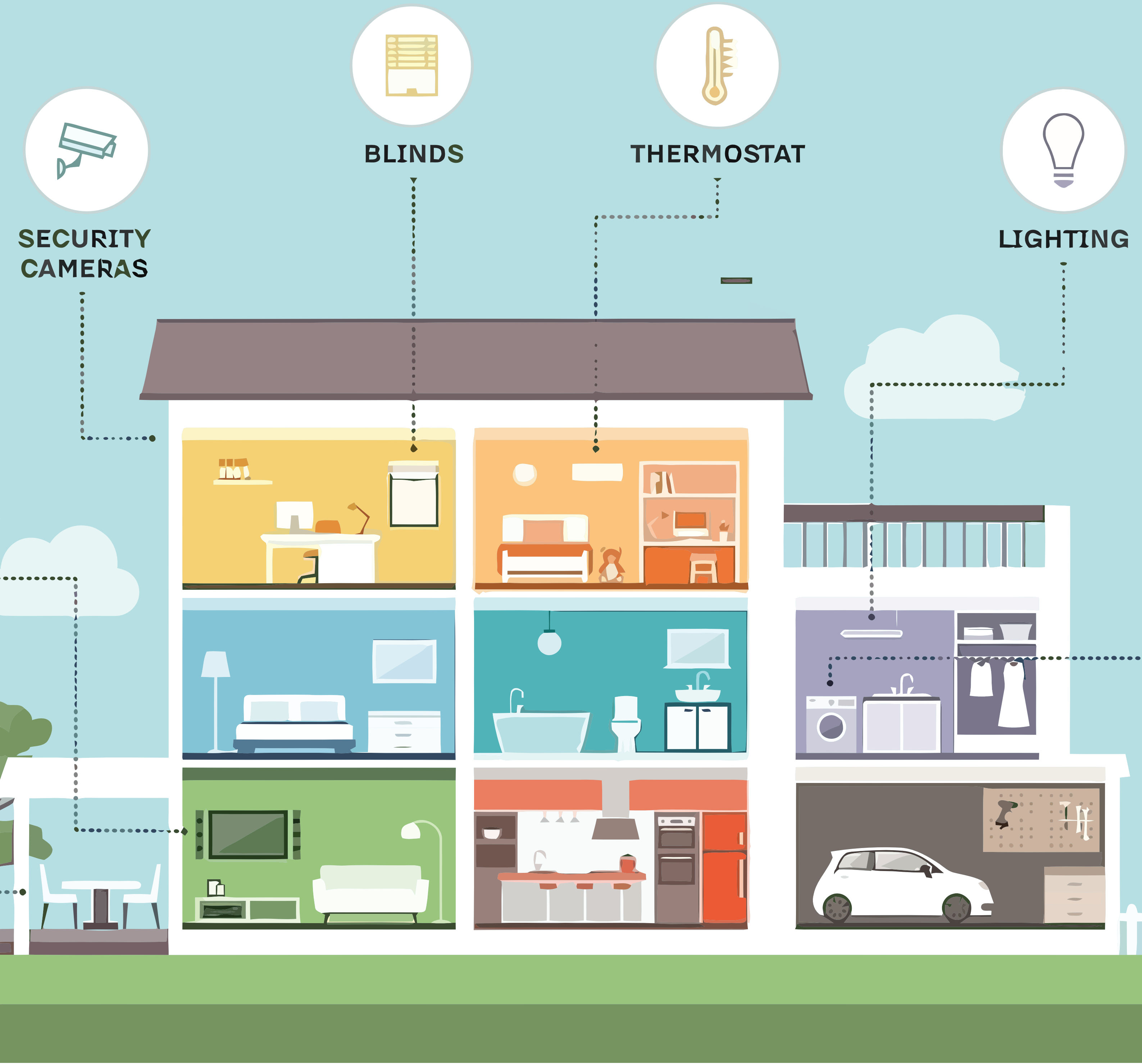
Charith Perera (Eds.)
PhD, MBA

Internet of Things

Systems Design

Advanced Lab Book



PUBLISHED BY IOT GARAGE

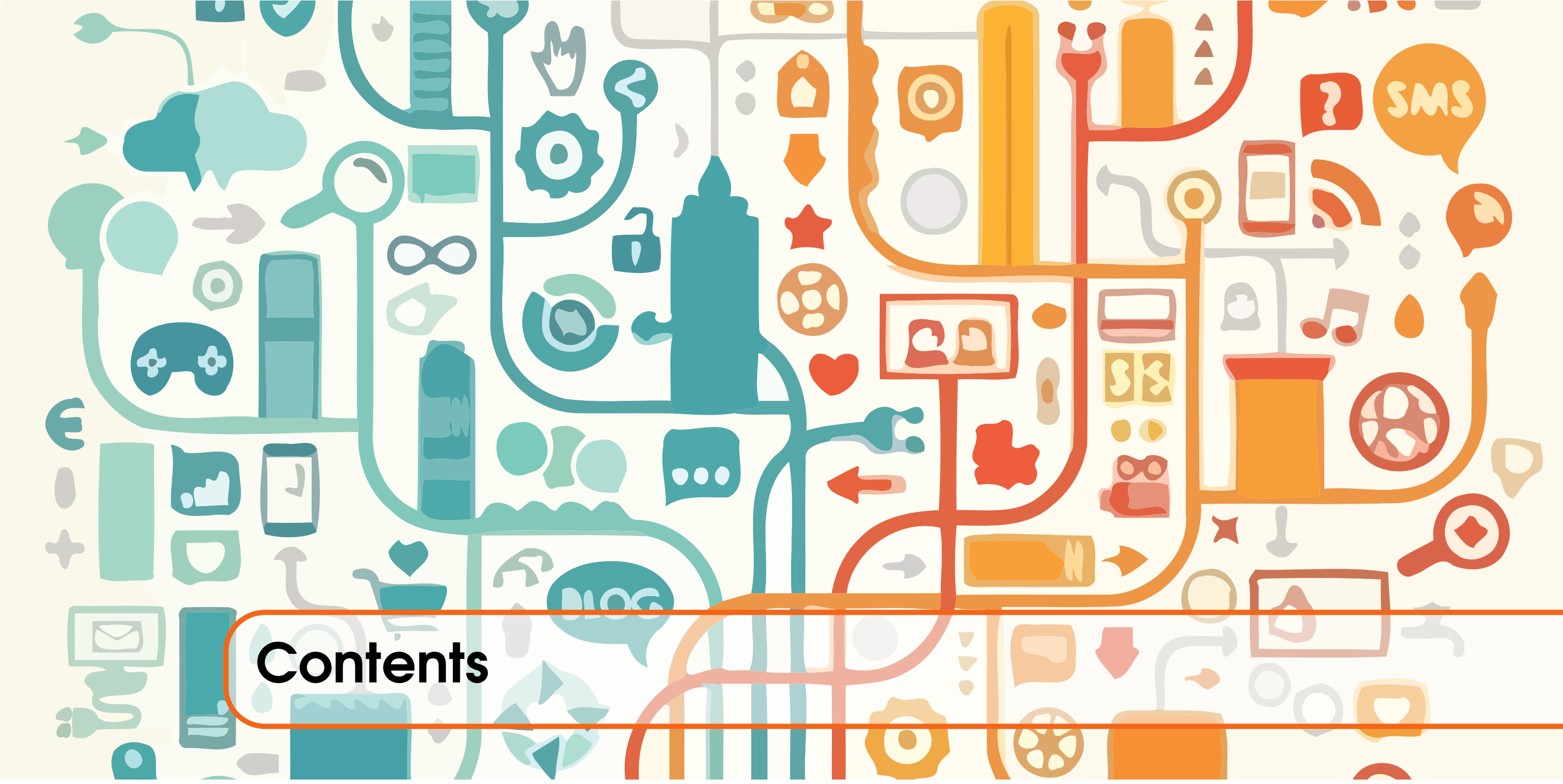
How to cite this book

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 undergraduate 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, actuators, 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. Throughout this lab book, we offer explanations, learning tips, external links, and references to relevant reading materials. If you find certain programming tasks difficult, you are encouraged to explore these resources for additional guidance. Although the suggested readings are optional, they provide valuable opportunities to deepen your understanding of IoT beyond the scope of the provided labs. Finally, please note that this is not a programming course; you are responsible for identifying and addressing any knowledge gaps by consulting the links and materials we have included.

Resources **— 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.

Accessing the Code Repository

All the Packet Tracer (`.pkt` or `.pka`) files and other resources required to complete the labs in this *IOT ADVANCED LAB BOOK* can be found in the following GitLab repository:

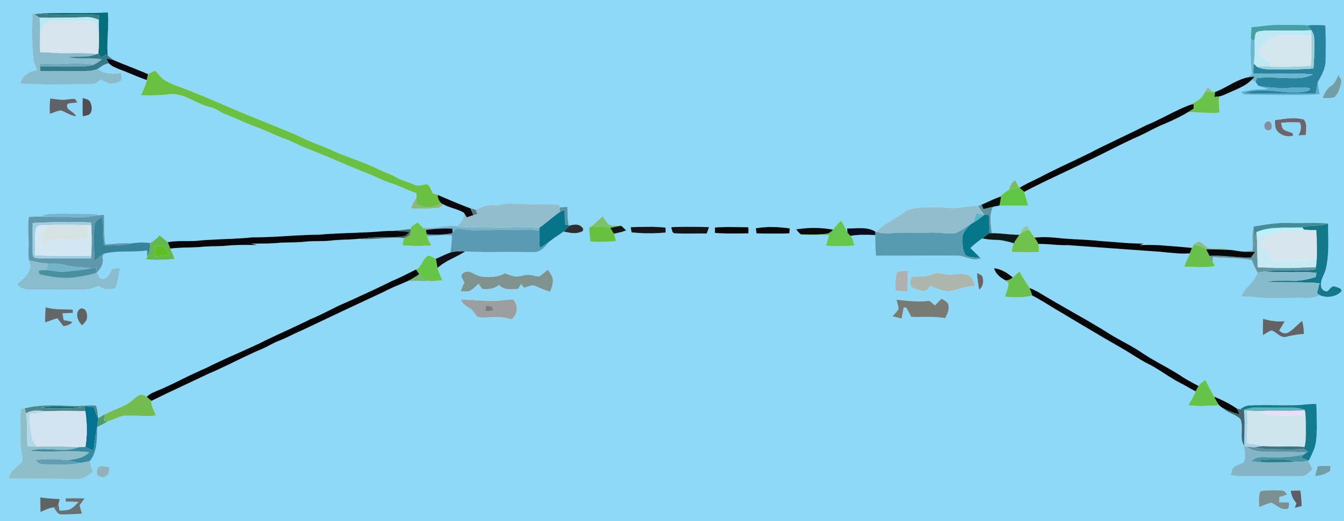
`https://gitlab.com/IOTGarage/iot-advanced-lab-book`

This repository includes lab files, scripts, sample code, and supplemental materials referenced throughout the labs. When working through any of the lab exercises, please refer to the respective folder or file in the repository to locate the matching examples. Any updates, bug fixes, or enhancements will also be made available here, so be sure to check back periodically for the most recent versions. By visiting the repository, you can:

- **Clone or Download the Files:** Pull down all relevant Packet Tracer files, scripts, and configurations needed for each lab.
- **Review Commit History:** Track how the files have evolved, exploring different versions and branches that may include experimental features or fixes.
- **Submit Issues:** If you encounter bugs or require clarification, open an issue and collaborate with the community for support or improvements.

Learn More about Cisco Packet Tracer: If you want to download Cisco Packet Tracer or learn more about its features, visit:

`https://www.netacad.com/cisco-packet-tracer`



1. Deploying and Cabling Devices

Introduction

This lab introduces you to the core functionalities of **Cisco Packet Tracer**, focusing on how to deploy network devices and connect them using the correct cabling techniques. By the end of this lab, you will have a clearer understanding of Packet Tracer's interface and how to simulate basic network layouts.

Objectives

- Gain an understanding of Cisco Packet Tracer's capabilities and the installation process to effectively deploy network simulations.
- Develop the ability to navigate and utilize Packet Tracer's interface to add, connect, and manage network devices with confidence.
- 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:

A. Open and explore a pre-configured Packet Tracer file.
B. Practice adding `routers`, `switches`, and `end devices` to a network topology.
C. Connect devices using the appropriate cabling methods.
D. Recognize the different cable types (straight-through vs. cross-over) and when to use them.

Overview of Packet Tracer

Packet Tracer is an exciting network design, simulation, and modeling tool that allows you to develop your skill set in networking, cybersecurity, and the Internet of Things (IoT). It enables 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 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 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.

Resources — 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** → **Open Samples** from the main menu.

The User Interface

Packet Tracer is designed to closely simulate real networks. It has two key features:

- **Device Configuration:** Allows you to add devices, create cable or wireless connections, and perform actions (selecting, deleting, inspecting, labeling, and grouping components).
- **Network Management:** Lets you open existing or sample networks, save your current network configuration, and modify user preferences.

Resources — The Packet Tracer User Interface | . Watch this video to learn how to use the menus and user interface in Packet Tracer. You will see an overview of the toolbars and build your first network.

A. Open the `Deploying and Cabling Devices.pkt` File

1. **Locate the File** Double-click on `Deploying and Cabling Devices.pkt` to launch it in Packet Tracer. If you are unable to locate the file, ensure that you have navigated to the correct directory.
2. **Check Installation** If the file does not open or displays an error regarding version mismatch, confirm your Packet Tracer version is installed correctly and up to date (e.g., version 8.x or above).
3. **Verify Initial View** A successful load typically shows a screen like Figure 1.1. You might see placeholders (e.g., "`Switch0`," "`PC1`"). If the interface differs significantly, re-check your file path or installation.

Suggestions for Opening Packet Tracer Files:

- If your file does not open on the first try, close and re-launch Packet Tracer.
- Occasionally, Packet Tracer may not refresh the file directory list if it was already running.
- Check your folder permissions (especially on institutional computers) to ensure that you have read access to the directory containing the `.pkt` file.
- Always keep a backup of the `.pkt` file in a separate folder or cloud storage, so you can revert to it if any issues occur.

B. Identify and Place Network Devices

In this section, you will learn how to find and place key network devices into your Packet Tracer workspace. Carefully follow these steps to organize your network foundation before proceeding to

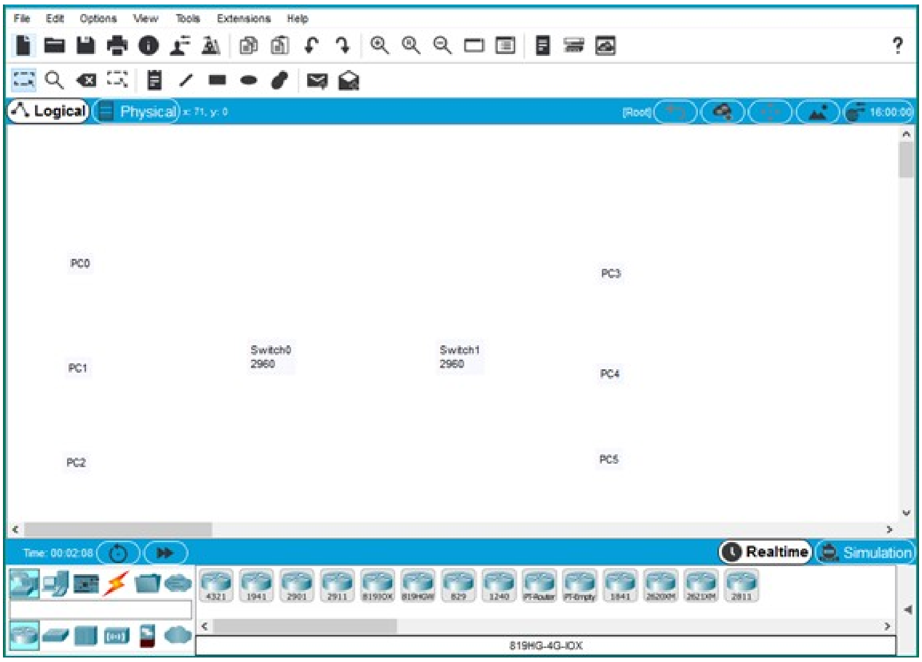


Figure 1.1: Initial interface of Packet Tracer upon opening `Deploying and Cabling Devices.pkt`. Notice the blank workspace and the logical/physical view tabs at lower left.

the cabling phase.

4. **Open the Device-Type Selection Box:**
   - Along the lower-left side of the Packet Tracer interface, you will see a *top row* of broad categories (**Network Devices**, **End Devices**, and **Connections**).
   - Directly beneath it, the *bottom row* refines these categories further into subcategories such as *Routers*, *Switches*, *Wireless Devices*, and *PCs*. Hover your mouse cursor over each icon to see a descriptive label appear.
5. **Add Two Switches:**
   - Click the *Switches* icon in the bottom row. You should see various switch models like `2960`, `2950`, and a `Generic Switch` in the Device-Specific Selection box.
   - Drag two `2960` switches into your workspace. These will be your central points for connecting PCs and other end devices. Packet Tracer will either auto-label them (`Switch0`, `Switch1`) or you can click the label to rename them as desired.
6. **Add Six PCs:**
   - Click *End Devices*, then select `PC-PT` from the device list. `PC-PT` is the standard personal computer model in Packet Tracer.
   - Place six PCs labeled `PC0` through `PC5` in the workspace. Packet Tracer will assign default labels automatically if you do not rename them.

Tips for Selecting and Placing Devices:

- If you are unsure which icon corresponds to a PC, hover your mouse cursor over each device icon to see its name (e.g., "`PC-PT`," "`Laptop-PT`").
- To quickly place multiple PCs in a row, hold down the `<CTRL>` key after selecting the `PC-PT` icon, and then click repeatedly in the workspace to place each PC without having to re-select the icon.
- If you need to relabel a device, simply double-click on the existing label in the workspace

and type a new name.
- The 2960 switches are commonly used for entry-level to intermediate-level labs and support essential features such as VLANs, trunking, and basic management.

Figure 1.2: Device-Type Selection Box in Packet Tracer

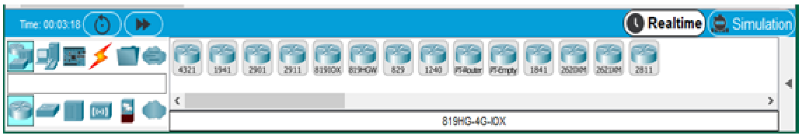


Figure 1.3: Top row = broad categories (Network Devices, End Devices, Connections), bottom row = subcategories (Routers, Switches, etc.).

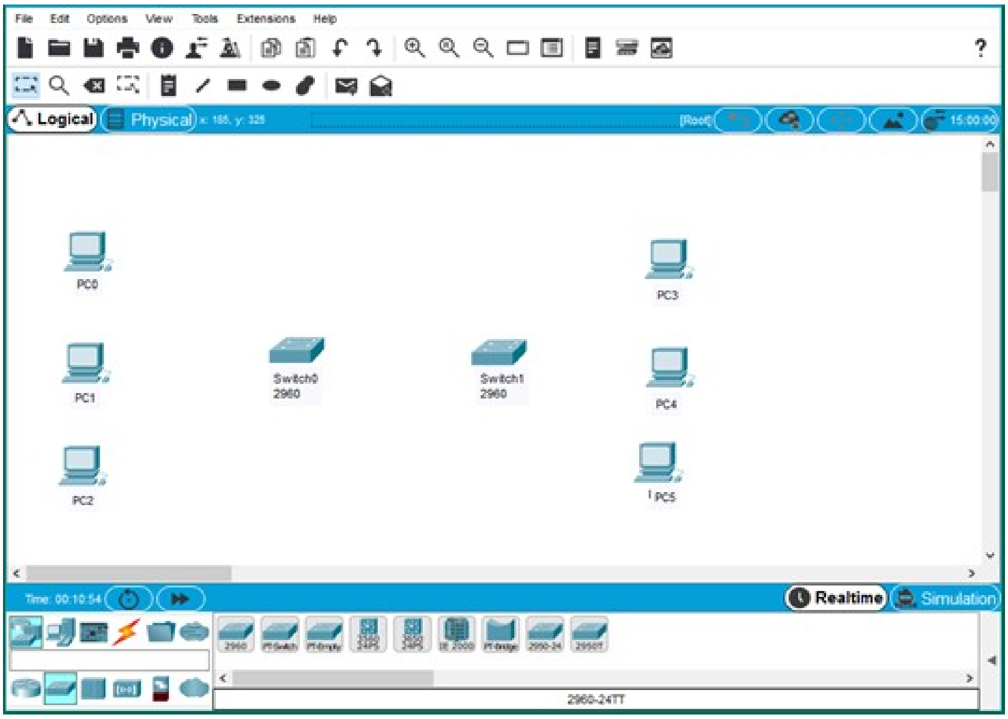


Figure 1.4: Workspace with two 2960 switches (`Switch0`, `Switch1`) and six PCs (`PC0`–`PC5`).

C. Connect PCs to Switches (Straight-Through)

In this section, you will physically connect PCs to switches using `Copper Straight-Through` cables. This type of cable is designed for linking end devices (like PCs) to intermediary devices (such as switches or routers). Follow these steps to ensure each device is properly connected and that the link lights turn green, indicating a live connection.

7. **Select Cable Type**
   - Click on the **Connections** icon, which looks like a lightning bolt at the bottom-left. A variety of cable options will appear, including `Copper Straight-Through`, `Copper Cross-Over`, `Fiber`, and others.
   - Choose `Copper Straight-Through`. This is the most common cable used to connect end devices (PCs) to switches or routers in a typical LAN setup.
8. **Connect PC0 to Switch0**
   - Click on `PC0` in the workspace. A small pop-up window (or dialog box) appears showing available interfaces. Select `FastEthernet0` (or the NIC port if labeled differently).
   - Next, click on `Switch0` and choose one of its available Fast Ethernet ports, for example `FastEthernet0/1`.
   - Observe the link lights on both the PC and the switch. Typically, one light may be amber and the other green initially; after a short period of negotiation (spanning tree, speed/duplex checks), both lights should turn green, signifying a stable and active connection.
9. **Connect Remaining PCs**
   - For instance, you can follow the sample pattern below:

$$\text{PC1 (FastEthernet0)} \to \text{Switch0 (FastEthernet0/2)}$$
$$\text{PC2 (FastEthernet0)} \to \text{Switch0 (FastEthernet0/3)}$$
$$\text{PC3 (FastEthernet0)} \to \text{Switch1 (FastEthernet0/1)}$$
$$\text{PC4 (FastEthernet0)} \to \text{Switch1 (FastEthernet0/2)}$$
$$\text{PC5 (FastEthernet0)} \to \text{Switch1 (FastEthernet0/3)}$$

   - To speed up the process of cabling multiple devices, hold down the `<CTRL>` key after selecting `Copper Straight-Through` from the Connections menu. Then, click each PC followed by the corresponding switch port. This allows you to place multiple cables without having to re-select the cable type each time.
10. **Validate Each PC Connection**
   - After each connection, check the LEDs (link lights) on the switch port. A stable green light typically indicates a successful physical connection and negotiation between the PC and the switch.
   - If a port remains amber or unlit for an extended period:
     – Verify that you used the `FastEthernet0` port on the PC and `Copper Straight-Through` (rather than `Cross-Over` or `Console`).
     – Ensure that both the PC and switch ports are powered on and not administratively shut down in the switch's configuration.
   - Once properly cabled, both link lights should eventually show green, indicating an active and healthy link.

Hints for Successful Cabling:

Confirming Cable Type: If you accidentally select the wrong cable type (e.g., `Copper Cross-Over`), the link might not come up. Double-check that the cable icon reads "`Copper Straight-Through`."

Checking Spanning Tree Delays: Switch ports can remain amber for a short time while Spanning Tree Protocol (STP) runs. This is normal; wait briefly for the port to transition to a forwarding state (green).

Troubleshooting: If a port stays amber indefinitely or does not turn on at all, you may have selected the wrong port type or the interface might be administratively `shutdown` in the switch config. You can open the switch's CLI or Config tab to investigate further. ■

D. Connect the Two Switches (Cross-Over)

In this section, you will connect the two switches together using a `Copper Cross-Over` cable. Although modern switches typically include *Auto-MDIX* support to handle cable type automatically, we will explicitly practice using a cross-over cable for clarity.

11. **Switch-to-Switch Cable**
    - When linking two *similar* devices (in this case, two switches), a **copper cross-over** cable is generally the recommended choice.
    - Even if your switches support *Auto-MDIX*, it's valuable to learn the traditional approach to avoid confusion and ensure compatibility in diverse environments.
12. **Select Cross-Over**
    - Return to the **Connections** menu (the lightning-bolt icon at the bottom-left of Packet Tracer). This reveals a variety of cable options.
    - From the `Device-Specific Selection` box that appears, choose the `Copper Cross-Over` option. Make sure not to select `Copper Straight-Through` by mistake.
13. **Use Gigabit Ports**
    - On `Switch0`, click the port labeled `GigabitEthernet0/1` for the cable connection. A pop-up will confirm your selection.
    - Then click on `Switch1` and also choose `GigabitEthernet0/1`. This ensures a higher-speed (Gigabit) connection between the two switches.
    - Initially, the port LEDs on both switches may display *amber* as the devices negotiate speed and duplex. After a short period, they should both turn *green*, indicating a successful link.
14. **Confirm Final Layout**
    - By now, all PCs should be connected to either `Switch0` or `Switch1` using **Straight-Through** cables.
    - The two switches should be linked together via a **Cross-Over** cable at `GigabitEthernet0/1` on each switch.
    - Compare your setup with Figure 1.5, ensuring that each interface shows a green link light and that no errors are reported in the `Packet Tracer` interface or logs.

Tips for Connecting Two Switches:

Auto-MDIX Caution: While Auto-MDIX often allows you to use a straight-through cable for switch-to-switch connections, practicing with a cross-over cable is useful for learning traditional network cabling methods and understanding how older devices function.

Checking Interface Status: If your link lights stay *amber* for too long or do not turn green at all, try these steps:
- Verify you selected the correct *GigabitEthernet* ports on both switches.
- Make sure the ports are up (not `administratively down`) in the switch Config or CLI.
- Ensure that you indeed chose `Copper Cross-Over` from the menu.

Troubleshooting Port Labels: If you are unsure about a particular switch port's label, hover over the port or check the switch's Config tab for port mappings. ■

E. Verify the Completed Topology

Once you have connected all PCs to their respective switches and linked the switches together, it's important to verify that your network topology is correct and fully functional.

15. **Check Against Figure 1.5**
    - Confirm that each PC is connected to a valid `FastEthernet0/x` port on one of the switches, using a **Straight-Through** cable.
    - Verify that the two switches are connected to each other with a **Cross-Over** cable on their respective `GigabitEthernet0/1` ports.
    - Figure 1.5 shows an example of the final layout. Your topology should closely match this diagram to ensure consistency and proper functionality.
16. **Green or Amber Links**
    - In Packet Tracer, ports may appear *amber* briefly while they negotiate speed and duplex, especially when using `Gigabit` ports or `Auto-MDIX` features.
    - If a port *never* transitions to green (remains amber or off), verify that you have selected the correct cable type (`Copper Cross-Over` or `Copper Straight-Through`) and the correct port (`FastEthernet` vs. `Gigabit` vs. `Console`). Also confirm the port is not administratively shut down in the switch settings.

Tips for Cable Types and Negotiation:
Auto-MDIX Support: Modern switches can often correct cable type mismatches automatically. However, the **standard approach** still recommends a Cross-Over cable for connecting two similar devices (e.g., switch-to-switch or router-to-router).
Double-Check Labeling: If your cables or ports are mislabeled, it could cause link failures. Make sure each label clearly indicates the correct interface (e.g., `FastEthernet0/1`, `GigabitEthernet0/1`). ■

17. **Save and Exit**
    - Once you confirm all connections are correct and link lights display green, go to **File** → **Save** and store your layout, for example as `DeployingAndCablingLab1.pkt`.
    - If your layout differs from Figure 1.5 or if links remain amber or off, re-check all cables and port selections before saving. You can remove or replace any incorrect cables to resolve connectivity problems.

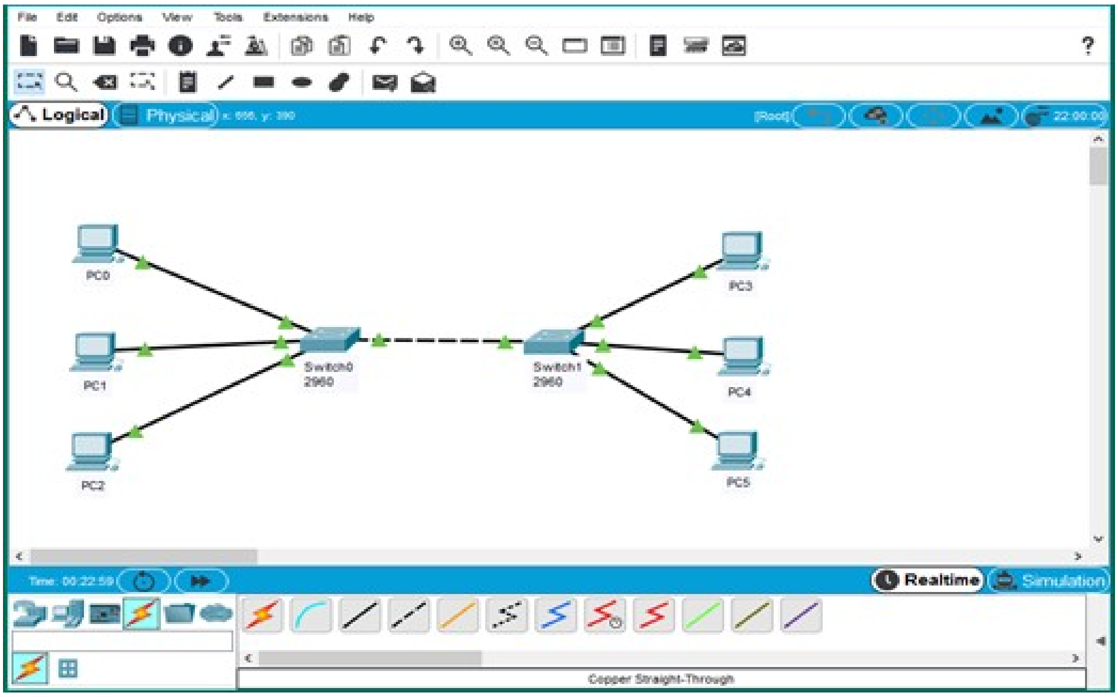


Figure 1.5: Completed Activity: PCs connected via Straight-Through to each switch, and the switches interlinked using Cross-Over at Gigabit ports.

Troubleshooting and Tips:

- **Cable Types Matter:**
  – Use `Straight-Through` for dissimilar devices (PC-to-switch).
  – Use `Cross-Over` for similar devices (switch-to-switch).
- **Multiple Cables:**
  – After selecting a cable type, hold `<CTRL>` to place multiple cables in sequence. Press *Esc* to exit cable placement mode.
- **Link Light Timers:**
  – Ports may show amber for a short time while negotiating speed/duplex. Wait a moment for them to turn green.
- **Re-check Port Selections:**
  – If you accidentally clicked a `Console` or `Serial` port, the link won't come up.

Measuring Success

- You have **two switches** in the workspace, each with **three PCs** connected via `Copper Straight-Through`.
- The **two switches** are linked together with `Copper Cross-Over` at their `Gigabit0/1` ports.
- All **link LEDs** have turned green, indicating active connections.
- You saved your final design as a `.pkt` file (e.g., `DeployingAndCablingLab1.pkt`).

— Further Exploration

- **Add IP Addresses:** If you assign IP addresses to each PC and switch (SVI interface), you can do a `ping` test in Packet Tracer's command prompt to confirm layer-3 connectivity.
- **Explore Physical View:** Switch to Physical view to visualize devices in "wiring closets," or add background images for a more realistic environment.
- **Experiment with VLANs or Router Connections:** Building on your basic topology, you can add VLANs on each switch or link them to a router to practice inter-VLAN routing or basic WAN setups.

Summary

You have successfully **deployed network devices** (switches, PCs) in Packet Tracer and **connected them** using correct cabling (`Straight-Through` for PC-to-switch, `Cross-Over` for switch-to-switch). With all ports active (green lights), you've established a basic functioning LAN. This foundation prepares you for more advanced tasks like assigning IP addresses, configuring VLANs, and integrating routers in subsequent labs.

2. Deploying Devices

Introduction

This lab shows you how to locate, deploy, and save multiple network devices in **Cisco Packet Tracer**. By the end, you will have explored different methods (drag-and-drop, copying, multi-selection) for placing routers, switches, and end devices in your workspace.

Objectives

- Open a sample file in Cisco Packet Tracer (`Deploying Devices.pkt`) to practice locating and deploying multiple network devices.
- Save the configured network file to ensure all settings and placements remain intact for future reference or assessment.
- Understand different methods for deploying devices (e.g., single-click, drag-and-drop, `<CTRL>` / `<SHIFT>` copy).
- (Optionally) configure your devices after placing them, preparing for troubleshooting or advanced network scenarios.

Lab Plan

In this lab, you will:

A. Open the `Deploying Devices.pkt` file in Cisco Packet Tracer.
B. Deploy routers, switches, and end devices using various placement methods.
C. Experiment with copying devices using `<CTRL>` or `<SHIFT>` techniques.
D. (Optionally) configure and then save the file for future reference.

Further Exploring 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.

Resources — Deploying Devices User Interface | . Watch this 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 2.3). 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.

Resources — 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.

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).
- **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.
- **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.

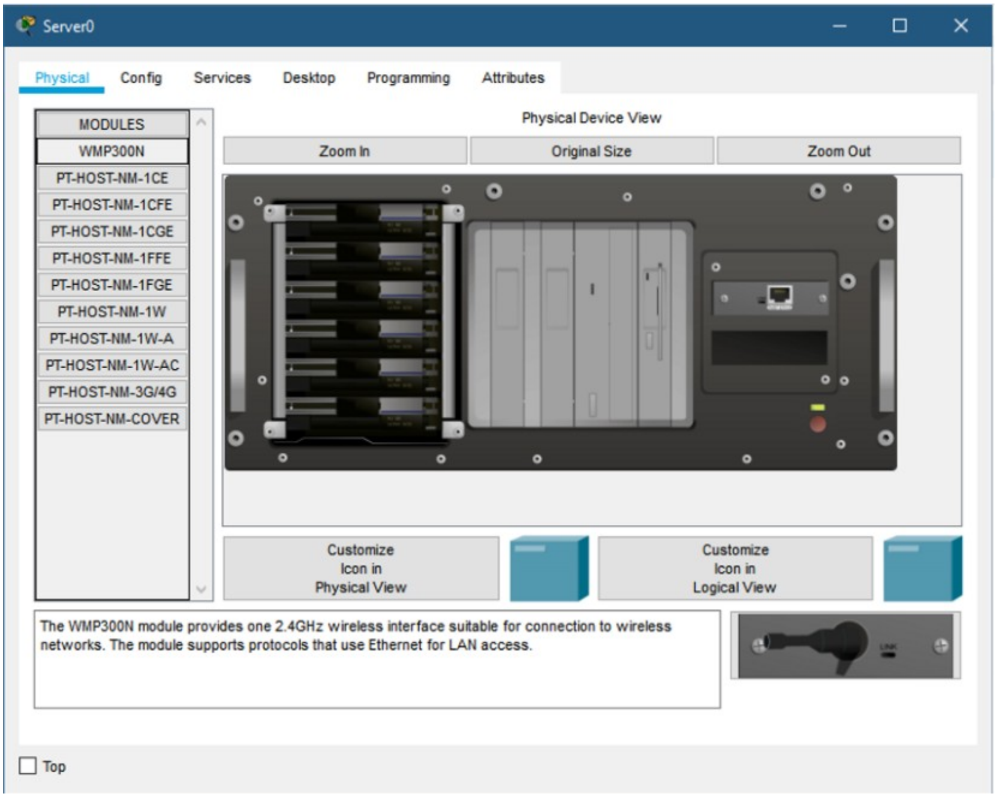


Figure 2.1: Physical Tab

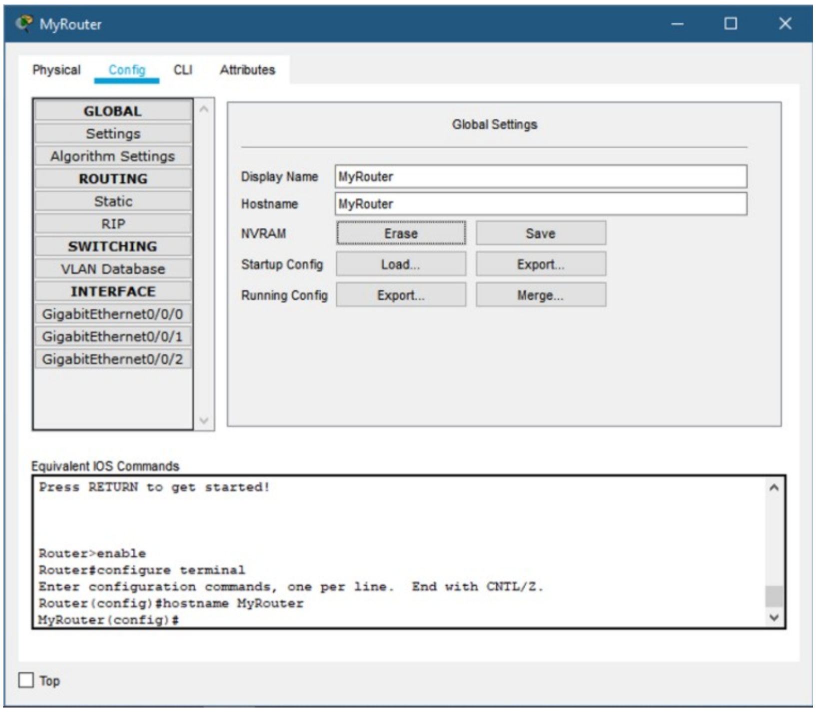


Figure 2.2: Config Tab

- **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,

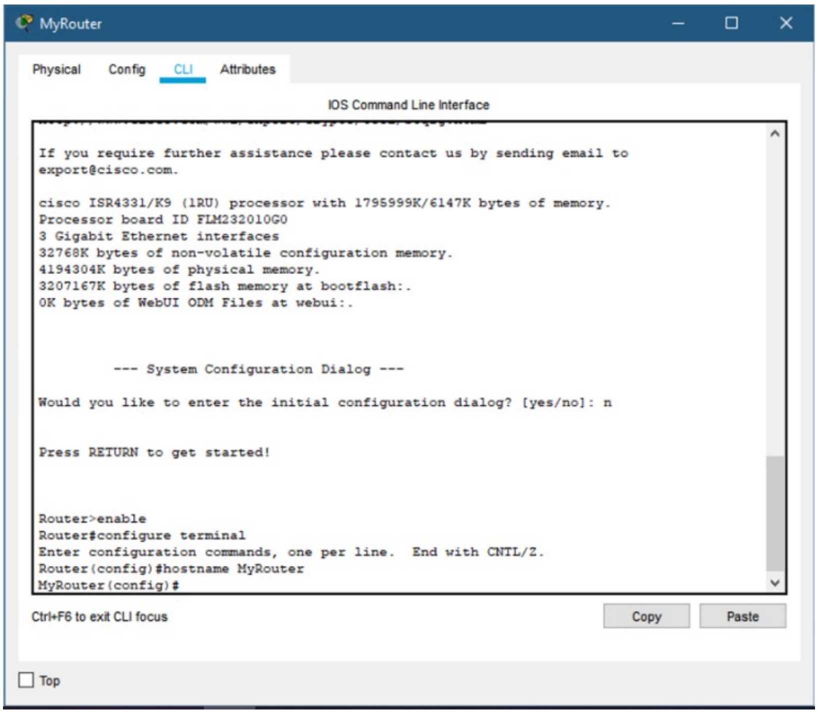


Figure 2.3: Command Line Interface (CLI) Tab

a web browser, and other applications.
- **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.

Resources — 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.

Resources — 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

Figure 2.4: Desktop Tab

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.

> Resources — **Create, Arrange, Uncluster, Delete, and Connect Clusters**. As a topology becomes larger and more complicated, clustering devices lets you combine them into a single

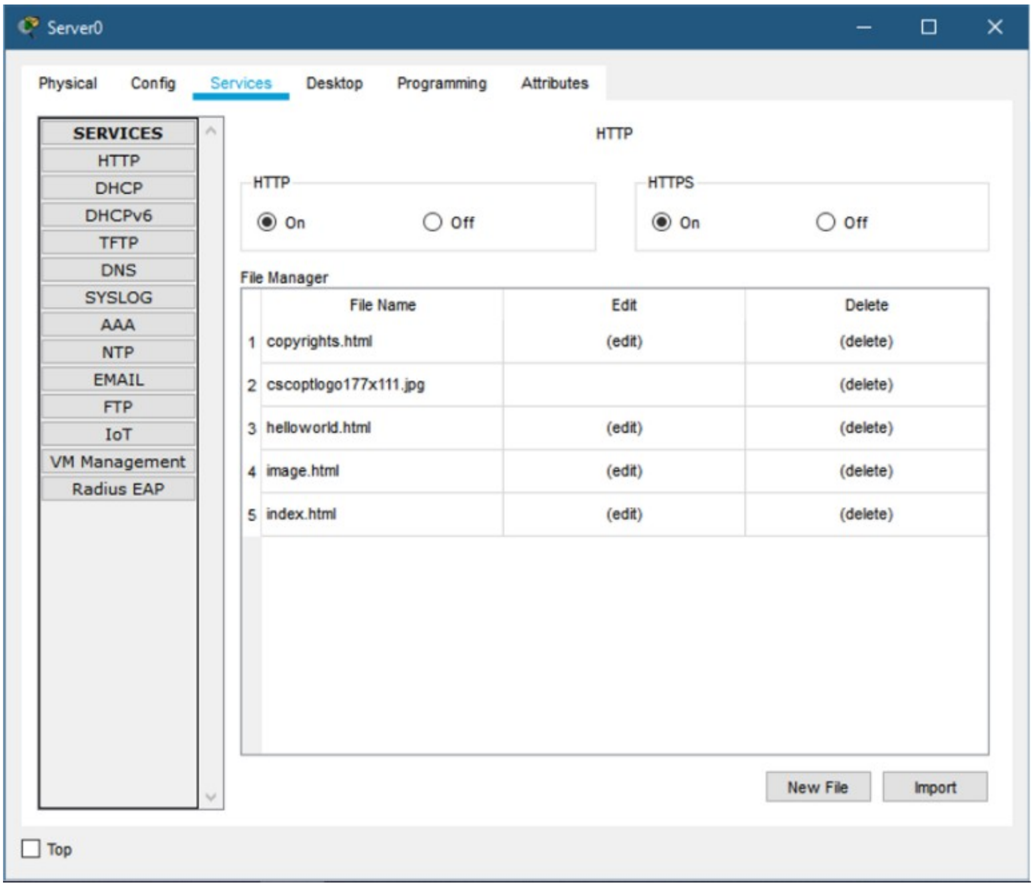


Figure 2.5: Services Tab

cloud icon to simplify the topology's appearance. You can uncluster or re-cluster devices as needed. This video shows how to create clusters, connect them, and keep your network organized.

Resources — Edit and Annotate a Topology. Networks often evolve over time. In Packet Tracer, you may need to modify and document your topology after you build it. This video explains how to edit and annotate an existing network design.

A. Open the Deploying Devices.pkt File

In this section, you will open a pre-configured Packet Tracer file named `Deploying Devices.pkt`. This file provides you with a basic network environment where you can practice deploying and managing various devices. Follow these steps carefully to ensure a smooth start.

1. **Locate the File:**
   Double-click on `Deploying Devices.pkt` to launch it in Cisco Packet Tracer. If you cannot locate the file, confirm that you have downloaded it from the GitLab repository or from the location your instructor or course materials have indicated. Sometimes, files can be stored in a `Downloads` folder or a class-specific directory, so be sure to check thoroughly.
2. **Check Version Compatibility:**
   If the file refuses to open or you see a "version mismatch" error, verify that your installed version of Cisco Packet Tracer is up to date (version 8.x or higher is recommended). If

needed, visit the official Cisco Networking Academy site or your institution’s software portal to download and install the most recent release.

3. **Observe the Initial Workspace:**
   After opening the file, you may see placeholder labels indicating where certain devices (like `Router0` or `Router1`) are supposed to go. Your workspace might look similar to Figure 2.6. These placeholders serve as a guide to help you position and identify devices correctly. If your screen appears significantly different, confirm you have opened the correct file and are running the appropriate Packet Tracer version.

> **Helpful Suggestions for Opening Packet Tracer Files:**
>
> **File Organization:** Keep your `.pkt` files in a dedicated course folder, so you can easily find and manage them for future labs or reference.
>
> **Backup Copies:** Save a backup copy of `Deploying Devices.pkt` (e.g., `DeployingDevicesBackup.pkt`) before making changes, in case you need to revert to the original setup.
>
> **Troubleshooting:** If you experience persistent issues when opening the file, try restarting Packet Tracer or checking that your computer meets the minimum requirements for the software. ■

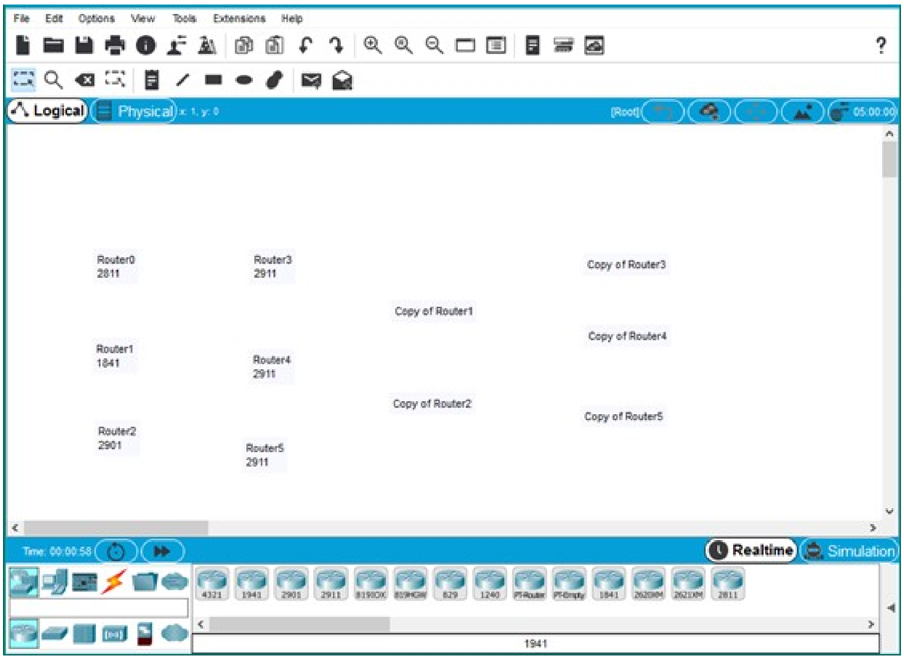


Figure 2.6: Starting point of `Deploying Devices.pkt`, often with labeled spots for routers or switches.

B. Learn How to Deploy Devices

In this section, you will practice placing different network devices (such as routers and switches) onto the predefined spots in your Packet Tracer workspace. Follow the steps below to ensure your devices are positioned correctly and saved for future work.

4. **Identify Labeled Spots:**
   If the file displays labels (e.g., `Router0`, `Switch1`), these hints suggest which router or switch models to place in those locations. Matching the labels helps keep your network

layout organized and clear.

5. **Open the Router Category:**
   - In the lower-left panel of Packet Tracer, select **Network Devices** from the top row of category icons.
   - Next, click **Routers** in the bottom row. You should now see a list of router models such as `2811`, `2911`, `1841`, and so forth (see Figure 2.7).

Figure 2.7: Device-Specific Selection Box

6. **Drag-and-Drop Placement:**
   - To place a router in a labeled spot, click and hold the icon of your chosen router (e.g., `2811`).
   - Drag it over to the label `Router0` in the workspace, then release your mouse.
   - This method is especially helpful when you want to accurately match the device label on the workspace.
7. **Single-Click Placement:**
   - Alternatively, click the router model once (for example, `1841`).
   - Move your cursor to where `Router1` is labeled on the workspace and click again to place the device.
   - This approach simplifies adding devices one at a time to various spots.
8. **Use `<CTRL>` or `<SHIFT>` to Copy:**
   - `<CTRL> Key:` Hold down `<CTRL>` after selecting a device (e.g., a router). Each subsequent click in the workspace adds another copy of that same device.
   - `<SHIFT> Key:` You can also highlight one or more devices you have already placed, then hold `<SHIFT>` (or `<CTRL>`) and drag/click to copy them to new spots. This is useful if you need multiple routers or switches of the same type.
9. **Check Your Final Layout:**
   - Your workspace might look similar to Figure 2.8, with routers (and possibly switches) positioned at the labeled locations.
   - If any device is misplaced, simply click on it and press the `Delete` key to remove it, or go to **Edit** → **Undo**. Then reposition or re-add the device as needed.

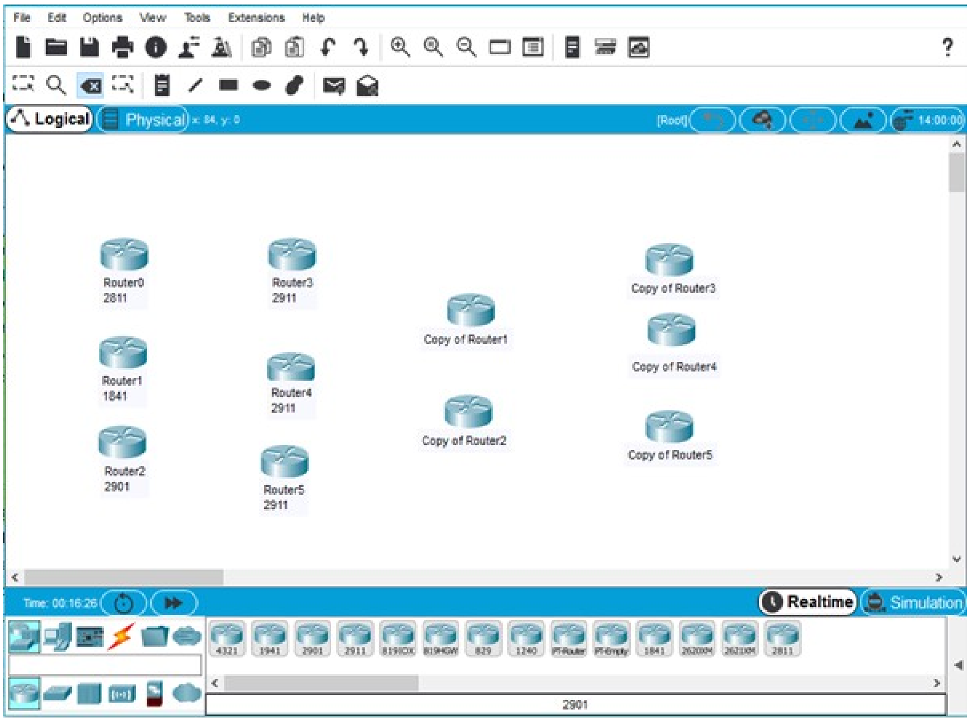


Figure 2.8: Sample final layout with various routers placed in the workspace.

10. **Save the File:**
    - When you are satisfied with your device placements, go to **File** → **Save** and name your file, for instance, `DeployingDevicesLab2.pkt`.
    - Keeping Packet Tracer open allows you to continue to the next steps (such as cabling or configuring the devices). If you close Packet Tracer, you can reopen the `.pkt` file later to pick up where you left off.

Suggestions for Placing Devices:

Plan Ahead: Before placing devices, visualize how you want your network to be organized. Consider spacing so that cables remain clear and easy to read.

Use Labels: If your assignment or lab instructions specify naming devices (e.g., `RouterA`, `RouterB`), you can rename them by clicking on the device label in the workspace.

Saving Time: If you know you will need multiple routers of the same type, use the `<CTRL>` or `<SHIFT>` copying method to speed up placement.

C. (Optional) Configure or Inspect the Devices

If you would like to take a closer look at the routers or switches you have placed—or even begin basic configuration—Packet Tracer offers two main approaches. Simply click on a device in the workspace to open its configuration window. You will then see two primary tabs:

- **Config** tab (GUI-based): This tab provides a user-friendly, graphical interface where you can make changes such as:
  - Setting the *Display Name* or *Hostname* of the device.
  - Adjusting *Interface* settings (e.g., `FastEthernet0/0`, `GigabitEthernet0/1`).
  - Turning *services* on or off (if the device supports services like DHCP or DNS).
  - Viewing the *Equivalent IOS Commands* generated by your GUI actions, allowing you

to learn the CLI syntax.
- **CLI** tab (console): This tab gives you access to the device's Command-Line Interface, simulating a real Cisco IOS environment. From here, you can:
  - Enter `enable` or `configure terminal` mode.
  - Use IOS commands (e.g., `show running-config`, `interface`, `ip address`) to configure or inspect the device.
  - Practice troubleshooting commands (e.g., `ping`, `traceroute`, `show ip interface brief`).

Tip: Any settings or configuration changes you make in either the **Config** tab or the **CLI** tab will automatically appear in the other. This mirroring lets you see how the GUI-based actions translate into IOS commands in real-time.

Saving Your Changes:

Once you are satisfied with your device configuration or inspection, select **File** → **Save**. Packet Tracer will store your changes in the `.pkt` file. The next time you open this file, your updated device configurations will be intact.

For more complex tasks, such as setting *passwords*, *SSH configuration*, or *routing protocols*, refer to the corresponding sections or labs in your course materials.

If you plan to continue cabling or adding more devices, remember to save periodically, ensuring no progress is lost if your session unexpectedly closes.

Troubleshooting and Tips

Mismatch Errors: If you get warnings about an older or newer Packet Tracer version, try updating.

Device Not Appearing: Ensure you selected the right subcategory (e.g., **Routers**, **Switches**, **End Devices**).

Undo/Redo: Packet Tracer does not always have a robust `Undo` option. If you misplace something, you can *Delete* and re-add it.

File Save Format: Use `.pkt` if you only need the topology without instructions or scoring.

Measuring Success

- The **Deploying Devices.pkt** file opens without errors.
- You can **place routers, switches, or end devices** using single-click or drag-and-drop.
- **<CTRL> or <SHIFT>** copying is understood and tested to replicate multiple devices quickly.
- (Optional) Basic device configurations remain after saving, verified by reopening the `.pkt` file.

— Further Exploration

The remainder of this lab includes several Packet Tracer Activities (PTA) in the `LAB 02 - Deploying Devices -> Optional` folder. You can try:

LAB 2.1—Connect Devices using Wireless Technologies

- Connect a laptop to an office WLAN and verify internet access.

- Pair devices via Bluetooth, enabling discovery and selection to test connectivity.
- Enable a mobile hotspot on a smartphone and connect a laptop for stable browsing.

LAB 2.2—Configuring and Simulating Office and Home Networks

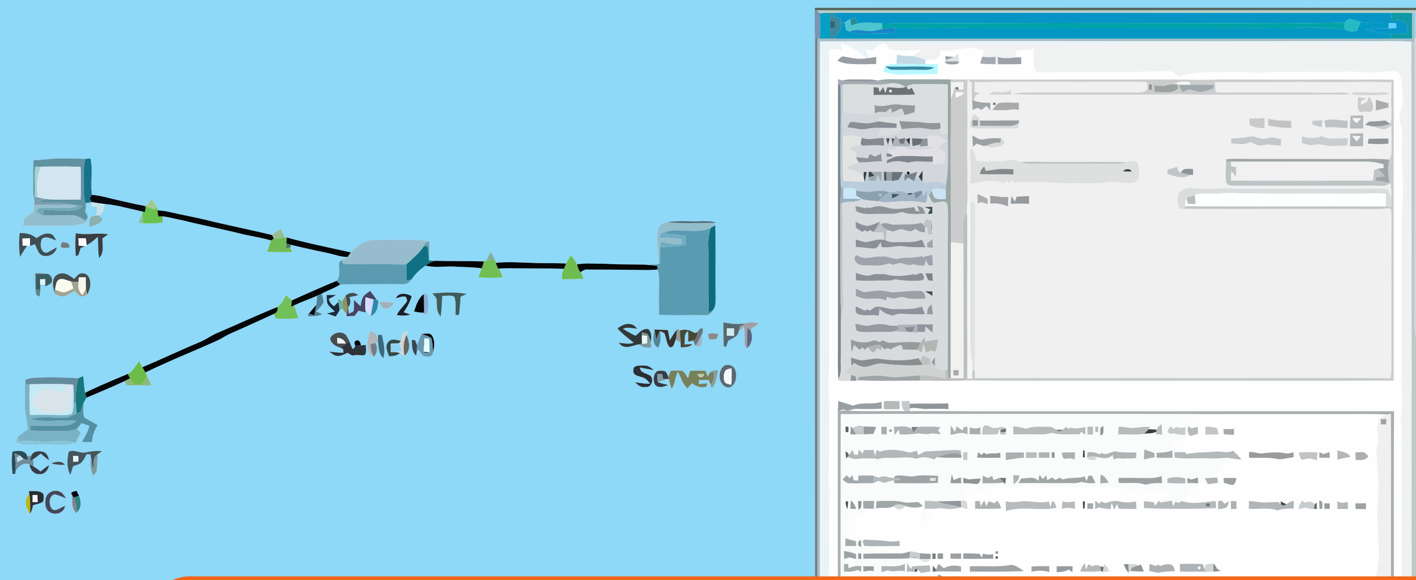
- Install an extra switch in the office rack, physically mounting and linking it to existing hardware.
- Cable a PC to the switch and confirm network settings.
- Manage clusters for grouping interconnected devices, optimizing performance and redundancy.
- Add a second home cluster and integrate it seamlessly with the first.

LAB 2.3—Configuring and Managing Network Devices Using CLI

- Establish a console connection with a device to access its **CLI**.
- Transfer configuration information (upload config or manually type commands).
- Save the changes (e.g., `write memory` or `copy run start`) to preserve them after reboot.

Summary

In this lab, you learned how to **open and place devices** in an existing Packet Tracer file (`Deploying Devices.pkt`). You explored **various placement methods** (drag-and-drop, single-click, `<CTRL>`-copy) and optionally configured them using the Config or CLI tabs. By saving your `.pkt` file, you ensure your device placements and settings persist for later labs or troubleshooting exercises.



3. Configure End Devices

Introduction

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. You will also use command-line tools to verify connectivity and troubleshoot basic networking issues.

Objectives

- Launch Packet Tracer and create a small network topology with a switch, two PCs, and a server.
- Assign IP settings (address, subnet mask, gateway) on end devices.
- Verify connectivity using `ping` and optionally a web browser.
- Explore basic switch configuration via the **Config** tab or CLI interface.

Lab Plan

In this lab, you will:

A. Launch Packet Tracer and start from a blank Logical workspace.
B. Build a simple network topology (one switch, two PCs, one server) and assign IP addresses.
C. Test connectivity with `ping` and web-browser checks.
D. Save your network file for future use or assessment.

Resources — 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.

Resources — 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.

A. Launch Packet Tracer and Prepare the Workspace

This section guides you through starting Cisco Packet Tracer and verifying that you have the correct interface and toolbars displayed for the labs ahead.

1. **Open Packet Tracer:**
   Locate the Packet Tracer icon on your desktop or in your applications folder. Double-click the icon to launch the program. You should see a **default Logical workspace**, typically a blank gray area where you will soon place network devices (see Figure 3.1).
2. **Confirm the Interface:**
   Look at the lower-left side of the Packet Tracer window. Ensure you can see the major categories:
   - *Network Devices*
   - *End Devices*
   - *Connections*

   If you do not see these, or if the interface seems significantly different (e.g., missing menus or a "version mismatch" error), update your Packet Tracer installation to version 8.x or later.
3. **Identify the Starting View:**
   By default, you begin in the *Logical* workspace. You should see:
   - An empty gray canvas for creating your network.
   - A toolbar at the bottom listing device icons and cable types.
   - A toolbar on the upper-left side for switching between *Realtime* and *Simulation* modes, among other options.

   Your screen should resemble Figure 3.1. If it appears drastically different, verify you are indeed in the *Logical* view rather than the *Physical* view (the toggle for these views is in the top-left corner).

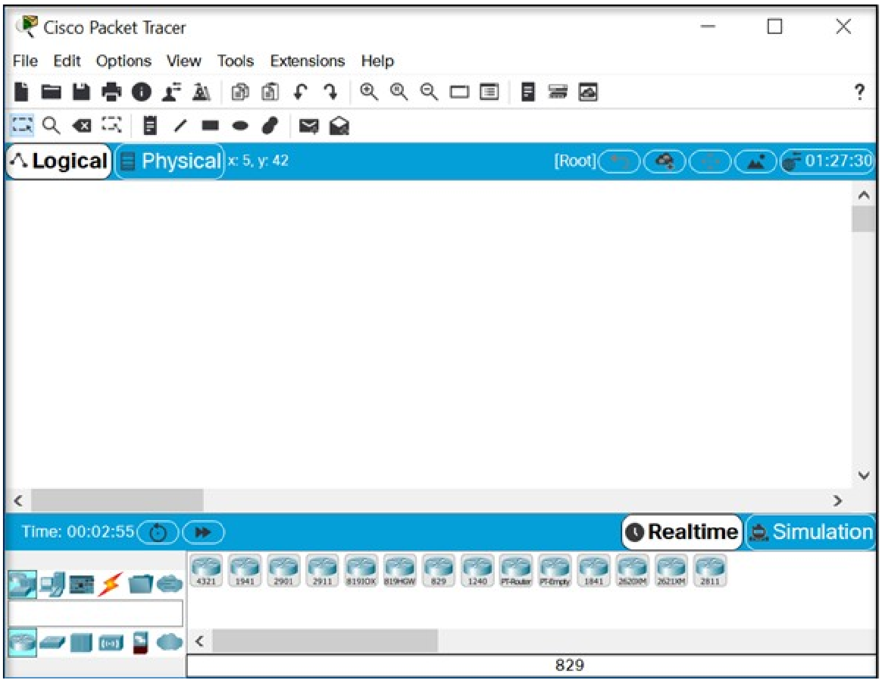


Figure 3.1: Initial Workspace in Packet Tracer

B. Build the Topology and Assign IP Settings

4. **Place Devices and Cables**
   - From the bottom-left device categories in Packet Tracer, add the following devices onto the workspace:
     - **Switch0**
     - **PC0**
     - **PC1**
     - **Server0**
   - Connect each end device to **Switch0** using a *Copper Straight-Through* cable. For instance:
     - PC0 → Switch0 (*FastEthernet0/1*)
     - PC1 → Switch0 (*FastEthernet0/2*)
     - Server0 → Switch0 (*FastEthernet0/3*)
   - Wait a few seconds for the link lights to turn green, indicating active and functional connections.

Tips for Building the Topology:
Make sure you drag the correct device icons (e.g., *PC* versus *Laptop*, or *Server* versus *Generic* IoT) to avoid confusion later.
If a link light stays *red*:
- Double-check the cable type (it should be *Copper Straight-Through* for end devices to switch).
- Confirm the device ports match (e.g., *FastEthernet0/1* on the switch with *FastEthernet0* on the PC).
- Ensure the devices are powered on (by default, they usually are in Packet Tracer).

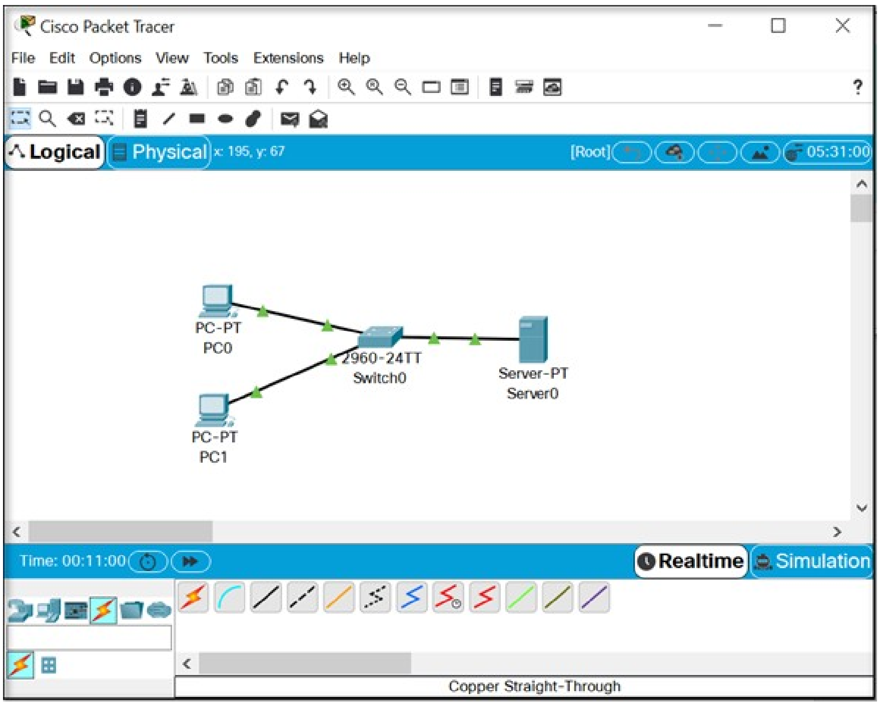


Figure 3.2: Network Topology Configuration in Cisco Packet Tracer

5. **Configure the Server's IP**
    - Click **Server0**, then select: *Desktop* → *IP Configuration*.
    - Enter `192.168.1.1` for the IP Address and `255.255.255.0` for the Subnet Mask.
    - (Optional) Set the Default Gateway to `192.168.1.254` if you plan to connect a router later.

Why Configure the Server First?
By assigning the **Server** an IP address early on, you can test all other PCs against a "known target."
This helps you quickly diagnose if any new device on the network is correctly configured (it should be able to *ping* `192.168.1.1`).

6. **Configure PC0**
    - Click **PC0**, then select: *Desktop* → *IP Configuration*.
    - Assign:
        - IP Address: `192.168.1.2`
        - Subnet Mask: `255.255.255.0`
        - (Optional) Default Gateway: `192.168.1.254` if you have one.
    - Next, open the **Command Prompt** on PC0's *Desktop*. Type:

```
ping 192.168.1.1
```

    - Figure 3.3 shows how the *Command Prompt* should appear.

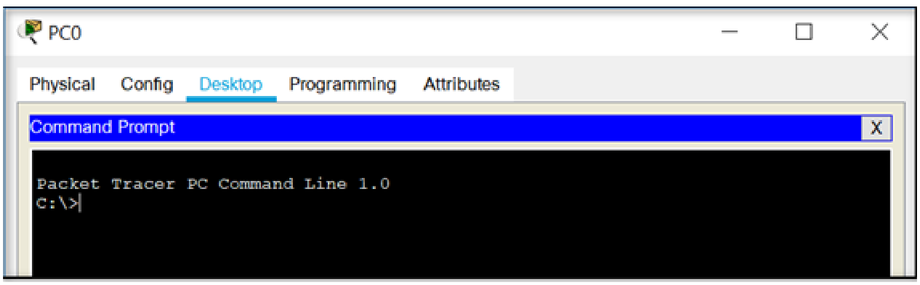


Figure 3.3: Command Prompt in Cisco Packet Tracer

    - If everything is configured correctly, you should see *successful replies* (see Figure 3.4).

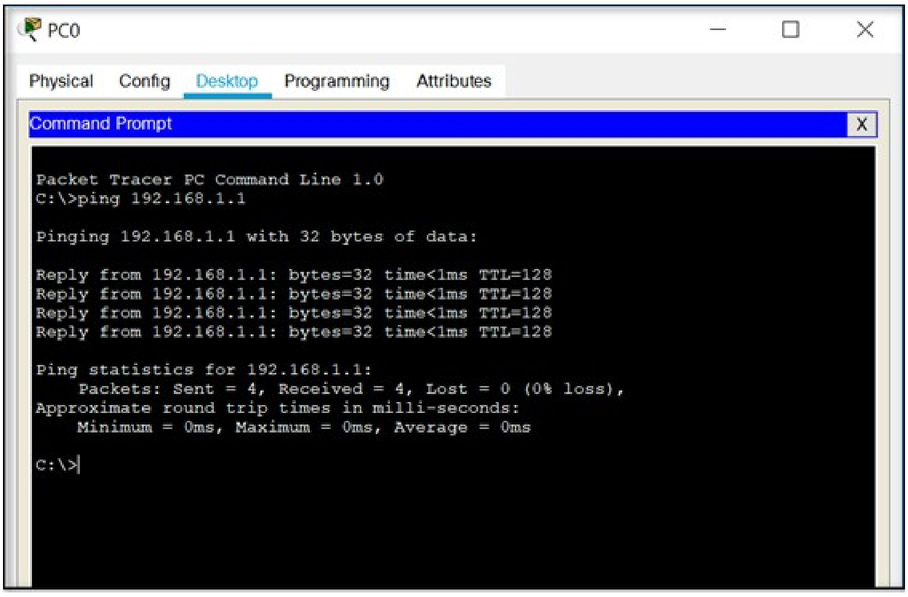


Figure 3.4: Successful Ping Test in Cisco Packet Tracer

Troubleshooting Pings:

If `ping 192.168.1.1` fails from PC0:

- Verify **PC0**'s IP address is on the same subnet (`192.168.1.x`).
- Check cabling or switch port assignments.
- Re-check **Server0**'s IP configuration.

7. **Configure PC1**
   - Repeat the same process as with PC0:
     - IP Address: `192.168.1.3`
     - Subnet Mask: `255.255.255.0`
     - Default Gateway: `192.168.1.254` (if applicable)
   - Confirm you can reach the server using:

```
ping 192.168.1.1
```

8. **Test the Web Browser (Optional)**
   - If you have the server's *HTTP* service enabled, open **PC0** or **PC1**, then choose *Desktop* → *Web Browser*.
   - Type `192.168.1.1` in the URL field and click [Go]. You may see the server's default page (as in Figure 3.5) if the server is hosting a default site.

Exploring HTTP Features:

If you see a web page, it means the server is responding to HTTP requests. This is a **quick check** to ensure layer 7 (application layer) connectivity.

If no page appears, verify that the *HTTP* service is *On* under the *Services* tab on **Server0**.

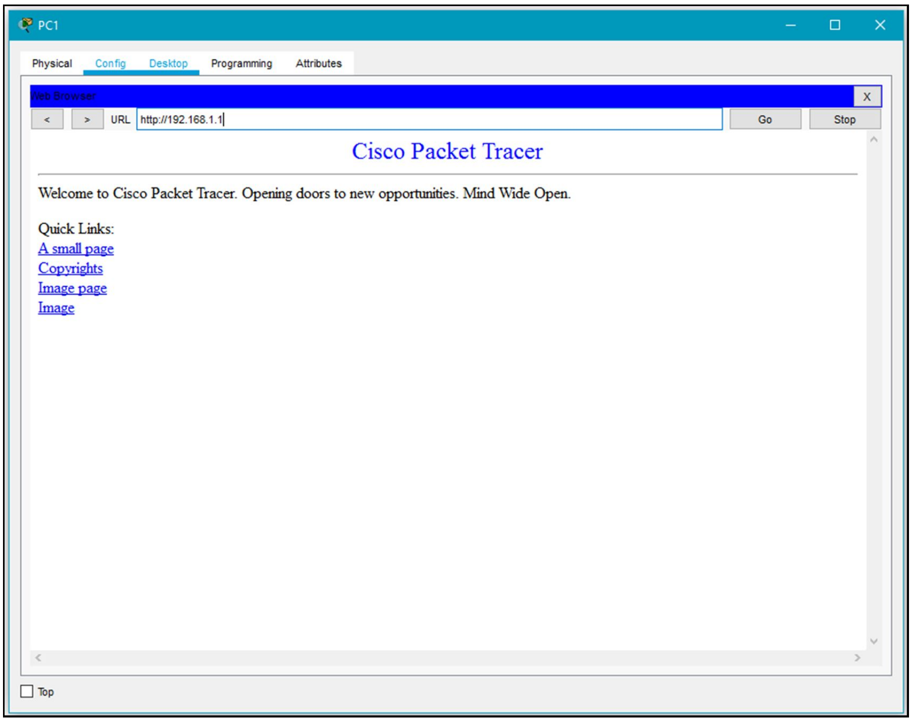


Figure 3.5: Testing the Server's Web Page via PC1

C. Explore Switch Configuration and Save

9. **View Basic Switch Settings**
    - Click on **Switch0** and select the *Config* tab. Under *Global Settings*, rename the switch (e.g., "SwitchLab3"), as illustrated in Figure 3.6.

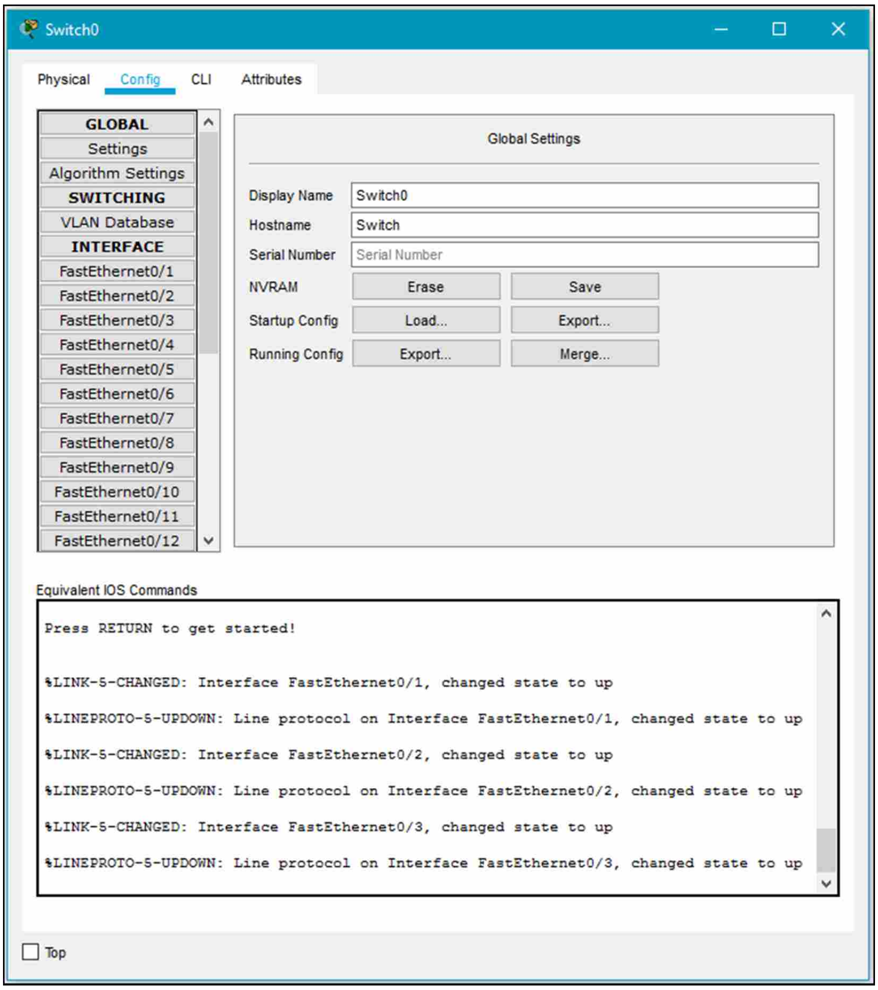


Figure 3.6: Config Tab on Switch0 in Cisco Packet Tracer

- Observe the interface configuration options. You can:
  - *Shutdown* any port if you want to disable it.
  - Adjust *bandwidth* or *duplex* to simulate different network conditions.
- Each change you make in the *Config* tab automatically generates the *Equivalent IOS Commands* displayed at the bottom. This helps you learn actual Cisco CLI syntax while using a graphical interface.

Tips for Navigating Switch Settings:
If you plan to manage the switch remotely (via Telnet or SSH), you may also want to set a management IP on the switch's *VLAN 1* interface and enable a default gateway.
Renaming the switch (e.g., "SwitchLab3") is a best practice, especially if you have multiple switches in a large topology.
The *Equivalent IOS Commands* section is an excellent way to compare the Packet Tracer GUI approach with real-world CLI commands.

10. **CLI Mode (Optional)**
    - To view or configure the switch as you would in a real environment, click the *CLI* tab. You will see something like:

```
Switch>enable
Switch#configure terminal
```

```
Switch(config)#hostname SwitchLab3
```

- As shown in Figure 3.7, these steps replicate actual commands you would type on a Cisco switch.
- The *Config* tab is simply a shortcut; using the CLI is great practice for real-world networking skills.

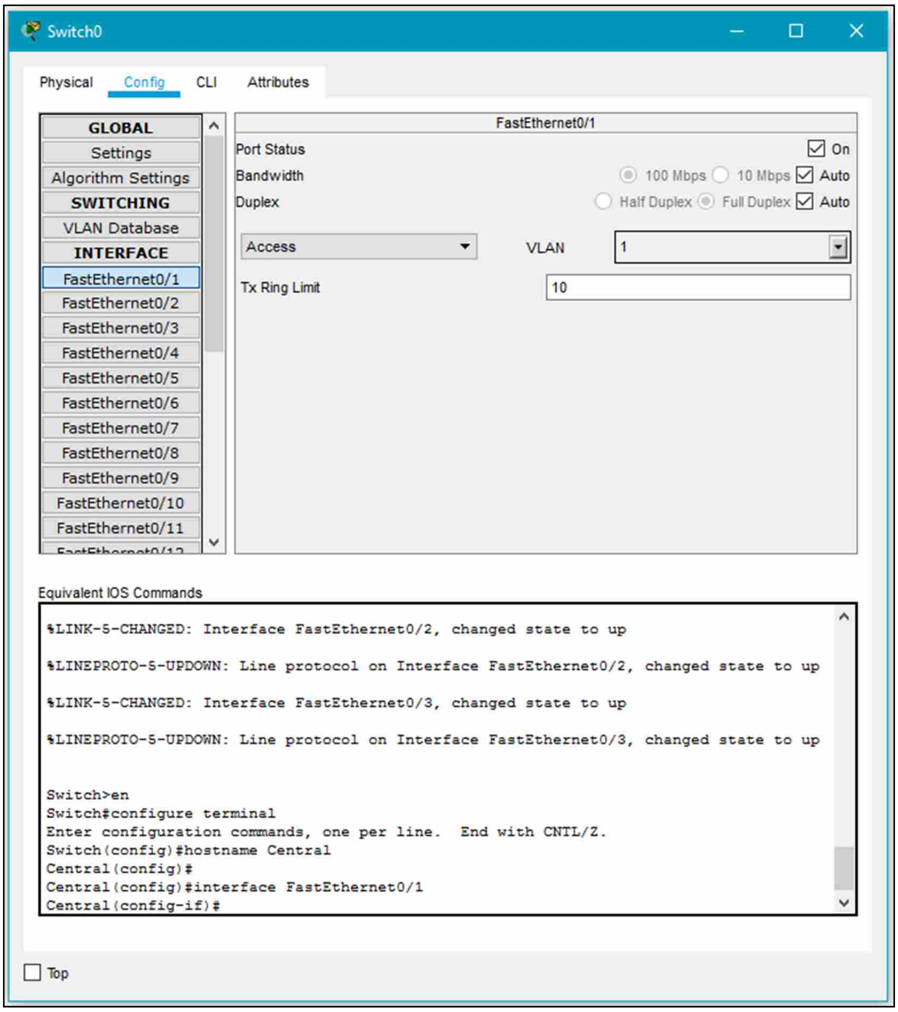


Figure 3.7: Switching to the CLI Tab in Cisco Packet Tracer

Tips for CLI Usage:
Remember the key commands for saving your configuration in a real switch:

```
Switch# copy running-config startup-config
```

In Packet Tracer, simply *saving* the Packet Tracer file will preserve your configuration. However, practicing the copy command is still worthwhile. ■

11. **Save Your File**
    - From the Packet Tracer menu, select **File** → **Save As** and name the file, for example: `ConfigureEndDevicesLab3.pkt`.
    - Reopening this file later will keep all your IP configurations and switch name changes.

Troubleshooting and Tips

No Ping Reply: Double-check IP addresses (typos are common). Ensure a *straight-through* cable is used for PC-switch links.

Switch Ports Amber: Some delay is normal for link negotiation. If never green, verify you didn't `shutdown` the interface or mismatch speed/duplex settings.

Subnet Mismatch: If the server uses `255.255.255.248` but PCs use `255.255.255.0`, pings will fail.

CLI vs. Config Tab: Real Cisco gear typically uses CLI. Packet Tracer's Config tab is educational, mapping directly to CLI commands for easy reference.

Measuring Success

- **PC0, PC1, and Server0** all respond to `ping` requests.
- **Web Browser** (on PC1 or PC0) can load the server's default page if `HTTP` is active.
- **Switch** changes (hostname, interface shutdown) reflect in the *Equivalent IOS Commands*.
- Your **.pkt file** is saved and re-openable, preserving the IP settings and switch configuration.

Summary

In this lab, you **configured a small network** with a switch, two PCs, and a server. You assigned IP addresses, tested `ping`, optionally tested HTTP, and explored how to rename or adjust switch settings. These steps prepare you for more advanced labs with routing, wireless, and additional features in Cisco Packet Tracer.

4. Create a Simple Network Using Packet Tracer

Introduction

In this lab, you will learn how to **build and configure a simple network** in Cisco Packet Tracer. You will place and connect various network devices, including a PC, a wireless router, a cable modem, a cloud, and a server. You will then verify connectivity, test basic services, and finally save your `.pkt` file for future use. By following these steps, you will gain hands-on practice in creating a straightforward but realistic network scenario.

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 to ensure the network is functional (e.g., `ping`, web browsing, DNS lookups).
- Save the Packet Tracer file and exit the application, securing the completed network configuration.

Lab Plan

In this lab, you will:

A. Launch Packet Tracer and create a *new* workspace.
B. Add devices (*PC*, *Wireless Router*, *Cable Modem*, *Cloud*, and *Cisco.com Server*) to form the topology in Figure 4.1.
C. Assign IPs or use *DHCP* to ensure each device can communicate.
D. Verify connectivity (e.g., `ping`, domain name resolution).
E. Save and close your project.

Topology and Addressing

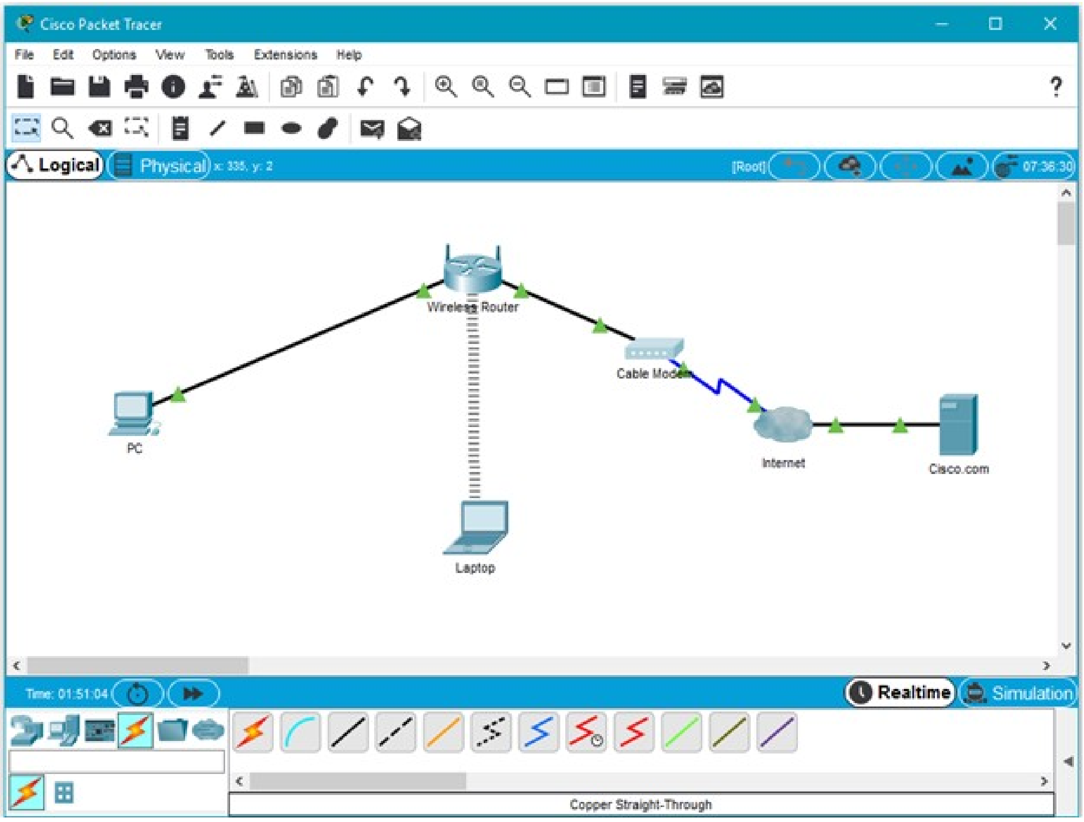


Figure 4.1: Topology of a Simple Network in Cisco Packet Tracer

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		

Some devices will receive addresses via DHCP, while others will use static assignments. The **Wireless Router** and **Cisco.com Server** will serve or use these IP settings as shown.

Resources — 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.

Resources — 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.

A. Build the Network Topology

1. **Launch Packet Tracer and Start a New Workspace**
   Double-click the Packet Tracer icon (or open its executable directly). After it starts, a blank *Logical* workspace should appear, as shown in Figure 4.2.

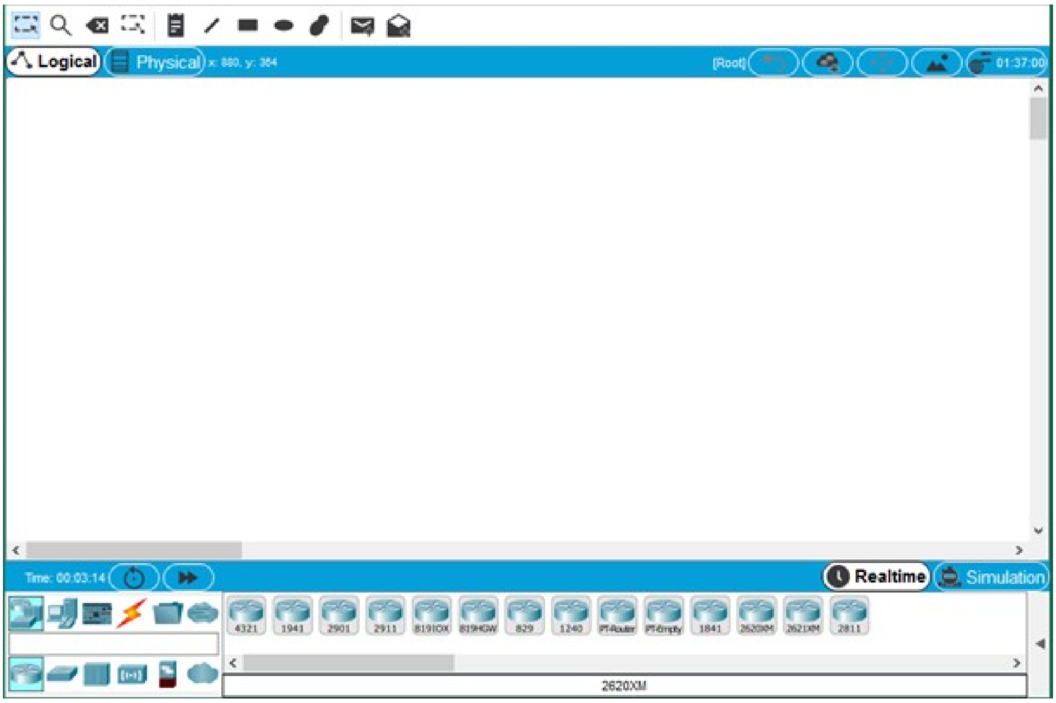


Figure 4.2: Adding Network Devices to the Workspace in Cisco Packet Tracer

2. **Place and Connect Devices**
   Use the *Device-Type Selection* box (on the left pane of Packet Tracer) to place the following:
   - A **PC** (or Laptop)
   - A **Wireless Router**
   - A **Cable Modem**
   - A **Cloud**
   - A **Cisco.com Server**

   — **Why do this?.** Each device represents a specific role:
   - **PC / Laptop**: End-user workstation where you can test connectivity (pings, web browsing, etc.).
   - **Wireless Router**: Provides local network access (wired + wireless) and often includes a built-in DHCP server for IP assignments.
   - **Cable Modem**: Simulates an internet service provider's (ISP) residential modem.
   - **Cloud**: Represents the ISP or WAN connection that links your local network to the outside world.
   - **Cisco.com Server**: Acts as a remote server hosting `Cisco.com` domain services such as DNS, web pages, or additional configurations.

   Placing all these devices helps you practice a realistic end-to-end setup, mirroring a home or small-office network accessing external internet services.

   Optional Rename: If desired, click any device, select the **Config** tab, and modify the *Display Name* (e.g., rename *Wireless Router* to *HomeRouter*).

Cabling:

- PC → **Wireless Router** using *Copper Straight-Through*
- **Wireless Router** → **Cable Modem** using *Copper Straight-Through*
- **Cable Modem** → **Cloud** using *Coaxial*
- **Cloud** → **Cisco.com Server** using *Copper Straight-Through*

— **Why do this?.** Different cable types mimic real-world hardware scenarios:

- **Copper Straight-Through**: Standard Ethernet cable between most LAN devices (PC to router, router to switch, etc.).
- **Coaxial**: Commonly used from the modem to the ISP network or cloud, reflecting typical broadband connections.

Ensuring you select the correct cable type in Packet Tracer prevents errors (such as no link lights) and creates a more accurate simulation of how home or small-office networks connect to an ISP.

B. Configure the Devices

3. **Wireless Router Setup**

Wireless:

- Click the **Wireless Router**, then select the **GUI** tab and choose **Wireless** (as shown in Figure 4.3).
- Under **Network Name (SSID)**, type in `HomeNetwork`.

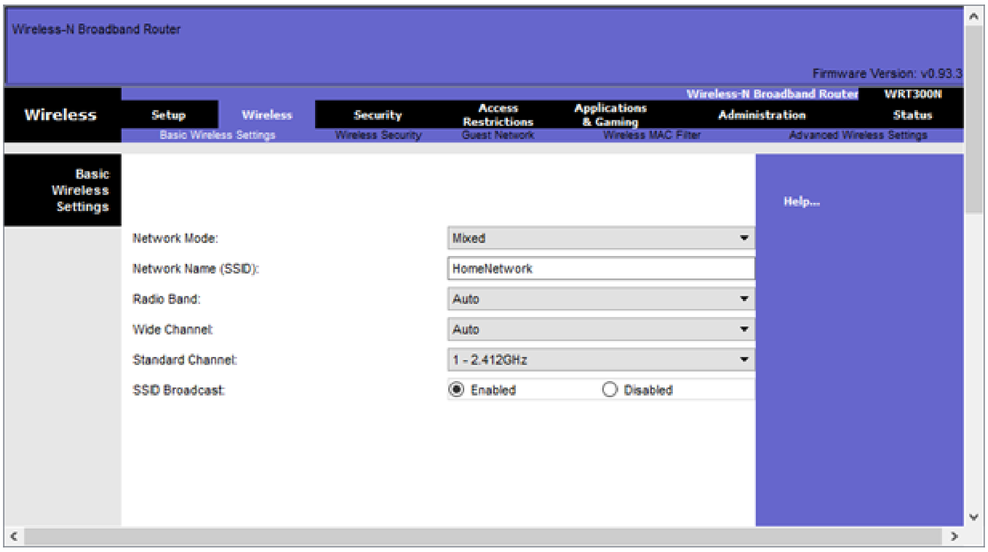


Figure 4.3: (Wireless Tab) Configuring the Wireless Network in the Wireless Router

— **Why do this?.** Renaming your SSID to `HomeNetwork` helps laptops and other wireless devices quickly identify and connect to the correct Wi-Fi. This setup mirrors what you'd find on a typical home or small office router.

Internet Setup:

- In the **Setup** tab, ensure the **DHCP** option is enabled.
- For **DNS**, enter `208.67.220.220`.
- Click **Save Settings**.

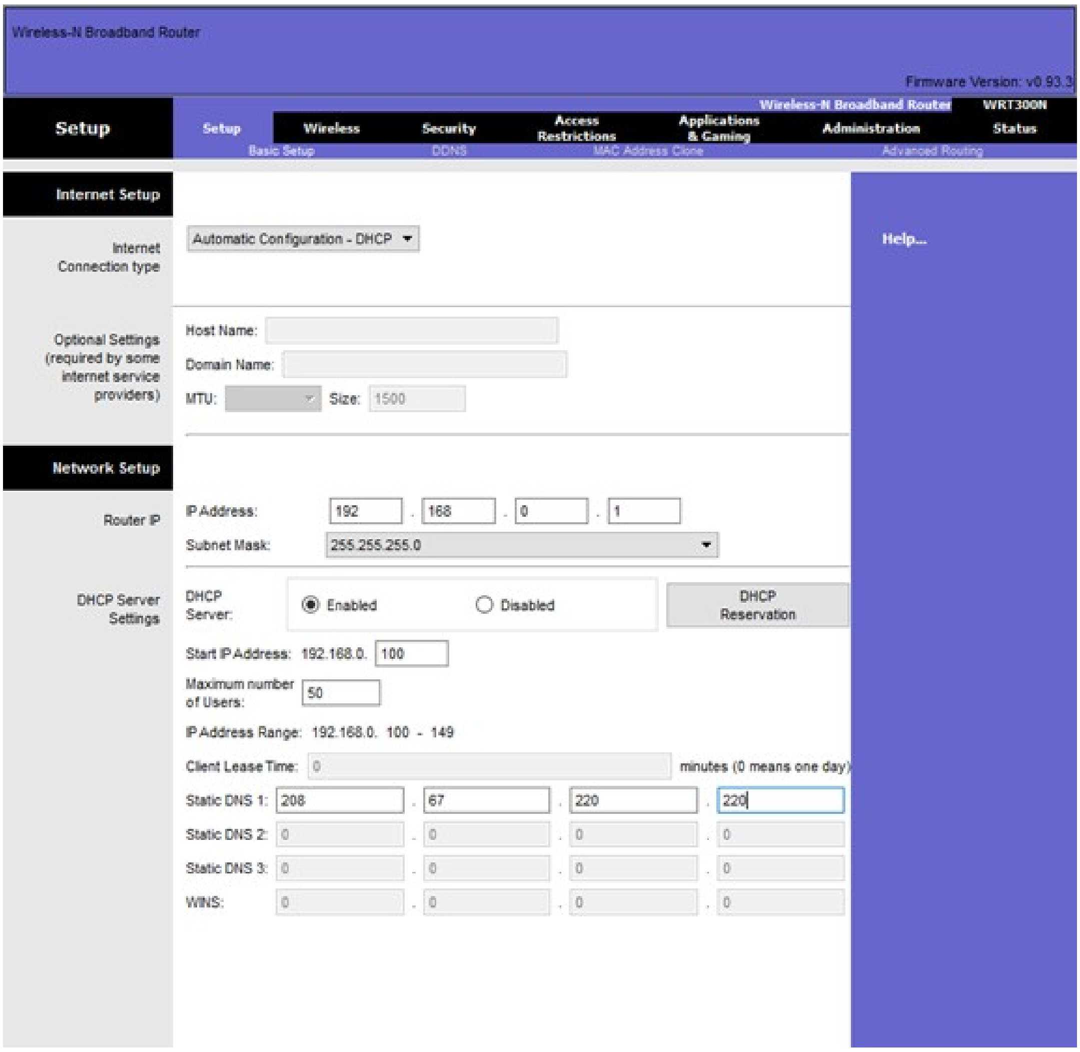


Figure 4.4: (Setup Tab) Configuring the Internet Connection on the Wireless Router

> **— Why do this?.** Keeping **DHCP** active on the router automatically provides IP addresses to all connected LAN and wireless clients. Setting **DNS** ensures that those clients can resolve domain names (like `google.com`) without needing manual configuration. This simulates a real small office or home router scenario.

4. **Laptop Wireless Configuration**

   Physical Module:

   - Power off the Laptop, remove its *Ethernet NIC*, and install a **Wireless WPC300N** interface card. Then power it back on.

   > **— Why do this?.** Packet Tracer laptops default to a wired network interface. Replacing it with a wireless module emulates how real laptops typically connect via Wi-Fi, giving you a more authentic experience in configuring wireless connectivity.

   Connect to Wi-Fi:

   - Select the Laptop's **Desktop** tab, then go to **PC Wireless**.
   - Find the SSID `HomeNetwork` and click *Connect*.

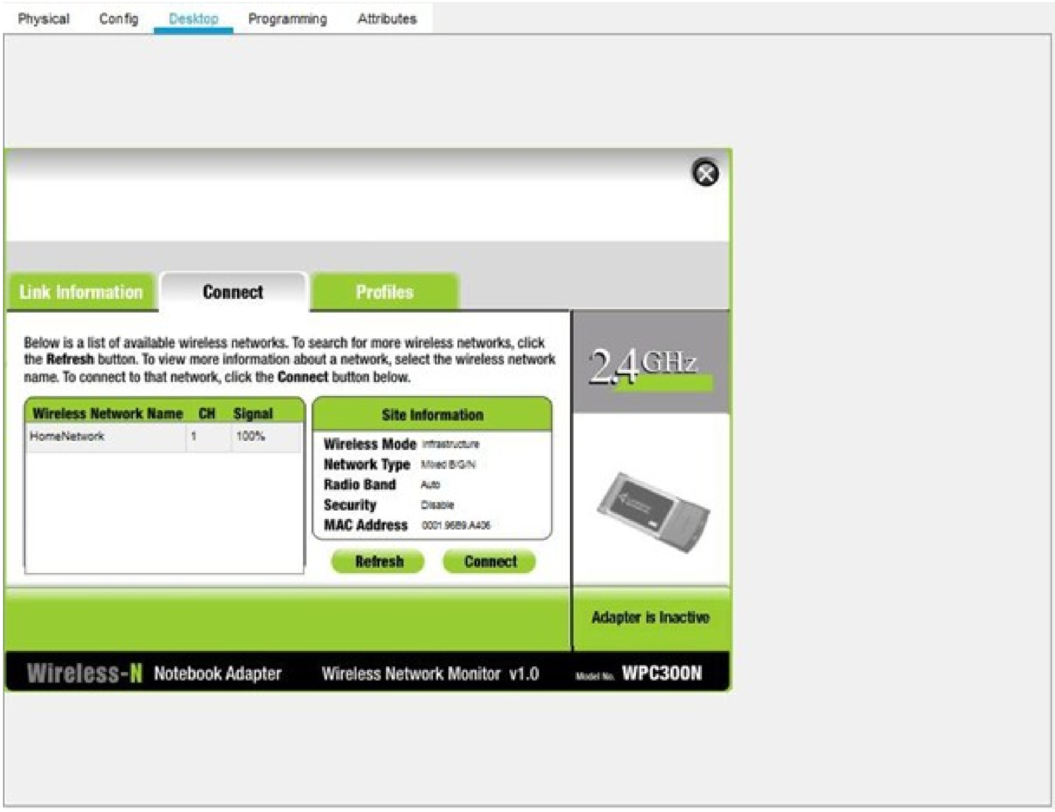


Figure 4.5: (Laptop) Connecting to the `HomeNetwork` Wireless Network

— Why do this?. Just like a real laptop would scan for Wi-Fi networks, this step ensures your laptop joins `HomeNetwork`. Once connected, it will receive an IP address (assuming DHCP is active on the router).

5. **PC (Wired) Using DHCP**

- On the PC, go to **Desktop** → **IP Configuration** and select `DHCP`.
- After a moment, the PC should receive an IP address from the Wireless Router's DHCP service.

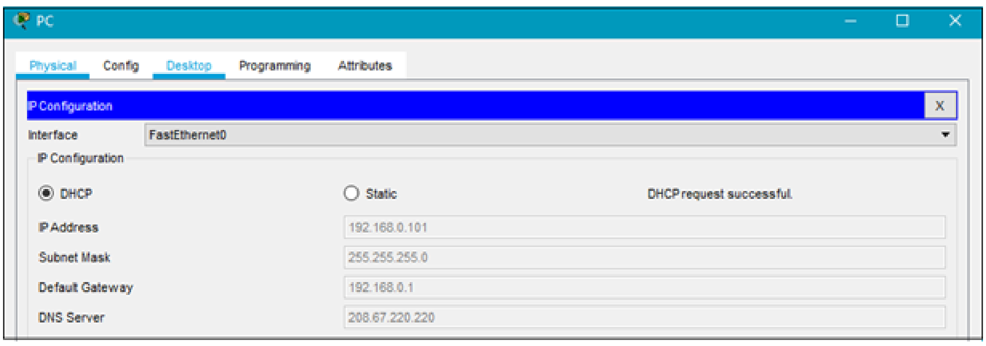


Figure 4.6: Configuring the PC to Use DHCP

> **— Why do this?.** Using DHCP automates IP address assignment, which is common in home or office setups. It saves time and reduces the chance of IP conflicts. You can verify your new IP address by opening the **Command Prompt** and running:
>
> ```
> ipconfig /all
> ```

Once you see a valid `192.168.0.x` address, the PC is ready for network communication.

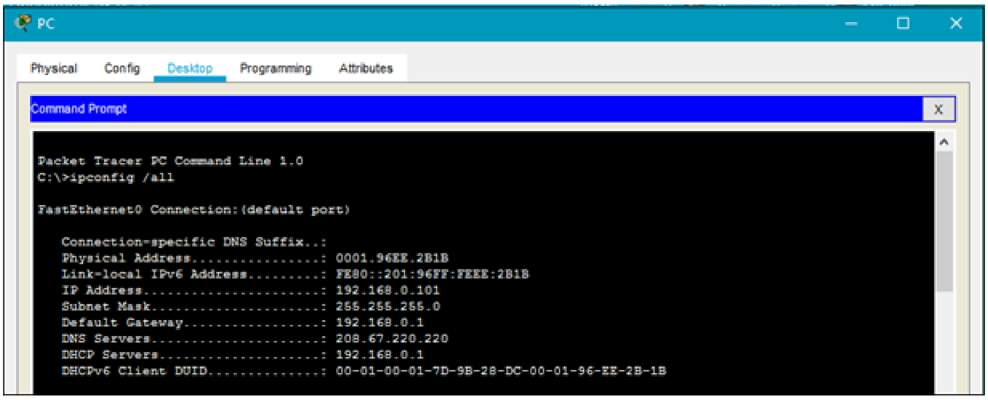


Figure 4.7: Verifying IP Address Assignment Using `ipconfig /all`

6. **Internet Cloud Configuration**

Physical Modules:

- Under the **Physical** tab of the Cloud device, confirm that:
  - `PT-CLOUD-NM-1CX` is installed for coaxial connections.
  - `PT-CLOUD-NM-1CFE` is installed for copper (Ethernet) connections.
- If either is missing, power off the Cloud, insert the module(s), and then power it on again.

Connections and Provider:

- In **Config** → **Cable**, link *Coaxial* to *Ethernet* by selecting each interface and clicking *Add*.
- In **Config** → **Ethernet**, set *Provider Network* to **Cable**.

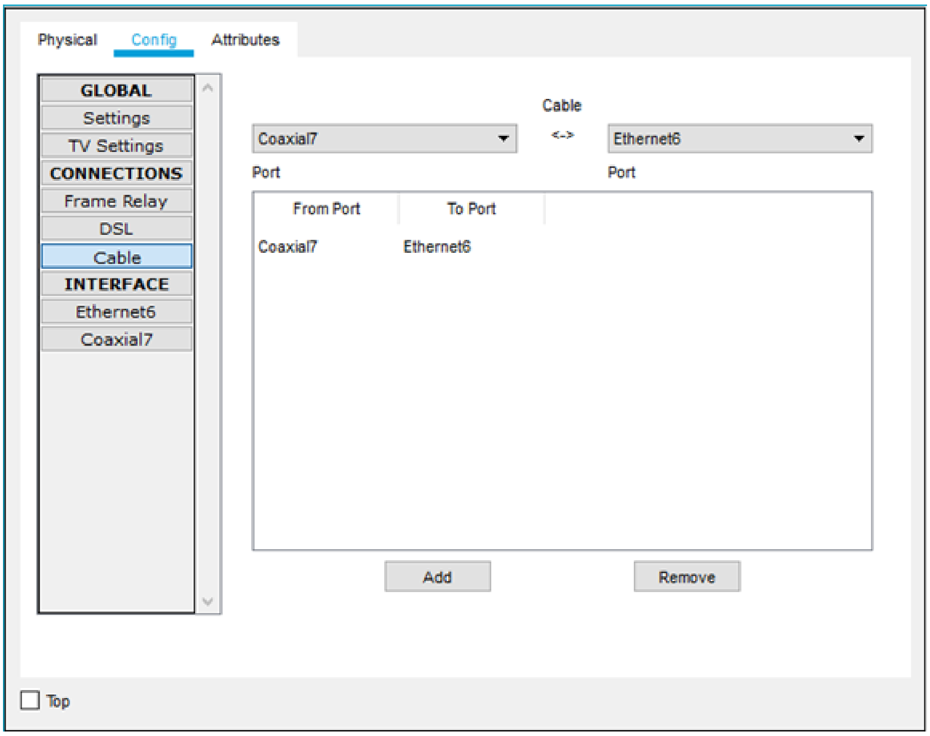


Figure 4.8: (Cloud) Configuring the Internet Cloud Connections

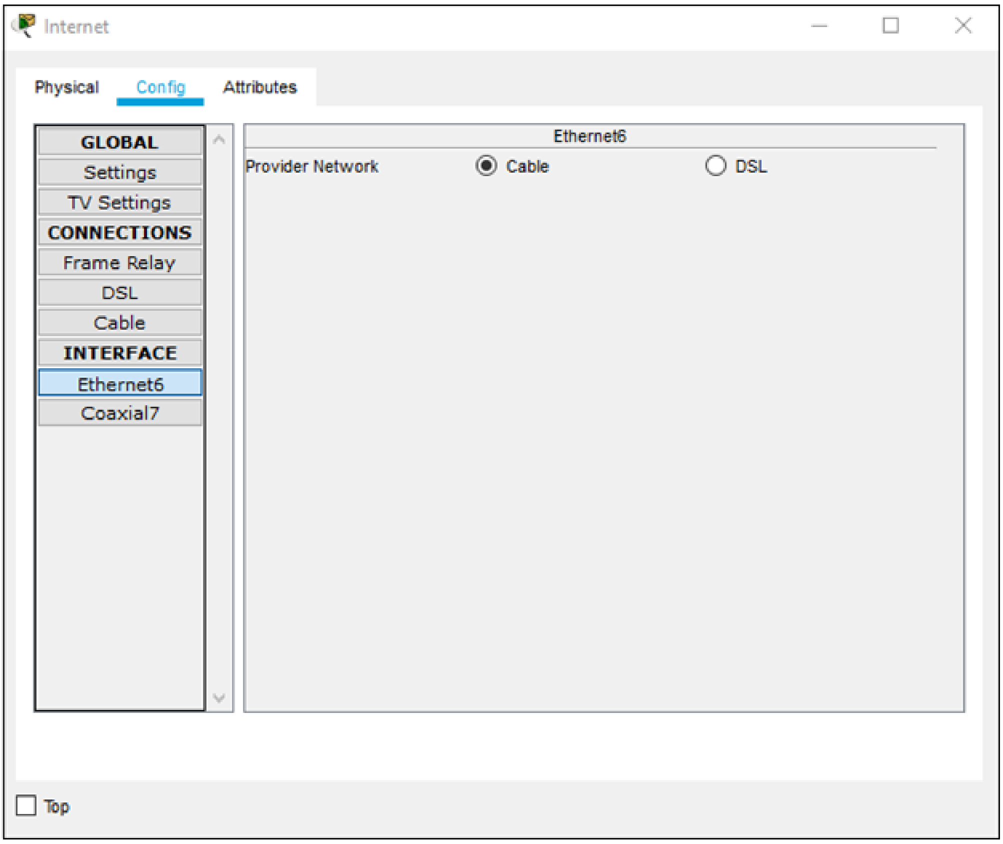


Figure 4.9: (Cloud) Setting the Provider Network Type to Cable

— Why do this?. The Cloud device in Packet Tracer simulates your ISP link. Matching cable types (*coax* for the Cable Modem and *Ethernet* for internal traffic) creates a realistic WAN scenario, showing how a home network might connect to an outside provider.

7. **Cisco.com Server Setup**

DHCP Service:

- Go to **Services** → **DHCP** on the Cisco.com Server, and switch it **On**.
- Create a DHCP pool (e.g., `DHCPpool`) with:
  - **Default Gateway**: `208.67.220.220` (or an address as needed)
  - **DNS Server**: `208.67.220.220`
  - **Starting IP Address**: `208.67.220.1`
  - **Subnet Mask**: `255.255.255.0`
  - **Max Users**: 50
- Click **Add** to confirm the pool.

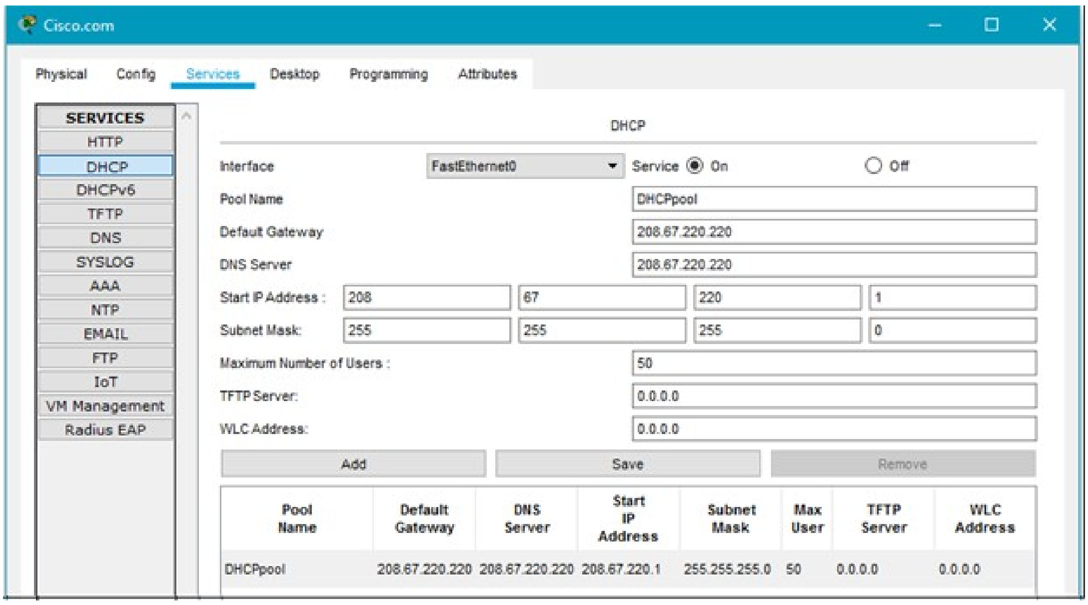


Figure 4.10: (Cisco.com Server) Configuring as a DHCP Server

— Why do this?. While your *Wireless Router* already provides DHCP for your local `192.168.0.x` subnet, the server can also offer DHCP for a separate `208.x.x.x` subnet. This is useful for simulating multi-subnet scenarios or advanced network topologies.

DNS Service:

- Under **Services** → **DNS**, enable it by toggling the switch to **On**.
- Add a record for `Cisco.com` (Type: A) pointing to `208.67.220.220`.

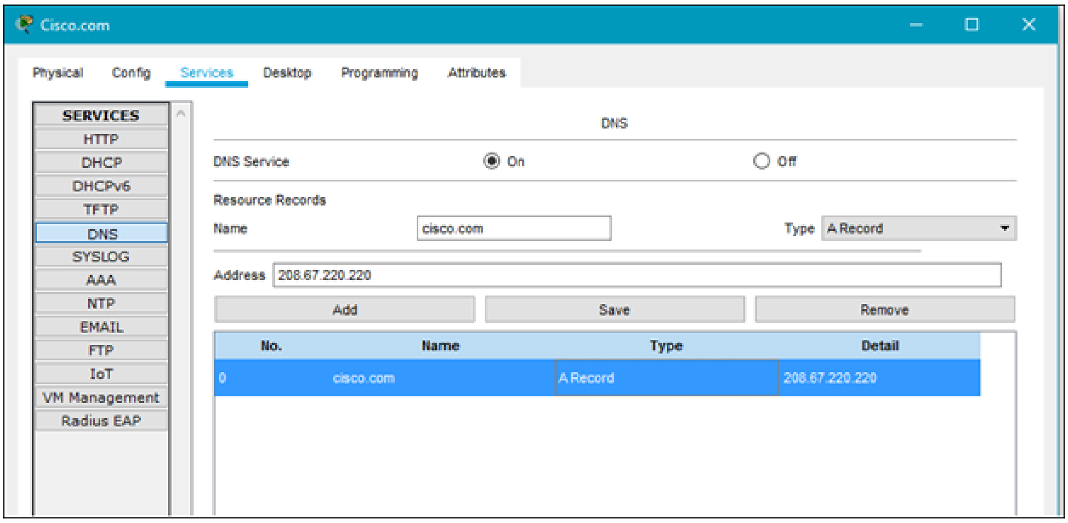


Figure 4.11: (Cisco.com Server) Configuring as a DNS Server

— **Why do this?.** Creating a DNS record for `Cisco.com` directs that hostname to `208.67.220.220`. That way, local devices can simply **ping Cisco.com** to confirm that DNS is resolving correctly and that they can reach the server.

Global Settings:

- In **Config** → **Settings**, switch from `DHCP` to `Static` to ensure a fixed IP configuration.
- Set **Gateway** to `208.67.220.1`, and **DNS Server** to `208.67.220.220`.

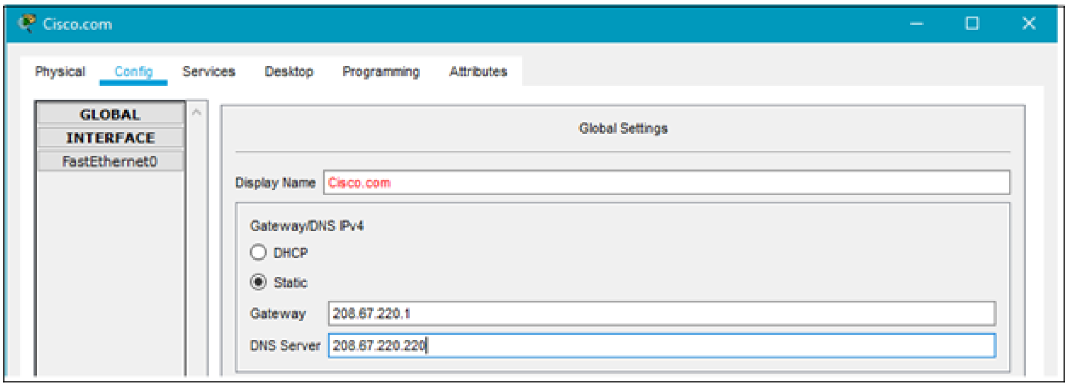


Figure 4.12: (Cisco.com Server) Configuring Global Settings

— **Why do this?.** Servers typically need a **static IP address** so client devices always know where to reach DNS, DHCP, or hosted webpages. A dynamic IP would force clients to constantly adapt to a changing address.

FastEthernet0 Interface:

- Under **Config** → **FastEthernet0**, choose `Static` and assign:
  - IP: `208.67.220.220`
  - Subnet Mask: `255.255.255.0`
- Make sure the port status is **On**.

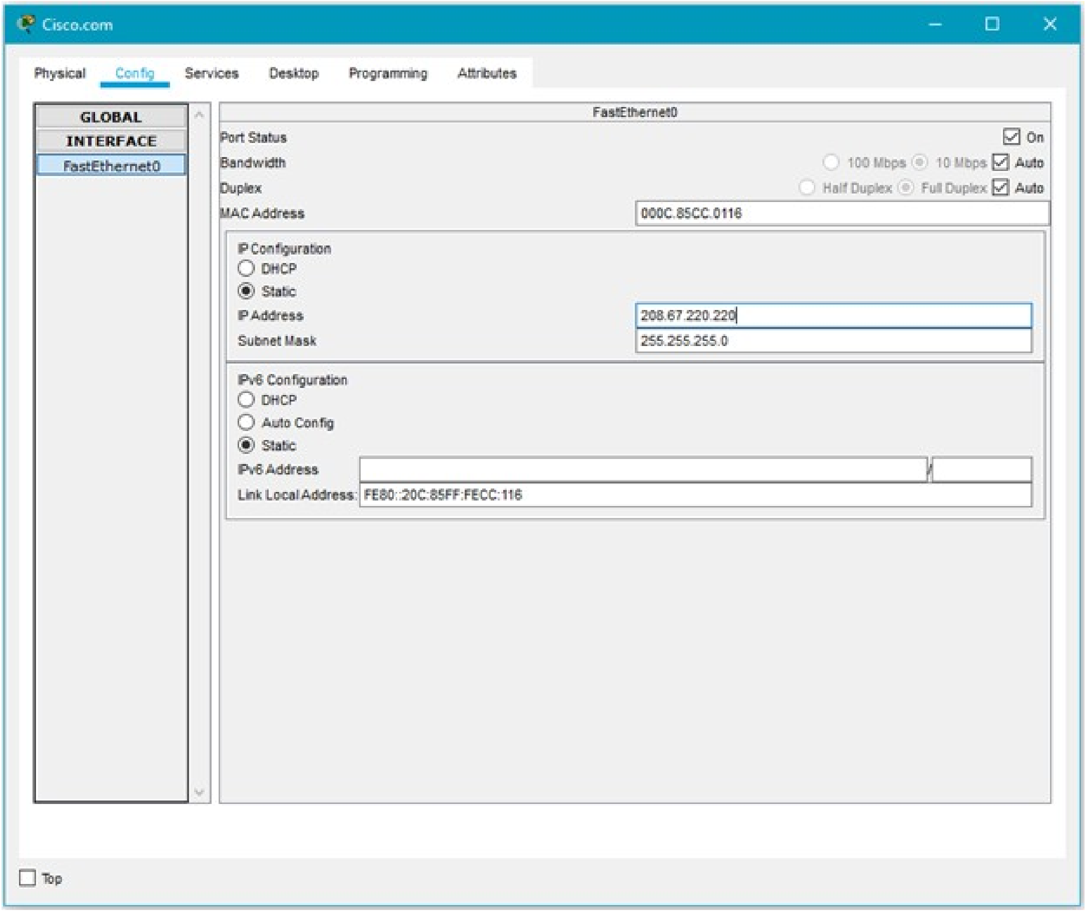


Figure 4.13: (Cisco.com Server) Configuring FastEthernet0 Interface

C. Verify Connectivity

8. **Refresh PC IP and Ping Domain**
   On your PC, open the **Command Prompt** (*Desktop* → *Command Prompt*) and enter the following commands:

```
ipconfig /release
ipconfig /renew
ping Cisco.com
```

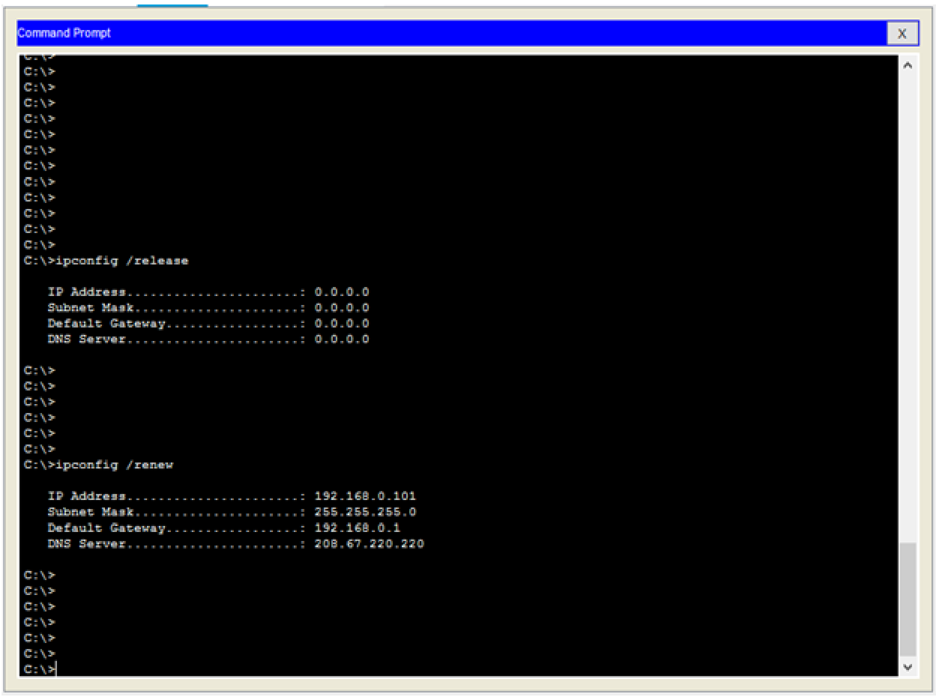


Figure 4.14: (PC) Refreshing the IPv4 Settings

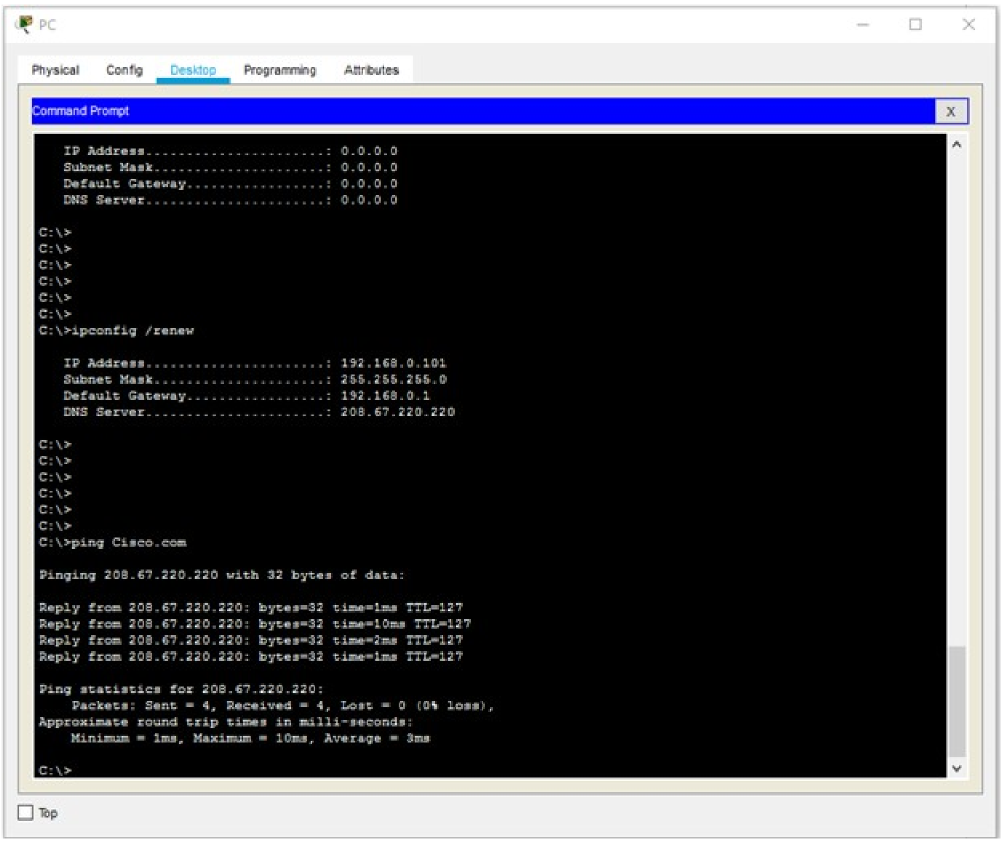


Figure 4.15: (PC) Testing Connectivity to `Cisco.com`

— Why do this?.
- `ipconfig /release` and `ipconfig /renew` ensure that your PC drops any old IP address and obtains a fresh one from the DHCP server (whether it's the router or the `Cisco.com` server).
- `ping Cisco.com` confirms two things simultaneously:
  (a) **IP Connectivity:** Your PC can reach the external network and specifically the `Cisco.com` server's IP address.
  (b) **DNS Resolution:** Your PC can correctly translate the hostname `Cisco.com` into `208.67.220.220`. Successful replies mean both DHCP and DNS are configured properly.
- If you see timeouts or an "unknown host" error, re-check:
  - The **Cisco.com** server's IP and DNS settings.
  - The **Wireless Router** or **Server** DHCP configurations.
  - Physical connectivity (e.g., correct cabling, green link lights).

D. Save and Close Packet Tracer

9. **Save the .pkt File**
   Go to **File** → **Save As**, choose a name like `SimpleNetworkLab4.pkt`, and confirm *Save as type* is `Packet Tracer Activity File` (`.pkt`).

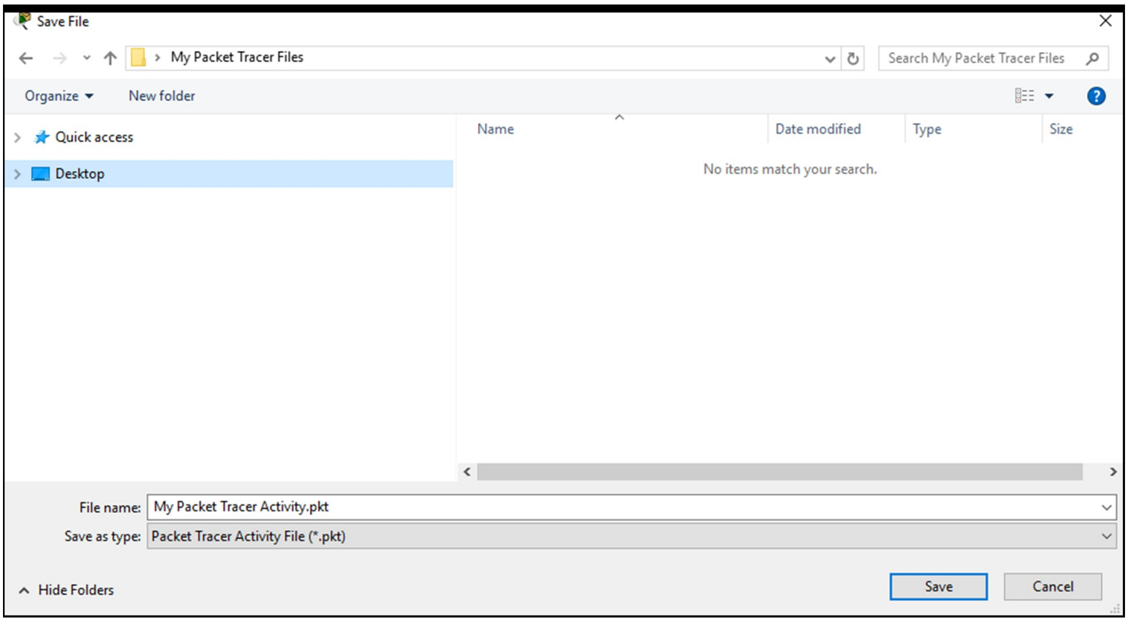


Figure 4.16: Saving the Network Configuration as a Packet Tracer Activity File (`.pkt`)

10. **Close Packet Tracer**
    Click the "X" or select **File** → **Exit** to finalize your session. This ensures your newly created and configured network is safely stored.

You have now created a simple, fully functional network in Cisco Packet Tracer. You've connected devices using both wired and wireless connections, configured DHCP and DNS services on a server, verified connectivity, and saved your project. This foundation prepares you for more advanced networking concepts such as routing, VLANs, or additional services in subsequent labs.

Troubleshooting and Tips

DHCP Failure: If PC/laptop do not get an IP, confirm DHCP is *enabled* on the Wireless Router and ensure no conflicts with the Cisco.com server's DHCP.

Cable Types: Use `Coaxial` from modem to cloud, `Straight-Through` for PC-to-router.

Wireless Issues: If the laptop can't connect, verify the *Wireless WPC300N* module is installed and you selected "HomeNetwork."

DNS Delay: The first `ping Cisco.com` may pause before replying as it resolves the domain name for the first time.

Measuring Success

- Your **PC** obtains a `192.168.0.x` IP via the Wireless Router's DHCP.
- The **Laptop** connects to "HomeNetwork" and also gets a valid IP.
- **Cisco.com Server** replies to `ping Cisco.com`, proving DNS and DHCP are functional.
- All device configs are **retained** after you save/reopen the `.pkt` file.

— Further Exploration

LAB 4.1-Create a Simple Network

- Connect a router, switch, and multiple end devices using correct cables and network hardware.
- Set up network settings on endpoints and confirm they can communicate and access the LAN.

LAB 4.2- Monitor Your Network using a Network Controller

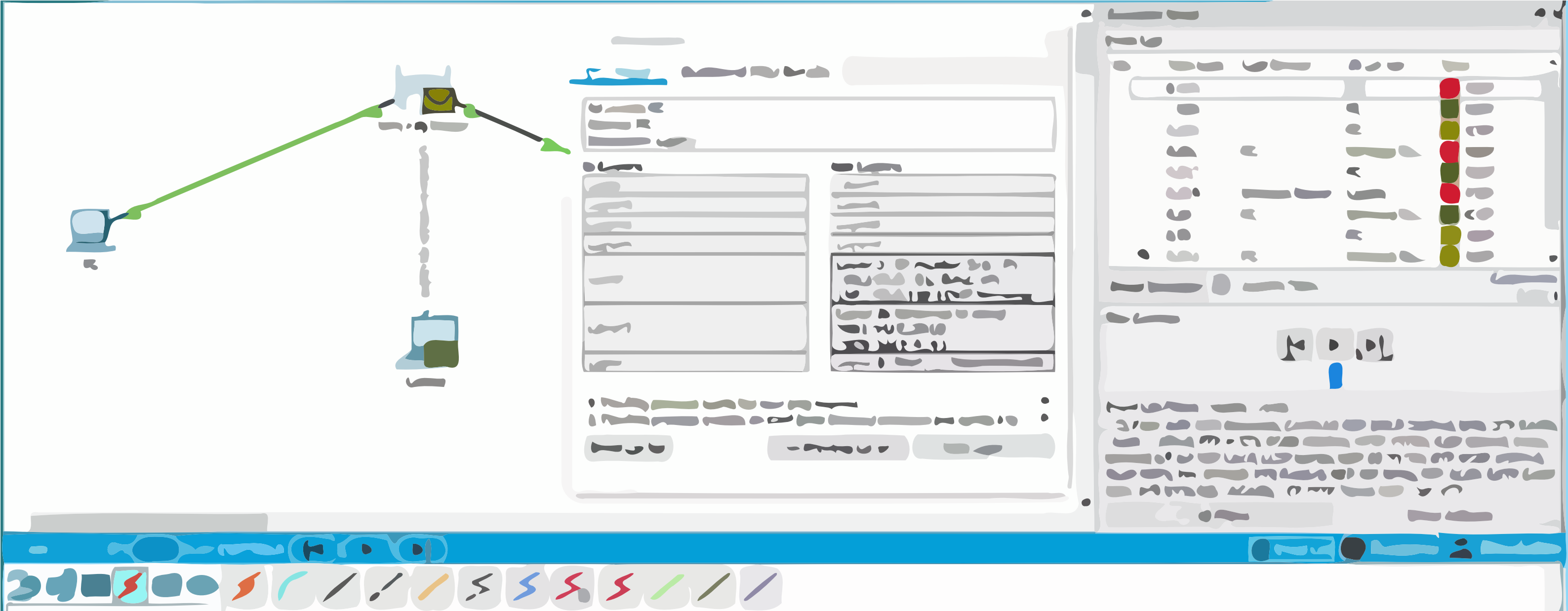
- A network controller lets you manage, monitor, and configure supported devices via GUI and APIs.
- Review the API docs in Packet Tracer's Help for advanced usage.
- Deploy a controller in the existing infrastructure, then use it to track network performance and resources.

LAB 4.3- Manage and Configure Your Network using a Network Controller

- Install and configure a network controller for optimal network administration.
- Let the controller discover and inventory all connected devices.
- Integrate a new device physically and logically; ensure the controller recognizes it.

Summary

You have created a small network with a **wireless router**, **cable modem**, **cloud**, **Cisco.com server**, plus a PC and laptop. You configured DHCP, DNS, and Wi-Fi, then tested it by **pinging Cisco.com**. Finally, you saved the topology as a `.pkt` file. This foundation lets you explore advanced labs on routing, controllers, or security in the future.



5. Explore Network Functionality Using PDUs

Introduction

In this lab, you will learn how to use **Simulation mode** in Cisco Packet Tracer to create and analyze Protocol Data Units (PDUs). You will practice basic and advanced PDU creation to investigate network connectivity, security, and services. You will also examine PDU contents for deeper insight into the OSI model, and finally build more complex PDUs for detailed scenarios.

Objectives

- Investigate network functionality using Packet Tracer's **simulation mode** by creating and capturing PDUs to evaluate connectivity and security.
- Create **simple PDUs** to replicate network functionality for troubleshooting and testing.
- View the contents of PDUs to understand **OSI layers** and data flow mechanisms.
- Build **complex PDUs** with advanced settings to simulate and analyze detailed network scenarios.

Lab Plan

A. Create and Capture PDUs in Simulation Mode
B. Create a Simple PDU
C. View the Contents of PDUs
D. Create a Complex PDU

Background

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.

Resources — **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.

Resources — **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.

Resources — **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

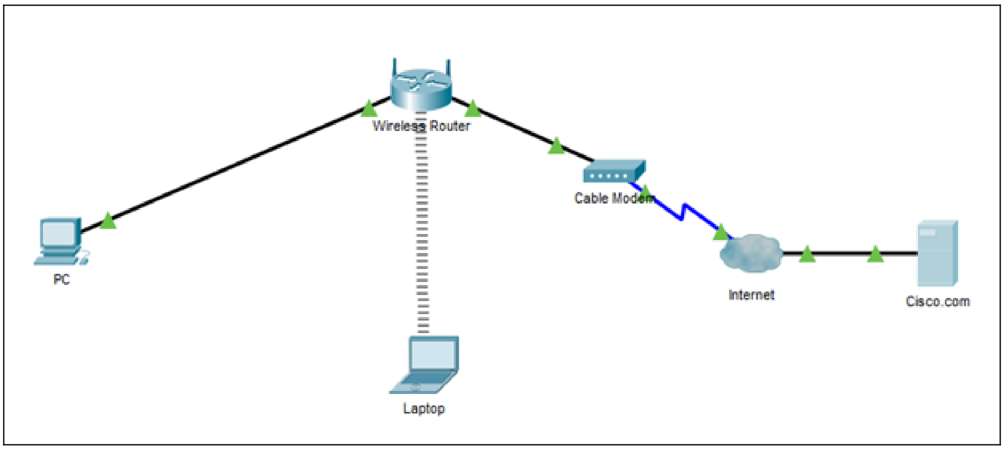


Figure 5.1: Network Topology in Cisco Packet Tracer

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		

A. Create and Capture PDUs in Simulation Mode

This section shows you how to use Simulation Mode in Cisco Packet Tracer to slow down and analyze the flow of network traffic in detail. By creating and capturing PDUs (Protocol Data Units), you can observe exactly how data moves through your network, identify potential issues, and gain deeper insight into various protocols.

1. **Why Simulation Mode?**
   By default, Packet Tracer runs in **Realtime** mode, where data continuously flows through the network without interruption. In **Simulation** mode, you can slow or freeze time and inspect PDUs *packet by packet*. This is crucial for understanding protocols such as ICMP, DNS, and HTTP at a deeper level.

   > **— Why do this?.** Simulation mode provides a step-by-step view of network traffic. This granular perspective is invaluable for troubleshooting or learning how different OSI layers (from Layer 2 up to Layer 7) encapsulate data. You can watch each packet move hop-by-hop, see ARP requests and responses, and explore how services like DNS or HTTP function on a real-time scale.

2. **Open the `.pka` File from Lab 4**
   Locate your file from Lab 4 (e.g., `CreateASimpleNetworkLab4.pka`) and open it in Packet Tracer. In the bottom-right corner of the interface, click the **Simulation** tab to switch from Realtime mode to Simulation mode (see Figure 5.2).

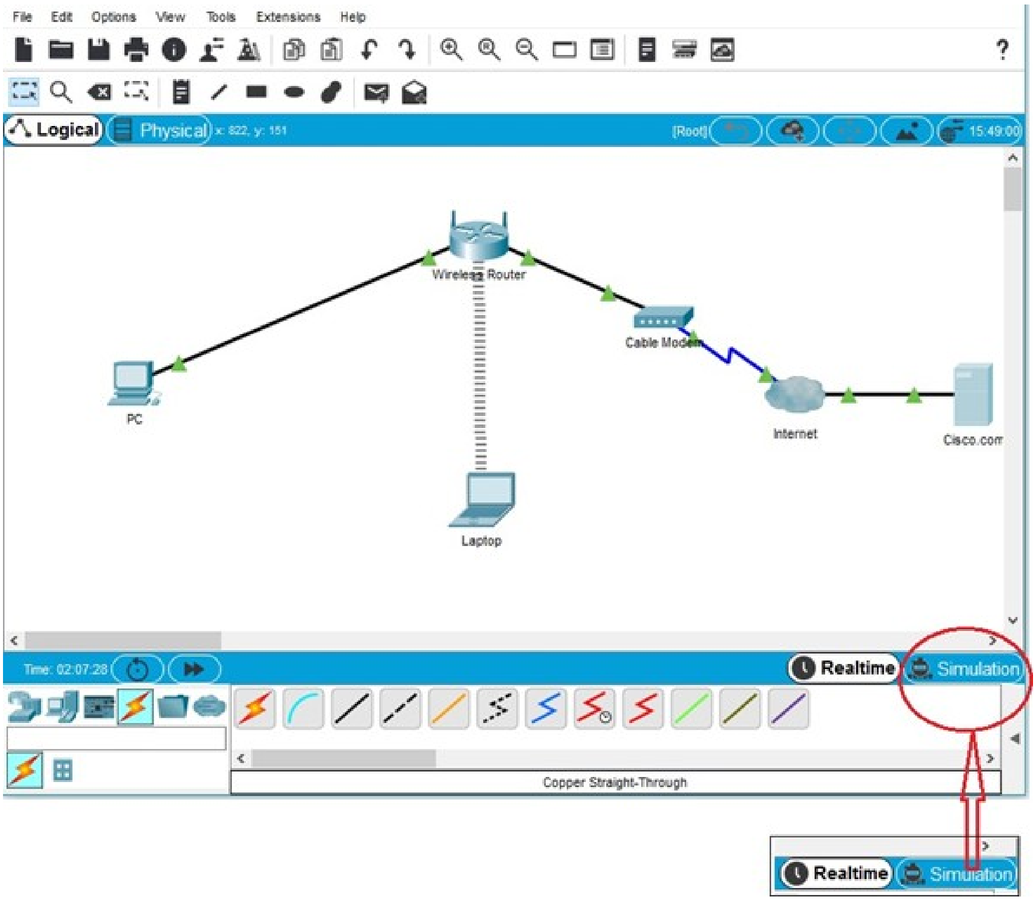


Figure 5.2: Switching to Simulation Mode in Cisco Packet Tracer

> **— Why do this?.** Switching to Simulation mode halts normal data flow, enabling you to capture and analyze PDUs in a controlled environment. This confirms that your Lab 4 network (or any existing setup) behaves as expected. Moreover, it allows you to precisely follow the path of a packet to identify issues such as misconfiguration, routing loops, or DNS failures.

Tips for Using Simulation Mode:

Adjusting Simulation Speed: In the Simulation panel, you can *Capture/Forward* packets one step at a time or choose `Auto Capture/Play` to proceed automatically. Use the *Play Speed* slider to control how fast the packets move.

Filtering Traffic: If the Event List becomes too crowded, click **Edit Filters** to show or hide specific protocol traffic (e.g., only ICMP or DNS). This helps you focus on the protocols you're currently investigating.

Clearing PDUs: Use the **Delete** button in the Event List to remove unnecessary or old PDU entries, keeping your workspace organized while you capture new traffic. ■

B. Create a Simple PDU

In this step, you will generate a simple ICMP ping to verify connectivity between two devices—such as a PC and a laptop—in Simulation mode. This allows you to follow the packet's journey hop-by-hop.

3. **Send a Ping from PC to Laptop**
   Locate and click the **Add Simple PDU** icon (it looks like a closed envelope) on the top toolbar. Then:
   - Click on the **PC** (the source of the ping).
   - Click on the **Laptop** (the destination).

   Refer to Figure 5.3 to see an example of setting up a Simple PDU in Packet Tracer.

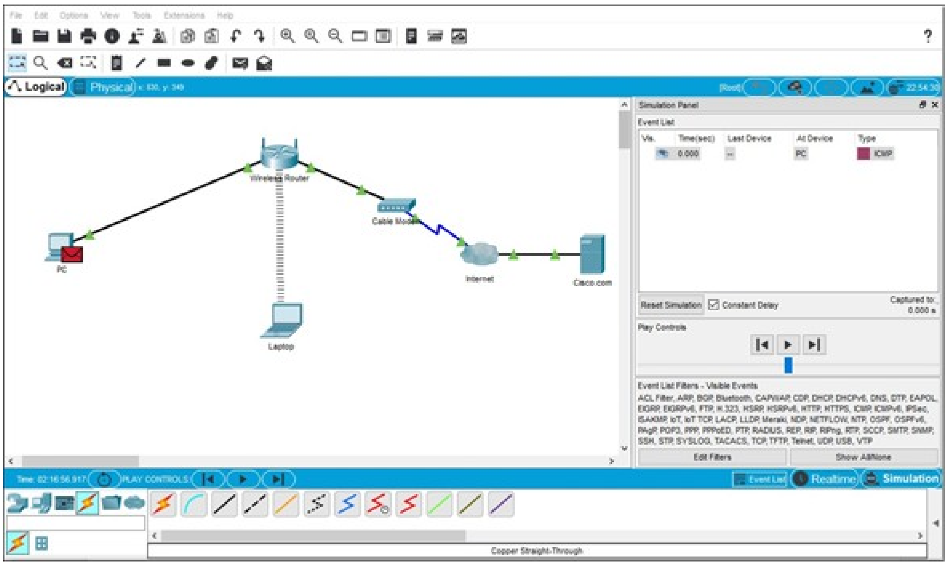
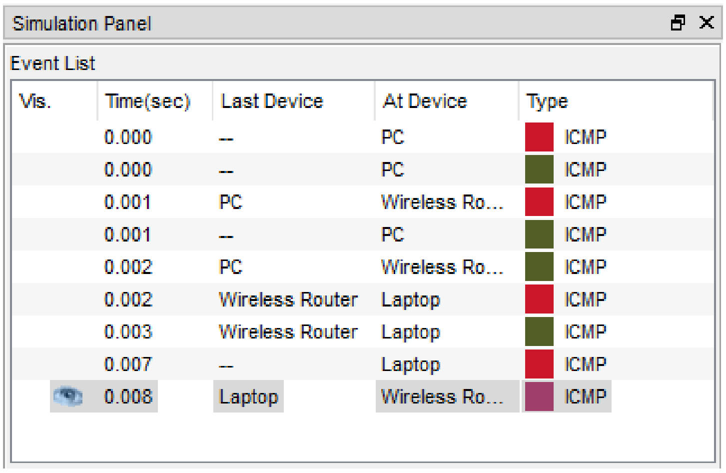


Figure 5.3: Creating and Sending a Simple PDU

4. **Monitor Traffic in Simulation**
   After creating the Simple PDU, open the Event Simulation panel by clicking the gray arrow at the bottom-right corner of the interface. Use the **Capture/Forward** button repeatedly to advance the simulation step by step:
   - Observe how the *ICMP* ping packet travels from the PC to the laptop.
   - Watch for the return packet from the laptop back to the PC.

   Figure 5.4 shows an example of how the Simulation Panel displays each step.



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: Observing Network Traffic in the Simulation Panel

— Why do this?. A **Simple PDU** (essentially a *ping*) is the quickest way to verify basic connectivity. As you *Capture/Forward* through each simulation step, you can confirm whether the devices successfully reach each other and observe how *ICMP* packets move through your network. This provides a clear demonstration of the OSI model in action.

Tips for Creating Simple PDUs:

Resetting the Simulation: If you need to start over, you can delete the PDU in the Event List and recreate it. This clears any existing simulation events and gives you a fresh view.

Multiple Tests: You can create multiple Simple PDUs (pings) between different devices to check various paths in your network.

Filtering Traffic: If you only want to view *ICMP* traffic, use the **Edit Filters** option in Simulation mode to hide other protocols and reduce clutter. ■

5. **Examine OSI Model Details**
   After sending a ping, locate the **Type** column in the Event List. Click the green square next to your PDU to open the **PDU Information** window (Figure 5.5). You can switch to the **OSI Model** tab to observe how data is processed at each layer (Figure 5.6). For a more granular view, select **Outbound PDU Details** to see the specific headers (Ethernet, IP, ICMP) that encapsulate your data (Figure 5.7).

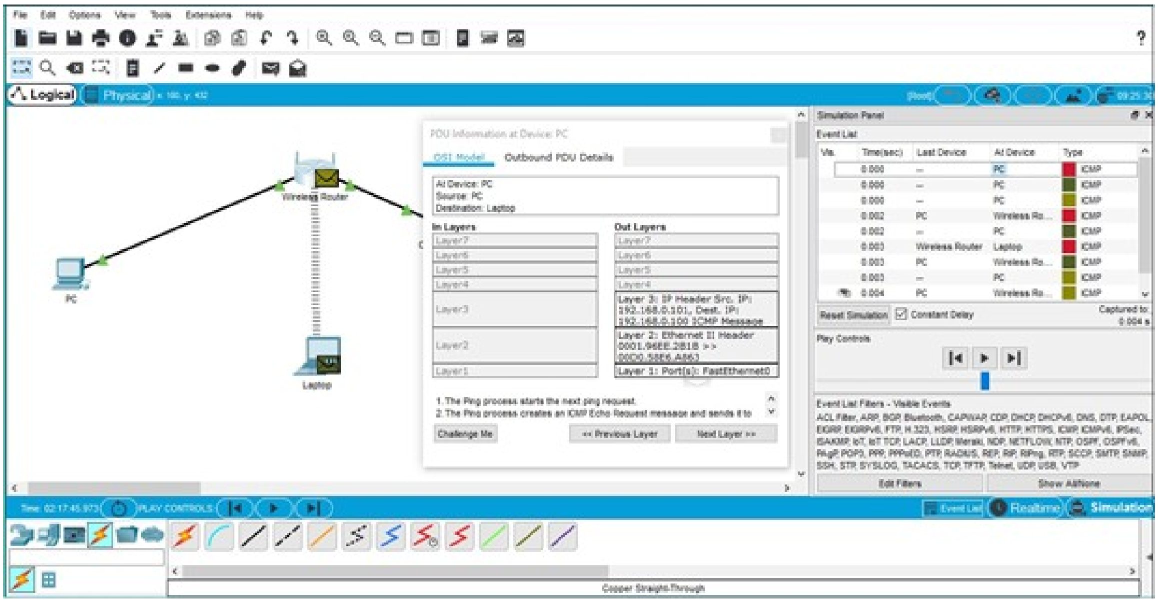


Figure 5.5: Viewing PDU Information in Cisco Packet Tracer

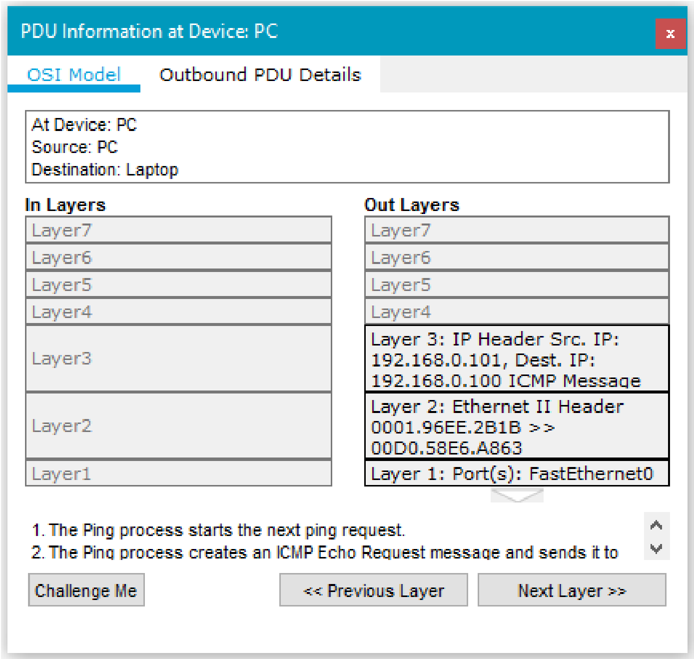


Figure 5.6: PDU Details in the OSI Model Tab

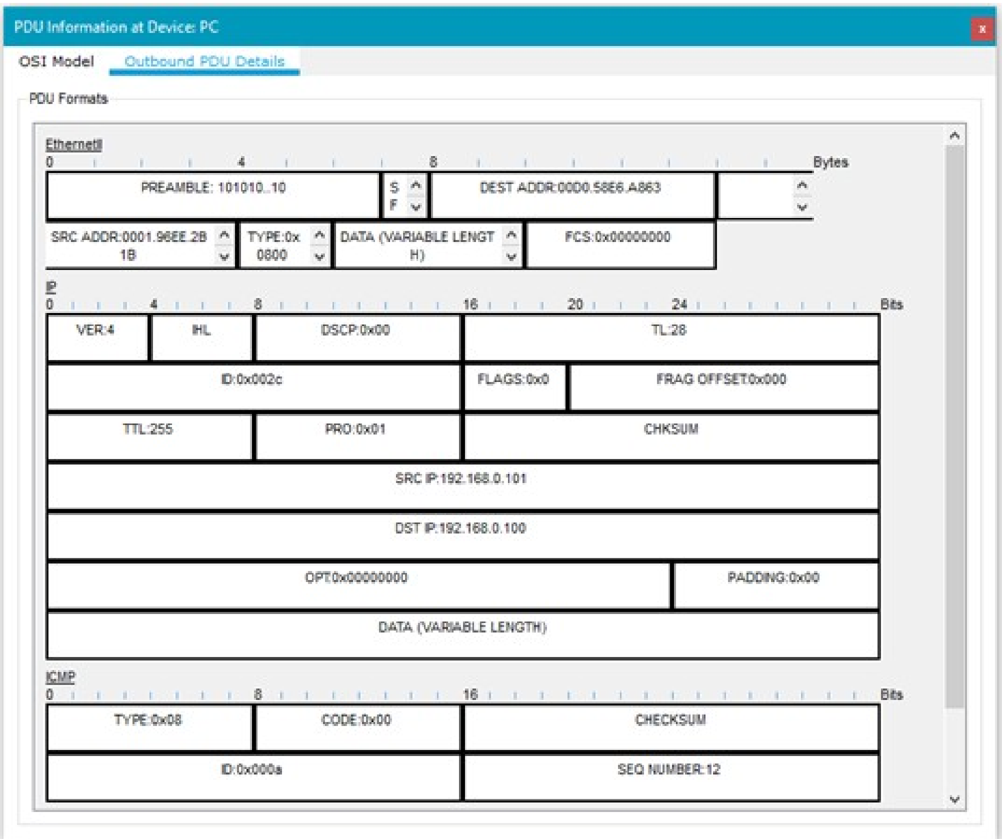


Figure 5.7: Outbound PDU Details (Ethernet/IP/ICMP Headers)

— Why do this?. Observing the OSI layers in each PDU shows you exactly how data is encapsulated and de-encapsulated. For example, an ICMP echo request (ping) is carried inside an IP packet, which in turn is carried inside an Ethernet frame at Layer 2. This deep-dive makes it easier to diagnose misconfigurations, dropped packets, or any unusual behaviors at specific layers in the OSI model.

6. **Remove the Simple PDU (Optional)**
   If you need a clean slate for a new test or want to reset your simulation view, go to the *Event Simulation* pane. Click **Delete** on the existing PDU to clear it from the Event List. You can then create new PDUs or run additional tests without clutter.

Further Analysis Tips:

Inbound vs. Outbound Details: You can also look at *Inbound PDU Details* to see how data is processed upon arrival at a device and *Outbound PDU Details* to see how data is prepared for transmission.

Layer-by-Layer Troubleshooting: If something goes wrong, the OSI Model tab helps you pinpoint if there's an addressing issue (Layer 3), a framing problem (Layer 2), or a missing service configuration (Layers 5–7).

Multiple PDUs at Once: When investigating more complex networks, you can open multiple PDUs simultaneously to compare how different packets travel. ■

D. Create a Complex PDU

In some scenarios, you might want to send repeated pings or more advanced test packets to observe continuous traffic flow or simulate higher volumes of data transfer. Packet Tracer's **Complex PDU** feature allows you to do exactly that.

7. **Send Periodic Pings**
   Click the **Add Complex PDU** icon (it looks like an open envelope, usually found next to the Simple PDU icon). Then:
   (a) Select the **PC** (source device) first.
   (b) Select the **Laptop** (destination device) second.
   (c) A *Create Complex PDU* window appears. Configure the following fields:
      - **Source IP**: `192.168.0.101` (example)
      - **Destination IP**: `192.168.0.100` (example)
      - **Periodic**: Check this box to enable repeated pings.
      - **Interval**: Set it to 5 seconds (or another desired frequency).

— Why do this?. Setting *Periodic* pings at 5-second intervals allows you to see a constant flow of ICMP packets in Simulation Mode. This is particularly helpful for testing how your network behaves under repeated requests, detecting if any device goes offline, or assessing how the network handles multiple simultaneous pings.

8. **Capture/Forward or Auto Capture/Play**
   From the *Event Simulation* panel, you can:
   - Use **Capture/Forward** to manually step through each ping event.
   - Click **Auto Capture/Play** to watch the repeated pings flow automatically in the Event List. Press the button again if you want to pause.

   If you need to remove the complex PDU and start fresh, select the PDU in the *Event Simulation* pane and click **Delete**.

Working With Complex PDUs:

Adjust Intervals: If you want a faster test, reduce the interval to, say, 2 seconds. If you want a slower, less intrusive test, increase the interval (10–15 seconds).

Multiple Complex PDUs: You can create more than one Complex PDU for different source–destination pairs to observe heavier traffic patterns and potential collision domains in larger networks.

Filtering Traffic: If you only want to see the ICMP traffic generated by your Complex PDUs, you can use the **Edit Filters** option in Simulation Mode to hide other protocols (like ARP, DNS, etc.).

Analyzing Over Time: Let the simulation run for a while. If any pings begin failing, you've likely discovered a misconfiguration, cable fault, or device shutdown in your network.

Troubleshooting and Tips

Simulation Speed: If traffic updates too quickly, use **Capture/Forward** to manually step through.

Deleting PDUs: Clear out old PDUs if the Event List grows too large, preventing confusion.

OSI vs. Inbound/Outbound Details: The OSI Model tab is a simplified overview, while Inbound/Outbound PDU Details show raw headers. Both views are helpful.

Periodic PDU Overload: Setting too many repeated pings or short intervals can flood the simulation. Manage intervals wisely.

Measuring Success

- You observe **ping** traffic in Simulation mode, confirming connectivity from Lab 4's network.
- You inspect **PDU details** (Layers 2–3, ICMP) for correct encapsulation.
- You create a **Complex PDU** that sends repeated pings, visible in the Event Simulation list.

— Further Exploration

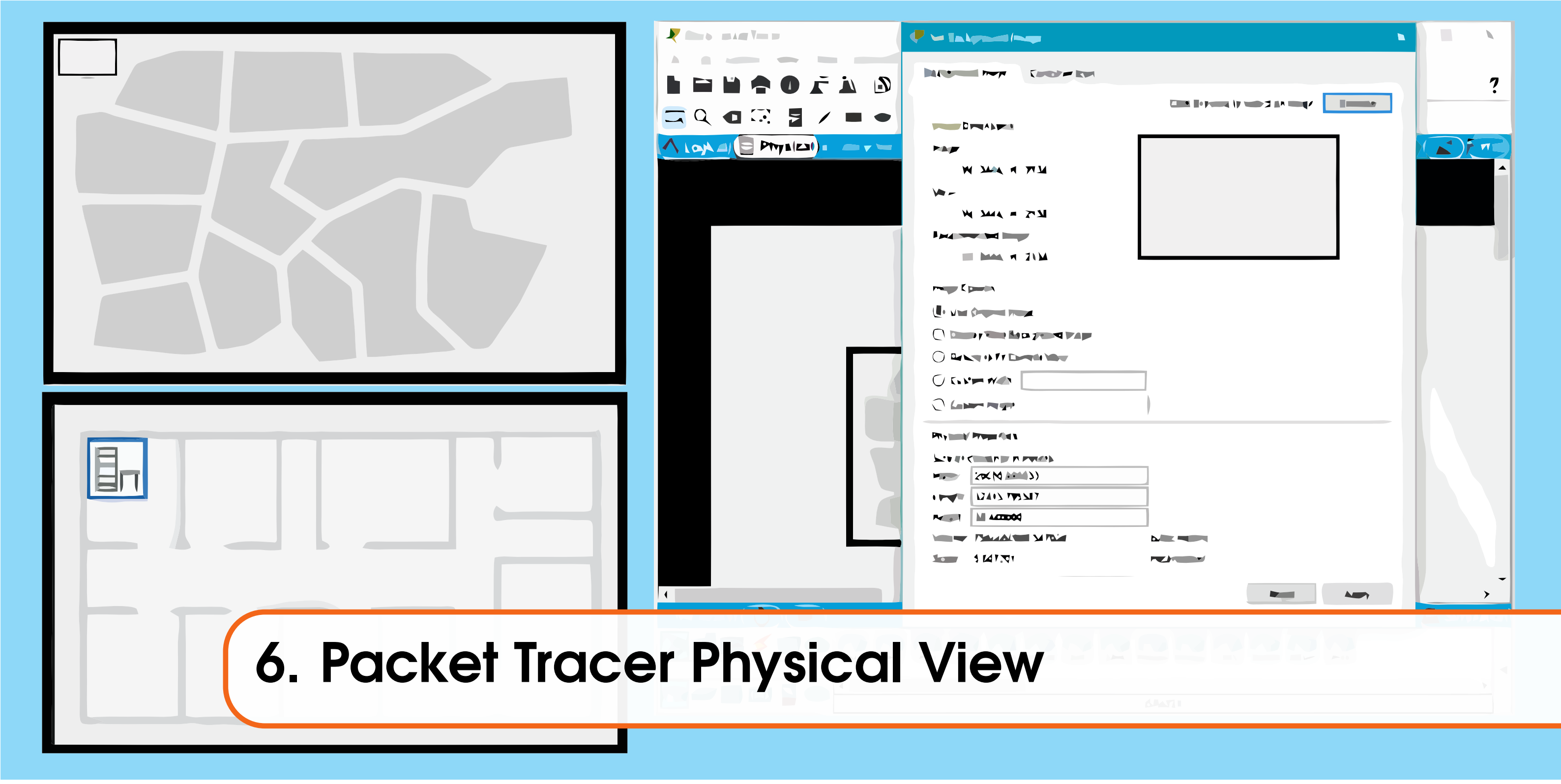
LAB 5.1-PDUs to Explore Network Functionality

In this Packet Tracer activity, you will use Simulation mode to create PDUs that explore network functionality. Note: Simulation mode does not work in Physical mode, so Physical mode is locked.

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

Summary

In this lab, you have **created and analyzed PDUs** in Packet Tracer's Simulation mode—from basic ICMP pings to advanced periodic ones. You also examined OSI model encapsulation and used the Event List for diagnosis. Building on your network from Lab 4, you now have deeper packet-level insight to help with troubleshooting and future network design tasks.



6. Packet Tracer Physical View

Introduction

In this lab, you will learn how to use the **Physical view** in Cisco Packet Tracer to enhance your understanding of network topologies in a real-world context. You will add backgrounds (such as maps and city images), create containers for cities and buildings, and place wiring closets to hold network devices. Additionally, you will explore file types (`.pkt`, `.pkz`, `.pka`) and see how Packet Tracer can be used for assessments.

Objectives

- **Explore** the Physical view in Packet Tracer to better visualize network layouts within a physical environment.
- **Navigate and customize** the physical workspace by adding cities, corporate offices, and wiring closets.
- **Simulate** wireless coverage areas based on device placement, aiding in network design and visualization.
- **Understand** different Packet Tracer file and assessment types (`.pkt`, `.pkz`, `.pka`) and their uses in networking education.

Lab Plan

A. **Open the Physical View & Add a Background**
B. **Edit Containers & Add Devices to a Wiring Closet**
C. **Experiment with Additional Designs**

Background

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.

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.

Resources — **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.

Resources — **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.

Resources — **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.

Resources — **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.

Resources — **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.

A. Open the Physical View & Add a Background

In this section, you will switch from the default **Logical** view to the **Physical** view in Packet Tracer. By adding a custom background image (such as a map), you can visualize your network layout more realistically and plan device placement, cable lengths, and wireless coverage with greater accuracy.

1. **Launch Packet Tracer and Check Default View**
   When you start Cisco Packet Tracer, it generally opens the **Logical** view by default, as illustrated in Figure 6.1. To access the **Physical** view, locate and click the **Physical** button near the top-left portion of the interface (Figures 6.2 and 6.3). By default, you should see *Intercity* as the top-level container in the Physical view.

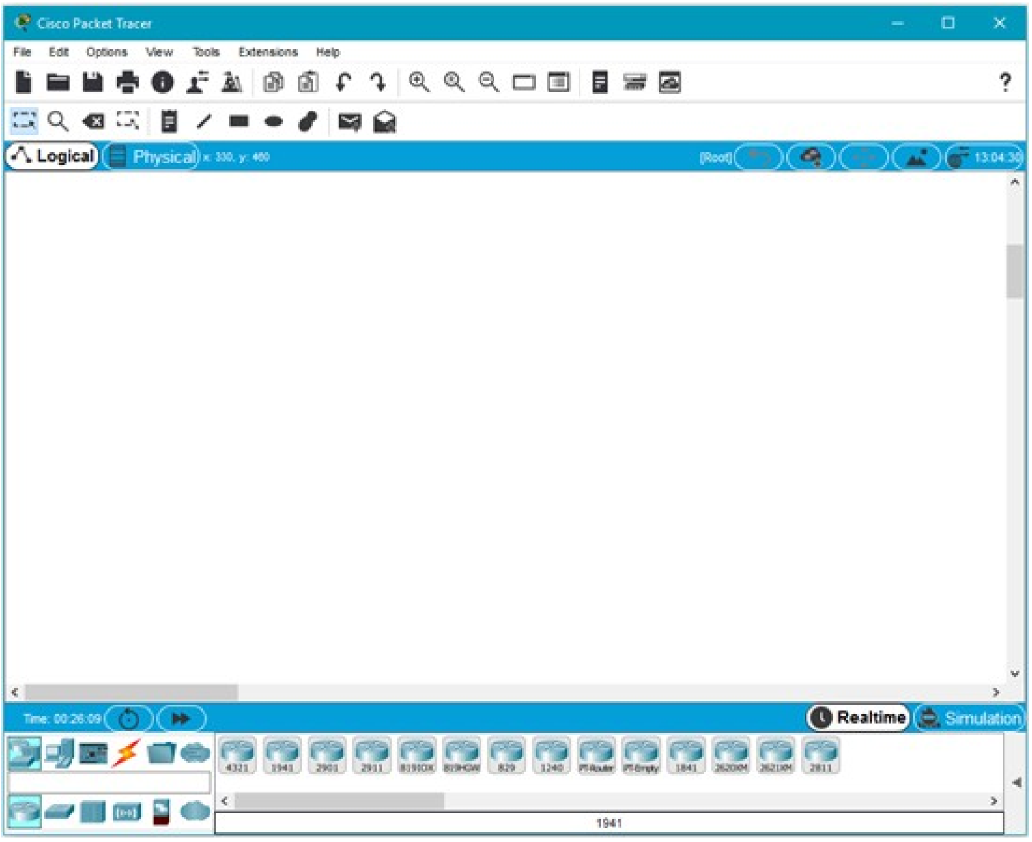


Figure 6.1: Default Logical View upon Launching Packet Tracer

Figure 6.2: Switching from Logical to Physical View

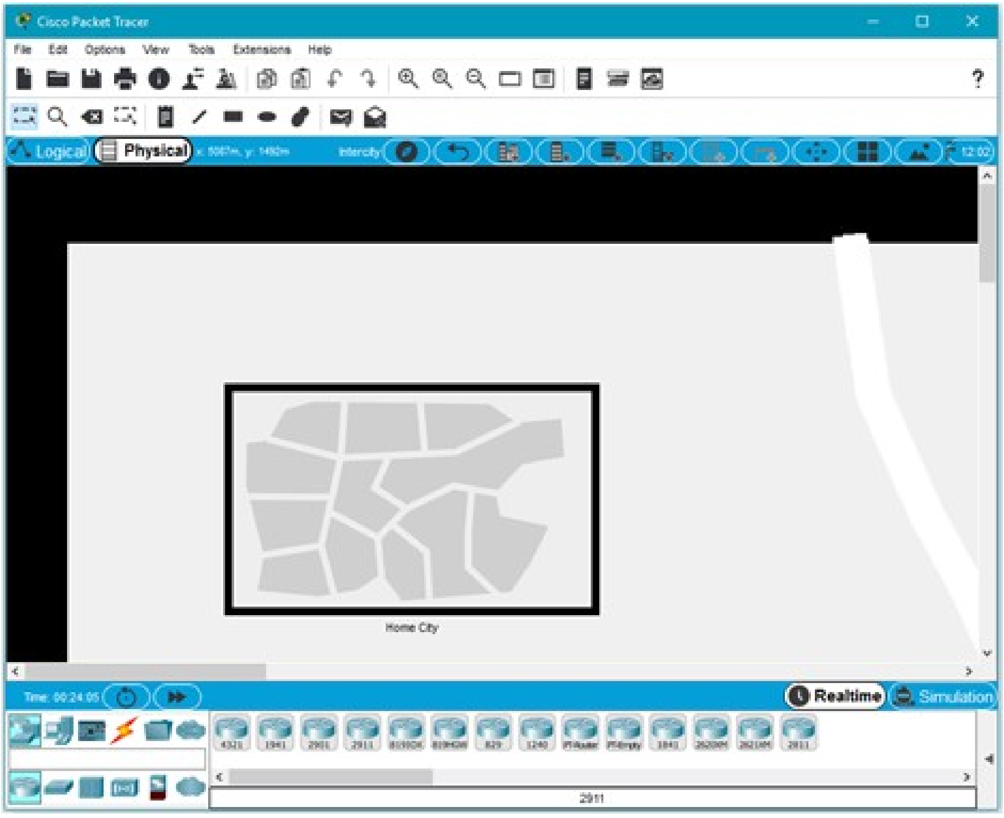


Figure 6.3: Physical View in Cisco Packet Tracer (Intercity Level)

Why Use Physical View?
Realistic Context: The Physical view allows you to simulate actual locations like cities, buildings, and wiring closets, giving you a more concrete sense of device placement and distance.
Advanced Planning: When you design a larger network, especially one involving multiple floors or rooms, the Physical view helps you plan cable routes or wireless coverage more efficiently.
Container Hierarchy: The top-level *Intercity* container can include *cities*, which in turn contain *buildings*, and then *wiring closets*, mirroring real-world infrastructure.

2. **Download and Apply a Background Image**
Navigate to a royalty-free image site like `https://pixabay.com` to find a suitable image (for instance, a world map or property outline). Save the image to a known location on your computer. Then, with the **Intercity** container active in the Physical view, do the following:
   - Click the **Set Background** button at the top.
   - In the dialog box, click **Browse** to locate and select your downloaded image.
   - Click **Apply** to set this image as your Physical view background.

   Figures 6.4, 6.5, and 6.6 illustrate this process.

Figure 6.4: Applying a Physical View Background Image

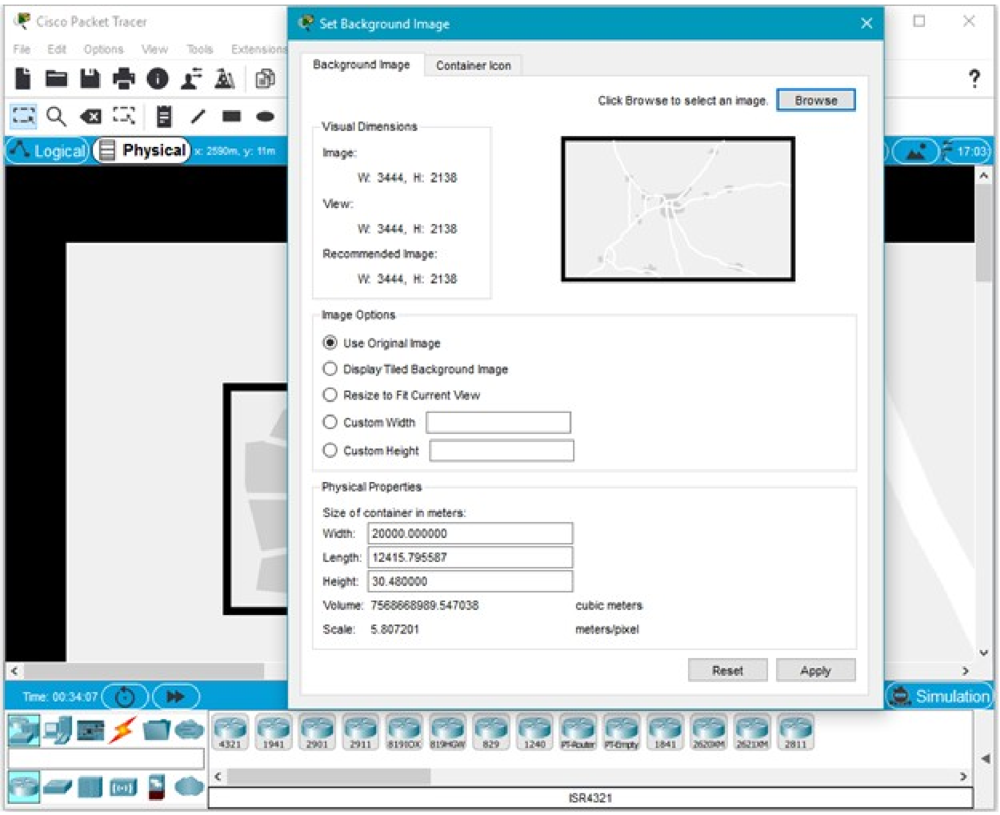


Figure 6.5: Setting a Background Image in the Physical View

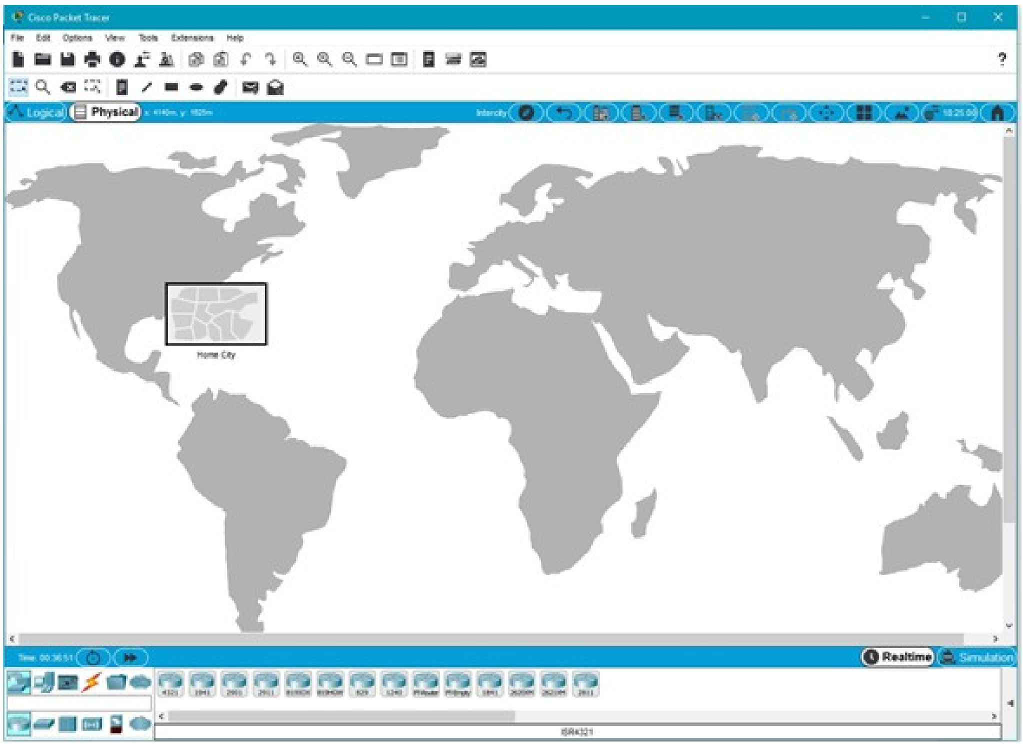


Figure 6.6: Physical View with the New Map Background

Additional Pointers for Background Images:
Choose Clear Images: Pick a background image with high contrast and clarity, so your network devices, city blocks, or building outlines remain visible over it.
Aligning Containers: Once set, you can move or resize containers (like *cities* or *buildings*) so they align well with your new background image.
File Formats: Packet Tracer supports common image formats (like JPEG or PNG). Make sure your downloaded file is saved in a compatible format.
Size Considerations: A very large image can slow down the interface. If your map is huge, consider resizing it before importing. ■

B. Edit Containers & Add Devices to a Wiring Closet

In this section, you will organize your network containers (cities, buildings, wiring closets) and populate them with devices. This helps mirror a realistic environment where physical locations and device racks are accurately represented.

3. **Relocate and Customize a City Container**
   In the **Intercity** view, look for the **Home City** container. Click and drag it to the desired spot on your newly placed background (see Figure 6.7). If you want to give this city its own custom backdrop, open the container and repeat the *Set Background* process. You may also rename "Home City" to something more descriptive like "Atlanta" (Figures 6.8–6.12).

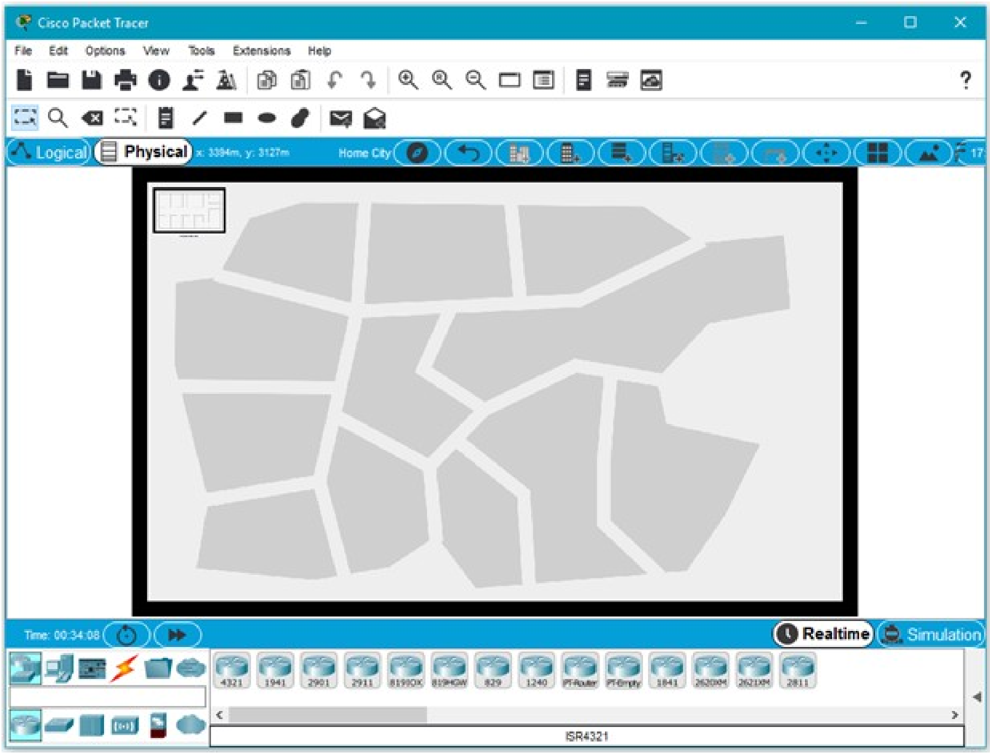


Figure 6.7: Editing and Moving the Home City Container

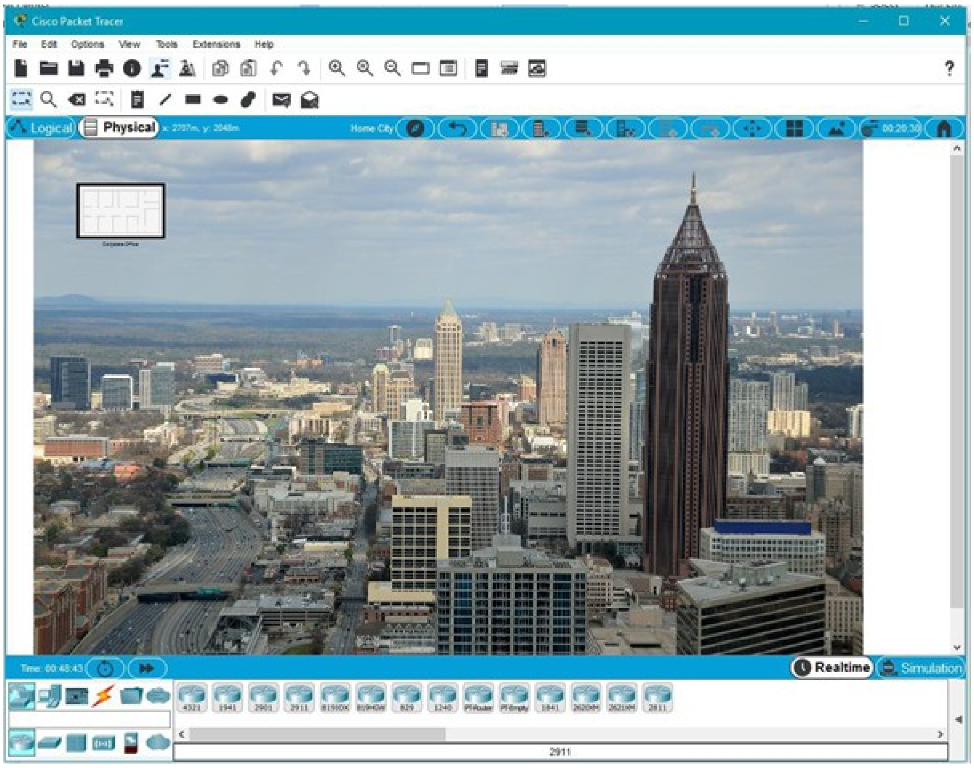


Figure 6.8: Applying a City Background to Home City

Figure 6.9: Physical View Tool Bar Showing "Back" and the New City Background

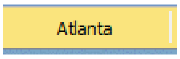


Figure 6.10: Renaming the Home City to "Atlanta"

Figure 6.11: New Atlanta Container in the Physical Toolbar

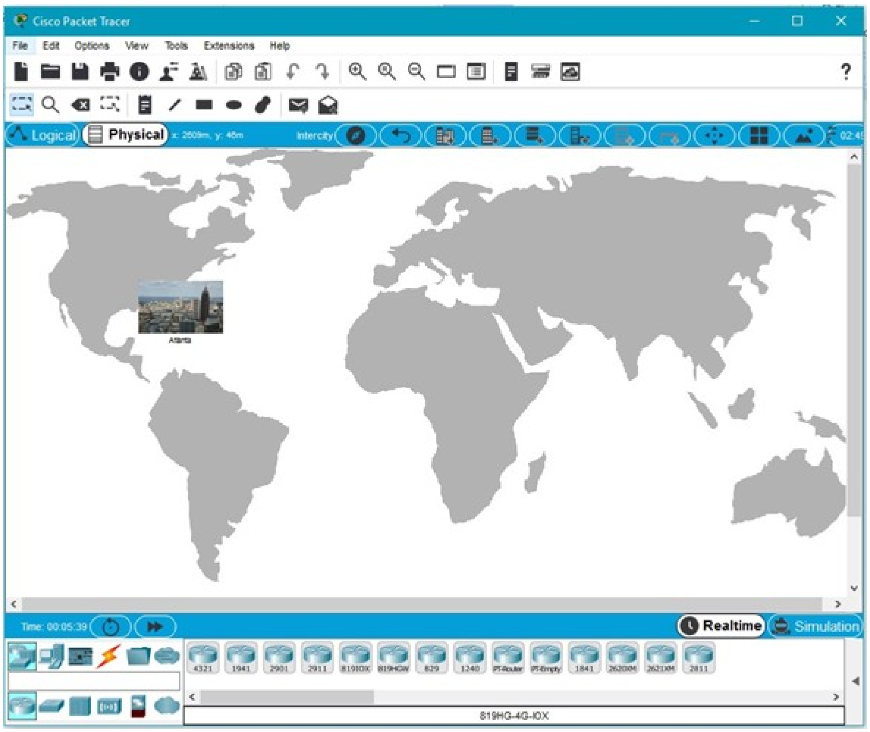


Figure 6.12: Returning to the Home City View

Container Hierarchy:
Why Rename? Using real-world city names (e.g., "Atlanta," "New York") makes your topology more intuitive and easier to present or document.
Nested Containers: Remember that *Intercity* sits at the top level, which can contain multiple *Cities*. Each *City* can hold multiple *Buildings*, and each Building can have one or more *Wiring Closets*.
Positioning and Sizing: You can drag containers around your background and resize them if you need to represent different geographic areas or building sizes.

4. **Access Corporate Office and the Main Wiring Closet**
   After renaming and relocating your city container (e.g., "Atlanta"), you should see a **Corporate Office** container inside it (Figure 6.13). Click the *Corporate Office* to open and view its background (Figure 6.14). Inside the office, look for the **Main Wiring Closet** container. Open it, and you should see an empty workspace (Figure 6.15).

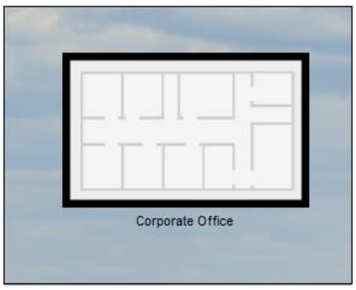


Figure 6.13: Corporate Office Container on the Home City Background

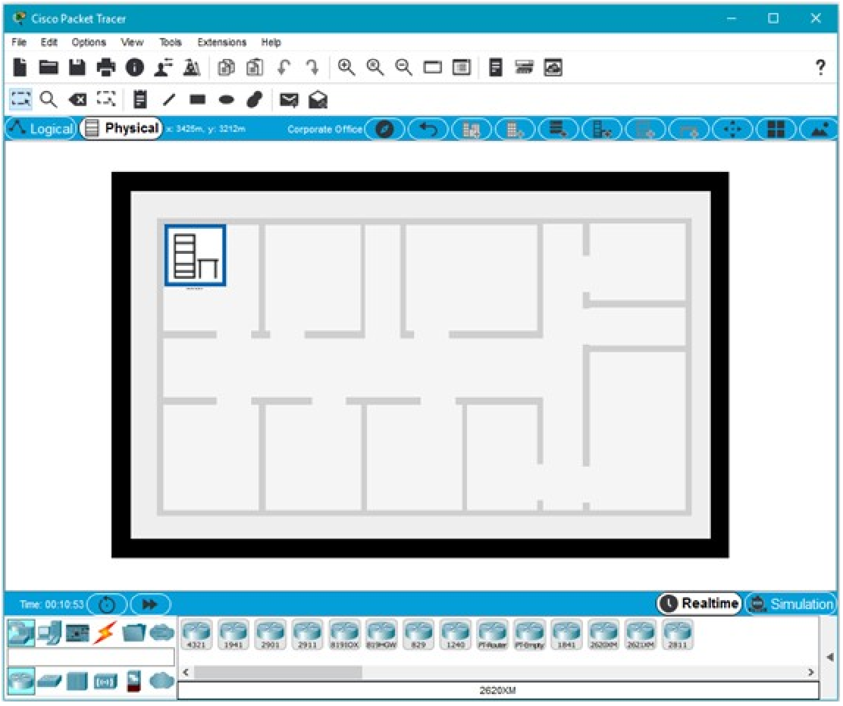


Figure 6.14: Zooming Out to View the Default Corporate Office Background

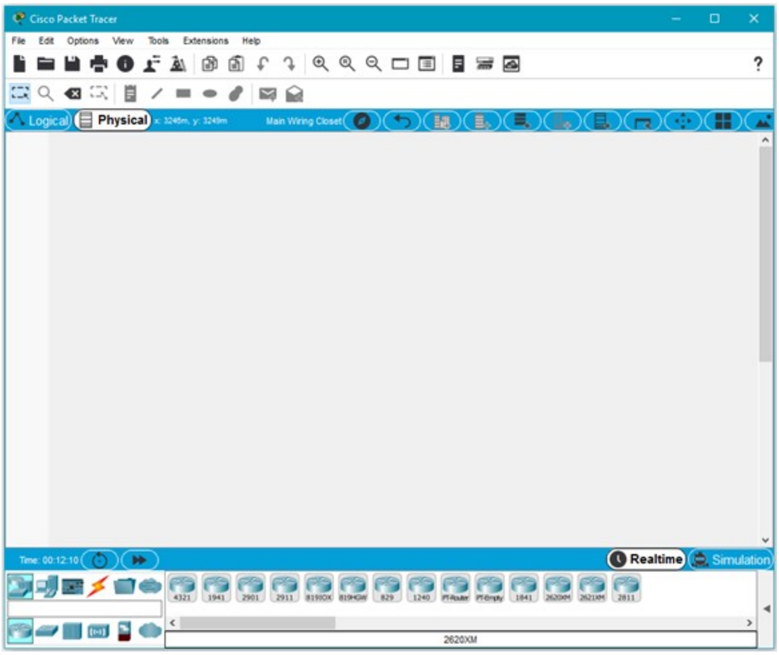


Figure 6.15: Main Wiring Closet Container with a Blank Workspace

5. **Add Devices to a Wiring Closet**
   With the *Main Wiring Closet* open, you can begin placing devices such as a **Router**, **Switch**, **Server**, or **Cable Modem** (Figures 6.16 and 6.17). Because you are in the **Physical** view, each device appears in a rack, simulating real-world equipment placement.
   - If you wish to cable these devices, temporarily switch to **Logical View** (Figure 6.18) to easily connect the interfaces. Then return to the **Physical View** to see the cables in the

rack (Figure 6.19).

- This back-and-forth process reflects how an administrator might plan cables in a real server room (Physically) while also handling the logical configuration (IP addresses, VLANs, etc.).

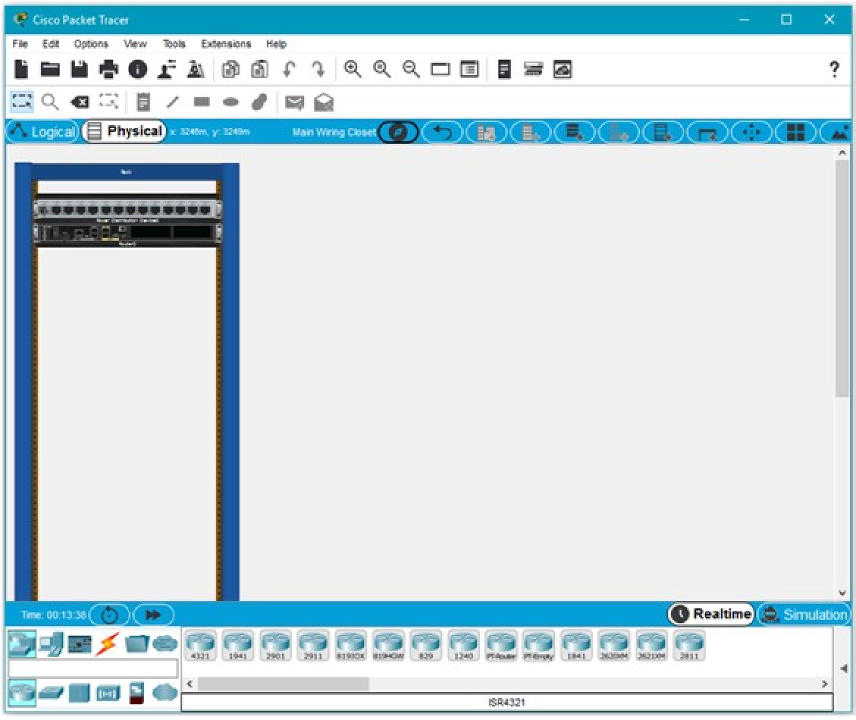


Figure 6.16: Adding a Router to the Rack in the Main Wiring Closet

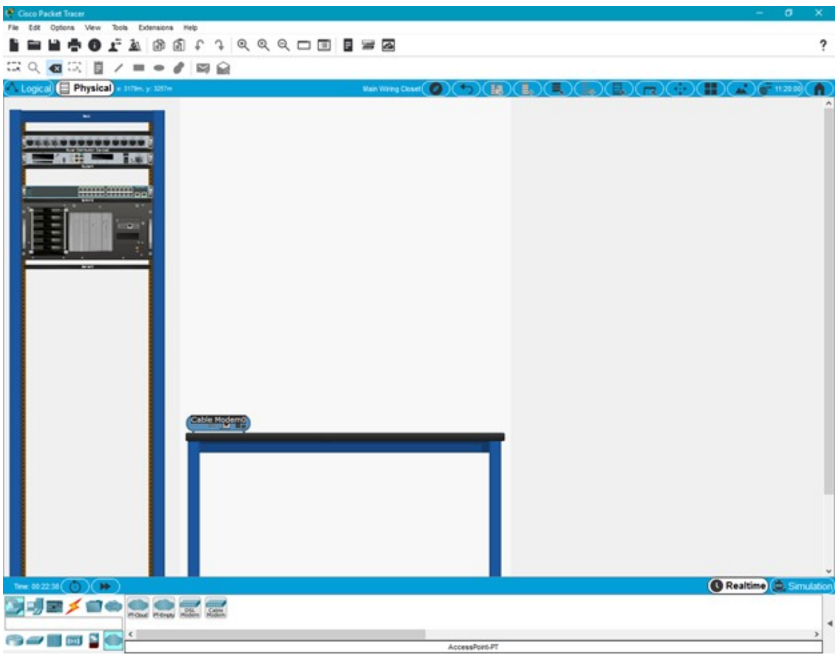


Figure 6.17: Add More Devices to the Wiring Closet

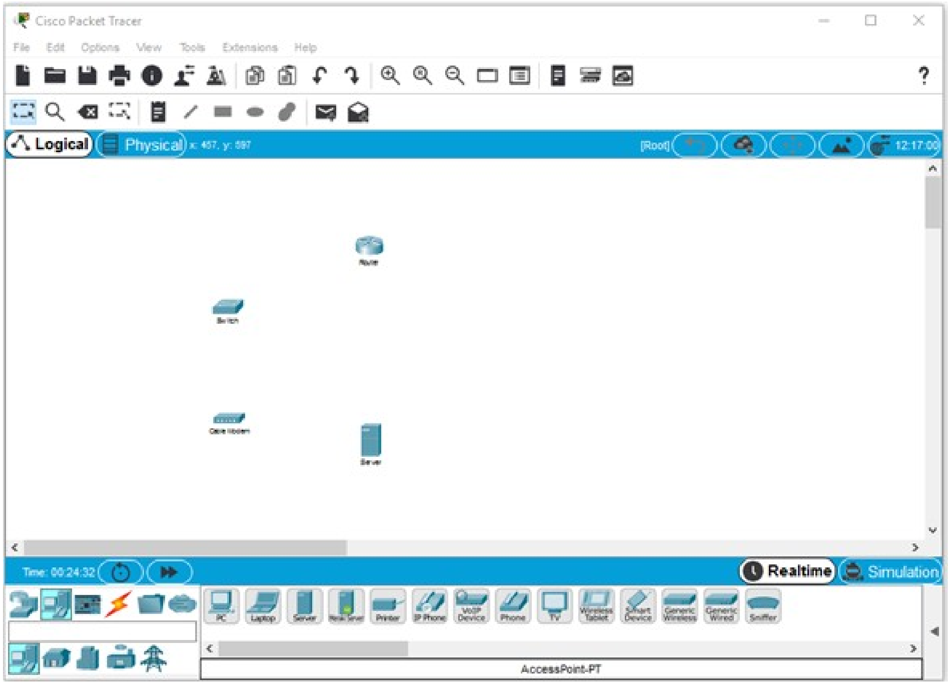


Figure 6.18: Adding Cabling to Devices in the Logical View

Figure 6.19: Physical View of Network Devices with Connected Cables

Wiring Closet Best Practices:

Rack Organization: Keep routers, switches, and servers stacked in a way that makes sense for your network's design. In real scenarios, you might have dedicated racks for core switches, edge routers, or server clusters.

Cabling Consistency: Use color-coded cables or consistent labeling to reduce confusion. Packet Tracer offers different cable color options for clarity.

Logical vs. Physical Views: Toggling between the two views helps you maintain both a conceptual (logical) and physical (rack and cable) representation of your network.

Save Frequently: Building out large physical topologies can be time-consuming. Save your work periodically in case of crashes or unexpected errors.

C. Experiment with Additional Designs

Once you're familiar with the Physical View basics—such as adding containers, customizing backgrounds, and placing devices in racks—you can broaden your topology and experiment with more complex scenarios.

6. **Expand Your Physical Topology**
   Now that you're comfortable navigating the **Physical View** and customizing containers, explore more advanced designs:
   - Create additional **cities** at the Intercity level, or place more **buildings** inside your main city to represent different office locations or campus sites.
   - Add **multiple wiring closets** within your Corporate Office, each containing distinct sets of devices (e.g., one closet for edge routers, another for distribution switches).
   - Inspect **wireless coverage** overlays if you add wireless access points or devices to different rooms or floors, ensuring you can see which areas have strong or weak signals.

Ideas for Advanced Physical Designs:

Multi-Floor Buildings: If your "Atlanta" city container has a large building, consider creating multiple floors or wiring closets to simulate real-world vertical network layouts.

Redundancy and Failover: Add extra switches or routers in different wiring closets to practice configuring link redundancy or spanning-tree scenarios.

Geographically Distributed Networks: Add another city (e.g., "Boston") at the Intercity level, and connect it to Atlanta with WAN links for a multi-site simulation.

Resources — **Packet Tracer File Types**. Learn about `.pkt`, `.pkz`, and `.pka` files—how they differ and how they can be used for labs or distributing activities.

Resources — **Packet Tracer Assessment Types**. Explore how PTSAs and PTMOs facilitate self-evaluations, formal quizzes, and skill assessments in Cisco Networking Academy.

Measuring Success

- You can navigate **Logical** and **Physical** views, exploring containers (Intercity, City, Corporate Office, Wiring Closet).
- A **background image** (e.g., world map) is successfully applied at Intercity or city level and remains after saving.
- **Containers** (e.g., "Atlanta," "Corporate Office," "Main Wiring Closet") are appropriately renamed and reorganized to match a real hierarchy.
- Devices placed in **Physical View** (e.g., in racks) also appear cabled in **Logical View**, confirming consistent setup.
- Hovering over cables or devices in **Physical View** shows the correct interface data, indicating proper structured-cabling setup.

— Further Exploration

LAB 6.1-Create Realistic Structured Cabling in the Physical Workspace and Cabling Devices in a Rack

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.

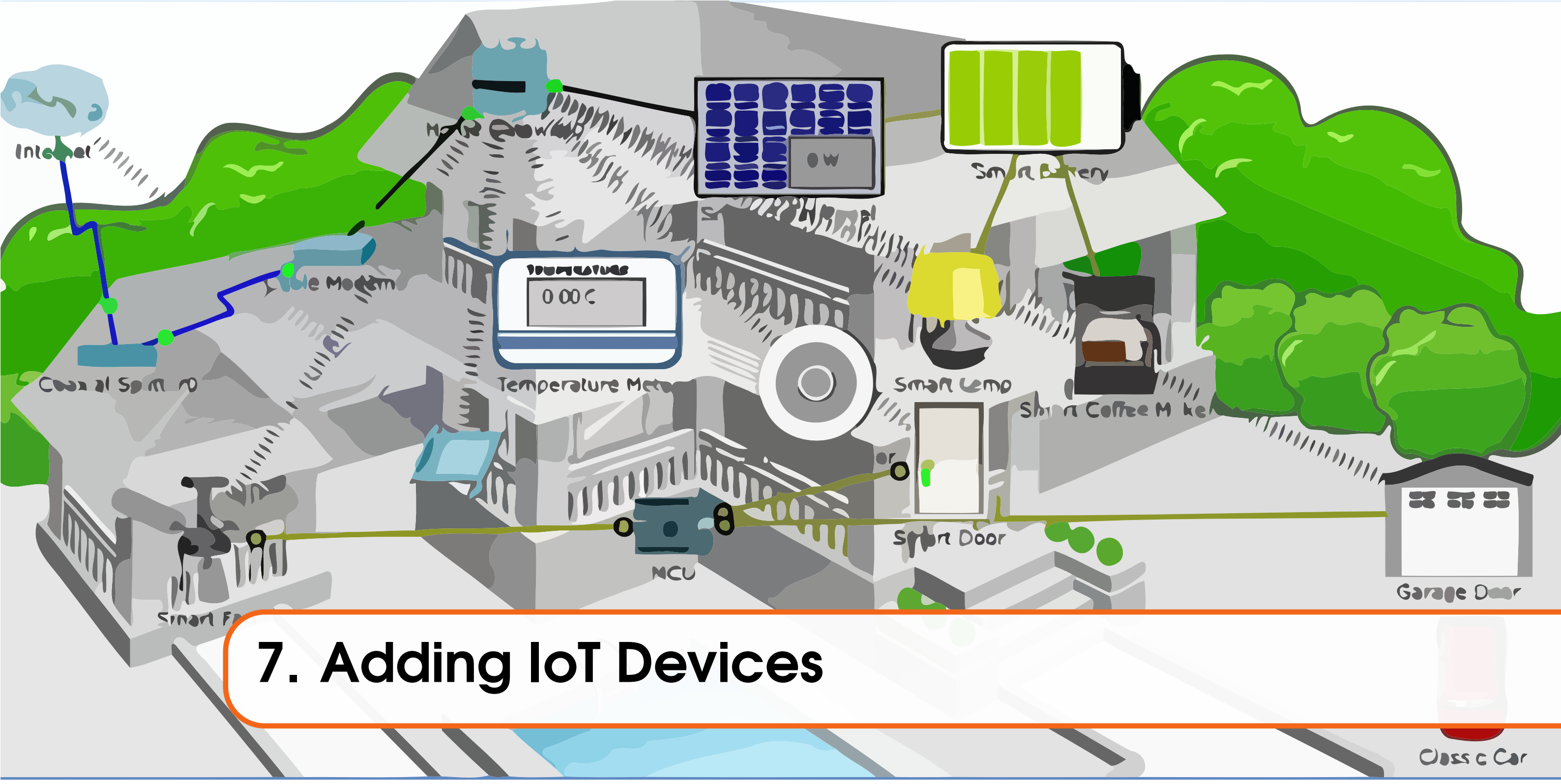
LAB 6.2-Connect Devices using Wireless Technologies

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 connecting from the device list.
- Enable the mobile hotspot feature on the smartphone and connect the laptop to this network to access the internet using the cellular connection.

Summary

In this lab, you explored **Packet Tracer's Physical View** to design more realistic representations of your network environment. You applied backgrounds, created or edited containers (cities, buildings, wiring closets), placed devices in racks, and switched between Physical and Logical views for cabling. You also learned about **Packet Tracer file types** and assessment methods. With these skills, you can mirror real-world topologies—deepening your practical understanding of network infrastructure.



7. Adding IoT Devices

Introduction

This lab focuses on discovering, connecting, and configuring various **IoT devices** in Cisco Packet Tracer. You will learn to integrate both wired and wireless smart devices, set up network parameters, and experiment with remote control of a smart home environment. By the end, you should be able to create and modify *smart homes*, *smart cities*, or *smart factories* with confidence.

Objectives

- Discover and identify **IoT devices** available in Cisco Packet Tracer (sensors, actuators, gateways).
- Connect IoT devices to the network using **wired or wireless** connections.
- Configure and control IoT devices (network parameters, device attributes) via a **registration server** or home gateway.
- Experiment with customizing **smart environments** to explore IoT functionalities.

Lab Plan

A. **Explore the Existing Smart Home Network**
B. **Add Wired IoT Devices**
C. **Add Wireless IoT Devices**

Background

The *Internet of Things (IoT)* in Packet Tracer involves networked sensors, actuators, and smart devices that collect and share data. Packet Tracer includes features like:

- Environmentally reactive devices (responding to sun, wind, rain, etc.).
- Configurable actions based on changing environmental values.
- Scripting options for home gateways or servers to remotely manage these IoT nodes.

Packet Tracer provides everything needed to create simulated **smart homes, smart cities, and smart factories** by leveraging built-in IoT components and remote management.

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

Resources — 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.

Resources — 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.

A. Explore the Existing Smart Home Network

In this section, you will open and review a pre-configured Smart Home network in Packet Tracer. You will see how the network is organized, which IoT devices are available, and how the Home Gateway manages those devices.

1. **Open the `Smart_Home_Network.pkt` File:**
    - Double-click on `Smart_Home_Network.pkt` to open it in Packet Tracer.

- Immediately go to `File` → `Save As` and save a local copy, for example `MySmartHome_Lab7.pkt`. This ensures your modifications won't affect the original file.

2. **Examine IoT End Devices:**
   - In the lower-left corner of the Packet Tracer interface, select **End Devices** (top row) and **Home** (bottom row).
   - You will see various smart home IoT devices, such as an air conditioner or a coffee maker, in the Device-Specific Selection box (Figures 7.1 and 7.2).

Figure 7.1: Device-Type Selection Box

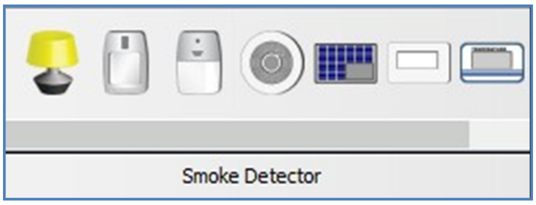


Figure 7.2: Device-Specific Selection Box (Smart Home IoT Devices)

3. **Observe the Prebuilt Smart Home Network:**
   - Switch to the **Logical** workspace if not already there; you should see a *Smart Home* topology with various devices and a *Home Gateway*.
   - Hover your mouse over any device (e.g., *Smart Fan*) to see a brief tooltip with device info (Figures 7.3 and 7.4).

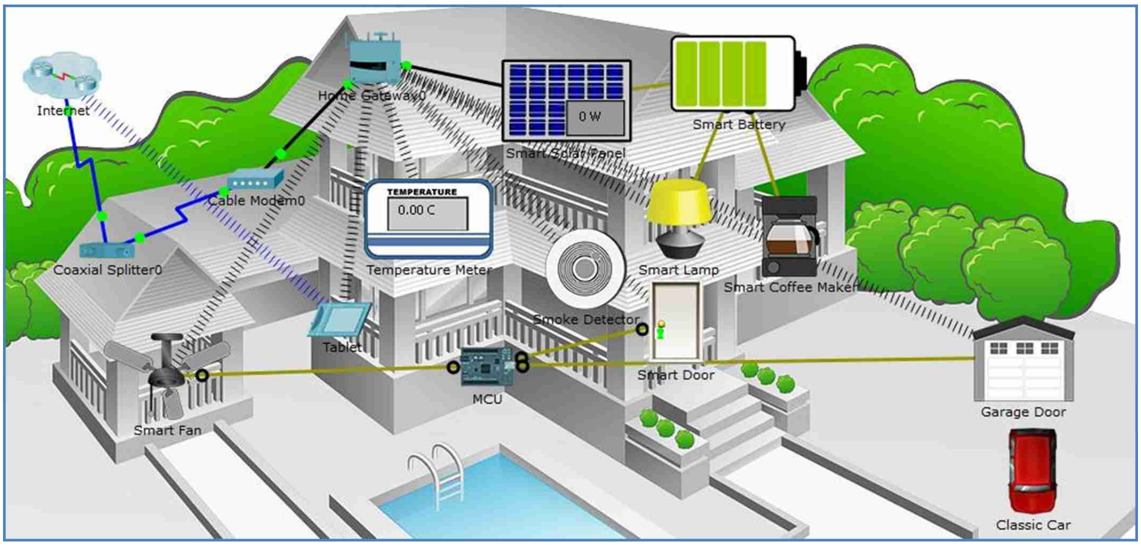


Figure 7.3: Smart Home Network

Figure 7.4: Viewing Device Information in a Smart Home Network

4. **Activating Devices:**
   - To toggle a device *on* or *off* manually, hold down the `Alt` key and hover over the IoT device. This simulates a quick local control mechanism for testing purposes.
5. **Check the Home Gateway (Infrastructure Device):**
   - Locate the *Home Gateway* icon (Figures 7.5 and 7.6). Click it to open its configuration window.
   - In the **Physical** tab, examine the device's hardware layout. This view simulates how the gateway might look in a real environment.

Figure 7.5: Home Gateway Icon

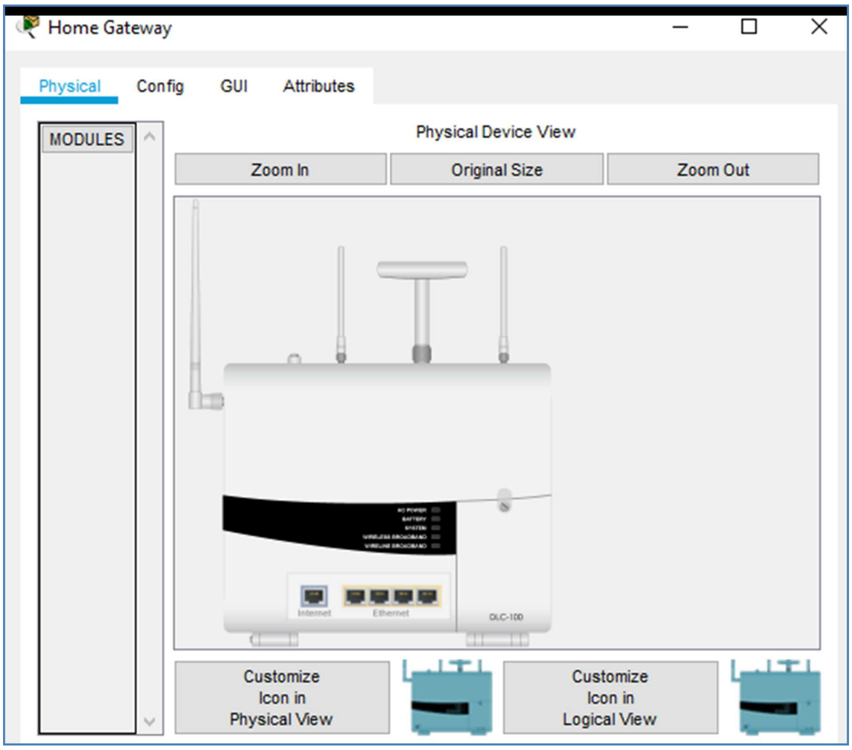


Figure 7.6: Physical Tab of the Home Gateway

6. **LAN and Wireless Settings:**
   - In the **Config** tab, click **LAN** to see the IP address settings (Figure 7.7). This section may show the gateway's default IP address or subnet.
   - Select the **Wireless** option to note the SSID and *WPA2* passphrase (Figure 7.8). These are crucial for any wireless IoT device that needs to join the network securely.

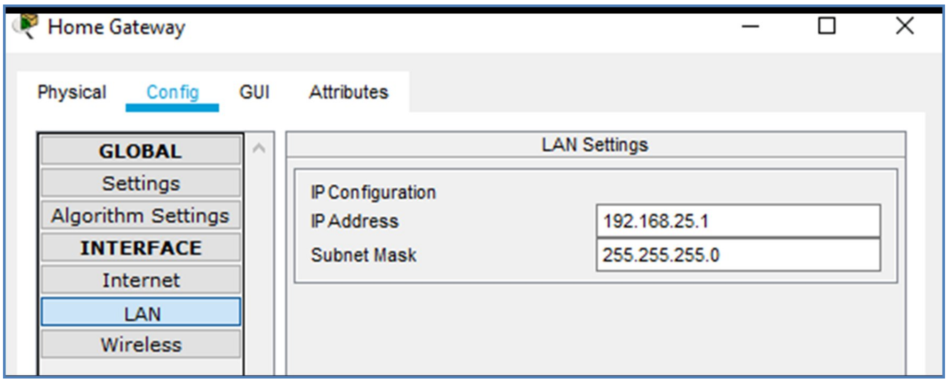


Figure 7.7: Config Tab of the Home Gateway (LAN Settings)

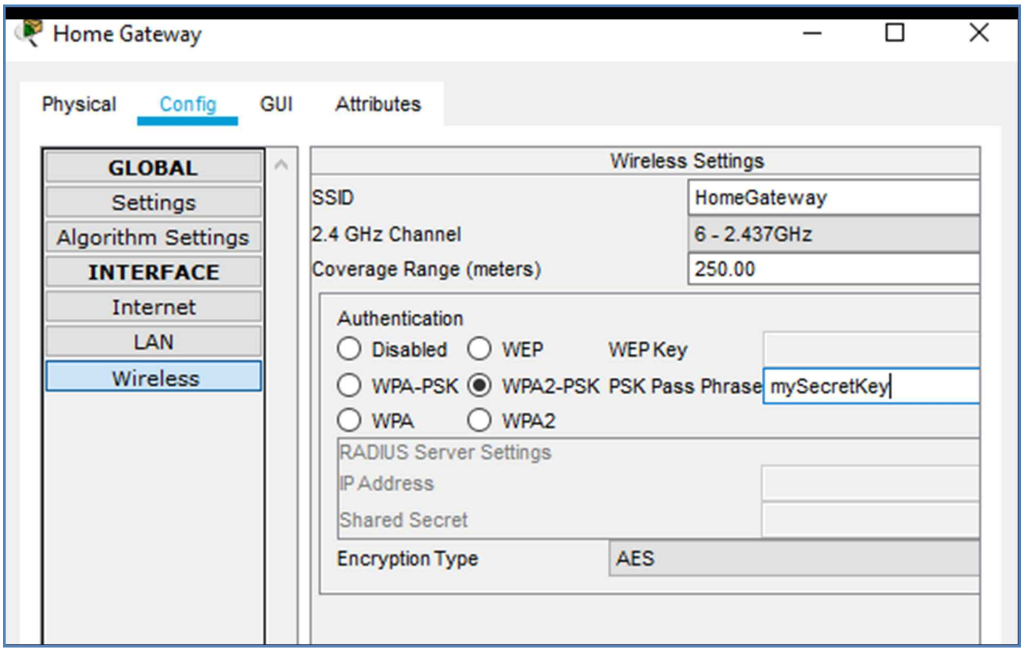


Figure 7.8: Configuring Wireless Settings on the Home Gateway

7. **Tablet and Web Browser:**
   - Click the **Tablet** icon (Figure 7.9). Then, under **Desktop**, select **Web Browser**.
   - In the browser, enter `192.168.25.1` (the Home Gateway's IP). The default credentials are typically `admin/admin`.

Figure 7.9: Tablet Device Icon

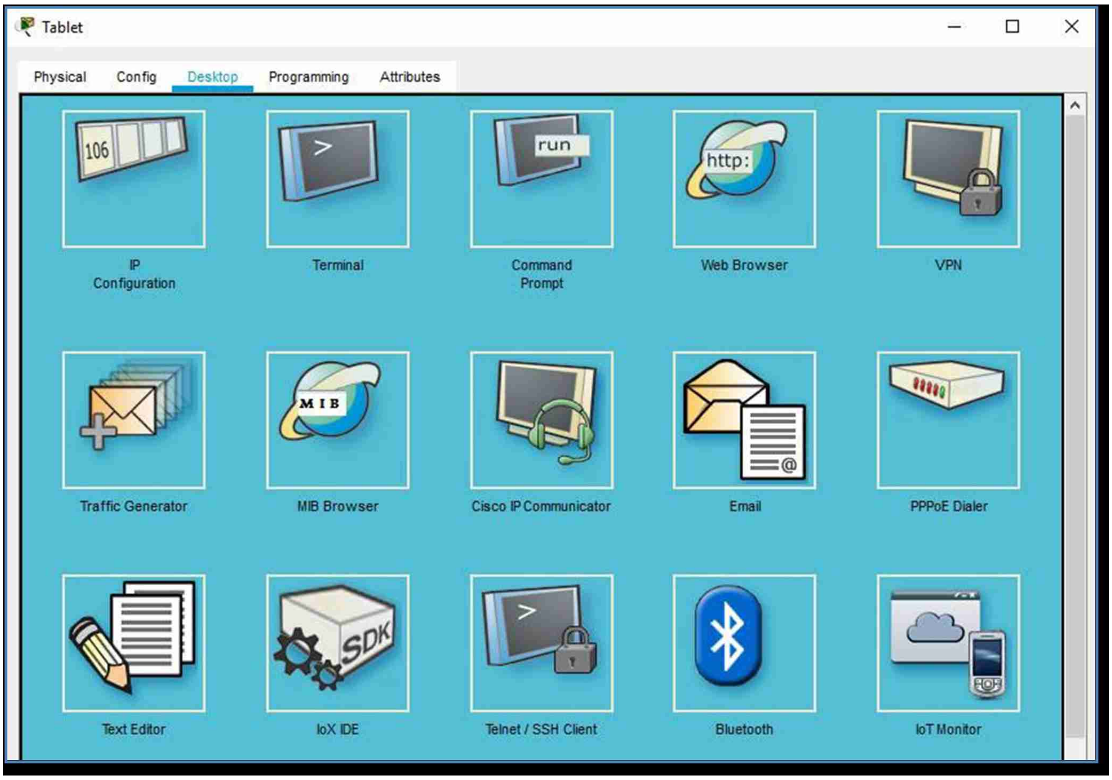


Figure 7.10: Web Browser in Tablet

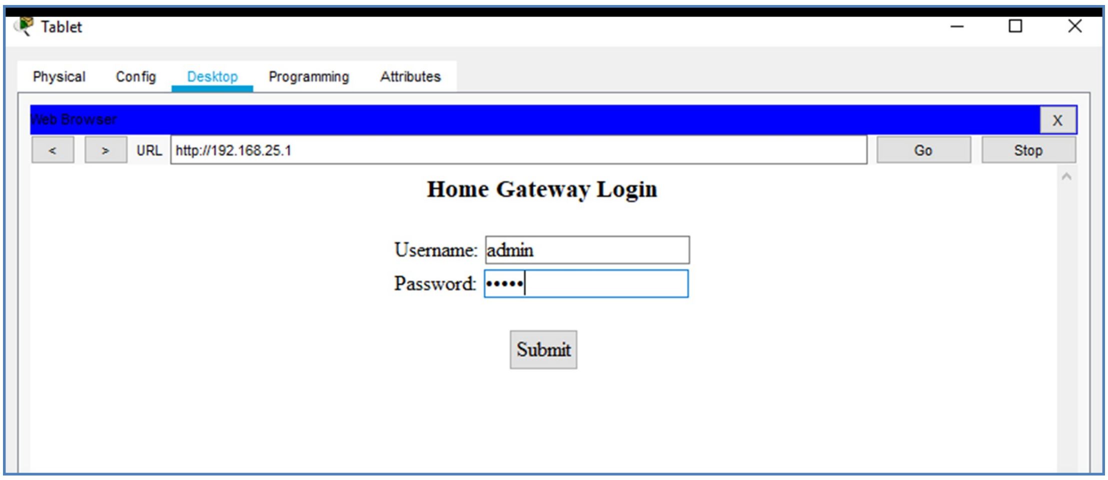


Figure 7.11: Logging into the Home Gateway

8. **IoT Server – Devices List:**

- After logging in, you should see a list of *connected IoT devices* under the **IoT Server Devices** section (Figures 7.12 and 7.13).
- From here, you can toggle device settings or rename them as desired.

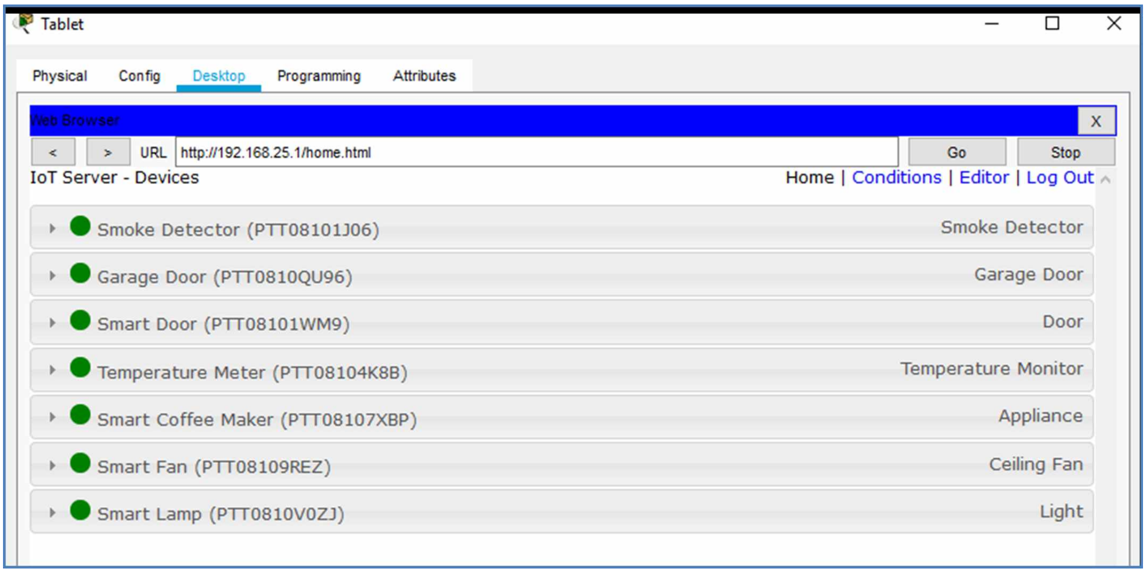


Figure 7.12: Home Gateway Web Interface

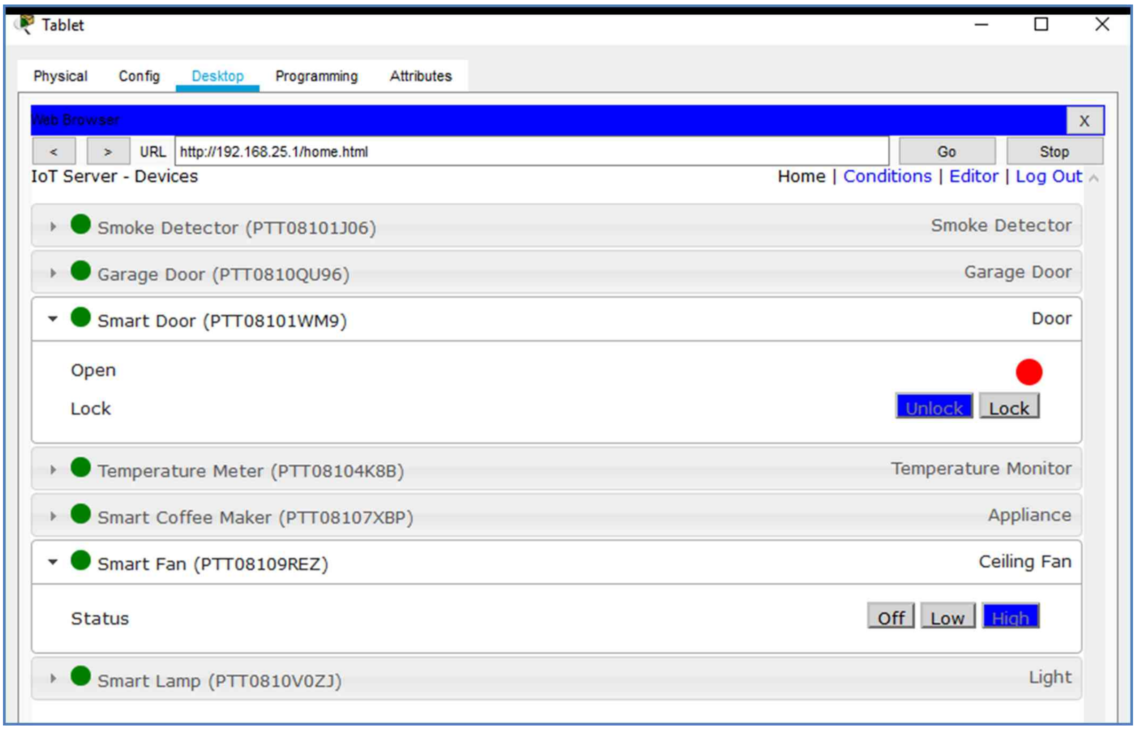


Figure 7.13: Status and Settings of Connected IoT Devices

Once you're finished reviewing the device list, you can close the Tablet window.

Navigating a Prebuilt Smart Home:

Explore Device Types: Packet Tracer offers a variety of IoT devices (sensors, cameras, fans). Hover over each to discover their capabilities and possible configuration options.

Use the Gateway Interface: The Home Gateway acts as a central registration and management point for your IoT devices. Logging into `192.168.25.1` is often the quickest way to see which devices are recognized and how they are controlled or monitored.

Experiment Cautiously: Before renaming or removing devices, consider saving your file under a new name to maintain a safe backup of the original Smart Home setup.

B. Add Wired IoT Devices

In this section, you will integrate new *wired* IoT devices (e.g., a lawn sprinkler) into your existing smart home network. By assigning them to `DHCP` and registering them with the Home Gateway, you can remotely manage and monitor these devices just like any other smart home appliance.

9. **Cable a Device to the Network:**
   a) **Place a Lawn Sprinkler**
   From the Device-Specific Selection box, choose the *Lawn Sprinkler* icon and click in the workspace to place it. This device will initially appear as something like `IoT0` or `Sprinkler-PT` in the workspace.
   b) **Connect the Sprinkler to the Home Gateway**

      - Select **Connections** (the lightning-bolt icon) in the lower-left menu.
      - Choose **Copper Straight-Through**.
      - Click the sprinkler's `FastEthernet0` port and then click an available Ethernet port on the Home Gateway.

   After a brief moment, the link lights should turn green if the cable and port selection are correct.
10. **Configure the Sprinkler for Network Connectivity:**
   a) **Open the Device Window**
   Locate the newly placed lawn sprinkler device in your workspace and click it. Initially, it may be labeled something like `IoT0`, as shown in Figure 7.14.

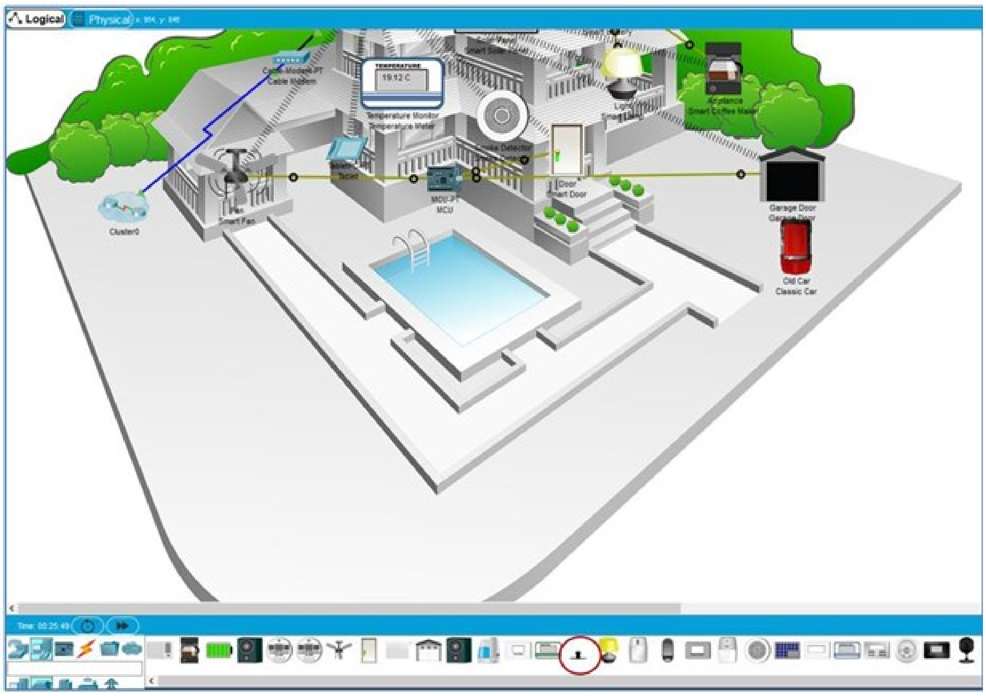


Figure 7.14: Lawn Sprinkler Device Icon

b) **Config Tab Settings**
In the device's configuration window:

- Under *Global Settings*, change the **Display Name** to *Sprinkler1*.
- For the **IoT Server** field, select *Home Gateway* from the drop-down list.

Next, click **FastEthernet0** on the left menu and set *IP Configuration* to `DHCP` (Figures 7.15 and 7.16). This instructs the sprinkler to obtain its IP address automatically from the Home Gateway.

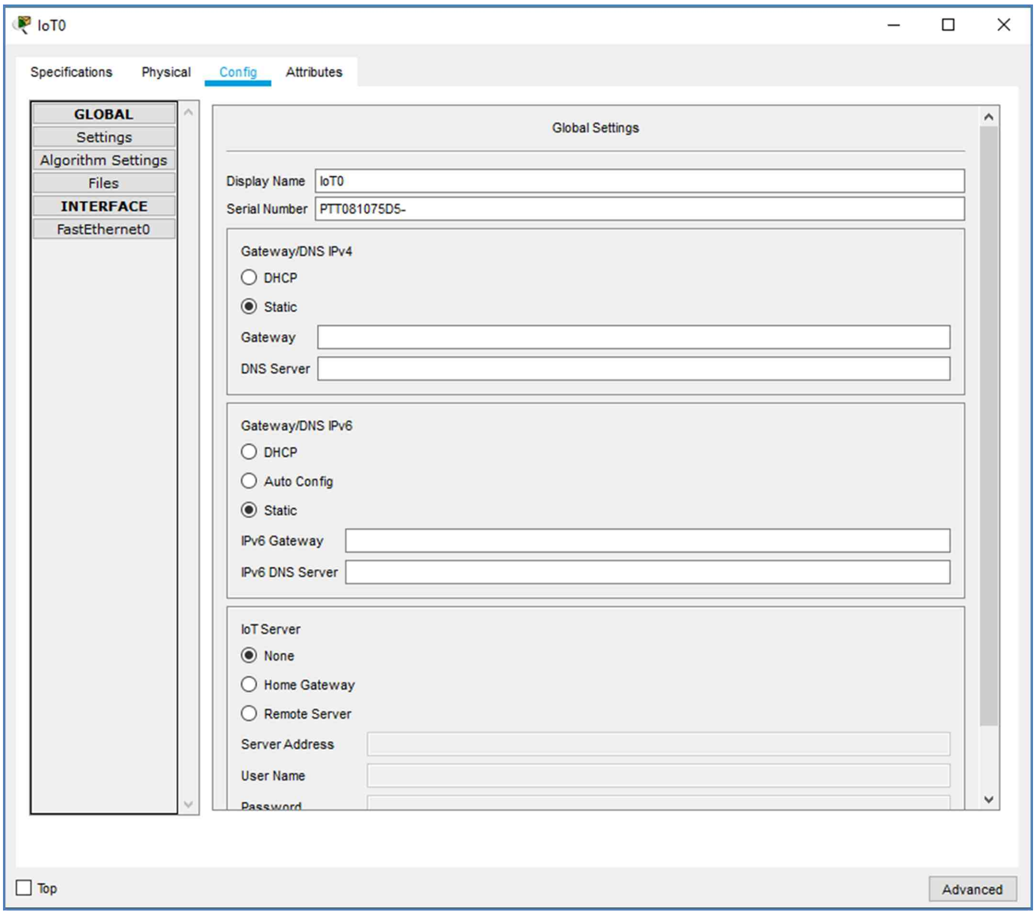


Figure 7.15: Configuring the IoT Device (Global Settings)

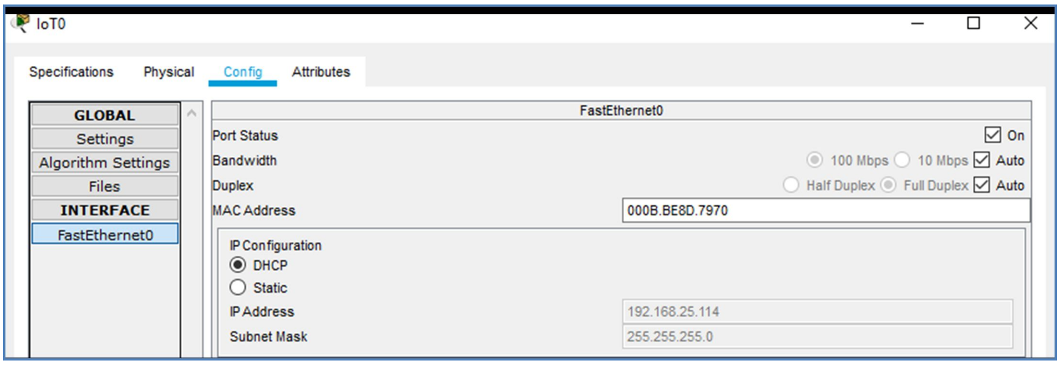


Figure 7.16: Changing IP Configuration to DHCP on FastEthernet0

Once finished, close the configuration window for *Sprinkler1*.

c) **Verify Connectivity**
Open the Home Gateway's web interface again on your Tablet (by entering `192.168.25.1` in the browser). The sprinkler should now be listed under the *IoT Server Devices* section, as shown in Figure 7.17, indicating successful registration.

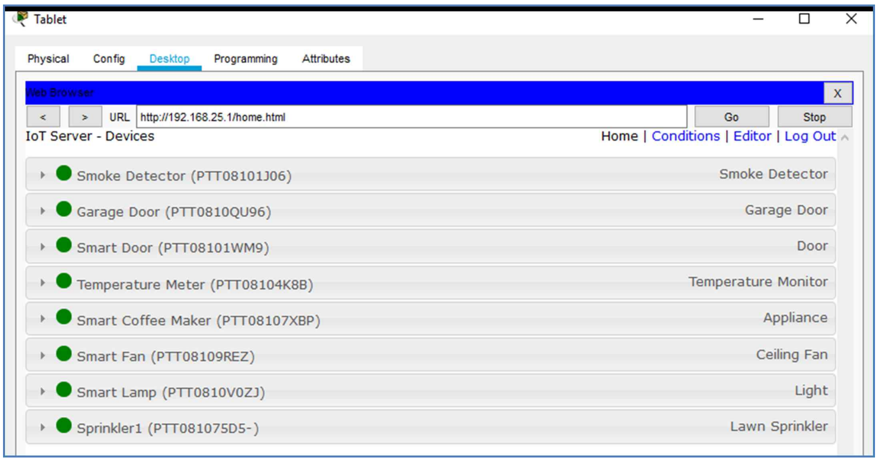


Figure 7.17: IoT Server – Devices List (Sprinkler1 Appears)

11. **Experiment**
    Consider adding other **wired IoT devices**, like a *Coffee Maker* or a *Door Sensor*. Simply:
    a) Place the device in the workspace.
    b) Cable it to the Home Gateway using a *Copper Straight-Through* connection.
    c) Assign `DHCP` under its *FastEthernet* configuration.
    d) Check the *IoT Server Devices* list in the Gateway's interface to confirm it appears.

    Each device you add and properly configure will show up in the same IoT management list, letting you monitor or control them remotely.

Wired IoT Setup Tips:

DHCP vs. Static IPs: Using DHCP simplifies assigning addresses to multiple IoT devices. If you need more control, consider assigning static IPs so you know exactly where each device is on your network.

Changing Display Names: Give each device a descriptive name (e.g., `FrontYardSprinkler`, `KitchenCoffeeMaker`), making it easier to identify them in the gateway interface.

Testing Connectivity: Beyond the gateway interface, you can *ping* each new IoT device's IP address from a PC or Tablet to confirm end-to-end connectivity. ■

C. Add Wireless IoT Devices

In this section, you will introduce *wireless* IoT devices to your smart home network. By installing the proper wireless module and configuring WPA2 settings, you can connect sensors (like a wind detector) to the Home Gateway without using cables.

12. **Add a Wireless Device to the Network:**
    a) **Place a Wind Detector**
    From the **Device-Specific Selection** box, click the *Wind Detector* icon and place it in the workspace. Figures 7.18 and 7.19 show what these steps look like.

Figure 7.18: Device-Specific Selection Box

Figure 7.19: Wind Detector

b) **Add a Wireless Module**
Click the *Wind Detector*, then choose **Advanced** and go to the **I/O Config** tab (Figure 7.20). Change the `Network Adapter` to `PT-IOT-NM-1W`, which enables wireless connectivity for this IoT device.

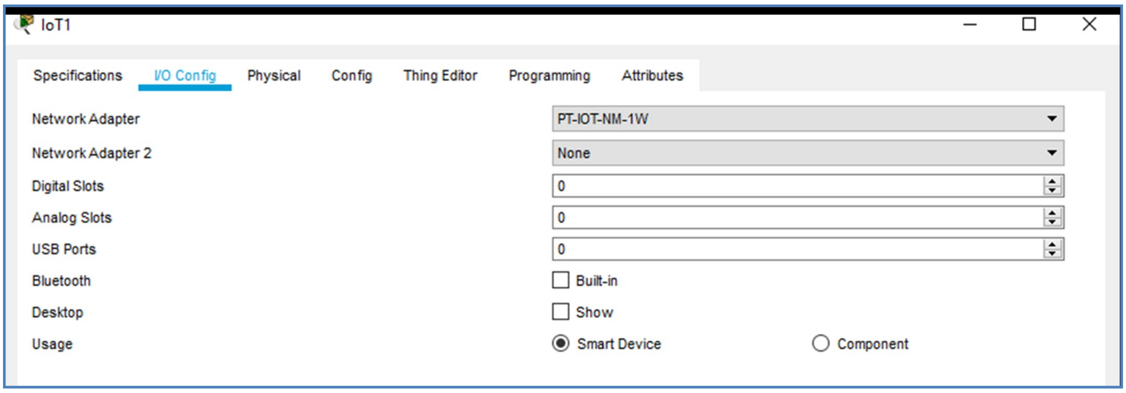


Figure 7.20: I/O Config Tab for the Wind Detector

c) **Configure Wireless Settings**
Switch to the **Config** tab, then select **Wireless0**:

- Set **Authentication** to `WPA2-PSK` (a common security method for wireless networks).
- Under **PSK Pass Phrase**, enter `mySecretKey`, or the passphrase you noted in the Home Gateway's wireless settings.
- The Wind Detector should automatically connect to the Home Gateway's SSID once these values are set (Figures 7.21 and 7.22).

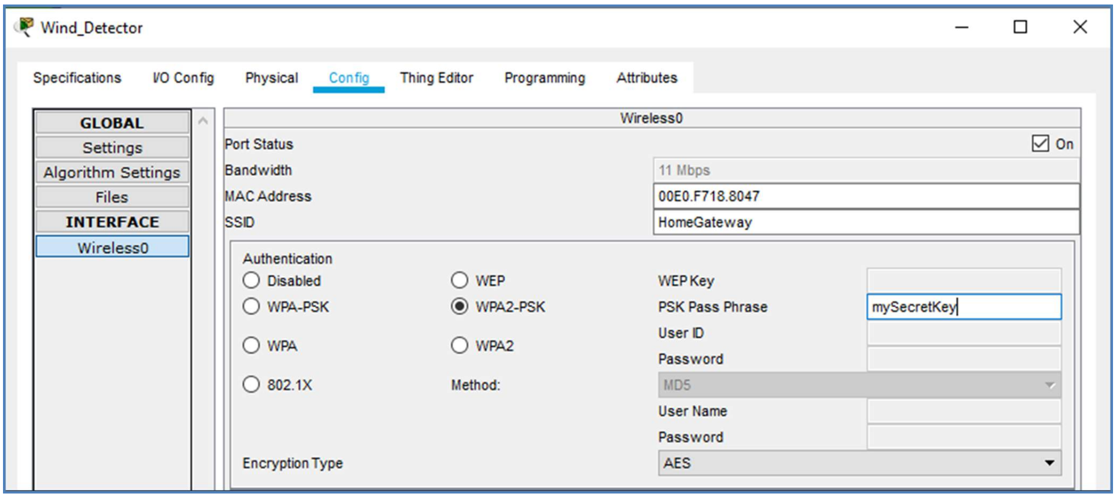


Figure 7.21: Wireless Settings for the Wind Detector

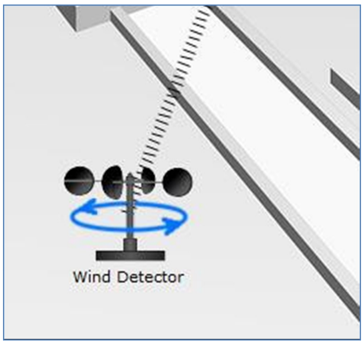


Figure 7.22: Wireless Link Formation (Illustration)

d) **Verify the Device**
Revisit the Home Gateway's web interface on your Tablet (by entering its IP, such as `192.168.25.1`). In the IoT Server devices list, confirm that *Wind Detector* appears (Figure 7.23), indicating a successful wireless connection.

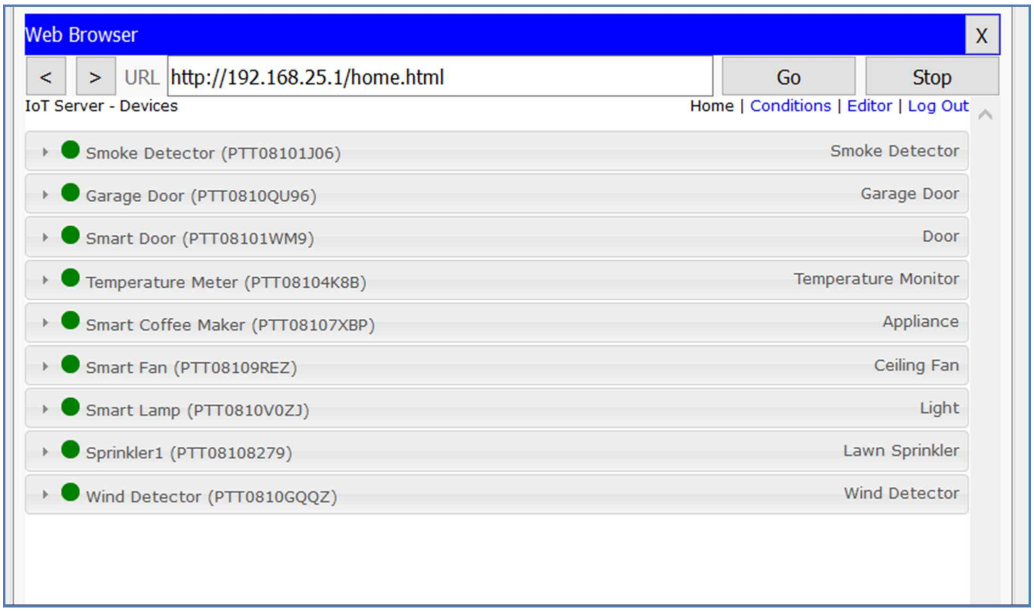


Figure 7.23: IoT Server – Devices List (Wind Detector Added)

13. **Experiment**
    Feel free to add **more wireless IoT devices**, such as a *Temperature Sensor* or *Motion Detector*. Use the same `SSID` and `WPA2-PSK` passphrase (e.g., `mySecretKey`). Verify each device in the Home Gateway's interface to confirm they're recognized and online.

Wireless IoT Configuration Tips:

Check Signal Strength: In a more complex Packet Tracer environment, you might need to consider signal coverage or adjust the device's placement to ensure a reliable wireless connection.

Name Your Devices: Rename each IoT device (e.g., *WindDetectorLivingRoom*) to easily track them in the Home Gateway's management list, especially if you plan to add many sensors.

DHCP vs. Static IP: Most wireless IoT devices in Packet Tracer default to DHCP, but you can assign static IPs if you want a fixed address for troubleshooting or advanced testing.

Security Options: While `WPA2-PSK` is common, you can also explore other encryption or authentication schemes in the Home Gateway for a more secure or specialized setup. ■

Measuring Success

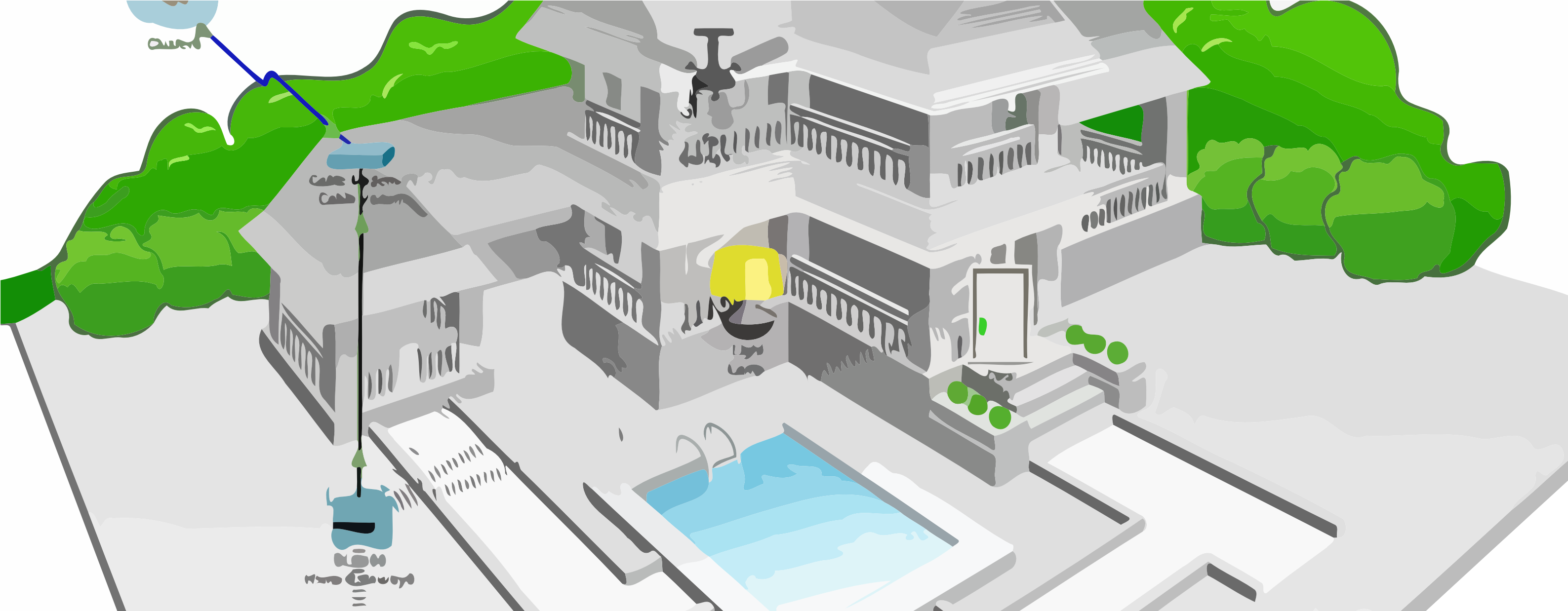
- Your newly added **wired IoT devices** (e.g., Lawn Sprinkler) appear in the IoT Server list on the Home Gateway.
- The **wireless IoT devices** (e.g., Wind Detector) successfully join the home network with the correct WPA2-PSK credentials.
- Each added IoT device obtains a DHCP IP and can be toggled or monitored from the Tablet's web interface.
- Holding the `Alt` key over certain devices (e.g., Smart Fan) shows them powering on/off, confirming the IoT functionality is active.

■

> **— Further Exploration**
> Please feel free to download the Packet Tracer Activity (PTA) version of this above tutorial from the Git Repository.

Summary

In this lab, you discovered how to integrate both **wired and wireless IoT devices** into a Packet Tracer smart home environment. You examined existing sensors, placed new ones (via cables or Wi-Fi), and used the home gateway's web interface to confirm connectivity. This hands-on approach shows how real-world IoT deployments might be managed—through consistent naming, IP settings (DHCP), and registration with a gateway—enabling streamlined monitoring and control of smart devices.



8. Connect and Monitor IoT Devices

Introduction

In this lab, you will learn how to connect and monitor smart home devices by leveraging a **Home Gateway** device. You will explore how to register IoT devices, configure a wireless tablet, and control various smart devices within a single network environment. By the end of this lab, you should be comfortable with adding, configuring, and remotely managing IoT devices such as fans, lamps, and doors.

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 home gateway's **features**, including its physical, configuration, GUI, and attribute tabs.
- Register and **monitor IoT devices** through a home gateway, practicing the steps for connecting and configuring them within a network.
- Control and **interact with smart devices** remotely using a tablet, PC, or smartphone, deepening your understanding of IoT device management.

Background

In this section, you will connect a home gateway and several IoT devices to an existing home network, then monitor these devices through the home gateway. Specifically, you will:

- Add a home gateway to the network (both physical and logical connections).
- Configure IoT devices for wireless connectivity.
- Add a wireless tablet and connect it to the home gateway.
- Register IoT devices so they appear in the home gateway's IoT server list.
- Test and verify that your smart devices are discoverable and controllable from a remote tablet.

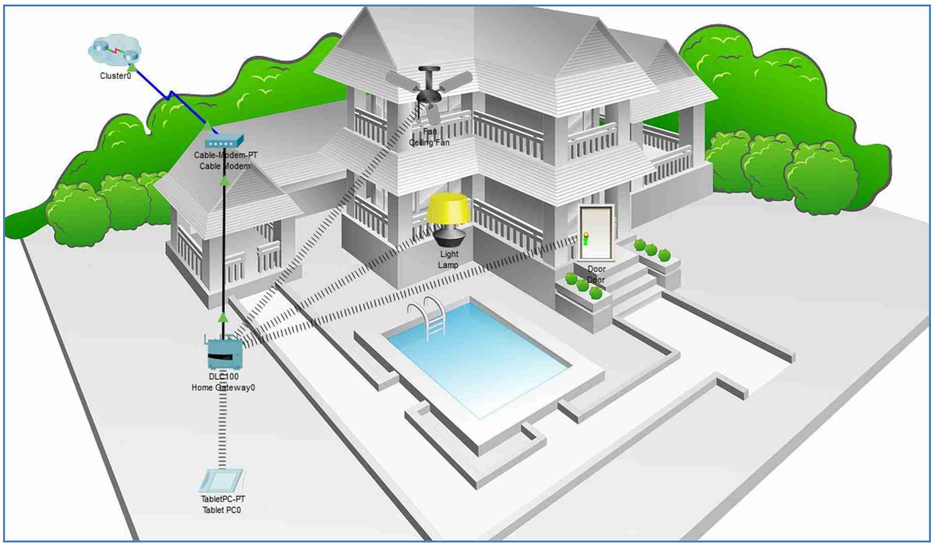


Figure 8.1: Smart Home Network Overview

Lab Plan

A. **Add a Home Gateway to the Network**
B. **Connect IoT Devices to the Wireless Network**
C. **Add a Wireless Tablet to the Network**
D. **Register IoT Devices with the Home Gateway**

A. Add a Home Gateway to the Network

In this section, you will integrate a **Home Gateway** into an existing IoT network topology. The Home Gateway will help manage and monitor connected IoT devices, serving as a central access point for configuration and control.

1. **Open the** `Connect and Monitor IoT Devices.pkt` **File:**
   - Launch Cisco Packet Tracer and open the file named `Connect and Monitor IoT Devices.pkt`.
   - To preserve the original file, choose `File` → `Save As` and rename it (e.g., `Connect_and_Monitor_IoT_Yo`
2. **Place and Cable the Home Gateway:**
   - In the lower-left area of Packet Tracer, select the **Device-Type Selection** box. Then click the *Wireless Devices* icon.
   - Locate the **Home Gateway** device in the list. Click it once, then click anywhere in the *Logical* workspace to place it there (Figure 8.2).

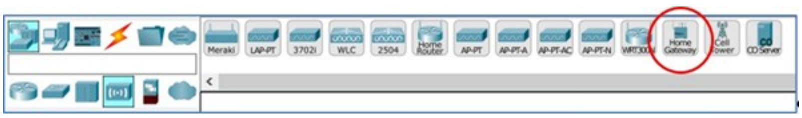


Figure 8.2: Placing the Home Gateway in the Logical Workspace

   - Next, select *Copper Straight-Through* from the cable options (lightning-bolt icon).
   - Click the Home Gateway, then choose `Port 1` (or a similar Ethernet port).
   - Click the **Cable Modem** and connect the other end of the cable to its *Internet* port.

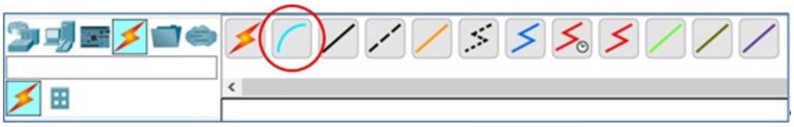


Figure 8.3: Connecting the Home Gateway to the Cable Modem

3. **Verify Link Lights:**
    - Wait a few seconds for the ports to negotiate. Both the Home Gateway and the Cable Modem should display green link lights, indicating a successful physical connection (Figure 8.4).
    - If the lights remain off or amber for an extended period, confirm you chose *Copper Straight-Through* rather than another cable type, and ensure both devices are powered on by default.

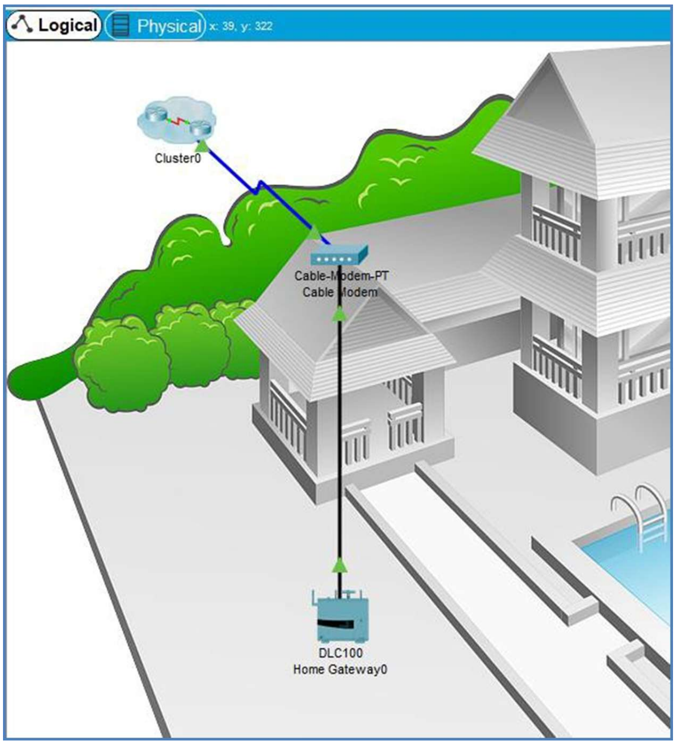


Figure 8.4: Active Link Indicators between Home Gateway and Cable Modem

Home Gateway Placement Tips:

Future Configuration: After placing the Home Gateway, you may need to set IP addresses, turn on DHCP, or configure wireless settings. This will be detailed in subsequent steps or labs.

Cabling Consistency: Use consistent cable colors (if desired) to distinguish between different types of connections, such as WAN links vs. LAN cables.

Saving Progress: Consider saving your Packet Tracer file again at this point, so you can easily revert to this stage if you need to.

B. Connect IoT Devices to the Wireless Network

In this section, you will attach wireless adapters to select IoT devices (e.g., a fan, door, or lamp) and configure them to join the Home Gateway's Wi-Fi network via `DHCP`.

4. **Add Wireless Adapters and Configure Each Device:**

   a) **Fan Setup**
   Locate the **Fan** icon in your workspace and click to open its configuration window. In the *Config* tab, click the *Advanced* button (near the bottom-right corner) to reveal additional settings.

   - Switch to the *I/O Config* sub-tab, and under *Network Adapter*, select `PT-IOT-NM-1W`. This module enables wireless connectivity for the fan.
   - Refer to Figure 8.5 to see how to choose the `PT-IOT-NM-1W` adapter.

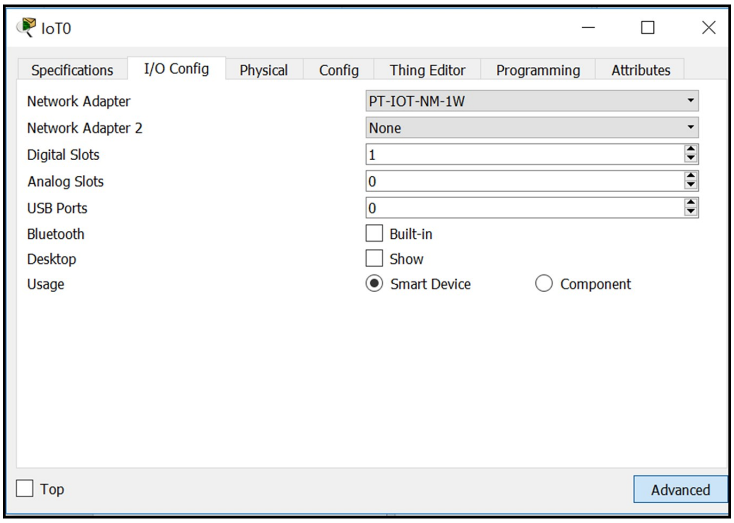


Figure 8.5: Selecting the PT-IOT-NM-1W Wireless Adapter in *I/O Config*

After adding the wireless module, switch back to the *Config* tab. Under *Settings*, rename the device to `Ceiling Fan` for clarity (see Figure 8.6).

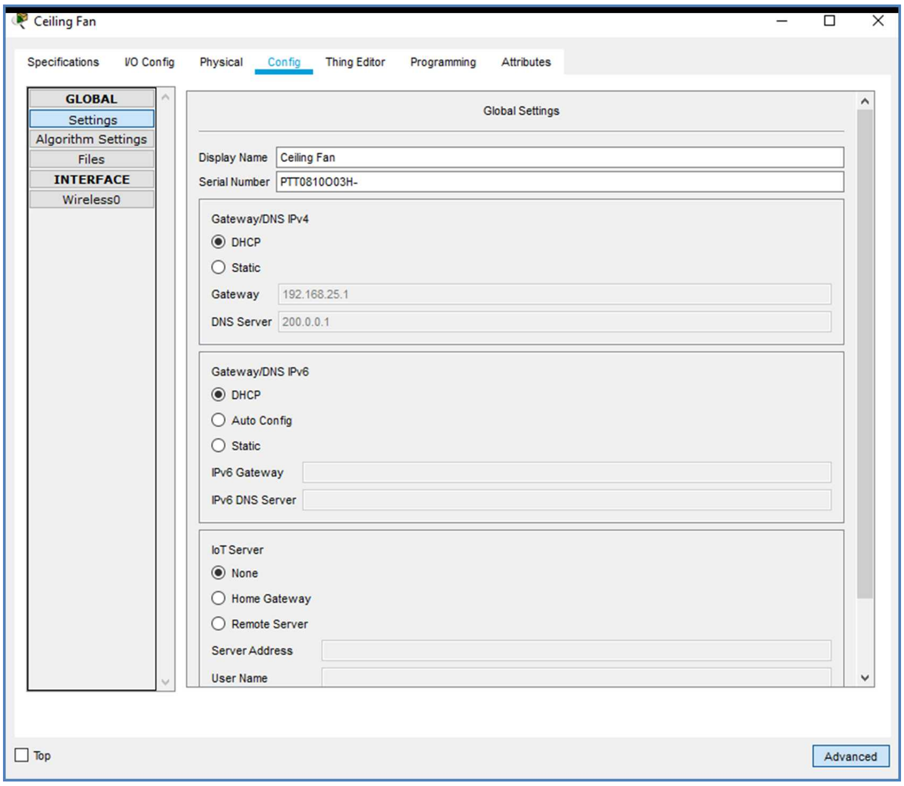


Figure 8.6: Renaming the Device to "Ceiling Fan"

b) **SSID and IP Configuration**
While still in the *Config* tab, click on **Wireless0**:

- Set `SSID` to `HomeGateway` (matching the SSID configured on your Home Gateway).
- Ensure that `DHCP` is selected so the fan automatically obtains an IP address.
- If the Home Gateway is properly configured, you should see the fan receive an IP such as `192.168.25.100`.

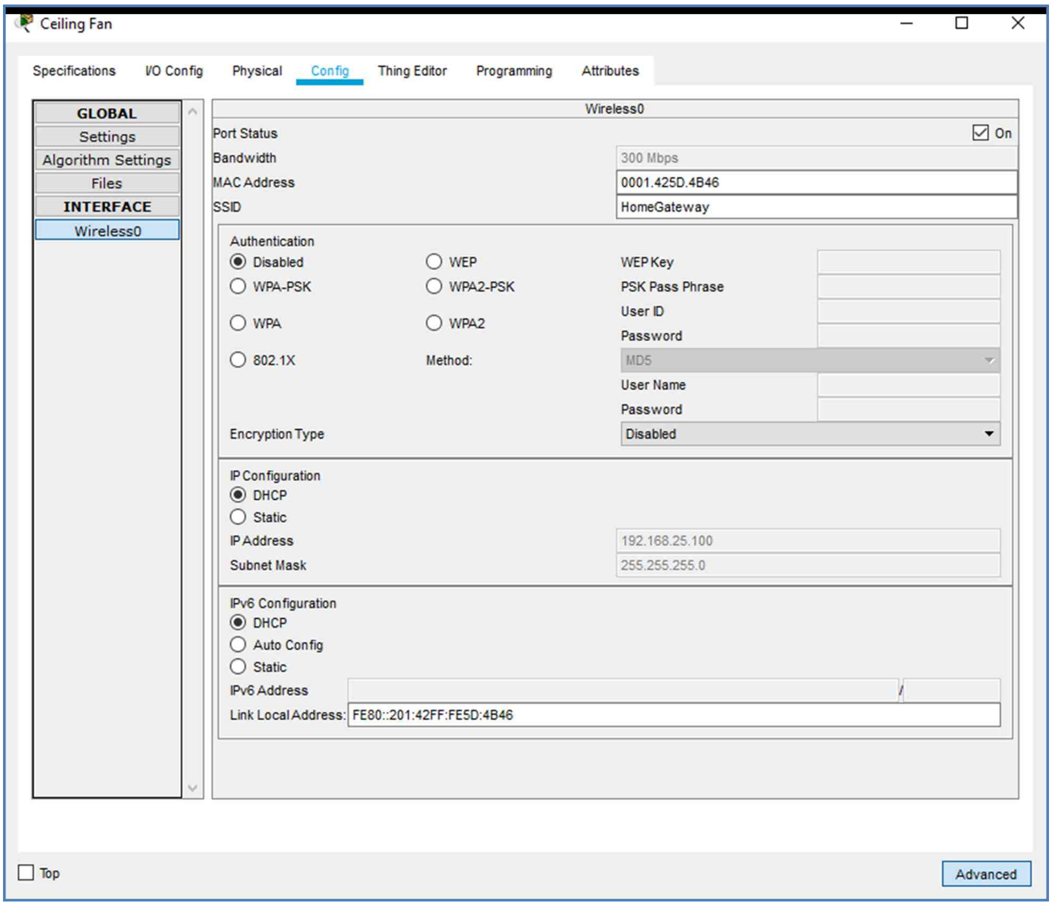


Figure 8.7: Confirming DHCP and SSID on the *Wireless0* Interface

c) **Door and Lamp**
Repeat the above steps for your **Door** and **Lamp** devices:
   i. Install the wireless adapter (`PT-IOT-NM-1W`) in the *I/O Config* tab.
   ii. Assign the same `SSID` (`HomeGateway`).
   iii. Select `DHCP` for IP assignment.
   iv. Provide a descriptive name (e.g., `FrontDoor` or `LivingRoomLamp`).

After these changes, each device should appear in the Home Gateway's device list once it successfully joins the network.

Wireless Device Setup Tips:

Checking Security Settings: If your Home Gateway uses WPA2 security with a passphrase (e.g., `mySecretKey`), ensure each device matches those settings under *Wireless0* to connect successfully.

Monitoring IP Addresses: You can verify each device's new IP address by reopening its *Config* tab or by checking the Home Gateway's interface for a device list.

Renaming for Clarity: Giving each device a unique, descriptive name (e.g., `CeilingFanBedroom`, `BackDoor`, `KitchenLamp`) will make it easier to manage in the future.

Troubleshooting: If a device fails to obtain an IP address:
- Re-check the `SSID` and passphrase.
- Ensure the Home Gateway has `DHCP` enabled for its wireless network.

- Make sure you have not exceeded the DHCP pool size.

C. Add a Wireless Tablet to the Network

In this section, you will introduce a *Wireless Tablet* to your IoT environment. The tablet will connect to the `HomeGateway` SSID via DHCP and allow you to manage and monitor your IoT devices through a web interface.

5. **Add the Tablet:**
   - In the *Device-Type Selection* box (lower-left corner), choose **End Devices**.
   - Locate the **Wireless Tablet** icon, then click inside the *Logical* workspace to place it (Figure 8.8).

Figure 8.8: Adding the Wireless Tablet to the Workspace

6. **Connect Tablet to HomeGateway:**
   a) **SSID Settings**
      - Click the **Tablet** icon in the workspace to open its configuration.
      - Go to *Config* → **Wireless0**.
      - Change the `SSID` from `Default` to `HomeGateway` (the SSID used by your Home Gateway).
      - Wait briefly for the tablet to obtain an IP address automatically from the gateway's `DHCP` server (Figure 8.9).

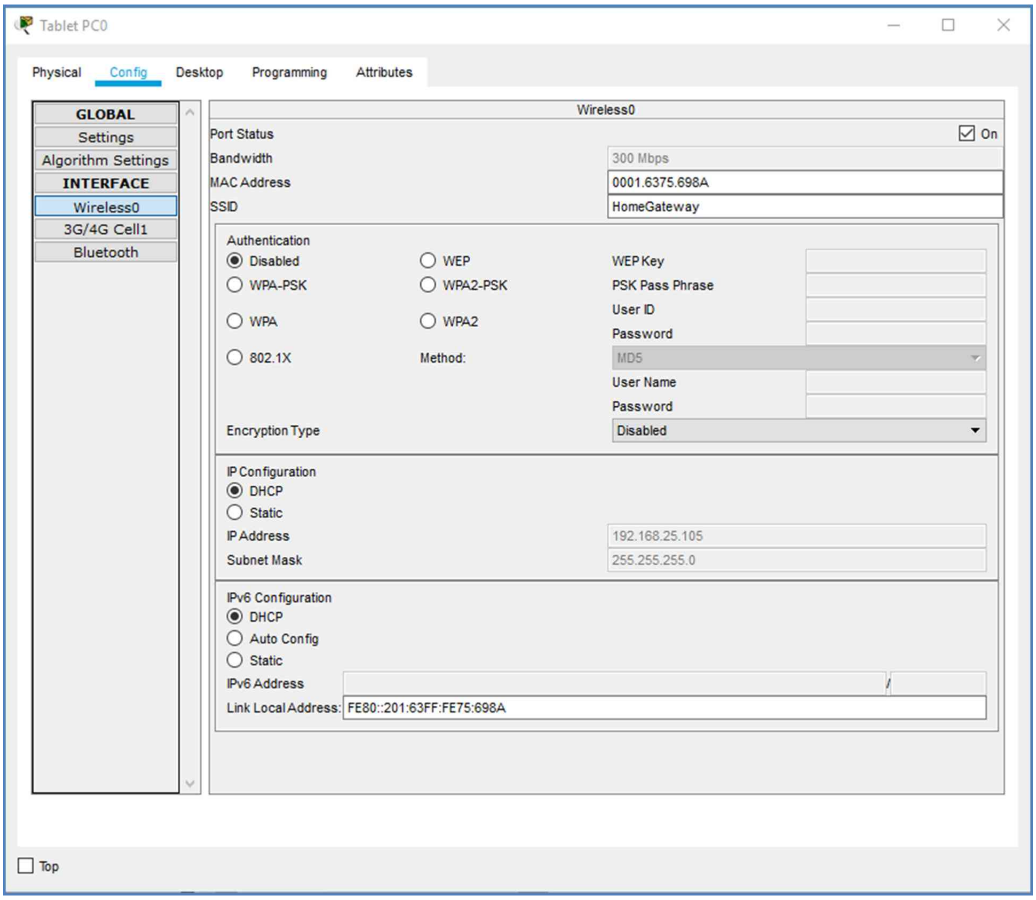


Figure 8.9: Configuring the Tablet's Wireless0 Interface for HomeGateway

b) **Home Gateway Login**

- Switch to the tablet's *Desktop* tab and open the **Web Browser**.
- In the URL field, type `192.168.25.1` (the Home Gateway's IP) and click *Go*.
- At the login screen (Figure 8.10), enter the default credentials `admin` / `admin`, then click *Submit*.
- If no devices are registered yet, the IoT Server – Devices list may be empty. You can close the tablet window or continue exploring other settings as needed.

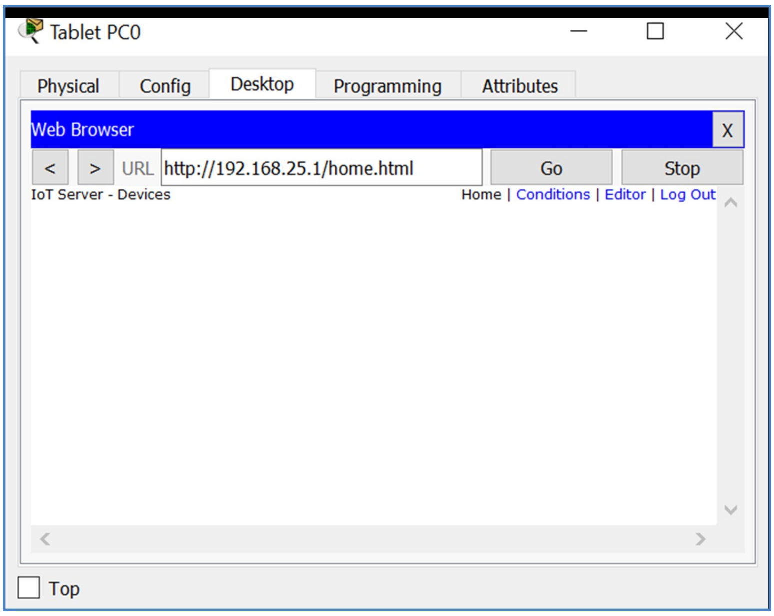


Figure 8.10: Home Gateway Login from the Tablet's Web Browser

Wireless Tablet Usage:

Check IP Assignment: After connecting, the tablet's IP should appear under *Config* → *Wireless0* or *Desktop* → *IP Configuration*. Ensure it's on the same subnet as the Home Gateway (e.g., `192.168.25.x`).

Web-Based Management: The tablet is a convenient interface for managing all connected IoT devices. Once they are registered with the gateway, you can view their statuses, toggle them on or off, and modify settings directly from the tablet's browser.

Security Considerations: If your Home Gateway uses `WPA2` or another security method, ensure the tablet matches those credentials under *Wireless0*.

Further Configuration: For advanced features (e.g., creating user accounts, setting device schedules), check additional tabs in the Home Gateway's web interface. ■

D. Register IoT Devices with the Home Gateway

Once you have configured your IoT devices (e.g., *Ceiling Fan*, *Lamp*, *Door*) to connect via wireless and obtain IP addresses (using DHCP), the final step is to "register" them with the Home Gateway. Registration allows the gateway to monitor and control each device centrally.

7. **Set Each Device to Use Home Gateway:**
   a) **Ceiling Fan**

      - Open the *Ceiling Fan* device window.
      - Navigate to *Config* → *Settings*.
      - Change the *IoT Server* selection to **Home Gateway**. This action associates the fan with the local gateway's IoT management interface (see Figure 8.11).
      - Close the Ceiling Fan window.

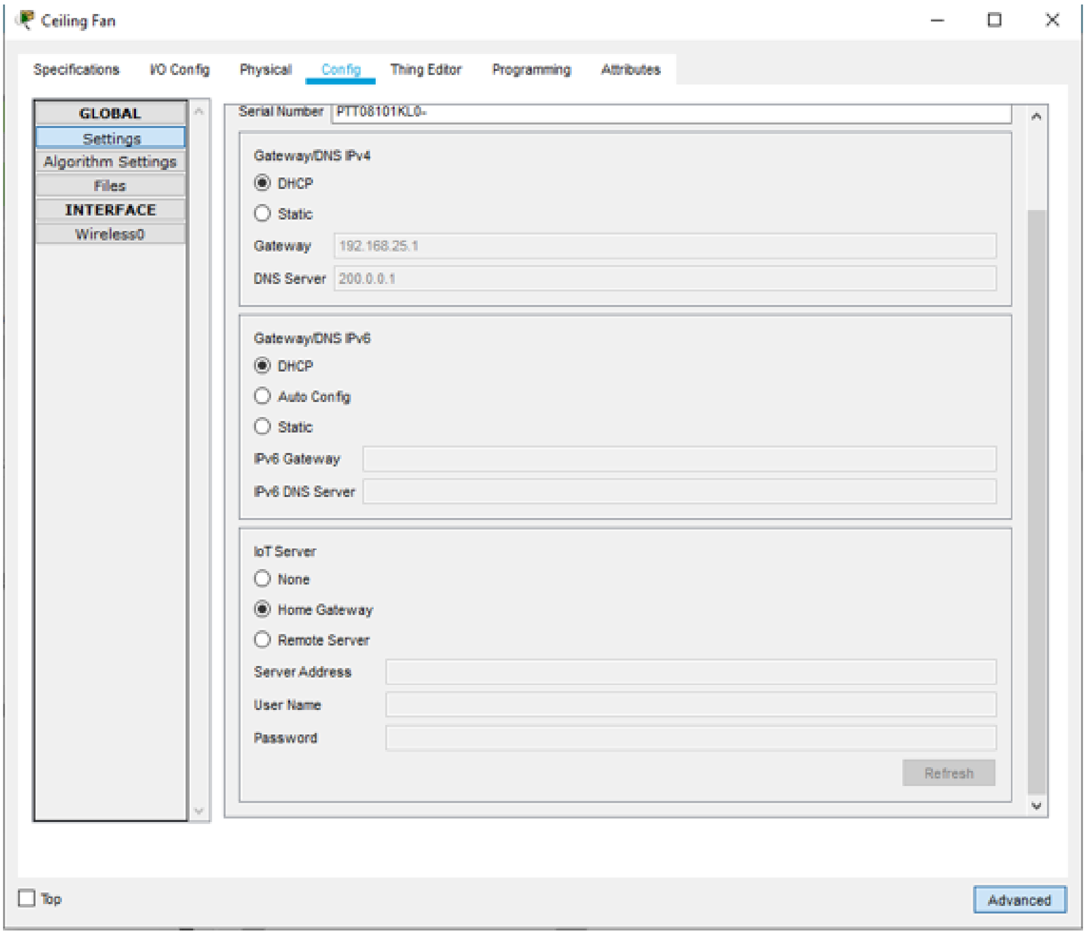


Figure 8.11: Registering the Ceiling Fan with the Home Gateway

b) **Lamp and Door**

- Repeat the same process for the *Lamp* and *Door* devices:
  i. Open each device's configuration window.
  ii. Go to *Config* → *Settings*.
  iii. Change the *IoT Server* to `Home Gateway`.

8. **Verify Registration:**
   - Return to the **Wireless Tablet**, open the *Web Browser*, and reconnect to `192.168.25.1` (the Home Gateway IP).
   - Log in with the default credentials `admin/admin`.
   - After a brief moment, you should see the **Ceiling Fan**, **Door**, and **Lamp** listed under the *IoT Server – Devices* section, indicating successful registration (Figure 8.12).

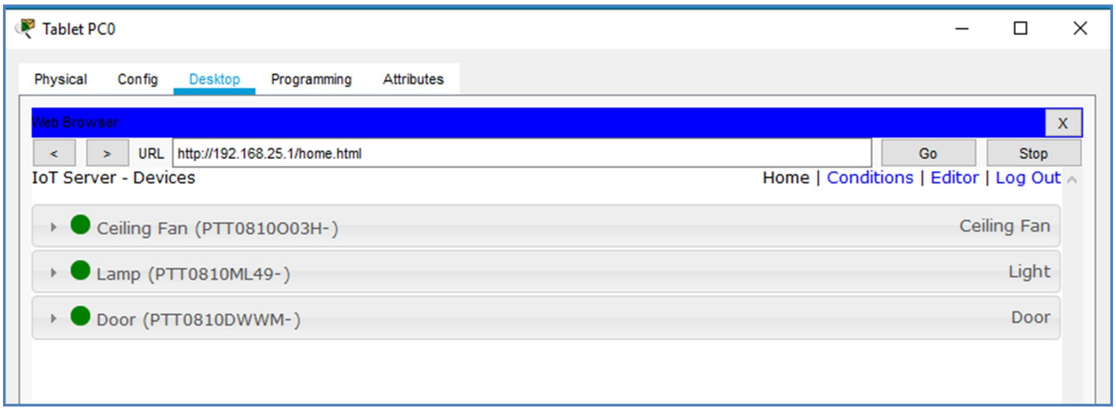


Figure 8.12: Home Gateway Server Showing All Registered IoT Devices

Verifying Connectivity:

If your devices do not appear, ensure they have:

- The correct `SSID` (`HomeGateway`) and matching security settings.
- An IP address obtained via `DHCP` (check *Config* → *Wireless0*).
- Time to fully register; sometimes a short delay is normal before the gateway updates.

You can also open the *Command Prompt* on the tablet's *Desktop* and use `ping <Device-IP>` to confirm connectivity if you know each device's IP address.

Measuring Success — Lab 8: Connect and Monitor IoT Devices

- The **home gateway** appears on the network with green link lights and obtains correct IP details from the cable modem.
- Your **Ceiling Fan**, **Door**, and **Lamp** successfully connect via wireless and register with the home gateway, each showing a valid DHCP IP.
- The **tablet** or end-user device receives an IP address from the home gateway network and can **log in** to the gateway's web interface.
- All **IoT devices** appear in the gateway's *IoT Server – Devices* list, allowing remote monitoring and control.
- You can toggle or view statuses (e.g., power on/off) of each IoT device from the tablet's web browser, confirming the entire smart home network is functional.

— Further Exploration

LAB 8.1 - Connect to a Home Gateway and Monitor Network

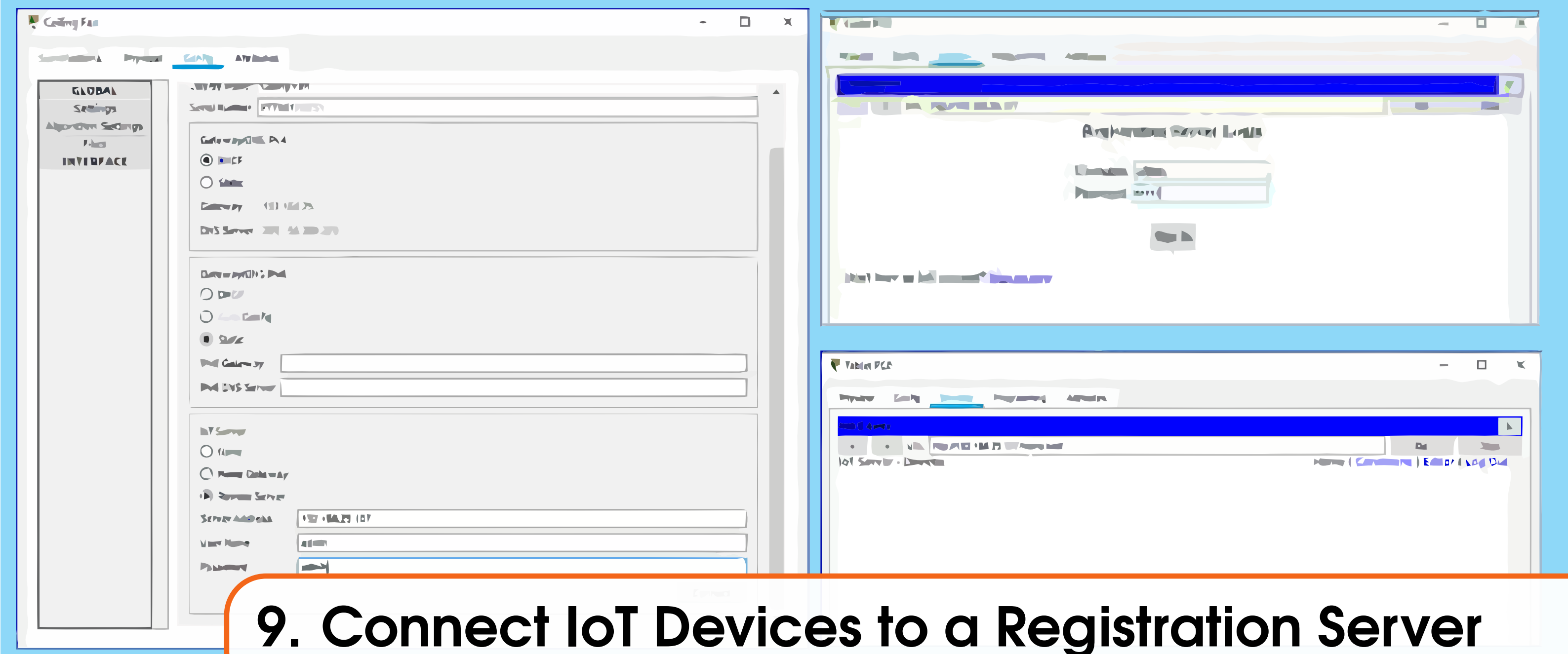
In this activity, you will add a home gateway and several IoT devices to an existing home network and monitor them through the home gateway.

- 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 (e.g., PCs, 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 (wirelessly or wired) and setting them up for proper communication with the network.
- Pair Bluetooth devices by enabling Bluetooth, making them discoverable, and connecting

> them through the network's Bluetooth settings.

Summary

In this lab, you successfully connected a **home gateway** to a cable modem, configured multiple *IoT devices* for wireless access, and added a *tablet* to manage the entire environment. By registering each device with the home gateway, you confirmed they appear in its **IoT Server** list and can be remotely monitored or controlled. This foundational setup prepares you for more advanced IoT labs involving remote servers or additional sensors in your smart home network.



9. Connect IoT Devices to a Registration Server

Introduction

In this lab, you will learn how to **register IoT devices** with a **dedicated Registration Server**, enabling *centralized control* and *monitoring* of smart devices. You will configure a remote server, connect new devices, and ensure they properly integrate into the existing network. By the end of this lab, you should be able to manage and monitor your IoT devices through a server rather than a local home gateway.

Objectives

- Configure IoT devices to register with a **remote server**, enabling centralized control and monitoring of smart devices.
- Set up and manage a **dedicated registration server**, exploring its configuration options and 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 the registration server, ensuring proper integration and operation within the network.

Background

Beyond using a local home gateway, **IoT devices** can also register with a *dedicated Registration Server* for remote monitoring, configuration, or programming. This approach offers broader network services (e.g., Web, DHCP, DNS, email, FTP) on the same server. Devices connect to the wireless or wired network, then register to the server, which can even reside offsite. This setup reflects many real-world smart homes, allowing homeowners to control devices over the internet.

Key Points:

- A dedicated server can sit on the home LAN or beyond (internet).
- The server must be *online*, with relevant services (*IoT*) turned on.
- Devices register by specifying the server's IP address and authentication credentials.

- A remote client (tablet, PC, smartphone) logs into the same server to monitor or configure these devices.

The following steps will demonstrate how to:

- Connect and configure the registration server.
- Register IoT devices to the server (instead of a home gateway).
- Verify that all devices show up in the server's IoT management interface.

> **Resources — Registering Devices to a Dedicated Registration Server | .** Learn how to create and control a small IoT home network by switching from a local home gateway to a dedicated registration server. We will integrate IoT devices for remote access and centralized management.

The Smart Home Network

Figure 9.1 shows a sample **Smart Home Network** where you will add a registration server and new IoT devices.

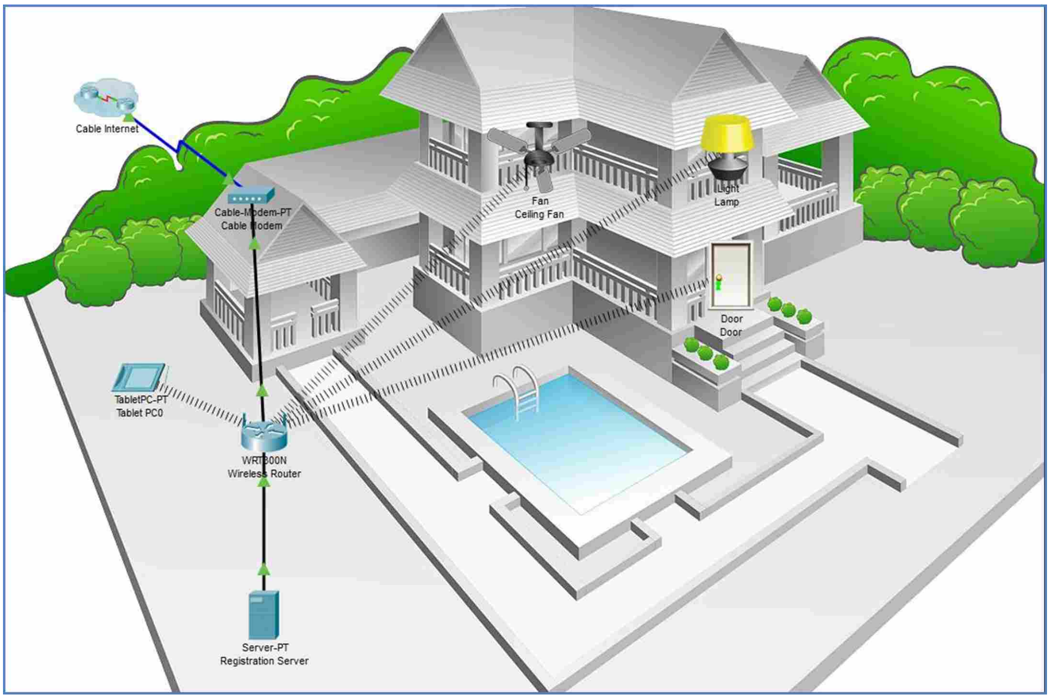


Figure 9.1: Smart Home Network with Proposed Registration Server

Lab Plan

A. **Add a Registration Server to the Network**
B. **Register IoT Devices to the Registration Server**

Scenario

You will integrate a **registration server** into an existing home network and configure several IoT devices so that they register and report to the server. This approach allows *centralized monitoring and control* of all IoT devices.

A. Add a Registration Server to the Network

In this section, you will introduce a dedicated *Registration Server* into your smart home or IoT network. This server will allow you to centralize control and monitoring of your IoT devices, rather than relying on a local home gateway for registration.

1. **Open the** `Registration_Server.pkt` **File:**
   - Launch Cisco Packet Tracer and locate the file named `Registration_Server.pkt`.
   - Go to `File` → `Save As` and store a new copy locally, for example `RegistrationServer_Lab9.pkt`. This preserves the original file for future reference.
2. **Place the Server in the Logical Workspace:**
   - In the lower-left panel, select **End Devices**.
   - Locate the **Server** icon and drag it into your *Logical* workspace (see Figure 9.2 for an example).

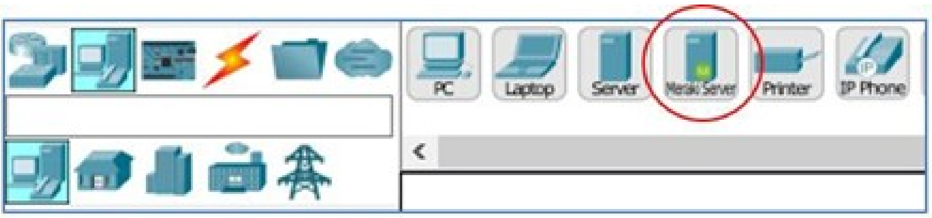


Figure 9.2: Adding the Server from End Devices

3. **Connect the Server to the Wireless Router:**
   - Use a **Copper Straight-Through** cable to connect the server's `FastEthernet0` port to a *LAN* port on the wireless router.
   - After a brief moment, you should see a green link light on each end, indicating an active connection.
4. **Enable the IoT Registration Service:**
   - Click the server to open its configuration window, then switch to the *Services* tab.
   - Select **IoT** from the left pane, and click the "**On**" button to activate it (Figure 9.3).

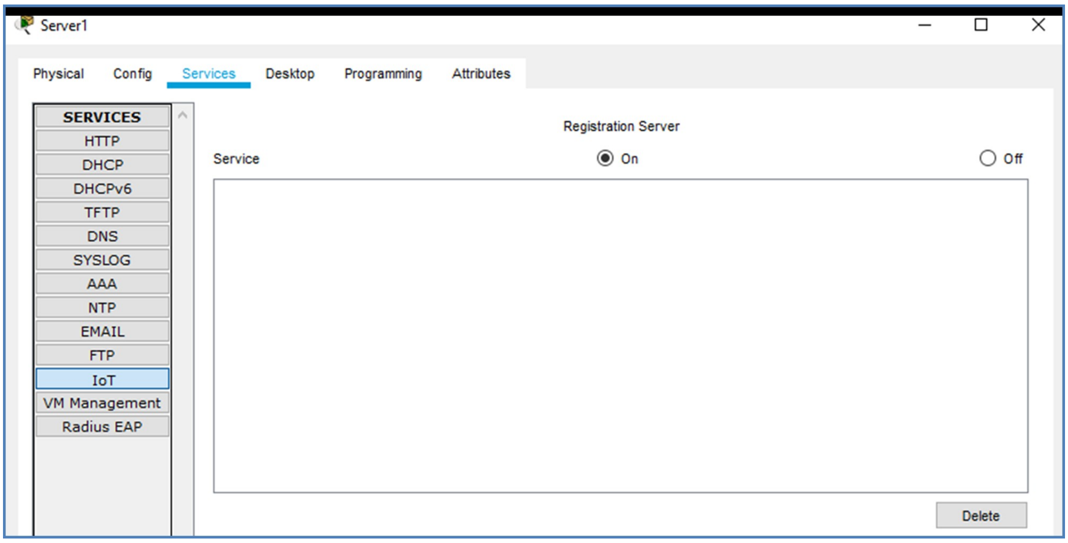


Figure 9.3: Turning On the IoT Service on the Server

5. **Configure the Server Settings:**

- Move to the *Config* tab in the server's window.
- Under *Global Settings*, rename the device to something like `Registration Server` for clarity.
- For `DHCP/DNS IPv4`, choose `DHCP` so this server automatically obtains an IP address from the router.

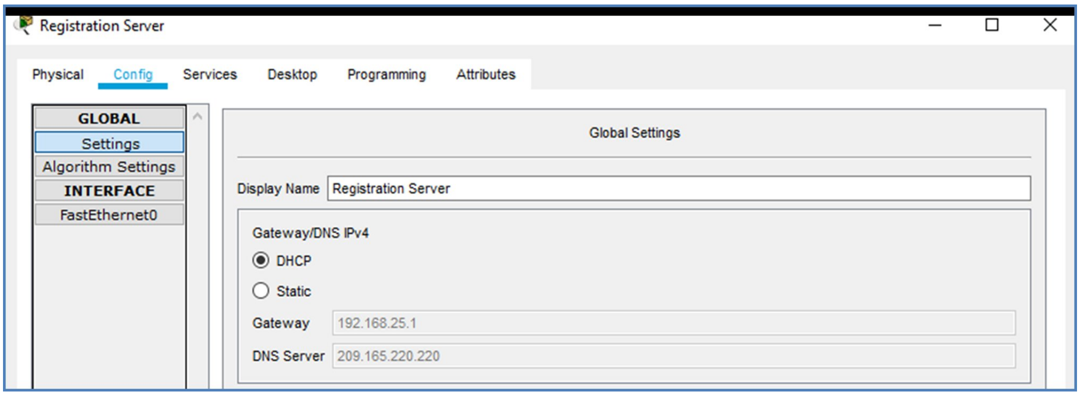


Figure 9.4: Renaming and Setting Server to Obtain IP via DHCP

6. **Check the Assigned IP:**
   - Click on the *Desktop* tab, then select *IP Configuration*.
   - Confirm that the server has acquired a valid IP (e.g., `192.168.25.107`) from the DHCP pool (Figure 9.5).

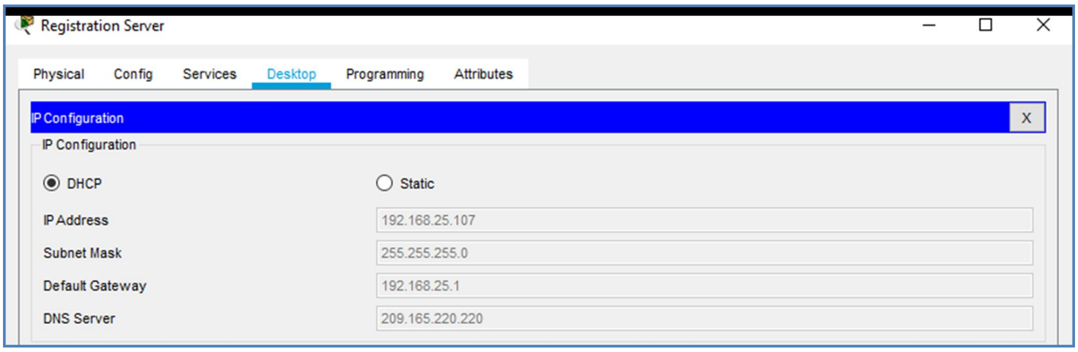


Figure 9.5: Server Obtaining an IPv4 Address from DHCP

7. **Close the Server Window**
   - You can now close the server's configuration window. Your *Registration Server* is ready for IoT devices to register with it, rather than a local gateway.

Notes on Registration Servers:

Centralized Management: This setup allows you to manage all IoT devices from a single location, which is particularly useful for larger networks or multi-site deployments.

Additional Services: In Packet Tracer, you can also enable other services (like `DNS`, `DHCP`, or `HTTP`) on the same server, making it an all-in-one solution.

IP Conflicts: If the router is also providing DHCP to other devices, ensure your server does not inadvertently run its own DHCP server in a conflicting pool (unless intentionally designed).

Security Configurations: Later, you can customize authentication (usernames and passwords), or even secure communication channels, for more realistic IoT deployments.

B. Register IoT Devices to the Registration Server

In this section, you will create a user account on the *Registration Server* and switch your IoT devices from using a local Home Gateway to registering with the `Remote Server`. This setup allows for centralized device management and monitoring in larger or more distributed networks.

8. **Create an Account on the Registration Server:**
   - Open the **Tablet**, then go to *Desktop* → *Web Browser*.
   - Enter the server's IP address (e.g., `192.168.25.107`) in the URL field and click **Go**.

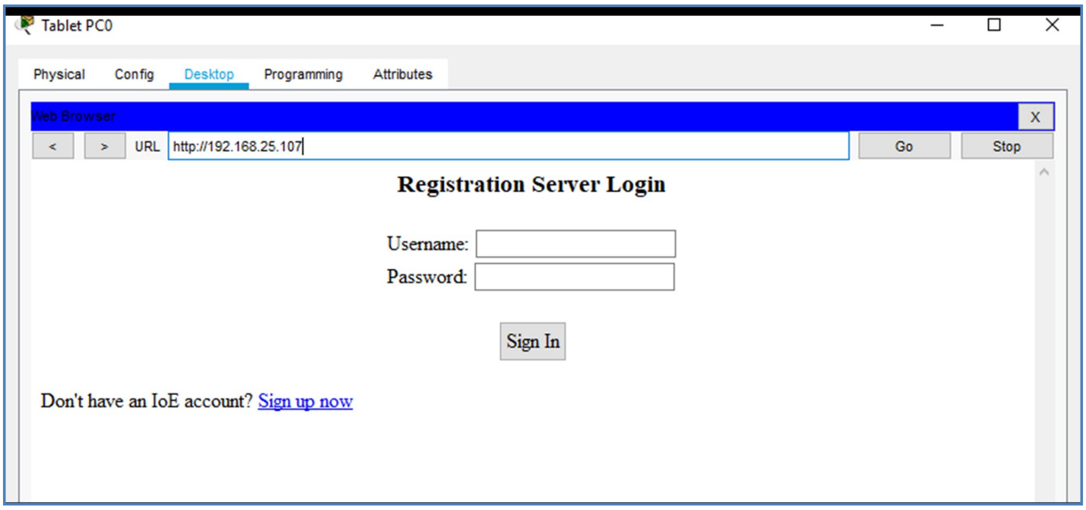


Figure 9.6: Initial Registration Server Login Page

   - If prompted, select **Sign Up Now** to create a new IoT user account.
   - Provide a *Username* and *Password*, then click **Create**.
   - After creating your account, you should be returned to the login or main IoT screen.

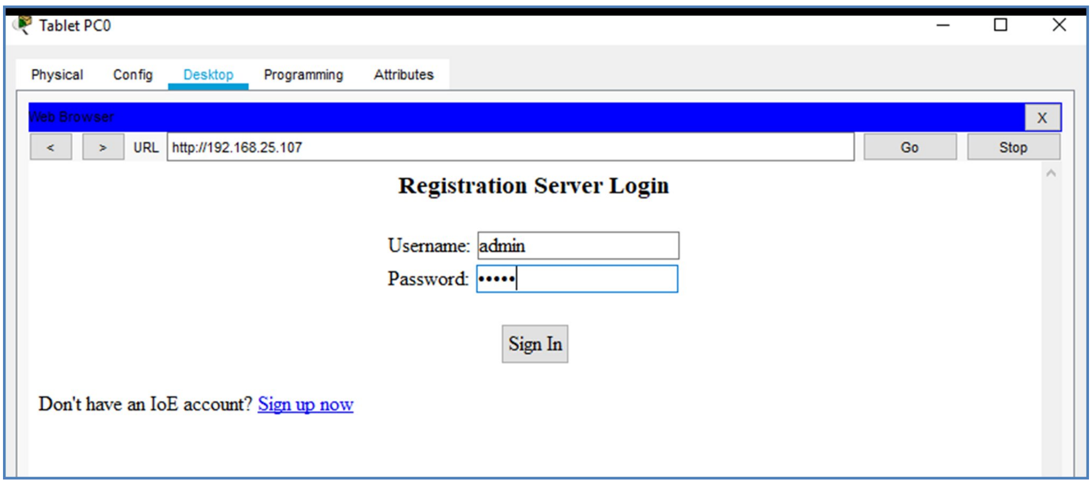


Figure 9.7: Creating an IoT Account on the Registration Server

9. **Verify No Devices Are Registered Yet:**

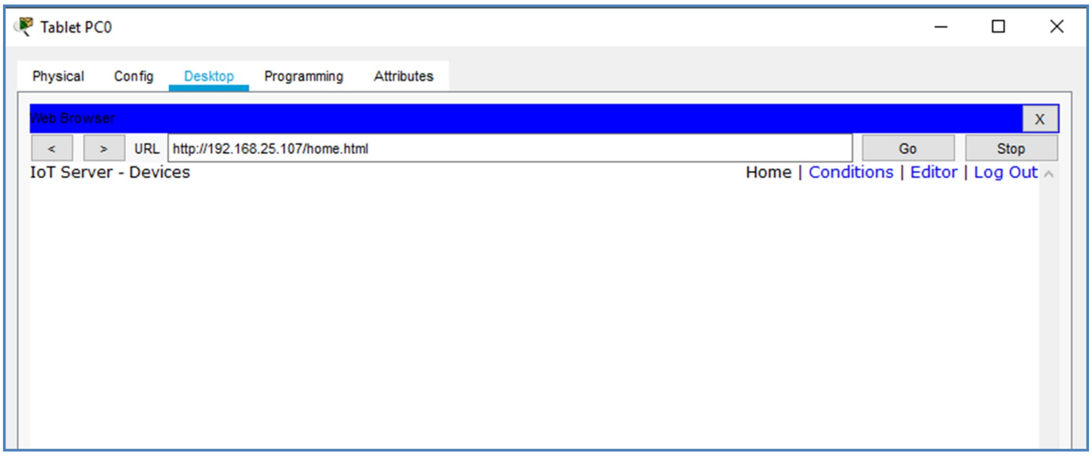


Figure 9.8: IoT Server — No Devices Listed Yet

Home Gateway vs. Remote Server:
If you see a "Home Gateway" device in your network, note that any IoT devices associated with the Home Gateway will *not* appear under the Registration Server until you reconfigure them to use "Remote Server" instead.

10. **Configure IoT Devices to Use the Registration Server:**

    - For the **Ceiling Fan**, open its configuration window. Go to *Config* → *Settings*, and set `IoT Server` to **Remote Server**.
    - Enter the `Registration Server` IP (e.g., `192.168.25.107`) and the **Username/-Password** you just created.
    - Click **Connect** or **Refresh** to initiate registration (Figure 9.9).

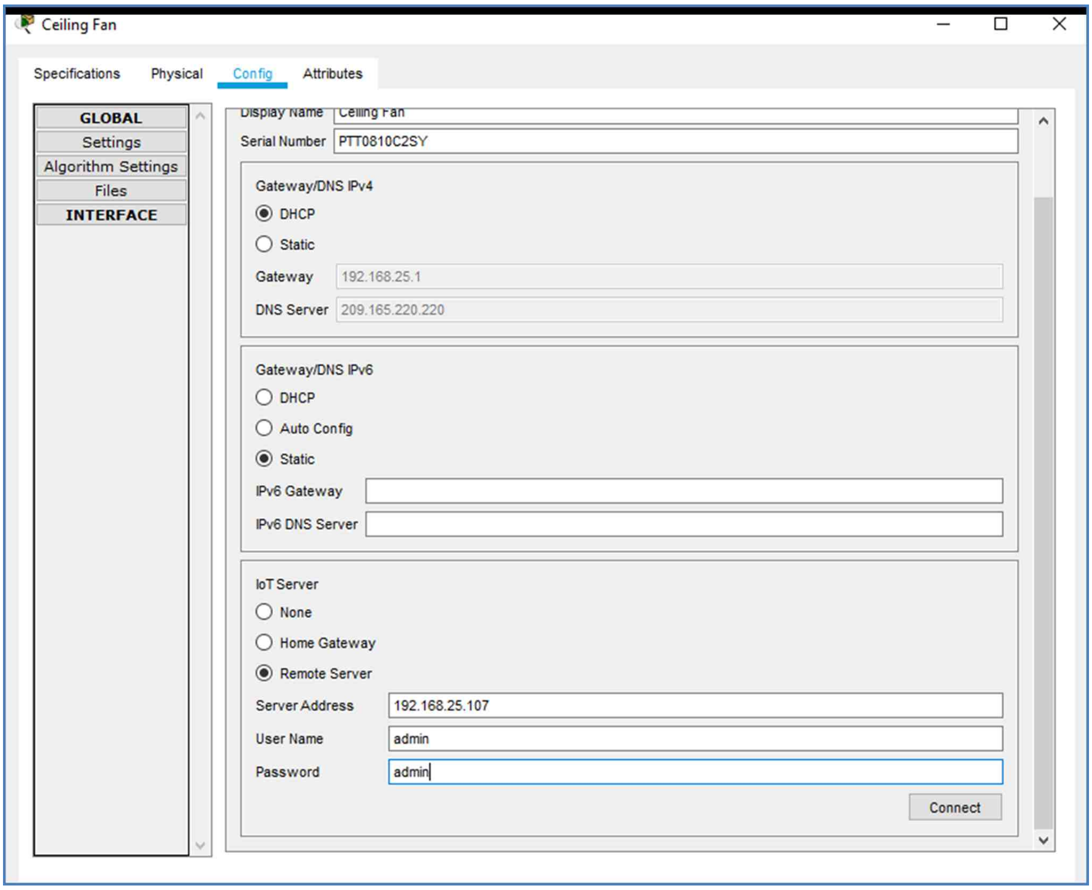


Figure 9.9: Registering the Ceiling Fan with the Remote Server

- Repeat these steps for any additional devices (e.g., **Lamp**, **Door**), making sure to switch from "Home Gateway" or "None" to `Remote Server`, with correct credentials.

11. **Verify IoT Devices on the Registration Server:**
    - Return to the **Tablet**, open the `Web Browser`, and log in again with the same IP and credentials.
    - After a short delay, your newly registered devices (**Ceiling Fan**, **Lamp**, **Door**, etc.) should appear in the IoT Server **Devices** list (Figure 9.10).

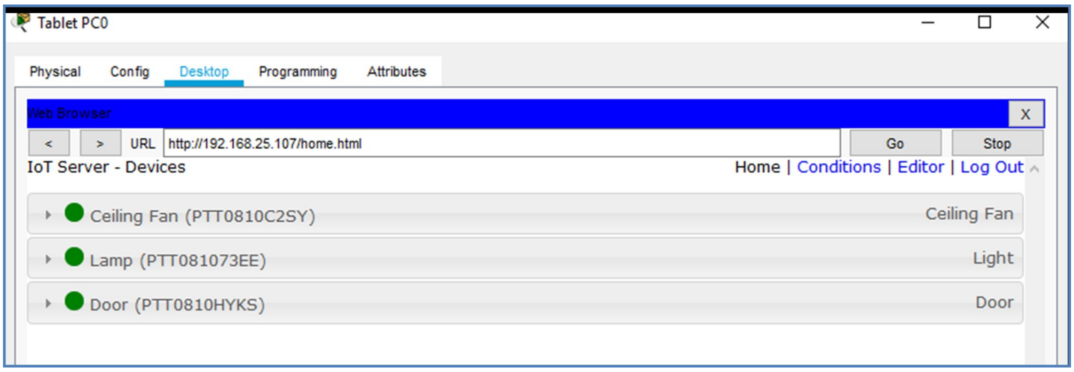


Figure 9.10: Newly Registered Devices Showing in the IoT Server List

Troubleshooting Device Registration:

If no devices appear, verify:

- **Correct Server IP**: Ensure you typed the right IP address of the Registration Server.
- **Credentials**: Double-check your username and password.
- **Wi-Fi Connectivity**: Confirm each IoT device is still connected to the correct SSID and has a valid IP address.
- **Refresh Delay**: Sometimes devices take a few seconds to show up; click **Refresh** if available.

12. **Close Packet Tracer:**
    - After confirming all IoT devices appear in the remote server's management page, you can either close Packet Tracer or keep exploring features such as remote device control, scheduling, or sensor data collection.

Measuring Success – Lab 9: Connect IoT Devices to a Registration Server

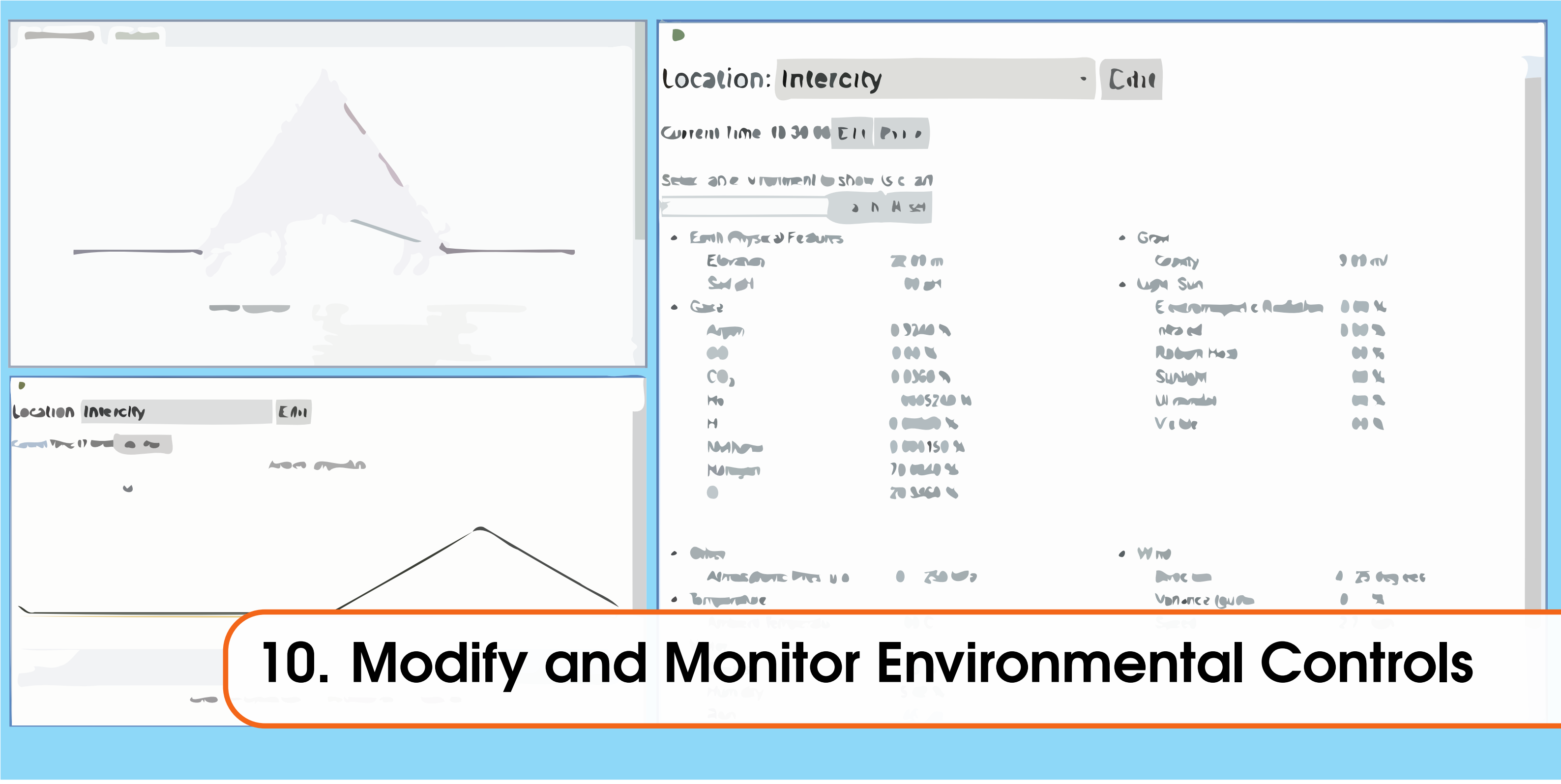
- The **Registration Server** is placed on the network, obtains an IP address (DHCP or Static), and *IoT Service* is turned **On**.
- A new **IoT account** is created from the tablet/PC browser, ensuring successful communication between the server and remote device.
- **Ceiling Fan**, **Lamp**, and **Door** switch from Home Gateway registration to **Remote Server** with correct IP, username, and password.
- All **IoT devices** appear in the *IoT Server* device list, confirming successful integration with the remote server.
- You can log in again from the tablet/PC to see or control the registered devices, validating the entire remote-connection flow.

— Further Exploration

- **Multi-Server Designs:** Place a second registration server on a different network to explore cross-network IoT device registration.
- **Security Enhancements:** Enable advanced authentication or encryption if the server supports it.
- **Scaling Up:** Add more devices or services (FTP, DNS) to the same server to simulate real-world IoT aggregator scenarios.

Summary

You successfully deployed a dedicated **Registration Server** in an existing smart home network, switched devices from local gateway registration to *Remote Server*, and verified they appeared in the server's IoT management interface. This setup is crucial for real-world IoT ecosystems, where multiple devices are centrally managed and accessible via the internet.



10. Modify and Monitor Environmental Controls

Introduction

In this lab, you will learn how to **modify and monitor environmental controls** within Cisco Packet Tracer's Physical workspace. You will explore built-in *environmental elements* (e.g., temperature, sun, humidity) and see how to adjust them in different containers (intercity, cities, buildings, wiring closets). By the end, you should understand how *environmental sensors* and *actuators* respond to these conditions, allowing you to create and test automated reactions (e.g., turning on a fan when temperature reaches a threshold).

Objectives

- Learn to **modify and monitor** environmental controls in Packet Tracer's Physical view to simulate smart homes or buildings.
- Experiment with setting up and adjusting **sensors and actuators** to react to changes (temperature, light, humidity).
- Configure and test **automated responses** (e.g., fan activation, light-level adjustment) based on sensor readings.
- Use IoT platforms and software tools to **remotely monitor and control** environmental conditions in a simulated environment.

Background

Cisco Packet Tracer's *Physical Workspace* includes a robust **environmental system** that simulates day/night cycles, weather elements, and other conditions. Each *container* (e.g., intercity, city, building, wiring closet) has **24 default environmental elements** such as temperature, humidity, rain, wind, and more. Devices can *affect* or *respond to* these elements. For instance:

- A **Fire Sprinkler** will raise the water level and humidity in a container.
- An **Old Car** increases ambient temperature and various gas emissions when turned on.
- A **Smoke Detector** can trigger alarms if the smoke element surpasses a certain threshold.

By default, these environmental elements follow a *24-hour cycle* (e.g., sun rises at 6 AM, sets at

6 PM). You can override or adjust these values via the **Environment** button in the Physical view. Here's how it works:

- A child container (e.g., a building) *inherits* baseline conditions from its parent (e.g., the city).
- Changes in a child container do *not* affect the parent, but the child eventually *converges* back to the parent's baseline (via **transference**).
- **Transference rates** define how quickly child environments revert to or diverge from their parent's environment.

> **Resources — Environmental Controls in Packet Tracer | .** Explore Packet Tracer's environmental features: see how to modify elements like temperature or humidity, set conditions and triggers, and watch IoT devices respond within each container's environment.

Key Environment Terminology

- **Current Time:** Inside a container, time increments in 30-minute steps. One real second = 30 container-minutes, cycling from 0 (midnight) to 11:59.
- **KeyFrame:** A single moment in the 24-hour day used to set or view an environmental value.
- **KeyFrame Graph:** A graph of how environmental elements (e.g., temperature) vary throughout the cycle.
- **Transference:** Dictates how a child container's environment converges with or drifts from its parent container's baseline.

Lab Plan

A. **Explore Environmental Controls**
B. **Edit Environment Elements**

A. Explore Environmental Controls

In this section, you will learn how to view and analyze the environmental elements (such as temperature, humidity, rain, and wind) that Packet Tracer can simulate in its **Physical** workspace. These environmental controls let you create realistic weather or climate conditions for testing IoT devices that react to changes in temperature or humidity.

1. **Open the** `PT_Environmental_Controls.pkt` **File:**

   - Launch *Cisco Packet Tracer* and open the file `PT_Environmental_Controls.pkt`.
   - Immediately perform a `File` → `Save As` to create a working copy, for example `Env_Controls_Lab10.pkt`. This preserves the original file and lets you freely experiment with changes.

2. **Switch to Physical View:**
   At the top-left corner of the Packet Tracer interface, locate and click the **Physical** view icon. By default, Packet Tracer launches in **Logical** view (see Figure 10.1).

Figure 10.1: Switching to Physical View in Packet Tracer

3. **Open the Environments Window:**
   Once in **Physical** view, locate the **Environment** button on the far-right side of the toolbar, as shown in Figure 10.2. Click it to open the Environment panel.

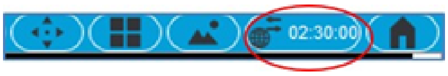


Figure 10.2: Accessing the Environment Panel

4. **Explore Intercity Environmental Elements:**
   You should now see a panel displaying the environment settings for the **Intercity** level (Figure 10.3). Scroll through the list to see various elements like temperature, humidity, rain, and wind speed. These elements influence the climate conditions within this top-level container.

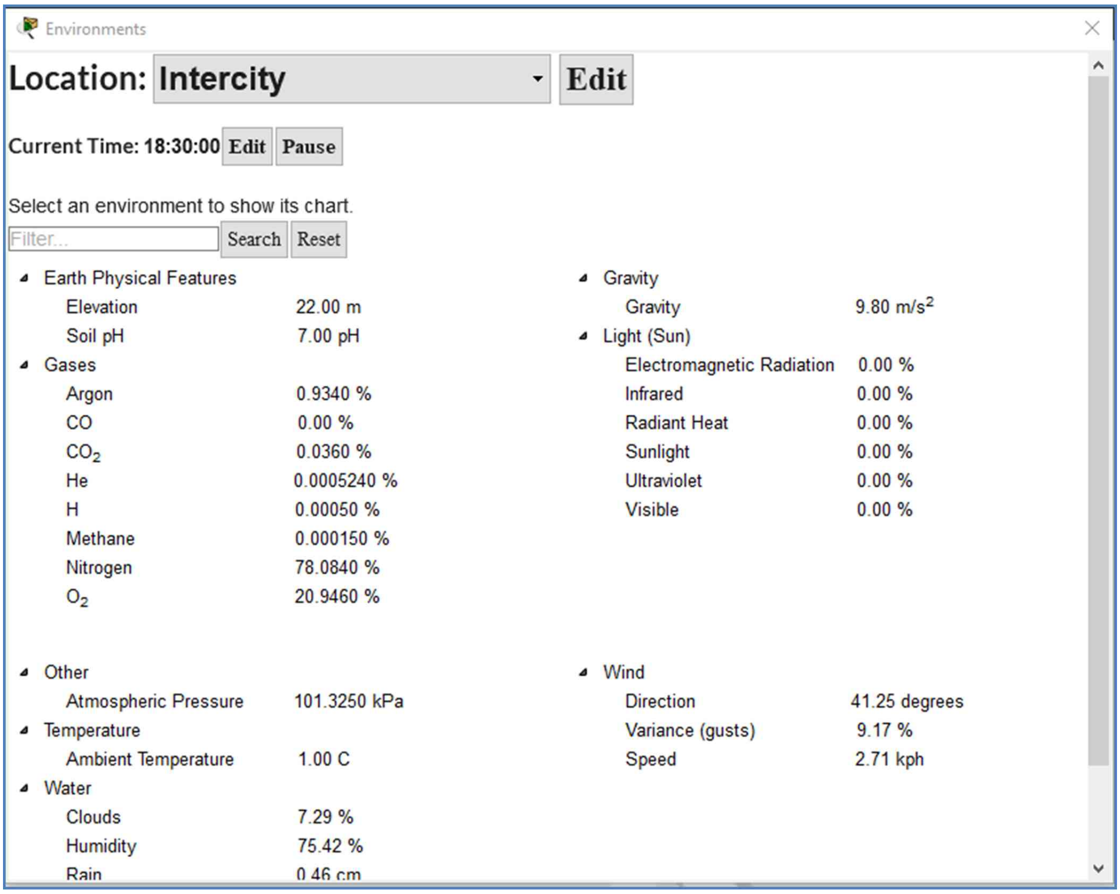


Figure 10.3: Viewing Environmental Elements for Intercity

5. **Check Ambient Temperature Chart:**
   Look for *Temperature*, specifically *Ambient Temperature*, to view a chart showing daily temperature changes (Figure 10.4). Each 24-hour cycle has keyframes that define temperature highs and lows throughout the day.

Figure 10.4: Ambient Temperature in the Intercity Container

6. **Observe Temperature Fluctuations:**
   If you let the simulation run for a few minutes, you can monitor how the ambient temperature changes over the 24-hour cycle (Figure 10.5). Packet Tracer updates these graphs in real time.

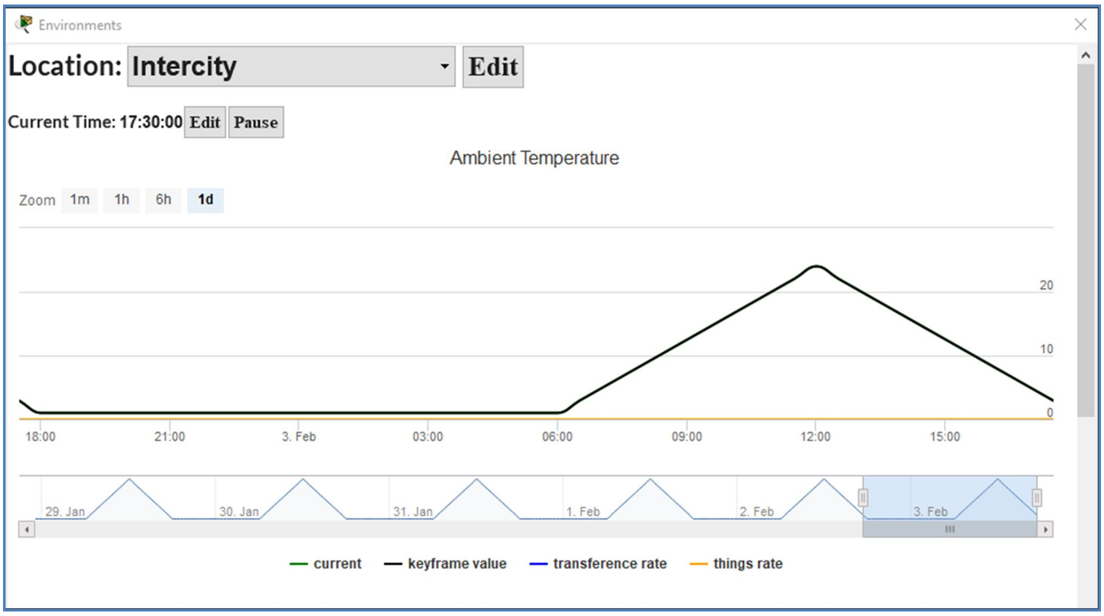


Figure 10.5: Chart Illustrating Temperature Fluctuations Over Time

Managing Time and Data Updates:

Realtime vs. Simulation Mode: Environmental data typically updates in **Realtime** mode. You can use **Simulation** mode to slow or pause network traffic, but the environment animations and cycles may not progress in the same way as in Realtime.
Rapid Day/Night Cycles: If you want to watch how an entire day of temperature changes occurs more quickly, speed up the simulation clock or advance time to see how your IoT devices might respond to temperature swings.
Container Inheritance: Remember that environments in child containers (e.g., a city or a building) inherit baseline values from their parent (*Intercity*), so changes at the top level filter down, although child containers can have *local overrides*.

B. Edit Environment Elements

In this section, you will modify specific environmental elements (e.g., temperature, humidity) within the **Physical** workspace by using the Keyframe Graph. This allows you to simulate different weather or seasonal patterns (like a hot summer day) and see how your IoT devices might respond to the changes.

7. **Enter Environment Edit Mode:**
   In the *Environments* panel for **Intercity**, click the **Edit** button. This opens a *Keyframe Graph*, where you can adjust environmental values across a 24-hour cycle (Figure 10.6).

Figure 10.6: Selecting **Edit** for the Intercity Environment

8. **Explore the Keyframe Graph:**
   A timeline appears with multiple lines representing different environmental variables (Figure 10.7). Each line has keyframes that define the value of that variable at specific times of day.

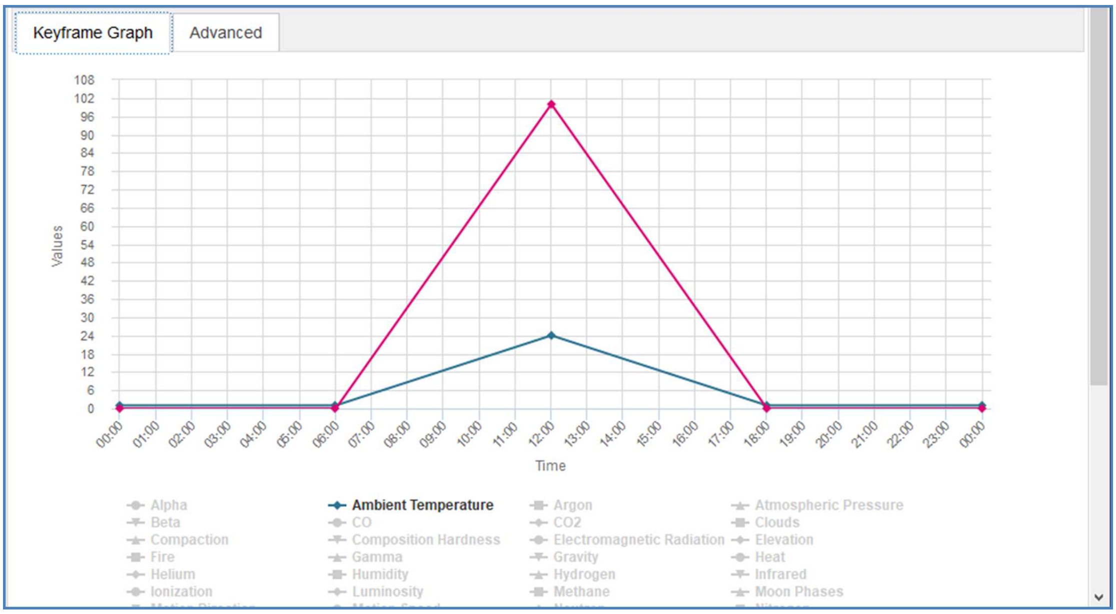


Figure 10.7: **Intercity** Keyframe Graph for Environmental Elements

9. **Adjust Ambient Temperature Curve:**
   If you want to simulate a warm summer day, you can click and drag the temperature keyframes to set approximate values like:
   - **00:00 (midnight)**: 20°C
   - **06:00**: 28°C
   - **12:00 (noon)**: 37°C
   - **18:00**: 28°C
   - **23:59 (night)**: 20°C

   Figure 10.8 shows how you might raise the temperature profile for a hotter scenario.

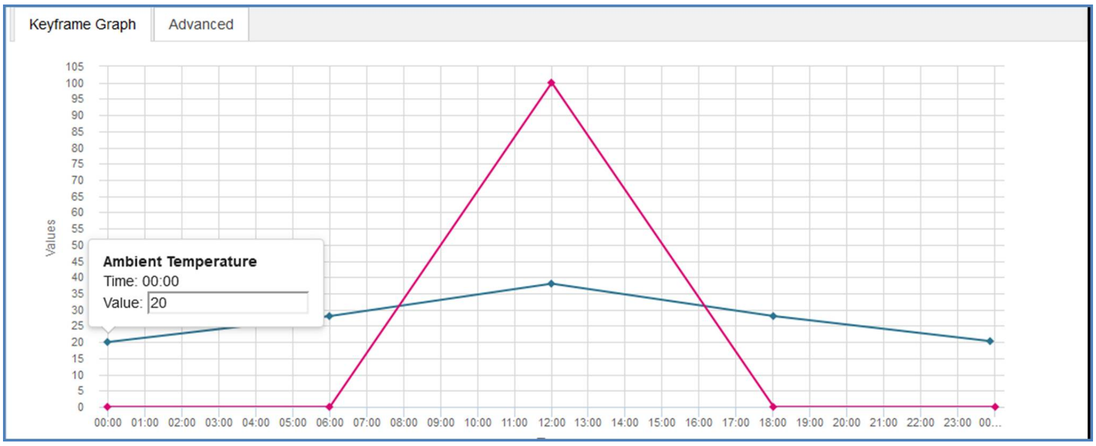


Figure 10.8: Raising Temperature Values for a Summer Scenario

10. **Return to Viewing Mode:**
    When you finish adjusting values, click the **View** button (Figure 10.9) to exit Keyframe editing and return to the standard environment view.

Figure 10.9: Switching Back to **View** Mode

11. **Verify the Updated Temperature Graph:**
    The *Ambient Temperature* chart now reflects the changes you made, displaying a hotter day profile (Figure 10.10). Over time, Packet Tracer will cycle through these keyframes, simulating the temperature fluctuations you set.

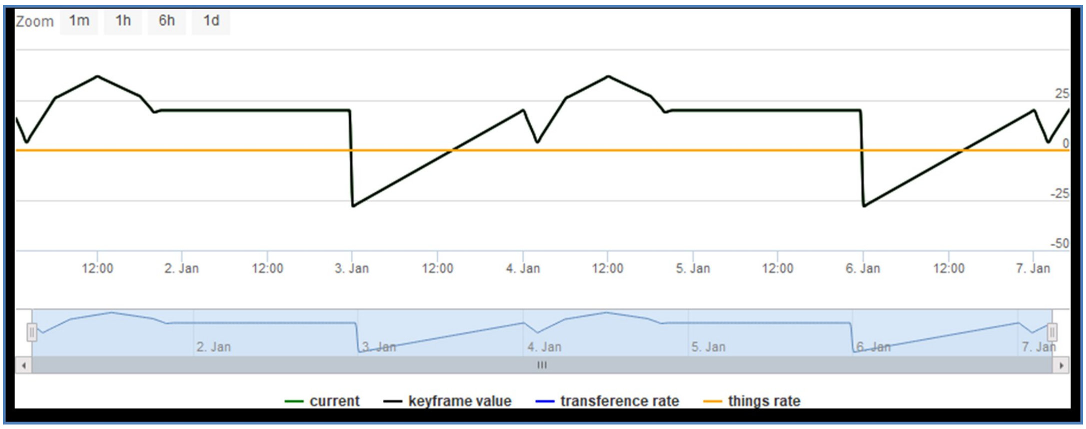


Figure 10.10: Updated Temperature Graph Reflecting Edits

12. **Additional Figures for Environment Details:**
    Packet Tracer also provides more visual aids (Figures 10.11–10.13) to help you understand how environment data is tracked:

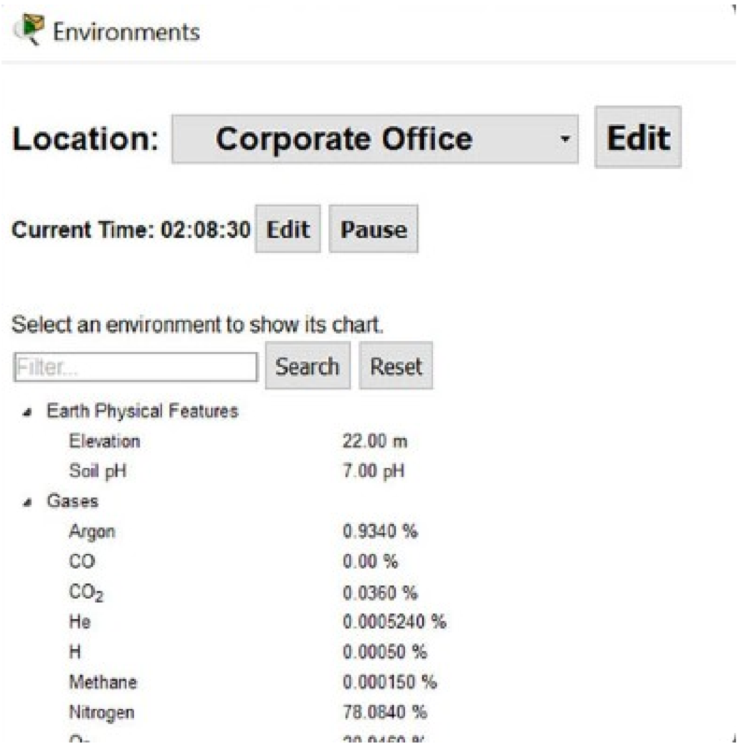


Figure 10.11: Current time

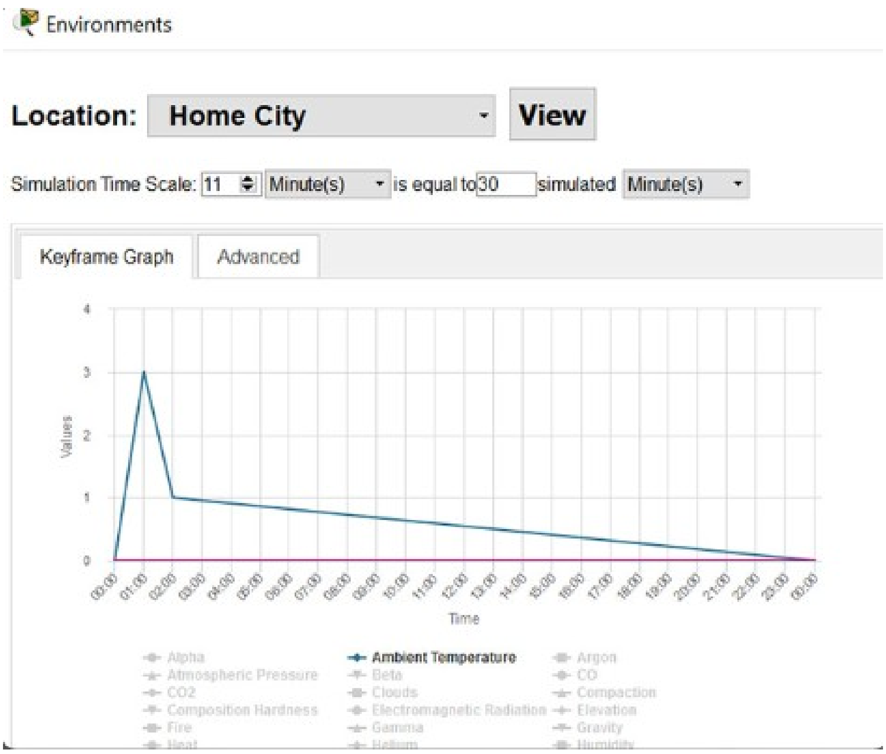


Figure 10.12: KeyFrame graph

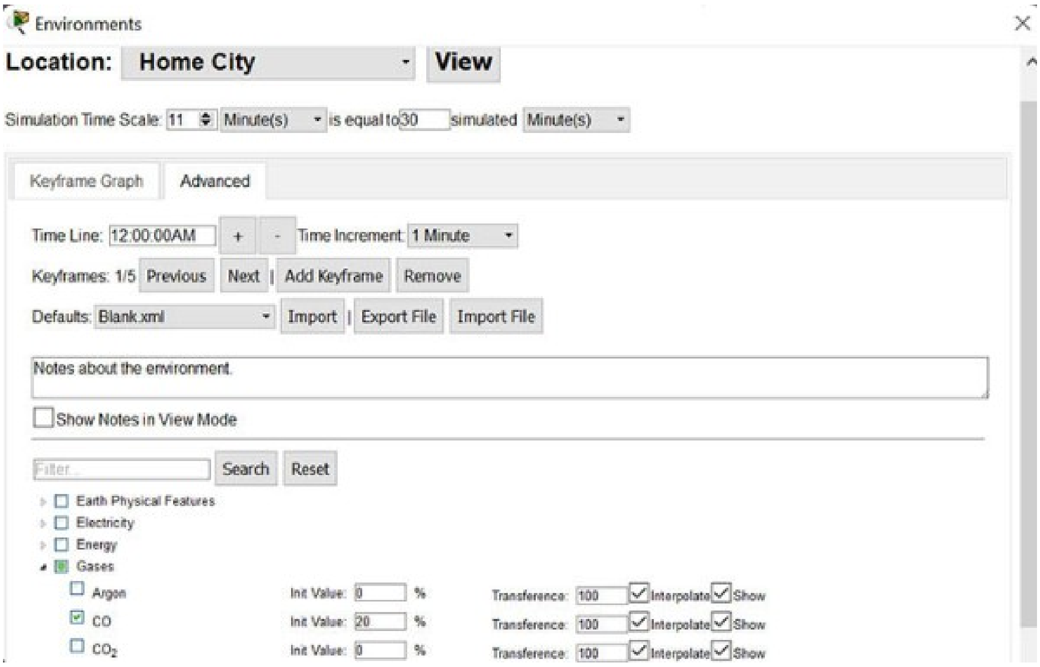


Figure 10.13: Advanced tab

Editing Environmental Elements:

Practice Various Scenarios: Try lowering temperatures to simulate winter, or adding extra wind/rain in the Keyframe Graph to test how devices respond to storms.

Child Containers Inheritance: Remember that changes made at **Intercity** level can trickle down to child containers (cities, buildings). If you want local conditions (e.g., a warmer building interior vs. outdoor temperature), edit the child container directly or override specific elements.

Save Frequently: Environmental settings can be complex. Save your Packet Tracer file often in case you want to revert to an earlier climate profile. ■

Measuring Success

- **Modified Cycle:** Your adjusted temperatures (or other elements) show up correctly in the KeyFrame Graph.
- **Visual Confirmation:** Over time, the environment panel or chart reveals your new day/night pattern, confirming your changes are active.
- **Device Interaction:** IoT sensors or actuators (e.g., fans, sprinklers) reflect the environment changes (e.g., turning on at high temps).
- **Transference Behavior:** Child containers gradually converge to the parent's baseline, or maintain their adjusted environment if you set it periodically.

■

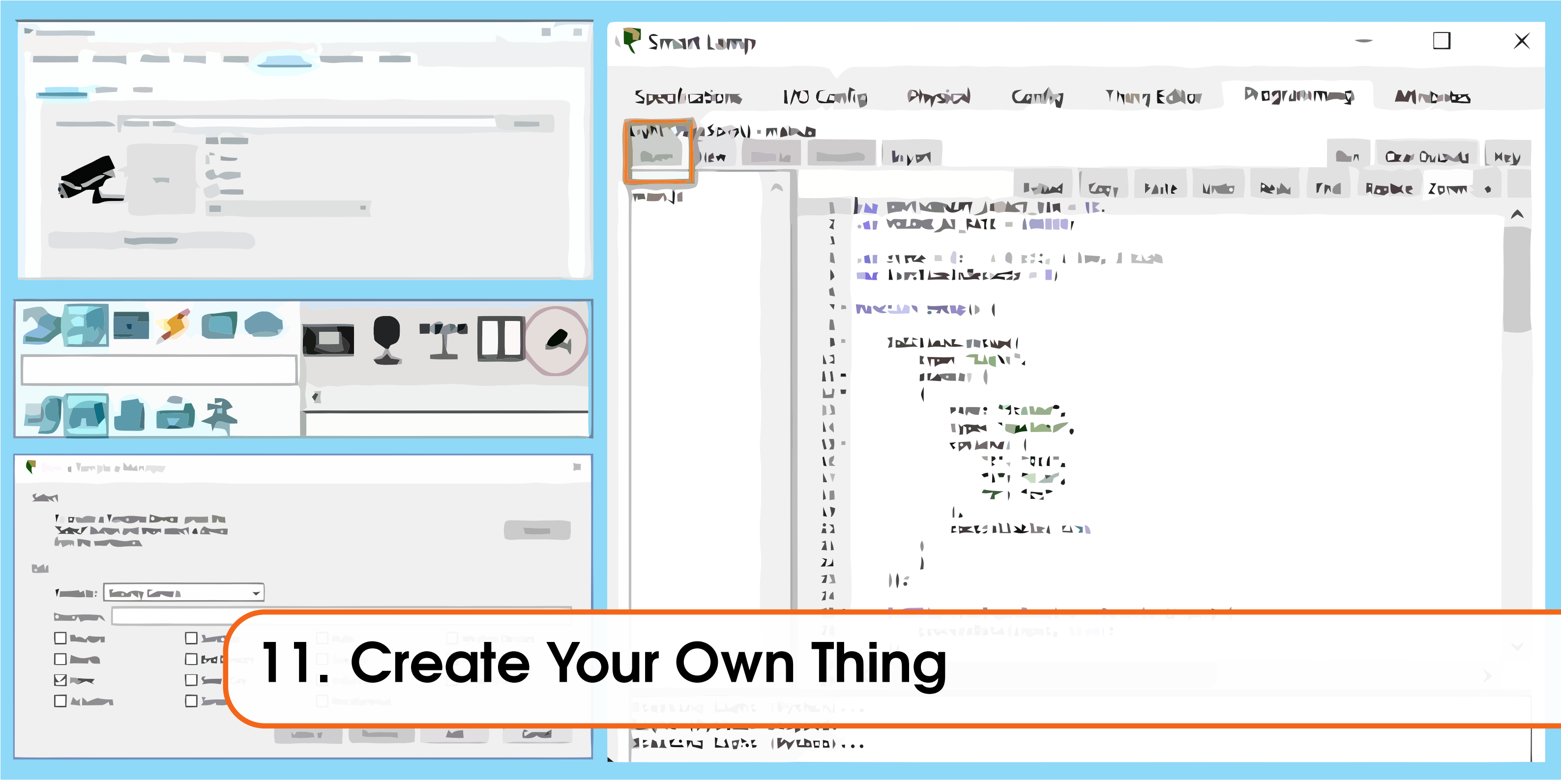
— Further Exploration

- **Multi-Container Scenarios:** Experiment with separate temperature/humidity overrides in a building while the city remains at defaults.
- **Automated Scripts:** Attach scripts to devices that react to environment triggers (e.g., a fan turning on when $\geq 30°C$).

- **Weather Variation:** Try adding wind or rain changes to see how devices (like wind turbines or sprinklers) respond.

Summary

You have now **modified and monitored environmental controls** in Packet Tracer's Physical workspace. By using KeyFrame Graphs, you adjusted day/night cycles or weather elements. You also saw how child containers inherit from parent environments, converging back via *transference*. This enables realistic simulation of climate or weather conditions in IoT deployments, letting you observe sensor and actuator responses in a fully simulated environment.



11. Create Your Own Thing

Introduction

In this lab, you will learn how to **create and customize IoT devices** (also called “Things”) in Cisco Packet Tracer. You will decide what your new Thing does, how it connects to the network, and which graphics or scripts it uses to represent different states and behaviors. By the end of this lab, you should feel comfortable building unique IoT devices, integrating them into smart network environments, and saving them as Packet Tracer templates for future reuse.

Objectives

- **Explore** IoT device customization by creating and personalizing a new “Thing.”
- Understand the **components and architecture** of a Thing, including sensors, actuators, and controllers.
- **Configure and program** your custom IoT device, enabling unique, functional smart systems.
- **Test and troubleshoot** your personalized IoT device, ensuring correct operation within an IoT network.

Background

Packet Tracer provides numerous ready-made IoT devices, but it also lets you **create your own Thing** to meet specific needs. This involves:

- Defining what the Thing does and how it connects to the network (wired or wireless).
- Assigning **custom graphics** to show different states (e.g., on/off or open/closed).
- Adapting or writing **scripts** that define its behavior via the *Advanced* → *Programming* tabs.
- Saving your new device as a **Packet Tracer template**, so it appears alongside standard IoT devices.

Typically, you locate a device script similar to your desired functionality and adapt it to the new device. Once created, you can share or reuse the custom “Thing,” as long as others have the same local template files.

Resources — Creating and Connecting a Thing | . Watch these videos to see how to create, modify, and save a new custom IoT "Thing" in Packet Tracer, from defining icons and states to writing or editing the device's scripts.

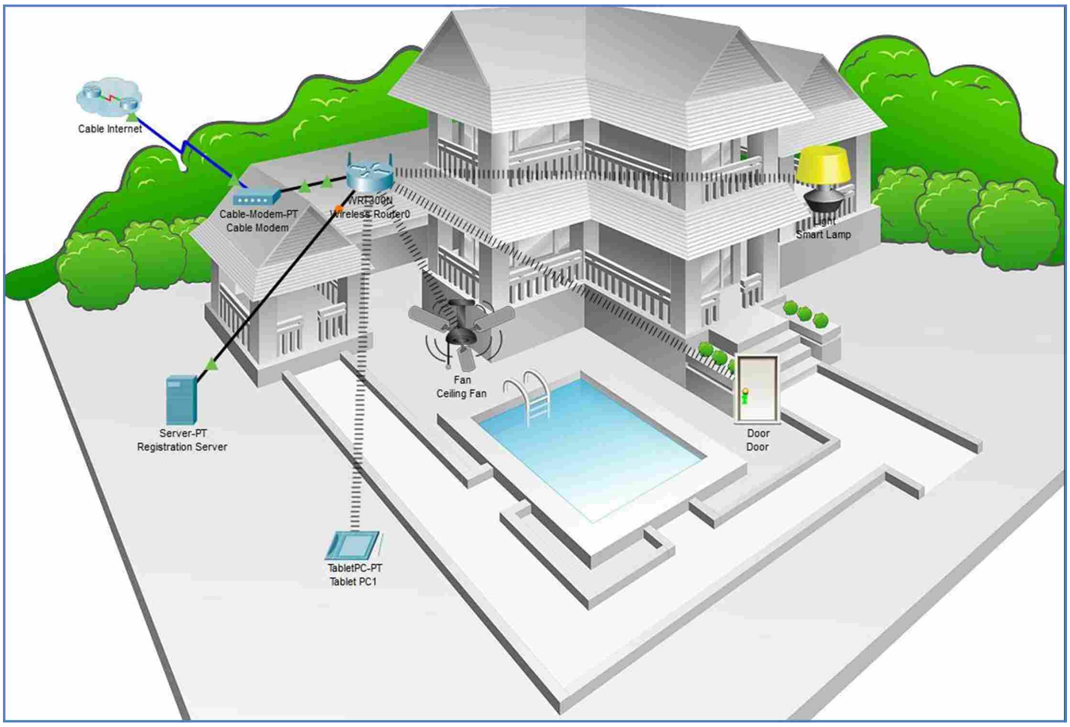


Figure 11.1: A sample Smart Home Environment, ready for adding a custom IoT device.

Lab Plan

In this lab, you will:

A. **Open and examine** the `Create_Your_Own_Thing.pkt` file, preparing the workspace for a generic IoT device.
B. **Configure** the device's display name, component properties, and custom icon.
C. **Add** a network adapter (wired or wireless) to connect the new Thing.
D. **Save** the device as a Packet Tracer template, verifying it appears in the device list for future use.

Required Software

- Cisco Packet Tracer 8.x (or newer), installed on your system.
- The Packet Tracer file `Create_Your_Own_Thing.pkt` (plus any custom images for icons).

A. Open and Examine the Lab File

In this section, you will load a pre-configured Packet Tracer file and prepare a generic IoT "Thing" for customization. By renaming and positioning your new device, you lay the groundwork for creating a unique IoT object with specialized behaviors.

1. **Launch Packet Tracer and Load the File:**
   Locate and open `Create_Your_Own_Thing.pkt` in Cisco Packet Tracer. To avoid overwrit-

ing the original file, immediately go to **File** → **Save As** and store a copy under a new name, such as `MyCustomThing.pkt`. This ensures you can freely make changes without losing the original setup.

2. **Add a Generic IoT "Thing" to the Workspace:**
   In the **Device-Type Selection** box (usually at the bottom-left of the Packet Tracer interface), look for a *Thing* icon. Depending on your version of Packet Tracer, you might find it under *End Devices* or *Components*.
   (a) Drag the *Thing* icon into your *Logical* workspace (see Figure 11.2).
   (b) This device will act as the foundation for your custom IoT object.

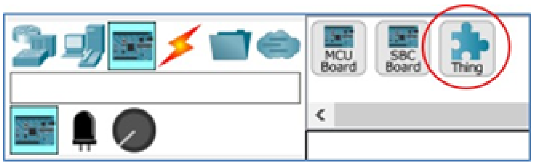


Figure 11.2: Selecting the "Thing" item in the Device Selection box.

3. **Rename the New Thing:**

   (a) Click on the newly placed *Thing* in the workspace to open its configuration window.
   (b) Switch to the *Config* tab.
   (c) Under **Global Settings**, locate the *Display Name* field. Replace the default name with a more descriptive one, such as "Security Camera."
   (d) Press *Enter* or click elsewhere to confirm the change (Figure 11.3).

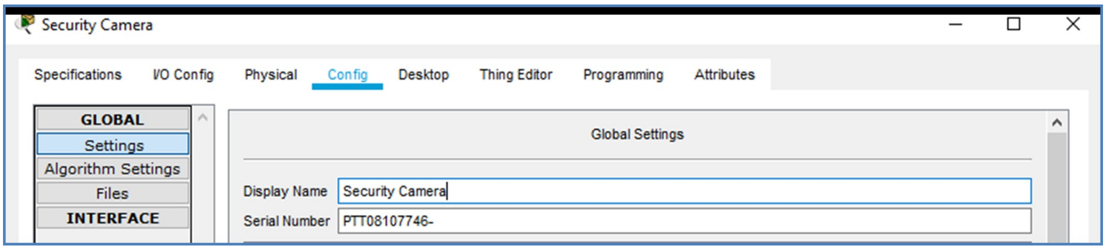


Figure 11.3: Renaming the device as "Security Camera."

Getting Started with Custom IoT Devices:

File Versioning: Keeping a separate file (e.g., `MyCustomThing.pkt`) lets you experiment with new features without risking the original lab setup.

Naming Conventions: Use meaningful names like `SecurityCamera`, `SmartLock`, or `GardenSensor` to keep track of your custom devices, especially if you plan to add multiple Things later.

Location and Organization: If your network is large, place the Thing near relevant areas (e.g., near a router or in a specific building) to reflect a realistic placement in the Logical workspace. ■

B. Configure Properties and Icon

Now that you have placed and renamed your new IoT "Thing," you can specify its internal component name, slot mapping, and visual appearance. This step is crucial for customizing how your device will behave and look in Packet Tracer.

4. **Open the Thing Editor (*Properties* Tab):**
    - Click on the device's *Config* window (where you renamed it), then locate and click the **Advanced** button (typically near the bottom-right corner).
    - Select the *Thing Editor* tab that appears, and within it, click on the **Properties** sub-tab.
5. **Set Component Name and Slot Mapping:**
    - Under *Component Name*, enter a descriptive label, such as `Security Camera`.
    - For *Slot Mapping*, choose `Digital` and `Slot 1`. This tells Packet Tracer how the device's internal states (e.g., on/off) will be mapped to digital signals.
6. **Upload a Custom Icon:**
    - Click the **New** button to open a file browser.
    - Select a suitable image (either `.png` or `.jpg`) that you want to use as this device's icon—perhaps a small camera image if you're building a *Security Camera* device.
    - Once selected, Packet Tracer automatically saves this graphic for use with your custom Thing.

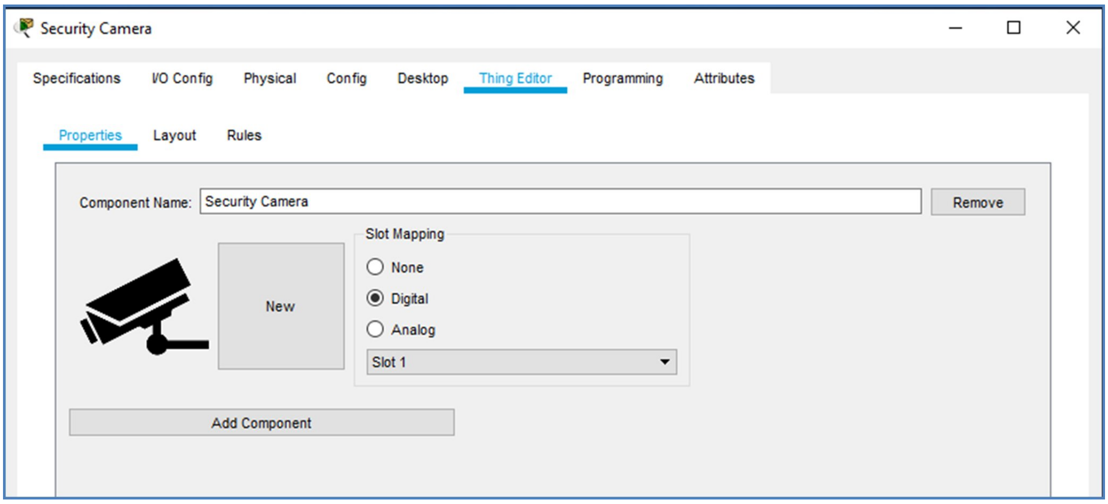


Figure 11.4: Defining properties and uploading a custom icon in the Thing Editor.

Managing Multiple States and Icons:
You can define additional icons later in the *Rules* sub-tab to represent `LOW` (off) or `HIGH` (on) states. For example, you might use a gray icon for the camera when it's inactive and a colored icon when it's active.
If your device requires multiple sensors or slots (e.g., temperature, motion), you can configure additional `Slot Mapping` entries in this same *Properties* tab.
Keep icon file sizes small to ensure Packet Tracer performance is not impacted, especially in larger projects with many custom images.

C. Add to the Network

In this section, you will give your custom IoT device a network interface (wired or wireless) and verify that it can communicate with other devices on the LAN (or WLAN). This step ensures your new "Thing" is properly connected and ready to exchange data.

7. **Select a Network Adapter:**
   While still in the **Advanced** configuration window, switch to the **I/O Config** tab:
   - Choose `PT-IOT-NM-1CFE` for a **wired** Fast Ethernet interface.
   - Choose `PT-IOT-NM-1W` for a **wireless** interface.

   Figure 11.5 shows how to select an adapter type for your camera device.

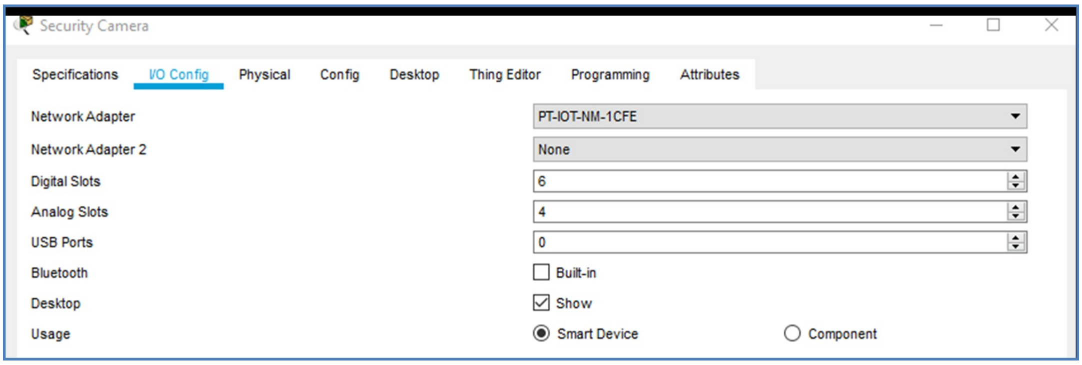


Figure 11.5: Choosing a wired (CFE) or wireless (1W) adapter for the camera.

8. **Connect the Device:**
   - **Wired Connection:**
     (a) In the *Connections* menu (lightning-bolt icon), select *Copper Straight-Through*.
     (b) Click the `FastEthernet0` port on your camera (or "Thing").
     (c) Click on a corresponding Ethernet port on a router or switch.
     (d) After a brief moment, you should see green link lights if cabling is correct.
   - **Wireless Connection:**
     (a) In *Config* → **Wireless0**, ensure the `SSID` matches your network's wireless name.
     (b) If your network uses WPA2 or another security setting, enter the passphrase accordingly.
     (c) Once configured, the device should automatically associate with the Wi-Fi network if the signal is in range and the credentials are correct.
9. **Enable DHCP (Wired) or Confirm IP (Wireless):**
   - For **wired** devices, go to *Config* → **FastEthernet0** and set **IP Configuration** to `DHCP`.
     – This tells your device to request an IP address from the network's DHCP server (commonly found on a router or dedicated server).
   - For **wireless** devices, once they associate with the correct `SSID` and security settings, they typically receive an IP from the DHCP server automatically (assuming DHCP is active on the wireless router or access point).

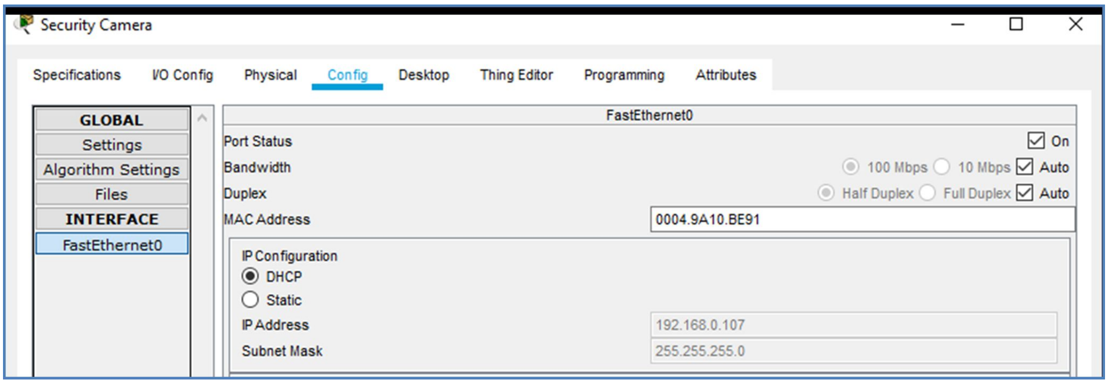


Figure 11.6: Configuring the interface for DHCP (wired example).

Network Adapter Selection:
Check for DHCP Server: If your device does not obtain an IP, verify that there is an active DHCP server on your network (often on the main router).
Static IP Option: If DHCP is not available or you prefer static addressing, simply select *Static* in the IP Configuration and assign a unique IP/subnet mask/gateway manually.
Wireless Signal Strength: For wireless connections in Packet Tracer, be mindful of distance and signal coverage. If your device is placed too far from the access point, it may fail to connect.

10. **Test Network Reachability:**

    - On another device in the same network, open *Desktop* → *Command Prompt*.
    - Type `ping <Camera-IP>` (e.g., `ping 192.168.1.50`), where `<Camera-IP>` is the address assigned to your custom Thing.
    - If you receive replies, it indicates your new Thing is successfully online and can communicate within the network.

Troubleshooting Network Connectivity:

Cables and Ports: For wired connections, ensure you used the correct cable type (Straight-Through vs. Cross-Over) and the correct ports (`FastEthernet0` on the Thing, `Fa0/1` or similar on the switch/router).

Subnet Consistency: Double-check that your Thing's IP, subnet mask, and gateway match the rest of the network. A mismatch can lead to ping failures.

Verify Device Power: In rare cases, if your device is powered off in the Physical tab, turn it on (by toggling the power switch) so it can operate.

Check Security Settings (Wireless): If using WPA2, the passphrase must be exact; a single typo will prevent connection.

D. Save as a Packet Tracer Template

Once your custom IoT device is configured and functioning on the network, you can save it as a *Device Template* in Packet Tracer. This allows you to quickly reuse it in future labs or share it with others.

11. **Open Device Template Manager:**
    - Go to **Tools** → **Custom Device Dialog** to launch the *Device Template Manager*.

- Click **Select**. The manager will temporarily disappear.
- Click your **Security Camera** (or the custom device you have created) in the workspace. This action re-opens the Device Template Manager, now referencing that specific device.

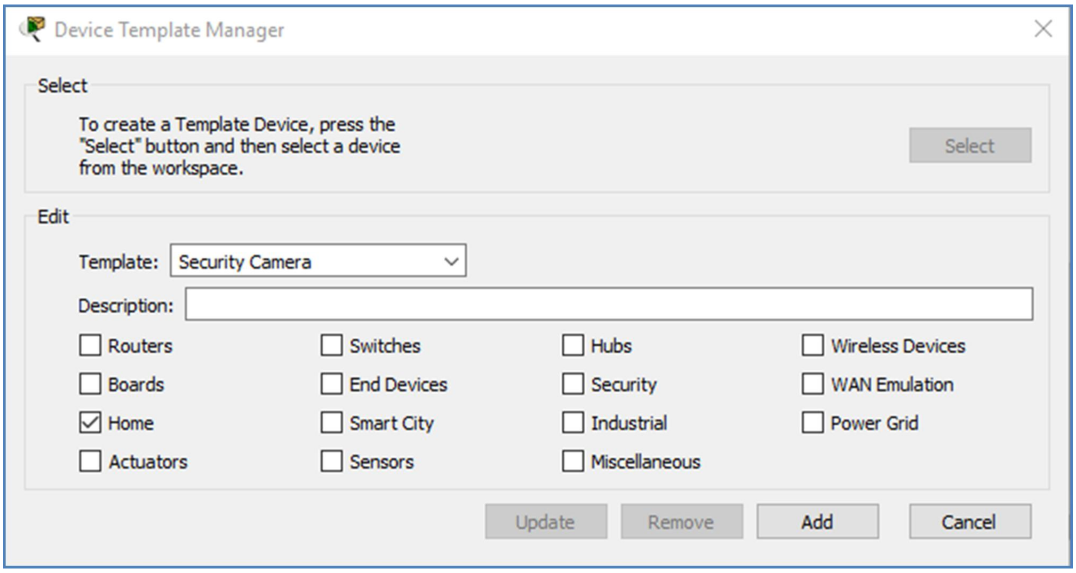


Figure 11.7: Marking the "Home" category for your custom `Security Camera`.

12. **Add and Save the Template:**
    - In the *Template Name* field, enter `Security Camera` (or whichever name you chose).
    - Select a category, such as **Home**, by checking the box next to it. This determines where your device will appear in the Packet Tracer interface.
    - Click **Add**. A "*Save File in Template Folder*" dialog appears.
    - Keep the default filename (e.g., `Security Camera`) or rename if desired. Click **Save** to store it in Packet Tracer's local template folder.

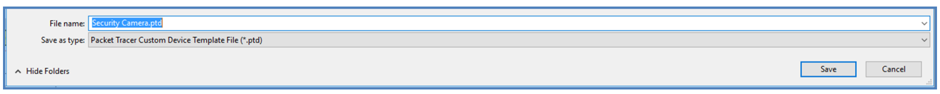


Figure 11.8: Saving the new device template to Packet Tracer's local folder.

13. **Verify in the Device Selection Box:**
    - Optionally, close and re-open Packet Tracer or open a new `.pkt` file (after saving your current work).
    - In the *Device-Type Selection* box, under the **Home** category (or the category you chose), look for your `Security Camera` device (Figure 11.9).
    - You can now drag-and-drop this custom device into any future Packet Tracer project without having to recreate its configuration or icon.

Figure 11.9: Confirming the custom `Security Camera` appears in the "Home" category.

Using Templates in Future Labs:

Consistent Naming: If you plan to distribute your template, keep the name short and descriptive (e.g., `SecCam-PT`) so others can easily recognize it.

Template Folder Location: Packet Tracer stores templates in a local folder on your computer. You can share this folder with classmates or move it between computers if needed.

Updates to the Template: If you modify your device (new icons, scripts), simply repeat this process to overwrite the old template or save a new version under a different name. ■

The Programming Environment

Packet Tracer supports *JavaScript*, *Python*, and *Visual Blocky* for device scripting.

1. Open your device, then click the **Advanced** button.
2. Select the **Programming** tab to create or open scripts.
3. In the left panel, you may open or import existing code or start a new project.

Adapting Existing Scripts:

1. Highlight a script in the left pane and click *Open* to display the code on the right.
2. Use the edit buttons (copy, paste, find) to modify it for your new device.
3. Closing the *Programming* tab saves any changes automatically.

Or you can remove old code entirely and *start from scratch*.

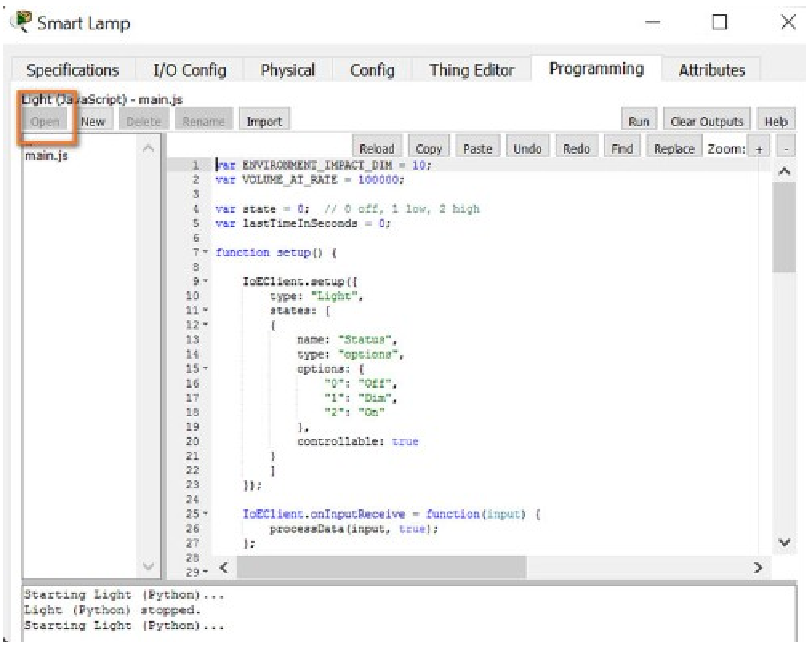


Figure 11.10: Opening or creating scripts in the Programming tab.

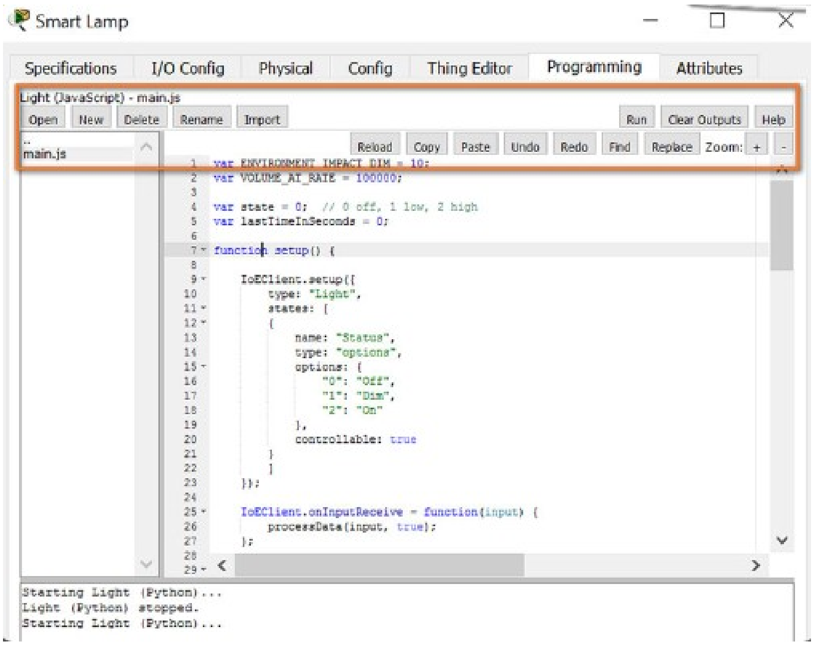


Figure 11.11: Using editing buttons (copy, paste, find) to adapt code for your new Thing.

Measuring Success

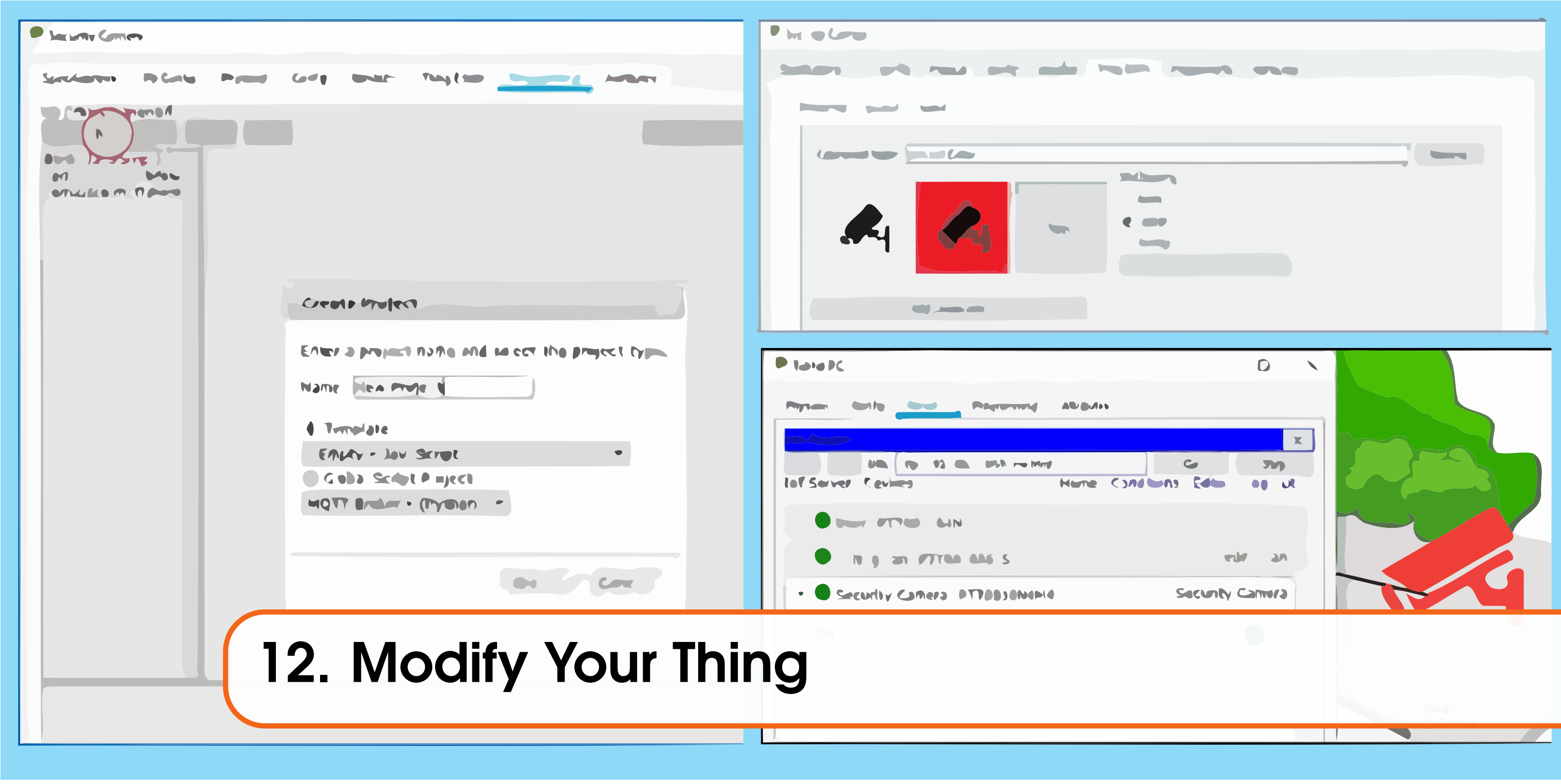
- Your new IoT device (e.g., **Security Camera**) obtains an IP address (if using DHCP) and responds to a `ping`.
- You see the correct **icon** in the workspace, reflecting any states you've defined.
- You have saved a **template**, verified it in the *Home* category, and can reuse this device in future Packet Tracer projects.
- Any **scripts** you adapted or wrote function as intended.

— Further Exploration

- **Network Integration:** Connect your custom Thing to a Registration Server for remote control.
- **Multiple States:** Add more than two states (on/off, blinking, etc.) to explore advanced transitions.
- **Code Variation:** Rewrite the device script in Python or Visual Blocky to practice different Packet Tracer IoT programming modes.

Summary

You have successfully **created a new IoT Thing** in Packet Tracer, assigning a name, custom icon, network interface, and optional scripts. You also saved the device as a **template** for future use. These skills enable you to design specialized IoT devices and integrated smart networks for more complex simulations.



12. Modify Your Thing

Introduction

In this lab, you will learn how to **modify and enhance an existing IoT device** (also called a "Thing") within Cisco Packet Tracer. Specifically, you will build on the *Security Camera* device created in an earlier activity, adding new icons for different states, importing code from a **Motion Detector**, and testing the updated camera via a Registration Server. This process demonstrates how to adapt existing Packet Tracer scripts to create new or more advanced functionalities.

Objectives

- Learn to **add and customize device icons (LOW/HIGH states)** for an existing IoT device.
- **Reuse and edit** code from another IoT device (Motion Detector) to expand or alter functionality.
- **Test and troubleshoot** your modified device, confirming it behaves as intended.
- Further develop **IoT programming and configuration** skills, enabling more complex smart systems.

Lab Plan

In this lab, you will:

A. Open and examine the `Modify_Your_Thing.pkt` file containing an existing *Security Camera* device.
B. Add an extra icon/image to represent the camera's "activated" (HIGH) state.
C. Import code from the *Motion Detector* device, adapt it, and paste it into the camera's script.
D. Test your updated camera in the IoT environment, verifying activation states on a Registration Server.

Required Software

- **Cisco Packet Tracer 8.x** (or newer) installed on your system.
- The Packet Tracer file: `Modify_Your_Thing.pkt`.

- (Optionally) Additional images (`.png` or `.jpg`) for new "activated" icons.

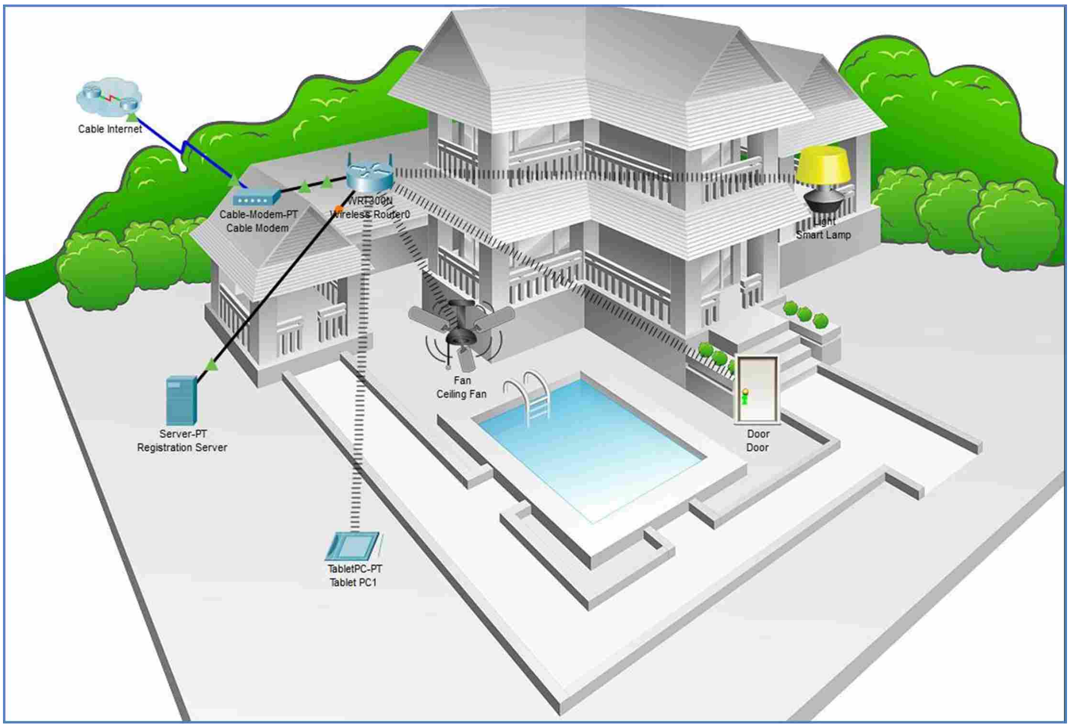


Figure 12.1: Smart Home Environment with a router, Registration Server, cable modem, ceiling fan, door, lamp, and the existing Security Camera.

A. Open Lab and Add Extra Icon

In this section, you will edit an existing IoT device (*Security Camera*) by adding a second icon to represent its "activated" state. This process helps you visualize different operating modes or statuses for your custom device in Packet Tracer.

1. **Open the** `Modify_Your_Thing.pkt` **File**
   - Launch Packet Tracer and open `Modify_Your_Thing.pkt`.
   - Immediately perform **File** → **Save As** to create a new copy, for example `MyModifiedCamera.pkt`. This ensures you can safely modify the file without affecting the original.
   - Confirm you see a *Security Camera* device in the workspace.
2. **Access the Security Camera Configuration**
   - Click on the **Security Camera** icon to open its configuration window.
   - At the bottom-right, select the *Advanced* button to reveal additional tabs like *Thing Editor* and *Programming*.
3. **Navigate to the Thing Editor (Properties Tab)**
   - In the *Thing Editor* tab, click on the *Properties* sub-tab.
   - You should see the default (inactive) camera icon. This icon typically represents the device's `LOW` or "off" state.

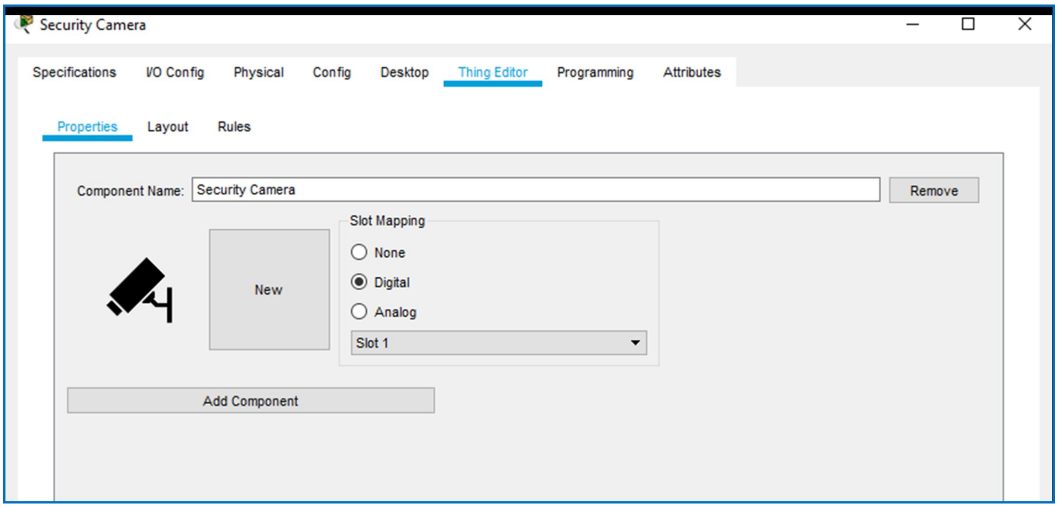


Figure 12.2: Accessing the Thing Editor's Properties to prepare for adding a second icon.

4. **Add a New Icon for Activation**

- Click the **New** button to open a file-browse dialog.
- Choose an alternate graphic, such as a *red camera icon*, to denote the camera's "activated" or `HIGH` state.
- Packet Tracer will import the image and store it with your custom device.

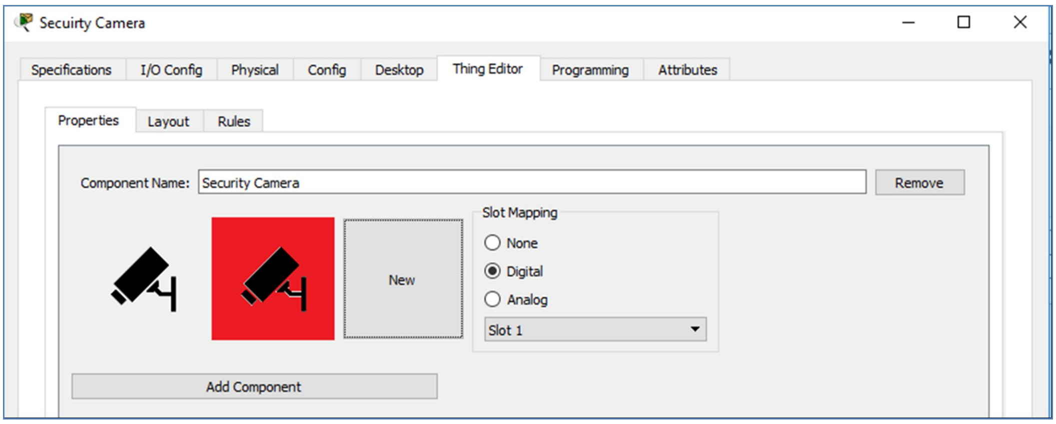


Figure 12.3: Selecting a different image for the Security Camera's activated state.

Choosing and Managing Icons:
If you do not already have a suitable camera icon, you can quickly create or download a small `.png` file. Ensure that the image file is not too large, or it may appear oversized in Packet Tracer and slow down your workspace.
Use distinct and clearly identifiable icons for each state (e.g., *gray camera* for inactive, *red camera* for active). This helps you recognize status changes at a glance.
Keep your image naming simple (e.g., `SecCamInactive.png`, `SecCamActive.png`) to avoid confusion if you have multiple icons or states. ■

B. Set Rules and Duplicate States (LOW/HIGH)

After adding an alternate icon for your device's "activated" state, you need to define how the camera switches between `LOW` (inactive) and `HIGH` (active). The **Rules** tab in the *Thing Editor* lets you map these states to distinct images.

5. **Open the Rules Tab**

   - In the *Thing Editor*, switch to the **Rules** sub-tab.
   - Here, you can create or modify "rules" that tie together digital slot values (e.g., `LOW`, `HIGH`) with the images you uploaded.

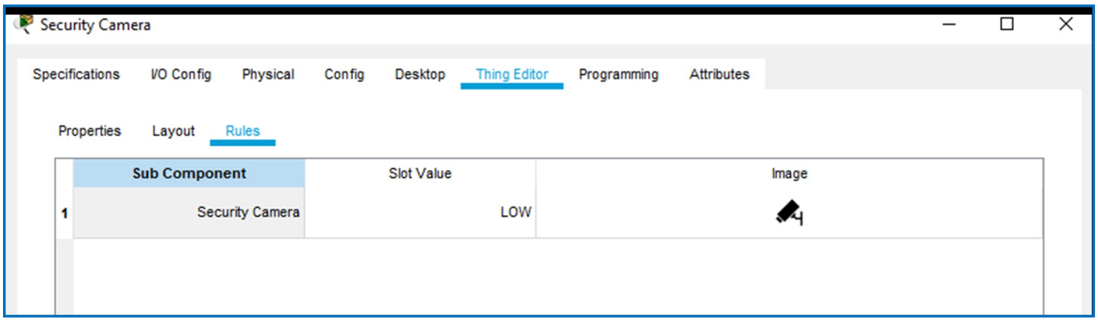


Figure 12.4: Rules tab for sub-components; the camera's default icon is mapped to LOW.

6. **Add Two State Lines**

   - Click *Add Component* to create the first line of rules:
     - **Sub Component**: `Security Camera` (*must match the "Component Name" from the Properties sub-tab*)
     - **Slot Value**: `LOW` (the "inactive" or `0` state)
     - **Image**: the **original** (inactive) icon
   - Click *Add Component* again to create the second line:
     - **Sub Component**: `Security Camera`
     - **Slot Value**: `HIGH` (the "active" or `1` state)
     - **Image**: the **newly uploaded** (activated) icon

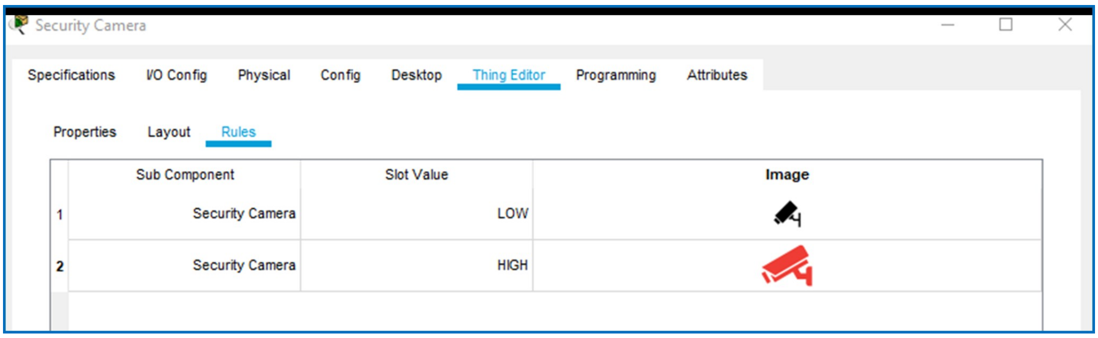


Figure 12.5: Two lines: one for LOW state, one for HIGH state. The second uses the "red camera" icon.

Configuring State Icons:
Sub Component Must Match: The **Sub Component** field must exactly match the *Component Name* you specified under *Properties* (e.g., "Security Camera"). A mismatch here will prevent the rule from applying.
Slot Value Importance: **Slot Value** links your device's digital input (`LOW` or `HIGH`) to a specific image. If your device script sets the camera's state to `HIGH`, Packet Tracer will display the "active" icon.
Multiple States: You can repeat this process to add additional states (e.g., `MEDIUM` or `BLINKING`), each referencing a different icon. This is useful for devices with more than two states (on/off).

C. Import and Adapt Motion Detector Code

In this section, you will give your *Security Camera* a functional script by reusing and modifying code from an existing IoT device—the **Motion Detector**. This process accelerates development by letting you build on proven JavaScript logic rather than coding from scratch.

7. **Check the Camera's Programming Tab**

   - In the *Security Camera* configuration window, select the *Programming* tab.
   - If it shows "*No Project Opened*," that means no custom script is currently attached.

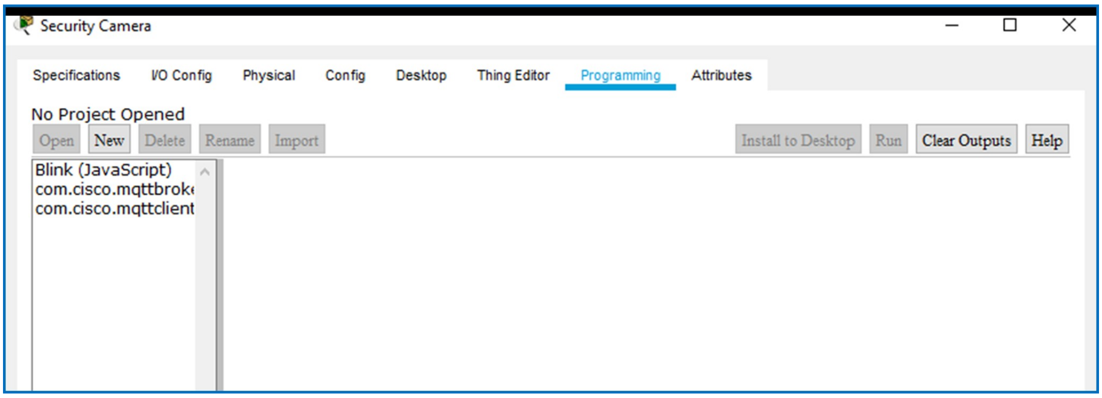


Figure 12.6: Blank "Programming" tab for the camera, indicating no existing script.

8. **Import Code from a Motion Detector**
   i. **Place a Motion Detector:** In the *End Devices* (bottom-left) → *Home* category, drag a **Motion Detector** into your workspace.
   ii. **Open its Programming Tab:** In the *Advanced* → **Programming** section, select `Motion Detector (JavaScript)` in the left pane and click `Open`.
   iii. **Copy the Code:** Click `main.js` to display the source. Press `Ctrl + A` to select all lines, then click `Copy`.
   iv. **Remove the Motion Detector (Optional):** Close the Motion Detector config window. You may delete it from the workspace if no longer needed.

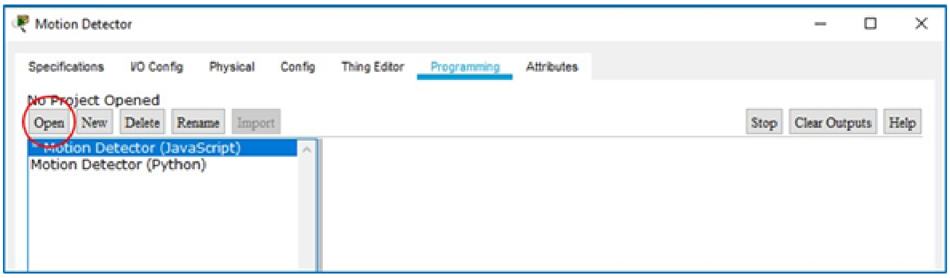


Figure 12.7: Accessing the Motion Detector's JavaScript code in the Programming tab.

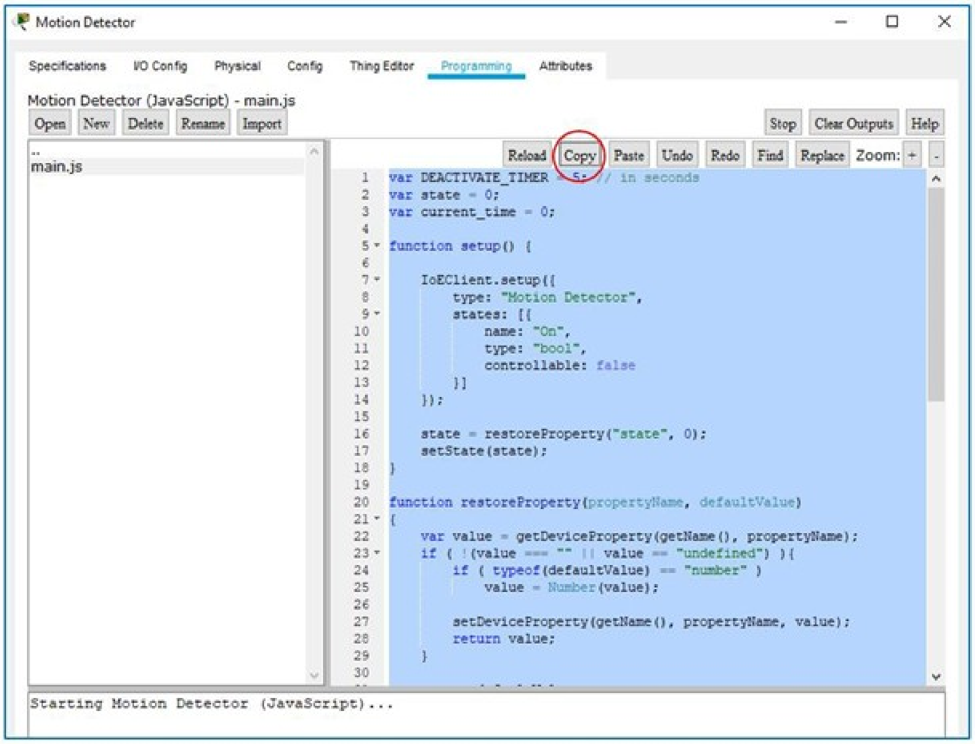


Figure 12.8: Selecting and copying all lines of code to reuse in our camera.

9. **Create a New Project in the Security Camera**
   i. **Return to the Camera:** Open the *Security Camera* config once again and switch to the *Programming* tab.
   ii. **Start a New Project:** Click `New` above the left pane. In the *Create Project* dialog, enter a name like `Security Camera`, then click `Create`.

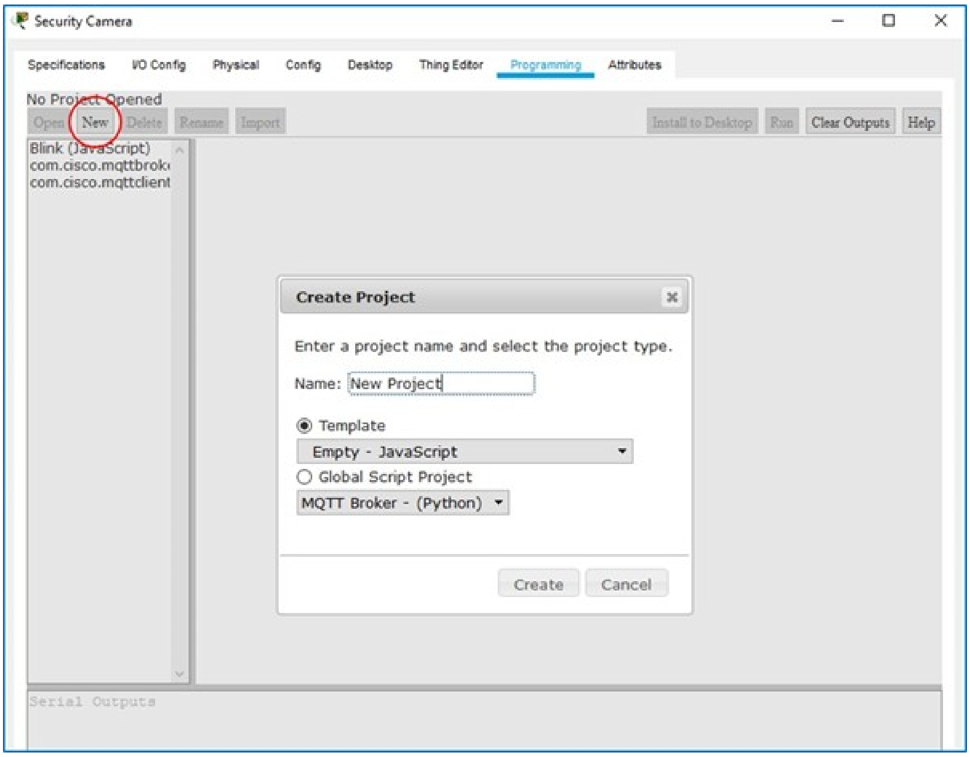


Figure 12.9: Creating a new JavaScript project within the camera's Programming tab.

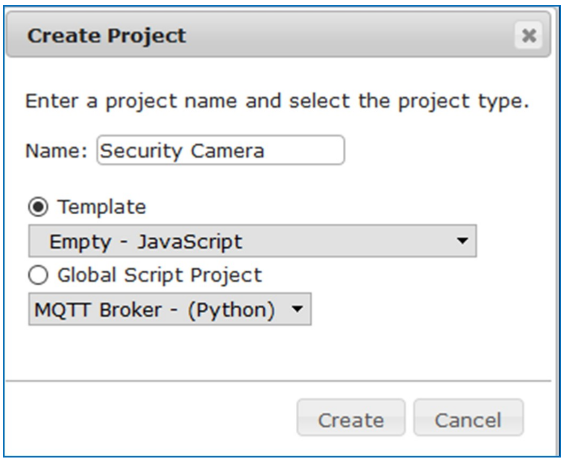


Figure 12.10: Naming the project "Security Camera."

10. **Paste the Copied Code**
    i. Open `main.js` in the left pane of your new `Security Camera` project.
    ii. Click `Paste` to insert the previously copied script from the Motion Detector.

Figure 12.11: Opening `main.js` within “Security Camera (JavaScript).”

Figure 12.12: Pasting the Motion Detector code into the new `main.js`.

11. **Edit the “type” Field**

    - Look for a line near the top of the code (around line 8) that reads `type: "Motion Detector"`.
    - Change it to `type: "Security Camera"` (or the name of your custom device).

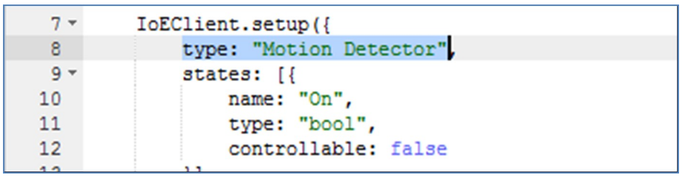


Figure 12.13: Locating the line referencing `"Motion Detector"`.

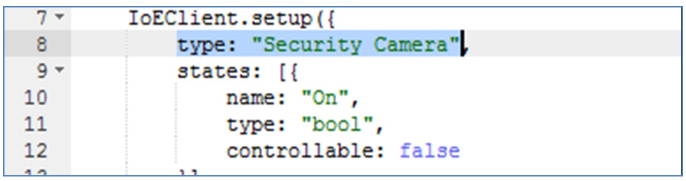


Figure 12.14: Replacing “Motion Detector” with “Security Camera.”

Adapting the Motion Detector Code:
If you see other references to `"Motion Detector"` or states like `"on"`, `"off"`, feel free to rename them for clarity.
Adjust any timers, thresholds, or behaviors (e.g., `detectMotion()`) to match how you want your *Security Camera* to react (e.g., “activate” when triggered).
You can insert additional functions to log messages, send alerts, or switch icons as needed.
■

12. **Run the Program**

- Click the Run button. If no errors appear in the console, your camera script should be active.
- You can close the Security Camera's configuration window. Re-open it anytime to tweak code or icons.

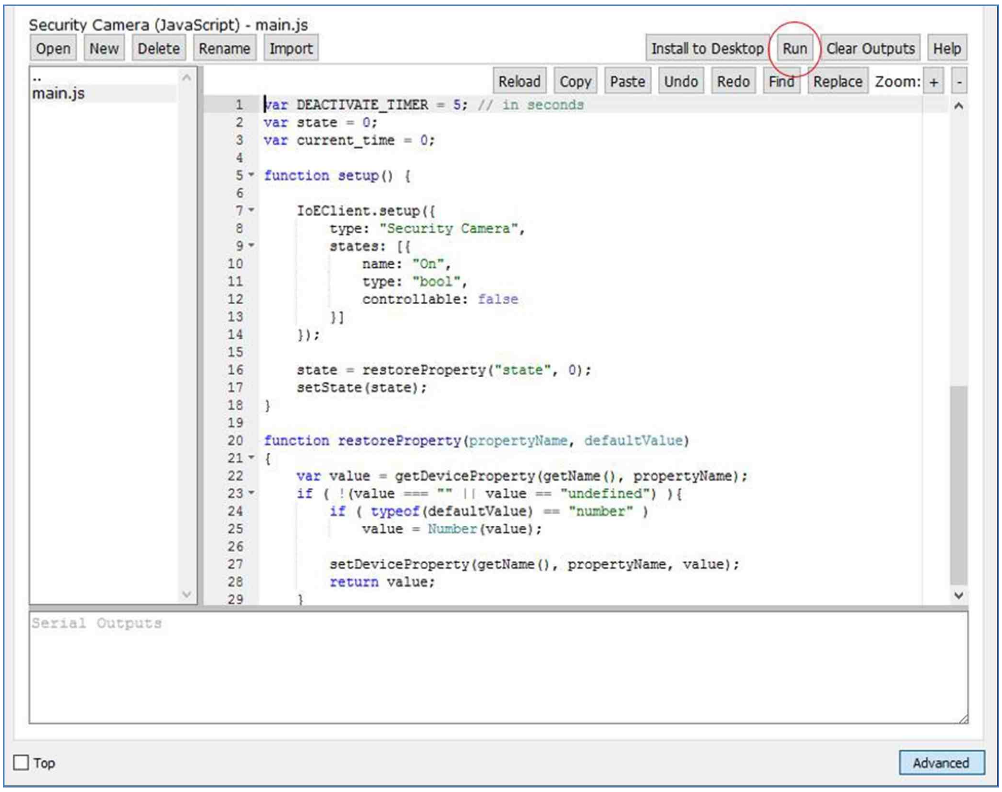


Figure 12.15: Running the camera script to ensure it initializes without errors.

Script Integration Tips:

Testing Basic Functionality: Try `Alt`-hovering over the camera or using the *Rules* tab to see if the icon switches between `LOW` and `HIGH` states. This confirms the script can handle basic events.

Debugging: If an error appears, check the `Output` or `Console` in Packet Tracer's Programming tab to identify syntax issues or missing references.

Advanced Behaviors: You can enhance the code with timers (e.g., auto-return to `LOW` after 30 seconds) or triggers (e.g., camera only records when `HIGH`). ■

D. Test the Modified Camera

Now that you have added a second icon and adapted the camera's code (originally from a Motion Detector), it's time to see these changes in action. In this section, you will verify that your new `HIGH` (activated) icon displays correctly and that the Registration Server recognizes the updated device status.

13. **Access the Registration Server via Tablet PC**

    i. Click the **Tablet PC** device to open its configuration window.
    ii. Go to *Desktop* → **Web Browser**.

iii. In the address bar, enter the Registration Server's IP (e.g., `192.168.0.106`) and click *Go*.
iv. Log in with the appropriate credentials (e.g., `cisco / cisco123`), unless otherwise specified by your lab setup.

14. **Hover with Alt to Trigger "Activated" Icon**

- In the tablet's web interface, the *IoTServer–Devices* pane may show your *Security Camera* as `On` but not necessarily "activated."
- Move the Tablet window aside. In the Packet Tracer workspace, **hold down the `Alt` key** and hover your mouse over the camera icon.
- The camera's icon should switch from `LOW` (inactive) to `HIGH` (activated). In many cases, the Registration Server interface updates to show a green dot or an "activated" status (Figure 12.16).

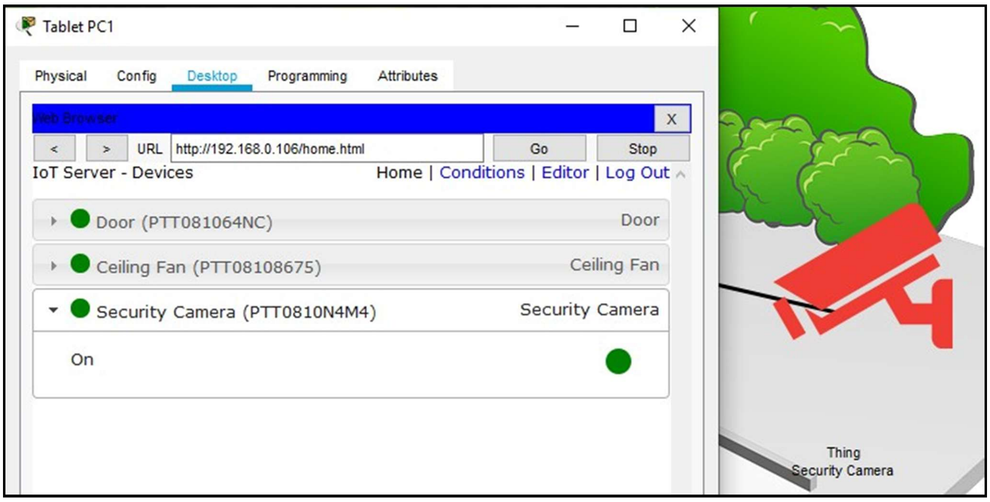


Figure 12.16: Activating the Security Camera in Packet Tracer; holding `Alt` switches it to the "activated" state.

15. **Experiment with Other IoT Edits**

- Consider further customizing the `main.js` script to add additional states (e.g., `MEDIUM`, `BLINKING`) or functionality (like a timer that reverts from `HIGH` to `LOW` after 30 seconds).
- Any changes in the code that affect the camera's digital states or icons will also appear in the Registration Server's device list, allowing for more dynamic control and monitoring.
- You can repeat a similar process on other IoT devices if you want them to have multiple icon states or custom JavaScript behaviors.

Additional Testing and Tuning:

Check Console Output: If you run into unexpected behavior, revisit the *Programming* tab in the Security Camera's config and look at the `Output` or `Console` for error messages.

Syncing Visual States: In some cases, you may want the device's `HIGH` state to automatically revert to `LOW` after a period, which can be done by adding a `setTimeout` or similar timer in your JavaScript code.

Registering Remotely vs. Locally: If your camera is registered to a *Registration Server* (rather than a local Home Gateway), be sure to keep the correct `IoT Server` setting in *Config* →

Settings.

Measuring Success

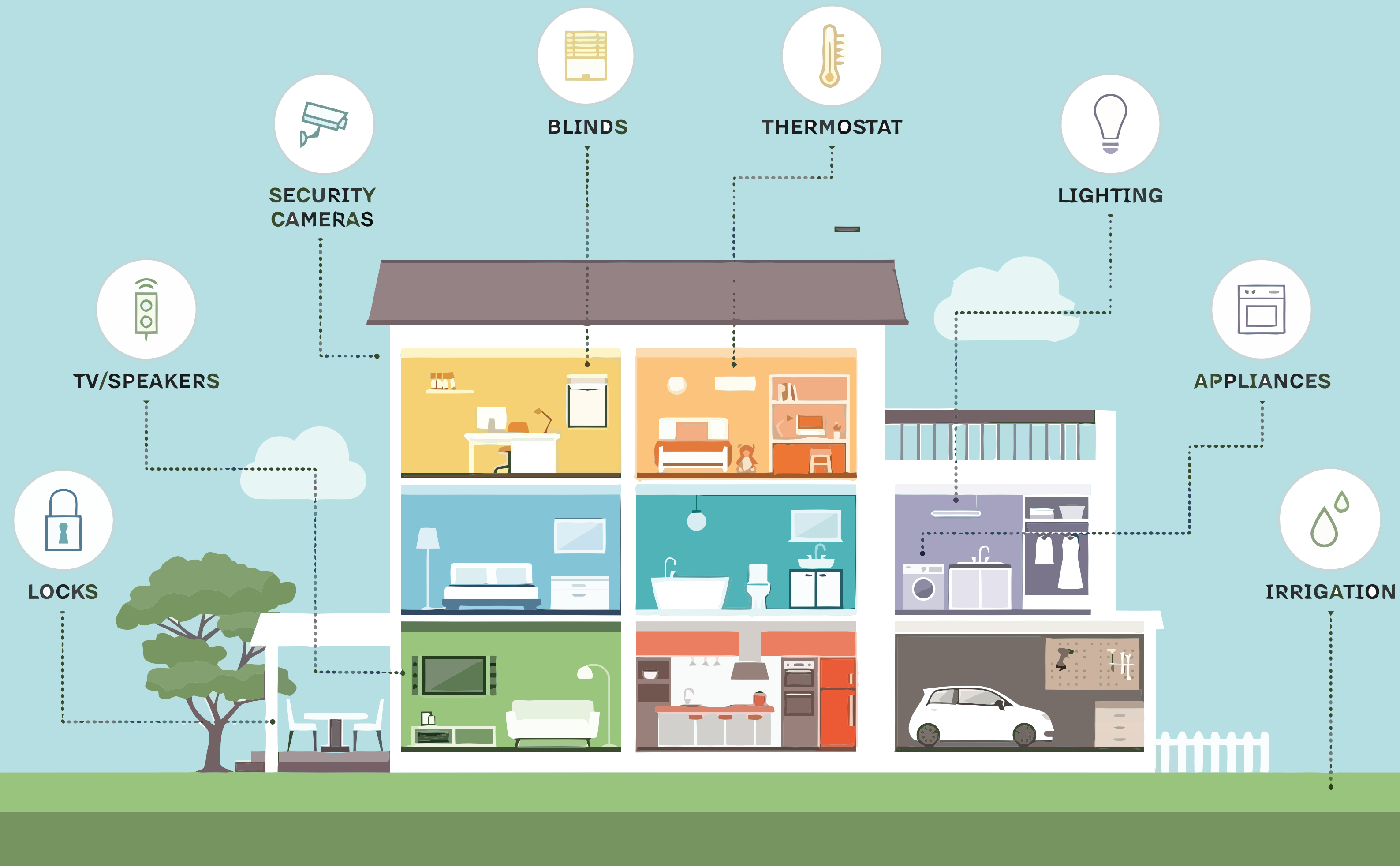
- **Custom Icon States:** Your camera now has two states (LOW/HIGH) with distinct icons, and these icons change accordingly when you Alt-hover.
- **Script Integration:** The *Motion Detector* code successfully runs on the camera device, with the `type` field changed to `"Security Camera"`.
- **Registration Server Feedback:** The server interface updates to show `On` (green dot) or similar for the camera's activated state.
- **No Errors on Run:** Clicking `Run` in the Programming tab shows no immediate console errors, indicating a valid code adaptation.

Summary

In this lab, you **modified the custom Security Camera** by adding a second icon (for `HIGH` state) and importing code from the *Motion Detector*. You then tested its activation in Packet Tracer via the **Alt** hover and verified the updated device state on the Registration Server. This illustrates how *existing* IoT scripts can be adapted to create *new or improved* Things, accelerating smart home development.

— Further Exploration

- Experiment with more states (e.g., `MEDIUM`) or alternative icons to handle multi-level device statuses.
- Incorporate timers or triggers so that the camera returns to `LOW` state automatically after a set duration.
- Explore how the `Security Camera` can interact with sensors or environmental values (e.g., turning on if motion or darkness is detected).


BLINDS
THERMOSTAT
SECURITY CAMERAS
LIGHTING
TV/SPEAKERS
APPLIANCES
LOCKS
IRRIGATION