Birzeit University Faculty of Engineering and Technology

Department of Electrical and Computer Engineering

Computer Network || ENCS3320

Second Semester, 2024/2025

Cisco Packet Tracer-Second Project Report

Prepared By:

Waad ziadeh	**1220423**	**Section:5**
Saja Sayara	**1220601**	**Section:4**
Aya Fares	**1222654**	**Section:3**

Date: 19 JUNE 2025

Abstract

The goal of this project is to design, configure, and test a multi-area computer network using Cisco Packet Tracer, combining both theoretical knowledge and hands-on skills in computer networking. The network is divided into five main areas: Core, University, Street, Home, and Datacenter. We applied essential concepts such as IP addressing, subnetting, static and dynamic routing (using OSPF), switching, VLANs, and network services including DNS, DHCP, Web, and Email servers.

Throughout the project, we used Packet Tracer to simulate real-world scenarios by connecting various devices like routers, switches, access points, servers, and end-user devices (PCs, laptops, smartphones, tablets). Dynamic IP configurations were implemented through DHCP, while secure wireless connections were established using WPA2 encryption. We also used NAT with PAT to manage internet access and preserve IP addresses.

Advanced routing protocols like OSPF were used for intra-domain routing between the five areas, while network functionality was verified using ping, tracert, and service tests (web browsing, email exchange, DNS resolution). The datacenter was set up to host essential services like a web server (with custom HTML content), a mail server (supporting SMTP and POP3), and a DNS server with proper resource records.

This project helped us strengthen our understanding of how large-scale networks operate. It gave us valuable experience in troubleshooting, teamwork, and writing technical documentation. Most importantly, it allowed us to connect classroom concepts with practical implementation in a simulated environment.

Contents

Table of figures

List of Tables

Theory

→ Network Address Translation (NAT)

Network Address Translation (NAT) is a service that enables private IP networks to use the internet and cloud. NAT translates private IP addresses in an internal network to a public IP address before packets are sent to an external network[1].

How does NAT work?

Network Address Translation (NAT) is a service that operates on a router or edge platform to connect private networks to public networks like the internet. NAT is often implemented at the WAN edge router to enable internet access in core, campus, branch, and colocation sites[1].

With NAT, an organization needs one IP address or one limited public IP address to represent an entire group of devices as they connect outside their network. Port Address Translation (PAT) enables one single IP to be shared by multiple hosts using IP and port address translation[1].

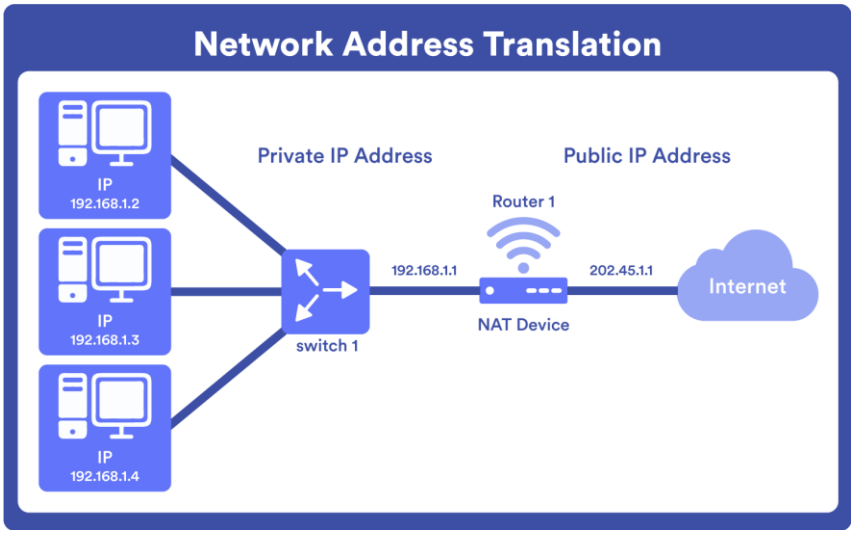


Figure 1: Network Address Translation

The types of NAT:

- **Static NAT**: Creates a fixed one-to-one mapping between a private IP and a public IP, allowing external devices to access internal devices via the public IP[2].
- **Dynamic NAT**: Assigns private IPs to a pool of public IPs dynamically, ensuring outbound connectivity but without a consistent public IP for each session[2].
- **Port Address Translation (PAT):** Also called NAT overload, it enables multiple private IPs to share one public IP by using unique port numbers for each connection[2].

Advantages of NAT:

- Efficient IP Usage: NAT enables multiple devices within a local network to access the internet through a single public IP, conserving the limited pool of IPv4 addresses[2].
- Improved Security: By hiding internal IP addresses, NAT provides an extra layer of protection, making it harder for external networks to directly access internal devices[2].
- Simplified Network Management: NAT allows internal network modifications without altering public IP configurations, making network administration more flexible[2].

Disadvantages of NAT:

- Protocol Limitations: Certain protocols that include IP information in their payloads may face issues with NAT, potentially causing connectivity problems[2].
- Performance Impact: Translating IP addresses can introduce delays and may reduce efficiency in high traffic environments[2].
- Challenges with Peer-to-Peer Connections: NAT complicates the setup of direct inbound connections, making it harder to use peer-to-peer services and applications effectively[2].

→ Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol is a network protocol used to automate the process of assigning IP addresses and other network configuration parameters to devices (such as computers, smartphones, and printers) on a network. Instead of manually configuring each device with an IP address, DHCP allows devices to connect to a network and receive all necessary network information, like IP address, subnet mask, default gateway, and DNS server addresses, automatically from a DHCP server.

This makes it easier to manage and maintain large networks, ensuring devices can communicate effectively without conflicts in their network settings. DHCP plays a crucial role in modern networks by simplifying the process of connecting devices and managing network resources efficiently[3].

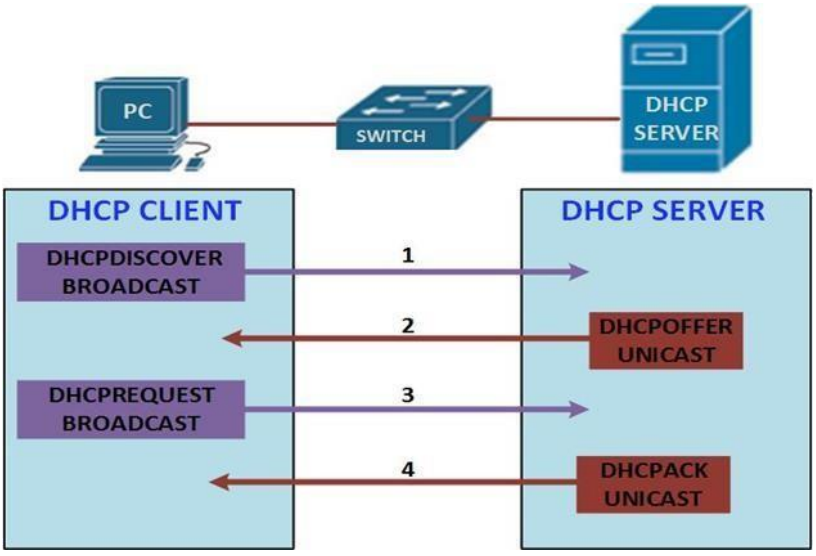


Figure 2:Dynamic Host Configuration Protocol (client-server scenario)

Limitations of DHCP:

- Potential Security Risks: Without adequate security measures, unauthorized devices could gain access, and rogue DHCP servers may cause network disruptions.
- Reliance on DHCP Server: The functioning of network devices depends on the availability of the DHCP server; a server failure could prevent devices from obtaining or renewing IP addresses.

→ 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, This interaction relies on communication protocols like **HTTP** and **HTTPS** .[4]

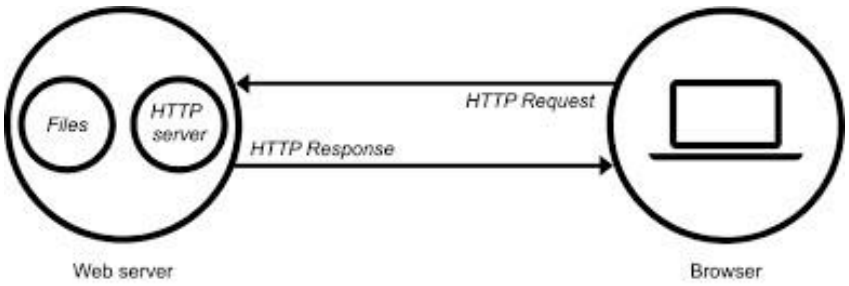


Figure 3: web server scenario

HTTP	HTTPS
HTTP stands for **HyperText Transfer Protocol.** In HTTP, the URL begins with "http://".	HTTPS stands for **HyperText Transfer Protocol Secure**. In HTTPS, the URL starts with "https://".
HTTP uses port number **80** for communication.	HTTPS uses port number **443** for communication.
Hyper-text exchanged using HTTP goes as plain text i.e. anyone between the browser and server can read it relatively easily if one intercepts this exchange of data and due to which it is Insecure.	HTTPS is considered to be secure but at the cost of processing time because Web Server and Web Browser need to exchange encryption keys using Certificates before actual data can be transferred.
HTTP Works at the **Application layer**.	HTTPS works at **Transport Layer**.
HTTP speed is **faster** than HTTPS.	HTTPS speed is **slower** than HTTP.

HTTP is used to transfer text, video, and images via web pages.	HTTPS is used to transfer data securely via a network.

Table 1: HTTP vs HTTPS protocols

→ Email

Email is a popular communication method that enables users to exchange messages electronically over a network, such as the internet. It relies on specific protocols to facilitate the transfer of messages between email clients (e.g., Outlook, Gmail) and servers. Two essential protocols used in email communication are POP3 and SMTP.

SMTP	POP3
SMTP stands for **Simple Mail Transfer Protocol.**	POP3 stands for **Post Office Protocol** version 3.
It is used for **sending** messages.	It is used for **accessing** messages.
SMTP is also known as **PUSH** protocol.	POP3 is also known as **POP** protocol.
The port number of SMTP is **25, 465, and 587** for secured connection (TLS connection).	The port number of POP3 is **110 or port 995** for SSL/TLS connection.
It is implied between sender mail server and receiver mail server.	It is implied between receiver and receiver mail server.

Table 2: SMTP vs POP3 protocols

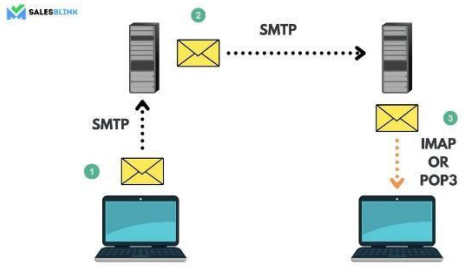


Figure 4: SMTP vs POP3 protocols

→

Domain Name System (DNS)

The IP addresses of all websites are stored in the Domain Name System (DNS). DNS is responsible for establishing the right IP address for domain names such as 'google.com' when users type them into web browsers. The addresses are then used by browsers to communicate with source servers in order to access website information and display it to users. DNS servers, which are services that answer DNS queries, make this all possible.

A server is a device or program that provides services to other programs known as "clients." Most modern desktop and mobile operating systems have DNS clients, which allow web browsers to communicate with DNS servers[5].

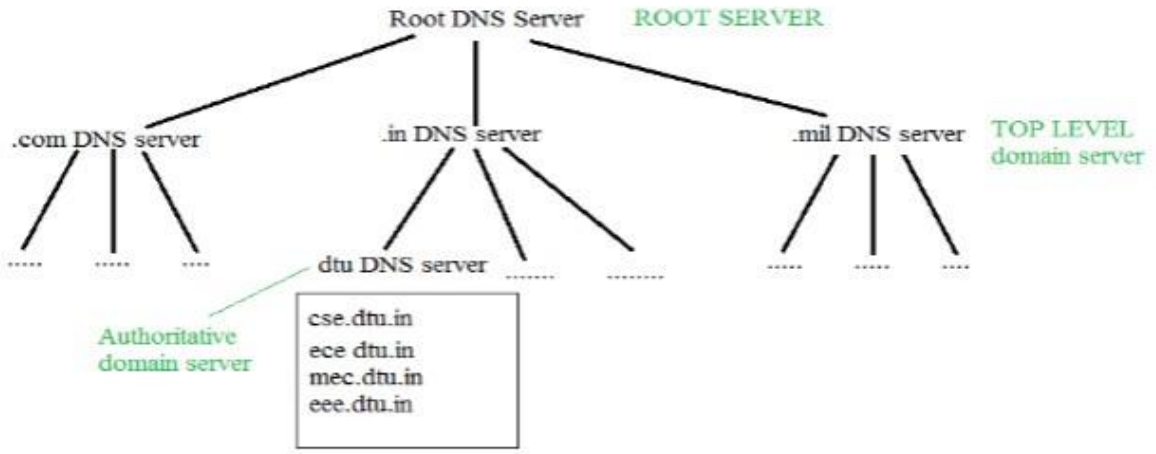


Figure 5: DNS server

→

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[6].

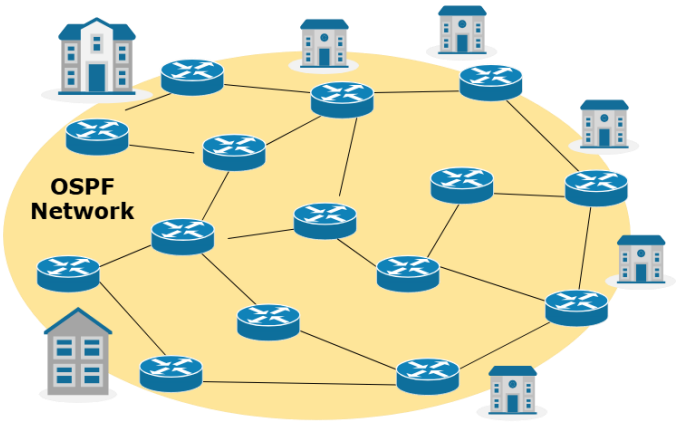


Figure 6:OSPF links

→ Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) is an essential network protocol that orchestrates how data packets traverse the internet, enabling seamless communication among various networks, devices, and technologies. As the principal protocol for routing information between autonomous systems (AS), BGP is pivotal for ensuring global connectivity across the internet. It exchanges routing data and potential paths, enabling packets to navigate the most efficient routes through intricate network infrastructures, thus enhancing speed and reliability of data transmission. BGP is crucial not only for upholding the internet's architecture but also for facilitating the integration of emerging networks and technologies [7].

Figure 7:BGP between ASes

→

Subnetting

Subnetting is the process of dividing a large network into smaller networks called "subnets." Subnets provide each group of devices with their own space to communicate, which ultimately helps the network to work easily. This also boosts security and makes it easier to manage the network, as each subnet can be monitored and controlled separately.

Our IP address will depend on our university ID = 1220423, so the address that we will start from is **104.23.8.0/23**

In binary: 01101000.00010111.00001000.00000000

Fixed part — depends on number of hosts we use bits

Subnetting Solution Steps

Main Network:
Main IP: 104.23.8.0/24 (256 IPs available)

Step 1: Large Networks (62 Hosts)

Requirement: 62 Hosts → Needs /26 subnet (64 IPs)

- 104.23.8.0 → NET1-A network → needs 62 hosts → /26
  Binary: 104.23.8.00000000 → 6 host bits
  Range: 104.23.8.0 - 104.23.8.63
- 104.23.8.64 → NET1-B network → needs 62 hosts → /26
  Binary: 104.23.8.01000000 → 6 host bits
  Range: 104.23.8.64 - 104.23.8.127

Step 2: Medium Networks (30 Hosts)

Requirement: 30 Hosts → Needs /27 subnet (32 IPs)

- 104.23.8.128 → NET2 → /27
  Binary: 104.23.8.10000000 → 5 host bits
  Range: 104.23.8.128 - 104.23.8.159
- 104.23.8.160 → NET3 → /27
  Binary: 104.23.8.10100000 → 5 host bits
  Range: 104.23.8.160 - 104.23.8.191
- 104.23.8.192 → NET4 → /27
  Binary: 104.23.8.11000000 → 5 host bits
  Range: 104.23.8.192 - 104.23.8.223

Step 3: Small Networks (2 Hosts)

Requirement: 2 Hosts → Needs /30 subnet (4 IPs)

- 104.23.8.224 → NET0-A → /30
  Binary: 104.23.8.11100000
  Range: 104.23.8.224 - 104.23.8.227
- 104.23.8.228 → NET0-B → /30
  Binary: 104.23.8.11100100
  Range: 104.23.8.228 - 104.23.8.231
- 104.23.8.232 → NET0-C → /30
  Binary: 104.23.8.11101000
  Range: 104.23.8.232 - 104.23.8.235

Subnetting table:

Subnet	Subnet Mask	CIDR	Network IP	Broadcast IP	First IP	Last IP	Hosts
NET1-A	255.255.255.192	/26	104.23.8.0	104.23.8.63	104.23.8.1	104.23.8.62	**62**
NET1-B	255.255.255.192	/26	104.23.8.64	104.23.8.127	104.23.8.65	104.23.8.126	**62**
NET2	255.255.255.224	/27	104.23.8.128	104.23.8.159	104.23.8.129	104.23.8.158	**30**
NET3	255.255.255.224	/27	104.23.8.160	104.23.8.191	104.23.8.161	104.23.8.190	**30**
NET4	255.255.255.224	/27	104.23.8.192	104.23.8.223	104.23.8.193	104.23.8.222	**30**
NET0-A	255.255.255.252	/30	104.23.8.224	104.23.8.227	104.23.8.225	104.23.8.226	**2**
NET0-B	255.255.255.252	/30	104.23.8.228	104.23.8.231	104.23.8.229	104.23.8.230	**2**
NET0-C	**255.255.255.252**	**/30**	**104.23.8.232**	**104.23.8.235**	**104.23.8.233**	**104.23.8.234**	**2**

Table 3: subnetting table

Results and Discussions

Our topology

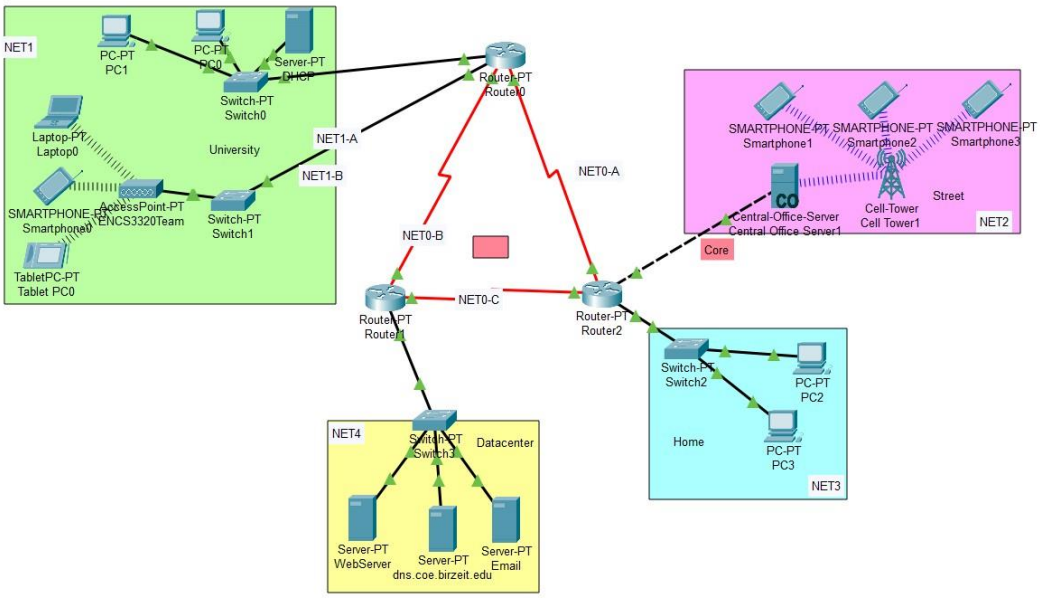


Figure 8: Full topology

In this section, we constructed a topology using **Packet Tracer**, based on the IP addresses determined in **Part 0**. As illustrated in the figure above, the topology is divided into the areas

We assigned IP addresses to each area and then configured the IPs for the end systems and routers **statically**.

Core network Area 0

Configure the interfaces of all routers as instructed in the figure

Router 0

- For Router R0 – fa0/0, we assigned the first IP address after the network IP (**104.23.8.1**) with a subnet mask of **255.255.255.192**.

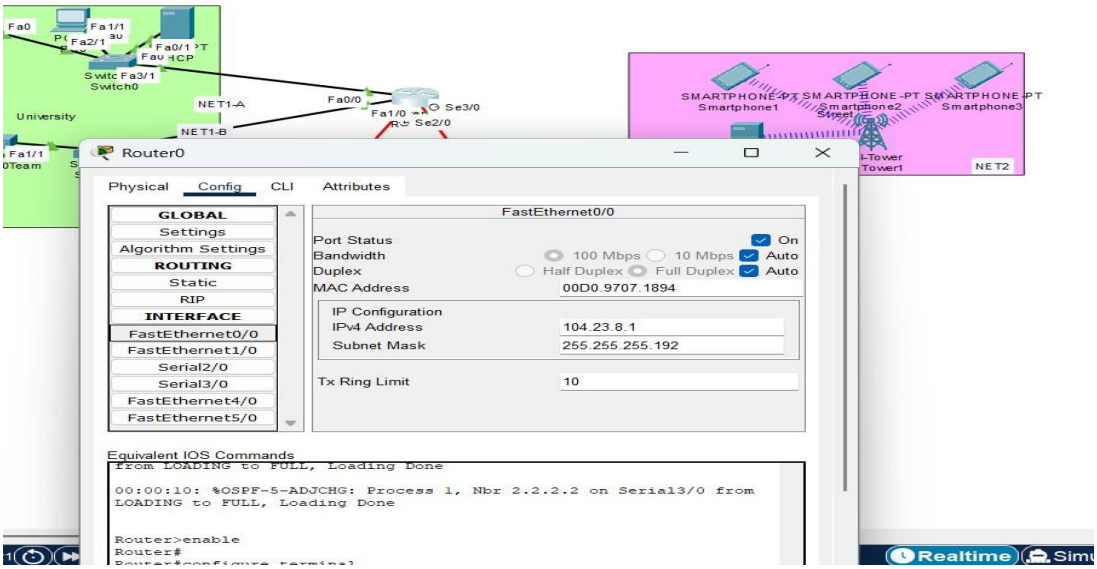


Figure 1 R0 – fa0/0

- For Router R0 – fa1/0, we assigned the first IP address after the network IP (**104.23.8.65**) with a subnet mask of **255.255.255.192**.

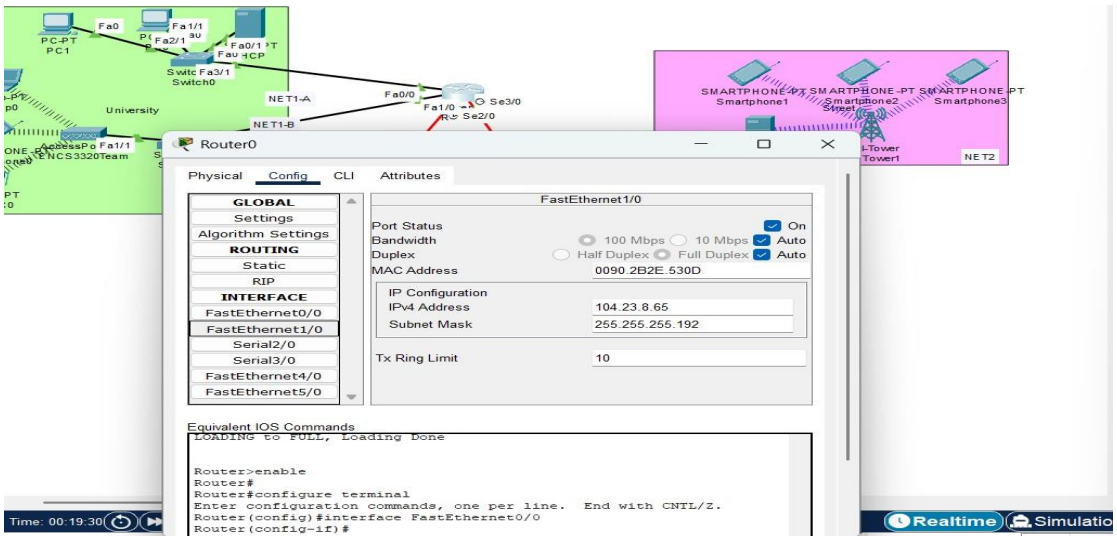


Figure 2 R0 – fa1/0,

- For Router R0 – se2/0, we assigned the first IP address after the network IP (**104.23.8.229**) with a subnet mask of **255.255.255.252**.

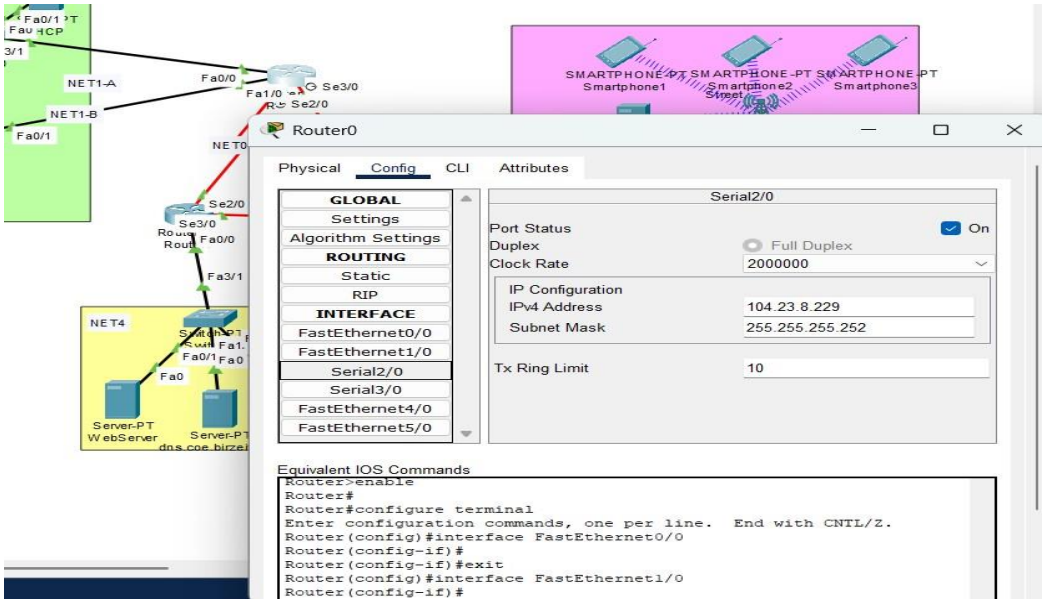


Figure 1 R0 – se2/0

- For Router R0 – se3/0, we assigned the first IP address after the network IP (**104.23.8.225**) with a subnet mask of **255.255.255.252**.

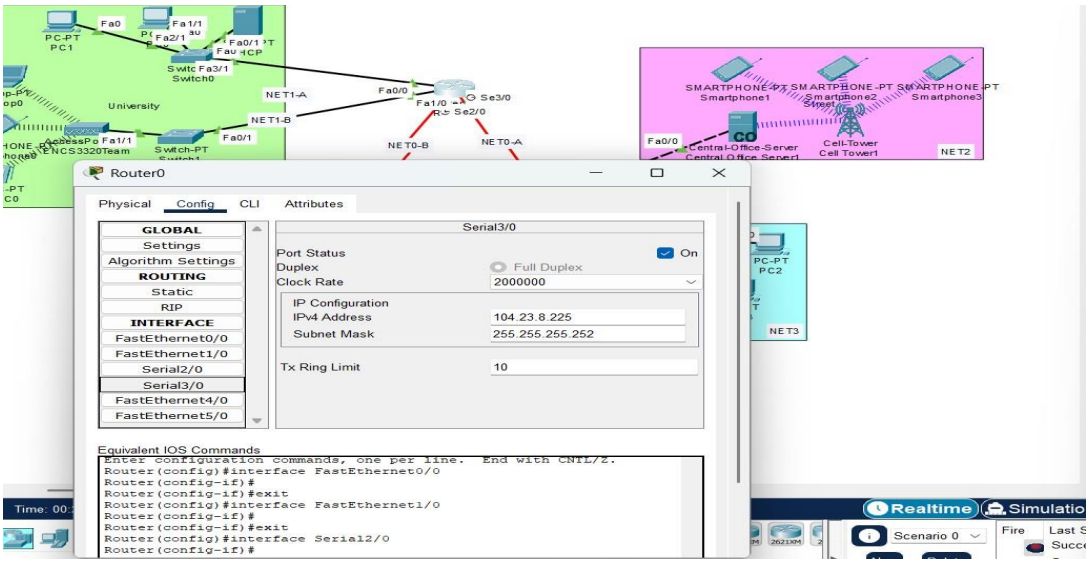


Figure 2 R0 – se3/0

Router One

- For Router R1 – fa0/0, we assigned the first IP address after the network IP (**104.23.8.193**) with a subnet mask of **255.255.255.224**.

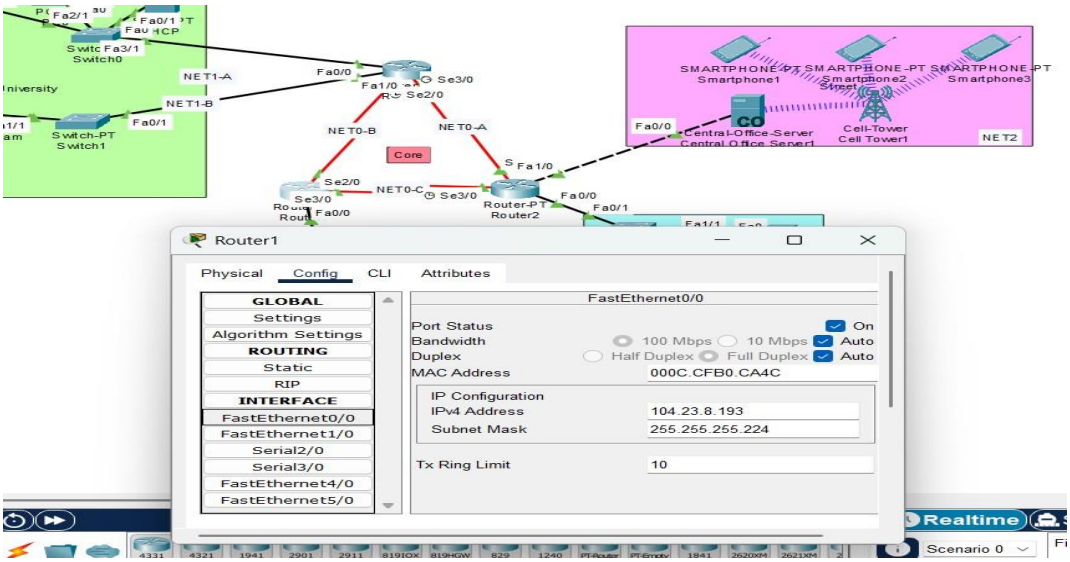


Figure 3 R1 – fa0/0

- For Router R1 – se2/0, we assigned the first IP address after the network IP (**104.23.8.230**) with a subnet mask of **255.255.255.252**.

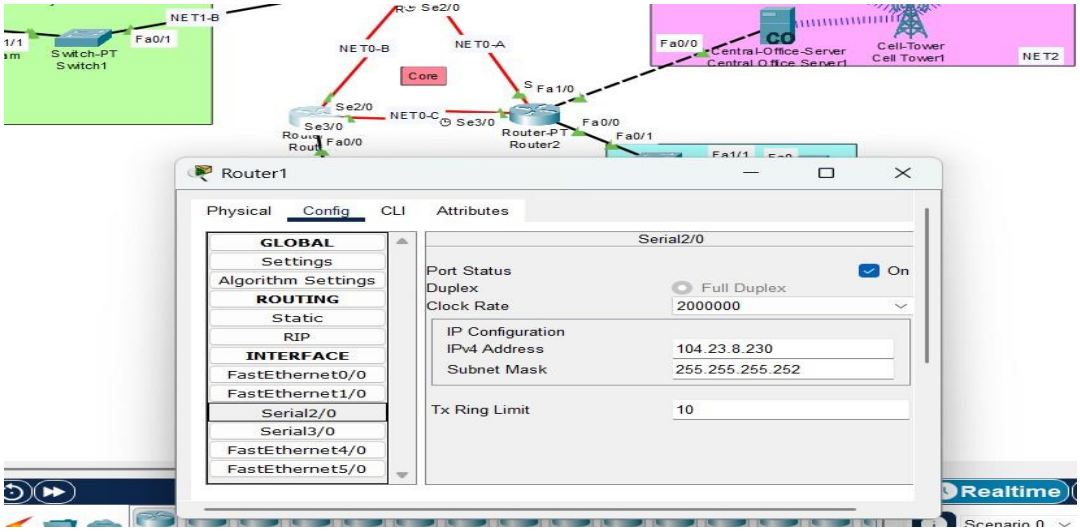


Figure 4 R1 – se2/0

- For Router R1 – se3/0, we assigned the first IP address after the network IP (**104.23.8.233**) with a subnet mask of **255.255.255.252**.

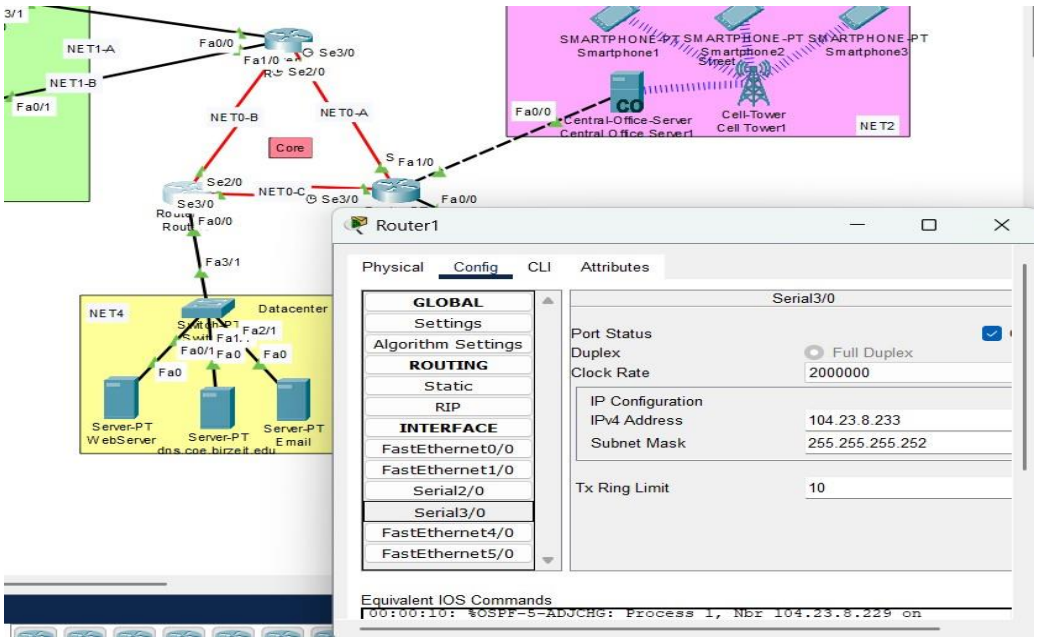


Figure 5 R1 – se3/0

Router Two

- For Router R2 – fa0/0, we assigned the first IP address after the network IP (**104.23.8.161**) with a subnet mask of **255.255.255.224**.

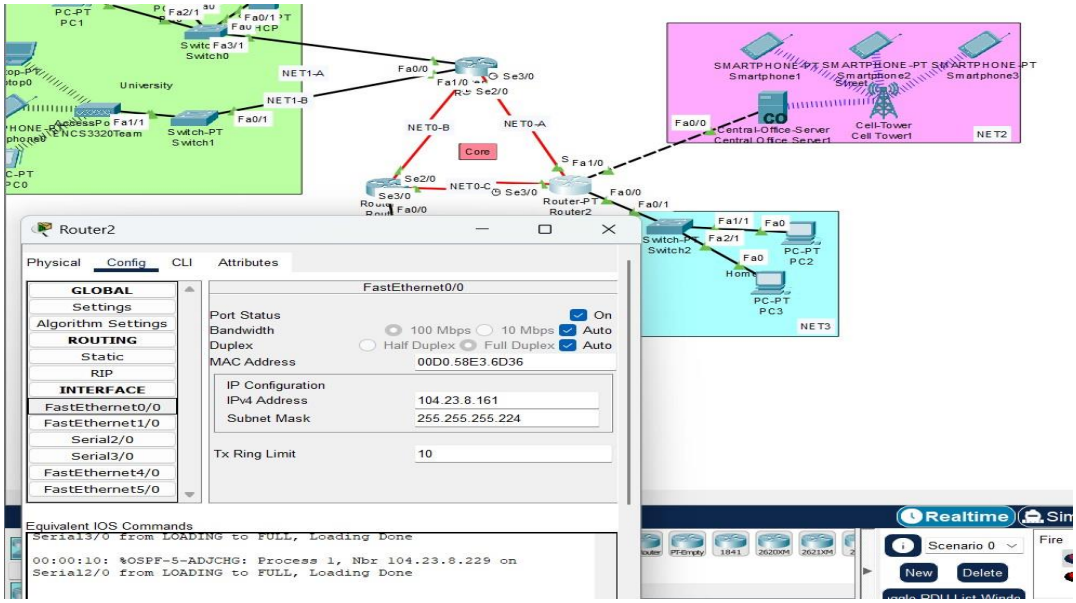


Figure 6 R2 – fa0/0

- For Router R2 – fa1/0, we assigned the first IP address after the network IP (**104.23.8.129**) with a subnet mask of **255.255.255.224**.

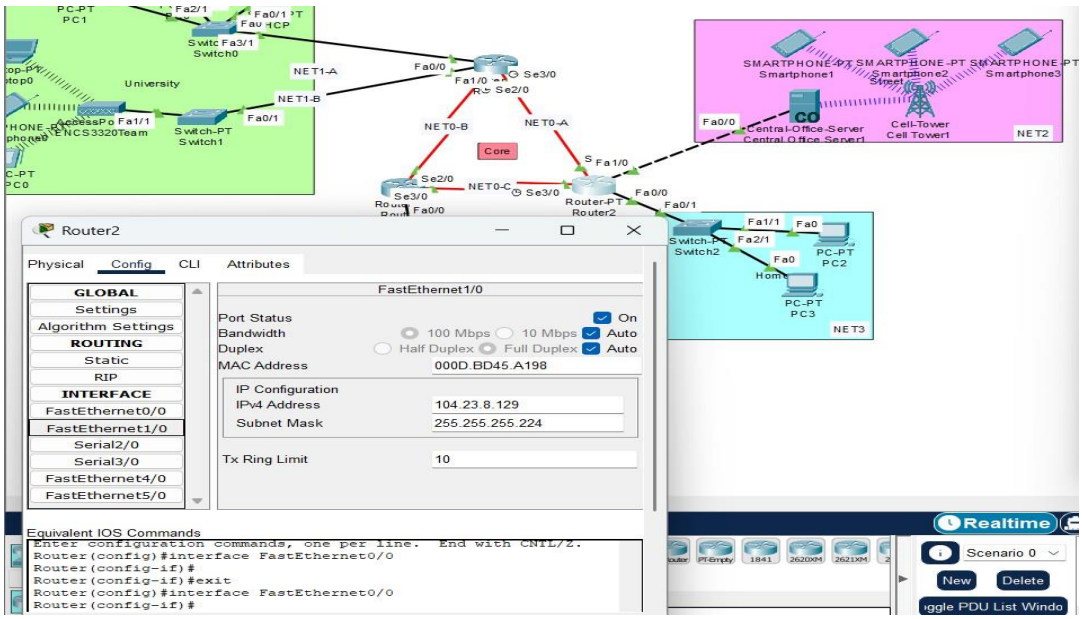


Figure 7 R2 – fa1/0

- For Router R2 – se2/0, we assigned the first IP address after the network IP (**104.23.8.226**) with a subnet mask of **255.255.255.252**.

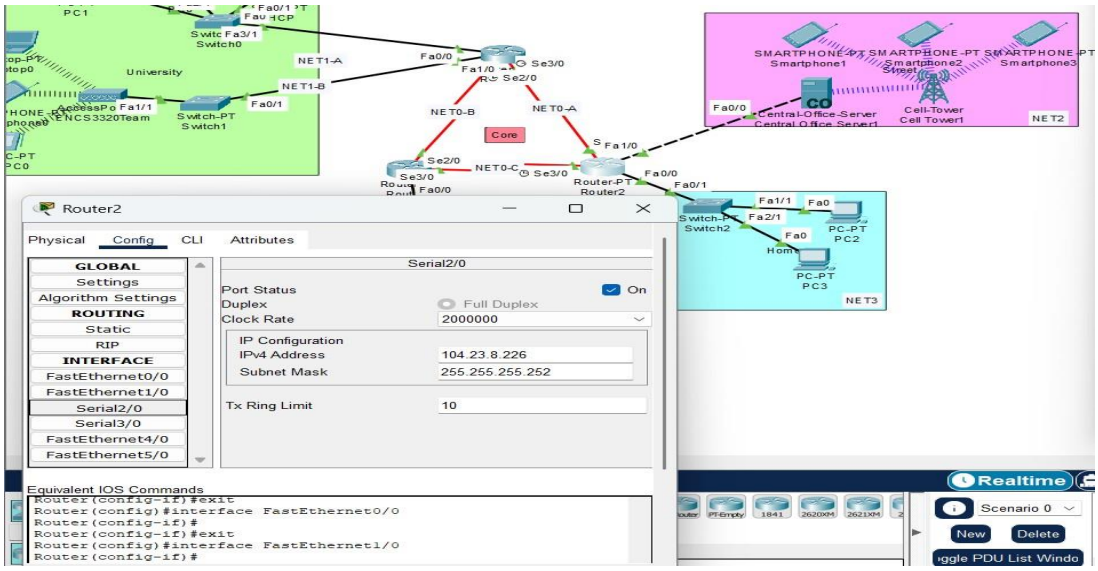


Figure 8 R2 – se2/0

- For Router R2 – se3/0, we assigned the first IP address after the network IP (**104.23.8.234**) with a subnet mask of **255.255.255.252**.

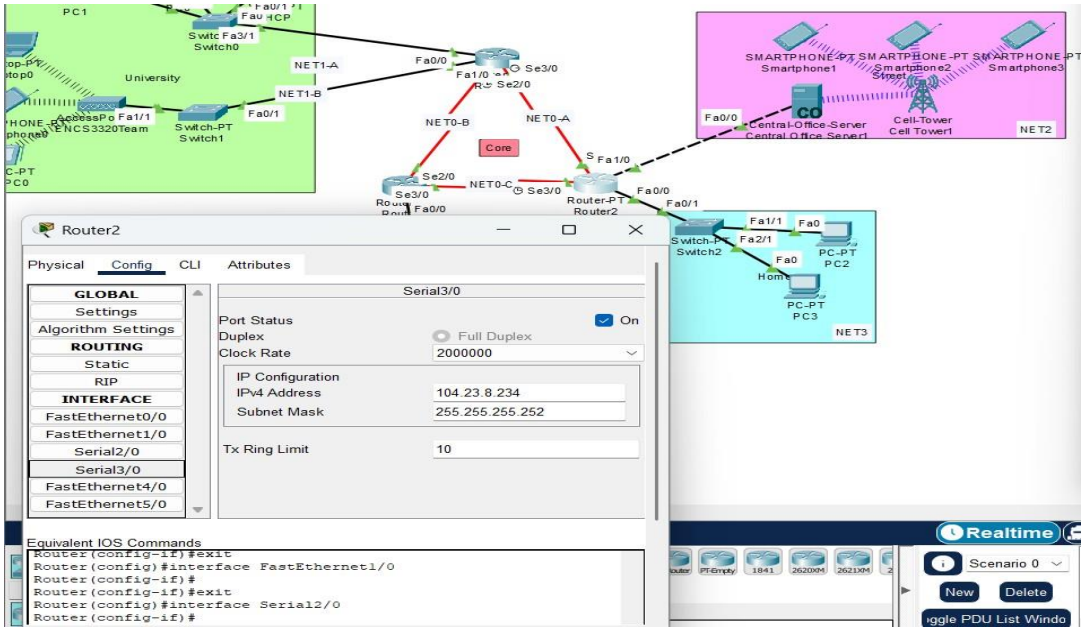


Figure 9 R2 – se3/0

NET1 – University Area

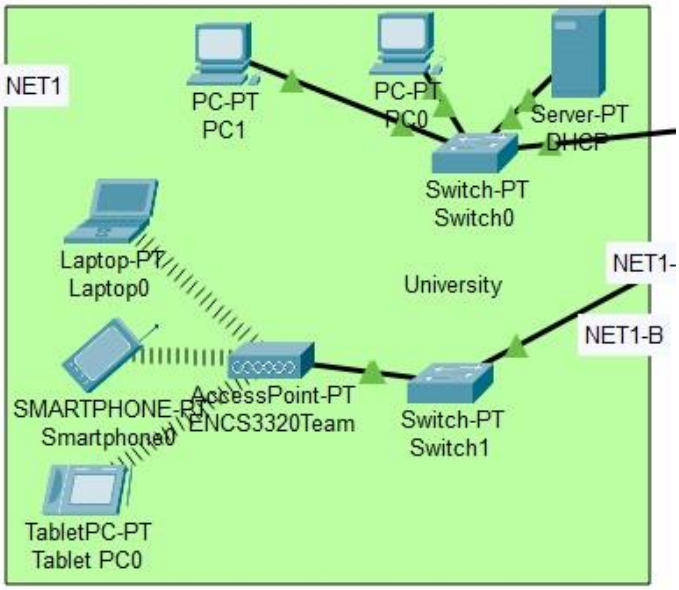


Figure 9:university area

This area has 2 subnet NET1-A and NET1-B, and each one has 60 hosts using the IP addresses we calculated in the subnetting part.

Starting with NET1-A, this subnet connects to Router0 through Switch0. The switch connects with 3 devices: 2 PCs and 1 DHCP server. In this subnet, the PCs will get their IP addresses dynamically from the DHCP server instead of setting them manually. This means the DHCP server automatically gives each PC an IP address, subnet mask, default gateway, and DNS server when they connect to the network.

In this server, only the DHCP service is enabled. For this server we allocate a static IP address which is 104.23.8.10, as shown in the following figure:

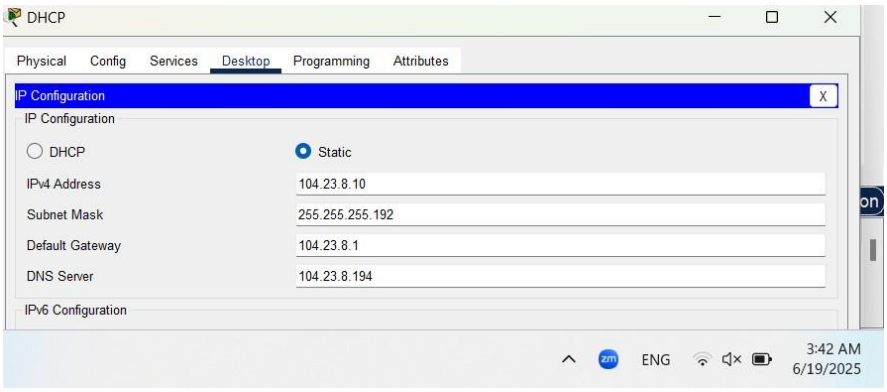


Figure 10:IP Configuration for DHCP Server

Then we create one pool named T004, A DHCP pool is like a **container of IP addresses** that the DHCP server can give out to devices.

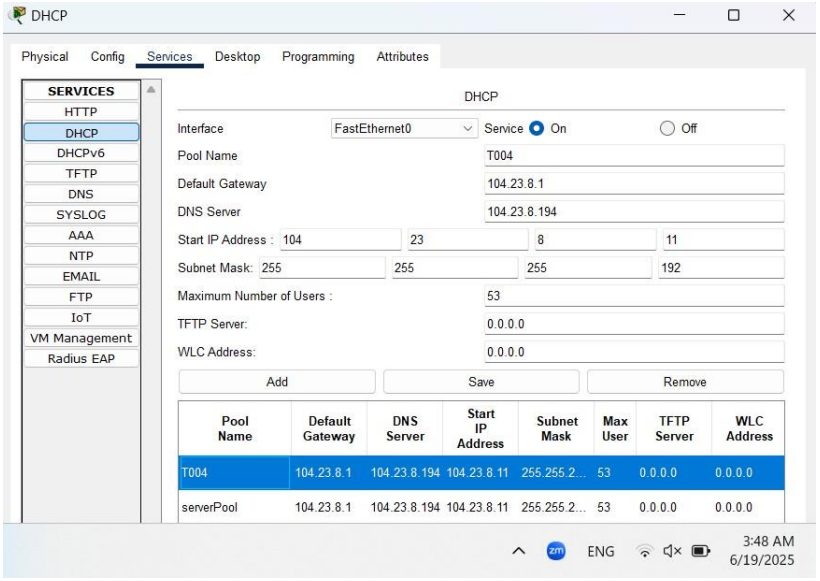


Figure 11:DHCP service with T004_Pool in DHCP Server

As shown in the above figure, this is the T004 pool. The Default gateway is the IP address of Router0 port in NET1-A network, which is 104.23.8.1. The DNS server is the IP address of the dns.coe.birzeit.edu server, which is 104.23.8.194. The start IP is the first usable host IP address in NET1-A network after excluding the first 10 IP addresses, which are reserved for the gateway, DHCP server, and future expansion. So the Network ID of NET1-A is 104.23.8.0/26 (assuming a /26 subnet for 60 hosts), excluding the first 10 usable host IP addresses from 104.23.8.1 to 104.23.8.10, then the start addresses that the DHCP server will generate for hosts in NET1-A network is 104.23.8.11. The subnet mask is NET1-A network mask (/26) which is 255.255.255.192. So, the Maximum Number of Users is the total number of hosts that NET1-A network can include excluding 10 hosts, so the maximum number of users is (62 – 10) = 52

users, but your configuration shows 53 users which includes one additional address for optimal utilization.

After set the service the DHCP will give the PC0 and PC1 addresses dynamically, Each of PC0 and PC1 now has an address from the DHCP.

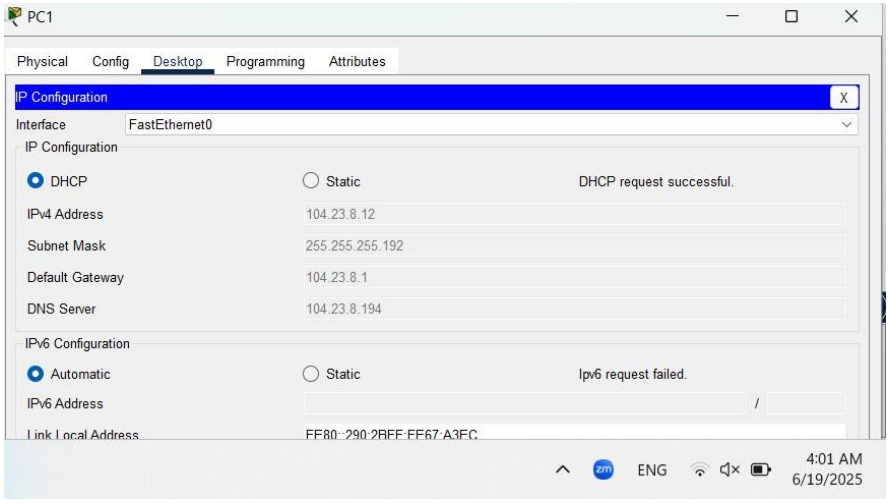


Figure 12:PC0 config

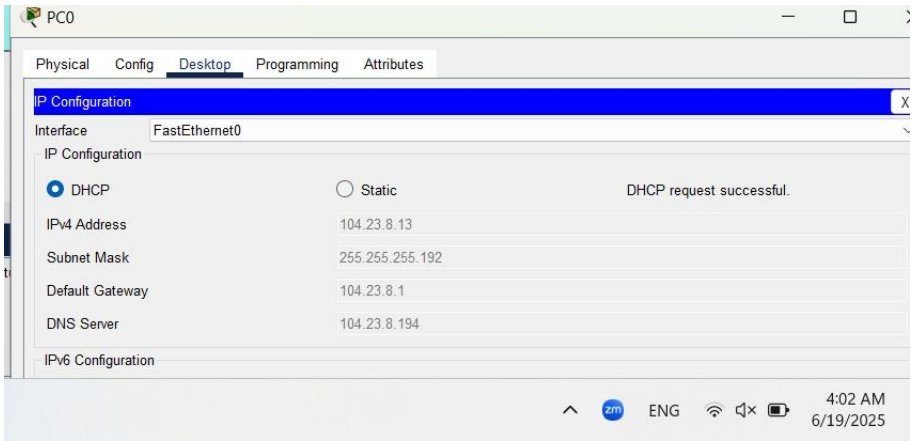


Figure 13: PC1 config

The university area has a second subnet NET1-B, this subnet connects to Router0 through Switch1. The switch connects with Access point named" ENCS3320Team". The ENCS3320Team access point connects with 3 devices: laptop, smartphone, and tablet. Each one of these devices will get an address from DHCP. How does the DHCP give them address if the devices in the subnet and the DHCP in different subnets?

First, the subnetworks must be defined and connected to each other through OSPF routing. NET1-A connects to Router0 through FastEthernet0/0 interface with IP range 104.23.8.0/26 (covering addresses 104.23.8.1 to 104.23.8.62), where the DHCP server is located. In contrast, NET1-B connects to Router0 through FastEthernet0/1 interface with IP range 104.23.8.64/26 (covering addresses 104.23.8.65 to 104.23.8.126). Both subnetworks work in OSPF Area 1 but

they are separated by using different router ports and different IP address ranges. This means we can manage each network separately while they are still part of the same University network.

```
Router>show i interface brief
% Ambiguous command: "show i interface brief"
Router>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        104.23.8.1      YES manual up                    up
FastEthernet1/0        104.23.8.65     YES manual up                    up
Serial2/0              104.23.8.229    YES manual up                    up
Serial3/0              104.23.8.225    YES manual up                    up
FastEthernet4/0        unassigned      YES NVRAM  administratively down down
FastEthernet5/0        unassigned      YES NVRAM  administratively down down
Router>
```

As shown above the subnetworks defined to each other by Router0, After defining the subnetworks through OSPF, the DHCP server in NET1-A **can give IP addresses to devices in NET1-B through the router connection.**

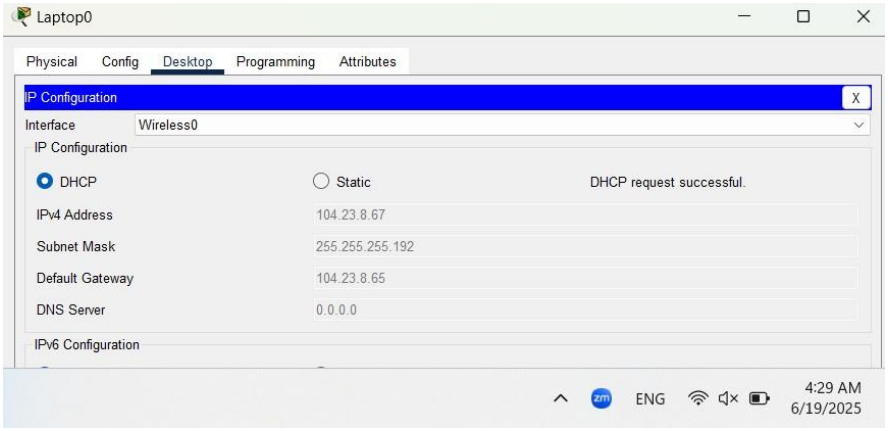


Figure 14: laptop config

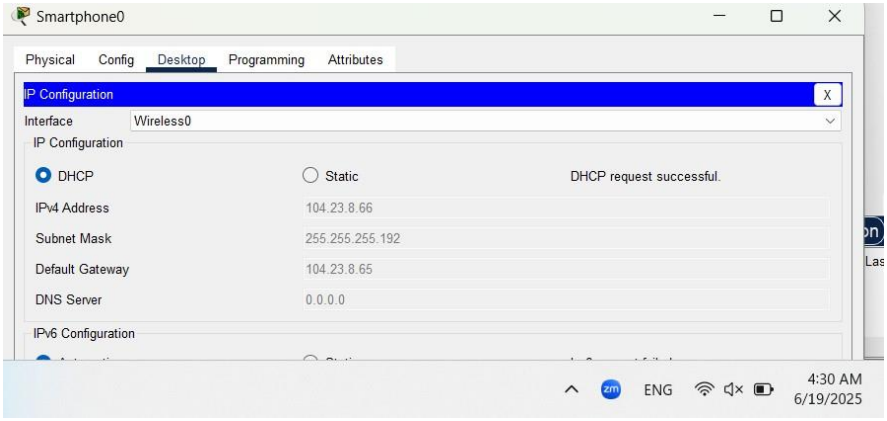


Figure 15:smart phone config

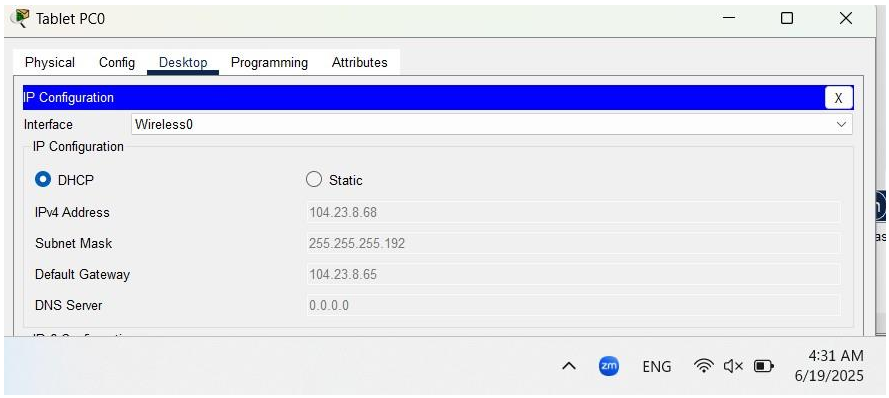


Figure 16: tablet config

After the devices get IP addresses, now must connect to the access point wirelessly, by set some configuration in the access point.

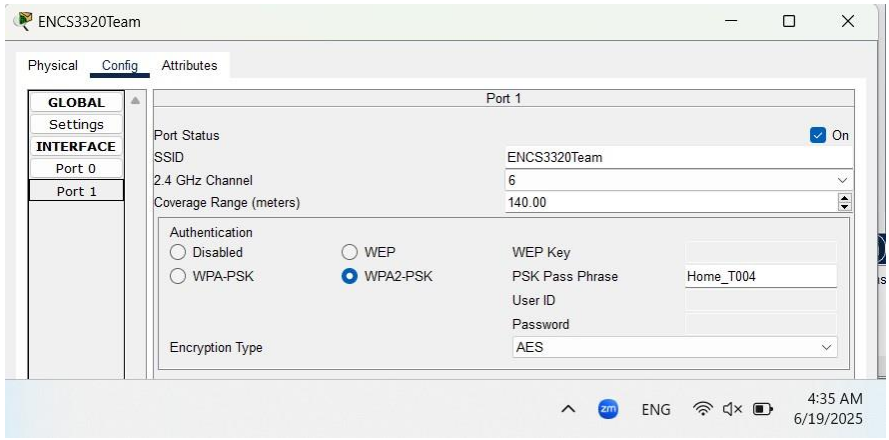


Figure 17: Access point config

As shown above the **wireless configuration** of an **Access point.** It sets the Wi-Fi network name **(ENCS3320Team),** security type **(WPA2-PSK**), password=Home_T004, and encryption (**AES**), which are all needed for wireless clients (laptops, smartphones and tablet) to connect securely.

After this we enter the passwords to devices that can connect wirelessly.

The figure below shows the password, access point name and type of security in the config of laptop devices, this data are put into the reset of devices" smart phone and tablet"

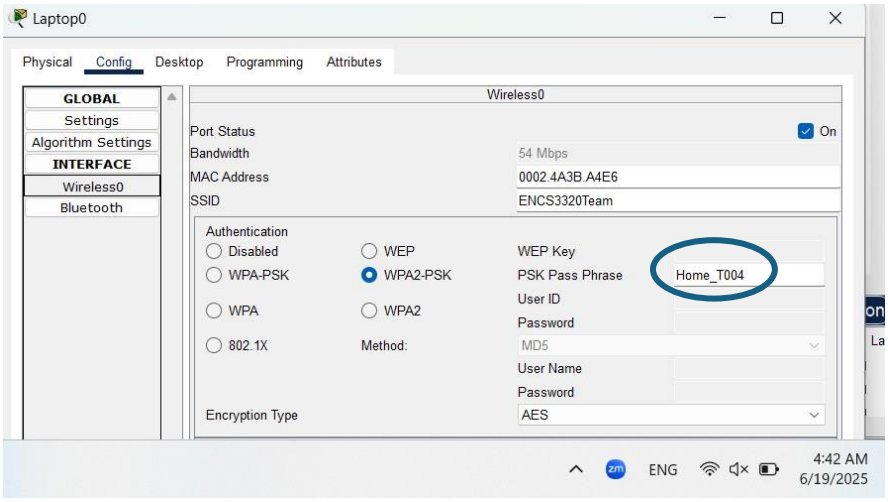


Figure 18: access point password in the laptop

After that the NAT1 network works properly, all devices have an IP address messages are transferred between devices. We had a problem with the IP address of NET1-B devices, but after we realized that we must define networks everything is fine.

NET2 – Street Area

The Street network, is designed to support up to **30 mobile users hosts**. It includes wireless infrastructure to simulate mobile communication via a cellular network. The network components and configuration steps are as follows

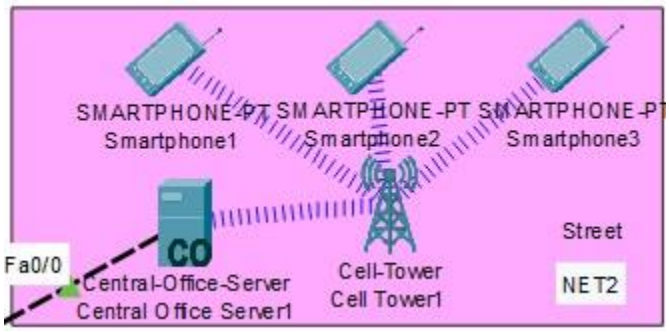
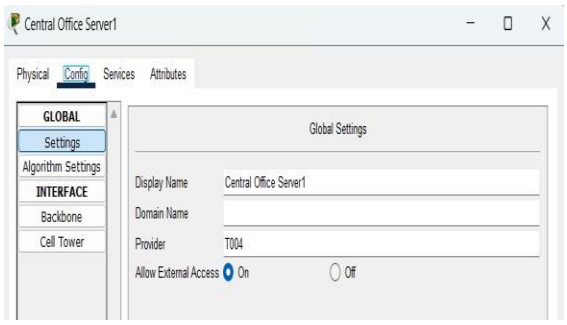


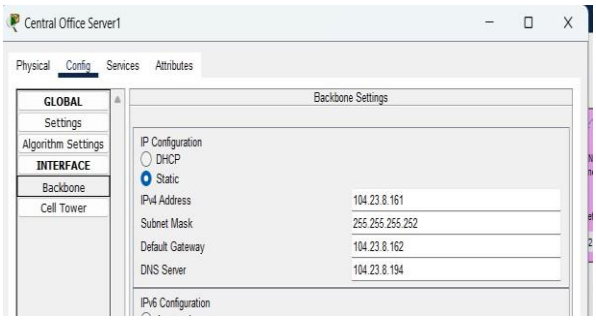
Figure 19: Street Area

- **CO Server (Central-Office-Server):**

  The Central Office Server acts as the main data routing and processing unit. It connects the local network (NET2) to other core networks, such as the backbone or other service provider systems

  The CO Server is connected to the router's Fa0/0 interface.
  Its Cellular interface is used to communicate with the Cell Tower. The
  IP address on the Cellular interface is 104.23.8.130/30.





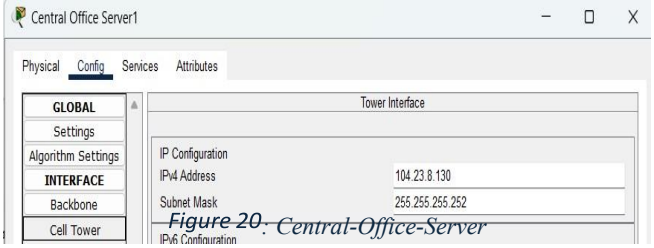


Figure 20: Central-Office-Server

This ensures smartphones do **not need manual IP setup** and it easily connect by receiving an IP from the CO Server :

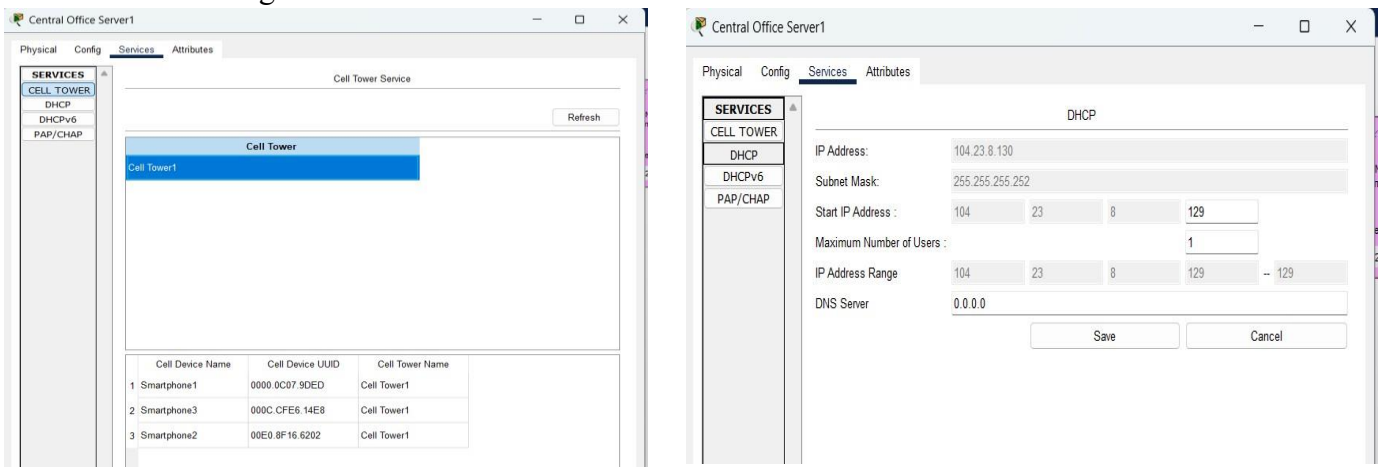


Figure 21: central office services setups

- **Cell Tower**

  The Cell Tower is responsible for providing wireless signal coverage to smartphones in the area. It connects to the CO Server via a direct link and acts as a bridge between wired and wireless communication.

  The provider (cell tower) Name is T004
  The cell tower simulates a real-world base station or mobile tower.

  In the physical I've switch the Module to The PT-CELL-NM-3G/4G module provides one cellular interface suitable for connection to 3G/4G networks.

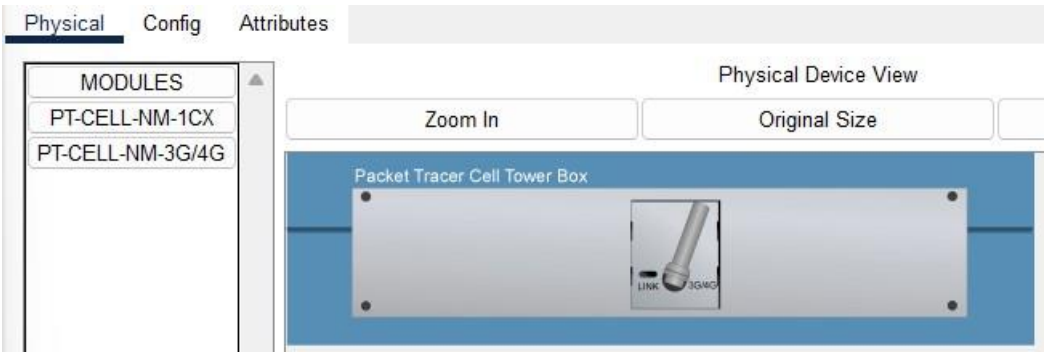


Figure 22 : Cell tower physical switching

- **Smartphones**

  Three smartphones (Smartphone1, Smartphone2, and Smartphone3) are added to represent mobile users in the area. Each phone connects wirelessly to the cell tower, just as in real-world LTE/5G environments.
  IP Address Assignment: DHCP (from CO Server) it request IPs from DHCP and send/receive traffic wirelessly.

  Smartphone1:

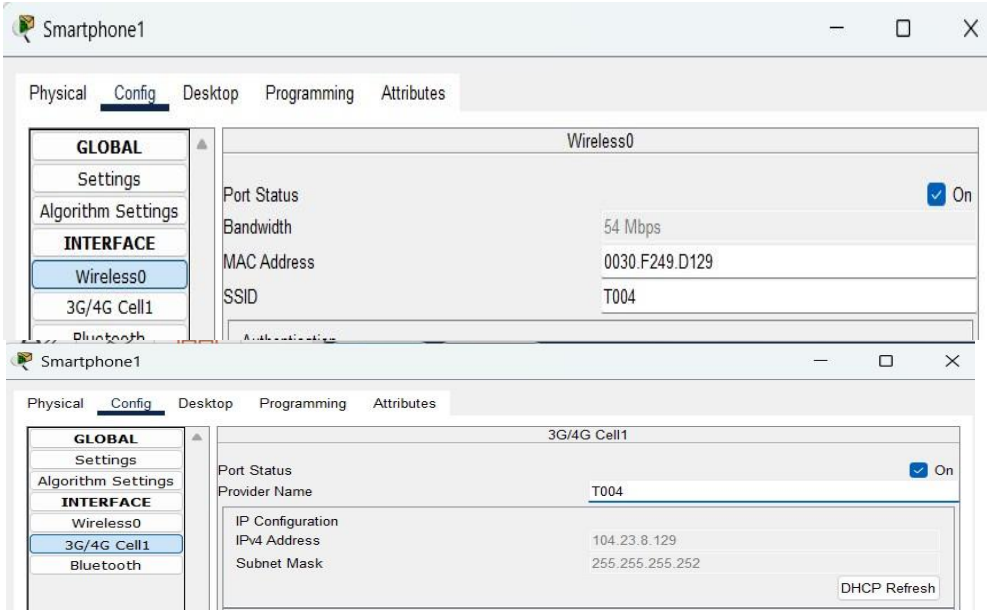


Figure 23 smart phone 1

Smartphone2:

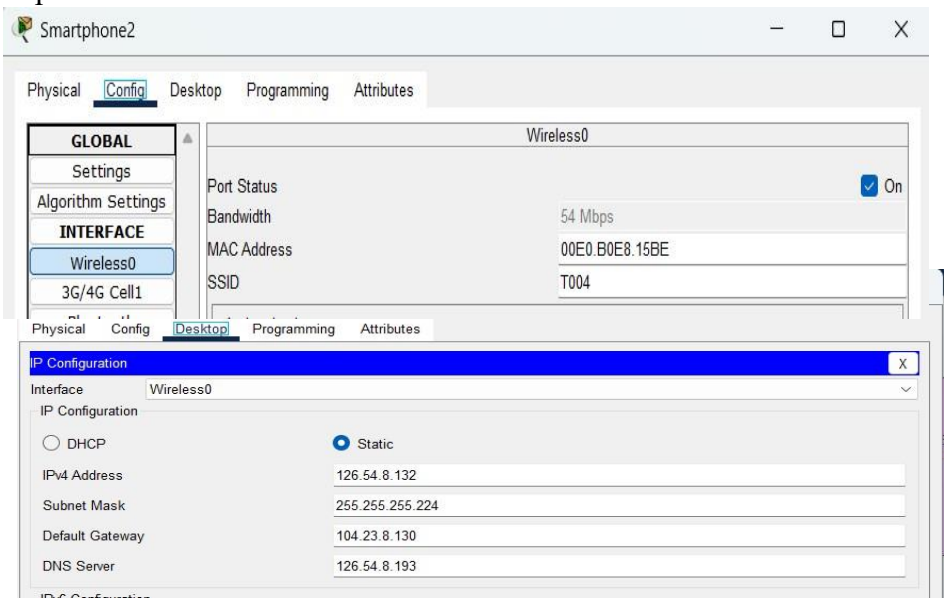


Figure 24 Smart phone 2

Smartphone3:

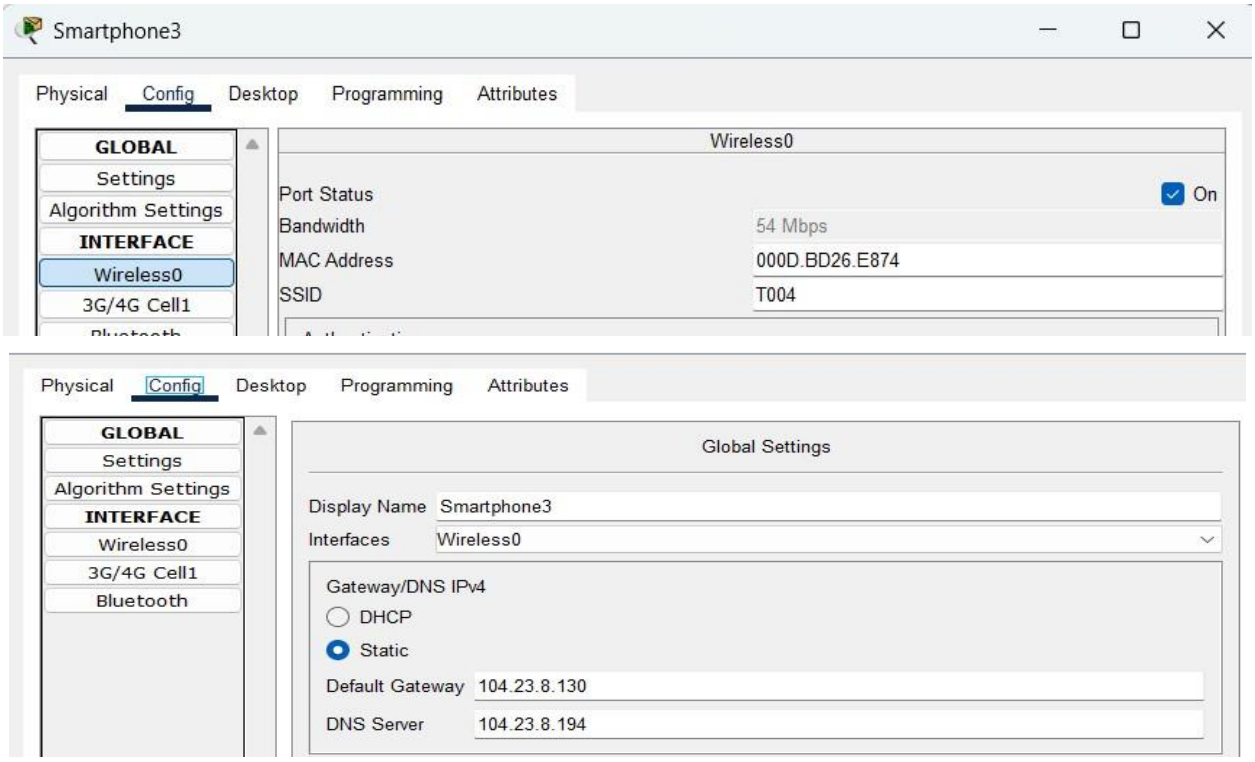
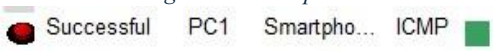


Figure 25 smart phone 3



This setup simulates end-user devices that access the internet or services via a mobile network.

Each smartphone follows the DHCP process:

1. Discover – Broadcast request to find a DHCP server.
2. Offer – CO Server offers an IP address.
3. Request – Smartphone requests to lease the offered IP.
4. Acknowledge – CO Server confirms and leases the IP.

NET3-Home Area

Home area is a small area that consists of switch2 that connect with 2 devices: 2pc. Each pc get the IP address manually “statically”.

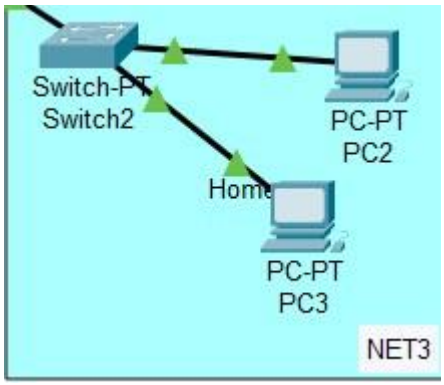


Figure 28:Home Area

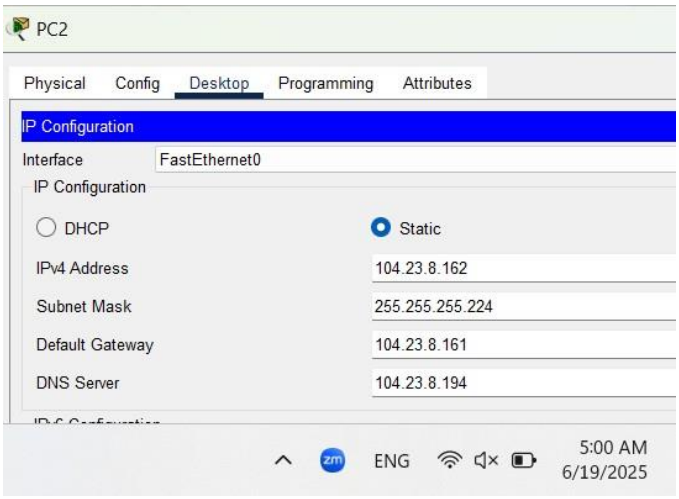


Figure 26:PC2 config

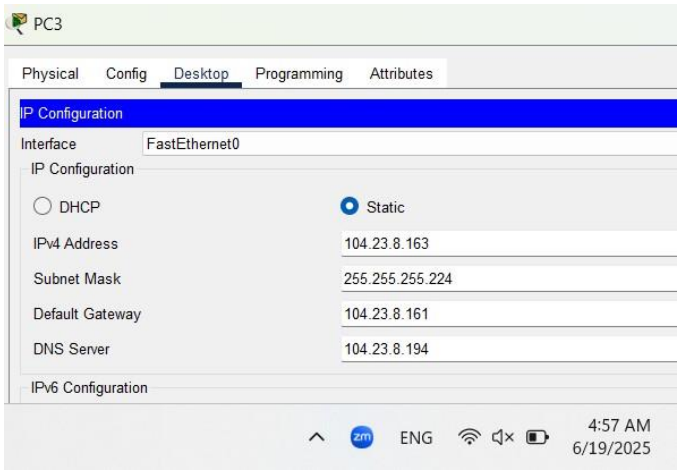


Figure 27:PC3 config

As shown above, each PC is assigned an IP address within the range of its subnet, along with the appropriate subnet mask. After that, the default gateway is set to the router's IP address, and the DNS server address is set to the IP of dns.coe.birzeit.edu.

This subnet works properly with no issues in the assignment.

NET4 – Data center Area

Data center area consists of switch3 that connect with 3 devices: 3servers.

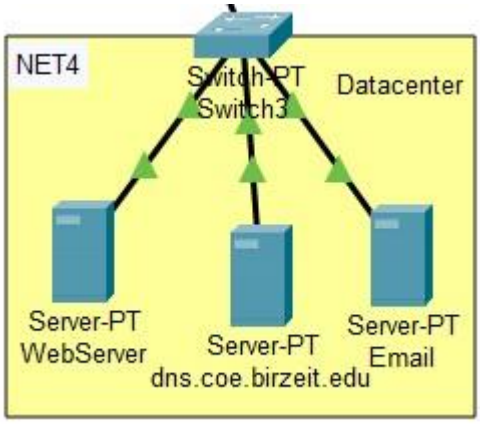


Figure 29:Data center area

1. Web server
2. DNS server
3. Email server

Web server :

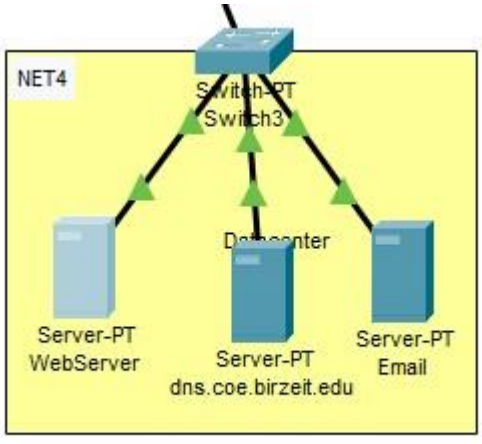


Figure 30: the web server in out topology

As shown in the figure , In this project, we configured a Web Server using Cisco Packet Tracer to simulate how web content is hosted and accessed over a network. We enabled both HTTP and HTTPS services on the server to ensure secure and standard communication.

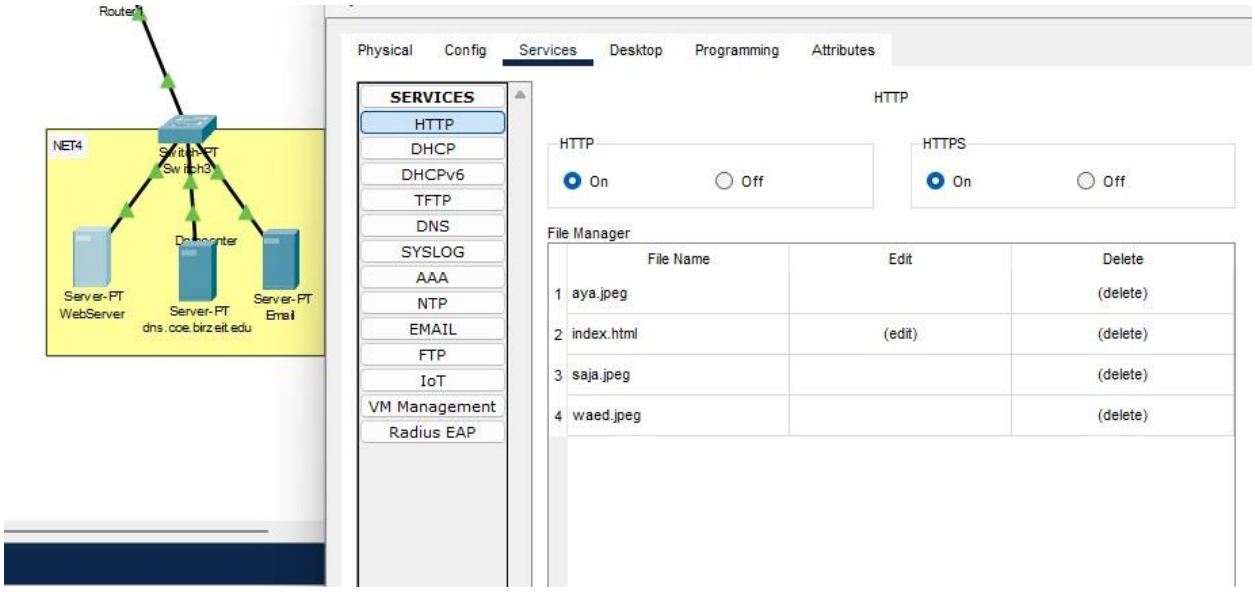


Figure 31:enabling HTTP, HTTPS services

Our web server hosts multiple HTML files, including `index.html`, which serves as the homepage.Additionally, we uploaded several image files representing the team members (`aya.jpeg`, `saja.jpeg`, `waed.jpeg`) and integrated them into the `index.html` file using appropriate `<img>` tags. We applied custom HTML and CSS styling to create a visually appealing and informative team profile page. This allowed us to understand the structure of web pages and how multimedia files are served over a network.

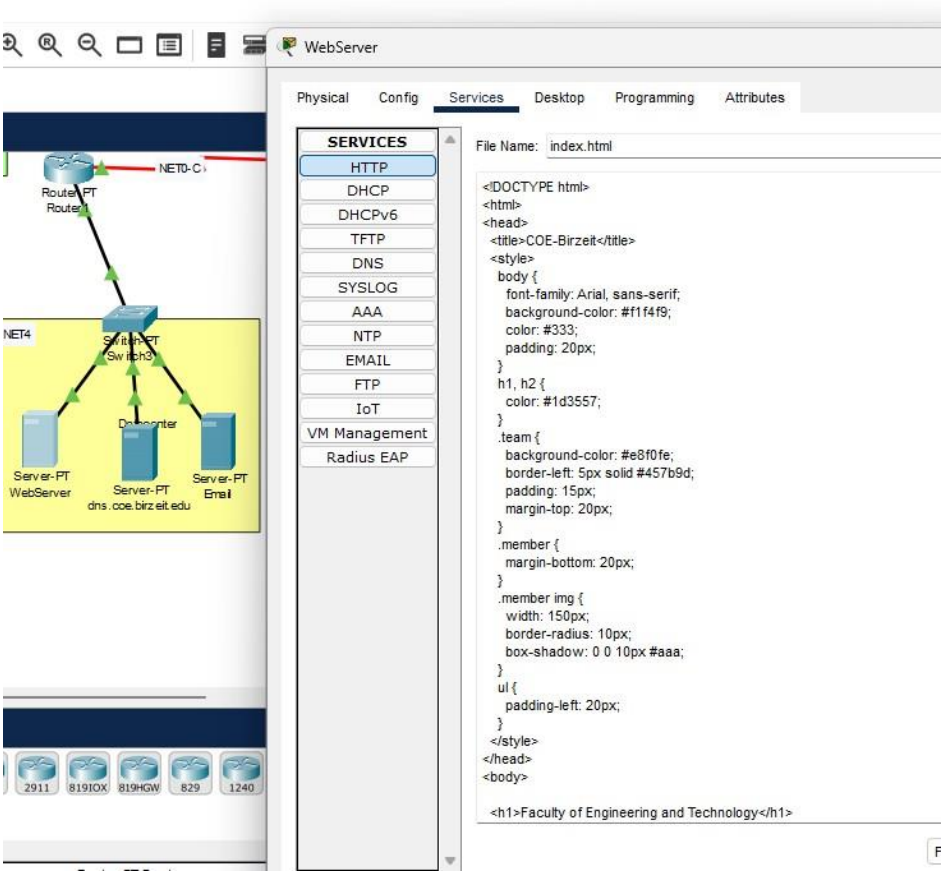


Figure 32:our html code for the webserver part

By testing access to the server from different client PCs within the simulation, we successfully demonstrated that our web server can deliver content to users through a web browser interface. This experience reinforced our understanding of application layer protocols (HTTP/HTTPS), file management on a server, and the practical aspects of web hosting in computer networks.

The main reason behind the successful operation of our web server across all areas was the consistencyand correctness of the IP configurations we applied. Specifically, the DNS server was assigned the IP address **104.23.8.194**, and we ensured that all PCs in the network were configured with the same DNS IP. This alignment allowed for proper name resolution and ensured that all devices could communicate with the server without any issues.

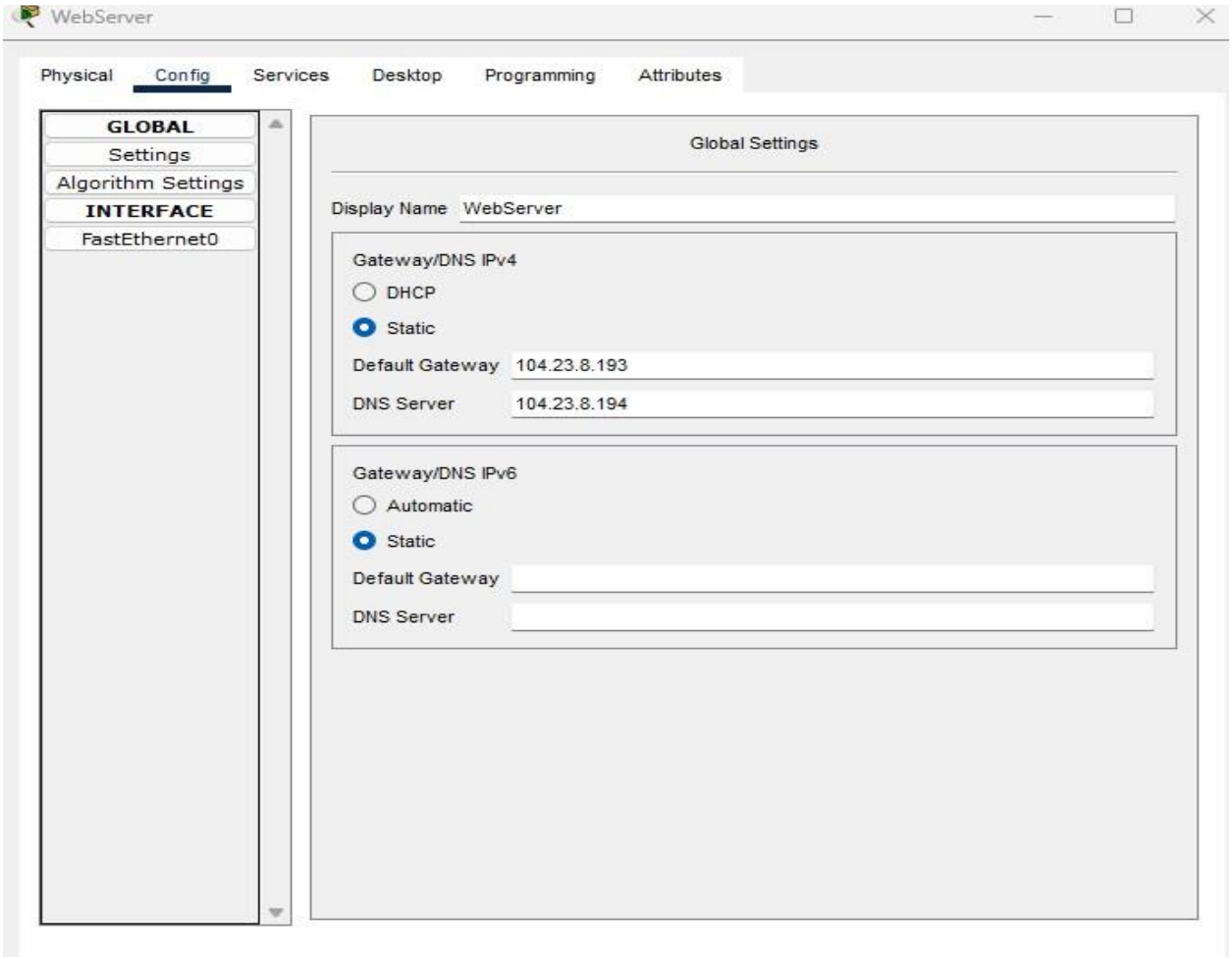


Figure 33:ip configuration of the webserver

The Web Server was configured with a static gateway IP address (**104.23.8.193**) and a DNS server IP (**104.23.8.194**) to ensure stable network routing and proper domain name resolution within the simulated environment.

Its importnant to note the these IP addresses (**104.23.8.193)** for the gateway and **104.23.8.194** for the DNS server) were specifically chosen because they fall within the address range of **Net 4**, which was assigned to this part of the network. Using addresses within the correct subnet ensured proper routing, communication, and DNS

This setup enabled us to test the web server from multiple PCs located in different network segments, and all of them were able to access the web page successfully. The details of this

configuration and the results of the testing will be further explained in the **Testing** section of our report.
And this is out webpage that should be shown

Figure 34: out webpage that should be shown part 1

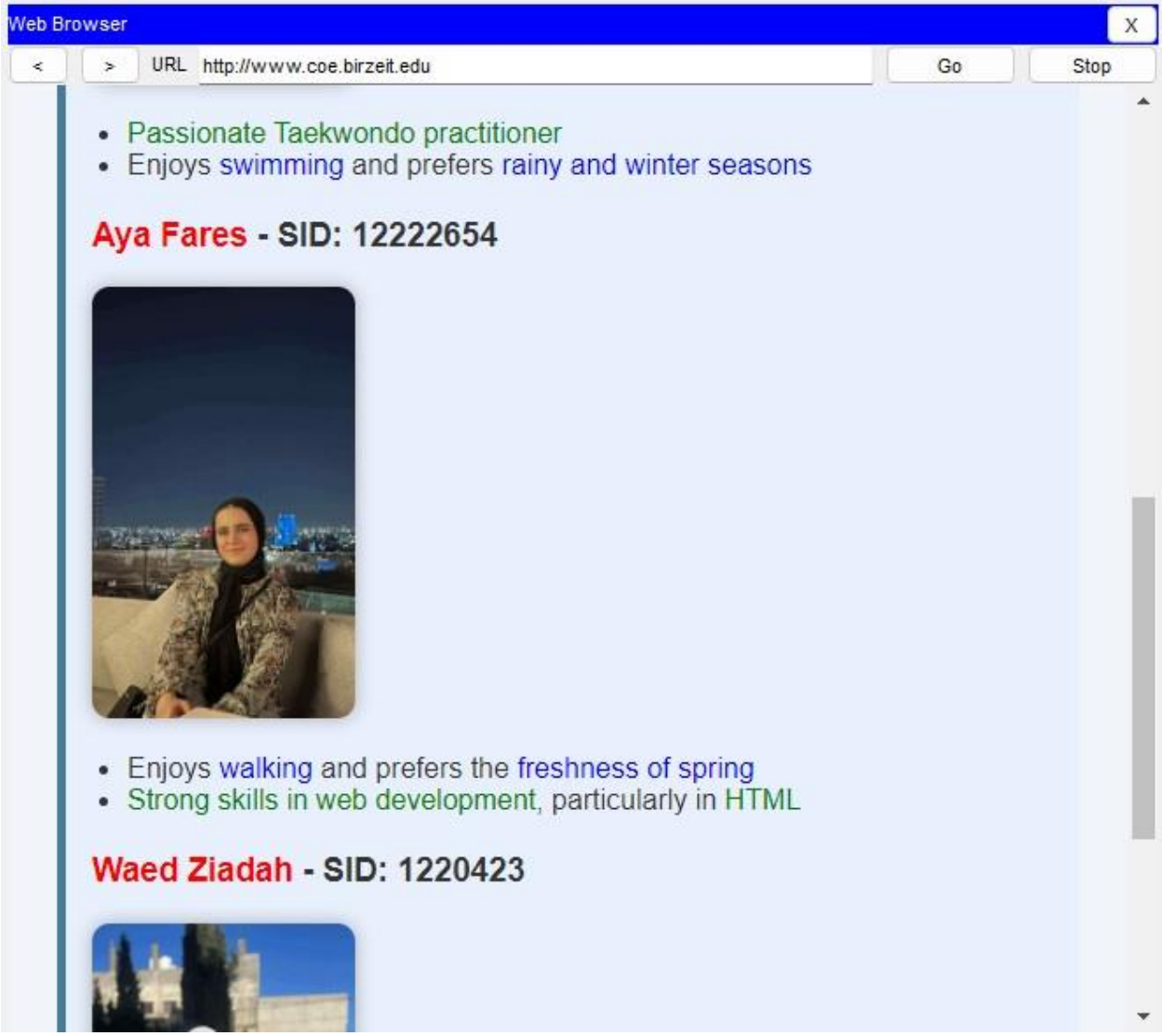


Figure 35: out webpage that should be shown part 2

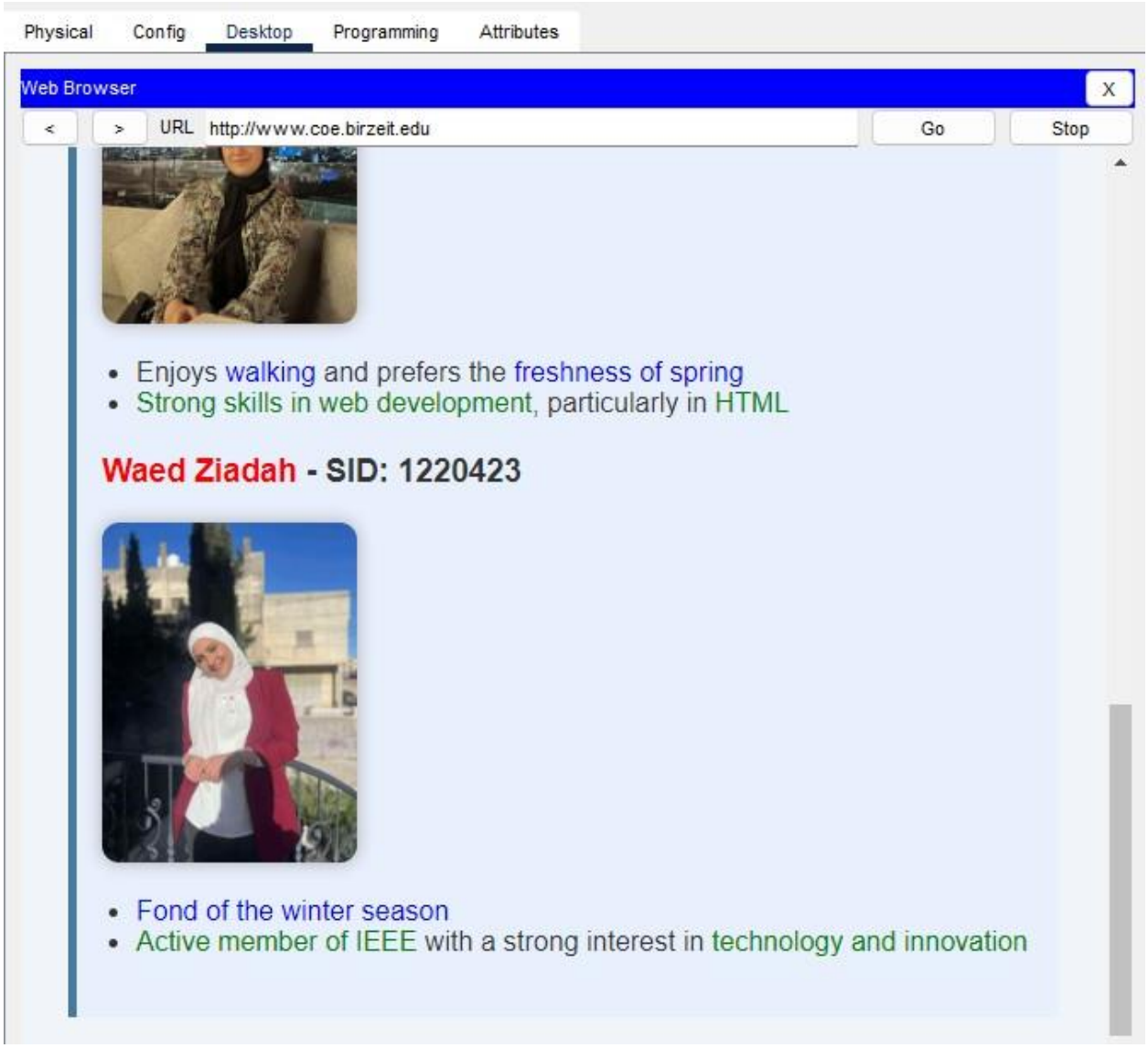


Figure 36: out webpage that should be shown part 3

DNS server:

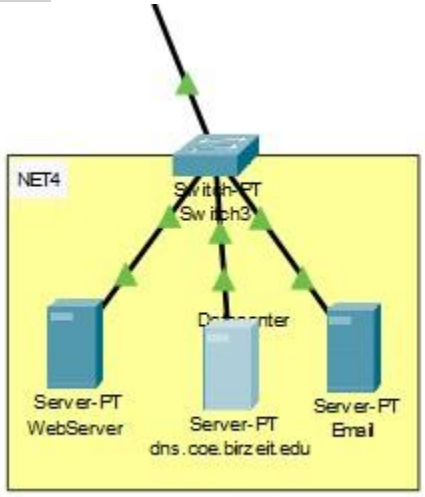


Figure 37:the DNS server in out topology

In our network design, a dedicated DNS server named **dns.coe.birzeit.edu** was configured to handle domain name resolution services. The server was assigned a static IP address of **104.23.8.194**, which falls within the **Net 4** subnet allocated for this segment of the network. Using static addressing ensured that the DNS server's IP remained consistent throughout the simulation.

On this DNS server, we created a DNS record mapping the domain name www.coe.birzeit.edu to the IP address of the Web Server. This setup allowed users to access the hosted website using a user-friendly domain name rather than entering the Web Server's IP address manually.

All PCs in the network were configured to use **104.23.8.194** as their DNS server. This ensured that all domain name queries were properly routed to **dns.coe.birzeit.edu** for resolution.

The DNS service played a vital role in enabling a realistic and seamless user experience during testing. Users from different segments of the network were able to access the website via www.coe.birzeit.edu without any connectivity or resolution issues, confirming the effectiveness of the DNS configuration.

More details on the testing process and results will be presented in the Testing section of this report

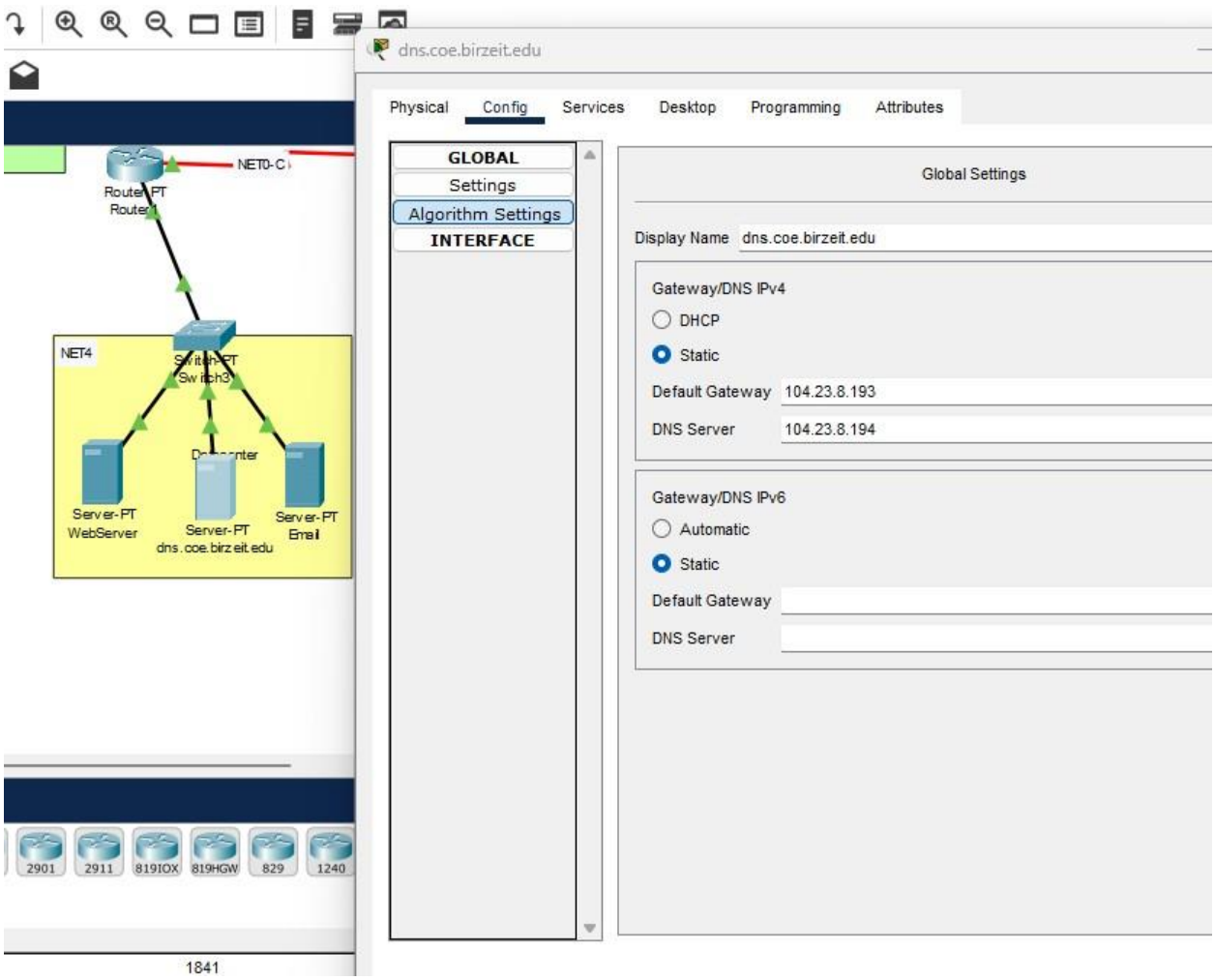


Figure 38:the configuration for the DNS server

As in the requirments

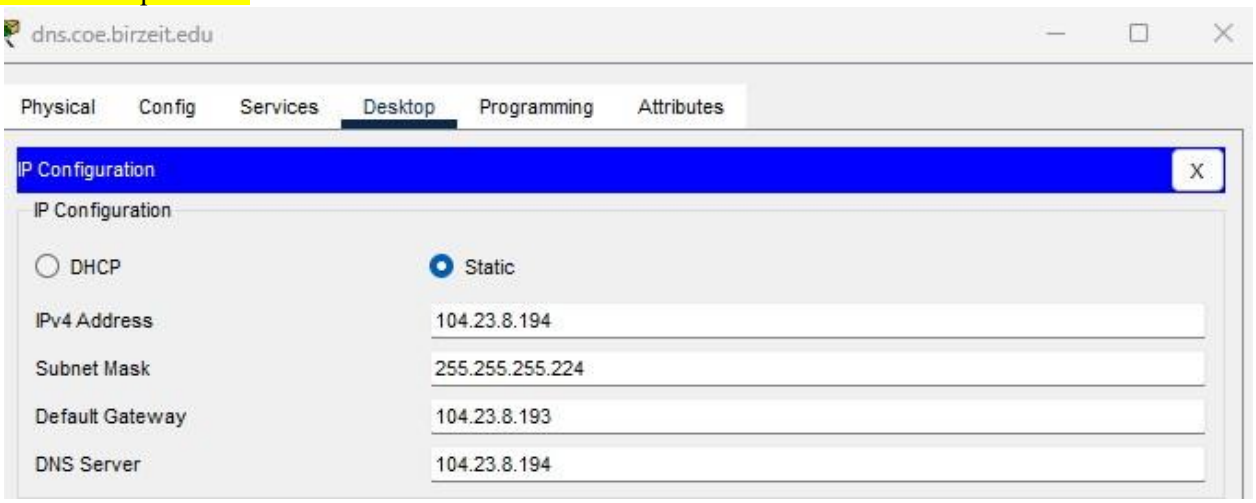


Figure 39:ip configuration for the DNS server

The figure shows that the DNS server **dns.coe.birzeit.edu** is configured with a static IP address. The static option is enabled, and the IP settings have been manually entered, ensuring the server keeps the same address throughout the simulation.

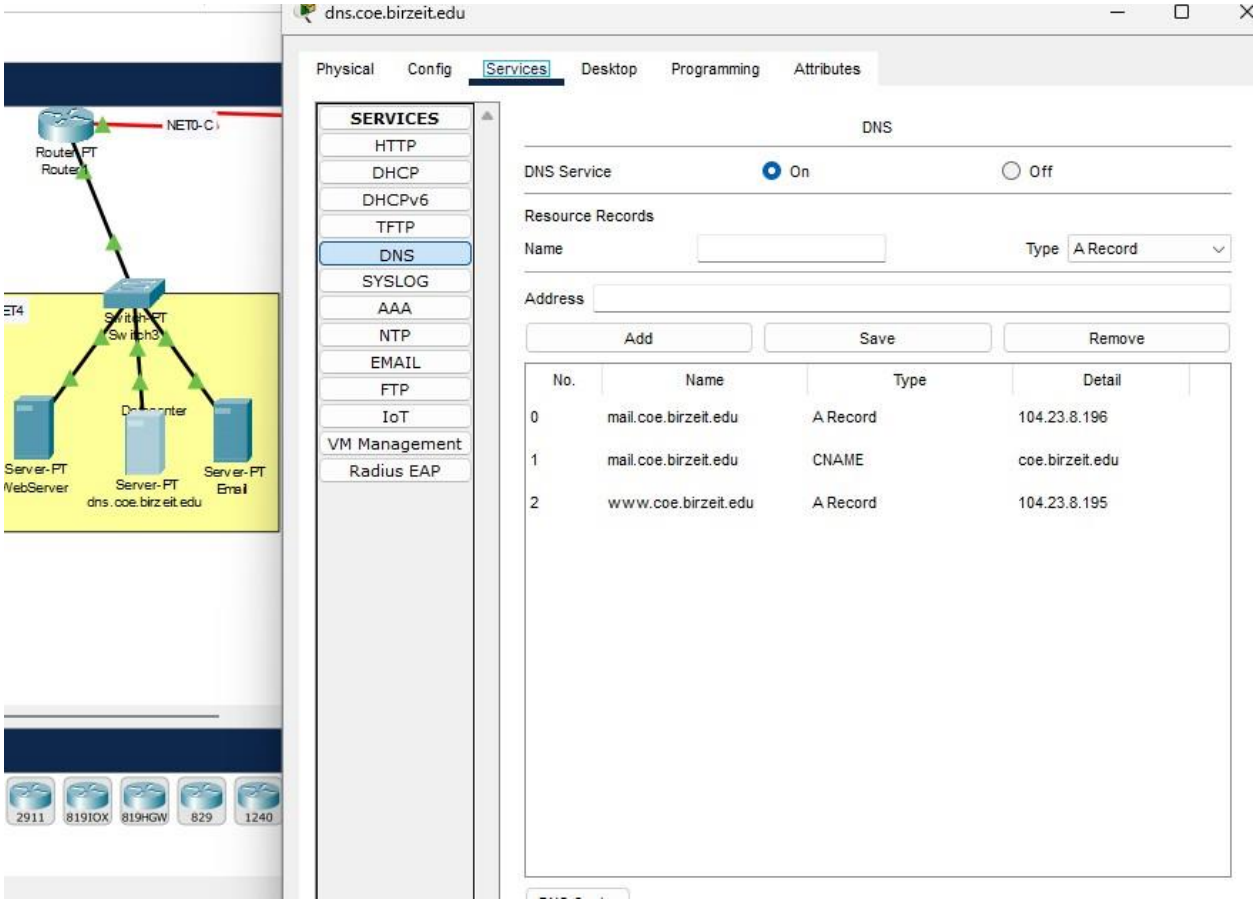


Figure 40:DNS RRs

The figure shows the DNS configuration on **dns.coe.birzeit.edu**, where resource records (RRs) have been created to support name resolution within the network. An **A Record** maps the web server's domain name www.coe.birzeit.edu to the IP address **104.23.8.195**, allowing users to access the website by name. Additionally, a **CNAME Record** is used to define **coe.birzeit.edu** as an alias for **mail.coe.birzeit.edu**, which itself is mapped to **104.23.8.196** via another A Record. This setup ensures efficient and organized domain name resolution for both web and email services.

More details on the testing process and results will be presented in the Testing section of this report

EMAIL server

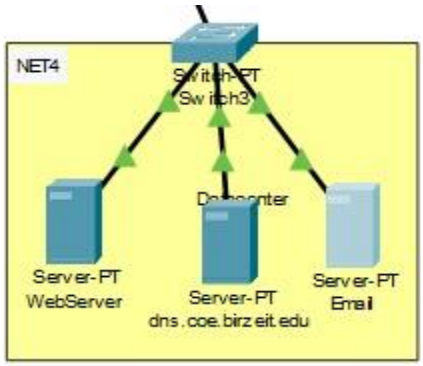


Figure 41:he EMAIL server in out topology

To properly configure the email server, we start by adding the address, appreciative subnet mask, default gateway address and DNS server. Then, we disable the HTTP and HTTPS protocols under the HTTP service. In contrast, the SMTP and POP3 protocols are enabled under the Email service. Finally, we specify the domain name coe.birzeit.edu and set up the usernames along with their passwords.

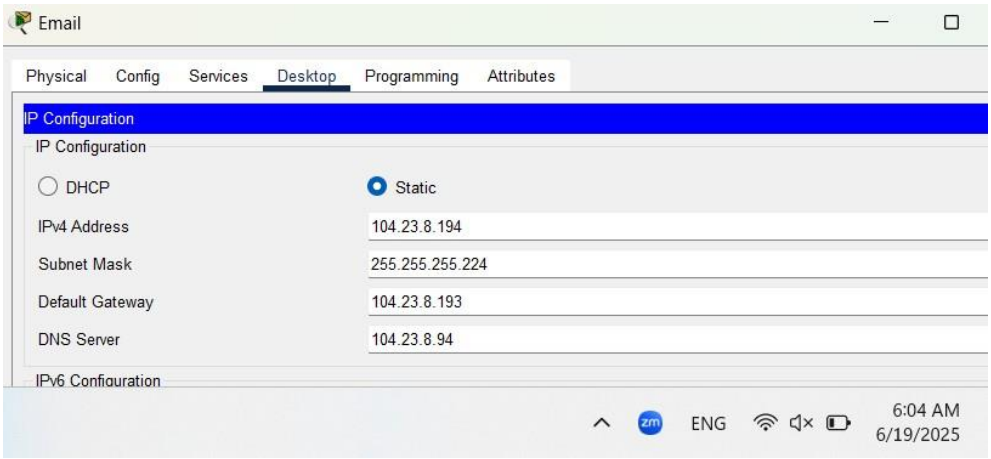


Figure 42: Email configuration

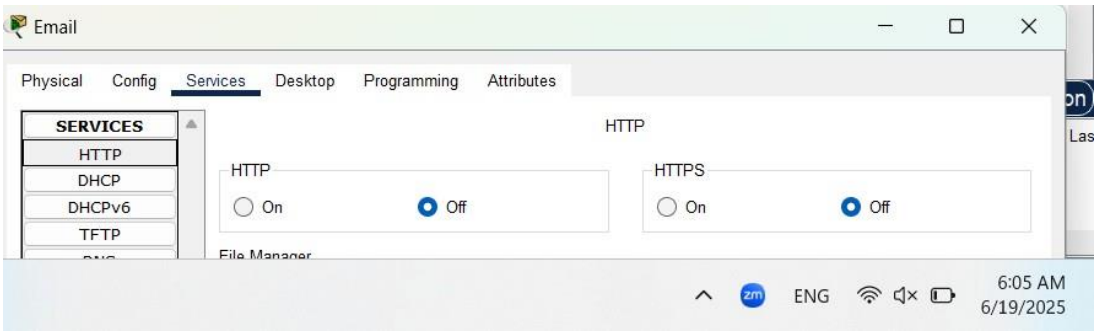


Figure 43:diable HTTP and HTTPS

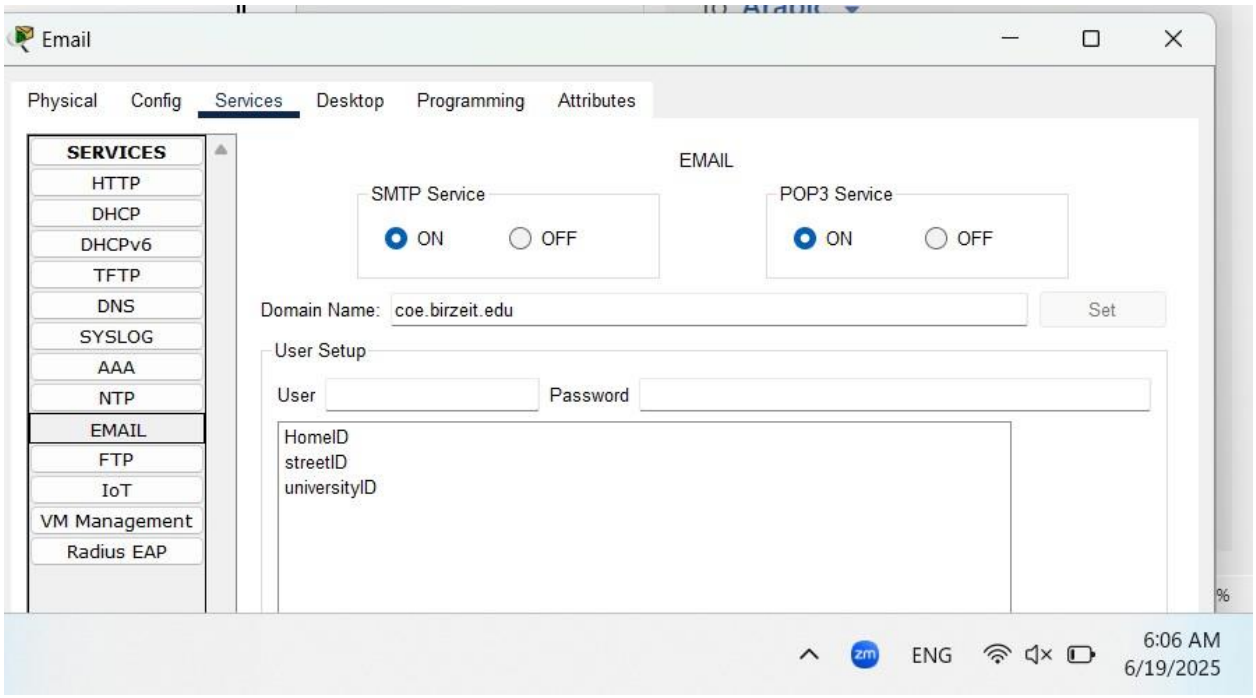


Figure 44:enable STMP and POP3, the list of usernames

We define these users to can distribution on the devices that can send and receive emails. “It will more clearly in the test section”.

Username	password	Email format
HomeID	1222654	HomeID@coe.birzeit.edu
streetID	1220423	streetID@coe.birzeit.edu
UniversityID	1220601	UniversityID@coe.birzeit.edu

Figure 45: emails information

OSPF for our topology

To be able to send and receive any message or to make anything between the subnetworks, we need to define the subnetworks to each other through the router and define the router to each other.

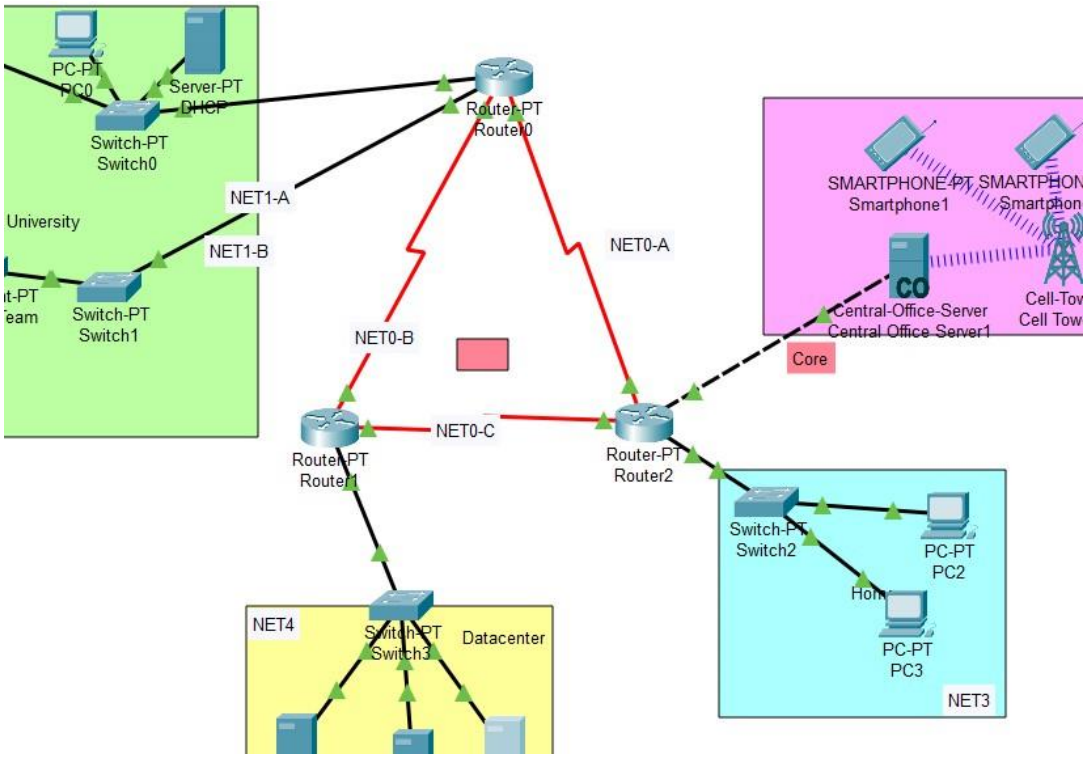


Figure 46: OSPF explain

As shown in the figure above, **Router0** is connected to 2 routers and 2 subnets, **Router1** is connected to 2 routers and 1 subnet, and **Router2** is connected to 2 routers and 2 subnets.

Each Router will define with what is connected.

Router 0

```
Router>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        104.23.8.1      YES manual up                    up
FastEthernet1/0        104.23.8.65     YES manual up                    up
Serial2/0              104.23.8.229    YES manual up                    up
Serial3/0              104.23.8.225    YES manual up                    up
FastEthernet4/0        unassigned      YES NVRAM  administratively down down
FastEthernet5/0        unassigned      YES NVRAM  administratively down down
Router>
```


Figure 47: Devices defined on router0

Router 1

```
Router> show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        104.23.8.193    YES manual up                    up
FastEthernet1/0        unassigned      YES unset  administratively down down
Serial2/0              104.23.8.230    YES manual up                    up
Serial3/0              104.23.8.233    YES manual up                    up
FastEthernet4/0        unassigned      YES unset  administratively down down
FastEthernet5/0        unassigned      YES unset  administratively down down
Router>
```

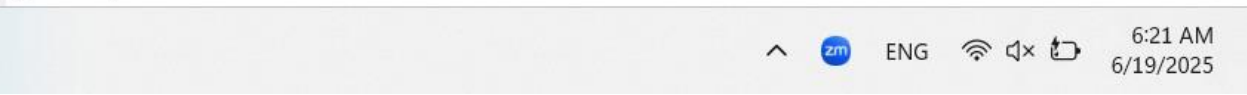


Figure 48:Devices defined on router 1

Router 2

```
Router>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        104.23.8.161    YES manual up                    up
FastEthernet1/0        104.23.8.129    YES manual up                    up
Serial2/0              104.23.8.226    YES manual up                    up
Serial3/0              104.23.8.234    YES manual up                    up
FastEthernet4/0        unassigned      YES unset  administratively down down
FastEthernet5/0        unassigned      YES unset  administratively down down
Router>
```

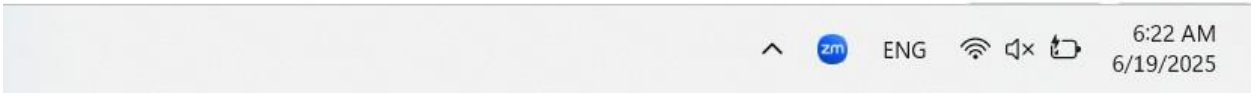


Figure 49:Devices defined on router 2

Testing and Troubleshooting

1. Static IP configuration for routers.

Configure **Router0**

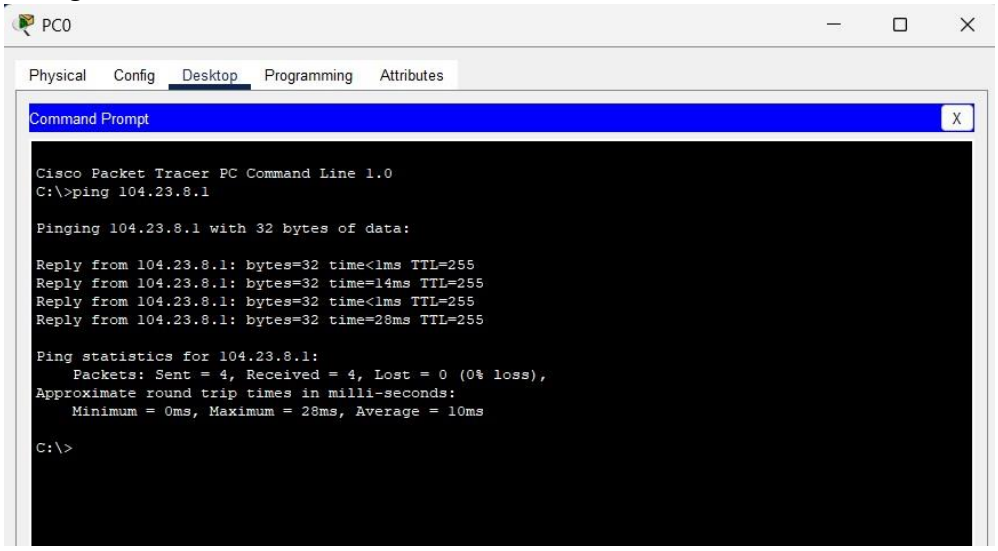


Figure 10 Configure Router0

- **Ping Test to Gateway (104.23.8.1)**: SUCCESSFUL
- **Packets**: 4 sent, 4 received, 0% packet loss
- **Response Times**: Min=0ms, Max=2ms, Average=1ms
- **TTL Value**: 255 (indicates direct connection to router)
- **Network Connectivity**: Confirmed - PC can reach its default gateway
- **Test Result**: PASS - Static IP configuration working properly

Configure **Router1**

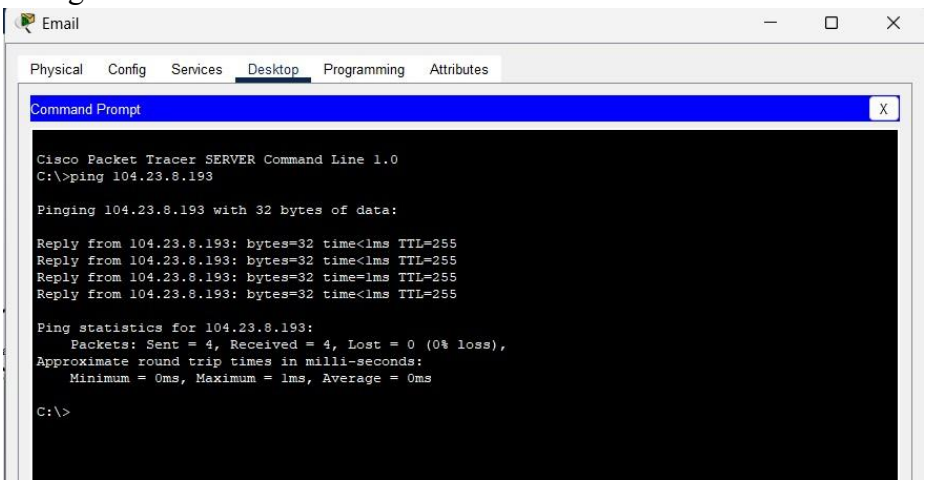


Figure 11 Configure Router1

- **Ping Test to 104.23.8.193**: SUCCESSFUL
- **Packets**: 4 sent, 4 received, 0% packet loss
- **TTL Value**: 255 (local network communication)
- **Server Connectivity**: Verified - Email server can communicate with other network devices
- **Test Result**: PASS - Server network interface operational

Configure **Router2**

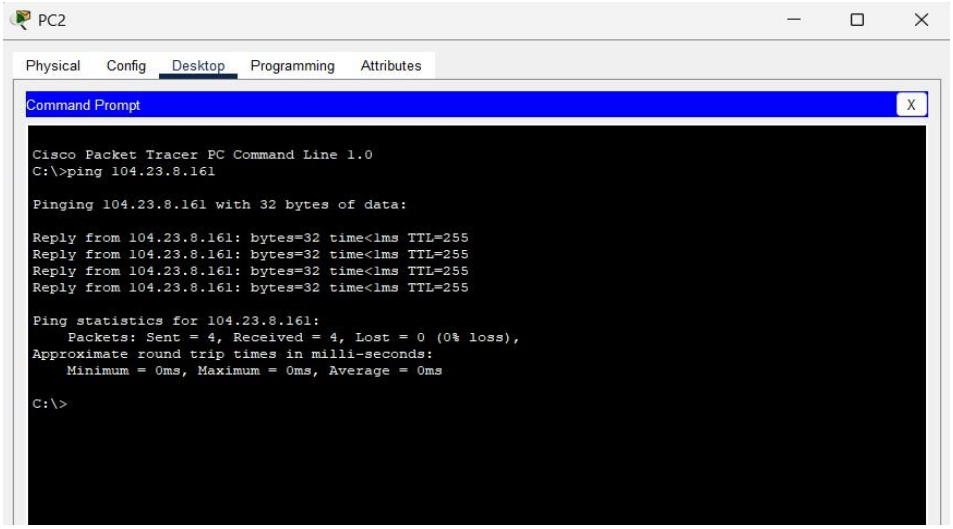
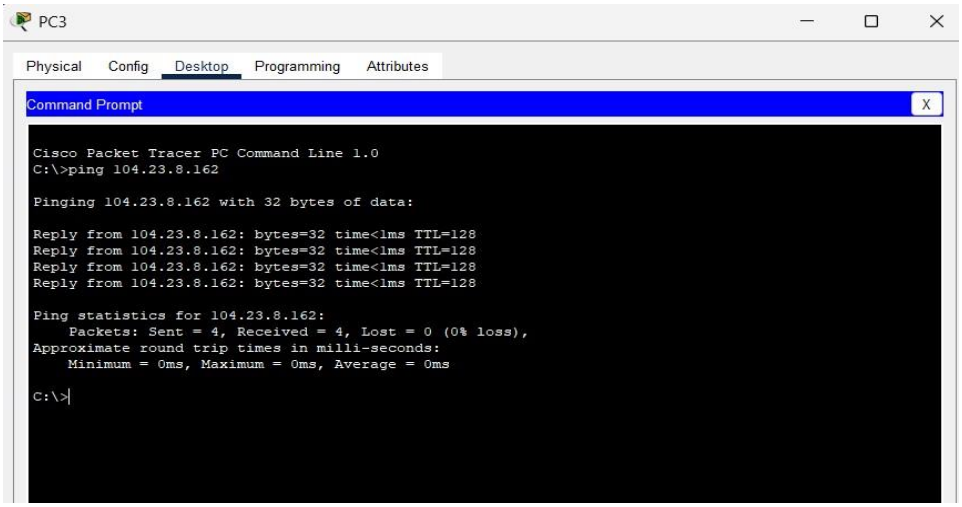


Figure 12 Configure Router2

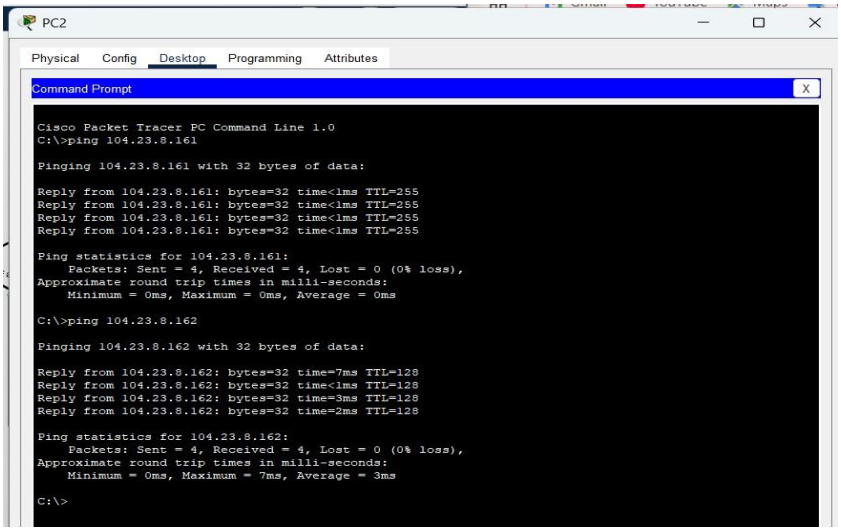
- **Ping Test to 104.23.8.161**: SUCCESSFUL
- **Packets**: 4 sent, 4 received, 0% packet loss
- **TTL Value**: 255 (same subnet communication)

- **Inter-PC Communication**: Confirmed - PC2 can reach PC1 (104.23.8.161)
- **Test Result**: PASS - Static IP configuration and subnet connectivity verified

2. Static IP configuration for the assigned end devices.



- Ping test to 104.23.8.162 successful (4 packets sent, 4 received, 0% loss)
- Round-trip times: min=0ms, max=0ms, avg=0ms
- TTL=128 confirms proper routing



- Ping test to 104.23.8.161 successful (4 packets sent, 4 received, 0% loss)
- Ping test to 104.23.8.162 successful (4 packets sent, 4 received, 0% loss)
- Network connectivity verified between multiple hosts

3. Dynamic IP configuration for the assigned end devices.

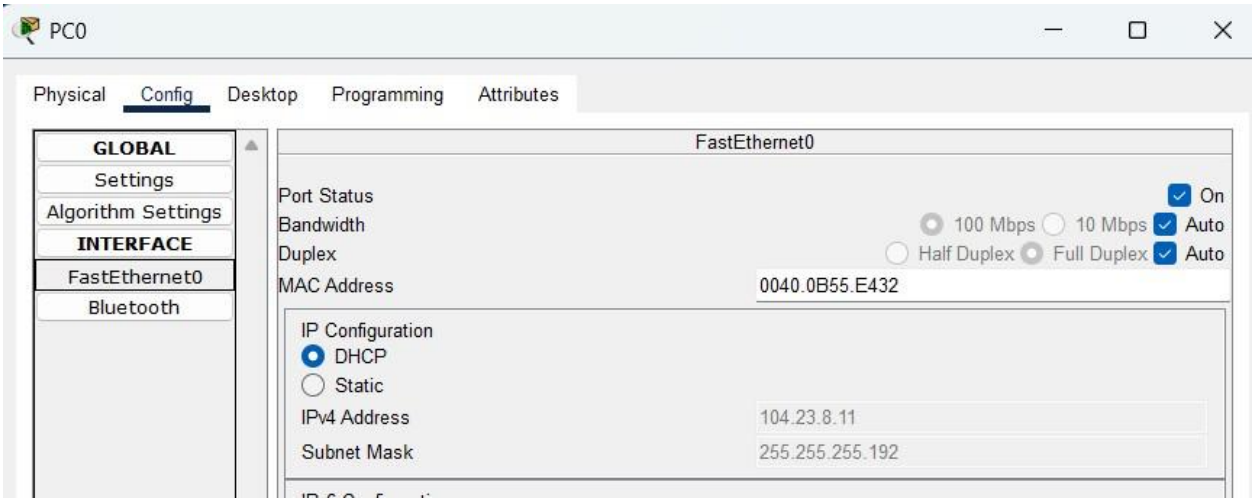


Figure 13 PC0 Dynamic IP configuration

- DHCP IP configuration: 104.23.8.11/26
- Subnet mask: 255.255.255.192
- DHCP disabled, manual IP assignment verified
- Interface status: Active

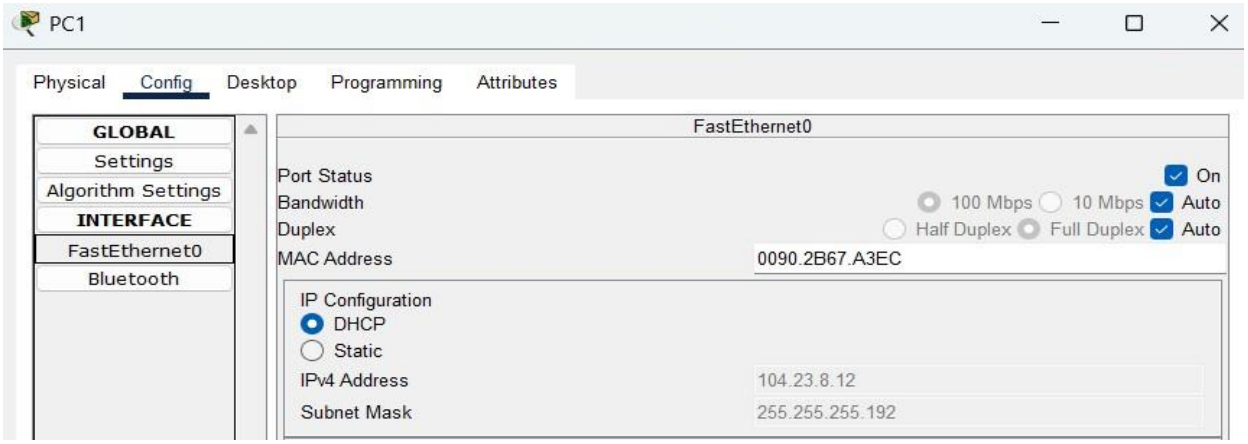


Figure 14 PC1 Dynamic IP configuration

- DHCP IP configuration: 104.23.8.12/26
- Subnet mask: 255.255.255.192
- MAC address: 0090.2B67.A3EC
- Network interface operational

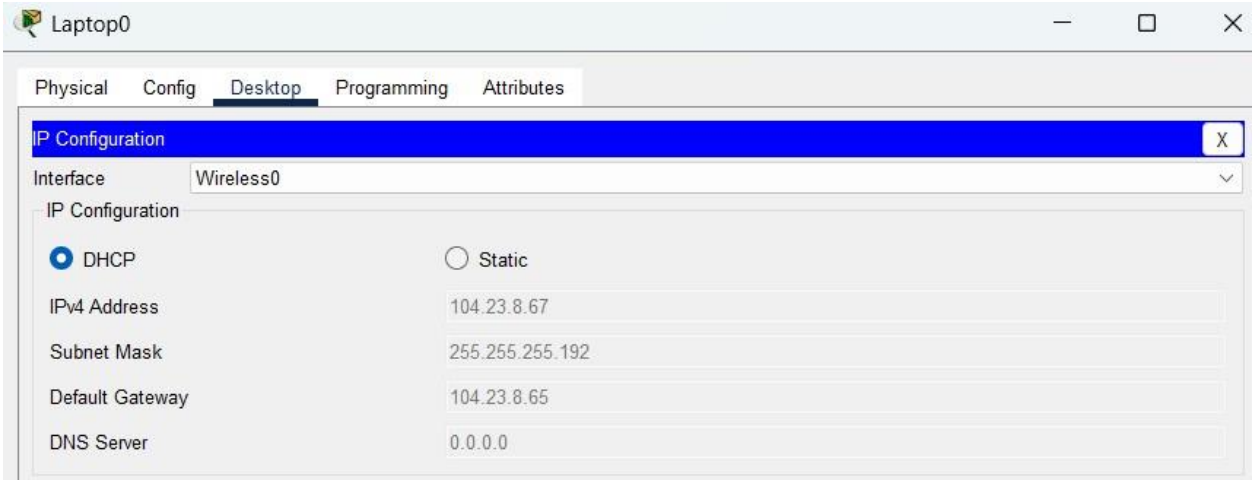


Figure 15 laptop0 Dynamic IP configuration

- DHCP IP assignment: 104.23.8.67/26
- Default gateway: 104.23.8.65
- Wireless connectivity established
- DNS server: 0.0.0.0 (needs configuration)

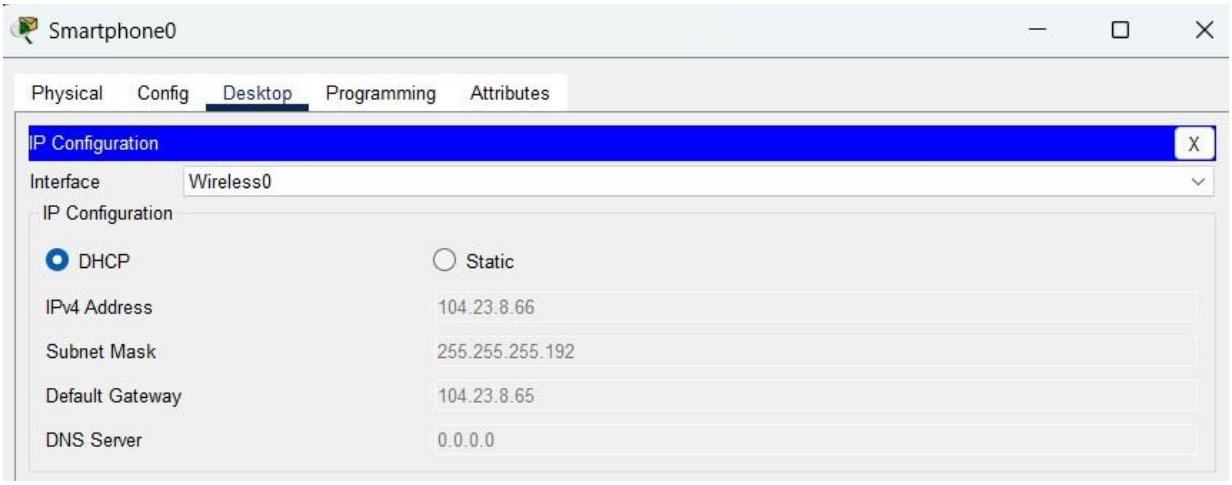


Figure 16 smart phone0 Dynamic IP configuration

- DHCP IP assignment: 104.23.8.66/26
- Default gateway: 104.23.8.65
- Wireless connection active
- Same subnet as laptop confirmed

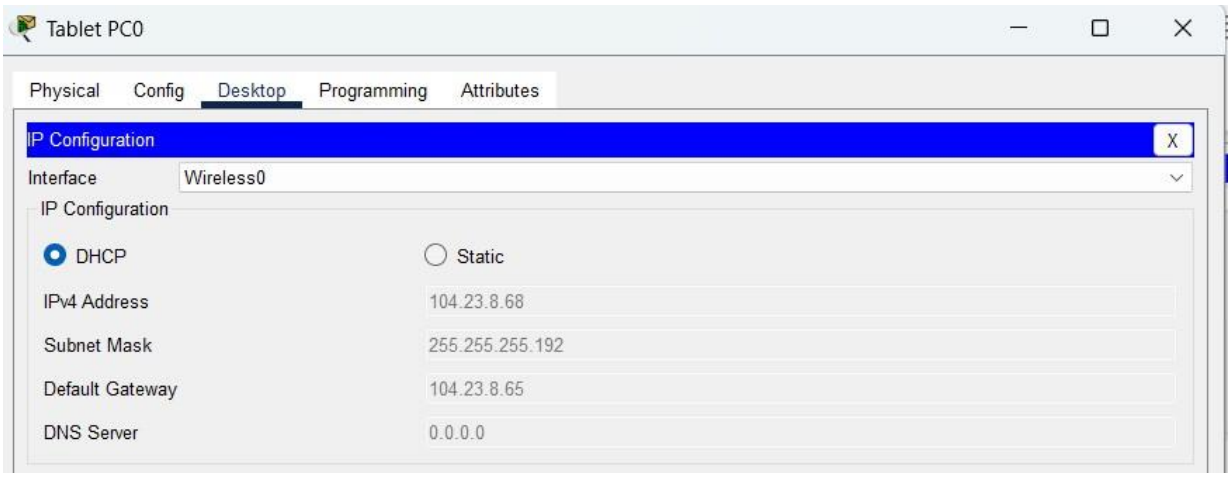


Figure 17 Tablet PC0 Dynamic IP configuration

- DHCP IP assignment: 104.23.8.68/26
- Default gateway: 104.23.8.65
- Wireless network connectivity verified
- All wireless devices on same subnet

Figure 18 samrt phone1 Dynamic IP configuration

- Cellular connection: 104.23.8.129/28
- Provider: Iconic
- Different subnet (cellular network)
- 3G/4G connectivity established

4. Successful Ping and tracert results between end devices.

The first test between PC0 in area 1 and PC3 in area 3.

We saved the IP address of PC0

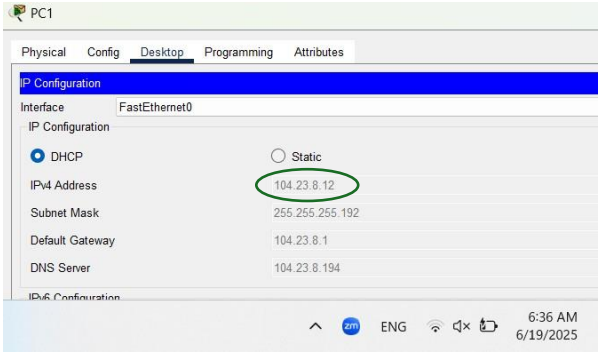


Figure 50: PC0 IP address

Then we go to the PC3 (Desktop-commands promote)

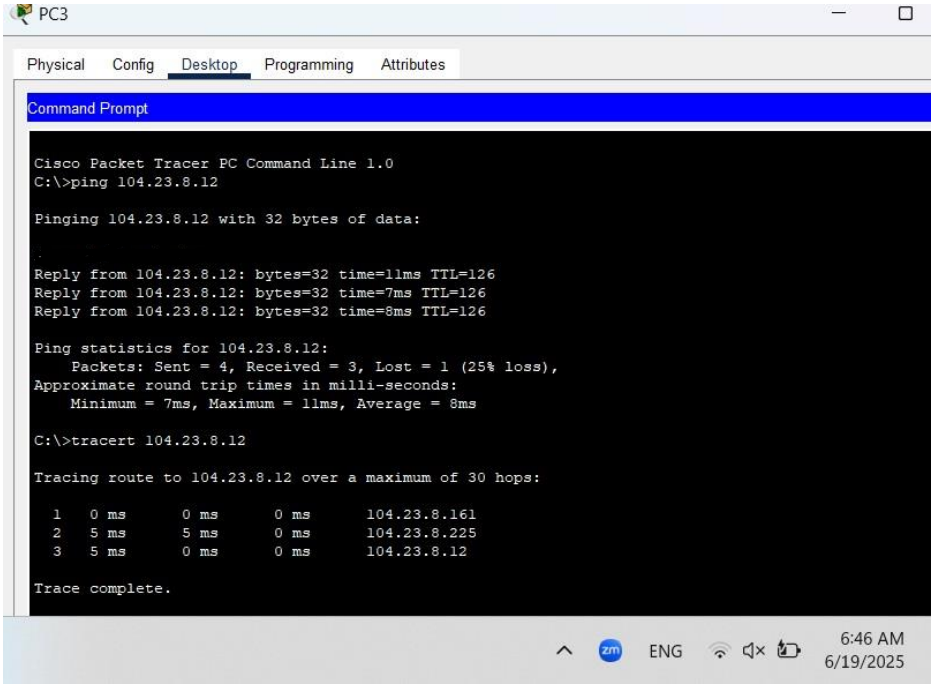


Figure 51: ping and tracert PC0 and PC3

I will again this process but between device from area 2 with area 1,Between 2 smartphones.

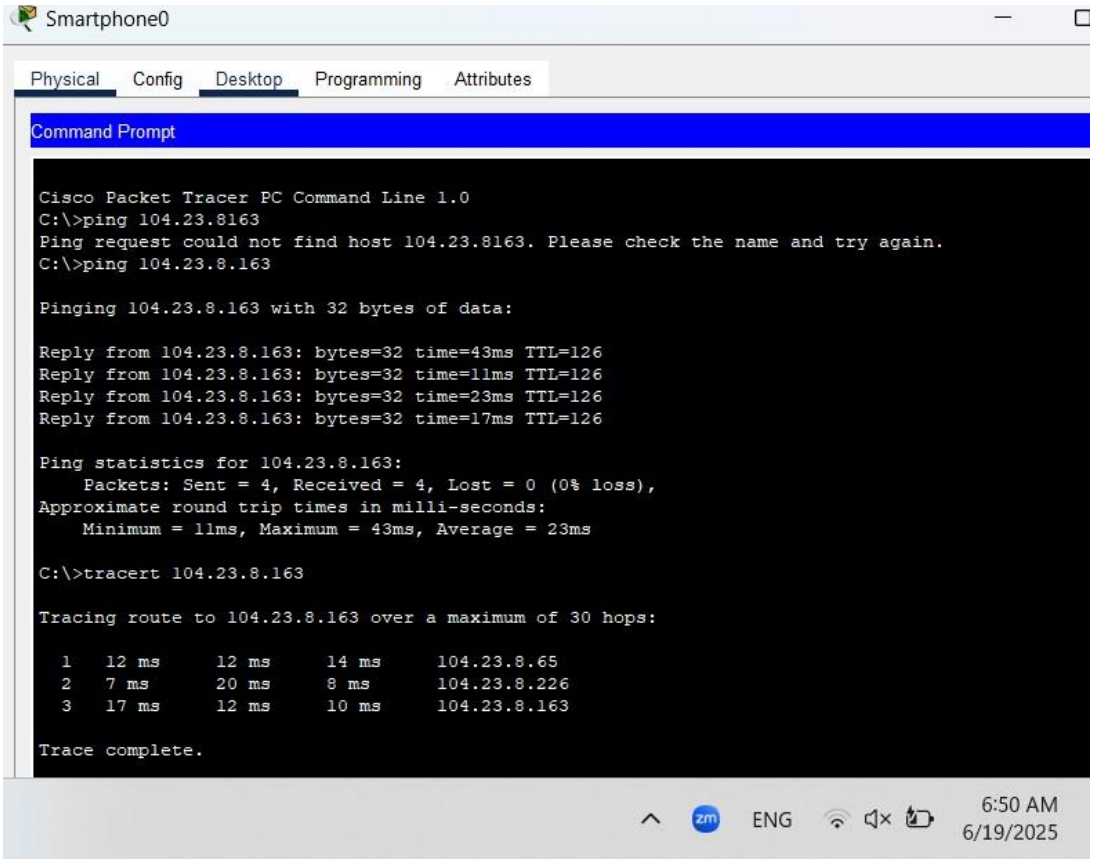


Figure 52: ping and tracert 2 smartphones

5. Email service with the user setup on the mail.coe.birzeit.edu.
   As shown above in NET3 section the SMTP and POP3 services are enabled

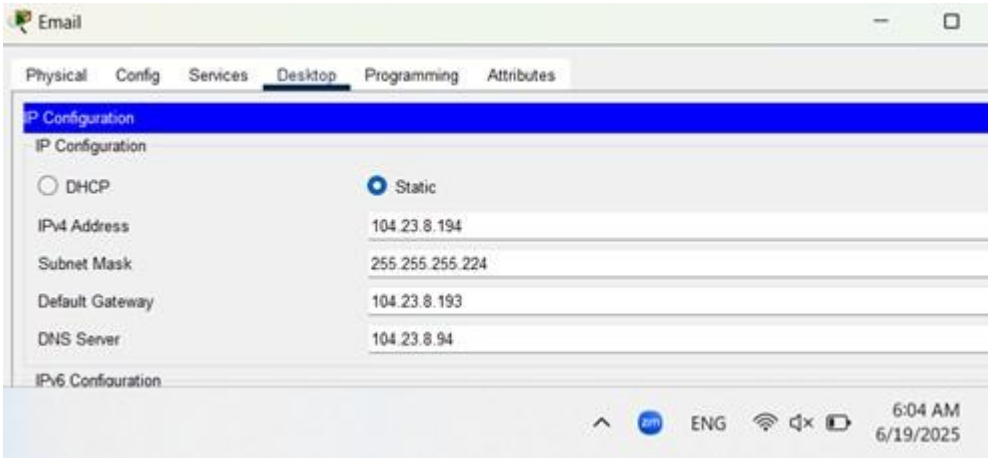


Figure 53:IP configuration for email

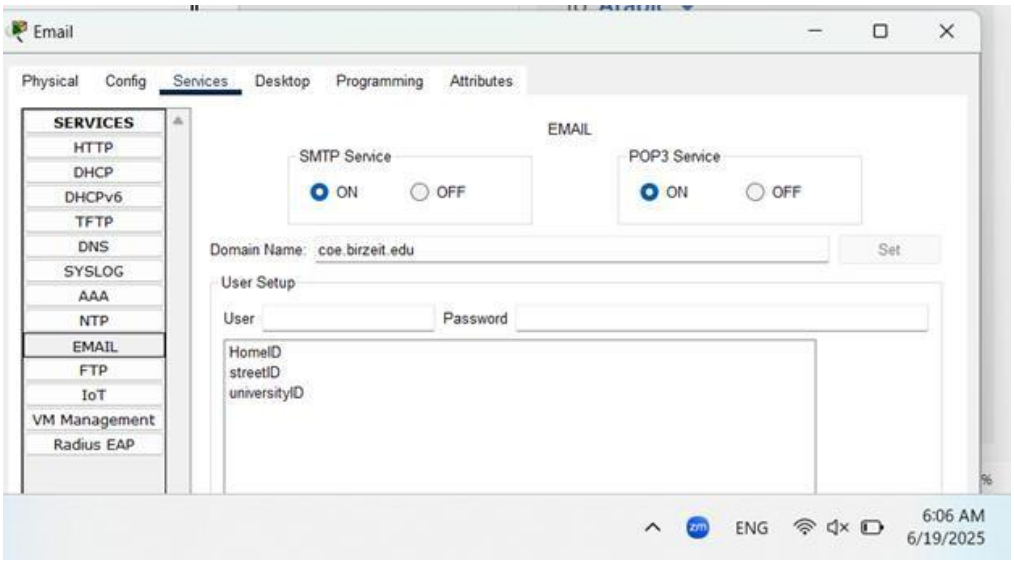


Figure 54: usernames and domain name

Username	password	Email format
HomeID	1222654	HomeID@coe.birzeit.edu
streetID	1220423	streetID@coe.birzeit.edu
UniversityID	1220601	UniversityID@coe.birzeit.edu

Figure 55:usernames with passwords and email format

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

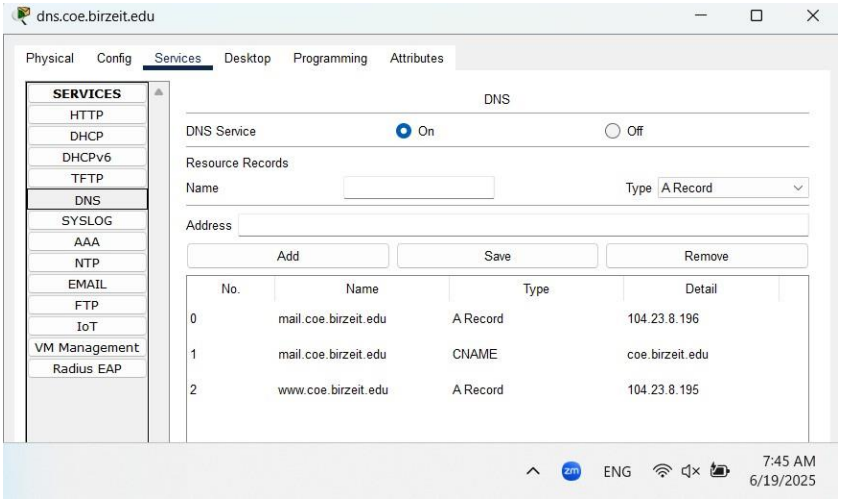


Figure 56:DNS services with RRs

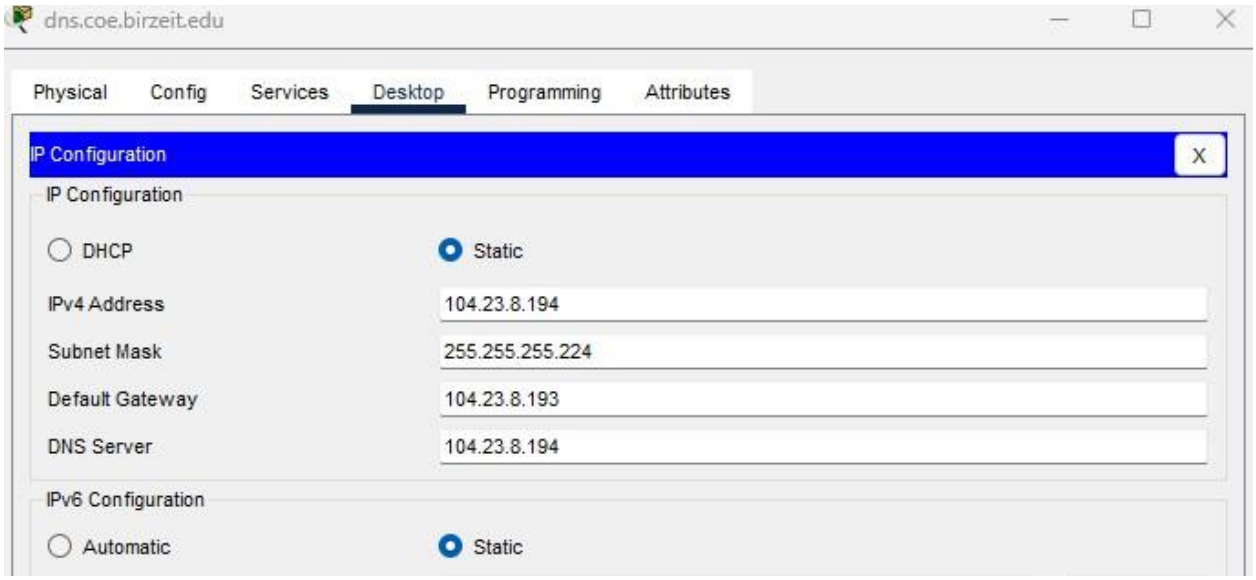


Figure 57:IP configuration for DNS server

7. , and for the WEB SERVER , Successful access to the webserver www.coe.birzeit.edu from some of the end devices.

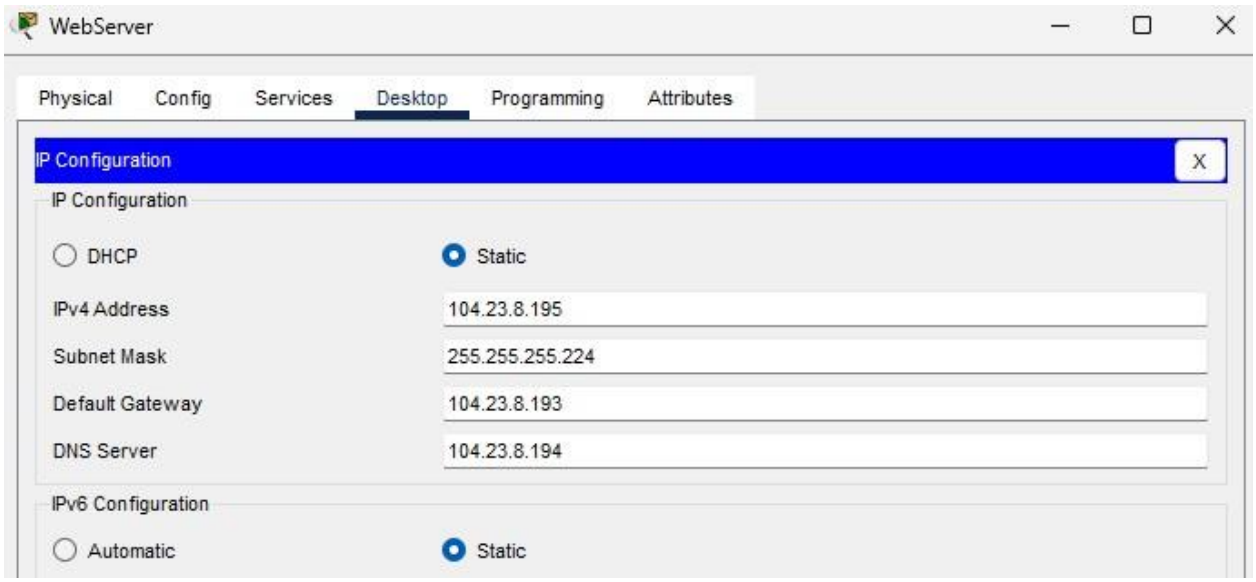


Figure 58: ip configuration for the web server

Here , we will show that when try from any pc in any area , enter the web-server its working successfully

For example pc2, that in the Home area :
First we click in the pc , and then choose desktop , then the web browser , as shown in the figure

Figure 59: pc1 desktop for web testing

After that , we write the URL that is from the DNS for the Web SERVER :

Figure 60:writing the correct URL on PC2

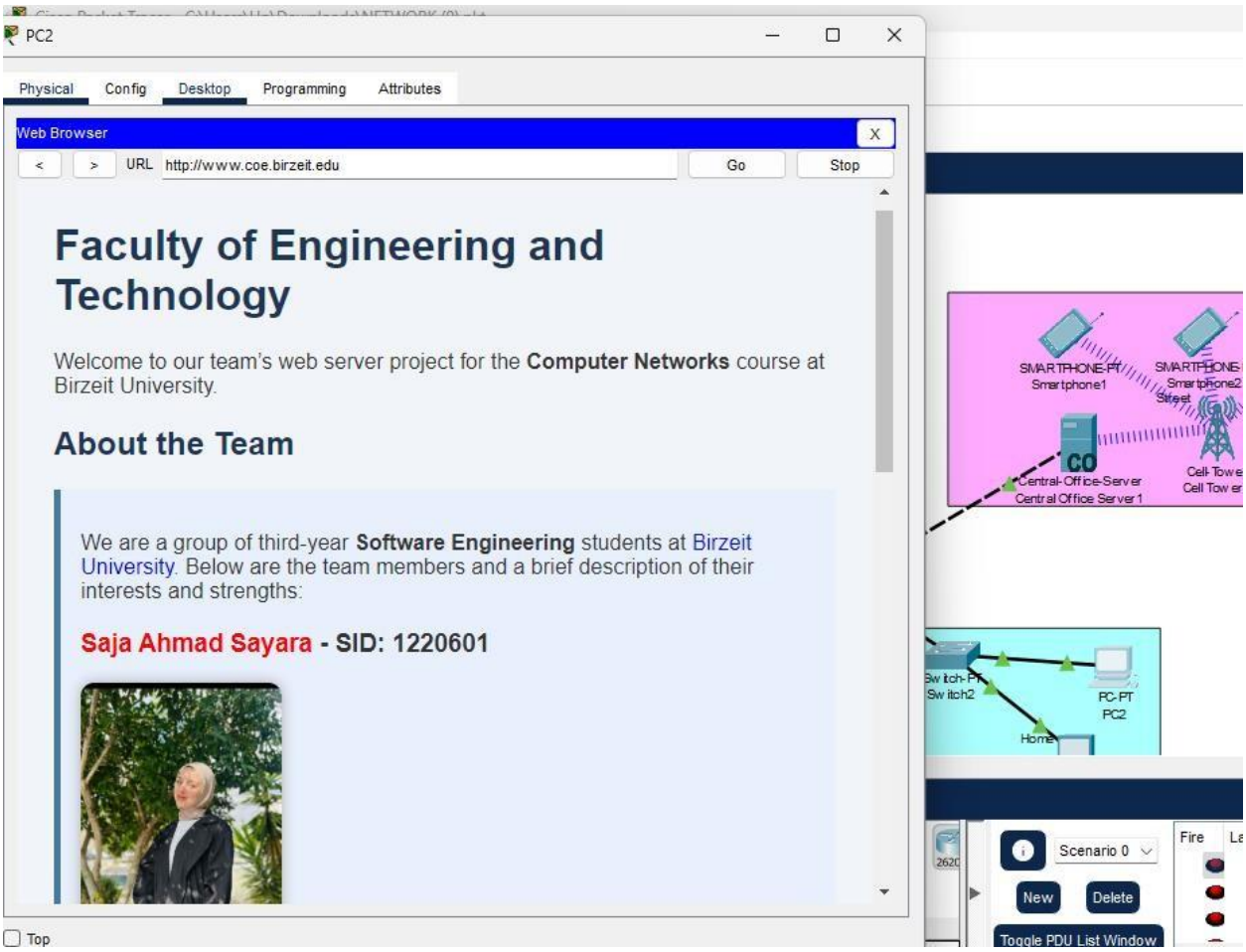


Figure 61: here is a successively entering the web page from pc2

And for another pc in another area :

PC0 , on university area :

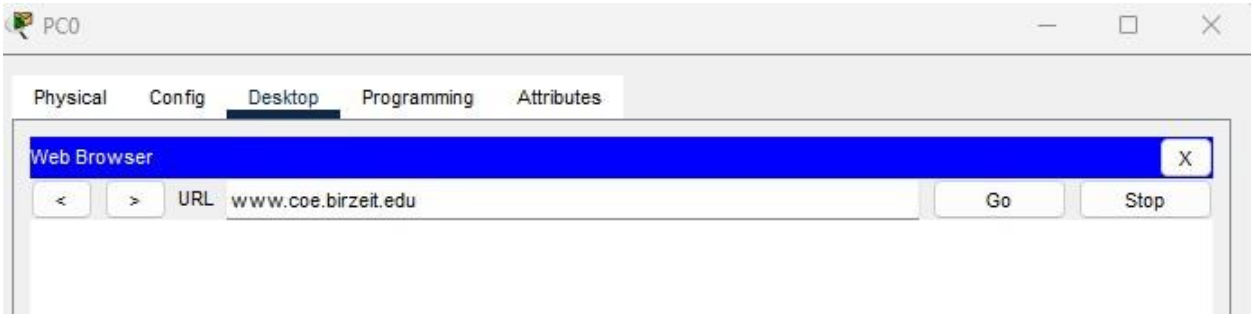


Figure 62:writing the correct URL on PC0

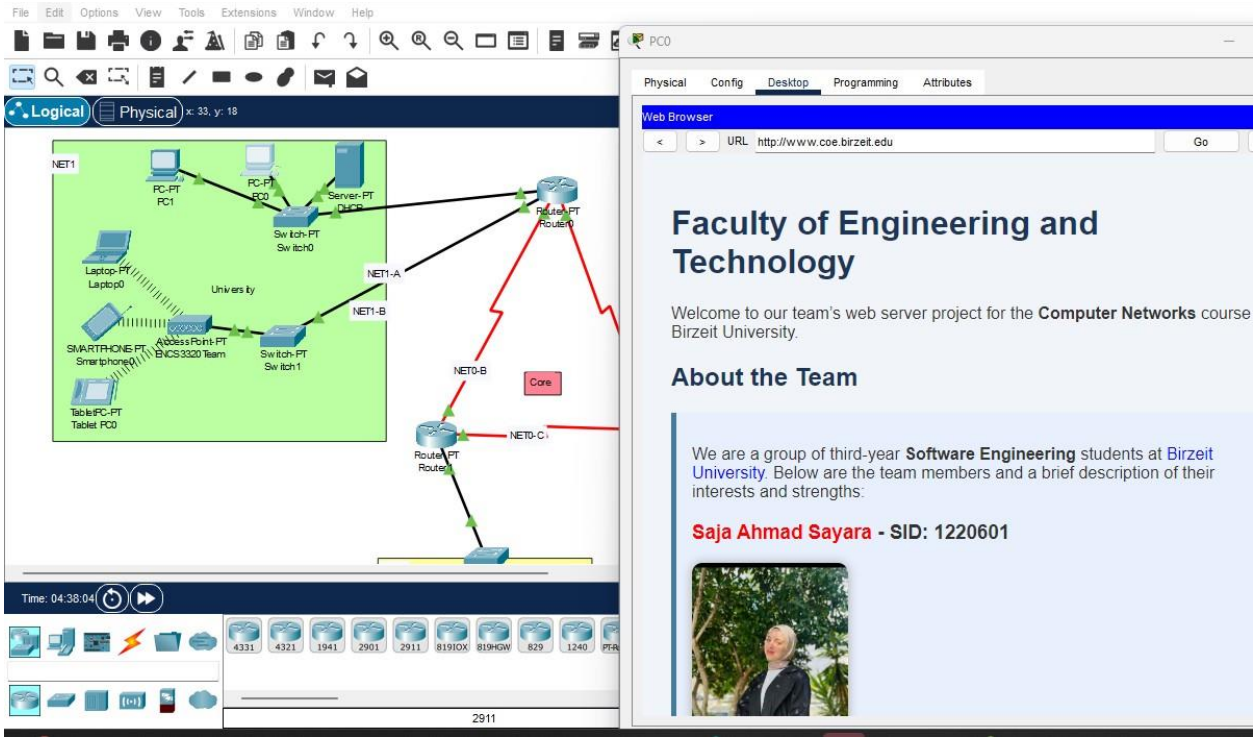


Figure 63:here is a successively entering the web page from pc0

During testing, we verified the web server functionality from multiple PCs located in different network segments, and all were able to successfully access the hosted web page. We also attempted to access the server using a smartphone device in Packet Tracer; however, due to simulation limitations, the mobile browser did not fully load the page — which is expected behavior in this environment.

8. Email client configuration for coe.birzeit.edu account.

From desktop-email in the PC1 we set this data, to can send or receive message for this email so I define the email on this pc.

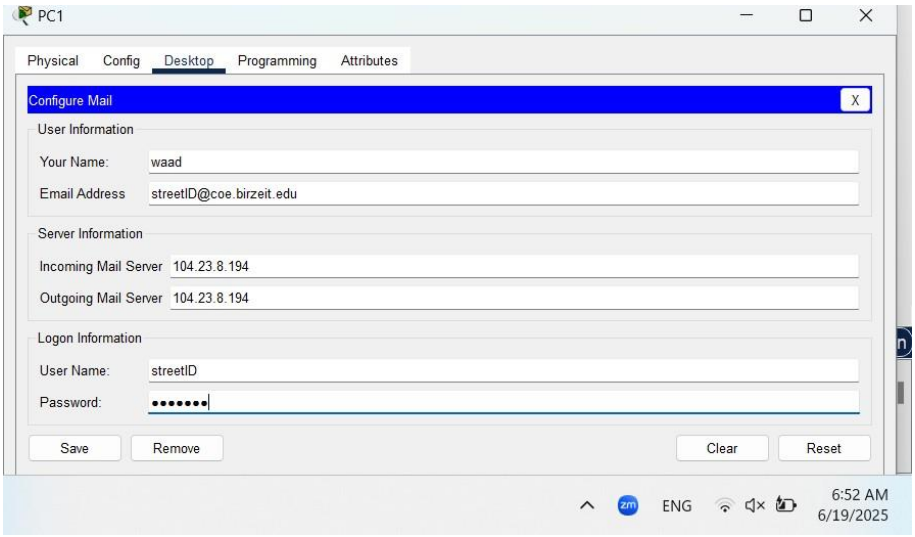


Figure 64: PC1 email data

Now we define another email on another PC "PC2" to can send or receive messages from username streetID.

Now to be all thing clearly we define streetID on PC1 and on PC2 we define HomeID. After defining them we can easily send and receive emails.

The figure below shows the message on PC2 that we want to send it from HomeID to streetID.

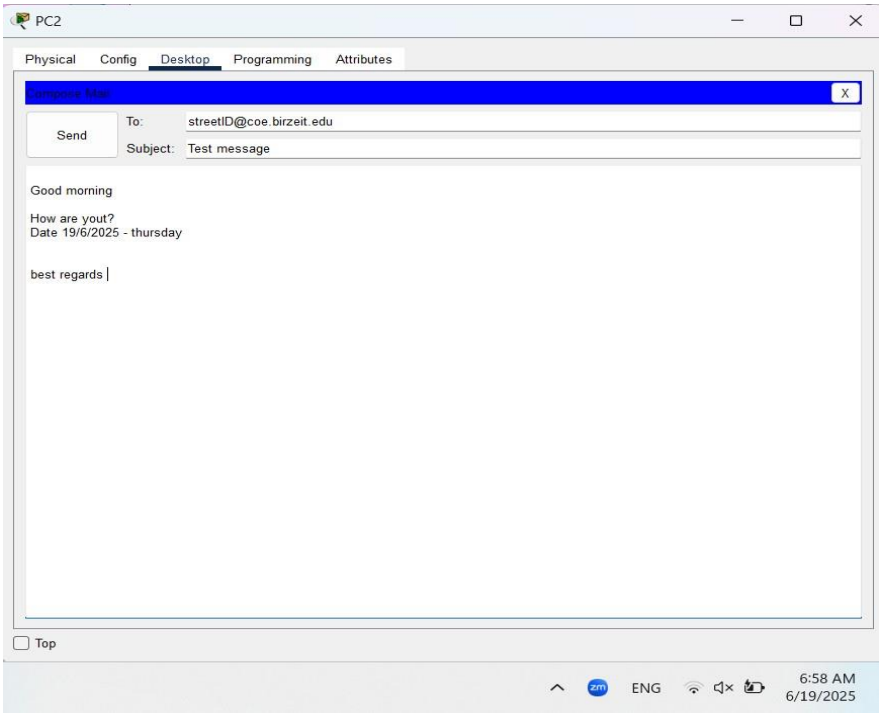


Figure 65: the message

This notification means the message send successfully

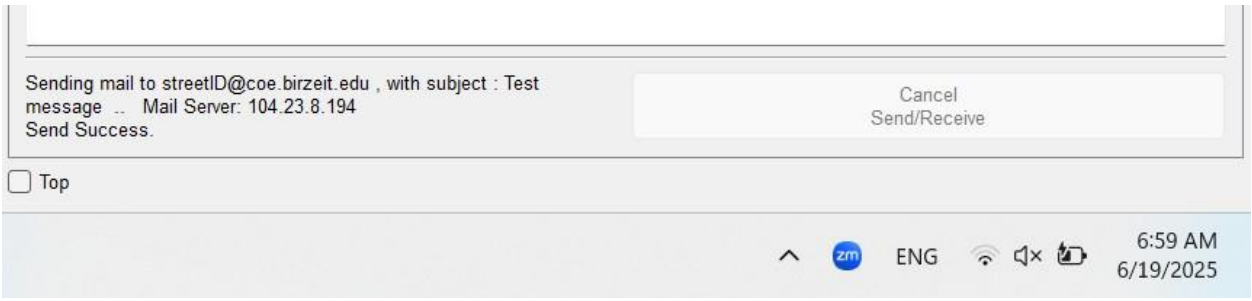


Figure 66: successful message send notification

The figure below shows that the message was received from the HomeID(PC2) to streetID(PC1). And the notification at the bottom of the screen shows that the email was received successfully.

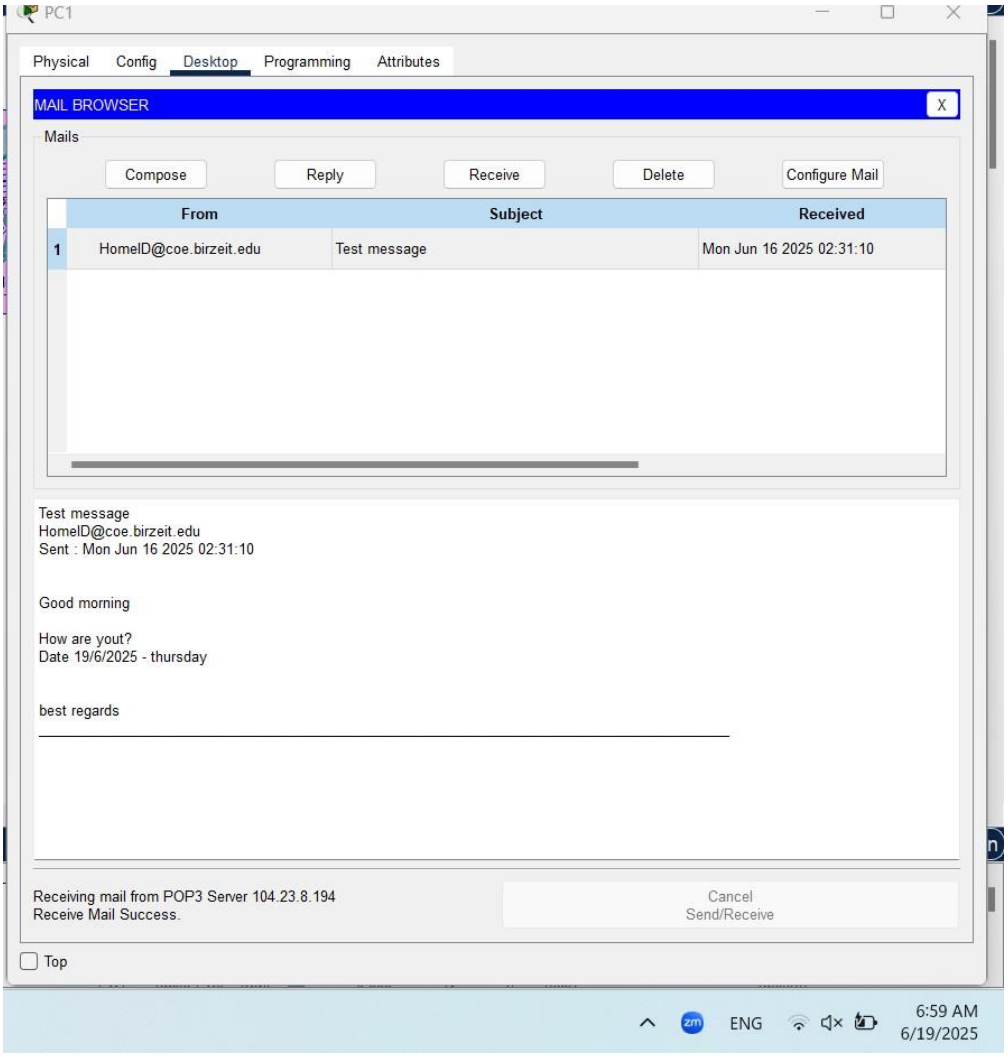


Figure 67:message received successfully

From streetID email I reply to the HomeID and we have a notification that shows that the email sends successfully.

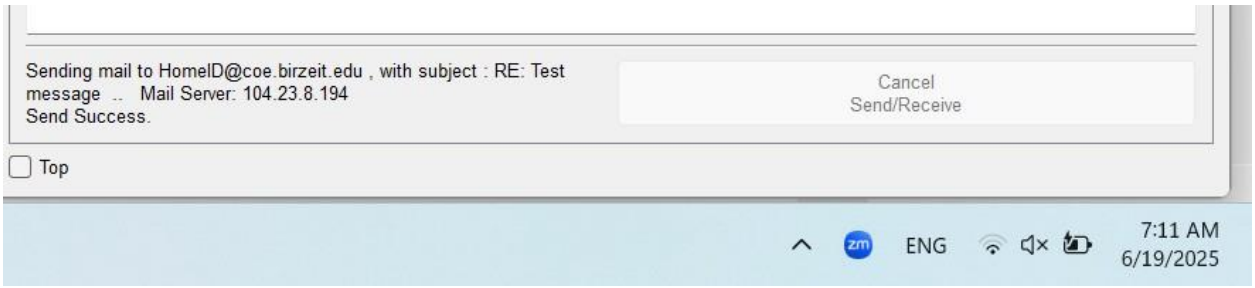


Figure 68: email replay successfully

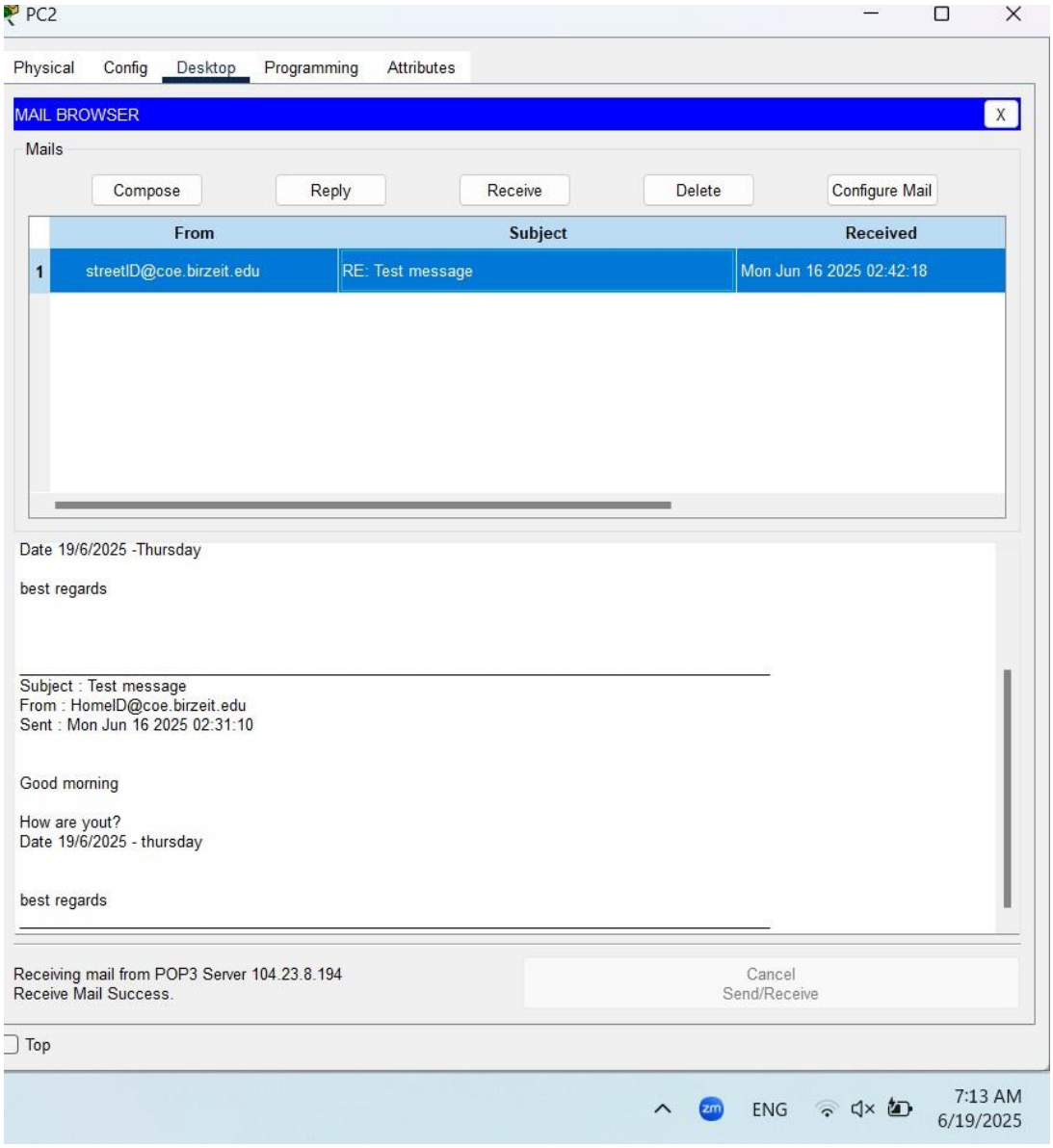


Figure 69:email replay received successfully

We can repeat this process between any end devices.

Teamwork

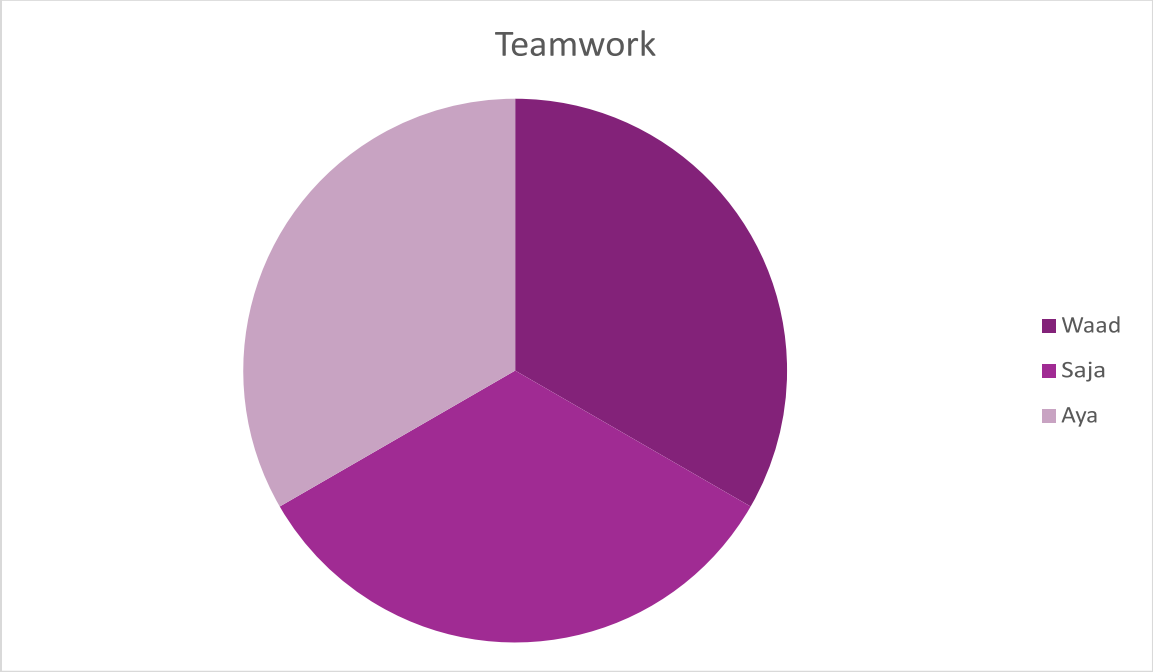


Figure 70:teamwork chart

References

Each reference can be accessed through the number next to the text