Federal State Autonomous Educational Institution of Higher Education
"NATIONAL RESEARCH UNIVERSITY
HIGHER SCHOOL OF ECONOMICS
Tikhonov Moscow Institute of Electronics and Mathematics
MS Information Security & Artificial Intelligence Technologies

Work report / Laboratory work No: 1.0.5, 1.5.5, 2.3.7
on the course “Protection of Computer Networks and Systems"

Performed by: Khanzada
Mubashir Hassan
Khanzada
Mubashir Hassan
Teacher: Ilyukhin R.V
Senior Venerable. Ilyukhin R.V.

Moscow, 2025

Contents

Task 1.0.5 - Logical and Physical Mode Exploration - Packet Tracer

Introduction

This task focused on exploring Cisco Packet Tracer to understand how different networking devices, cables, and configurations are represented and used within both logical and physical views. The activity included identifying device categories, investigating wiring closets, connecting end devices with proper cables, installing and configuring a backup router, and becoming familiar with the overall network layout. The practical exercises provided a step-by-step opportunity to interact with networking components and understand their functions in real-world scenarios.

Part 1: Exploring the Bottom Toolbar

What are the subcategories for **Network Devices**?

Answer: Routers, Switches, Hubs, Wireless Devices, Security, and WAN Emulation

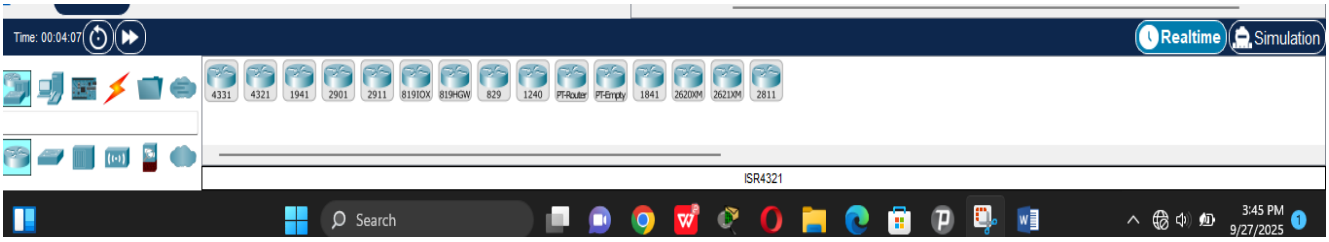

Figure 1

Part 2: Investigate Devices in a Wiring Closet

The Branch Office Wiring Closet was inspected in Physical mode. The rack contains a router and switches. The devices with a wired connection to switch ALS2 are: ALS1, Access_Point, and WebServer

In Logical Mode, the device connected to the Access_Point was identified as:

Laptop_1

In Physical Mode, the device connected to the Access_Point is physically located **On the Table**.

Part 3: Connect End Devices to Networking Devices

Different cables were used to establish connections. A Copper Straight-Through cable was connected from PC_1 to switch ALS2 for network access. A Console cable was then connected from PC_1 to the Edge_Router for management access.

Part 4: Install a Backup Router

The Shelf was inspected, which contains an inventory of uninstalled devices for the Seward Branch Office.

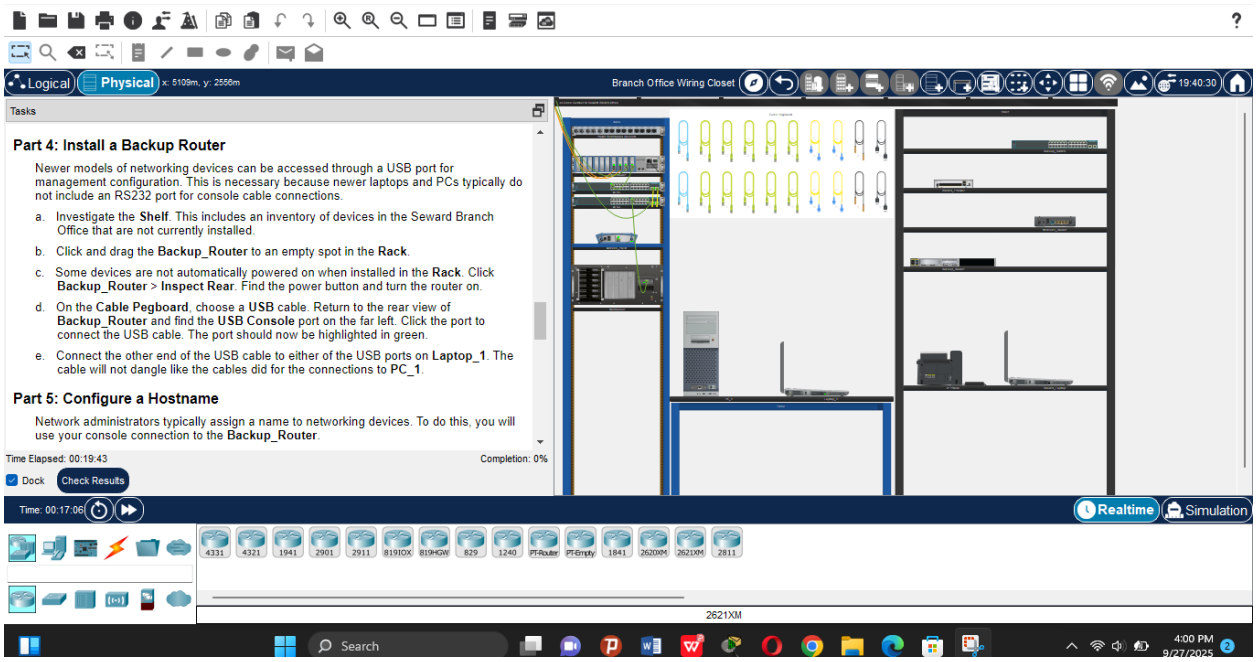

Figure 2

a. Click and drag the **Backup_Router** to an empty spot in the **Rack**.

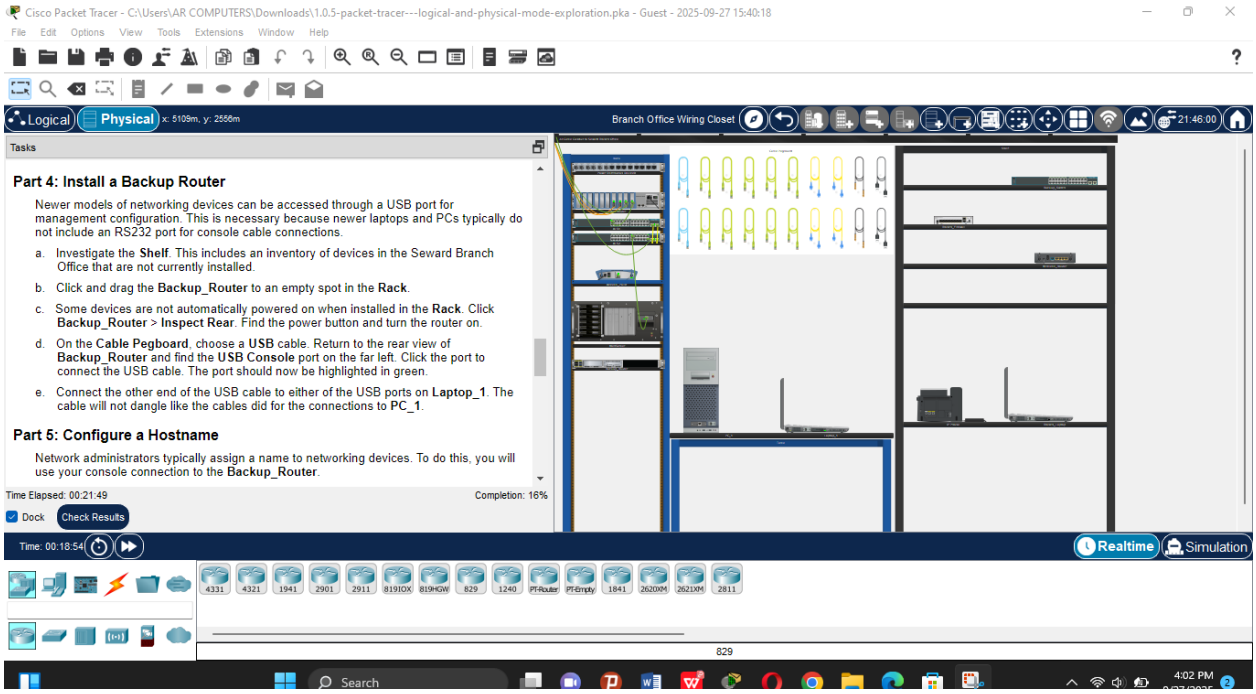

Figure 3

The Backup_Router was powered on from its rear panel. A USB cable was then connected from the Cable Pegboard to the router's USB Console port for management.

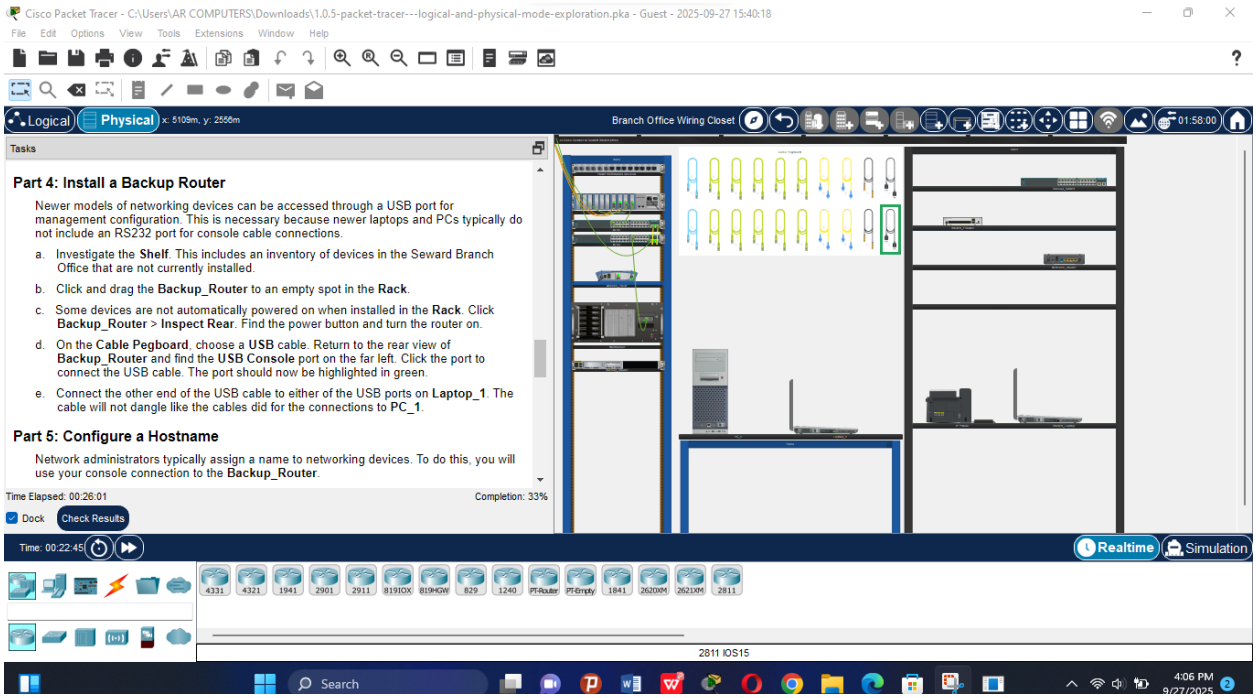

Figure 4

b. Connect the other end of the USB cable to either of the USB ports on **Laptop_1**. The cable will not dangle like the cables did for the connections to **PC_1**.

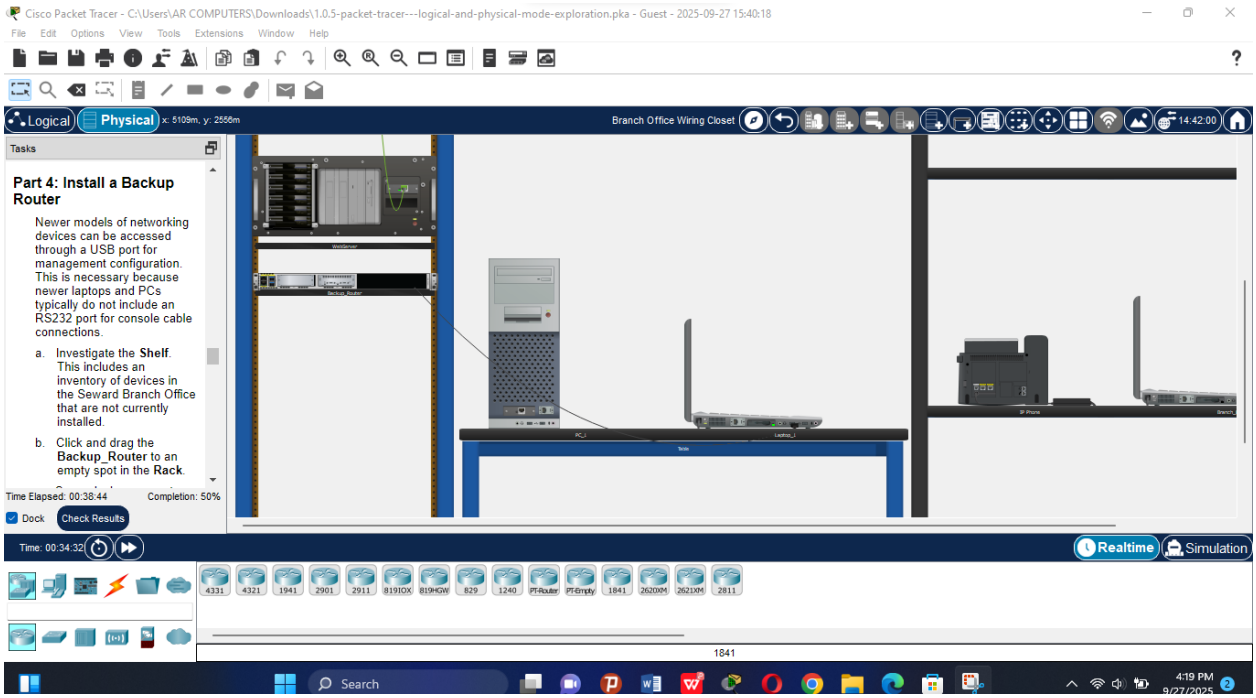

Figure 5

Part 5: Configure a Hostname

The Terminal application on Laptop_1 was accessed to establish a console connection with the Backup_Router..

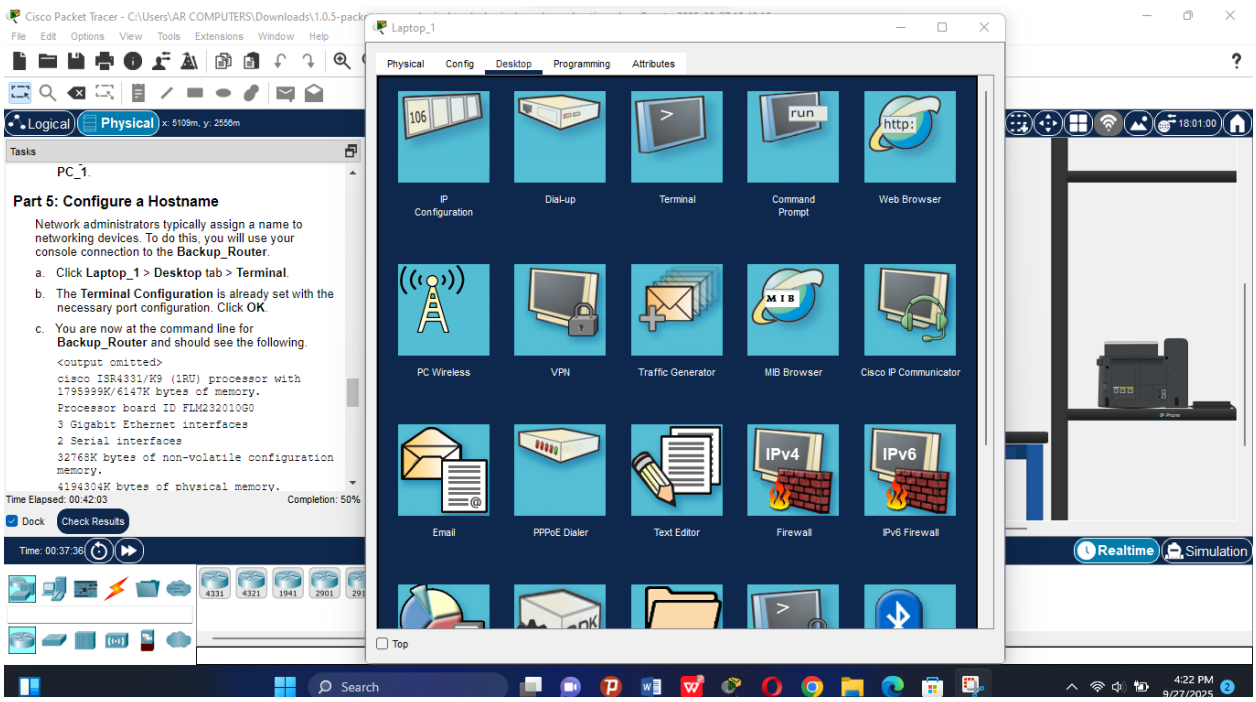

Figure 6

The terminal session was started, and the initial configuration dialog was declined by answering "no".

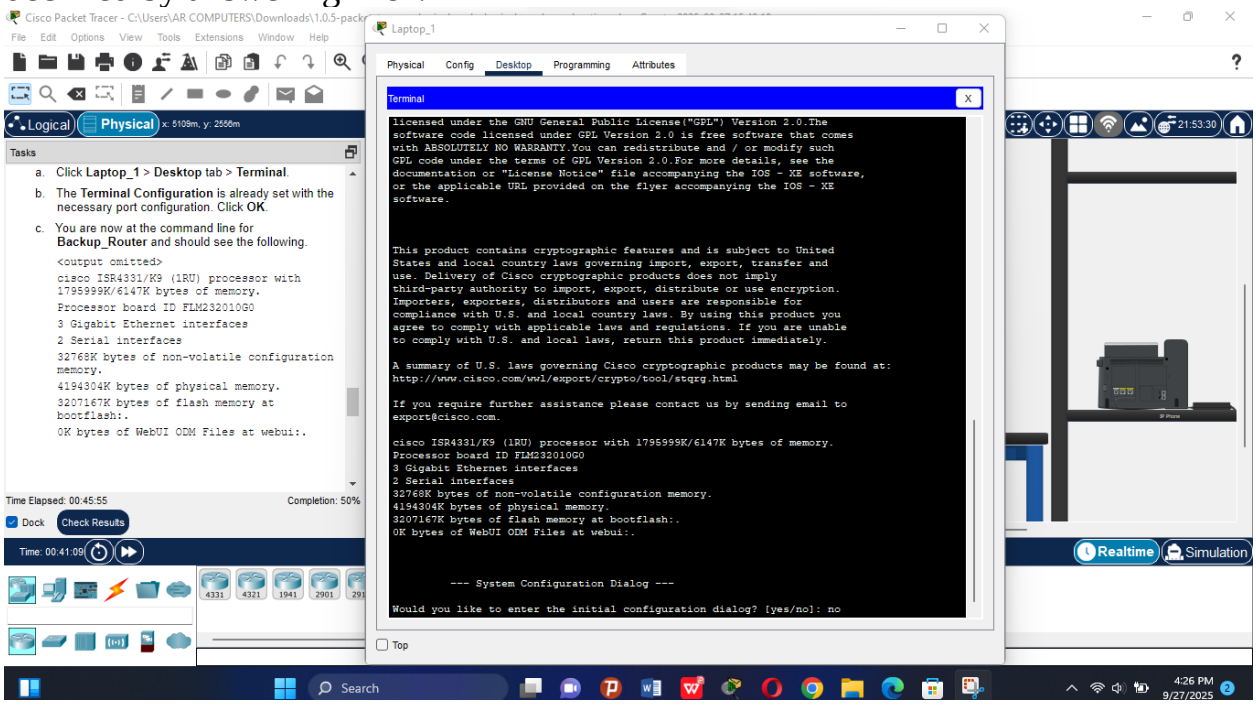

Figure 7

The router was configured with the hostname **Edge_Router_Backup** using the command line interface. The commands enable, configure terminal,

and hostname Edge_Router_Backup were successfully executed, changing the prompt from Router to Edge_Router_Backup.

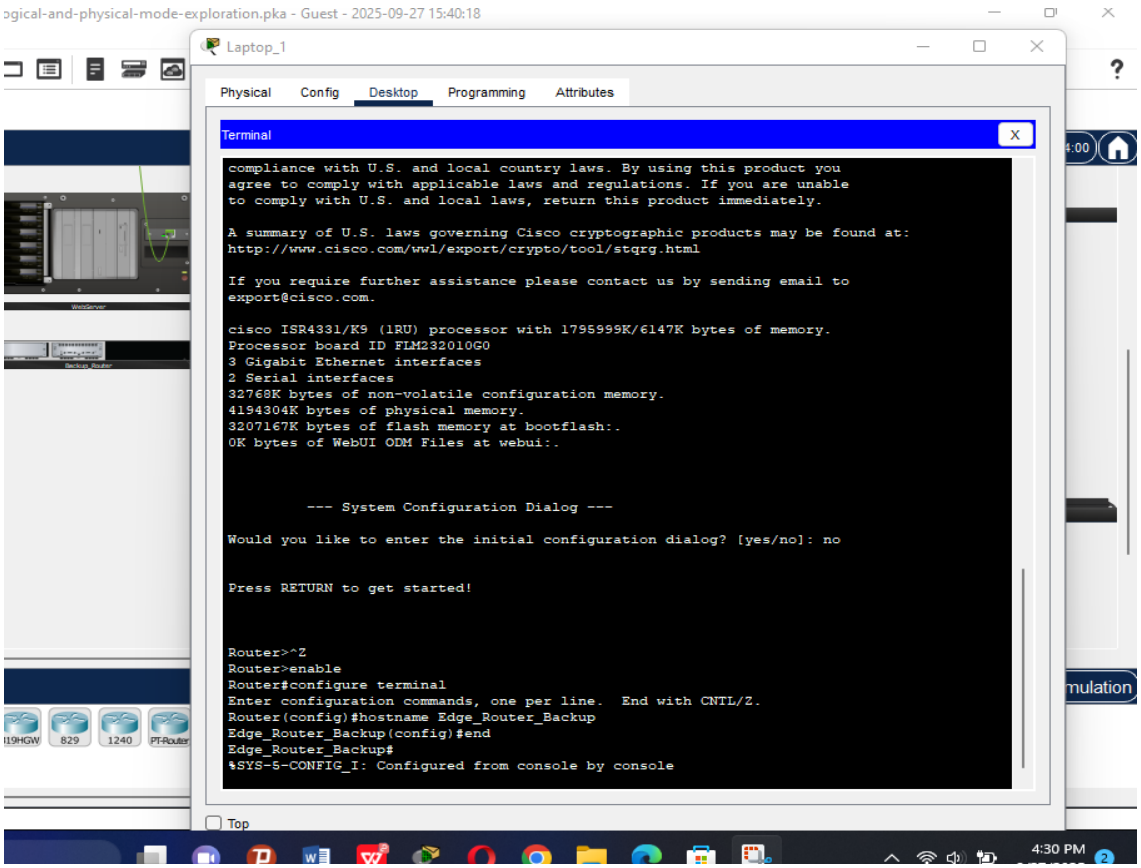

Figure 8

Display name remained as Backup_Router while hostname changed to Edge_Router_Backup, showing Packet Tracer maintains separate name settings.

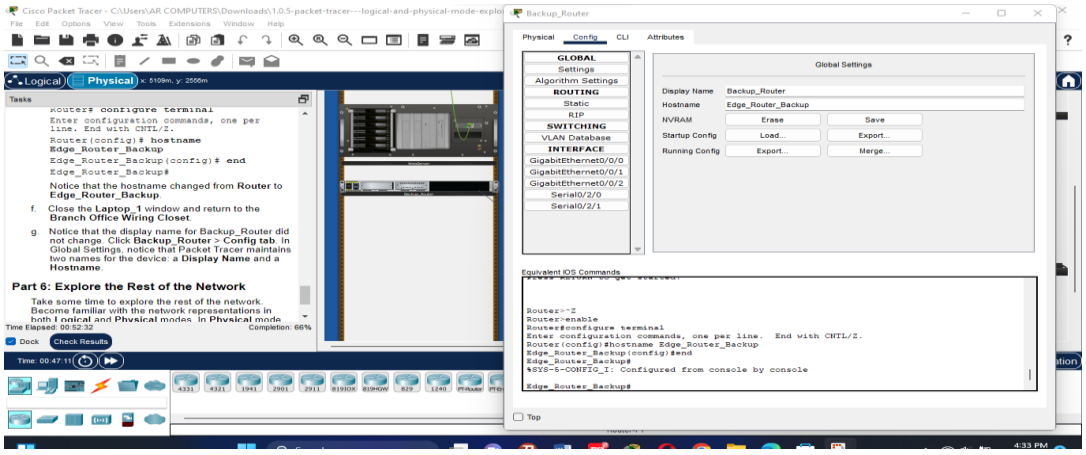

Figure 9

Part 6: Explore the Rest of the Network

The wider network, including the Wellington Data Center and Teleworker Home, was explored in both Logical and Physical modes to understand the overall topology.

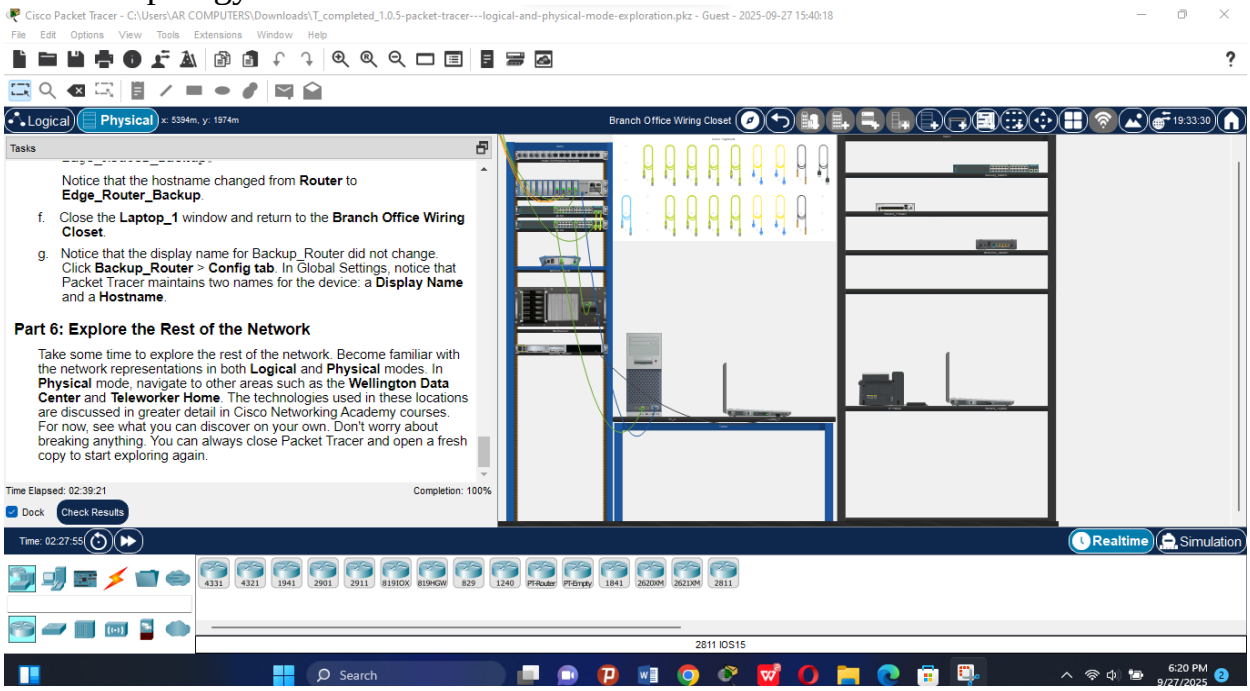

Figure 10

Conclusion

Through this task, I gained practical experience in handling various networking devices and connections in Packet Tracer. I learned how to recognize device categories, establish wired and wireless connections, use console and USB cables for management, and configure a router hostname. This activity improved my understanding of how physical and logical network topologies work together, and how administrators manage devices within a network. Overall, the task provided a strong foundation for building more advanced networking skills.

Task 1.5.5 Network Representation - Packet Tracer

Introduction

This task explored the representation of networks within Cisco Packet Tracer by identifying and analyzing different network components, connections, and topologies. The activity involved recognizing intermediary and end devices, understanding the client-server model, comparing different types of network media, and distinguishing between LANs and WANs. It also provided opportunities to think critically about how real-world businesses and home users connect to the internet.

Objectives

The network model in this activity incorporates many of the technologies that you will master in your CCNA studies. It represents a simplified version of how a small to medium-sized business network might look. Feel free to explore the network on your own. When you are ready, proceed through the following steps and answer the questions.

Note: It is not important that you understand everything you see and do in this activity. Feel free to explore the network on your own. If you wish to proceed more systematically, follow the steps below. Answer the questions to the best of your ability.

Instructions

Step 1: Identify common components of a network as represented in Packet Tracer

The icon toolbar categories were examined. The intermediary device categories are: **Routers, Switches, Hubs, Wireless Devices, and WAN Emulation**.

Network topology analysis revealed:

- Endpoint devices: **15**
- Intermediary devices (excluding clouds): **11**
- Non-desktop end devices: **8**
- Different media connection types: **4**

Step 2: Explain the purpose of the devices

a. In Packet Tracer, only the Server-PT device can act as a server. Desktop or Laptop PCs cannot act as a server. Based on your studies so far, explain the client-server model.

   Answer: In today's networks, a single computer. what we call a "host" is pretty versatile. It is not locked into just one job. What really decides its role is the type of software we install on it.

   For example, when we install software designed to provide information (like a website or an email service), that host becomes a server. Its main purpose is to wait for requests and deliver data to other machines on the network.

   On the other hand, a host becomes a client when we use software that's built to find and display that information. A web browser like Chrome or Firefox is a perfect example of client software; it's all about asking for and showing us web pages.

   The interesting part is that these roles aren't permanent. Any regular computer acting as a client can be turned into a server just by installing server software on it. So, the line between client and server is really defined by the applications we choose to run.

b. List at least two functions of intermediary devices.

   Answer: Network devices perform several critical functions to keep data moving efficiently and securely. They regenerate signals to maintain signal strength over distances and use routing information to find the best paths across the network. When errors or broken links occur, these devices alert others and can automatically redirect traffic along backup pathways to avoid disruptions. They also intelligently manage traffic by classifying messages based on priority, ensuring that time-sensitive data, like video calls, gets through first. Finally, they act as gatekeepers by enforcing security policies, deciding which data is permitted to pass through and which should be blocked.

c. List at least two criteria for choosing a network media type.

Answer: When selecting network cabling, several key factors must be considered. The first is the maximum distance the cable can carry a signal without it degrading. Next, you have to evaluate the physical environment where the cable will be installed, such as whether it will be run indoors, outdoors, or in areas with electrical interference. The required speed and volume of data transmission is another critical factor, as different media have different capabilities. Finally, the overall cost of the media itself and the expense of installing it will always play a decisive role in the final choice.

Step 3: Compare and contrast LANs and WANs

a. Explain the difference between a LAN and a WAN. Give examples of each.

Answer: The main difference between a LAN and a WAN comes down to geographical scale. A LAN (Local Area Network) connects devices within a confined area, like a single home, office building, or school campus, providing network access to a localized group of users.

In contrast, a WAN (Wide Area Network) covers a much broader geographical area, which can range from a few miles to spanning entire countries or continents. The most common example of a WAN is the internet itself. Other examples include a MAN (Metropolitan Area Network), which connects a city, and the private networks that large companies use to link their remote offices together into a single corporate intranet.

b. In the Packet Tracer network, how many WANs do you see?

Answer: There are two the Internet and the Intranet WANs.

c. How many LANs do you see?

Answer: You can easily spot all three of them because each one is outlined with a distinct border and has its own label.

d. The internet in this Packet Tracer network is overly simplified and does not represent the structure and form of the real internet. Briefly describe the internet.

Answer: The Internet comes into play primarily when we need to access information or services located outside of our own immediate network.

Essentially, it functions as a massive, worldwide web of interconnected smaller networks, creating a global system of internetworks.

e. What are some of the common ways a home user connects to the internet?

Answer: DSL, dial-up, Cable, cellular, and satellite

f. What are some common methods that businesses use to connect to the internet in your area?

Answer: In my area, businesses typically connect to the internet using several methods. Common options include high-reliability dedicated leased lines, Metro Ethernet (Metro-E) for fast metropolitan-area connections, and more widely available services like DSL and cable. For businesses in remote locations where wired options are limited, satellite internet is also a viable choice.

Challenge Question

The activity provided optional challenges to practice expanding networks, including adding new end devices and intermediary equipment to existing LANs, plus creating completely new multi-LAN networks in separate Packet Tracer files for further exploration.

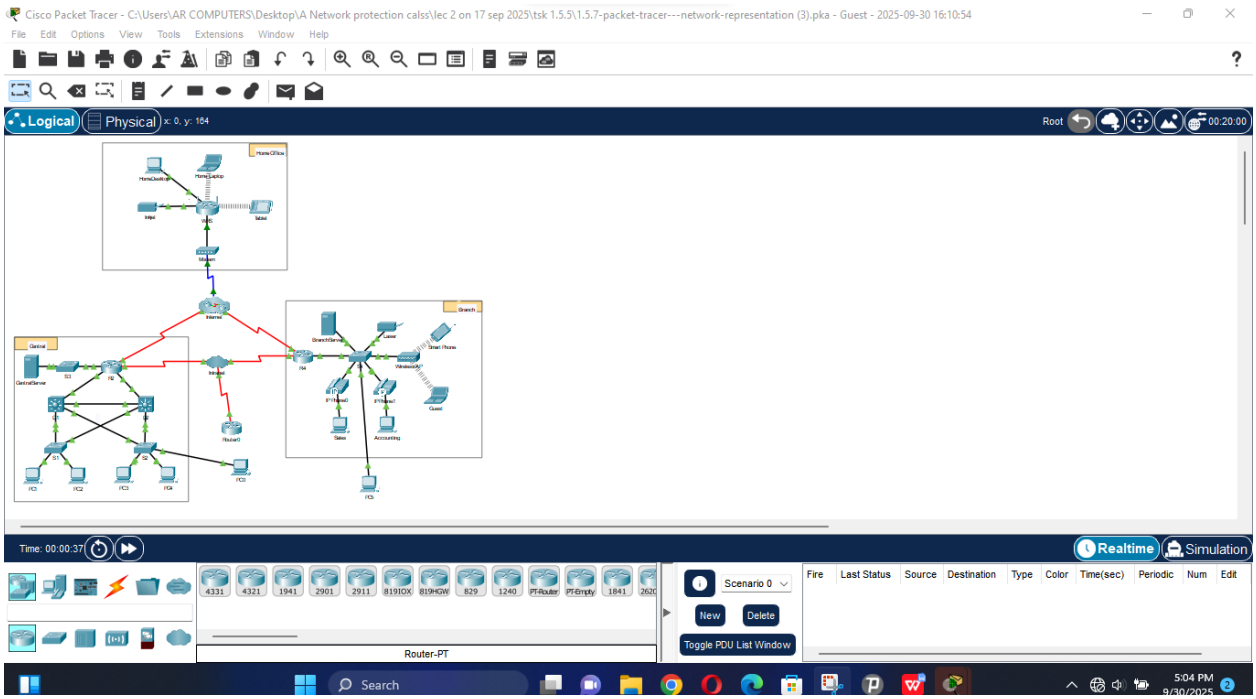

Figure 11

Conclusion

By completing this task, I developed a stronger understanding of how Packet Tracer models real-world network environments. I learned to identify device roles, explain their functions, and compare network scales such as LANs and WANs. Additionally, the task highlighted the importance of media selection, intermediary device functions, and different internet connection methods for both home and business use. Overall, this activity deepened my foundational knowledge of network representation and prepared me for more advanced design and troubleshooting exercises.

Task 2.3.7 Navigate the IOS - Packet Tracer

Introduction

This task focused on navigating the Cisco IOS within Packet Tracer by practicing the use of different EXEC modes, configuration commands, and context-sensitive help. The activity included establishing console connections, accessing the command-line interface (CLI), exploring IOS help functions, switching between user and privileged EXEC modes, and learning how to set the system clock. These exercises provided hands-on experience with the fundamental commands and workflows that network administrators use daily.

Objectives

Part 1: Establish Basic Connections, Access the CLI, and Explore Help

Part 2: Explore EXEC Modes

Part 3: Set the Clock

Background / Scenario

In this activity, you will practice skills necessary for navigating the Cisco IOS, such as different user access modes, various configuration modes, and common commands used on a regular basis. You will also practice accessing the context-sensitive Help by configuring the **clock** command.

Instructions

Part 1: Establish Basic Connections, Access the CLI, and Explore Help

Step 1: Connect PC1 to S1 using a console cable.

a. A console cable was used to connect PC1 to switch S1. The cable was attached to the RS-232 port on PC1 and the Console port on S1.

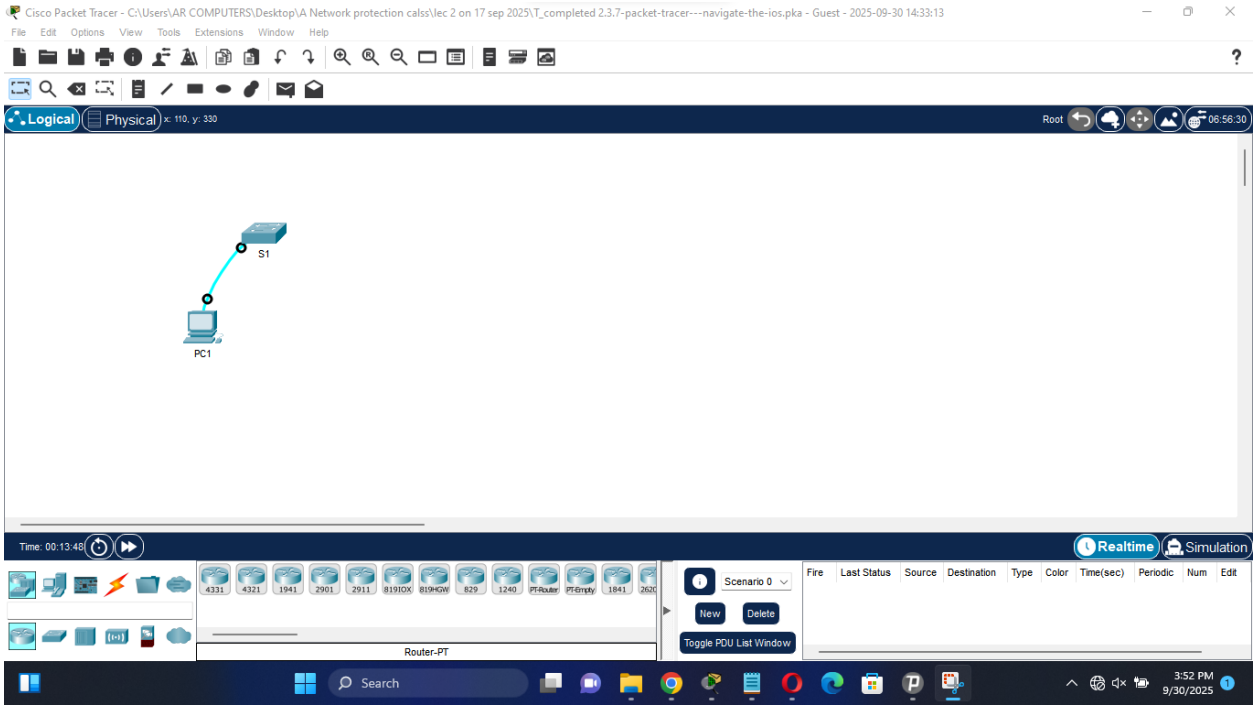

Figure 12

Step 2: Establish a terminal session with S1.

The Terminal application on PC1 was accessed. The terminal was configured with **9600** bits per second. After pressing Enter, the prompt displayed was **S1>**.

Step 3: Explore the IOS Help.

Context-sensitive help was used. The command beginning with 'C' is connect. After typing t?, the commands displayed were telnet, terminal, traceroute. After typing te?, the commands displayed were telnet terminal.

Part 2: Explore EXEC Modes

In Part 2 of this activity, you will switch to privileged EXEC mode and issue additional commands

Step 1: Enter privileged EXEC mode.

Using help and command completion:

- The enable command description is "**Turn on privileged commands**"

- Typing en<Tab> completes to **enable**
- After entering enable mode, the prompt changed from **S1>** to **S1#**
- In privileged EXEC mode, **5** commands begin with 'C': clear, clock, configure, connect, copy

Step 2: Enter Global Configuration mode

The configure command was entered in privileged EXEC mode, displaying the message: **"Configuring from terminal, memory, or network [terminal]?"** After pressing Enter to accept the default, the prompt changed to **S1(config)#**, indicating global configuration mode. The exit command was then used to return to privileged EXEC mode (**S1#**).Part 3: Set the Clock

Step 1: Use the clock command.

The show clock command displayed the time as **UTC Mon Mar 1 1993**, showing the year as **1993**. Attempting to set the time with the incomplete clock command resulted in a "**% Incomplete command**" error. Using help (clock ?), the parameter "**set**" was identified. Further help (clock set ?) specified the required time format "**hh:mm:ss**". The command clock set 15:00:00 31 Jan 2035 was used to successfully configure the time. Verification with show clock confirmed the new setting: ***15:0:4.869 UTC Tue Jan 31 2035**.

Step 2: Explore additional command messages.

Testing incomplete/incorrect commands returned these errors:

- cl<Tab>: **% Ambiguous command: "cl"**
- clock: **% Incomplete command**
- clock set 25:00:00: **% Invalid input detected** (invalid time)
- clock set 15:00:00 32: **% Invalid input detected** (invalid date)

Conclusion

By completing this task, I gained valuable practice in interacting with Cisco IOS and understanding the differences between user EXEC, privileged EXEC, and global configuration modes. I also learned how to use context-sensitive

help to build and complete commands, troubleshoot errors, and correctly configure the device clock. Overall, this activity strengthened my command-line navigation skills and provided a solid foundation for more advanced network configuration and management tasks.