Faculty of Engineering and Technology

Department of Electrical and Computer Engineering

ENCS3320 – Computer Networks (Term 1242)

Project #2 (Cisco Packet Tracer)

Team Members

Aya AbuSneineh	**1221414**	**Section: 4**
Ahmad Sous	**1221371**	**Section: 4**
Mousa Zahran	**1220716**	**Section: 4**

Date : June, 19, 2025

Table of Contents

Table of figures

Theory and Procedure

1. IP Addressing and Subnetting

In computer networks, IP addressing and subnetting are essential to ensure that every device (host) can communicate within its own network and with other networks. Subnetting is the process of dividing a larger IP address block into smaller, manageable subnetworks (subnets), each with a specific range of addresses. This allows efficient utilization of IP addresses, improved network performance, and simplified management and routing.

The primary goal of subnetting is to allocate IP address ranges to different parts of a network based on the number of required hosts, while minimizing waste. For each subnetwork, the following elements must be identified:

- **Network Address**: The starting IP address of the subnet (all host bits are 0).
- **Broadcast Address**: The last IP address in the subnet (all host bits are 1).
- **Usable IP Range**: The range of IPs that can be assigned to devices (from Network +1 to Broadcast -1).
- **Subnet Mask**: Determines how many bits are used for the network portion; can be expressed in **CIDR notation** (e.g., /26).

In this project, we use **Variable Length Subnet Masking (VLSM)** to allocate address space efficiently, assigning larger subnets to networks with more hosts and smaller ones to those with fewer. This method helps avoid IP address wastage and improves routing efficiency in the network topology.

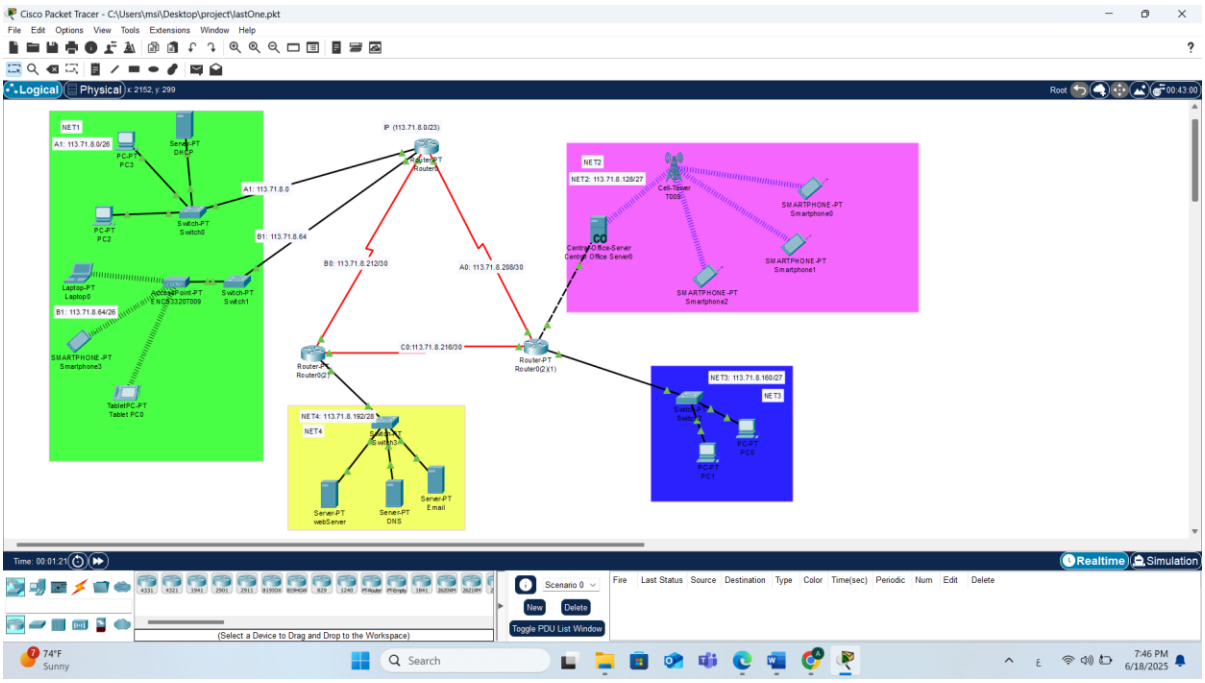


Figure 1:Complete Network Topology

As shown in Figure 1, each network in the topology requires a different number of hosts. Therefore, we performed on the main IP address block 113.71.8.0/23 to efficiently allocate IP addresses without wasting address space.

To calculate the number of usable IP addresses in any subnet, we use the following simple rule:

Usable IPs = $2^{(32 - \text{CIDR})} - 2$

This minus two because:

- 1 address is reserved for the network address
- 1 address is reserved for the broadcast address

For each subnet, the following values were calculated:

- The Network Address (first address in the block)
- The First Usable IP (Network + 1)
- The Last Usable IP (Broadcast - 1)
- The Broadcast Address (last address in the block)

Core-Router Link A0: 113.71.8.208/30

113.71.8.11010000

- Subnetwork: A0

- Required Hosts: 2
- Subnet Address: 113.71.8.208
- Network Address: 113.71.8.208
- First IP: 113.71.8.209
- Last IP: 113.71.8.210
- Broadcast Address: 113.71.8.211
- CIDR: /30
- Subnet Mask: 255.255.255.252

Core-Router Link B0: 113.71.8.212/30

113.71.8.11010100

- Subnetwork: B0
- Required Hosts: 2
- Subnet Address: 113.71.8.212
- Network Address: 113.71.8.212
- First IP: 113.71.8.213
- Last IP: 113.71.8.214
- Broadcast Address: 113.71.8.215
- CIDR: /30
- Subnet Mask: 255.255.255.252

Core-Router Link C0: 113.71.8.216/30

113.71.8.11011000

- Subnetwork: C0
- Required Hosts: 2
- Subnet Address: 113.71.8.216
- Network Address: 113.71.8.216
- First IP: 113.71.8.217
- Last IP: 113.71.8.218
- Broadcast Address: 113.71.8.219
- CIDR: /30

- Subnet Mask: 255.255.255.252

Uninversity-NET1-A: 113.71.8.0/26

113.71.8.00000000

- Subnetwork: NET1-A
- Required Hosts: 60
- Subnet Address: 113.71.8.0
- Network Address: 113.71.8.0
- First IP: 113.71.8.1
- Last IP: 113.71.8.62
- Broadcast Address: 113.71.8.63
- CIDR: /26
- Subnet Mask: 255.255.255.192

Uninversity-NET1-B: 113.71.8.64/26

113.71.8.01000000

- Subnetwork: NET1-B
- Required Hosts: 60
- Subnet Address: 113.71.8.64
- Network Address: 113.71.8.64
- First IP: 113.71.8.65
- Last IP: 113.71.8.126
- Broadcast Address: 113.71.8.127
- CIDR: /26
- Subnet Mask: 255.255.255.192

Street-NET2: 113.71.8.128/27

113.71.8.10000000

- Subnetwork: NET2
- Required Hosts: 30
- Subnet Address: 113.71.8.128
- Network Address: 113.71.8.128

- First IP: 113.71.8.129
- Last IP: 113.71.8.158
- Broadcast Address: 113.71.8.159
- CIDR: /27
- Subnet Mask: 255.255.255.224

New Subnets

- ***First Subnet (/28)***
- Subnet Address: 113.71.8.128
- Usable IPs: 113.71.8.129 to 113.71.8.142
- Broadcast: 113.71.8.143
- Example: Central Office Server = 113.71.8.130
- ***Second Subnet (/28)***
- Subnet Address: 113.71.8.144
- Usable IPs: 113.71.8.145 to 113.71.8.158
- Broadcast: 113.71.8.159
- Example: Cell Tower = 113.71.8.145

Home-NET3: 113.71.8.160/27

113.71.8.10100000

- Subnetwork: NET3
- Required Hosts: 20
- Subnet Address: 113.71.8.160
- Network Address: 113.71.8.160
- First IP: 113.71.8.161
- Last IP: 113.71.8.190
- Broadcast Address: 113.71.8.191
- CIDR: /27
- Subnet Mask: 255.255.255.224

Datacenter-NET4: 113.71.8.192/28

113.71.8.11000000

- Subnetwork: NET4
- Required Hosts: 15
- Subnet Address: 113.71.8.192
- Network Address: 113.71.8.192
- First IP: 113.71.8.193
- Last IP: 113.71.8.206
- Broadcast Address: 113.71.8.207
- CIDR: /28
- Subnet Mask: 255.255.255.240

2. Building Topology Task

1. Core network (Area 0)

Area 0 forms the backbone of the network and interconnects all other areas. It includes **three routers** connected via **point-to-point serial links**, with each connection assigned to a dedicated subnet: **NET0-A**, **NET0-B**, and **NET0-C**.

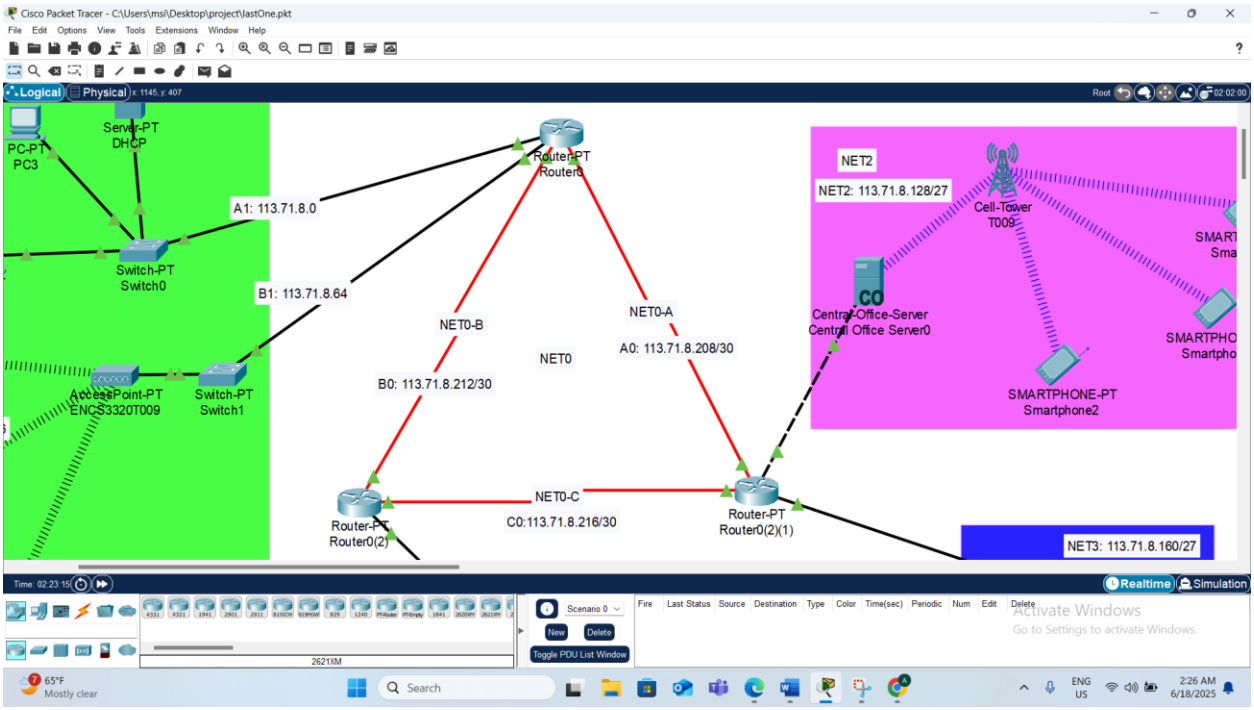


Figure 2:Area 0 topology with three routers connected via serial links

We configured **static IP addresses** on all router interfaces manually, based on the subnetting plan.

The following interface types were used:

- **FastEthernet (F0/0, F0/1):** for LAN connections
- **Serial (S0/0/0, S0/0/1):** for WAN connections between routers

Configuration Summary:

- **Area:** 0 (Backbone)
- **Devices:** 3 Routers (Router-PT)
- **Subnetworks:** NET0-A, NET0-B, NET0-C

- **IP Assignment:** Static, based on subnetting
- **Routing Protocol:** OSPF (Area 0)

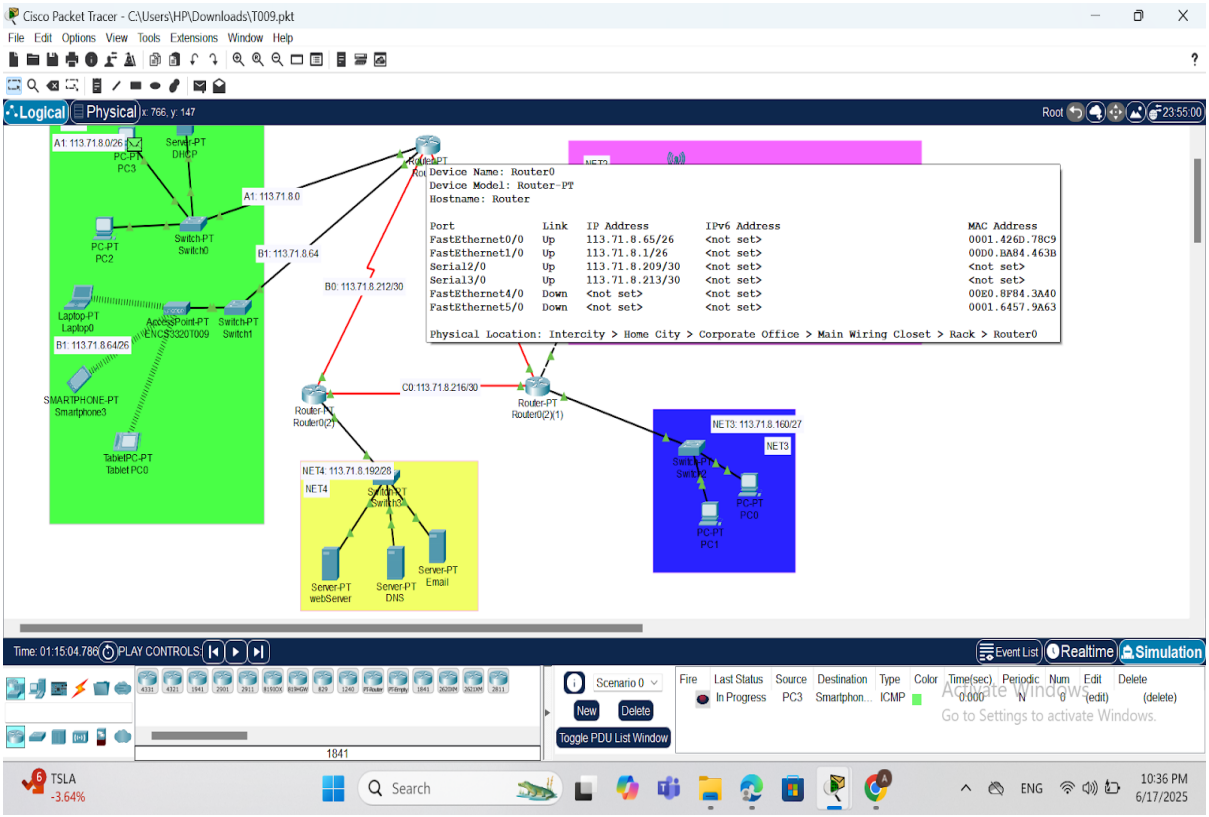


Figure 3:Static IP configuration on Router0's FastEthernet and Serial interfaces based on subnetting plan

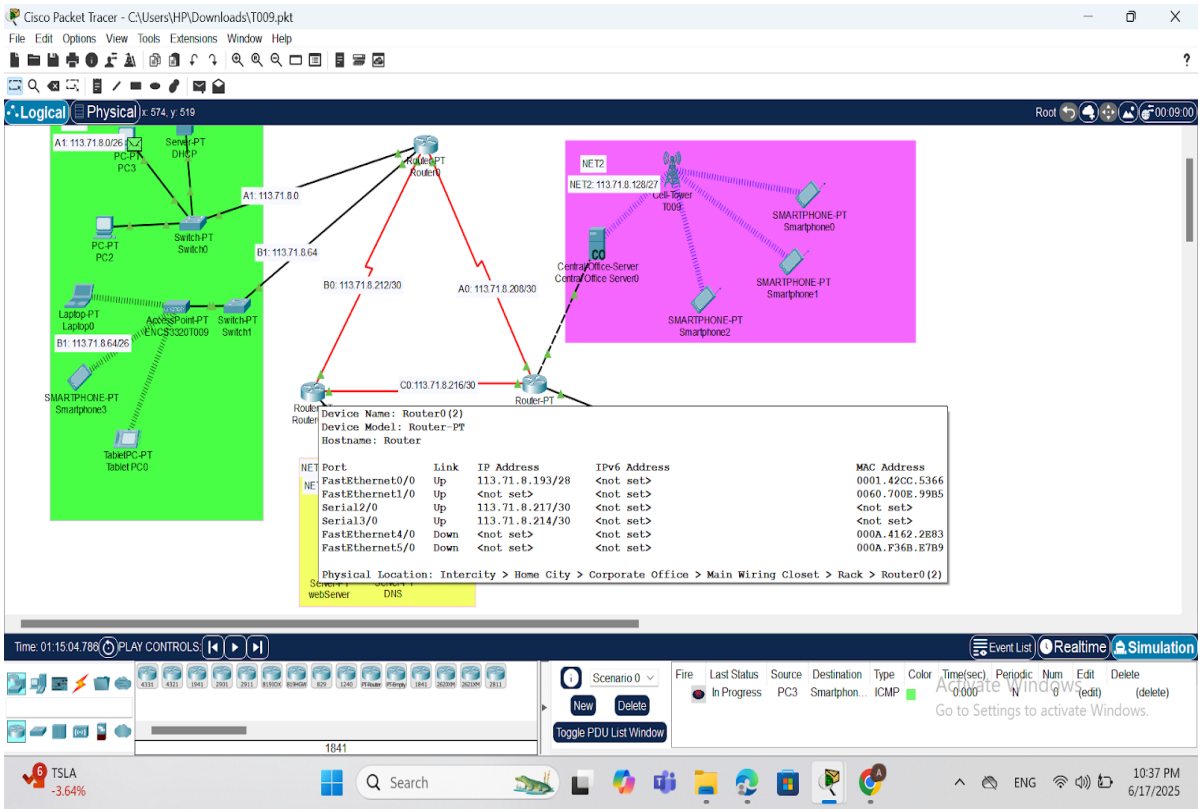


Figure 4:Static IP configuration on Router0(2)'s FastEthernet and Serial interfaces based on subnetting plan

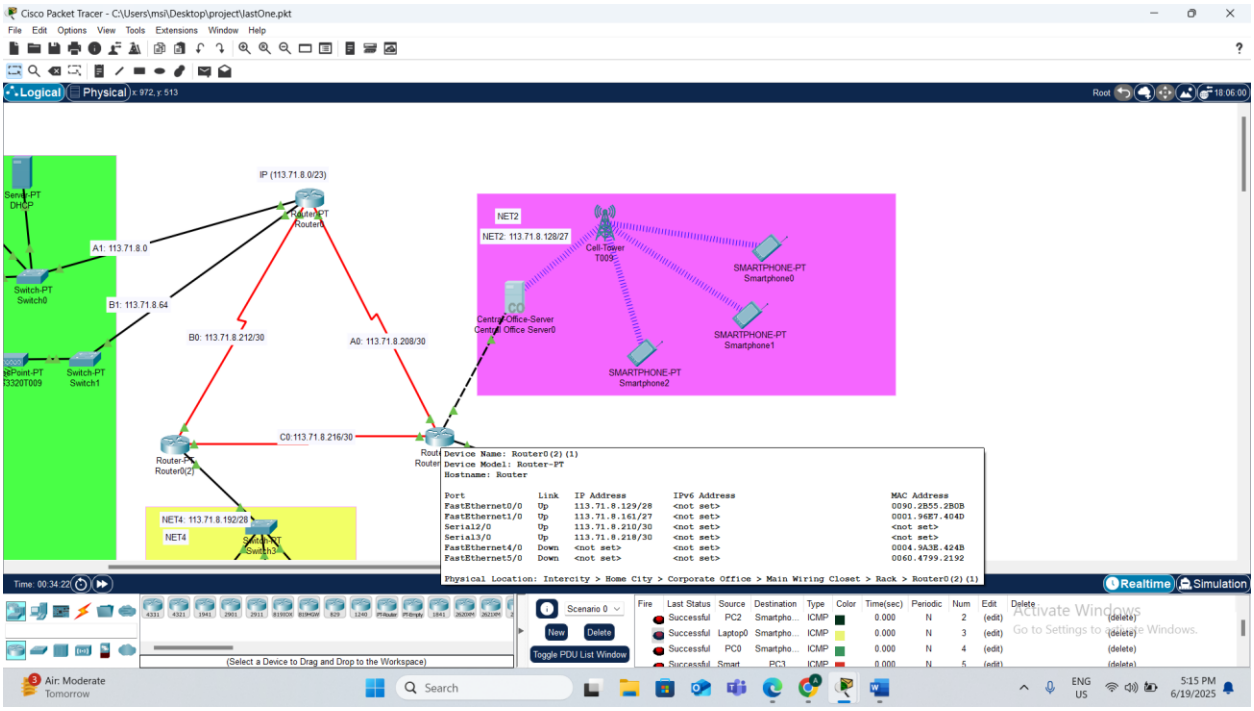


Figure 5:Static IP configuration on Router2(1)'s FastEthernet and Serial interfaces based on subnetting plan

2. University Network – Area 1 (NET1)

Area 1 represents the **University Network** and contains two subnetworks: **NET1-A** and **NET1-B**. It is connected to the core network (Area 0) via a dedicated router interface. The setup involves both wired and wireless access, with dynamic IP addressing for end devices.

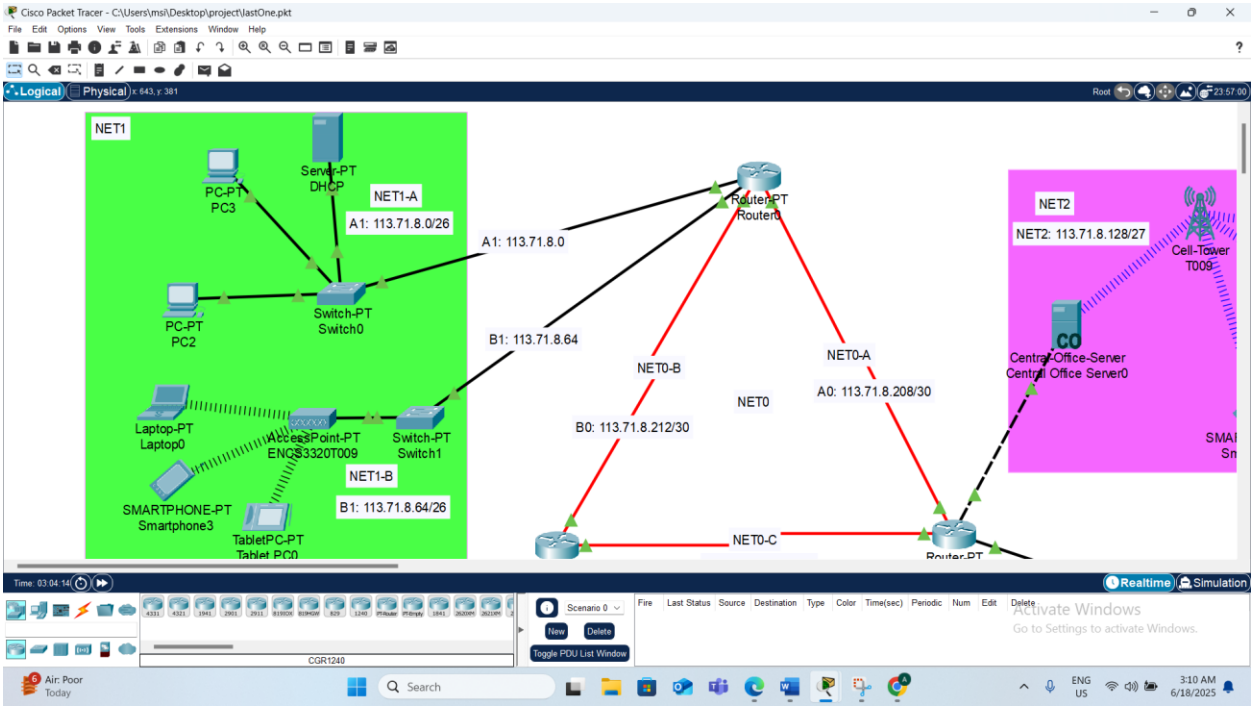


Figure 6:Area1

A. NET1-A (University Network - Subnetwork A)

NET1-A is a wired network within the university network connected through a switch and linked to the university router. Static IP addresses were assigned to the router and switch interfaces based on the subnetting plan to ensure efficient network organization.

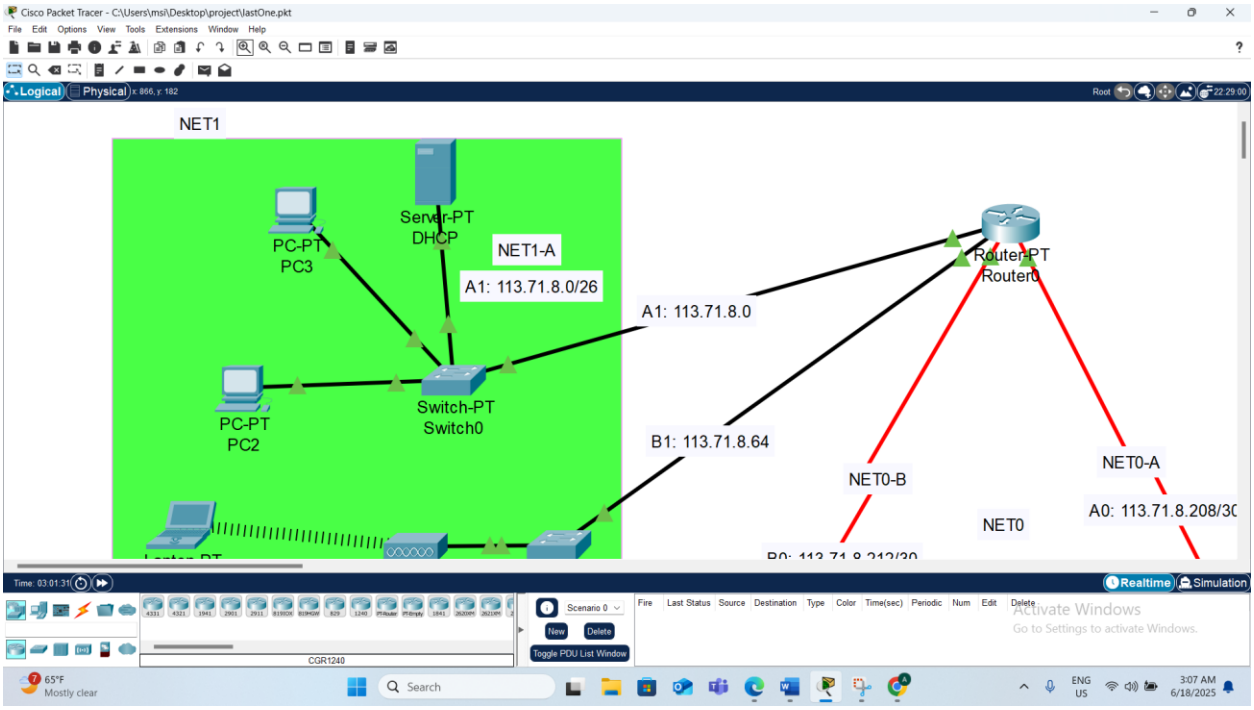


Figure 7:NET1-A

In this network, the **DHCP** service was enabled to automatically assign IP addresses to connected devices such as desktop and laptop computers, simplifying management and reducing errors caused by manual configuration. The DHCP server is responsible for distributing IP addresses as well as essential network information like the default gateway, subnet mask, and DNS server.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used to automatically assign Internet Protocol (IP) addresses and other related configuration parameters to network devices (hosts), such as desktop computers, laptops, tablets, mobile phones, or thin clients. Each host requires a unique IP address to communicate effectively across the network or the internet [1].

Instead of relying on manual IP configuration, DHCP automates this process, thereby minimizing configuration errors and administrative overhead. Furthermore, DHCP supports dynamic reassignment of IP addresses when devices are relocated within the network. In addition to IP addresses, DHCP servers also distribute essential parameters such as the **Subnet Mask**, **Default Gateway**, and **DNS server address**, which are crucial for proper routing and name resolution in the network [1].

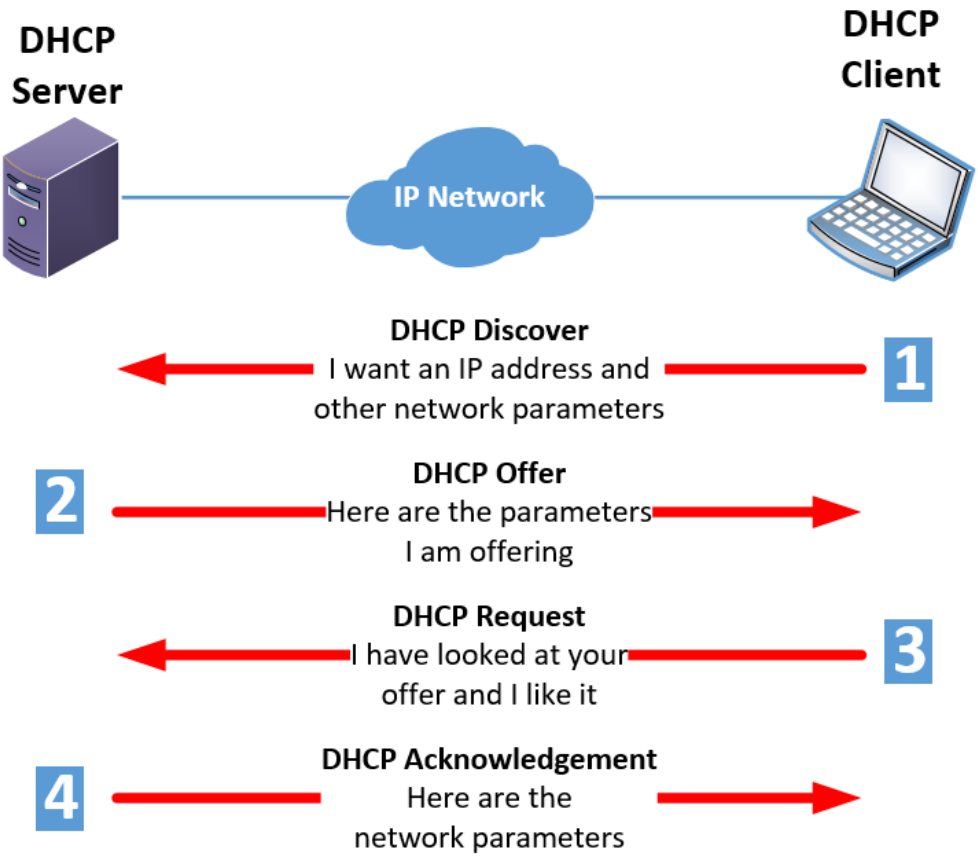


Figure 8: How DHCP Protocol Works [2]

Advantages of DHCP:

Automatic IP Assignment: Saves time and avoids manual errors by automatically assigning IP addresses.

Simplifies Network Management: Centralized control makes managing large networks easier.

Efficient Use of IP Addresses: Recycles unused IP addresses, optimizing address allocation.

Supports Mobile Devices: Devices get new IPs automatically when they move between network

Disadvantages of DHCP:

Single Point of Failure: If the DHCP server goes down, devices can't get IP addresses and lose connectivity.

Security Risks: Without proper security, unauthorized devices might connect to the network.

IP Address Conflicts: Mismanagement can cause overlapping IP assignments.

Limited for Static IPs: DHCP is less suited for devices needing permanent IP addresses, like servers.

Practical Implementation in the Project:

The DHCP service was implemented within the **University Network (NET1-A)**. A **DHCP server (Server-PT)** was connected to the first switch in the network alongside **two PCs (PC-PT)**, which received their IP addresses automatically from the DHCP server.

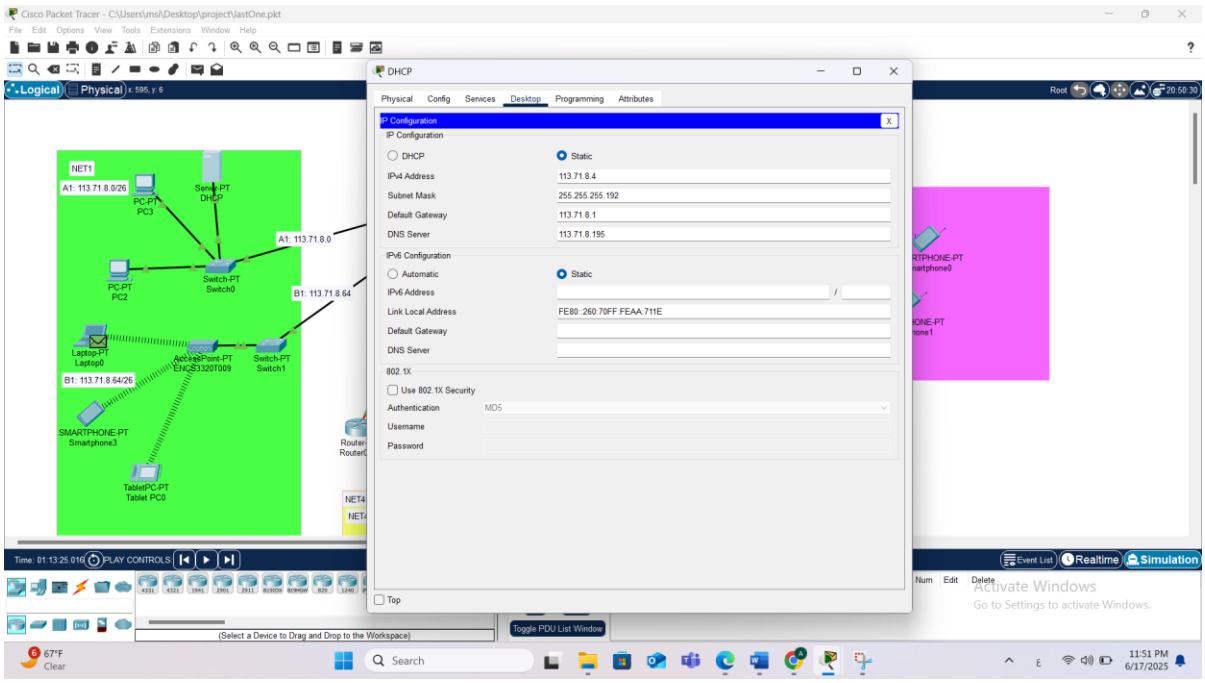


Figure 9:Static IP configuration for the DHCP server in NET1-A

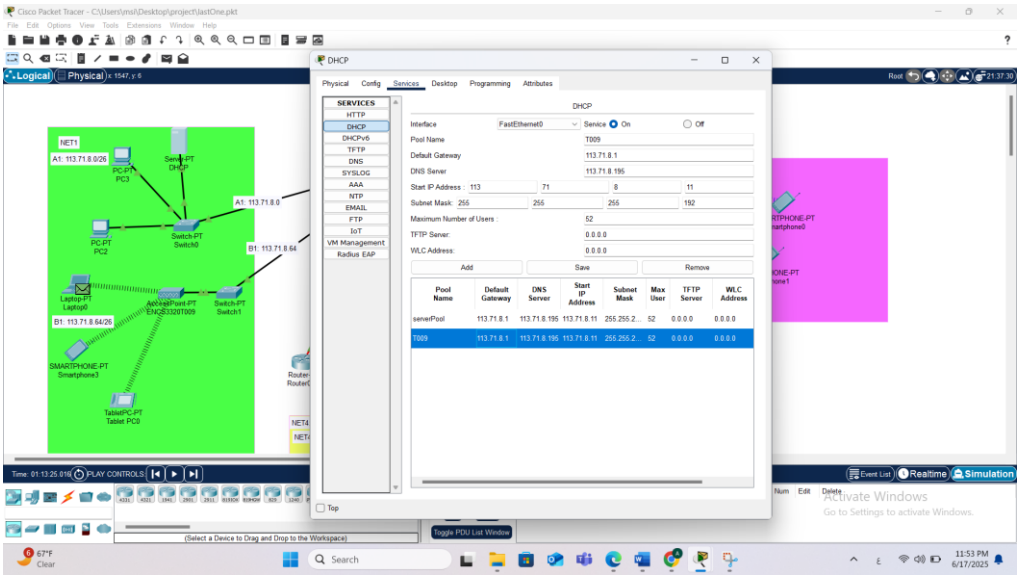


Figure 10:DHCP pool settings including gateway, DNS, start IP, and subnet mask

The server was configured as follows:

- **Only the DHCP service was enabled**.
- **Static IP address assigned to the server**: 113.71.8.4
- **Pool Name**: T009
- **Default Gateway**: 113.71.8.1 (router interface in NET1-A)
- **DNS Server**: 113.71.8.195 (IP address of dns.coe.birzeit.edu)
- **Start IP Address**: 113.71.8.11 (first usable IP address after excluding the first 10 addresses)
- **Subnet Mask**: 255.255.255.192
- **Maximum Number of Users**: 52 (total usable addresses after exclusions)

Justification for Using DHCP:

DHCP was chosen to provide a flexible and efficient method for distributing IP addresses within the network. This reduces the need for manual configuration and minimizes the risk of errors. It is particularly suitable for environments with mobile or frequently changing devices, such as laptops and smart devices, enabling automated and accurate IP configuration and network connectivity.

B. NET1-B (University Network - Subnetwork B)

NET1-B is a wireless network configured using an Access Point connected to the university switch. The network includes several mobile devices such as laptops, tablets, and smartphones that connect wirelessly.

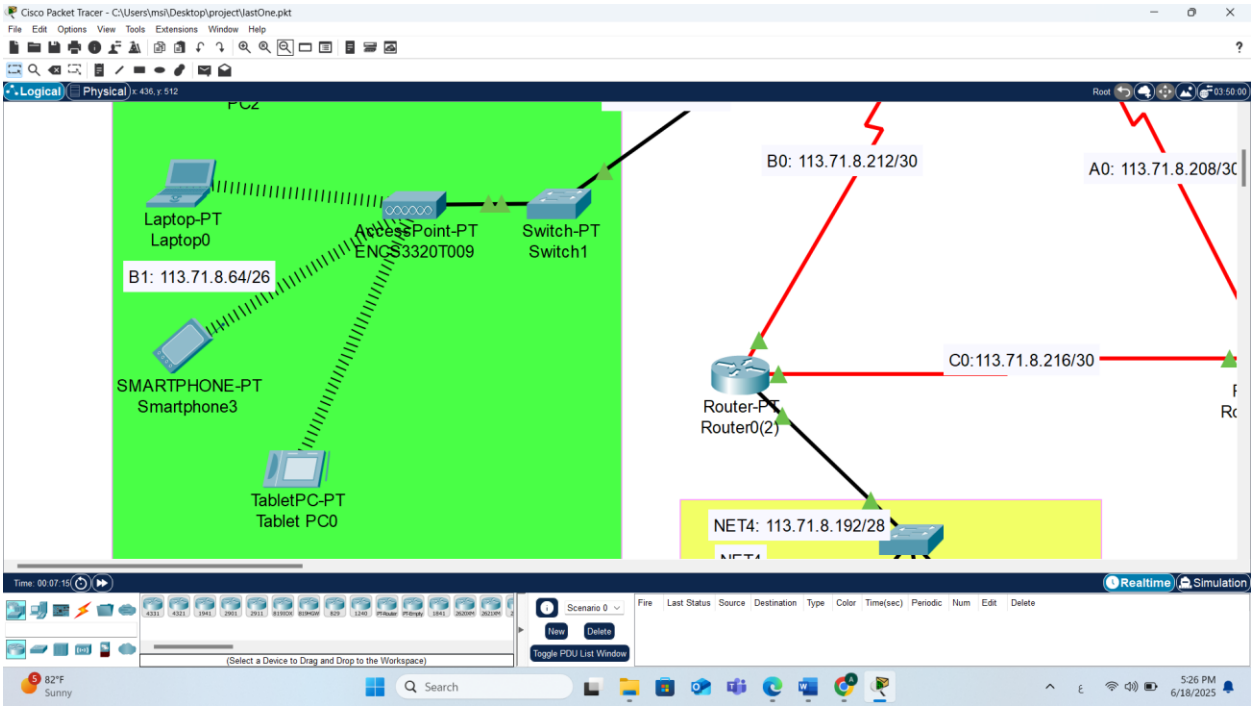


Figure 11:NET1-B

Access Point in NET1-B

The Access Point is a device that allows wireless devices like laptops, tablets, and smartphones to connect to the wired network via radio waves. In NET1-B, the Access Point is connected to the switch to provide secure wireless coverage within the university network.

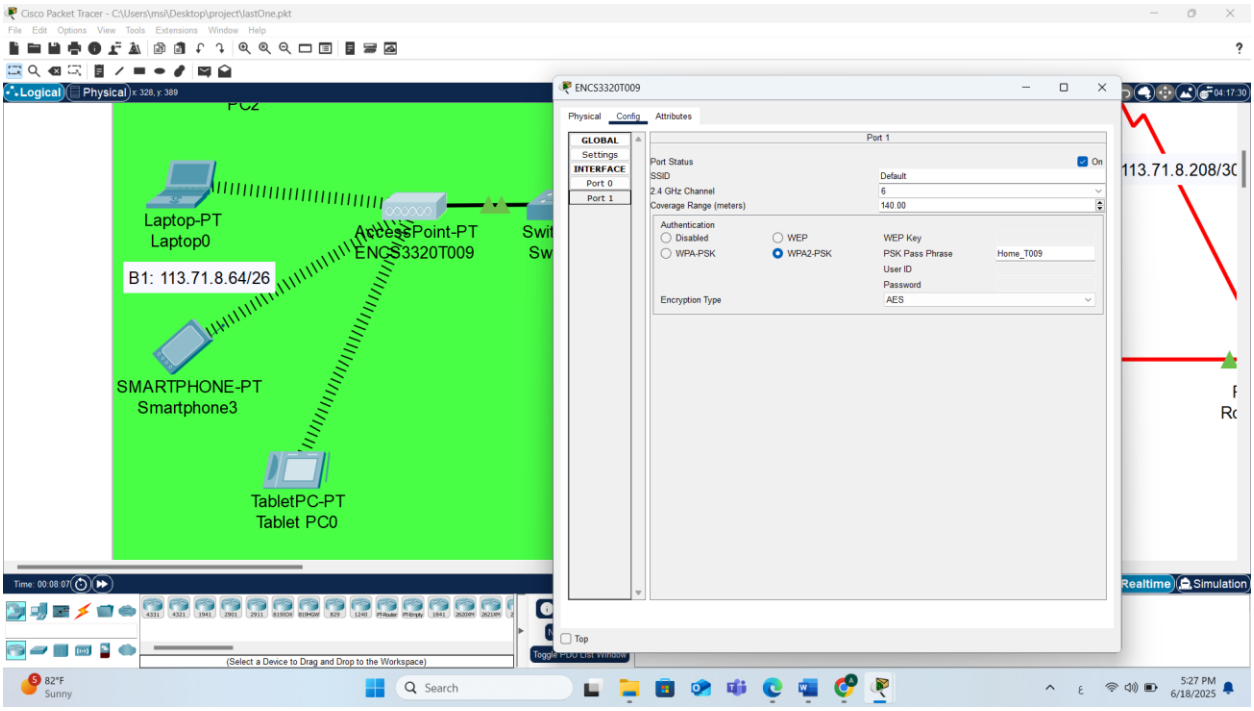


Figure 12:The setting of the access point

The access point was configured using the **WPA2 Personal** security protocol with **AES** encryption, and a team-specific security key was set to: **Home_T009**, ensuring a secure and reliable connection. The access point manages wireless connectivity and provides stable coverage within the university network.

3. Street Network (NET2 – Area 2)

The **Street Network** consists of a single subnet (**NET2**) and serves as the communication layer between smartphones and the central office. The router interface was activated and assigned an IP address based on the subnetting plan. A **Central Office Server (CO Server)** was added and connected directly to the router to serve as a bridge for network services.

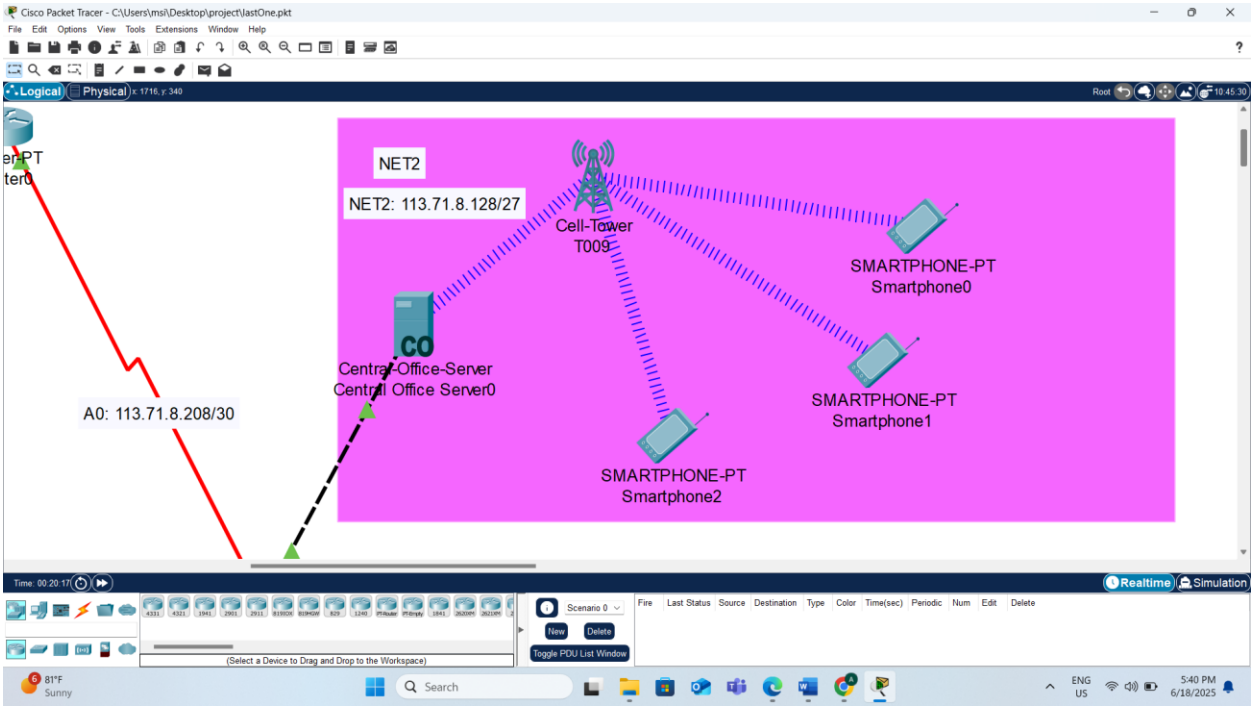


Figure 13:NET2

A **Cell Tower** was added in the **Street Network (NET2)** to simulate mobile connectivity. This tower provides **3G/4G wireless internet access** to smartphones within the area. The tower was configured with the name **T009**, and the **provider name** was also set to **T009**. It was connected directly to the **Central Office Server (CO Server)**, which handles backend communication and network services. Three smartphones were wirelessly connected to the tower, allowing them to access the network and demonstrate realistic mobile connectivity within the simulated environment .

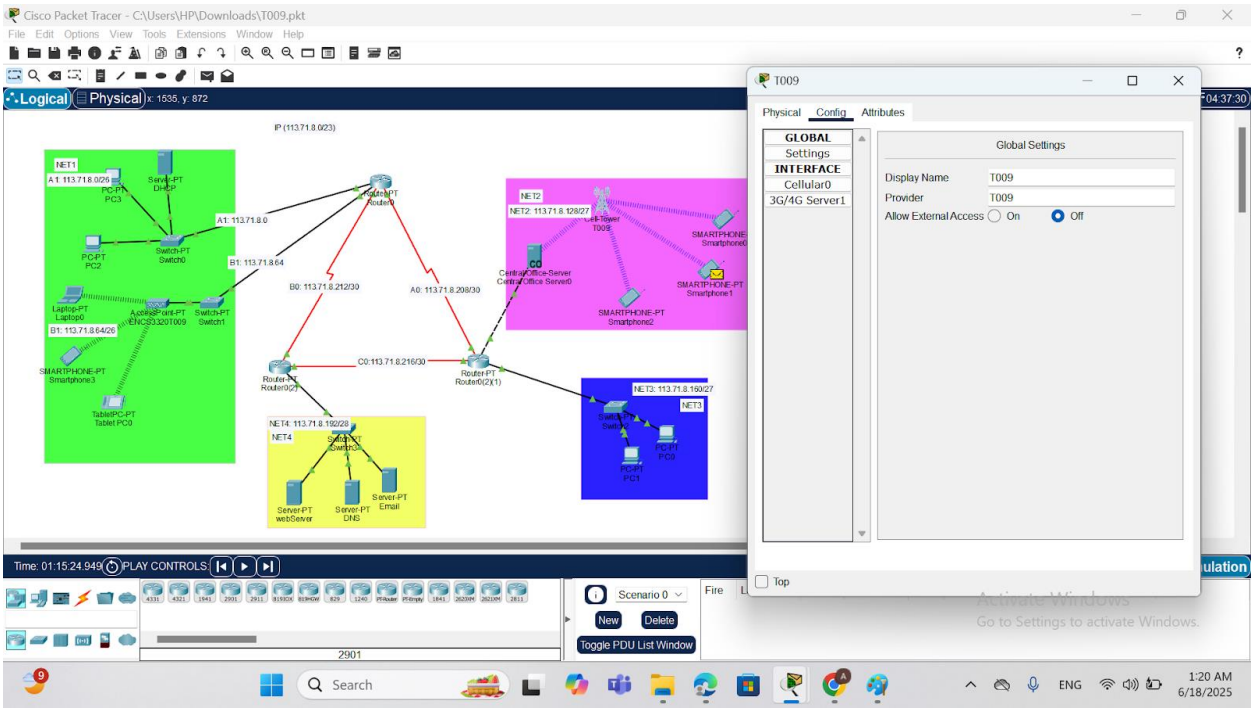


Figure 14:cell Tower name and provider

The **Central Office Server (CO Server)** was configured within the **Street Network (NET2)** to act as a bridge between the **Cell Tower** and the core network. The server was assigned a **static IP address** of 113.71.8.145 with a **subnet mask** of 255.255.255.240 on the interface connected to the Cell Tower.

For the **Backbone** connection, a second interface was configured with the IP address 113.71.8.130, using a **subnet mask** of 255.255.255.240, and the **default gateway** was set to 113.71.8.129

This configuration ensures seamless communication between the Cell Tower and the core network, making the CO Server a vital component in connecting external devices to the internal infrastructure.

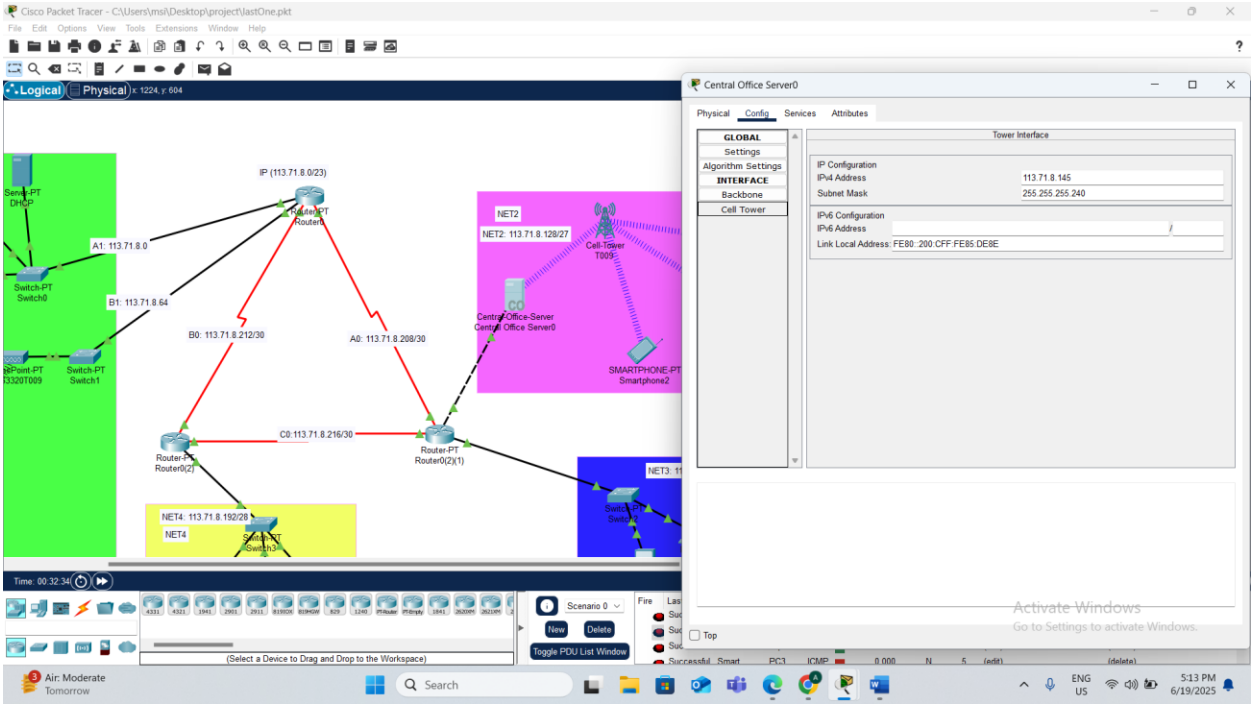


Figure 15:Static IP configuration for CO Server interface connected to Cell Tower

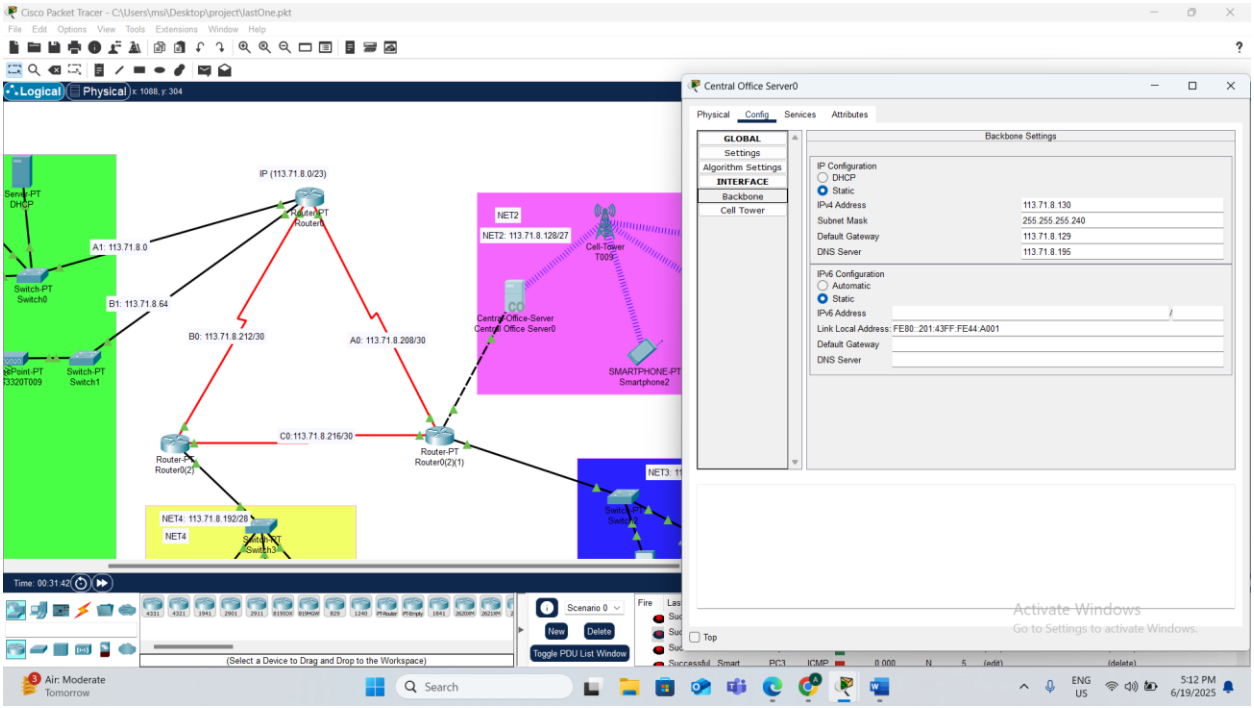


Figure 16:CO Server interface setup for Backbone connection

4. Home network (Area 3):

The **Home Network (Area 3)** consists of a single subnetwork (NET3) designed for basic connectivity. The router interface connected to this network was activated and assigned a static IP address according to the subnetting scheme. A single switch was added to serve as the central hub for local devices. Two PCs were connected to the switch, and each was manually configured with a static IP address. This setup allows the home devices to communicate locally and access services across the wider network through the router.

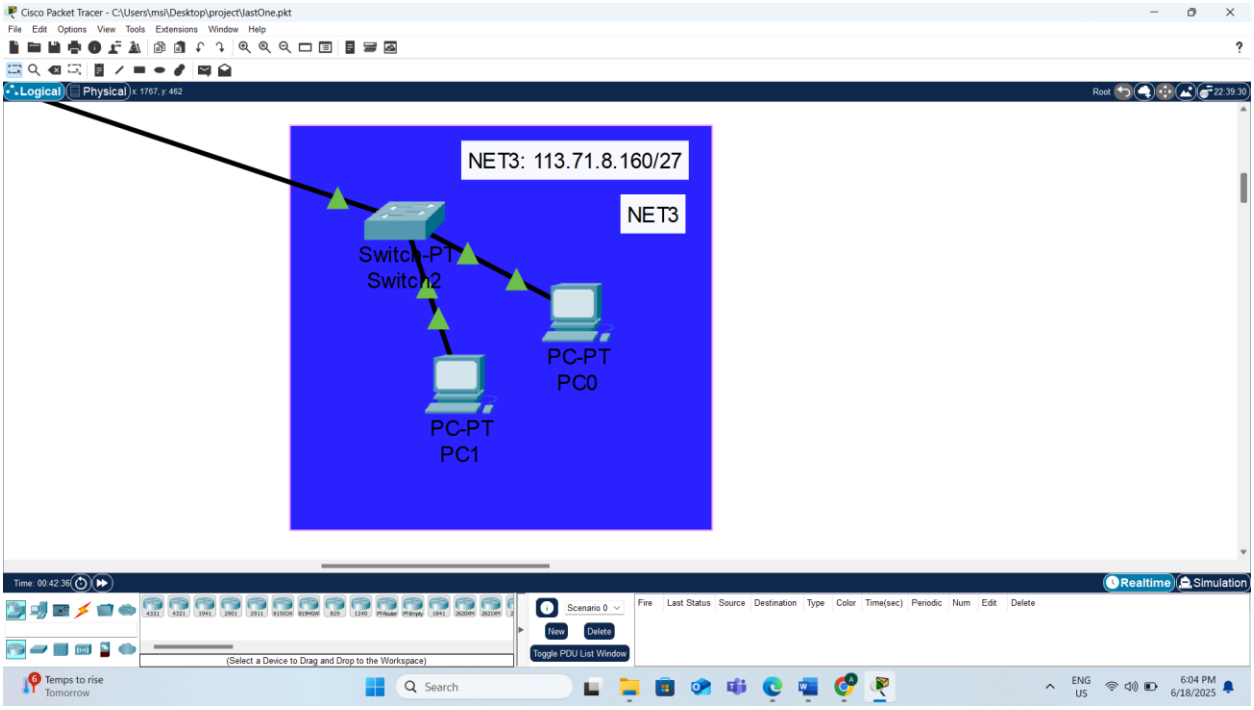


Figure 17:NET3

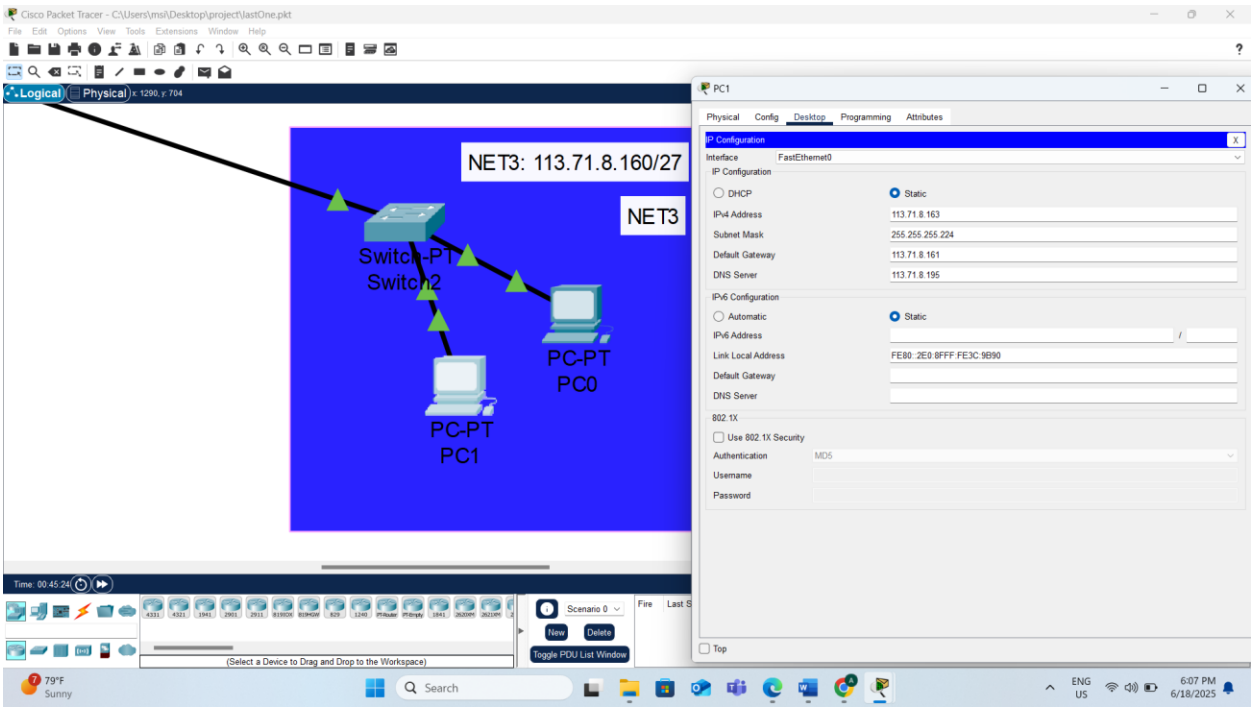
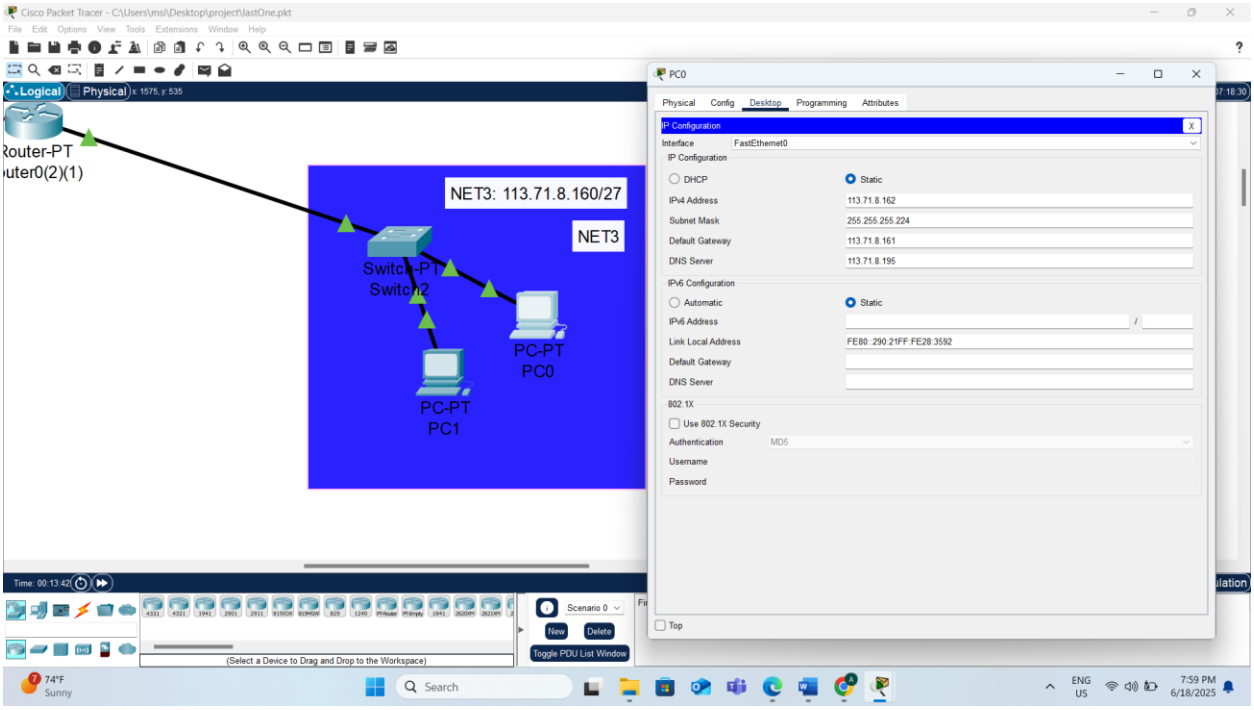


Figure 18:NET3 configured with one switch and two PCs using static IPs connected to the router



5. Datacenter Network (NET4):

The Datacenter area consists of a single subnetwork (NET4), connected via a router interface with a manually assigned static IP. A switch was added to connect three essential servers: a Web Server, a Mail Server, and a DNS Server.

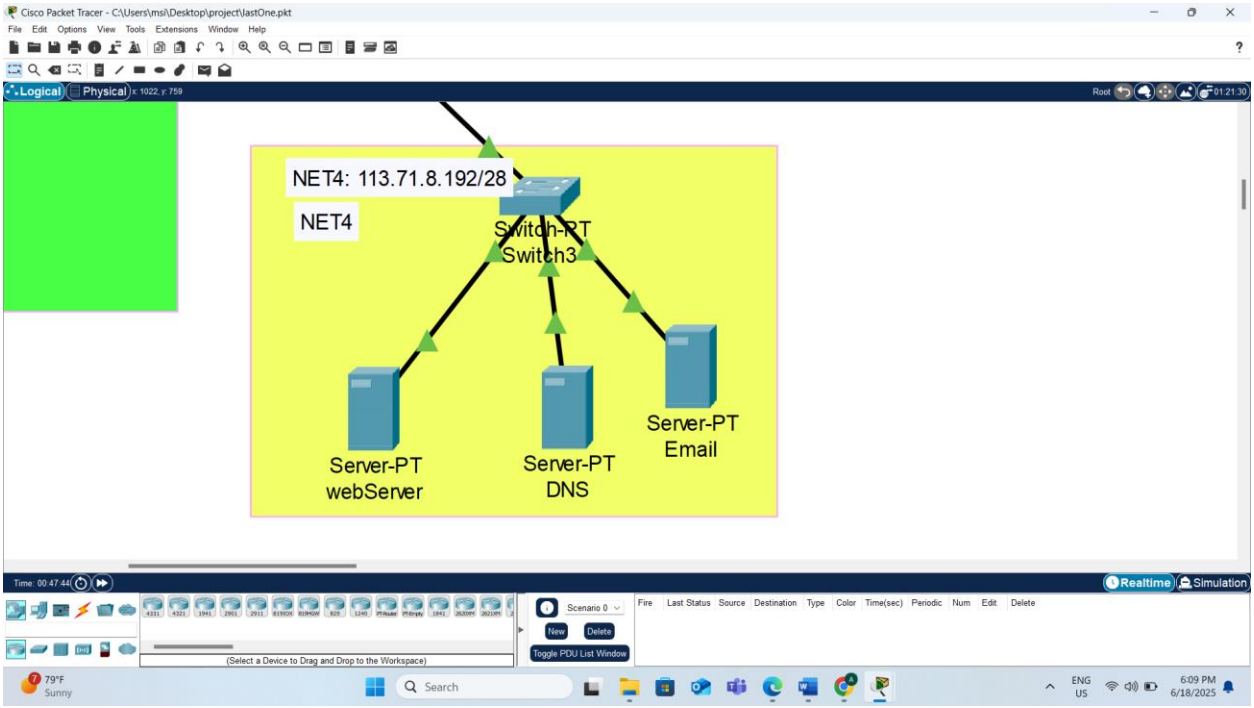


Figure 19:NET-4

1. Web server

A web server is a system—either software, hardware, or both—that stores, processes, and delivers web content to users over the Internet using the HTTP or HTTPS protocol. When a user's browser sends a request (like visiting a website), the web server responds by delivering the appropriate resources, such as HTML pages, images, videos, or data [3].

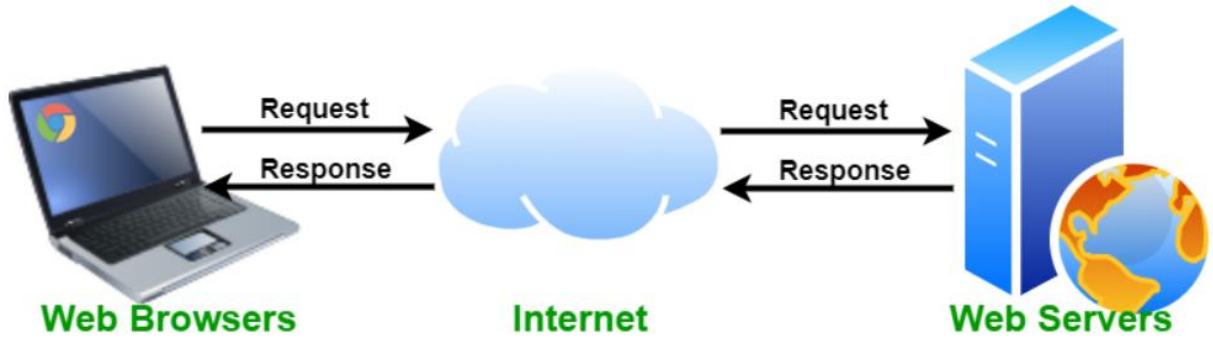


Figure 20 : Working of a Web Server[3]

HTTP (HyperText Transfer Protocol)

HTTP is a protocol used for transmitting data between a web browser and a server. It allows users to access websites and resources like images, text, and videos over the internet. However, HTTP does not encrypt the data being transmitted, which means any information sent using HTTP (such as login credentials or personal details) can potentially be intercepted by attackers. Because of this lack of security, HTTP is generally considered unsafe for websites that handle sensitive or private information. It is still used in some cases for public content or internal network communications where encryption is not necessary [4].

HTTPS (HyperText Transfer Protocol Secure)

HTTPS is the secure version of HTTP, designed to protect data exchanged between a user and a website. It uses encryption protocols like TLS (Transport Layer Security) to ensure that the data cannot be read or altered by unauthorized parties during transmission. HTTPS not only encrypts the content but also verifies the identity of the website through a digital certificate, adding an extra layer of trust. This makes HTTPS essential for secure online activities such as banking, shopping, or logging into accounts. Most modern websites now use HTTPS by default to protect users' privacy and ensure data integrity [4].

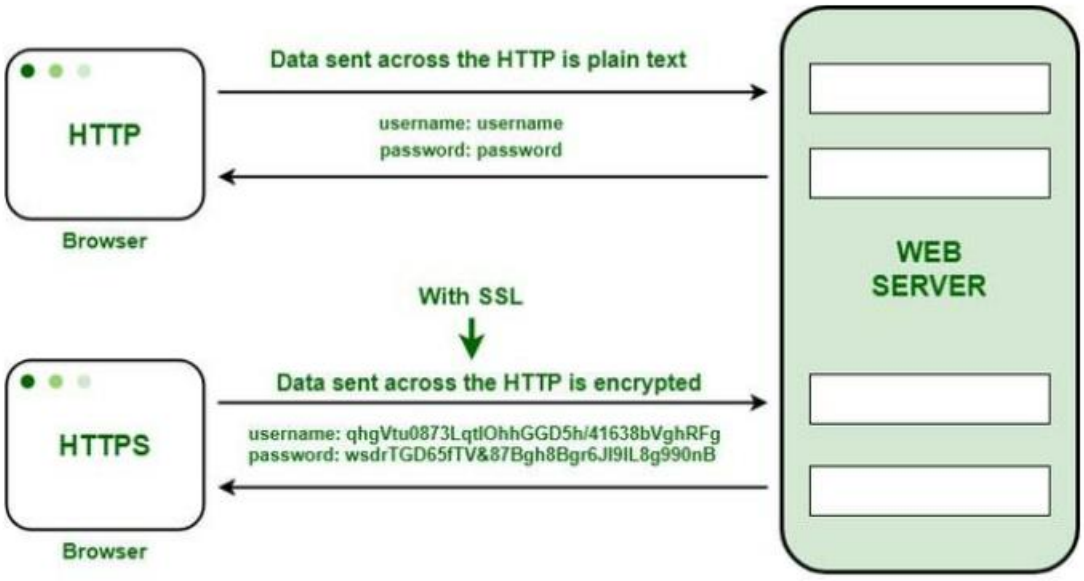


Figure 21 : How HTTP and HTTPS Protocols Work [5]

Practical Application in the Project:

A **Web Server** was implemented within the **Data Center Network (NET4)** using a dedicated **Server-PT**. The configuration was as follows:

- Assigned a **static IP address**: `113.71.8.194`.
- Enabled only **HTTP** and **HTTPS** services.
- Assigned the domain name: `www.coe.birzeit.edu`.
- The domain name was mapped via a **DNS server** hosted on a separate Server-PT with the static IP address: `113.71.8.195`.

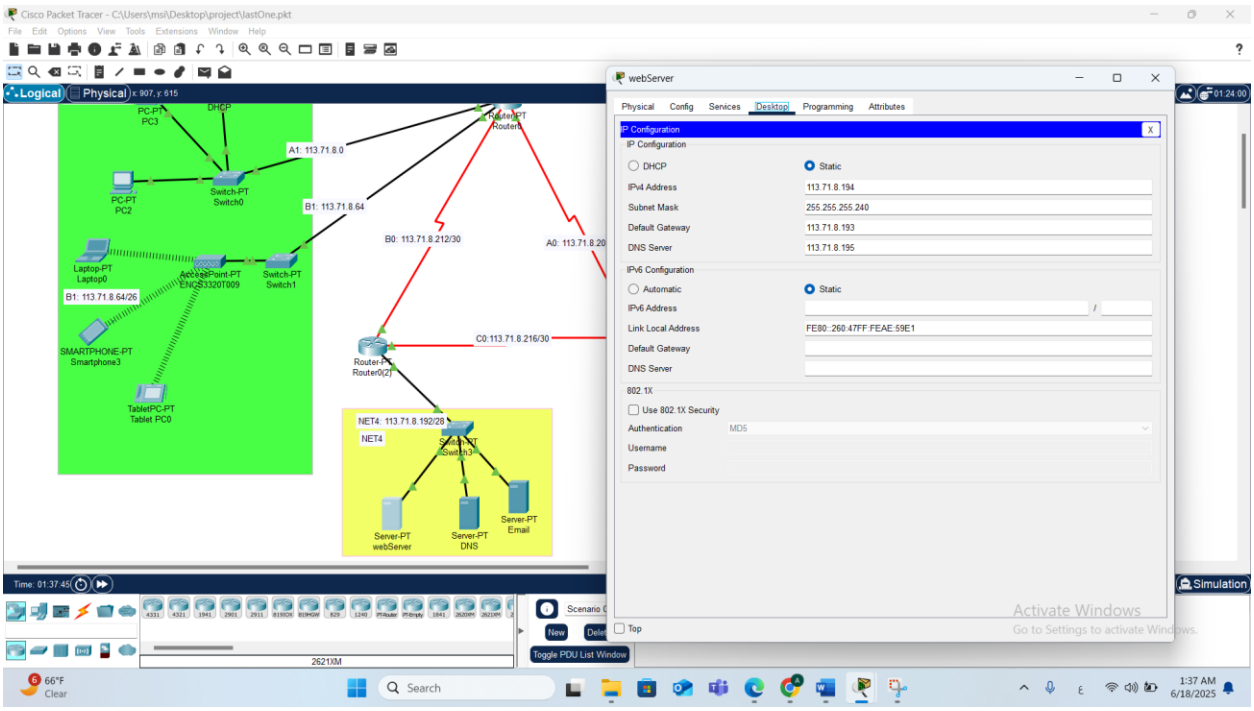


Figure 22:Static IP configuration for the web sever server in NET4

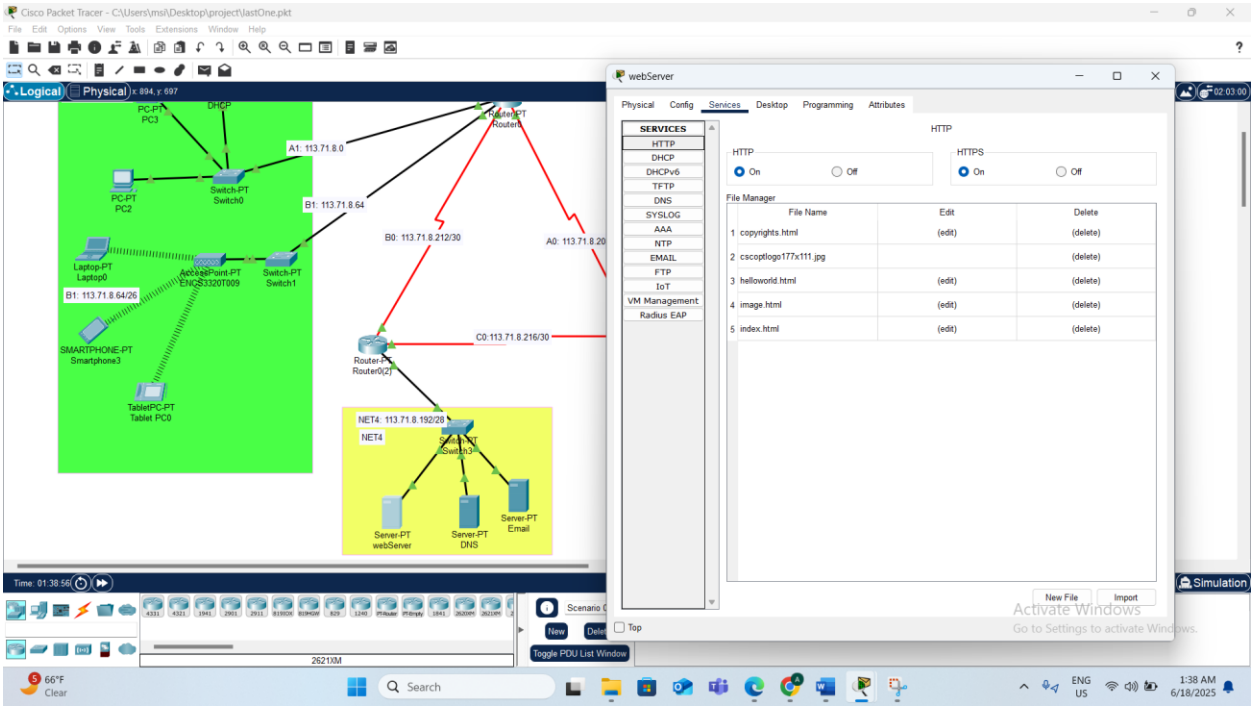


Figure 23:Configuring the web server with static IP and enabling HTTP & HTTPS protocols

Website Content:

A custom homepage (`index.html`) was created and deployed on the web server. It included the following:

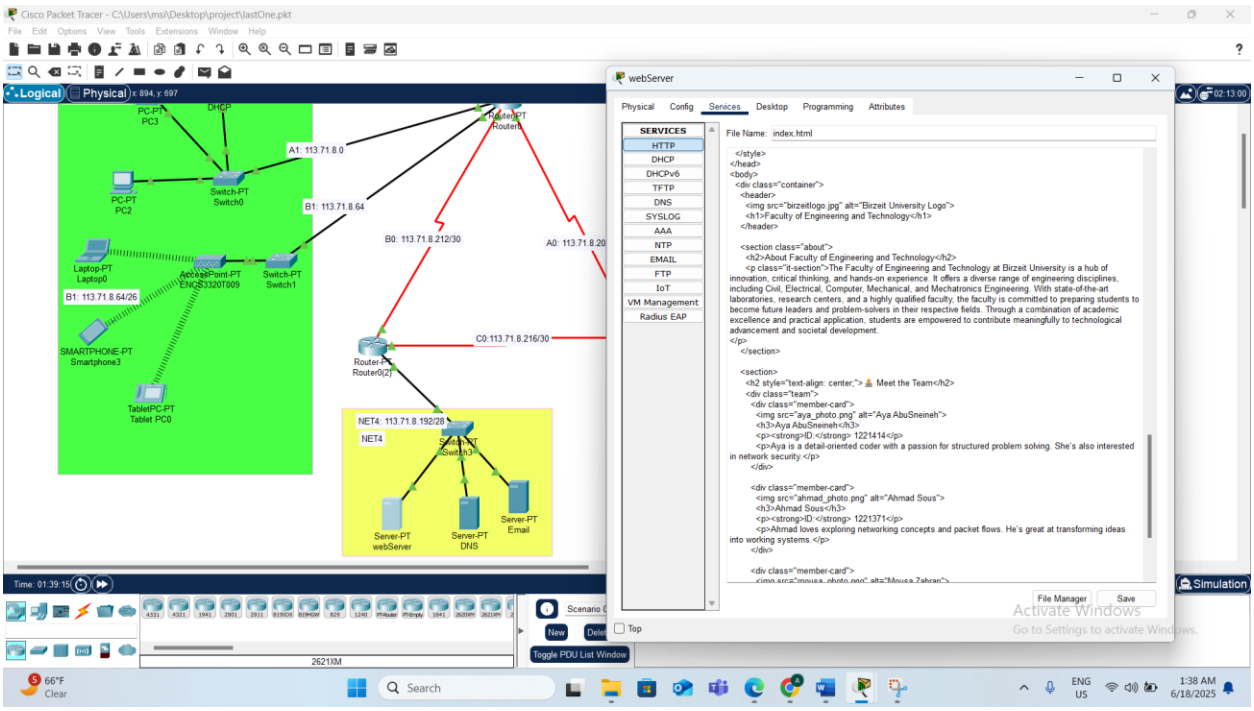


Figure 24:Customizing the index.html page with tab title, page title, faculty description, and team member details

- **Tab Title:** `COE-Birzeit`
- **Page Title:** `Faculty of Engineering and Technology`
- **Sections Included:**
  - An overview of the **Faculty of Engineering and Technology**.
  - Detailed profiles of the **team members**.
  - Properly formatted **text**, **images**, and **bullet-point lists**.

Justification for Using Web Services:

Web services were implemented to simulate a realistic and essential internet-based application. Enabling **HTTP** and **HTTPS** allows users to experience both standard and secure methods of accessing websites.

- **HTTP** provides basic access for non-sensitive content.
- **HTTPS** emphasizes the importance of **encrypted, secure communication**, as used in modern websites.

2. Emile server

An **email server** is a specialized computer system responsible for sending, receiving, and storing email messages. It works using standardized protocols such as **SMTP (Simple Mail Transfer Protocol)** for sending emails, and **IMAP (Internet Message Access Protocol)** or **POP3 (Post Office Protocol)** for retrieving them. When a user sends an email, the message is routed through an outgoing mail server (SMTP), which then delivers it to the recipient's incoming mail server (using IMAP or POP3). Email servers are a crucial part of the internet's communication infrastructure, allowing people and organizations to exchange messages quickly and reliably. They can be hosted by large providers like Gmail and Outlook, or run privately by organizations for internal communication [6].

SMTP (Simple Mail Transfer Protocol)

SMTP is the standard protocol used to **send emails** from a client (like Gmail or Outlook) to an email server and between email servers themselves. When you hit "send" on an email, your device uses SMTP to deliver the message to the recipient's mail server. SMTP works as a **push protocol**, meaning it pushes emails to their destination, but it doesn't retrieve emails. It's designed to transfer outgoing messages only and is usually paired with a different protocol (like IMAP or POP3) to handle incoming mail [7].

POP3 (Post Office Protocol version 3)

POP3 is a protocol used to **retrieve emails** from a remote server to a local device. It downloads emails from the server and stores them locally on the user's device, then typically deletes them from the server (unless configured otherwise). This makes it ideal for users who want offline access to their emails, but it's less suitable for accessing email from multiple devices, since the messages don't stay synchronized. POP3 is a **pull protocol**, focusing on fetching email from the server rather than sending it [7].

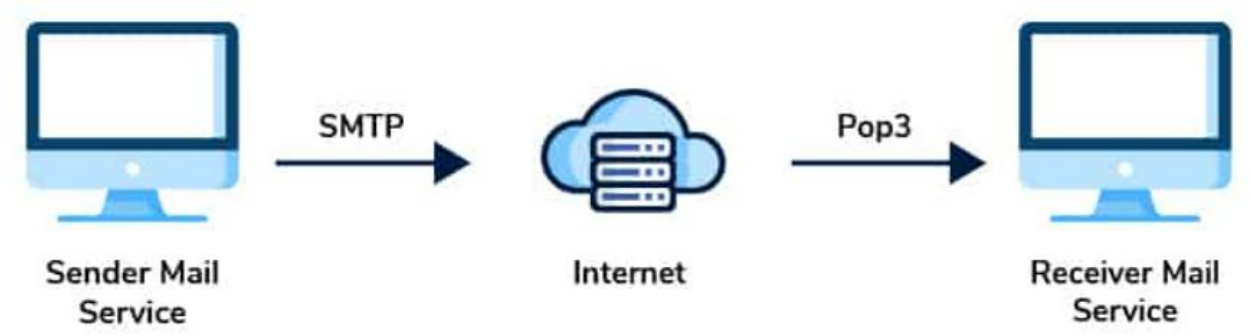


Figure 25 : Email Transmission and Retrieval using SMTP & POP3 [8]

Practical Application in the Project:

The email server was implemented within the **Data Center Network (NET4)** using a dedicated Server-PT with a static IP address of 113.71.8.196. Both **SMTP** and **POP3** services were enabled on this server, and the **domain name** for the email system was set as:coe.birzeit.edu.

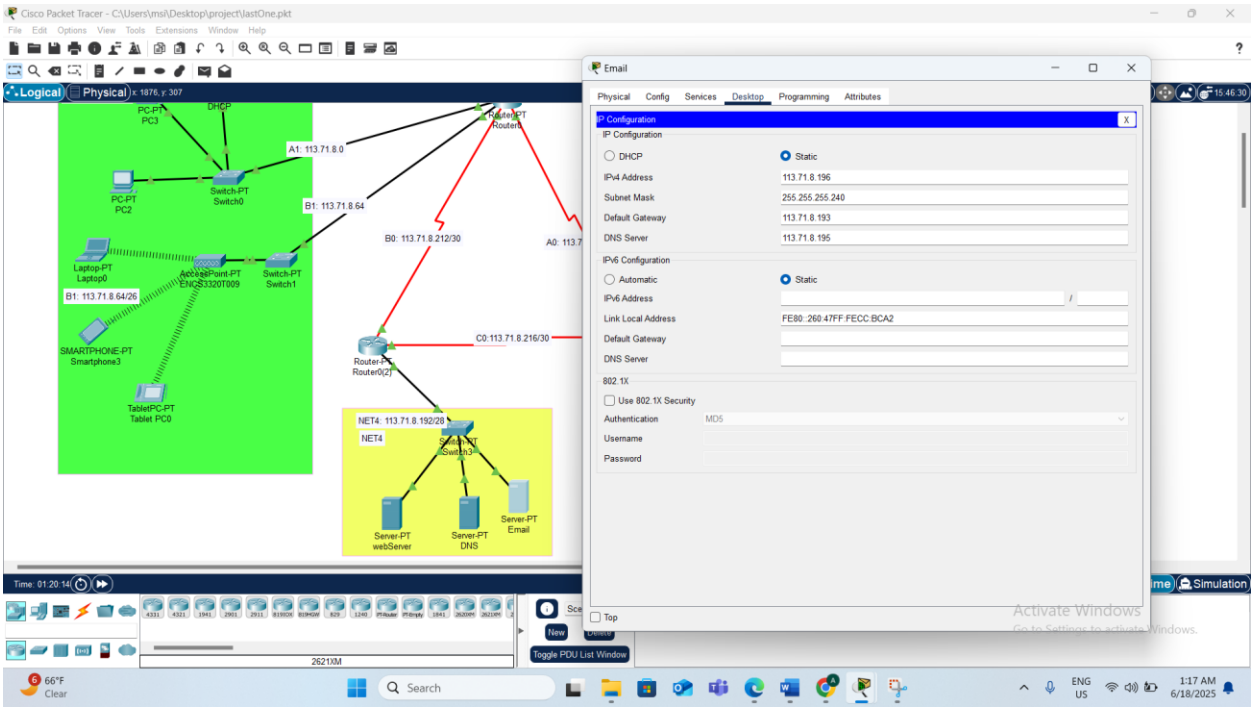


Figure 26:Configuring the mail server mail.coe.birzeit.edu with SMTP and POP3 enabled

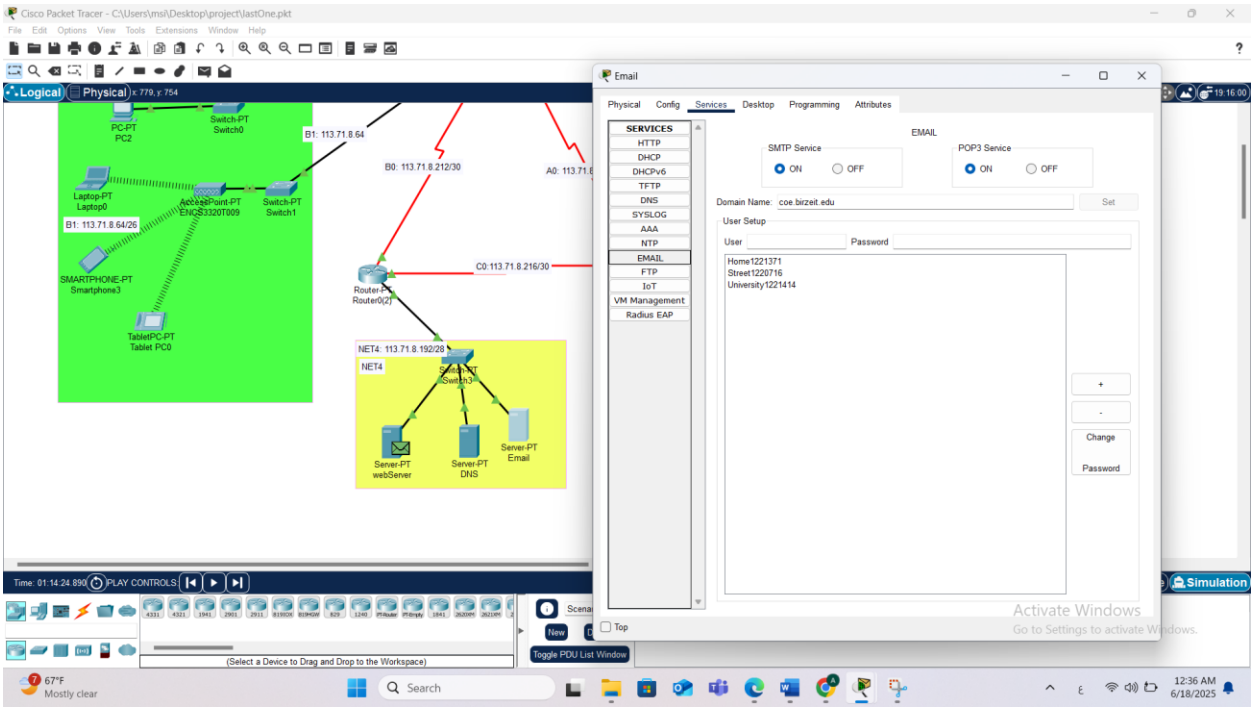


Figure 27:Creating three email accounts for the different networks

Three email accounts were created, distributed across different networks as above:

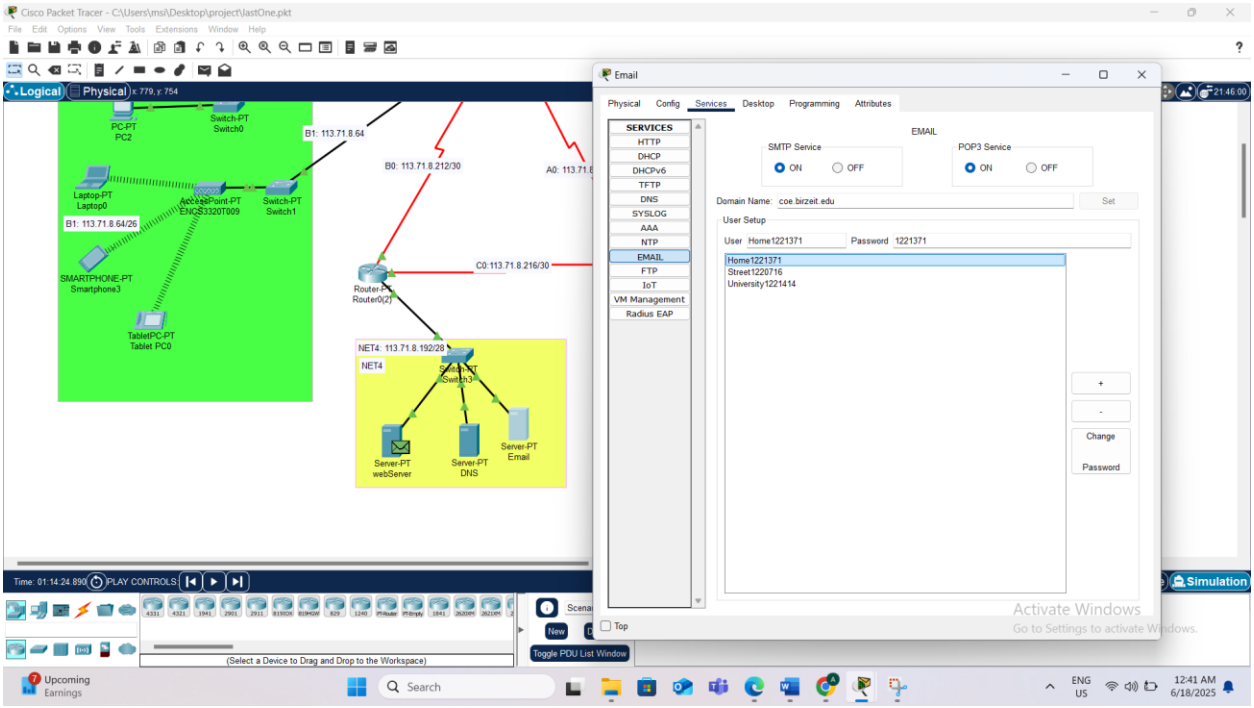


Figure 28:Setting up the email client for one of the users

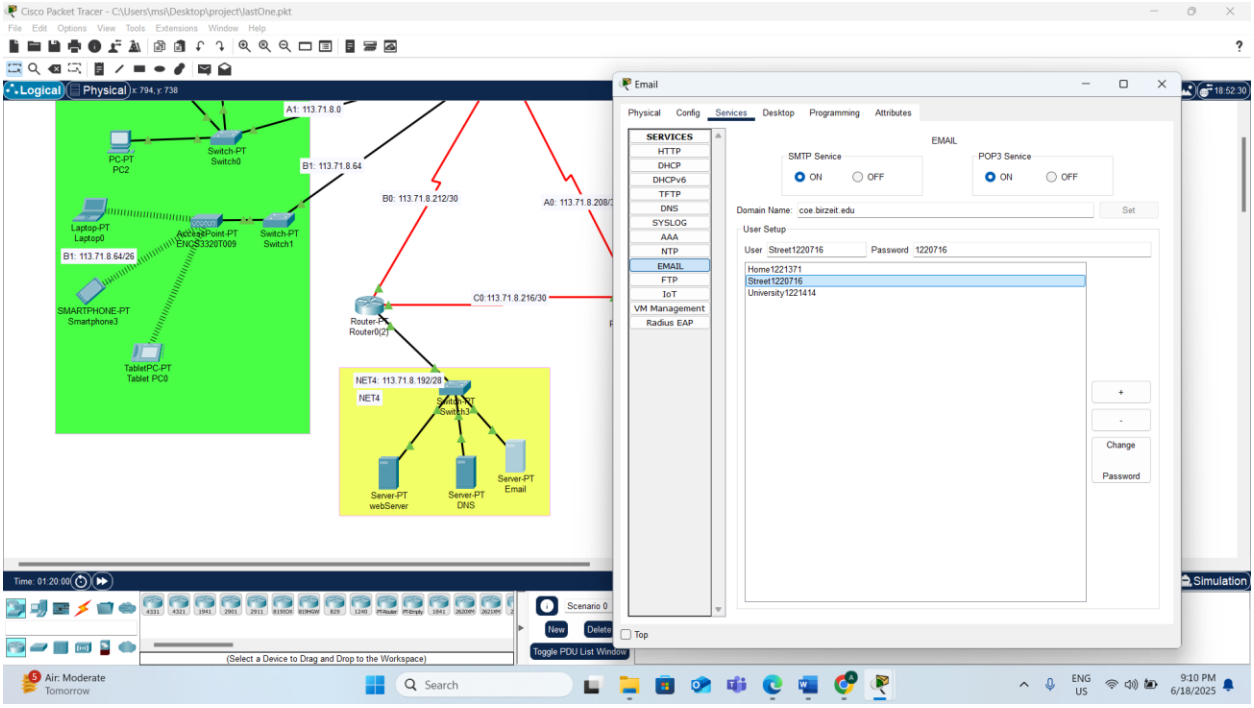


Figure 29:Setting up the email client for one of the users

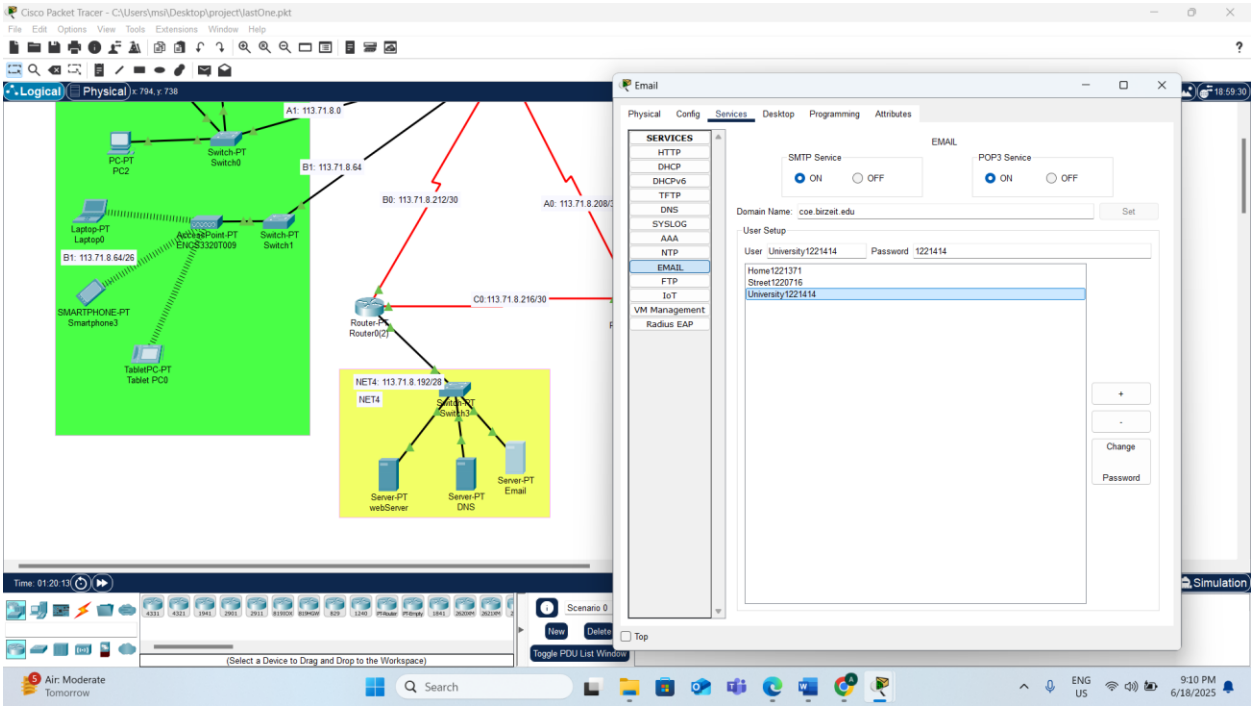


Figure 30:Setting up the email client for one of the users

After account creation, **email clients** were configured in each of the three networks (Home, Street, University), using the address mail.coe.birzeit.edu as the mail server, which was previously linked in the DNS.

Successful sending and receiving of emails between users across different networks was verified using SMTP and POP3 protocols through Packet Tracer configuration interfaces.

Justification for Using Email Services:

Email protocols were implemented to represent a critical service in the network, providing a communication means between users in different networks. The choice of SMTP and POP3 protocols was due to their standardized support in Packet Tracer tools, enabling a realistic environment to simulate email operations as in real-world networks.

3. Domain Name System (DNS):

The Domain Name System (DNS) is the infrastructure responsible for translating human-readable domain names (such as `www.example.com`) into numerical IP addresses that devices use to communicate over the internet. DNS plays a crucial role in simplifying user experience by eliminating the need to memorize complex IP addresses, functioning much like a phonebook for the internet[9].

The DNS resolution process involves four main stages: First, the **DNS resolver** collects the request from the browser. Then, it forwards the query to the **root server**, which redirects it to the appropriate **Top-Level Domain (TLD) server**, such as `.com` or `.net`. Finally, the query reaches the **authoritative server**, which holds the actual IP address of the requested domain and returns it to the user to access the website [9].

DNS servers are generally categorized into two types: **recursive servers**, which handle the entire lookup process on behalf of the user, and **authoritative servers**, which store the original DNS records. Without DNS, most internet functions would be severely disrupted, making it a core component of network infrastructure[9].

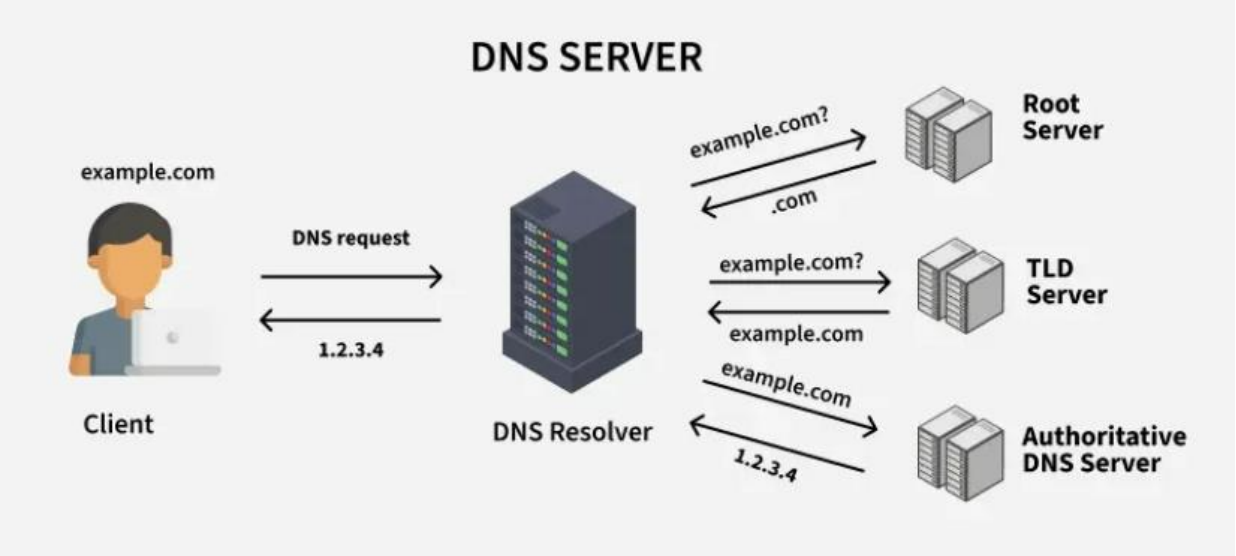


Figure 31 : DNS server [10]

Advantages of DNS :

User-Friendly: Translates difficult IP addresses into easy-to-remember domain names.

DNS eliminates the need for users to memorize complex strings of numbers.

Load Balancing: DNS can distribute incoming traffic across multiple servers.

Efficient: Provides fast resolution of frequently accessed websites by implementing caching.

Disadvantages of DNS :

Vulnerable: Attacks target it through DNS spoofing or DDoS, aiming to hamper access to websites.

Complex: Requires proper configuration and maintenance of DNS records; otherwise, issues will arise during resolution.

Practical Implementation in the Project:

The DNS service was implemented within the **Datacenter Network (NET4)** using a dedicated **DNS server (Server-PT)** assigned a static IP address: 113.71.8.195. The server was configured to run only the DNS service.

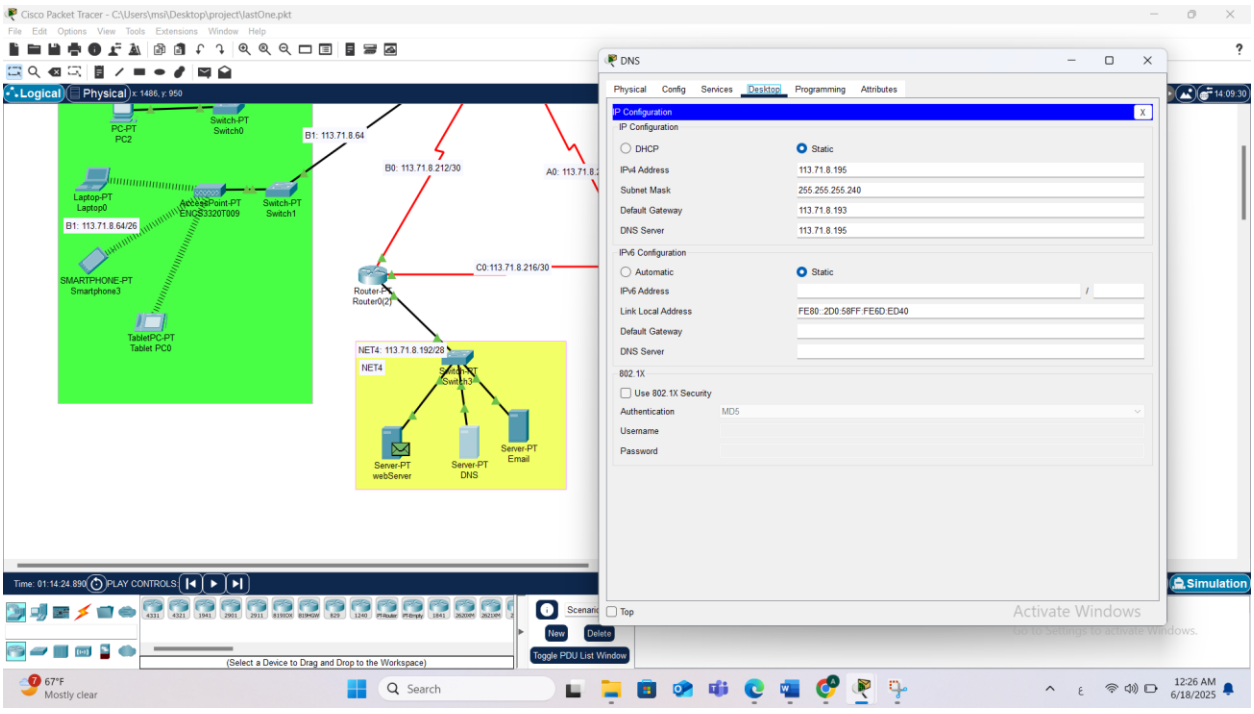


Figure 32:Static IP configuration of the DNS server in the Datacenter network (NET4)

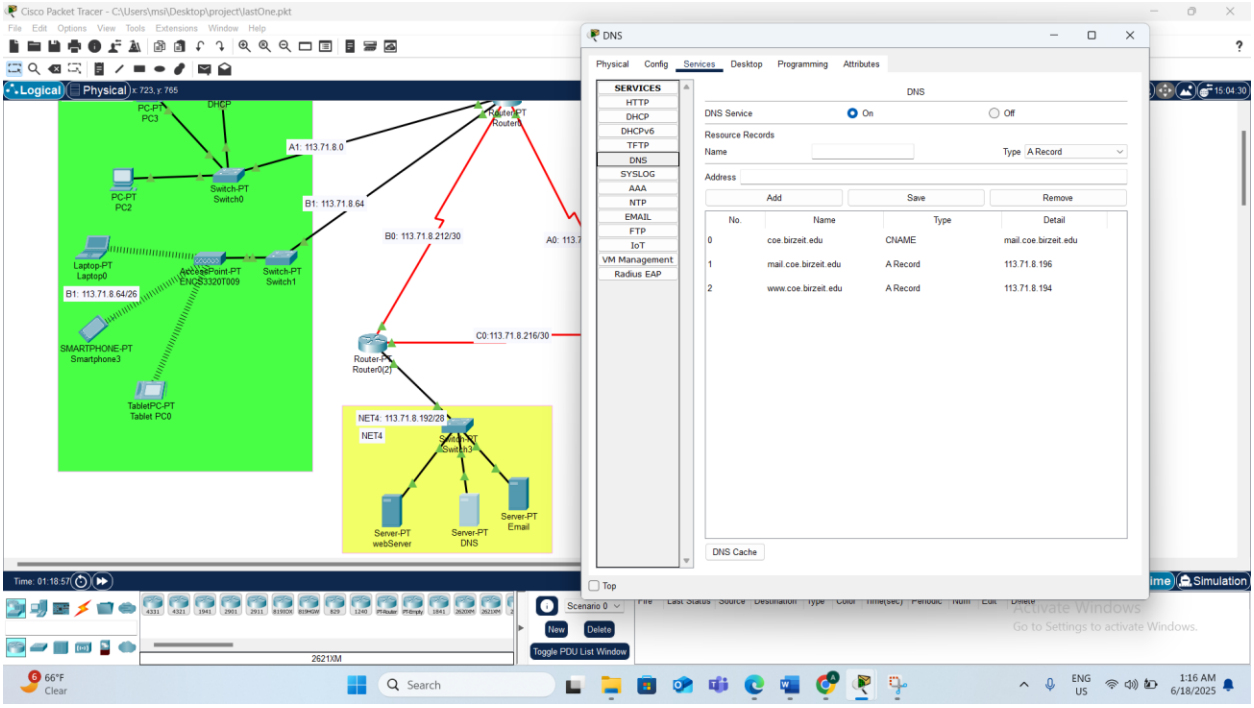


Figure 33:Configuration of DNS Resource Records (RRs), including A and CNAME records for coe.birzeit.edu

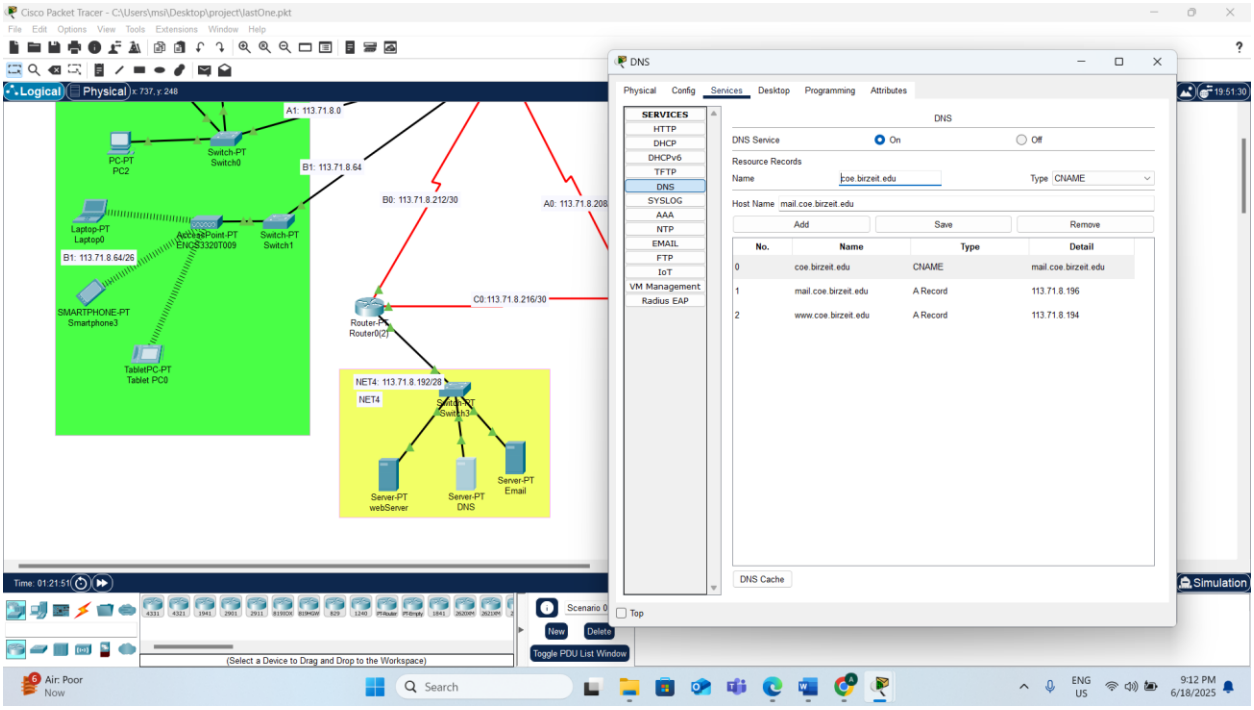


Figure 34:record CNAME

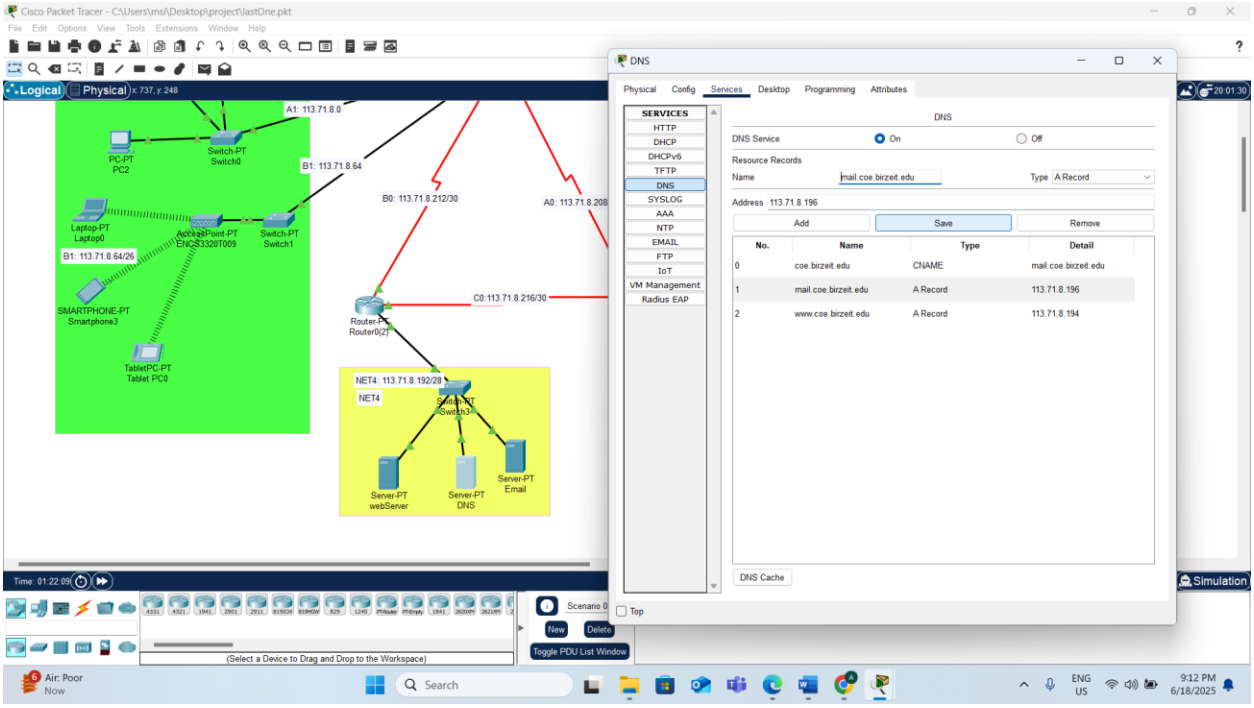


Figure 35:record A for mail server in DNS server

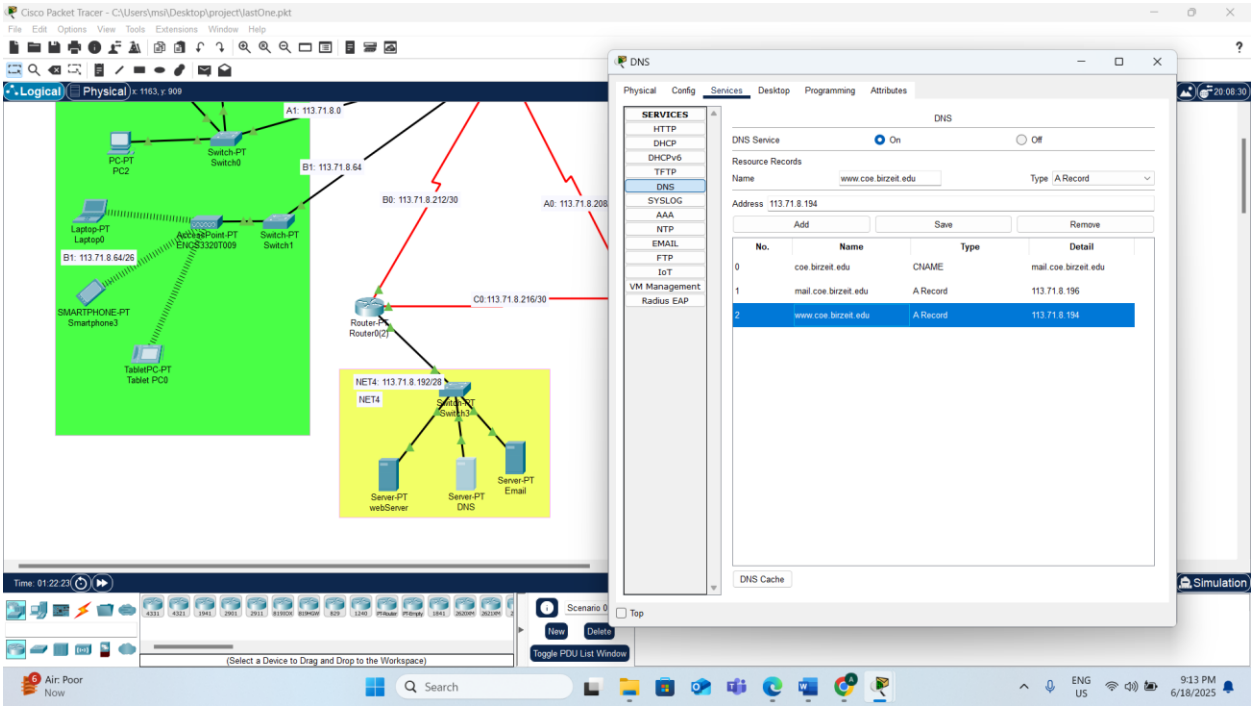


Figure 36 : record A for web server in DNS

The **Resource Records (RRs)** were added to the DNS configuration:

This configuration allowed client devices to access the **web** and **email** services using domain names instead of numerical IP addresses.

Client devices in the **University**, **Home**, and **Street** networks were configured to use the DNS server at 113.71.8.195 as their default name resolver. This ensured proper name resolution and successful access to hosted services.

Justification for Using DNS:

DNS was implemented to enhance usability, enabling users to access services through readable domain names instead of IP addresses. Hosting a local DNS server within the network improved name resolution speed and reliability while reducing dependency on external DNS servers, thus increasing network efficiency and security.

Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is an advanced link-state routing protocol deployed within IP networks to determine the most effective path for data transport. Leveraging the Shortest Path First (SPF) algorithm, OSPF is particularly well-suited for environments that demand dynamic routing capabilities. Operating at the network layer, OSPF routers go through several states to establish robust connections with fellow routers, including initiating contact, exchanging vital routing information, and achieving full synchronization of network topologies . This process ensures that all OSPF routers have an up-to-date and precise understanding of the network layout, enabling them to quickly adapt to network changes. This adaptability is crucial for maintaining efficient and reliable data routing in large, complex network infrastructures [11] .

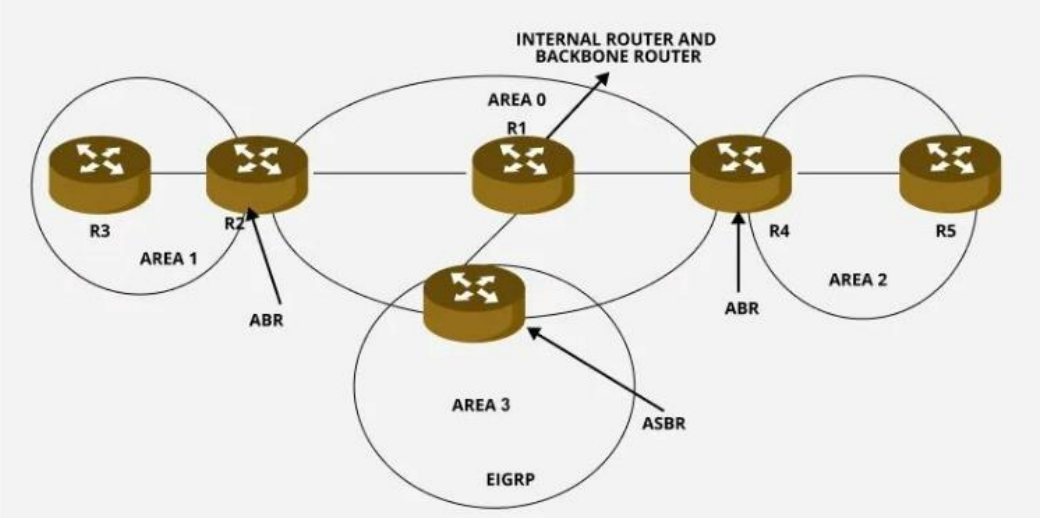


Figure 37 : OSPF Network Topology [11]

The Open Shortest Path First (OSPF) protocol is configured on all routers to manage routing between the five network areas: Area 0, Area 1, Area 2, Area 3, and Area 4. The OSPF process is initiated on each router using the command `router ospf 1`, where `1` is the chosen Process-ID for consistency across the network. Then, each router advertises its connected networks into the OSPF routing domain with the `network` command, specifying the network address, wildcard mask, and corresponding area ID. This setup ensures dynamic and efficient routing between all subnetworks in the topology.

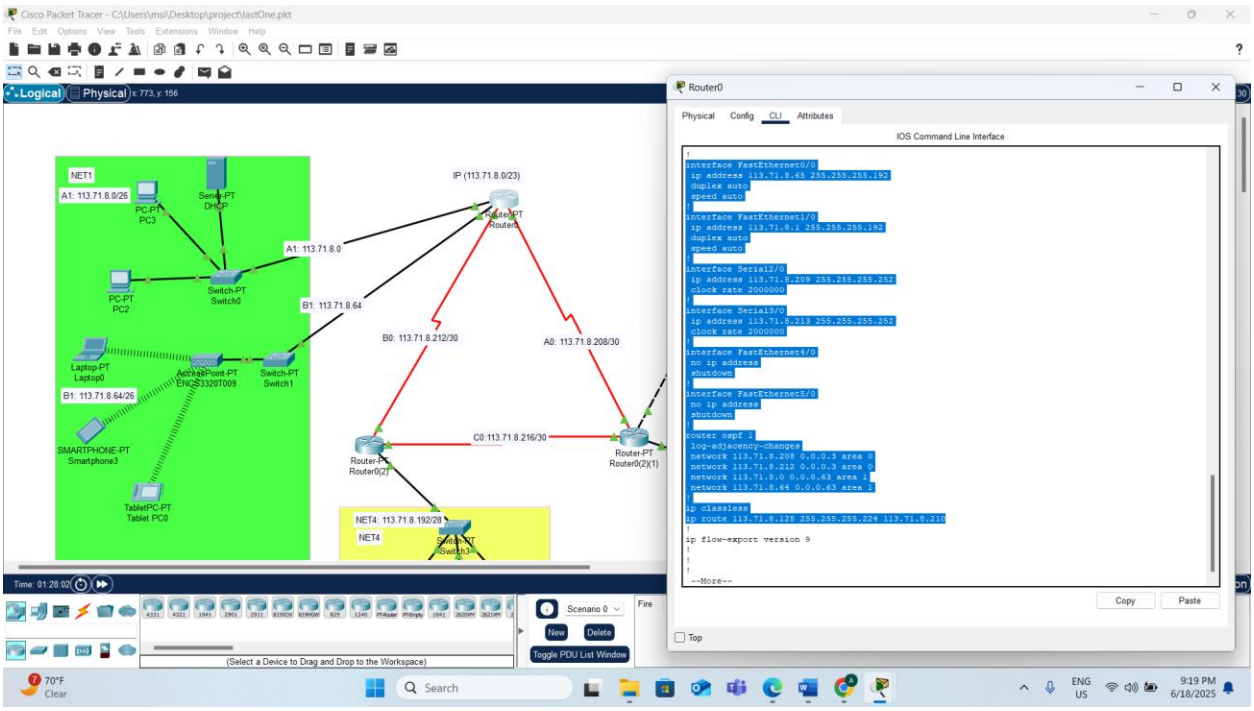


Figure 38:Static IP configuration for router(0) interfaces and OSPF setup

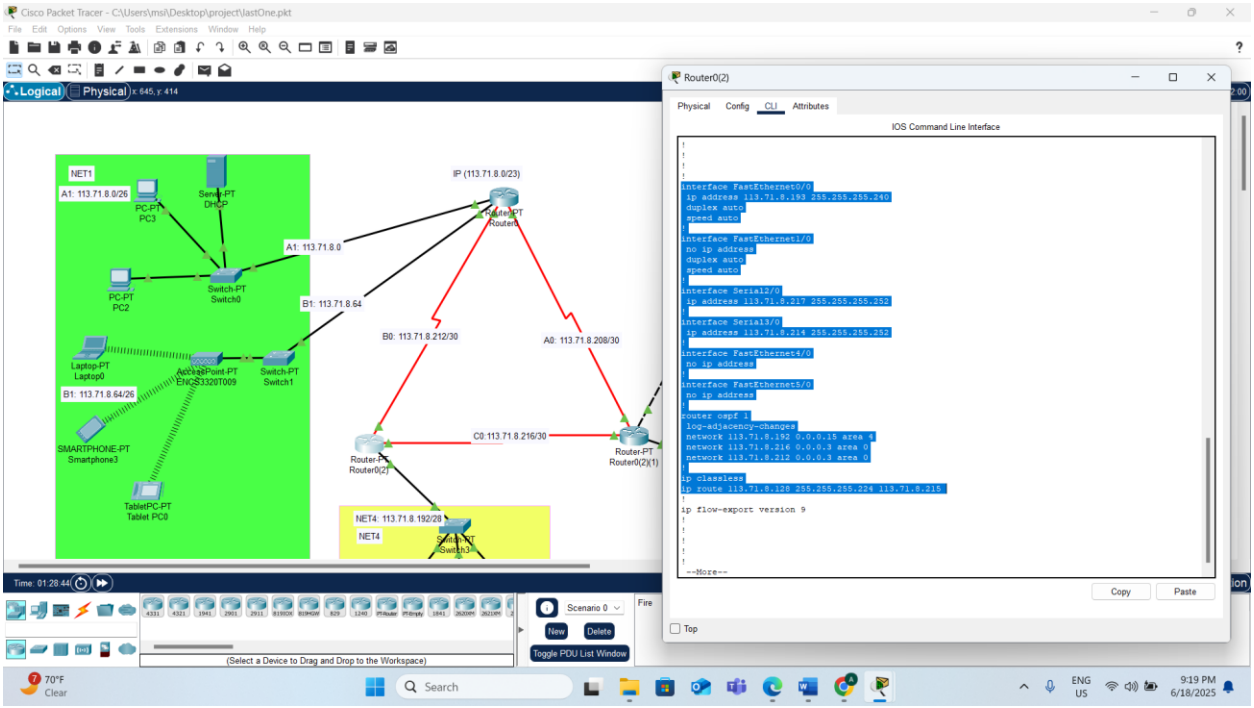


Figure 39:Static IP configuration for router0(2) interfaces and OSPF setup

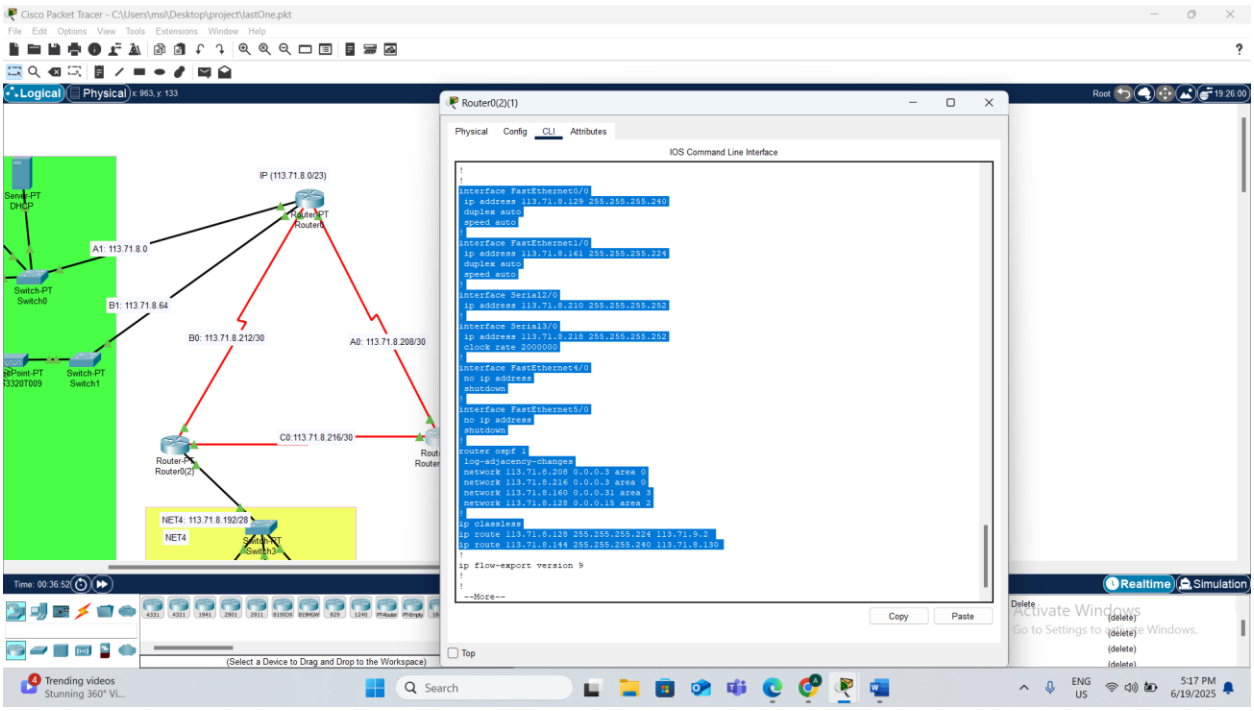


Figure 40:Static IP configuration for router0(2)(1) interfaces and OSPF setup

Results and discussion

- **Static and Dynamic IP Configuration for end devices**

Some devices got static IPs. We gave these IPs by hand.

Other devices used DHCP. They got their IPs automatically from the DHCP server.

We checked the IPs by using the ipconfig command.

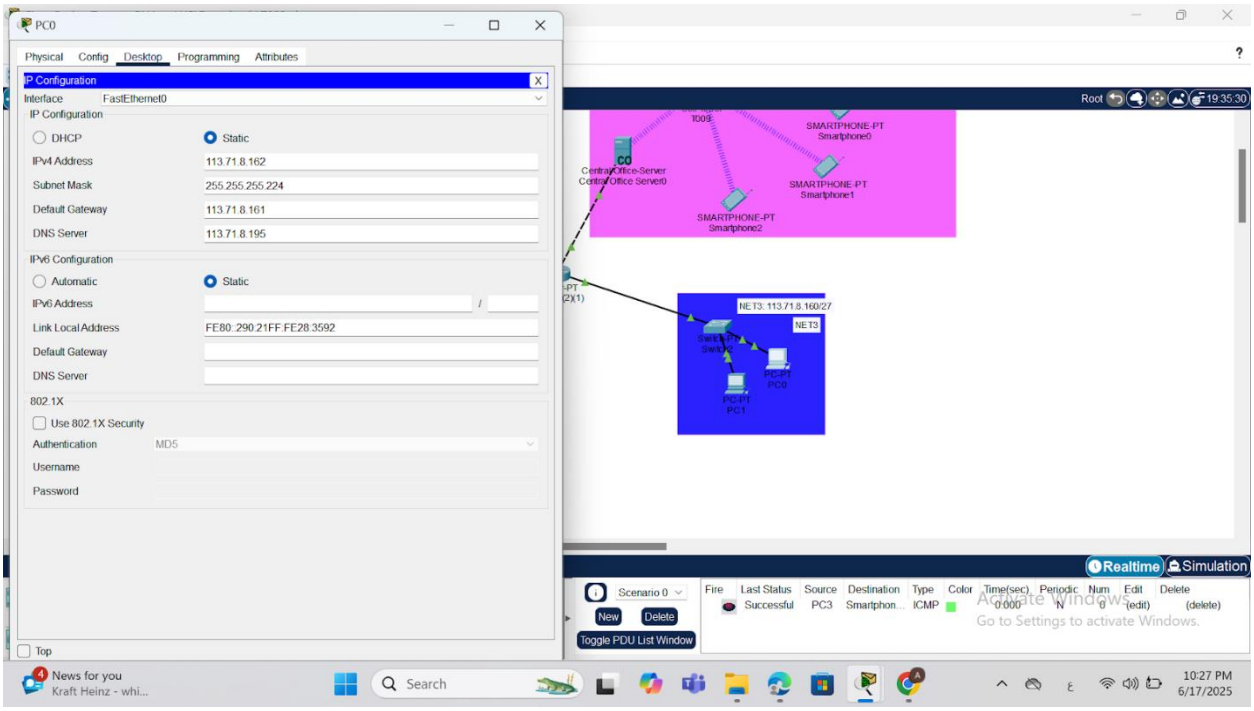


Figure 41:Static IP configuration for a PC0 in the Home network

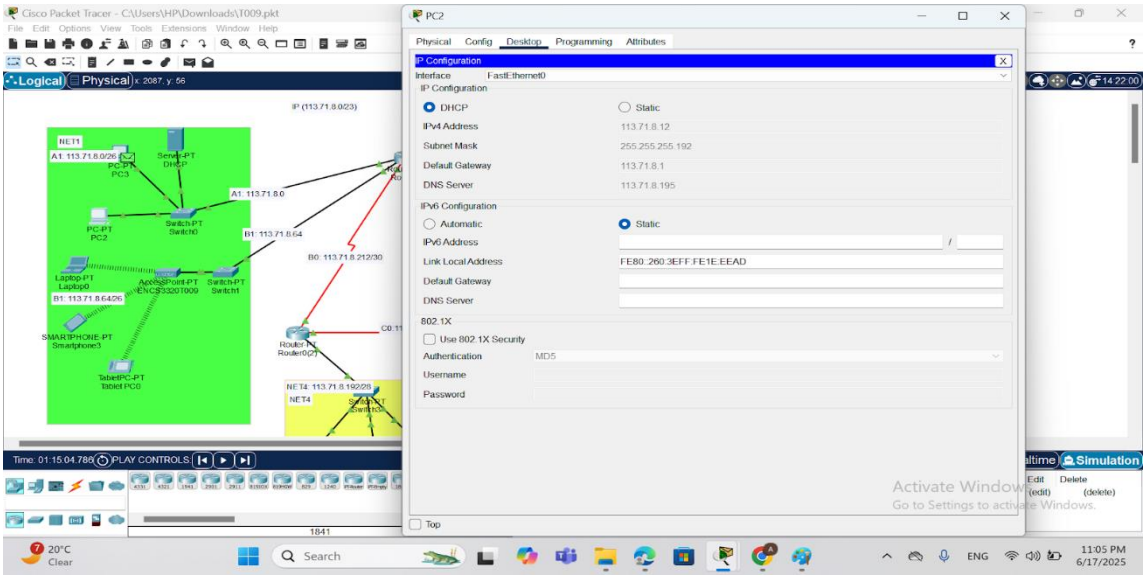


Figure 42:A PC3 receives IP automatically from the DHCP server

smartphones were connected to the Cell Tower using 3G/4G network. It received an IP address from the DHCP server. We checked the IP address on the phone, and it shows that DHCP is enabled and working correctly.

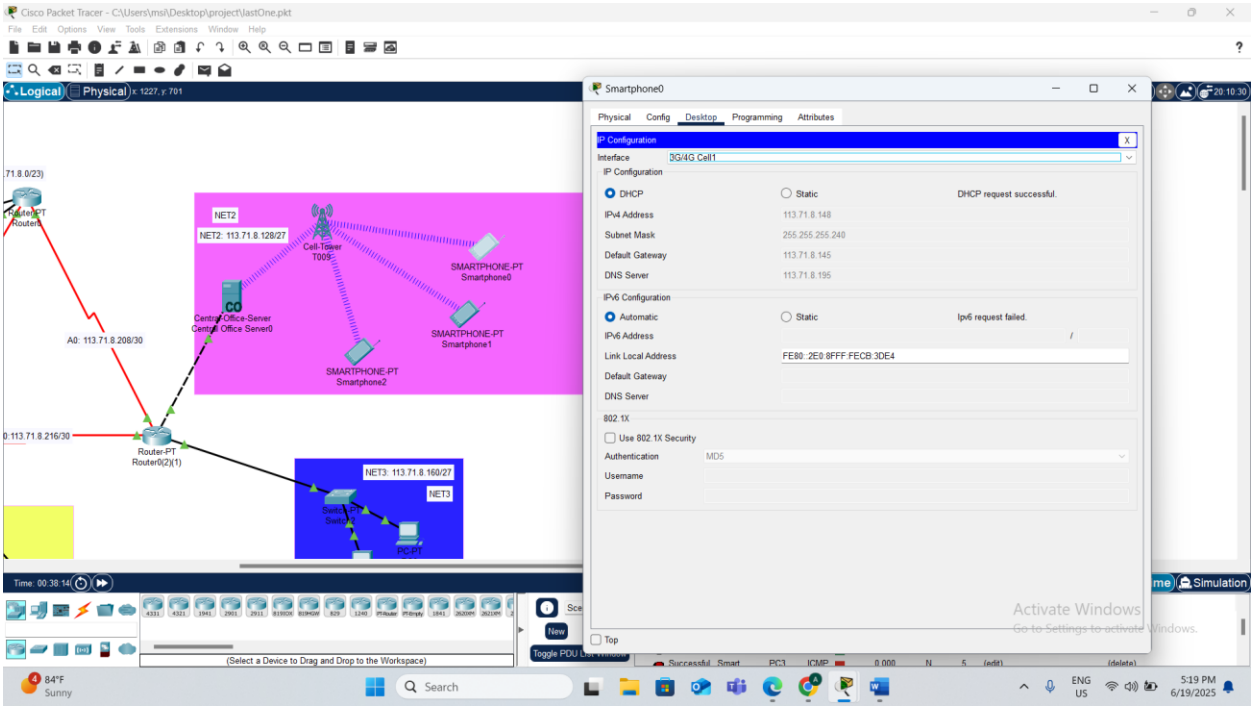


Figure 43:Smartphone0 connected to the Cell Tower using 3G/4G and received IP address from DHCP server automatically

- **Successful Ping and Tracert between end devices:**

We used the ping and tracert commands to test the network connectivity between different devices.

All results were successful, with 0% packet loss and stable response times.

The tracert results showed the full routing paths, proving that OSPF is working correctly.

From Area 3 (Home area) TO All Areas

A. Between the PC1 in Home area and Web Server in Datacenter area

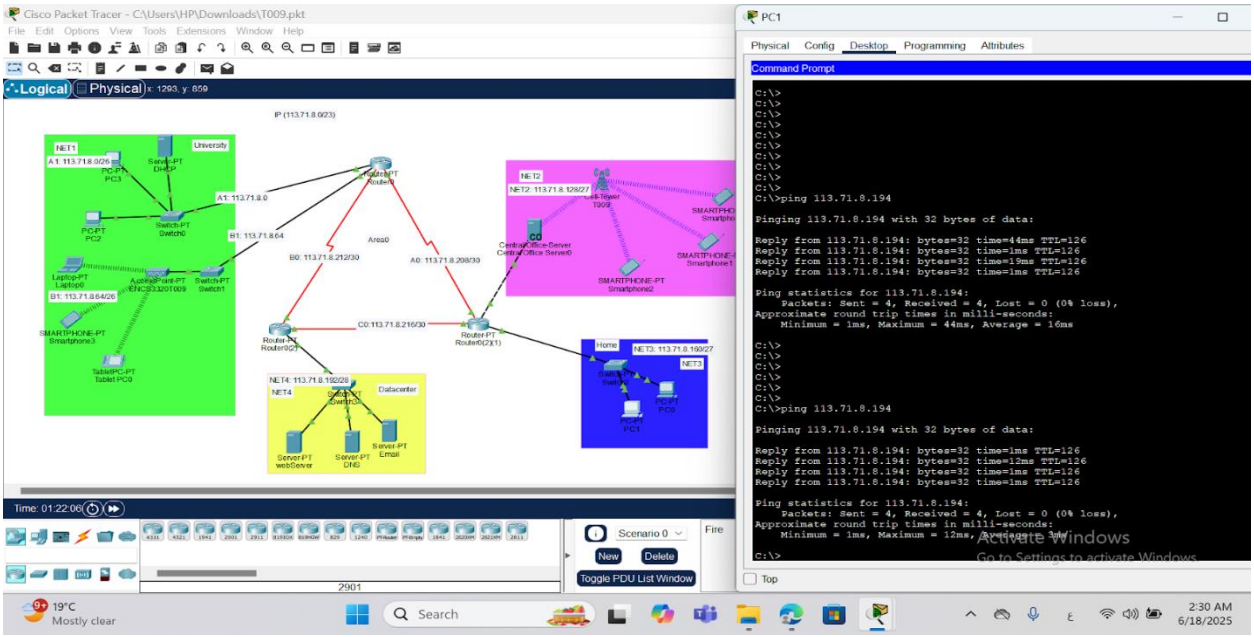


Figure 44:Successful ping test from PC to 113.71.8.194 with 0% packet loss and low delay.

We used the ping command to check if the device can talk to another device in the network.

We sent 4 packets from PC1 in the Home area to the IP address 113.71.8.194(Web server) in the (Datacenter area).

All 4 packets were received. This means the connection is working very well.

There was no loss (0%), and that shows the network is stable.

The reply time was very fast:

- Minimum time = 1 ms
- Maximum time = 12 ms
- Average time = 3 ms

The numbers show that the network is fast and there is no delay.

The TTL = 126 means that the packet passed through 2 routers, which is normal in this network.

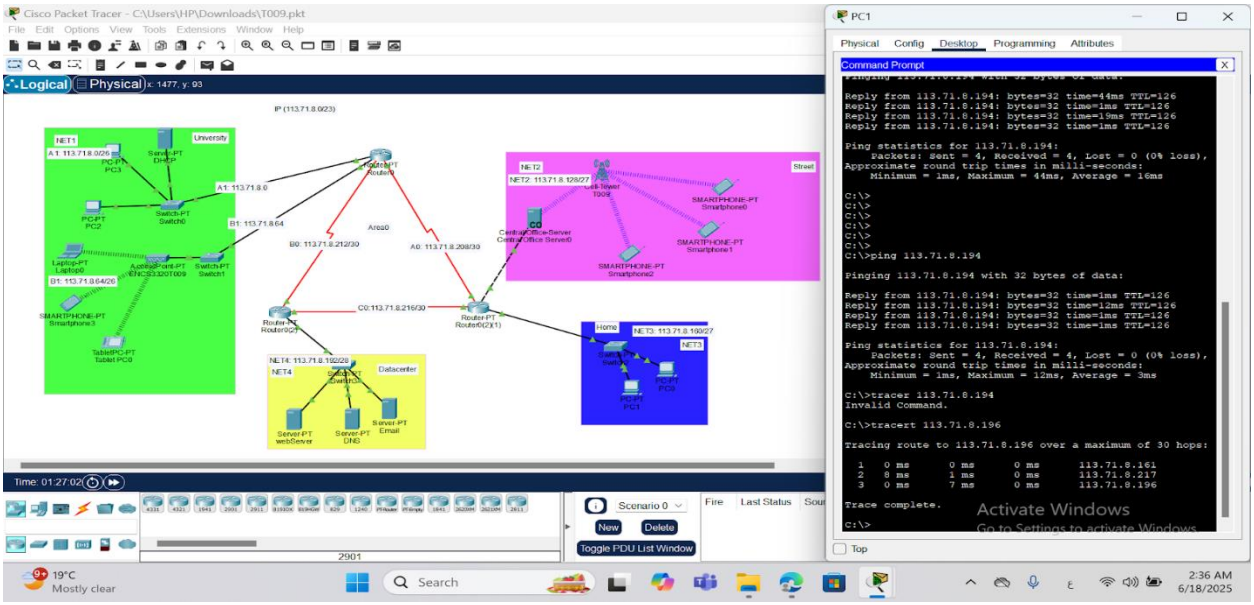


Figure 45:Traceroute result to 113.71.8.196 passing through 3 hops with no delay or loss

We used the tracert command to check the path between the device PC1 and the IP address 113.71.8.196.

The result shows that the packet passed through 3 devices (hops):

1. 113.71.8.161 → first router (very fast: 0 ms) router 2
2. 113.71.8.217 → second router (delay was between 0–8 ms) router 1
3. 113.71.8.196 → final destination (target device)

The trace was completed successfully.

The response times were fast, and there were no errors or timeouts.

This means the OSPF routing is correct and the network is connected properly

B. Between the PC0 in Home area and DNS Server in Datacenter area

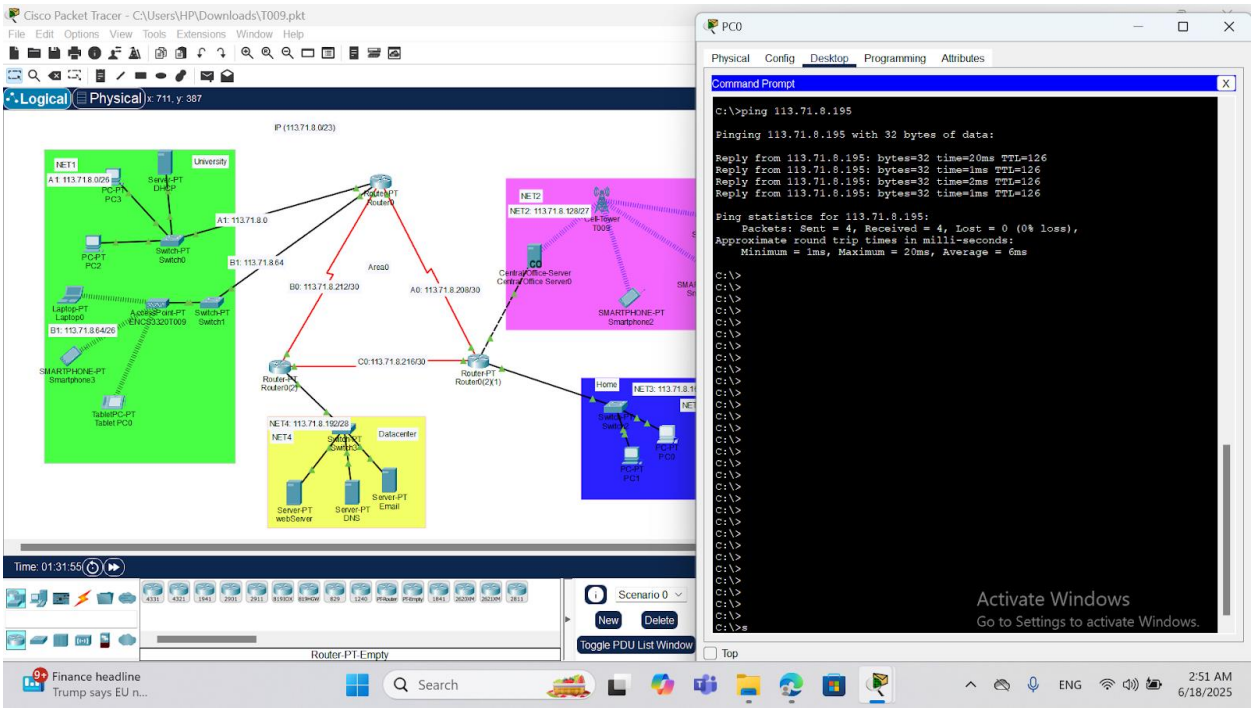


Figure 46:Successful ping test from PC0 to 113.71.8.195 with 0% packet loss and low delay

We used the ping command to test the connection to the IP address 113.71.8.195.

All 4 packets were received, and none were lost .This means the network connection is working correctly.

The reply times were:

- Minimum = 1 ms
- Maximum = 20 ms
- Average = 6 ms

These are good times. The connection is fast and stable.

The TTL value was 126, which means the packet passed through 1 or 2 routers, which is normal.

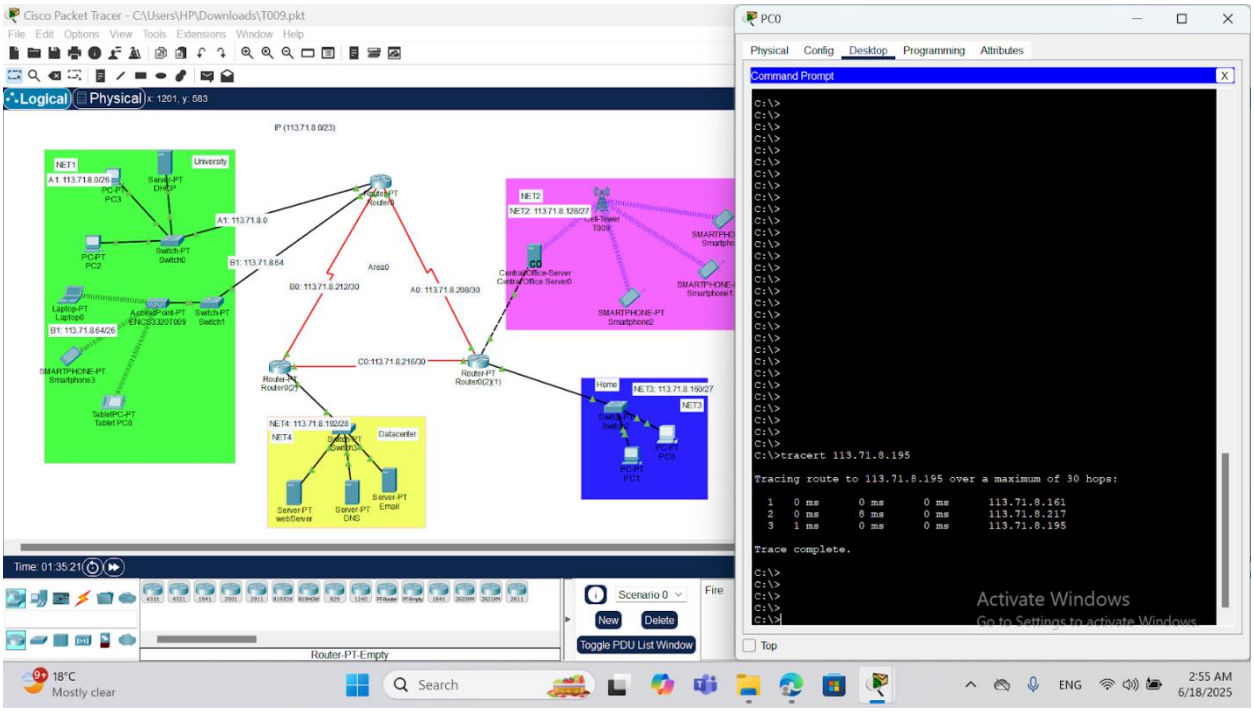


Figure 47:Traceroute to 113.71.8.195 completed in 3 hops with no delay or timeout

We used the tracert command to test the path from this device to the IP address 113.71.8.195.

The traceroute shows that the packet reached the destination in 3 hops:

1. First hop: 113.71.8.161 router 2
2. Second hop: 113.71.8.217 router 1
3. Third hop: 113.71.8.195 (the target device)

All hops replied quickly with very low delay (0–8 ms), and the trace finished successfully.

This shows that:

- All routers between the source and destination are working
- OSPF routing is correct
- The network is fast and connected properly

C. Between the PC0 in Home area and MailServer in Datacenter area

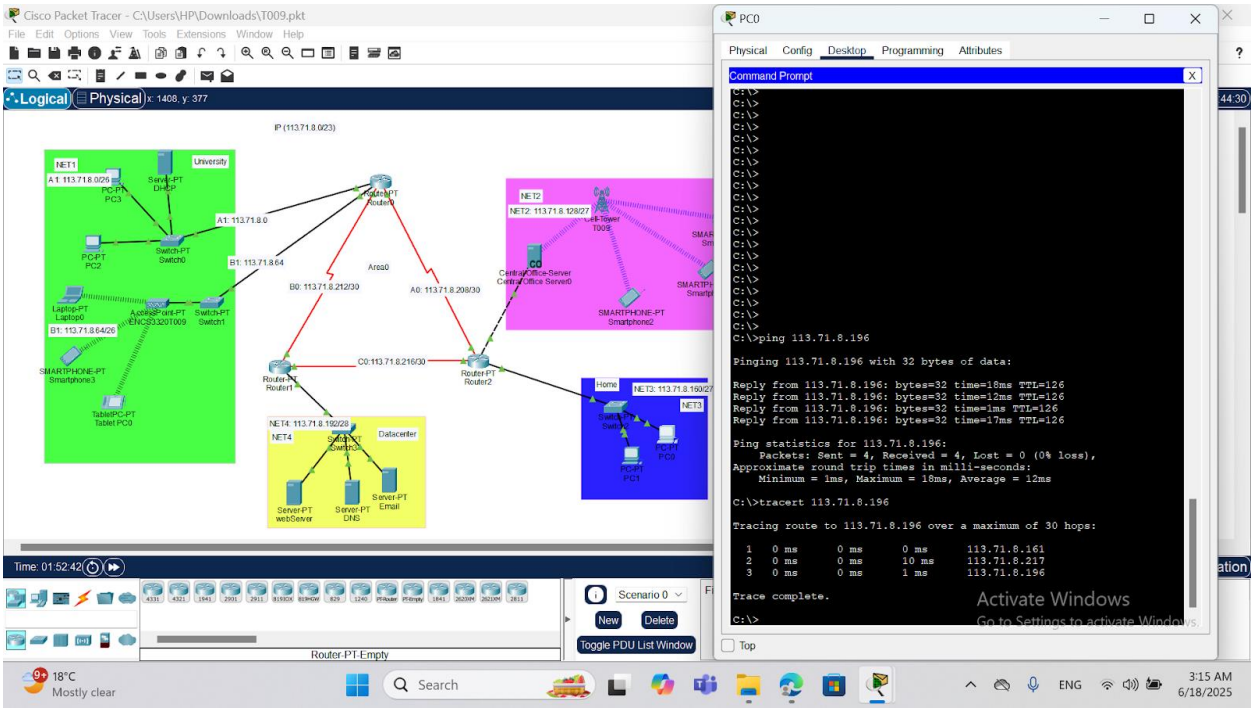


Figure 48:Ping and tracert test to 113.71.8.196

Ping Test

We used the ping command to test the connection to the device with IP address 113.71.8.196.

- All 4 packets were received
- There was 0% packet loss, which means the network is working well
- The reply times were fast:
    - Minimum = 1 ms
    - Maximum = 18 ms
    - Average = 12 ms

The TTL = 126, which means the destination was 1 or 2 hops away. This is normal.

This result shows that the device is reachable, and the network connection is stable and fast.

Traceroute Test

We also used the tracert command to check the path from this PC to 113.71.8.196.

The packet passed through 3 hops:

1. 113.71.8.161 → first router Router 2
2. 113.71.8.217 → second router Router 1
3. 113.71.8.196 → destination

- The trace finished successfully
- No errors or timeouts
- Delay was very low: between 0 ms and 10 ms

This means the routing (OSPF) is working correctly, and the connection is very fast.

C. Between the PC1 in Home area andSmartphone0 in Street area:

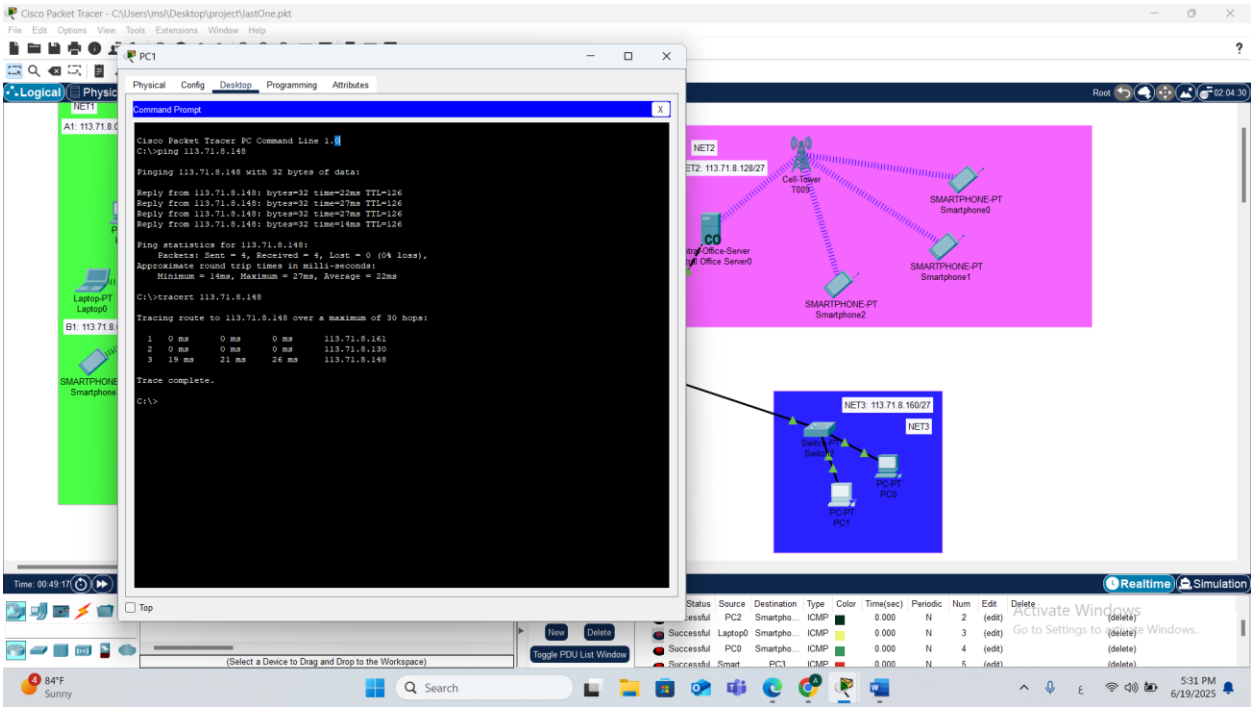


Figure 49:ping and tracert test to 113.71.8.148

Ping Test

We used the ping command to check the connection to 113.71.8.148.

- All 4 packets were received
- There was 0% packet loss, which means the connection is good
- The reply times were:
  - Minimum = 14 ms
  - Maximum = 27 ms
  - Average = 22 ms

The TTL = 126, which shows that the destination is close (1–2 hops away). The network is stable and there are no problems.

Traceroute Test

We used the tracert command to see the path from our PC to 113.71.8.148.

The packet passed through 3 hops:

1. 113.71.8.161 Router 2
2. 113.71.8.130 Central Switch

3. 113.71.8.148 (destination)

Each hop responded correctly, with no timeout.

The response times were between 0 ms and 26 ms, which is good.

This shows that:

• The routing is working

• The destination is reachable

• OSPF is configured correctly

E. Between the PC1 in Home area and laptop0 in University area:

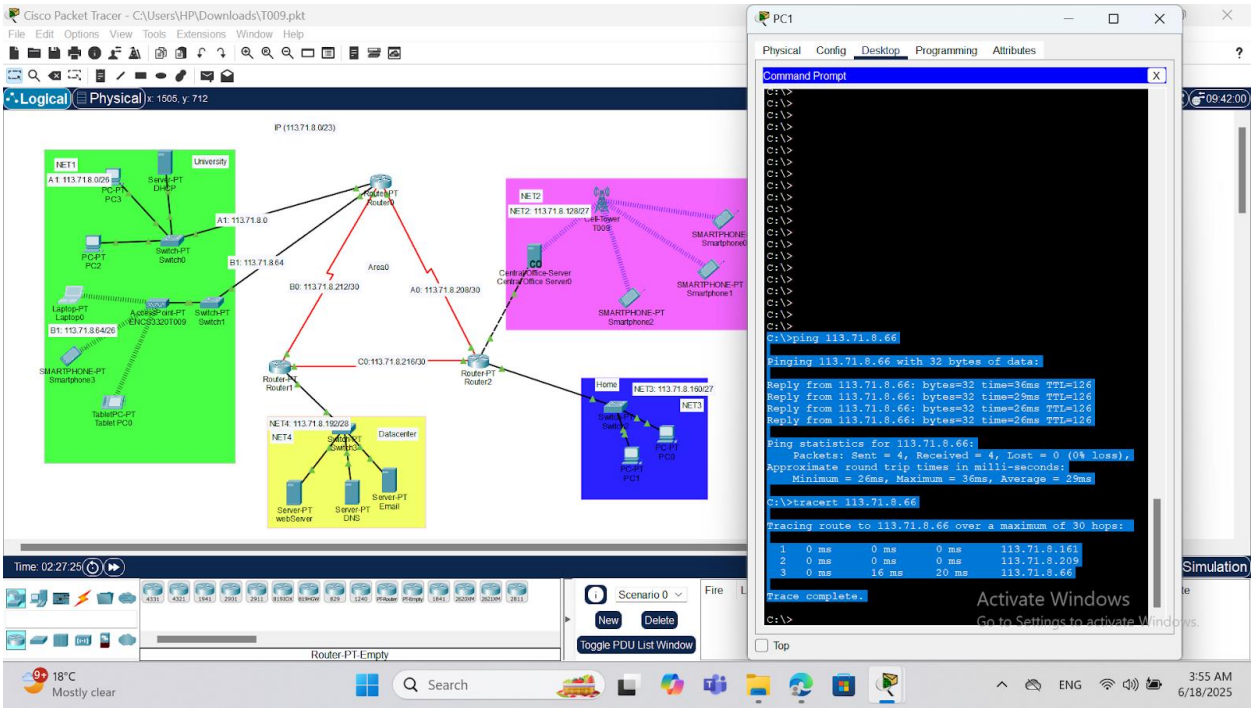


Figure 50:Ping and tracert test to 113.71.8.66

Ping Test

We used the ping command to test the connection to the IP address 113.71.8.66.

- All 4 packets were received
- 0% packet loss, which means the device is reachable
- The reply times were good:
    - Minimum = 26 ms
    - Maximum = 36 ms
    - Average = 29 ms

The TTL = 126, which shows the device is close (about 2 hops away).The connection is stable and the delay is low.

Traceroute Test

We also used the tracert command to see the path from our PC to 113.71.8.66.

The traceroute went through 3 hops:

1. 113.71.8.161 Router 2
2. 113.71.8.209 Router 0
3. 113.71.8.66 (destination)

All routers responded quickly.

The delay was very low: from 0 ms to 20 ms.

This confirms that the routing is working, and the destination is reachable without problems.

F. Between the PC0 in Home area and PC2 in University area:

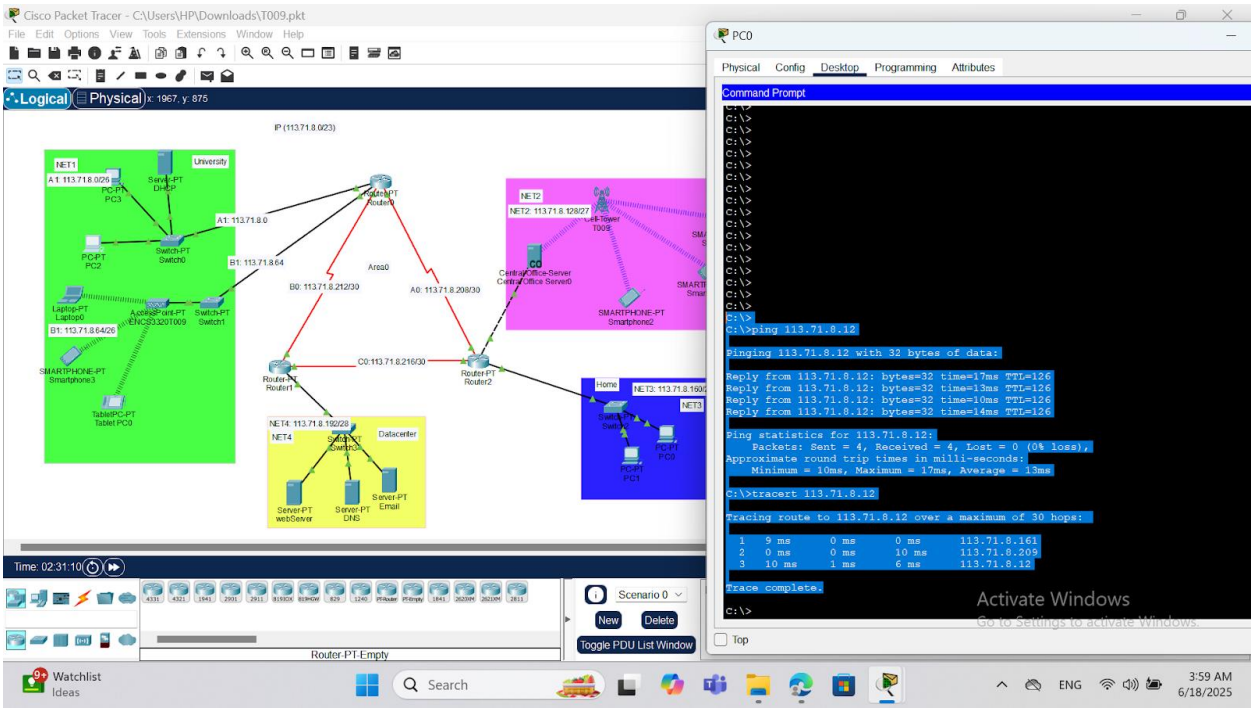


Figure 51:Ping and tracert test to 113.71.8.12

Ping Test

We used the ping command to check the connection to 113.71.8.12.

- All 4 packets were received
- 0% packet loss means the connection is working well
- The reply times were:
    - Minimum = 10 ms
    - Maximum = 17 ms
    - Average = 13 ms

The TTL = 126, showing the device is close in the network (1–2 hops away).The response was fast and the connection is stable.

Traceroute Test

We used the tracert command to see the path to the same device.

It passed through 3 hops:

1. 113.71.8.161 Router 2
2. 113.71.8.209 Router 0
3. 113.71.8.12 (destination)

All hops responded with very low delay (between 0 ms and 10 ms).There were no errors or timeouts.

This shows the routing and OSPF are working correctly.

From Area 2 (Street area) TO All Areas

A. Between the smartPhone0 in Street area and Web Server in Datacenter area

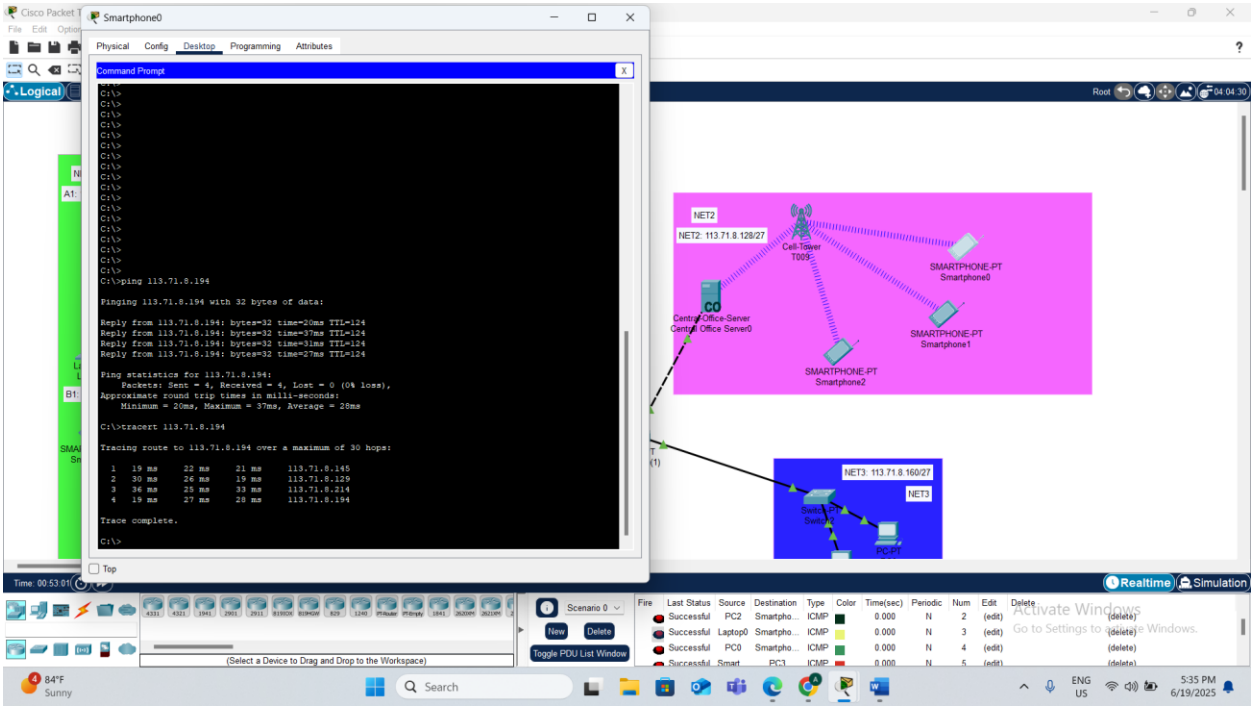


Figure 52:Ping and Tracert test to 113.71.8.194

Ping Test

We used the ping command to check the connection to 113.71.8.194.

- All 4 packets were received
- There was 0% packet loss, which means the connection is good
- The reply times were:
  - Minimum = 20 ms
  - Maximum = 37 ms
  - Average = 28 ms

The TTL = 124, which indicates the destination is slightly farther than previous devices but still within a few hops.

The network is stable and no issues were detected.

Traceroute Test

We used the tracert command to see the path from our PC to 113.71.8.194.

The packet passed through 4 hops:

1. 113.71.8.145
2. 113.71.8.129
3. 113.71.8.214
4. 113.71.8.194 (destination)

Each hop responded correctly, with no timeouts.

The response times were between 19 ms and 36 ms, which is within a normal and healthy range.

This shows that:

• The routing is working

• The destination is reachable

• OSPF is configured and forwarding traffic correctly

B. Between the smartPhone1 in Street area and TabletPc0 in University area

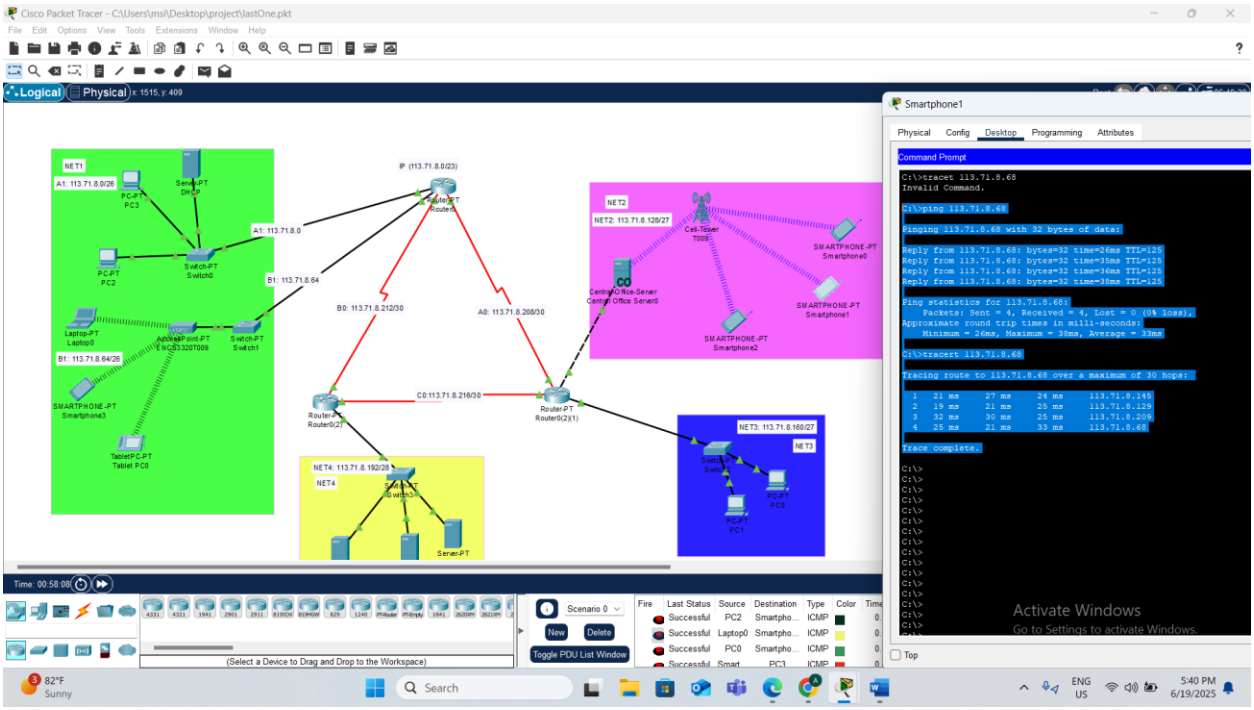


Figure 53:Ping and tracert test to 113.71.8.68

Ping Test

We used the ping command to check the connection to 113.71.8.68.

- All 4 packets were received
- There was 0% packet loss, which indicates a stable connection
- The reply times were:
  - Minimum = 26 ms
  - Maximum = 38 ms
  - Average = 33 ms

The TTL = 125, which means the destination is a few hops away (approximately 2–3 hops).

The network is performing well with no signs of packet loss or delay issues.

Traceroute Test

We used the tracert command to trace the path from our PC to 113.71.8.68.

The packet passed through 4 hops:

1. 113.71.8.145 (Local Router)

2. 113.71.8.129 (Core Switch)
3. 113.71.8.209 (Intermediate Router)
4. 113.71.8.68 (destination)

Each hop responded successfully with no timeouts.

The response times ranged between 19 ms and 33 ms, indicating efficient routing.

This confirms that:

• The routing path is correct

• The destination is reachable

• OSPF is functioning as expected

C. Between the smartPhone2 in Street area and PC2 in University area:

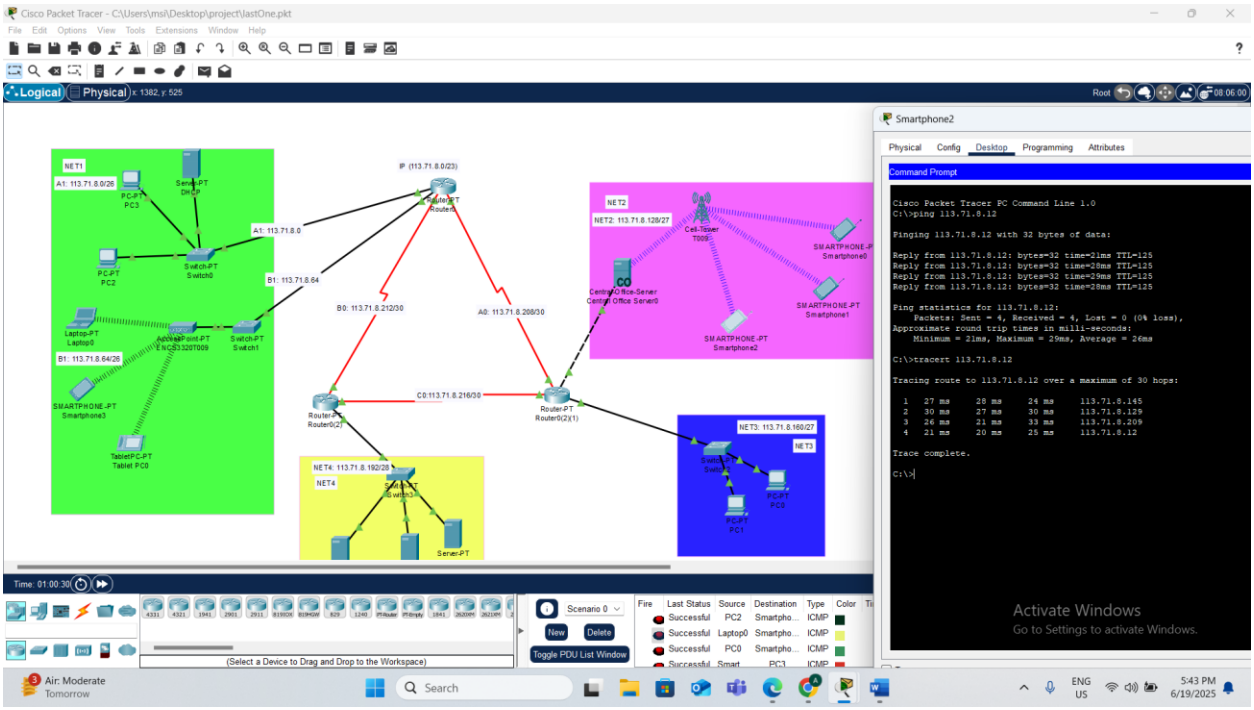


Figure 54:Ping and tracert test to 113.71.8.12

Ping Test

We used the ping command to check the connection to 113.71.8.12.

- All 4 packets were received
- There was 0% packet loss, which confirms a reliable connection
- The reply times were:
  - Minimum = 21 ms
  - Maximum = 29 ms
  - Average = 26 ms

The TTL = 125, which suggests the destination is 2–3 hops away.

Overall, the network is stable and functioning properly.

Traceroute Test

We used the tracert command to trace the route from our PC to 113.71.8.12.

The packet passed through 4 hops:

1. 113.71.8.145 (Local Router)

2. 113.71.8.129 (Core Switch)
3. 113.71.8.209 (Intermediate Router)
4. 113.71.8.12 (destination)

All hops responded successfully, with no timeouts.

The response times ranged between 20 ms and 33 ms, which is considered healthy.

This shows that:

• The routing is properly configured

• The destination is reachable

• OSPF is running correctly across the network

D. Between the smartPhone0 in Street area and PC0 in Home area:

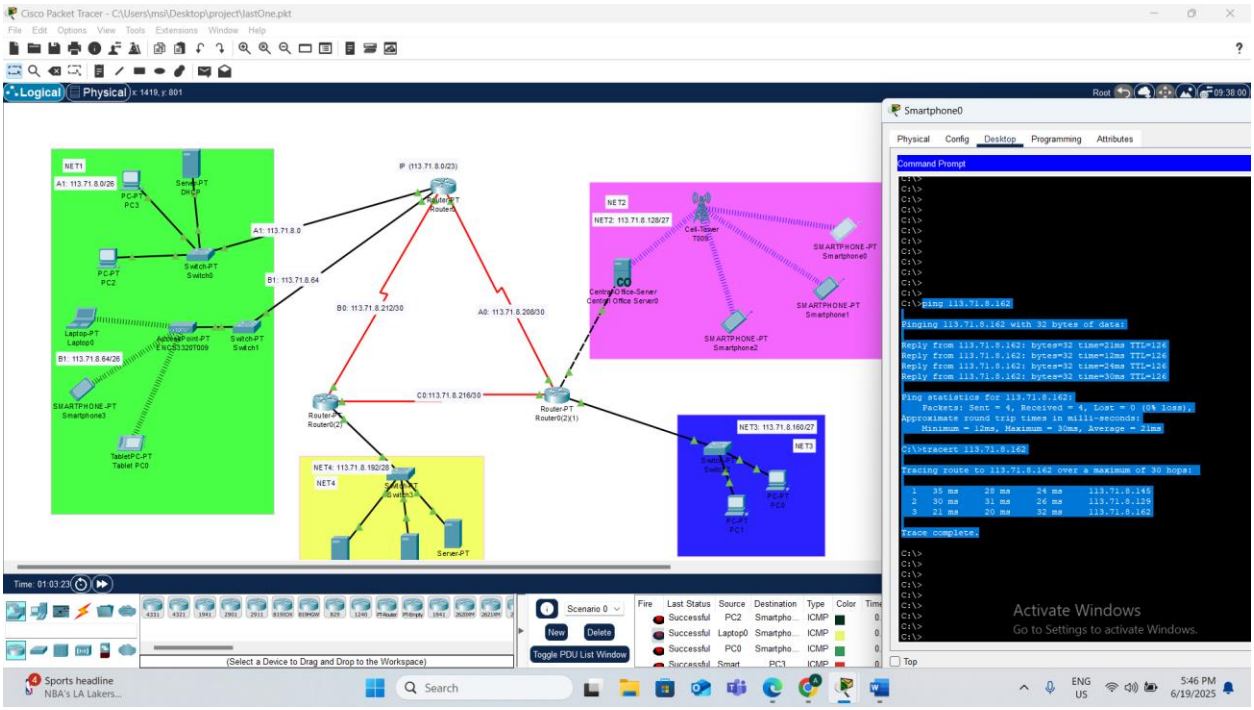


Figure 55:Ping and tracert test to 113.71.8.162

Ping Test

We used the ping command to check the connection to 113.71.8.162.

- All 4 packets were received
- There was 0% packet loss, indicating a stable and reliable connection
- The reply times were:
  - Minimum = 12 ms
  - Maximum = 30 ms
  - Average = 21 ms

The TTL = 126, which means the destination is very close (1–2 hops away).

The network is functioning smoothly with low latency and no issues detected.

Traceroute Test

We used the tracert command to trace the route from our PC to 113.71.8.162.

The packet passed through 3 hops:

1. 113.71.8.145 (Local Router)

2. 113.71.8.129 (Core Switch or Distribution Device)

3. 113.71.8.162 (destination)

All hops responded correctly with no timeouts.

The response times ranged from 20 ms to 35 ms, which is considered efficient.

This confirms that:

• The routing path is working correctly

• The destination is reachable

• OSPF is configured and forwarding traffic without issues

From Area 1 (University area) TO All Areas

A. Between PC3 in University area and mail server in Datacenter area

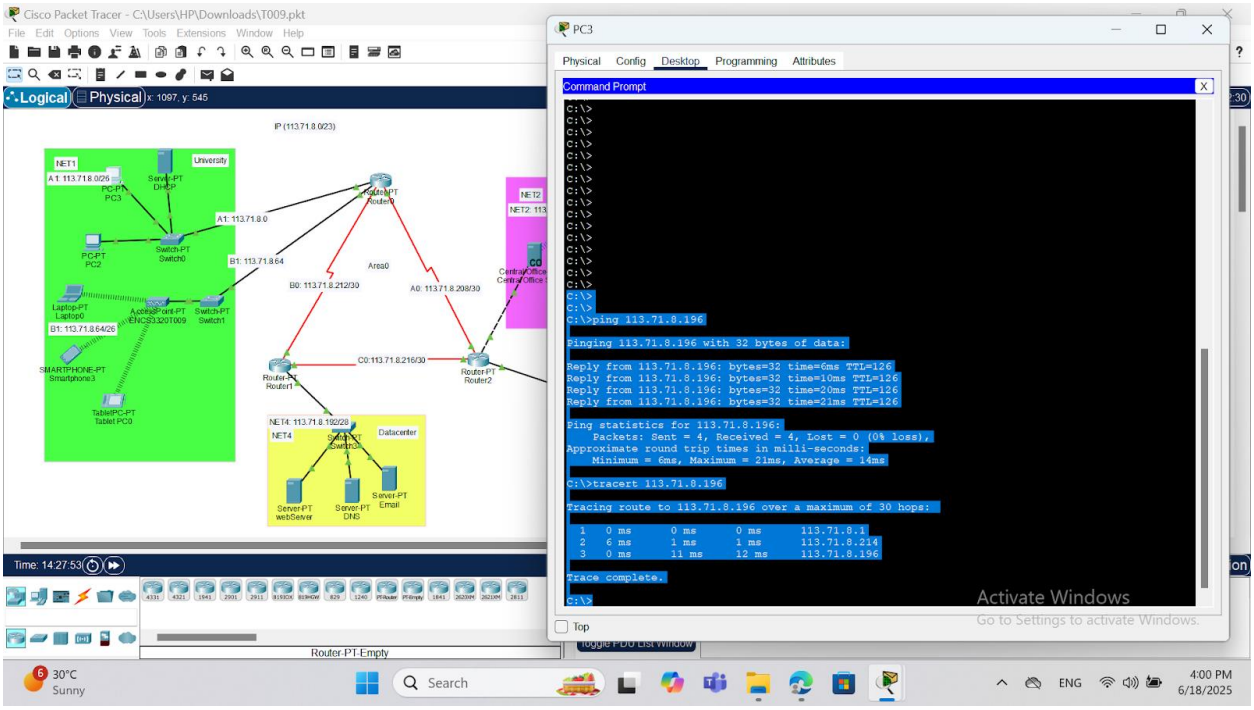


Figure 56:Ping and tracert test to 113.71.8.196.

Ping Test

We used the ping command to test the connection to the IP address 113.71.8.196.

- All 4 packets were received
- There was 0% packet loss, meaning the connection is reliable
- The response times were:
    - Minimum = 6 ms
    - Maximum = 21 ms
    - Average = 14 ms

The TTL = 126, showing that the destination is close (1 or 2 hops away). The ping replies were fast and stable.

Traceroute Test

We also used the tracert command to check the route to 113.71.8.196.

The packet passed through 3 hops:

1. 113.71.8.1 Router 0
2. 113.71.8.214 Router 1
3. 113.71.8.196 (destination)

All hops responded successfully, and there were no timeouts.

The delay was low, between 0 ms and 12 ms.

This confirms that the OSPF routing is configured properly, and the connection is working well.

B. Between PC2 in University area andPC0 in Home area

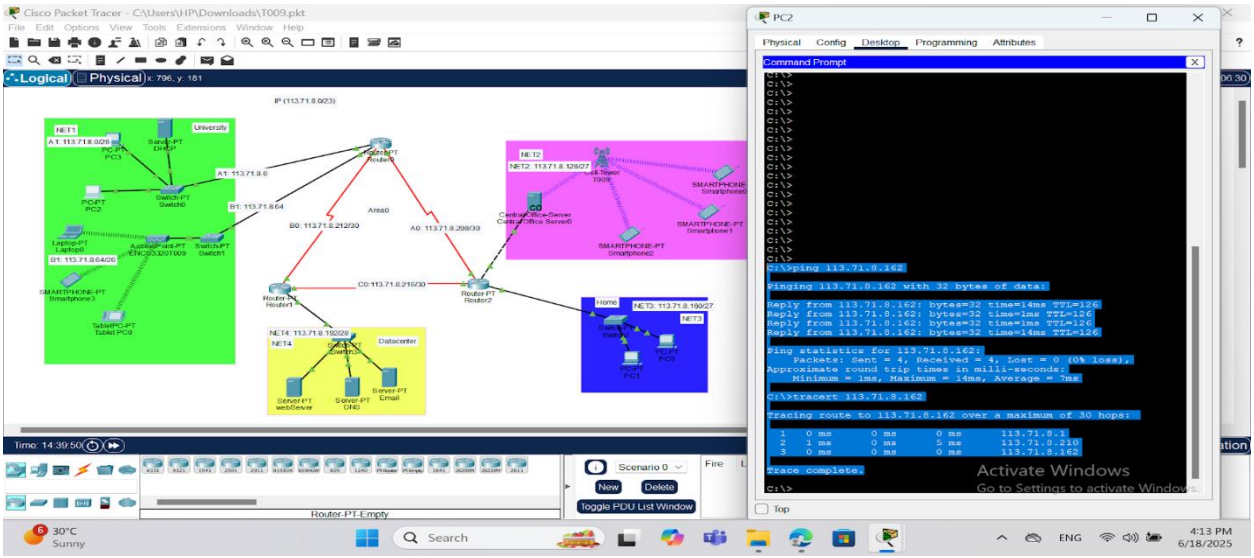


Figure 57:Ping and tracert test to 113.71.8.162

Ping Test

We used the ping command to check the connection to 113.71.8.162.

- All 4 packets were received
- 0% packet loss, which means the connection is working
- The reply times were very fast:
    - Minimum = 1 ms
    - Maximum = 14 ms
    - Average = 7 ms

The TTL = 126, meaning the destination is very close (1 or 2 hops away). The results show a stable and fast network.

Traceroute Test

We used the tracert command to trace the route to 113.71.8.162.

The packet passed through 3 hops:

1. 113.71.8.1 Router 0

2. 113.71.8.210 Router 2
3. 113.71.8.162 (destination)

Each hop responded quickly and without errors. The delay was between 0 ms and 5 ms, which is excellent.

This means that OSPF routing is working properly, and the connection is clear and fast.

C .Between PC3 in University area and smartphone1 in Street area

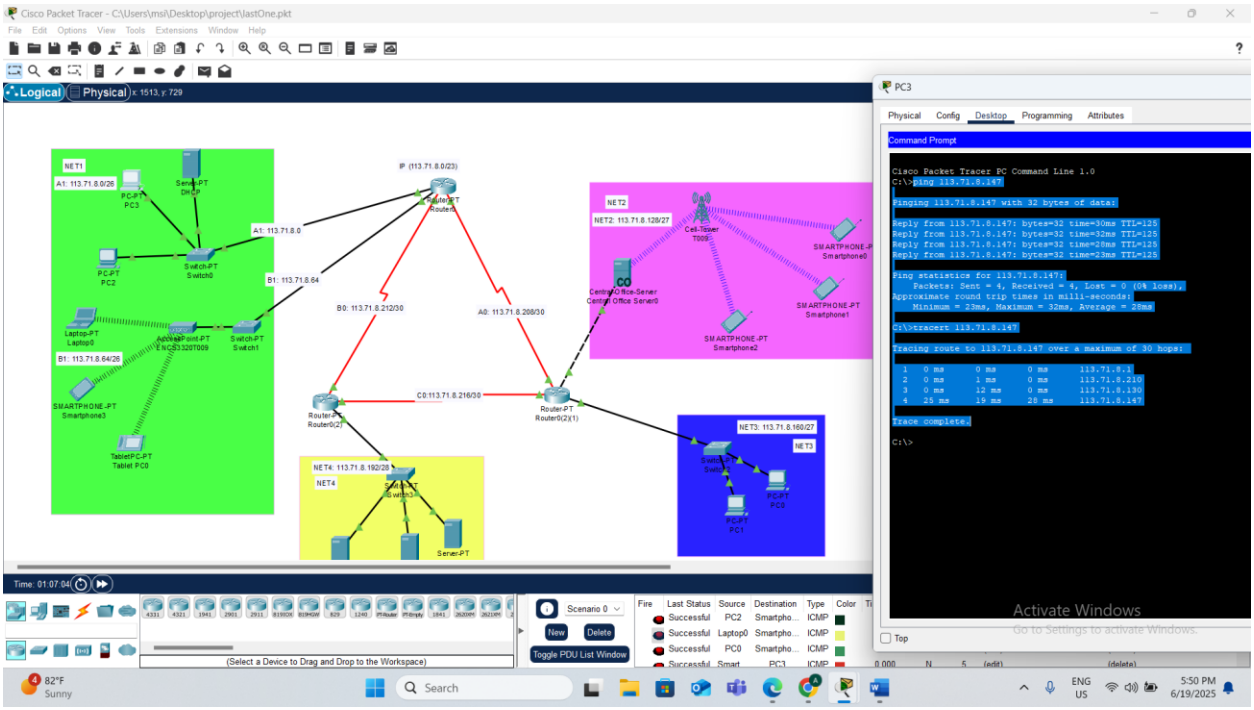


Figure 58:Ping and tracert test to 113.71.8.147

Ping Test

We used the ping command to check the connection to 113.71.8.147.

- All 4 packets were received
- There was 0% packet loss, which confirms a stable connection
- The reply times were:
  - Minimum = 23 ms
  - Maximum = 32 ms
  - Average = 28 ms

The TTL = 125, indicating that the destination is 2–3 hops away.

The latency is low and consistent, which reflects good network performance.

Traceroute Test

We used the tracert command to trace the route from our PC to 113.71.8.147.

The packet passed through 4 hops:

1. 113.71.8.1 (Local Gateway or PC's default router)

2. 113.71.8.210 (Access Switch or Internal Router)
3. 113.71.8.130 (Core Router or Distribution Layer)
4. 113.71.8.147 (destination)

Each hop responded with no timeouts and very low response times (0–28 ms).

This confirms that:

• The network path is properly configured

• The destination is reachable

• OSPF routing is working as intended

D .Between PC2 in University area and smartphone3 in University area

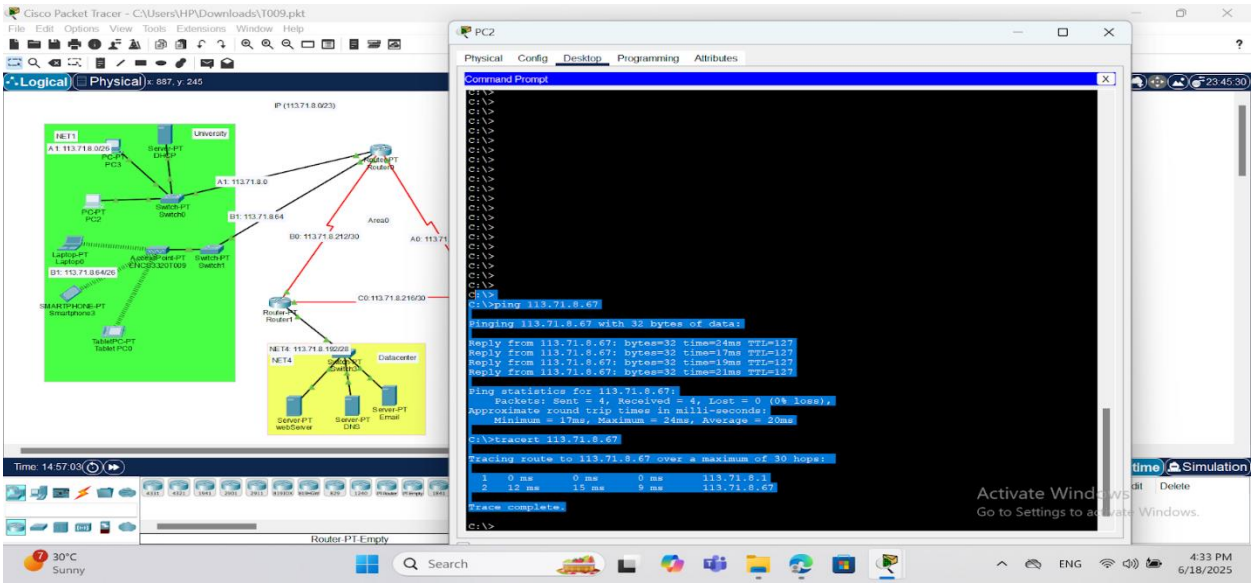


Figure 59:Ping and tracert test to 113.71.8.67

Ping Test

We used the ping command to test the connection to 113.71.8.67.

- All 4 packets were received
- 0% packet loss
- The response times were fast:
    - Minimum = 17 ms
    - Maximum = 24 ms
    - Average = 20 ms

The TTL = 127, which means the destination is very close, probably only 1 hop away.

This shows the connection is stable, fast, and working perfectly.

Traceroute Test

We used the tracert command to check the path from our device to 113.71.8.67.

The packet passed through only 2 hops:

1. 113.71.8.1

2. 113.71.8.67 (destination)

Both hops responded quickly with no timeouts.

The delay was very low: between 9 ms and 15 ms.

This confirms that the OSPF routing is correct and the destination is directly connected or very close.

From Area 4 (Datacenter area) TO All Areas

A. Between DNS server in Datacenter Area and PC1 in Home area

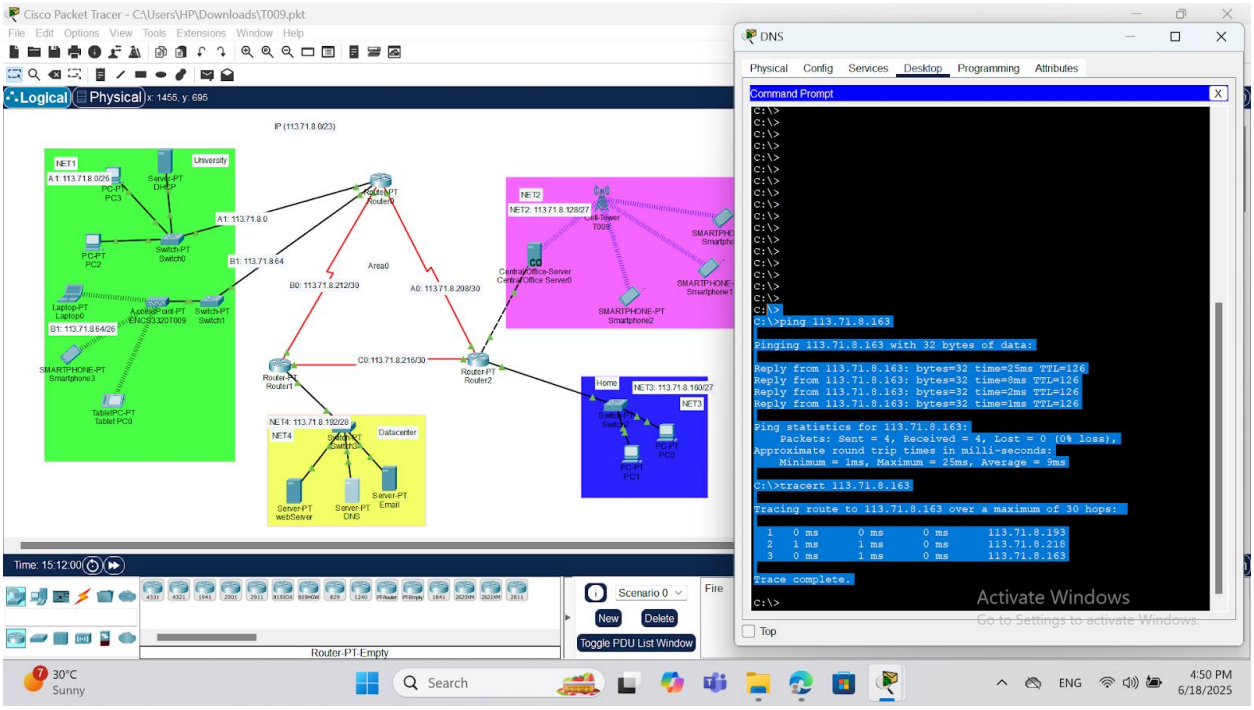


Figure 60:Ping and tracert test to 113.71.8.163

Ping Test

We used the ping command to test the connection to 113.71.8.163.

- All 4 packets were received
- 0% packet loss, meaning the connection is stable
- The response times were:
    - Minimum = 1 ms
    - Maximum = 25 ms
        - Average = 9 ms

The TTL = 126, showing that the destination is close (1 or 2 hops away). The network is working quickly and with no errors.

Traceroute Test

We used the tracert command to trace the route to 113.71.8.163.

The packet passed through 3 hops:

113.71.8.193 Router 1

113.71.8.218 Router 2

113.71.8.163 (destination)

All hops replied successfully and very fast — between 0 and 1 ms.There were no delays or errors in the path.

This means the OSPF routing is configured properly, and the destination is reachable.

B. Between Web server in Datacenter Area and PC2 in University area

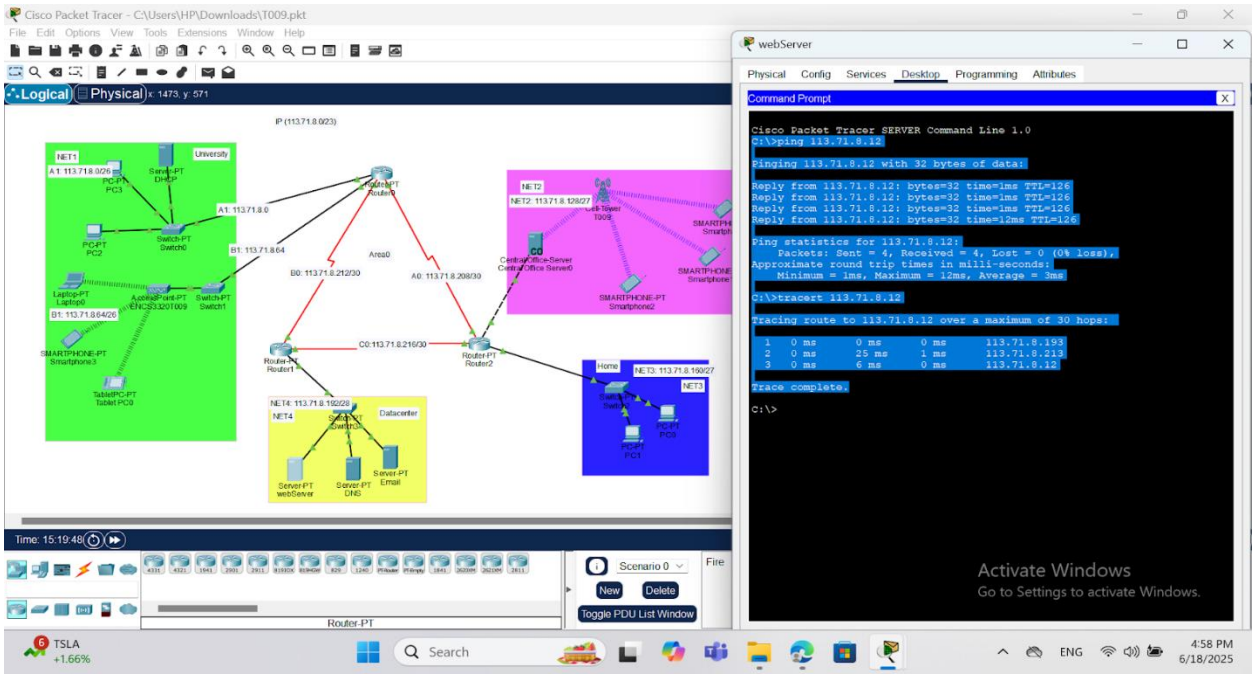


Figure 61:Ping and tracert test to 113.71.8.12

Ping Test

We used the ping command to test the connection to 113.71.8.12.

All 4 packets were received

0% packet loss, which means the connection is perfect

The response times were:

- Minimum = 1 ms
- Maximum = 1`2 ms
- Average = 3 ms

The TTL = 126, which shows the device is very close (probably 1 or 2 hops away). The results show a fast, stable, and healthy network connection.

Traceroute Test

We used the tracert command to see the route from the PC to 113.71.8.12.

The path included 3 hops:

113.71.8.193 Router 1

113.71.8.213 Router 0

113.71.8.12 (destination)

All hops responded successfully.The delay was very low: between 0 ms and 25 ms, with no timeouts.

This confirms that OSPF routing is working correctly and the destination is reachable.

C. Between Mail server in Datacenter Area and smartphone2 in Street area

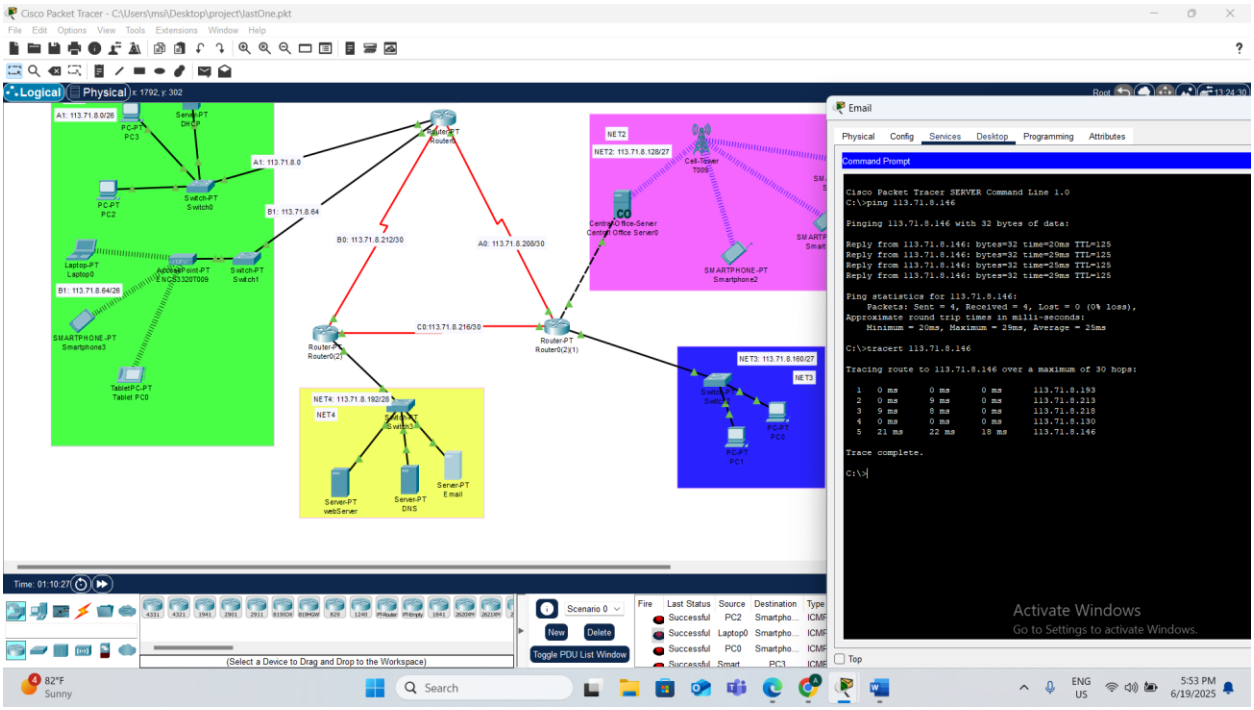


Figure 62:Ping and tracert test to 113.71.8.146

Ping Test

We used the ping command to check the connection to 113.71.8.146.

- All 4 packets were received
- There was 0% packet loss, which indicates a stable and reliable connection
- The reply times were:
  - Minimum = 20 ms
  - Maximum = 29 ms
  - Average = 25 ms

The TTL = 125, which suggests the destination is 2–3 hops away.

The connection is stable with low latency and no performance issues.

Traceroute Test

We used the tracert command to trace the route from our PC to 113.71.8.146.

The packet passed through 5 hops:

1. 113.71.8.193 (Local Router or Gateway)

2. 113.71.8.213 (Intermediate Router)
3. 113.71.8.218 (Transit Device or Switch)
4. 113.71.8.130 (Core Router)
5. 113.71.8.146 (destination)

All hops responded successfully with no timeouts.

The response times ranged between 0 ms and 22 ms, indicating efficient routing.

This confirms that:

• The routing path is functional

• The destination is reachable

• OSPF is working correctly across the path

D. Between DNS server in Datacenter Area and laptop0 in University area

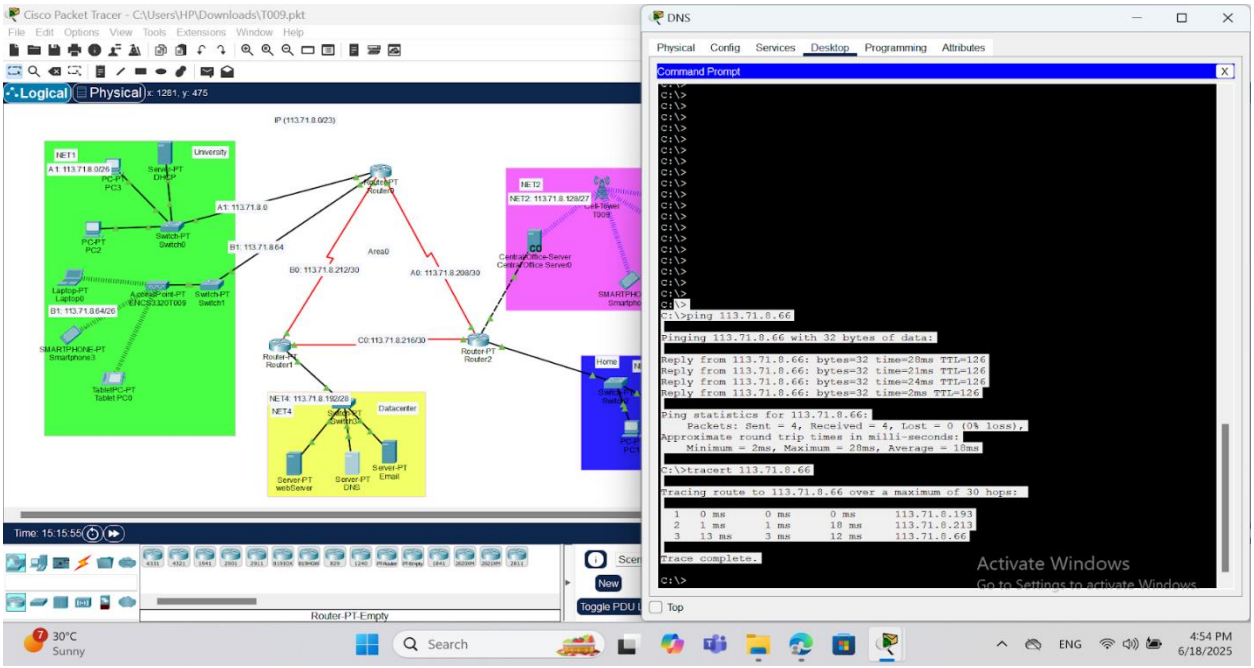


Figure 63:Ping and tracert test to 113.71.8.66

Ping Test

We used the ping command to test the connection to the device with IP 113.71.8.66.

- All 4 packets were received
- 0% packet loss shows the connection is working
- The response times were:
    - Minimum = 2 ms
    - Maximum = 28 ms
    - Average = 18 ms

The TTL = 126, meaning the device is close (about 2 hops away).This test confirms that the network connection is stable and fast.

Traceroute Test

We used the tracert command to trace the route to 113.71.8.66.

The packet passed through 3 hops:

1) 113.71.8.193 Router 1
2) 113.71.8.213 Router 0
3) 113.71.8.66 (destination)

All hops responded correctly and very fast, with response times between 0 ms and 18 ms.

- **Email client configuration and Successful sending and receiving of emails between the users from different networks for coe.birzeit.edu account**

1. Create Email for client PC1 in Home area.

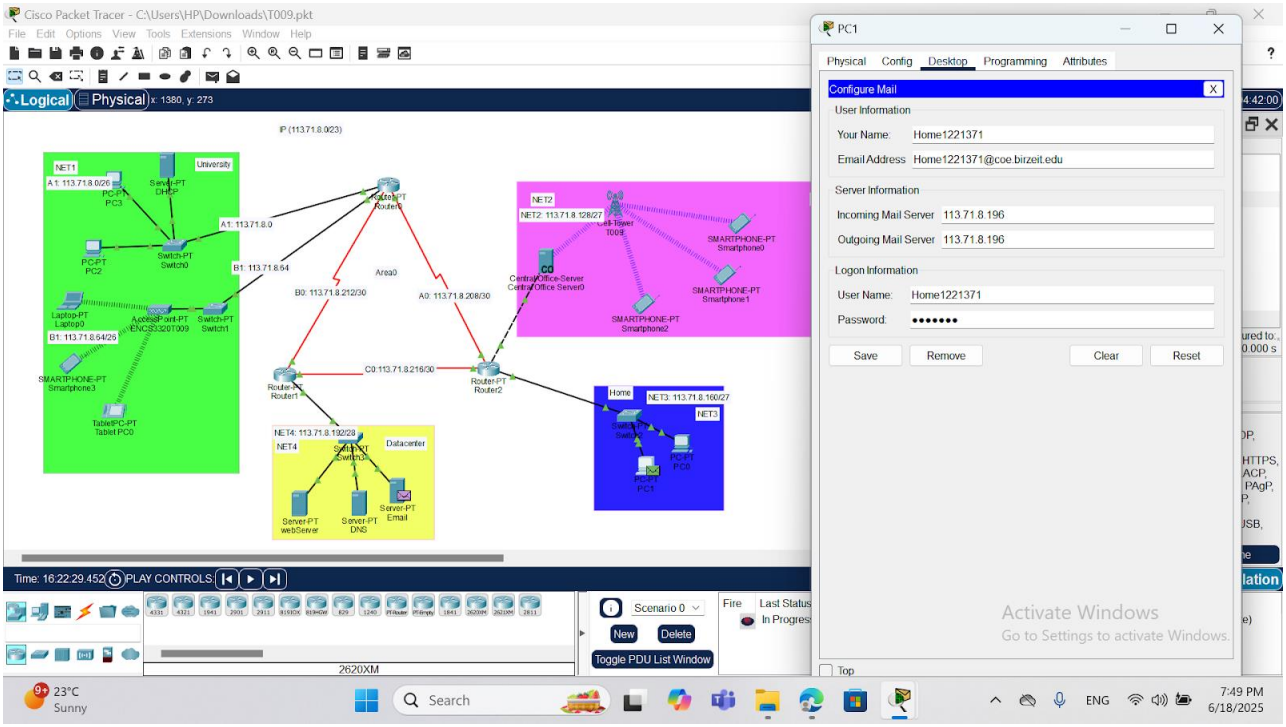


Figure 64:CREATE Email for client PC1 IN Home area

2. Create Email for client laptop0 in University area.

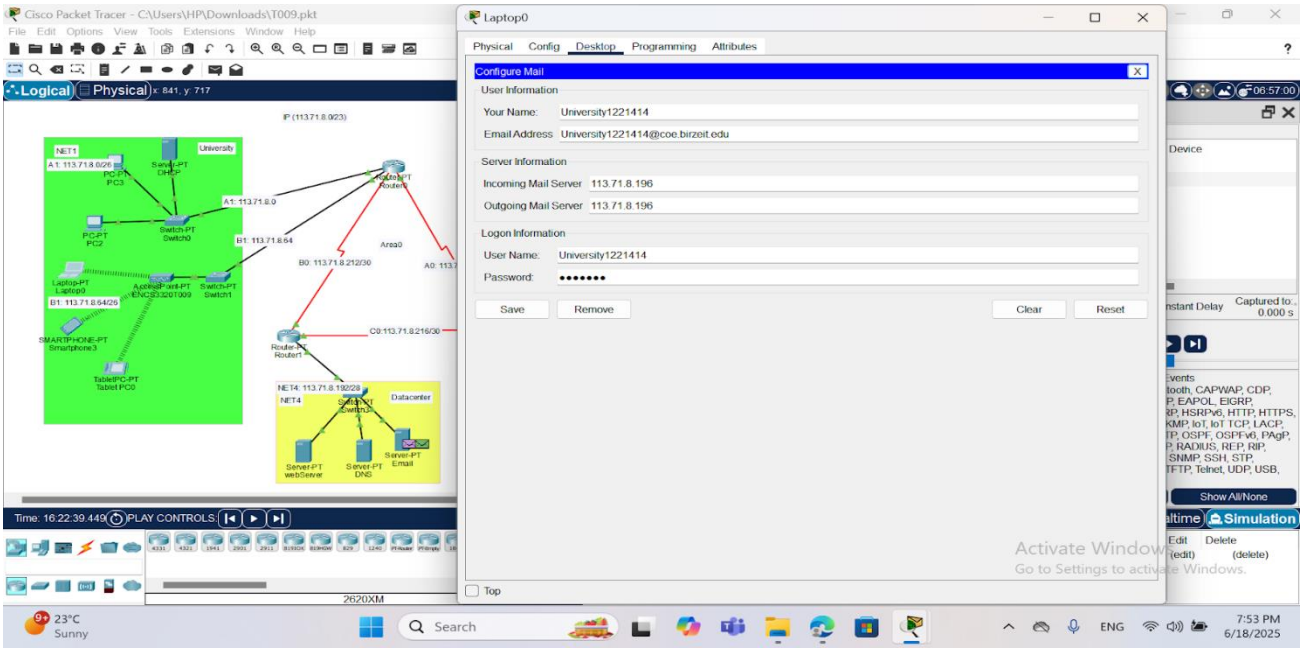


Figure 65:Creare Email for client laptop0 in University area

3. Create massage Email for pc1 in home area

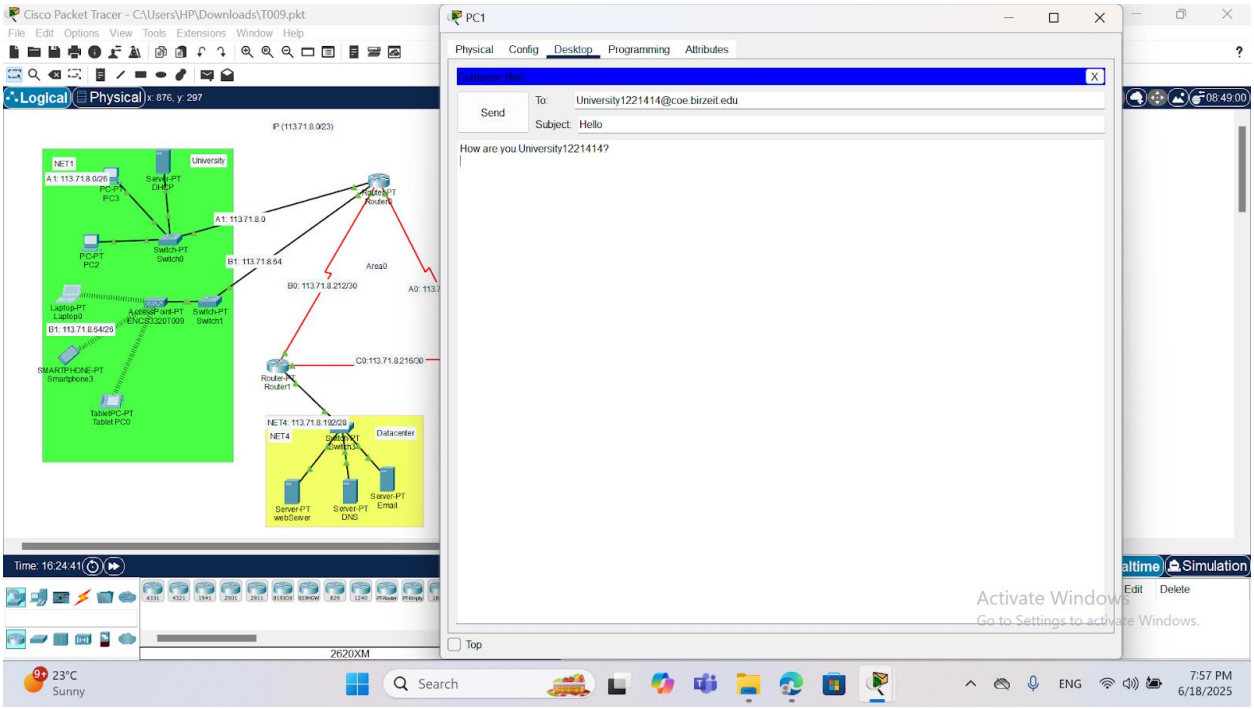


Figure 66:Create massage Email for pc1 in home area

4. sending message Email successful

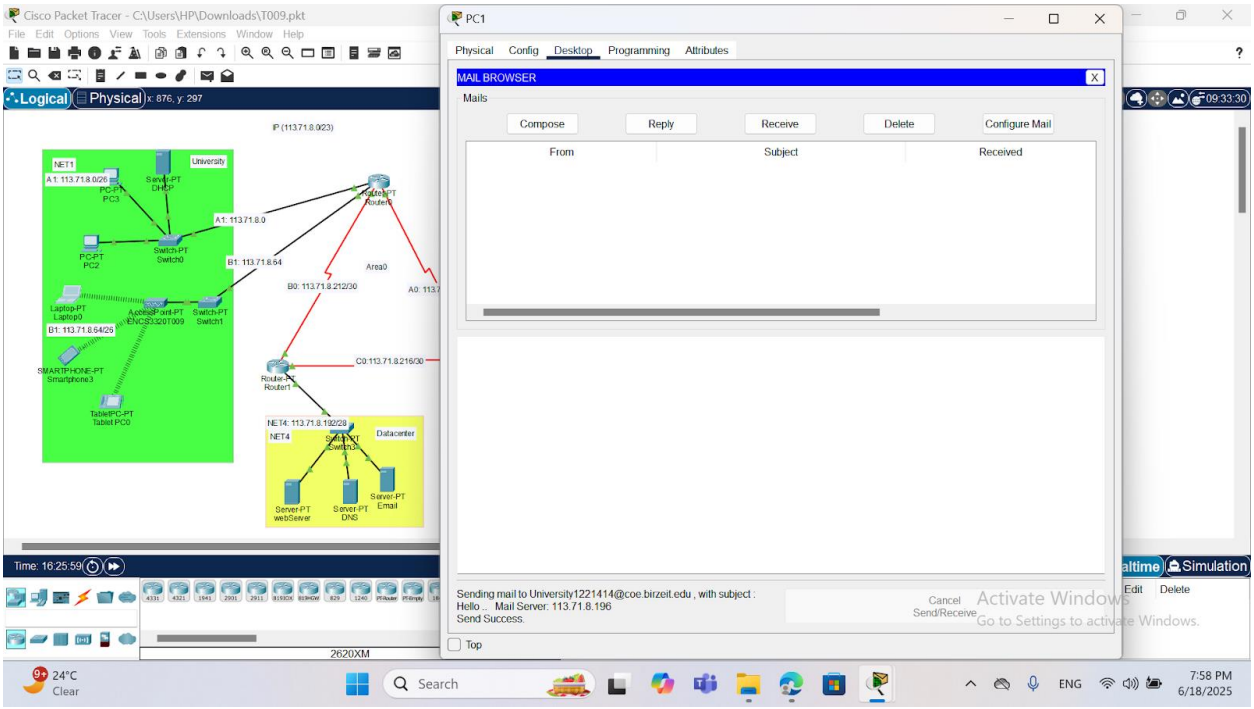


Figure 67:sending message Email successful

5. receiving message Email successfully in laptop0 in university area

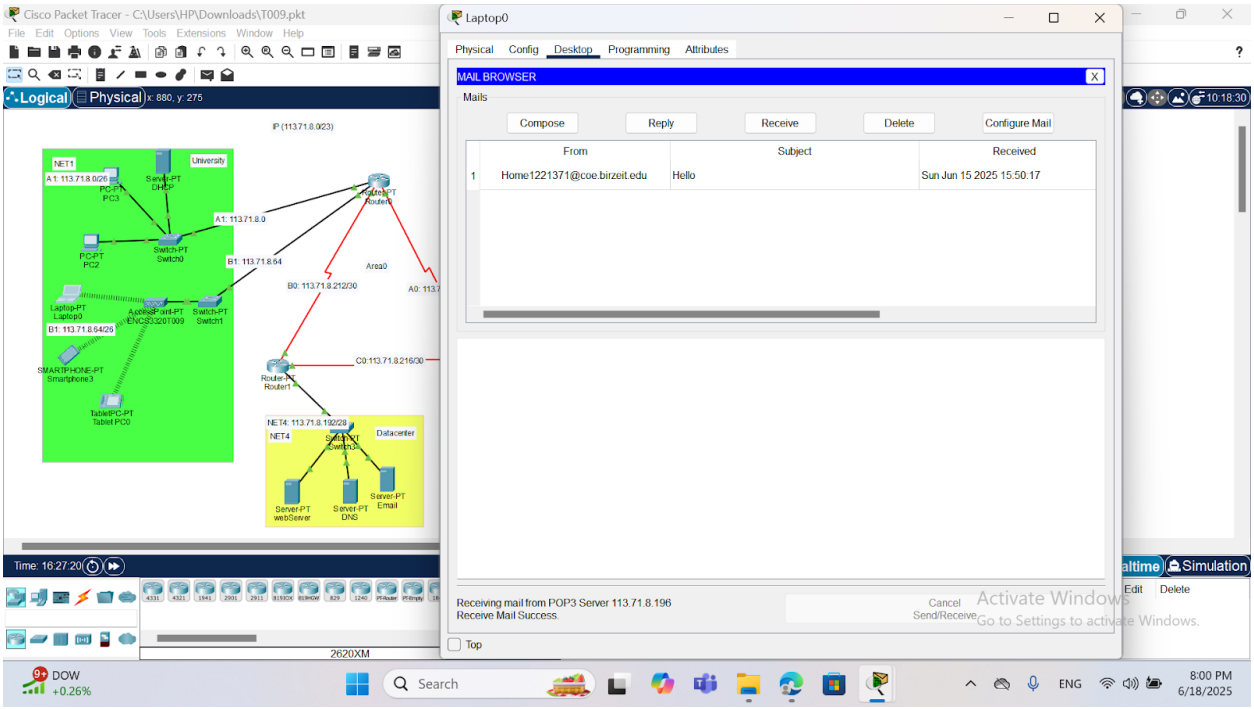


Figure 68:receiving message Email successfully in laptop0 in university area

6. massage that receive

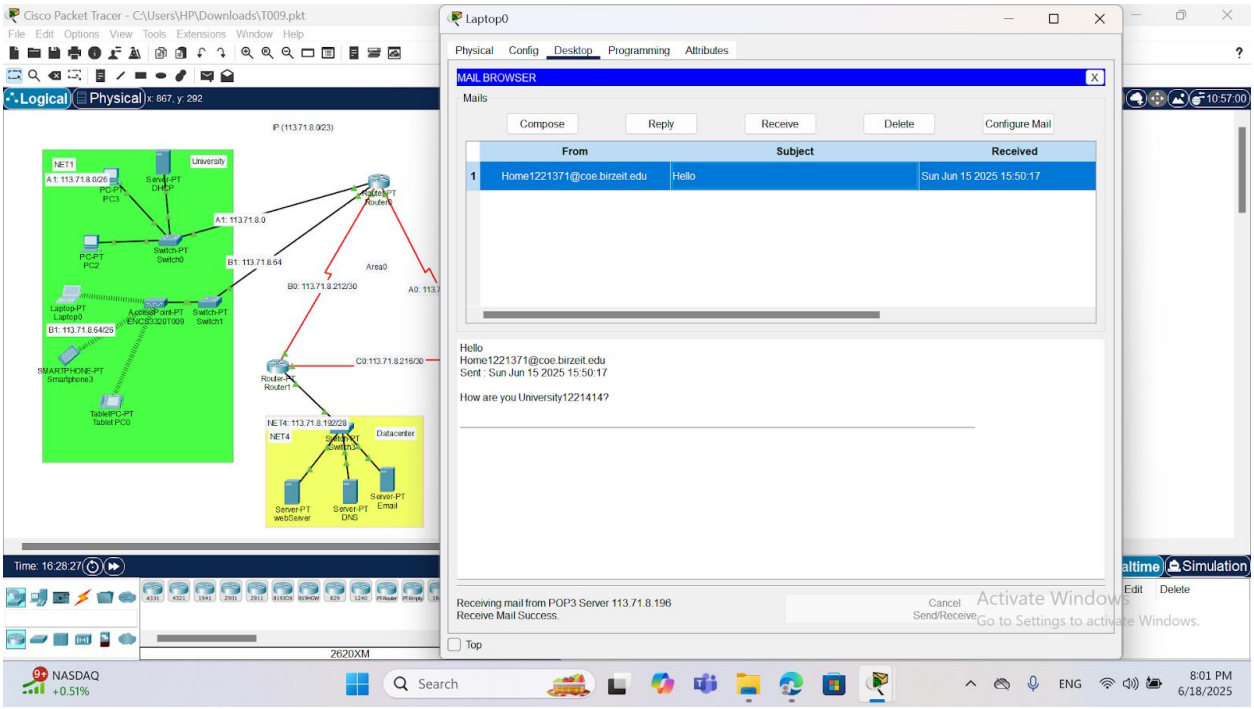


Figure 69:the massage receive in laptop0

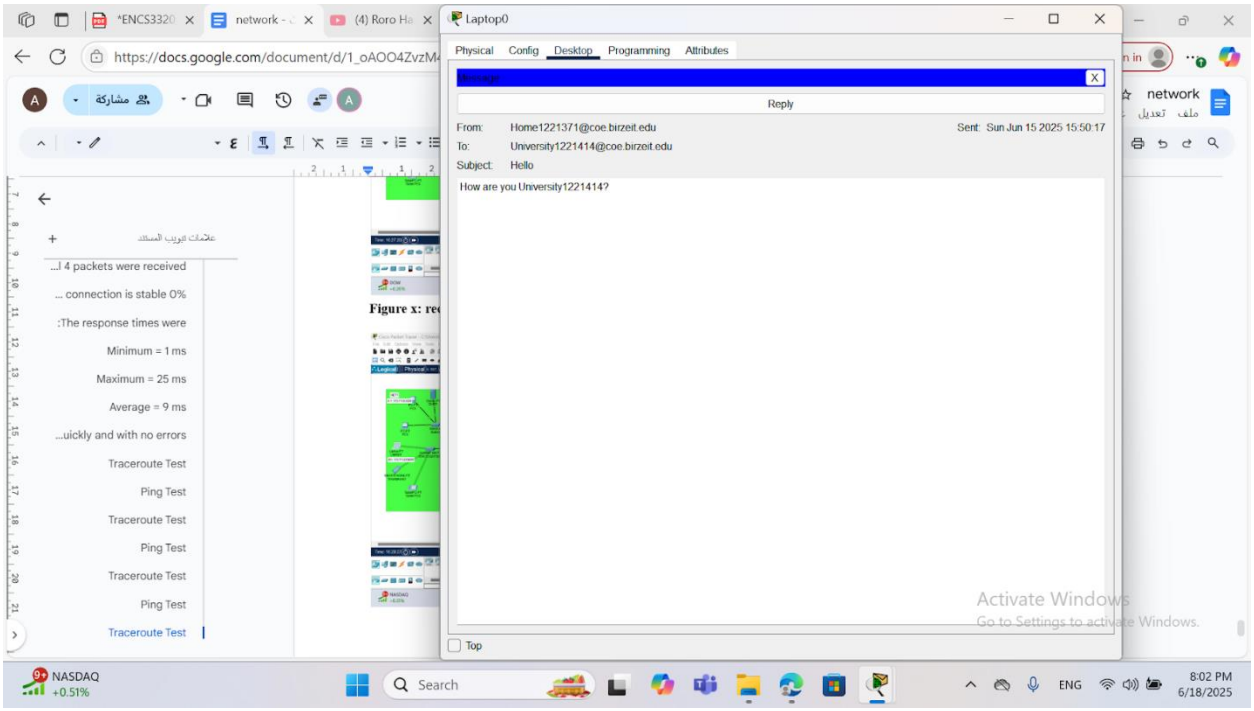


Figure 70:the massage receive in laptop0 (cont)

- **Successful access to the webserver www.coe.birzeit.edu from**

The web page hosted on the web server was accessed successfully from different end devices using the domain name. The DNS resolved the name correctly.

Note: Due to limitations in Cisco Packet Tracer's web browser simulation, the tab title defined within the HTML `<title>` tag (e.g., “COE-Birzeit”) does not appear when viewing the webpage. The simulator renders only the body content of the HTML page, and does not process head elements such as the tab title.

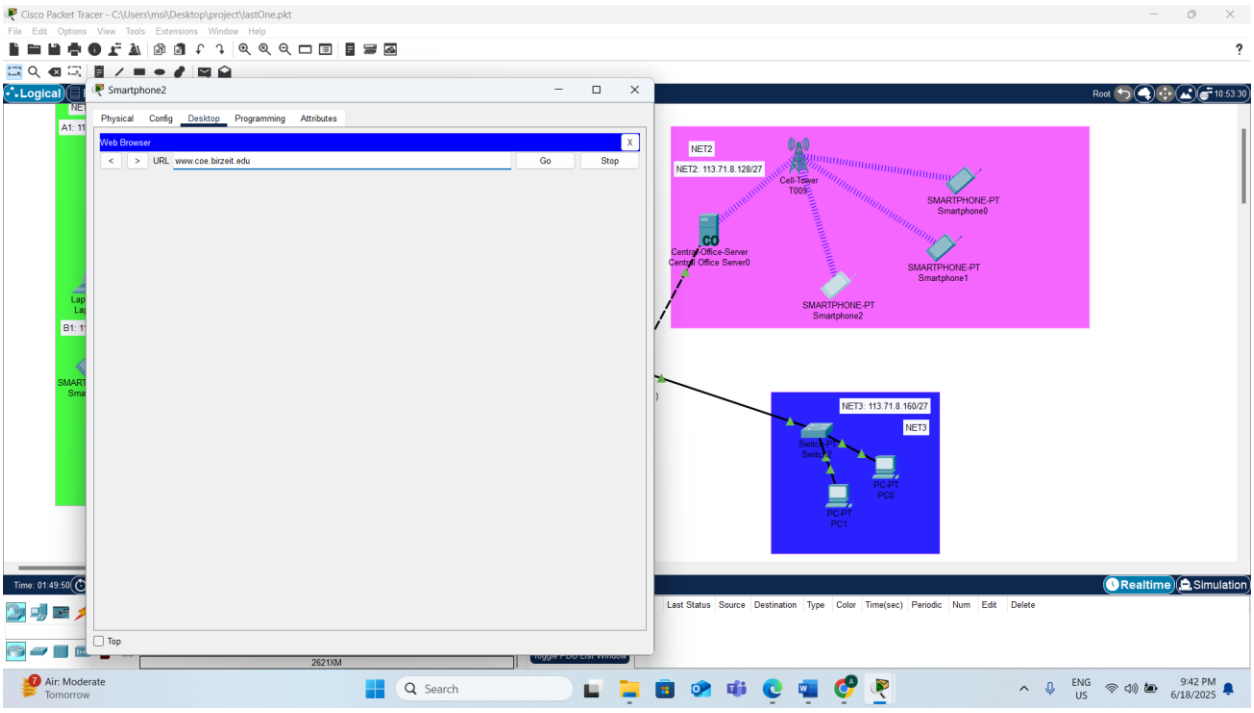


Figure 71:Assigning the web server URL to the smartphone browser

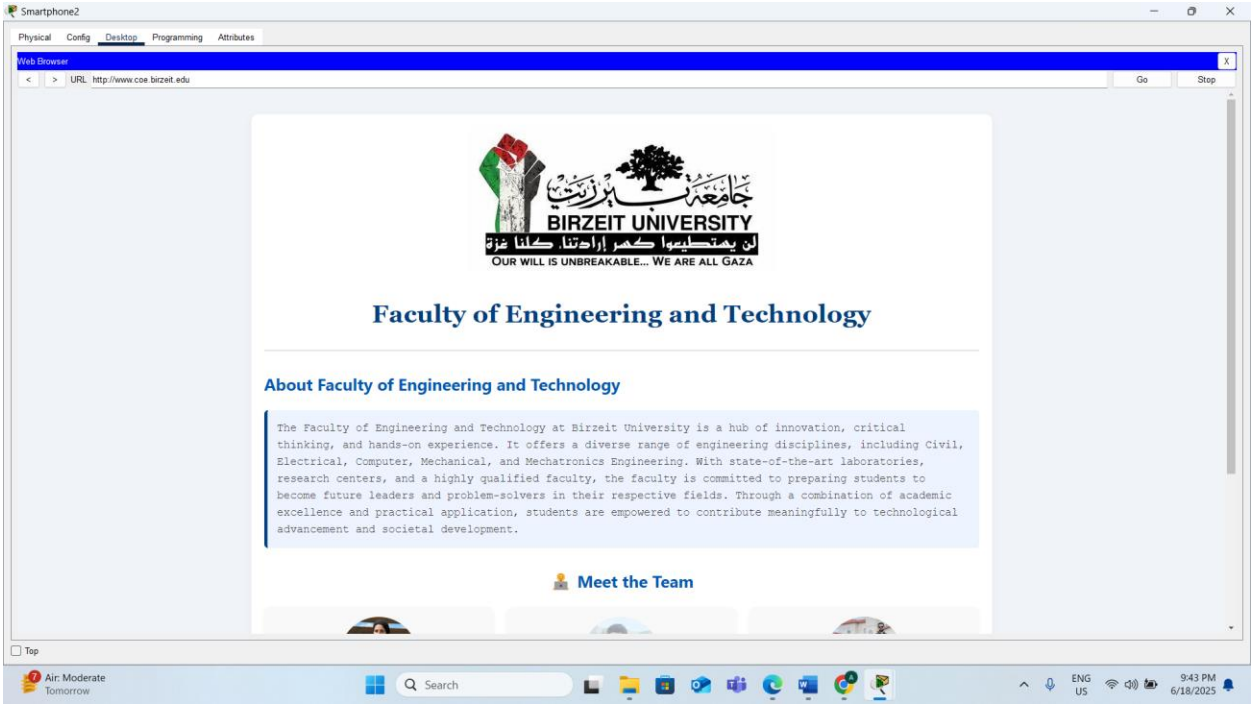


Figure 72:Web page

Figure 73::Web page (cont)

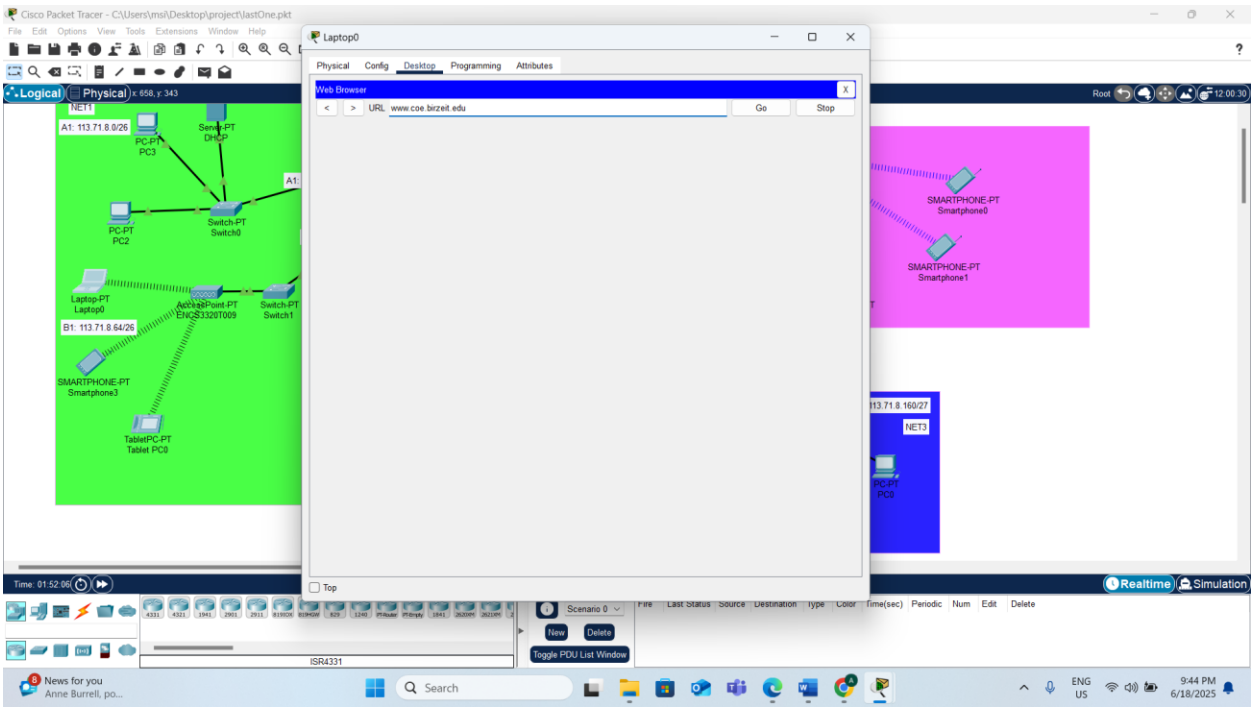


Figure 74:Assigning the web server URL to the laptop browser

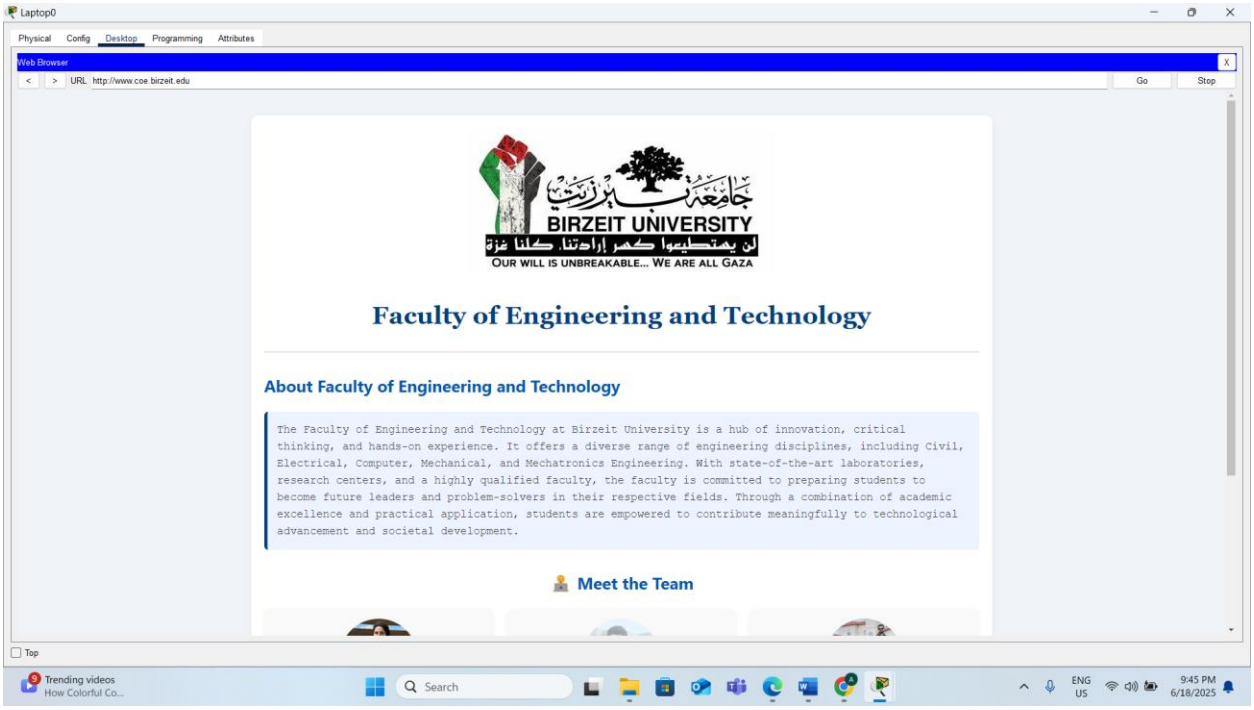


Figure 75::Web page

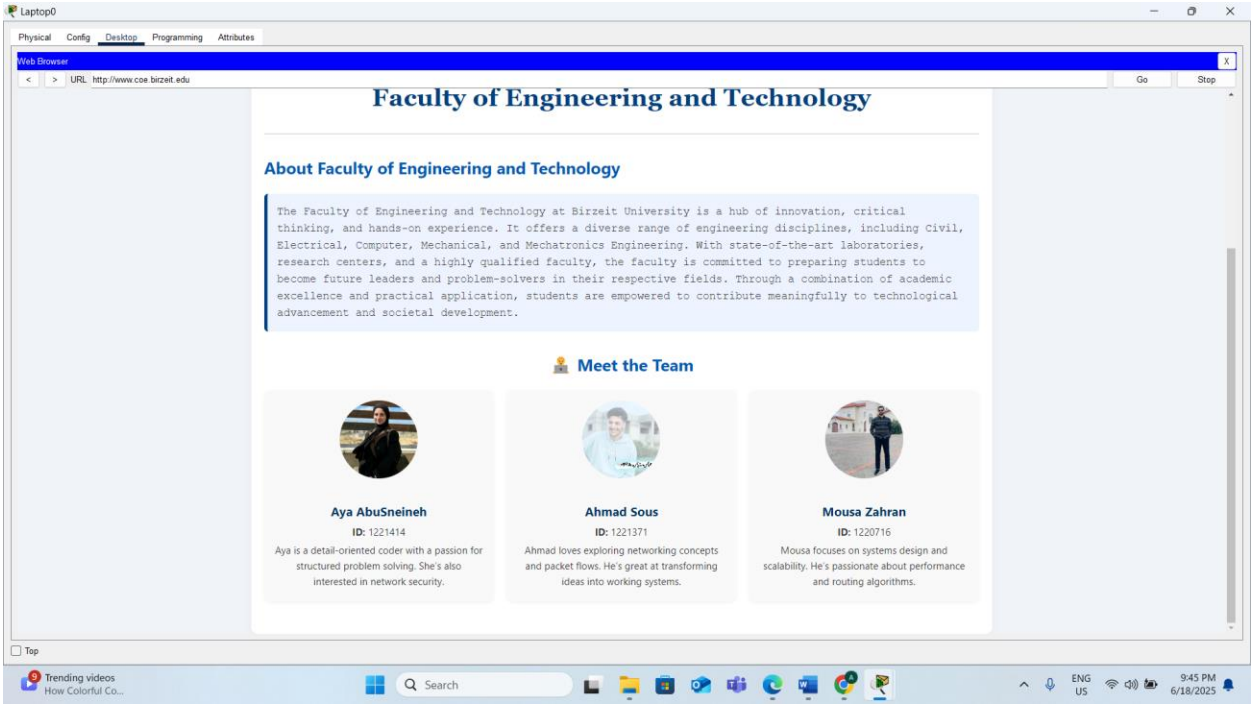


Figure 76:Web page (cont)

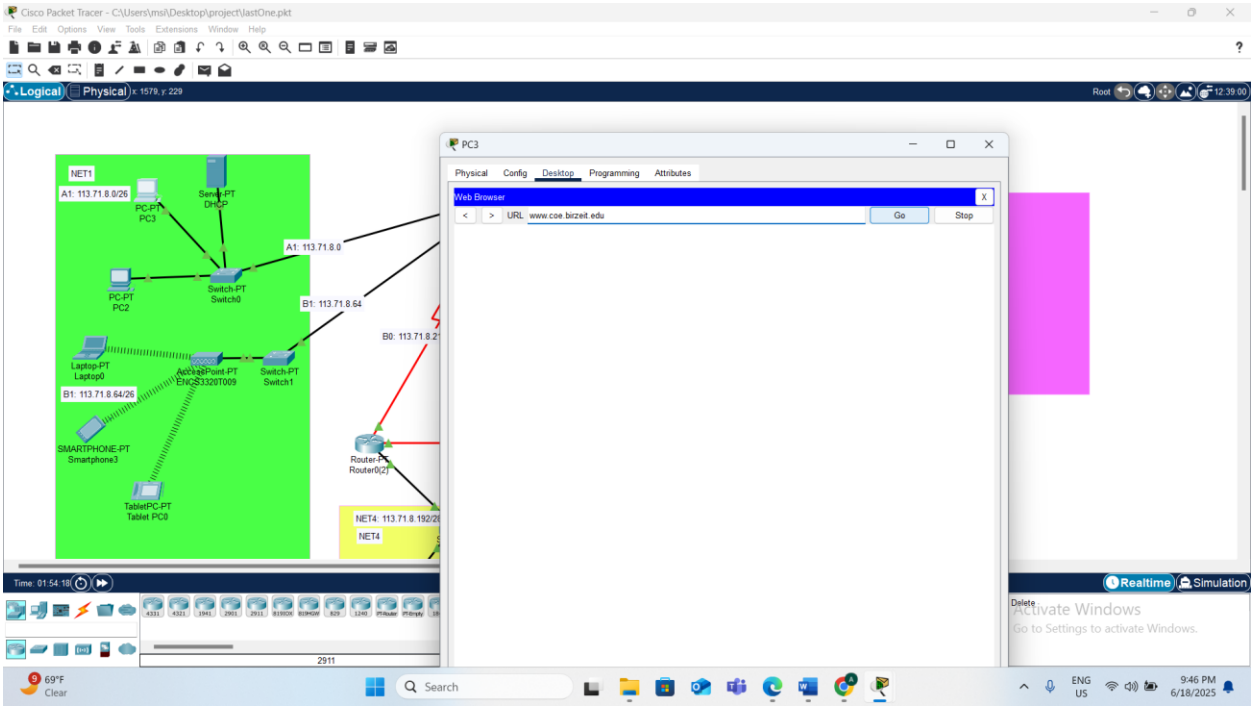


Figure 77:Assigning the web server URL to the PC browser

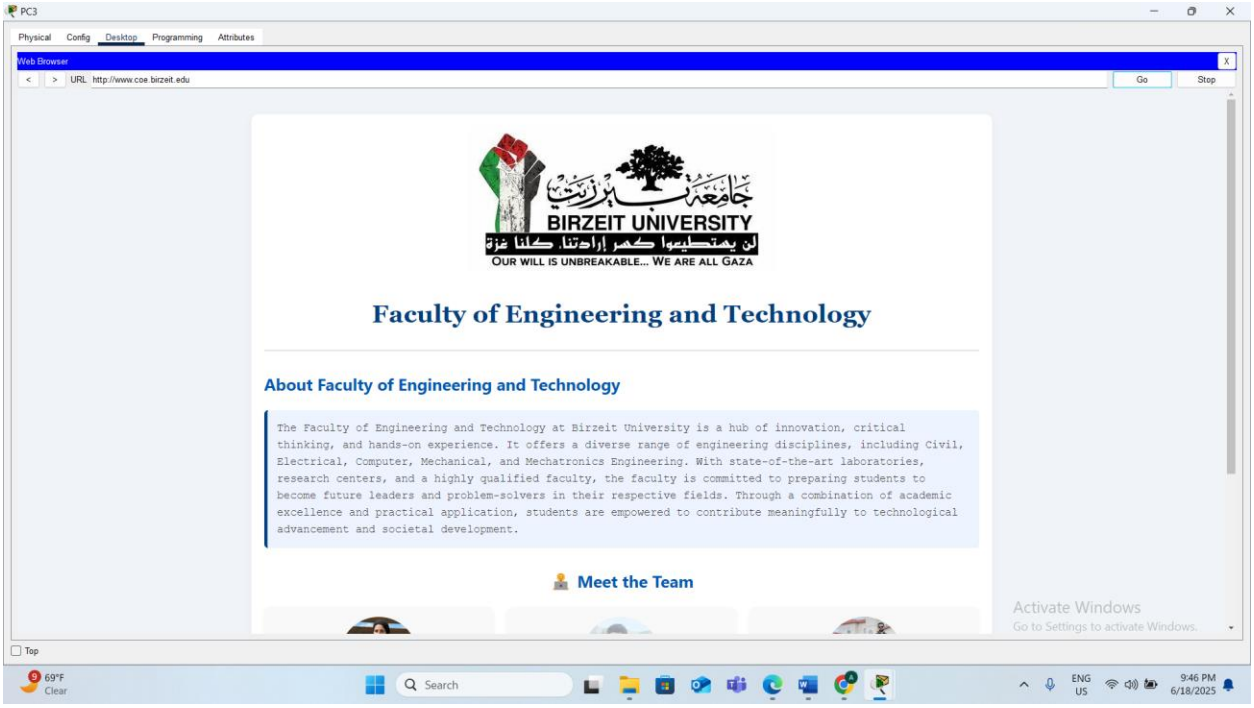


Figure 78:Web page

Figure 79:Web page(cont)

Issues and Limitations

During the development and configuration of the network project in Cisco Packet Tracer, several technical and practical challenges were encountered:

1. **Unidirectional Communication between Router and Central Office Server**
   When sending messages from the router to the Central Office (CO) server, communication failed, while sending from the CO server to the router worked properly. This reflects a limitation in the server response handling in Packet Tracer simulations.
2. **Email Server Configuration Requirements**
   For the mail functionality to work correctly, both the incoming and outgoing mail servers needed to be explicitly set to the IP address of the configured mail server. Without this setting, clients failed to send or receive emails properly.
3. **Web Server Image Hosting Issues**
   Images embedded in the index.html page of the Web Server did not appear at first. It was discovered that Packet Tracer only allows image loading from local directories within the project environment — external URLs (e.g., Google image links) were not accepted. Proper display required placing the images in the same folder as the HTML file.
4. **HTML Rendering Limitations**
   Features such as browser tab titles ("COE-Birzeit") and advanced formatting were not displayed when accessing the page via smartphone browsers in Packet Tracer, due to the limited rendering capabilities of the simulator.
5. **Ambiguity in Instructional Report**
   The provided project report contained some ambiguous sections, making it unclear where to place certain configurations such as the producer settings or specific IP roles. This led to confusion and required extra clarification and adjustments.

Despite these limitations, the final implementation achieved the project goals with fully connected networks and working services across different areas. However, awareness of these challenges is crucial for future improvements or real-world deployment.

Teamwork

This project was completed by three students. Each team member worked on different parts of the network.

- **Ahmad** worked on **AREA 0** and **AREA 4**. He configured the servers (Web, DNS, Email), added the users in the mail server, created the DNS records, and uploaded the HTML file to the web server. He also configured OSPF routing for the routers.
- **Aya** worked on **AREA 1** and assisted in **AREA 2**. She configured the DHCP server, the wireless access point, and all the devices in AREA 1. She also helped edit the HTML file for the website and configured the routers in AREA 4.
- **Mousa** worked on **AREA 2** and assisted in **AREA 4**. He configured the routers and devices in this area and helped with testing the network and verifying routing.

All team members communicated and collaborated throughout the project. Everyone completed their part and shared ideas to finish the work on time. In addition, they worked together on the report: **Aya** handled the theory and configuration sections, **Ahmad** conducted the testing, and **Mousa** performed the subnetting.

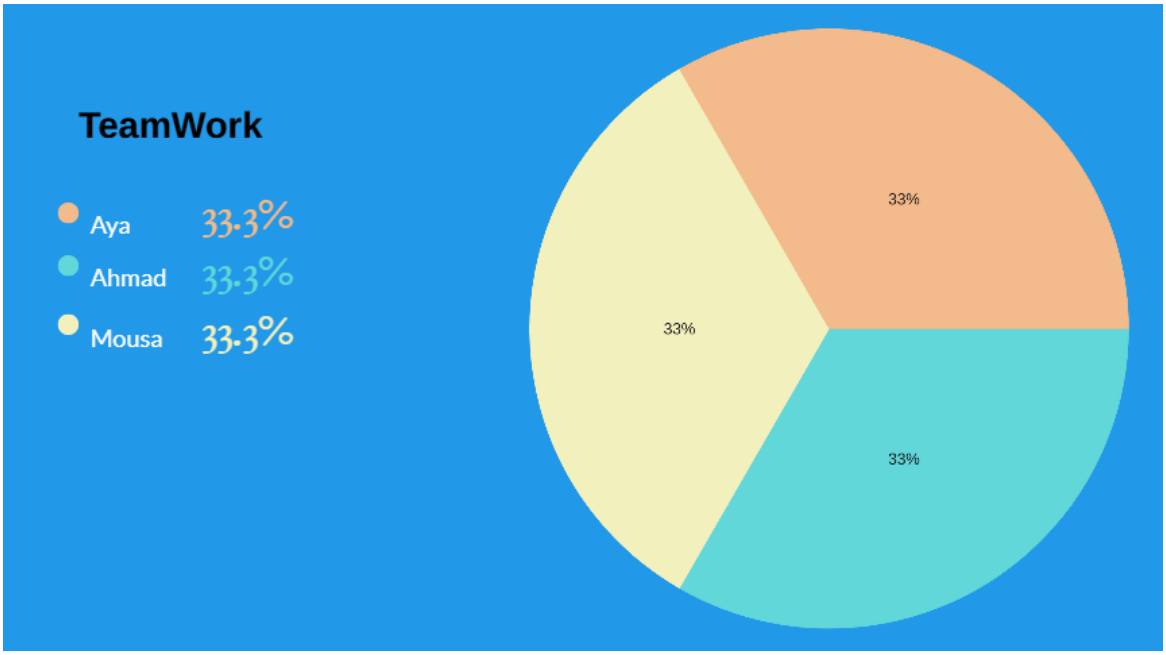


Figure 80:Teamwork

References

[1] : https://www.akamai.com/glossary/what-is-dhcp

[2] : https://info.teledynamics.com/blog/dhcp-options-for-voip-and-uc-systems

[3] : https://www.geeksforgeeks.org/node-js/web-server-and-its-type/

[4] : https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/Overview

[5] : https://www.geeksforgeeks.org/computer-networks/difference-between-http-and-https/

[6] : https://www.one.com/en/email/what-is-an-email-server

[7] : https://www.geeksforgeeks.org/computer-networks/difference-between-smtp-and-pop3/

[8] : https://postmansmtp.com/imap-vs-pop3-vs-smtp/

[9] : https://www.fortinet.com/resources/cyberglossary/what-is-dns

[10] : https://www.geeksforgeeks.org/computer-networks/difference-between-dns-and-dhcp/

[11] : https://www.geeksforgeeks.org/computer-networks/open-shortest-path-first-ospf-router-roles-configuration/