeat this process until the PDU reaches its destination. Record the PDU information you gathered from pinging 172.16.31.5 to 10.10.10.2 into a spreadsheet using a format like the sample table shown below:

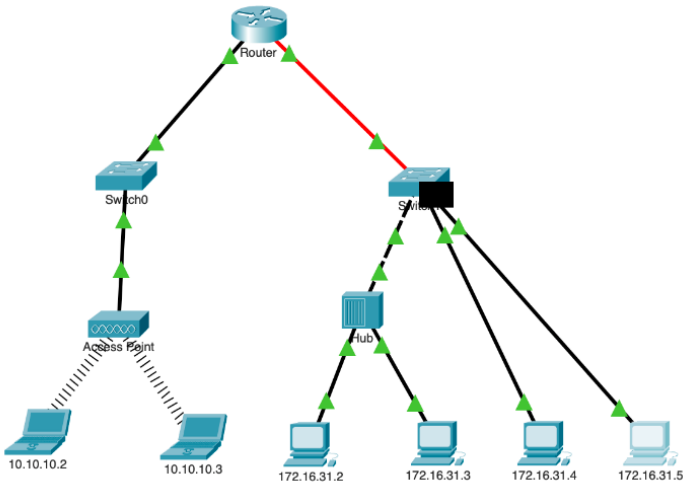
At Device	Dest. MAC	Src MAC	Src IPv4	Dest IPv4
172.16.31.5	00D0:BA8E:741A	00D0:D311:C788	172.16.31.5	10.10.10.2
Switch1	00D0:BA8E:741A	00D0:D311:C788	N/A	N/A
Router	0060:2F84:4AB6	00D0:588C:2401	172.16.31.5	10.10.10.2
Switch0	0060:2F84:4AB6	00D0:588C:2401	N/A	N/A
Access Point	N/A	N/A	N/A	N/A
10.10.10.2	00D0:588C:2401	0060:2F84:4AB6	10.10.10.2	172.16.31.5

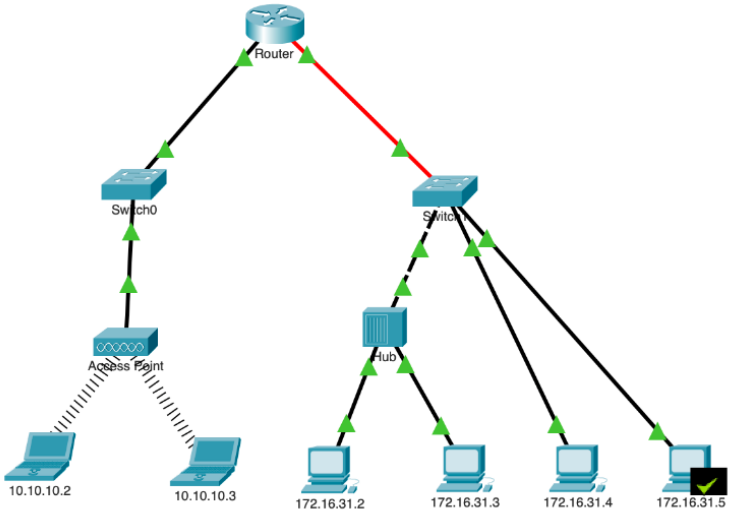
Commands/Results:

Safaan Shawl
A2305222148

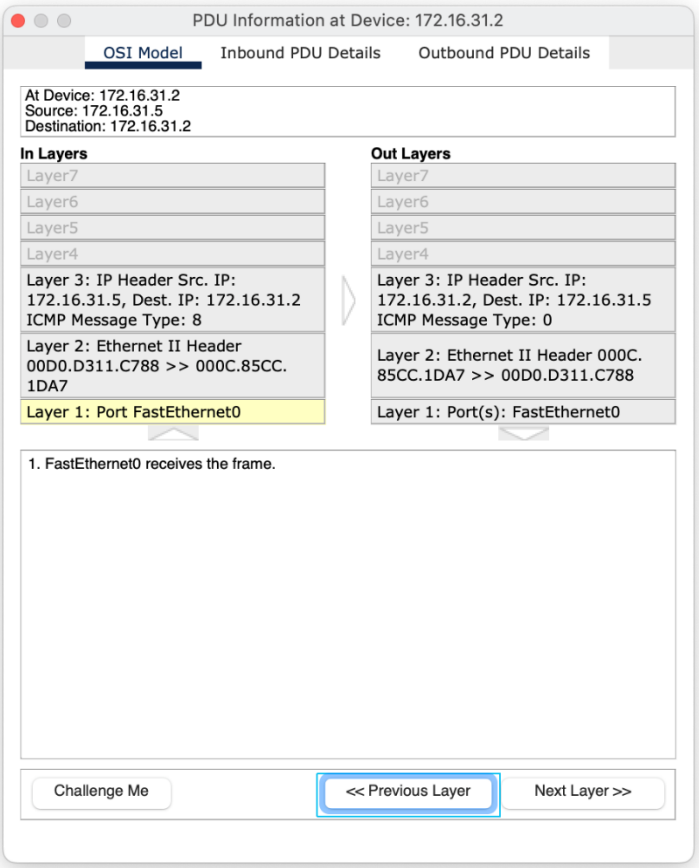


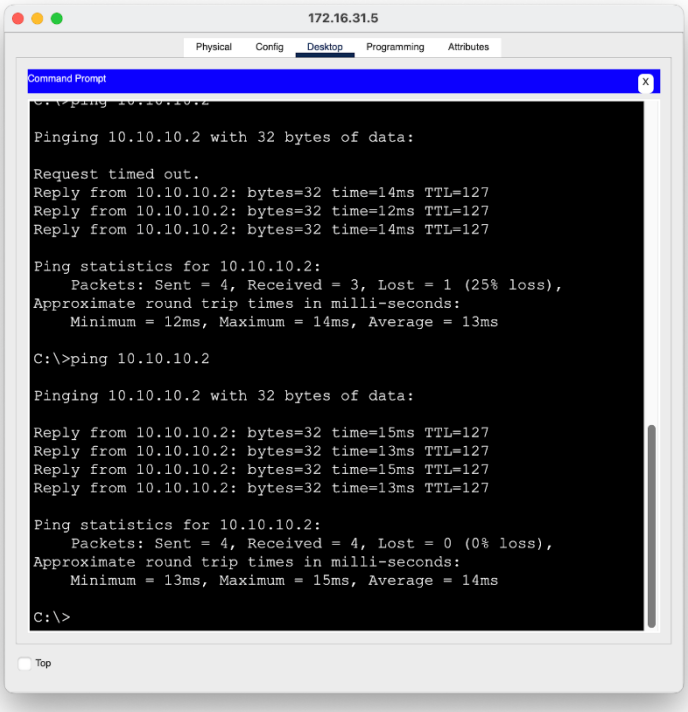


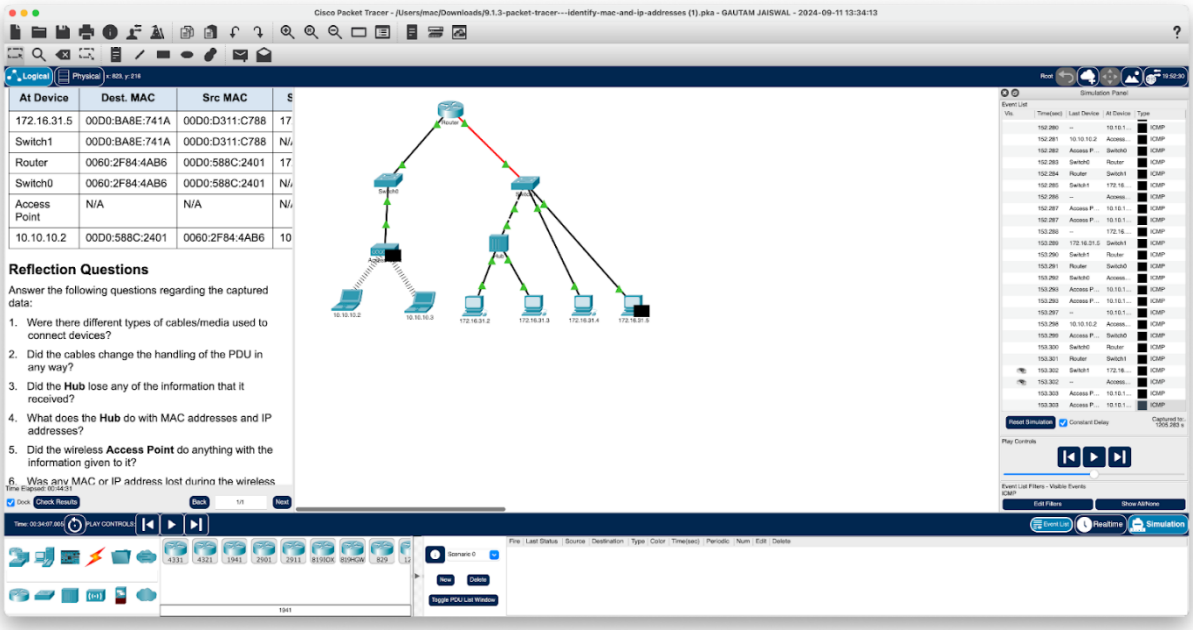




Safaan Shawl
A2305222148







Safaan Shawl
A2305222148

Experiment 10

Aim: - Examine the ARP table (Packet Tracer 9.2.9)

Theory: In networking, Address Resolution Protocol (ARP) is crucial for mapping IP addresses to MAC addresses, enabling communication within a local network. When a device initiates a ping to a destination without knowing the MAC address, it first sends an ARP broadcast to discover it. The switch forwards this ARP request, and once the destination responds, the switch records the MAC address in its table for future use. ARP requests are typically issued when a device needs to send data to another device whose MAC address is unknown. Routers and switches maintain ARP tables and MAC address tables to facilitate efficient packet routing and forwarding.

Instructions:

Part 1: Examine an ARP Request

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

Open a command prompt

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

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

Close a command prompt

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.

Question:

Is this address listed in the table above?

Question:

How many copies of the PDU did **Switch1** make?

What is the IP address of the device that accepted the PDU?

e. Open the PDU and examine Layer 2.

Question:

What happened to the source and destination MAC addresses?

f. Click **Capture/Forward** until the PDU returns to **172.16.31.2**.

Question:

How many copies of the PDU did the switch make during the ARP reply?

Step 2: Examine the ARP table.

a. Note that the ICMP packet reappears. Open the PDU and examine the MAC addresses.

Question:

Do the MAC addresses of the source and destination align with their IP addresses?

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

c. Click **172.16.31.2** and enter the **arp –a** command.

Question:

To what IP address does the MAC address entry correspond?

In general, when does an end device issue an ARP request?

Part 2: Examine a Switch MAC Address Table

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

Open a command prompt

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.

Question:

How many replies were sent and received?

Close a command prompt

Safaan Shawl
A2305222148

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.

Question:

Do the entries correspond to those in the table above?

b. Click **Switch0**, then the **CLI** tab. Enter the **show mac-address-table** command.

Questions:

Do the entries correspond to those in the table above?

Why are two MAC addresses associated with one port?

Part 3: Examine the ARP Process in Remote Communications

Step 1: Generate traffic to produce ARP traffic.

Open a command prompt

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

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

c. Type **arp –a**.

Question:

What is the IP address of the new ARP table entry?

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

e. Repeat the ping to 10.10.10.1.

Question:

How many PDUs appear?

Close a command prompt

f. Click **Capture/Forward**. Click the PDU that is now at **Switch1**.

Question:

What is the target destination IP destination address of the ARP request?

g. The destination IP address is not 10.10.10.1.

Question:

Why?

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.

Question:

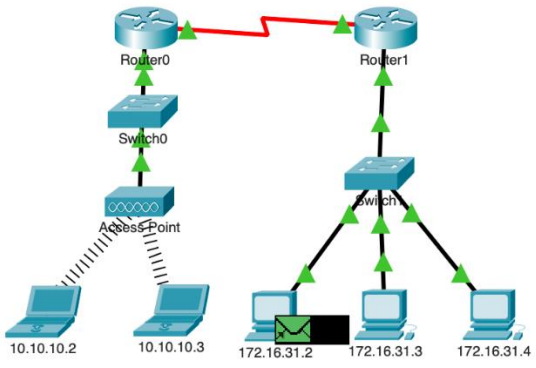
How many MAC addresses are in the table? Why?

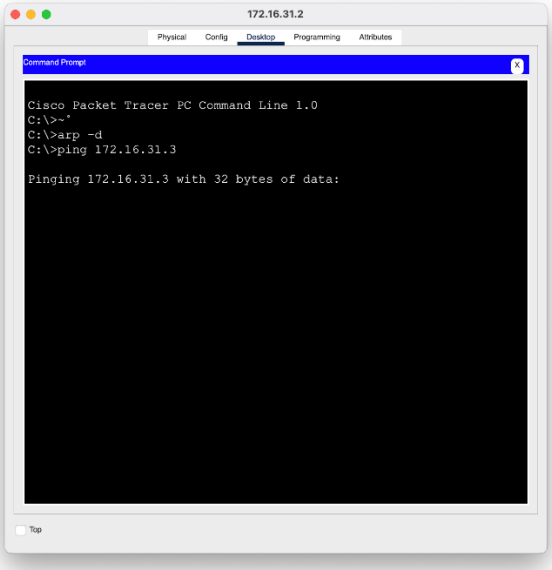
c. Enter the **show arp** command.

Questions:

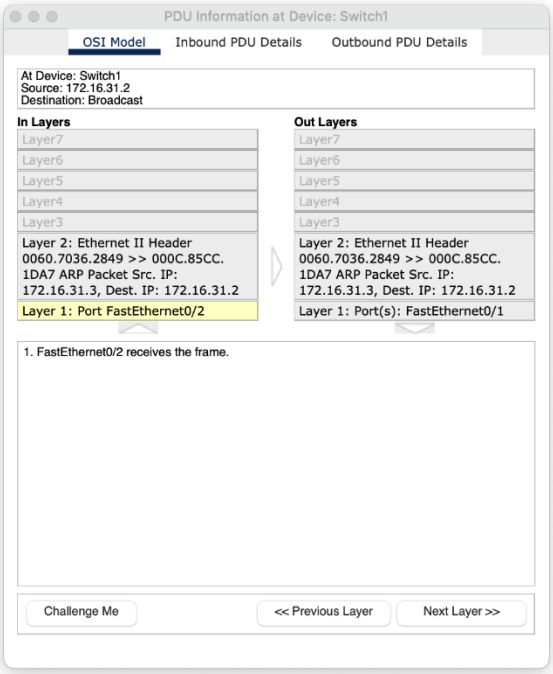
Is there an entry for **172.16.31.2**?

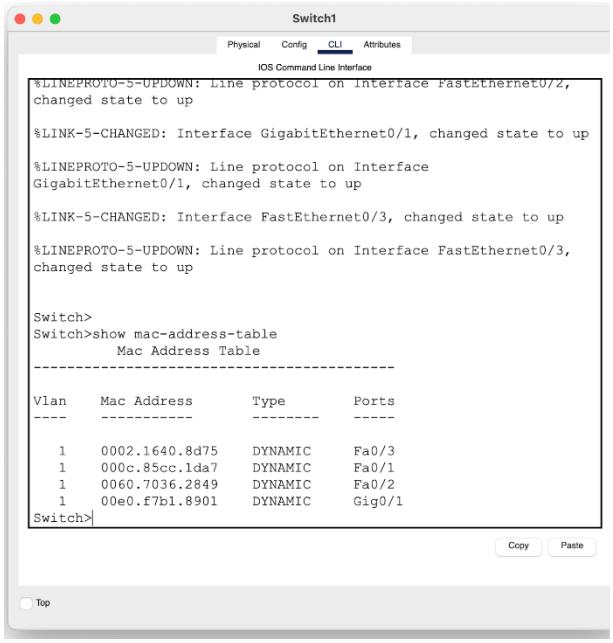
What happens to the first ping in a situation where the router responds to the ARP request?

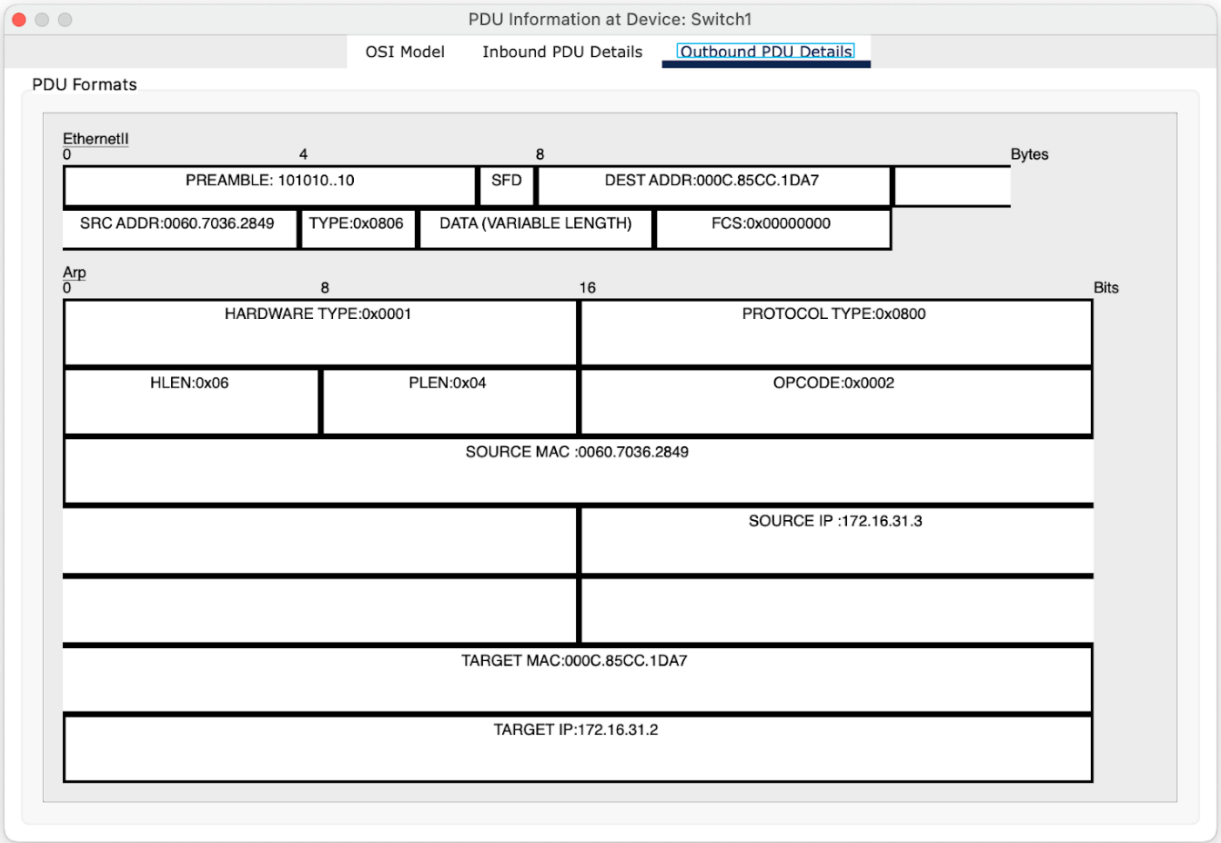




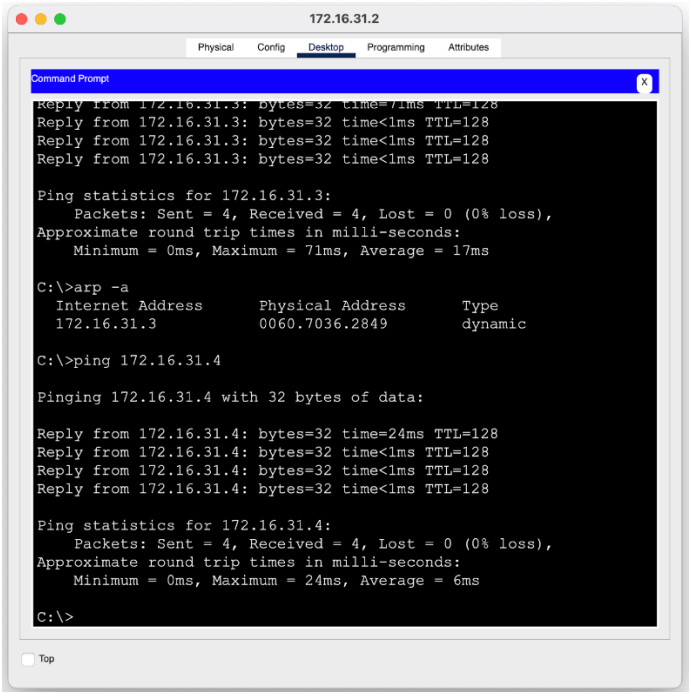
Safaan Shawl
A2305222148

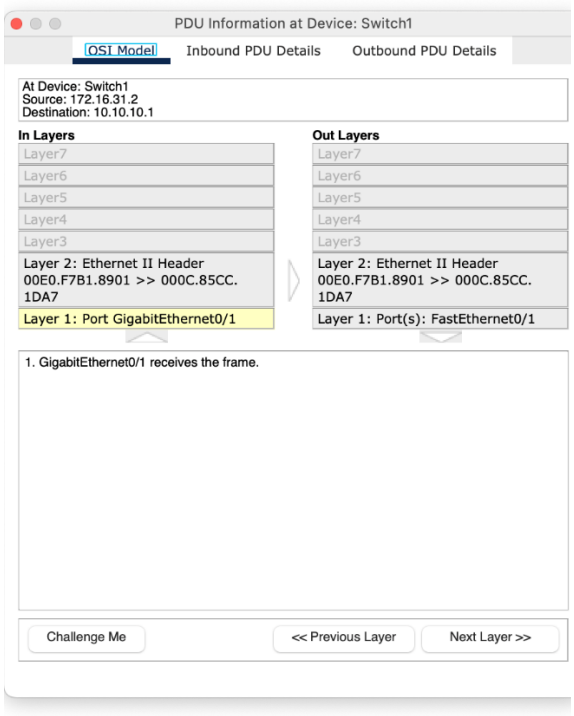


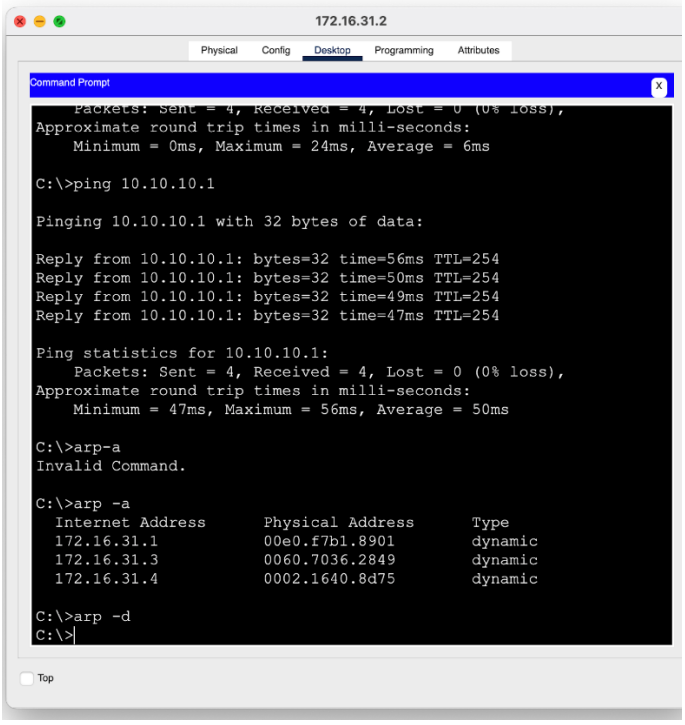


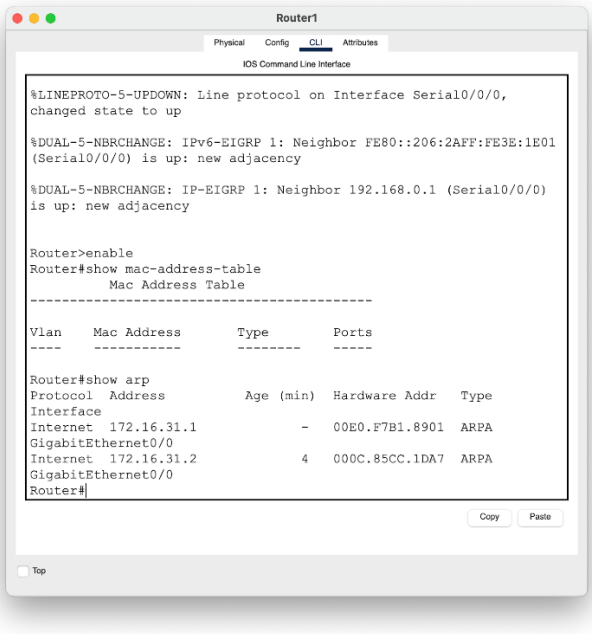


Safaan Shawl
A2305222148

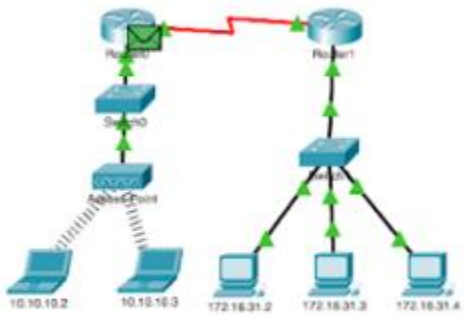








Safaan Shawl
A2305222148



Safaan Shawl
A2305222148

Experiment 11

Aim: Configure Initial Router Settings (Packet Tracer 10.1.4)

Theory: In this experiment, we begin by configuring a router to secure its access and settings. First, the router's default configuration is verified through a console connection. Basic settings such as the hostname, encrypted passwords, and a Message of the Day (MOTD) banner are then configured to warn unauthorized users. Privileged EXEC access is secured using both unencrypted and encrypted passwords, and all plain-text passwords are encrypted. After verifying the initial configuration, the running configuration is saved to NVRAM to ensure it persists after a reboot. Optionally, the configuration can be backed up to flash for added security.

Instructions:

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**

What is the router's hostname?

How many Fast Ethernet interfaces does the Router have?

How many Gigabit Ethernet interfaces does the Router have?

How many Serial interfaces does the router have?

What is the range of values shown for the vty lines?

c. 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?

Safaan Shawl
A2305222148

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 IOS configuration modes.

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. Configure **R1** as the hostname.

b. Configure Message of the day text: **Unauthorized access is strictly prohibited.**

c. Encrypt all plain text passwords.

Use the following passwords:

1) Privileged EXEC, unencrypted: **cisco**
2) Privileged EXEC, encrypted: **itsasecret**
3) Console: **letmein**

Step 2: Verify the initial settings on R1.

a. Verify the initial settings by viewing the configuration for R1.

What command do you use?

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?

If you are not prompted for a password before reaching the user EXEC prompt, what console line command did you forget to configure?

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?

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

Safaan Shawl
A2305222148

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?

What is the shortest, unambiguous version of this command?

Step 2: Optional: 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 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?

Which of these files would you guess is the IOS image?

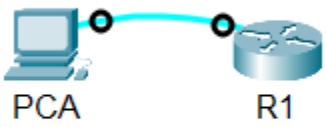
Why do you think this file is the IOS image?

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

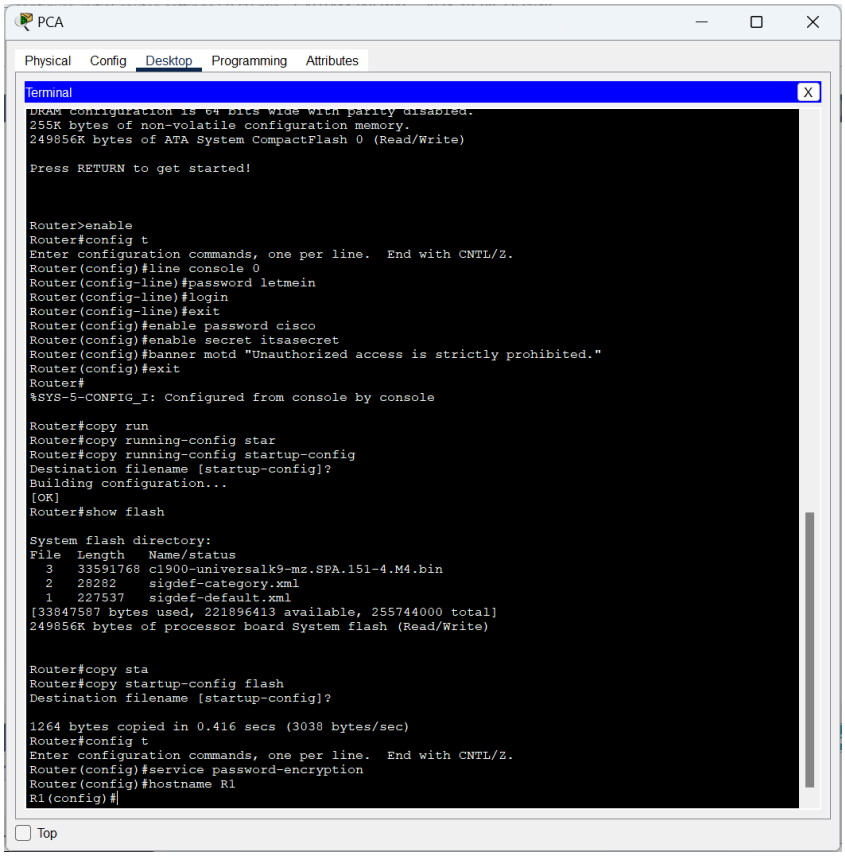
The router prompts you to store the file in flash using the name in brackets. If the answer is yes, then press **ENTER**; if not, type an appropriate name and press **ENTER**.

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

Commands/Results:



Safaan Shawl
A2305222148



Safaan Shawl
A2305222148

Experiment 12

Aim: - Connect a router to a LAN (Packet Tracer 10.3.4)

Theory: In this networking task, router configuration and interface management are key to establishing communication between devices. Using commands like `show ip interface brief`, administrators can verify the IP address and status of interfaces. Additionally, configuring interfaces with IP addresses and descriptions, and saving configurations to NVRAM ensures the network is well-documented and persistent. The routing table, displayed with `show ip route`, reveals both directly connected and dynamically learned routes, such as OSPF routes, which are essential for efficient packet forwarding. Testing connectivity between PCs and routers confirms proper configuration, ensuring seamless communication across the network's LANs and WANs.

Instructions:

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**.

Questions:

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

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

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

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**?
2) What is the MAC address of the GigabitEthernet 0/0 interface?
3) What is the bandwidth (BW) of the GigabitEthernet 0/0 interface?

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

Questions:

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

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

1) How many serial interfaces are there on **R1** and **R2**?
2) How many Ethernet interfaces are there on **R1** and **R2**?
3) Are all the Ethernet interfaces on **R1** the same? If no, explain the difference(s).

Step 3: Display the routing table on R1.

Questions:

a. What command displays the contents of the routing table?

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

1) How many connected routes are there (uses the **C** code)?
2) Which route is listed?
3) How does a router handle a packet destined for a network that is not listed in the routing table?

Safaan Shawl
A2305222148

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**:

Open configuration window

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. Configure an interface description that indicates the device to which 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.

Question:

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

Close configuration window

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 are active.

Questions:

How many interfaces on **R1** and **R2** are configured with IP addresses and in the "up" and "up" state?
What part of the interface configuration is NOT displayed in the command output?
What commands can you use to verify this part of the configuration?

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

Questions:

1) How many connected routes (uses the **C** code) do you see on each router?
2) How many OSPF routes (uses the **O** code) do you see on each router?
3) If the router knows all the routes in the network, then the number of connected routes and dynamically learned routes (OSPF) should equal the total number of LANs and WANs. How many LANs and WANs are in the topology?
4) Does this number match the number of C and O routes shown in the routing table?

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

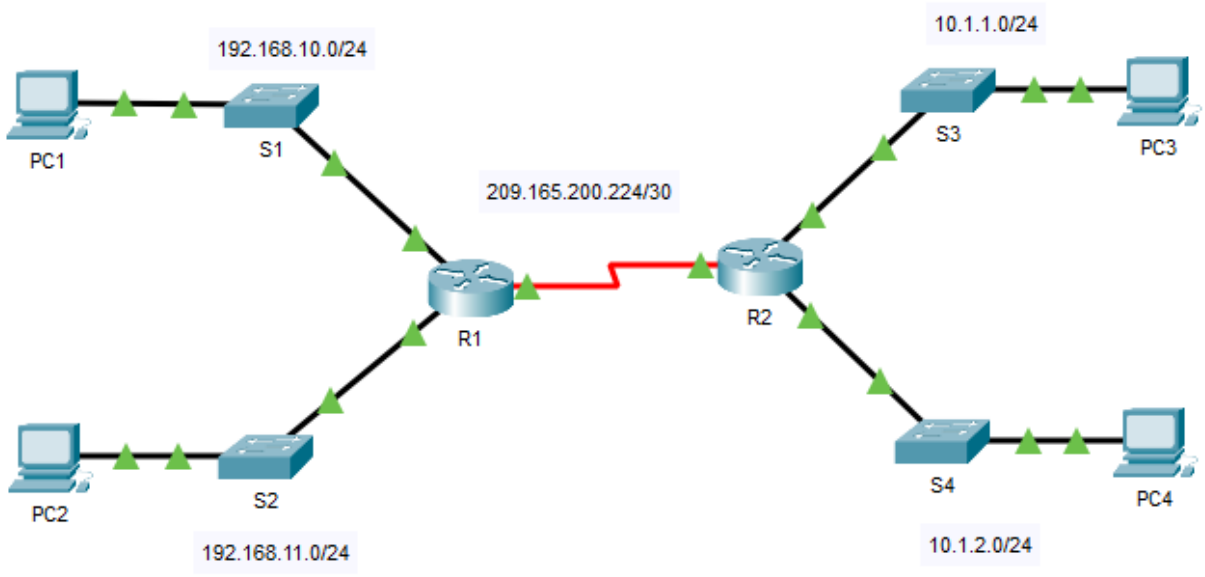
Step 2: Test end-to-end connectivity across the network.

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 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.

Safaan Shawl
A2305222148



R1

Physical Config CLI Attributes

IOS Command Line Interface

```
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

10:30:10: %OSPF-5-ADJCHG: Process 10, Nbr 209.165.200.226 on Serial0/0/0 from LOADING to FULL,
Loading Done


User Access Verification

Password:

R1>enable
Password:
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

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

R1(config-if)#description LAN connection to S1
R1(config-if)#end
R1#
%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 = 0/0/1 ms

R1#
```

Copy Paste

Top

R1

Physical Config CLI Attributes

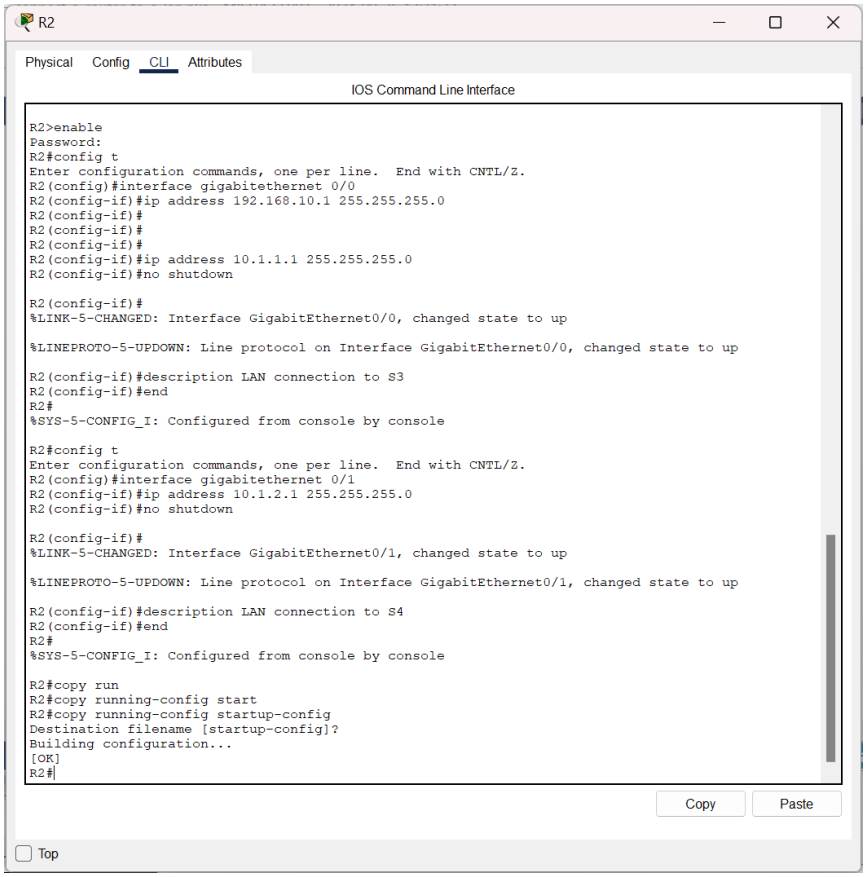
IOS Command Line Interface

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

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

R1(config-if)#description LAN connection to S1
R1(config-if)#end
R1#
%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 = 0/0/1 ms

R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ip address 192.168.11.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

R1(config-if)#description LAN connection to S2
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#copy run
R1#copy running-config start
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Copy Paste

Top

Safaan Shawl
A2305222148



Safaan Shawl
A2305222148

Experiment 13

Aim: Troubleshoot Default Gateway Issues (Packet Tracer 10.3.5)

Theory: In this experiment, we troubleshoot default gateway issues in a network using a methodical approach. First, network documentation is verified, and missing information such as default gateways is completed. Local and remote connectivity tests are performed to isolate issues. Based on the findings, appropriate solutions are suggested, implemented, and verified. Common problems include incorrect IP addressing or missing default gateways, which prevent communication across networks. Once the solutions are applied, the network is re-tested to ensure all connectivity issues are resolved. This step-by-step process is essential for identifying and fixing network issues efficiently.

Instructions:

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.

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 and verify one solution at a time. Implementing more than one solution could introduce additional issues in a more complex scenario.

Safaan Shawl
A2305222148

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?

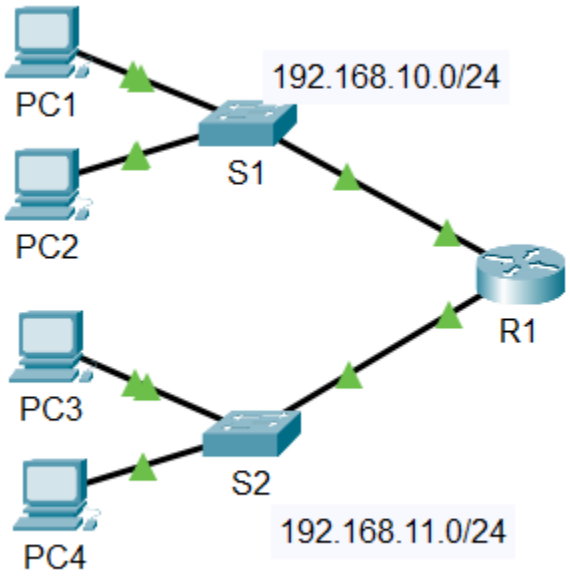
b. If the problem is resolved, indicate so in your documentation. For example, in the table above, a simple checkmark would suffice in the "Verified" column.

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.

Commands/Results:



Safaan Shawl
A2305222148