Packet Tracer - Build a Home Network

Objectives

Part 1: Connect and Configure Devices

Part 2: Use Network Services

Part 3: Use Packet Tracing to Visualize Network Communication

Background / Scenario

In this Packet Tracer (PT) activity, you will setup a home network. You will connect and configure wired and wireless devices. To make it easier for guests to connect to the network, you will also configure a guest wireless network. After the network is operational, you will configure email, transfer files, and investigate the email and domain name servers. Finally, you will explore how Packet Tracer simulates network communications.

Note: The Packet Tracer activity opens in **Physical** mode. However, you can complete it in either **Physical** mode or **Logical** mode. You can switch between these modes at any time to compare the differences by clicking the **Logical** (Shift+L) and **Physical** (Shift+P) buttons. However, in other activities in this course you may be locked out of one mode or the other.

Note: Not all tasks in this activity are graded. However, at any time you can click **Check Results** to see your progress towards completing the scored parts of this activity.

Instructions

Part 1: Connect and Configure Devices

In Part 1, you will connect home network components including a cable modem and a home router. You will connect a wired printer and two PCs to the network. You will also configure wireless local area networks (WLANs) for both family members and guests. Finally, you will verify all devices have connectivity.

Step 1: Explore the three accessible networks in Greenville.

Note: The **Data Center** is locked in this activity.

a. In **Physical** mode, click each location and explore each network. Click **Back level** (Alt+Left) to return to **Greenville**.

b. Switch to **Logical** mode. Click each cloud to view the logical topologies for the corresponding sites that you visited in **Physical** mode.

c. Switch back to **Physical** mode. You can complete Part 1 and Part 2 in either mode. **Physical** mode is recommended. However, Part 3 must be completed in **Logical** mode.

Step 2: Identify the devices in the Home network.

a. Click **Home** and locate all the devices in the home network.

Note: You may need to zoom in to see the device name or move the mouse over a device to see its name in the pop-up information box for the device.

b. In the home office, there are six devices: a wireless router and modem behind the desk on the bottom shelf, a webcam on the top shelf, a printer and a PC on the desk, and a laptop on the table in front of the couch.

c. In the bedroom, there is one PC.

d. In the living room, there is a smartphone on the small table in front of the chair and a laptop on the coffee table.

Step 3: Connect the router to the modem.

A technician from the Internet Service Provider (ISP) has already connected the modem to the **ISP/Telco** network. You need to connect the modem to the home router.

a. In the **Bottom Toolbar**, click **Connections** (lightning bolt icon), and then click **Copper Straight-Through**.

b. Click **Home_Modem**, and select **Port 1**,

c. Click **Home Wireless Router**, and then select the **Internet** port to make the connection. You will see a green triangle when you have made the connection.

Step 4: Connect the wired hosts to the switch ports on the router.

From the **Bottom Toolbar**, use a **Copper Straight-Through** cable to connect the **FastEthernet0** port on each of the following devices to the **Home Wireless Router**.

- **Family PC**
- **Home Office PC**
- **Home Printer**

Step 5: Configure the Home Wireless Router.

Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addressing to devices connected to the network. Home routers typically ship with DHCP already configured and quick start guide for owners to complete the network setup. Steps for the owner typically include connecting a wired PC to the new home router, opening a web browser, and then making configuration changes. Packet Tracer simulates this process.

a. Click **Home Office PC** > **Desktop** tab > **IP Configuration**.

b. Click **DHCP** to automatically receive IP addressing from the **Home Wireless Router**, which will take a few seconds. Notice that the **Default Gateway** IP address is 192.168.0.1.

c. Close the **IP Configuration** dialog box, and then click **Web Browser**.

d. Enter the default gateway IP address **192.168.0.1** in the URL field, and then click **Go**.

e. Enter **admin** for both **User Name** and **Password**, and then click **OK**. The **Home Wireless Router** graphical user interface (GUI) opens in the **Web Browser** window.

Does this present a potential security vulnerability?

Step 6: Modify the DHCP configuration on the Home Wireless Router.

a. In **Network Setup**, change **Router IP** from 192.168.0.1 to **192.168.100.1**. Leave the **Subnet Mask** as **255.255.255.0**.

b. In **DHCP Server Settings**, the DHCP Server should be **Enabled**.

c. Leave the **Start IP Address** field set to **100**, but change **Maximum number of Users** to **25**.

d. A server running the Domain Name Service (DNS) translates web addresses into an IP addresses. Enter **10.2.0.125** as the **Static DNS 1** address.

e. Scroll to the bottom of the page and click **Save Settings**. After a moment, you will lose your connection to the router.

Why do you think the home router dropped the connection to the PC?

Note: Verify that **Home Office PC** has IP addressing the conforms to the new DHCP configuration. It may be necessary to open a **Command Prompt** and enter the command **ipconfig /release** and then **ipconfig /renew** to force **Home Office PC** to send out a new DHCP request.

f. In the **Web Browser**, enter the new default gateway IP address **192.168.100.1** in the URL field.

g. Enter **admin** as the **User Name** and **Password**, and the click **OK**. This verifies that the **Home Office PC** can reconnect to the configuration interface for the **Home Wireless Router**.

h. Close the **Home Office PC** window.

Step 7: Configure the Family PC for DHCP addressing.

a. In the bedroom, click **Family PC** > **Desktop** > **IP Configuration**.

b. Click **DHCP** to automatically receive IP addressing from the **Home Wireless Router**, which will take a few seconds.

Step 8: Configure two wireless local area networks (WLANs) for family members.

In this step, you will configure the Service Set Identifier (SSID) for two WLANs. When you are in a public place and trying find an available Wi-Fi network, the SSID is the name on the list of wireless networks available to your device. The SSID is not always broadcast to all users. It can be hidden as well. If it is hidden, the user must already know the SSID and then manually enter it before the wireless client can connect to the WLAN.

a. Click **Home Office PC** > **Desktop** > **Web Browser**, and then enter **192.168.100.1** to connect to the **Home Wireless Router**. Log in with the **admin** credentials.

b. Click the **Wireless** tab. In the Basic Wireless Setting, notice there are three WLANs you can configure: one for **2.4 GHz** and two for **5 GHz**. You may need to scroll down.

c. For all three WLANs, change **Network Mode** from Disabled to **Auto**.

d. For the **2.4 GHz** and **5 GHz - 2** WLANs, configure the **Network Name (SSID)** to be **HomeNet** and select **Enabled** for **SSID Broadcast**.

e. Scroll to the bottom of the page and click **Save Settings**.

Step 9: Configure a WLAN guest network.

The guest WLAN limits access to the internal network and provides access to the internet only.

a. Under the **Wireless** menu, click the submenu **Guest Network**.

b. For **5 GHz -1**, click **Enable Guest Profile**.

c. Enter **Guest** as the **Network Name (SSID)**.

d. Verify **Broadcast SSID** is enabled.

e. For **Security mode**, click the dropdown and select **Disabled**.

f. Scroll to the bottom of the page and click **Save Settings**.

g. Close the **Home Office PC** window.

Note: The wireless router is only partially configured. In its present state, it is **dangerously insecure**. In a later activity, you will learn the important settings that must be made on a wireless network device to secure it. We do not recommend leaving a wireless router partially configured like this for even a short period of time.

For example, someone outside the home with a cell phone could connect to the home WLANs to steal bandwidth or worse. The SSIDs are broadcasted and no network security is configured. Because DHCP is supplying IP addressing, the IP address of the default gateway (the **Home Wireless Router**) can be seen in the phone IP configuration. You already know about the problem with keeping the default administrator password in effect.

Step 10: Verify connectivity.

At this point, all the devices should have connectivity to the internet and each other. Verify connectivity by opening the **Web Browser** on any device and browse to **web.isp.net**. After a brief delay, you should see the ISP website will open. Packet Tracer may take up to a minute to converge.

Part 2: Use Network Services

In Part 2, you will investigate how email, file transfer, and DNS services are simulated in Packet Tracer.

Step 1: Send and receive email messages.

a. In the bedroom, click **Family PC** > **Desktop** > **Email**.

b. Click **Configure Mail** to view the settings that are configured in the email client. Note the name and email address that are configured. This identifies the sender's account. The incoming and outgoing email servers are located in the ISP/Telco network.

c. Close the **Configure Mail** window, and then click **Compose**.

d. Send an email to your friend Tanya. Enter **tanya@mail.isp.net** in the **To** field, add a **Subject**, type a short message, and then click **Send**.

At the bottom of the Mail Browser window, notice the "Send Success" message.

e. Close the **Family PC** window, and then click **Back level** (Alt+Left) to go up one level to Greenville. Click **Cafe** to enter the location.

f. Locate and click the **Cafe Customer** laptop, and then click **Desktop** > **Email** to open the email client on Tanya's computer.

g. Click **Receive**. Packet Tracer may take up to a minute to converge. You should see the email that you just composed arrive in Tanya's inbox. Click the message to read it.

h. If you want, click **Reply** to send a message back as Tanya, and then go back to the **Home** network and read the new message.

Step 2: Upload a file to an FTP server.

File Transfer Protocol (FTP) allows you to transfer of files over a network to a remote server. The files can then be retrieved from the server by users that have the appropriate permission. In this step, you will transfer a file from the Home Office PC to the FTP server in ISP/Telco network. You will then download that file from the server to another computer.

a. Navigate to **Greenville**, and click **ISP/Telco** to enter the location.

b. In the **Rack**, locate and click the **Web/FTP** server.

c. Click the **Services** tab, and then **FTP**. Notice that two user accounts are configured: **cisco** and **mytransfer**. Also notice that the list of Files is currently empty.

d. Make note of one of the usernames and its associated password, you will use it later.

Which of the accounts is the least secure? Explain.

e. Navigate to the **Home** network, and then click the **Home Office PC** > **Desktop** > **Command Prompt**. At the prompt, type a question mark (**?**) to display the commands that are available. Press the space bar to see all the commands. Notice the **ftp** command is in the list.

f. Enter the **dir** command to show the files that are present on the PC. You will transfer the **2021_prospectus.txt** file to the FTP server.

g. Enter the **ftp ftp.isp.net** command to connect to the FTP services running on the **Web/FTP** server at **ISP/Telco**.

h. Enter the username and password that you made note of previously.

i. If you entered the correct credentials, you should see an acknowledgement that you have logged in to the server. The prompt changes to **ftp>**. Enter a question mark to see what commands are available in this mode.

Most of the commands are typical file management commands. You will use the **put** and **get** commands. The **put** command sends a file to the server. The **get** command retrieves a file from the server.

j. Enter the **put** command followed by the name of the file that you will transfer, **2021_prospectus.txt**.

k. Enter the **dir** command to verify that the file is now present on the server, and then enter the **quit** command to terminate the FTP session.

Step 3: Download a file from an FTP server.

a. Navigate to the **Cafe**.

b. Click **Cafe Customer** laptop > **Desktop** > **Command Prompt**.

c. Use the same command and credentials to connect to the FTP server.

d. Enter the **get** command followed by the name of the file, **2021_prospectus.txt**.

e. Enter the **quit** command to close the FTP client.

f. Use the **dir** command to verify that the file is now stored on the laptop C: drive.

Step 4: Investigate the Email server in the ISP/Telco network.

a. Navigate to the **ISP/Telco** network, and then click the **EMAIL** server > **Services** > **EMAIL**.

Notice that the **Domain Name** for the server is configured here. Also notice that the two email accounts you used previously are also configured.

b. Close the **EMAIL** server window.

Step 5: Investigate DNS server in the ISP/Telcom network.

a. Click the **DNS** server > **Services** > **DNS**.

Notice there are six DNS entries already configured on the server. For each entry, the domain name is mapped to the IP address of the server that is running the service. For example, the IP address of the mail server is 10.2.0.200.

b. Close the **DNS** server window.

Step 6: Challenge: Configure a new email account.

Challenge yourself to go a bit farther by trying the following suggestion. If you get stuck, use the preconfigured examples on the servers and clients to guide you.

a. Navigate to the **EMAIL** server and configure a new email account. To add the new account, click the **+** symbol after filling in the new username and password.

b. Navigate to a computer in the **Home** or **Cafe** network and configure the email client.

c. Send and reply to an email message using your new accounts.

Part 3: Use Packet Tracing to Visualize Network Communication

Packet Tracer offers **Realtime** and **Simulation** modes. The work you have done so far used **Realtime** mode. You will now use **Simulation** mode. **Simulation** mode offers a detailed window into the processes that are behind network communication. Many people are completely unaware of these processes because they are transparent to the user. Users do not see these processes in action, only the result of the processes, which is either successful or failed communication over the network.

However, it is extremely important that cybersecurity professionals have a strong understanding of network communication processes because threat actors often abuse these processes to attack networks. In addition, many network security protection measures, such as intrusion prevention systems (IPS) or firewalls control network processes to keep threat actors out of networks.

In Part 3, you will use **Simulation** mode to observe how network protocols work together to enable network communication.

Note: This activity is not intended as a complete tutorial on the use of **Simulation** mode. For an explanation of the detailed operation of **Simulation** mode, watch the video tutorials that you can access inside Packet Tracer. Click the **Help** menu, and then **Tutorials**.

Step 1: Observe ARP and ICMP in operation.

a. **Simulation** mode only works in **Logical** mode. Click **Logical** to switch to the logical view.

b. Click **Simulation** mode the lower right corner of the Packet Tracer window. The **Simulation Panel** will open.

c. The **Event List** will display all the packets transmitted in **Simulation** mode. Right now, **Simulation** mode is paused; therefore, you will not see any traffic yet. It is useful to filter for only the protocol events that you want to observe. To do this, begin by toggling **Show All/None** at the bottom of the **Simulation Panel** to None. You should see "None" is now listed under "Event List Filters - Visible Events". This clears all the protocols from the list.

d. Click **Edit Filters**. Here, you can select the protocols that you want to see simulated. In the **IPv4** tab, select **ARP** and **ICMP**, and then close the window to apply the new filter. Now under "Event List Filters - Visible Events", you should see "ARP,ICMP" listed.

e. Navigate to the **Home** network. Determine the IP address of the **Home Printer** by moving the mouse over it to view the device information popup window.

f. From the **Home Office PC**, open the **Command Prompt** and enter the **arp -d** command. This clears out any entries the Home Office PC has in its ARP table.

g. Enter the **ping 192.168.100.5** command. Network traffic is currently paused in **Simulation** mode. Therefore, nothing will happen just yet.

h. In the **Simulation Panel** > **Play Controls** section, click the **Capture Then Forward** button, which is to the right of the **Play** button. In the topology and the **Simulation Panel**, you will see **Home Office PC** get ready to send out an ARP request.

i. Click the colored tile next to the first ARP event. The **PDU Information** window opens. Here you can examine details about the select protocol data unit (PDU). In this case, you have selected the first ARP message sent by **Home Office PC**.

In the PDU Information window, click Outbound PDU Details. The source MAC address (SRC ADDR) is **000A.F325.A89D**.

What is the destination MAC address (DEST ADDR) for this PDU?

j. Click **Capture then Forward** several times and watch the PDUs as they move from device to device. Continue clicking until you see the first ICMP type event.

Which devices receive ARP PDUs?

Which device sent an ARP PDU back to the **Home Office PC**?

After learning the MAC address for the printer, the **Home Office PC** sends out an ICMP Echo Request packet. It then waits for a reply before sending out the next ICMP Echo Request packet.

k. Continue clicking **Capture then Forward** until the remainder of the ICMP Echo Request and Echo Reply messages have been sent and received.

l. In the **Simulation Panel**, click **Reset Simulation**. Repeat the **arp -d** and **ping** commands again, as necessary, to learn more about the basic communication processes occurring when one device pings another device on the local network. When you are ready to move one, be sure the click **Reset Simulation**.

Step 2: Observe HTTP in operation.

The Hypertext Transfer Protocol or HTTP is used by web browsers to request web pages from web servers.

a. In the **Simulation Panel**, click **Edit Filters**, deselect **ARP** and **ICMP**, click the **Misc** tab, and then select **HTTP**. Close the window to apply the new filter.

b. On the **Home Office PC**, open the **Web Browser**.

c. Enter the IP address of the **Home Wireless Router**, which is 192.168.100.1.

d. Click the **Capture and Forward** button several times until you are prompted to login.

e. Enter **admin** as the username and password, and then click **OK**.

f. Continue clicking **Capture then Forward** until the HTTP PDU from the **Home Office PC** reaches the **Home Wireless Router**. Although not simulated in Packet Tracer, in a real network this PDU would contain the username and password as plaintext.

The HTTP protocol has no means of encrypting the sent data. Someone on the network could use a sniffer tool, such as Wireshark, to view the contents of the packets and intercept the username and password information. For this reason, HTTP is considered an insecure protocol. Any confidential information, such as passwords, credit card numbers, or personal information should be transmitted using secure HTTP or HTTPS. HTTPS adds encryption to HTTP.

g. Click **Capture then Forward** until the HTTP PDU from **Home Wireless Router** arrives at **Home Office PC**. The router GUI should now appear in the browser window.

Answer Key

Part 1: Connect and Configure Devices

Step 1: Explore the three accessible networks in Greenville.

Step 2: Identify the devices in the Home network.

Step 3: Connect the router to the modem.

Step 4: Connect the wired hosts to the switch ports on the router.

Step 5: Configure the Home Wireless Router.

Does this present a potential security vulnerability?

Yes! The documentation for home wireless routers is easy to find on the internet. Anyone can attempt to connect to the router using the default login. If they are successful, they can make unauthorized changes to the network and possibly steal data or damage computers.

Step 6: Modify the DHCP configuration on the Home Wireless Router.

Why do you think the home router dropped the connection to the PC?

The network address of the router was changed. The PC and the router are no longer on the same IP network so the connection is dropped.

Step 7: Configure the Family PC for DHCP addressing.

Step 8: Configure two wireless local area networks (WLANs) for family members.

Step 9: Configure a WLAN guest network.

Step 10: Verify connectivity.

Part 2: Use Network Services

Step 1: Send and receive email messages.

Step 2: Upload a file to an FTP server.

Which of the accounts is the least secure? Explain.

The cisco/cisco account is very insecure because the password and the username are the same and the password is very simple.

Step 3: Download a file from an FTP server.

Step 4: Investigate the Email server in the ISP/Telco network.

Step 5: Investigate DNS server in the ISP/Telcom network.

Step 6: Challenge: Configure a new email account.

Part 3: Use Packet Tracing to Visualize Network Communication

Step 1: Observe ARP and ICMP in operation.

What is the destination MAC address (DEST ADDR) for this PDU?

The destination is shown as broadcast or FF.FF.FF.FF.FF.FF.

Which devices receive ARP PDUs?

All the connected devices should receive one ARP PDU because it was a broadcast message.

Which device sent an ARP PDU back to the **Home Office PC**?

The Home Printer.

Step 2: Observe HTTP in operation.