

FINAL PROJECT SCREENSHOTS:

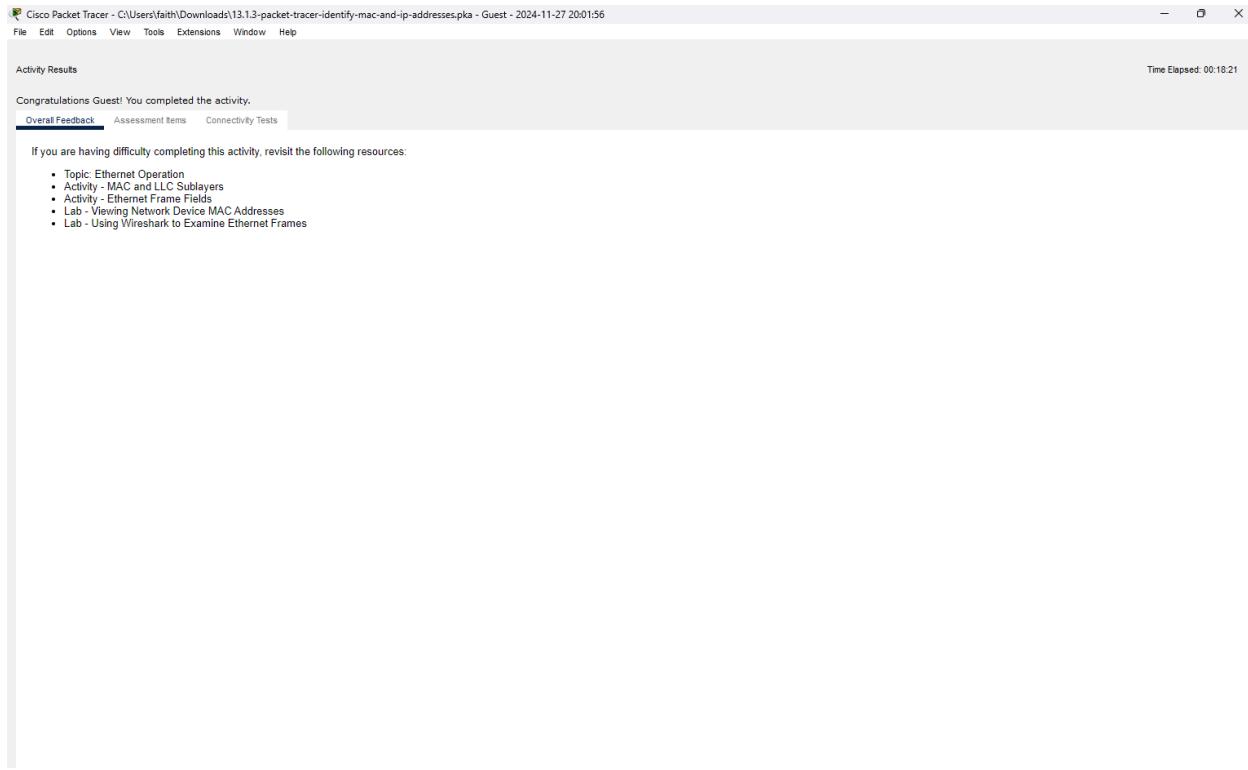
Faith Kuuipo Muller

CS 300-01-1

Dr. Joseph Del Rosario

December 3rd, 2024

Networking Basics



PT Activity: 00:18:05

outbound PDU details.

What type of PDU is this?

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.

- For the cable that connects the Accounting switch with Finance switch, click the green triangle on the Accounting switch side of the link.
- Drag that end of the cable to the Edge router and connect the cable to port GigabitEthernet 1/0.
- 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.)

- 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.
- 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?
What IPv4 network is assigned to the Sales network?

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.

- Return to the Command Prompt for Sales 2 and verify that its ARP cache is empty. If it is not, delete any entries.
- Switch to Simulation mode.
- Ping Sales 1 from Sales 2.
- 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.

Which devices receive the ARP broadcasts this time?

Step 2: Ping other hosts.

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

What is the benefit of using multiple IPv4 networks, or subnetworks, within an enterprise?

Note: The network topology that is used in the activity is for demonstration purposes only. While it is possible that a real enterprise network could use a router in this way, there are more optimal topologies that achieve these results. You will learn about other design approaches in later networking courses.

Time Elapsed: 00:18:05 Completion: 83%

Top Dock Check Results Back 1/1 Next

Realtime Simulation

Time: 00:16:17

4321 4321 1941 2901 2911 81910X 81910W 829 1240 1240 1841 2620

2620XM

7011

PT Activity: 01:56:39

Uptime Router	GU0	ISW1	GU0
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

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

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

- 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.
- 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.
 - Click the printer and open the Config tab.
 - Click the FastEthernet0 interface in the left-hand pane.
 - Enter the addressing information from the Addressing Table.
- Because the two computers are on the same network, their IPv4 addresses will be similar, their subnet masks and default gateways will be identical.

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

Part 3: Verify the End Device Configuration and Connectivity

Step 1: Verify connectivity between the two PCs.

- 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.
- 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.

Time Elapsed: 01:56:39 Completion: 100%

Top Dock Check Results Back Next

Logical Physical x 1, y: 371 Root 19:59:30

Realtime Simulation

Copper Straight-Through

Cisco Packet Tracer - C:\Users\faith\Downloads\16.1.5-packet-tracer---the-client-interaction.pka - Guest - 2024-12-02 04:38:59

File Edit Options View Tools Extensions Window Help

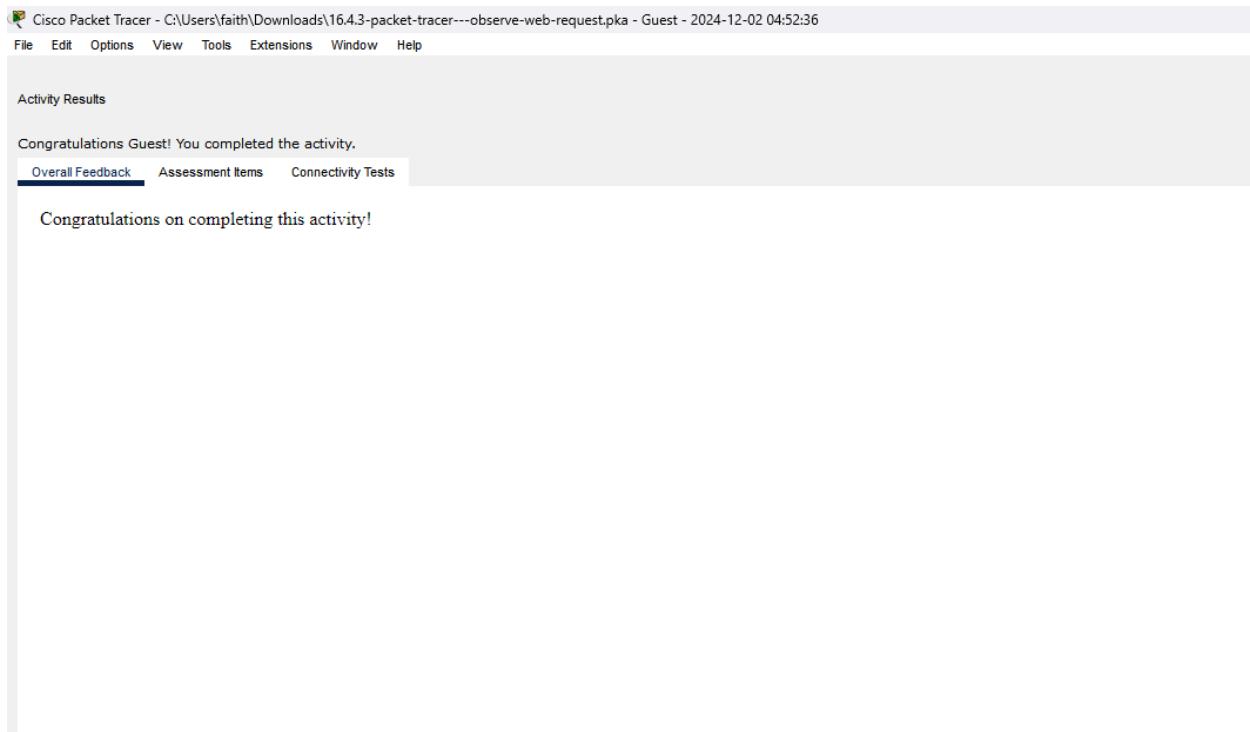
Activity Results

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All Show Incorrect Items

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



Cisco Packet Tracer - C:\Users\faith\Downloads\16.5.3-packet-tracer---use-ftp-services (1).pka - Guest - 2024-1...

File Edit Options View Tools Extensions Window Help

Logical Physical x: 496, y: 244 Root 08:26:00

PC Home Wireless Router FTP Server

PT Activity: 00:06:26

Enter your command below to send it 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>
```

d. 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.

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

Step 2: Download the file from the FTP server.

- 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>
```

- Enter quit to exit the FTP client when finished.
- 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.

- Log into the FTP server again to delete the file sampleFile_FTP.txt.
- 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?

- Enter quit to exit the FTP client when finished.

Time: 00:06:20 Time Elapsed: 00:06:26

Completion: 100% Back Top Dock Check Results Next

4331 4321 1941 2901 2911 81910X 81910W 829 1240 Ptxbutor Ptxbutor 1841 2621

2901



PT Activity: 00:04:57

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

- Access the Command Prompt on each PC and enter the command ipconfig /all at the prompt.
- 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

- Select the PC that is incorrectly configured.
- Click the Desktop tab > IP Configuration tab to correct the misconfiguration.

Time Elapsed: 00:04:57

Completion: 100%

Realtime Simulation

(Select a Device to Drag and Drop to the Workspace)

File Edit Options View Tools Extensions Window Help

Activity Results

Congratulations Guest! You completed the activity.

[Overall Feedback](#) [Assessment Items](#) [Connectivity Tests](#)

Congratulations on completing this activity!



Networking Basics

Course Outline

Resources

Search course outline

Module 11: Dynamic Addressing with DHCP

100%

Checkpoint Exam: The Internet Protocol

100%

Module 12: Gateways to Other Networks

100%

Module 13: The ARP Process

100%

Module 14: Routing Between Networks

100%

Checkpoint Exam: Communication Between Networks

100%

Module 15: TCP and UDP

100%

Cisco Networking Academy

Networking Basics

Course Outline Resources

Search course outline

Checkpoint Exam: Communication Between Networks 100%

Module 15: TCP and UDP 100%

Module 16: Application Layer Services 100%

Module 17: Network Testing Utilities 100%

Checkpoint Exam: Protocols for Specific Tasks 100%

Networking Basics Course Final Exam 100%

This screenshot shows the Cisco Networking Academy course progress page for the 'Networking Basics' course. The page includes a header with the Cisco Networking Academy logo and a navigation bar with back, forward, and search functions. Below the header, the course title 'Networking Basics' is displayed next to the Cisco Networking Academy logo. Two tabs are present: 'Course Outline' and 'Resources', with 'Course Outline' being the active tab. A search bar for the course outline is also visible. The main content area lists several course components with their completion status: 'Checkpoint Exam: Communication Between Networks' (100%), 'Module 15: TCP and UDP' (100%), 'Module 16: Application Layer Services' (100%), 'Module 17: Network Testing Utilities' (100%, highlighted with a blue border), 'Checkpoint Exam: Protocols for Specific Tasks' (100%), and 'Networking Basics Course Final Exam' (100%). Each item has a green progress bar and a downward arrow icon.

Exploring Internet of Things with Cisco Packet Tracer

Cisco Packet Tracer - C:\Users\faith\Downloads\10.2.3-packet-tracer---examine-nat-on-a-wireless-router.pka - Guest - 2024-11-21 22:23:51

File Edit Options View Tools Extensions Window Help

Logical Physical x: 4, y: 584

Root 00:18:30

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.

- 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**.
- 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.
- Note the IP address of the default gateway. Close the IP Configuration when done.
- 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.
- Click **Status** menu option in the upper right-hand corner. When selected, it displays the Router sub-menu page.
- 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.

The address seen here is the address assigned to the Internet port on the wireless router.
Is this a private or public address?

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

- Click **Local Network** within the Status sub-menu bar.
- Scroll down to examine the Local Network information. This is the address assigned to the Internal network.
- 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?

Time Elapsed: 00:13:25 Completion: 100%

Dock Check Results Back 1/1 Next

Realtime Simulation

Time 00:01:04

4331 4322 1941 2903 2911 81910X 81910W 829 1240 PTEmpy 1841 263

1941

Scenario 0 New Delete Toggle PDU List Window

Cisco Packet Tracer - C:\Users\faith\Downloads\1.1.3-packet-tracer-add-iot-devices-in-pt.pka - Guest - 2024-12-02 23:37:00

File Edit Options View Tools Extensions Window Help

Logical Physical x: 388, y: 584

Root 10:30:00

Step 3: Verify that the Lawn Sprinkler is on the network.

- Click the **Tablet**.
- If necessary, log back into the **Home Gateway**.
- The device **Smart Sprinkler** now appears at the bottom of the list of IoT Server - Devices. Note: It may take a few seconds for Smart Sprinkler to be listed.

Step 4: Add a Water Level Monitor.

- In the Device-Specific Selection box, click the **Water Level Monitor** (End Devices > Home > Water Level Monitor), and then click in the workspace where you would like to place it.
- Click the **Water Level Monitor**, and then click **Advanced** to display more tabs.
- Click the **Config** tab and change the **Display Name** to **Water Meter**.
- Set the **IoT Server** to **Home Gateway**.
- Click **Wireless0** and verify the **Water Meter** is using **HomeGateway** as the SSID.
- Configure the wireless network pass phrase.
- Verify it is configured to receive an IP address from the DHCP server on **Home Gateway**.
- Click the **I/O Config** tab, and then change the number of **Digital Slots** to 1.
- For the **Usage** setting, change it to **Component**.
- Connect the **Water Meter** to the **Smart Sprinkler**.

Click Connections in the Device-Type Selection box, and then click the **IoT Custom Cable** in the Device-Specific Selection box. Click the **Smart Sprinkler** and connect one end of the cable to the D0 interface. Click the **Water Meter** and connect the cable to the D0 interface.

Step 5: Verify that the Water Meter is on the network.

- Click the **Smartphone**, and then **Desktop** tab > **Web Browser**.
- Log into the **Home Gateway**.
- The device **Water Meter** now appears at the bottom of the list of IoT Server - Devices.

Step 6: Add other IoT devices.

Experiment by adding other types of IoT devices to the smart home wireless network.

Time Elapsed: 00:39:45 Completion: 100%

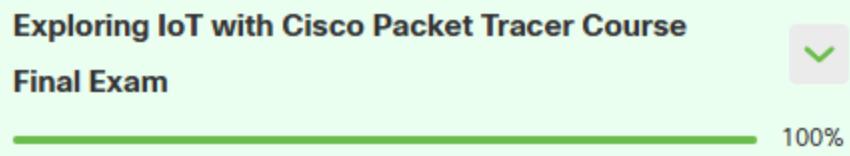
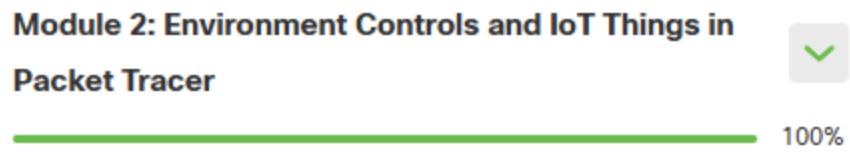
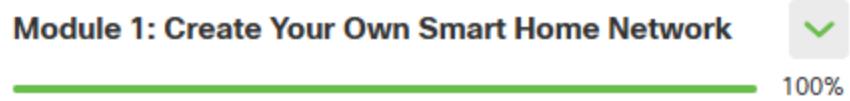
Dock Check Results Back 1/1 Next

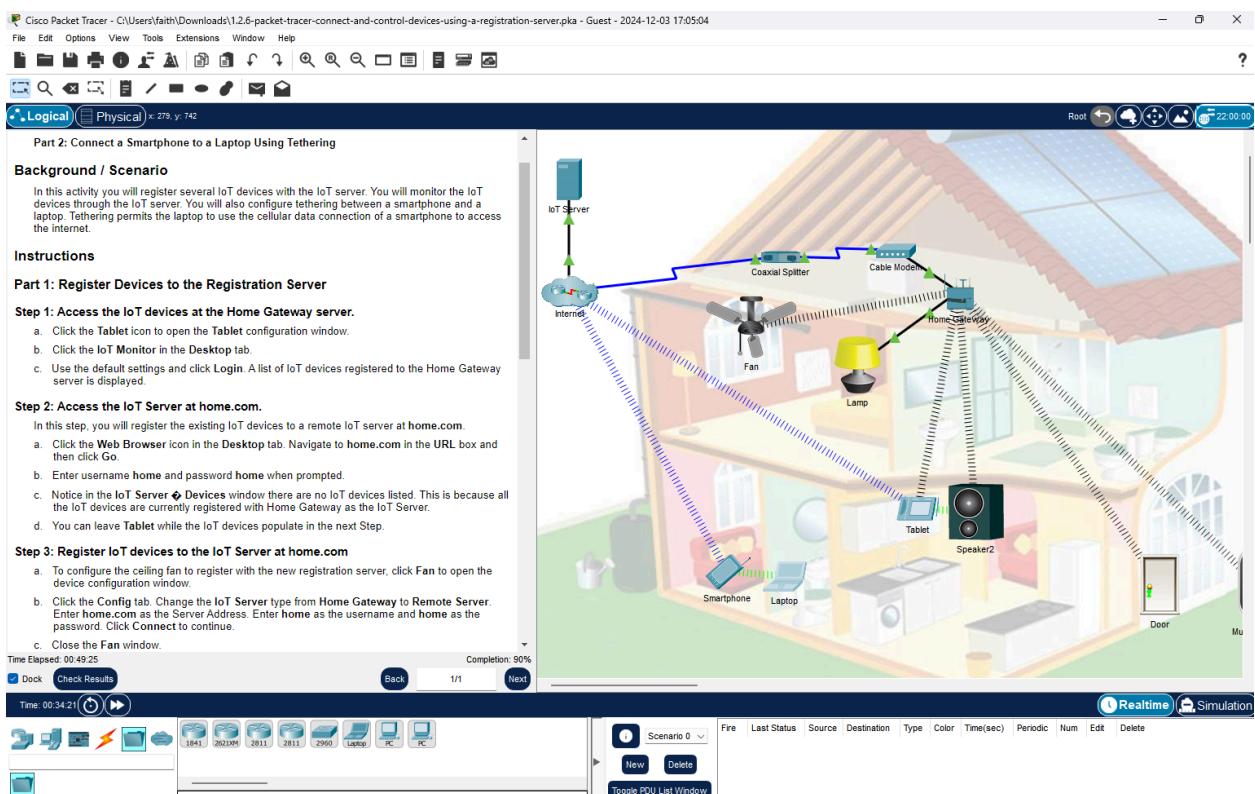
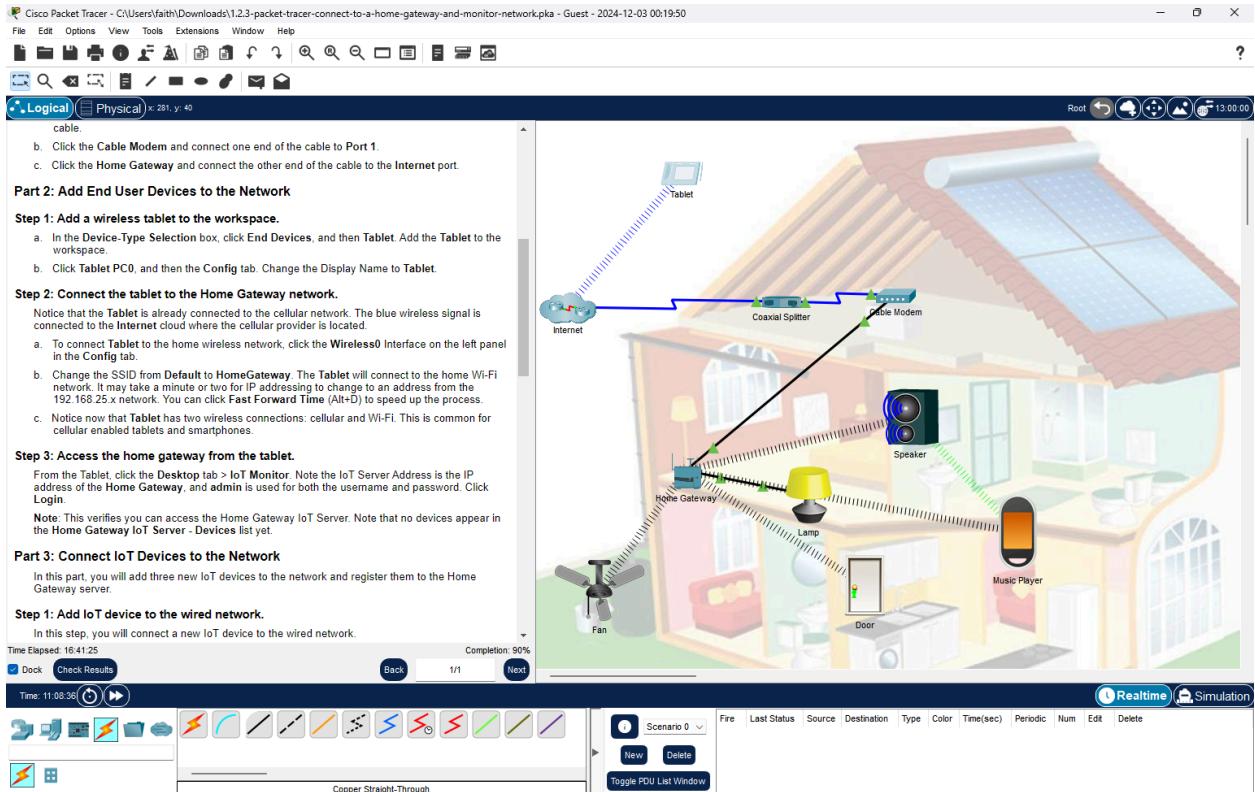
Realtime Simulation

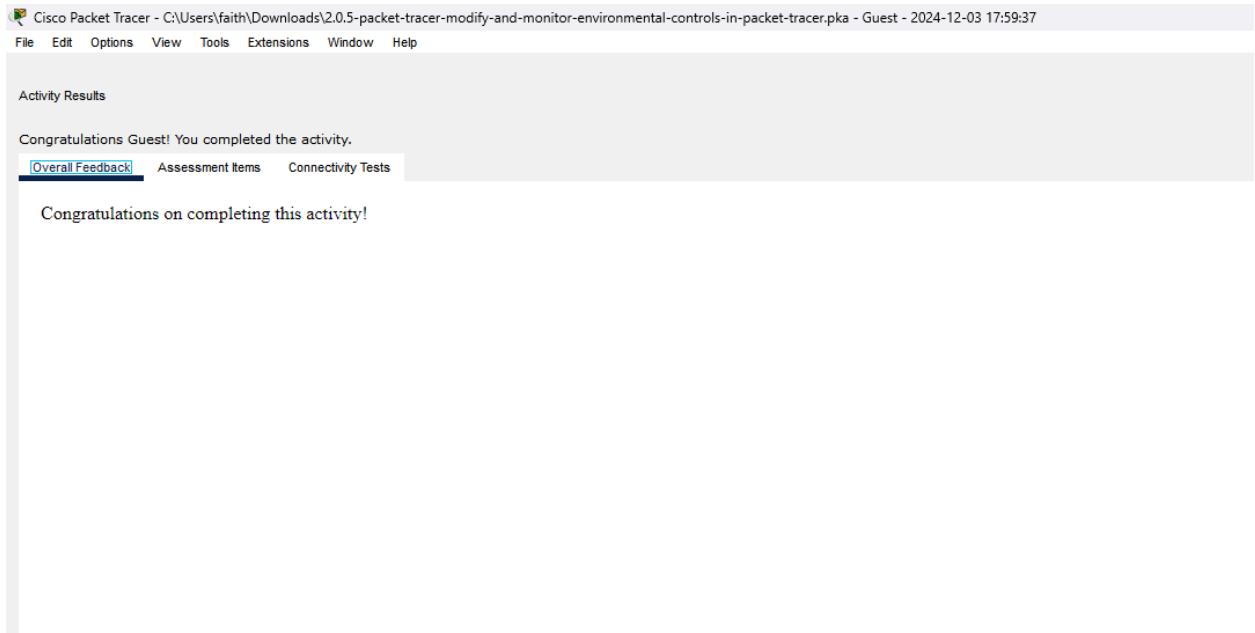
Time 00:29:30

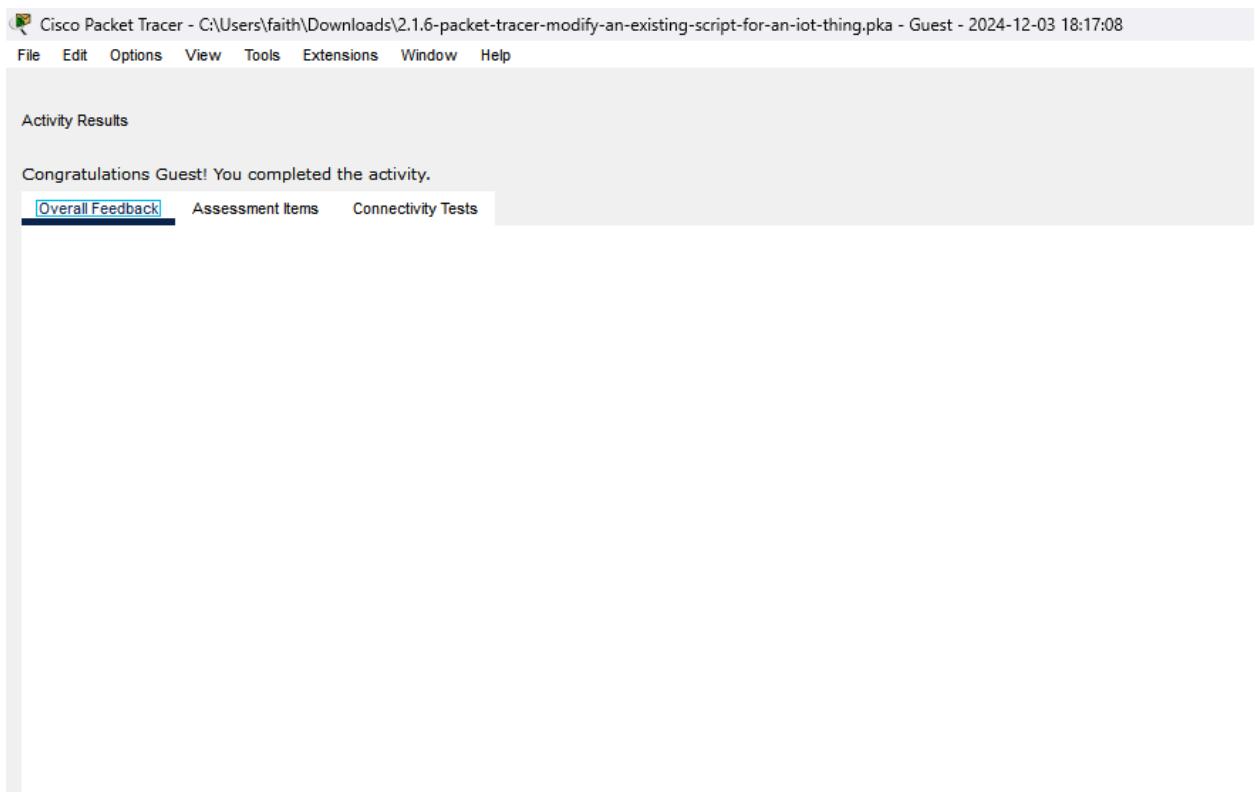
IoT Custom Cable

Scenario 0 New Delete Toggle PDU List Window









Introduction to IoT and Digital Transformation

Screenshot of a web browser showing the Cisco Networking Academy course outline for "Introduction to IoT and Digital Transformation". The current section is "5.1.1 Types of Data".

Course Outline:

- Module 1: Everything is Connected
- Module 2: Everything Becomes Programmable
- Module 3: Everything Generates Data
- Module 4: Everything Can be Automated
- Module 5: Everything Needs to be Secured** (highlighted)
- Module 6: Educational and Business Opportunities
- Introduction to the Internet of Things and Digital Transformation Final Exam

5.1.1 Types of Data:

Expand each heading below to see examples of PII and Informational data.

PII:

- Rain gauge value
- Number of cars through an intersection
- Hospital emergency use per state
- Average plane capacity
- House thermometer reading
- Census data
- Immigration values
- Average potato crops per province
- Next train time per station
- Average gas consumption per flight

Screenshot of Cisco Packet Tracer showing a network diagram and configuration steps.

Network Diagram:

```
graph LR; PC --- WR[Wireless Router]; WR --- CM[Cable Modem]; CM --- Internet; CM --- cisco_srv[cisco.srv]
```

Configuration Steps:

Step 1: Configure the Wireless Router.

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

b. 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 was sufficient for most of the time you have been using the Internet. 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.

c. 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.

- Power off Laptop by clicking the power button on the side of the laptop.
- 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.
- 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.
- 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.

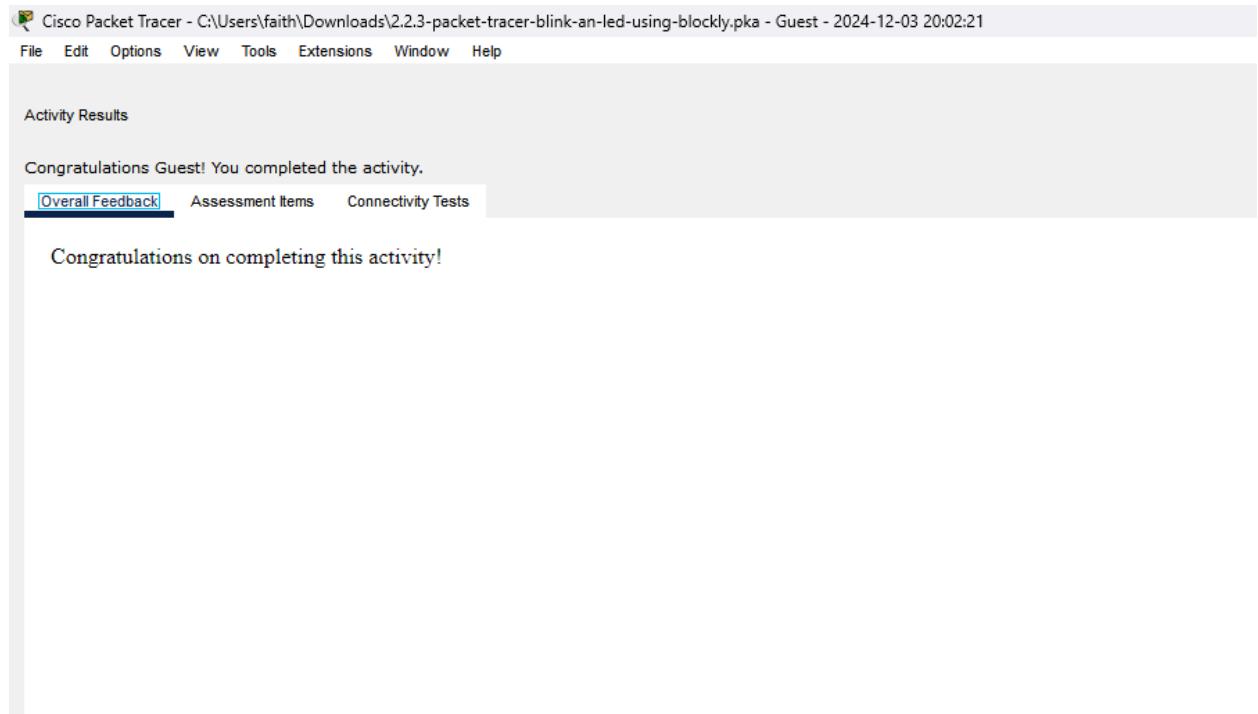
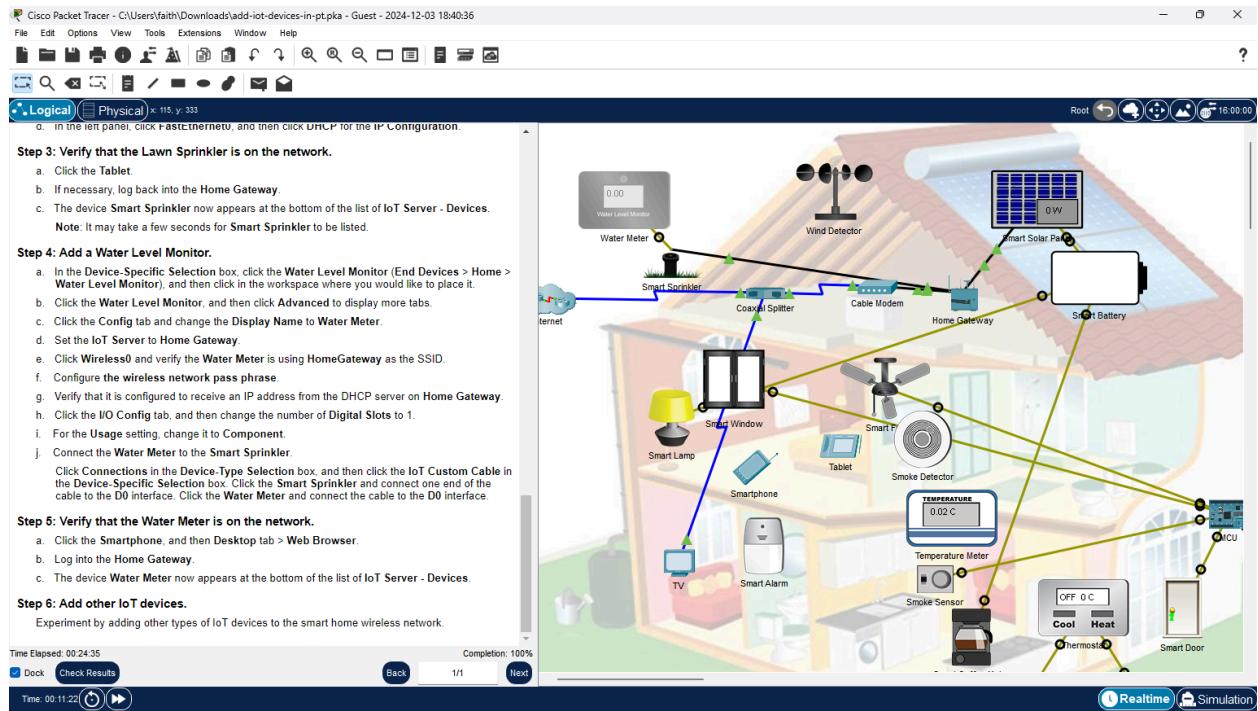
d. Select the Connect tab. After a slight delay, the wireless network HomeNetwork will be visible in the list of wireless networks. Click Refresh if necessary to see the list of available networks. Select the HomeNetwork. Click Connect.

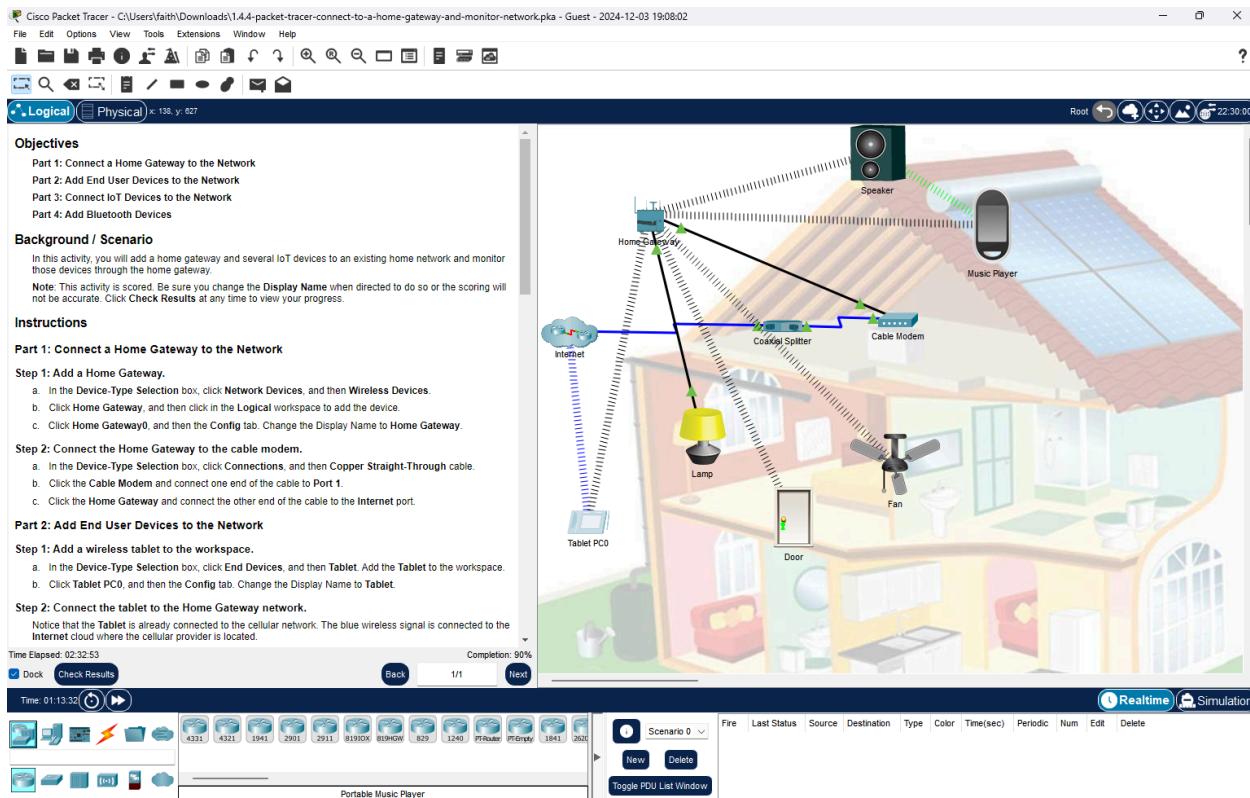
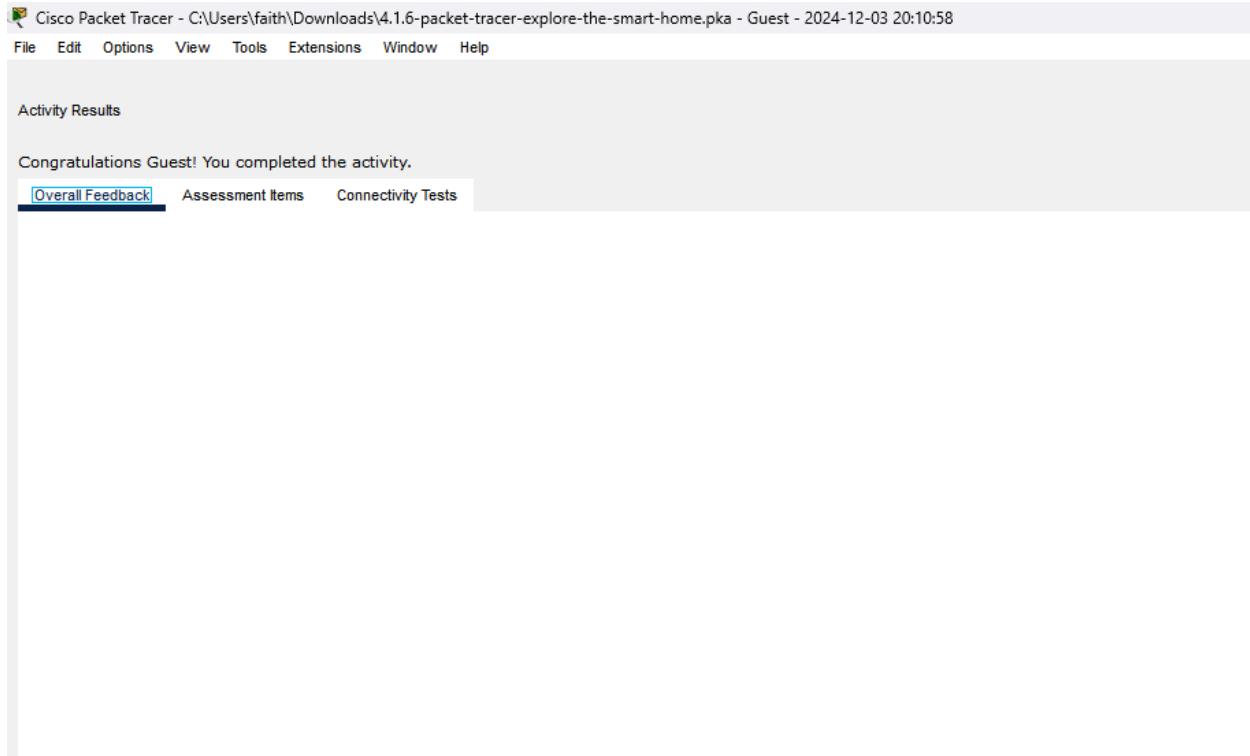
e. Close PC Wireless. Select Web Browser in the Desktop tab.

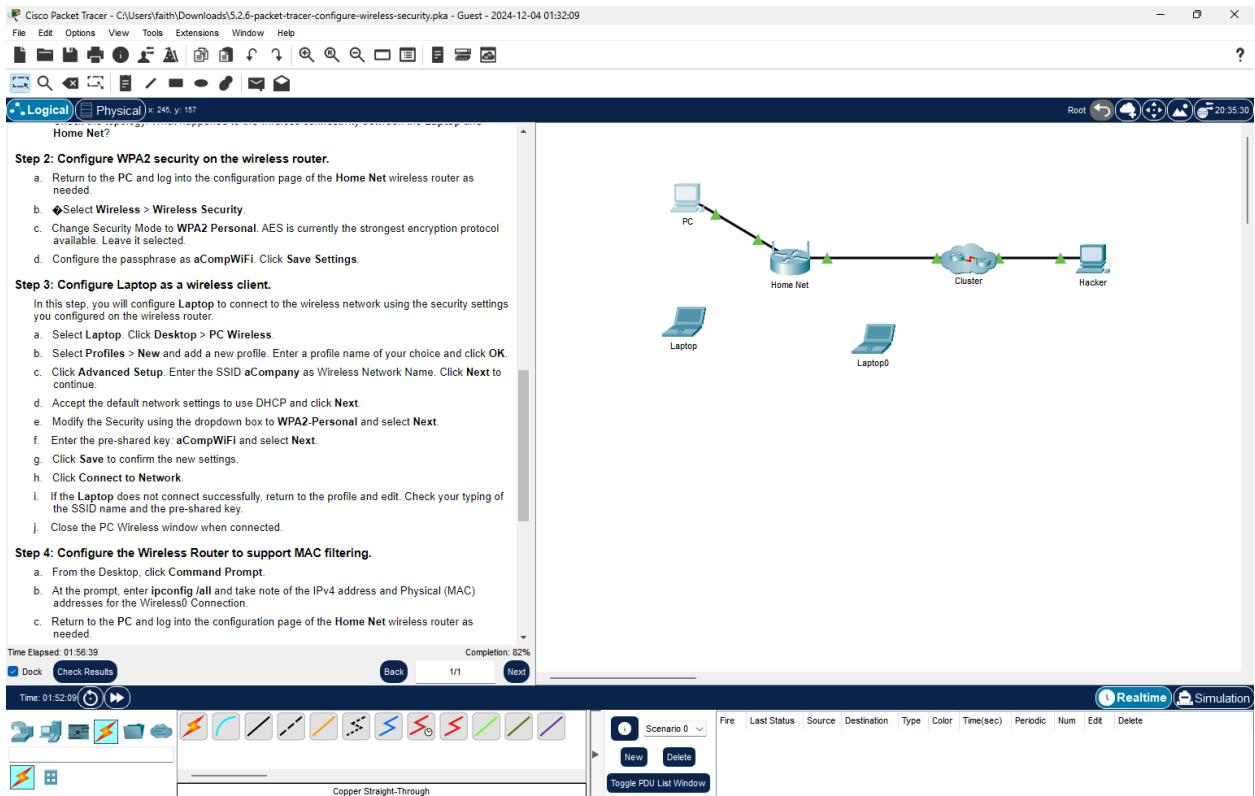
f. In the Web Browser, navigate to cisco.srv.

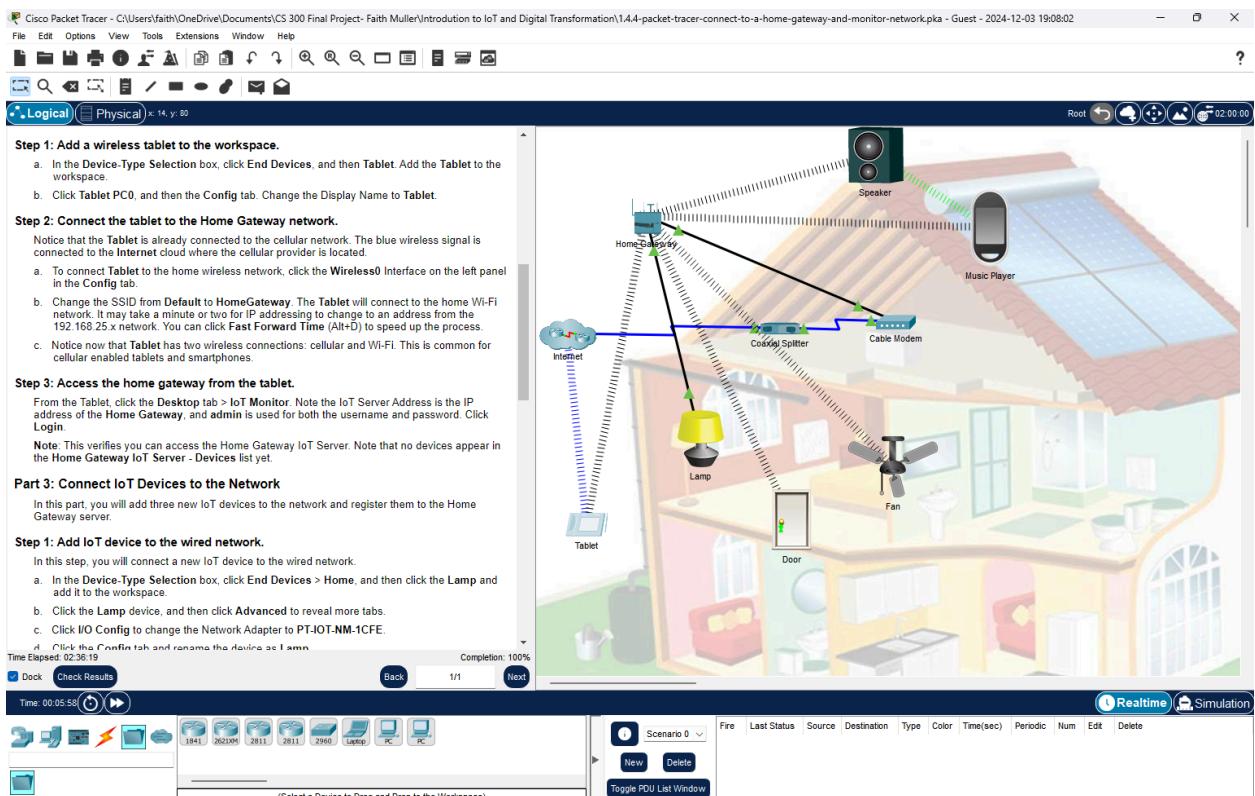
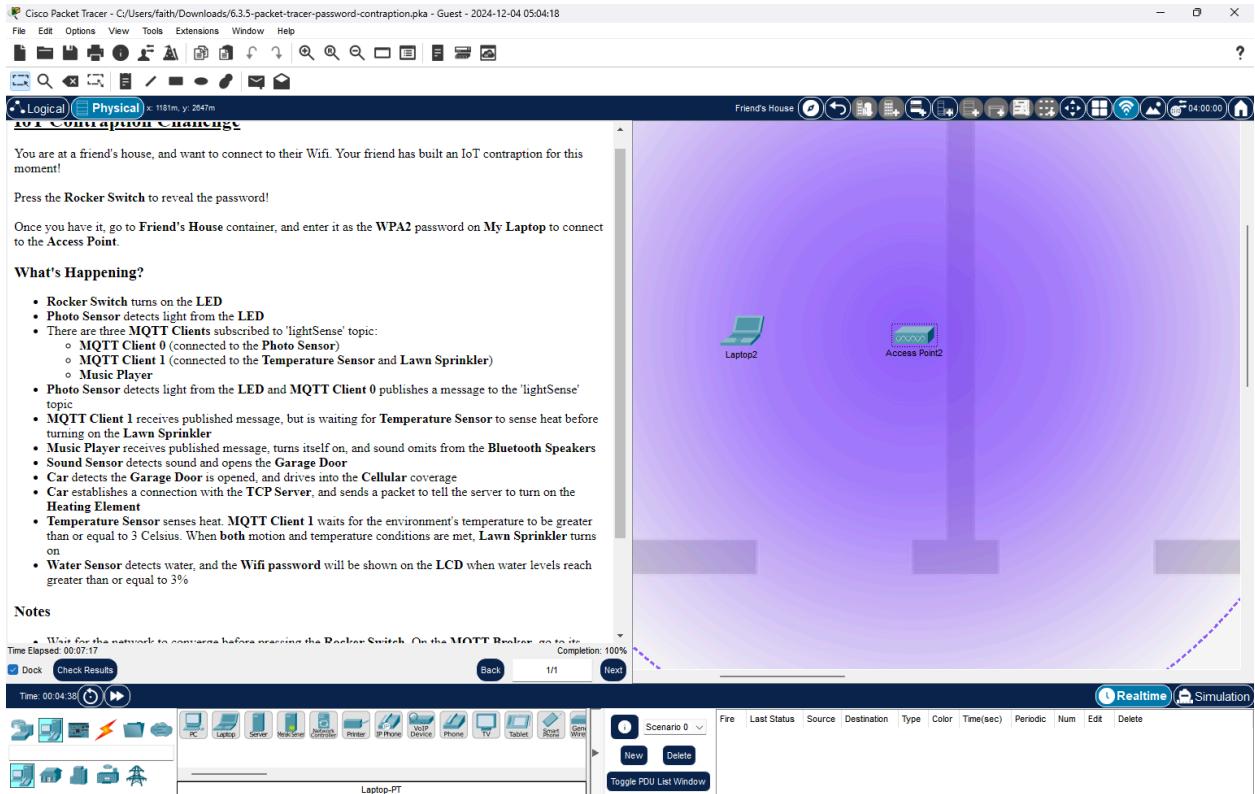
Bottom Panel:

Time Elapsed: 00:09:50 Dock Check Results Back 1/1 Next Time: 00:09:37 Realtime Simulation Scenario 0 New Delete Toggle PDU List Window









Final proof:

 MODULE Threat Analysis Issued On: Nov 17, 2024	 MODULE Cybersecurity Administration Issued On: Nov 17, 2024	 MODULE Exploring Networking with Cisc... Issued On: Nov 03, 2024	 MODULE Network Access Basics Issued On: Oct 13, 2024
 MODULE Network Basics Issued On: Oct 13, 2024	 MODULE Getting Started with Cisco Pack... Issued On: Sep 20, 2024		

 MODULE Automating Things Issued On: Dec 03, 2024	 MODULE Programming Things Issued On: Dec 03, 2024	 MODULE Digital Transformation Issued On: Dec 03, 2024	 MODULE Exploring IoT with Cisco Packet... Issued On: Dec 03, 2024
 COURSE Networking Basics Issued On: Dec 02, 2024	 MODULE Networking Protocols Basics Issued On: Dec 02, 2024	 MODULE Network Communications Basics Issued On: Dec 02, 2024	 MODULE Internet Protocol Basics Issued On: Nov 21, 2024
 COURSE Introduction to Cybersecurity Issued On: Nov 17, 2024	 MODULE Resource Specialist Issued On: Nov 17, 2024	 MODULE Network Defense Issued On: Nov 17, 2024	 MODULE System Safeguards Issued On: Nov 17, 2024

[Profile](#)[Badges & Certificates](#)[Discounts](#)[Learning History](#)Search by name, course. 

Offering All Offerings

Type All

Sort Latest

