BIRZEIT UNIVERSITY

Department of Electrical and Computer Engineering

ENCS3320- COMPUTER NETWORKS

Second Semester – 2025/2026

Project #2 Report (Cisco Packet Tracer)

Prepared by:

Name: Ansam Hamayel	**ID:** 1220463	**Section:** 3
Name: Taima Nazal	**ID:** 1220701	**Section:** 3
Name: Mays Al-Reem Hroub	**ID:** 1220081	**Section:** 4

Submission Date: 19/6/2025

List of figures

List of tables

Abstract

In this project, we designed and implemented a full network system. The network includes five main areas: the core, university, street, home, and datacenter. Each area was configured with the appropriate devices, addressing, and services based on a given topology.
We started by calculating the subnetting based on the last four digits of student Taima's ID, then assigned IP addresses to each subnetwork according to the number of required hosts. OSPF routing was configured to connect all areas. We also set up a DHCP server for dynamic IP assignment, and configured DNS, web, and mail servers in the datacenter to simulate real-life services.
The project helped us apply what we learned in class in a practical way. We faced several configuration challenges during implementation, especially when dealing with wireless settings and email delivery, but we were able to troubleshoot and fix them. By the end of the project, the network was working correctly, with all devices able to communicate and access the necessary services.

Theory and Procedure

This project focuses on designing and executing a structured multi-segment network that simulates various real-world scenarios, such as university, street, home, and datacenter environments. The aim is to interconnect these segments through routers, switches, and suitable IP subnetting, while enabling end-to-end communication throughout the entire topology.The implementation relies on structured subnetting, dynamic routing, and network services deployment using Cisco Packet Tracer.

Each subnet was designed based on the number of hosts needed in each segment. The address space was efficiently divided into multiple subnets such as NET0 for router-to-router connections, NET1 for university users, NET2 for street-level users, NET3 for home users, and NET4 for datacenter services.

Subnetting table was used to efficiently divide the given IP addresses that configure the routers. To enable communication between the different subnets, the dynamic routing protocol OSPF (Open Shortest Path First) was implemented using Area 0 across all three routers.

In terms of services, a DNS server was configured to resolve hostnames for various servers in the network (such as mail and web servers). A DHCP server was set up to automatically assign IP addresses to university clients, simplifying device management and configuration. The mail server was configured with SMTP and POP3 services and populated with email accounts for team members from different subnets.Wireless connectivity was implemented using an Access Point and a Cell Tower to connect wireless devices such as smartphones and tablets.

The network was simulated using Cisco Packet Tracer, where all connections were tested, name resolution, DHCP address assignment, and email exchange. Devices such as smartphones, PCs, laptops, and wireless access points were configured and integrated into the corresponding subnetworks, including the use of wireless authentication and cell tower simulation for mobile connectivity.

Here is the explanation of some concepts that are used for implementing the project requirements:

❖ OSPF (Open Shortest Path First)

OSPF is a dynamic routing protocol that facilitates the sharing of routing information between routers. It uses link-state information to build a complete map of the network topology. In this project, OSPF was implemented in Area 0 to enable automatic route learning and fast convergence between routers in the core.

Open Shortest Path First (OSPF) is a dynamic link-state routing protocol and one of the Interior Gateway Protocols (IGPs) used within a single Autonomous System (AS). It enables routers to exchange topology information and build a complete and synchronized map of the network. Each OSPF router uses Link State Advertisements (LSAs) to share information about its directly connected neighbors and interface costs. All routers then use this information to construct an identical database and apply Dijkstra's algorithm to calculate the shortest path tree, which is used to populate their routing tables.The primary advantage of OSPF is its ability to quickly adapt to network changes and ensure fast convergence by recalculating optimal routes automatically. It also supports hierarchical routing using areas, which reduces routing overhead and improves scalability.

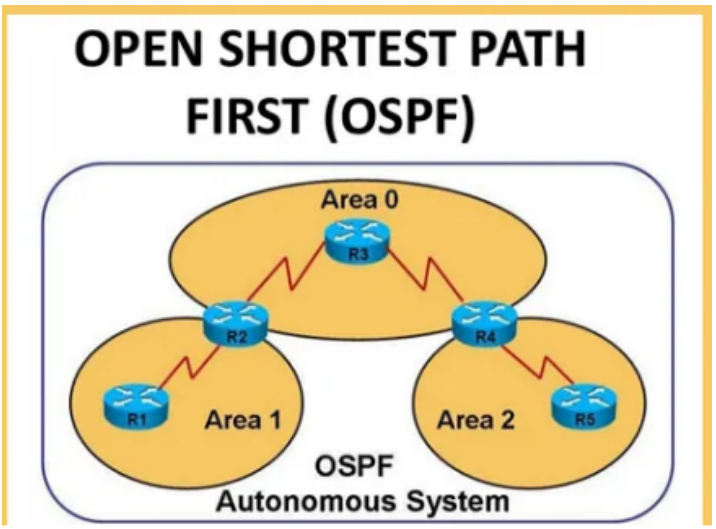

figure 1. Open Shortest Path First

❖ DHCP (Dynamic Host Configuration Protocol)

The Dynamic Host Configuration Protocol (DHCP) is used in our network to automatically assign IP addresses to end devices, such as PCs, laptops, tablets, and smartphones. Instead of configuring IP settings manually on each device, the DHCP server dynamically provides IP addresses, subnet masks, default gateways, and DNS information. This ensures easier management, avoids IP conflicts, and saves time during network deployment.

In this project, the DHCP server was implemented in the university subnet (NET1-A) to simplify the configuration of devices and to centralize IP address management across multiple subnets using appropriate DHCP pools.

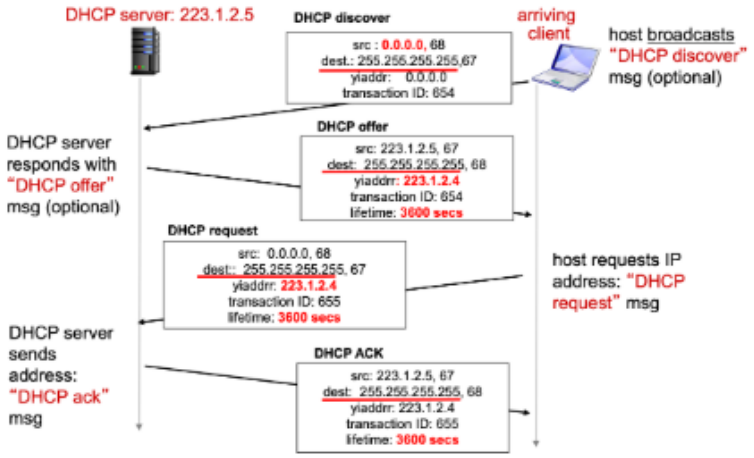

figure 2. Dynamic Host Configuration Protocol

❖ DNS (Domain Name System)

DNS is a hierarchical and distributed naming system that allows users to access services using user-friendly domain names instead of numeric IP addresses. It operates through a sequence of queries involving a local resolver, root DNS servers, top-level domain (TLD) servers, and authoritative DNS servers. This process ensures efficient and accurate name resolution across the network. Without DNS, users would have to manually remember the IP addresses of every resource, which is highly impractical.

DNS translates domain names such as (www.coe.birzeit.edu) into IP addresses. A DNS server was installed in the datacenter to translate hostnames for internal services such as the mail and web servers.

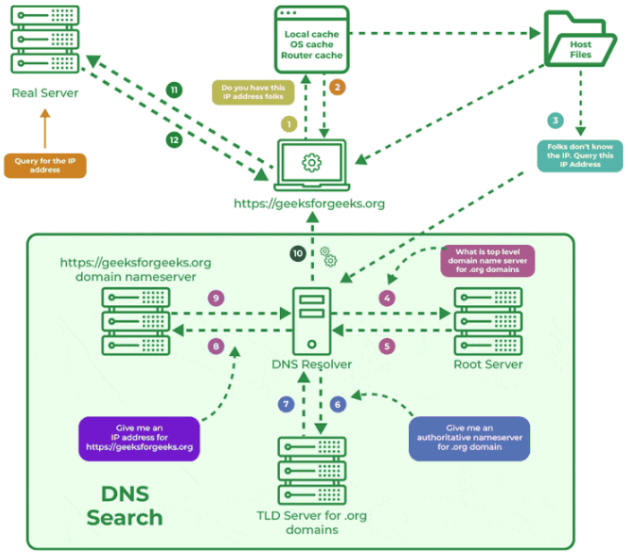

figure 3. Domain Name System

❖ SMTP and POP3

SMTP and POP3 are two core protocols used in email communication.

SMTP (Simple Mail Transfer Protocol) is used to send emails, whereas POP3 (Post Office Protocol v3) is used to receive them. In the project, the mail server employed both protocols to enable message transfer between users in different subnets.

SMTP operates by having the SMTP client communicate with the SMTP server in three stages: the handshake (connection setup), the email transfer phase, and termination. POP3, on the other hand, works by downloading emails from the server to the client, allowing offline access and freeing up server storage.

figure 4. SMTP and POP3

❖ Access Point (AP)

An Access Point enables wireless connection for end devices. In the university network (NET1-B), an AP was deployed and secured with WPA2 encryption, allowing devices such as smartphones and tablets to connect wirelessly.

In general, wireless access points can operate in various modes depending on the deployment scenario. These include Local Mode, Bridge (or Mesh) Mode, FlexConnect Mode, Client Mode, and others. For example, in Local Mode, APs forward traffic through a CAPWAP tunnel to the wireless controller, while in Bridge Mode, APs extend wireless connectivity between remote networks. Additionally, monitor and sniffer modes allow APs to support tasks such as intrusion detection and wireless troubleshooting.

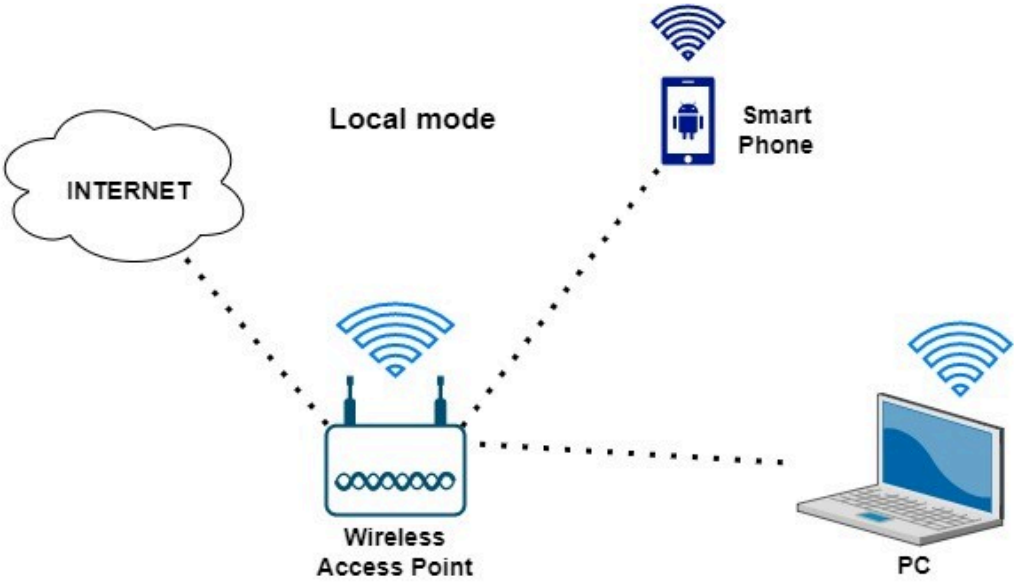

figure 5. Access Point (AP)

❖ Cell Tower Simulation

A cell tower was employed in the street network (NET2) to simulate street-level wireless communication, and configured with a provider name. Smartphones were connected wirelessly to this tower to reflect mobile connectivity.

In real-world cellular systems, each device communicates with nearby towers using a unique identifier called the **IMSI** (International Mobile Subscriber Identity). While this allows the network to authenticate and provide service to the user, it also exposes a potential security risk. Attackers can exploit this connection using rogue base stations—commonly known as **IMSI catchers** or **fake cell towers**—to intercept sensitive data, track devices, or launch denial-of-service (DoS) attacks without detection.

These threats highlight the importance of secure configurations and awareness when simulating or deploying mobile networks in practice.

figure 6. Cell Tower Simulation

Results and Discussions

Task 1: IP Subnetting

To meet the device requirements of each area in the specified topology, we split the primary IP network, 170.1.8.0/23, into a number of subnetworks for this task. While providing flexibility for future growth, the design guarantees effective use of IP addresses. Using powers of two (i.e., 2^n ≥ # of hosts + 2) and CIDR notation, we implemented the rule of using the smallest subnet mask that can support the number of required hosts.

Subnetwork	Hosts Needed	CIDR	Subnet Mask	Network Address	Broadcast Address	Usable IP Range
NET1-A	60	/26	255.255.255.192	170.1.8.0	170.1.8.63	170.1.8.1 – 170.1.8.62
NET1-B	60	/26	255.255.255.192	170.1.8.64	170.1.8.127	170.1.8.65 – 170.1.8.126
NET2	30	/27	255.255.255.224	170.1.8.128	170.1.8.159	170.1.8.129 – 170.1.8.158
NET3	20	/27	255.255.255.224	170.1.8.160	170.1.8.191	170.1.8.161 – 170.1.8.190
NET4	15	/27	255.255.255.224	170.1.8.192	170.1.8.223	170.1.8.193 – 170.1.8.222
NET0-A	2	/30	255.255.255.252	170.1.8.224	170.1.8.227	170.1.8.225 – 170.1.8.226
NET0-B	2	/30	255.255.255.252	170.1.8.228	170.1.8.231	170.1.8.229 – 170.1.8.230
NET0-C	2	/30	255.255.255.252	170.1.8.232	170.1.8.235	170.1.8.233 – 170.1.8.234

table 1. Subnetting table

The base network 170.1.8.0/23, which offers 512 IP addresses in total, was used to compute the subnetting. To prevent fragmentation, subnets were assigned in descending order of host count. Taking into account both host and infrastructure IPs (such as routers), each subnetwork has enough IPs to support all necessary devices. A pool of unused addresses (ranging from

170.1.8.220 to 170.1.9.255) is still available for future expansion. All project requirements, such as support for DHCP, static IPs, and server configurations, are met by this allocation.

Important Notes

During the initial phase of the project, an error occurred in identifying the correct student ID when generating the base IP address for Task 1. Instead of using the correct student ID **1220701**, which would result in a base IP of **107.1.8.0/23**, the subnetting and subsequent configurations were mistakenly carried out (switching between 7 and 0) using the address **170.1.8.0/23**.However, by the time the mistake was noticed, the entire network design — including IP addressing, Packet Tracer topology, server configuration, and routing — had already been implemented and verified based on the incorrect IP address.As modifying the IP scheme at this stage would require rebuilding the entire project from scratch, we respectfully request that the work be evaluated as-is, considering the effort, correctness of logic, and completeness of the design.We acknowledge the importance of accuracy and take full responsibility for the mistake. This note is provided to clarify the reason for the discrepancy between the student ID and the IP address used in the project.

Task 2: Building Topology

We have built the following topology using Cisco Packet Tracer Program. This diagram shows the interconnection of all areas (Area 0–4) with routers and proper subnetting based on the project requirements

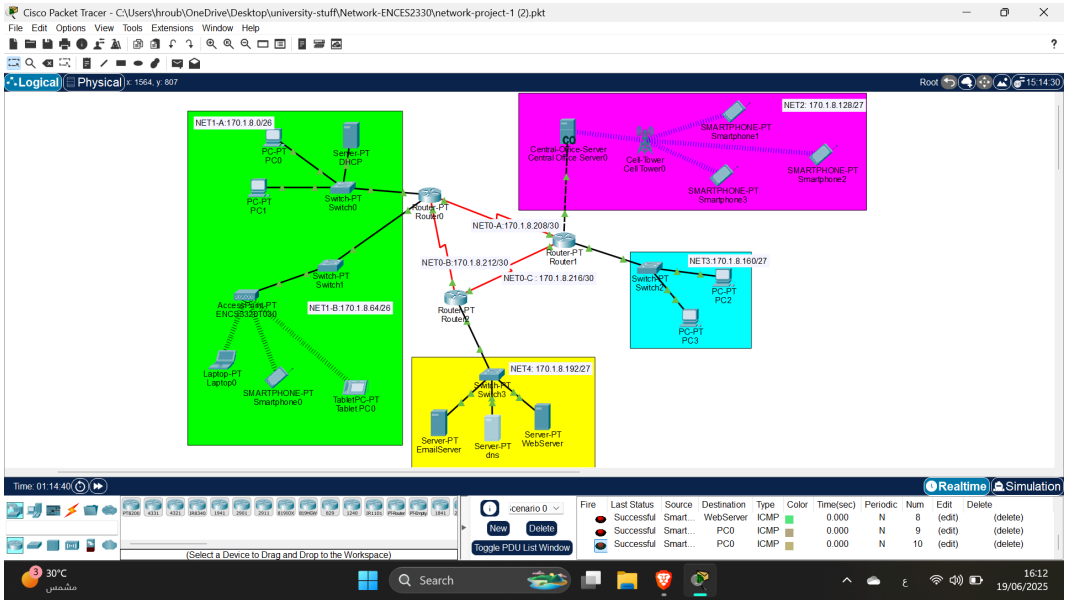

figure 7. network topology

Static IP configurations for routers

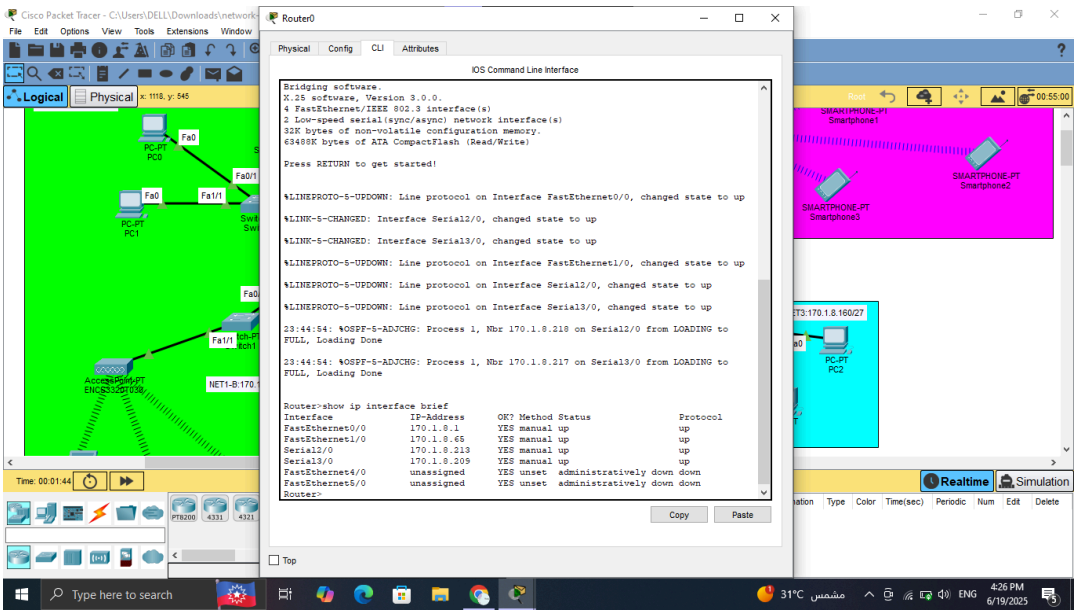

figure 8. IP configuration for router 0

The above figure shows the static IP configuration for Router 0. Assigning IP addresses to interfaces is essential for routing and ensures proper communication across networks.

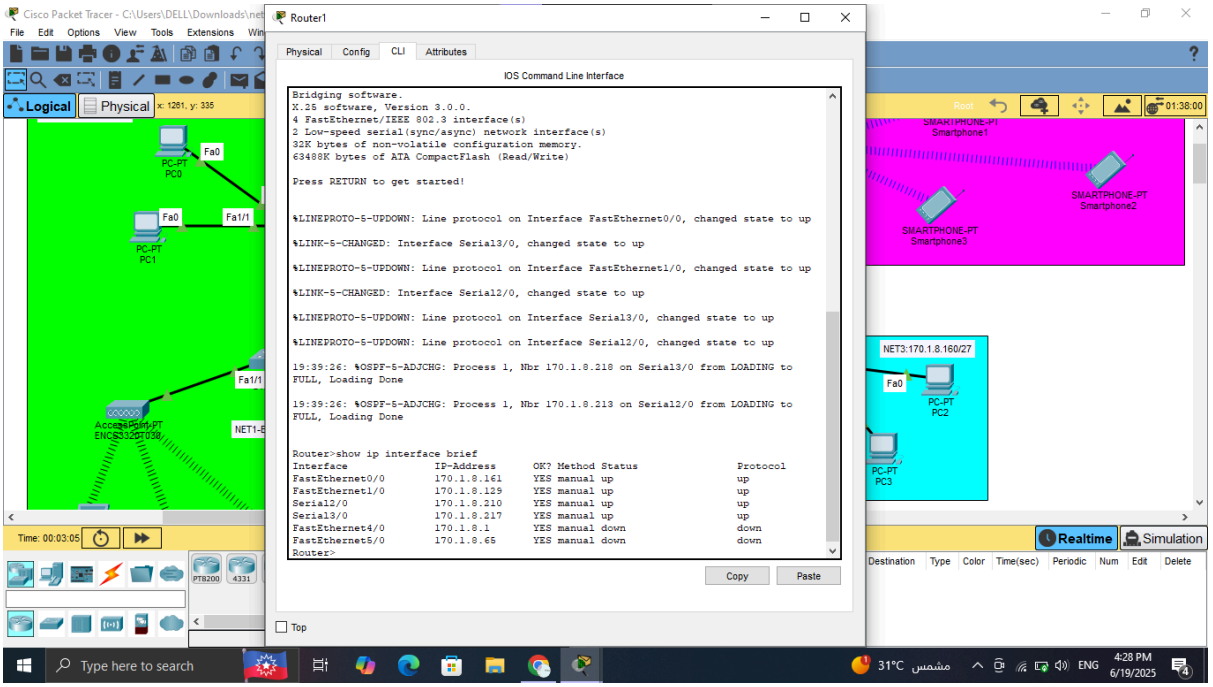

figure 9. IP configuration for router 1

Static IP addresses were set on Router 1 to connect the university networks with the core network. This is necessary for enabling OSPF routing and connectivity.

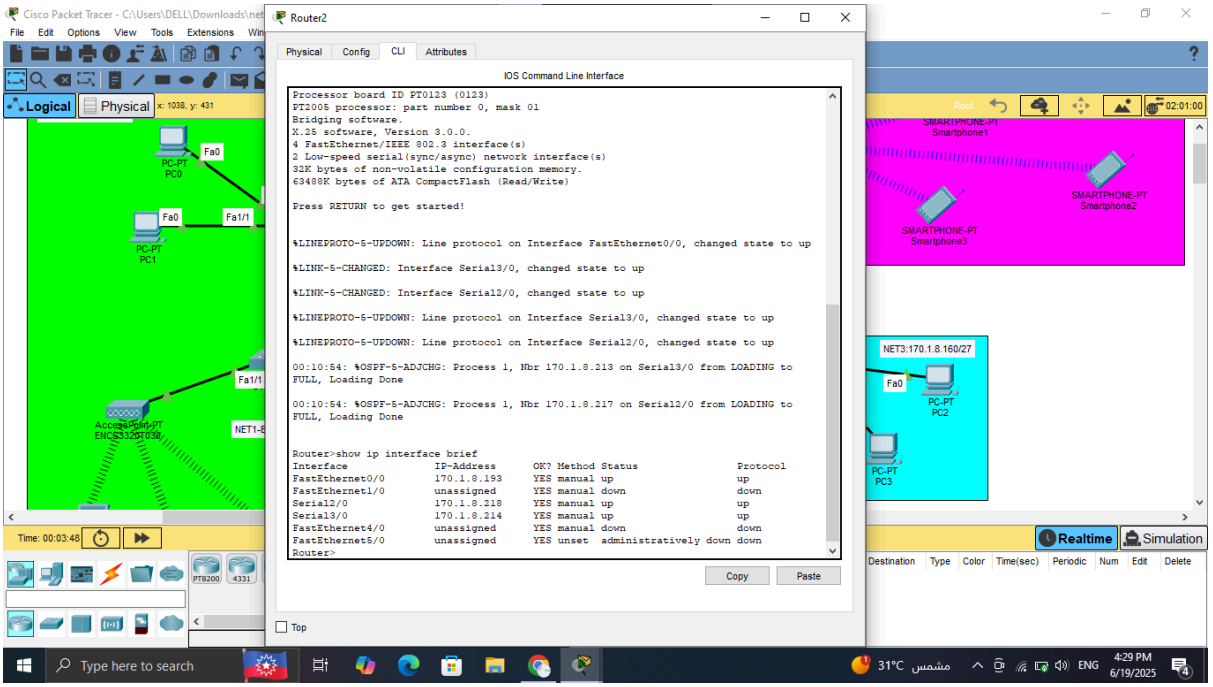

figure 10. IP configuration router 2

Router 2 connects the home, street, and datacenter networks. Static IPs were set correctly to enable full routing functionality in the network.

Dynamic IP configuration for the assigned end device

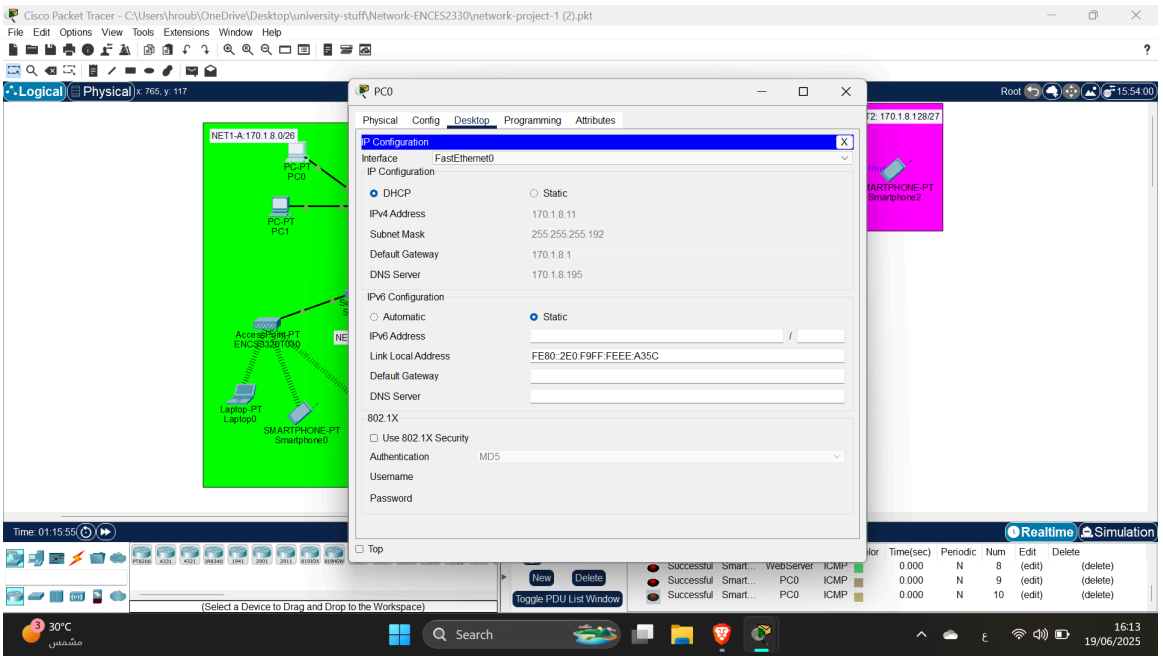

figure 11. IP config for PC0

PC0 received its IP address dynamically from the DHCP server. This shows that the DHCP service is working properly in the university network.

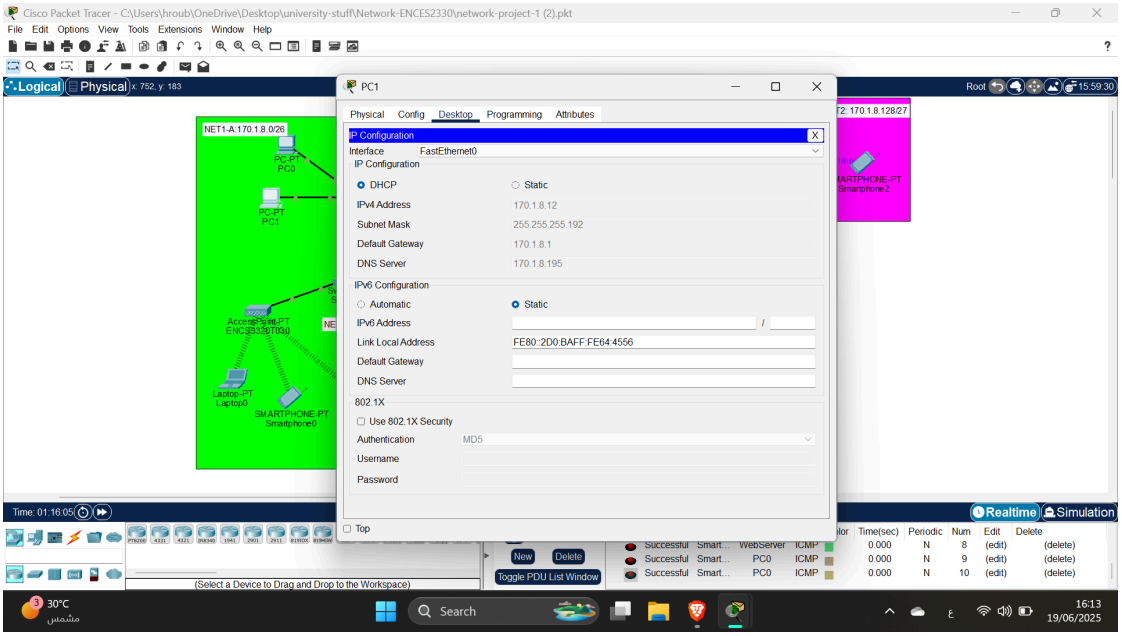

figure 12. IP config for PC1

PC1 also obtained its IP through DHCP successfully, confirming that the DHCP configuration is correct and serving multiple clients.

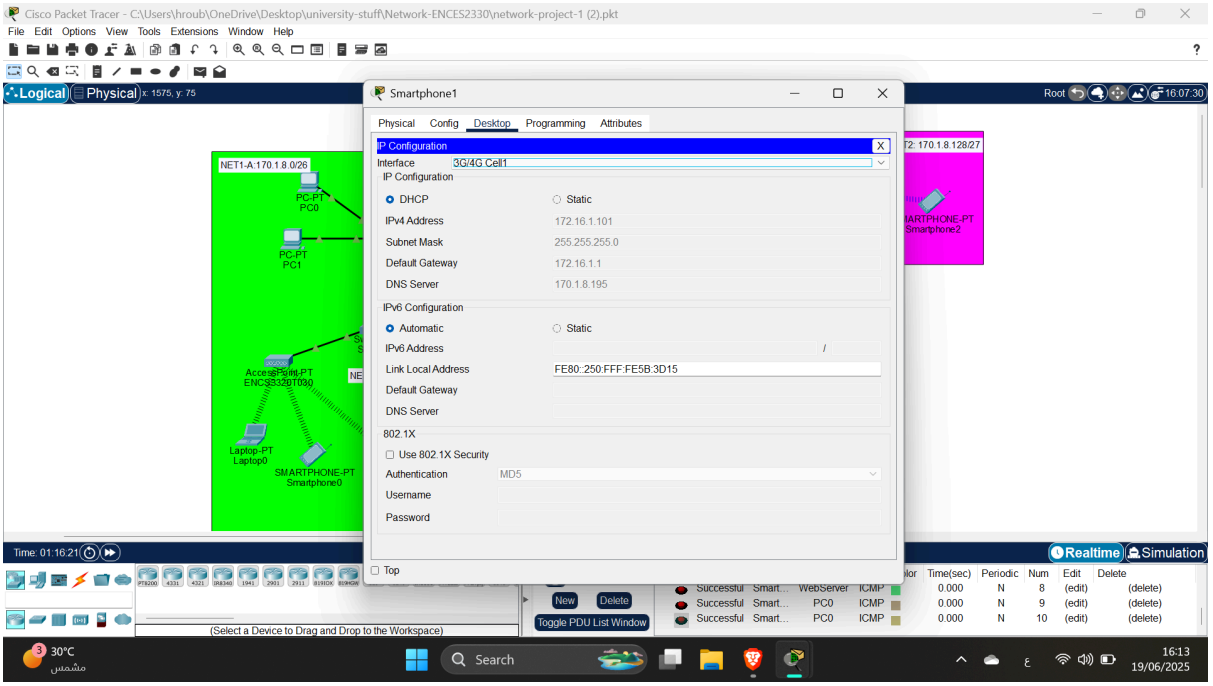

figure 13. IP config for SMARTPHONE1

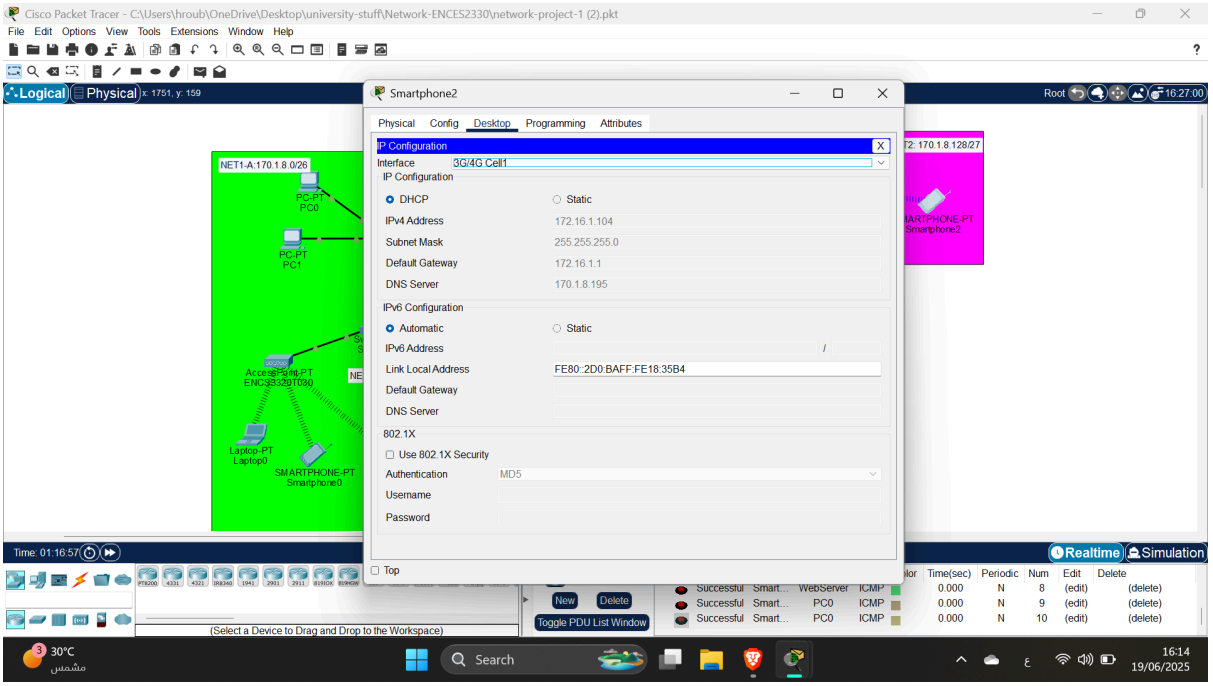

figure 14. IP config for SMARTPHONE2

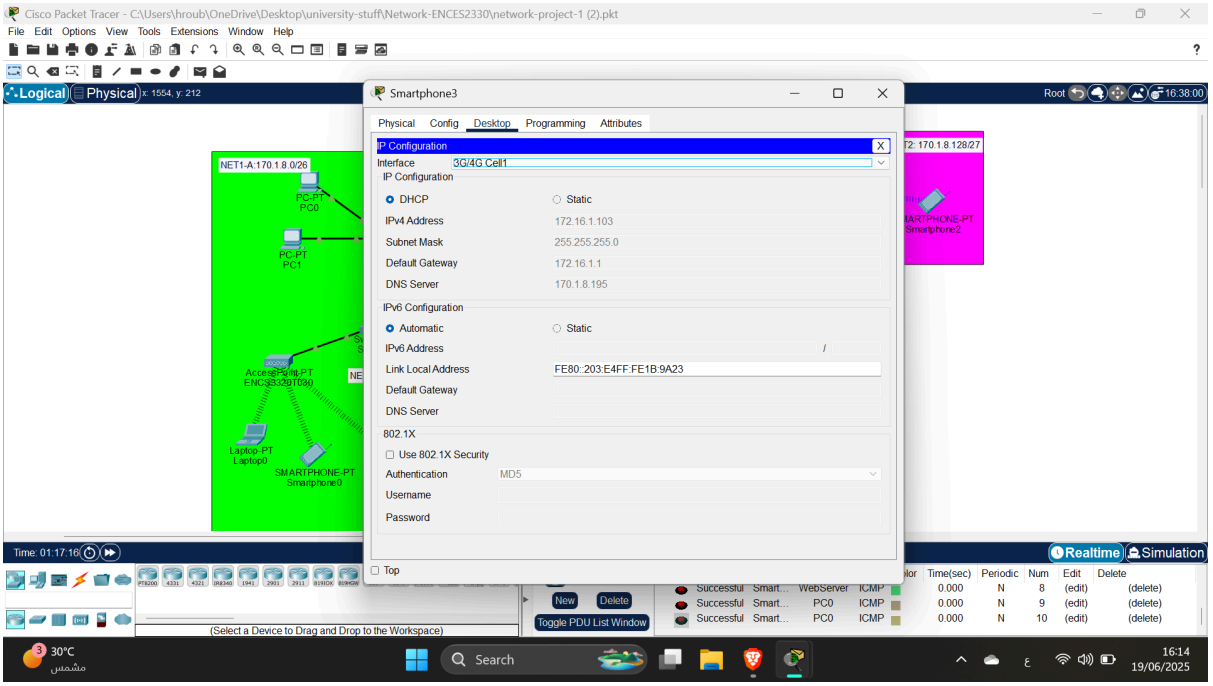

figure 15. IP config for SMARTPHONE3

The 3 Figures (13-15): All smartphones received IP addresses via wireless connections (Access Point or Cell Tower), which confirms proper wireless network configuration.

Static IP configuration for the assigned end devices

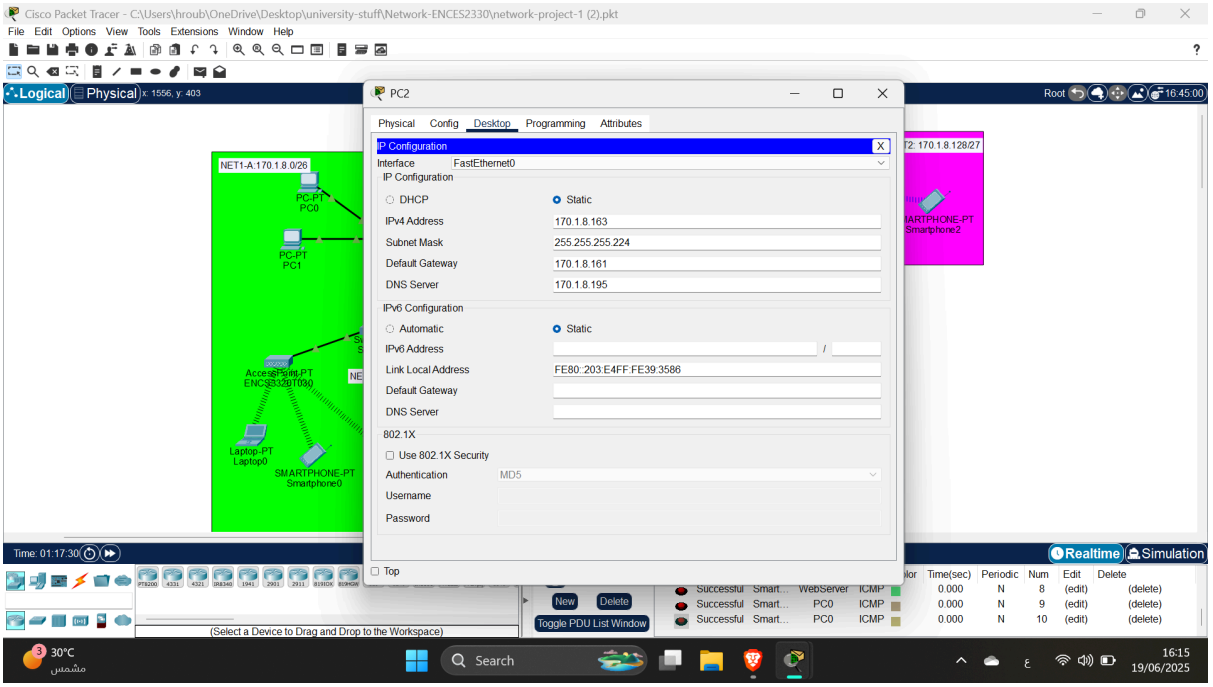

figure 16. IP config for PC2

A static IP address was assigned to PC2 in the home network. This setup helps ensure direct communication with servers and other devices.

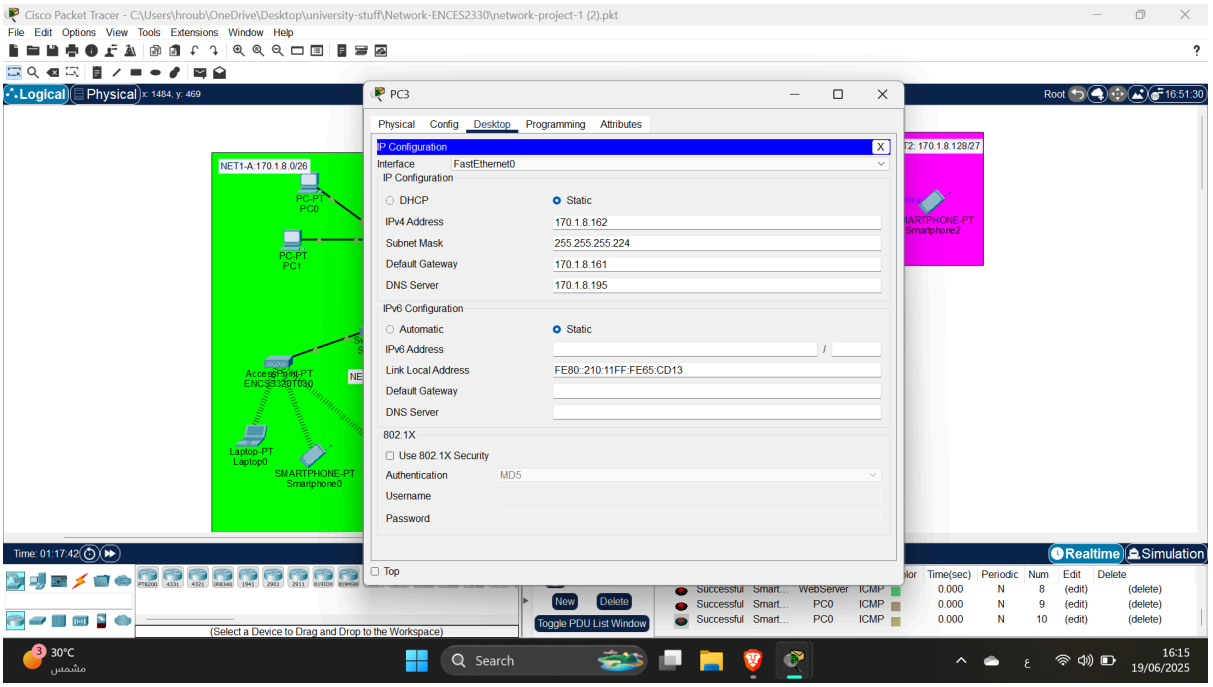

figure 17. IP config for PC3

PC3 also has a static IP in the same home network, allowing for internal and external connectivity testing.

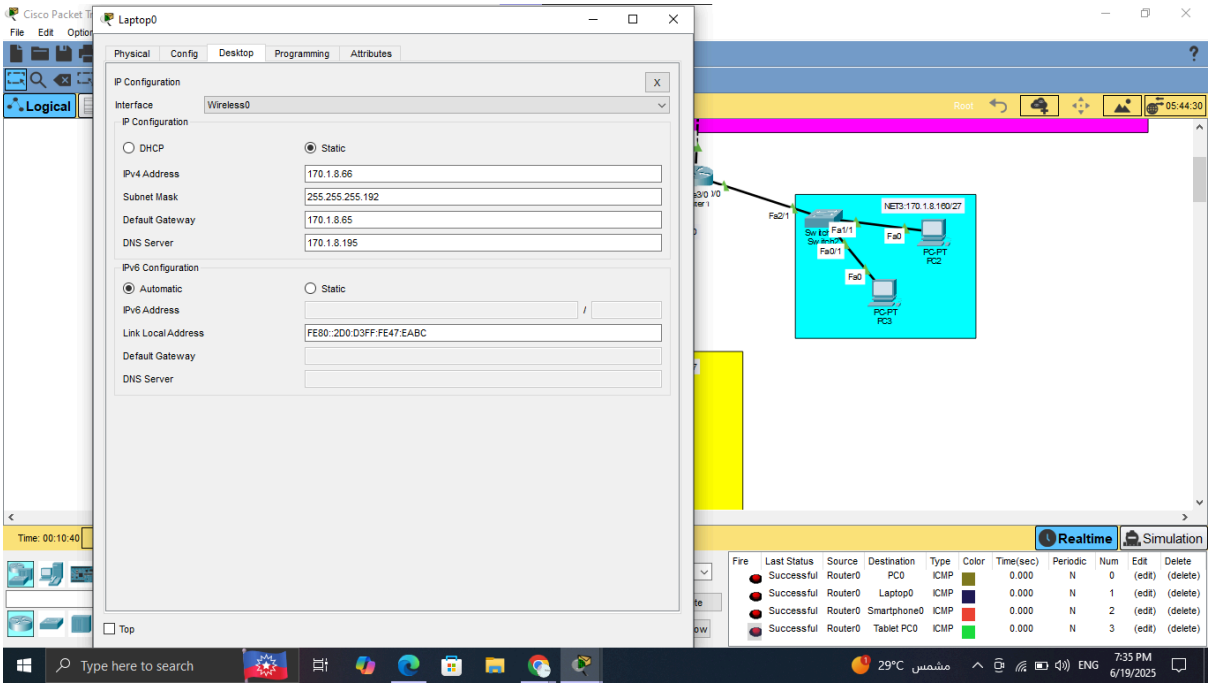

figure 18. IP config for Laptop 0

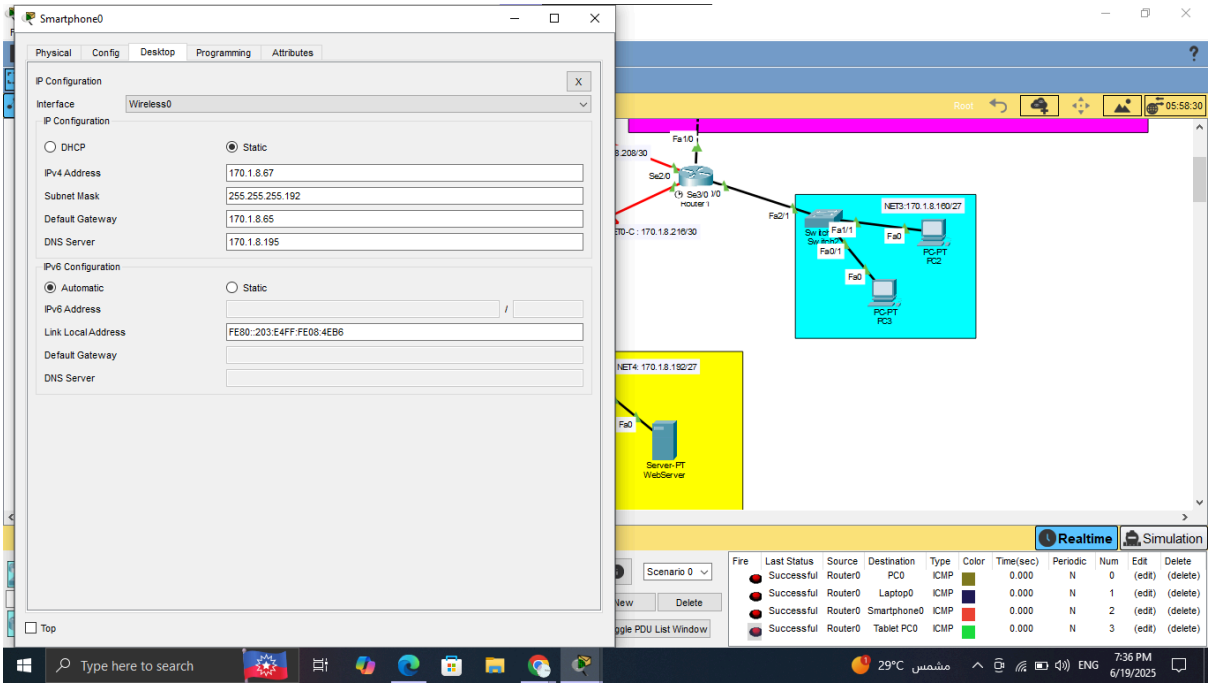

figure 19. IP config for Smartphone 0

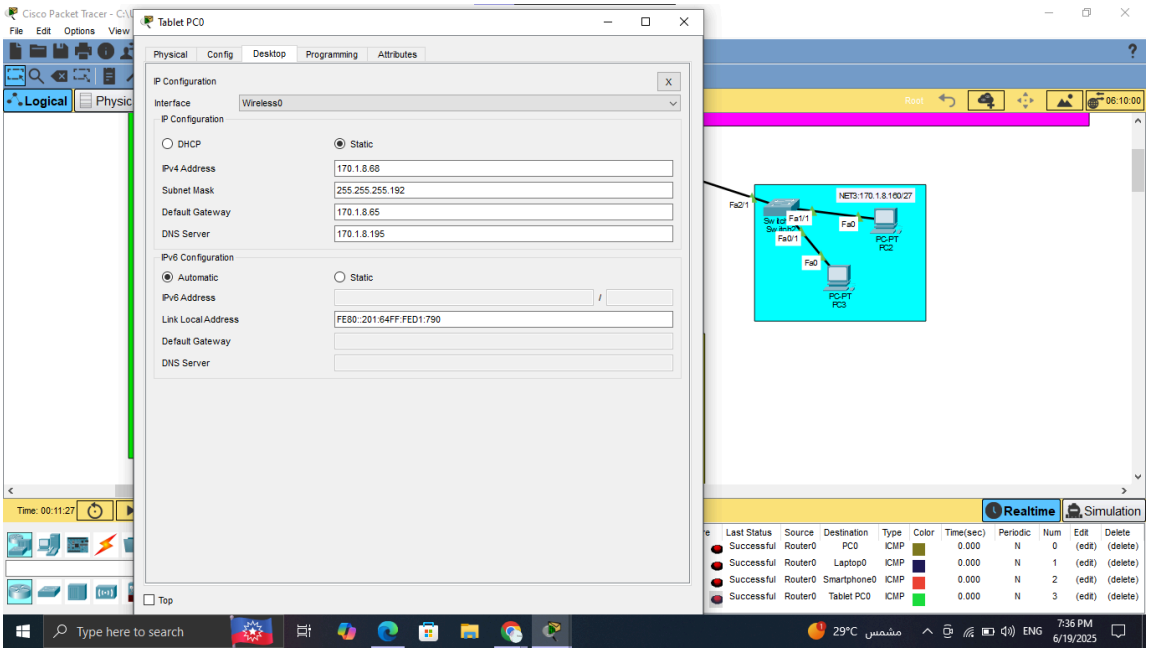

figure 20. IP config for Tablet

The tablet was manually configured with a static IP address due to DHCP assignment issues during testing. Although the project requires dynamic IP through the access point, the static configuration was temporarily applied to ensure the device could connect and communicate within the network. Connectivity was successfully verified using this setup.

Access point configuration

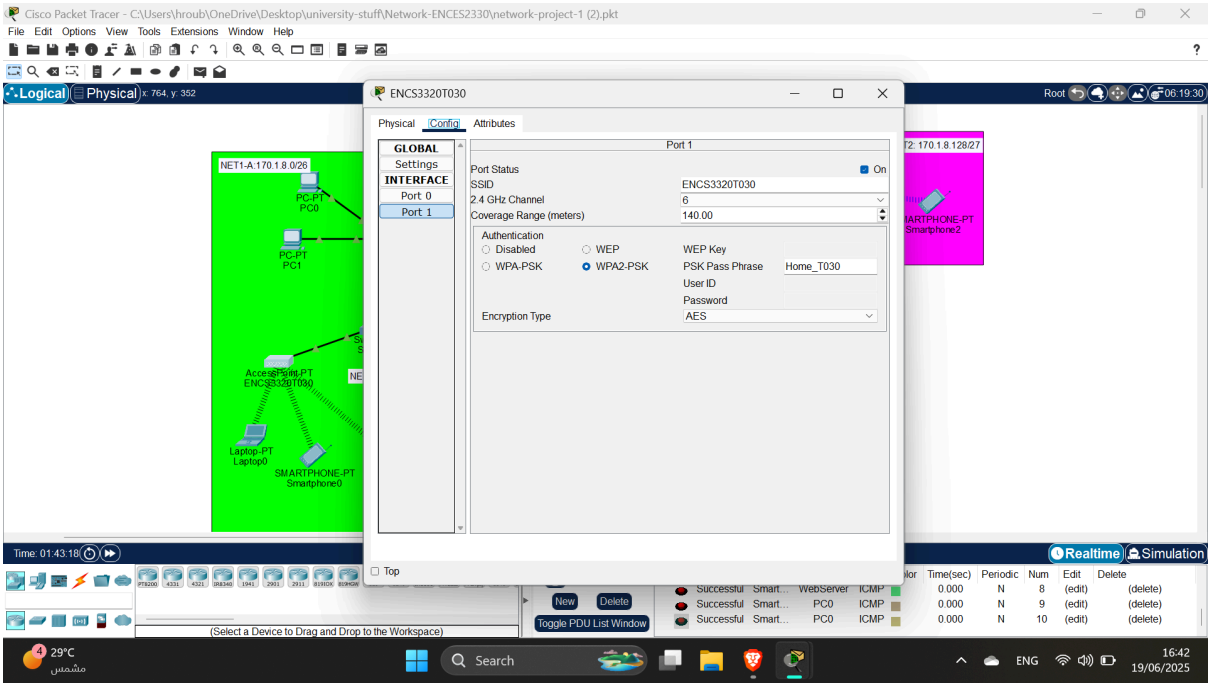

figure 21. IP config for AP

The access point was configured with WPA2 security and a custom SSID. This enables secure wireless access for end devices like the tablet and smartphone.

Successful Ping and tracert results between end devices

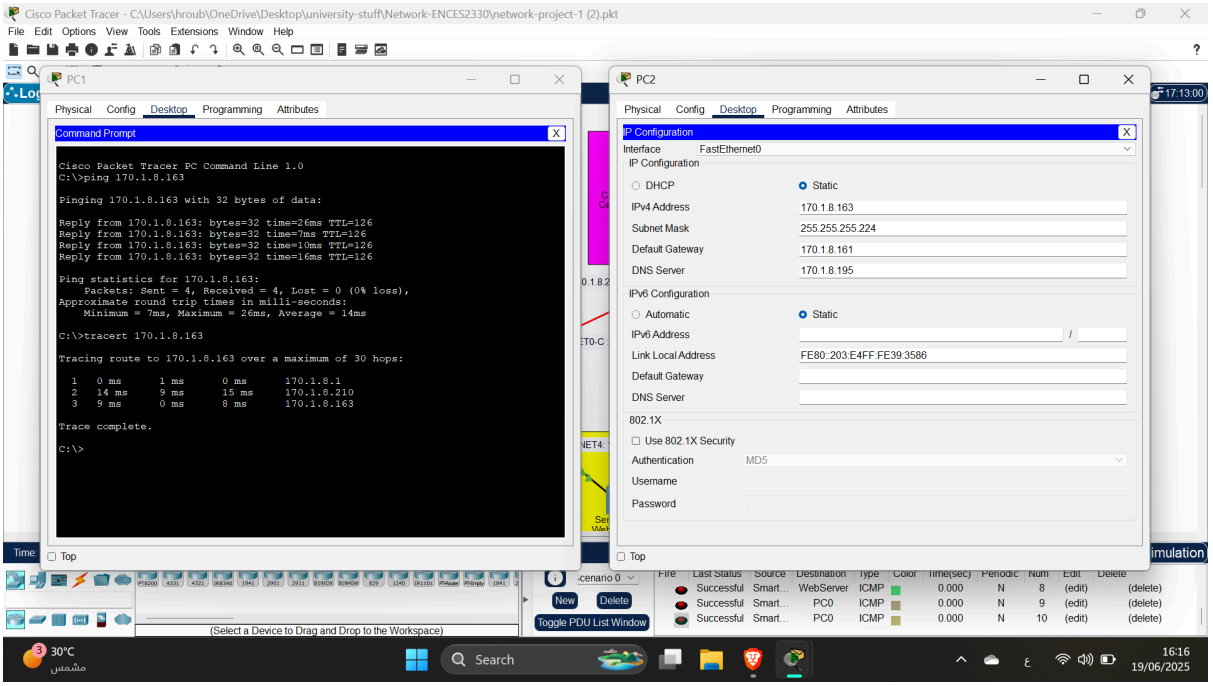

figure 22. successful ping and tracert between two end devices

The ping and tracert between PC1 and PC2 were successful, proving that the routing (OSPF) is working correctly and devices across networks can communicate.

IP configuration of Web, Email, DNS, and DHCP servers

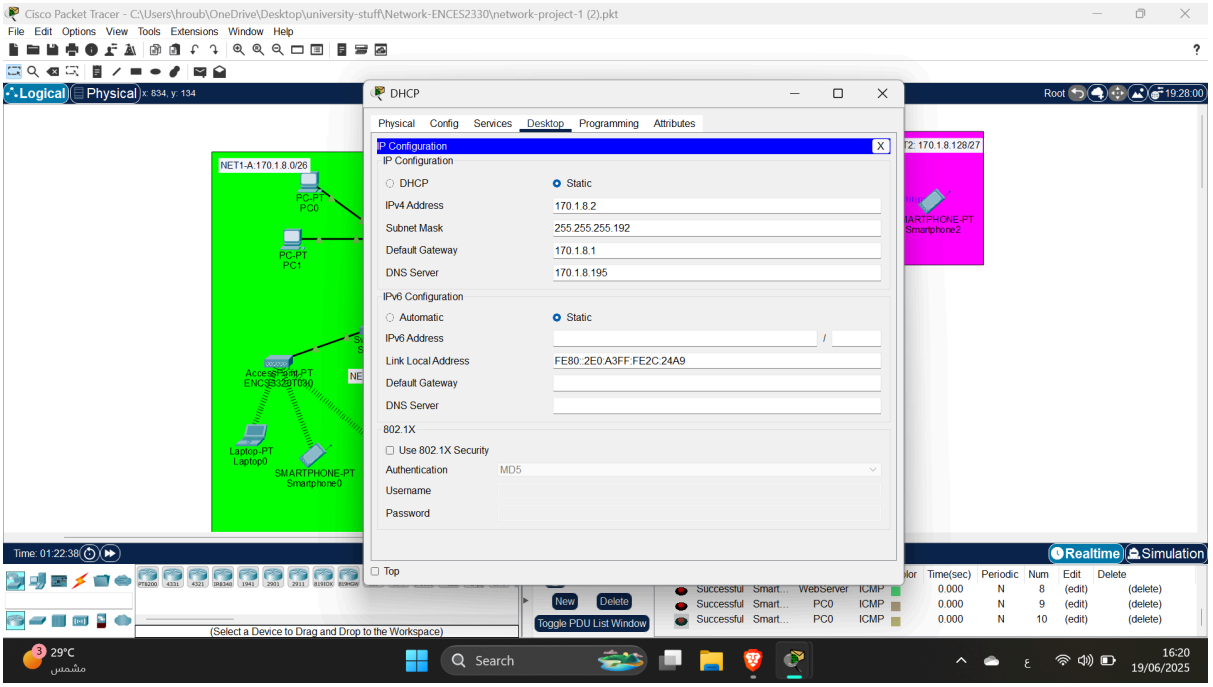

figure 23. IP configuration for DHCP server

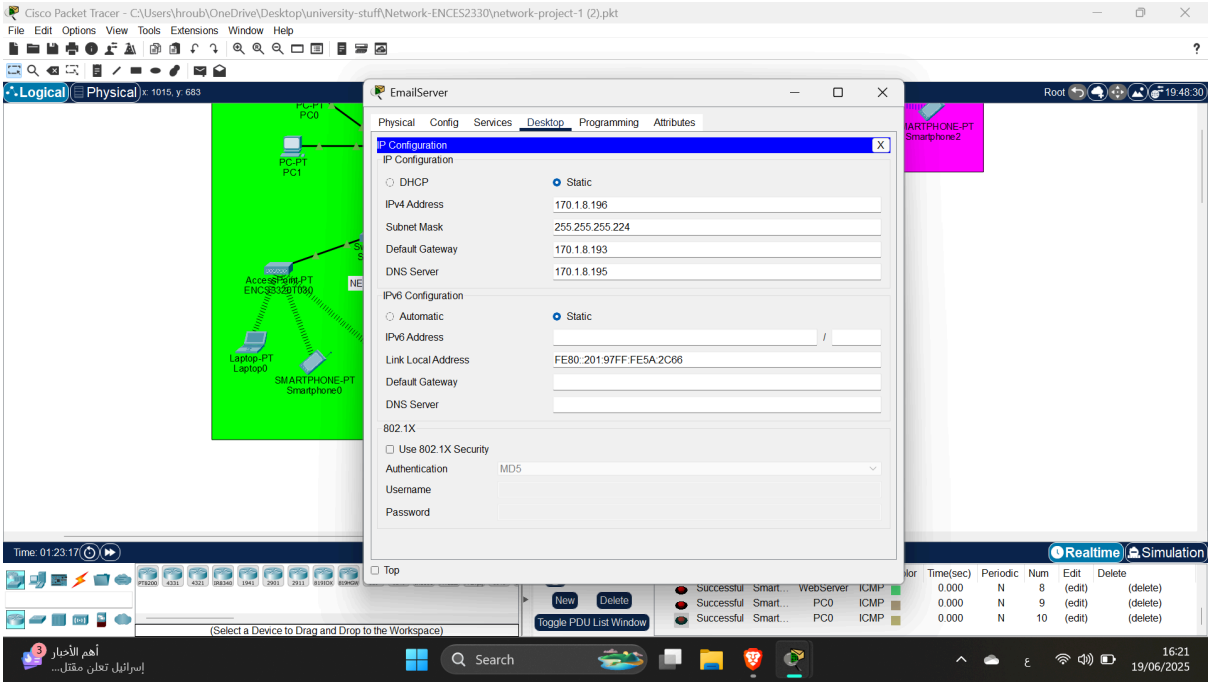

figure 24. IP configuration for Email server

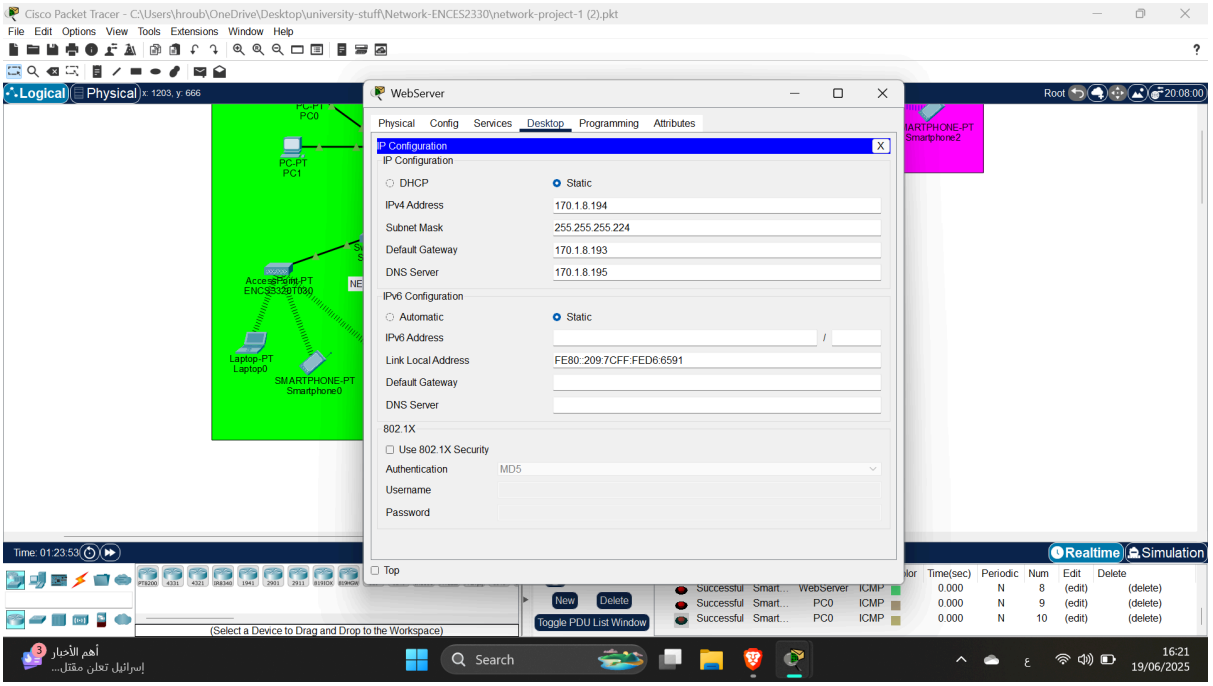

figure 25. IP configuration for Web server

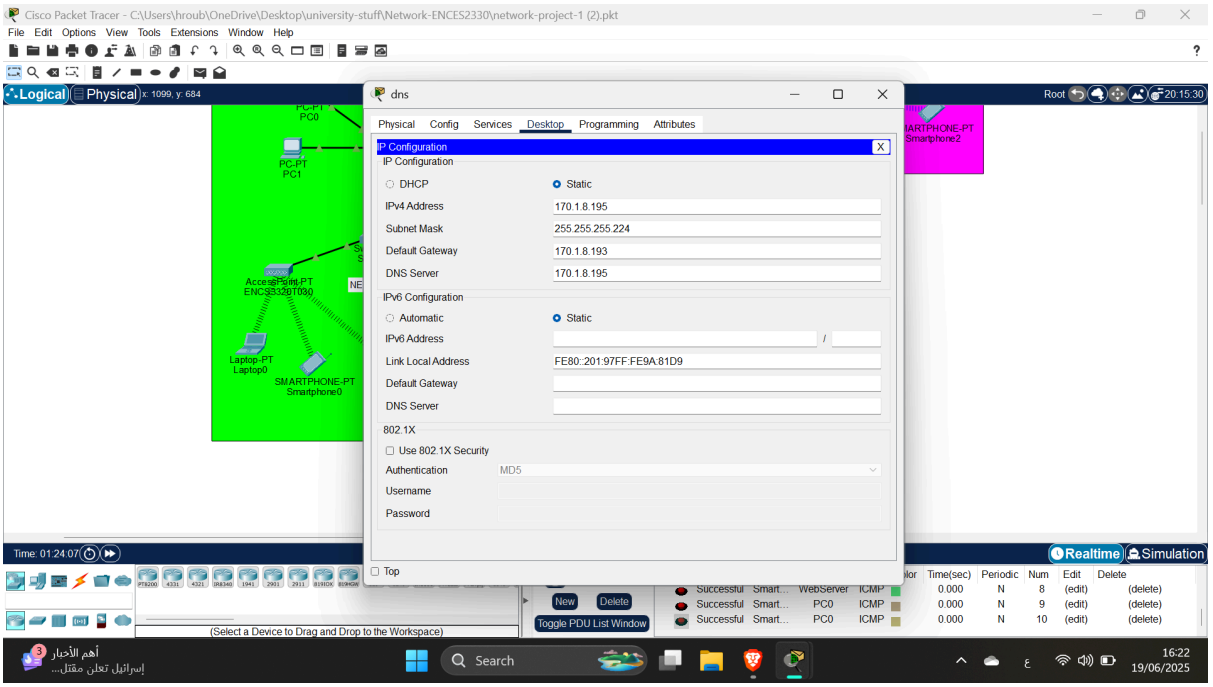

figure 26. IP configuration for DNS server

In this part :Each server was assigned a correct static IP. These configurations are important to provide core services like IP assignment, email, domain resolution, and website access.

Email service with the user setup on the mail.coe.birzeit.edu

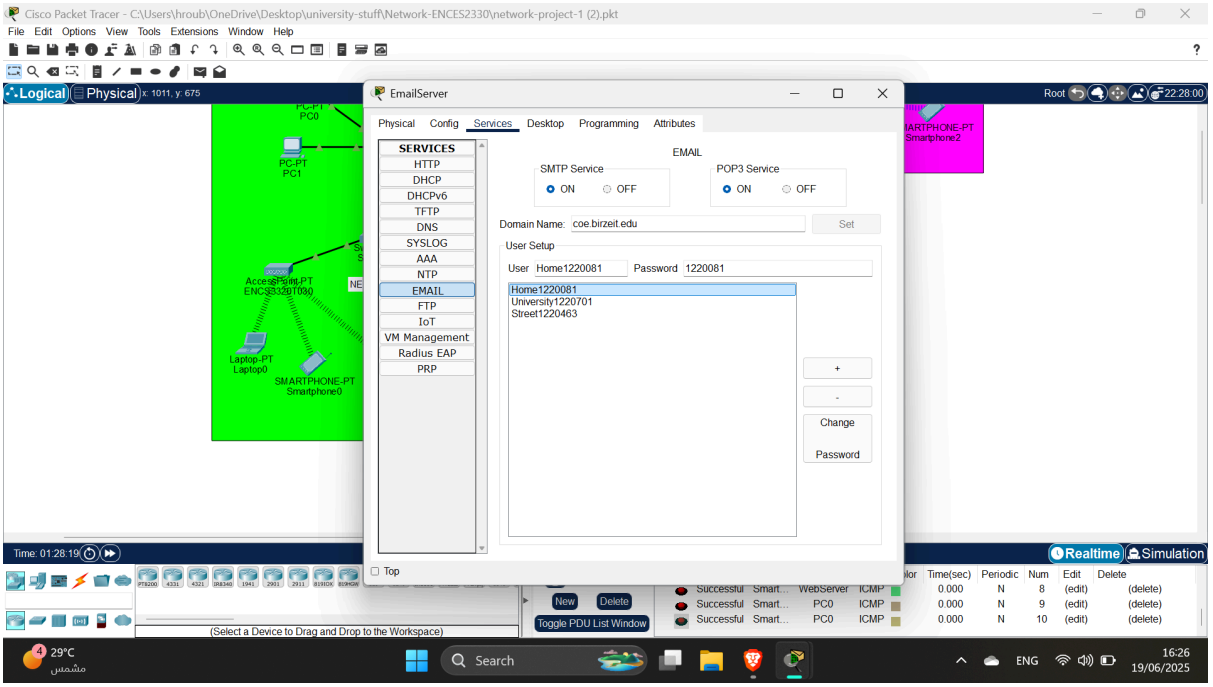

figure 27. Email service configuration

Email service was set up with user accounts and SMTP/POP3 enabled. This allows devices in different networks to send and receive emails.

DNS service with the RRs on the dns.coe.birzeit.edu

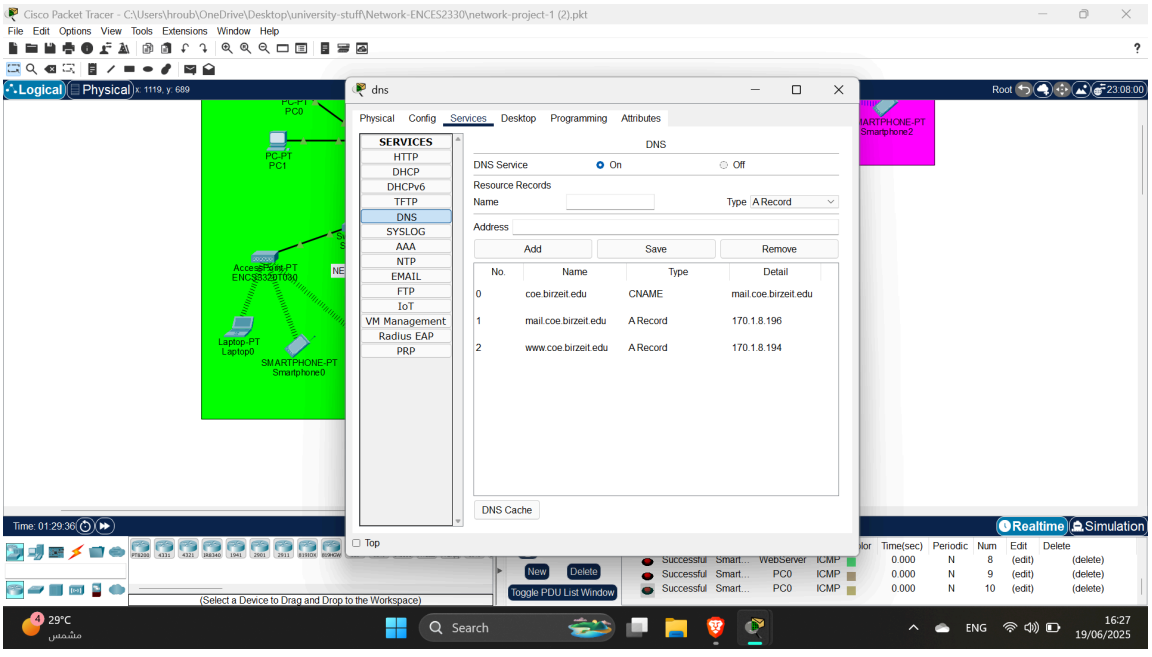

figure 28. DNS service with RRs

The DNS server was configured with all required Resource Records (RRs). This allows devices to resolve domain names like www.coe.birzeit.edu.

Successful access to the webserver www.coe.birzeit.edu from some of the end devices

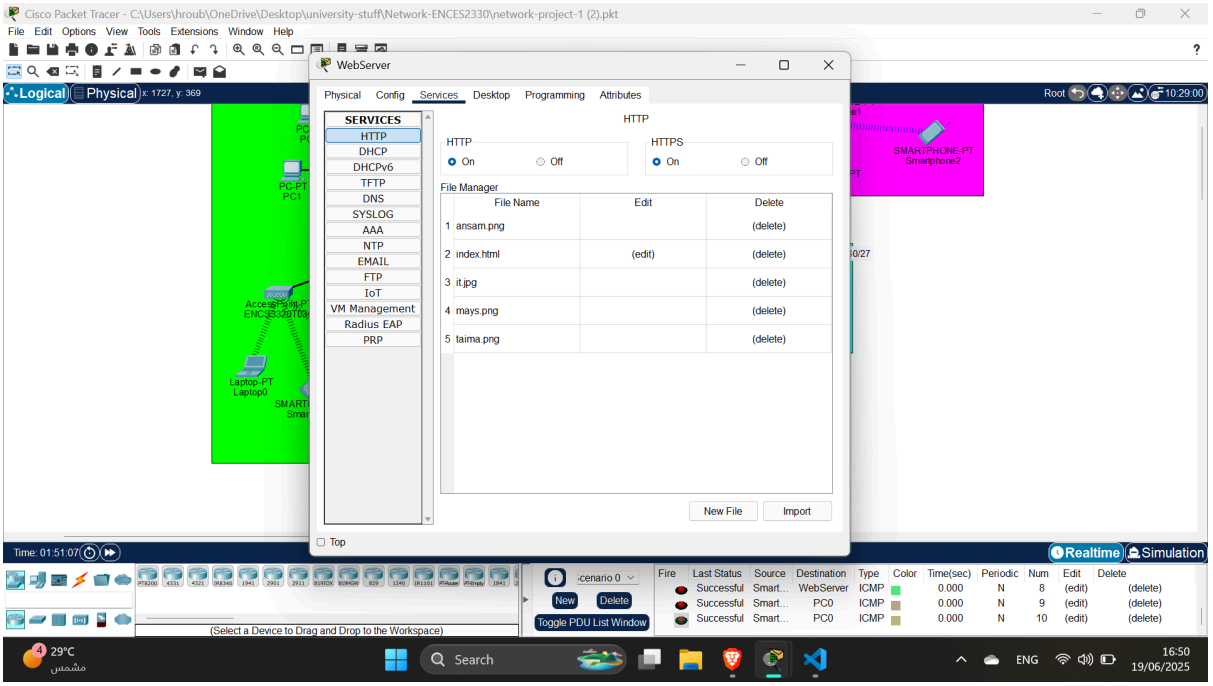

figure 29. Service configuration for Web server

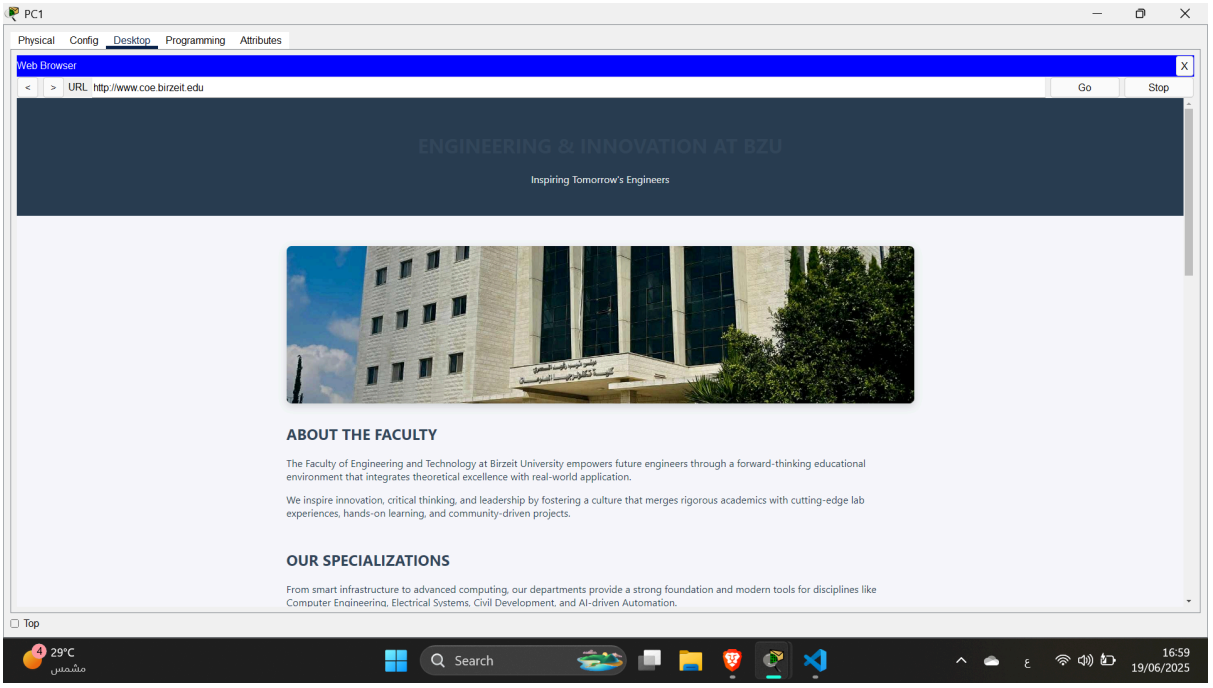

figure 30. PC1 accessing web page

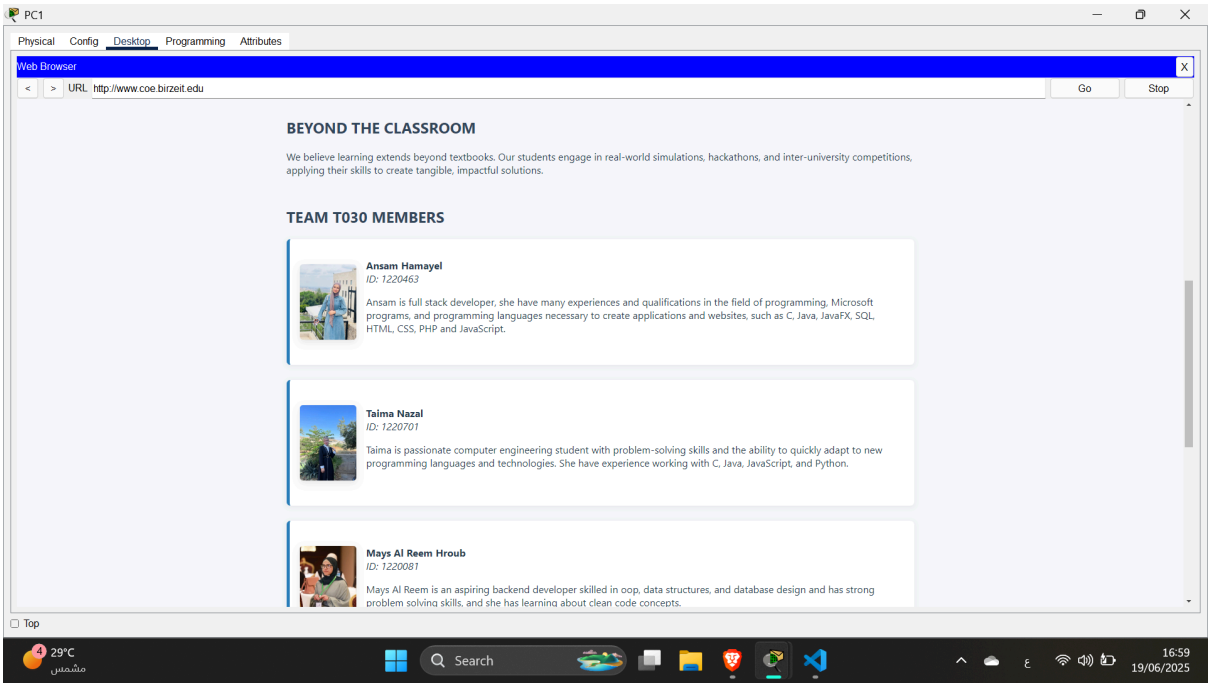

figure 31. PC1 accessing web page (cont.)

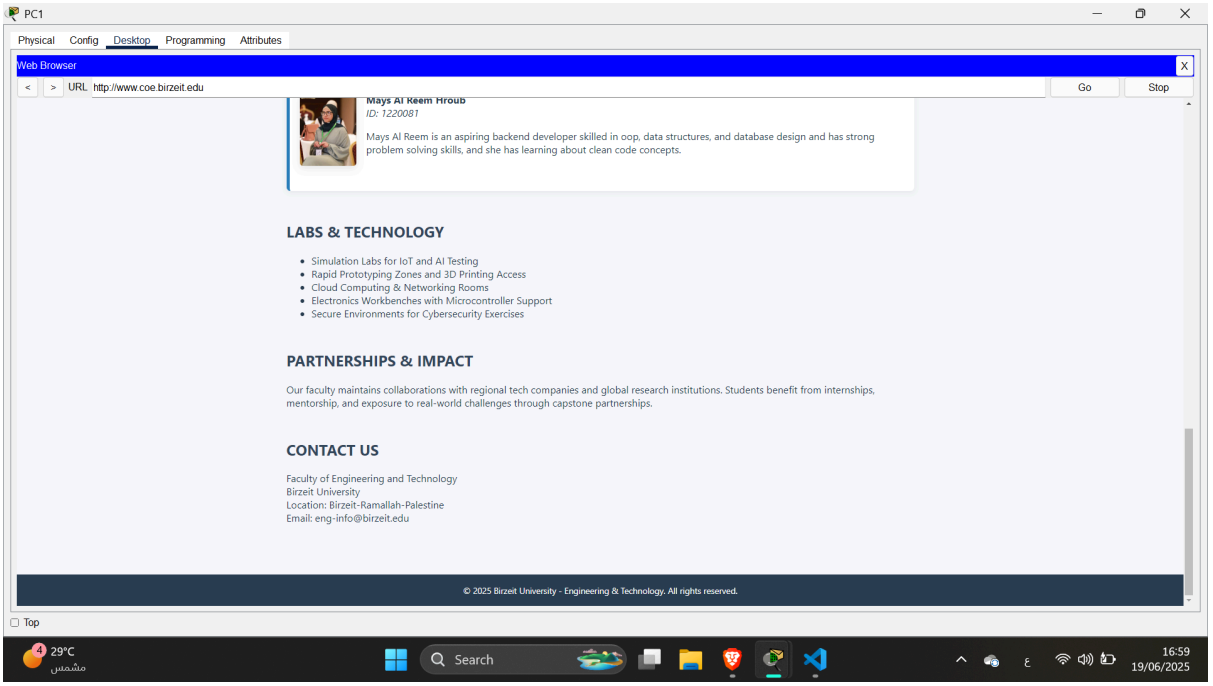

figure 32. PC1 accessing web page (cont.)

In this part : PC1 accessed the web page hosted on the internal web server. This confirms that both the web server and DNS are functioning correctly.

Email client configuration for coe.birzeit.edu account

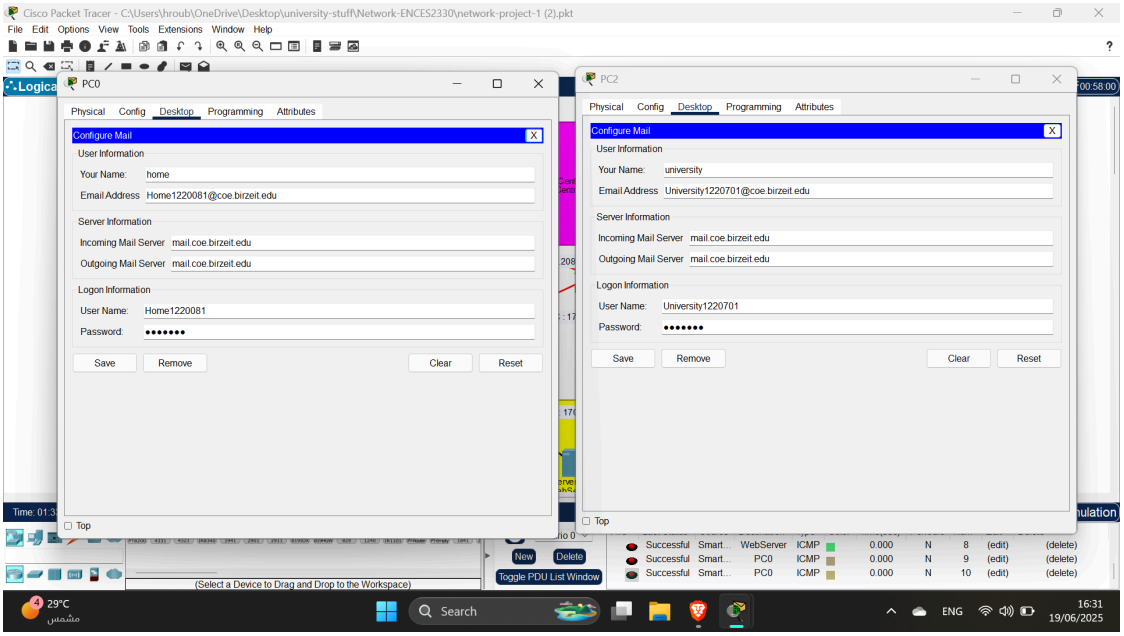

figure 33. Email configuration for end device PC0 and PC2

Email clients were configured using the server credentials. This setup enables email communication for team members in different subnets.

Successful sending and receiving of emails between the users from different networks

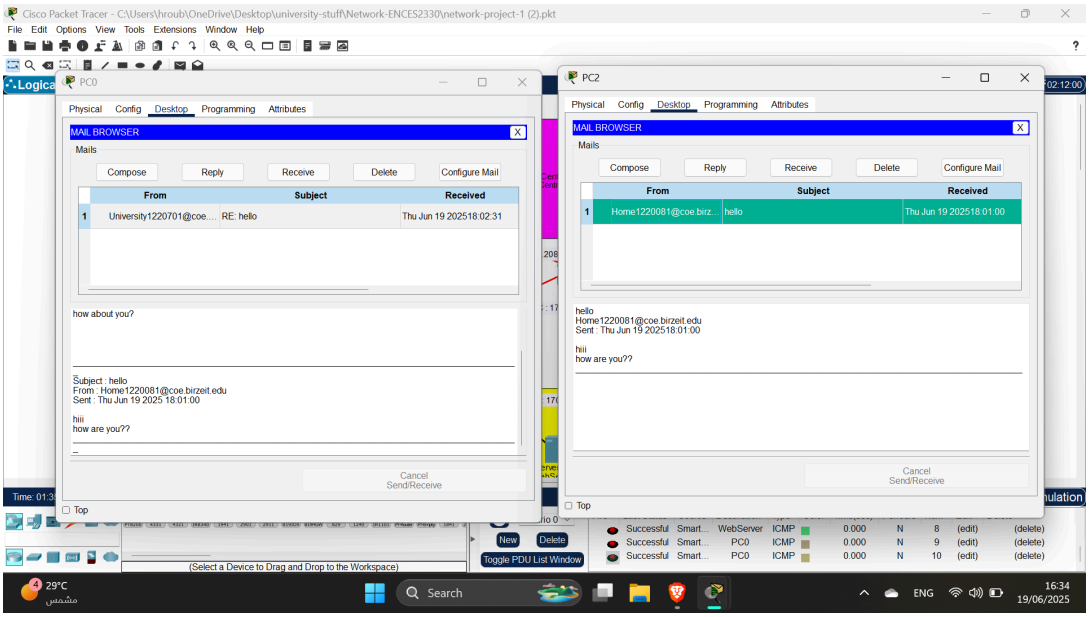

figure 34. PC2 sends email to PC0, and PC0 replies to PC2

This screenshot shows successful email exchange between users in different networks, verifying that email services are working properly across the entire topology.

Task 3: Routing Configuration

We used Open Shortest Path First (OSPF) for routing on the five areas (Area 0, Area 1, Area 2, Area 3, Area 4) in the topology. We configured OSPF on each of the three routers using the following command and passing 1 as the process-id:
(config)# router ospf <Process-ID>

And adding the required networks to the OSPF protocol using the following command:
(config-router)# network <ID-Address> <Wildcard Mask> area <Area-ID>

Which takes the IP address of the network, the wildcard mask which is like the complement of the subnet mask, and the area id. This command defines an interface on which OSPF runs and defines the area ID for that interface.

The following figures show the OSPF configuration for each router:

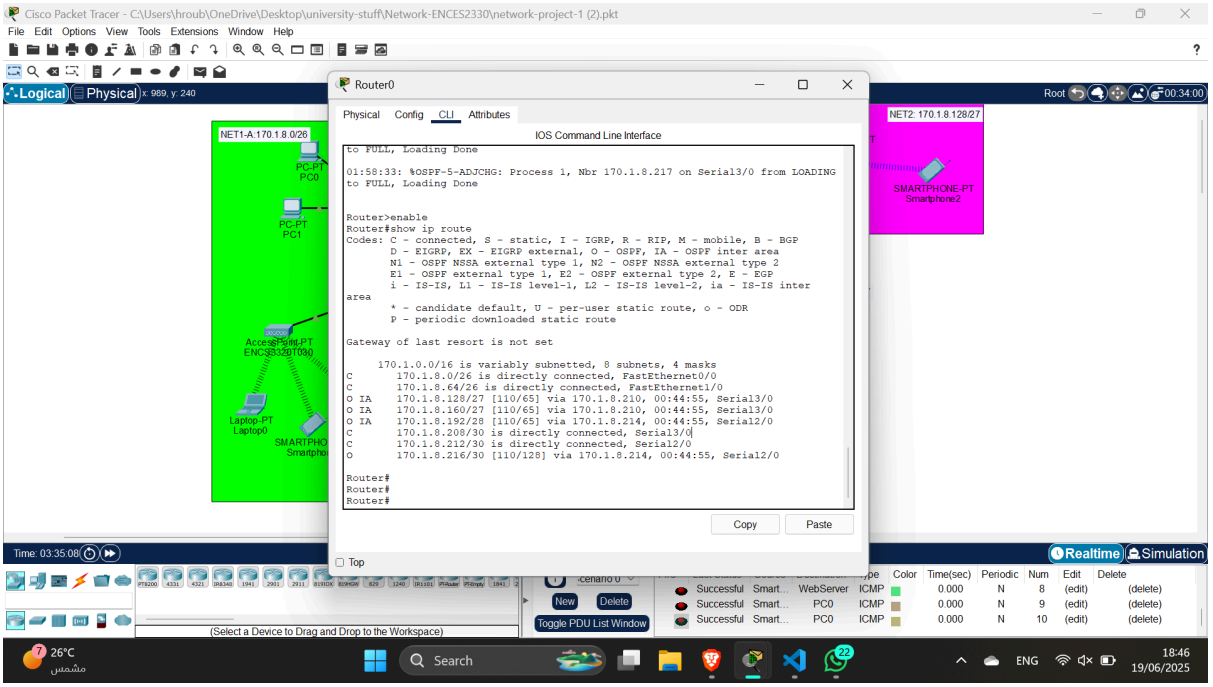

figure 35. OSPF config for router 0

Router 0 has **three directly connected networks**:

- 170.1.8.0/26 via FastEthernet0/0
- 170.1.8.64/26 via FastEthernet1/0
- 170.1.8.208/30 and 170.1.8.212/30 via Serial interfaces

It has learned **OSPF Inter-Area (IA) routes** from other routers:

- 170.1.8.128/27, 170.1.8.160/27, 170.1.8.192/28 are learned from Area 1 and Area 4
- 170.1.8.216/30 is learned through OSPF from Router 2

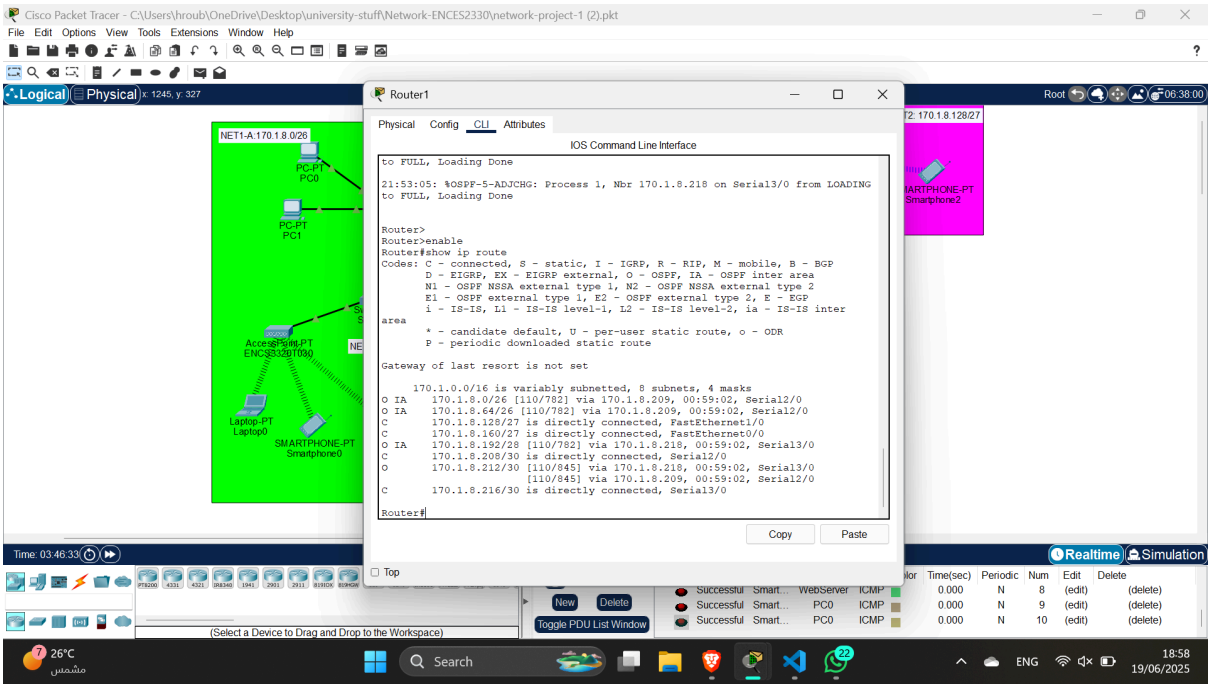

figure 36. OSPF config for router 1

Directly connected networks:

- 170.1.8.128/27 and 170.1.8.160/27 (likely from University Area 1)
- 170.1.8.208/30 (Serial link to Router 0)
- 170.1.8.216/30 (Serial link to Router 2)

Learned routes via OSPF:

- 170.1.8.0/26, 170.1.8.64/26: from Router 0 (Area 0)
- 170.1.8.192/28: from Router 2 (Area 4)

- 170.1.8.212/30: two paths → learned from both Router 0 and Router 2 (shows **redundancy**)

This shows that router 1 is correctly exchanging OSPF routes with router 1 and 2.

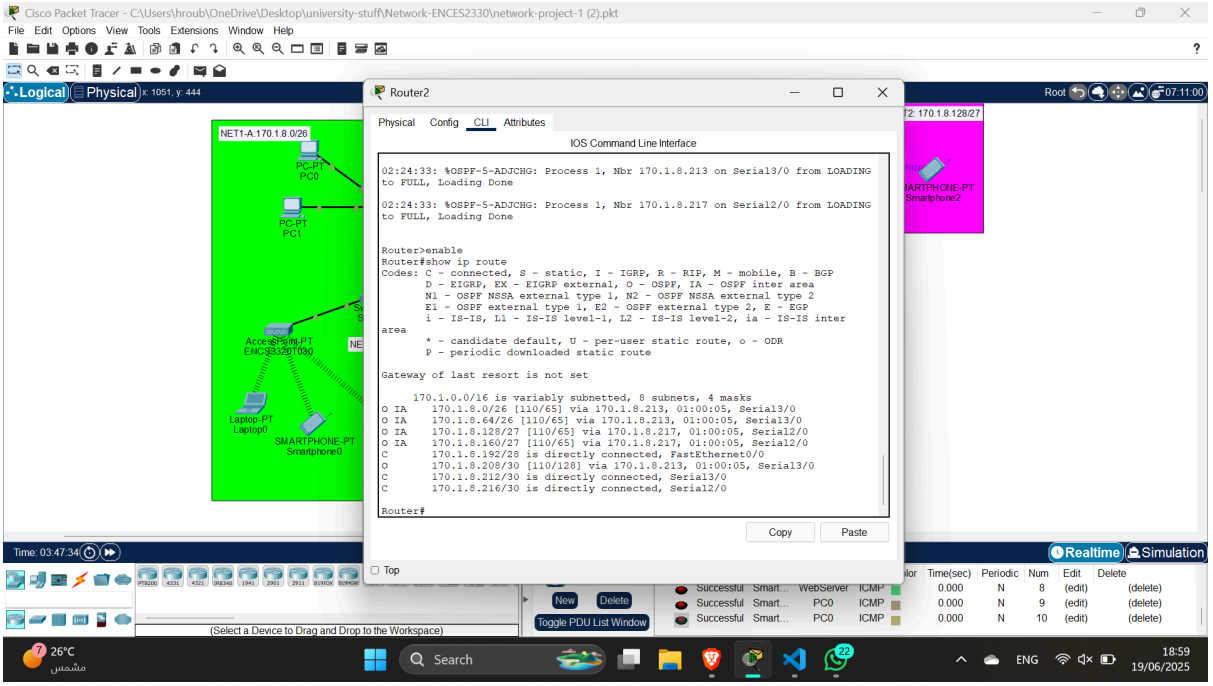

figure 37. OSPF config for router 2

Directly connected networks:

- 170.1.8.192/28 (likely from DataCenter Area 4)
- 170.1.8.212/30 (link to Router 0)
- 170.1.8.216/30 (link to Router 1)

OSPF-learned routes:

- 170.1.8.0/26, 170.1.8.64/26: from Router 0
- 170.1.8.128/27, 170.1.8.160/27: from Router 1
- 170.1.8.208/30: from Router 0

This proves that router 2 is learning routes from both router 0 and 1.

Issues and Limitations

Issues and Challenges

1. Difficulty configuring Access Point and smartphone settings

Some wireless devices, such as smartphones, automatically connect to the wrong network instead of the desired cell tower.

Limitations

1. Full reliance on Packet Tracer only

The program is a simulation only and does not reflect actual network performance, especially in terms of latency or data load.

2. Performance not tested under real conditions.

The network was not tested under real conditions, such as heavy traffic congestion or real-world DNS issues.

3. Port Limitations in Virtual Routers

Some routers come with a limited number of ports.

4. Lack of a centralized network management control panel

Every configuration is done manually on each device/router, and there is no unified administrative interface.

Teamwork

We ensured that the tasks were distributed fairly among all group members, with each person contributing to areas such as networking, testing, or writing the report. We held online meetings to discuss our progress and make sure that no one is facing any issues.

Task 1: Completed by Taima.
Task 2: Completed by Ansam (a + b + c), Ansam & Taima (d), Taima (e) .
Task 3: Completed by Mays Al-Reem.

Writing the report was done by all group members equally.

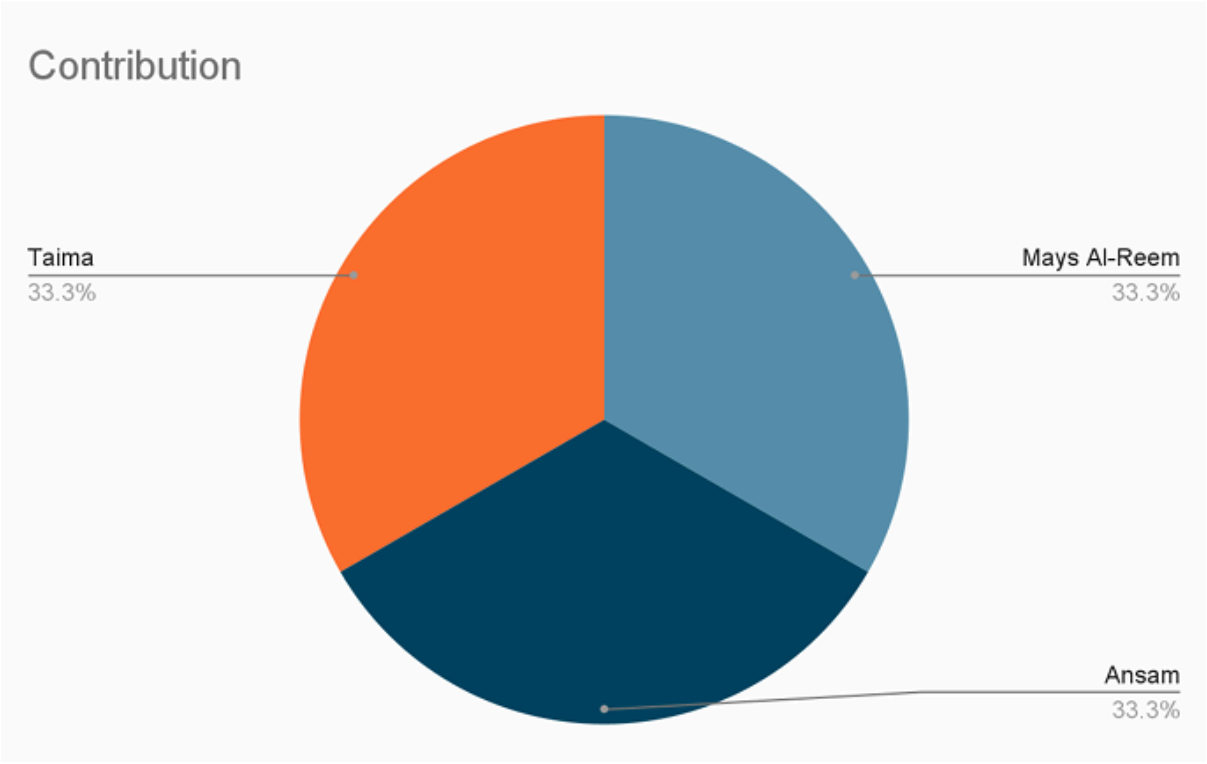

figure 38. teamwork chart

Conclusion

By the end of this project, we were able to design and implement an integrated network spanning multiple real-world environments, such as our home, university, and street, using the OSPF routing model and detailed IP networks using Cisco Packet Tracer. The project required careful address planning, logical subnetting, and configuration of various settings such as email, DHCP, and OSPF. Working on the project strengthened our network configuration skills, discovered the importance of organization in dealing with complex networks, and learned how to respond to real-world problems that may arise during infrastructure setup. Despite the technical challenges we faced, the project provided a valuable learning experience in a highly realistic environment and is an important step toward building advanced network engineering skills.

References

https://www.geeksforgeeks.org/computer-networks/domain-name-system-dns-in-application-layer/

https://jayeshkumarjangir49.medium.com/how-is-open-short-path-first-routing-protocol-implemented-51544d00cb37

https://postmansmtp.com/imap-vs-pop3-vs-smtp/

https://zindagitech.com/different-types-of-modes-in-wireless-access-points-aps/

https://www.firstpoint-mg.com/imsi-catcher-protection/