**1)) question) Packet Tracer - Configure a Wireless Router and Clients**

# Objectives

**Part 1: Connect the Devices**

**Part 2: Configure the Wireless Router**

**Part 3: Configure IP Addressing and Test Connectivity**

# Background / Scenario

Your friend, Natsumi, heard that you are studying networking. She asked you to come over and help her connect her new home to the cable TV network. You need to connect the correct cables to the correct devices, connect devices to a home wireless router, and configure the router to provide IP addresses to network clients. Natsumi also wants you to setup a wireless LAN for her home network, so you will configure that as well. You are confident that this will be an easy process and the network will be setup in no time!

# Instructions

## Part 1: Connect the Devices

The work area shows the interior of your friend’s house. Scroll the window to get a sense of the layout of the house and the location of the devices. In this part, you will connect all the labeled devices.

### Step 1: Connect the coaxial cables.

Natsumi's cable company delivers internet and video services to her home through a coaxial cable. The cable is connected to an outlet in her home. A splitter device separates the internet data service from the video service. This enables the two services to be connected to the appropriate devices. You will connect the internet service to the cable modem, and the video service to the television.

a.     In Network Components, click **Connections** (the lightning bolt).

b.     Locate and click the icon for the **Coaxial** cable. It is the blue zigzag icon.

c.     Click the **Cable Splitter** and select the **Coaxial1** port.

d.     Click the **Cable Modem** and select **Port 0**.

e.     Repeat the previous steps to connect **Coaxial2** on the **Cable Splitter** to **Port 0**on the **TV**.

f.      Click the **TV**, and then click **ON** for **Status**. If your connections are correct, you should see an image appear that represents a TV program.

### Step 2: Connect the network cables.

There are two PCs in Natsumi’s house. They don’t have wireless LAN adapters, so they will be connected with Ethernet cables. The home wireless router is the center of the network. It enables devices that are configured on the home network to communicate with each other and the internet. The router includes a network switch that accepts wired connections for up to four hosts. You will connect the PCs to these ports.

For the **Home Wireless Router** to access the internet over the cable TV provider network, the cable modem must be connected to the home wireless router internet port. This is done with a copper straight-through cable.

a.     Click **Connections**, and then **Copper Straight-Through** cable. It looks like a solid black line.

b.     Connect**Port 1** on the **Cable Modem** to the **Internet** port of the**Home Wireless Router**.

c.     Click the **Office PC** and connect the cable to the **FastEthernet0** port. Locate the **Home Wireless Router** and click it. Connect the other end of the cable to the **GigabitEthernet 1** port to complete the connection.

d.     Repeat the previous steps to connect the **Bedroom PC** to the **GigabitEthernet 2** port on the **Home Wireless Router**.

The wired home network is now fully connected to the internet through the cable TV provider network.

## Part 2: Configure the Wireless Router

Most home wireless routers are configured by using a graphical user interface (GUI) that is accessed through your computer's web browser. In this part, you will access the home wireless router through the browser on the **Office PC** and configure Natsumi’s home network.

### Step 1: Access the home wireless router GUI.

a.     Click **Office PC** > **Desktop** tab, and then **IP Configuration**.

b.     Click **DHCP**. DHCP will automatically configure the **Office PC** to be on the same IP network as the **Home Wireless Router**.

c.     After a brief delay, the values for the **IP Configuration** should automatically update. The IPv4 address should start with the number 192. If it does not, click **Fast Forward Time**, which is just below the network topology in the lower left-hand corner. This will speed up the simulation of DHCP.

d.     Make note of the address for the default gateway. The default gateway is the device that provides devices on the home network with access to outside networks, such as the internet. In this case, the default gateway address is the address of the **Home Wireless Router**.

e.     Keeping the **Office PC** window open, close the **IP Configuration** window, and then click **Web Browser**. Enter the IP address of the **Home Wireless Router** (the default gateway address) into the **URL** box and click **Go**.

f.      Newly installed home routers are configured with default credentials. Enter **admin** for both the **User Name** and **Password**. You should now see the GUI for the **Home Wireless Router**appear and are ready to configure Natsumi’s network. Adjust the window size, as necessary, to see more of the interface.

**Note**: Default passwords on real-world devices should be changed immediately because it is widely known, including threat actors.

### Step 2: Configure basic settings.

In this step, you will configure a new username and password for the wireless router and limit the number of IP addresses that DHCP will issue to host that are connected to the network.

Natsumi only has a few devices to that will connect the network, and she will not have a lot of friends visiting. She thinks that no more than 10 devices would connect to her network at any one time. You decide to lower the number of users to 10. Your friend lives in a densely populated part of town, so it is possible that many people could see her wireless network.

a.     You are currently viewing configuration options under the **Setup** tab. Locate the **Network Setup** area. This is where you can configure the router’s DHCP server settings. Locate the **Maximum Number of Users** field, enter **10**. Scroll down to the bottom of the page and click **Save Settings**. You must save settings on every page of the GUI that you make changes.

**Note**: It is possible that you will lose your connection to the router. Click **Go** in the web browser to reload the GUI page. You may need to close the **Web Browser**, click **IP Configuration**, and toggle between **DHCP** and **Static** to refresh the IP addressing for **Office PC**. Then verify the **Office PC** has an IP address configuration that starts with 192, open the **Web Browser** again, enter the router's IP address, and re-authenticate with **admin** as the default credentials.

b.     Click the **Administration** tab. Here, you can change the default **admin** password. Enter and confirm **MyPassword1!** as the new password. Scroll to the bottom of the page and click **Save Settings**.

You will be prompted to login again. Enter **admin** as the User Name and **MyPassword1!** as the new password, and the click **Continue**.

### Step 3: Configure a wireless LAN.

At this point, you are ready to configure Natsumi's wireless network so that she can connect her wireless devices to the internet over Wi-Fi.

a.     Scroll back to the top of the window, and then click the **Wireless** tab.

b.     For the **2.4 GHz** network, click **Enable** to activate the network radio.

c.     Change the **Network Name (SSID)**from **Default** to **MyHome**. When people look for Wi-Fi networks to connect to, they will see this network name. The network name can be hidden, but this can make it a little harder for guests to connect to the network. Scroll to the bottom of the page and click **Save Settings**.

d.     Now you will configure security on the **MyHome** network. This will prevent unauthorized people from connecting to the wireless network. Scroll back to the top of the window, and then click the **Wireless Security** under the **Wireless** tab.

e.     Notice that security is currently disabled on all three wireless networks. You are only using the **2.4 GHz** network. Click the dropdown menu for the **2.4 GHz** network and select **WPA2 Personal**. This is the strongest security that this router offers for wireless networks.

f.      More settings are revealed. WPA2 Personal requires a passphrase that must be entered by anyone who wants to connect to the wireless network. Enter **MyPassPhrase1!** as the **Passphrase**. Note that capitalization is important.

g.     Scroll to the bottom of the page and click **Save Settings**, and then close the **Web Browser** for the Office PC.

## Part 3: Configure IP Addressing and Test Connectivity

Now that the router is configured, in this part you will configure IP addressing for the PCs and laptop and verify that they can connect to the internet.

### Step 1: Connect the laptop to the wireless network.

a.     Click the **Laptop** in the living room, and then the **Desktop** tab > **PC Wireless**.

b.     Click the **Connect** tab. After a short delay you should the wireless network that you configured previously appear in the list of wireless network names.

c.     Click the name of the network that you created, and then click the **Connect** button.

d.     Enter the passphrase that you configured early for the wireless network in the **Pre-shared Key** field, and then click **Connect**.

e.     Click the **Link Information** tab. You should see the message: **You have successfully connected to the access point**.

f.      Click the **More Information** button to see details about the connection. If the IP address does not begin with **192**, click the **Fast Forward Time** several times to speed up the simulation.

g.     Close the **PC Wireless** app and open the **Web Browser**. Verify that the **Laptop** can now connect to **skillsforall.srv**, clicking **Fast Forward Time** until the page loads. This verifies that the **Laptop** has internet connectivity.

### Step 2: Test connectivity from the Office PC.

You know that the Office PC can connect to the network because you used it to configure the router. However, can it also access the internet? If it can, then you will know that the wired network is properly connected and configured.

a.     Click **Office PC** > **Desktop** tab > **Web Browser**.

b.     Enter **skillsforall.srv** and click **Go**. After a brief delay, you should see the webpage appear. If necessary, click **Fast Forward Time** several times to speed up the convergence.

Loading an external website verifies that internet connectivity for the **Office PC**.

### Step 3: Configure the bedroom PC.

a.     For the **Bedroom PC**, open **IP Configuration** and set it to **DHCP**. Verify that the Bedroom PC received an IP address that begins with **192**.

b.     Close the **IP Configuration** window and open the **Web Browser**. Verify that the **Bedroom PC** can now connect to **skillsforall.srv**, clicking **Fast Forward Time** until the page loads. This verifies that the **Bedroom PC** has internet connectivity.

You have now completed connecting network devices, configuring the router and wireless LAN, and configuring hosts to connect to the network. All devices should be able to connect to the internet. Your job is done and Natsumi has offered to cook dinner for you as a reward for your help.

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**2) Question) Packet Tracer - Connect to a Web Server**

# Objectives

Observe how packets are sent across the Internet using IP addresses.

# Instructions

## Part 1: Verify connectivity to the web server

a.     Open the source host command prompt window. Select **PC0**.

b.     Select the Desktop Tab > Command Prompt.

c.     Verify connectivity to the web server. At the command prompt, ping the IP address of the web server by entering **ping 172.33.100.50**.

PC> **ping 172.33.100.50**

Pinging 172.33.100.50 with 32 bytes of data:

Reply from 172.33.100.50: bytes=32 time=0ms TTL=127

Reply from 172.33.100.50: bytes=32 time=0ms TTL=127

Reply from 172.33.100.50: bytes=32 time=0ms TTL=127

Reply from 172.33.100.50: bytes=32 time=0ms TTL=127

Ping statistics for 172.33.100.50:

Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

A reply verifies connectivity from the client to the destination web server. The reply may time out initially while devices load and ARP is performed.

d.     Close the command prompt window only, by selecting the x within the command prompt window. Be sure to leave the PC0 configuration window open.

## Part 2: Connect to the Web Server via the web client

a.     In the Desktop tab on PC0, select **Web Browser**.

b.     Enter **172.33.100.50** into the URL and click **Go**. The web client will connect to the web server via the IP address, and open the web page.

What messages did you see after the web page has finished loading?

*Answer Area*

Welcome to the Learn IP Web Site  
You were able to reach this website because you had the IP address of the web server. The connecting PC also had a web client running on the device.

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 3) Packet Tracer - Configure DHCP on a Wireless Router

### Objectives

* Connect 3 PCs to a wireless router
* Change the DHCP setting to a specific network range
* Configure the clients to obtain their address via DHCP

### Background / Scenario

A home user wants to use a wireless router to connect 3 PCs. All 3 PCs should obtain their address automatically from the wireless router.

### Instructions

### Part 1: Set up the network topology

1. Add three generic PCs.
2. Connect each PC to an Ethernet port to the wireless router using straight-through cables.

### Part 2: Observe the default DHCP settings

1. After the amber lights have turned green, click **PC0**. Click the **Desktop** tab. Select **IP Configuration**. Select **DHCP** to receive an IP address from **DHCP Enabled Router**.

Record the IP address of the default gateway:

Answer Area

**192.168.0.1**

Show Answer

1. Close the **IP Configuration** window.
2. Open a Web Browser.
3. Enter the IP address of the default gateway recorded earlier into the URL field. When prompted, enter the username **admin** and password **admin**.
4. Scroll through the Basic Setup page to view default settings, including the default IP address of the wireless router.
5. Notice that DHCP is enabled, the starting address of the DHCP range and the range of addresses available to clients.

### Part 3: Change the default IP address of the wireless router.

1. Within the Router IP Settings section, change the IP address to: **192.168.5.1**.
2. Scroll to the bottom of the page and click **Save Settings.**
3. If it is done correctly, the web page will display an error message. Close the web browser.
4. Click **IP Configuration** to renew the assigned IP address. Click **Static**. Click **DHCP** to receive new IP address information from the wireless router.
5. Open the web browser, enter the IP address **192.168.5.1** in the URL field. When prompted, enter the username **admin** and password **admin**.

### Part 4: Change the default DHCP range of addresses.

1. Notice the DHCP Server Start IP Address is updated to the same network as the Router IP.
2. Change the Starting IP Address from 192.168.5.100 to **192.168.5.126.**
3. Change the Maximum Number of Users to **75**.
4. Scroll to the bottom of the page and click **Save Settings**. Close the web browser.
5. Click **IP Configuration** to renew the assigned IP address. Click **Static**. Click **DHCP** to receive new IP address information from the wireless router.
6. Select **Command Prompt**. Enter **ipconfig**.

Record the IP address for PC0:

Answer Area

**192.168.5.126**

Show Answer

### Part 5: Enable DHCP on the other PCs.

1. Click **PC1**.
2. Select **Desktop** tab.
3. Select IP Configuration.
4. Click **DHCP**.

Record the IP address for PC1:

Answer Area

**192.168.5.127**

Show Answer

1. Close the configuration window.
2. Enable DHCP on **PC2** following the steps for PC1.

### Part 6: Verify connectivity

1. Click **PC2** and select the **Desktop** tab.
2. Select Command Prompt.
3. Enter **ipconfig** at the prompt to view the IP configuration.
4. At the prompt, enter **ping 192.168.5.1** to ping the wireless router.
5. At the prompt, enter **ping 192.168.5.127** to ping PC1.
6. The pings to all devices should be successful.

## 4) Packet Tracer - Examine NAT on a Wireless Router

### Objectives

* Examine NAT configuration on a wireless router
* Set up 4 PCs to connect to a wireless router using DHCP
* Examine traffic that crosses the network using NAT

### Instructions

**Part 1: Examine the configuration for accessing external network.**

1. Add 1 PC and connect it to the wireless router with a straight-through cable. Wait for all link lights to turn green before moving onto the next step or click Fast Forward.
2. On the PC, click Desktop. Select IP Configuration. Click DHCP to enable each device to receive an IP address via the DHCP on the wireless router.
3. Note the IP address of the default gateway. Close the IP Configuration when done.
4. Navigate to the web browser and enter the IP address of the default gateway in the URL field. Enter the username admin and password admin when prompted.
5. Click Status menu option in the upper right-hand corner. When selected, it displays the Router sub-menu page.
6. Scroll down the router page to the internet connection option. The IP address assigned here is the address assigned by the ISP. If no IP address is present (0.0.0.0 appears), close the window, wait for a few seconds and try again. The wireless router is in the process of obtaining an IP address from the ISP DHCP server.

Is this a private or public address?

Answer Area

**Private IP address**

Show Answer

### Part 2: Examine the configurations for accessing the internal network.

1. Click Local Network within the Status sub-menu bar.
2. Scroll down to examine the Local Network information. This is the address assigned to the internal network.
3. Scroll down further to examine the DHCP server information, and range of IP addresses that can be assigned to connected hosts.

Are these private or public addresses?

Answer Area

**Public IP address**

Show Answer

1. Close the wireless router configuration window.

### Part 3: Connect 3 PCs to the wireless router.

1. Add 3 more PCs and connect them to the wireless router with straight-through cables. Wait for all link lights to turn green before moving onto the next step or click Fast Forward.
2. On each PC, click Desktop. Select IP Configuration. Click DHCP to enable each device to receive an IP address via the DHCP on the wireless router. Close the IP Configuration when done.
3. Click Command Prompt to verify each device IP configuration using ipconfig /all command.  
   Note: These devices will receive a private address. Private addresses are not able to cross the internet, therefore, NAT translation must occur.

### Part 4: View NAT translation across the wireless router.

1. Enter Simulation mode by clicking the Simulation tab in the lower right-hand corner. The Simulation tab is located next to the Realtime tab and has a stopwatch symbol.
2. View traffic by creating a Complex PDU in Simulation mode:
   * From the Simulation Panel, click Show All/None to change visible events to none. Now click Edit Filters and under the Misc tab checkmark the boxes for TCP and HTTP. Close the window when done.
   * Add a Complex PDU by clicking on the opened envelope located in upper menu.
   * Click one of the PCs to specify it as the source.
3. Specify the Complex PDU settings by changing the following within the complex PDU window:
   * Under PDU Settings > Select Application should be set to: HTTP.
   * Click ciscolearn.nat.com server to specify it as the destination device.
   * For the Source Port, enter 1000.
   * Under Simulation Settings, select Periodic. Enter 120 seconds for the Interval.
   * Click Create PDU in the Create Complex PDU window.

### Part 5: View the header information of the packets that traveled across the network.

1. Examine the headers of the packets sent between a PC and the web server.
   1. In the Simulation Panel, double click the 3rd line down in the event list. This displays an envelope in the work area that represents that line.
   2. Click the envelope in the work area window to view the packet and header information.
2. Click the Inbound PDU details tab. Examine the packet information for the source (SRC) IP address and destination IP address.
3. Click the Outbound PDU details tab. Examine the packet information for the source (SRC) IP address and destination IP address.  
   Notice the change in SRC IP address.
4. Click through other event lines to view those headers throughout the process.
5. When finished, click Check Results to check your work.

## 4) question ) Packet Tracer - Examine NAT on a Wireless Router

### Objectives

* Examine NAT configuration on a wireless router
* Set up 4 PCs to connect to a wireless router using DHCP
* Examine traffic that crosses the network using NAT

### Instructions

**Part 1: Examine the configuration for accessing external network.**

1. Add 1 PC and connect it to the wireless router with a straight-through cable. Wait for all link lights to turn green before moving onto the next step or click Fast Forward.
2. On the PC, click Desktop. Select IP Configuration. Click DHCP to enable each device to receive an IP address via the DHCP on the wireless router.
3. Note the IP address of the default gateway. Close the IP Configuration when done.
4. Navigate to the web browser and enter the IP address of the default gateway in the URL field. Enter the username admin and password admin when prompted.
5. Click Status menu option in the upper right-hand corner. When selected, it displays the Router sub-menu page.
6. Scroll down the router page to the internet connection option. The IP address assigned here is the address assigned by the ISP. If no IP address is present (0.0.0.0 appears), close the window, wait for a few seconds and try again. The wireless router is in the process of obtaining an IP address from the ISP DHCP server.

Is this a private or public address?

Answer Area

**Private IP address**

Show Answer

### Part 2: Examine the configurations for accessing the internal network.

1. Click Local Network within the Status sub-menu bar.
2. Scroll down to examine the Local Network information. This is the address assigned to the internal network.
3. Scroll down further to examine the DHCP server information, and range of IP addresses that can be assigned to connected hosts.

Are these private or public addresses?

Answer Area

**Public IP address**

Show Answer

1. Close the wireless router configuration window.

### Part 3: Connect 3 PCs to the wireless router.

1. Add 3 more PCs and connect them to the wireless router with straight-through cables. Wait for all link lights to turn green before moving onto the next step or click Fast Forward.
2. On each PC, click Desktop. Select IP Configuration. Click DHCP to enable each device to receive an IP address via the DHCP on the wireless router. Close the IP Configuration when done.
3. Click Command Prompt to verify each device IP configuration using ipconfig /all command.  
   Note: These devices will receive a private address. Private addresses are not able to cross the internet, therefore, NAT translation must occur.

### Part 4: View NAT translation across the wireless router.

1. Enter Simulation mode by clicking the Simulation tab in the lower right-hand corner. The Simulation tab is located next to the Realtime tab and has a stopwatch symbol.
2. View traffic by creating a Complex PDU in Simulation mode:
   * From the Simulation Panel, click Show All/None to change visible events to none. Now click Edit Filters and under the Misc tab checkmark the boxes for TCP and HTTP. Close the window when done.
   * Add a Complex PDU by clicking on the opened envelope located in upper menu.
   * Click one of the PCs to specify it as the source.
3. Specify the Complex PDU settings by changing the following within the complex PDU window:
   * Under PDU Settings > Select Application should be set to: HTTP.
   * Click ciscolearn.nat.com server to specify it as the destination device.
   * For the Source Port, enter 1000.
   * Under Simulation Settings, select Periodic. Enter 120 seconds for the Interval.
   * Click Create PDU in the Create Complex PDU window.

### Part 5: View the header information of the packets that traveled across the network.

1. Examine the headers of the packets sent between a PC and the web server.
   1. In the Simulation Panel, double click the 3rd line down in the event list. This displays an envelope in the work area that represents that line.
   2. Click the envelope in the work area window to view the packet and header information.
2. Click the Inbound PDU details tab. Examine the packet information for the source (SRC) IP address and destination IP address.
3. Click the Outbound PDU details tab. Examine the packet information for the source (SRC) IP address and destination IP address.  
   Notice the change in SRC IP address.
4. Click through other event lines to view those headers throughout the process.
5. When finished, click Check Results to check your work.

5)) question 🙋

**Packet Tracer - Identify MAC and IP Addresses**

# Objectives

**Part 1: Gather PDU Information for a Local Network Communication**

**Part 2: Gather PDU Information for a Remote Network Communication**

# Instructions

## Part 1: Gather PDU Information for a Local Network Communication

In this part, you will study how a device on a local network does not need a default gateway to communicate with another device on the same local network.

**Note**: Review the Reflection Questions in Part 3 before proceeding with this part. It will give you an idea of the type of information you will need to gather.

a.     Click host **172.16.31.3** and open the **Command Prompt**.

b.     Enter the **ping 172.16.31.2** command. This command will issue a series of ICMP echo request packets to the destination. If the packets reach the destination, it will send echo-reply messages pack to the source of the ping requests.

c.     Click the **Simulation** mode button to switch to simulation mode. Repeat the **ping 172.16.31.2** command. An envelope icon that represents a PDU appears next to **172.16.31.3**.

d.     Click the PDU and locate the following information in both the **OSI Model** and **Outbound PDU Details** tabs. The **Outbound PDU Details** tab shows simplified packet and frame headers for the PDU. You should observe the following details regarding addressing for the PDU.

·         At Device: **172.16.31.3**

·         Source MAC Address: **0060.7036.2849**

·         Destination MAC Address: **000C:85CC:1DA7**

·         Source IP Address: **172.16.31.3**

·         Destination IP Address: **172.16.31.2**

e.     Click **Capture / Forward (the right arrow followed by a vertical bar)** and the PDU moves to the next step in its journey. Use the OSI model tab to gather the same information from Step 1d. Repeat this process until the PDU reaches its destination. For each step on the path to delivery, record the information for each PDU into a spreadsheet that uses a format like the table shown below. The information for the first step is shown in the table.

**Example Spreadsheet Format**

*Blank Line, No additional information*

| **At Device** | **Src MAC** | **Dest. MAC** | **Src IPv4** | **Dest IPv4** |
| --- | --- | --- | --- | --- |
| 172.16.31.3 | 0060.7036.2849 | 000C:85CC:1DA7 | 172.16.31.3 | 172.16.31.2 |
| Switch 2 | 0060.7036.2849 | 000C:85CC:1DA7 | N/A | N/A |
| 172.16.31.2 (in) | 000C:85CC:1DA7 | 000C:85CC:1DA7 | 172.16.31.3 | 172.16.31.2 |
| 172.16.31.2 (out) | 0060.7036.2849 | 0060.7036.2849 | 172.16.31.2 | 172.16.31.3 |

Hide Answer

*Blank Line, No additional information*

f.      You will notice that the information for the inbound PDU is unchanged.

#### Question:

In the PDU information window, click the tab for the outbound PDU. How does the addressing differ, and why? Record the addressing in your table.

***Answer Area***

**The source and destination address are reversed in both the frame and packet because this PDU will be sent back to host 172.16.31.3. This message will be a ping echo-reply.**

Hide Answer

g.     Return to **Realtime** mode.

## Part 2: Gather PDU Information for a Remote Network Communication

To communicate with remote networks, a gateway device is necessary. The gateway device connects two or more networks together. In this part, you will study the process that takes place when one device communicates with another device that is on a remote network. Pay close attention to the MAC addresses used.

**Note**: Move your mouse over the **Router**. You will see information about the addressing of the router interfaces. Refer to these addresses as you observe the PDU flow through the router.

a.     Return to the **Command Prompt** for **172.16.31.3**.

b.     Enter the **ping 10.10.10.2** command. The first couple of pings may time out.

c.     Switch to **Simulation** mode and repeat the **ping 10.10.10.2** command. A PDU appears next to **172.16.31.3**.

d.     Click the PDU and note the following information tab:

·         At Device: 172.16.31.3

·         Source MAC Address: 0060.7036.2849

·         Destination MAC Address: 00D0:BA8E:741A

·         Source IP Address: 172.16.31.3

·         Destination IP Address: 10.10.10.2

#### Question:

What device and interface has the destination MAC address that is shown?

***Answer Area***

**The router interface FasteEthernet1/0**

Hide Answer

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. Enter details for both the inbound and outbound PDUs at the Router.

*Blank Line, No additional information*

| **At Device** | **Src MAC** | **Dest. MAC** | **Src IPv4** | **Dest IPv4** |
| --- | --- | --- | --- | --- |
| 172.16.31.3 | 00D0:D311:C788 | 00D0:BA8E:741A | 172.16.31.3 | 10.10.10.2 |
| Switch 2 | 0060.7036.2849 | 00D0:BA8E:741A | N/A | N/A |
| Router (in) | 0060.7036.2849 | 00D0:BA8E:741A | 172.16.31.3 | 10.10.10.2 |
| Router (out) | 00D0:588C:2401 | 0060:2F84:4AB6 | 172.16.31.3 | 10.10.10.2 |
| Switch 1 | 00D0:588C:2401 | 0060:2F84:4AB6 | N/A | N/A |
| Access Point | N/A | N/A | N/A | N/A |
| 10.10.10.2 | 0060:2F84:4AB6 | 00D0:588C:2401 | 10.10.10.2 | 172.16.31.5 |

*Blank Line, No additional information*

6th question)

**Packet Tracer - Observe Traffic Flow in a Routed Network**

# Objectives

**Part 1: Observe Traffic Flow in an Unrouted LAN**

**Part 2: Reconfigure the Network to Route Between LANs**

**Part 3: Observe Traffic Flow in the Routed Network**

# Background / Scenario

The company that you work for has been asked to propose a new network design for XYZ LLC. XYZ is a startup company that has recently experienced success with their product offerings. They will be expanding, and their network will need to grow with them. Currently, the network is configured with a single IP network for hosts in all departments. This design has become inefficient and network delays are becoming increasingly noticeable. You have been asked to help prepare the proposal with the sales team. The sales team will propose a solution in which network efficiency is enhanced by implementing routing between separate department networks. You are working on a demonstration of how having multiple routed networks in a business can improve network efficiency. Follow the instructions to go through the demonstration to help propose a new network to XYZ LLC.

# Instructions

## Part 1: Observe Traffic Flow in an Unrouted LAN

The XYZ network consists of about 150 devices that are connected to a LAN. The LAN is configured on a single IPv4 network. Hosts in different departments are connect to switches which are then connected to the **Edge** router. The router only routes traffic between the LAN and the internet, represented by the **ISP** cloud. Because only one IP network is used in the LAN, all departments are on the same network.

The Packet Tracer topology is simplified. It only shows some of the departments and hosts. Assume that the behavior that you will demonstrate is happening at far greater scale than what is shown in the PT network.

In this part, you will use Packet Tracer simulation mode to observe how traffic flows through an unrouted LANs.

### Step 1: Clear the ARP cache on host Sales 1.

Hover your mouse over the **Sales 1** host to see its IP address. Make note of it.

a.     Click **Sales 1** > **Desktop** tab > **Command Prompt**, and then enter the **arp -a**command. There should be no MAC addresses in the ARP cache. If there are entries in the ARP cache, use the **arp -d** command to delete them.

### Step 2: Observe traffic flow in the network.

a.     Click the **Simulation** mode button in the lower right-hand corner of the PT window to switch from **Realtime** to **Simulation** mode.

b.     Open the **Command Prompt** for **Sales 2**, and then enter the **ping** command followed by the IP address of **Sales 1**.

c.     Use the **Capture then Forward** button (the triangle pointing to the right with a vertical bar attached) in the **Play Controls** of the **Simulation Panel** to begin to execute the **ping** command. You will see a colored envelope icon appear next to Sales 2. This represents a PDU. Click the **Capture then Forward** button to move the PDU to the first device on its path to the destination device. Click the PDU envelope to inspect the contents.

#### Questions:

What are the source and destination MAC and IP addresses for the frame and packet?

***Answer Area***

**The frame source MAC address is the MAC address of Sales 1. The destination MAC address is the MAC broadcast address of FFFF.FFFF.FFFF. The packet source IP address is the IP address of Sales 1. The destination IP address is the destination of Sales 2.**

Hide Answer

Why is the destination MAC address the broadcast address?

***Answer Area***

**Because the host ARP cache is empty, the host must first issue an ARP request to obtain the destination MAC address so that the frame can be addressed to the Sales 1.**

Hide Answer

d.     Advance the PDUs through the network until a new PDU (different color) is created at **Sales 2**.

#### Questions:

Which hosts and other types of devices needed to process the ARP request packets?

***Answer Area***

**All hosts and the router interface**

Hide Answer

What is the impact of this on efficient operation of the network as it is currently configured?

***Answer Area***

**Even though the destination for the ping requests may be adjacent to the requesting source, if the host has an empty ARP cache, an ARP request is sent that must be processed by every host on the network. ARP cache entries are removed after a preset period of time. With many hosts on a network, ARP broadcasts will be issued more frequently. This requires network resources to be taken away for the work-related traffic.**

Hide Answer

e.     A new PDU with a different color has appeared at Sales 2. Click the new PDU and inspect its contents. Look at the outbound PDU details.

#### Question:

What type of PDU is this?

***Answer Area***

**It is the first ICMP echo-request packet that is issued by ping from host Sales 2.**

Hide Answer

f.      Return to **Realtime** mode.

## Part 2: Reconfigure the Network to Route Between LANs.

In this part, you will demonstrate the benefits of routing between department networks. First, you will cable each network switch to connect directly to a router interface. Then, you will reconfigure the hosts to receive addresses on two new IPv4 networks that are created by the router.

### Step 1: Change device connections.

The three switches are connected to each other with copper straight through cables.

a.     For the cable that connects the **Accounting** switch with **Finance** switch, click the green triangle on the **Accounting** switch side of the link.

b.     Drag that end of the cable to the **Edge** router and connect the cable to port **GigabitEthernet 1/0**.

c.     Repeat this step for the link between **Finance** and **Sales**. Connect to the available GigabitEthernet port.

### Step 2: Configure the hosts with addresses on the new LANs.

Each interface of the **Edge** router was previously configured to put each department on its own IPv4 network. The hosts will receive their new IP addresses from the router. However, it will take time for the hosts on the **Finance** and **Sales** networks to receive their new IP addresses. (The hosts on the Accounting network will remain on 192.168.1.0/24.)

a.     To speed up the process of getting new IP addresses, open a **Command Prompt** on each of the four devices in the **Finance** and **Sales** networks.

b.     Enter the **ipconfig /renew** command. This will force the host to request a new IP address from the DHCP server that is running on the **Edge** router. You should see confirmation of new IP addressing.

What IPv4 network is assigned to the **Finance** network?

***Answer Area***

**192.168.2.0/24**

Hide Answer

What IPv4 network is assigned to the **Sales** network?

***Answer Area***

**192.168.3.0/24**

Hide Answer

## Part 3: Observe Traffic Flow in the Routed Network.

In this part, you will observe how traffic now flows through a routed network.

### Step 1: Ping Sales 1 from Sales 2.

a.     Return to the **Command Prompt** for **Sales 2** and verify that its ARP cache is empty. If it is not, delete any entries.

b.     Switch to **Simulation** mode.

c.     Ping **Sales 1** from **Sales 2**.

d.     Use the **Capture then Forward** button to step the PDUs through the network. Observe how the ARP request message flows through the network this time.

#### Question:

Which devices receive the ARP broadcasts this time?

***Answer Area***

**Only Sales 1 and the router interface that is connected to the Sales department network process the PDU.**

Hide Answer

### Step 2: Ping other hosts.

Repeat this demo by pinging other hosts and the internet server. Observe the flow of the ARP request PDUs.

#### Question:

**7TH QUESTION)**

**Packet Tracer - Create a LAN**

# Addressing Table

| **Device** | **Interface/Port** | **IPv4 Address** | **Subnet Mask** |
| --- | --- | --- | --- |
| Admin PC | NIC | DHCP | N/A |
| Manager PC | NIC | DHCP | N/A |
| Printer | NIC | 192.168.1.100 | 255.255.255.0 |
| www.cisco.pt | NIC | 209.165.200.225 | N/A |

*Blank Line, No additional information*

# Objectives

=   Connect Network Devices and Hosts

=   Configure Devices with IPv4 Addressing

=   Verify the End Device Configuration and Connectivity

=   Use Networking Commands to View Host Information

# Background / Scenario

A new branch office is opening, and you have been asked to set up the LAN. The network devices are already set up, but you need to connect them and the hosts together. You also need to configure IPv4 addressing on the end devices and verify that they can reach local and remote resources.

# Instructions

## Part 1: Connect Network Devices and Hosts

### Step 1: Power on the end devices and Office Router.

a.     Click each device and open its Physical Tab. **Note**: There is no power switch on the switch model used in this activity.

b.     Locate the power switch for each device in the Physical Device View window.

c.     Click the power switch to turn the device on. You should see a green light near the power switch to indicate that the device is powered on.

### Step 2: Connect the end devices.

Use the table and instructions to connect the network devices and hosts to create the physical network.

**Connections Table**

| **Device** | **Interface/Port** | **Connected to Device** | **Connection Interface/Port** |
| --- | --- | --- | --- |
| Office Router | G0/0 | ISP1 | G0/0 |
| Office Router | G0/1 | Switch | G0/1 |
| Admin PC | NIC (F/0) | Switch | F0/1 |
| Manager PC | NIC (F/0) | Switch | F0/2 |
| Printer | NIC (F/0) | Switch | F0/24 |

*Blank Line, No additional information*

**Note:** In the table above, interfaces designated with **G** are GigabitEthernet interfaces. Interfaces that are designated with **F** are FastEthernet interfaces.

a.     Connect the networking devices according to the information in the **Connections Table** using Ethernet copper straight-through cables. For the internet to Office Router connection, select the device and port from the dropdown menus that appear when you click the cloud with connections tool selected.

b.     Connect the two PCs and the printer to the office switch according to the information in the connections table. Use copper straight-through cables.

c.     You should see green link lights on all connections after a brief delay.

## Part 2: Configure Devices with IPv4 Addressing

### Step 1: Configure the hosts with addressing information.

a.     The Admin and Manager PCs should receive their IP addressing information from DHCP. The Office Router has been configured to supply IP addresses to hosts on the branch office LAN. Click the PCs and go to the Desktop tabs on each PC. Open the IP Configuration application and configure the PCs to receive their IP addresses dynamically.

b.     Printers and servers are often manually configured with addressing because other devices on the network are configured to access them using IP addresses. Manual configuration with a static address will ensure that the IP addresses of these devices do not change.

1)    Click the printer and open the Config tab.

2)    Click the FastEthernet0 interface in the left-hand pane.

3)    Enter the addressing information from the Addressing Table.

c.     Because the two computers are on the same network, their IPv4 addresses will be similar, their subnet masks and default gateways will be identical.

#### Questions:

Why do you think the IPv4 addresses are different, but the subnet masks and default gateways are the same?

***Answer Area***

**Answers will vary. Each device on the network must have a unique identifier. The IPv4 address is one way of uniquely identifying each network host or device. The default gateway represents the way of communicating with devices that are NOT on the local network.**

Hide Answer

The printer does not require a default gateway because it will only be accessed by hosts on the local network. However, if you need to configure it with a default gateway, which value will the printer use? How can you determine this from the other devices in the network?

***Answer Area***

**You can determine the default gateway value to use by looking at the values that PCs have been configured with by DHCP, or by determining the IP address of the Office Router Ethernet interface that is connected to the branch office LAN.**

Hide Answer

## Part 3: Verify the End Device Configuration and Connectivity

### Step 1: Verify connectivity between the two PCs.

a.     Go to the desktops of the PCs and check the IP addressing configuration. You should see that the PCs have dynamically received IP addresses on the 192.168.1.0 255.255.255.0 network. You should also see that they have received addresses for the Default Gateway and DNS server settings.

b.     From the command prompt on Admin PC, ping the IP address of the Printer. Repeat this process for the Manager PC. You should see successful pings for each. This verifies that the PCs and the printer are powered on, and correctly connected and addressed.

### Step 2: Verify connectivity to the internet.

From the desktop of the PCs, open the Web Browser. Enter the IP address of the internet server to display the webpage. Repeat the process but connect using the URL of the server.

#### Question:

## Part 4: Use Networking Commands to View Host Information

The networking commands that are available from command prompt on PCs are very similar to those that are available in Windows. In this part of the activity, you will use **ipconfig** and **tracert** to learn more about the LAN.

### Step 1: Use the ipconfig command.

The **ipconfig** command displays details about the addressing that is configured on a host.

#### Question:

Open a command prompt on one of the PCs and enter the **ipconfig** command and make note of the information that is returned. Now enter the **ipconfig /all** command. What additional information is displayed?

***Answer Area***

**The ipconfig /all displays information about the physical (MAC) address of the NIC. It also displays the DHCP and DNS server addresses. In Windows, many additional details are displayed. Type ipconfig /all from the command prompt of a PC to view all the information that Windows displays with this command.**

Hide Answer

### Step 2: Use the tracert command.

The **tracert** command uses ICMP to return information about the routers that are passed as packets go from the source PC to the destination.

Trace to a remote destination by going to one of the PCs and entering **tracert** followed by the URL of the web server.

#### Questions:

8TH QUESTION)

**Packet Tracer - The Client Interaction**

# Objectives

Observe the client interaction between the server and PC.

# Background / Scenario

Clients, such as desktop PCs, request services from servers. The lab environment, using physical PCs and servers, supports a full range of services. In a simulated environment, the number of services is limited. Packet Tracer allows the addition of simulated network servers that support DHCP, DNS, HTTP, and TFTP. Packet Tracer also supports the addition of simulated PCs that can request these services. This activity uses a simple network consisting of a PC connected directly to a server configured to supply DNS services as well as hosting a web page through an HTTP server. This activity will track the flow of traffic that happens when a web page is requested, how the IP address of the web page is resolved, and the web page is delivered.

# Instructions

## Part 1: Enter simulation mode.

When Packet Tracer starts, it presents a logical view of the network in realtime mode.

Click the **Simulation Mode** to enter simulation mode. The simulation mode icon is located in the bottom right-hand of the logical workplace.

## Part 2: Set Event List Filters.

In simulation mode, the default is to capture all events. You will use filters to only capture DNS and HTTP events.

a.     In the **Event List Filters** section, click **Show All/None**to clear all the checks.

b.     Click **Edit Filters**. Under the IPv4 tab, select **DNS**. Under the Misc tab, select **HTTP**. Close the window when done. The **Event List Filters**shows DNS and HTTP as the only visible events.

## Part 3: Request a web page from the PC.

You will open a simulated web browser on the PC and request a web page from the server.

a.     Click **PC**. Click **Desktop**tab and click **Web Browser**.

b.     A simulated web browser opens. Type **www.example.com**into the URL box and click **Go** button to the right. Minimize the PC window.

## Part 4: Run the simulation.

a.     In the **Play Controls**section of the **Simulation Panel**, click **Play**. The exchange between the PC and the server is animated and the events are added to the **Event List**.

These events represent the PC’s request to resolve the URL to an IP address, the server’s providing of the IP address, the PC's request for the web page, the server’s sending the web page in two segments, and the PC’s acknowledging the web page.

b.     Click **View Previous Event**to continue when the buffer is full.

## Part 5: Access a specific PDU.

a.     Restore the simulated PC window. Notice there is a web page displayed in the Web Browser. Minimize the simulated browser window.

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

## Part 6: Examine the contents of the PDU Information Window.

The first tab in the PDU Information window contains information about the inbound and/or outbound PDU as it relates to the OSI model. Click **Next Layer >>** repeatedly to cycle through the inbound and outbound layers and read the description in the box below the layers to get an overview of how the exchange works.

Examine the PDU information for the other events to get an overview of the entire exchange process.

*End of document*

9th question)

**Packet Tracer - Observe Web Request**

# Objectives

View the client/server traffic sent from a PC to a web server when requesting web services.

# Instructions

## Part 1: Verify connectivity to the web server.

a.     Click **External Client** and access the **Command Prompt**from the **Desktop**tab.

b.     Use the **ping**command to reach the URL **ciscolearn.web.com**.

PC> **ping ciscolearn.web.com**

Notice the IP address included in the ping output. This address is obtained from the DNS server and resolves to the domain name ciscolearn.web.com. All traffic forwarded across a network uses source and destination IP address information.

c.     Close the Command Prompt window but leave the External Client desktop window open.

## Part 2: Connect to the web server.

a.     From the Desktop window, access the **Web Browser**.

b.     In the URL block, type **ciscolearn.web.com**.

\*Be sure to read the web page that is displayed. Leave this page open.

c.     Minimize the External Client window but do not close it.

## Part 3: View the HTML code.

a.     From the Logical topology, click **ciscolearn.web.com** server.

b.     Click the **Services** tab > **HTTP**tab. Then next to the **index.html** file click**(edit)**.

c.     Compare the HTML markup code on the server that creates the Web Browser display page on the External Client. This may require that you re-maximize the External Client window if it shrunk when you opened the server window.

d.     Close both the External Client and web server windows.

## Part 4: Observe traffic between the client and the web server.

a.     Enter Simulation mode by clicking the **Simulation** tab in the lower right-hand corner.

b.     Double click the Simulation Panel to unlock it from the PT window. This allows you to move the Simulation Panel to view the entire network topology.

c.     View traffic by creating a Complex PDU in Simulation mode.

1)    From the **Simulation Panel**, select **Edit Filters**.

2)    Click the Misc tab to verify that only the boxes for TCP and HTTP are selected.

3)    Add a Complex PDU by clicking the open envelope located above the Simulation mode icon.

4)    Click the **External Client** to specify it as the source. The **Create Complex PDU** window will appear.

d.     Specify the Create **Complex PDU** settings by changing the following within the Complex PDU window:

1)    Under PDU Settings, Select Application should be set to **HTTP**.

2)    Click the **ciscolearn.web.com** server to specify it as the destination device. Notice the IP address of the web server will appear in the destination box within the complex PDU window

3)    For the Starting Source Port, enter **1000**.

4)    Under Simulation Settings, select Periodic Interval and type **120** seconds.

e.     Create the PDU by clicking the box **Create PDU** in the **Create Complex PDU** window.

1)    Observe the traffic flow by clicking **Play** in the Simulation Panel. Speed up the animation by using the play control slider.

When the Buffer Full window appears, click **View Previous Events** to close the window.

2)    Scroll through the Event List. Notice the number of packets that traveled from source to destination. HTTP is a TCP protocol, which requires connection establishment and acknowledgement of receipt of packets, considerably increasing the amount of traffic overhead.

10th question)

## Packet Tracer - Use FTP Services

### Addressing Table

| Device | Interface | IP Address | Subnet Mask |
| --- | --- | --- | --- |
| FTP Server (ftp.pka) | NIC | 209.165.200.226 | 255.255.255.224 |

### Objectives

· Upload a file to an FTP server

· Download a file from an FTP server.

### Background / Scenario

File Transfer Protocol (FTP) is a commonly used application to transfer files between clients and servers on the network. The server is configured to run the service where clients connect, login, and transfer files. FTP uses port 21 as the server command port to create the connection. FTP then uses port 20 for data transfer.

In this activity, you will upload a file to an FTP server. You will also download a file from an FTP server.

### Instructions

### Part 1: Upload a file to an FTP server.

In this part, you will locate the file sampleFile.txt and upload it to an FTP server.

### Step 1: Locate the file.

1. **Click PC-A.**
2. Click **Desktop**.
3. Click **Command Prompt.**
4. At the prompt, click ? to list the available commands.
5. Enter **dir** to see the files on the PC. Notice that there is a sampleFile.txt file in the C:\ directory.

C: > **dir**

Volume in drive C has no label.

Volume Serial Number is 5E12-4AF3

Directory of C:\

12/31/1969 17:0 PM 26 sampleFile.txt

26 bytes 1 File(s)

### Step 2: Connect to the FTP server

1. FTP to the FTP server at**209.165.200.226**or **ftp.pka**.

C:\> **ftp 209.165.200.226**

Trying to connect...209.165.200.226

Connected to 209.165.200.226

1. Enter the username **student**and password **class** to gain access.

220- Welcome to PT Ftp server

Username:**student**

331- Username ok, need password

Password:

230- Logged in

(passive mode On)

### Step 3: Upload a file to an FTP server

1. Enter ? to see the commands available in the ftp client.

ftp> **?**

?

cd

delete

dir

get

help

passive

put

pwd

quit

rename

ftp>

1. Enter **dir** to see the files available on the server.

ftp> **dir**

Listing /ftp directory from 192.168.1.3:

0 : asa842-k8.bin 5571584

1 : asa923-k8.bin 30468096

2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768

3 : c1841-ipbase-mz.123-14.T7.bin 13832032

1. Enter put sampleFile.txt to send the file to the server.

ftp> **put sampleFile.txt**

Writing file sampleFile.txt to 209.165.200.226:

File transfer in progress..

[Transfer complete - 26 bytes]

26 bytes copied in 0.08 secs (325 bytes/sec)

ftp>

1. Use the **dir** command again to list the contents of the FTP server to verify that the file has been uploaded to the FTP server.

### Part 2: Download a file from an FTP server.

You can also download a file from an FTP server. In this part, you will rename the file sampleFile.txt and download it from the FTP server.

### Step 1: Rename the file on an FTP server.

1. At the **ftp>**prompt, rename the file **sampleFile.txt**to **sampleFile\_FTP.txt**.

ftp> **rename sampleFile.txt sampleFile\_FTP.txt**

Renaming sampleFile.txt

ftp>

[OK Renamed file successfully from sampleFile.txt to sampleFile\_FTP.txt]

ftp>

1. At the **ftp>**prompt, enter**dir** to verify the file has been renamed.

### Step 2: Download the file from the FTP server.

1. Enter the command **get sampleFile\_FTP.txt** to retrieve the file from the server.

ftp> **get sampleFile\_FTP.txt**

Reading file sampleFile\_FTP.txt from 209.165.200.226:

File transfer in progress...

[Transfer complete - 26 bytes]

26 bytes copied in 0.013 secs (2000 bytes/sec)

ftp>

1. Enter **quit** to exit the FTP client when finished.
2. Display the contents of the directory on the PC again to see the image file from the FTP server

### Step 3: Delete the file from the FTP server.

1. Log into the FTP server again to delete the file **sampleFile\_FTP.txt**.
2. Enter the command to delete the file**sampleFile\_FTP.txt**from the server.

What command did you use to remove the file from the FTP server?

Answer Area

***ftp> delete sampleFile\_FTP.txt***

11th question)

## Packet Tracer - Use Telnet and SSH

### Addressing Table

| Device | Interface | IP Address | Subnet Mask |
| --- | --- | --- | --- |
| HQ | G0/0/1 | 64.100.1.1 | 255.255.255.0 |
| PC0 | NIC | DHCP | |
| PC1 | NIC | DHCP | |

### Objectives

In this activity, you will establish a remote connection to a router using Telnet and SSH.

· Verify connectivity.

· Access a remote device.

### Instructions

### Part 1: Verify Connectivity

In this part, you will verify that the PC has IP addressing and can ping the remote router.

### Step 1: Verify IP address on a PC.

1. From a PC, click **Desktop**. Click Command Prompt.
2. At the prompt, verify that the PC has an IP address from DHCP.

What command did you use to verify the IP address from DHCP?

Answer Area

***ftp> ipconfig***

Hide Answer

### Step 2: Verify connectivity to HQ.

Verify that you can ping the router HQ using the IP address listed in the Addressing Table.

### Part 2: Access a Remote Device

In this part, you will attempt to establish a remote connection using Telnet and SSH.

### Step 1: Telnet to HQ.

At the prompt, enter the command telnet 64.100.1.1

Were you successful? What was the output?

Answer Area

***No.***

***C:\> telnet 64.100.1.1***

***Trying 64.100.1.1 ...Open***

***[Connection to 64.100.1.1 closed by foreign host]***

Hide Answer

### Step 2: SSH to HQ.

The router is properly configured to not allow insecure Telnet access. You must use SSH.

At the prompt, enter the command **ssh -l admin 64.100.1.1.** Enter the password **class** when prompted

C:\> **ssh -l admin 64.100.1.1**

**----------------------------------------------------------------------------------------------------**

12th question)

**Packet Tracer - Use the ipconfig Command**

# Objectives

·         Use the **ipconfig**command to identify incorrect configuration on a PC.

# Background / Scenario

A small business owner cannot connect to the internet with one of the four PCs in the office. All the PCs are configured with static IP addressing using 192.168.1.0 /24 network. The PCs should be able to access **www.cisco.pka** webserver. Use the **ipconfig /all**command to identify which PC is incorrectly configured.

# Instructions

## Part 1: Verify Configurations

a.     Access the **Command Prompt**on each PC and type the command **ipconfig /all**at the prompt.

b.     Examine the IP address, subnet mask, and default gateway configuration for each PC. Be sure to record this IP configuration for each PC to help identify any PCs that are incorrectly configured.

## Part 2: Correct Any Misconfigurations

a.     Select the PC that is incorrectly configured.

b.     Click the **Desktop**tab > **IP Configuration**tab to correct the misconfiguration

13th question)

## Packet Tracer - Use the ping Command

### Objectives

Use the **ping** command to identify an incorrect configuration on a PC.

### Background / Scenario

A small business owner learns that some users are unable to access a website. All PCs are configured with static IP addressing. Use the **ping** command to identify the issue.

### Instructions

### Part 1: Verify connectivity.

Access the **Desktop** tab > **Web Browser**of each PC and enter the URL **www.cisco.pka.** Identify any PCs that are not connecting to the web server.

**Note:** All the devices require time to complete the boot process. Please allow up to one minute before receiving a web response.

Which PCs are unable to connect to the web server?

Answer Area

***PC2***

Hide Answer

### Part 2: Ping the web server from PC with connectivity issues.

1. On the PC, access the **Command Prompt** from the **Desktop** tab.
2. At the prompt, enter **ping www.cisco.pka**.

Did the ping return a reply? What is the IP address displayed in the reply, if any?

Answer Area

***Reply was returned with 192.15.2.10 as the IP address for www.cisco.pka.***

Hide Answer

### Part 3: Ping the web server from correctly configured PCs.

1. On the PC, access the **Command Prompt** from the **Desktop** tab.
2. At the prompt, enter **ping www.cisco.pka**.

Did the **ping** return a reply? What is the IP address returned, if any?

Answer Area

***Answers will vary. The default gateway is 192.168.1.1 in this example. For a home network using a wireless router, the default gateway address can be the same IP address as the wireless router.***

Hide Answer

### Part 4: Ping the IP address of the web server from PCs with connectivity issues.

1. On the PC, access the **Command Prompt** from the **Desktop** tab.
2. Attempt to reach the IP address of the web server with the **ping**command.

Did the ping return a reply? If so, then the PC can reach the web server via IP address, but not domain name. This could indicate a problem with the DNS server configuration on the PC.

### Part 5: Compare the DNS server information on the PCs.

1. Access the **Command Prompt** of the PCs without any issues.
2. Using the command **ipconfig /all**, examine the DNS server configuration on the PCs without any issues.
3. Access the **Command Prompt** of the PCs with connectivity issues.
4. Using the command **ipconfig /all**, examine the DNS server configuration on the PCs with misconfigurations. Do the two configurations match?

### Part 6: Make any necessary configuration changes on the PCs.

1. Navigate to the **Desktop** tab of the PCs with issues, make any necessary configuration changes in **IP Configuration.**
2. Using the **Web Browser** within the **Desktop** tab, connect to **www.cisco.pka** to verify that the configuration changes resolved the problem.

---------------------------------------------------------------------------------------------------------------------------

14th question)

**Packet Tracer - Create a Simple Network**

# Objectives

In this activity, you will build a simple network in Packet Tracer in the Logical Workspace.

**Part 1: Build a Simple Network**

**Part 2: Configure the End Devices and Verify Connectivity**

# Instructions

## Part 1: Build a Simple Network

In this part, you will build a simple network by deploying and connecting the network devices in the Logical Workspace.

### Step 1: Add network devices to the workspace.

In this step, you will add a PC, laptop, and a cable modem to the Logical Workspace.

A cable modem is a hardware device that allows communications with an Internet Service Provider (ISP). The coaxial cable from the ISP is connected to the cable modem, and an Ethernet cable from the local network is also connected. The cable modem converts the coaxial connection to an Ethernet connection.

Using the Device-Type Selection Box, add the following devices to the workspace. The category and sub-category associated with the device are listed below:

=   **PC**: End Devices > End Devices > PC

=   **Laptop**: End Devices > End Devices > Laptop

=   **Cable Modem**: Network Devices > WAN Emulation > Cable Modem

### Step 2: Change display names of the nework devices.

a.     To change the display names of the network devices, click the device icon in the Logical Workspace.

b.     Click the **Config** tab in the device configuration window.

c.     Enter the new name of the newly added device into the **Display Name** field: PC, Laptop, and Cable Modem.

### Step 3: Add the physical cabling between devices on the workspace.

Using the Device-Type Selection Box, add the physical cabling between devices on the workspace.

a.     The PC will need a copper straight-through cable to connect to the wireless router. Using the Device-Type Selection Box, click **Connections** (lightning bolt icon). Select the copper straight-through cable in the Device-Specific Selection Box and attach it to the **FastEthernet0** interface of the PC and the **Ethernet 1** interface of the wireless router.

b.     The wireless router will need a copper straight-through cable to connect to the cable modem. Select the copper straight-through cable in the Device-Specific Selection Box and attach it to the internet interface of the wireless router and the **Port 1** interface of the cable modem.

c.     The cable modem will need a Coaxial cable to connect to the internet cloud. Select the Coaxial cable in the Device-Specific Selection Box and attach it to the **Port 0** interface of the cable modem and the **Coaxial 7** interface of the internet cloud.

## Part 2: Configure the End Devices and Verify Connectivity

In this part, you will connect a PC and a laptop to the Wireless router. The PC will be connected to the network using an Ethernet cable. For the Laptop, you will replace the wired Ethernet network interface card (NIC) with a wireless NIC and connect the Laptop to the router wirelessly.

After both end devices are connected to the network, you will verify connectivity to cisco.srv. The PC and the Laptop will each be assigned an IP (Internet Protocol) address. Internet Protocol is a set of rules for routing and addressing data on the internet. The IP addresses are used to identify the devices on a network and allow the devices to connect and transfer data on a network.

### Step 1: Configure the PC.

You will configure the PC for the wired network in this step.

a.     Click the **PC**. In the **Desktop** tab, navigate to **IP Configuration** to verify that DHCP is enabled and the PC has received an IP address.

Select **DHCP** for the IP Configuration heading if you do not see an IP address for the IPv4 Address field. Observe the process as the PC is receiving an IP address from the DHCP server.

DHCP stands for dynamic host configuration protocol. This protocol assigns IP addresses to devices dynamically. In this simple network, the Wireless Router is configured to assign IP addresses to devices that request IP addresses. If DHCP is disabled, you will need to assign an IP address and configure all the necessary information to communicate with other devices on the network and the internet.

b.     Close **IP Configuration**. In the **Desktop** tab, click **Command Prompt**.

c.     At the prompt, enter **ipconfig /all** to review the IPv4 addressing information from the DHCP server. The PC should have received an IPv4 address in the 192.168.0.x range.

**Note:** There are two types of IP addresses: IPv4 and IPv6. An IPv4 (internet protocol version 4) address is a string of numbers in the form of x.x.x.x as you have been using in this lab. As the internet grew, the need for more IP addresses became necessary. So IPv6 (internet protocol version 6) was introduced in the late 1990s to address the limitations of IPv4. The details of IPv6 addressing are beyond the scope of this activity.

d.     Test connectivity to the cisco.srv from the PC. From the command prompt, issue the command **ping cisco.srv**. It may take a few seconds for the ping to return. Four replies should be received.

### Step 2: Configure the Laptop.

In this step, you will configure the Laptop to access the wireless network.

a.     Click **Laptop**, and select the **Physical** tab.

b.     In the **Physical** tab, you will need to remove the Ethernet copper module and replace it with the Wireless WPC300N module.

1)    Power off **Laptop** by clicking the power button on the side of the laptop.

2)    Remove the currently installed Ethernet copper module by clicking on the module on the side of the laptop and dragging it to the **MODULES** pane on the left of the laptop window.

3)    Install the wireless **WPC300N** module by clicking it in the **MODULES** pane and dragging it to the empty module port on the side of the Laptop.

4)    Power on the **Laptop** by clicking the Laptop power button again.

c.     With the wireless module installed, connect the Laptop to the wireless network. Click the **Desktop** tab and select the **PC Wireless**.

d.     Select the **Connect**tab. After a slight delay, the wireless network **HomeNetwork** will be visible in the list of wireless networks. Click **Refresh** if necessary to see the list of available networks. Select the **HomeNetwork**. Click **Connect**.

e.     Close **PC Wireless**. Select **Web Browser** in the Desktop tab.

f.      In the Web Browser, navigate to **cisco.srv**.

# Reflection

Now that you have verified connectivity to cisco.srv, use the command **ipconfig** from the Command Prompt to fill out the IP addressing table below:

| **Device** | **IPv4 Address** | **Subnet Mask** | **Default Gateway** |
| --- | --- | --- | --- |
| PC | Answer Area | Answer Area | Answer Area |
| Laptop | Answer Area | Answer Area | Answer Area |

*Linea en blanco - sin información adicional*

| **Device** | **IPv4 Address** | **Subnet Mask** | **Default Gateway** |
| --- | --- | --- | --- |
| PC | 192.168.0.2 | 255.255.255.0 | 192.168.0.1 |
| Laptop | 192.168.0.3 | 255.255.255.0 | 192.168.0.1 |

Hide Answer

*Blank Line, No additional information*

The IP addresses for the end devices can range from 192.168.0.2 – 192.168.0.254. Each NIC will get a unique IP address in the same network.

The subnet mask is used to differentiate the host and the network ID portion of the IP address. You can relate the IP address to your street address. The subnet mask defines the length of the street name. The network part of the address is your street, 192.168.0. The house number is the host port of the IP address. For the IP address 192.168.0.2, the house number is 2 and the street is 192.168.0. If there is more than one house on the same street, for example, house number 3, will have an address 192.168.0.3. The maximum number of houses on this street is 253, ranging from 2 to 254