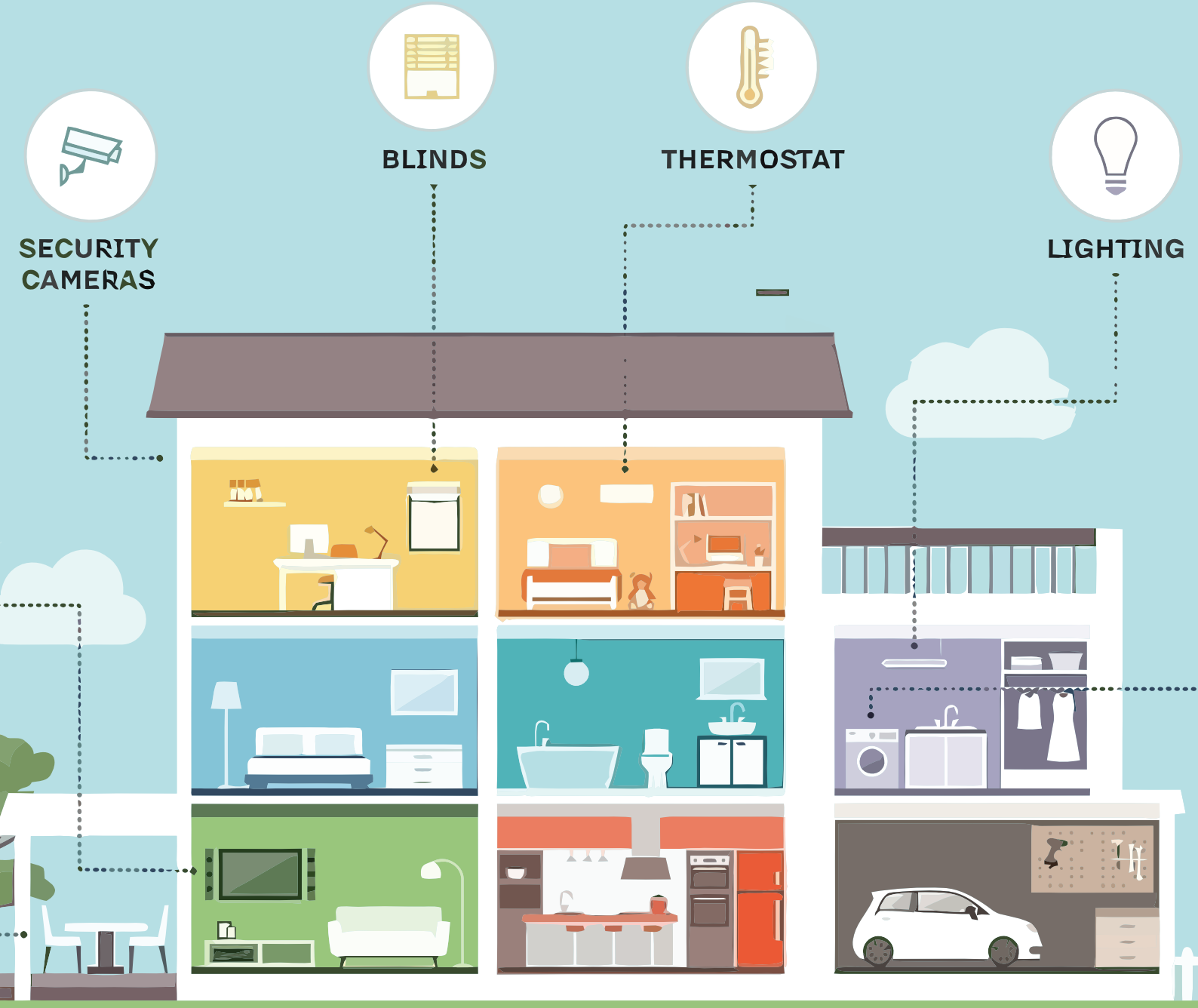
Charith Perera (Eds.)
PhD, MBA

Internet of Things

Systems Design

Advanced Lab Book

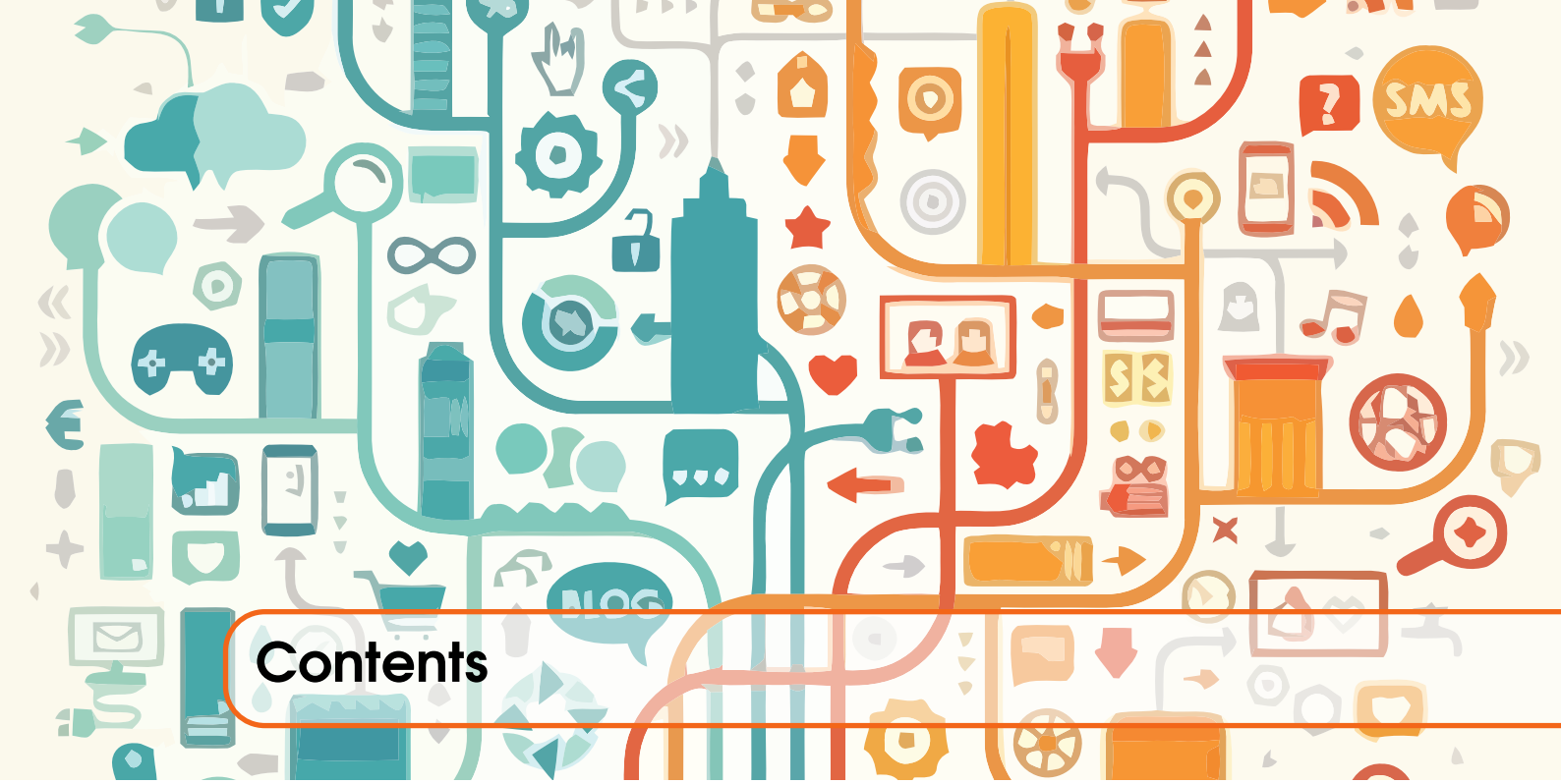


PUBLISHED BY IOT GARAGE

How to cite this book
Charith Perera (Eds.), Internet of Things: Systems Design Advanced Lab Book, IOT Garage, 2025

Contributing Authors (alphabetical order)
Hakan Kayan, Yasar Majib

Version 1.0, (Latest) January 2025



Contents

Preface

This IOT ADVANCED LAB BOOK is primarily compiled to support the university courses on *'Internet of Things: Systems Design'* at both under graduate and postgraduate levels. It is also designed to complement the IOT LAB BOOK. The IOT LAB BOOK primarily focuses on end-to-end IoT systems development, combining microcontrollers, single-board computers and IoT cloud platforms. This ADVANCED LAB BOOK aims at complex IoT network design, and simulations.

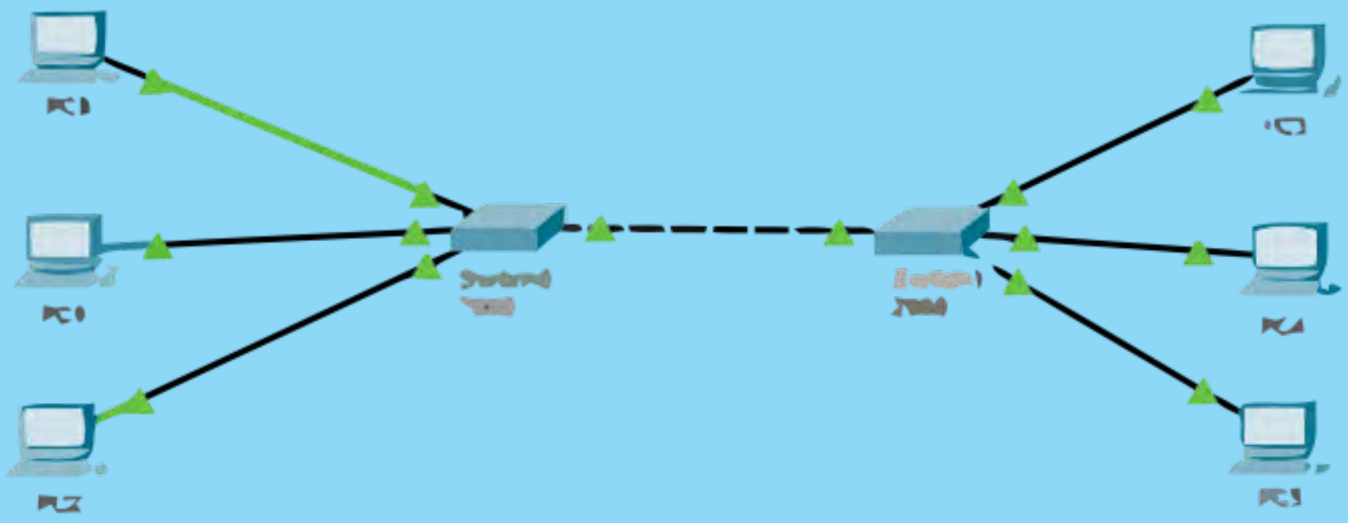
CISCO Packet Tracer is a powerful network simulation tool developed by Cisco Systems, designed to help students and professionals visualize, build, and troubleshoot network systems without the need for physical hardware. As an educational tool, it is invaluable for understanding complex concepts and scenarios in networking and the Internet of Things (IoT).

With Packet Tracer, users can simulate the configuration of Cisco routers and switches using a command-line interface similar to that used in real life. This functionality extends to IoT simulations, allowing learners to integrate and manage IoT devices within various network configurations. Users can create virtual representations of networks including IoT devices like sensors, actuaries, and connected appliances, making it possible to observe and control their interactions in real-time simulated environments.

The tool's intuitive drag-and-drop interface makes it accessible for beginners, yet it is robust enough to offer detailed, advanced simulations for more experienced users. Cisco Packet Tracer primarily supports a simplified form of JavaScript for creating interactive activities and simulations, especially in the context of the Internet of Things (IoT). This allows users to script behaviors and automate responses within the simulated network environment, which is particularly useful for modeling complex network scenarios and IoT integrations. Additionally, while not a programming language per se, Packet Tracer allows users to configure devices using Cisco's IOS commands through its command-line interface (CLI). This CLI-based interaction mimics the actual configuration and troubleshooting commands used on real Cisco devices, providing a realistic experience for learning network setup, management, and security.

— Further information, links and references. We will use this structure throughout this lab book to provide you with additional information and references. They are marked in orange colour bar on the left-hand side. If you are not interested in exploring further, you are more than welcome to skip these small sections. Throughout the lab book, we provided explanations, external links, and references to reading material. Especially if you do not understand certain programming tasks it may be worth reading those links. Further, these links will guide you to explore the universe of IoT on your own, beyond the labs we have provided here. Finally, we want to emphasise that this is not a programming course. It is up to you to fill the gaps in your knowledge by referring to the links we provided.

Video **— Resources (Optional)** . To enhance your learning experience, we sometimes provide additional links to online resources, such as video tutorials. Please note that some of these resources may become outdated over time. We will try our best to replace them with updated content when appropriate replacements are available. Consequently, some features demonstrated in these video resources may not be available in the current version of the software you are using, due to software updates. In such circumstances, we recommend using your common sense to explore whether you can replicate and find the same functionalities in your current software version. If you are unable to replicate them, we suggest using a search engine or other AI tools available to further explore. Unless there is a specific reason to remove them, we will keep these video tutorials intact over time to capture and demonstrate the historical evolution of the software tool in terms of user interfaces and capabilities.



1. Deploying and Cabling Devices

Objective

- Gain an understanding of Cisco Packet Tracer's capabilities and installation process to deploy network simulations effectively.
- Develop the ability to confidently navigate and utilize Packet Tracer's interface to add, connect, and manage network devices.
- Acquire hands-on experience in deploying various network devices and connecting them using appropriate cabling within the simulation environment.
- Learn to simulate the physical aspects of network deployments by selecting, organizing, and physically connecting devices using different types of cables.

Lab Plan

In this lab, you will learn how to configure and simulate the deployment and connection of various network devices using Cisco Packet Tracer. You will practice adding routers, switches, and end devices to a network topology and connect them using appropriate cabling techniques.

Overview of Packet Tracer

Packet Tracer is an exciting network design, simulation and modelling tool that allows you to develop your skill set in networking, cybersecurity, and the Internet of Things (IoT). It allows you to model complex systems without the need for dedicated equipment. Cisco Packet Tracer is an innovative network simulation and visualization tool. This free software helps you to practice your network configuration and troubleshooting skills via your desktop computer or an Android or iOS based mobile device. Packet Tracer is available for both the Linux and Windows desktop environments.

With Packet Tracer you can choose to build a network from scratch, or use a pre-built sample network. Packet Tracer allows you to easily explore how data traverses your network. Packet Tracer provides an easy way to design and build networks of varying sizes without expensive lab equipment.

Video — Overview of Packet Tracer | . For additional help and practice using Packet Tracer, please visit the Tutorials located under Help in the Packet Tracer program. To view some examples of how Packet Tracer can be used, select File, then Open Samples from the main menu.

The User Interface

Packet Tracer is a versatile tool designed for simulating real networks. It offers capabilities to enhance your network management experience. First, the **Device Configuration** allows you to add devices and establish connections using cables or wireless methods. Within this, you can also perform actions such as selecting, deleting, inspecting, labeling, and grouping network components. Second, the **Network Management** empowers you to open existing or sample networks, save your current network configuration, and modify user preferences. In summary, Packet Tracer provides an essential environment for network professionals, facilitating network design, testing, and troubleshooting.

Video — The Packet Tracer User Interface | . Watch this video to learn how to use the menus and the user interface of the Packet Tracer network. This video go through a couple different menus within Packet Tracer, including toolbars and building your first network.

Step 1: Open the Deploying and Cabling Devices Packet Tracer file

- Double click on the `Deploying and Cabling Devices.pkt` file to open it. You should be presented with a screen similar to that shown in the illustration in Figure 1.1. If the file does not open, make sure you have properly installed the Packet Tracer application program.

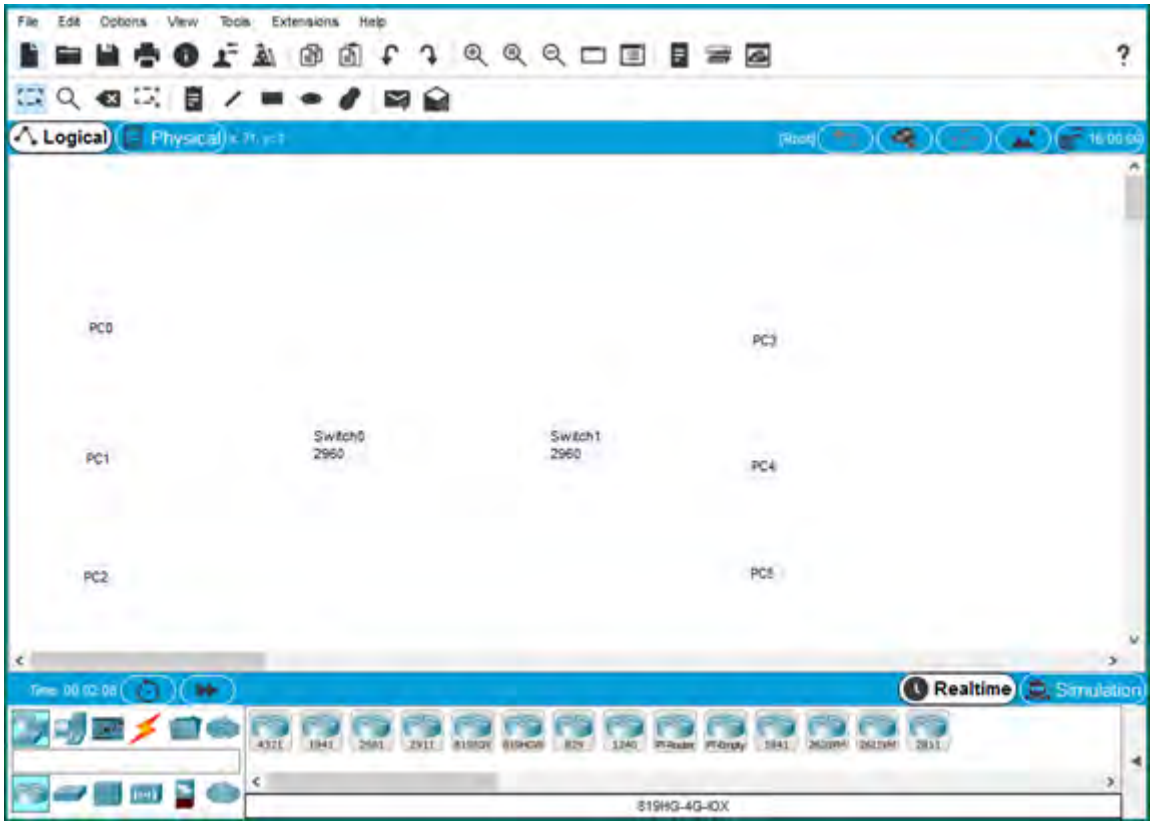


Figure 1.1: Packet Tracer user interface when file open

Step 2: Learn how to Deploy Devices and Cable them in Packet Tracer

1. The first task in this activity is to practice using the Device-Type Selection box as shown in Figure 1.2.

Figure 1.2: Device-Type Selection Box

2. The top row of icons represents categories of devices and the bottom row represents subcategories. Point at the top row of icons slowly and look at the Label box between the rows; the names of the categories will appear. Now point at the lower row icons and you will see their names appear.

3. In this activity we will deploy `switches` and `PCs`. Point at the lower row icons until you see one labeled Switches. Click on that icon and you will see the devices in the Device-Specific Selection box change as shown in Figure 1.3.

Figure 1.3: Device-Specific Selection Box

   A click on the Switches icon shows the `switches` available in Packet Tracer. Please deploy two 2960 switches over the `Switch0` and `Switch1` labels in the workspace.

4. Now click on the End Devices category in the Device-Type Selection box, and deploy six `PCs`. If you are unsure of which device is the `PC`, just point at the device in the Device-Specific Selection box and look at the label area below the devices; it should say `PC-PT`. (Remember that you do not have to select the PC icon six times to deploy them. There is a shortcut). Your workspace should now look like the Figure 1.4:

5. We are now going to connect the `PCs` to the `switches`.

6. Click on the category that looks like a lightning bolt labeled Connections. In the Device-Specific Selection box, there will appear a series of cable types. Select the Copper Straight-Through cable type. Now point at the center of `PC0` and click on it. You will see a pop-up menu appear showing the cable connection types. Point at, and click on the `FastEthernet0` selection. Now a wire will appear anchored to the PC.

7. Point at `Switch0`, and click on it. Another pop-up menu will appear with a much larger set of selections. Point at and click on the `FastEthernet0/1` selection. The cable will now be connected and two blinking link lights will appear, one green and one amber. After a while the amber light will turn green for reasons you will understand as you learn about

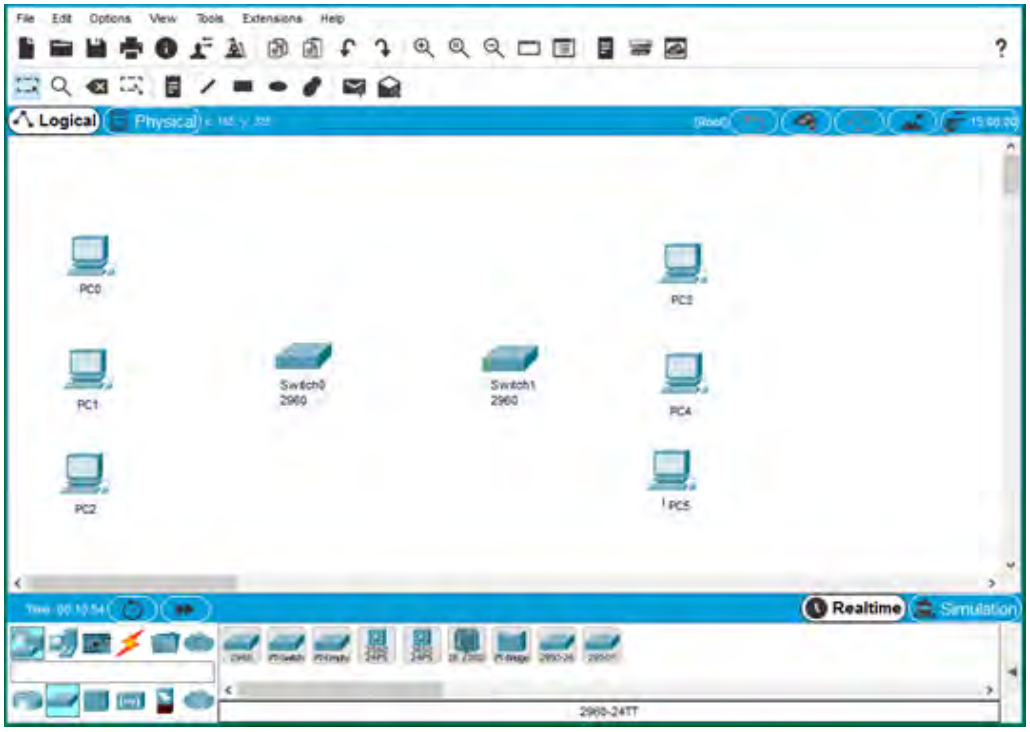


Figure 1.4: Workspace with Switches and PCs

networking.

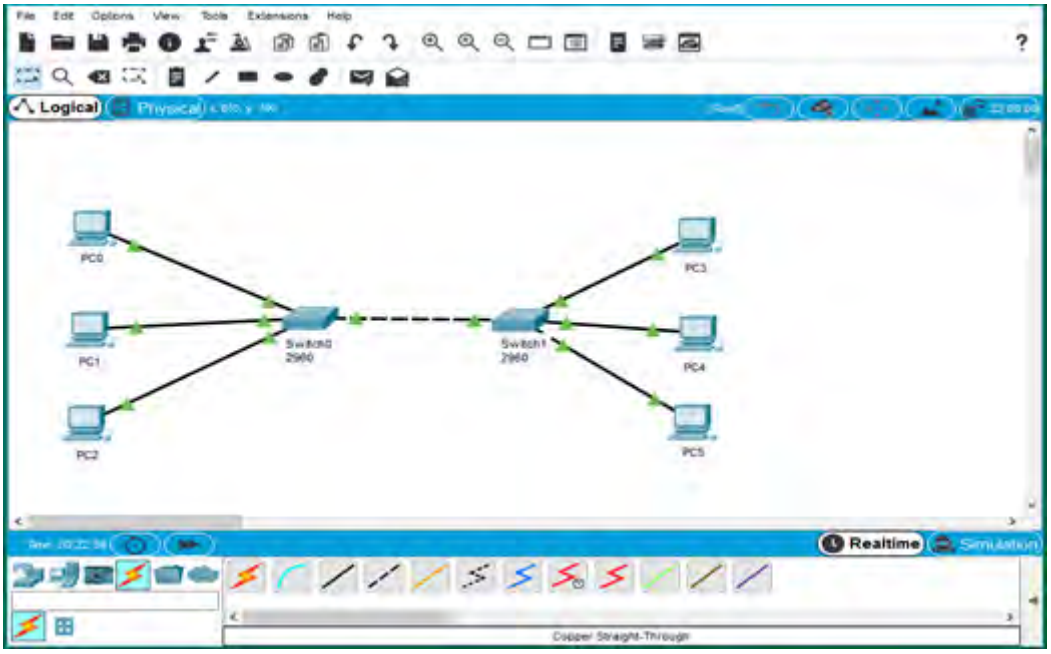


Figure 1.5: Completed Activity

8. We are next going to cable all six `PCs` to the `switches`.
   Either select the cable each time or use the `<CTRL>` key just like in the first activity. This is the set of connections to be done:

- PC1 FastEthernet0 to Switch0 FastEthernet0/2
- PC2 FastEthernet0 to Switch0 FastEthernet0/3
- PC3 FastEthernet0 to Switch1 FastEthernet0/1
- PC4 FastEthernet0 to Switch1 FastEthernet0/2
- PC5 FastEthernet0 to Switch1 FastEthernet0/3

If you used the <CTRL> key to do multiple copies cancel it by clicking on the cancel indicator.

9. Now we need a different type of cable to connect the two switches.
   Select a Copper Cross-Over cable. Click on it and then point at and click on Switch0. From the pop-up menu select the Gigabit0/1 interface near the bottom of the list. Then point at and click Switch1 and select the same interface from this list. The cable will appear and both link lights will be amber but will eventually turn to green after about a minute.

10. The completed activity should look like the Figure 1.5:
    If your workspace looks like the above image, save the file, and exit Packet Tracer. If the workspace does not look like the above image, you might want to try the activity again to practice.

2. Deploying Devices

Objectives

- Open a sample file in Cisco Packet Tracer to practice locating and deploying multiple network devices.
- Save the configured network file to ensure all settings and deployments are retained for assessment and future use.
- Understand different methods for deploying devices in a simulated network environment, enhancing familiarity with the Cisco Packet Tracer interface.
- Practice network device configuration to enhance troubleshooting skills and prepare for real-world networking challenges .

Lab Plan

In this lab, you will learn how to deploy multiple network devices in Cisco Packet Tracer. You will practice locating and placing routers, switches, and end devices within a network topology. The lab will also guide you through different methods of device deployment to enhance your familiarity with the Cisco Packet Tracer interface.

Finding and Deploying Devices

Since Packet Tracer simulates networks and network traffic, the physical aspects of these networks also needs to be simulated. This includes actually finding and deploying physical devices, customizing those devices, and cabling those devices. After the physical deployment and cabling is done, then it is time for configuration of the interfaces used to connect the devices.

In this activity, you will open a sample file, locate and deploy multiple devices, and then save the file.

Step 1: Open the Deploying Devices Packet Tracer file.

- Double click on the `Deploying Devices.pkt` file to open it. You should be presented with a screen similar to that shown in Figure 2.1. If the file does not open, make sure you have properly installed the Packet Tracer application program.

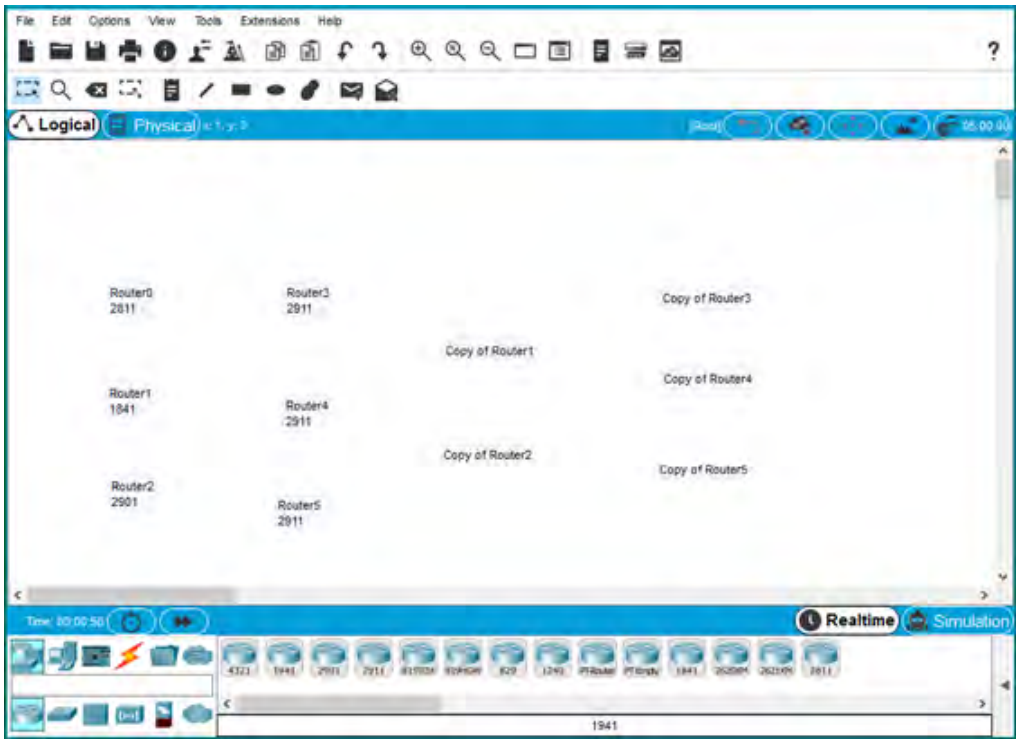


Figure 2.1: Beginning Stage

Step 2: Learn how to Deploy Devices in Packet Tracer.

1. A list of device labels is visible in the workspace, we will use various methods to deploy the listed devices.
   a) First locate the 2811 router in the Device-Specific Selection box pictured below.

Figure 2.2: Device-Specific Selection Box

   b) Using your mouse, click on the `2811` router, and while holding the mouse button down, drag the router over the `Router0` label, then release.

   c) Now click on the `1841` router in the Device-Specific Selection box and then click on the label `Router1` in the workspace.

   d) Now click on the `2901` router in the Device-Specific Selection box and then click on the label `Router2` in the workspace.

> **— Tip: 1.** If you want to put multiple devices of the same type onto the workspace, the clicking and dragging can become very tedious. To avoid this hold down the <CTRL> key as you click on the device in the Device-Specific Selection box.

e) Hold down the <CTRL> key and click on the 2911 router in the Device-Specific Selection box. Now click on the labels Router3, Router4, and Router5. To cancel the operation, click on the Cancel symbol where the 2911 router was in the Device-Specific Selection box.

> **— Tip: 2.** The user may also copy devices on the workspace in two ways.

f) Method 1: Drag your cursor over the devices that you want to copy. Drag a box over Router3, Router4 and Router5. They should appear faded. Hold down the <CTRL> key and drag Router3 over the label Copy of Router3.

g) Method 2: Hold down the <SHIFT> key and click on the devices to be copied. Select Router1 and Router2. Click on Router1 and Router2 while holding down the <SHIFT>key. They will again have a faded look. Point at Router1, hold down the <CTRL> key and drag the devices over the label Copy of Router1 and release.

Your screen should look like the image below if you have deployed the devices correctly. If the file does not look correct, reload the file, and start over.

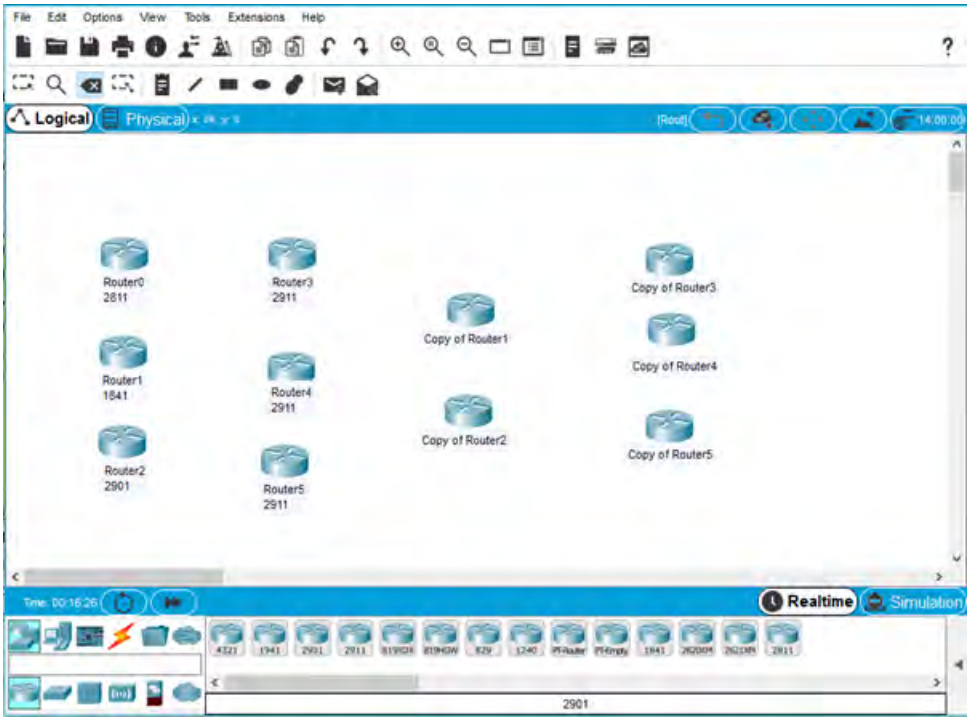


Figure 2.3: Final Look

If the file looks correct, Save your activity file. Exit Packet Tracer

Device Configuration

Once your network has been created, it is time to configure the devices and components. Packet Tracer has the capability to configure the different intermediate and end devices that make up your network. To access the configuration interface of any devices first click on the device that you wish to configure. A popup window will appear displaying a series of tabs. Different types of devices have different interfaces.

Video — **Deploying Devices User Interface I**. Watch this video to video to learn how to configure devices and components in your simulated network. We're going to go through and get comfortable with the options and the menus inside of Cisco Packet Tracer.

GUI and Command-Line Interface (CLI) Configuration

For intermediate devices such as routers and switches, there are two methods of configuration available. Devices can be configured or investigated via a **Config tab (a GUI interface)** or a **command-line interface (CLI)** (Figure 2.6). The Config tab does not exist in most physical equipment. This tab is a learning tab in Packet Tracer. If you don't know how to use the command line interface, this tab provides a way to "fill in the blank" to do basic configurations. It will show the equivalent CLI commands that would do the same thing if using the Command Line Interface. The CLI interface requires knowledge of device configuration.

Video — **Explore Device Configuration Using the CLI (Console)**. The CLI tab provides access to the command line interface of a Cisco device. Using the CLI tab requires knowledge of device configuration with Cisco Internetwork Operating System (IOS). Here, you can practice configuring Cisco devices at the command line. CLI configuration is a necessary skill for more advanced networking implementations. The IOS equivalent of any settings that are made in the Packet Tracer Config tab are mirrored in the CLI.

— Tabs in Packet Tracer. Packet Tracer also provides a variety of tabs for device configuration including the following. The tabs that are shown depend on the device you are currently configuring. You may see other tabs on different devices.

- **Physical:** The Physical tab provides an interface for interacting with the device including powering it on or off or installing different modules, such as a wireless network interface card (NIC).

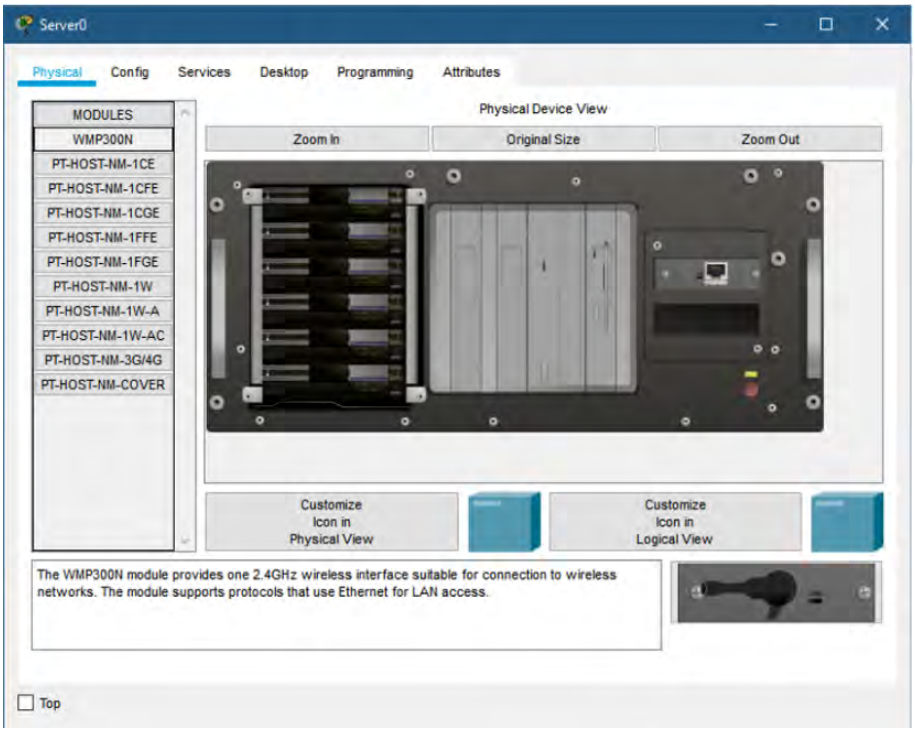


Figure 2.4: Physical Tab

- **Config:** For intermediate devices such as routers and switches, there are two ways to access device configurations. Configurations can be accessed via a Config tab, which is a Graphical User Interface (GUI). Configurations can also be accessed using a command line interface (CLI).
  - The Config tab does not simulate the functionality of a device. This tab is unique to Packet Tracer. If you don't know how to use the command line interface, this tab provides a way to use a Packet Tracer-only GUI to configure basic settings. As settings are changed in the GUI, the equivalent CLI commands appear in the Equivalent IOS Commands window. This helps you to learn the CLI commands and the Cisco Internetwork Operating System (IOS) while you are using the Config tab.
  - For example, in the figure, the user has configured MyRouter as the name of the device. The Equivalent IOS Commands window shows the IOS command that achieves the same results in the CLI.
  - In addition, device configuration files can be saved, loaded, erased, and exported here.

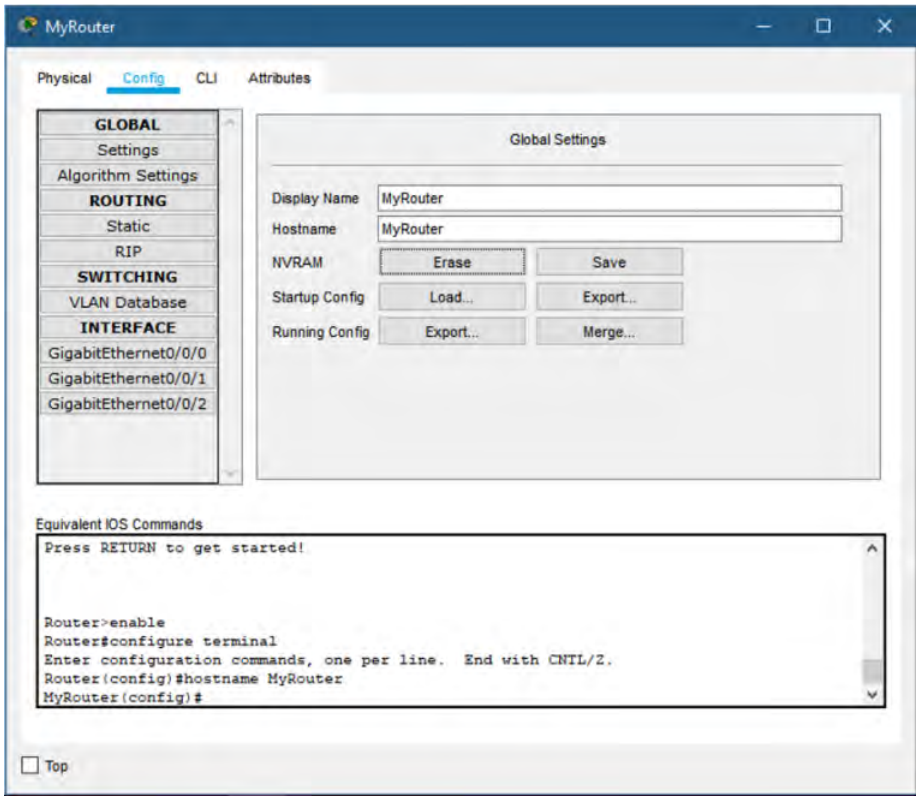


Figure 2.5: Config Tab

- **CLI:** The CLI tab provides access to the command line interface of a Cisco device. Using the CLI tab requires knowledge of device configuration with IOS. Here, you can practice configuring Cisco devices at the command line. CLI configuration is a necessary skill for more advanced networking implementations.
  Note: Any commands that were entered from the Config tab are also shown in the CLI tab.

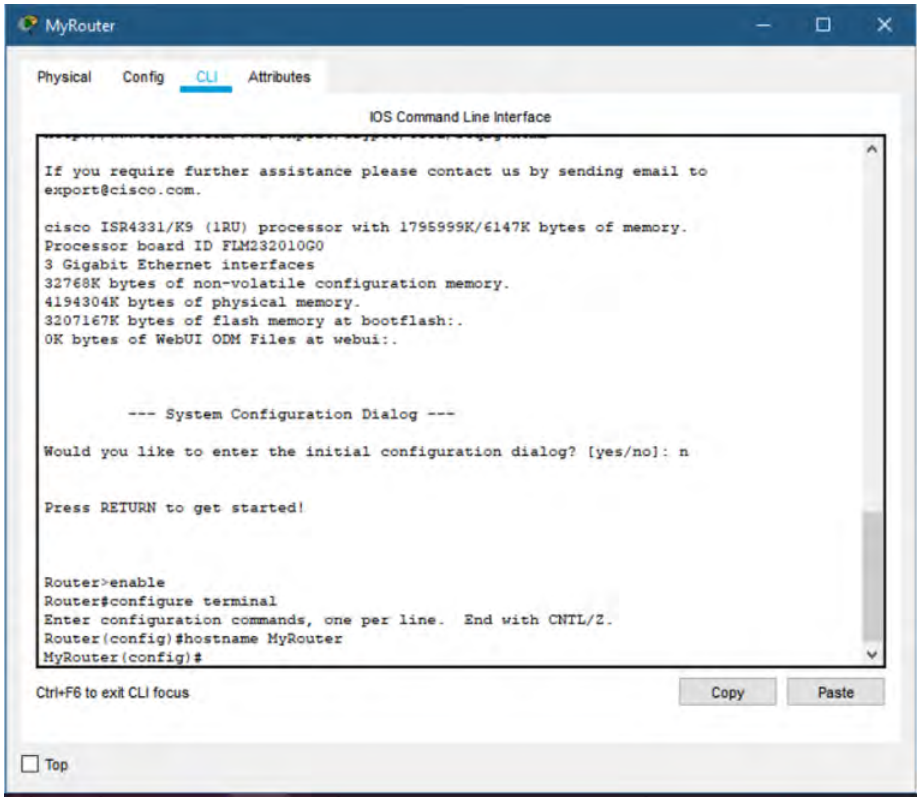


Figure 2.6: Config Tab

- **Desktop:** For some end devices, such as PCs and laptops, Packet Tracer provides a desktop interface that gives you access to IP configuration, wireless configuration, a command prompt, a web browser, and other applications.

Figure 2.7: Desktop Tab

- **Services:** A server has all of the functions of a host with the addition of one more tab, the Services tab. This tab allows a server to be configured with common server processes such as HTTP, DHCP, DNS, or other services, as shown in the figure.

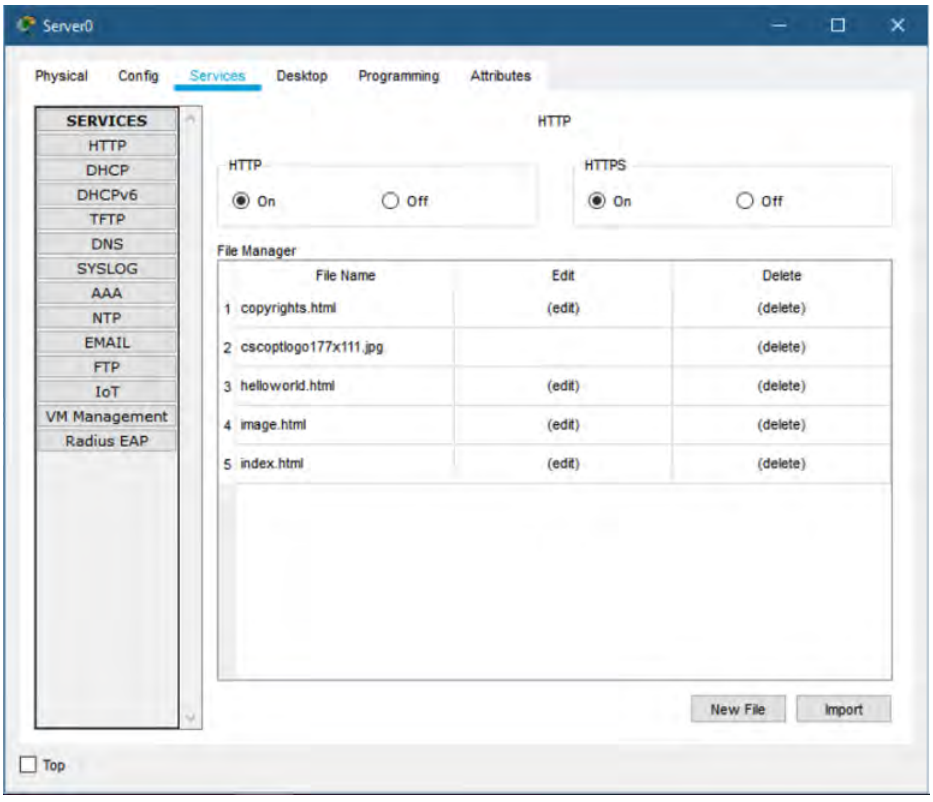


Figure 2.8: Services Tab

Video — Inspect Devices in Physical Mode. Watch this video to learn how to inspect devices in physical mode. Physical Mode offers a realistic view of the network topology, resembling an actual network environment. This mode allows users to visually inspect devices, their physical connections, and the layout of the network infrastructure.

Video — Cable Devices in Physical Mode. Watch this video to learn how to connect devices with various types of cables. Cabling devices in Physical Mode helps simulate the actual process of connecting network hardware in a real-world environment.

Cisco Packet Tracer File Types

Packet Tracer has the ability to create four different types of files. These file types are used for different purposes and include: `.pka`, `.pkt`, `.pksz`, and `.pkz`.

The `.pka` File Type The `.pka` file type is a Packet Tracer Activity file and is the file type you will experience most often. Think of the "a" in `.pka` as meaning "activity." A Packet Tracer Activity has an instructions window. The activity is usually scored as well. This file type contains two networks: an initial network and an answer network. The initial network opens when you launch the activity. The answer network runs in the background and can be used to provide scoring and feedback to learners as they complete the activity. Learners do not have access to the answer network in a `.pka` file.
The Packet Tracer Activity instructions window provides the procedures required to complete the activity, assignment, or assessment. The instructions window can also display completion percentage to track how much of the activity has been successfully completed. The Check Results feature can be enabled to provide feedback.

The `.pkt` File Type The `.pkt` file type is created when a simulated network is built in Packet Tracer and saved. The `.pkt` file can also have graphic background images embedded within it. However, `.pkt` files have no instructions window or activity scoring.

The `.pksz` File Type The `.pksz` file type is specific to Packet Tracer Tutored Activities (PTTA). These files bundle a `.pka` file, media assets, and a scripting file for the hinting system. These activities provide support, in the form of contextualized hints, for students who are working on completing the activity.

The `.pkz` File Type You will see Save As PKZ... in the File menu. This file type was previously used to embed images and other files in a Packet Tracer file. However, images are now embedded directly within a regular `.pkt` or `.pka` file by default. Therefore, consider `.pkz` as a deprecated file type.

Video — Create, Arrange, Uncluster, Delete, and Connect Clusters. As a topology becomes larger and more complicated, clustering devices lets you combine devices into a single cloud icon to simplify the appearance of the topology. You can click the newly created cloud icon to view the devices in the new cluster. To uncluster a group of devices, highlight the cloud icon and delete it with the Delete tool, by choosing the uncluster option. Click Play in the video to learn more about creating, arranging, un-clustering, deleting, and connecting clusters.

Video — Edit and Annotate a Topology. Network design is an iterative process. Networks are usually modified after being built. Similarly, the simulated Packet Tracer networks that you create or work with may require edits to make improvements over the initial design. Therefore, it is important to understand how to modify and document networks in Packet Tracer.

(Optional PTA 1): Connect Devices using Wireless Technologies

— Packet Tracer Activities (PTA). The remainder of this lab consists of series of Packet Tracer Activities (PTA). All the PTA files are in the lab folder. Previously we learn about various files types including `.pka`, `.pkt`, `.pksz`, and `.pkz`. Here is the opportunity to use PTA file type in practise. The Packet Tracer Activity instructions window provides the procedures required to complete the activity, assignment, or assessment. The instructions window can also display completion percentage to track how much of the activity has been successfully completed. The Check Results feature can be enabled to provide feedback.

Objectives

- Connect a laptop to the office WLAN by selecting the network, entering the required credentials, and verifying the connection to ensure internet access.
- Pair devices using Bluetooth by enabling Bluetooth, making the devices discoverable, selecting them from the available list, and testing the connection.
- Enable mobile hotspot on the smartphone, connect the laptop to it, and verify the internet connection for stable browsing and online activities.

Lab Plan

In this lab, you will use various wireless technologies to connect end devices within an office environment. The activity focuses on configuring and monitoring wireless connections in the Physical Mode, providing a realistic representation of how wireless networks are set up and managed.

Part 1: Connect a Laptop to the Office WLAN

- Double click on the `Connect Devices using Wireless Technologies.pka` file to open it.

Step 1: Install a wireless module to a Laptop

a) Click the Laptop to open the configuration window.

b) Under the Physical tab, power off the Laptop by clicking the power button.

c) Remove the Ethernet module `PT-LAPTOP-NM-1CFE` from the laptop by dragging it from the Laptop to the list on the left.

d) Insert the wireless module `WPC300N` by dragging it from the list on the left to the Laptop.

e) Power on the Laptop.

Step 2: Connect Laptop to the office WLAN

a) Click the Desktop tab and select the PC Wireless tool.

b) Click the Connect tab and wait until the `Employee SSID` WLAN is displayed. Note that you may have to click Refresh.

c) Click the `Employee SSID` to select it. Click Connect.

d) Enter `Cisco123` as the pre-shared key and click Connect.

e) After connecting to the wireless network, close the PC Wireless window.

f) Click the Config tab and select `Wireless0` in the left pane to verify in the IP Configuration section that the Laptop has been assigned an IP address.

g) Open the Web Browser from the Desktop. Navigate to `office.srv` to verify that the Laptop has connectivity.

h) Close the Laptop window.

Part 2: Connect Devices with Bluetooth Technology

In this part, you will connect a Bluetooth speaker to a tablet installed with a music player via Bluetooth.

Step 1: Enable Bluetooth ports on devices

a) Click the Bluetooth Speaker.

b) Click the Config tab.

c) Click Bluetooth on the left pane and check that the Port Status is On. Note that the speaker is not paired with the Office Tablet.

Step 2: Connect Bluetooth devices

a) Open the Office Tablet.

b) Click the Config tab.

c) Click Bluetooth in the left pane and check the On box for Port Status.

d) Click Discover and the Bluetooth Speaker device should be discovered.

e) Select the Bluetooth Speaker in the Devices list and click Pair. The status should change to "Paired, Connected". If prompted for permission to connect, click Yes.

f) To test the Bluetooth connection, click the Desktop tab and select Music Player. Click Play/Stop to start the music. Note: Make sure your speaker is on.

g) Click Play/Stop again to stop the sound.

Part 3: Tether a Laptop to Use a Cellular Network via the Smartphone

In this part, you will tether a laptop to a smartphone via Bluetooth. The laptop will use the cellular network to access a website.

Step 1: Enable Bluetooth on the Laptop

a) Click the User-Laptop. Select the Config tab.

b) Click Bluetooth on the left panel. Click On for the Port Status.

c) Leave the User-Laptop Bluetooth window open.

Step 2: Connect a smartphone to the Cellular network and enable Bluetooth

a) Click the Smartphone to open the configuration window.

b) Click the Config tab. Check the On box for the Cellular Tethering setting in the Global

Settings.

c) Click the `3G/4G Cell1` interface. Verify that the Smartphone has an IP address from the cellular network.

d) Click Bluetooth in the left pane and check the On box for the Port status on the Smartphone.

Step 3: Connect Bluetooth devices and tethering to laptop

a) On the Bluetooth configuration for the Smartphone, click Discover to search for nearby Bluetooth enabled-devices.
   - Note: If Smartphone does not appear after a while, move Smartphone closer to User-Laptop and `click Discover` again.

b) Select User-Laptop and click Pair. A pop-up window appears and asks for permission. Click Yes. The two devices are connected via Bluetooth.

c) Return to the User-Laptop. In the Bluetooth panel of the Config tab, highlight Smartphone and click Tether.

d) At the bottom pane of the Bluetooth configuration, notice that User-Laptop has now obtained an IP address.

e) To test connectivity, navigate to `office.srv`. Click Desktop > Web Browser. Enter `office.srv` in the URL field. You can fast forward time to speed up the process.

(Optional PTA 2): Explore Device Configuration using the CLI

Objectives

- Establish a console connection to the device using a console cable and appropriate terminal software to access the device's command-line interface.
- Transfer the configuration information to the device by using terminal commands to upload the necessary configuration files or manually entering the configuration commands.
- Save the updated configuration on the device by executing the command to write the running configuration to the startup configuration, ensuring it is retained after a reboot.

Background / Scenario

A new switch, `Office-SW2`, is being added to the network. Before placing a networking device into a network, the device must be configured and tested. Many types of networking devices, such as switches and routers, may not be preconfigured with enough information to make them accessible through an Ethernet or wireless connection. It may be necessary to load an initial configuration using another method. A console connection and a terminal emulation application provide a convenient way to access the device without having to be on an active network.

Part 1: Connect to the Device Using a Console Connection

In this part, you will use the terminal emulation program on the laptop to access the command line interface (CLI) on the `Office-SW2` switch and view the configuration information.

Console connections are made between a laptop or computer and the networking device using a cable designed to provide a direct cable connection. In this Packet Tracer activity, the cable is identified as Console and is shown as a light blue cable.

Step 1: Use the Terminal Emulation application on the laptop to access the CLI on the switch

Use the Terminal Emulation program on the laptop to access the CLI on the switch.

a) Click the Laptop0 on the table in the Physical Workspace.

b) Click the Desktop tab in the configuration window.

c) Open the Terminal application. The Terminal Configuration window contains the settings that will be used to communicate with the switch. Accept the defaults and click OK.

d) A terminal window will open and the switch console will be displayed. If the switch is not yet fully powered up, messages may scroll on the screen. Wait until the scrolling stops and the message `Press RETURN to get started!` appears on the screen. Press ENTER.

Question: What prompt appears on the switch console screen?

Step 2: Access the Privileged EXEC mode to view configuration information

Cisco networking devices open in User EXEC mode by default when accessing the device through a console connection. User EXEC mode provides access to the device to view information about the status and operation of the device. In order to alter the configuration on the device, you must enter the Privileged `EXEC` mode.

a) At the `Switch>` prompt, enter a question mark (`?`) and press `ENTER`. A list of commands that are available in User EXEC mode will be displayed.
Question: What is the last command displayed in the list?

b) To enable the Privileged `EXEC` mode, type `enable` at the prompt and press `ENTER`.

```
Switch> enable
Switch#
```
Notice that the prompt has changed to indicate Privileged EXEC mode.

c) Enter a question mark (?) at the prompt. A list of available commands will be displayed. If the message -More- appears at the bottom of the screen, press the spacebar to advance to the next screen.
Question: What is the last command in the list for Privileged EXEC mode?

d) Enter the `show running-config` command to view the current configuration running on the device and press ENTER.
```
Switch# show running-config
```
The configuration information will display one screen at a time. Press CTRL-C to return to the switch prompt. The running configuration consists of configuration information that a Cisco IOS device uses to operate on a network. In this case, because the switch is new, it has a minimal default configuration.

Part 2: Copy Configuration Information to the Device

In this part, you will copy configuration information into the device. You will change the device name and set a password for the console connection.

Step 1: Enter global configuration mode

To configure a device, you must first enter the configuration mode. Enter the command `configure terminal` and press ENTER.
```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
```
Notice how the switch prompt changes to indicate that you are now in the configuration mode.

Step 2: Copy the commands and paste the commands to the switch

a) Copy the commands shown below. Select the list of commands below and press CTRL-C to copy to the clipboard.
```
hostname Office-SW2
line con 0
password Cisco123
login
end
```

b) To paste the commands into the switch, right-click at the switch prompt and select Paste from the drop-down menu. The commands will appear on the console as shown:
```
Switch(config)# hostname Office-SW2
Office-SW2(config)# line con 0
Office-SW2(config-line)# password Cisco123
Office-SW2(config-line)# login
Office-SW2(config-line)# end
Office-SW2#
%SYS-5-CONFIG_I: Configured from console by console
```
The commands are now active on the switch. Commands entered in configuration mode take effect immediately and become part of the running configuration on the device. Press ENTER. Notice that switch prompt has changed to reflect the new name assigned to the device.

Step 3: Test the new configuration settings

a) The new configuration commands set a password for the console connection. To test that configuration change, type `exit` and press ENTER.

b) The screen will refresh and the `Press RETURN to get started!` message will display. Press ENTER.
Question: What message is shown on the console?

c) Enter the password `Cisco123` and press ENTER.
Note: The password will not display on the screen. The User EXEC prompt will appear.

Your completion percentage should be 75

Part 3: Save the Updated Configuration to the Device

In this part, you will save the configuration changes to permanent memory on the device. If the configuration changes are not saved, they will be lost if the device loses power or is intentionally rebooted. When a Cisco IOS devices starts, it reads the configuration file that is permanent memory and loads it into the running configuration in RAM. Configuration changes are only made to the running configuration. The changes must be saved so that they will become available to a device on startup.

Step 1: Use the enable command to enter the Privileged EXEC mode on the switch

```
Office-SW2> enable
   Office-SW2#
```

Step 2: Copy the current running configuration to the startup configuration

a) Use the `copy running-config startup-config` command to save the current configuration running on the device to the startup configuration that will load when the device powers up. Press ENTER to accept the default filename.

```
Office-SW2# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

b) To verify that the configuration changes were saved properly, reload the device using the `reload` command. Press ENTER to proceed. Reloading the router will reboot the IOS software and IOS will load the saved configuration file. If the new configuration was made and saved in permanent memory, the device will prompt you for a password to access the device console.

```
Office-SW2# reload
Proceed with reload? [confirm]
```

c) Press ENTER when the message `Press RETURN to get started!` appears. If the configuration was saved successfully, the User Access Verification message will be displayed.

d) Enter the password `Cisco123` at the password prompt. If the password is correct, the User EXEC prompt will appear.

Your completion percentage should be 100

(Optional PTA 3): Edit Topologies

Objectives

In this activity, you will install a patch panel and a wall mount. You will then use these to connect network devices in the office to the equipment in the wiring closet.

- Install an additional switch in the office network rack by mounting it securely and connecting it to the existing network infrastructure.
- Connect a PC to the office network by plugging it into an available port on the switch and configuring its network settings.
- Manage and configure network clusters by setting up and maintaining groupings of interconnected devices to optimize performance and redundancy.
- Integrate a second home cluster into the network by connecting it to the existing infrastructure and configuring it to work seamlessly with the primary cluster.

Part 1: Add an Additional Switch to the Rack in the Office Network

a) In the Wiring Closet, click and drag switch `Office-SW2` from the Shelf on the right to the Rack on the left. It can be placed on any open space on the Rack.

b) Select a copper straight-through cable from the Cable Pegboard.

c) Connect the cable to switchport `FastEthernet 0/1` on switch `Office-SW2` and connect the other end to Jack 1 on the Patch Panel.

d) Select another copper straight-through cable from the Cable Pegboard.

e) Connect the cable to switchport `GigabitEthernet 0/1` on switch `Office-SW2` and connect the other end to switchport `GigabitEthernet 1/1/1` on `Office-SW1`.

Part 2: Connect a PC to the Office Network

Step 1: Connect PC to wall mount

a) Return to the Office topology using the `Alt-Left Arrow` key.

b) Add a straight-through cable from the `Office-User` to the copper wall mount.

c) Click the Connections icon (i.e., orange lightning bolt) in the bottom left-hand corner.

d) Select a copper straight-through cable.

e) Connect the cable to the `Copper Wall Mount1` and select `Jack1`. Connect the other end of the cable to `FastEthernet0` on `Office-User`.

f) Select another copper straight-through cable.

g) Click the `Copper Wall Mount1` and select `Punch Down1`.

h) Connect the other end of the cable to `Punch Down1` on the Patch Panel in the Equipment Cabinet. Click the Equipment Cabinet label in the lower right corner of the office.

i) Click `Rack`, then `Patch Panel`, then `Punch Down1`.

Step 2: Test network connectivity from PC-PT

From `Office-User`, ping the `Office-Admin` PC at `192.168.20.5`.

a) Select the `Office-User` and click the Desktop tab.

b) Click the Command Prompt.

c) In the Command Prompt, ping the `Office-Admin` PC. The pings should be successful.

```
C:\> ping 192.168.20.5
```

d) Exit the Command Prompt. Open a Web Browser and navigate to `office.srv`. It should be successful.
If it is not successful, verify that the cables are connected correctly.

Part 3: Work with Clusters

Step 1: View the city in logical mode

a) While still in the Office, click Back Level.

b) Change the Packet Tracer workspace to Logical mode.

Step 2: Un-cluster and re-cluster the devices in an existing cluster

a) Click anywhere in the workspace, hold the mouse button down and drag a rectangle around the Library cluster to select it.

b) With the Library cluster selected, press delete on the keyboard.

c) You will be prompted to confirm the delete. Click Uncluster in the Confirm Delete dialog box.
Note: If the Library cluster is deleted, instead of unclustered, click undo (`Ctrl + Z`), or reset the activity. (Click File > Reset Activity or `Alt + N`)

d) All the devices in the Library should now be un-clustered on the workspace. Click Select or `Esc` to change the cursor from an X to a pointer.

Step 3: Re-cluster the devices in the Library cluster

a) Click anywhere in the workspace, hold the mouse button down and drag a rectangle around all the un-clustered library devices to select them.

b) With all the library devices selected, click the Create New Cluster (`Shift + U`) in the top-right corner of the workspace.

c) If you missed a device during the re-cluster process, click Move Object (`Shift + M`) and click the object to be moved. Select the desired location. In this example, it will be `Cluster1 > Move to Cluster1`.

d) When the devices are re-clustered, click the cluster name and change it back to Library.

Part 4: Add a Second Home Cluster to the Network

Step 1: Add devices to the workspace

Add a PC, Home Gateway, and a Cable Modem to the workspace.

a) From the End Devices Selection Box, select PC from the End Devices and add it to the workspace.

b) From the Network Devices Selection Box, place a Home Gateway from the Wireless Devices and cable modem from WAN Emulation Devices onto the workspace.

Step 2: Connect the devices in the Second Home cluster

a) Select a copper straight-through cable and connect the `FastEthernet0` port of `PC0` to the `Ethernet 1` port of the `Home Gateway1`.

b) Select another copper straight-through cable and connect the `Internet` port of the `Home Gateway1` to `Port 1` of the `Cable Modem0`.

Step 3: Cluster the devices

a) Click anywhere in the workspace, hold the mouse button down and drag a rectangle around all the un-clustered devices for the Second Home to select them.

b) With all the devices selected, click the Create New Cluster icon in the top right corner of the workspace.

c) When the devices are clustered, click the cluster name and change it to Second Home.

Step 4: Connect the Second Home to the ISP

a) Select the blue Coaxial cable. Click the Second Home cluster.

b) In the device list for the Second Home, select the `Cable Modem0` and connect the cable to `Port 0` which is a coaxial port on the modem.

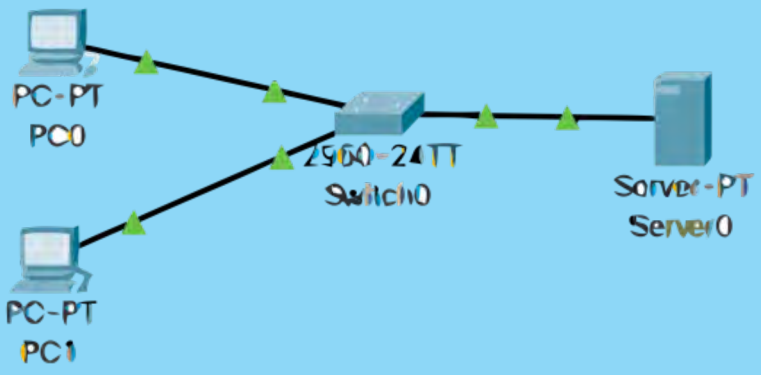
c) Click the ISP cluster and select the `Cloud0` device and `Coaxial9`.

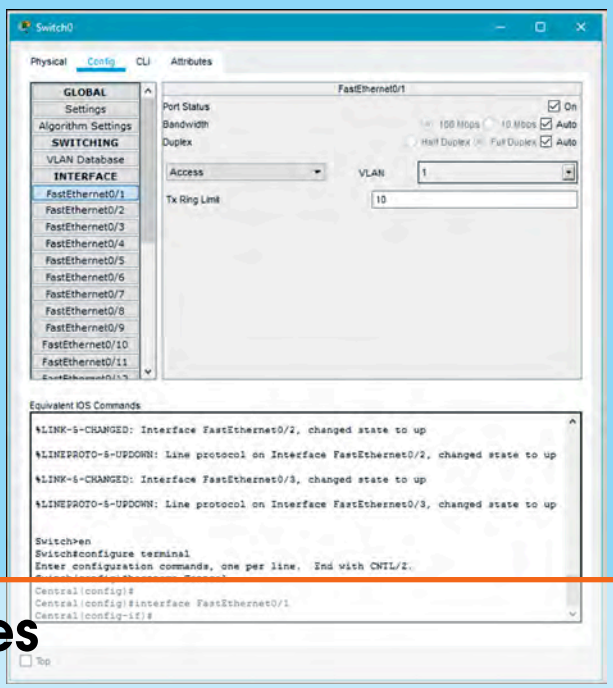
d) The Second Home cluster is now connected to the ISP.

Step 5: Use a Note to document the devices added to the Second Home cluster

a) Document which items were added to the second home cluster. Click the `Place Note icon` in the tool bar then click the workspace next to the Second Home cluster to add a note.

b) In the note, type the devices that were added to the Second Home cluster.





3. Configure End Devices

Objectives

- Open a sample file in Cisco Packet Tracer to practice locating and deploying multiple network devices.
- Save the configured network file to ensure all settings and deployments are retained for assessment and future use.
- Understand different methods for deploying devices in a simulated network environment, enhancing familiarity with the Cisco Packet Tracer interface.
- Practice network device configuration to enhance troubleshooting skills and prepare for real-world networking challenges.

Lab Plan

In this lab, you will learn how to configure end devices in a network using Cisco Packet Tracer. You will practice setting IP addresses, subnet masks, and default gateways for PCs and servers. Additionally, you will use command prompt tools to test network connectivity and troubleshoot issues.

Video — Determining End Device IP Addresses. Determining the IP addresses of end devices is a crucial step in network configuration and troubleshooting. End devices such as PCs, laptops, servers, and printers need IP addresses to communicate within a network. This guide outlines the steps to find and verify IP addresses for end devices.

Video — Device Connection Types. Cisco Packet Tracer provides various types of connections that can be used to link devices in a network. Understanding these connection types is essential for building accurate network topologies.

Step 1: Launch Packet Tracer

a) Launch Packet Tracer on your PC or laptop computer

Double click on the Packet Tracer icon on your desktop or navigate to the directory that contains the Packet Tracer executable file and launch Packet Tracer. Packet Tracer should open with a blank default Logical topology workspace as shown in the Figure 3.1.

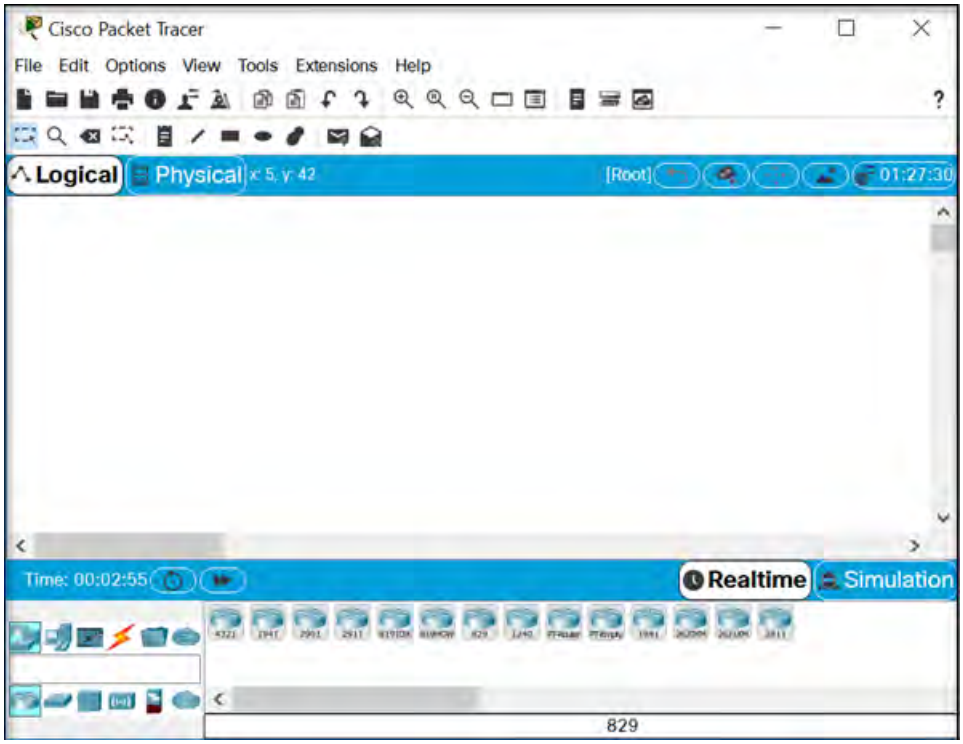


Figure 3.1: Initial Worksapce

Step 2: Build the topology

1. Create the network shown in Figure 3.2 (If help is required, please refer to previous activities).
   a) Use port `FastEthernet0/1` on the switch for `PC0`
   b) Use port `FastEthernet0/2` on the switch for `PC1`
   c) Use port `FastEthernet0/3` on the switch for `Server0`

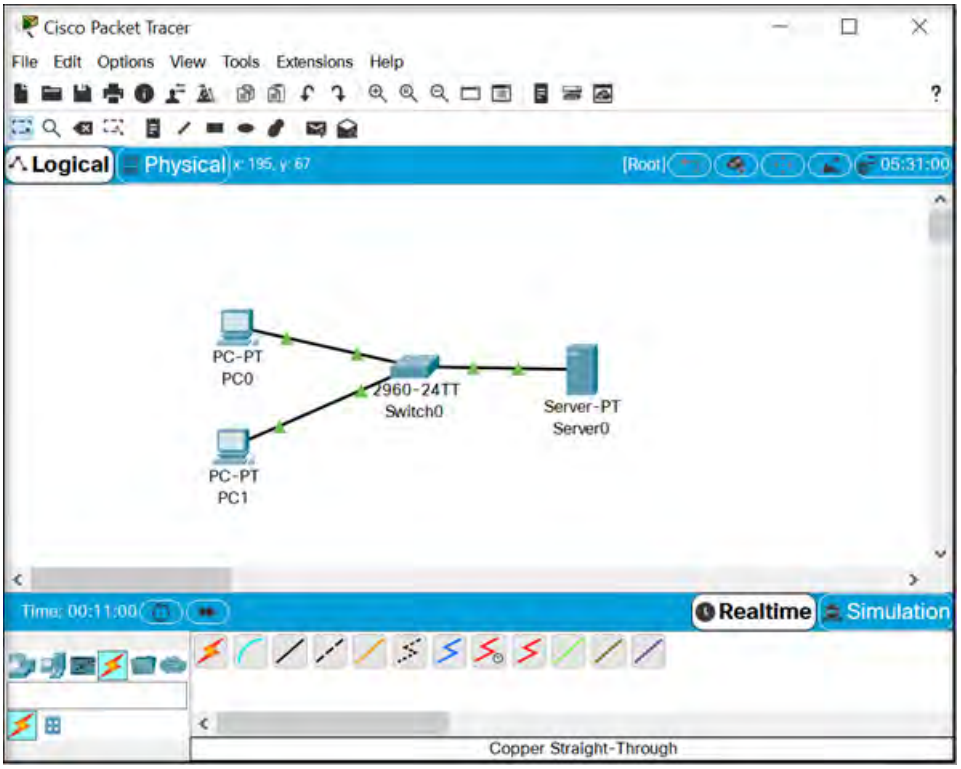


Figure 3.2:

2. Once the link lights all turn green, click on Server0. Then configure it as follows:
   a) Click on the Desktop tab.
   b) Click on the IP Configuration icon.
   c) Click on the IP Address dialog box.
   d) Type in `192.168.1.1` as the address and press enter.
   e) A default value of `255.255.255.0` should appear in the Subnet Mask field.
   f) Nothing else in this dialog box needs to be configured, so click the "X" in the upper right corner to close the IP Configuration window.
   g) Click the red "X" in the upper right corner to close the `Server0` window.
3. Click on PC0. Then configure it as follows:
   a) Click on the Desktop tab.
   b) Click on the IP Configuration icon.
   c) Click on the IP Address dialog box.
   d) Type in 192.168.1.2 as the address and press enter.
   e) A default value of 255.255.255.0 should appear in the Subnet Mask field.
   f) Nothing else in this dialog box needs to be configured, so click the "X" in the upper right corner to close the IP Configuration window

g) Click on the icon labeled Command Prompt and the following prompt should appear:

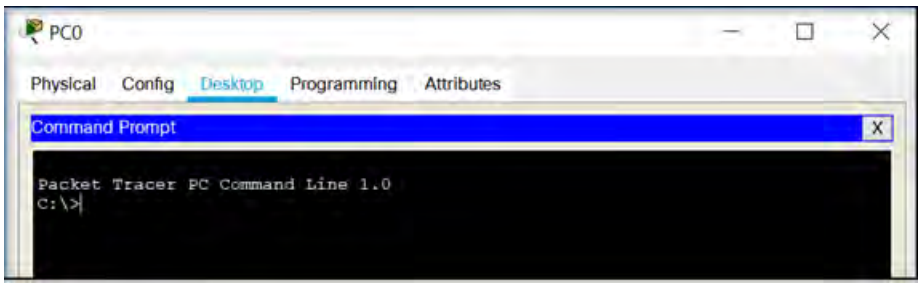


Figure 3.3:

h) Type the following command in the prompt: ping 192.168.1.1 and press enter.

i) If you have done everything correctly, you should see the following output. Your output could vary a little but the reply statements should be there. If the replies are not there, try redoing the device configuration to this point.

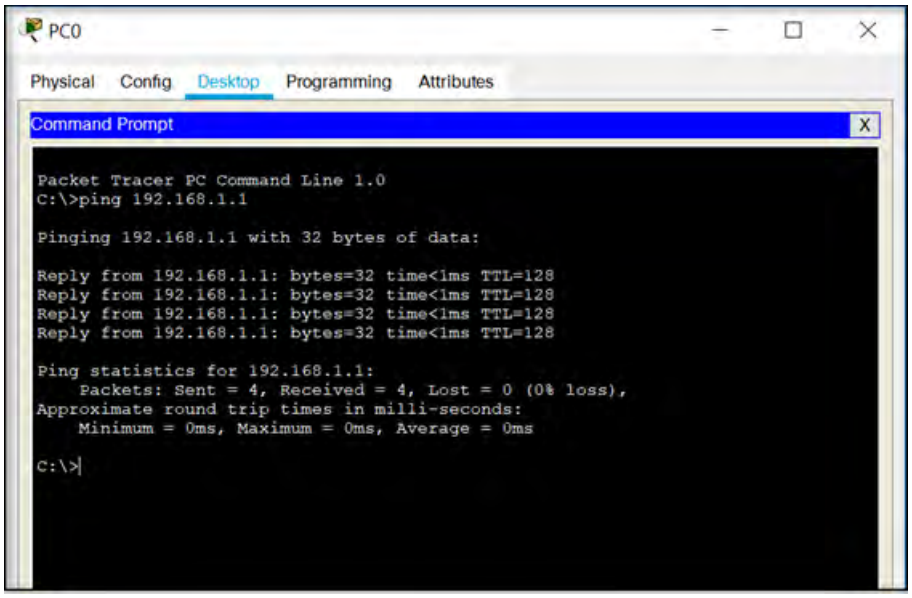


Figure 3.4:

j) Click the “X” next to the Command Prompt title bar.

k) Click the red “X” in the upper right corner to close the PC0 window.

4. Repeat the same configuration and ping steps from #3 on PC1, except use 192.168.1.3 as the IP address. The results should be the same.
   a) Finally, click on PC1 again.
   a) Click on the Desktop tab, if it is not already open.

   b) Click on the Web Browser icon.

   c) Type 192.168.1.1 in the URL box and click the [GO] button.

   d) You should observe the following. If you do not, repeat the earlier steps to confirm

the configuration. This happens because the web server feature is on by default in the server and PC1 just connected to the default page.

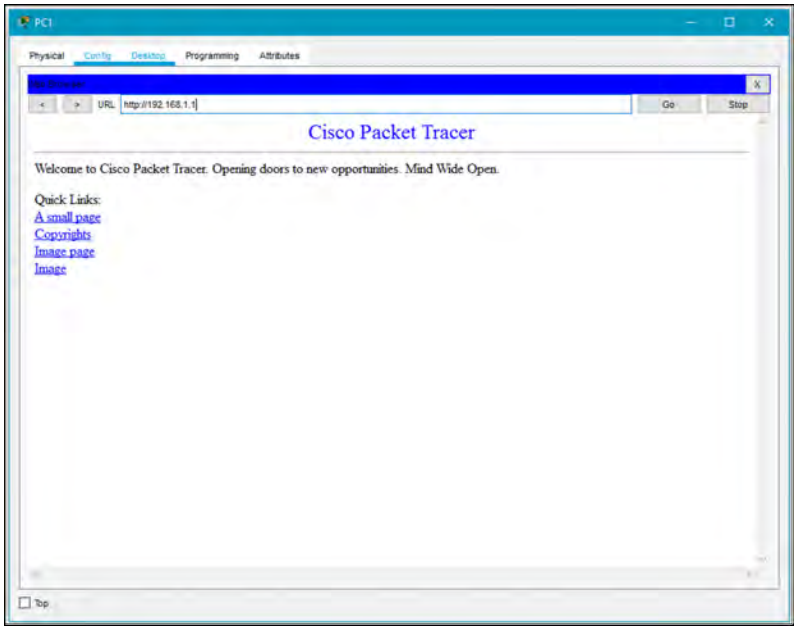


Figure 3.5:

e) Click on a link and then use the front and back arrows to the left of the URL box to move forward and backward through the pages.

f) When done, click the "X" next to the Web Browser title bar.

g) Click the red "X" in the upper right corner to close the PC0 window.

The next section involves some basic configuration of network devices, in this case a switch. Routers have the same tabs as switches so their interface works the same way.

5. Click on Switch0, then click on the Config tab. Note: Previously, a warning about not using the Config tab was given because it is not available on real networking equipment, but we are explaining this tab for two reasons.

   a) Some simple devices only have config tabs.

   b) The config tab can be useful for basic learning of commands, especially for beginners.

   a) Clicking on the Config tab shows a list of components that can be configured on this device. We are not going to cover what these components are, as that is learned in a networking course, but we will show how to navigate and use the interface.

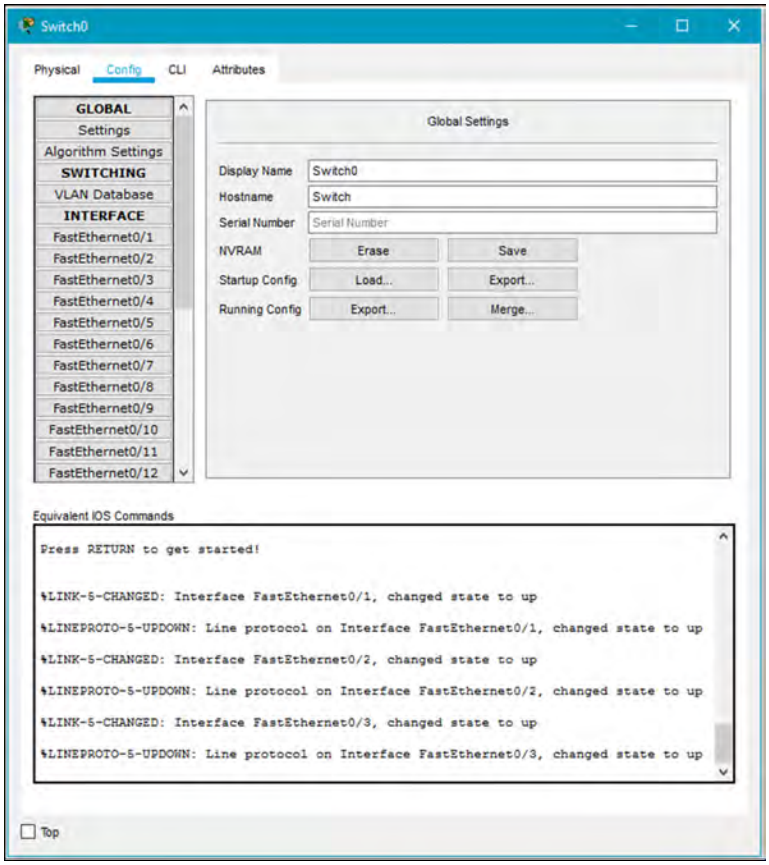


Figure 3.6:

b) The Global Settings tab allows a user to change the name of a device that displays in the workspace. It also allows for changing the internal name shown at the command line prompt as well as buttons for saving, loading, exporting, and erasing configuration files.

c) Double click in the Hostname dialog box highlighting the word Switch, type Central and press enter. Packet Tracer will display the IOS commands necessary to accomplish the name change in the Equivalent IOS Commands box. The commands displayed should be as follows:
   - Switch>enable
   - Switch#configure terminal
   - Enter configuration commands, one per line. End with CNTL/Z.
   - Switch(config)#hostname Central
   - Central(config)#

   These would be the commands that would be entered to do the same thing from the command line interface or CLI. If you didn't know how to do this from the CLI, the Config tab would show the commands to illustrate how it should be done.

d) Clicking on the FastEthernet0/1 label will bring up an Ethernet interface to be configured.

e) Notice the Equivalent IOS Commands box below. It shows a command of "interface FastEthernet0/1" which would have been the command used to select the interface from the CLI.

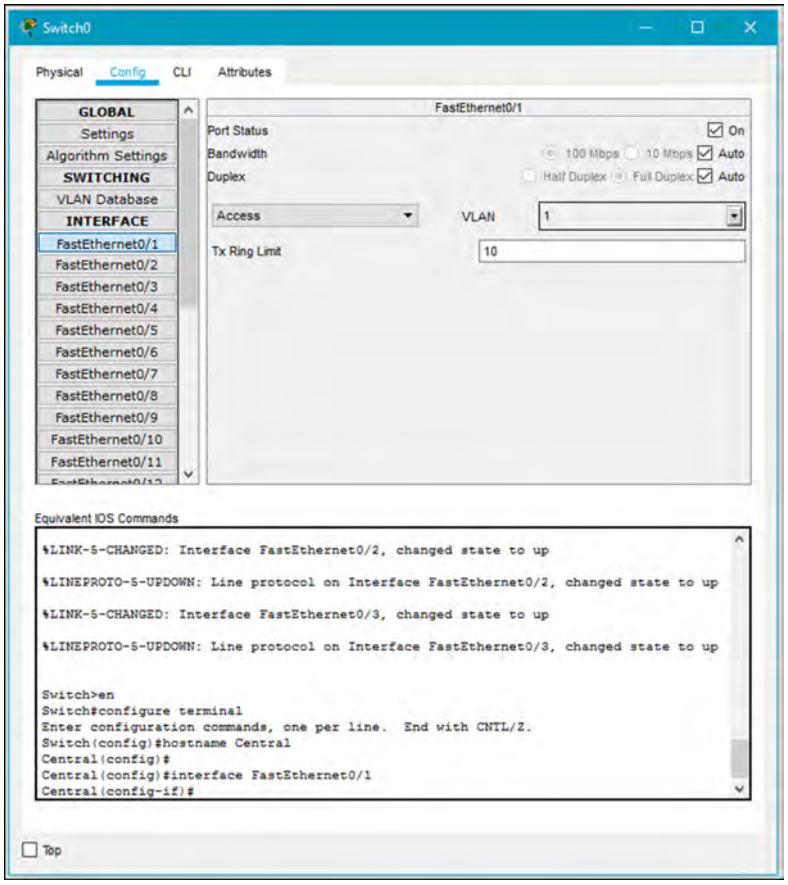


Figure 3.7:

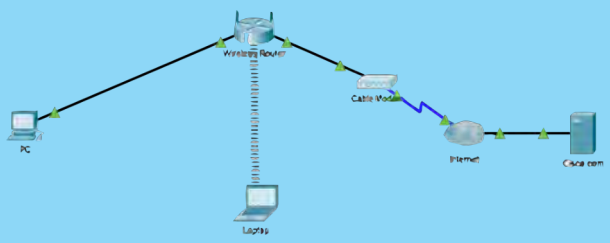
f) Select the CLI tab to switch to the CLI interface. Notice that the same commands that were in the Equivalent IOS Commands box are listed in the CLI window.

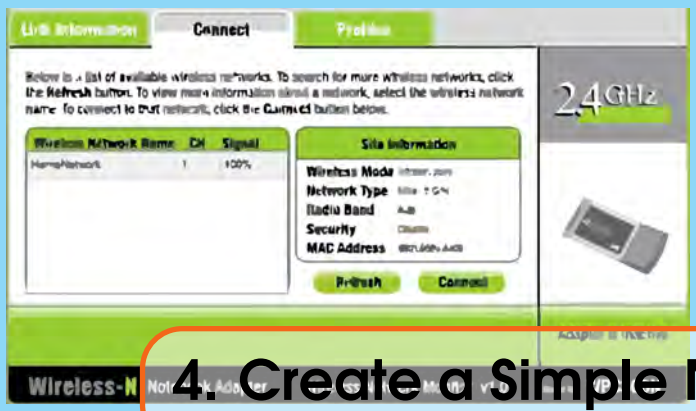
g) Click right beside the command prompt at the bottom of the list that looks like this: "Central(config-if)#"

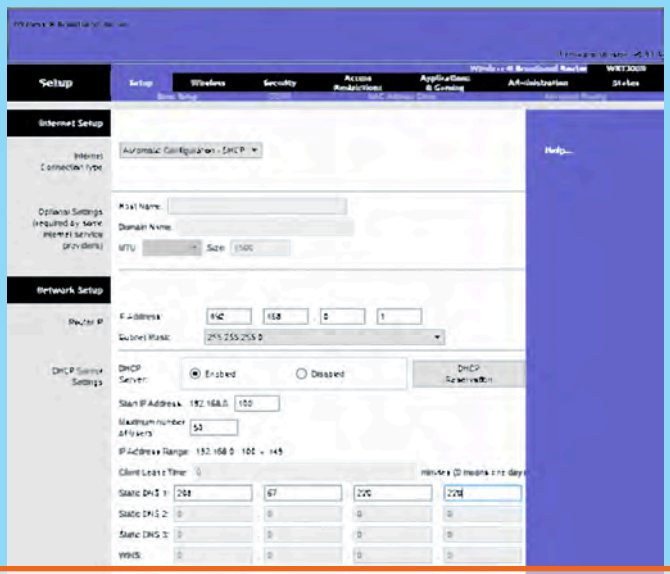
h) Then type shutdown, and press enter twice
   - Central(config-if)#shutdown
   - Central(config-if)#
   - %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
   - %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
   - Central(config-if)#

   This command just shut the interface down from the command line.

i) Click the red "X" in the upper right corner to close the Server CLI window. Notice how the link lights for the connection between PC0 and Switch0 are red. Because the interface on the switch was shut down, the connection is no longer active and shows red.
   This covers some basic configuration and operation of end devices in Packet Tracer. Please save and close the activity, then exit Packet Tracer.







4. Create a Simple Network Using Packet Tracer

Objectives

- Build a simple network in the logical topology workspace by placing and connecting network devices appropriately.
- Configure network devices to establish communication between them using IP addressing.
- Test connectivity between network devices to ensure proper network setup and functionality.
- Save the Packet Tracer file and exit the application, securing the completed network configuration.

Lab Plan

In this lab, you will learn how to create a simple network topology using Cisco Packet Tracer. You will practice adding network devices such as routers, switches, and end devices to the workspace and configure them for communication. You will also test connectivity between the devices to verify the network setup.

Topology

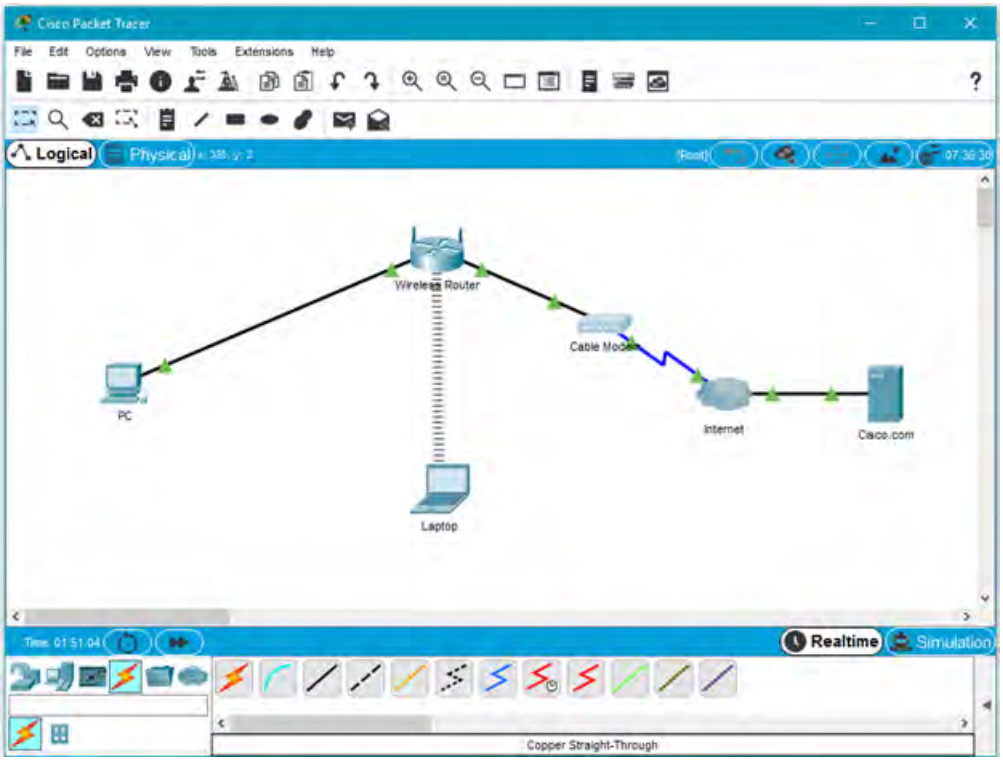


Figure 4.1:

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC	Ethernet0	DHCP		192.168.0.1
Wireless Router	LAN	192.168.0.1	255.255.255.0	
Wireless Router	Internet	DHCP		
Cisco.com Server	Ethernet0	208.67.220.220	255.255.255.0	
Laptop	Wireless0	DHCP		

Objectives

a) Part 1: Build a Simple Network in the Logical Topology Workspace
b) Part 2: Configure the Network Devices
c) Part 3: Test Connectivity between Network Devices
d) Part 4: Save the File and Close Packet Tracer

Background / Scenario

In this activity you will build a simple network in Packet Tracer from scratch and then save the network as a Packet Tracer Activity File (.pkt).

Part 1: Build a Simple Network in the Logical Topology Workspace

Step 1: Launch Packet Tracer.

a) Launch Packet Tracer on your PC or laptop computer

Double click on the Packet Tracer icon on your desktop or navigate to the directory that contains the Packet Tracer executable file and launch Packet Tracer. Packet Tracer should open with a blank default Logical topology workspace as shown in the figure.

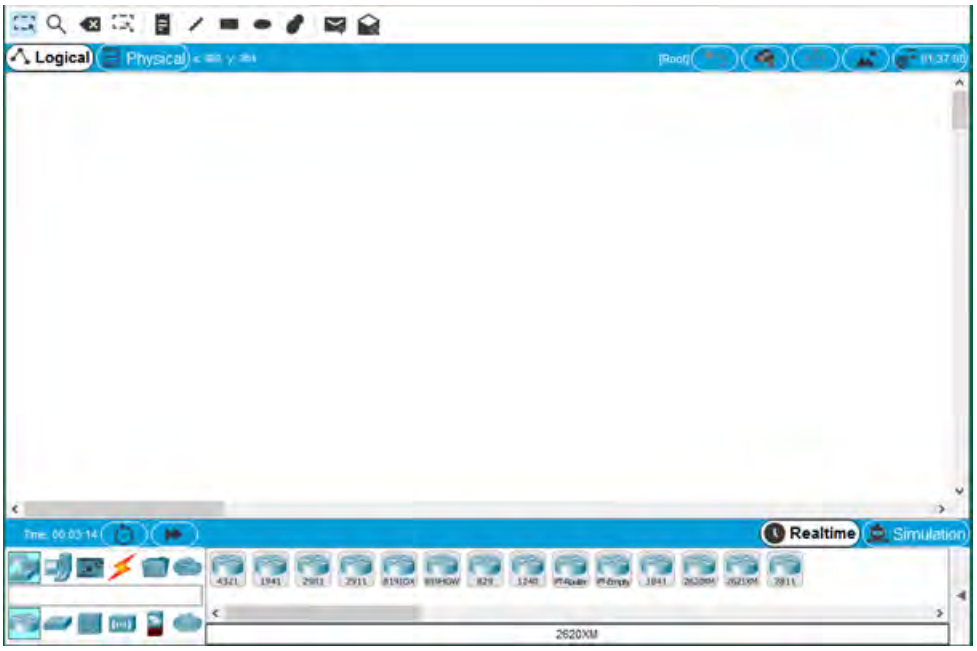


Figure 4.2:

Step 2: Build the topology

a) Add network devices to the workspace.
Using the device selection box, add the network devices to the workspace as shown in the topology diagram.
To place a device onto the workspace, first choose a device type from the Device-Type Selection box. Then, click on the desired device model from the Device-Specific Selection box.
Finally, click on a location in the workspace to put your device in that location. If you want to cancel your selection, click the Cancel icon for that device. Alternatively, you can click and drag a device from the Device-Specific Selection box onto the workspace.

b) Add network devices to the workspace.
Using the device selection box, add the network devices to the workspace as shown in the topology diagram
To place a device onto the workspace, first choose a device type from the Device-Type Selection box. Then, click on the desired device model from the Device-Specific Selection box.
Finally, click on a location in the workspace to put your device in that location. If you want to cancel your selection, click the Cancel icon for that device. Alternatively, you can click and drag a device from the Device-Specific Selection box onto the workspace.

c) Change display names of the nework devices.
To change the display names of the network devices click on the device icon on the Packet Tracer Logical workspace, then click on the Config tab in the device configuration window. Type the new name of the device into the Display Name box as show in the figure below.

Figure 4.3:

d) Add the physical cabling between devices on the workspace
Using the device selection box, add the physical cabling between devices on the workspace as shown in the topology diagram.
The PC will need a copper straight-through cable to connect to the wireless router. Select the copper straight-through cable in the device selection box and attach it to the FastEthernet0 interface of the PC and the Ethernet 1 interface of the wireless router.
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-selection box and attach it to the Internet interface of the wireless router and the Port 1 interface of the cable modem.
The cable modem will need a coaxial cable to connect to the Internet cloud. Select the coaxial cable in the device-selection box and attach it to the Port 0 interface of the cable modem and the coaxial interface of the Internet cloud.
The Internet cloud will need copper straight-through cable to connect to the Cisco.com server. Select the copper straight-through cable in the device-selection box and attach it to the Ethernet interface of the Internet cloud and the FastEthernet0 interface of the Cisco.com server.

Part 2: Configure the Network Devices

Step 1: Configure the wireless router

a) Create the wireless network on the wireless router
Click on the **Wireless Router** icon on the Packet Tracer Logical workspace to open the device configuration window.
In the **wireless router configuration** window, click on the **GUI tab** to view configuration options for the wireless router.
Next, click on the **Wireless tab** in the GUI to view the wireless settings. The only setting that needs to be changed from the defaults is the **Network Name (SSID)**. Here, type the name “HomeNetwork” as shown in the figure.

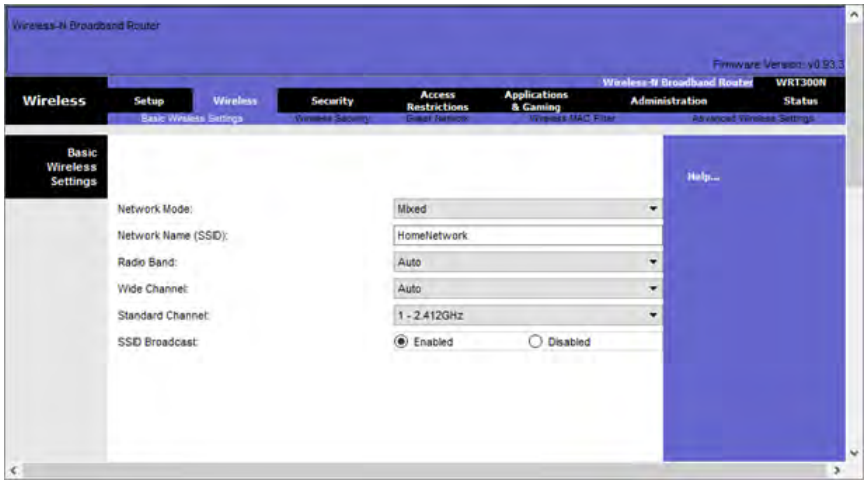


Figure 4.4:

Configure the Internet connection on the wireless router
Click on the Setup tab in the wireless router GUI.
In the DHCP Server settings verify that the Enabled button is selected and configure the static IP address of the DNS server as 208.67.220.220 as shown in the figure.

b) Click on the Save Settings tab.

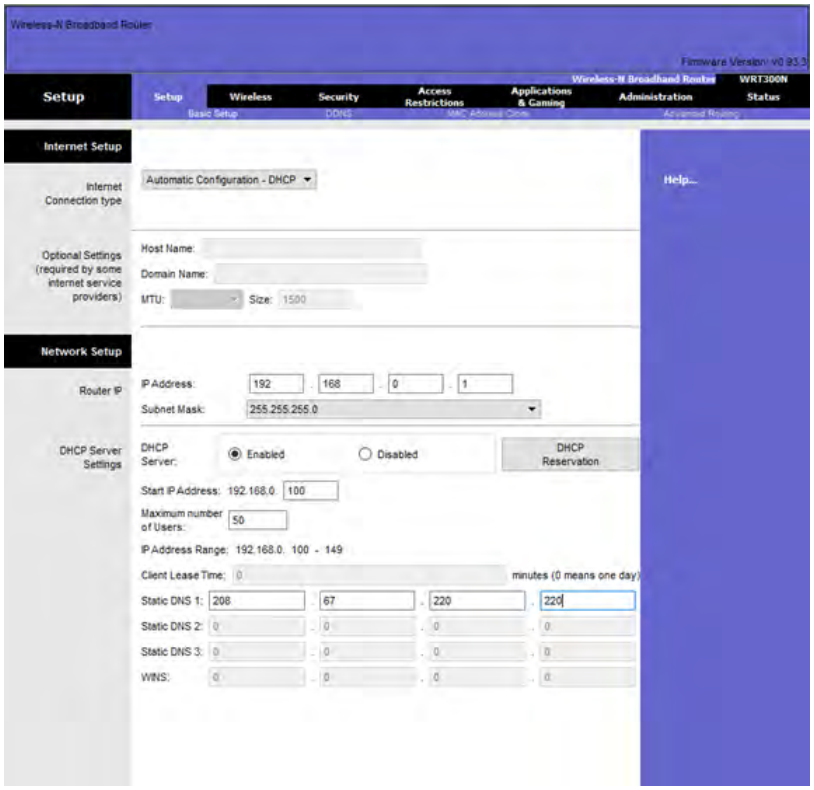


Figure 4.5:

Step 2: Configure the laptop

a) Configure the Laptop to access the wireless network
b) Click on the **Laptop icon** on the Packet Tracer Logical workspace and in the laptop configu-

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

c) To do this, you first power the Laptop off by clicking the power button on the side of the laptop. Then 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. Then install the Wireless WPC300N module by clicking on it in the MODULES pane and dragging it to the empty module port on the side of the laptop. Power the laptop back on by clicking on the Laptop power button again.
d) With the wireless module installed, the next task is to connect the laptop to the wireless network. Click on the **Desktop tab** at the top of the Laptop configuration window and select the **PC Wireless icon**.
e) Once the Wireless-N Notebook Adapter settings are visible, select the **Connect tab**. The wireless network "HomeNetwork" should be visible in the list of wireless networks as shown in the figure.
f) Select the **network**, and click on the **Connect tab** found below the Site Information pane.

Figure 4.6:

Step 3: Configure the PC

a) Configure the PC for the wired network Click Click on the **PC icon** on the Packet Tracer Logical workspace and select the **Desktop tab** and then the **IP Configuration icon**.
b) Click In the **IP Configuration window**, select the DCHP radio button as shown in the figure so that the PC will use DCHP to receive an IPv4 address from the wireless router.
c) Close the IP Configuration window.

Figure 4.7:

d) Click on the Command Prompt icon. Verify that the PC has received an IPv4 address by issuing the ipconfig /all command from the command prompt as shown in the figure. The PC should receive an IPv4 address in the 192.168.0.x range.

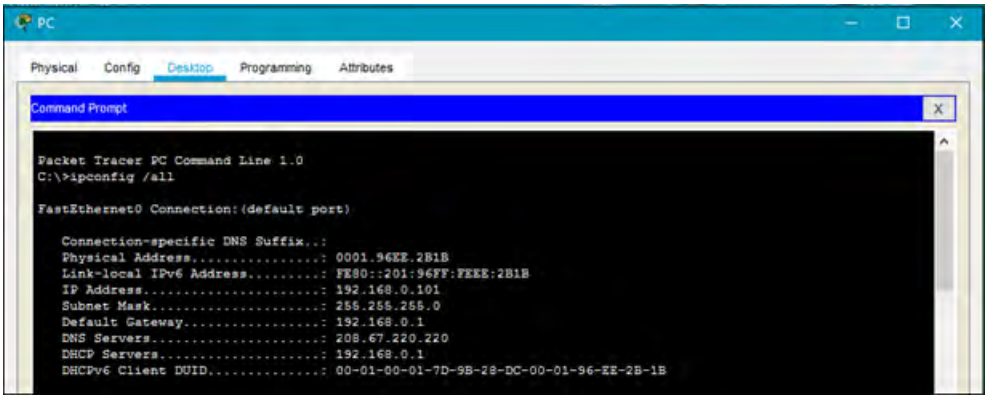


Figure 4.8:

Step 4: Configure the Internet cloud

a) Install network modules if necessary
Click on the Internet Cloud icon on the Packet Tracer Logical workspace and then click on the Physical tab. The cloud device will need two modules if they are not already installed. The PT-CLOUD-NM-1CX which is for the cable modem service connection and the PT-CLOUD-NM-1CFE which is for a copper Ethernet cable connection. If these modules are missing, power off the physical cloud devices by clicking on the power button and drag each module to an empty module port on the device and then power the device back on.

b) Identify the From and To Ports
Click on the Config tab in the Cloud device window. In the left pane click on Cable under CONNECTIONS. In the first drop down box choose Coaxial and in the second drop down box choose Ethernet then click the Add button to add these as the From Port and To Port as shown in the figure.

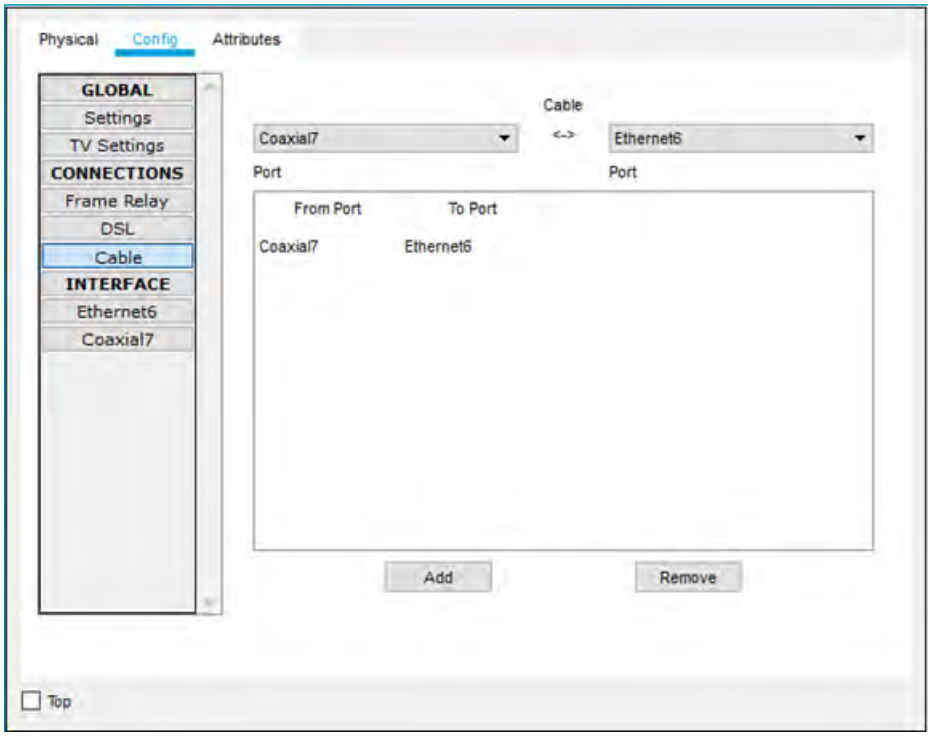


Figure 4.9:

c) Identify the type of provider While still in the Config tab click Ethernet under INTERFACE in the left pane. In the Ethernet configuration window select Cable as the Provider Network as shown in the figure.

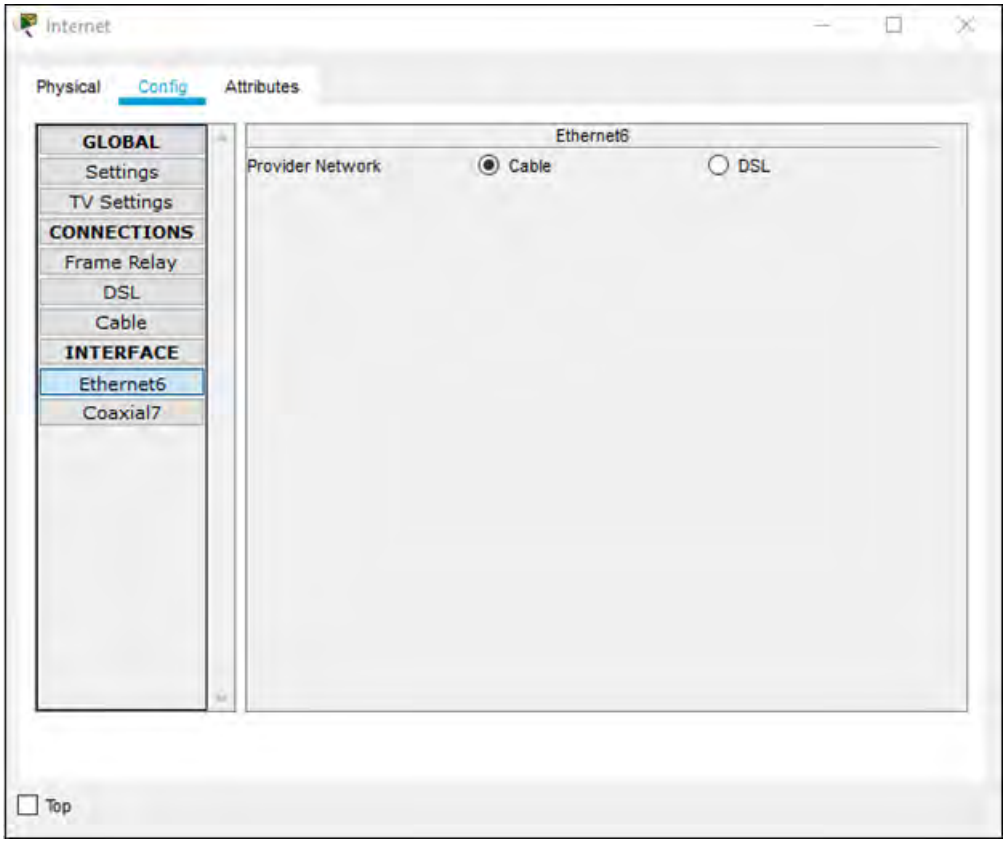


Figure 4.10:

Step 5: Configure the Cisco.com server

a) Configure the Cisco.com server as a DHCP server
Click on the Cisco.com server icon on the Packet Tracer Logical workspace and select the Services tab. Select DHCP from the SERVICES list in the left pane.
In the DHCP configuration window, configure a DHCP as shown in the figure with the following settings.

- Click On to turn the DCHP service on
- Pool name: DHCPpool
- Default Gateway: `208.67.220.220`
- DNS Server: 208.67.220.220
- Starting IP Address: 208.67.220.1
- Subnet Mask 255.255.255.0
- Maximum number of Users: 50

Click Add to add the pool

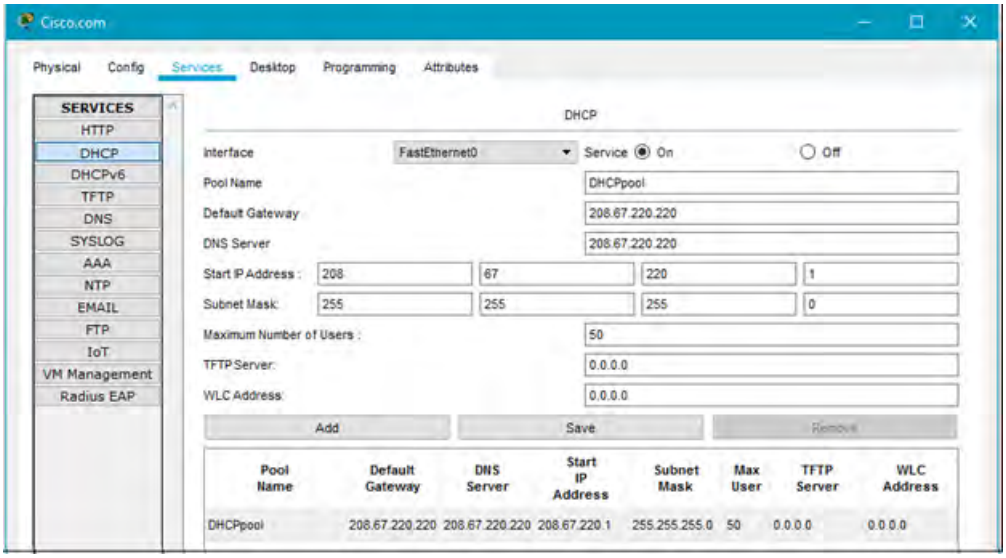


Figure 4.11:

b) Configure the Cisco.com server as a DNS server to provide domain name to IPv4 address resolution. While still in the Services tab, select DNS from the SERVICES listed in the left pane.
Configure the DNS service using the following settings as shown in the figure.
- Click On to turn the DNS service on
- Name: Cisco.com
- Type: A Record
- Address: 208.67.220.220

Click Add to add the DNS service settings

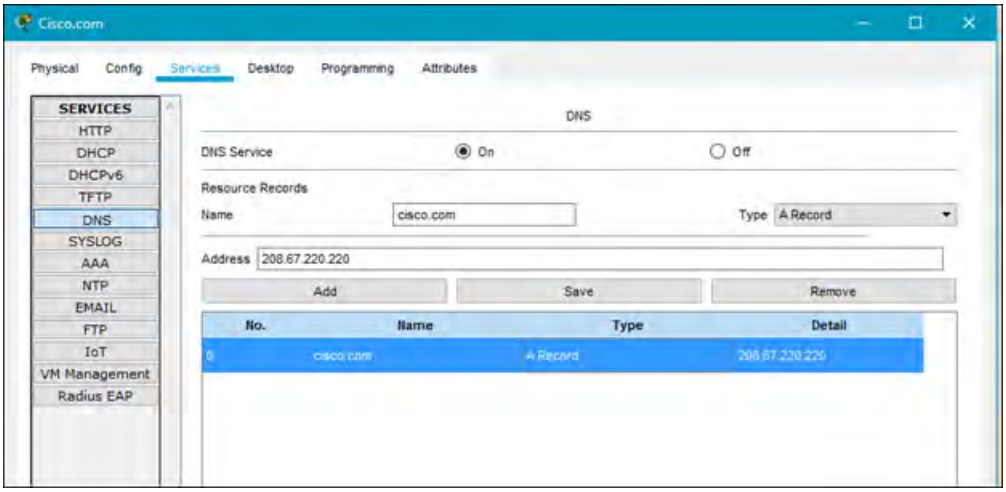


Figure 4.12:

c) Configure the Cisco.com server Global settings. Select the Config tab.
Click on Settings in left pane.
Configure the Global settings of the server as follows:
- Select Static
- Gateway: 208.67.220.1

- DNS Server: 208.67.220.220

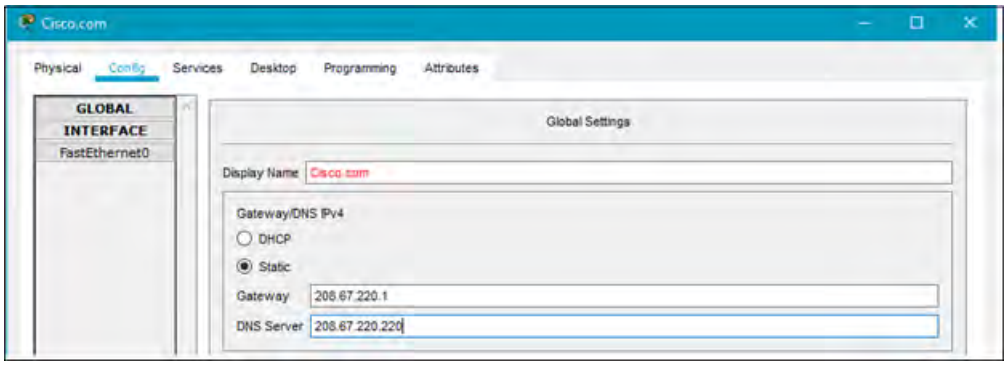


Figure 4.13:

d) Configure the Cisco.com server FastEthernet0 Interface settings.
Click on FastEthernet in left pane of the Config tab
Configure the FastEthernet Interface settings of the server as follows:
   - Select Static under IP Configuration
   - IP Address: 208.67.220.220
   - Subnet Mask: 255.255.255.0

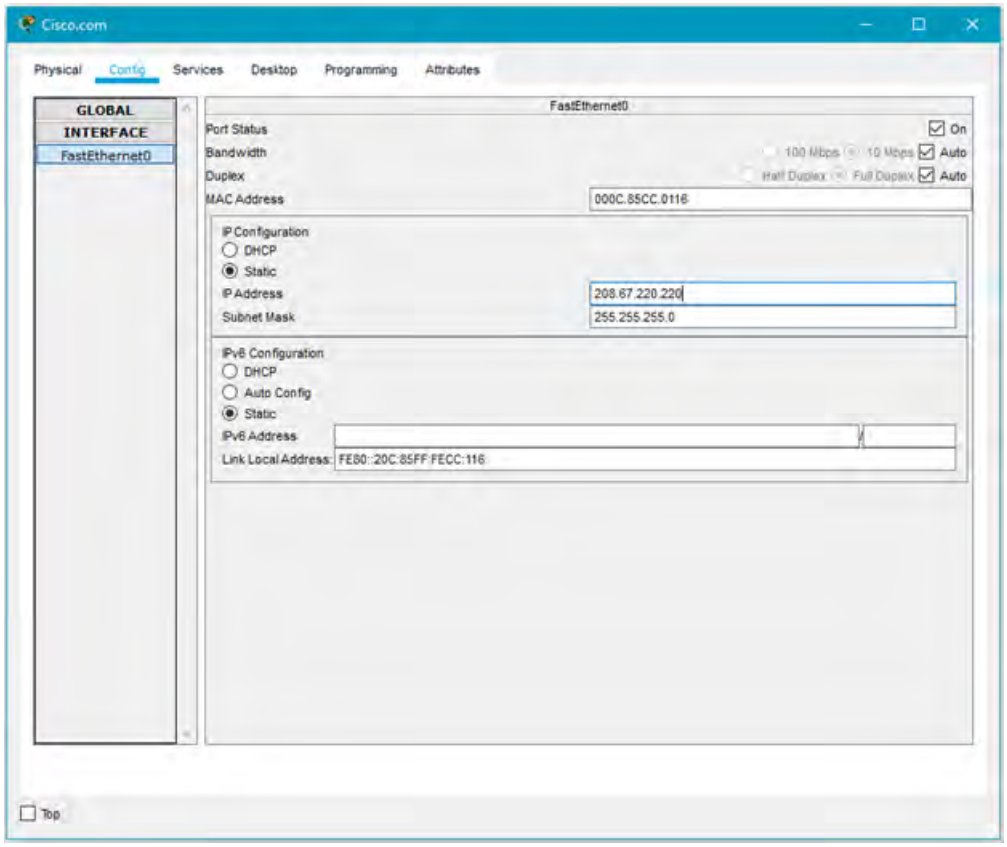


Figure 4.14:

Part 3: Verify Connectivity

Step 1: Refresh the IPv4 settings on the PC

a) Verify that the PC is receiving IPv4 configuration information from DHCP. Click on the PC on the Packet Tracer Logical workspace and then the select the Desktop tab of the PC configuration window.
Click on the Command Prompt icon
In the command prompt refresh the IP settings by issuing the commands ipconfig /release and then ipconfig /renew. The output should show that the PC has an IP address in the 192.168.0.x range, a subnet mask, a default gateway, and DNS server address as shown in the figure.

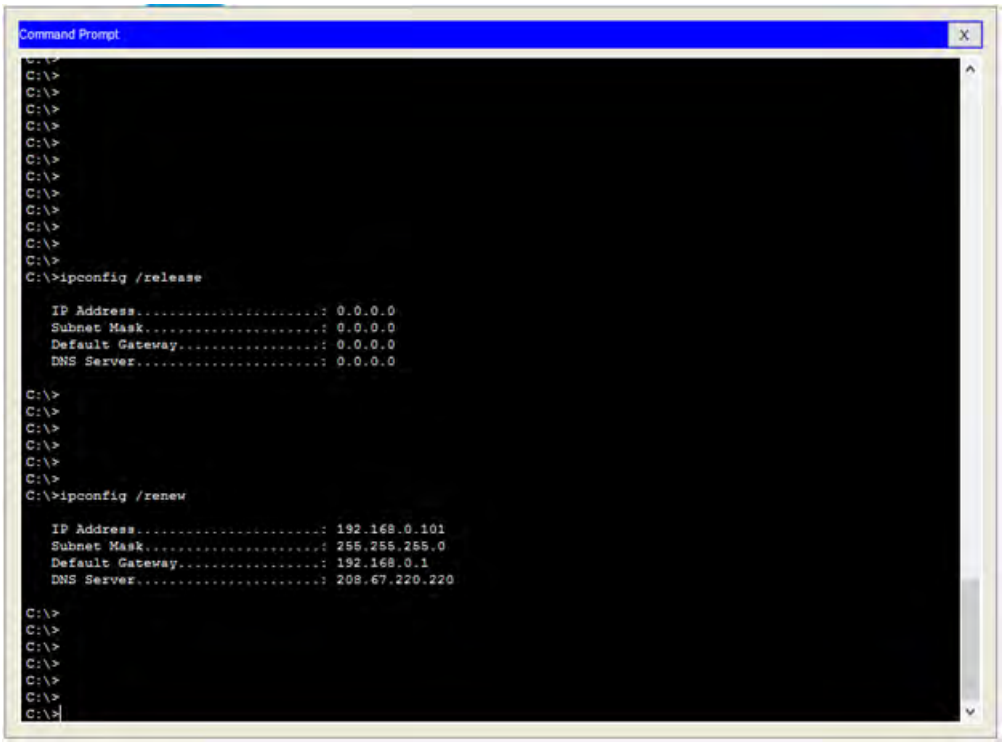


Figure 4.15:

b) Test connectivity to the Cisco.com server from the PC
From the command prompt, issue the command ping Cisco.com. It may take a few seconds for the ping to return. Four replies should be received as shown in the figure.

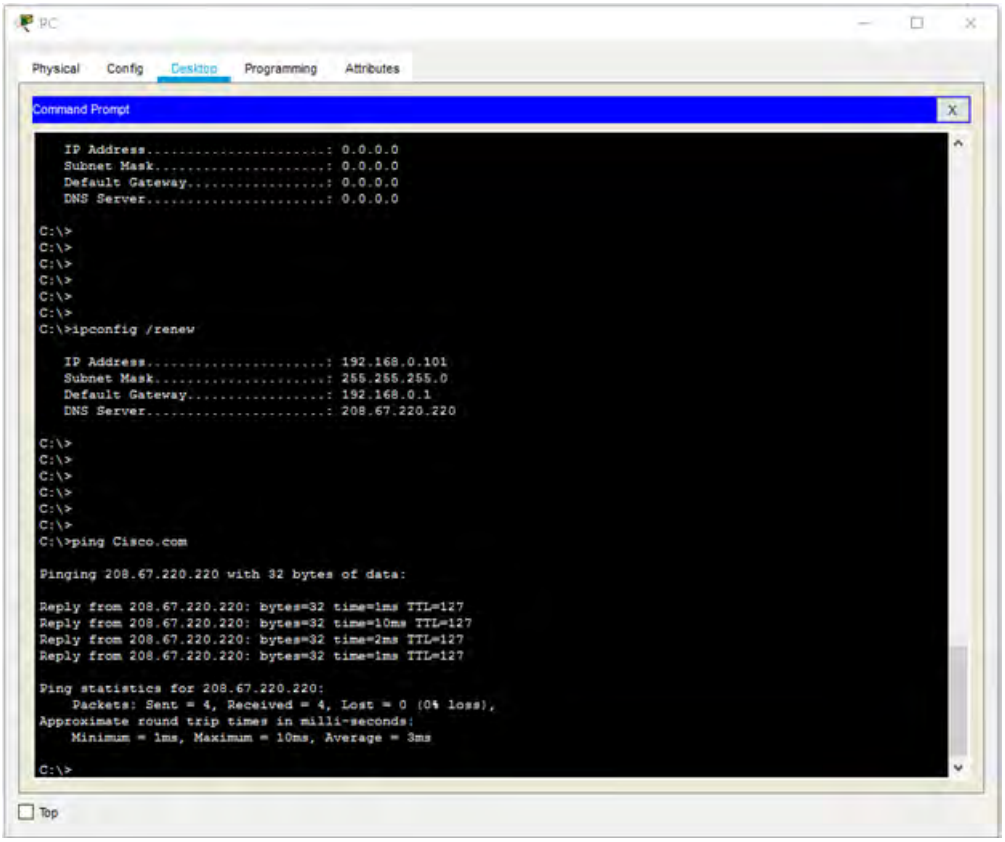


Figure 4.16:

Part 4: Save the File and Close Packet Tracer

Step 1: Save the File as a Packet Tracer Activity File (*.pkt)

To save the completed network, click on File in the Packet Tracer menu bar and then select Save A from the dropdown menu. In the the Save File window choose a directory to save the file to and give the file an appropriate file name. The Save as type defaults to Packet Tracer Activity File (*.pkt). Click Save to save the file.

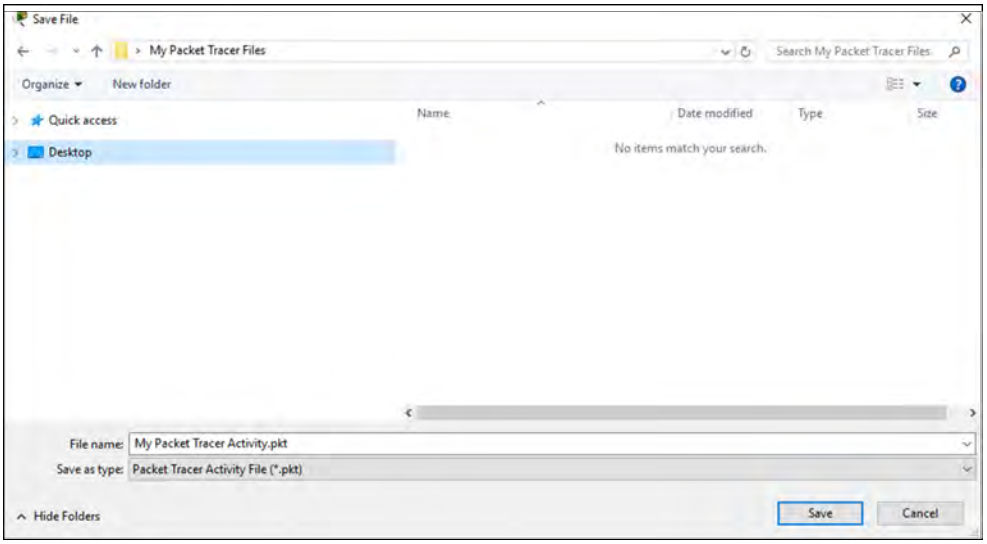


Figure 4.17:

Step 2: Close Packet Tracer

To close Packet Tracer you can either click the "X" in the top right corner of the Packet Tracer window or click on Exit in the file drop down menu.

Video — The Network Controller. Packet Tracer includes a simplified version of a Network Controller device. Network Controllers provide a centralized way to monitor and configure multiple compatible network devices from a single graphical user interface (GUI). You access the Network Controller interface by connecting a web browser to the IP address of the Network Controller management interface.

Video — Monitor Network Changes using a Network Controller. In Cisco Packet Tracer, a network controller can be used to monitor and manage network changes efficiently. Network controllers centralize the management of the network, allowing administrators to oversee network operations, apply configurations, and track changes across the entire network topology.

(Optional PKA 1): Create a Simple Network

Objectives

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

- Create a simple network by connecting a router, switch, and multiple end devices using appropriate cables and network hardware.
- Set up network settings on the end devices and test the connections to ensure they can communicate with each other and access the network.

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 network 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			
Laptop			

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.

The default gateway is analogous to the street intersection. The traffic from the 192.168.0 street has to exit through the intersection to another street. Another street is another network. In this network, default gateway is the wireless router that directs the traffic from the local network to the cable modem, and the traffic is then sent to the ISP.

(Optional PTA 2): Monitor Your Network using a Network Controller

Objectives

A network controller allows you to manage, monitor, and configure supported network devices via a graphical user interface (GUI) and APIs.

Note: The use of APIs is beyond the scope of this activity. For more information, review the API documents using the Help menu in Packet Tracer.

In this activity, you will set up a network controller to monitor a configured network via the GUI.

- Deploy a network controller by installing the necessary software or hardware and integrating it with the existing network infrastructure.
- Use the network controller to continuously monitor the network's performance, detect issues, and manage network resources effectively.

Part 1: Implement a Network Controller

Step 1: Connect a Network Controller to Office-SW1

a. While in the Wiring Closet, a previously configured Network Controller is located on the Shelf for your use. Move the Network Controller from the Shelf to the Rack and power on the Network Controller as necessary.

b. Right-click the Network Controller and click Inspect Rear to locate the `GigabitEthernet0` port. Connect the `GigabitEthernet0` port on the Network Controller to the `GigabitEthernet 1/0/19` port on Office-SW1 via a Copper Straight-Through cable.
The Network Controller has been previously assigned `192.168.20.5` as the IP address.

Step 2: Verify connectivity

a. To exit the Wiring Closet, click Back level (`Alt-Left`).

b. From Office-Admin, ping the Network Controller.

1. Click Office-Admin and select `Desktop > Command Prompt`.
2. At the prompt, enter `ipconfig` to verify that Office-Admin has received an IP address from the DHCP server. The IP address should be in the form of `192.168.20.x`, where `x` can range from 10 to 20.

```
C:\> ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:
Link-local IPv6 Address.........: FE80::20C:CFFF:FE46:E938
IPv6 Address....................: ::
IPv4 Address....................: 192.168.20.10
Subnet Mask.....................: 255.255.255.128
Default Gateway.................: ::
```

192.168.20.1

Note: If you did not receive an IP address, exit the Command Prompt and click IP Configuration. Verify that the PC is set to receive addressing information from DHCP.

3. At the prompt, enter `ping 192.168.20.5`. The pings should be successful.

```
C:\> ping 192.168.20.5

Pinging 192.168.20.5 with 32 bytes of data:

Reply from 192.168.20.5: bytes=32 time<1ms TTL=128
Reply from 192.168.20.5: bytes=32 time<1ms TTL=128
Reply from 192.168.20.5: bytes=32 time<1ms TTL=128
Reply from 192.168.20.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

If the pings are not successful, verify that the correct ports are used for the connection, and the Network Controller is powered on.

c. Exit the Command Prompt when finished.

Part 2: Monitor the Network

Step 1: Access the Network Controller via the GUI

a. From Office-Admin, open a web browser (click `Desktop > Web Browser`) and navigate to `192.168.20.5`.
b. When prompted to login, enter `admin` as the username and `Cisco123` as the password.
c. After you have logged in, you will be presented with the Dashboard view. When the Dashboard is refreshed, you will be provided information regarding the current state of the network. Explore the Dashboard menu located to the left of the Cisco logo.
Question: What menu items do you see?

Step 2: Document the network

Now that you have explored some of the features of the Network Controller, you will use the Note feature in Packet Tracer to document the network devices in the Office network.

a. In the Network Controller, navigate to the NETWORK DEVICE screen. (Click `Dashboard menu > Provisioning > NETWORK DEVICE`)
b. Click Place Note to document the network devices listed from the NETWORK DEVICE screen. Place the note in the white space next to the Office background. For example, this info should be part of the note:
`Office-SW1:  192.168.20.4`

Step 3: Discover new devices in the Office network

In this step, you will connect a wireless devices to the Office wireless network and observe the changes in the hosts listing.

a. From the web browser for Office-Admin, navigate to the Network Controller if necessary.
b. Navigate to the HOSTS screen. (Click `Dashboard menu > Assurance > HOSTS`). Note the host list.
c. Connect the Office Tablet and Smartphone to the wireless network. For each device, click the Config tab, select `Wireless0` in the left pane, and select ON for the Port Status. Verify

the devices receive an IP address from the DHCP server. The IP addresses will be from the 192.168.2.x /24 network, where x is ranged between 11 to 254. You can click Fast Forward Time (Alt + D) to speed up the process.

d. On the Network Controller, navigate to the DISCOVERY screen. (Click Dashboard menu > Provisioning > DISCOVERY) Select the already configured Discovery process named Office LAN. Click START to run the discovery process. When the discovery process is finished, the newly connected Office-Tablet and Smartphone are displayed in the Discovered Devices list.
e. Return to the HOSTS screen. Note the newly discovered hosts.
Question: What IP addresses are assigned to Office-Tablet and Smartphone?

(Optional PTA 3): Manage and Configure Your Network using a Network Controller

Objectives

In this activity, you will set up a network controller to monitor a configured network via the graphical user interface.

- Set up a network controller by installing it within the network environment and configuring it for optimal performance and management.
- Utilize the network controller to identify and catalog all connected devices within the network for easier management and monitoring.
- Integrate a new network device into the office network by connecting it physically, configuring its settings, and ensuring it is recognized by the network controller.

Part 1: Deploy a Network Controller

In this part, you will add a network controller to monitor the Office network.

Step 1: Connect a Network Controller to Office-SW1

a. In the Physical Mode, navigate, if necessary, to the simulated Wiring Closet (Equipment Cabinet) in the Office.
b. A new Network Controller is located on the Shelf for your use. Move the Network Controller from the Shelf to the Rack.
c. Connect the GigabitEthernet0 port on the Network Controller to the GigabitEthernet 1/0/19 port on Office-SW with a Copper Straight-Through cable.
d. Click the newly added Network Controller.
e. On the Physical tab, click the power button to turn on the Network Controller.
f. In the Config Window Global Settings, enter 192.168.20.1 as the IPv4 default gateway and 192.168.20.126 for the DNS Server.
g. In the left pane, click GigabitEthernet0. For the IPv4 Configuration, verify Static is selected. Enter 192.168.20.5 for IPv4 address and 255.255.255.128 for the subnet mask.

Step 2: Verify connectivity

a. From Laptop in the Wiring Closet, ping the interface of the Network Controller.
b. Click Laptop and select Desktop > Command Prompt.
c. At the prompt, enter ping 192.168.20.5. The pings should be successful.

```
C:\> ping 192.168.20.5
```

```
Pinging 192.168.20.5 with 32 bytes of data:

Reply from 192.168.20.5: bytes=32 time<1ms TTL=128
Reply from 192.168.20.5: bytes=32 time<1ms TTL=128
Reply from 192.168.20.5: bytes=32 time<1ms TTL=128
Reply from 192.168.20.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

If the pings are not successful, verify the IP addressing information has been entered correctly on the interface of the Network Controller.

Part 2: Device Discovery

In this part, you will configure a process on the network controller that will discover devices on the Office network.

Step 1: Access the Network Controller via the GUI

a. From Laptop, open a web browser (click `Desktop > Web Browser`) and navigate to `192.168.20.5`.
b. At the initial login screen, register a new user. Enter `admin` as the username and `Cisco123` as the password. Click `Setup` to continue.
c. Enter the credentials that you have just created to login as the new user.
d. After you have logged in, you will be presented with the Dashboard view. Maximize the browser window to see the full dashboard.

Step 2: Create the Credentials list

For the controller to discover devices on the network, it must know the credentials to use to access the devices. You must create a credentials list that will enable the controller to access the devices. Note that these credentials were configured previously on these devices.

a. Click `Dashboard > Provisioning > CREDENTIALS` to add a new credentials list for discovering the devices on the network.
b. Click `+ CREDENTIAL`.
c. In the New Credential window, enter `student` as the Username, `StudentPass` as the password, and `Cisco123` as the Enable Password. For the Description, enter `Student Profile`. The Description will be needed to create the Discovery Process. Click `OKAY` to continue.

Step 3: Create a Discovery Process

a. Click the `Dashboard Menu`, click `Provisioning > DISCOVERY` to discover devices on the local network.
b. Click `+ DISCOVERY`.
c. In the New Discovery window, use CDP as the Discovery Type. Enter `Office - LAN` as the name of this process. Enter `0.0.0.0` as the IP address so the controller will discover all the IP addresses on the local network. Select `student - Student Profile` as the CLI Credential List. Leave all other values as the default. Click `ADD` to continue.
d. It will take a few minutes for the discovery process to finish.
e. Click `Office - LAN` in the Discoveries list to see all of the discovered devices. Float your mouse over the devices in the equipment rack and locate them in the list of discovered devices.

Question: Why do some devices have multiple entries in the list of Discovered Devices?

f. Navigate to the Dashboard to see all the conditions of the local network. Click the gear icon in each section of the interface to see relevant details.
g. Close the web browser. Leave the Laptop window open for the next part.

Part 3: Add a New Network Device to the Office Network

In this part, you will add a new switch to the Office network and observe the changes on the Dashboard of the Network Controller.

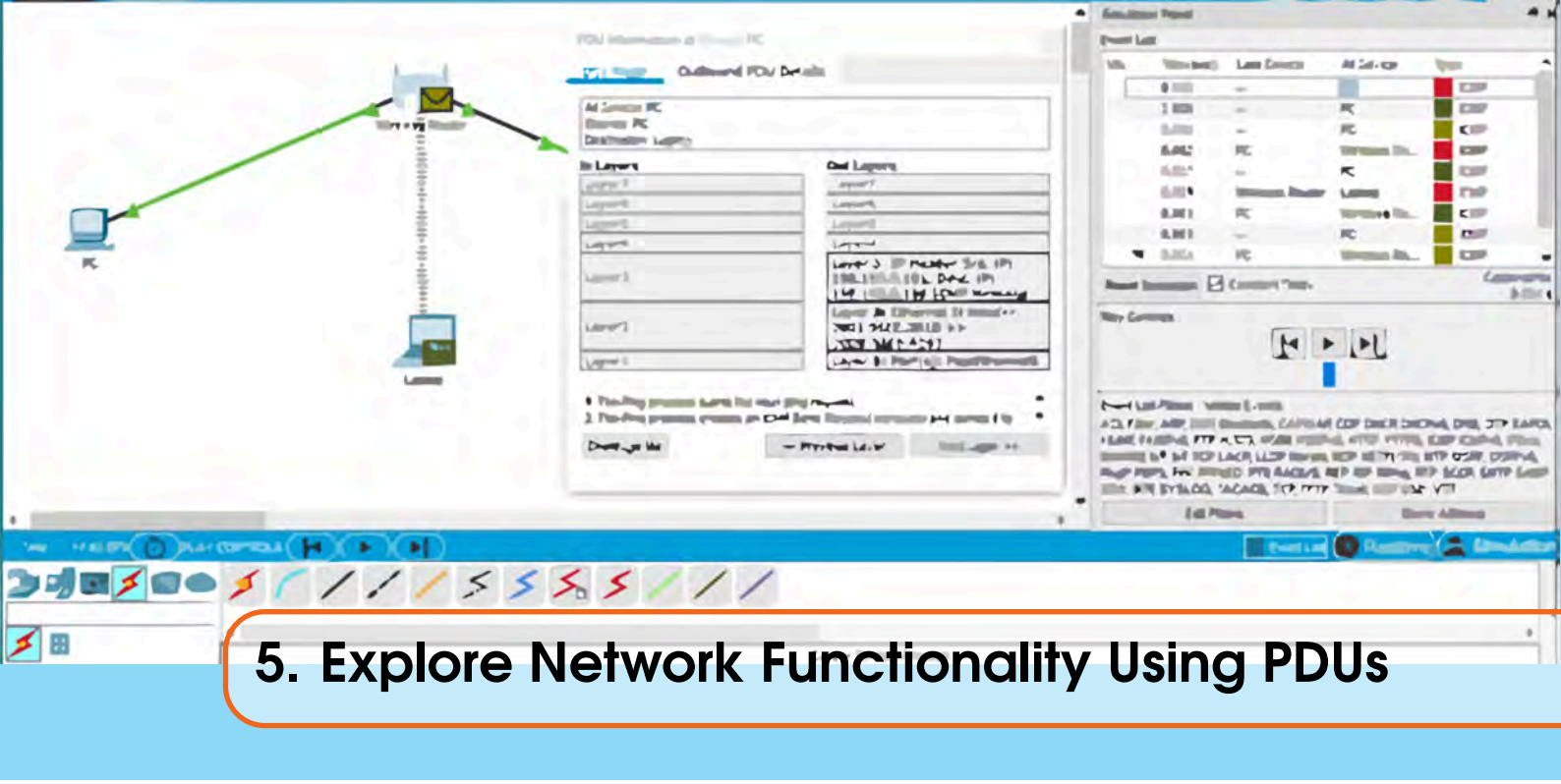
Step 1: Deploy a new switch on the network

a. Connect the `GigabitEthernet 0/1` port on Office-SW2 to `GigabitEthernet 1/0/5` on Office-SW using a Copper Straight-Through cable.
b. Click Laptop. Click `Desktop > Terminal`. Click `OK` to accept the defaults and access the CLI of Office-SW2.
c. Press Enter. Copy and paste the following commands into Office-SW2. These commands configure the Office-SW2 switch to operate on the network.

```
enable
configure terminal
hostname Office-SW2
interface vlan 20
ip address 192.168.20.7 255.255.255.128
no shut
enable secret Cisco123
username student privilege 1 password StudentPass
line vty 0 4
login local
interface range g0/1-2
switchport mode trunk
switchport trunk native vlan 20
interface range f0/1-24
switchport mode access
switchport access vlan 2
vlan 2
name UserNetwork
vlan 20
name Management
end
copy run start
```

Step 2: Review the network via the Network Controller

a. Log into the Network Controller via the web browser.
b. Click `Dashboard Menu > Provisioning > DISCOVERY`.
c. Open the list of devices on the `Office - LAN` that have been discovered by the controller. Verify that Office-SW2 is not in the list.
d. In the `Office LAN Discovery`, click `START` to start the discovery process manually. It will take a few minutes for the discovery process to finish.
e. Click the `Office LAN` to see all the discovered devices or navigate to the Dashboard to see all the conditions of the local network. Verify that the Office-SW2 switch is now present in the list of discovered devices.



5. Explore Network Functionality Using PDUs

Objectives

- Investigate network functionality using Packet Tracer's simulation mode by creating and capturing Protocol Data Units (PDUs) to evaluate basic connectivity and security.
- Create simple PDUs to replicate network functionality and use them for troubleshooting and testing purposes.
- View the contents of PDUs using various methods to understand the OSI model layers and the mechanisms of communication within a network.
- Create complex PDUs in simulation mode using advanced protocol settings to simulate and analyze more detailed network scenarios .

Lab Plan

In this lab, you will learn how to explore network functionality using Packet Tracer's simulation mode. You will practice creating and capturing Protocol Data Units (PDUs) to evaluate network connectivity, security, and services. Additionally, you will analyze the contents of PDUs and create complex PDUs for detailed network scenarios.

Creating PDUs in Simulation Mode

Packet Tracer provides a Simulation mode that allows you to create and capture PDUs to check several functions within your network, such as:

- Basic Connectivity – Can all devices communicate with each other?
- Security – Are access lists functioning as designed?
- Applications and Services – Are applications and services such as DNS, HTTP, and FTP functioning as designed?

The default mode for Packet Tracer is Realtime mode. In Realtime mode the time is continuously running as indicated by the clock in the lower right hand corner of the worksheet. In Simulation mode, time can be stopped or slowed to allow users to view data traffic one packet at a time. Simulation mode is used to observe network traffic in detail with time controlled directly by the

user.

Video — Network Simulation Mode. Network Simulation Mode in Cisco Packet Tracer allows users to simulate network operations, providing a dynamic environment to observe and analyze network behavior, troubleshoot issues, and understand data flow. This mode is essential for testing and verifying network configurations without the need for physical hardware.

Video — Creating PDUs in Simulation Mode. This is our CISCO Packet Tracer: Creating PDUs in Simulation Mode video. What does that mean? That means we are going to be creating messages that will move between devices in this network. We're going to be able to open up those messages and even view them. Check the video to see how to use Simulation mode to create simple PDUs to replicate ICMP and ARP functionality and how to create more complex PDUs from a list of protocols such as DNS, HTTP, Telnet, SSH, FTP, and many more.

Viewing the Contents of PDUs

Once the PDUs have been captured, you have several ways to view their contents. Viewing the contents of the PDUs can be used to verify connectivity, verify functionality, and troubleshoot issues. It is also a great tool for studying or reviewing the contents of the OSI model layers and the mechanisms of communication.

If viewed in OSI Model mode, you see a summary of the addresses and contents of the headers at each layer. If you select Inbound or Outbound PDU Details, the exact format of the appropriate headers is displayed.

Video — Viewing the Contents of PDUs. This is our Cisco Packet Tracer viewing the contents of PDUs, which are protocol data units, walkthrough video. In this video we're going to go through and watch the actual movement of data from source to one destination, and we're going to take a look inside the PDU information as the traffic moves.

Topology

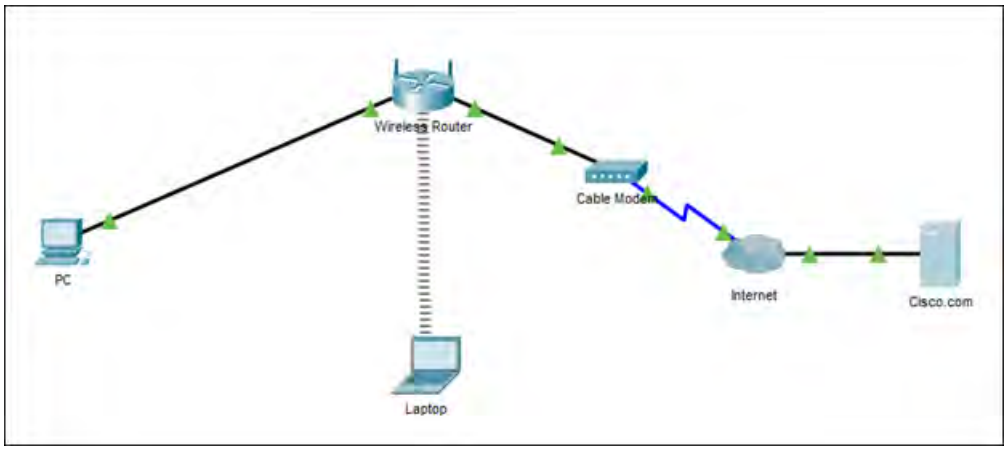


Figure 5.1:

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC	Ethernet0	DHCP		192.168.0.1
Wireless Router	LAN	192.168.0.1	255.255.255.0	
Wireless Router	Internet	DHCP		
Cisco.com Server	Ethernet0	208.67.220.220	255.255.255.0	
Laptop	Wireless0	DHCP		

Objectives

- Part 1: Create a Simple PDU in Simulation Mode
- Part 2: View Contents of PDUs
- Part 3: Create a Complex PDU in Simulation Mode

Background / Scenario

In this activity, you will open the saved Packet Tracer activity that was completed in Chapter 2 and use the Simulation mode to create PDUs to explore network functionality.

Part 1: Create a Simple PDU in Simulation Mode

Step 1: Open the .pka activity

a) Navigate to the .pka activity that was completed in Chapter 2.
Navigate to the directory that contains the Packet Tracer Activity that was completed in Chapter 2. Open the activity and click the Simulation mode icon in the bottom-right corner of the Packet Tracer window to open the Simulation panel.

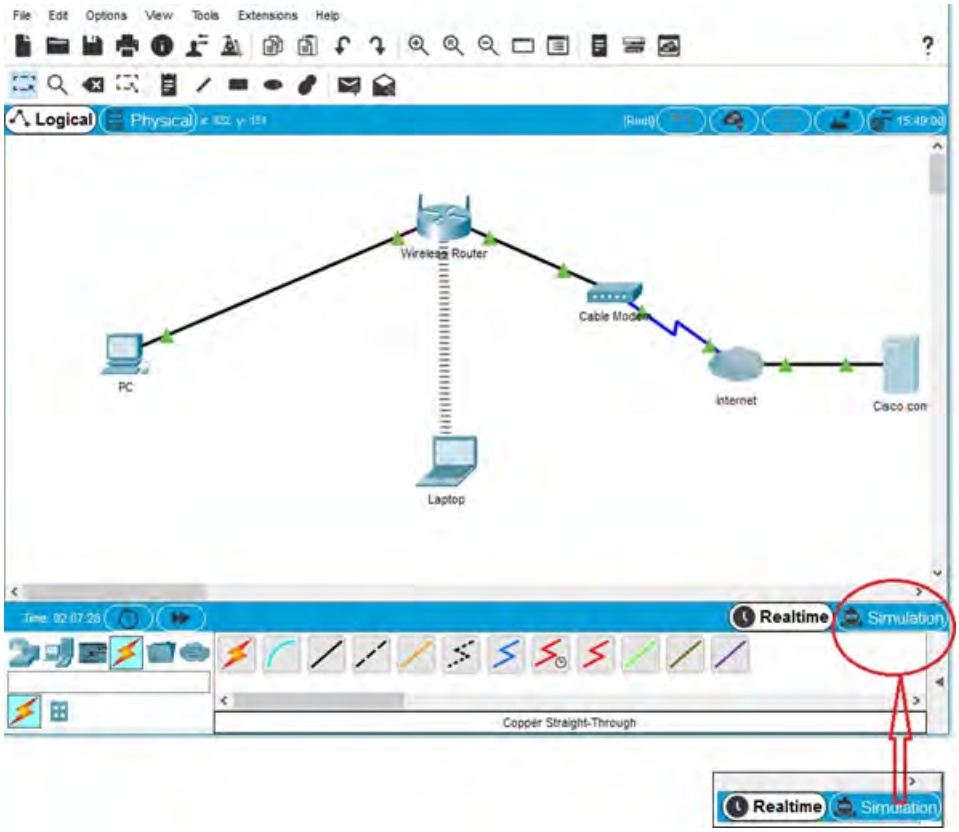


Figure 5.2:

Step 2: Create a simple PDU.

a) Create a simple PDU that sends a ping from the PC to the laptop
Click the Add Simple PDU icon (looks like a closed envelope) in the top pane of the Packet Tracer window. The curser will change to an envelope with a plus sign. Click the PC first so that it will become the source of the ping and then click the Laptop so that it will become the destination.
Expand the Event Simulation pane by clicking the gray arrow at the bottom right of the Packet Tracer Window.

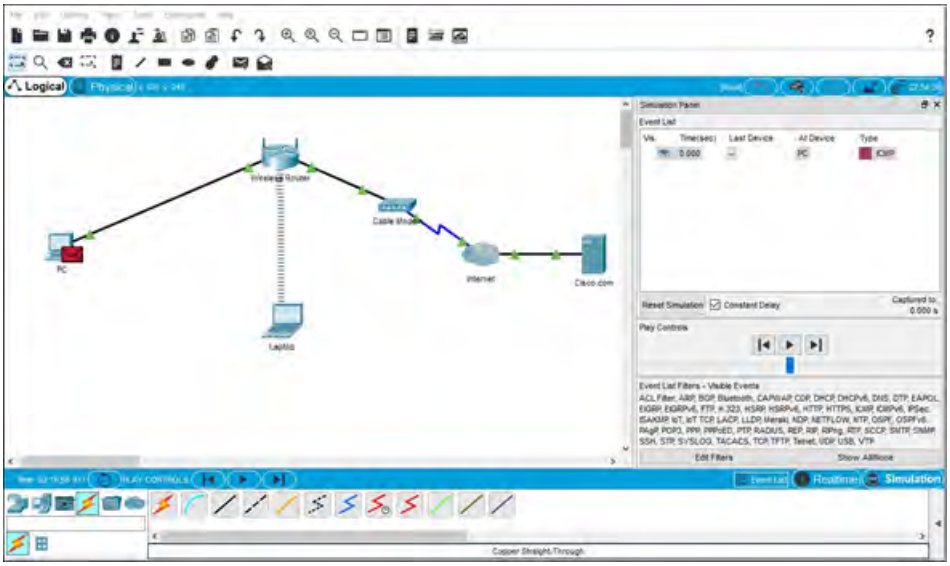
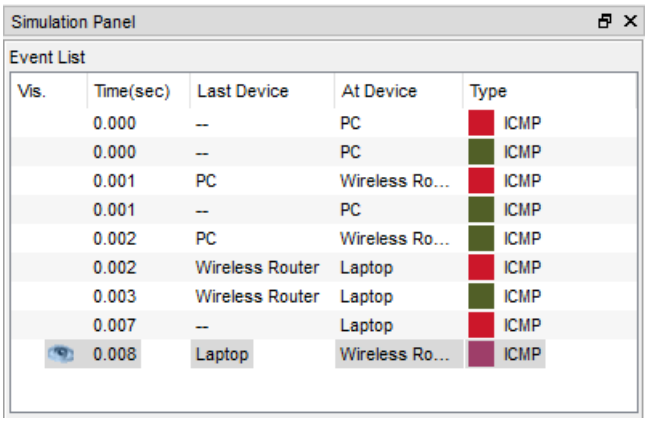


Figure 5.3:

b) Observe traffic moving through the network.
Click the Capture/Forward button and observe the traffic move through the network each time the button is clicked. Notice also that each time the Capture/Forward button is clicked, sent packets are displayed in the Event List window. Continue clicking the Capture/Forward button until the return ICMP packet makes it back to the PC.



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC	ICMP
	0.000	--	PC	ICMP
	0.001	PC	Wireless Ro...	ICMP
	0.001	--	PC	ICMP
	0.002	PC	Wireless Ro...	ICMP
	0.002	Wireless Router	Laptop	ICMP
	0.003	Wireless Router	Laptop	ICMP
	0.007	--	Laptop	ICMP
	0.008	Laptop	Wireless Ro...	ICMP

Figure 5.4:

Part 2: View Contents of PDUs

Step 1: Use event list to see PDU information

a) View the information of the first ICMP PDU packet from the PC.
In the Event List window, click the green square under the Type column for the first ICMP PDU at the top of the list. This will open the PDU Information at Device: PC window.

Figure 5.5:

Observe the information in the OSI Model tab. Notice that this is an outbound Layer 3 PDU and the source and destination IPv4 address is shown.

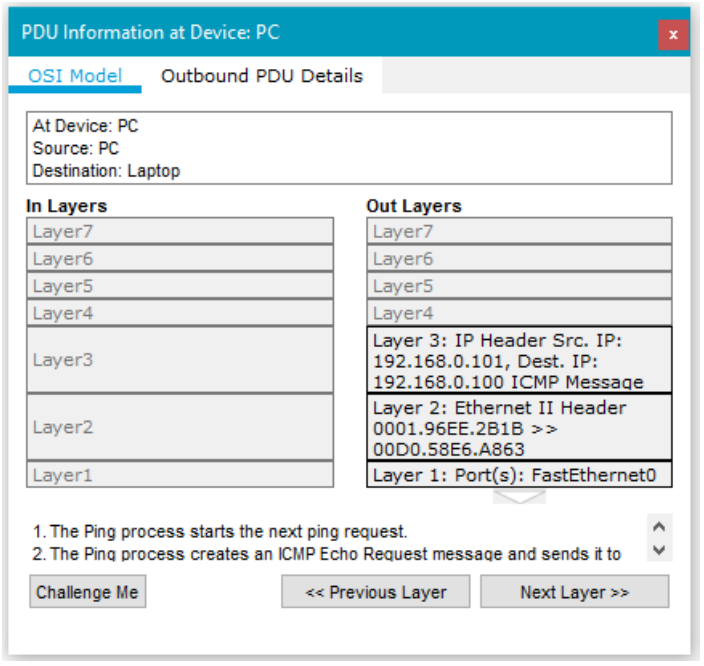


Figure 5.6:

Next, click the Outbound PDU Details tab. Notice that this tab shows details of the protocol headers.

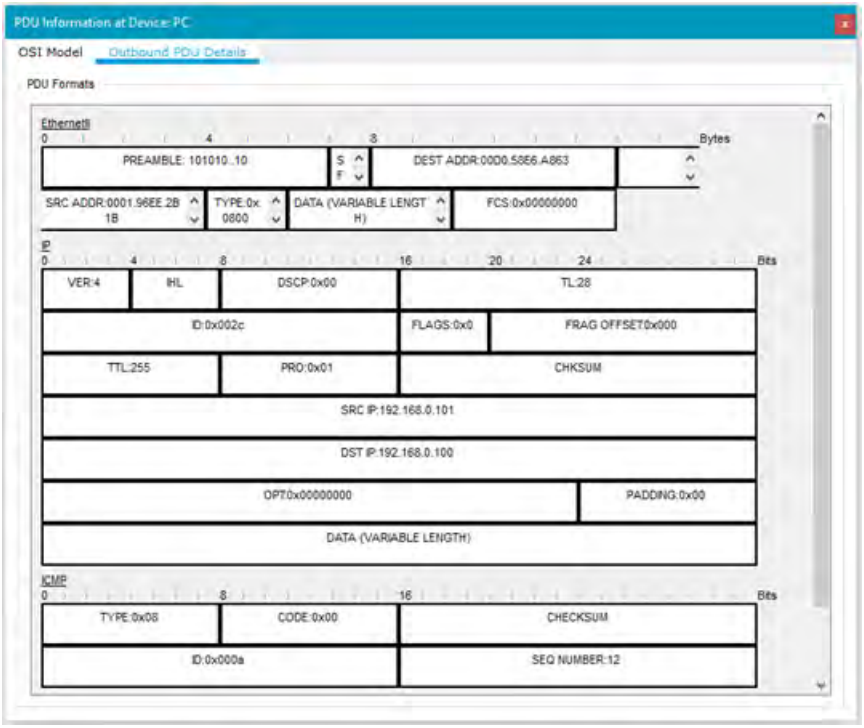


Figure 5.7:

b) Explore the contents of other PDUs that are listed in the Simulation panel and review the information that is available in each.

Step 2: Delete the simple PDU

a) Delete the simple PDU using the Event Simulation pane.
Click the Delete button in the Event Simulation pane at the bottom of the Packet Tracer window. Notice that this removes the simple PDU and clears out all PDUs from the Simulation Panel Event List.

Part 3: Create a Complex PDU in Simulation Mode

Step 1: Create a complex PDU

a) Add a complex PDU to send pings from the PC to the laptop.
Click the Add Complex PDU icon, the one that looks like an open envelope, in the right pane of the Packet Tracer window. The curser will change to an envelope with a plus sign. Click the PC first so that it will be the source device of the pings and then click the laptop so that it will be the destination.
The Create Complex PDU window will display.

b) Configure complex PDU settings to send the pings every 5 seconds.
In the Create Complex PDU window, there are many settings which can be customized. To send a ping every 5 seconds from the PC to the laptop, the Destination IP Address field must have the IPv4 address of the laptop, `192.168.0.100`. The Source IP Address field should be the IP address of the PC, `192.168.0.101`. At the bottom in the Simulation Settings section click Periodic and set the Interval to 5 seconds.

c) Observe traffic moving through the network.
Click the Auto Capture / Play button and watch the traffic move through the network and notice the PDUs populating the Simulation Panel Event List. Because we set the complex PDU to an Interval of 5 seconds, a new PDU will be created every 5 seconds. Click the Auto

Capture / Play button again to stop the simulation.
To delete the complex PDU, click the Delete button in the Event Simulation pane at the bottom of the Packet Tracer window.

(Optional PTA 1): Examine Packets in a Office

Objectives

In this Packet Tracer activity, you will use the Simulation mode to create PDUs to explore network functionality.

Note: Simulation mode does not work in Physical mode; therefore, Physical mode is locked.

- Generate a simple Protocol Data Unit (PDU) in simulation mode to observe basic network communication and data transfer processes.
- Examine the contents of PDUs to understand the data structure, headers, and payloads being transmitted across the network.
- Develop a complex PDU in simulation mode to analyze more intricate network interactions and detailed data exchange scenarios.

Part 1: Create a Simple PDU in Simulation Mode

Step 1: Enter the Office network

Click Office to view the logical network for the Office.

Step 2: Enter Simulation mode

Click the Simulation mode icon in the bottom-right corner of the Packet Tracer window to open the Simulation panel. This pauses all network traffic that occurs in Realtime mode.

Note: A pop-up window will open stating "Intercity is locked." Click on the okay tab in the window to close it. You will need to do this before continuing. You can center the Packet Tracer by scrolling the bar at the bottom of the Packet Tracer activity area.

Step 3: Create a simple PDU that sends a ping from Office-Admin to Printer0

a. Click Add Simple PDU in the top toolbar. It looks like a closed envelope. The cursor will change to an envelope with a plus sign when you move the cursor into the Packet Tracer activity area.
b. Click Office-Admin first so that it will become the source of the ping, and then click Printer0 so that it will become the destination.

Step 4: Observe traffic moving through the network

a. In the Play Controls area of the Simulation Panel, directly below the Reset Simulation button, click Capture/Forward, which is the button directly to the right of the Play button.
b. Observe the traffic move through the network each time the button is clicked. Notice also that each time Capture/Forward is clicked, sent packets are displayed in the Event List in the Simulation Panel.
c. Continue clicking Capture/Forward until the return ICMP packet makes it back to Office-Admin. Continue clicking on the Capture/Forward button quickly several times until you get a pop-up window that states "Buffer Full-Cisco Packet Tracer".
d. When the Buffer Full message pops up, click View Previous Events. If you accidentally click Clear Event List, click Reset Simulation and return to the beginning of this step.

Part 2: View Contents of PDUs

Step 1: Use the event list to see PDU information

View the information of the first ICMP PDU packet from the PC.

a. In the Event List window, find the Type column. You may need to expand the width of the Simulation Panel. To do so, click and drag the vertical bar on the left of the window.
b. In the Type column, click the first ICMP packet. This will open the PDU Information at Device: Office-Admin window.
c. Observe the information in the OSI Model tab. Notice that this is an outbound Layer 3 PDU and the source and destination IPv4 addresses are shown.
d. Click the Outbound PDU Details tab. Notice that this tab shows details of the protocol headers.
e. Close the PDU Information at Device: Office-Admin window.
f. Explore the contents of other PDUs that are listed in the Simulation Panel and review the information that is available in each.

Step 2: Delete the simple PDU

Double click the Delete button in the Event Simulation pane at the bottom of the Packet Tracer window. Notice that this removes the simple PDU and clears out all PDUs from the Event List in the Simulation Panel.

Part 3: Create a Complex PDU in Simulation Mode

Step 1: Add a complex PDU to send pings from the PC to the laptop

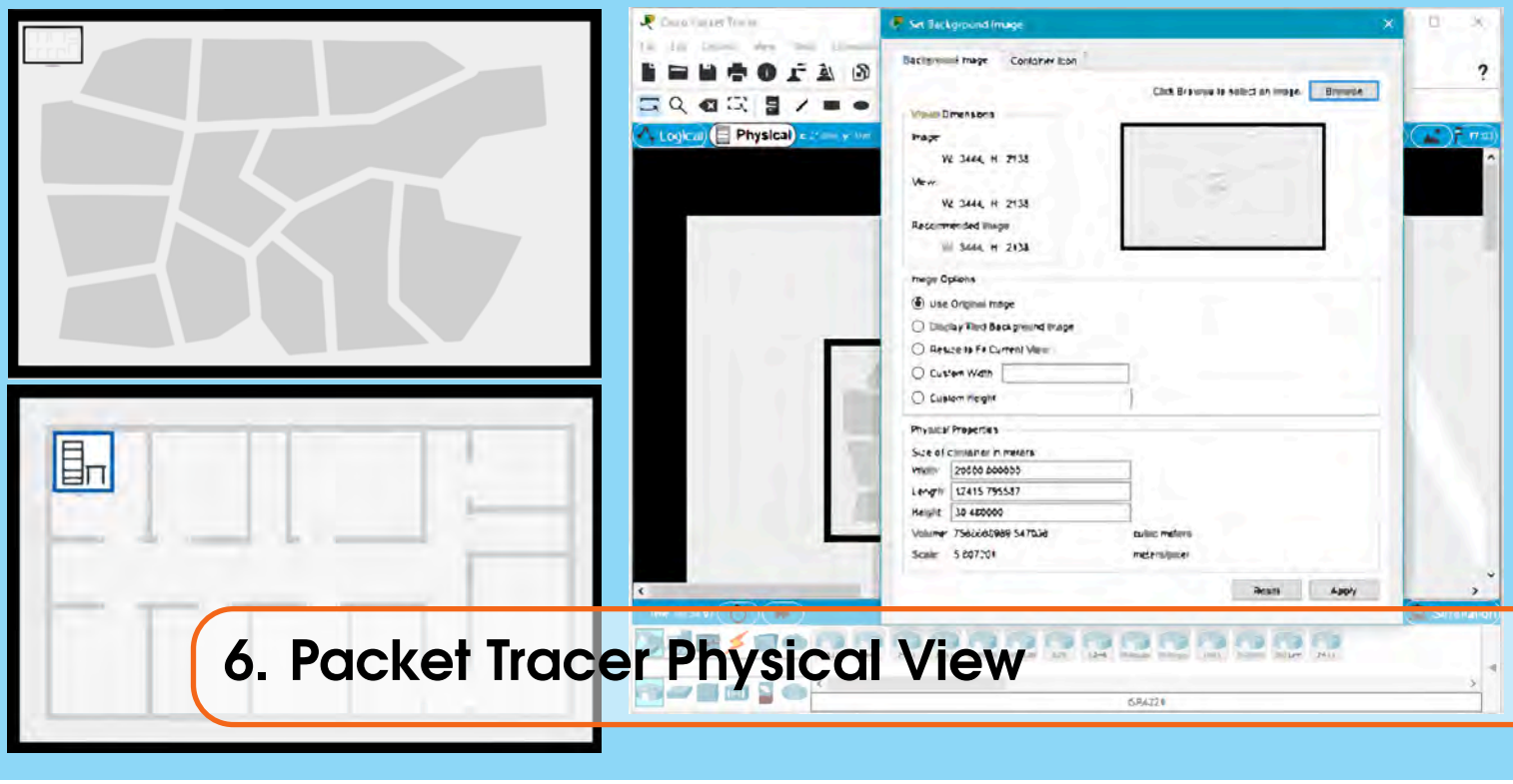
a. Click Add Complex PDU in the top toolbar. It looks like an open envelope.
b. Click Office-Admin first so that it will become the source of the ping. The Create Complex PDU window will display. Leave this window open.
c. Click Printer0 so that it will become the destination. Notice that the Destination IP Address field in the Create Complex PDU window is now set to the IPv4 address for Printer0. You can see the IPv4 address for Printer0 by hovering the pointer over it.

Step 2: Configure complex PDU settings to send the pings every 5 seconds

a. In the Create Complex PDU window, there are many settings which can be customized. Notice that PING is automatically selected as the application for this PDU.
b. The Sequence Number field must be populated with a value. Enter `1234`.
c. In the Simulation Settings section, click Periodic, and then set the Interval to 5 seconds.
d. Click Create PDU. The first `ICMP` packet is now shown in the Event List and a packet icon is shown over Office-Admin.

Step 3: Observe traffic moving through the network

a. Click Play in the Simulation Panel and watch the traffic move through the network. Notice the PDUs populating the Event List. in the Simulation Panel. A new PDU is created every 5 seconds.
b. Directly below the Play button is a slider. You can drag this right to speed up the animation or left to slow it down.
c. Click Play at any time to stop the simulation.
d. To delete the complex PDU, double click Delete in the Event Simulation pane at the bottom of the Packet Tracer window.



6. Packet Tracer Physical View

Objectives

- Explore the physical view in Packet Tracer to enhance understanding of network topology layout within a physical context.
- Navigate and customize the physical workspace, adding cities, corporate offices, and wiring closets to simulate realistic network environments.
- Use the physical view to simulate wireless coverage areas based on equipment placement, aiding in network design and visualization.
- Learn about different Packet Tracer file and assessment types, including .pkt, .pkz, .pka files, and their specific uses in networking education and evaluation.

Packet Tracer Usage

In this section, you are introduced to the Physical view. This mode allows you to place a logical network topology into a physical context. Packet Tracer creates various file types. The file types are introduced in this section and we also discuss how Packet Tracer is used as an assessment tool. At the completion of this section, you should be able to:

- Investigate the Packet Tracer Physical view.
- Explain Packet Tracer File and Assessment types.

The Packet Tracer Physical View

Now that you know the purpose and the use of the menus in the logical workspace, we will move on to learn about the physical workspace in Packet Tracer. The default view for Packet Tracer is Logical, which is equivalent to creating a logical diagram for the network. The other type of diagram used in networking is the physical diagram which not only shows the relationships of the network devices but also applies building and distance factors in making the design.

Packet Tracer has the physical workspace that allows you to make your network more realistic by adding backgrounds, buildings, and wiring closets. These features are important for documentation,

design, and visualization. You can see the actual layout of the network within a room or a building. This provides valuable information into the flow of traffic and the suitability and placement of equipment. The Physical view also has a great feature that shows the wireless coverage areas based on your equipment placement within buildings.

In this section, you will learn to:

- Navigate the physical workspace.
- Add cities, corporate offices, and branch offices.
- Add backgrounds into the cities and offices.
- Add wiring closets to the offices.
- Place networking devices into racks within the closets.

When the Physical view is shown, the basic organizational scheme is the following:

1. intercity
2. city
3. building
4. wiring closet

A user is able to add as many cities, buildings, and wiring closets as they need; however, there can only be one intercity. Containers of smaller sizes can be added at any level but larger containers cannot be added into smaller containers. For example, a building can be added to the intercity, but a city cannot be added to a building, and a building cannot be added to a wiring closet.

Video — The Packet Tracer Physical View. This is our Cisco Packet Tracer Physical View walkthrough video. So far we've always been in logical view, and the logical view over here with this logical view button and all we've been building is cabling and rolling out network devices. Watch this video to learn how to use the features of the physical workspace.

Video — Topology Overview. Creating a topology overview in Cisco Packet Tracer provides a visual representation of the network layout, including the arrangement and connections between various network devices. This helps in understanding the network structure and is crucial for planning, configuring, and troubleshooting the network.

Video — Structured Cabling. Structured cabling is an organized approach to the cabling infrastructure. In networking, you will want to manage your cables so that your workspace is more organized. In Packet Tracer Physical mode, you can organize the cables so that they are spanning across the entire room. You can use wall mounts, color-coded cables, and create bendpoints to organize your network cabling in a realistic way.

Video — Customize Background. Customizing the background in Cisco Packet Tracer allows you to add a personalized touch to your network design environment. This can include adding custom images, floor plans, or specific layout designs to the workspace, making it easier to visualize and organize your network components.

Video — Customize Device Icons. Customizing device icons in Cisco Packet Tracer allows you to personalize your network topology by changing the appearance of network devices. This can help in better visualization and identification of different devices within your network design.

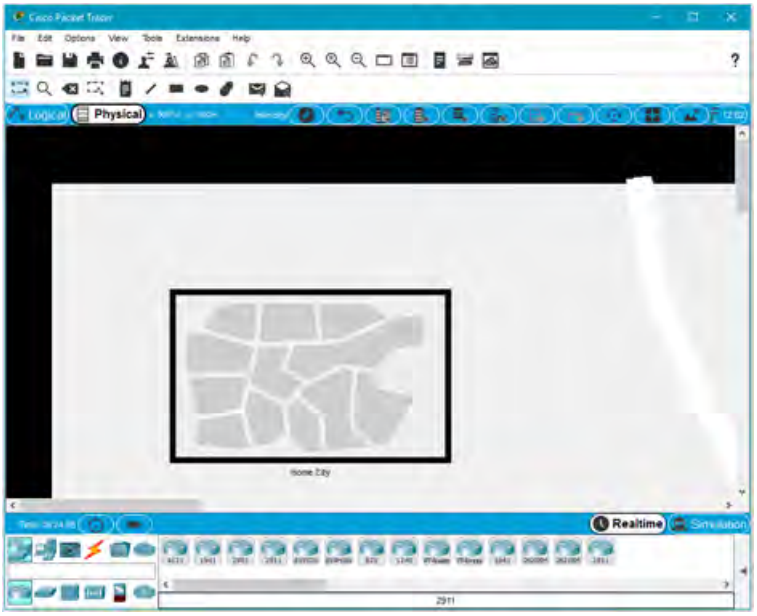


Figure 6.1:

Objectives

- Step 1 - Open the Physical View of Packet Tracer
- Step 2 - Apply a Physical View Background Image
- Step 3 - Edit and Move Between Containers
- Step 4 - Add Devices to a Wiring Closet
- Step 5 – Experiment

Background / Scenario

In this activity, you will use the Physical view of Packet Tracer to add backgrounds, containers, and network devices.

Step 1: Open the Physical View of Packet Tracer

a) Launch Packet Tracer.
When Packet Tracer opens, the default view is the Logical view.

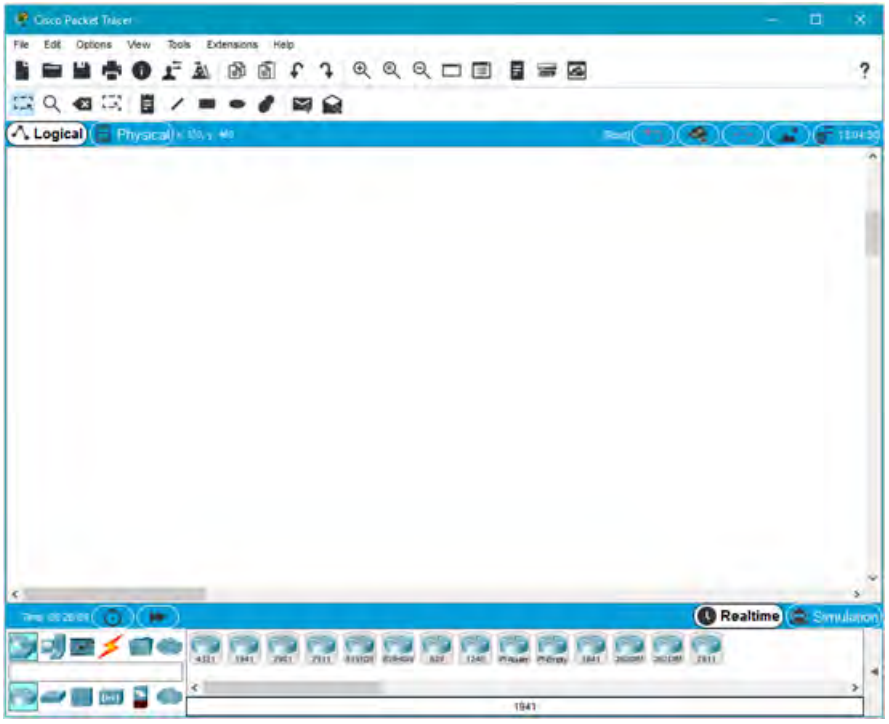


Figure 6.2:

b) Change to the Physical view. Click the Physical view button to change to the Physical view. The Physical view button is after the Logical view button in the top left portion of the workspace.

Figure 6.3:

The default Physical view is the Intercity.

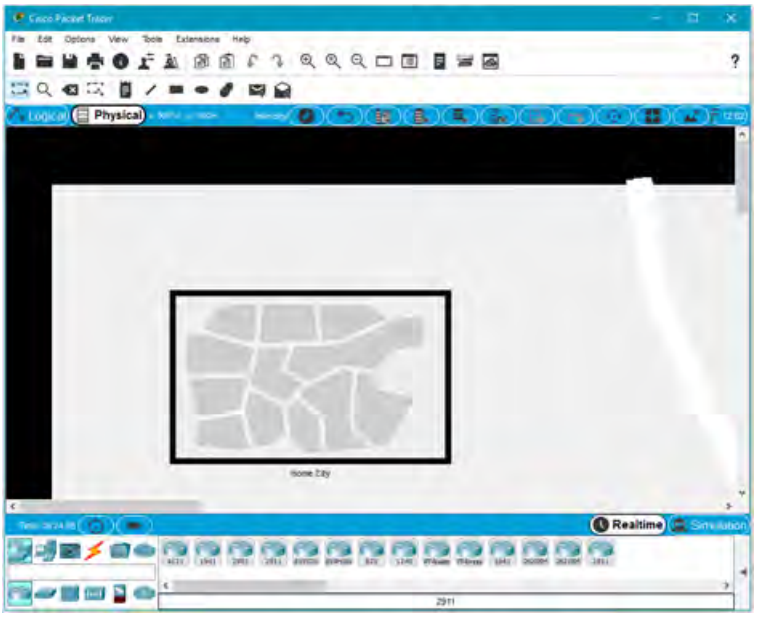


Figure 6.4:

Step 2: Apply a Physical View Background Image

a) Download the estate image from pixabay.
Navigate to the pixabay web site at https://pixabay.com and type world map into the All images search window. Click a map image in the result and save the image.
b) Load the saved image into Packet Tracer.
Make sure that Intercity is selected in the Physical view tool bar.

Figure 6.5:

Click Set Background at the top of the Packet Tracer window and in the Set Background Image window, click the Browse button to navigate to the saved image. Select the image and then click Apply. Close the Set Background Image window.

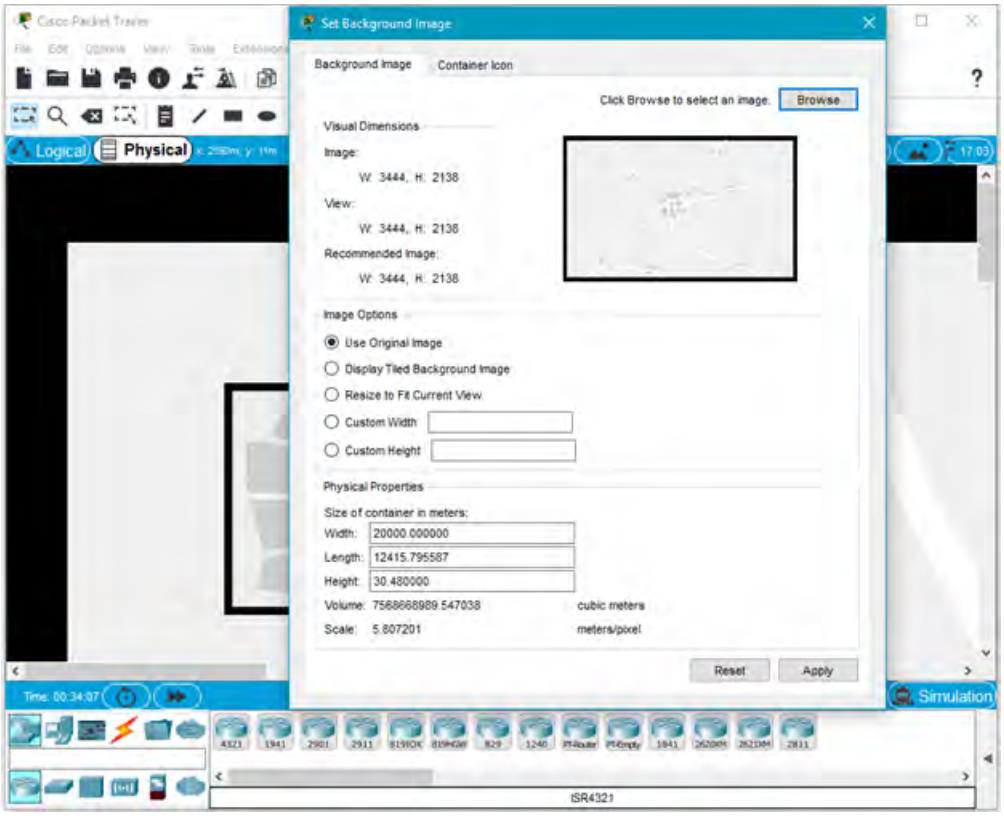


Figure 6.6:

After you click Apply, the image is saved as the Physical view background.

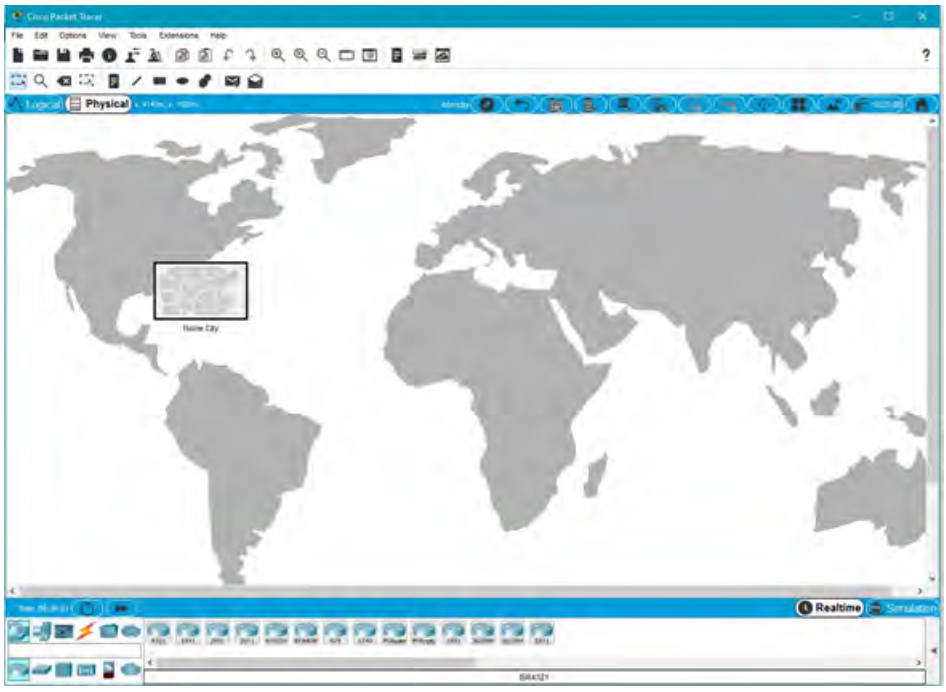


Figure 6.7:

Step 3: Edit and Move Between Containers

a) Relocate the Home City.
In the Intercity view is a Home City container. The Home City container can be moved to any location in the Physical view.
Click and drag the Home City container to any place on the world map background.

b) Apply a background image to the Home City.
Click the Home City container. Notice that the view changes and what is on the workspace now is the default Home City background. Zoom out by clicking the magnifying glass with the minus sign so that the whole background is visible.

c) Repeat Step 2 to download a city image from https://pixabay.com and apply it to the Home City background.

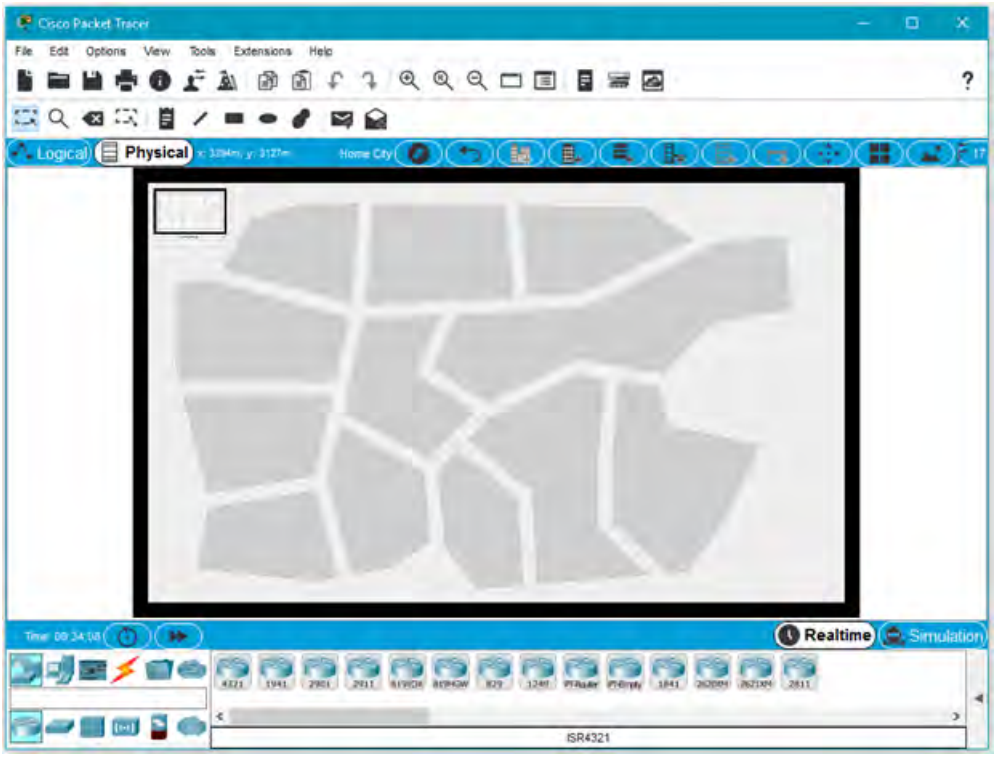


Figure 6.8:

Navigate to the pixabay web site at https://pixabay.com and type city image into the All images search window. Click a map image in the result and save the image.
Click Set Background at the top of the Packet Tracer window and in the Set Background Image window, click the Browse button to navigate to the saved image. Select the image and then click Apply. Close the Set Background Image window.
You may need to zoom in and recenter the background so it is fully visible in the workspace.

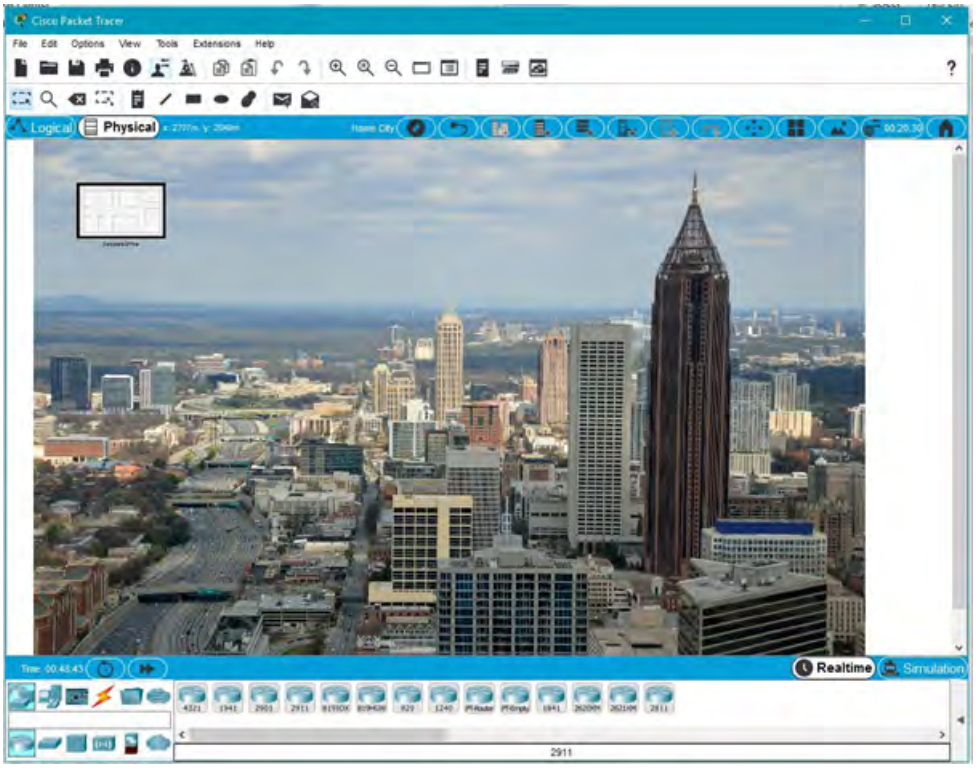


Figure 6.9:

If you click the Back menu item in the Physical view tool bar, you can see that the city background you applied is also now used on the Home City container in the Intercity view.

Figure 6.10:

Click the Home City text and change the name of the Home City container. In this example, the name is changed to Atlanta. This also changes the name of the Home City in the Physical view tool bar.

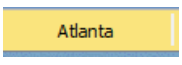


Figure 6.11:

Figure 6.12:

Click the Home City container to return to the Home City view.

Figure 6.13:

Step 4: Add Devices to a Wiring Closet

a) Enter the Corporate Office view.
There is a Corporate Office container on the Home City background.

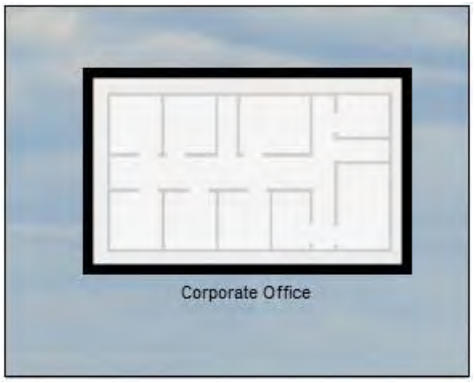


Figure 6.14:

Click the Corporate Office container and zoom out so that the default corporate office background is visible.

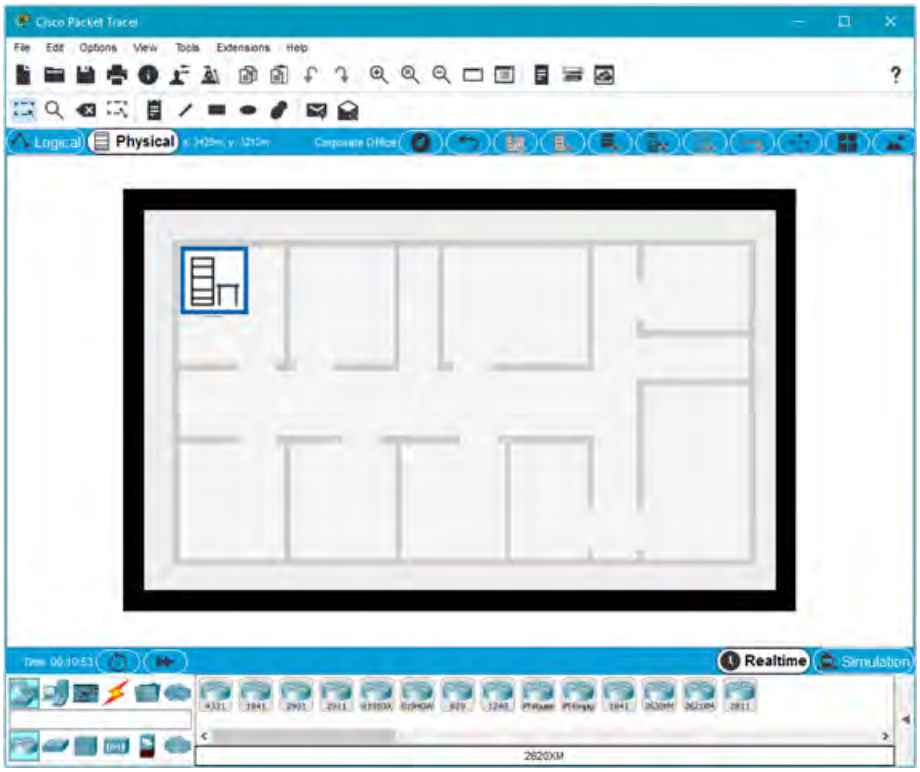


Figure 6.15:

The Corporate Office background includes another container called Main Wiring Closet. Click the Main Wiring Closet container.
The Main Wiring Closet container has a blank workspace.

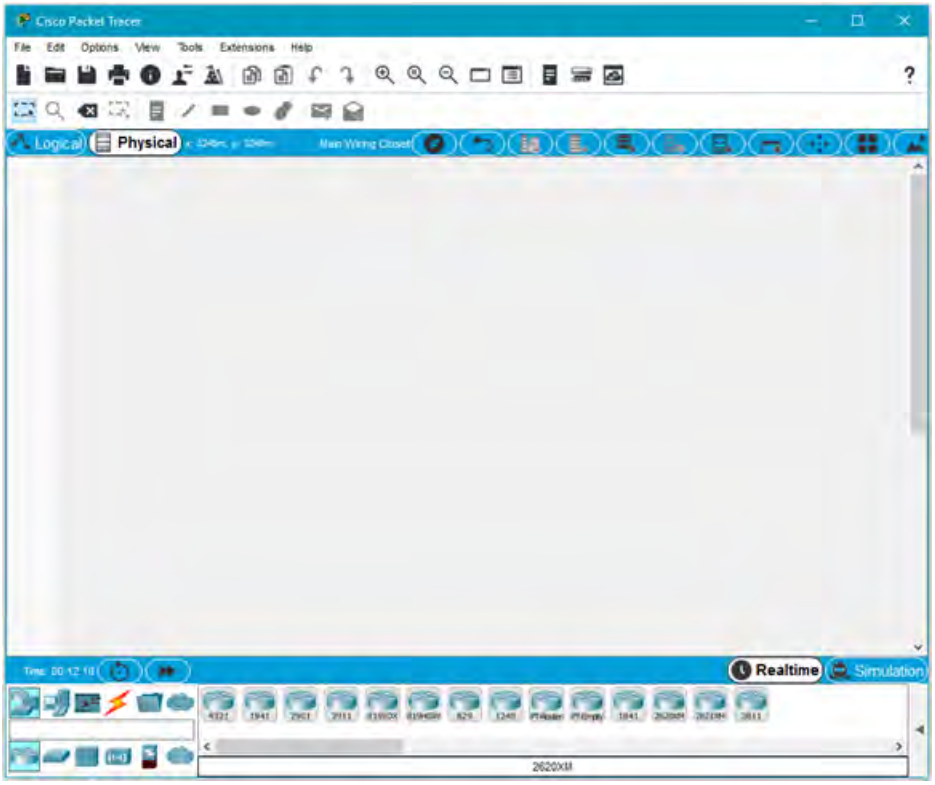


Figure 6.16:

b) Add devices to the Main Wiring Closet.
In the Main Wiring Closet view, add a router to the workspace just as you would in the Logical view by clicking a router in the device window and then clicking the workspace. Because we are in Physical view, Packet Tracer shows a rack with the router installed in the rack.

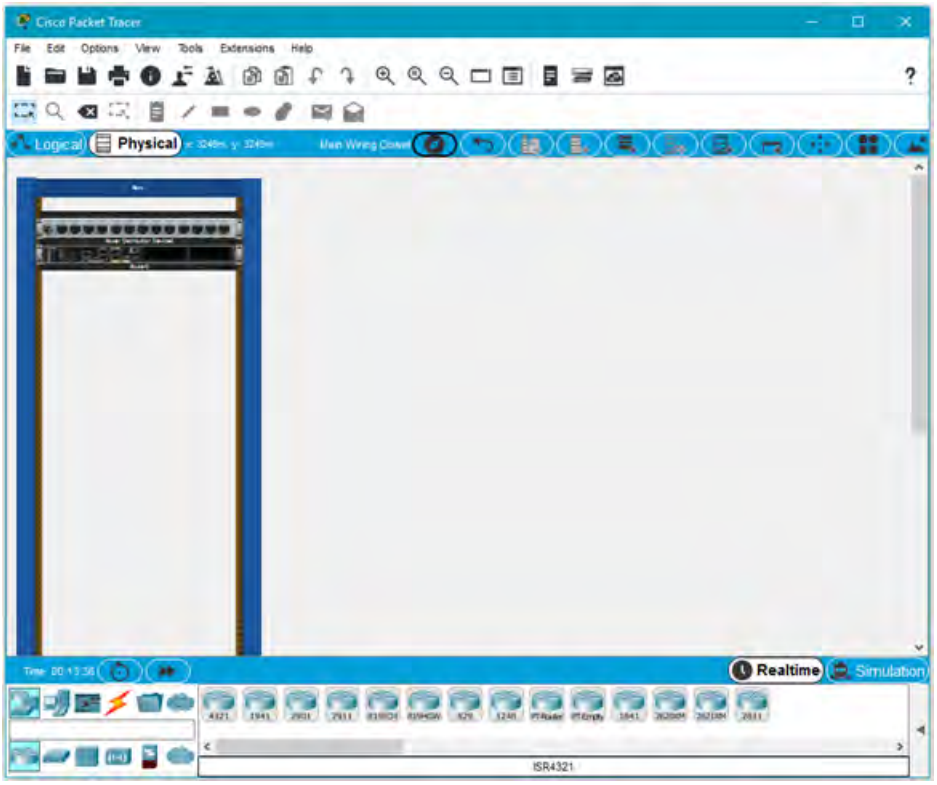


Figure 6.17:

c) Add more devices to the wiring closet.
Add a network switch, a generic server, and a cable modem to the wiring closet.

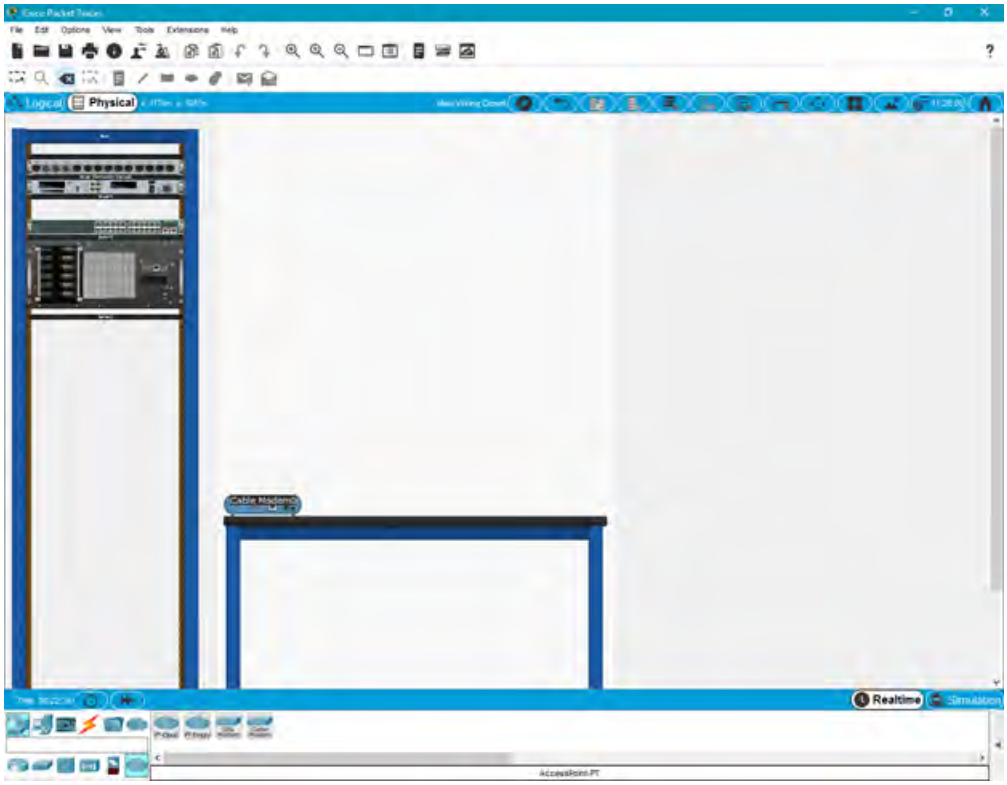


Figure 6.18:

d) Add cabling to the devices to the Main Wiring Closet.
To add cabling to the devices, switch back to the Logical view in Packet Tracer. You may need to zoom in and re-center the workspace to see the devices.
The devices are randomly placed in the Logical view workspace.

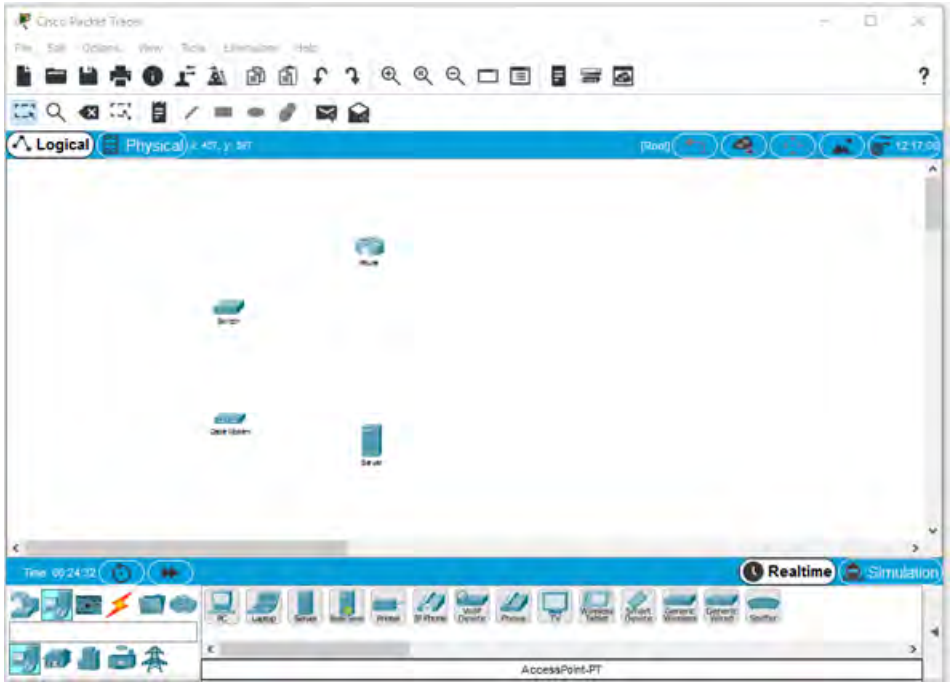


Figure 6.19:

Organize and connect the devices together using the appropriate cable types in the Logical view.

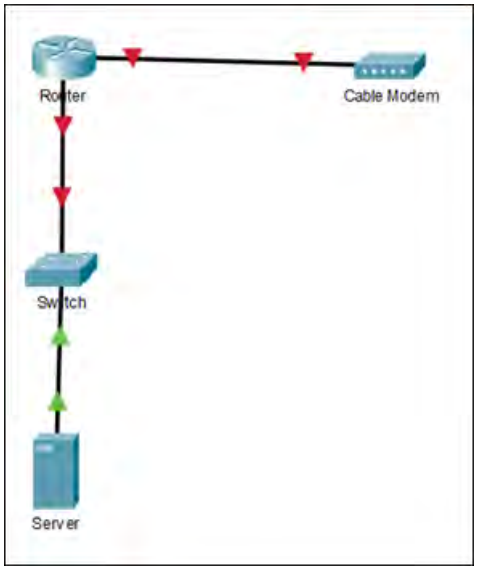


Figure 6.20:

Switch back to the Physical view. You may need to zoom in. There are now physical cables connected to the interfaces of the devices.

Figure 6.21:

Hover the mouse pointer over the cable ends to see information about each cable and interface.

Step 5: Experiment

Now that you know how to navigate the Physical view and add containers and network devices, experiment by adding additional containers to your Home City and to your Corporate Office. Try building more complex network wiring closets by adding additional types of devices.

Packet Tracer File Types

Packet Tracer has the ability to create three different types of files. These file types are used for different purposes and include: `.pkt, .pkz, and .pka.` The `.pkt` file type is used when a simulated network is built in Packet Tracer and saved. The `.pkt` file can also have backgrounds embedded within it. The `.pkz` file type is not used very often. It is a compressed file that allows the inclusion of other files, such as .pdf files, along with the Packet Tracer files.

The `.pka` file type is a Packet Tracer Activity file. This file type contains a Packet Tracer activity plus an instruction window. The instructions provide a walkthrough of the necessary processes required to complete the activity, assignment, or assessment. The instruction window also contains a completion percentage to track how much of the activity has been successfully completed. There is also a Check Results feature that can be configured to provide feedback.

Video — Packet Tracer File Types. This is our Cisco Packet Tracer File Type walkthrough video. In this video, we're going to walk through three different types of Packet Tracer file extensions that you may see inside of your Cisco Academy courses. Watch this video to see the differences and uses of each of the three file types.

Packet Tracer Assessment Types

Packet Tracer is used in the Networking Academy to assist in the design, creation and testing of networks and network applications. Packet Tracer is also used for purposes of self-evaluation, practice, and formal assessment. This section will display and discuss PTSAs and PTMOs. A PTMO (Packet Tracer as a Media Object) is an assessment item where a Packet Tracer Activity is part of the assessment item. Once the .pka is loaded, the student is provided with a small set of instructions to be completed. Once completed, they are able to return to the item to answer the

question based on their work.

A PTSA (Packet Tracer Skills Assessment) is used as a standalone skills-based assessment complete with a full set of instructions. Students are required to build, modify, and/or troubleshoot a network. PTSAs are often done in a timed environment. Once the student has completed the activity, they submit their work to netacad.com. Some PTSAs are configured to allow students to save their work and continue at a later time. Once a PTSA has been completed, the student will receive their score plus item level feedback. They also see a list of objectives of the PTSA along with information about what they did right and what they did wrong. All forms of feedback are intended to assist the student to improve their skills.

> **Video — Packet Tracer Assessment Types.** This is our Cisco Packet Tracer Assessment Usage walkthrough video. In this video we're going to take a look at two ways that we can use a Cisco Packet Tracer within our netacad.com assessments. Watch this video to see examples of the different assessment uses of Packet Tracer.

(Optional PTA 1): Create Realistic Structured Cabling in the Physical Workspace and Cabling Devices in a Rack

Objectives

In this activity, you will install a patch panel and a wall mount. You will then use these to connect network devices in the office to the equipment in the wiring closet.

- Securely install a patch panel in the wiring closet to organize and manage network cables effectively.
- Mount a wall bracket in the office to provide a stable location for network devices or equipment.
- Install an additional wall mount and connect the necessary cables to extend the network infrastructure and improve connectivity.

Part 1: Install a Patch Panel in the Wiring Closet

Step 1: Install a patch panel in the Rack

a. Click the Equipment Cabinet to access a simulated Wiring Closet.
b. To install a patch panel, click Connections in the Device-Type Selection Box, and then click Structured Cabling.
c. In the Device-Specific Selection Box, click the first option, which is Copper Patch Panel.
d. Click a desired location in the Rack to install the patch panel in the rack.
Note: For accurate grading, make sure the name of the patch panel is Patch Panel0.

Step 2: Connect the Office-SW1 to the patch panel

a. From the Cable Pegboard, select a Copper Straight-Through cable.
b. On the switch Office-SW1, click the `GigabitEthernet 1/0/13` port. Now locate and click Jack13 on the `Patch Panel0`.
Note: Recall that you can right click the switch and the patch panel, select Inspect Front, and then zoom in to better locate the desired ports. You can also use the global Zoom In tool on the tool bar.
c. Use the following table to finish the connections between the `Patch Panel0` and `Office-SW1`.

Office-SW1	Patch Panel0
G1/0/13	Jack13
G1/0/14	Jack14
G1/0/15	Jack15
G1/0/16	Jack16

d. If desired, you could also color code the cables in the rack. Right-click the desired cable, select `Color Cable`. Select or create the desired color, and click OK.
e. If you do not like the cables dangling, you can organize them. Right-click any white space in the rack and select `Manage All Cables on Rack`. Now all your cables are organized on the rack.
f. Click `Back level (Alt-Left)` to return to the Office.

Part 2: Attach a Wall Mount in the Office

Step 1: Install a wall mount

a. To install a wall mount, click Connections in the Device-Type Selection Box, and then click Structured Cabling.
b. In the Device-Specific Selection Box, click Copper Wall Mount.
c. Click the desired location on the wall next to the Equipment Cabinet.
Note: For accurate grading, make sure the name of the wall mount is Wall Mount0.
d. In the Device-Type Selection Box, click Connections, and then click Copper Straight-Through cable.
e. Click `Wall Mount0` and select `PunchDown1`. Then click the Equipment Cabinet (Wiring Closet) and select `Rack > Patch Panel0 > Punchdown13`.
f. Repeat for the rest of the available punchdowns on `Wall Mount0`.

Wall Mount (Next to Equipment Cabinet)	Patch Panel
Punchdown1	Punchdown13
Punchdown2	Punchdown14
Punchdown3	Punchdown15
Punchdown4	Punchdown16

g. Connect the PC `Office-Admin` and `Printer0` to any available jacks in the wall mount using Copper Straight-Through cables. After a minute or two, both devices will receive IP addressing information from the DHCP service running on the `Office-Server` inside the Equipment Closet.
h. Verify connectivity by navigating to the web site `http://office.srv`. Click `Office-Admin > Desktop > Web Browser`. Enter `office.srv` in the URL field. This may take up to a minute. You can click `Go` to refresh the web page request.

Step 2: Organize the cables

In the Physical mode, you can organize the cables so that they are spanning across the entire room.

a. Right-click the desired cable, select `Create BendPoint`.
b. Drag the black square to the wall. Continue to create bendpoints and drag the bend points into the walls or floor until the cable no longer goes across the middle of the room. Using the bendpoints has the same effects as running the cables into the walls in an office.
c. Repeat the steps until you are satisfied with the results.

Part 3: Connect an Additional Wall Mount and Cables

Now that you have connected AdminOffice and Printer0 to the network, connect more cables to the patch panel, add another wall mount, and connect the Office-User PC.

a. Return to the Equipment Closet and make the following connections:

Office-SW1	Patch Panel0
G1/0/21	Jack21
G1/0/22	Jack22
G1/0/23	Jack23
G1/0/24	Jack24

b. In the Office, add another Wall Mount next to the window and connect the wall mount to the patch panel using the following connections.
Note: For accurate grading, make sure the name of the wall mount is Wall Mount1.

New Wall Mount (Next to Window)	Patch Panel0
Punchdown1	Punchdown21
Punchdown2	Punchdown22
Punchdown3	Punchdown23
Punchdown4	Punchdown24

c. Connect the Office-User PC to your new wall mount.
d. After a minute or two, verify the Office-User PC received IP addressing information and then verify connectivity to the web site `office.srv`.
e. If desired, create bend points in the cables and organize them.

(Optional PTA 2): Connect Devices using Wireless Technologies

Objectives

In this Packet Tracer activity, you will use different wireless technologies to connect end devices in an office. The activity is performed in the Packet Tracer Physical Mode only.

- Establish a connection between the laptop and the office WLAN by selecting the network and entering the necessary login credentials.
- Pair devices via Bluetooth by enabling Bluetooth on both devices, making them discoverable, and selecting them from the list of available devices.
- Enable the mobile hotspot feature on the smartphone and connect the laptop to this network to access the internet using the cellular connection.

Part 1: Connect a Laptop to the Office WLAN

Step 1: Install a wireless module to a Laptop

a. Click the Laptop to open the configuration window.
b. Under the Physical tab, power off the Laptop by clicking the power button.
c. Remove the Ethernet module `PT-LAPTOP-NM-1CFE` from the laptop by dragging it from the Laptop to the list on the left.
d. Insert the wireless module `WPC300N` by dragging it from the list on the left to the Laptop.
e. Power on the Laptop.

Step 2: Connect Laptop to the office WLAN

a. Click the Desktop tab and select the PC Wireless tool.
b. Click the Connect tab and wait until the `Employee SSID` WLAN is displayed. Note that you may have to click Refresh.
c. Click the `Employee SSID` to select it. Click Connect.
d. Enter `Cisco123` as the pre-shared key and click Connect.
e. After connecting to the wireless network, close the PC Wireless window.
f. Click the Config tab and select `Wireless0` in the left pane to verify in the IP Configuration section that the Laptop has been assigned an IP address.
g. Open the Web Browser from the Desktop. Navigate to `office.srv` to verify that the Laptop has connectivity.
h. Close the Laptop window.

Part 2: Connect Devices with Bluetooth Technology

In this part, you will connect a Bluetooth speaker to a tablet installed with a music player via Bluetooth.

Step 1: Enable Bluetooth ports on devices

a. Click the Bluetooth Speaker.
b. Click the Config tab.
c. Click Bluetooth on the left pane and check that the Port Status is On. Note that the speaker is not paired with the Office Tablet.

Step 2: Connect Bluetooth devices

a. Open the Office Tablet.
b. Click the Config tab.
c. Click Bluetooth in the left pane and check the On box for Port Status.
d. Click Discover and the Bluetooth Speaker device should be discovered.
e. Select the Bluetooth Speaker in the Devices list and click Pair. The status should change to "Paired, Connected". If prompted for permission to connect, click Yes.
f. To test the Bluetooth connection, click the Desktop tab and select Music Player. Click Play/Stop to start the music. Note: Make sure your speaker is on.
g. Click Play/Stop again to stop the sound.

Part 3: Tether a Laptop to Use a Cellular Network via the Smartphone

In this part, you will tether a laptop to a smartphone via Bluetooth. The laptop will use the cellular network to access a website.

Step 1: Enable Bluetooth on the Laptop

a. Click the User-Laptop. Select the Config tab.
b. Click Bluetooth on the left panel. Click On for the Port Status.
c. Leave the User-Laptop Bluetooth window open.

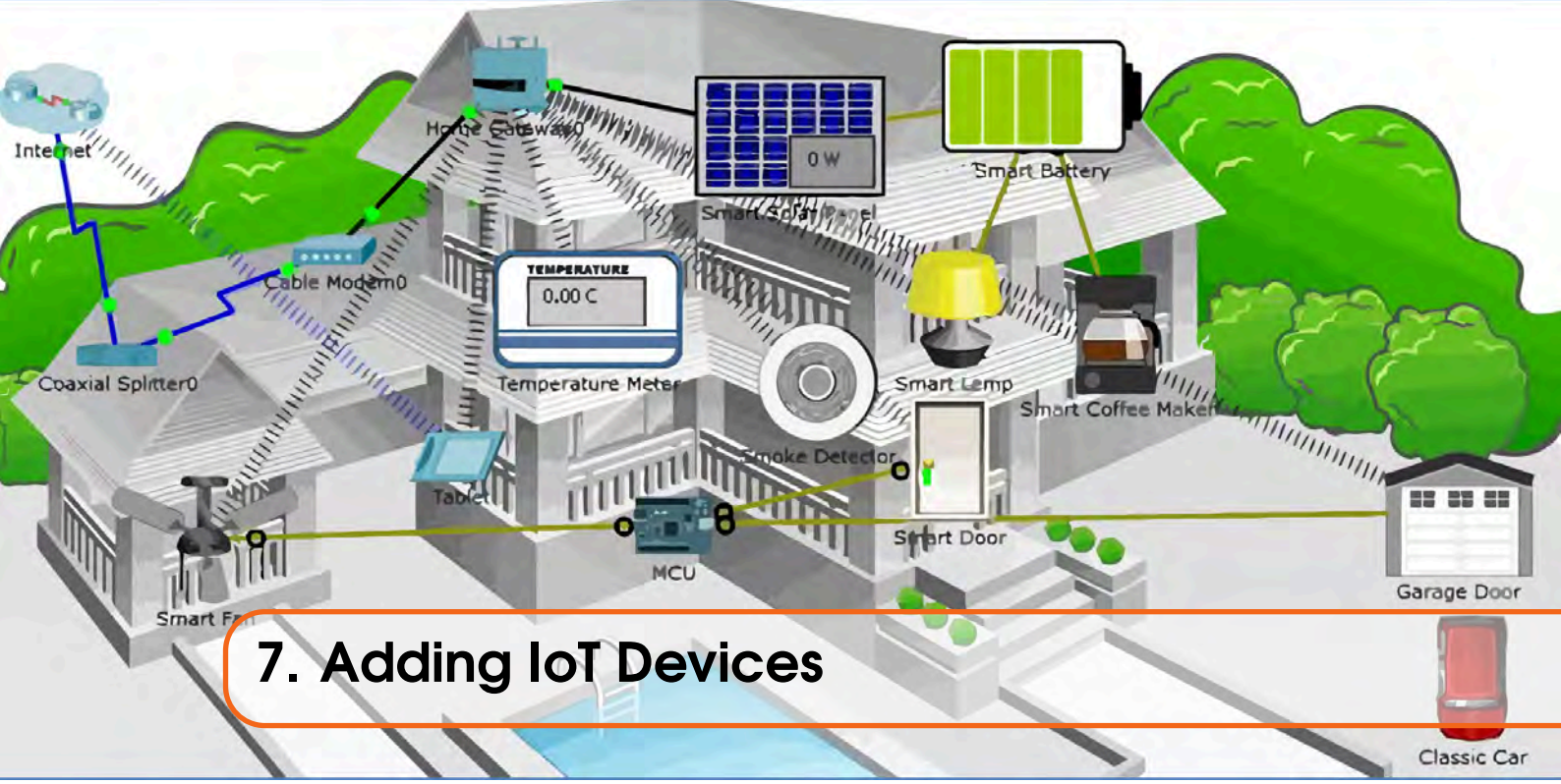
Step 2: Connect a smartphone to the Cellular network and enable Bluetooth

a. Click the Smartphone to open the configuration window.
b. Click the Config tab. Check the On box for the Cellular Tethering setting in the Global Settings.

c. Click the 3G/4G Cell1 interface. Verify that the Smartphone has an IP address from the cellular network.
d. Click Bluetooth in the left pane and check the On box for the Port status on the Smartphone.

Step 3: Connect Bluetooth devices and tethering to laptop

a. On the Bluetooth configuration for the Smartphone, click Discover to search for nearby Bluetooth enabled-devices.
Note: If Smartphone does not appear after a while, move Smartphone closer to User-Laptop and click Discover again.
b. Select User-Laptop and click Pair. A pop-up window appears and asks for permission. Click Yes. The two devices are connected via Bluetooth.
c. Return to the User-Laptop. In the Bluetooth panel of the Config tab, highlight Smartphone and click Tether.
d. At the bottom pane of the Bluetooth configuration, notice that User-Laptop has now obtained an IP address.
e. To test connectivity, navigate to `office.srv`. Click `Desktop > Web Browser`. Enter `office.srv` in the URL field. You can fast forward time to speed up the process.



7. Adding IoT Devices

Objectives

- Discover and identify various IoT devices available in Cisco Packet Tracer, enhancing understanding of their features and applications.
- Connect IoT devices to the network using both wired and wireless connections, practicing the setup and integration of smart devices.
- Configure and control IoT devices, including setting up network parameters, attributes, and remote access through a registration server or home gateway.
- Experiment with and customize smart environments, creating simulations for smart homes, cities, and factories to explore IoT functionalities .

IoT Components in Packet Tracer

In simple terms the IoT is a connection of networked sensors, actuators, and smart devices that collect and share data. Packet Tracer 7 contains many new features to support the IoT. This includes the addition of IoT devices that can be configured to react to certain environmental values such as sun, wind, rain, and humidity. These devices can be configured to take actions based on the changing environmental values, such as turning on lights or closing garage doors. The next few sections include instructions to locate the IoT devices, to connect them to your network, to configure and modify scripts to make them function, and to control these devices remotely. Packet Tracer provides everything you need to create simulated smart homes, smart cities, and smart factories. At the completion of this section, you should be able to describe:

- What IoT devices are available in Packet Tracer.
- Where IoT devices are located.
- How to connect IoT devices to your network.
- How sensors interact with smart devices.
- How different IoT devices work.
- Basic configuration of smart devices.

Configure IoT Devices using Packet Tracer

Packet Tracer has a wide variety of sensors and smart devices that will allow you to design smart homes, smart cities, smart factories, and smart power grids. To locate the available sensors and smart devices, select End Devices from the Device Selection box at the lower left-hand side of the screen. Next select one of the subcategories such as Home. In the Home subcategory, you will see many IoT devices such as an air conditioner, ceiling fan, coffee maker, and CO detector. These devices can be connected to your network wirelessly or with a physical cable.

To connect the devices to your network, you need a device, such as a home gateway or registration server. To find a home gateway, select Network Devices from the Device Selection box and then select Wireless Devices from the subcategories. To control the devices, you have two options:

1. You can interact directly with a device. Hold down the Alt key and at the same time click on the device to turn it on or off.
2. You can connect remotely over the network. Using a remote PC, tablet or smart phone, you can use a web browser to connect to the home gateway or registration server. From here, you can turn the devices on or off using the features of the home gateway or registration server.

To configure devices, click on the device to open it. Then, you have a multiple tabs to select:

- **Specifications** – describes the features, usage, local and remote control of the device
- **Physical** – available modules and power connections
- **Config** – shows display name, serial number, network configuration, and IoT server
- **Attributes** – display the device attributes such as MTBF, power consumption, and cost

To configuration home gateway, you click on device. Within device you have multiple tabs to select.

- **Physical** – available modules, and power
- **Config** – shows display name, interfaces (Internet, LAN, and wireless) to be configured
- **GUI** – shows services to be turned on/off
- **Attributes** – shows features and values related to device such as: mean time between failure (MTBF), cost, power sources, and wattage

Video — **Configure IoT Devices using Packet Tracer** . This is our Cisco Packet Tracer, Internet of Things walk-through video. In this video we're going to walk through many different smart devices that exist here. Watch this video to learn about locating, connecting, and configuring IoT devices in Packet Tracer.

Video — **Using IoT Devices in Packet Tracer** . Packet Tracer lets you simulate real networks, including smart networks that make use of IoT devices. It provides a number of IoT devices for a Smart Home network.

Add IoT Devices to a Smart Home

In this activity you will open a Packet Tracer file with an existing home network, explore the devices on the network and then add additional wired and wireless IoT devices.

The Smart Home Network

Figure 7.1:

Objectives

- Part 1: Explore the Existing Smart Home Network
- Part 2: Add Wired IoT Devices to the Smart Home Network
- Part 3: Add Wireless IoT Devices to the Smart Home Network

Background / Scenario

In this activity you will open a Packet Tracer file with an existing home network, explore the devices on the network, and then add additional wired and wireless IoT devices.

Part 1: Explore the Existing Smart Home Network

Step 1: Open the Smart_Home_Network.pkt file

a) Open the Smart_Home_Network.pkt file.
b) Save the file to your computer.

Step 2: Explore the Smart Home Network

a) Explore IoT end devices.
At the bottom left corner of the Packet Tracer window, locate and click the End Devices icon in the top row, and the Home icon in the bottom row of the Device-Type Selection box.

Figure 7.2:

Across the bottom of the Packet Tracer window, the Device-Specific Selection box displays the many different Smart Home IoT devices available.
Move the mouse pointer over each device and notice that the descriptive name of the device is displayed at the bottom of the Device-Specific Selection box. Take a moment to look at each device type.

Figure 7.3:

b) Explore the Smart Home network.

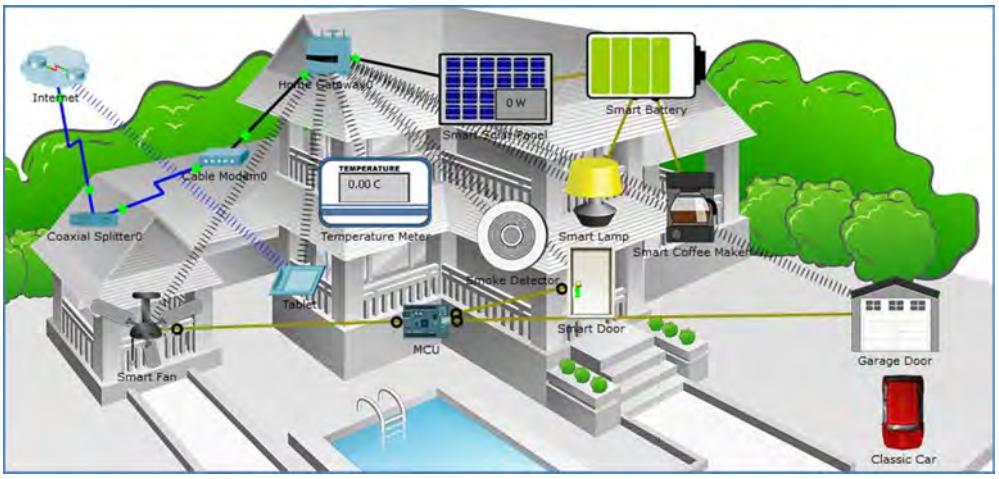


Figure 7.4:

In the Logical workspace is a prebuilt smart home network that consists of many wired and wireless IoT devices, and network infrastructure devices.
When you place your curser over a device, such as the Smart Fan, an informational window opens containing basic network information about that device.

Figure 7.5:

To turn on or activate a device, simply hold down the Alt key on the keyboard and then move the cursor over the device. Try this on each of the smart devices to observe what they do.
The smart home network also consists of infrastructure devices such as a home gateway. Click the Home Gateway icon to open the Home Gateway window.

Figure 7.6:

The Physical tab is selected by default and shows a picture of the Home Gateway.

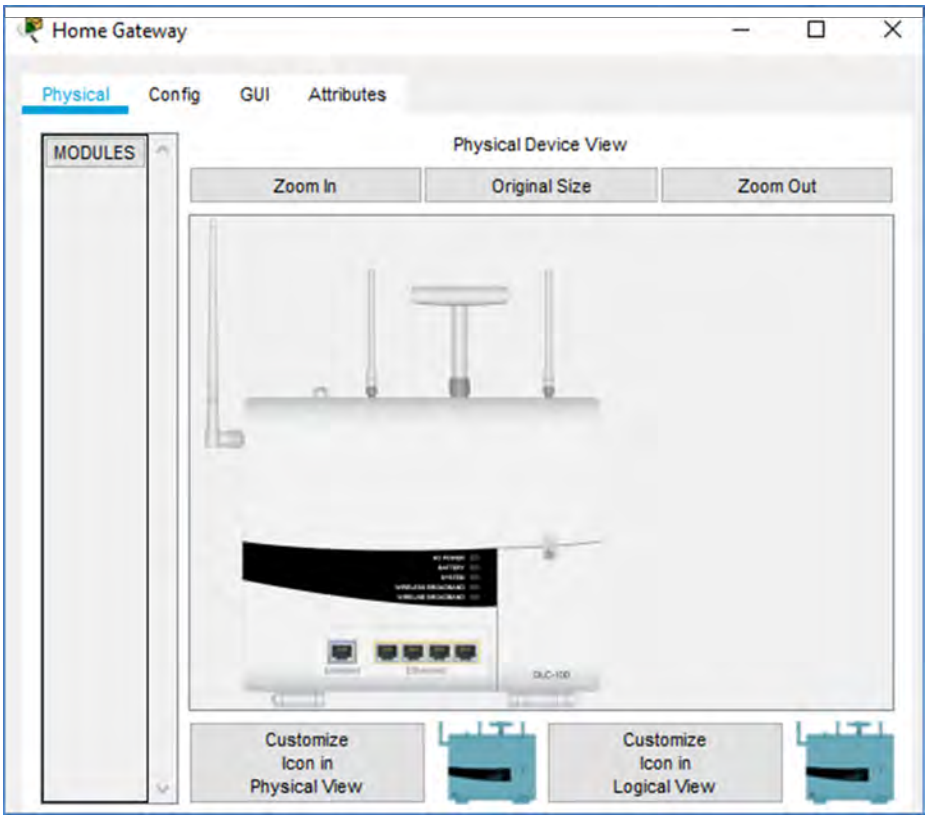


Figure 7.7:

Next, click the Config tab and then in the left pane click LAN to view the LAN Settings of the Home Gateway.
Write down the IP Address of the home network for future reference.

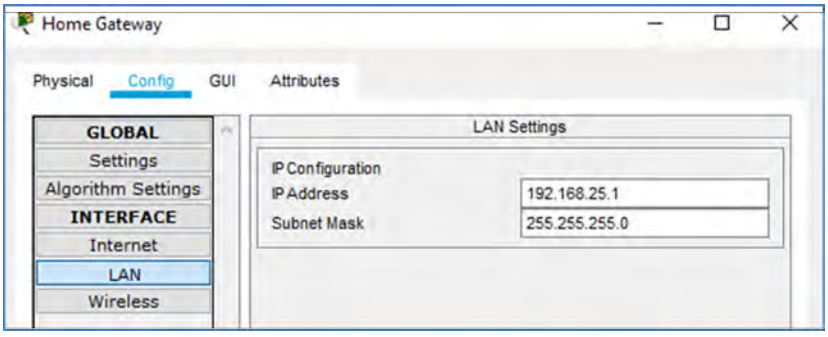


Figure 7.8:

Click Wireless in the left pane to view the wireless settings of the Home Gateway.
Write down the SSID of the home network _____ and the WPA2-PSK Pass Phrase _____ for future reference.

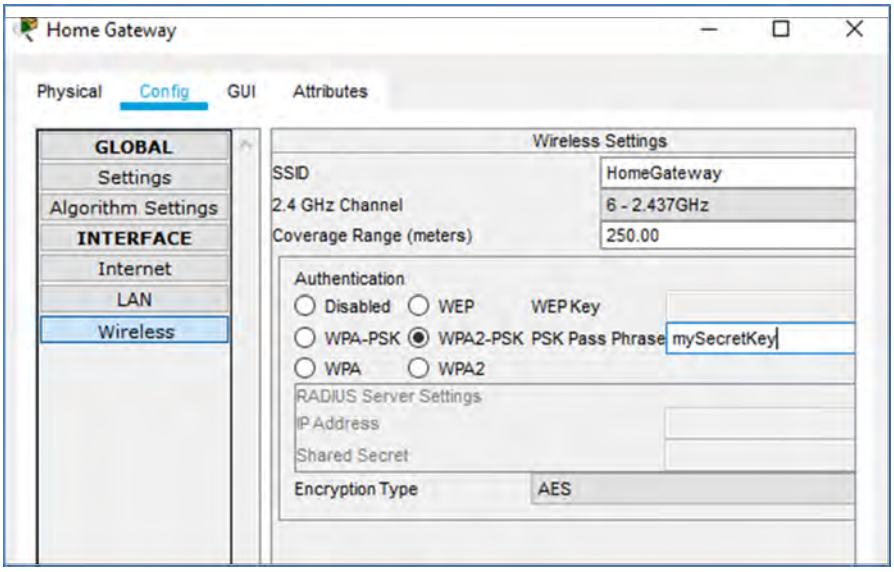


Figure 7.9:

Close the Home Gateway window.
Next, click the Tablet device icon to open the Tablet window.

Figure 7.10:

In the Tablet window, select the Desktop tab and then click the Web Browser icon.

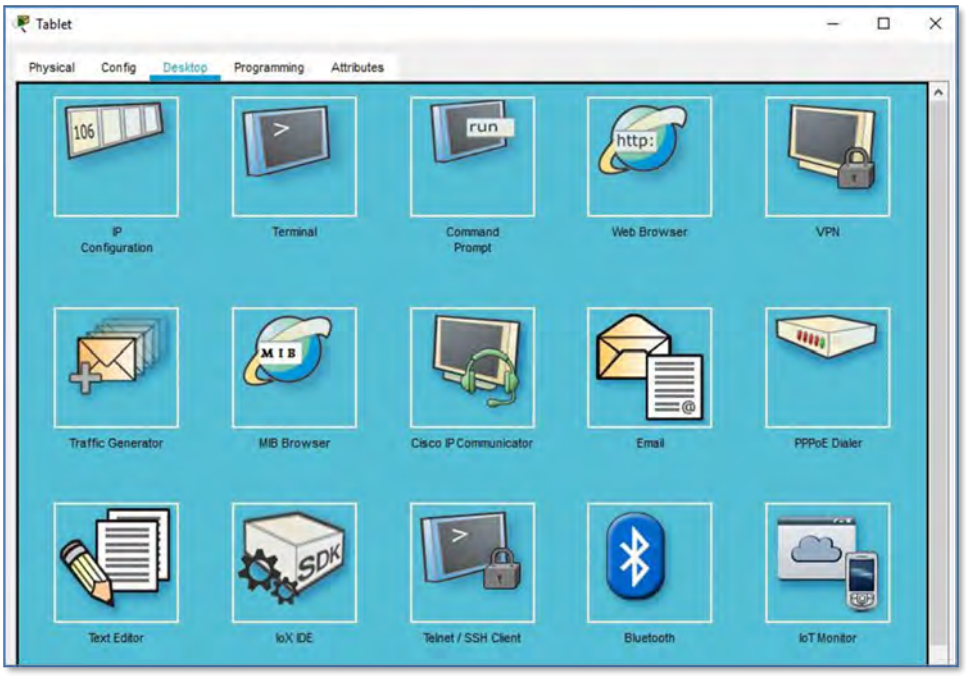


Figure 7.11:

In the Web Browser window, type the IP address of the Home Gateway 192.168.25.1 into the URL box and click Go. In the Home Gateway Login screen, type admin for both the username and the password and click Submit.

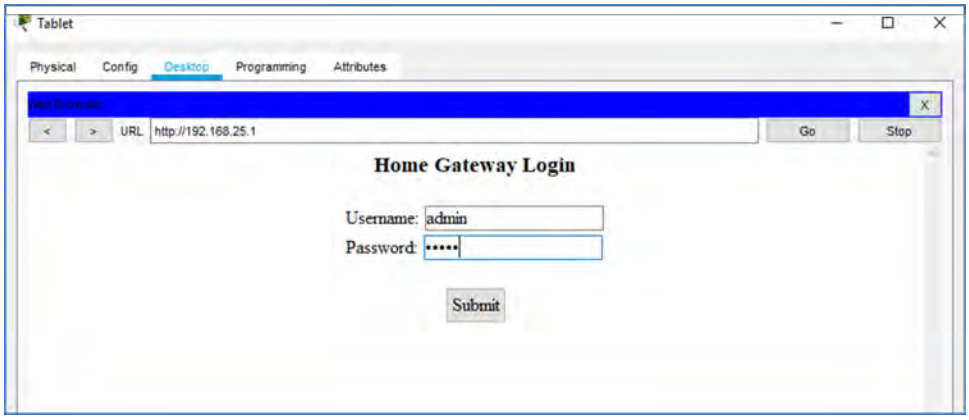


Figure 7.12:

After you have connected to the Home Gateway web interface, a list of all the connected IoT devices appears.

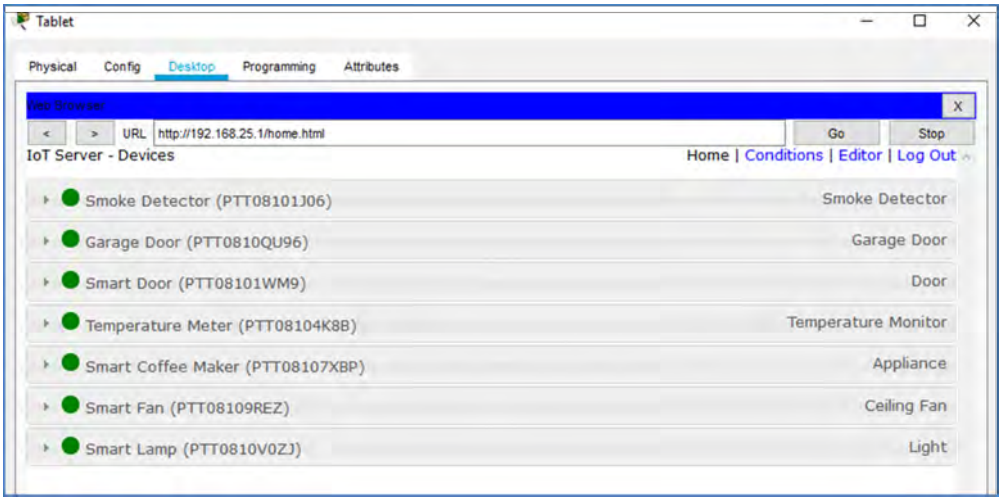


Figure 7.13:

When you click a device in the list, the status and settings of that device is displayed.

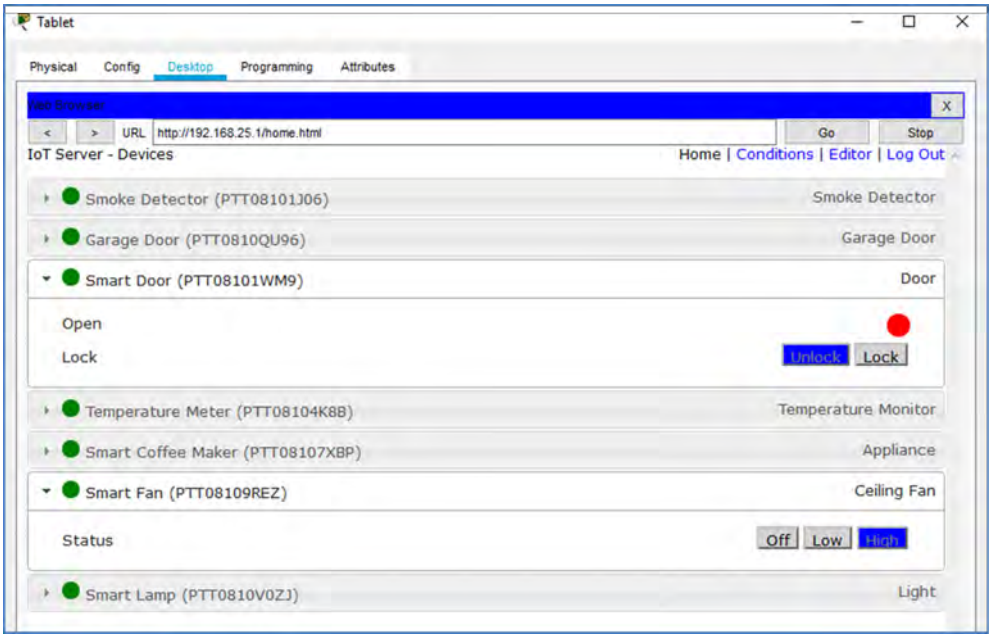


Figure 7.14:

Close the Tablet window.

Part 2: Add Wired IoT Devices to the Smart Home Network

Step 1: Cable a device to the network

a) a. In the Device-Specific Selection box, click the Lawn Sprinkler icon and then click in the workspace where you would like to locate the Lawn Sprinkler.

b) Cable the Fire Sprinkler to the Home Gateway.
In the Device-Type Selection box, click the Connections icon (this looks like a lightning bolt). Click the Copper Straight Through connector type icon in the Device-Specific Selection box. Then click the Sprinkler icon and connect one end of the cable to the Sprinkler's

FastEthernet0 interface. Next, click the Home Gateway icon and connect the other end of the cable to an available Ethernet interface.

Step 2: Configure the sprinkler for network connectivity

a) Click the Lawn Sprinkler device icon in the workspace to open the device window. Notice that right now the name of the Lawn Sprinkler is a generic IoT0.
The device window will open to the Specification tab which gives information about the device which can be edited.

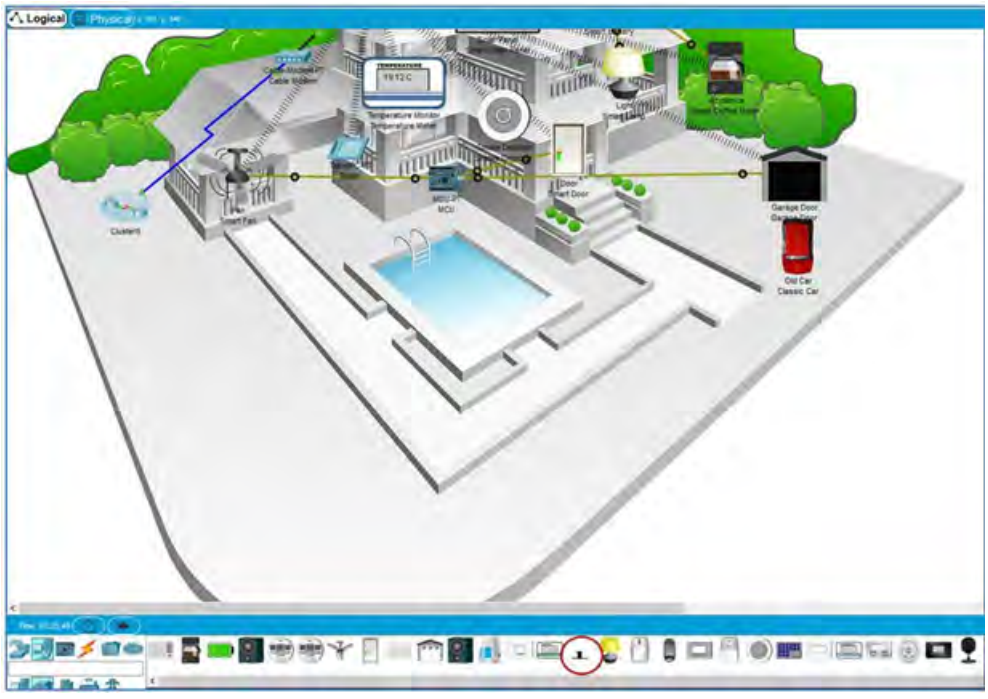


Figure 7.15:

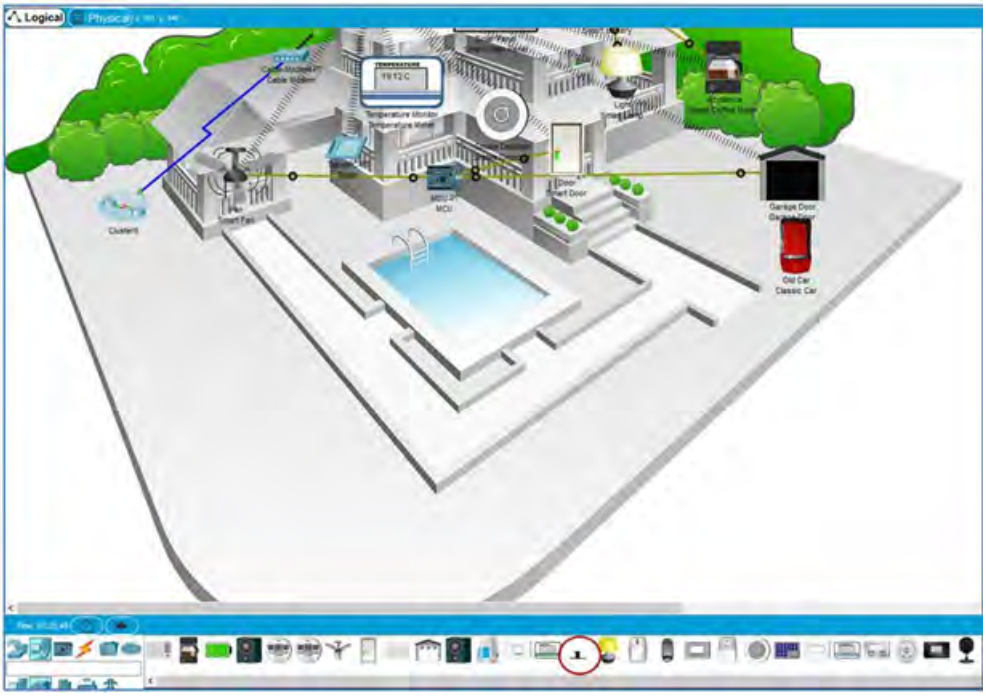


Figure 7.16:

b) Click the Config tab to edit the device configuration settings. In the Config tab, make the following changes to Settings:

- Set the Display Name to Sprinkler1 (notice the window name changes to Sprinkler1)
- Set the IoT Server to Home Gateway

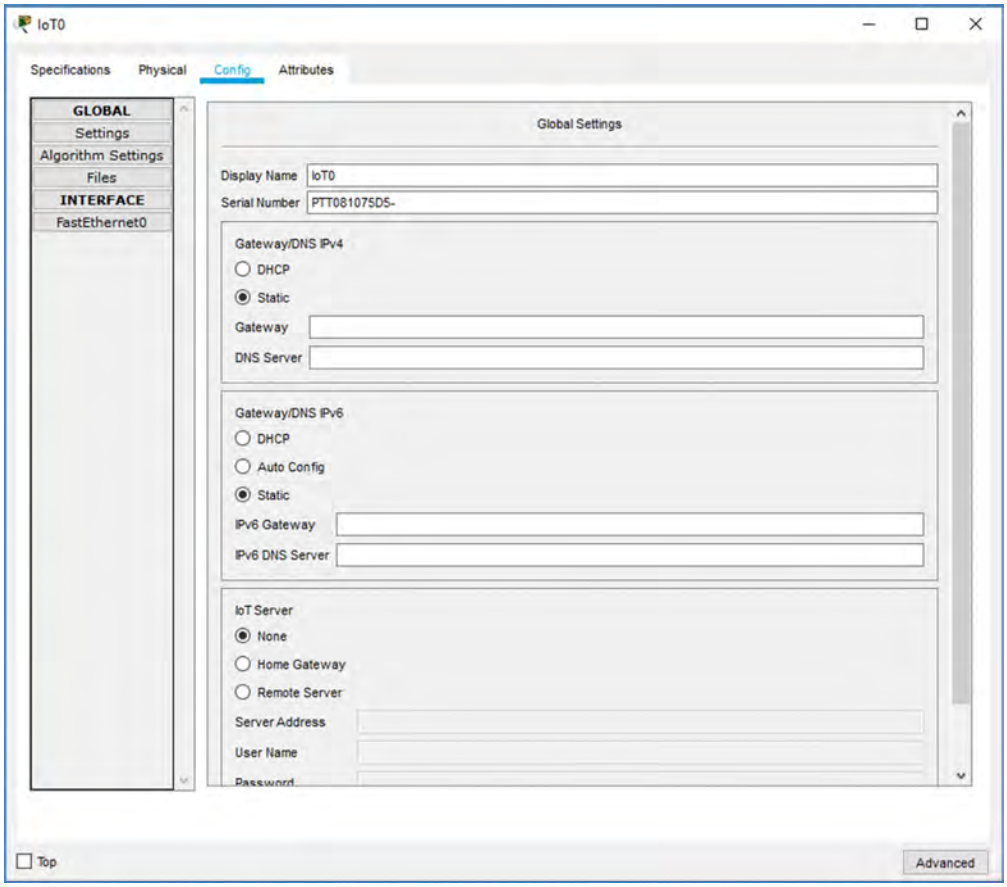


Figure 7.17:

Click FastEthernet0 and change the IP Configuration to DHCP.

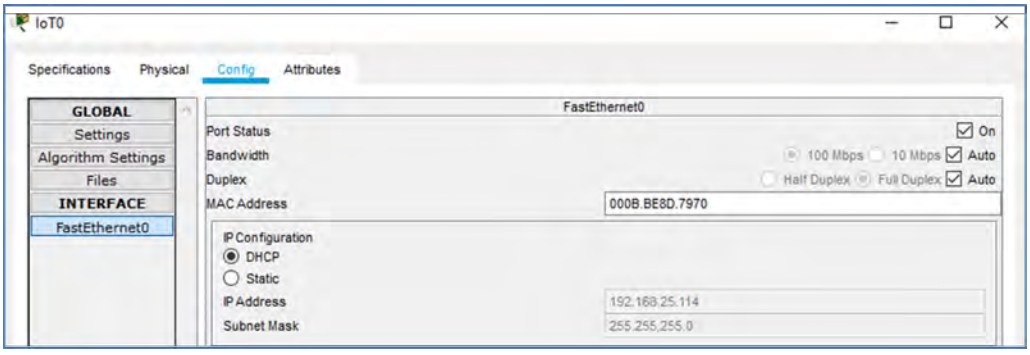


Figure 7.18:

Close the Sprinkler1 window.

c) Verify that the sprinker is on the network.
Log into the Home Gateway from the Tablet.
The device Sprinkler 1 should now appear in the IoT Server – Devices list.

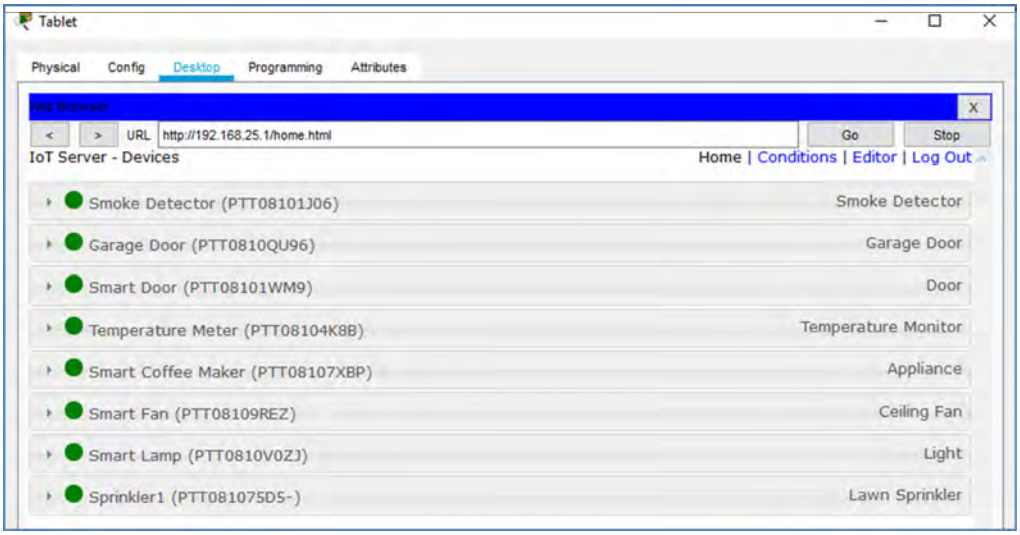


Figure 7.19:

Close the Tablet window.

Step 3: Experiment by adding other types of IoT devices to the smart home network.

Part 3: Add Wireless IoT Devices to the Smart Home Network

Step 1: Add a wireless device to the network

a) a. In the Device-Specific Selection box click the Wind Detector icon and then click in the workspace where you would like to locate the Wind Detector.

Figure 7.20:

Figure 7.21:

b) Add wireless module to the Wind Detector.
Click the Wind Detector icon in the workspace to open the IoT device window. In the bottom right corner of the IoT device window, click the Advanced button. Notice more tabs become visible at the top of the window. Click the I/O Config tab.

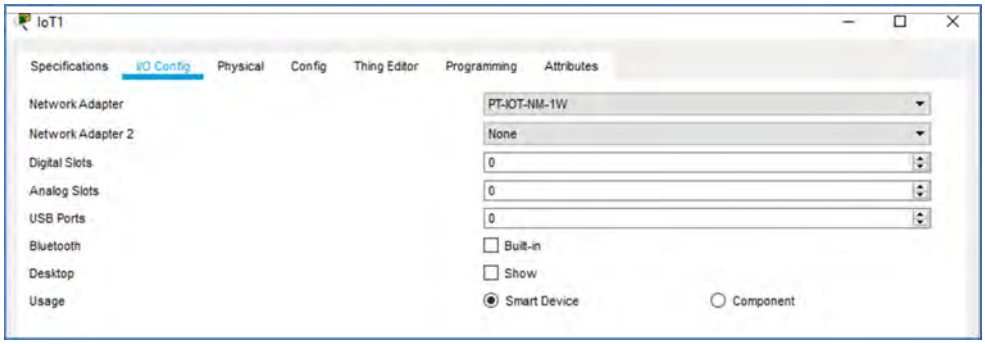


Figure 7.22:

Change the Network Adapter drop down list to PT-IOT-NM-1W, which is a wireless adapter.

c) Configure the Wind Detector for the wireless network.
Click the Config tab.
Next click Wireless0 in the left pane. Change the Authentication type to WPA2-PSK and in the PSK Pass Phrase box type mySecretKey. These are the wireless settings from the Home Gateway that you recorded in Part 1.

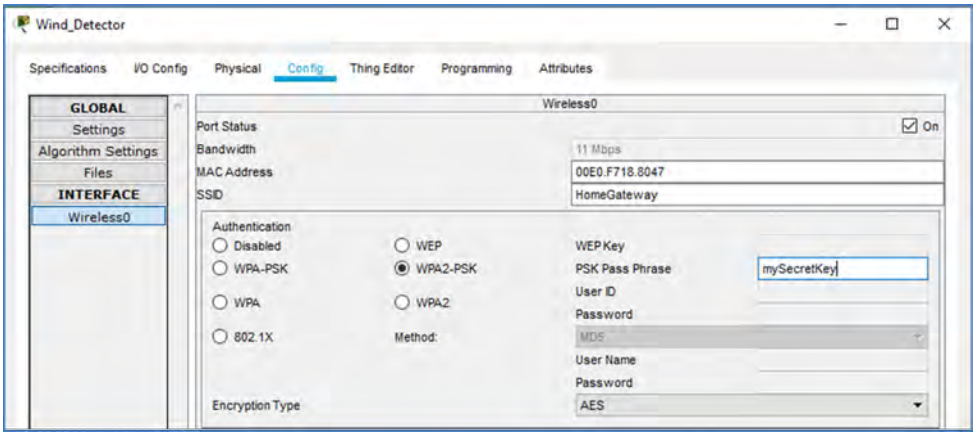


Figure 7.23:

A wireless connection should be formed between the Wind Detector and the Home Gateway.

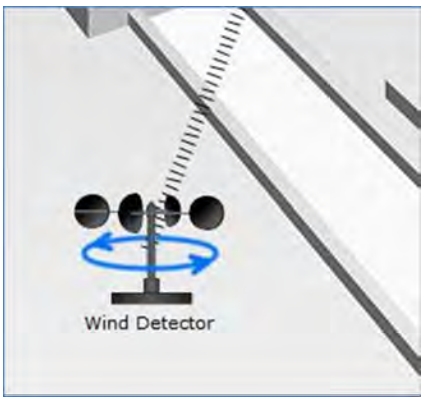


Figure 7.24:

d) Verify the Wind Detector is on the network.
Log into the Home Gateway from the Tablet.
The device Wind Detector should now appear in the IoT Server – Devices list.

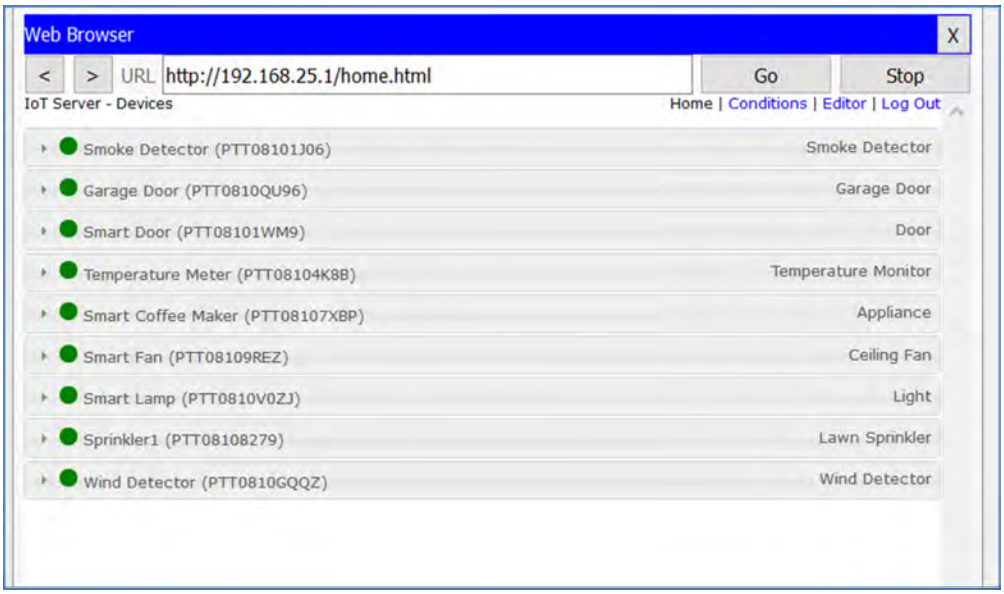
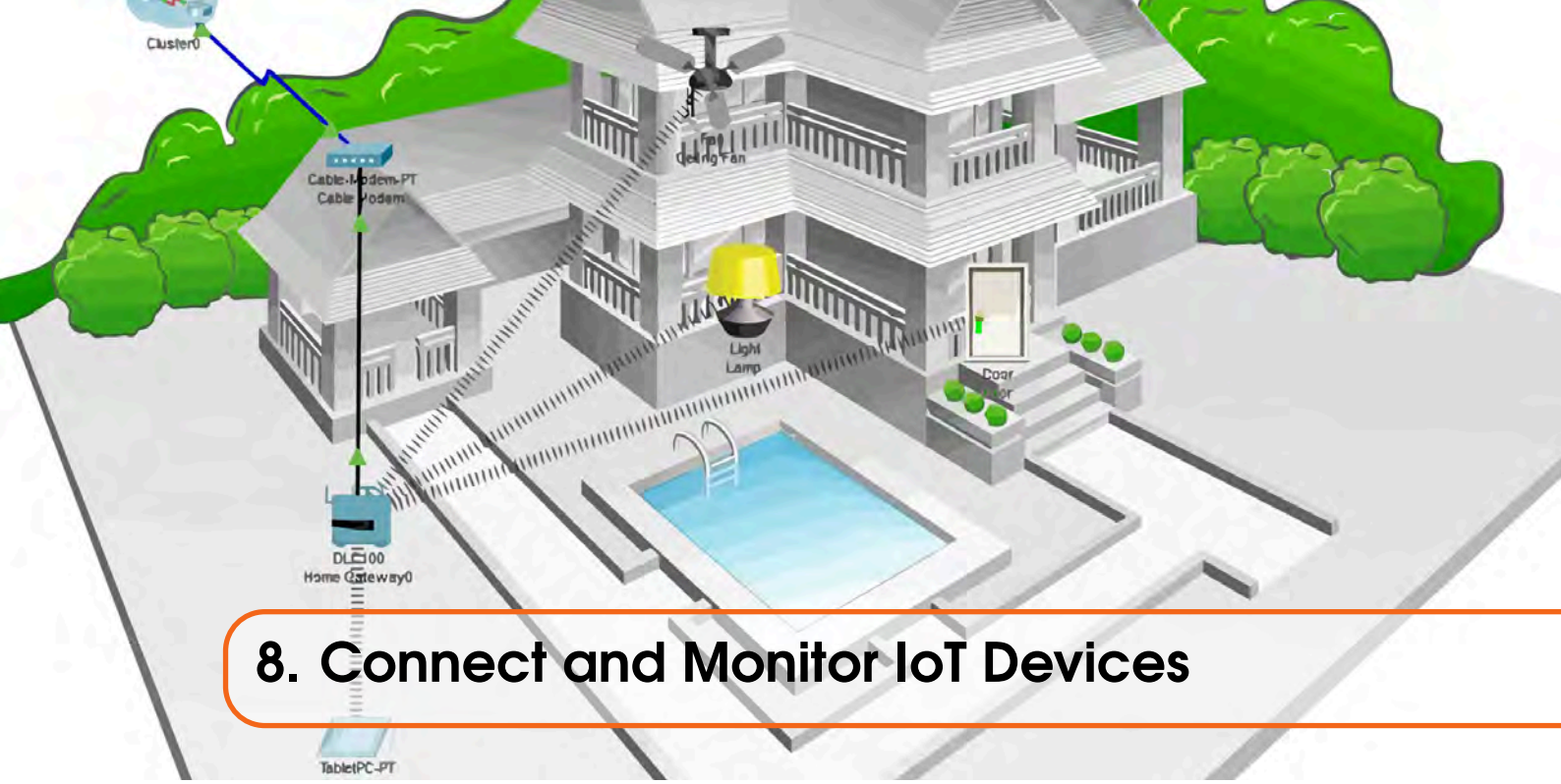


Figure 7.25:

Close the Tablet window.

Step 2: Experiment by adding other types of IoT devices to the smart home wireless network.



8. Connect and Monitor IoT Devices

Objectives

- Connect and control smart devices using a home gateway device or a remote registration server, creating and managing a small smart home network.
- Explore the various features and settings of a home gateway, including its physical, configuration, GUI, and attribute tabs, to understand its functionalities.
- Register and monitor IoT devices through a home gateway, practicing the steps for connecting and configuring smart devices within a network.
- Control and interact with smart devices remotely using a tablet, PC, or smartphone, enhancing understanding of IoT device management and monitoring.

Creating and Controlling a Small Smart Home Network

In this section you will learn how to connect and control smart devices using either a Home Gateway device or a remote registration server. At the completion of this section, you should be able to create and connect IoT devices into a small home network using the built-in registration server of the home gateway or a dedicated registration server.

The Home Gateway device acts as a local connection to your IoT smart devices. This device was designed to provide Internet access, wireless connectivity, and local logic for smart devices. The Home Gateway device provides an IoT registration service that is always turned on and an auto discovery service for Things in the local Ethernet and wireless network.

Once connected to the home gateway, the user can control and monitor the smart devices from their smartphone, tablet/PC. Once a home gateway device has been added to the logical workspace, click on the device. You will see the following:

- **Physical tab** – the device has an Internet port, four LAN ports, and multiple antennae
- **Config tab** – this shows the interfaces and network settings that are configurable
- **GUI tab** – this shows the registration server inside the device that allows for interaction with

IoT devices. It is on by default but can be turned off.
- **Attributes tab** – This is blank by default but can show features and values such as MTBF, cost, power source, and wattage.

After connecting the home gateway to an existing network, select the Config tab. The internet and the wireless interfaces should obtain IP addressing information from the network. To connect an IoT device, such as a fan, wirelessly, click on the fan and select the Config tab. The simple config tab appears. Select the Advanced button in the lower right hand corner to view more options. To configure and register the fan with the home gateway:

- Select I/O Config and then select wireless adapter from the network adaptors dropdown list.
- Select Config to verify that the fan has established a wireless connection to the correct SSID. This can also be done visually by viewing the fan in the workspace.
- Select Config/Settings and select the home gateway as the IoT server registration device.

To control the fan remotely:

- Add a tablet, PC, or smart phone to the workspace and connect it to the home gateway. Click on the remote device and select Desktop/IPConfig to verify connectivity.
- Return to the desktop and select the web browser. Use the default gateway address from the remote device as the URL. This is the address of the home gateway. Once into the home gateway, you should see the registered fan and be able to modify its settings.

Video — Creating and Controlling a Small Smart Home Network. This is our Cisco Packet Tracer Accessing and Monitoring Smarter Devices walk-through video. We have Packet Tracer and IOT coming together and utilizing something actually called a smart home gateway. We're going to build it from the ground up right here, right now. Watch this video to learn about creating and controlling a small IoT home network using a home gateway.

Video — Connect Devices to a Home Gateway and Monitor Network. Packet Tracer lets you connect and control smart devices using either a home gateway device or a remote registration server.

Connect Devices to a Home Gateway and Monitor

In this activity you will add a Home Gateway and several IoT devices to an existing home network and monitor those devices through the Home Gateway.

The Smart Home Network

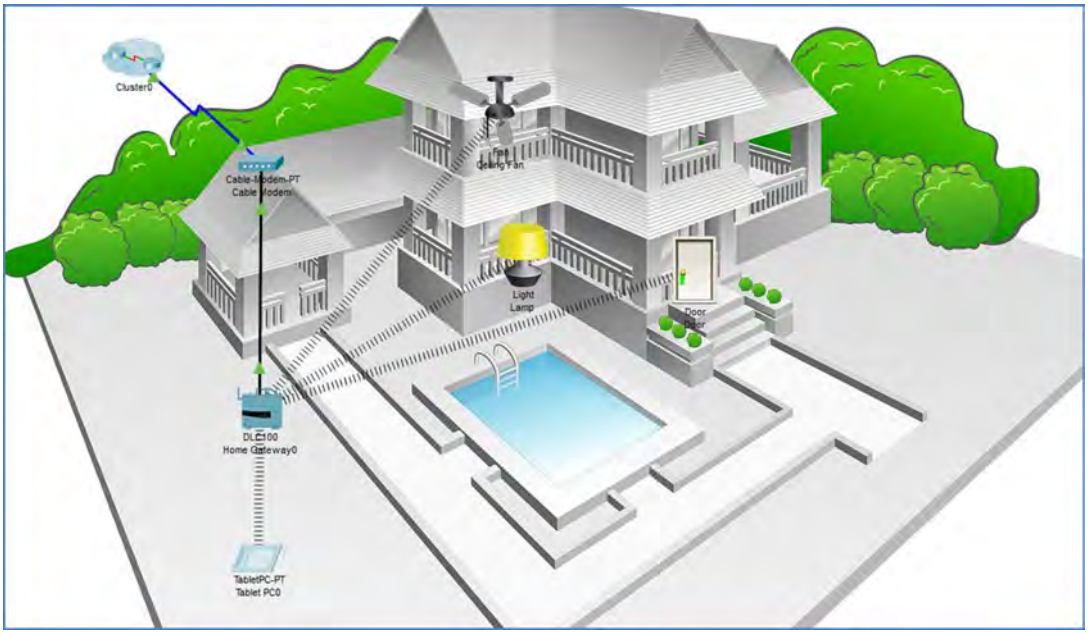


Figure 8.1:

Objectives

- Part 1: Add a Home Gateway to the Network
- Part 2: Connect IoT Devices to the Wireless Network
- Part 3: Add an End User Device to the Network

Background / Scenario

In this activity you will add a home gateway and several IoT devices to an existing home network and monitor those devices through the home gateway.

Part 1: Connect a Home Gateway to the Network

Step 1: Open the Smart Home.pkt file and save the file to your computer

Step 2: Adding a home gateway

a) Select the Home Gateway device.
Click the Wireless Devices icon in the Device-Type Selection box. Click the Home Gateway device icon and then click in the Logical workspace to add the device.

Figure 8.2:

b) Connect the home gateway to the cable modem.
Click the Copper Straight-Through connector icon in the Device-Type Selection box, then click the Home Gateway to add one end of the cable to Port 1 of the gateway. Next, click the Cable Modem icon to connect the other end of the cable to the Internet port.

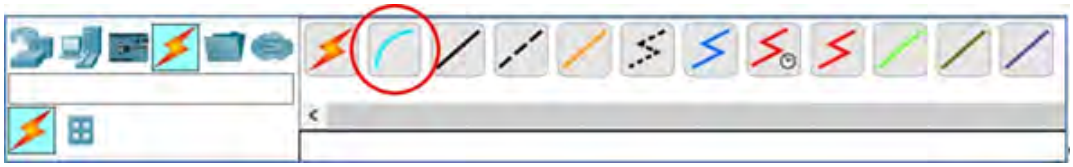


Figure 8.3:

After a few seconds both ends of the cable should have green lights that indicate that the link is up.

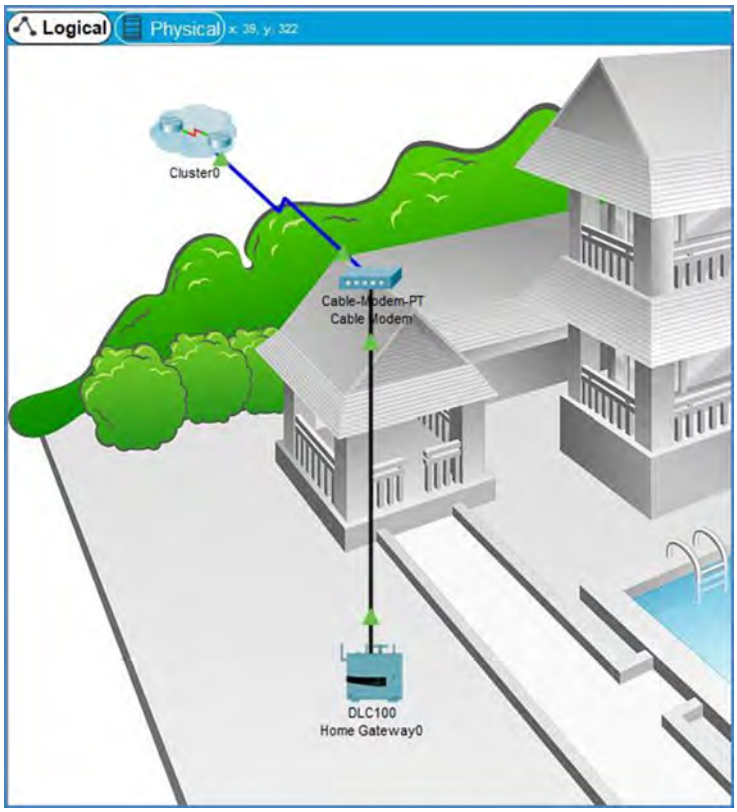


Figure 8.4:

Part 2: Connect IoT Devices to the Wireless Network

Step 1: Select wireless devices

a) Add a wireless adapter to the Fan device.
Click the Fan icon in the workspace to open the Config tab and then click the Advanced button in the bottom right corner of the window. Notice that the tabs at the top of the configuration window change. There are now more tabs.
Click the I/O Config tab and change the Network Adapter type to the PT-IOT-NM-1W wireless adapter.

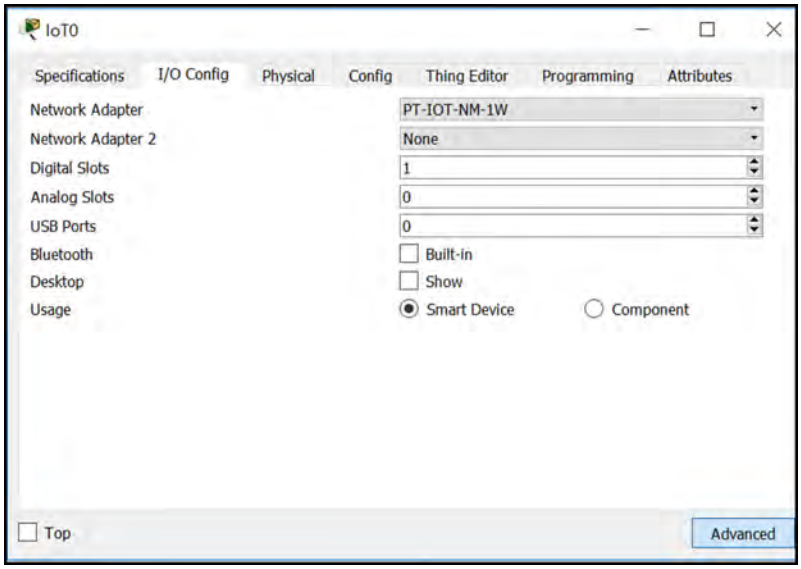


Figure 8.5:

b) Change the display name of the Fan device.
Click the Config tab. Global settings options should be visible, if not, select Settings in the left pane. In the Display Name box, type Ceiling Fan.

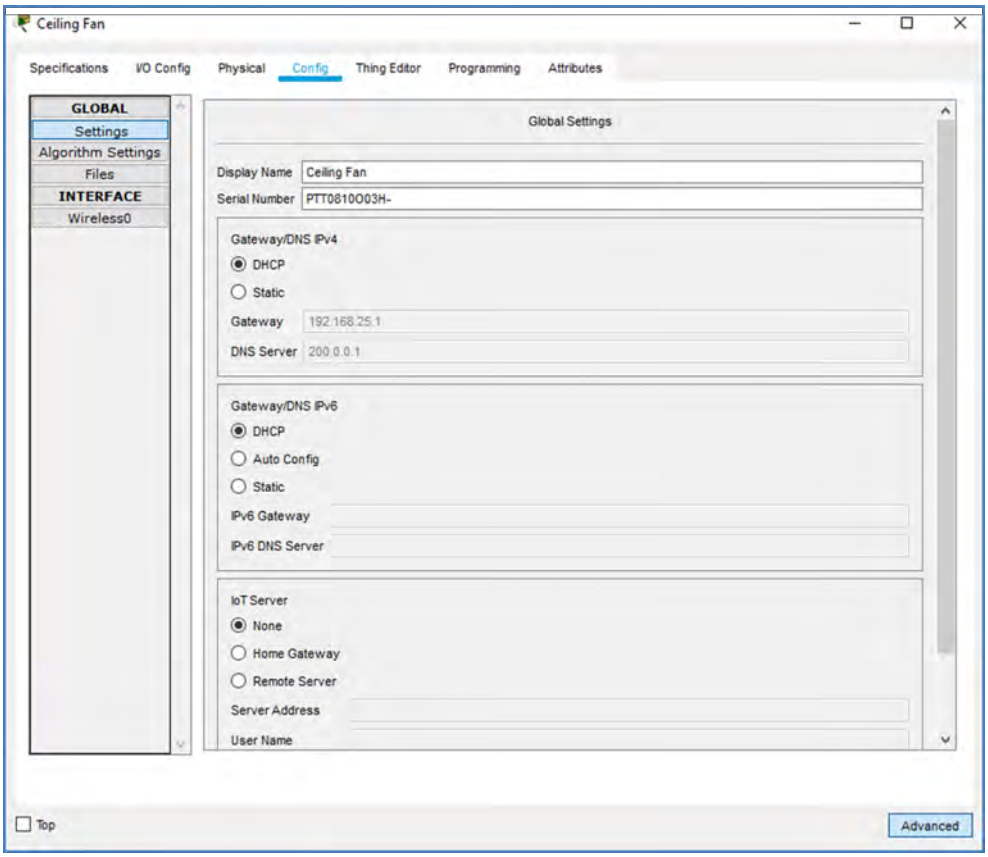


Figure 8.6:

c) Verify that the Ceiling Fan is connected to the wireless network.

While still in the Config tab, click the Wireless0 interface in the left pane.
In the configuration settings, the HomeGateway network should be listed in the SSID box. Verify that the DHCP is selected in the IP Configuration settings, and that the IP address is 192.168.25.100. This indicates that the fan is connected to the network and is receiving IP configuration information from the home gateway.

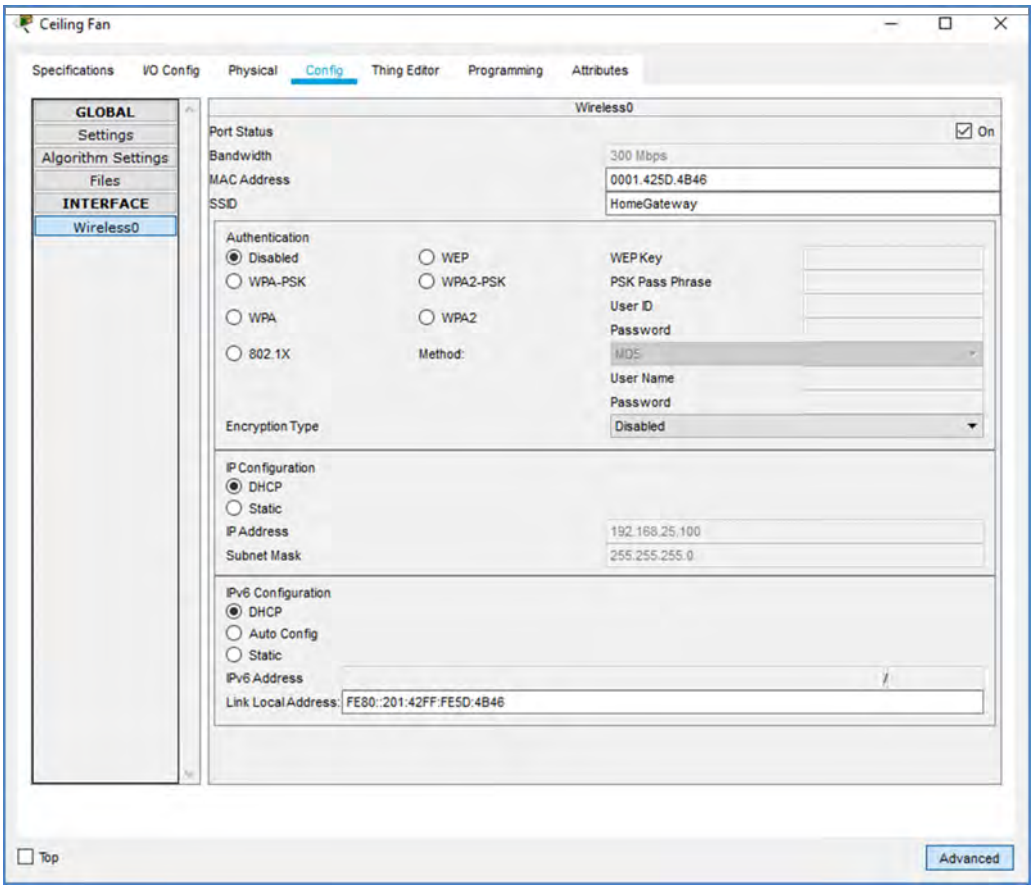


Figure 8.7:

Close the Ceiling Fan configuration window.

d) Connect the Door and the Lamp to the wireless network following the same steps used for the fan.

Part 3: Add a Wireless Tablet to the Network

Step 1: Add a wireless tablet to the workspace

a) Click the End Devices icon in the Device-Type Selection box and add the Wireless Tablet to the workspace.

Figure 8.8:

Step 2: Connect the wireless tablet to the HomeGateway network

a) Change the wireless tablet network settings.
Click the Wireless Tablet icon to open the tablet configuration window.
Click the Config tab and then click the Wireless0 Interface. Change the SSID from Default to HomeGateway. After the network SSID is changed the tablet should learn an IP address through DHCP within a few seconds.

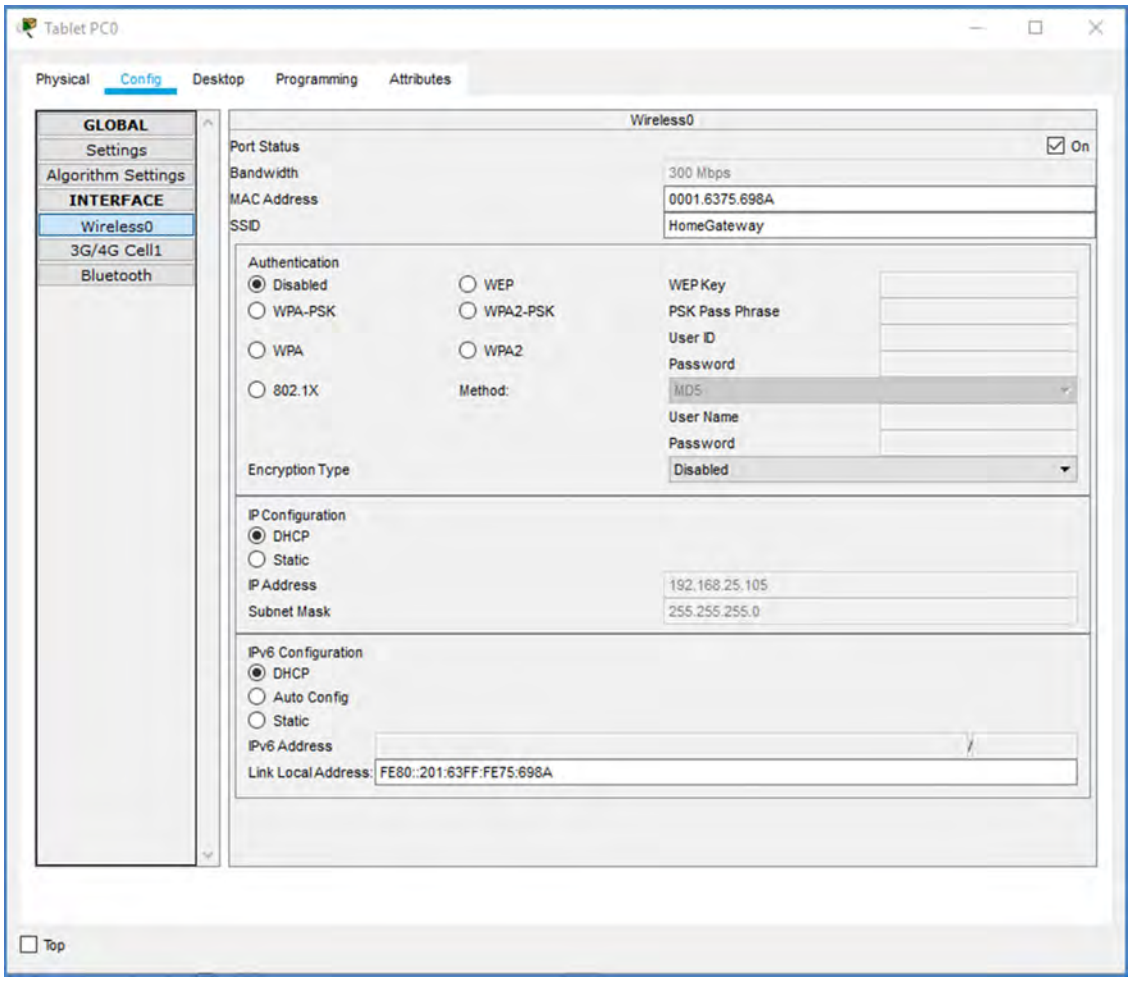


Figure 8.9:

b) Access the home gateway from the tablet.
Click the Desktop tab and then click the Web Browser icon to open a web browser. Type 192.168.25.1 (the address of the home gateway) in the URL box and click Go.
At the Home Gateway Login page, enter admin as the username and admin as the password and click the Submit button to connect to the Home Gateway server.
Note that no devices appear in the Home Gateway IoT Server - Devices list.

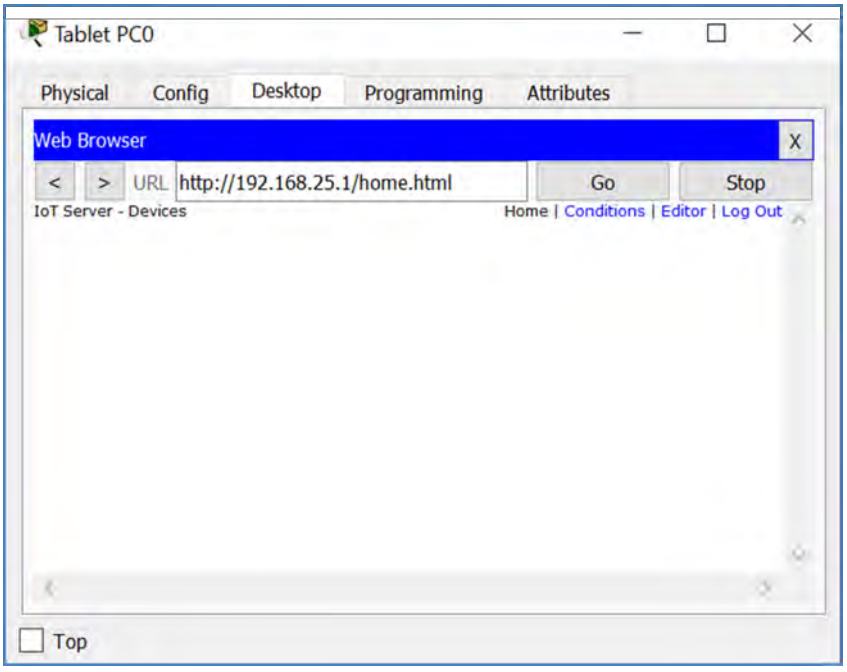


Figure 8.10:

Close the Tablet PC0 window.

Step 3: Configure IoT devices to register with the Home Gateway server

a) Register the ceiling fan to the home gateway server.
Click the Fan icon in the workspace, click the Config tab, and then click Settings in the left pane. At the IoT Server options list, click the Home Gateway button.

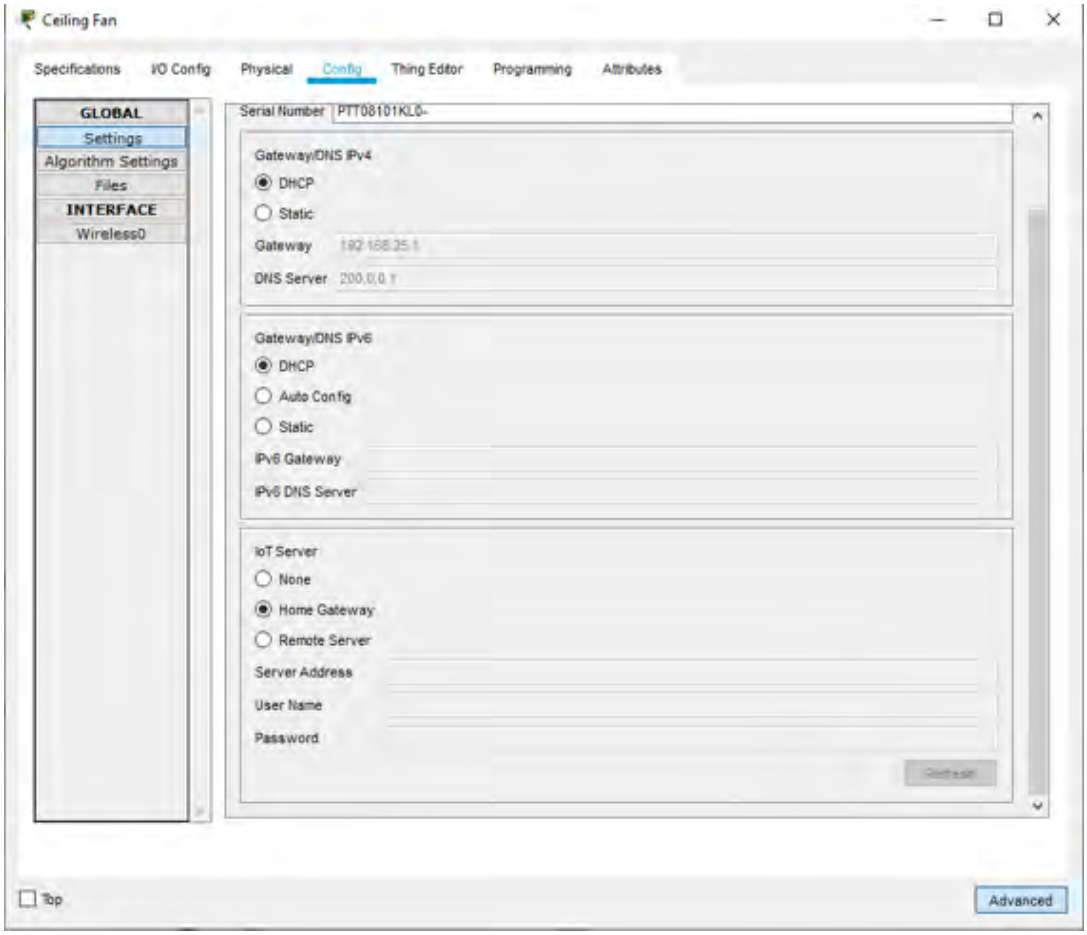


Figure 8.11:

Close the Ceiling Fan window.

Repeat the steps in 3a to register the Door and the Lamp devices to the home gateway.

b) Verify that the devices are now registered with the Home Gateway server. Click the Tablet icon in the workspace and open the web browser. Connect to the home gateway by typing 192.168.25.1 in the URL box and then click Go. Enter admin as the username and password and click Submit.

After a few seconds all three devices should be listed in the Home Gateway IoT Server – Devices list.

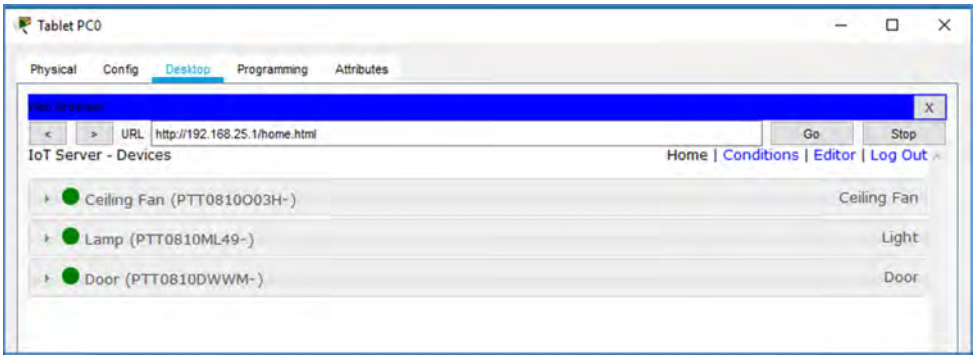


Figure 8.12:

Close the Tablet PC0 window.

(Optional PTA 1): Examine Packets in a Office

Objectives

In this activity, you will open a Packet Tracer file with an existing home network, explore the devices on the network, and then add additional wired and wireless IoT devices.

- Examine the current smart home network setup to understand the connected devices, their configurations, and the network architecture.
- Integrate wireless IoT devices into the smart home network by connecting them to the Wi-Fi network and configuring their settings.
- Connect wired IoT devices to the smart home network by physically linking them to the network infrastructure and setting up their configurations.

Part 1: Explore the Existing Smart Home Network

Step 1: Explore available IoT end devices

a. At the bottom left corner of the Packet Tracer window, locate and click the End Devices icon (`Ctrl + Alt + V`) in the top row, and the Home icon (`Ctrl + Alt + H`) in the bottom row.
b. The Device-Specific Selection box displays the many different Smart Home IoT devices available.
   Move the mouse pointer over each device and notice that the descriptive name of the device is displayed at the bottom of the Device-Specific Selection box. Take a moment to look at each device type.

Step 2: Explore the Smart Home network

a. In the Logical workspace is a prebuilt smart home network that consists of many wired and wireless IoT devices, and network infrastructure devices.
   When you place your cursor over a device, such as the Smart Fan, an informational window opens containing basic network information about that device.
b. To turn on or activate a device, hold down the `Alt` key, and then click the device you want to test. Try this on each of the smart devices to observe what they do.
c. Click the Home Gateway. The Physical tab is selected by default and shows a picture of the Home Gateway.
d. Click the Config tab, and then in the left pane click LAN to view the LAN settings of the Home Gateway.
   Record the IP Address of the home network for future reference.
e. Click Wireless in the left pane. Expand the window if necessary.
   Record the SSID of the home network.
   Record the `WPA2-PSK` Pass Phrase.
f. Click the Tablet device, and then click Desktop tab > Web Browser.
g. In the URL field, enter the IP address you recorded for the Home Gateway, and then click Go.
h. Enter `admin` for both the username and the password, and then click Submit.
i. A list of all the connected IoT devices appears. Click a device in the list to view its status and settings. Try interacting with some of the devices to see how you can manage their states from the Tablet. For example, open and close the Garage Door, turn on and off the Smart Lamp, and so on.

Part 2: Add Wireless IoT Devices to the Smart Home Network

Step 1: Add a wireless device to the network

a. In the Device-Specific Selection box, click the Wind Detector icon and then click in the workspace where you would like to locate the Wind Detector. (`End Devices > Home > Wind Detector`)
b. To configure the Wind Detector, click it, and then click the Config tab.
c. Change the Display Name to `Wind Detector`.
Note: To score correctly, the Display Name has to be the same as stated in the instructions.
d. At the bottom pane, change the IoT Server to `Home Gateway`.
e. Click `Wireless0` in the left pane. Change the Authentication type to `WPA2-PSK` and in the PSK Pass Phrase box, enter the pass phrase recorded in the previous part.
In a few seconds, a wireless connection should be formed between the Wind Detector and the Home Gateway. You can close the Wind Detector window.

Step 2: Verify that the Wind Detector is on the network

a. Click the Tablet.
b. If necessary, log back into the Home Gateway.
c. The device `Wind Detector` now appears at the bottom of the list of IoT Server - Devices.

Part 3: Add Wired IoT Devices to the Smart Home Network

Step 1: Cable a device to the network

a. In the Device-Specific Selection box, click Lawn Sprinkler (`End Devices > Home > Lawn Sprinkler`), and then click in the workspace where you would like to place it.
b. Click the Lawn Sprinkler, and then click Advanced at the bottom right corner. More tabs are now available.
c. Click the I/O Config tab.
d. In the drop-down menu for Network Adapter, change it to `PT-IOT-NM-1CFE` for a FastEthernet connection.
e. Cable the Lawn Sprinkler to the Home Gateway.
In the Device-Type Selection box, click the Connections icon (this looks like a lightning bolt). Click the Copper Straight Through connector type icon in the Device-Specific Selection box, and then click the Lawn Sprinkler icon and connect it to the `FastEthernet0` interface. Next, click the Home Gateway icon and connect the other end of the cable to an available Ethernet interface.

Step 2: Configure the Lawn Sprinkler for network connectivity

a. In the Lawn Sprinkler window, click the Config tab to edit the device configuration settings.
b. Set the Display Name to `Smart Sprinkler`.
c. Set the IoT Server to `Home Gateway`.
d. In the left panel, click `FastEthernet0`, and then click `DHCP` for the IP Configuration.

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

a. Click the Tablet.
b. If necessary, log back into the Home Gateway.
c. 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

a. 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.

b. Click the Water Level Monitor, and then click Advanced to display more tabs.
c. Click the Config tab and change the Display Name to `Water Meter`.
d. Set the IoT Server to `Home Gateway`.
e. Click `Wireless0` and verify the Water Meter is using `HomeGateway` as the SSID.
f. Configure the wireless network pass phrase.
g. Verify that it is configured to receive an IP address from the DHCP server on Home Gateway.
h. Click the I/O Config tab, and then change the number of Digital Slots to 1.
i. For the Usage setting, change it to Component.
j. 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

a. Click the Smartphone, and then Desktop tab > Web Browser.
b. Log into the Home Gateway.
c. 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.

(Optional PTA 1): Connect to a Home Gateway and Monitor Network

Objectives

In this activity, you will add a home gateway and several IoT devices to an existing home network and monitor those devices through the home gateway.

Note: This activity is scored. Be sure you change the Display Name when directed to do so or the scoring will not be accurate. Click Check Results at any time to view your progress.

- Establish a connection between the home gateway and the network by connecting it to the modem and configuring its network settings.
- Integrate end user devices, such as computers and smartphones, by connecting them to the network via Wi-Fi or Ethernet and configuring their network settings.
- Add IoT devices to the network by connecting them either wirelessly or through wired connections and setting them up for proper communication with the network.
- Pair Bluetooth devices with the network by enabling Bluetooth, making the devices discoverable, and connecting them through the network's Bluetooth settings.

Part 1: Connect a Home Gateway to the Network

Step 1: Add a Home Gateway

a. In the Device-Type Selection box, click Network Devices, and then Wireless Devices.
b. Click Home Gateway, and then click in the Logical workspace to add the device.
c. Click `Home Gateway0`, and then the Config tab. Change the Display Name to `Home Gateway`.

Step 2: Connect the Home Gateway to the cable modem

a. In the Device-Type Selection box, click Connections, and then Copper Straight-Through cable.
b. Click the Cable Modem and connect one end of the cable to Port 1.
c. Click the Home Gateway and connect the other end of the cable to the Internet port.

Part 2: Add End User Devices to the Network

Step 1: Add a wireless tablet to the workspace

a. In the Device-Type Selection box, click End Devices, and then Tablet. Add the Tablet to the workspace.
b. Click `Tablet PC0`, and then the Config tab. Change the Display Name to `Tablet`.

Step 2: Connect the tablet to the Home Gateway network

Notice that the Tablet is already connected to the cellular network. The blue wireless signal is connected to the Internet cloud where the cellular provider is located.

a. To connect `Tablet` to the home wireless network, click the `Wireless0` Interface on the left panel in the Config tab.
b. Change the SSID from `Default` to `HomeGateway`. The Tablet will connect to the home Wi-Fi network. It may take a minute or two for IP addressing to change to an address from the `192.168.25.x` network. You can click Fast Forward Time (`Alt+D`) to speed up the process.
c. Notice now that Tablet has two wireless connections: cellular and Wi-Fi. This is common for cellular enabled tablets and smartphones.

Step 3: Access the home gateway from the tablet

From the Tablet, click the Desktop tab > IoT Monitor. Note the IoT Server Address is the IP address of the Home Gateway, and admin is used for both the username and password. Click Login.

Note: This verifies you can access the Home Gateway IoT Server. Note that no devices appear in the Home Gateway IoT Server - Devices list yet.

Part 3: Connect IoT Devices to the Network

In this part, you will add three new IoT devices to the network and register them to the Home Gateway server.

Step 1: Add IoT device to the wired network

In this step, you will connect a new IoT device to the wired network.

a. In the Device-Type Selection box, click `End Devices > Home`, and then click the `Lamp` and add it to the workspace.
b. Click the `Lamp` device, and then click Advanced to reveal more tabs.
c. Click I/O Config to change the Network Adapter to `PT-IOT-NM-1CFE`.
d. Click the Config tab and rename the device as `Lamp`.
e. In the left panel, click `FastEthernet0`, and then select the `DHCP` radio button so that the lamp will receive an IPv4 address from the Home Gateway.
f. Click `Connections > Copper Straight-Thru` and connect the `Fastethernet0` port of the Lamp to one of the available Ethernet ports on Home Gateway.

Step 2: Add IoT devices to HomeGateway wireless network

In this step, you will connect two new IoT devices to the wireless network.

a. In the Device-Type Selection box, click `End Devices > Home`. Add a `Fan` and a `Door` to the workspace.
b. Change the display name of the fan to `Fan`.
c. Change the display name of the door to `Door`.
d. In the `Wireless0` configuration for each device, notice that the SSID is already set to `HomeGateway` and that each device received an IP address from the `192.168.25.x` network. You may need to click Fast Forward Time to speed up the process.

Step 3: Configure IoT devices to register with the Home Gateway server

For each of the three IoT devices, click the Config tab, then Settings in the left panel, if necessary. Scroll down to the IoT Server options list and click Home Gateway.

Step 4: Verify that the devices are now registered with the Home Gateway server

From the Tablet, click the Desktop tab > IoT Monitor, and then click Login. You should see entries for all three of the new IoT devices. Expand the entries to see details for the devices. Try controlling the devices and look at the results in the workspace.

Note: It may take a minute or two for the three devices to register with the server and be listed in the IoT Monitor.

Part 4: Add Bluetooth Devices

In this part, you will add a Bluetooth speaker to the wireless network. You will connect a portable music player to the speaker.

Step 1: Add a Bluetooth speaker to the wireless network

a. In the Device-Type Selection box, click `End Devices > Home`. Add a `Bluetooth Speaker` device to the workspace.
b. Notice the speaker automatically connected to the Home Gateway. After a few minutes, the speaker will be configured with an IP address from the `192.168.25.x` network.
c. Change the Display Name of the speaker to `Speaker`.
d. In the Config tab for the speaker, click Bluetooth in the left panel, and then turn Port Status to On.

Step 2: Add a portable media player to the wireless network

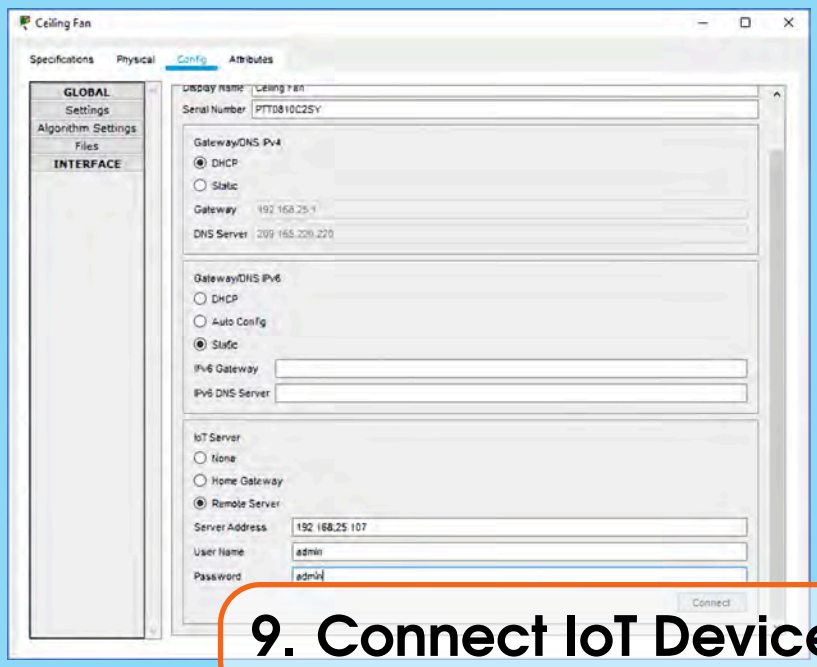
a. In the Device-Type Selection box, click `End Devices > Home`. Add a `Portable Music Player` to the workspace.
b. Notice the music player automatically connected to the Home Gateway. After a few minutes, it will be configured with an IP address from the `192.168.25.x` network.
c. Change the Display Name to `Music Player`.

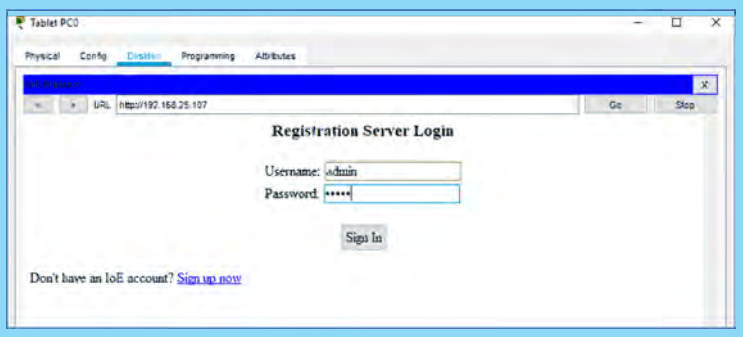
Step 3: Pair the music player to Speaker

a. Turn Bluetooth Port Status to On.
b. Click Discover under Discoverable Devices, click Speaker, click Pair, and then click Yes.
c. Hold down the `Alt` key and click Music Player. (Hint: Make sure the speakers for your physical computer are on.)

Step 4: Explore the network

Feel free to add more wired and wireless devices to the network. For IoT devices, hold down the `Alt` key and click the devices to interact with them. With the `Alt` key depressed, you can turn on the Music Player, open the Door, and turn on the Lamp and Fan. Don't forget that you can also control the IoT devices from the IoT Monitor app on the Smartphone or Tablet.





9. Connect IoT Devices to a Registration Server

Objectives

- Configure IoT devices to register with a remote server, enabling centralized control and monitoring of smart devices .
- Set up and manage a registration server, exploring its configuration options and understanding its role in IoT networks .
- Use registration servers to control and monitor smart devices, enhancing knowledge of centralized IoT device management .
- Test connectivity and functionality of IoT devices through a registration server, ensuring proper integration and operation within the network .

Registering Devices to a Dedicated Registration Server

IoT devices can also be registered to a dedicated Registration Server for remote monitoring, configuration, or programming. The dedicated registration server has the benefit of being able to provide many other services to your network, such as Web, DHCP, DNS, email, and FTP. With a dedicated server, IoT devices would first be connected to a wireless network and would then be configured to register to the server.

With a dedicated server, IoT devices would first be connected to a network and would then be configured to register to the server. The registration server can be on the local home network or on a network outside of the home that can be accessed over the internet. This remote configuration enables control of the Smart Home from the internet in the same way that real smart home IoT networks are controlled by the homeowner.

To connect and configure the registration server:

- Connect the server to your network using a wired or wireless connection.
- Click on the server and select Desktop/IP configuration. Ensure that DHCP has been turned on and then verify that the server is obtaining an IP addresse.
- Select Services/IoT and turn the Registration Server on.

To configure a remote device to interact with the registration server:

- Connect a remote device such as a tablet, PC, or smart phone to the wireless network.
- Click on the remote device and select Desktop/Web Browser. Use the IP address of the registration server as the URL.
- The first time you access the server, you will have to create a user login. Subsequent visits will require you to login using the login credentials. For security reasons, it is important to protect your IoT devices by using strong passwords on your server.

To register IoT devices with the Dedicated Server:

- Click on each device and select the Config tab.
- Select the remote server option under IoT server and supply the IP address of the server, plus the login information.
- Use the remote device to verify the presence of the registered IoT devices.

Video — Registering Devices to a Dedicated Registration Server I . This is our Cisco Packet Tracer connecting IoT devices to a designated registration server walkthrough video. We're going to step away from the home gateway wireless router and we're going to switch out to using a server that exists on the internet to interconnect our IoT devices. Watch this video to learn about creating and controlling a small IoT home network using a dedicated registration server.

Connect and Control Devices using a Registration Server

In this activity you will add a remote registration server and several IoT devices to an existing home network and monitor those devices through the remote registration server.

The Smart Home Network

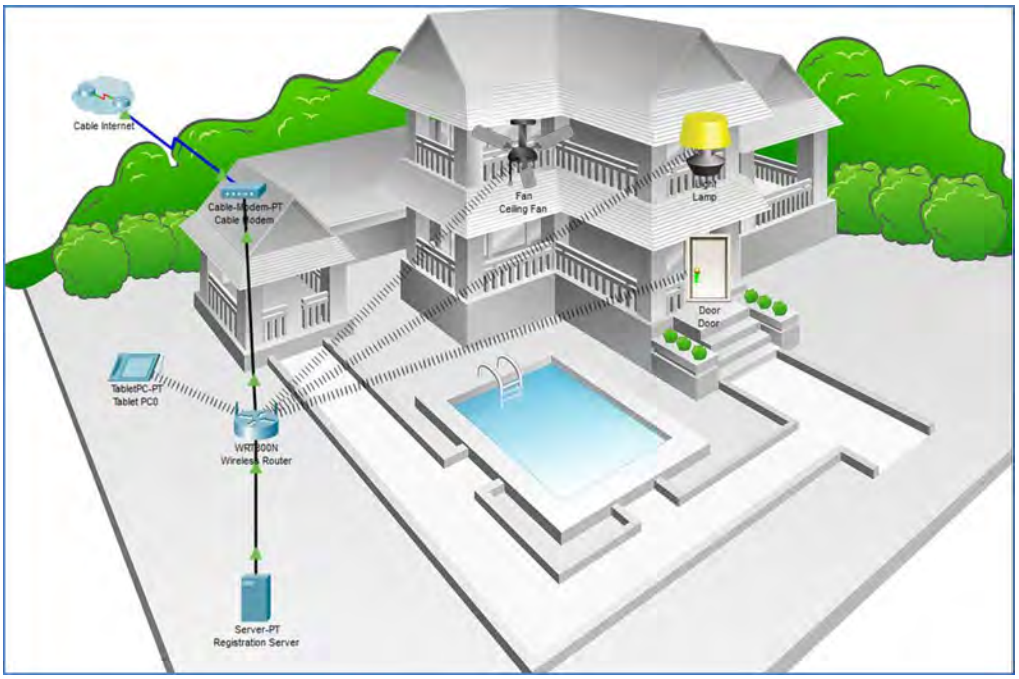


Figure 9.1:

Objectives

- Part 1: Add a Registration Server to the Network

- Part 2: Register IoT Devices to the Registration Server

Background / Scenario

In this activity you will add a registration server and several IoT devices to an existing home network and monitor those devices through the registration server.

Part 1: Add a Registration Server to the Network

Step 1: Open the Registration Server.pkt file and save the file to your computer

Step 2: Add a registration server on the network

a) Place the Server end device onto the workspace and connect it to the home gateway. Find the Server in the End Devices Selection box and drag it to the workspace.

Figure 9.2: Find the Server in the End Devices

b) b. Connect the server to the wireless router.
Using a copper straight-through cable, connect the server to the wireless router.

c) Enable the registration server service on the server.
Click the server in the workspace to open the configuration window. Click the Services tab and then click the IoT service in the left pane. Click the “On” button to enable the service.

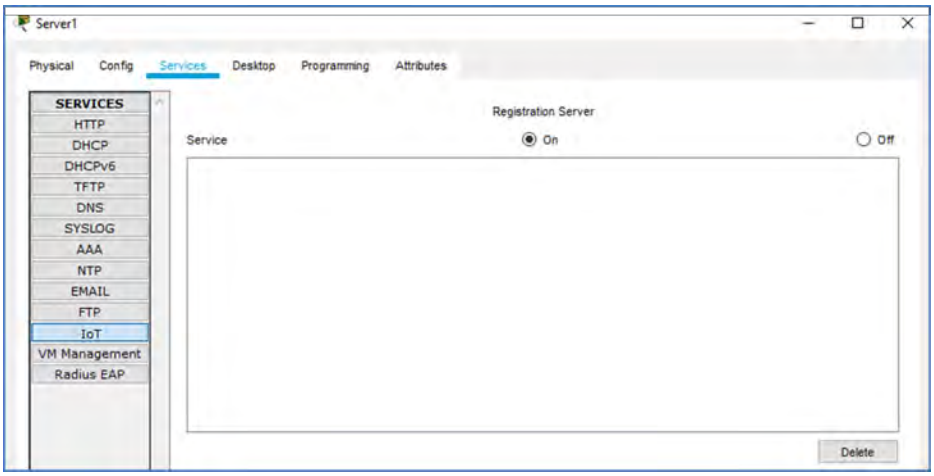


Figure 9.3:

d) d. Configure the server.
Click the Config tab. In the Global Settings window change the Display Name to Registration Server and change the DHCP/DNS IPv4 setting from the default Static to DHCP.

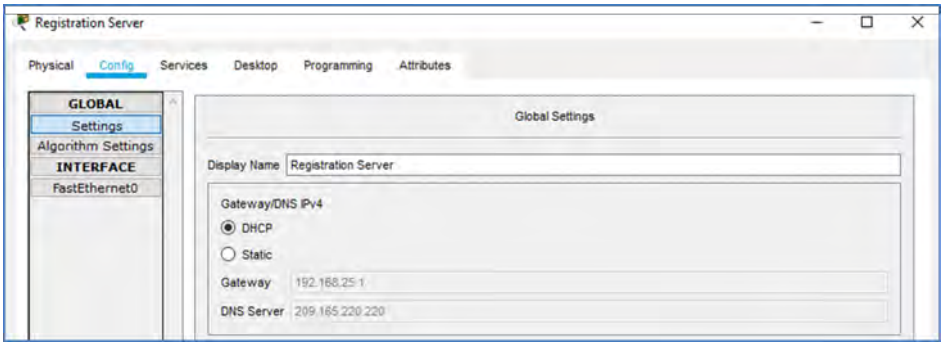


Figure 9.4:

Verify that the server has received an IPv4 address from the home gateway by clicking the Desktop tab and then the IP Configuration icon.

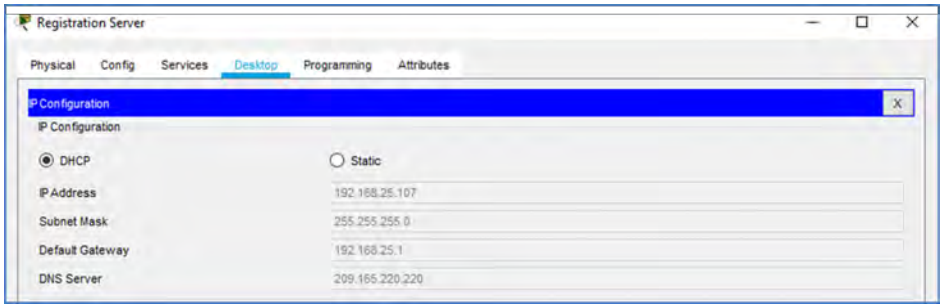


Figure 9.5:

Note that, in this example, the IPv4 address assigned to the server is 192.168.25.107. Yours may be different.
Close the Registration Server window.

Part 2: Register IoT Devices to the Registration Server

Step 1: Create a registration server account

a) a. Click the Tablet icon to open the Tablet configuration window. Click the Web Browser icon in the Desktop tab. Enter the IPv4 address of the Registration Server in the URL box and then click Go.
Because there is no IoT account created yet, one will need to be created. Click the Sign Up Now option.

Figure 9.6:

Select a username and password and then click Create to create the IoT account.

Figure 9.7:

Notice in the IoT Server – Devices window there are no IoT devices listed. This is because all the devices are still registered with the home gateway.

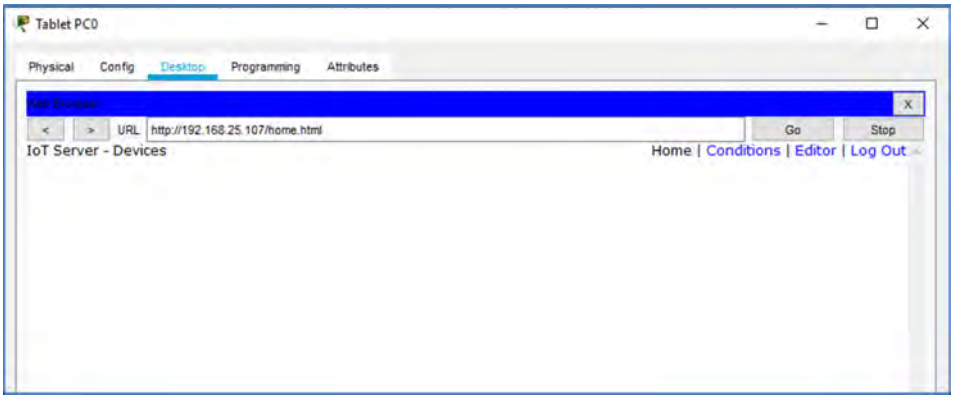


Figure 9.8:

Close the Tablet PC0 window.

Step 2: Register IoT devices to the registration server

a) Configure the ceiling fan to register with the registration server.
Click the Ceiling Fan icon in the workspace to open the device configuration window and then click the Config tab. Change the IoT Server type from Home Gateway to Remote Server. Enter the IP address of the registration server from Part 1, and the IoT account Username and Password created in Step 1 above. Next, click the Connect button.

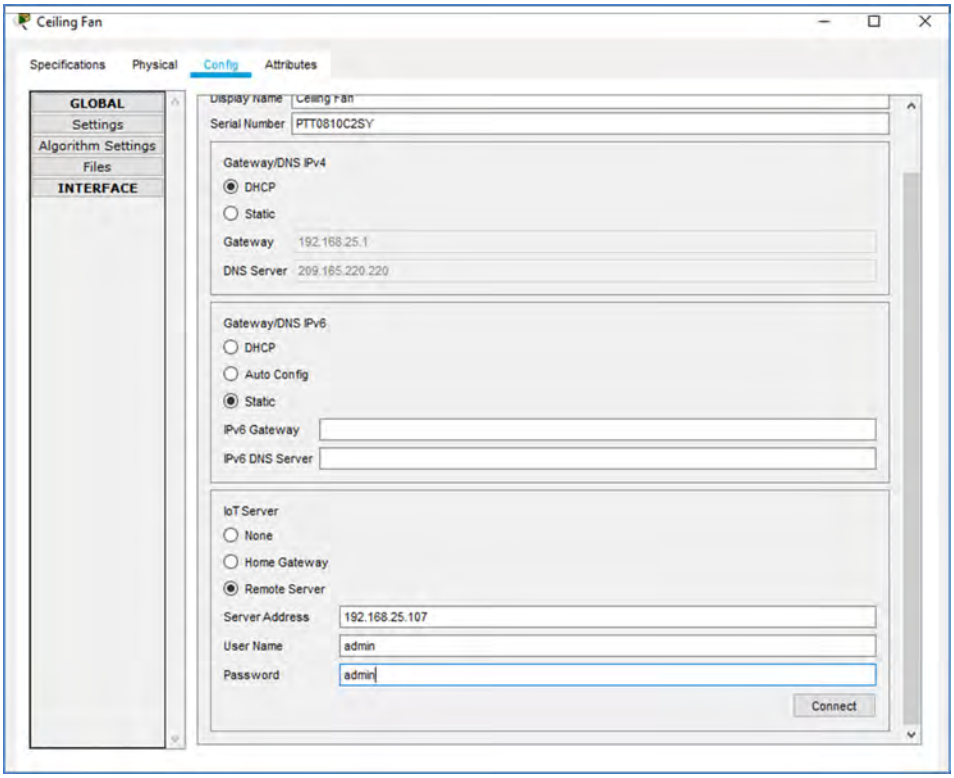


Figure 9.9:

Close the Ceiling Fan window.

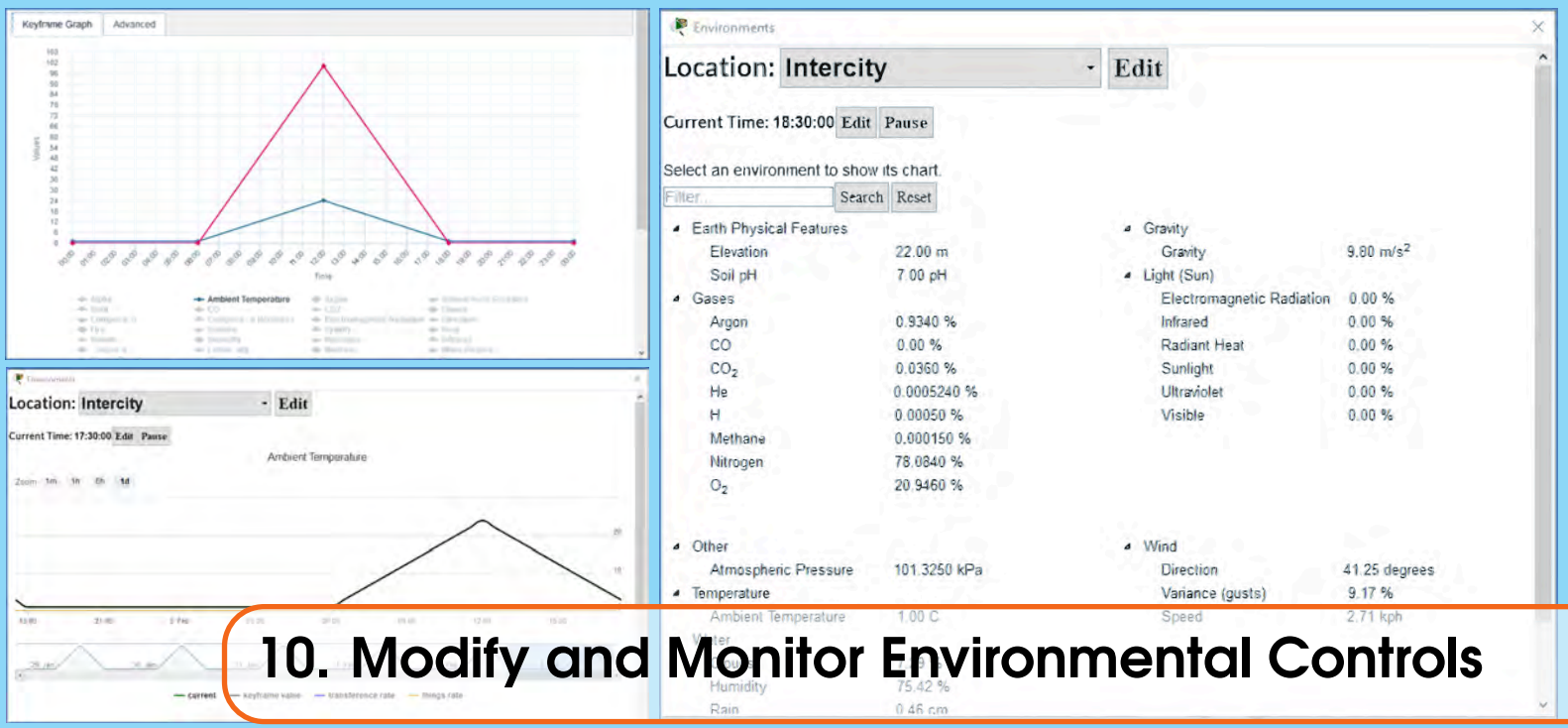
b) Configure the lamp and the door IoT devices to register with the registration server in the same manner.

Step 3: Verify that the IoT devices are registered to the registration server

Access the IoT registration server through the wireless Tablet web browser using credentials from Step 1 above.

The three IoT devices, the ceiling fan, the lamp, and the door should now be registered with the IoT server. Close the Tablet PC0 window.

Step 4: Close Packet Tracer



10. Modify and Monitor Environmental Controls

Objectives

- Learn to modify and monitor environmental controls within smart homes or buildings, gaining hands-on experience with IoT devices.
- Experiment with setting up and adjusting sensors and actuators to react to environmental changes such as temperature, light, or humidity.
- Configure and test automated responses for environmental conditions, such as turning on a fan or adjusting lighting based on sensor readings.
- Utilize IoT platforms and software tools to remotely monitor and control environmental controls, exploring the benefits of smart environments.

Packet Tracer Environment Controls

In this section, you will learn:

- The environmental controls that are available in Packet Tracer.
- How to configure environmental controls within containers.
- How smart devices interact with the Packet Tracer environmental elements.
- How to adjust environmental elements.
- How to set conditions and take action.

In the Physical Workspace there are containers. Each container, the intercity, city, buildings, and wiring closets, all have their own set of environmental values. There are 24 default environmental elements, such as temperature, rain, water level, wind speed, and snow. Many devices or Things affect or respond to the environment in some way. A Fire Sprinkler will raise the water level and humidity in a container. An old car will increase various gases and ambient temperature when turned on. A smoke detector can be used to trigger an alarm when the smoke in environment increases to a certain point.

If there are no devices configured to affect the environment, their values are looped on a 24-hour cycle. For example, the sun will come up at 6am and set at 6pm. The ambient temperature will

peak at 25°C at noon. This cycle is set on the intercity level and its ambient temperature range will propagate all the way down to the main wiring closet automatically. If a heater is added to the Corporate Office and turned on, the temperature inside the Corporate Office will increase along with all the containers within it.

Note however, the heater does not heat up the parent container, Home City, it will only heat up the child containers. When the heater is turned off, the Corporate Office will eventually converge to the parent container's ambient temperature, Home City, based on its transference value. Different containers may have different levels of insulation and thus different transference values; the transference values determine the rate that the child container converges with the parent container and works the same way for all environment types.

Video — Environmental Controls available in Packet Tracer I . This is our Cisco Packet Tracer, Environmental Controls walkthrough video. In this video, we're going further than just basic IoT devices. Here, we're going to talk about environmental conditions that exist within Cisco Packet Tracer itself. Watch this video to see the environmental elements available, how they work and how to modify them.

Configuring the Environment using Containers

Important terms and concepts:

- **Current time** – time inside a container that increments by 30 minute increments. Every 1 second in real time equates to 30 minutes in "Container" time. The timer goes from 0 (midnight) to 11:59. (Figure 10)
- **KeyFrame** – represents a single moment in time
- **KeyFrame graph** – A graph that shows the value of environmental elements at any given point in time throughout the day. (Figure 10)
- **Transference** - values that determine the rate that the child container converges with the parent container and works the same way for all environment types.

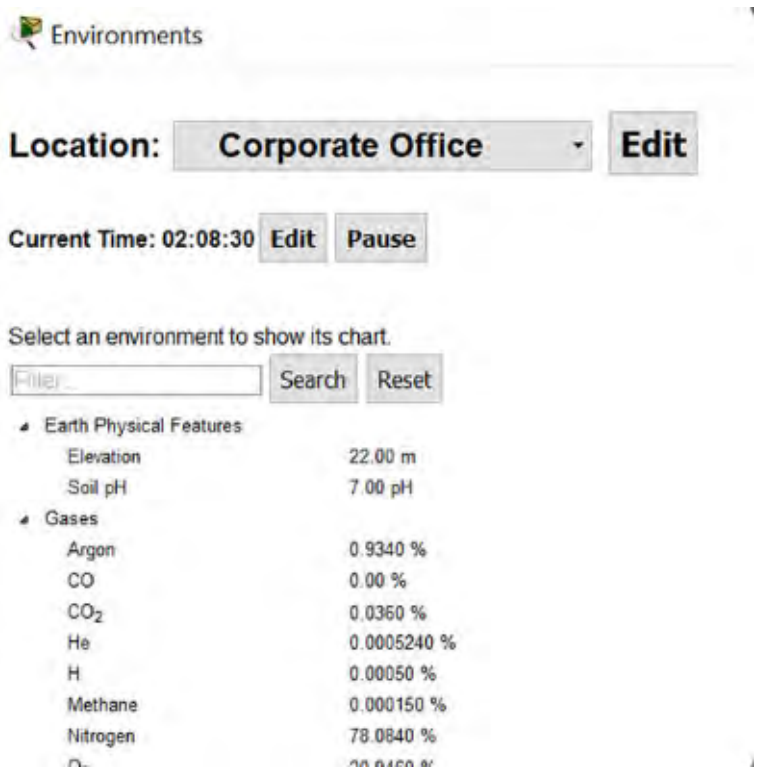


Figure 10.1: Current time

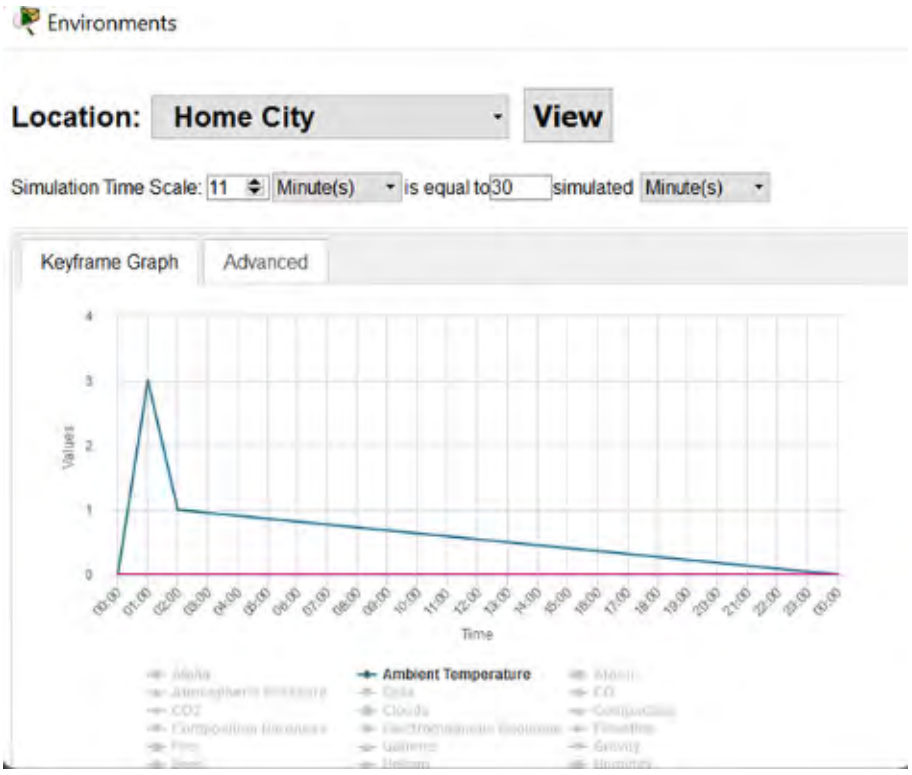


Figure 10.2: KeyFrame graph

To modify environmental elements within a container:

1. Select Environmental from the top right hand corner of the Physical view.
2. Select the appropriate container location.
3. Modify the time, if required.
4. Select Environmental Values/Edit – a keyframe graph will appear.
5. Select the Advanced tab and modify the required environmental conditions using the drop-down boxes as required.
   Note: Remember to hit enter after modifying a value to add that value. (Figure 10)
6. The modified values will be reflected immediately in the keyframe graph.
7. You can also manipulate the graph by dragging the timeline to modify the time and value of a particular environmental value.

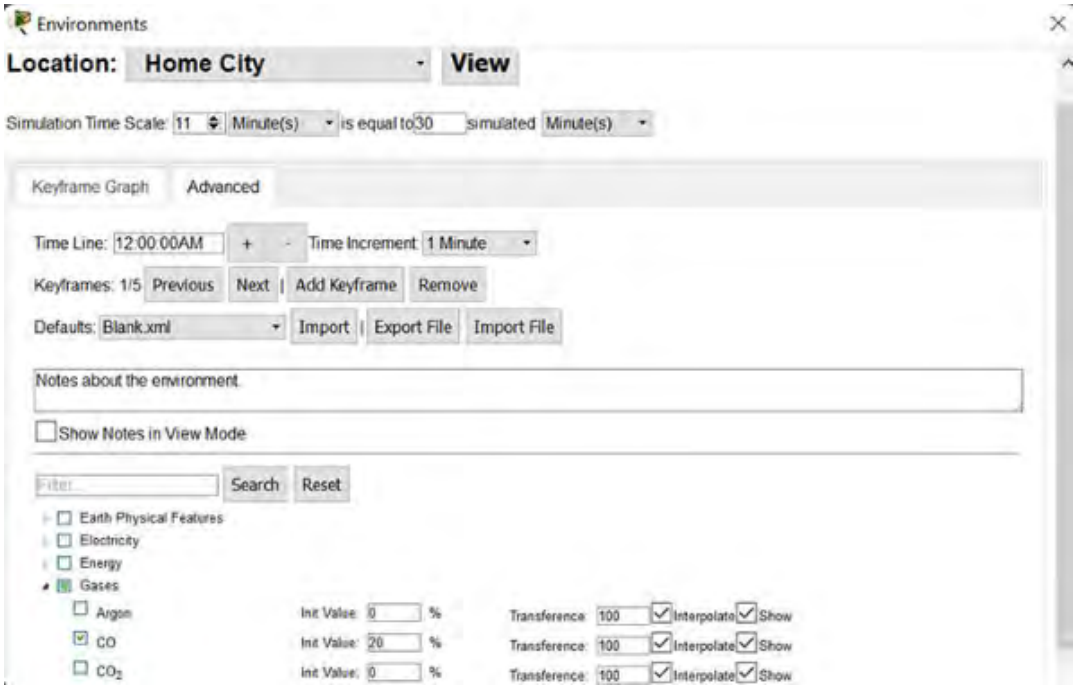


Figure 10.3: Advanced tab

Modify and Monitor Environmental Controls in Packet Tracer

In this activity you will use the Physical view in Packet Tracer to view and edit the environmental controls.

The Smart Home Network

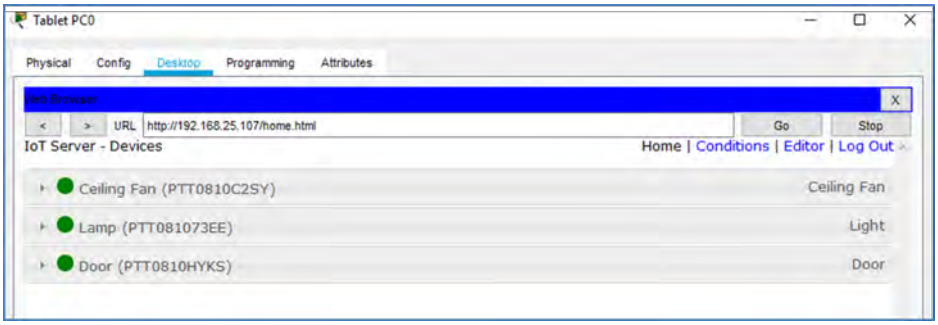


Figure 10.4:

Objectives

-
- Part 1: Explore Environmental Controls
- Part 2: Edit Environment Elements

Background / Scenario

In this activity you will use the Physical view in Packet Tracer to view and edit the environmental controls.

Part 1: Explore Environmental Controls

Step 1: Open the PT Environmental Controls.pkt file and save the file to your computer

Step 2: View the current environment values

a) Change to the Physical view in Packet Tracer.
Click on the Physical icon in the top left corner of the Packet Tracer workspace.

Figure 10.5:

b) Open the Environments window.
Click on the Environment button on the far right of the Packet Tracer Physical view menu bar.

Figure 10.6:

c) Explore the many environmental elements in the Intercity location.

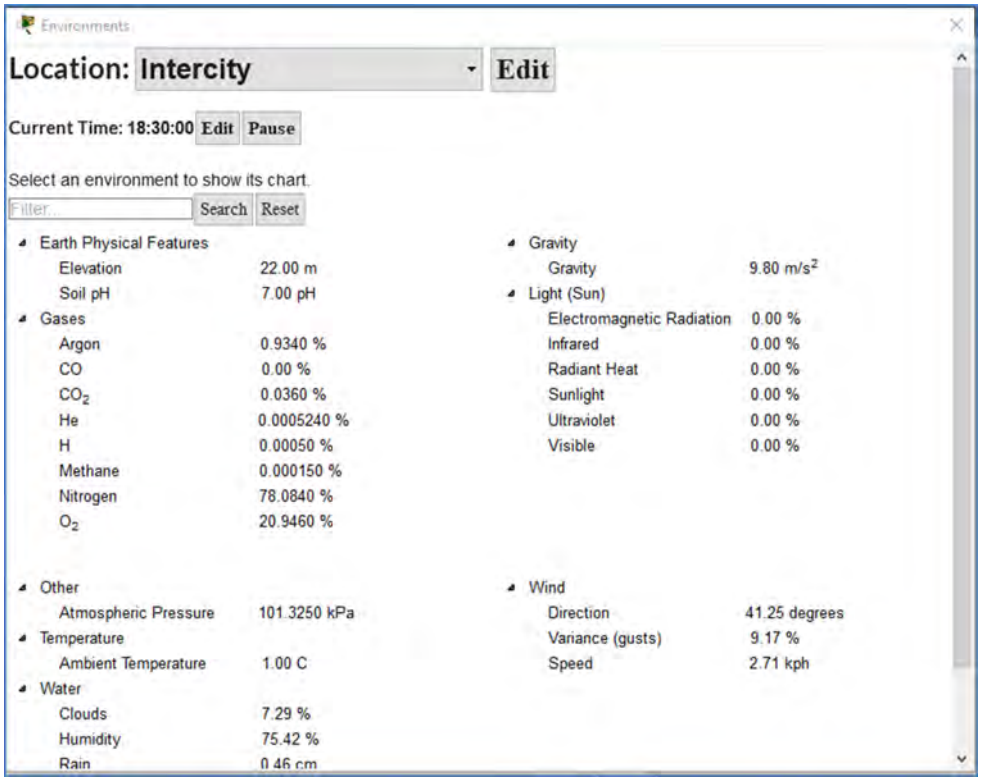


Figure 10.7:

d) Observe ambient temperature chart.
Scroll down the Environments window to the Temperature element and notice that the Ambient Temperature changes in degrees Celsius through the simulated 24 hour day period.

Figure 10.8:

Click on the Ambient Temperature element to open the Ambient Temperature chart. Keep the Environments window open for a few minutes to simulate several simulated days in the Packet Tracer environment.
Notice that after a few minutes the chart shows the temperature fluctuations over time.

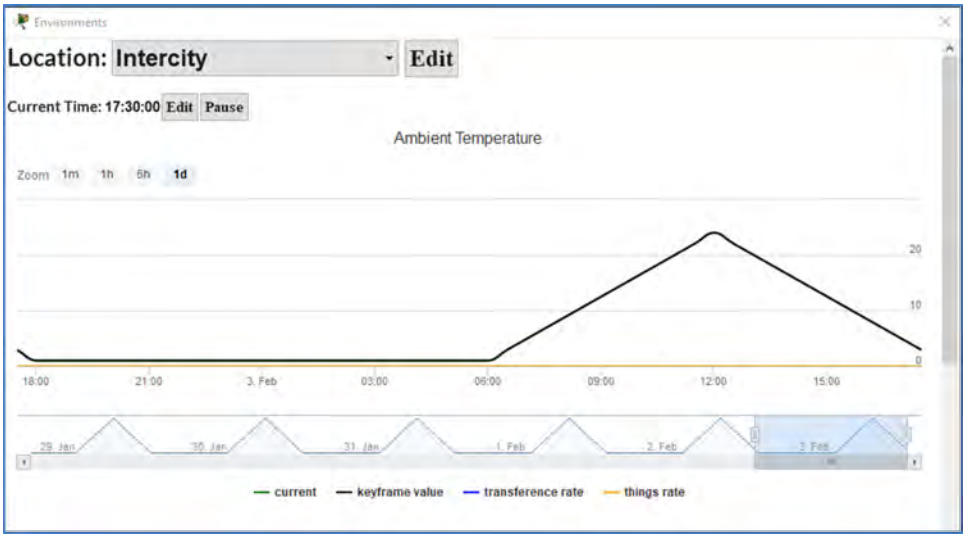


Figure 10.9:

e) Experiment with other environmental elements.
Click on other environmental elements and observe their charts over time. Do not close the Environments window. We will use it in part 2.

Part 2: Edit Environmental Elements

Step 1: Change to environment edit mode

a) Click on the Edit button for the Intercity location

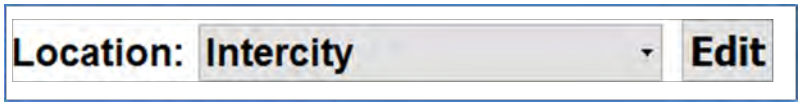


Figure 10.10:

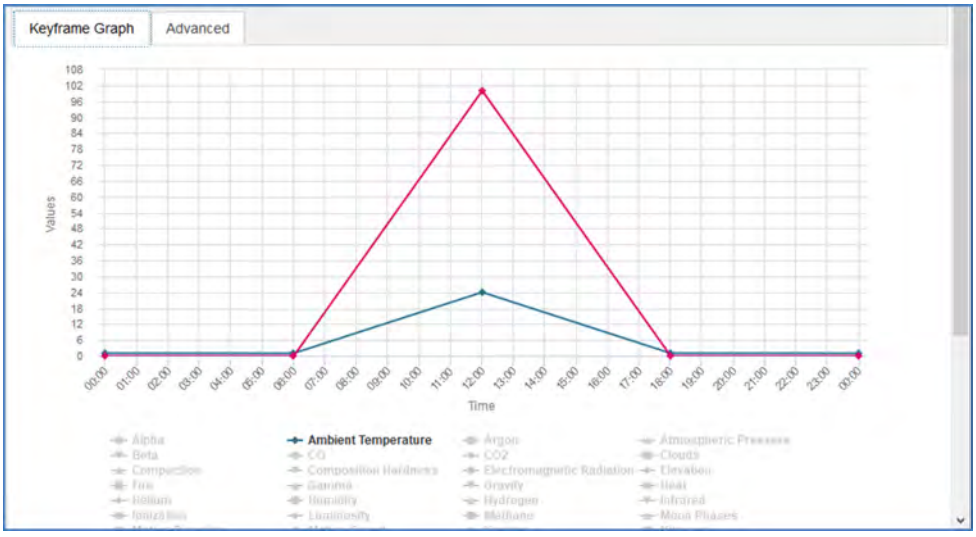


Figure 10.11:

Step 2: Edit the Ambient Temperature

a) Note the current Ambient Temperature setting
The Environment Keyframe Graph for the ambient temperature shows degrees Celsius starting at a low of zero degrees at midnight and a high of 24 degrees at midday.

b) Change the ambient temperature for the Intercity.
Using the Environment Keyframe Graph, change the ambient temperature for the 24 hour day by clicking on the blue Ambient Temperature line and dragging it up the graph.
To simulate a summer environment make the following changes:
Drag the beginning and end temperatures to 20 degrees, the 06:00 and 18:00 temperatures to 28 degrees and the mid-day temperature to 37 degrees.

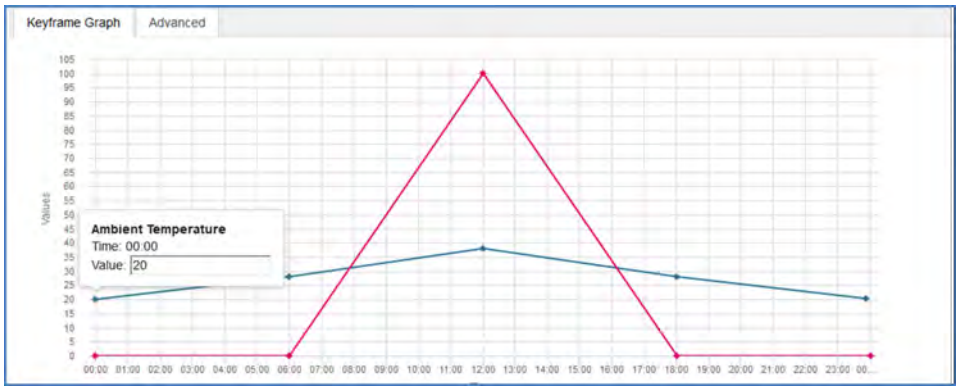


Figure 10.12:

Step 3: Observe changes in the environment

a) Return to Environment View mode
Click the View button for the Intercity location

Figure 10.13:

Note that the Ambient Temperature chart is now showing the temperature increase.

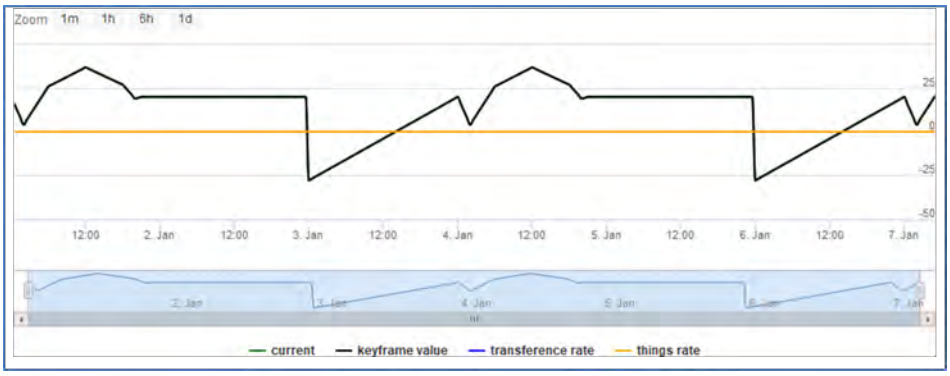


Figure 10.14:

Close the Environments window.

(Optional PKA 1): Modify and Monitor Environmental Controls

Objectives

IoT devices frequently use sensors to monitor the physical environment, and actuators to act in response to the conditions that are detected in the environment. Packet Tracer includes an interface for modifying environmental factors to test and activate IoT devices.

In this activity, you will learn how to edit Packet Tracer environmental controls.

- Investigate the available environmental controls to understand how to manage and adjust settings such as temperature, lighting, and humidity.
- Modify the environmental elements by changing their settings or configurations to achieve the desired conditions within the environment.

Part 1: Explore Environmental Controls

Step 1: Observe the Environmental Controls interface

To view the current environment values, do the following:

a. To open the Environments window, click Environment (`Shift+E`) on the far right of the Logical toolbar. The button displays a simulated 24-hour clock.
b. Explore the many environmental elements in the Intercity location.
c. Locate the Ambient Temperature element and notice that the temperature changes throughout the simulated 24-hour day period.
d. Click Ambient Temperature to open the Ambient Temperature chart. If necessary, scroll to the top of the Environments window to see the temperature fluctuations over time.
e. Explore the other environmental elements by clicking in the list and observing the charts over time. Notice the Hide Chart button, which you can click, if you wish to hide the chart.
f. You will continue using the Environments window in Part 2. To keep it open and on top, scroll to the bottom of the window and click Always on Top.

Part 2: Edit Environmental Elements

Step 1: Change to environment edit mode

With the Ambient Temperature chart open, click Edit next to the Intercity location.

Note: Do not click the Edit button next to the Current Time.

Step 2: Investigate the Ambient Temperature Keyframe Graph

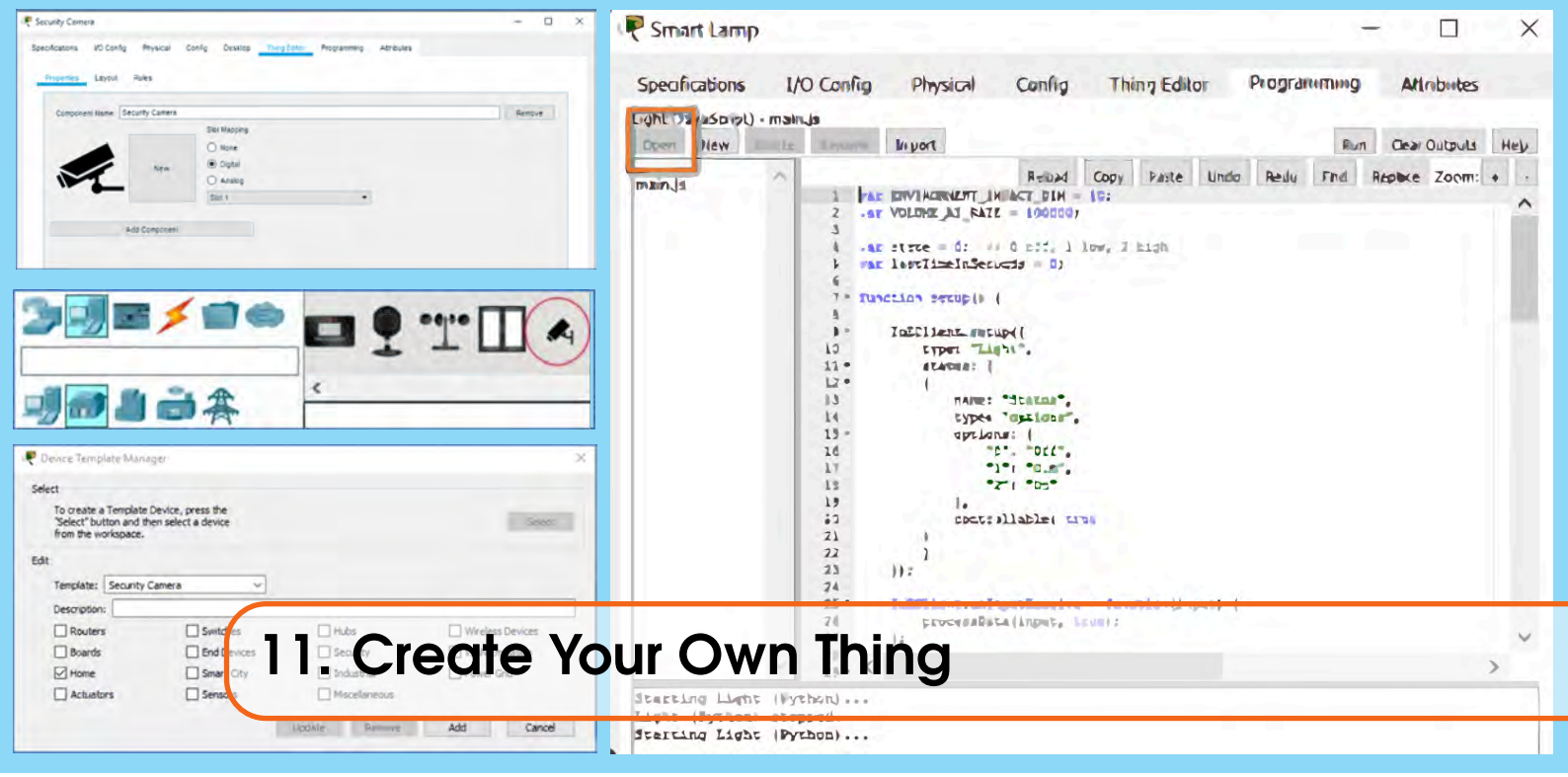
a. Scroll down and click the Sunlight entry below the chart to hide the Sunlight element.
Note: You may need to expand the height of your Environments window to see all the elements.
b. The environment Keyframe Graph tab for the ambient temperature shows degrees Celsius starting at a low of 0° at midnight and a high of 24° at midday. Notice the five small diamond handles at different times on the chart: 00:00, 06:00, 12:00, 18:00, and 23:59. Hovering your mouse over the small diamond handles reveals those times. These are keyframes.

Step 3: Change the ambient temperature for Intercity

You can change the ambient temperature for the 24-hour day by clicking and dragging each keyframe to the desired temperature value. Alternatively, you can enter the value in the popup box and press Enter to change the value. To simulate a summer environment, make the following changes. Set the beginning and end temperatures to 20°, the 06:00 and 18:00 temperatures to 28° and the mid-day temperature to 37°.

Step 4: Observe changes in the environment

a. Click View button for the Intercity location. Note that the Ambient Temperature chart is now showing the pattern of temperature changes that you configured in the previous step.
b. Look at the Ambient Temperature value in the table of environmental factors. Note that Packet Tracer interpolates between the key frame values to continuously vary the temperature. You should see the Ambient Temperature value vary from 20° to 37°.



11. Create Your Own Thing

Objectives

- Explore the customization of IoT devices, learning how to create and personalize smart devices for specific applications.
- Understand the components and architecture of a Thing, including sensors, actuators, and controllers.
- Develop skills in configuring and programming custom IoT devices, enabling unique and functional smart systems.
- Test and troubleshoot personalized IoT devices, ensuring they function correctly within an IoT network and achieve desired outcomes.

Creating and Programming Objects in Packet Tracer

In this section, you will learn:

- How to create a new Thing.
- How to connect your new Thing to the network.
- How to use available scripts for the new Thing.
- How to access the programming environment.
- How to review and modify existing scripts.

Creating and Connecting a Thing

Before attempting to create a new Thing, you need to decide what the Thing will do, how it will connect to the network, and how it will work. You need to find graphics to represent the states of your new Thing. Usually you will need two graphics, one to represent the beginning or default state and another to represent the end state. You also need to identify an existing Thing that functions in a similar manner as the new Thing. The existing script can then be modified to create the new script. Clicking on any IoT device that is in the workspace will reveal the specifications about that device. The specifications include:

- Features – how the device works or what it does. Devices can generate high and low values

based on a button being pushed or toggled on and off or they can detect certain environmental values (eg. Smoke or sunlight)
- Usage – Things may connect to other IoT devices in order to receive LOW or HIGH inputs or it may read the variable set in the Environment object
- Direct Control – shows you what keystrokes will allow you to physically interact with the Thing
- Local and Remote Control – shows how to control the Thing locally or remotely (if applicable)
- Data Specifications – how the values are produced or the port/slot used to connect to the sensor
- Example – Describes an example of how it works.

To create the new Thing:

1. Click the Advanced tab/Thing Editor from within the existing object specifications page.
2. Associate the new graphics to their respective states by clicking on a state and browsing to the location of the graphic on your local device. The images will be saved automatically.
3. Click on the Config tab to select the network adaptor to be used to connect to the network (if applicable).

To save the new Thing:

1. Select Tools/Custom Device Dialog from the uppermost toolbar.
2. Within the Device Template Manager.
   (a) Click on Select and click on the Thing to be saved.
   (b) Modify the template and description as appropriate.
   (c) Click on the type of new Thing.
   (d) Click on Add – the new template will be saved in the PT template file on the local disk and the customized Thing will now display with the other sensors.

NOTE: This local version of Packet Tracer, with the new Thing, can be sent to another user as long as the user also has the new template on their local disk.

Video — Creating and Connecting a Thing | . This is our Cisco Packet Tracer, Creating a Thing walk-though video. Watch this video to see how to create, modify, and save a new Thing.

The Smart Home Network

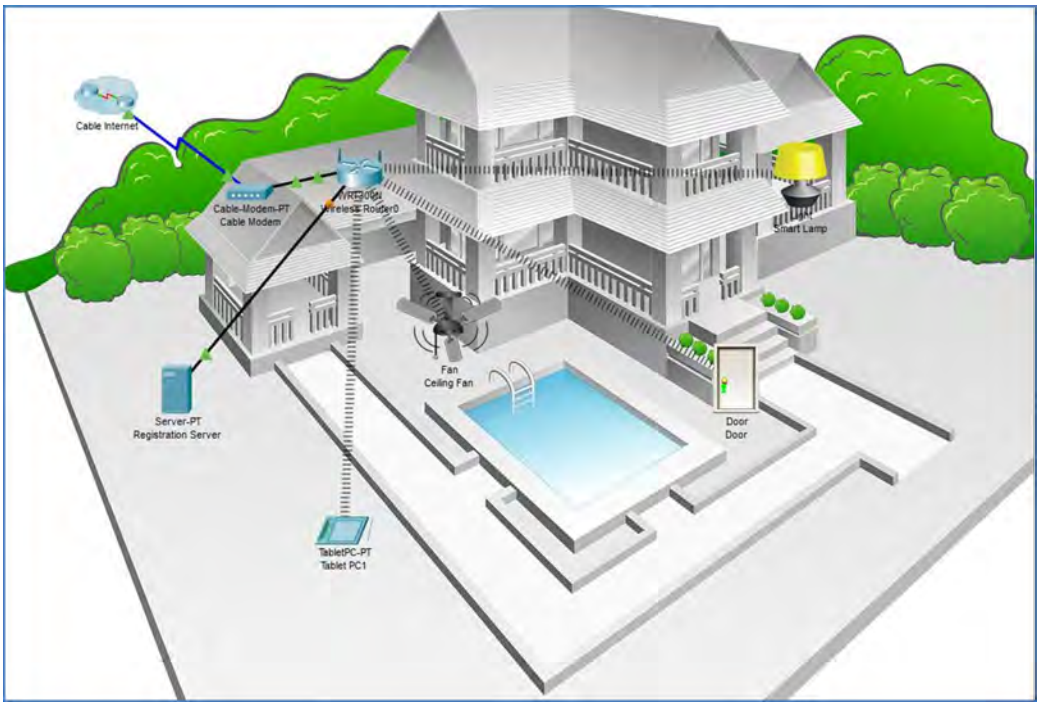


Figure 11.1:

Objectives

- Part 1: Create Your Own Thing
- Part 2: Save Your Own Thing

Background / Scenario

In this activity you will create a new IoT Thing, a security camera, and save the new Thing in Packet Tracer.

Part 1: Create Your Own Thing

Step 1: Open the Create Your Own Thing.pkt file and save the file to your computer.

a) Add a new device to the workspace.Select the Thing component from the device selection box.

Figure 11.2:

b) Change the display name of the device.
Click on the Thing in the Packet Tracer workspace to open the device configuration window. Click on the Config tab and then click on the Global Settings in the left side pane. Change the Display Name of the device to Security Camera.

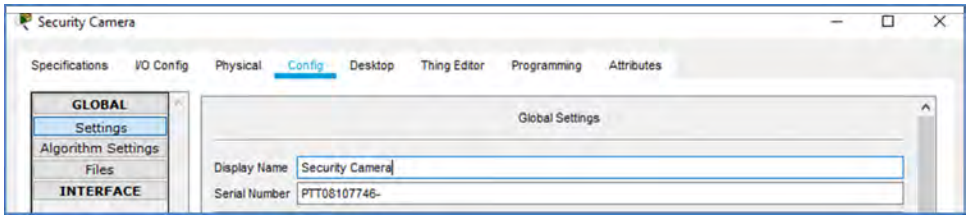


Figure 11.3:

Step 2: Change the device properties and icon.

Click on Advanced button in the bottom right of the device configuration window, then click on the Thing Editor Tab, and then the Properties tab.

Change Component Name to Security Camera.

Change Slot Mapping to Digital and Slot Number to 1.

To add an icon graphic, click the New button.

The Choose Image window will open allowing you to browse for a new icon. You can download a picture or graphic of a security camera from the Internet then browse to that directory to add it as a new icon.

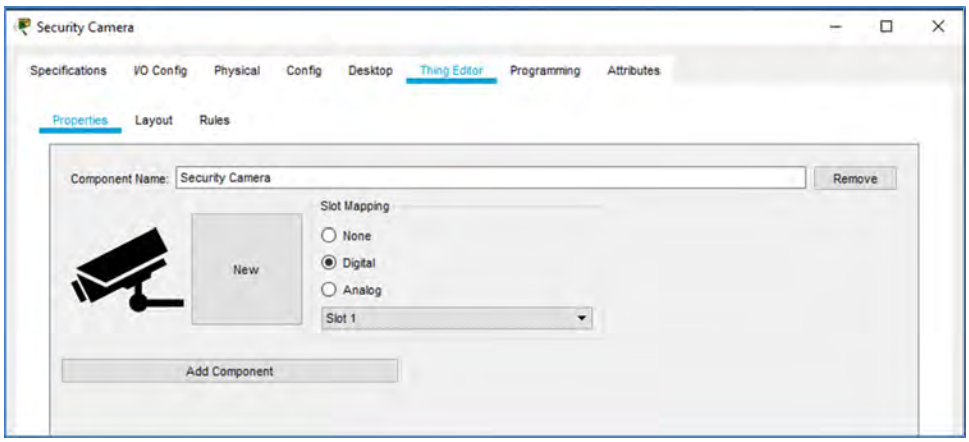


Figure 11.4:

Step 3: Add the security camera to the network.

a) Add a network adapter to the security camera.
Click on the Advanced button and then click on the I/O Config tab.
In the I/O Config window change the Network Adapter dropdown menu to the PT-IOT-NM-1CFE adapter. This is a copper Fast Ethernet cable adapter. (alternatively, the wireless adapter PT-IOT- NM-1W could be used to add the camera to the wireless network).

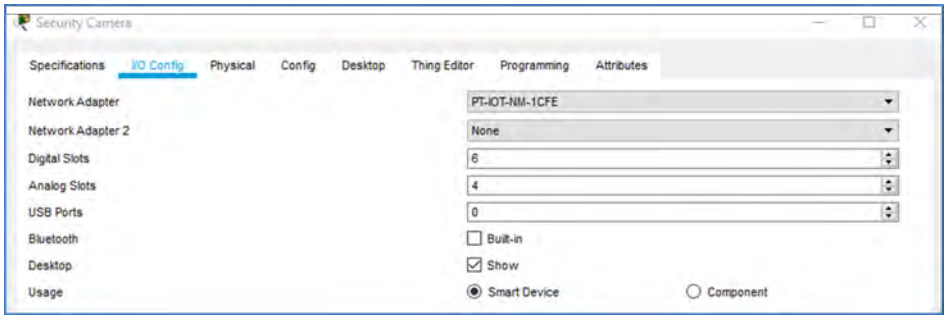


Figure 11.5:

b) Attach the security camera to the wired network.
Add a copper straight through cable from the Connections selection box from the camera FastEthernet port to an available Ethernet port on the wireless router.

c) Configure the security camera for DHCP.
Click on the Config tab and then click on the FastEthernt0 interface in the left side pane. Change the IP Configuration to DHCP.

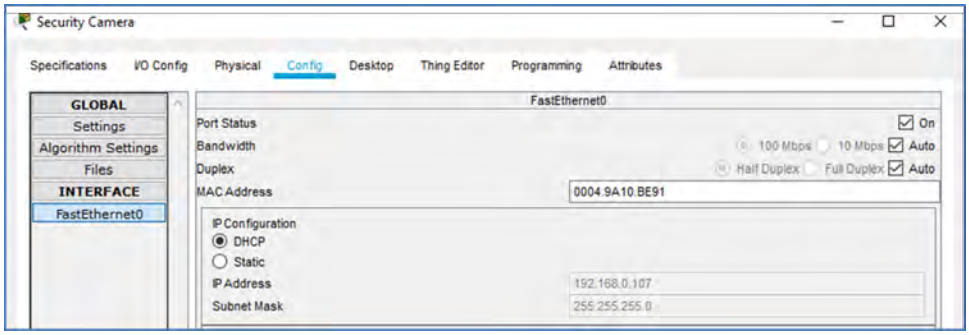


Figure 11.6:

Close Security Camera configuration window.

Part 2: Save the New Device

Step 1: Save the security camera as a Packet Tracer template.

a) Save the security camera using the Device Template Manager.
Click on Tools in the Packet Tracer menu and select Custom Device Dialog in the drop menu. In the Device Template Manager window click on the Select button.
The Device Template Manager window will disappear and then click on the Security Camera in the workspace which will bring the Device Template Manager window back up. Make sure the Template name is set to Security Camera. Choose a Packet Tracer template area by checking the Home checkbox.

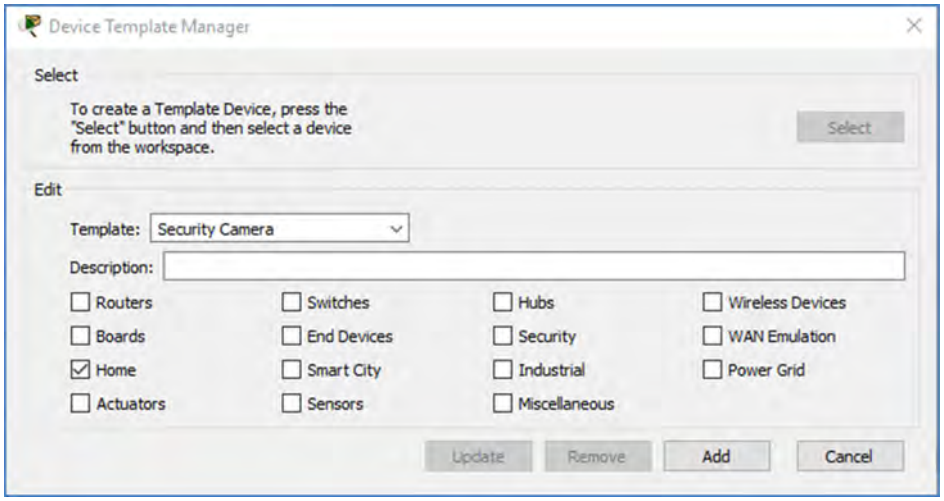


Figure 11.7:

Click Add in the bottom right of the Device Template Manager window. The Save File in Template Folder window opens. Keep the default file name of Security Camera and click Save.

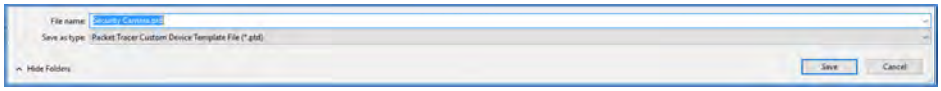


Figure 11.8:

Step 2: Verify the security device is saved as a Packet Tracer template.

a) Save your file and close Packet Tracer.
b) Open Packet Tracer.
Then security camera should now be in the list of Home devices in the Device Selection Box.

Figure 11.9:

Step 3: Save the Packet Tracer file and close Packet Tracer.

The Programming Environment

To be able to provide true IoT solutions, it is critical to have programming knowledge. Packet Tracer provides support for JavaScript, Python, and Visual Blocky. To enter the programming environment.

1. Open an IoT device and click on the Advanced button.
2. Select the Programming tab.

Once in the Programming area, you can program a new script or copy an existing script from another Thing. To modify an existing script to use for a new Thing:

1. Select the script in the panel to the left and select Open. (Figure 11)

2. The selected programming script will appear in the right hand panel and may be edited as appropriate. You can use the editing buttons (Figure 11) to make the script modification easier.
3. Once finished any required modifications, simply close the Programming tab and the changes will be saved.

It is also possible to completely delete the old script and program your Thing from scratch.

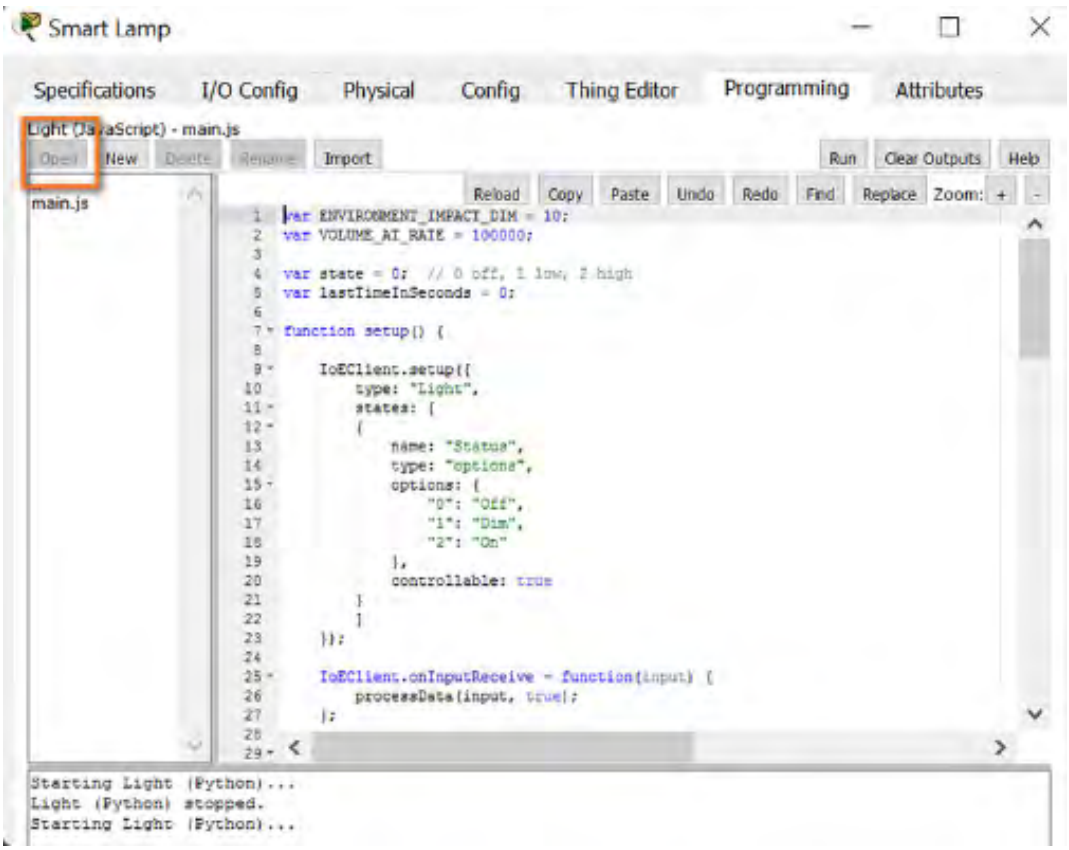


Figure 11.10: Select the script in the panel to the left and select Open.

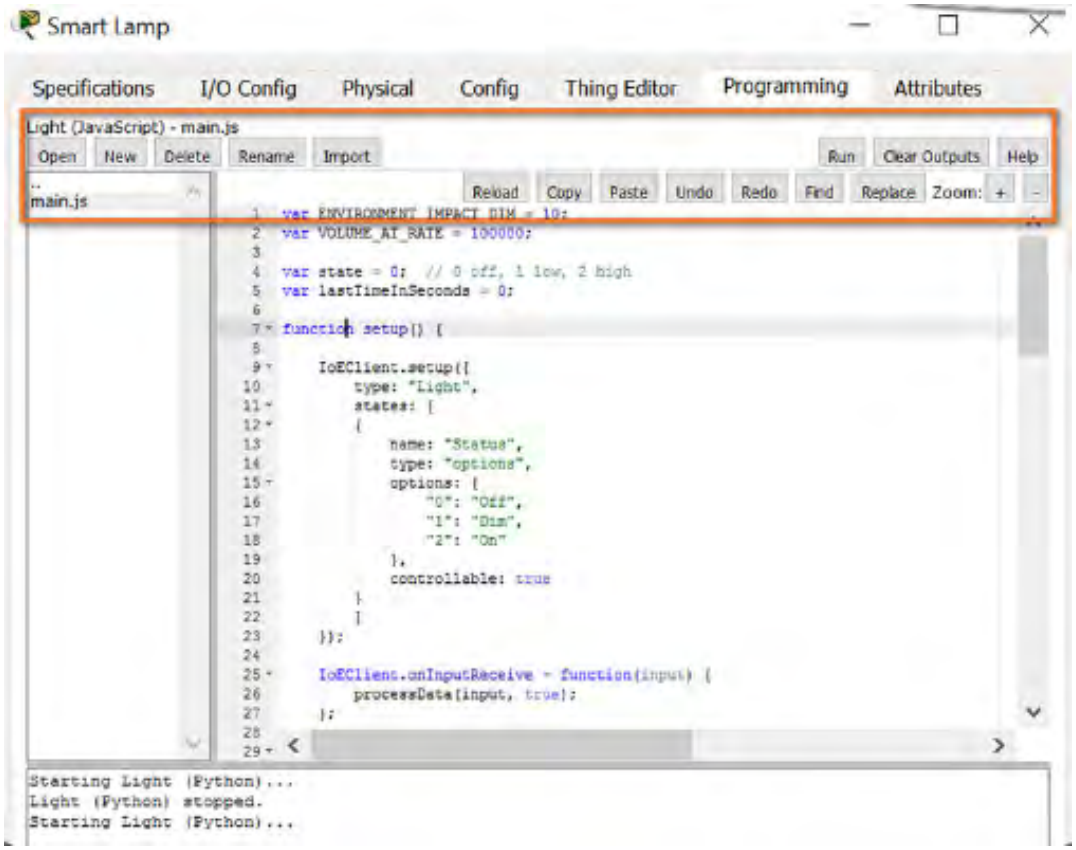


Figure 11.11: You can use the editing buttons to make the script modification easier.

(Optional PTA 1): Create Your Own IOT Thing

Objectives

In this activity, you will create a new IoT Thing, a security camera, and save the new Thing in Packet Tracer.

- Design and develop a new custom device or component, configuring its features and functionalities according to your specifications.
- Save your newly created device or component to ensure it is stored correctly and can be accessed or utilized in the future.

Part 1: Create Your Own Thing

In this part, you will create and configure a new IoT Thing, change its icon, and then connect it to the wireless network.

Step 1: Add a new generic IoT device

a. Open the Packet Tracer file.
b. Add a new device to the workspace by selecting the Thing item from the Components area of the Device Selection box.
c. Drag the Thing icon to the workspace.

Step 2: Change the Display Name of the device

a. Click the Thing to open the configuration window.
b. Click the Config tab and change the Display Name of the thing to `Security Camera`.

Step 3: Use the Thing Editor to change the properties of the Thing

a. Click the Thing Editor tab. The Properties subtab is selected by default.
b. Change the Component Name to `Security Camera`. This will identify the new Thing to the IoT network.
c. To configure the Thing to have a digital interface, click the Digital radio button, and then click the Slot Mapping drop-down menu and choose `Slot 1`.
Note: The next two substeps MUST be done in the instructions file, not the Packet tracer instructions window that opened with the Packet Tracer activity.
d. Open the instructions file for this activity if it is not already open.
e. Right-click the image below and select "Save image as", or its equivalent, from the menu. Save the file in a location that you can access later.
f. Return to the Properties configuration for the Security Camera and click the New button.
g. Locate the file that you saved, select it in the Choose Image dialog box, and then click Open to import the image. The Thing icon has now changed to the security camera icon.

Step 4: Add the security camera to the network

a. In the Security Camera configuration window, click the I/O Config tab.
b. Click the drop-down menu for Network Adapter and select `PT-IOT-NM-1W-AC` to add a Wi-Fi network adapter.
c. After a brief delay, you should observe the Security Camera connect to the wireless network.
d. Click the Config tab, and then click Wireless0 interface on the left. You may need to click the INTERFACE label to reveal the adapter.
e. In the IP Configuration section of the dialog, notice the adapter has received an IPv4 address in the `192.168.25.0/24` network.

Step 5: Test connectivity to the Security Camera

a. Click the Tablet > Desktop tab > Command Prompt.
b. Enter the ping command followed by the IPv4 address of the Security Camera. Reply messages indicate that the camera can be reached by other devices on the network.

Part 2: Save the New Device

In this part, you will save the new device as a device template. The new device can then be added to your Packet Tracer networks in the future without the need to recreate it.

Step 1: Save the security camera using the Device Template Manager

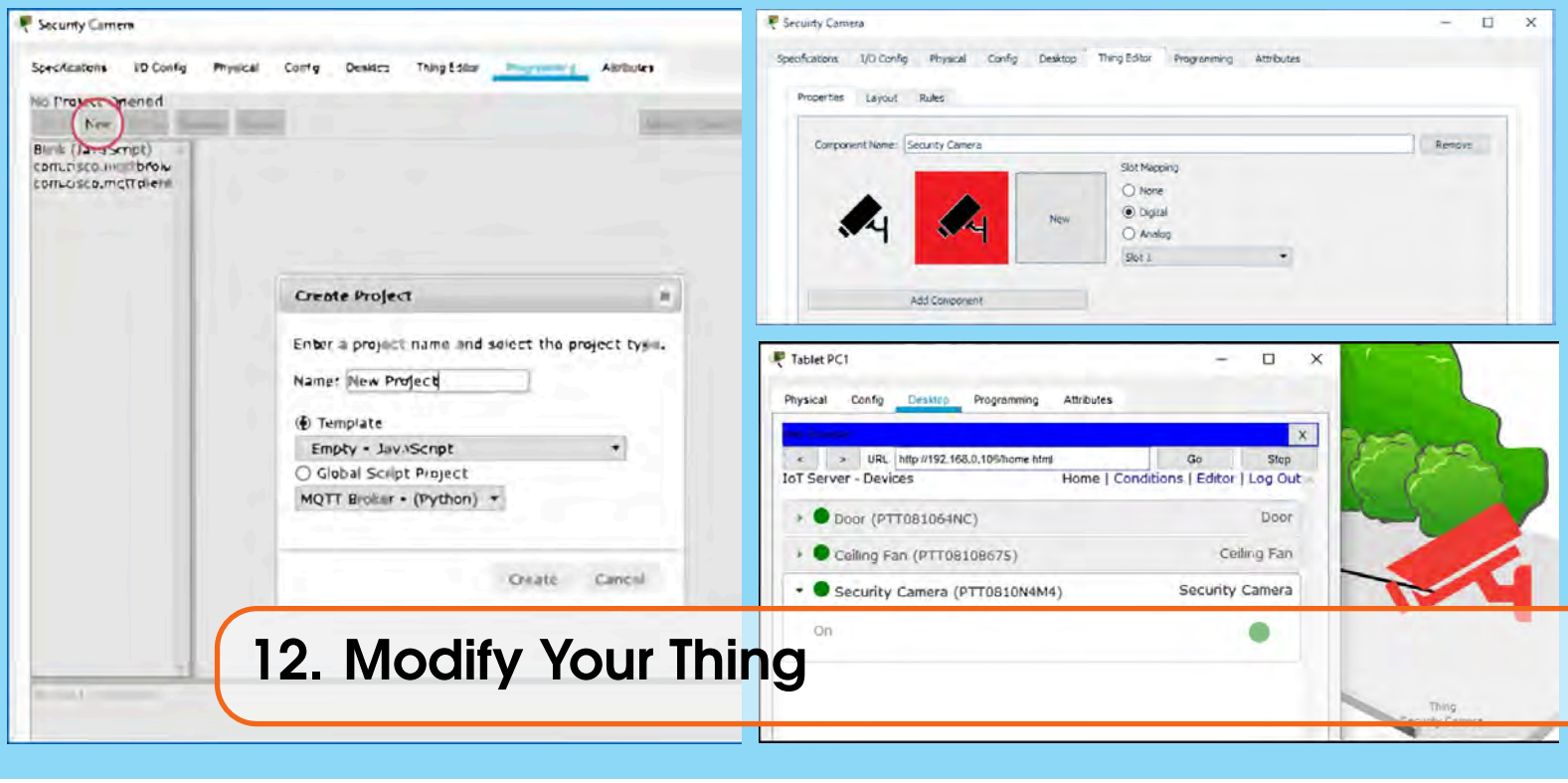
a. Click the Tools menu > Custom Device Dialog. The Device Template Manager window opens.
b. Click Select. The Device Template Manager window minimizes so you can locate and click the device you want to use as a template.
c. Click the Security Camera in the workspace. The Device Template Manager window returns with the name `Security Camera` in the Template field.
d. Click the Home checkbox. This configures the location of the new device in the Device Selection Box.
e. Click the Add button, and then click Save in the Save File in Template Folder dialog box. The new template must be saved in this folder.
f. In the Device Selection box, the Home is now selected. Scroll to the right to see your Security Camera has now been added.

Step 2: Verify the Security Camera is saved as a Packet Tracer template

a. Click File > New to open a new Packet Tracer file. Save your existing file, when prompted.

b. In the blank Packet Tracer file, notice that your Security Camera device is listed in the list of Home devices in the Device Selection Box.

You have created a new IoT device and connected it to the network. You have also saved the new device as a template so that it will be available to add to Packet Tracer networks in the future.



12. Modify Your Thing

Objectives

- Learn to modify and enhance existing IoT devices, building on previously created "Things" to customize functionality .
- Implement new features and capabilities in IoT devices, expanding their potential applications and uses .
- Test and troubleshoot modified IoT devices, ensuring they operate correctly and meet design specifications .
- Explore advanced IoT programming and configuration, gaining deeper insights into creating and managing complex smart systems .

In this activity you will modify and test a new Thing.

Packet Tracer provides a large number of devices that can be modified to create new Things. It is often easier to modify an existing object that has similar functionality to the Thing being created than it is to program an entirely new Thing.

Video — Reviewing and Modifying Scripts | . This is our Cisco Packet Tracer Modifying a Thing walkthrough video. We've got a wireless access point hooked to a router, to a network down below, and yes, there is a server named Mission Control. Watch this video to see how to program a new Thing.

The Smart Home Network

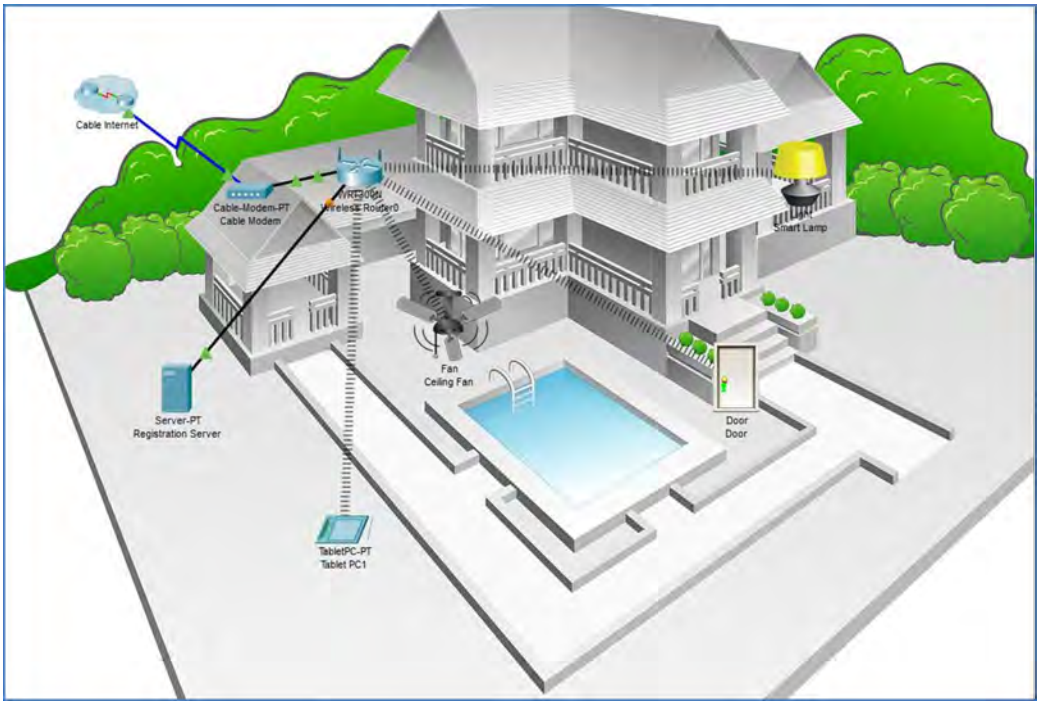


Figure 12.1: Smart Home Environment

Objectives

- Part 1: Modify Your Thing
- Part 2: Test Your Modified Thing

Background / Scenario

In this activity you will modify the security camera IoT device created in the previous activity.

Part 1: Modify Your Thing

Step 1: Open the Modify Your Thing.pkt file and save the file to your computer.

Step 2: Add an Additional Device

a) Add an additional device icon
Select the Security Camera on the Packet Tracer workspace to open the device configuration window.
Click on Advanced button in the bottom right of the device configuration window, then click on the Thing Editor tab, and then the Properties tab.

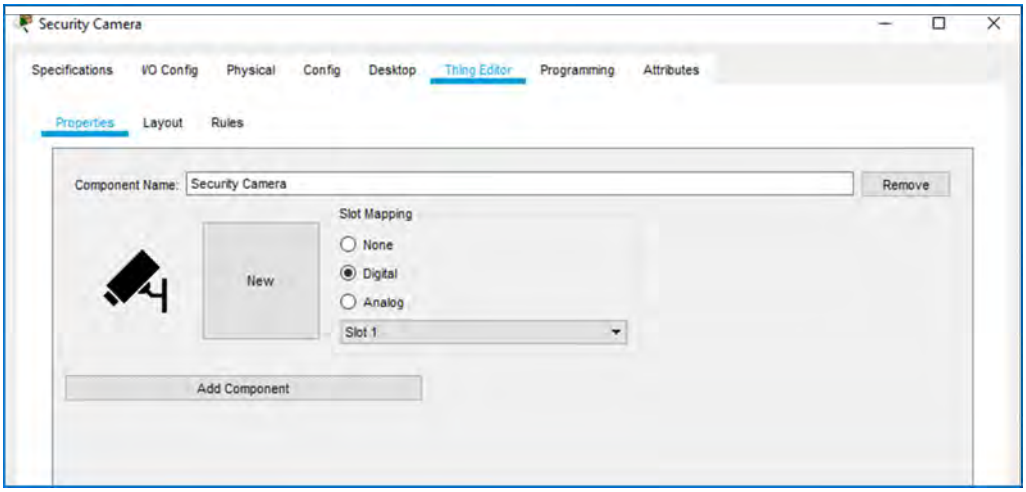


Figure 12.2:

Click on the New button.
A pane will open allowing you to browse for a new icon. Select a different image for the security camera for when it is activated.

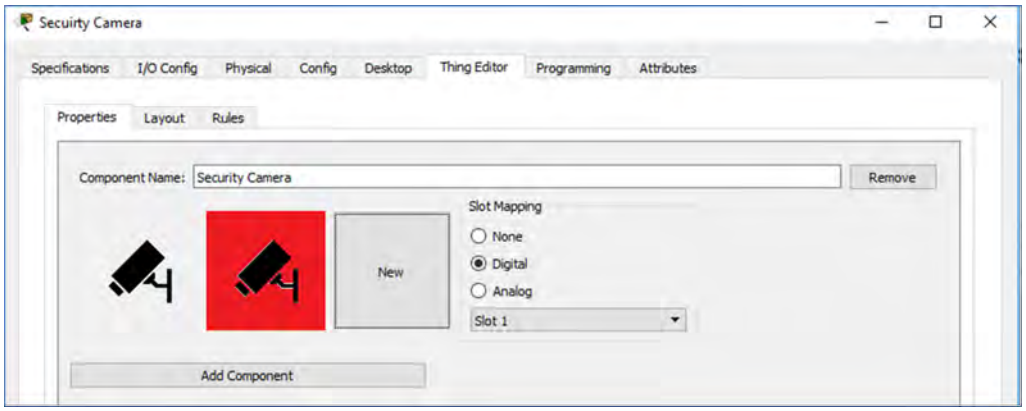


Figure 12.3:

Next, click on the Rules tab.
Then, click the Add Component button.
Click in the Sub Component column and select Security Camera in the drop down menu.
The Slot Value should change to LOW and the Image should show the security camera image that will be used as the icon when the camera is deactivated.

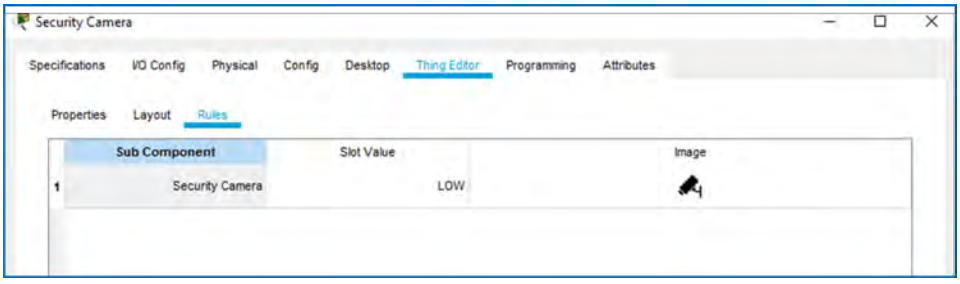


Figure 12.4:

Click the Add button again.
Click in the Sub Component column and select Security Camera in the drop down menu.
Click in the Slot Value column and select HIGH and click in the Image column and select the second security camera image that will be used as the activated icon.

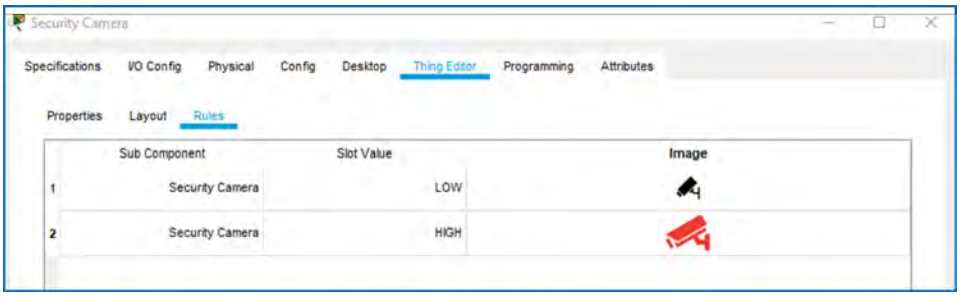


Figure 12.5:

Step 3: Copy programming code to the security camera.

a) View the existing programming code.
Click on the Programming tab.

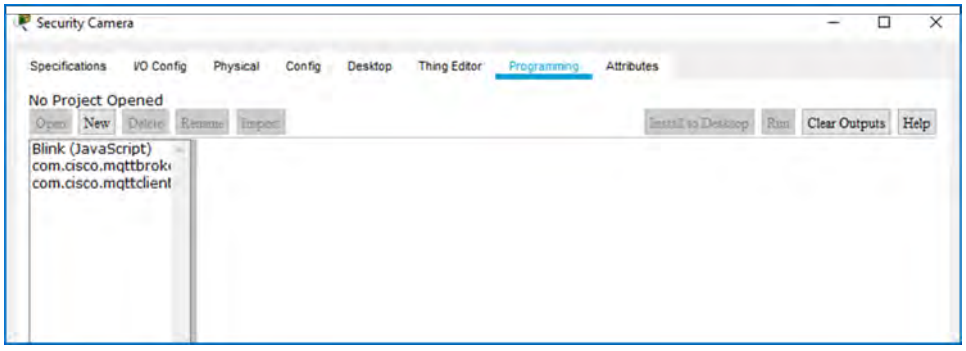


Figure 12.6:

Notice that there is no code yet for the device.
Minimize the Security Camera configuration window.

b) Copy code from existing Packet Tracer IoT device.
Add the Motion Detector IoT device to the Packet Tracer Workspace.

Figure 12.7:

Click on the Motion Detector to open the device configuration window, click on the Advanced button, then click on the Programming tab.
In the Programming tab, click on Motion Detector (JavaScript) in the left pane and click Open.

Figure 12.8:

Then click on main.js in the left pane and click Open. This opens the code associated with the Motion Detector in the code edit pane to the right.

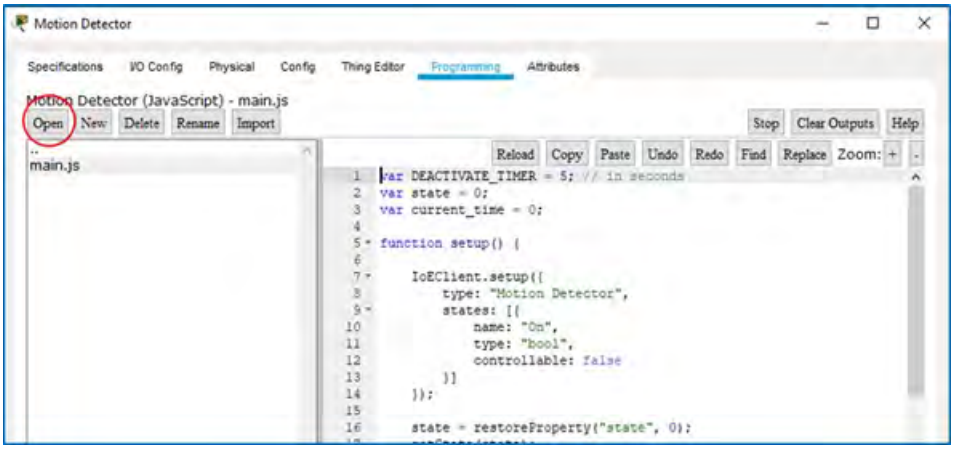


Figure 12.9:

To select all the programming script, click in the code edit pane and type Ctrl+A on the keyboard. Once all the script is selected, click Copy in the code edit pane menu.

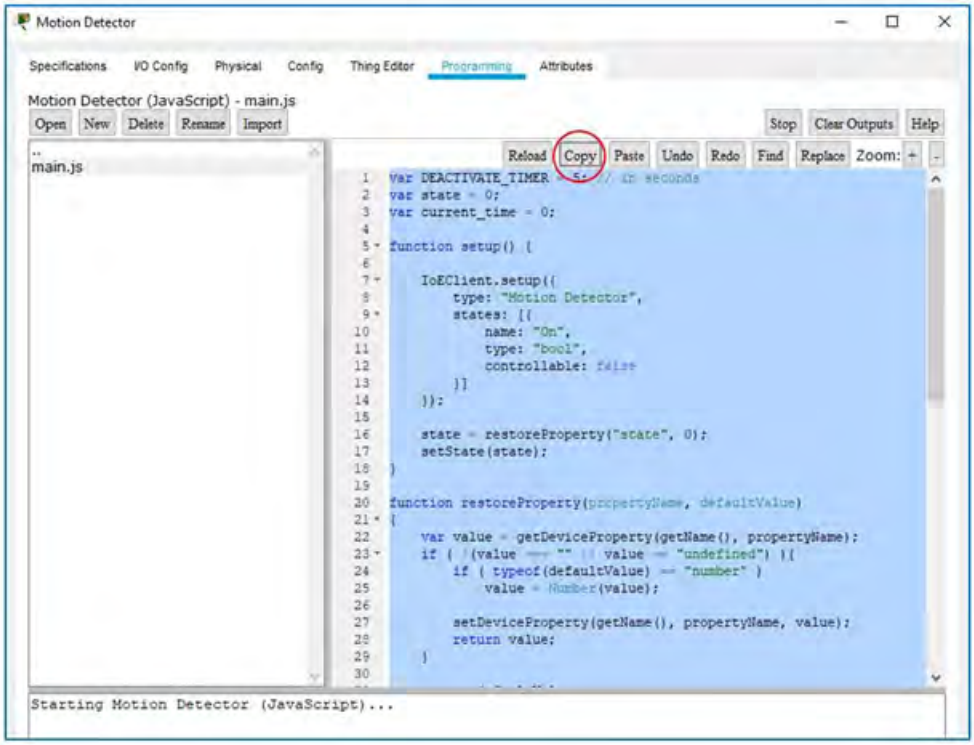


Figure 12.10:

Close the Motion Detector configuration window.

c) Paste the copied code to the security camera IoT device.
Re-open the Security Camera window and select the Programming tab if not already selected.
Click the New project button above the left pane. This opens the Create Project window.

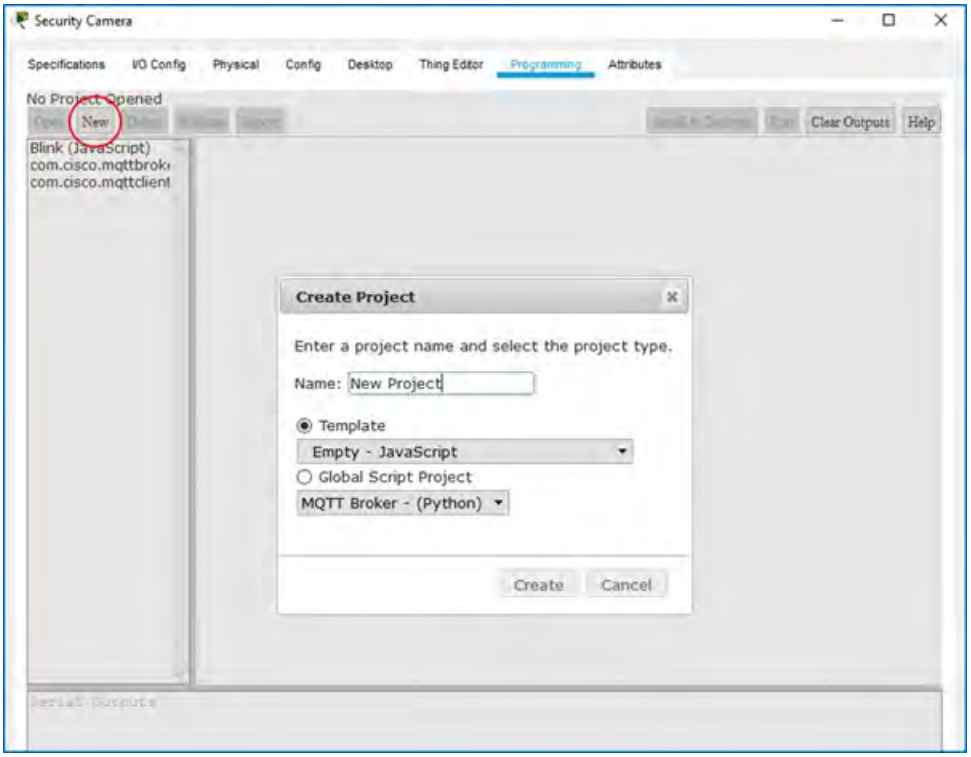


Figure 12.11:

In the Create Project window, create a new programming project named Security Camera by typing Security Camera in the Name box and clicking Create.

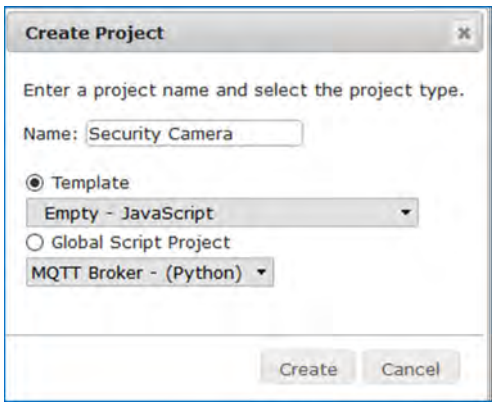


Figure 12.12:

To view the new project just created, click on the .. in the left pane and click Open

Figure 12.13:

Notice there is now a Security Camera (JavaScript) project in the left pane. Click on Security Camera project and click Open.

Figure 12.14:

Now click main.js and click Open.

Figure 12.15:

You can now paste the copied code from the Motion Detector into the code edit pane on the right. Click in the code edit pane and click on the Paste button to paste in the copied code.

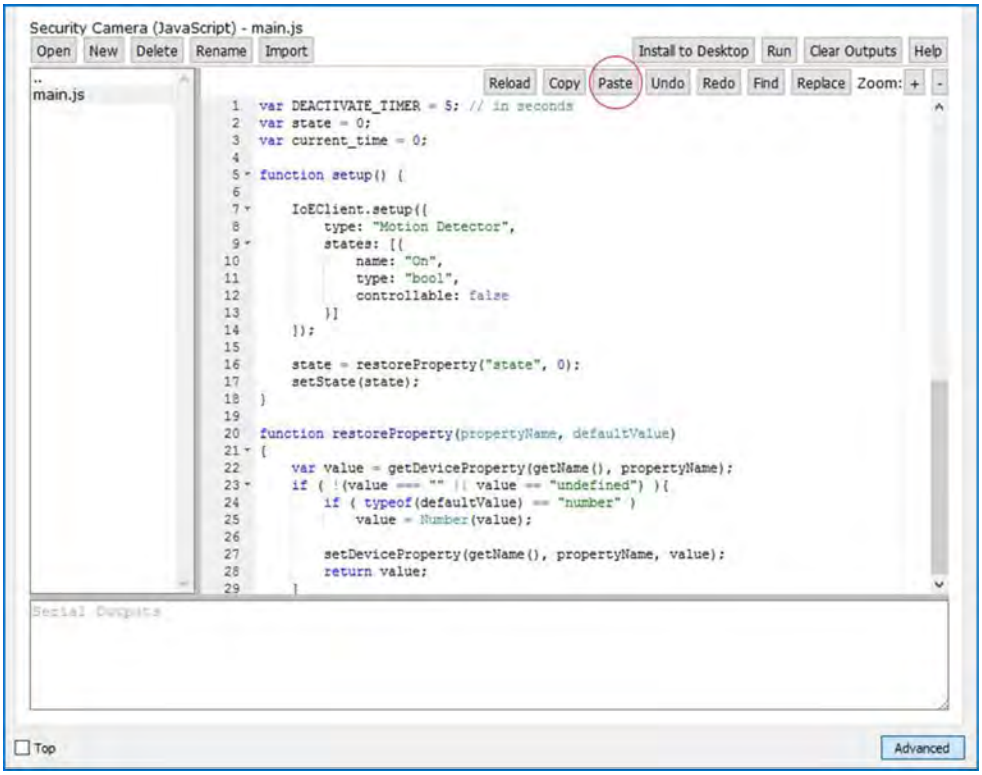


Figure 12.16:

Step 4: Edit the security camera programming code

The code copied from the Motion Detector needs to be edited to change the type to Security Camera. Click on the line that identifies the device and change the name. In this instance it is line 8.

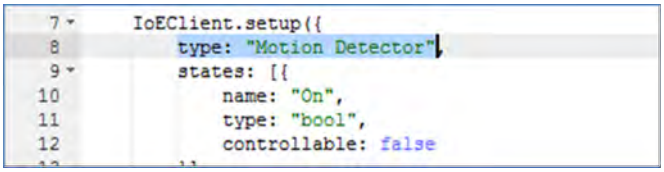


Figure 12.17:

Change "Motion Detector" to Security Camera

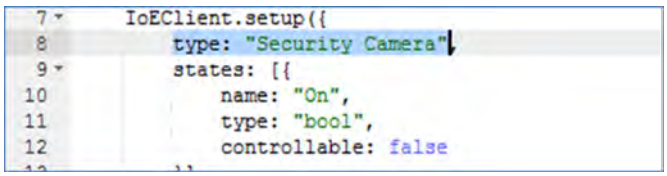


Figure 12.18:

Run the program by clicking on the Run Button.

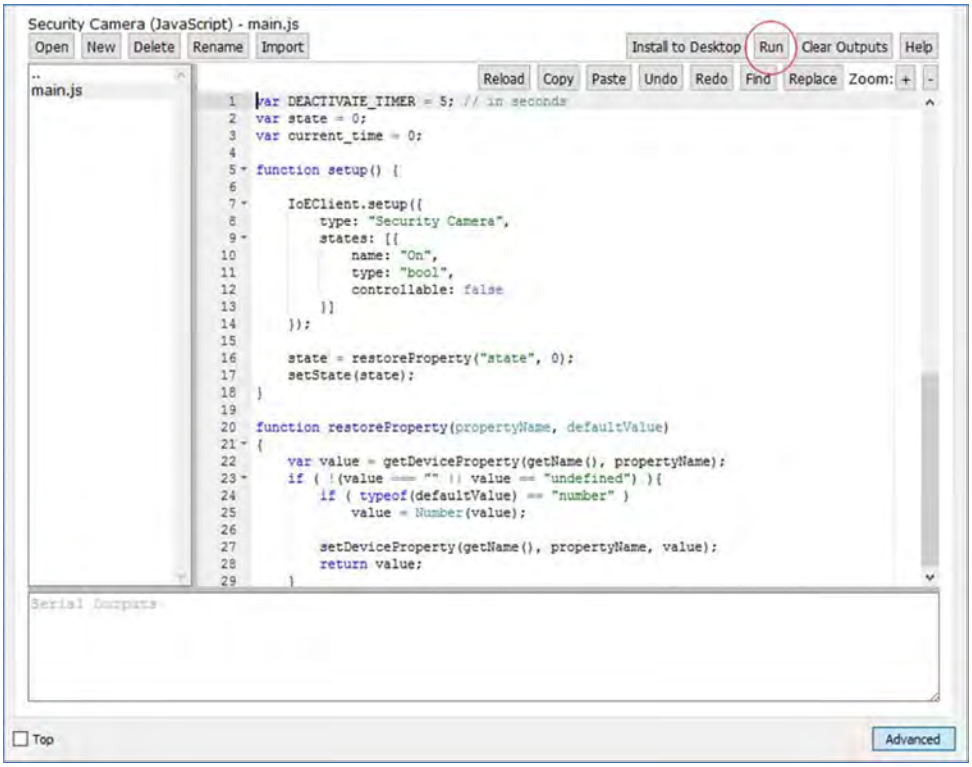


Figure 12.19:

Close the Security Camera configuration window.

Part 2: Test Modified Thing

Step 1: Access the Registration Server from the Tablet PC.

Click on the Tablet-PC to open the configuration window. Click on the Desktop tab, and select the Web Browser icon.

In the web browser pane type in the URL of the registration server 192.168.0.106 and click Go. In the Registration Server Login pane type in the following credentials and click Sign In.

Username: cisco Password: cisco123

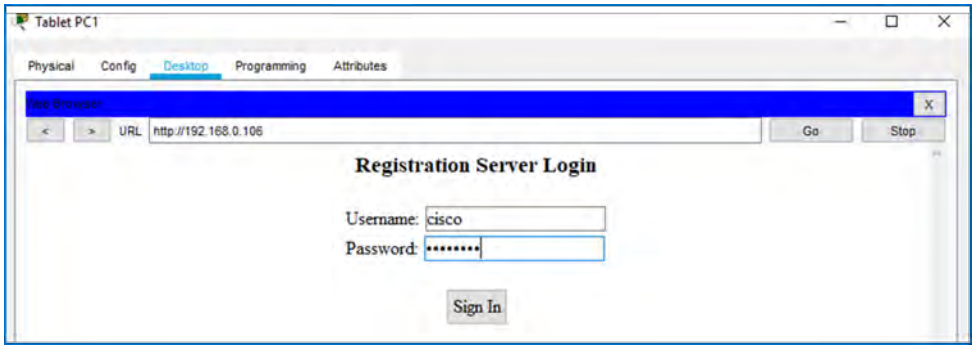


Figure 12.20:

In the IoTServer-Devices pane click on the Security Camera to expand the device information. Notice the Security Camera is On but not activated.

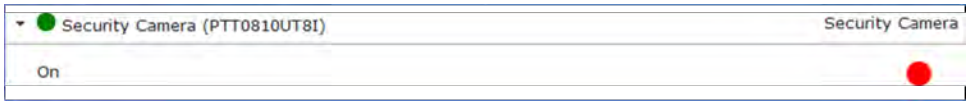


Figure 12.21:

Step 2: Activate the Security Camera.

Move the Tablet PC1 configuration window out of the way but still visible so that the Packet Tracer workspace is visible.

Hold down the Alt key on the keyboard and move the mouse curser over the Security Camera icon.

Notice that the icon will change to the image used as the activated icon and the Security Camera status changes to activated as indicated by the green dot in the Server-Devices list on the Registration Server.

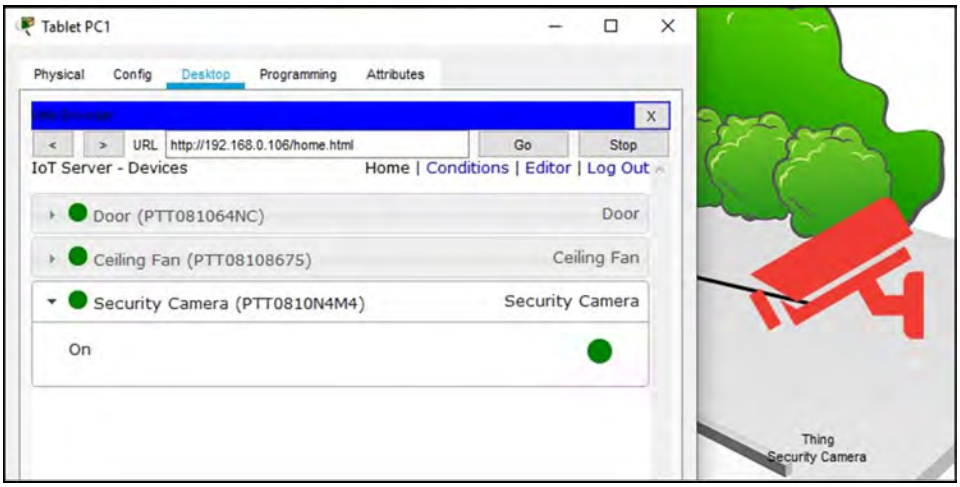


Figure 12.22:

Step 3: Experiment.

Experiment by adding other types of IoT devices and editing the programming of those devices to perform different functions.

(Optional PKA 1): Modify and Monitor Environmental Controls

Objectives

In this activity, you will modify the security camera IoT device created in the previous activity.

- Make changes to your custom device or component by adjusting its settings, features, or functionalities to improve or alter its performance.
- Evaluate the changes by testing the modified device or component to ensure it functions correctly and meets the desired specifications.

Part 1: Modify Your Thing

Step 1: Save the device icon from the instructions file

a) Open the HTML instructions file for this activity if it is not already open.

b) Right-click the image below and select the option to save the image as a file on your computer. This must be done from the instructions document; it cannot be done from the Packet Tracer instructions window.

c) Save the image in a folder where you can find it easily.

Step 2: Add an additional device icon

a) In the Packet Tracer file for this activity, click the Security Camera in the Packet Tracer workspace, and click the Config tab.

b) Click the Advanced button in the bottom right of the device configuration window, then click the Thing Editor tab. Be sure that the Properties tab is open. You will see the icon for the security camera that you worked with in the last activity.

c) Click the New button. This will allow you to add a second graphic for the security camera. Locate the file that you saved to your computer in Step 1 and click Open to insert the image. This image will represent the security camera when it is activated by motion, as indicated by the red light.

d) Next, click the Rules tab.

e) Then, click the Add button.

f) Click in the Sub Component column and select `Security Camera` in the drop-down menu.

g) The Slot Value should change to LOW and the Image should show the security camera image that will be used as the icon when the camera is not active (the camera without the red dot).

h) Click the Add button again.

i) Click in the Sub Component column and select `Security Camera` in the drop-down menu again.

j) Click in the Slot Value column and select HIGH and click in the Image column and select the security camera image that will be used as the activated icon (the camera with the red dot). This is the file that you saved in Step 1.

Step 3: Copy programming code from an existing IoT device

a) View the existing programming code by clicking the Programming tab. Notice that there is minimal code for the device.
Note: You may need to double-click `Blink (JavaScript)` and double-click `main.js` to view the code.

b) Minimize the Security Camera configuration window.

c) To copy code from an existing Packet Tracer IoT device, add the Motion Detector IoT device to the Packet Tracer workspace. You can find it under `End Devices > Home` in the device selection box. You will be adding motion detector functionality to the security camera by copying the code from the motion detector to the security camera.

d) Click the Motion Detector and click the Config tab, click the Advanced button, then click the Programming tab.

e) In the Programming tab, click `Motion Detector (JavaScript)` in the left pane and click

Open.

f) Click `main.js` in the left pane and click Open. This opens the code that is associated with the Motion Detector in the code edit pane to the right.

g) You will need to copy the entire script. To select all of the programming script, click in the code edit pane and press `Ctrl+A` on the keyboard. With all of the script selected, click Copy in the code edit pane menu.

h) Close the Motion Detector configuration window and delete the motion detector device.

Step 4: Create a new script in the security camera

a) To paste the copied code to the security camera IoT device, re-open the Security Camera window and select the Programming tab if not already selected.

b) Click the `..` (two dots) in the left pane and click Open to return the window to display `Blink (JavaScript)`.

c) Click the New project button above the left pane. This opens the Create File window.

d) In the Create File window, create a new programming project by typing `Security Camera` in the Name box and then clicking Create.

e) To view the new project just created, click the `..` (two dots) in the left pane and click Open.

f) Notice there is now a `Security Camera (JavaScript)` project in the left pane. Click the Security Camera project and click Open.

g) Click `main.js` and click Open.

h) You can now paste the copied code from the Motion Detector into the code edit pane on the right. Click in the code edit pane and click the Paste button to paste in the copied code.

Step 5: Edit the security camera programming code

a) The code that you copied from the Motion Detector needs to be edited to change the type value from Motion Detector to Security Camera. To do this, click the line that says `type: "Motion Detector"` in the code edit pane. In this instance, it is line 8.

b) Change the line from `type: "Motion Detector"`, to `type: "Security Camera"`
Note: The quotation marks and comma at the end of the statement are required.

c) Run the program by clicking the Run button.

Part 2: Test Your Modified Thing

Step 1: Register the security camera thing with the IoT Registration Server

a) In the security camera configuration window, click the Config tab.

b) In the IoT Server section of the pane on the right, click the Remote Server radio button. The IoT Registration Server is remote because it is connected to a network that is outside of the home network.

c) Enter the Server Address as `203.0.0.3`.

d) Enter the User Name as `home` and the Password as `home`.

e) Click the Connect or Refresh button to initiate the connection.

Step 2: Monitor and test the thing from the IoT Server

a) Access the IoT Registration Server from the Tablet. To do so, click the Tablet to open the configuration window. Click the Desktop tab and select the Web Browser icon. In the web browser window, enter the URL of the IoT Registration Server, `home.com`, and click Go.

b) In the Registration Server Login pane type in the following credentials and click Connect.
   - Username: `home`
   - Password: `home`

c) In the `IoTServer - Devices` pane, click the Security Camera to expand the device information. Notice the Security Camera is On but not activated, as indicated by the red dot.

d) Move the Tablet configuration window out of the way. It should be visible next to the PT workspace.

e) Hold down the `Alt` key on the keyboard and move the mouse pointer over the Security Camera icon. This signifies motion that should be detected by the camera.

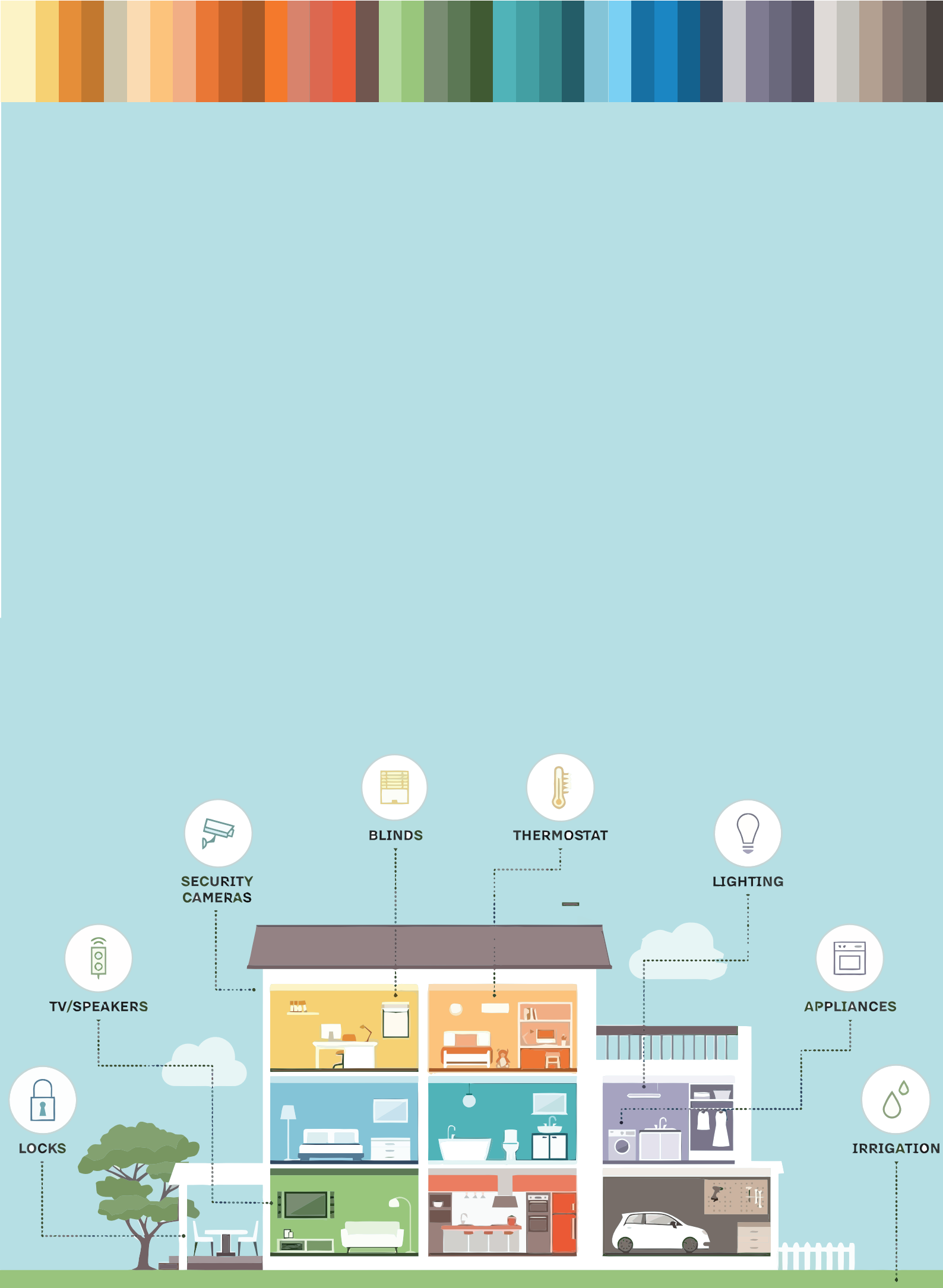
f) Notice that the icon will change to the image with the red dot. In the Tablet browser window, the Security Camera status changes to activated as indicated by the green dot in Security Camera display. If no additional motion is detected, the security camera will switch back to deactivated after a brief delay. You will see the green dot turn red and the deactivated camera icon display in the workspace.

g) You can also control the other devices that are registered with the server. The registration server provides a way that the home IoT network can be controlled from any end device that is connected to the internet. Try controlling the other devices and observe the results in the registration server interface and the workspace.

Step 3: Experiment

a) Experiment by adding other types of IoT devices and editing the programming of those devices to perform different functions.

b) Close Packet Tracer.


BLINDS
THERMOSTAT
SECURITY CAMERAS
LIGHTING
TV/SPEAKERS
APPLIANCES
LOCKS
IRRIGATION