Faculty of Engineering & Technology

Electrical & Computer Engineering Department

ENCS3320, Computer Networks

First Semester (2025/2026)

Project 2 – Cisco Packet Tracer

Team Members

Faris Sawalmeh	**1220013**	**Section: 2**
Mohammad Ewais	**1220053**	**Section: 5**
Yahia Sarhan	**1221858**	**Section: 2**

Instructor: Dr. Alhareth Zyoud & Ibrahim Nemer

Submission Date: June, 19, 2025

❖ Abstract

This project aims to **design**, **implement**, and **simulate** a comprehensive **computer network** using **Cisco Packet Tracer**. The primary goal is to enhance practical skills in **network topology design**, **IP subnetting**, **routing configuration**, and **deployment of essential network services** such as **Web**, **Email**, **DNS**, and **DHCP** servers.

The designed network consists of **five interconnected areas**: the **Core Network (Area 0)**, the **University Network (Area 1)**, the **Street Network (Area 2)**, the **Home Network (Area 3)**, and the **Datacenter Network (Area 4)**. An appropriate **IP addressing scheme** is developed based on the team leader's **Student ID**, ensuring efficient **subnetting** that accommodates the required number of hosts for each subnetwork.

Using **Cisco Packet Tracer**, various **network devices** such as **routers**, **switches**, **access points**, **servers**, **PCs**, **laptops**, **tablets**, **smartphones**, **printers**, and specialized elements like the **Central Office Server** and **Cell Tower** are configured and connected to replicate a realistic networking scenario.

Dynamic Host Configuration Protocol (DHCP) is implemented to automate IP address assignment for client devices, while **Domain Name System (DNS)** is configured to resolve domain names within the network. Additionally, a **Web Server** is set up to host a custom-designed website for the **Faculty of Engineering and Technology**, and an **Email Server** is configured to handle internal email communication using **SMTP** and **POP3** protocols.

The project employs the **Open Shortest Path First (OSPF)** routing protocol to ensure efficient routing and full network reachability across all areas. Rigorous **testing and troubleshooting** are conducted to verify **connectivity**, validate correct **IP configurations**, confirm successful **web access**, and ensure proper **email communication** between users in different networks.

Finally, the project results, including detailed configurations, **screenshots**, challenges faced, and teamwork contributions, are documented in a comprehensive **technical report**. This project strengthens students' skills in **network planning**, **configuration**, **service management**, and **collaborative problem-solving**, preparing them for real-world **network engineering** tasks.

Table of Contents

- **Abstract** 2
- **List of Figures** 5
- **List of Tables** 7
- **Theory & Procedure** 8
  - **Network Address Translation (NAT)** 8
  - **Dynamic Host Configuration Protocol (DHCP)** 9
  - **Web Server** 10
  - **Email Server (SMTP and POP3 Protocol)** 11
  - **Domain Name System (DNS)** 13
  - **Open Shortest Path First (OSPF)** 15
- **Results & Discussions** 17
  - **IP Subnetting** 17
  - **Our Topology** 18
  - **Core Network** 19
    - **IP Configuration for R0** 20
    - **IP Configuration for R1** 24
    - **IP configuration for R2** 28
  - **University network (Area 1)** 32
    1) NET1-A: 32
    - **IP Configuration for DHCP** 33
    2) **Net1-B:** 36
    - **Setting for Access point** 37
  - **Street Network (Area 2)** 38
  - **Home Network (Area 3)** 39
  - **Datacenter Network (Area 4)** 40
  - **Dynamic IP configuration for some end devices** 41
  - **IP Static Configuration for all end devices** 47
  - **Successful Ping and Tracert tests between end devices** 54

- **Ping Test** 55
- **Tracert Test** 58

➢ **IP Configuration for web server** 61

➢ **Testing for open web page from web server** 64

➢ **IP Configuration for DNS Server** 67

➢ **IP Configuration & all details for Email Server** 70

➢ **Testing for Email Sending & Receiving Between End Devices** 73

➢ **Testing for Successful open web page from some of end devices** 78

➢ **Routing Configuration** 80

❖ **Issues & Limitations** 86

❖ **Teamwork** 87

❖ **Conclusion** 88

❖ **References** 89

❖ List of Figures

Figure 1: □ Network Address Translation 8
Figure 2: Dynamic Host Configuration Protocol (client-server scenario) 9
Figure 3: ✉✉ SMTP and POP3 Protocols 13
Figure 4: DNS Mechanism 14
Figure 5: OSPF Network Topology 16
Figure 6: The full Topology 18
Figure 7: Core network system 19
Figure 8: Router0 – FastEthernet0/0 Interface Configuration (IPv4) 20
Figure 9: Router0 – FastEthernet1/0 Interface Configuration (IPv4) 21
Figure 10: Router0 – Serial2/0 Interface Configuration (IPv4) 22
Figure 11: Router0 – Serial3/0 Interface Configuration (IPv4) 23
Figure 12: IP Configuration for FastEthernet0/0 24
Figure 13: IP Configuration for FastEthernet1/0 25
Figure 14: IP Configuration for Serial2/0 26
Figure 15: IP Configuration for Serial3/0 27
Figure 16: IP Configuration for FastEthernet0/0 R2 28
Figure 17: IP Configuration for FastEthernet1/0 R2 29
Figure 18: IP Configuration for Serial2/0 30
Figure 19: IP Configuration for Serial3/0 31
Figure 20: University network 32
Figure 21: DHCP Server – Interface Settings 33
Figure 22: DHCP Server – IP Configuration 34
Figure 23: DHCP Server – Services Tab 35
Figure 24: NET1-B System 36
Figure 25: Access Point Setting 37
Figure 26: Street Network 38
Figure 27: Home Network 39
Figure 28: Datacenter Network 40
Figure 29: Smartphone1 (3G/4G) Cell1 Interface Configuration 41
Figure 30: Smartphone1 (Wireless0 Interface Configuration) 42
Figure 31: Smartphone2 – 3G/4G Cell1 Interface 43
Figure 32: Smartphone2 (Wireless0 Interface Configuration) 44
Figure 33: Smartphone3 – 3G/4G Cell1 Interface Configuration (IPv4) 45
Figure 34: Smartphone3 – Wireless0 Interface Configuration (IPv4) 46

Figure 35: PC0 – FastEthernet0 Interface Configuration (IPv4) 47
Figure 36: PC1 – FastEthernet0 Interface Configuration (IPv4) 48
Figure 37: Laptop0 – Wireless0 Interface Configuration (IPv4) 49
Figure 38: Smartphone0 – Wireless0 Interface Configuration (IPv4) 50
Figure 39: Tablet PC0 – Wireless0 Interface Configuration (IPv4) 51
Figure 40: PC2 – FastEthernet0 Interface Configuration (IPv4) 52
Figure 41: PC3 – FastEthernet0 Interface Configuration (IPv4) 53
Figure 42: Ping and Tracert Results 54
Figure 43: Ping from PC0 (NET1-A) 55
Figure 44: Ping from PC3 (NET 3) 56
Figure 45: Tracert test from Laptop0 58
Figure 46: Tracert Tablet (NET1-B) 59
Figure 47: WebServer – FastEthernet0 Interface Configuration (IPv4) 61
Figure 48: WebServer – Gateway and DNS IPv4 Configuration 62
Figure 49: WebServer – HTTP & HTTPS Services 63
Figure 50: Web Server Page Access Testing 64
Figure 51 : Team member who develop the web page 65
Figure 52: DNS Server – Configuration Overview 67
Figure 53: DNS Server – Resource Records 68
Figure 54: DNS Server – IP Configuration 69
Figure 55: Email Server – Global Settings 70
Figure 56: Email Server – IP Configuration 71
Figure 57: Email Server – SMTP & POP3 Services 72
Figure 58: Sending Email Client – Compose Mail 73
Figure 59: Email Client – Received Mail 74
Figure 60: Email Client – Configuration Tab 76
Figure 61: Email Client – Configuration Tab 77
Figure 62: Web Browser – Successful Test 78
Figure 63: Router0 – OSPF Configuration 80
Figure 64: Router1 – OSPF Configuration 82
Figure 65: Router2 – OSPF Configuration 84
Figure 66: Teamwork Chart 87

❖List of Tables

Table 1: IP Subnetting Table.....17

❖ Theory & Procedure

➢ Network Address Translation (NAT)

Network Address Translation (NAT) is a **networking mechanism** used to **modify the IP address information** in packet headers as data travels through a **router**. By doing this, **multiple internal devices** in a **private network** can **access external networks** using a **single shared public IP address**. This technique is essential for **efficient utilization of the limited IPv4 address space** and adds a layer of **security** by **hiding internal private IP addresses** from the outside world. Within the scope of this project, **NAT ensures proper communication** between the designed internal subnets and external servers, while maintaining **address conservation** and **network security**.

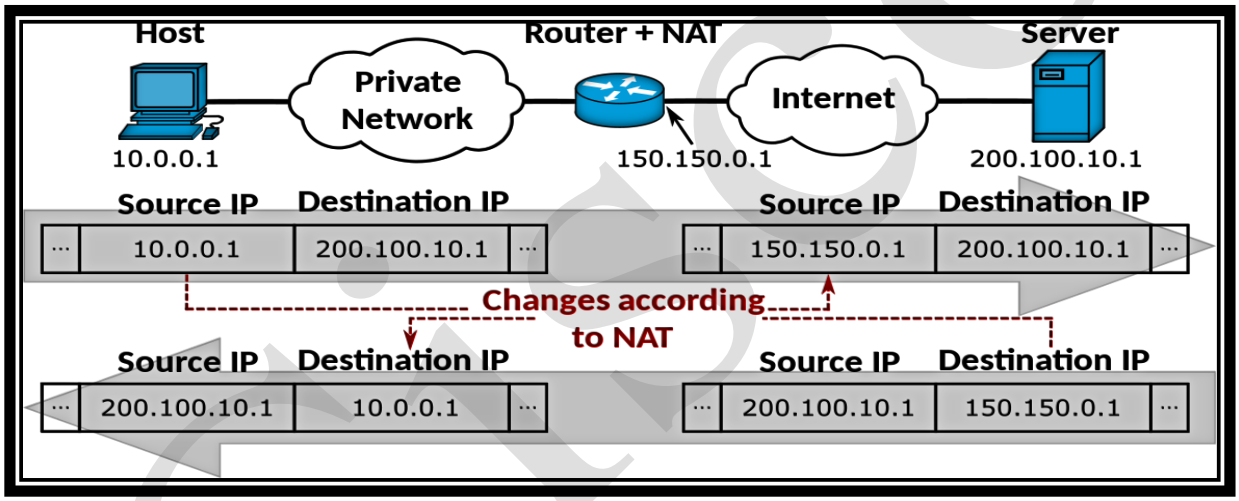


Figure 1: Network Address Translation

Types of NAT:

- **Static NAT:** Establishes a **permanent one-to-one mapping** between a **private IP address** and a **public IP address**. This allows **external users** to **consistently reach a specific internal device** through its **assigned public IP**, which is useful for hosting **internal servers** accessible from the Internet.
- **Dynamic NAT:** Provides **automatic mapping** between **private IPs** and a **pool of available public IPs**. When an internal device initiates a connection, it is temporarily assigned a **public IP from the pool**, ensuring **outbound communication** but **without a fixed public address** for repeated sessions.
- **Port Address Translation (PAT):** Also known as **NAT overload**, this technique allows **many internal devices** to **share a single public IP address** by differentiating connections using **unique port numbers**. PAT is highly efficient for **conserving public IPs** and is commonly used in **enterprise and home networks**.

Advantages of NAT:

- **Efficient IP Utilization: NAT** allows **multiple internal devices** to **access the Internet** through **one public IP address**, effectively **conserving the limited IPv4 address space**.
- **Enhanced Security:** By **concealing private IP addresses** from the external network, **NAT** adds an **additional security layer**, making it more difficult for **unauthorized external access** to internal resources.
- **Flexible Network Management: NAT** makes it possible to **change or expand the internal network** without needing to modify **public IP configurations**, simplifying **network administration and scaling**.

Disadvantages of NAT:

- **Protocol Compatibility Issues:** Some **network protocols** that embed **IP address information** within the payload can encounter **functionality problems** when passing through **NAT**.
- **Potential Performance Overhead: Address translation** introduces **processing delays**, which may **impact network performance**, especially in **high-traffic environments**.
- **Complexity for Peer-to-Peer Services: NAT** can make establishing **direct inbound connections** more challenging, complicating the use of **peer-to-peer applications** and services that require **unrestricted two-way communication**.

➢ Dynamic Host Configuration Protocol (DHCP)

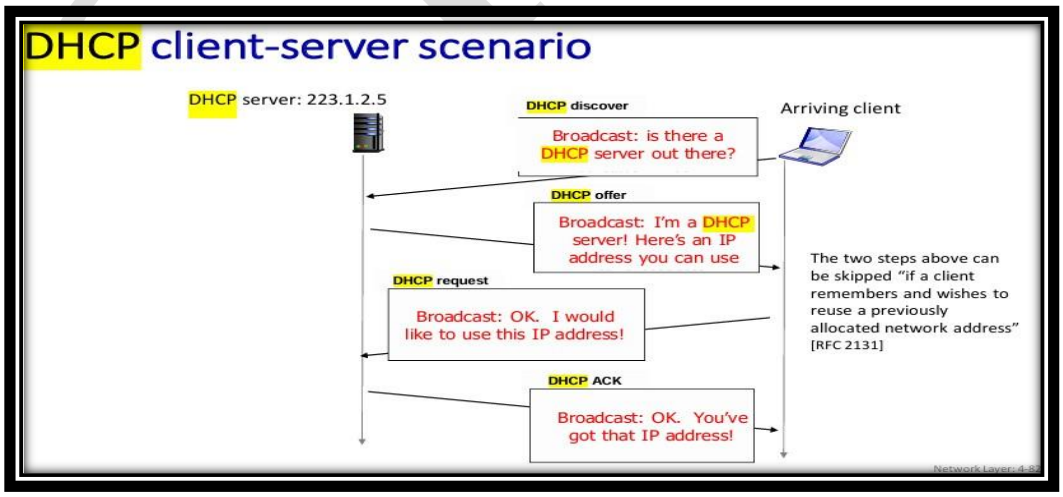


Figure 2: Dynamic Host Configuration Protocol (client-server scenario)

DHCP automates the **assignment of IP addresses** and other **network settings** such as the **default gateway** and **DNS servers**. In this project, **DHCP** is implemented within the **University Network**, where **PCs** and **wireless devices** obtain their configurations **dynamically** from a **DHCP server**, ensuring **scalability** and **ease of management**.

Advantages of DHCP:

- **Automated IP Assignment: DHCP** simplifies **network configuration** by **dynamically providing IP addresses**, significantly reducing the need for **manual setup** and administrative effort.
- **Efficient Address Management:** It ensures **optimal utilization** of the available **IP address pool**, preventing **address conflicts** and promoting **smooth network operation**.
- **Scalability and Flexibility: DHCP** allows **new devices** to join the **network seamlessly**, supporting **network growth** without the need for reconfiguring IP settings manually.

Limitations of DHCP:

- **Security Concerns:** Without proper **security controls**, unauthorized devices may **obtain IP addresses**, and **rogue DHCP servers** can disrupt network stability.
- **Server Dependency:** The operation of **network clients** is dependent on the **availability of the DHCP server**; if the server fails, devices may be unable to **receive or renew their IP configurations**, affecting connectivity.

➢ Web Server

In this project, a **Web Server** plays a critical role in providing **web-based access** to information within the designed network. The **Web Server** is deployed in the **Datacenter Network (Area 4)** and is configured to handle **HTTP** and **HTTPS** requests from **client devices** across the network.

Key responsibilities of the Web Server include:

- **Hosting a Website:** The **Web Server** hosts the official **website for the Faculty of Engineering and Technology**. This site provides **information** about the faculty, details about **team members**, and other relevant content.
- **Custom Web Page:** As required, the **index.html** page must be **customized** to include:
    - A **Tab Title** named "**COE-Birzeit**".
    - A **Page Title** reading "**Faculty of Engineering and Technology**".
    - A **description** of the faculty, organized **lists**, **images**, and properly **formatted text** to create a **professional and informative webpage**.

- **Static IP Configuration:** The **Web Server** must be assigned a **static IP address** within the designated **subnet for the Datacenter Network**, ensuring consistent reachability for clients and DNS resolution.
- **Connectivity with DNS:** To allow users to access the website easily, the **DNS Server** is configured with an **A Record** that maps the domain name (**www.coe.birzeit.edu**) to the **Web Server's IP address**. This enables devices to locate the server using the domain name instead of the numerical IP.
- **Client Access:** Devices in different areas of the network (**University, Street, Home, Core**) can access the website via a web browser by entering the **domain name** (**www.coe.birzeit.edu**). Successful access should be demonstrated through screenshots showing the **loaded webpage**.

The **Web Server configuration** must ensure that **both HTTP and HTTPS services** are enabled, allowing secure and standard web traffic. This setup illustrates practical implementation of **web hosting** within a controlled **network environment**, reflecting real-world **enterprise web services**.

➢ Email Server (SMTP and POP3 Protocol)

In this project, the **Email Server** is an essential component located within the **Datacenter Network (Area 4)**. It handles the **sending and receiving of emails** between users in different parts of the network (**Home**, **Street**, and **University**) by using the **SMTP** and **POP3 protocols**.

Key configurations and responsibilities:

- **Static IP Assignment:**
  The **Email Server** is configured with a **static IP address** within the **Datacenter subnet**, ensuring reliable connectivity for all users.
- **SMTP (Simple Mail Transfer Protocol):**
  - Used for **sending outgoing emails** from client devices to the **Email Server**.
  - The **SMTP service** must be enabled on the server, with the domain name set as **coe.birzeit.edu**.
- **POP3 (Post Office Protocol version 3):**
  - Used for **retrieving incoming emails** from the **Email Server** to client devices.
  - POP3 allows users to **download messages** and manage their emails locally.

- **User Accounts:**
    - Create **three user accounts**, each assigned to one network area (**Home**, **Street**, and **University**).
    - Each account should follow this format:
        - **Username:** {HomeSID, StreetSID, UniversitySID}
        - **Password:** The team member's **SID**
        - **Email Address:** **Username@coe.birzeit.edu**

- **Client Configuration:**
    - Each client device must be configured with the following email settings:
        - **Incoming Mail Server (POP3): mail.coe.birzeit.edu**
        - **Outgoing Mail Server (SMTP): mail.coe.birzeit.edu**
        - Correct **username** and **password** for authentication.
- **Testing:**
    - Perform tests by **sending and receiving emails** between the configured user accounts.
    - Include **screenshots** in the report to demonstrate successful email transmission and retrieval across the **Home**, **Street**, and **University networks**.

This configuration highlights the practical deployment of an **Email Server** in a real-world scenario, demonstrating how **SMTP** handles outgoing mail and **POP3** manages incoming mail, ensuring **reliable and secure email communication** within the designed network.

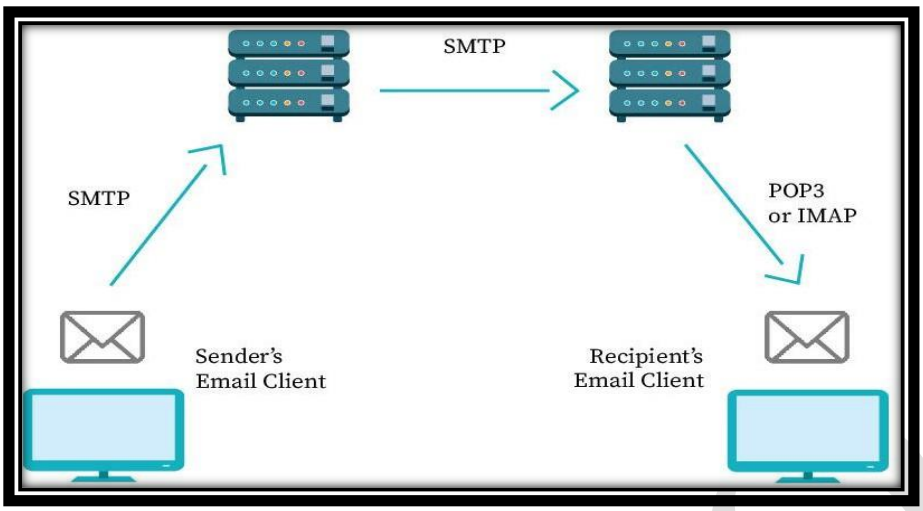


Figure 3: ✉✉ SMTP and POP3 Protocols

➢ Domain Name System (DNS)

In this project, the **Domain Name System (DNS)** is implemented as a crucial network service within the **Datacenter Network (Area 4)**. The **DNS Server** is responsible for translating **domain names** into **IP addresses**, allowing devices in the network to locate services easily without needing to remember numeric IPs.

Key configurations and functions:

- **Static IP Assignment:**
  The **DNS Server** is configured with a **static IP address** within the **Datacenter subnet**, ensuring stable and consistent name resolution for all network clients.
- **DNS Service Activation:**
  Only the **DNS service** must be enabled on this server to handle domain name queries efficiently.
- **Resource Records (RRs):**
  The **DNS Server** must include specific **Resource Records** to resolve names correctly:
  - **A Record:** Maps **www.coe.birzeit.edu** to the IP address of the **Web Server**.
  - **A Record:** Maps **mail.coe.birzeit.edu** to the IP address of the **Email Server**.
  - **CNAME Record:** Maps **coe.birzeit.edu** as an alias pointing to **mail.coe.birzeit.edu**.
- **Integration with Other Services:**

- The **DHCP Server** provides the **DNS Server's IP address** to clients so that all devices know which server to query for domain name resolution.
- This ensures that devices across the **University**, **Street**, **Home**, and **Core** networks can resolve and access the **Web Server** and **Email Server** using human-readable names.

- **Testing:**
  - Verify that the **DNS Server** correctly resolves all configured domain names by performing **ping tests** and accessing services (e.g., visiting **www.coe.birzeit.edu** from client browsers).
  - Include **screenshots** showing successful name resolution and connectivity.

This setup demonstrates how a **DNS Server** simplifies network usability by converting easy-to-remember **domain names** into the corresponding **IP addresses**, supporting smooth access to web and email services within the designed topology.

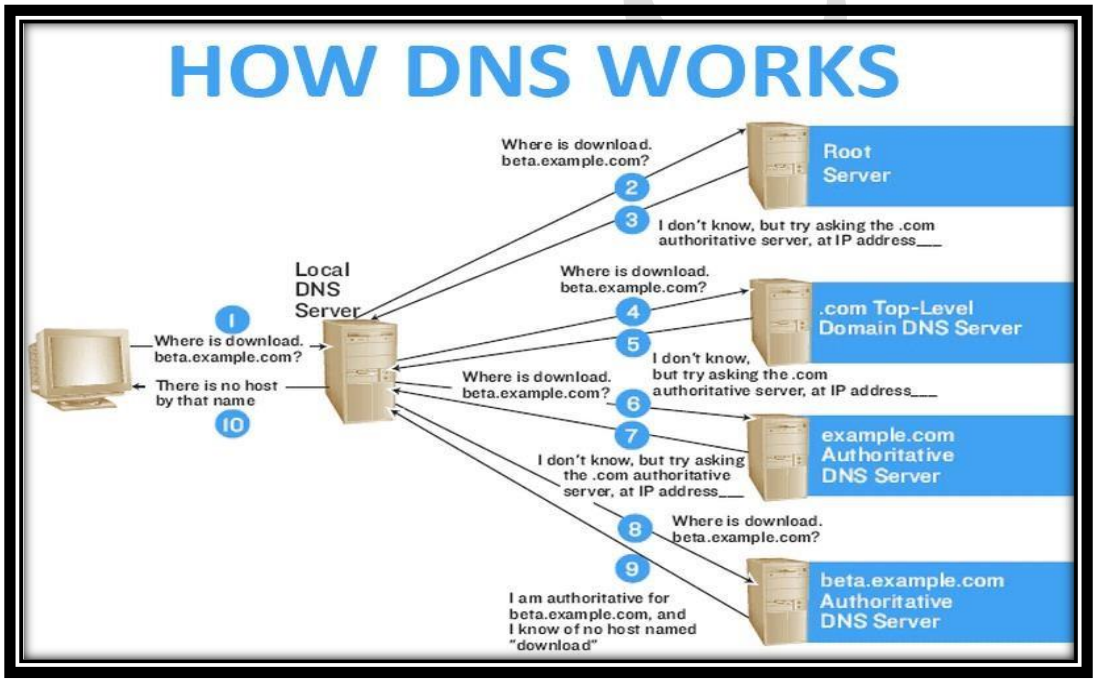


Figure 4: DNS Mechanism

➢ Open Shortest Path First (OSPF)

In this project, **Open Shortest Path First (OSPF)** is used as the main **interior gateway routing protocol** to ensure **dynamic and efficient routing** across all areas of the designed network topology.

Key configurations and functions:

- **Dynamic Routing:**
  OSPF dynamically determines the **best path** for data packets by calculating the **shortest and most cost-effective routes** between network devices. This reduces the need for manual route configuration and adapts automatically to network changes.
- **Areas Structure:**
  The network is divided into **five OSPF areas** as specified:
  - **Area 0:** Core Network
  - **Area 1:** University Network
  - **Area 2:** Street Network
  - **Area 3:** Home Network
  - **Area 4:** Datacenter Network
    Each area connects back to **Area 0 (Backbone)** to ensure optimal route propagation and loop-free communication.
- **OSPF Configuration on Routers:**
  - On each **Router**, the **OSPF process** must be started using:

    Router(config) # router ospf 1

    where 1 is the **process ID** used consistently across all routers.
  - Each relevant **network subnet** must be added to OSPF using:
    Router(config-router) # network <Network-Address> <Wildcard-Mask> area <Area-ID>
- **Reliable Routing:**
  By using **OSPF**, all routers automatically exchange routing information, leading to **fast convergence** and **optimal path selection** throughout the network.
- **Testing:**
  - Validate OSPF by checking routing tables on all routers to confirm that routes to all other networks are present.

- Use **ping** and **tracert** commands to verify end-to-end connectivity between devices in different areas.
- Include **screenshots** of routing tables and successful connectivity tests in your report.

This setup demonstrates how **OSPF** enables **scalable, robust, and efficient routing** within a multi-area network design, ensuring seamless data flow between the **Core**, **University**, **Street**, **Home**, and **Datacenter** networks.

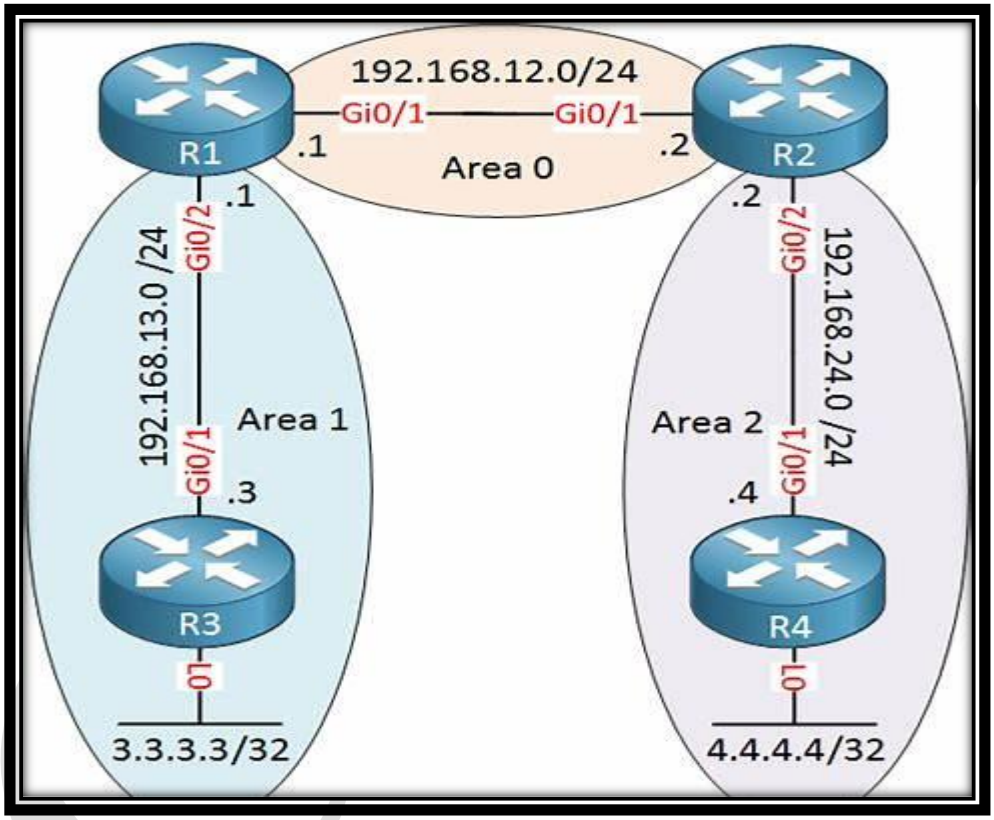


Figure 5: OSPF Network Topology

Figure Explanation:
This diagram illustrates a **multi-area OSPF network** where multiple **routers** connect different **OSPF areas** through a central **backbone (Area 0)**. Each **Area Border Router (ABR)** links a specific area to the backbone, enabling **efficient route exchange** and **loop-free communication**. This structure demonstrates how **OSPF** maintains **hierarchical routing**, optimizes **path selection**, and supports **scalability** within a large network.

❖ Results & Discussions

➢ IP Subnetting

Table 1: IP Subnetting Table

	B	C	D	E	F	G
1	1220053	1220013	1221858			
2						
3	vork Address	Broadcast Address	Usable IPs	CIDR	Subnet Mask	
4	13.8.0	100.13.8.63	100.13.8.1->100.13.8.62	/26	255.255.255.192	
5	13.8.64	100.13.8.127	100.13.8.65->100.13.8.126	/26	255.255.255.192	
6	13.8.128	100.13.8.159	100.13.8.129->100.13.8.158	/27	255.255.255.224	
7	13.8.160	100.13.8.191	100.13.8.161->100.13.8.190	/27	255.255.255.224	
8	13.8.192	100.13.8.207	100.13.8.193->206	/28	255.255.255.240	
9	13.8.208	100.13.8.211	100.13.8.109->100.13.8.210	/30	255.255.255.252	
10	13.8.212	100.13.8.215	100.13.8.213->100.13.8.214	/30	255.255.255.252	
11	13.8.216	100.13.8.219	100.13.8.217->100.13.8.218	/30	255.255.255.252	
12						

The provided **subnetting table** outlines essential details used in designing and managing IP networks. It includes the following key components:

- **Work Address:** Indicates the **starting IP address** of each subnet, representing the **network ID**.
- **Broadcast Address:** Defines the **last address** in each subnet, used for broadcasting messages to all hosts within that subnet.
- **Usable IPs:** Specifies the **range of assignable IP addresses** between the network and broadcast addresses, which can be allocated to end devices.
- **CIDR Notation:** Represents the **Classless Inter-Domain Routing (CIDR)** format (e.g., /26, /30), which defines the size and segmentation of each subnet.
- **Subnet Mask:** Lists the **subnet mask** corresponding to each CIDR value, used to determine the network and host portions of an IP address.

This table serves as a fundamental reference for **IP subnet planning**, allowing network administrators to efficiently segment a larger network into **smaller, manageable subnets**.

➢ Our Topology

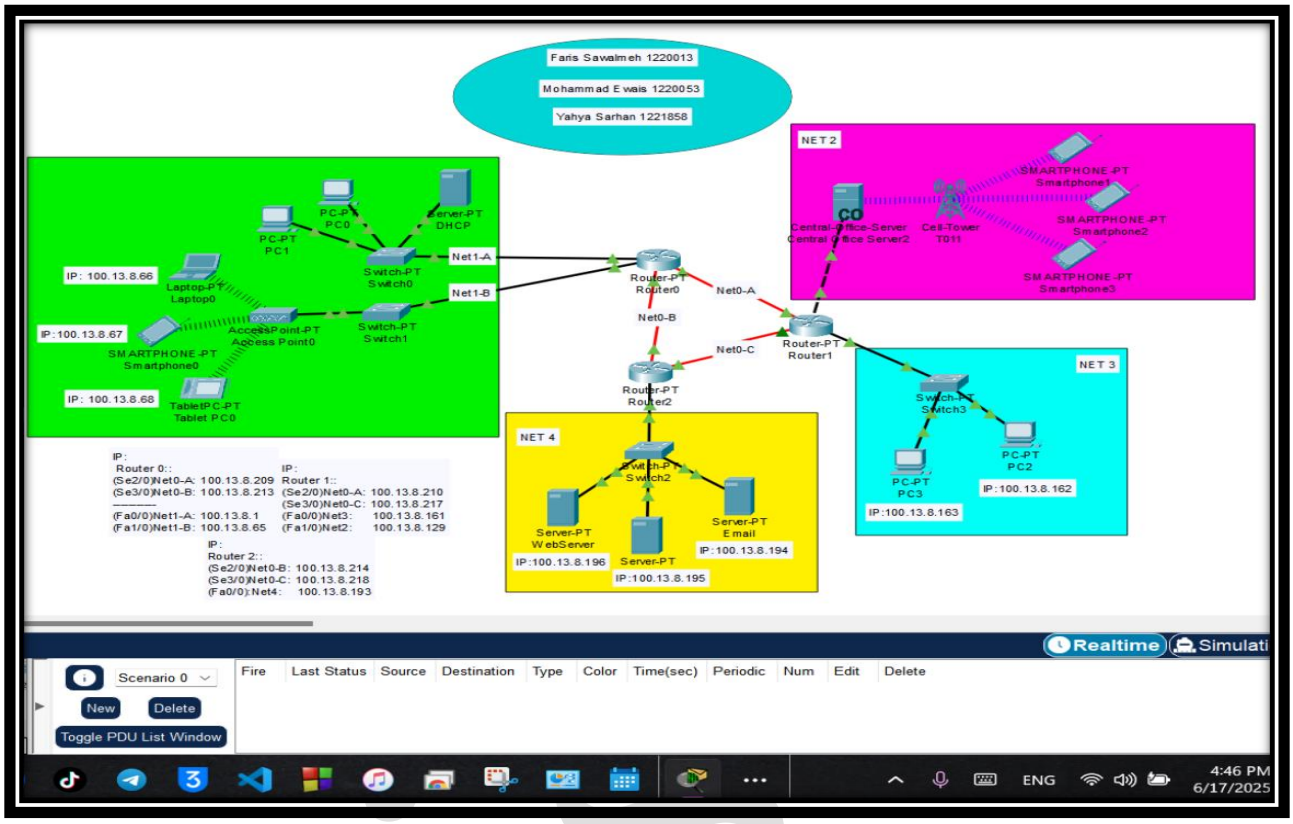


Figure 6: The full Topology

The second image illustrates a **comprehensive network topology**, comprising four interconnected subnetworks: **NET 1**, **NET 2**, **NET 3**, and **NET 4**. The layout includes:

- **Routers and Switches:** These networking devices form the **backbone of communication**, routing traffic between different subnets and ensuring efficient packet delivery.
- **End Devices:** A variety of end-user devices such as **PCs, laptops, smartphones, and servers** are shown connected to the network, each assigned a **unique IP address** within its respective subnet.
- **Central Server (NET 2):** Positioned within **NET 2**, a centralized server acts as the **core communication node**, facilitating services and data exchange across the entire network.
- **Communication Paths: Directional arrows** indicate the flow of communication between devices and across subnetworks, demonstrating **inter-network connectivity**.

This topology exemplifies a **well-structured enterprise network**, highlighting the integration of multiple subnets and devices to enable **scalable, secure, and reliable communication** across various departments or services.

➢ Core Network

The **Core Network** serves as the **central backbone** of the topology, providing connectivity between **all other segments**. It is composed of **three routers**, as illustrated in the figure:

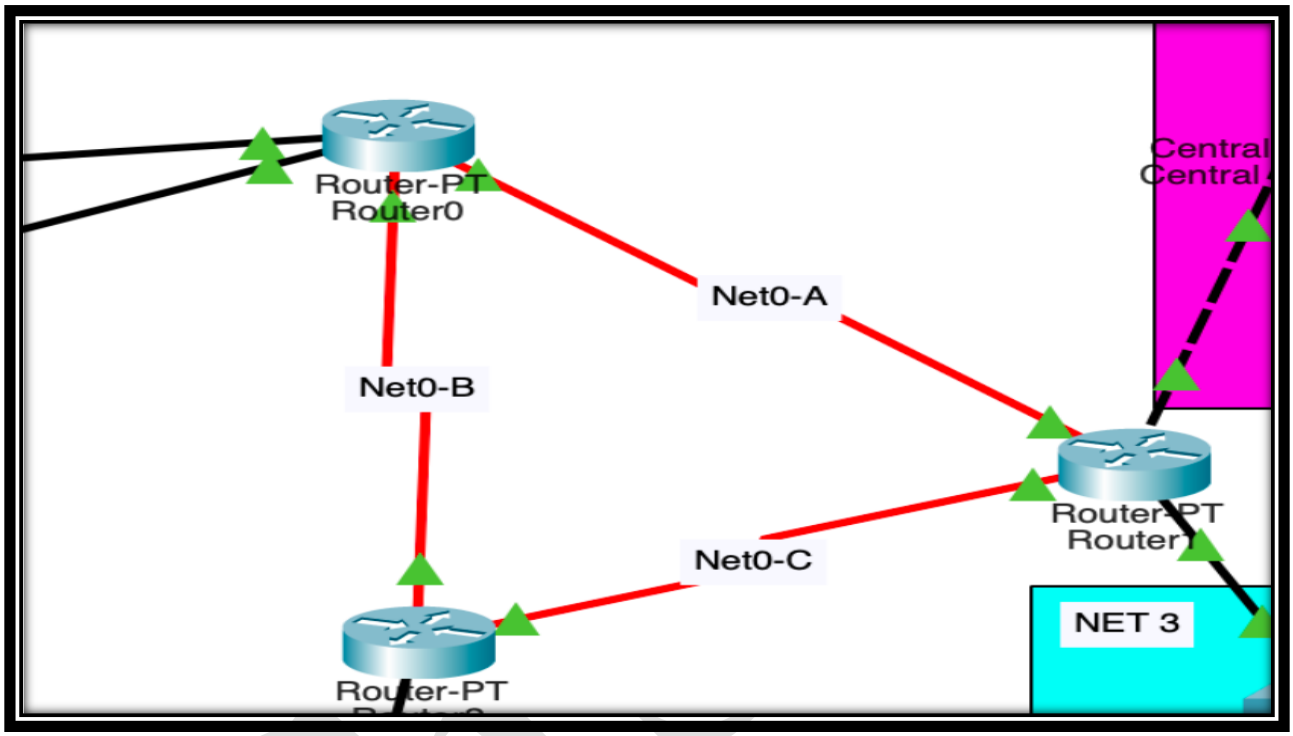


Figure 7: Core network system

- **IP Configuration for R0**

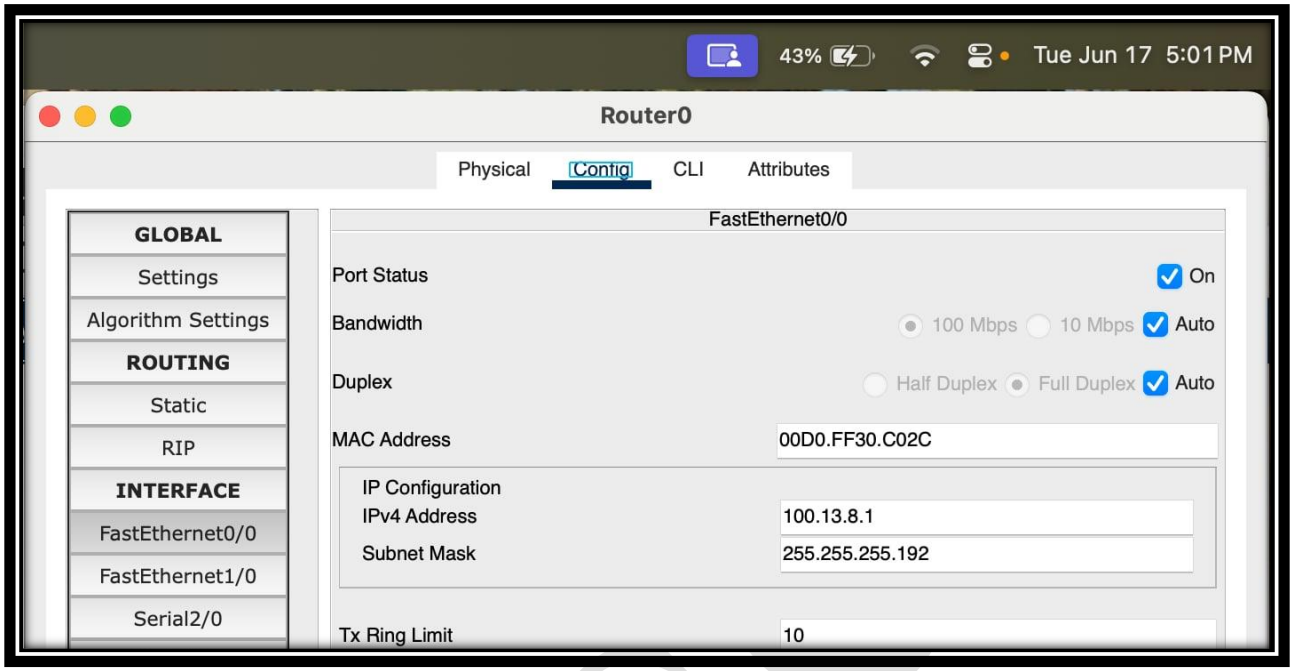


Figure 8: Router0 – FastEthernet0/0 Interface Configuration (IPv4)

Router0 – FastEthernet0/0 Interface Configuration (IPv4)

This screenshot shows the **IPv4 configuration** for the **FastEthernet0/0 interface** on **Router0**:

- **Port Status: Enabled (On)** — confirming that the Ethernet port is active and transmitting data.
- **Bandwidth:** Set to **Auto**, allowing automatic adjustment based on network traffic.
- **Duplex: Auto**, enabling the port to switch between half and full duplex as needed.
- **MAC Address: 00D0.FF30.C02C** — the unique hardware address for this interface.
- **IPv4 Address: 100.13.8.1**
- **Subnet Mask: 255.255.255.192**

Purpose: This configuration allows **Router0** to route data packets efficiently through its FastEthernet0/0 interface, ensuring stable and reliable communication within its assigned subnet.

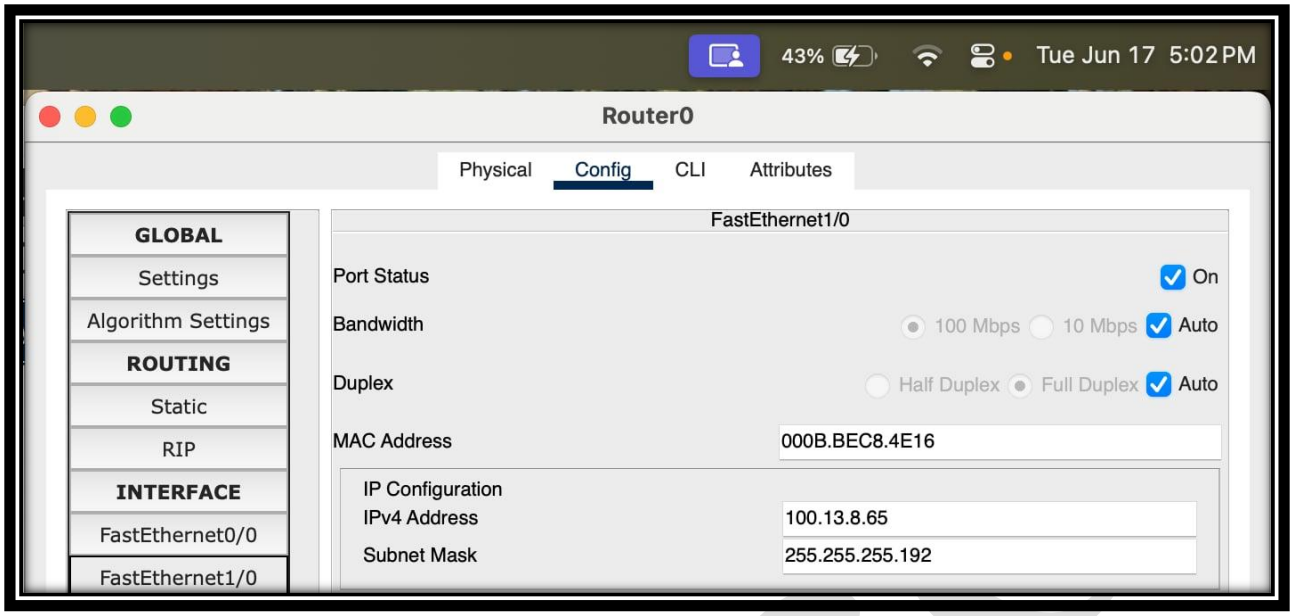


Figure 9: ⚙ Router0 – FastEthernet1/0 Interface Configuration (IPv4)

⚙ Router0 – FastEthernet1/0 Interface Configuration (IPv4)

This screenshot shows the **IPv4 configuration** for the **FastEthernet1/0 interface** on **Router0**:

- ✅ **Port Status: Enabled (On)** — confirming that the Ethernet port is active and transmitting data.
- ⚡ **Bandwidth:** Set to **Auto**, allowing dynamic speed adjustments based on network demand.
- 🔁 **Duplex: Auto**, enabling automatic switching between half and full duplex modes.
- 🏷 **MAC Address: 000B.BEC8.4E16** — the unique hardware address for this port.
- 📡 **IPv4 Address: 100.13.8.65**
- 📏 **Subnet Mask: 255.255.255.192**

🔗 **Purpose:** This configuration allows **Router0** to route data efficiently through its FastEthernet1/0 port, ensuring reliable communication within its assigned subnet.

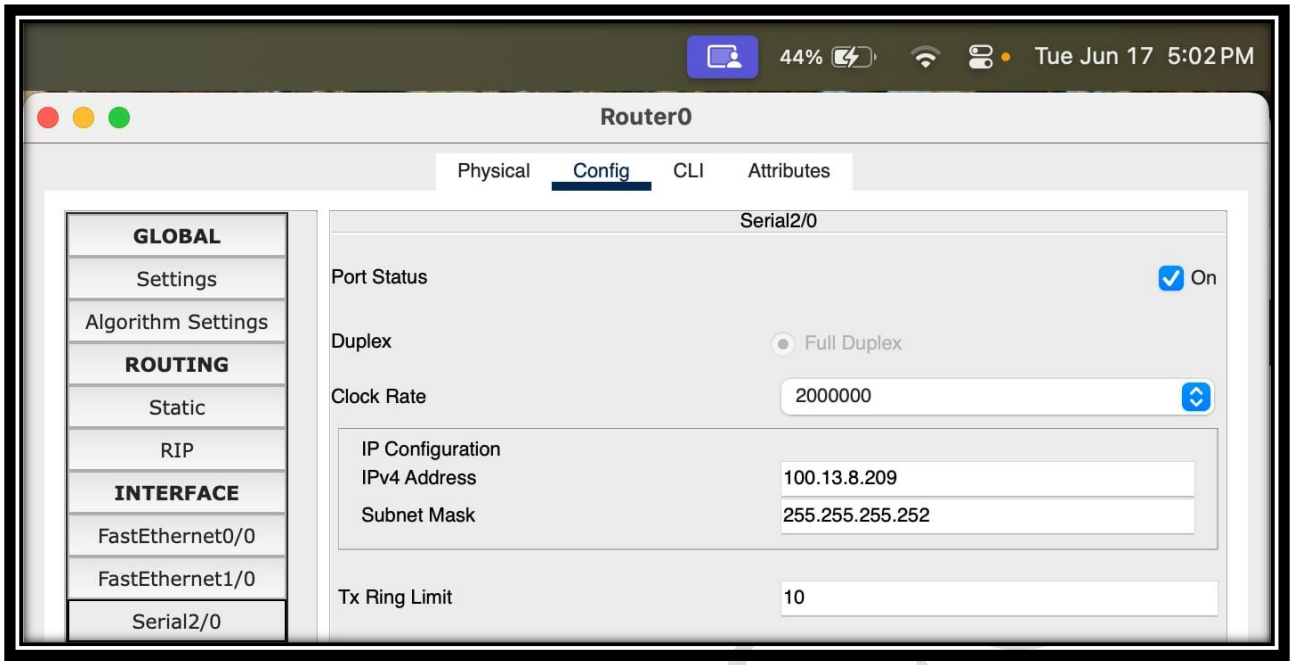


Figure 10: Router0 – Serial2/0 Interface Configuration (IPv4)

Router0 – Serial2/0 Interface Configuration (IPv4)

This screenshot shows the **IPv4 configuration** for the **Serial2/0 interface** on **Router0**:

- **Port Status: Enabled (On)** — confirming that the serial link is active and ready for data transmission.
- **Duplex: Full Duplex** (default for serial interfaces).
- **Clock Rate: 2000000 bps** — defining the speed at which the serial link operates.
- **IPv4 Address: 100.13.8.209**
- **Subnet Mask: 255.255.255.252**

Purpose: This configuration allows **Router0** to maintain a reliable point-to-point serial connection with another router, ensuring stable and efficient data transfer over the WAN.

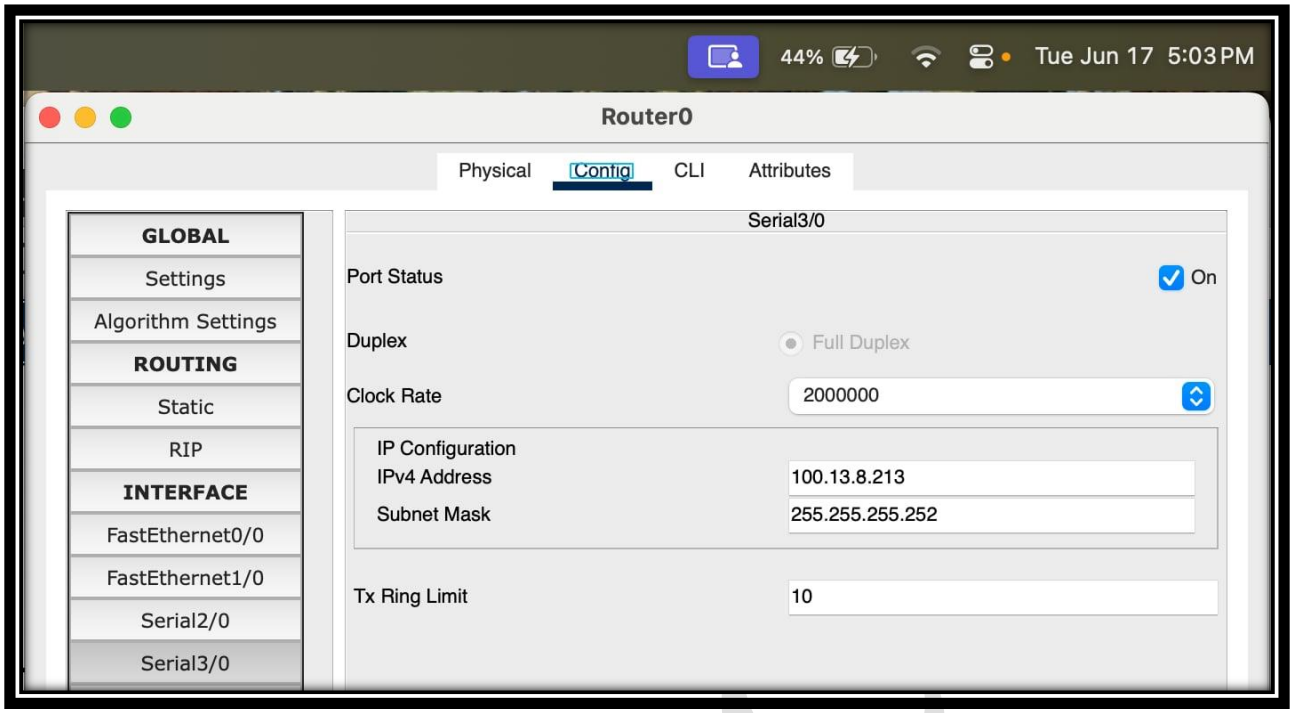


Figure 11: Router0 – Serial3/0 Interface Configuration (IPv4)

Router0 – Serial3/0 Interface Configuration (IPv4)

This screenshot shows the **IPv4 configuration** for the **Serial3/0 interface** on **Router0**:

- ✅ **Port Status: Enabled (On)** — indicating that the serial link is active and ready for data transmission.
- 🔁 **Duplex: Full Duplex** (standard for serial connections).
- ⏱️ **Clock Rate: 2000000 bps** — specifying the speed at which the serial interface transmits data.
- 📡 **IPv4 Address: 100.13.8.213**
- 📏 **Subnet Mask: 255.255.255.252**

🔗 **Purpose:** This configuration enables **Router0** to maintain a stable point-to-point serial connection with another router, ensuring reliable and efficient data exchange over the WAN link.

- **IP Configuration for R1**

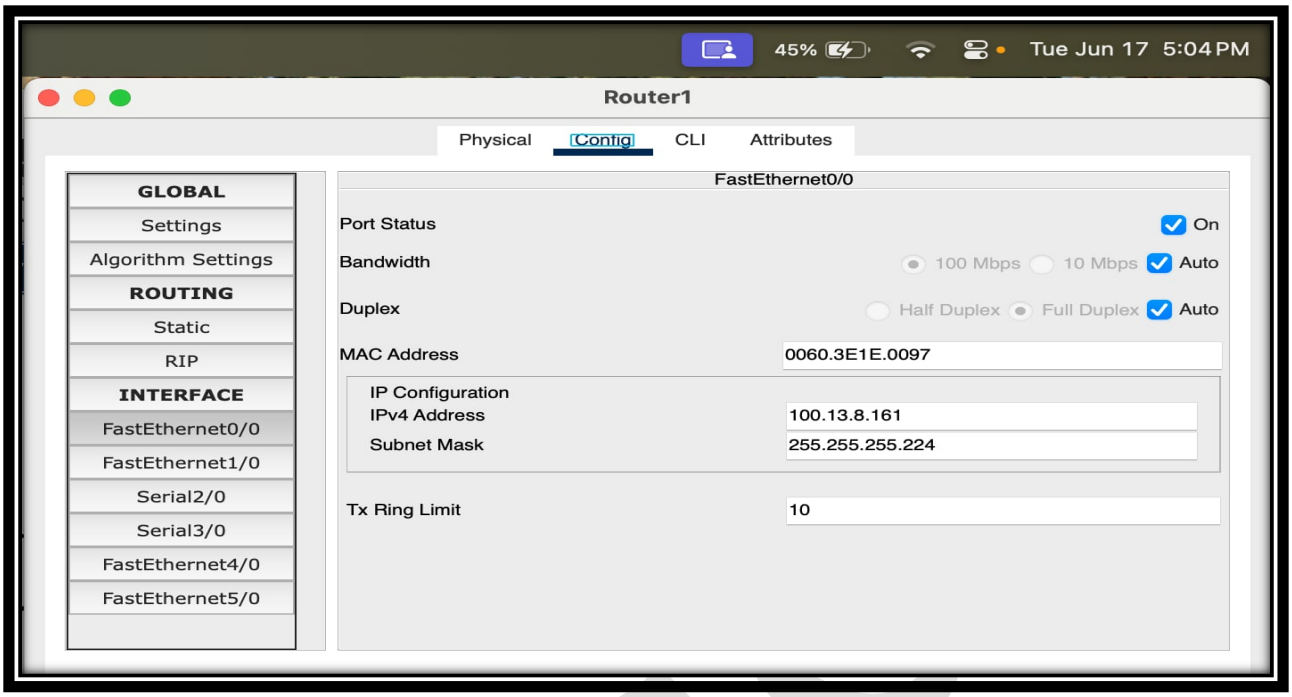


Figure 12: IP Configuration for FastEthernet0/0

Router1 – FastEthernet0/0 Interface Configuration (IPv4)

This image shows the **IPv4 configuration** of the **FastEthernet0/0 interface** on **Router1**:

- **Port Status: Enabled (On)** — indicating that the interface is active and transmitting data.
- **Bandwidth:** Set to **Auto**, allowing dynamic adjustment based on network conditions.
- **Duplex:** Configured as **Auto**, supporting both half and full duplex modes as needed.
- **MAC Address: 0060.3E1E.0097** — the unique hardware identifier for this interface.
- **IPv4 Address: 100.13.8.161**
- **Subnet Mask: 255.255.255.224**

Purpose: This configuration ensures that **Router1** can properly route packets through its FastEthernet0/0 port, maintaining reliable communication within its designated subnet.

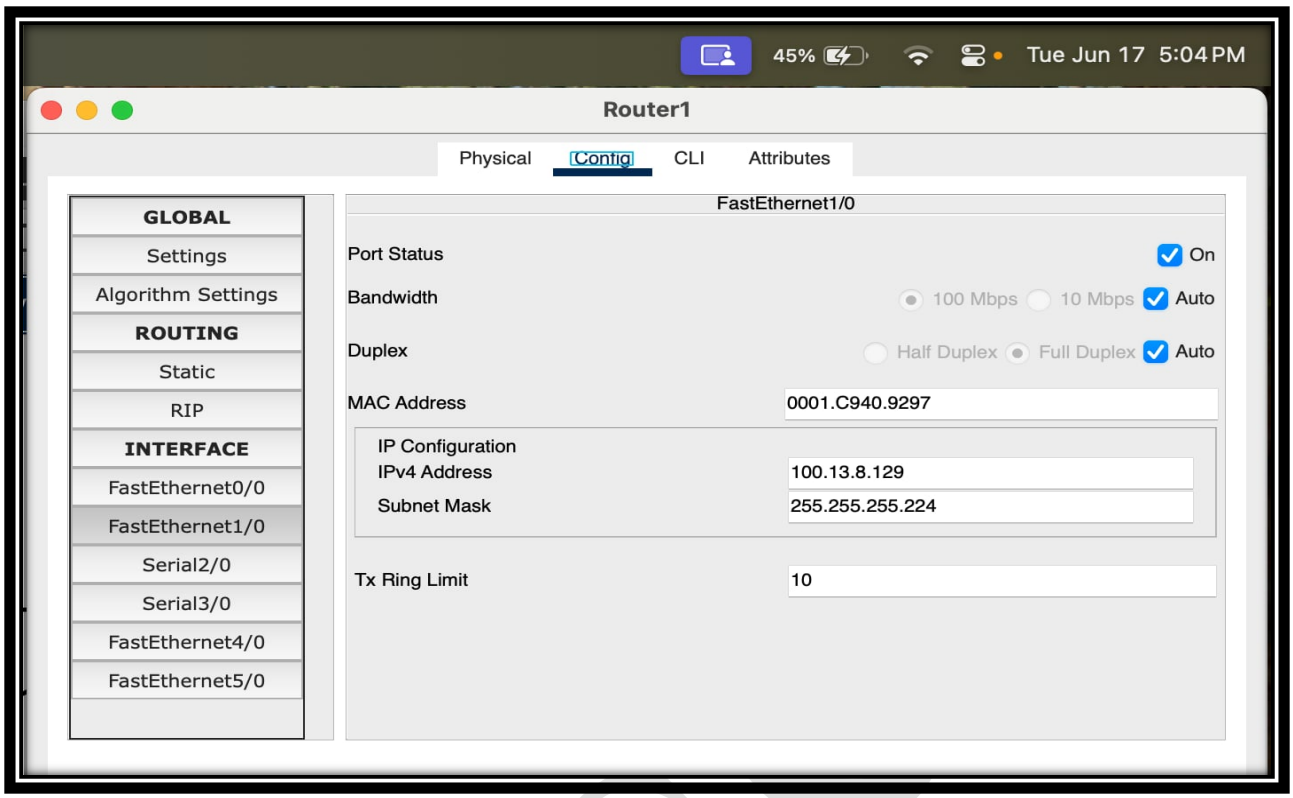


Figure 13: IP Configuration for FastEthernet1/0

Router1 – FastEthernet1/0 Interface Configuration (IPv4)

This screenshot shows the **IPv4 settings** for the **FastEthernet1/0 interface** on **Router1**:

- **Port Status: Enabled (On)** — confirming that the interface is active and transmitting data.
- **Bandwidth:** Set to **Auto**, allowing the router to adjust speed based on network requirements.
- **Duplex:** Configured as **Auto**, supporting optimal full-duplex communication as needed.
- **MAC Address: 0001.C940.9297** — the unique hardware ID for this port.
- **IPv4 Address: 100.13.8.129**
- **Subnet Mask: 255.255.255.224**

📎 **Purpose:** This configuration allows **Router1** to handle packet forwarding through the FastEthernet1/0 port, ensuring stable communication within its designated subnet.

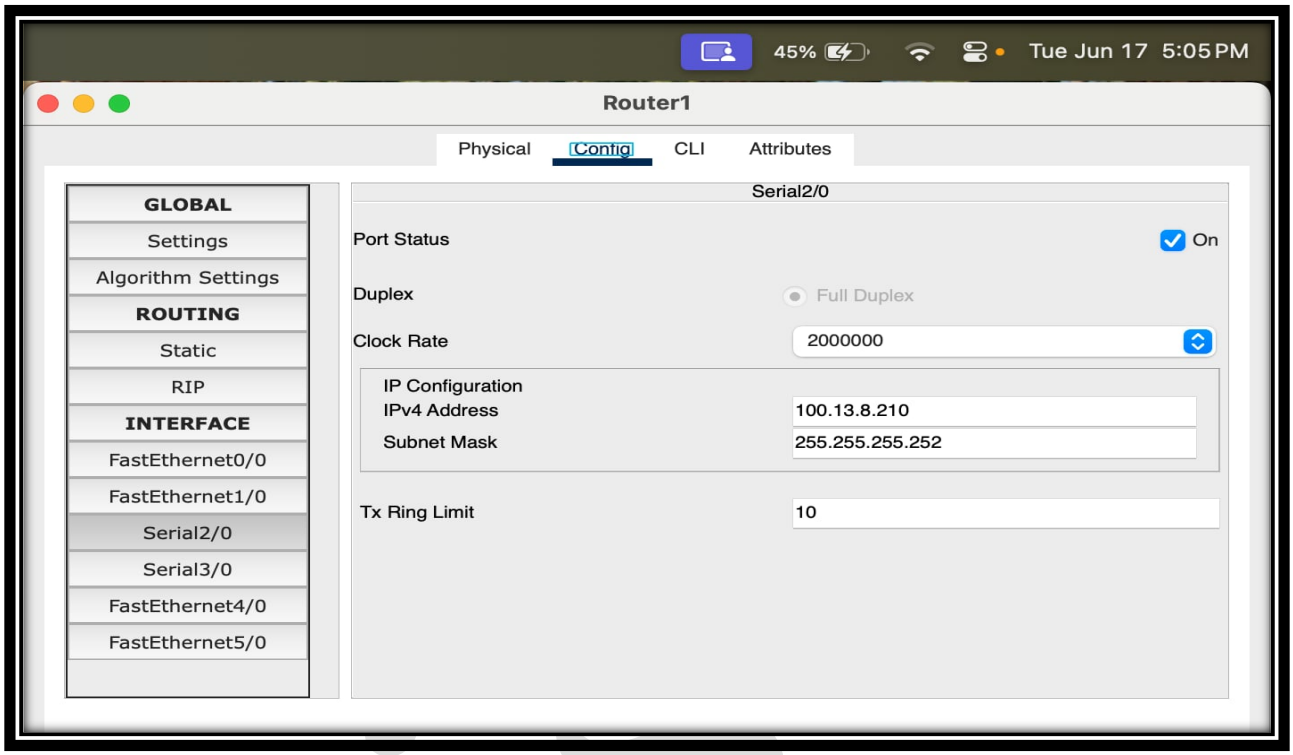


Figure 14: ⚙ IP Configuration for Serial2/0

📎 Router1 – Serial2/0 Interface Configuration (IPv4)

This screenshot shows the **IPv4 settings** for the **Serial2/0 interface** on **Router1**:

- ✅ **Port Status: Enabled (On)** — confirming that the serial link is active and ready for data transmission.
- 🔁 **Duplex: Full Duplex** (default for serial connections).
- ⏱ **Clock Rate: 2000000 bps** — defining the speed at which the serial interface transmits data.
- 📡 **IPv4 Address: 100.13.8.210**
- 📏 **Subnet Mask: 255.255.255.252**

📎 **Purpose:** This configuration allows **Router1** to establish a reliable serial link for point-to-point communication with another router, ensuring efficient data exchange over a WAN connection.

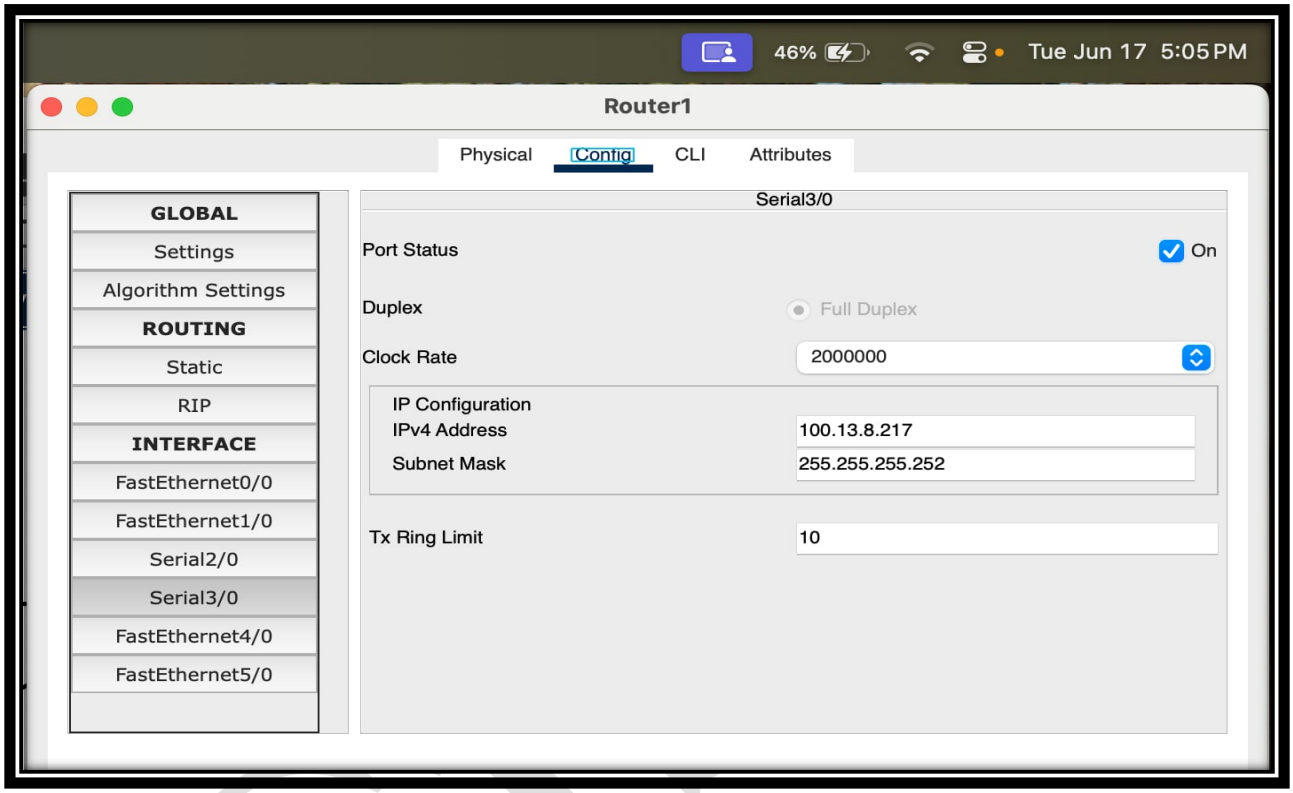


Figure 15: ⚙ IP Configuration for Serial3/0

📎 **Router1 – Serial3/0 Interface Configuration (IPv4)**

This screenshot displays the **IPv4 configuration** for the **Serial3/0 interface** on **Router1**:

- ✅ **Port Status: Enabled (On)** — indicating that the serial link is active and ready for data transmission.
- 🔁 **Duplex: Full Duplex** (standard for serial connections).
- ⏱ **Clock Rate: 2000000 bps** — defining the data transfer speed for the serial link.
- 📡 **IPv4 Address: 100.13.8.217**
- 📏 **Subnet Mask: 255.255.255.252**

📎 **Purpose:** This configuration allows **Router1** to establish a stable point-to-point serial connection with another router, ensuring efficient data communication over the WAN.

- **IP configuration for R2**

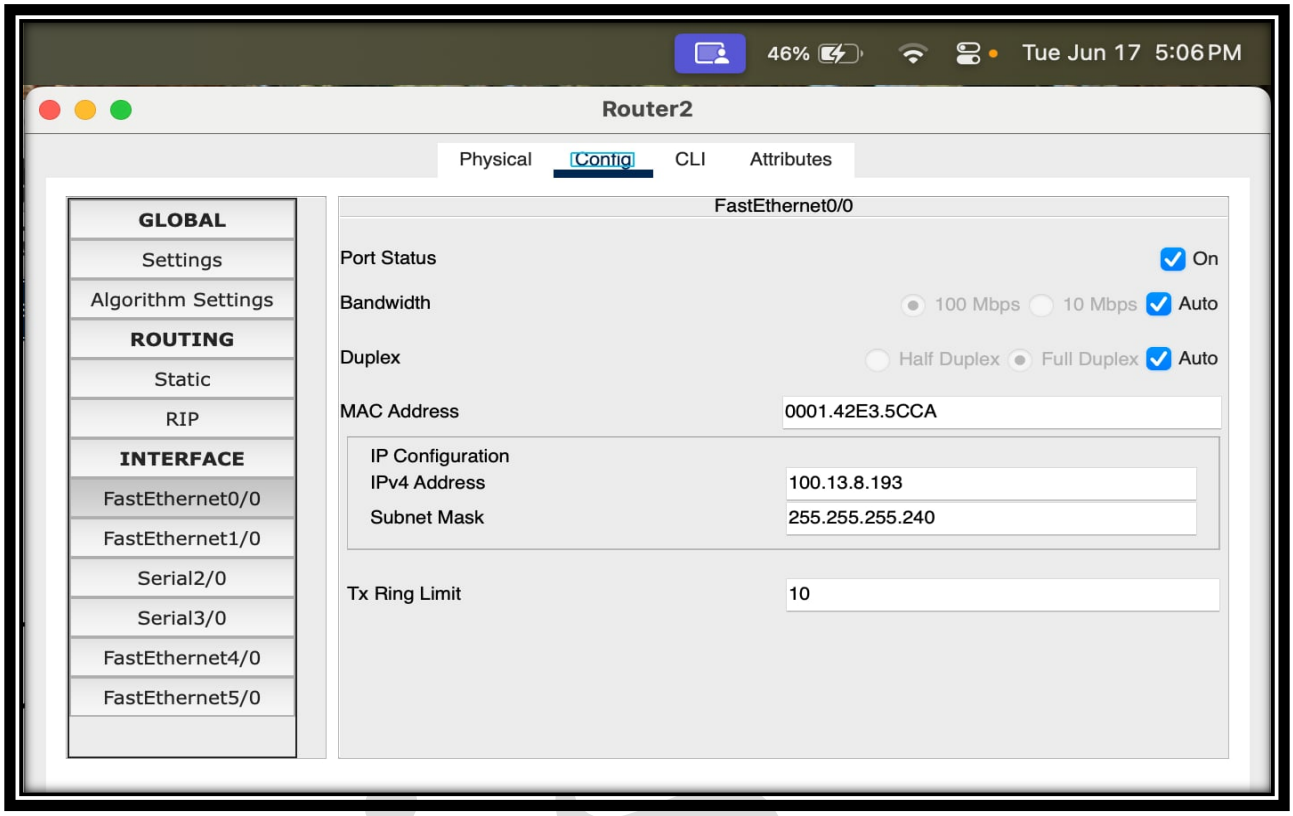


Figure 16: IP Configuration for FastEthernet0/0 R2

Router2 – FastEthernet0/0 Interface Configuration (IPv4)

This screenshot shows the **IPv4 configuration** for the **FastEthernet0/0 interface** on **Router2**:

- **Port Status: Enabled (On)** — indicating that the Ethernet port is active and operational.
- **Bandwidth:** Set to **Auto**, allowing dynamic speed adjustment as needed.
- **Duplex: Auto**, supporting both half and full duplex modes for optimal performance.
- **MAC Address: 0001.42E3.5CCA** — the unique hardware identifier for this port.
- **IPv4 Address: 100.13.8.193**
- **Subnet Mask: 255.255.255.240**

Purpose: This configuration ensures that **Router2** can handle data traffic through its FastEthernet0/0 interface, maintaining stable communication within its assigned subnet.

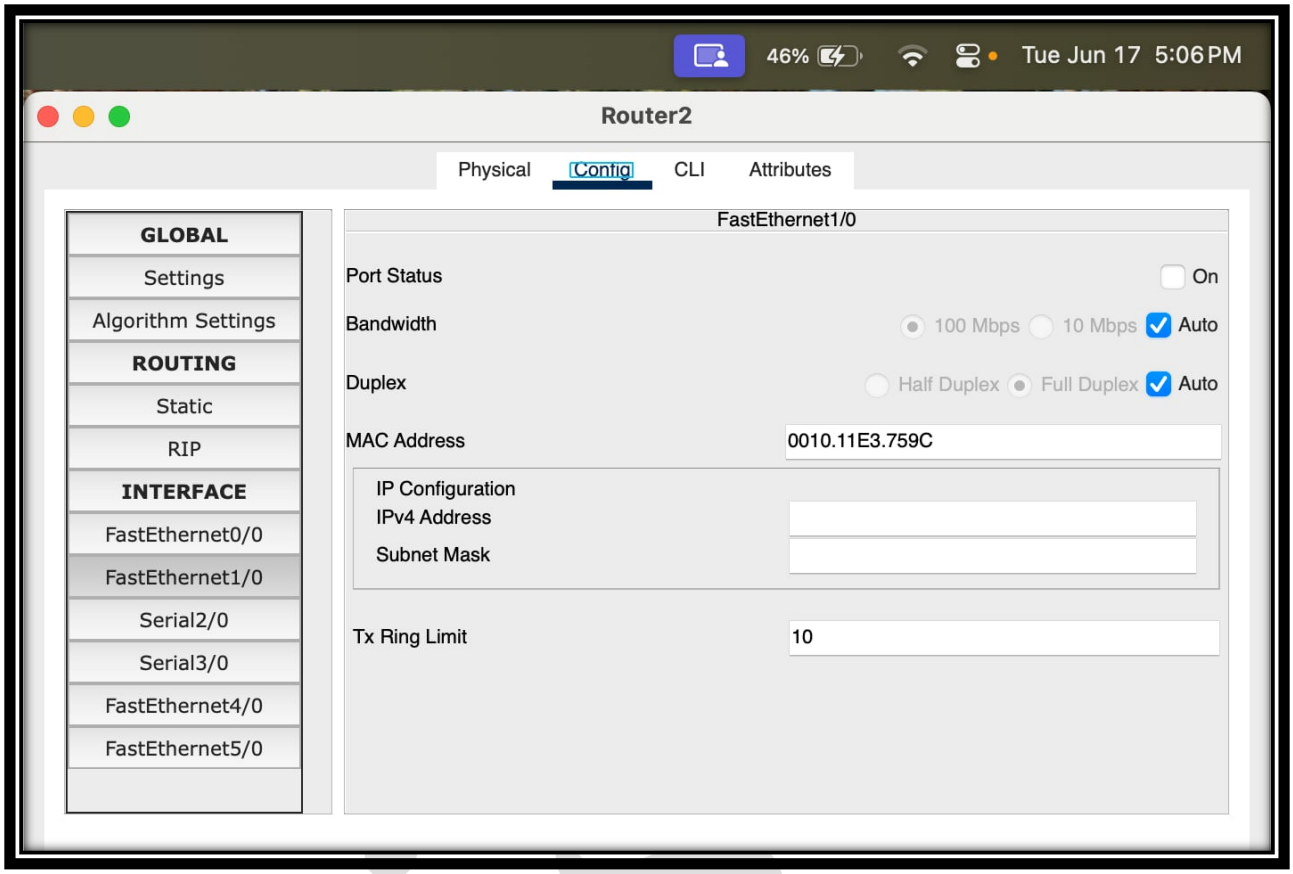


Figure 17: ⚙ IP Configuration for FastEthernet1/0 R2

⚙ Router2 – FastEthernet1/0 Interface Configuration (IPv4)

This screenshot shows the current status of the **FastEthernet1/0 interface** on **Router2**:

- ✕ **Port Status: Disabled (Off)** — indicating that this Ethernet port is currently inactive and not transmitting data.
- ⚡ **Bandwidth:** Configured as **Auto**, ready to adjust when the port is enabled.
- 🔁 **Duplex:** Set to **Auto**, allowing the interface to switch between half and full duplex as needed once active.
- 🏷 **MAC Address: 0010.11E3.759C** — the unique hardware identifier for this interface.
- 📡 **IPv4 Address: Not Assigned** — currently empty because the port is turned off.
- 📏 **Subnet Mask: Not Assigned**

🔗 **Note:** This port is available for future configurations or as a backup link when required.

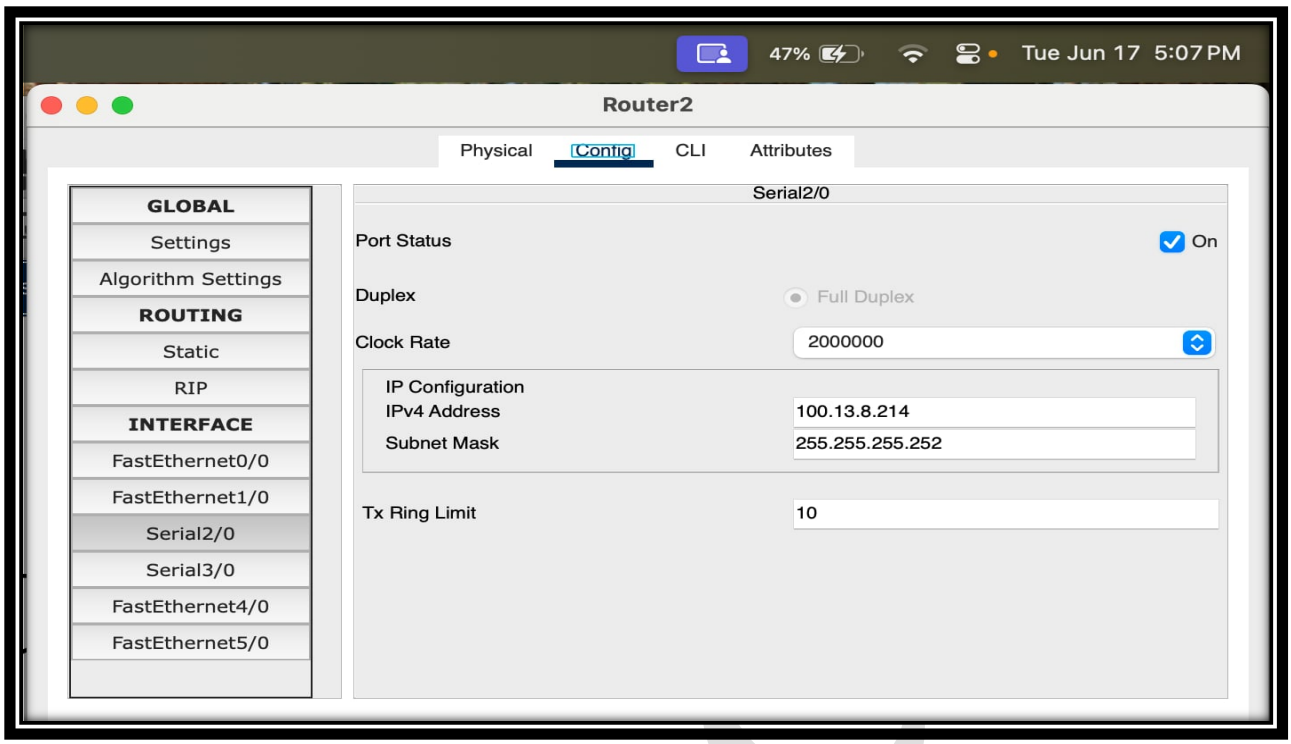


Figure 18: IP Configuration for Serial2/0

Router2 – Serial2/0 Interface Configuration (IPv4)

This screenshot displays the **IPv4 configuration** for the **Serial2/0 interface** on **Router2**:

- **Port Status: Enabled (On)** — indicating that the serial link is active and ready for data transfer.
- **Duplex: Full Duplex** (standard for serial interfaces).
- **Clock Rate: 2000000 bps** — defining the speed of the serial transmission.
- **IPv4 Address: 100.13.8.214**
- **Subnet Mask: 255.255.255.252**

Purpose: This setup enables **Router2** to establish a reliable point-to-point serial connection with another router, ensuring consistent data communication over the WAN link.

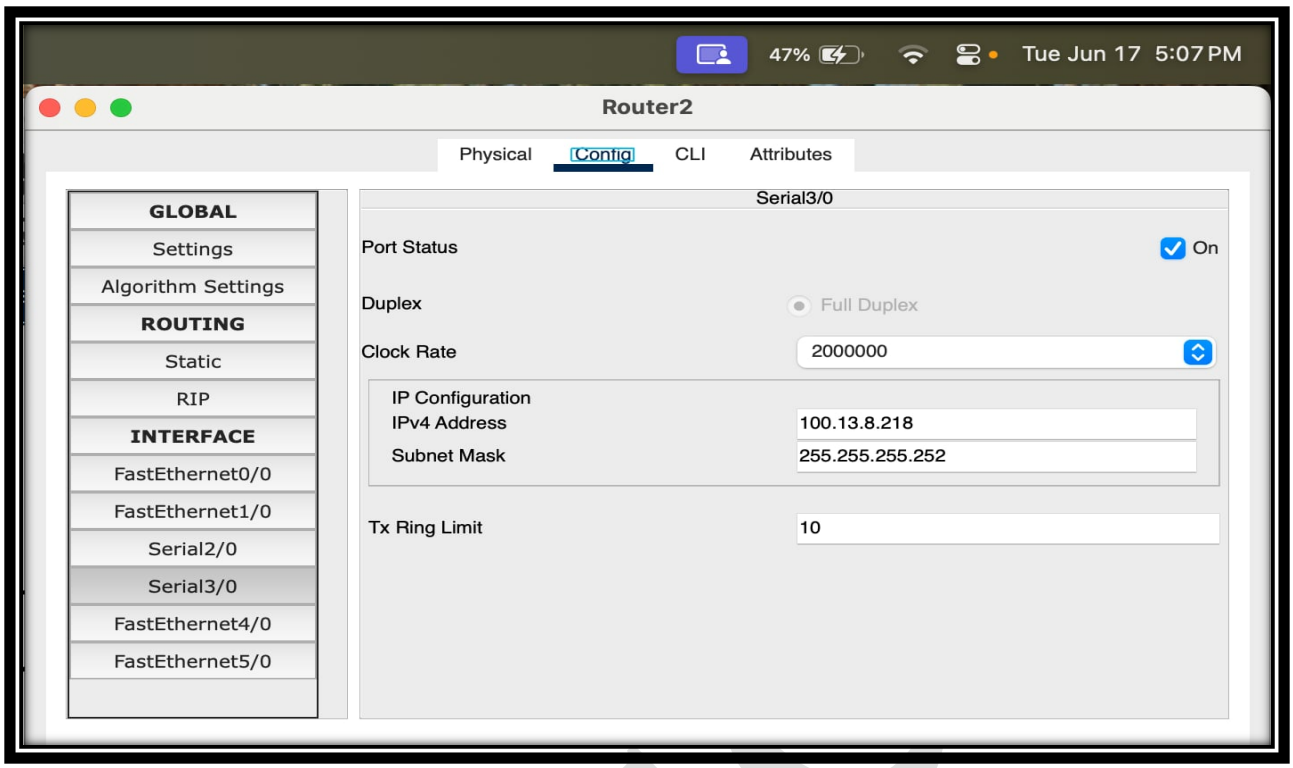


Figure 19: IP Configuration for Serial3/0

Router2 – Serial3/0 Interface Configuration (IPv4)

This screenshot shows the **IPv4 configuration** for the **Serial3/0 interface** on **Router2**:

- **Port Status: Enabled (On)** — confirming that the serial interface is active and transmitting data.
- **Duplex: Full Duplex** (default for serial connections).
- **Clock Rate: 2000000 bps** — specifying the speed of the serial link.
- **IPv4 Address: 100.13.8.218**
- **Subnet Mask: 255.255.255.252**

Purpose: This setup allows **Router2** to establish a stable point-to-point serial link with another router, ensuring secure and efficient data communication across the WAN

➢ University network (Area 1)

The **University Network (Area 1)** is organized into two logical sub-networks: **NET1-A** and **NET1-B**. This area ensures **connectivity** for **desktop users**, **mobile devices**, and provides access to essential services such as **DHCP**.

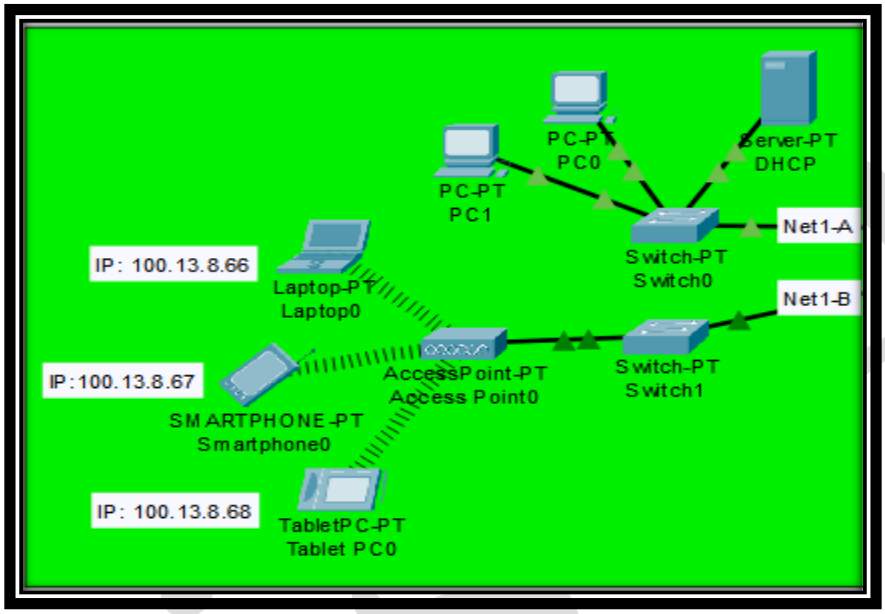


Figure 20: University network

1) NET1-A:

This segment represents the **wired portion** of the university's local network. It includes:

• **Two PCs** (**PC4** and **PC5**) connected through a **Switch**.

• A **Server** configured as a **DHCP server**.

• The DHCP server connects to the switch via **interface Fa0**.

• Both PCs use **FastEthernet interfaces (Fa0)** and are set to obtain **IP addresses dynamically** through DHCP.

• A **standard Switch-PT** is used to interconnect the PCs and server, linking to the rest of the network via its **uplink port Fa3/1**.

- **IP Configuration for DHCP**

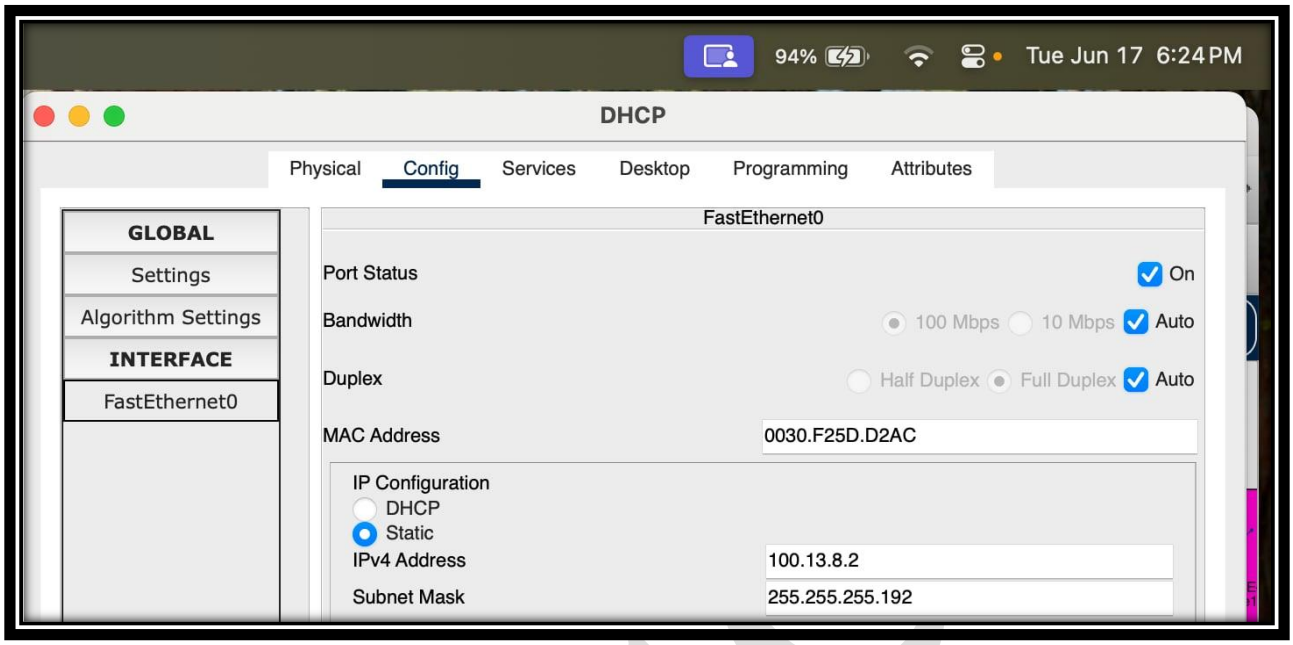


Figure 21: DHCP Server – Interface Settings

DHCP Server – Interface Settings

This screenshot shows the **FastEthernet0** interface configuration for the **DHCP Server**:

- **Port Status: On** — The interface is enabled and active.
- **Bandwidth: Auto** — Automatically adjusts the link speed.
- **Duplex: Auto** — Uses automatic full or half duplex as needed.
- **MAC Address:** 0030.F25D.D2AC — Unique identifier for this interface.
- **IP Configuration:**
  - **Static** — The server uses a fixed IP address.
  - **IPv4 Address:** 100.13.8.2
  - **Subnet Mask:** 255.255.255.192

Purpose:

This configuration ensures that the **DHCP Server** is reachable on a stable, predefined IP address and can assign IP addresses dynamically to other devices in the network.

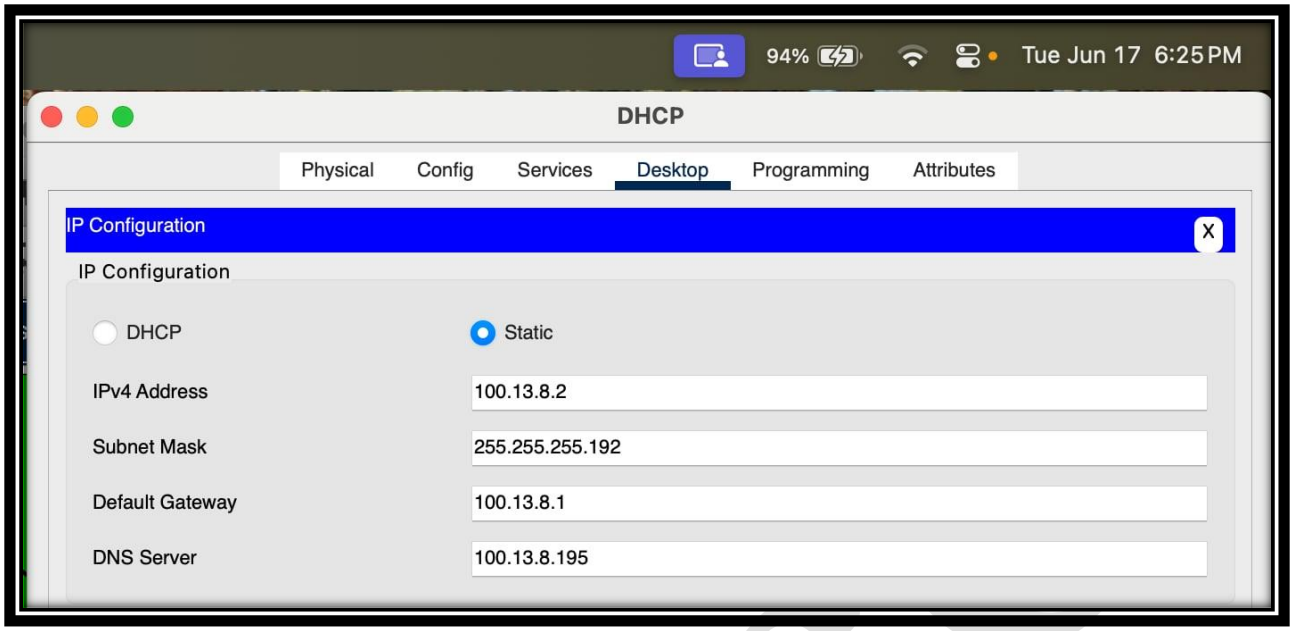


Figure 22: DHCP Server – IP Configuration

DHCP Server – IP Configuration

This screenshot shows the **IP Configuration** under the **Desktop** tab for the **DHCP Server**:

- **Static:** The server uses a manually assigned IP address (not from DHCP).
- **IPv4 Address:** 100.13.8.2 — The server's static IP on the network.
- **Subnet Mask:** 255.255.255.192 — Defines the network size.
- **Default Gateway:** 100.13.8.1 — The router's IP for forwarding packets outside this network.
- **DNS Server:** 100.13.8.195 — The IP address of the DNS server used to resolve domain names.

Purpose:

This configuration allows the **DHCP Server** to have a fixed network identity and proper routing and DNS resolution, while it dynamically assigns IP addresses to client devices.

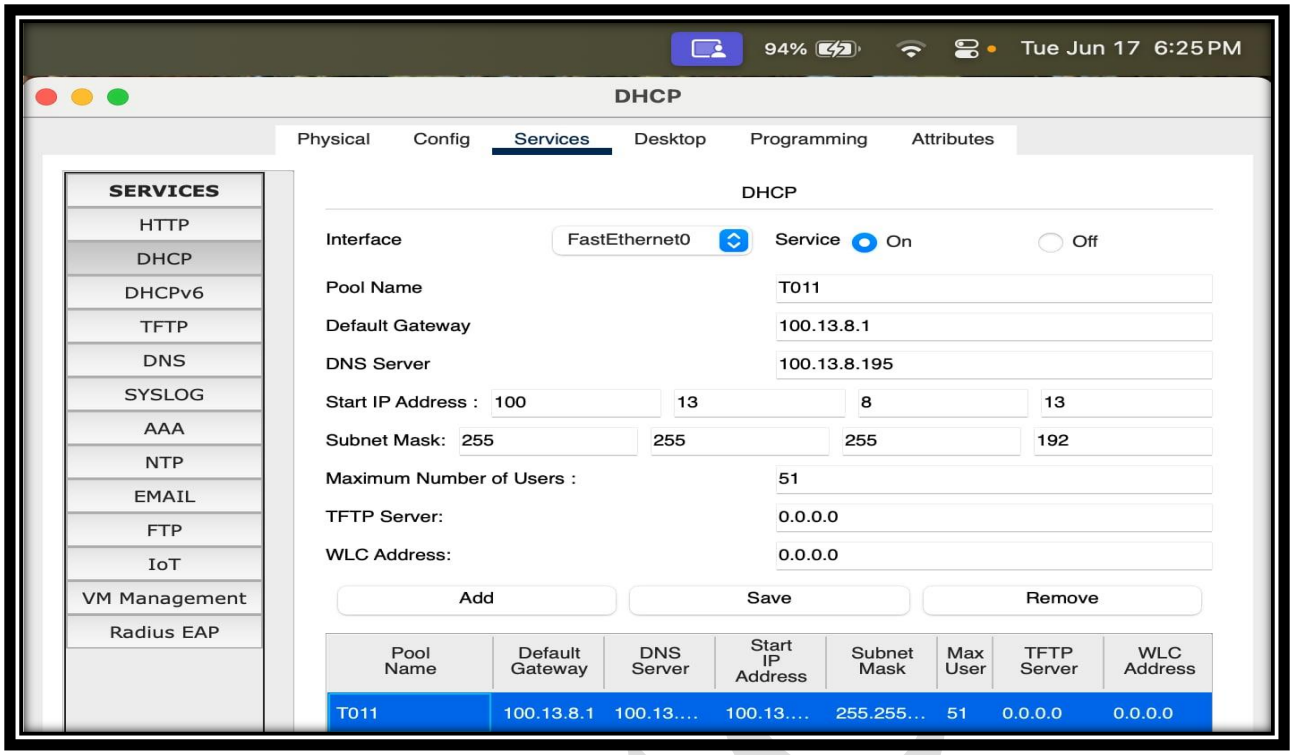


Figure 23: DHCP Server – Services Tab

DHCP Server – Services Tab

This screenshot shows the **DHCP service configuration** on the server:

- ✅ **Service: On** — The DHCP service is enabled to automatically assign IP addresses to clients.
- 🏷️ **Pool Name:** T011 — The name of the DHCP address pool.
- 🖥️ **Default Gateway:** 100.13.8.1 — The router's IP address, given to clients as their gateway.
- 🌍 **DNS Server:** 100.13.8.195 — The DNS server IP that will be assigned to clients.
- 📌 **Start IP Address:** 100.13.8.13 — The first IP address in the pool that DHCP can assign.
- 📏 **Subnet Mask:** 255.255.255.192 — Defines the network size and host range.
- 👥 **Maximum Number of Users:** 51 — The maximum number of devices that can receive an IP from this pool.
- 📂 **TFTP Server & WLC Address:** 0.0.0.0 — Not configured in this setup.

🔑 **Purpose:**
This configuration allows the DHCP server to **automatically manage and distribute IP addresses** and network settings (gateway & DNS) to client devices, making network management easier and more efficient.

2) Net1-B:

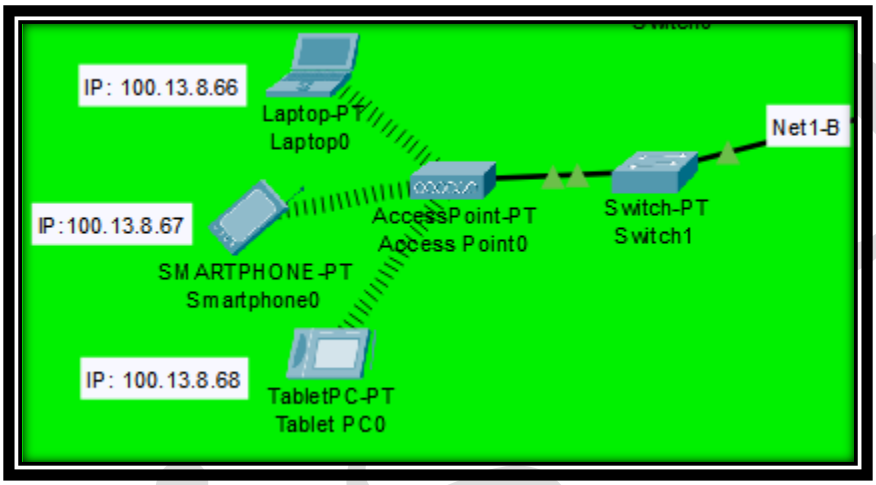


Figure 24: NET1-B System

📶 **Wireless Subnet (Net1-B)** — In this part of the project, you can see three devices:
💻 **Laptop** (IP: 100.13.8.66),
📱 **Smartphone** (IP: 100.13.8.67), and
📲 **Tablet** (IP: 100.13.8.68).

All these devices connect **wirelessly** to an **Access Point** 📡. The Access Point is then connected by cable to a **Switch** 🔗, which links them to the rest of the network.

🗂️ **DHCP Service** is working here ✅ — it automatically assigns IP addresses to each device, so users don't need to set them manually.

📡➡️🔀➡️🌐 **Summary:** This shows how the wireless side supports mobility and easy connectivity, allowing different wireless devices to join the main network **efficiently** and **securely**!

- **Setting for Access point**

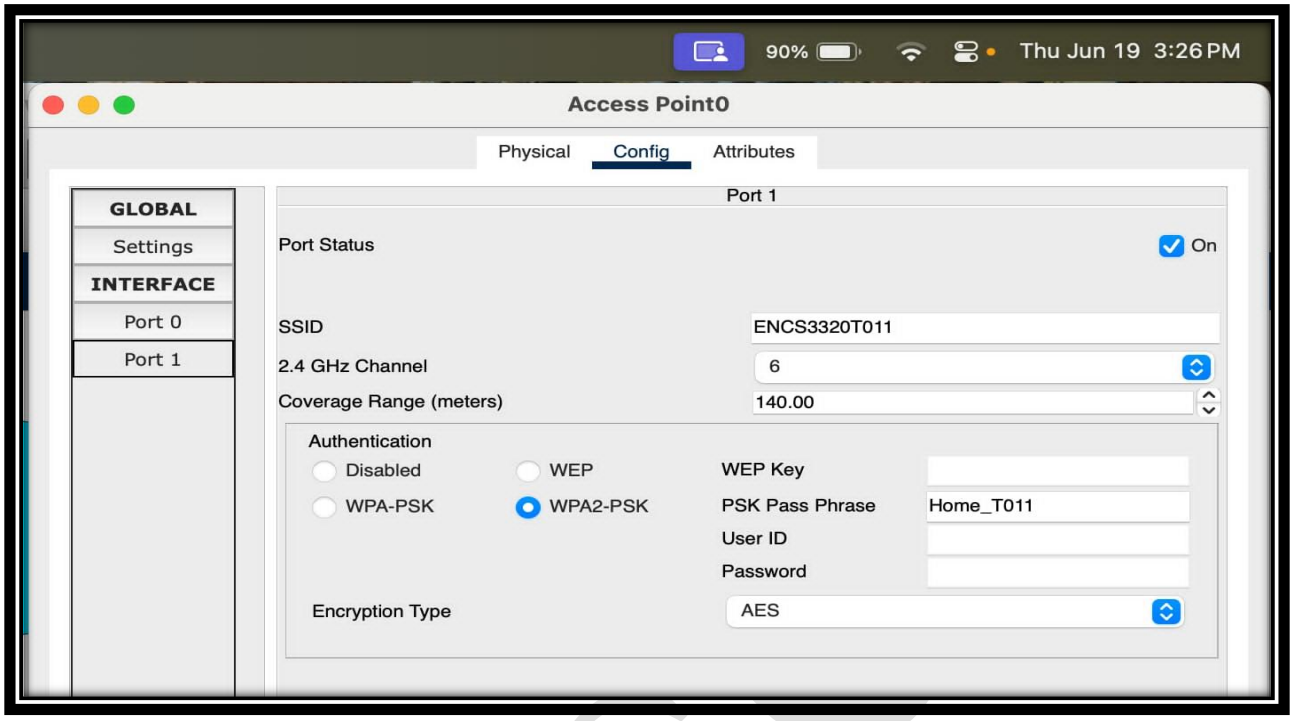


Figure 25: Access Point Setting

This screenshot shows the **configuration** ⚙️ of **Access Point0**, which is responsible for providing **secure wireless connectivity** 📶 in the network:

🔑 **Key Details:**

- ✅ **Port Status: On** — The AP is active and broadcasting.
- 📡 **SSID: ENCS3320T011** — This is the **network name** clients will see and connect to.
- 📶 **2.4 GHz Channel: 6** — Controls the frequency band, ensuring minimal interference.
- 📏 **Coverage Range: 140 meters** — Determines how far the Wi-Fi signal reaches.
- 🔒 **Authentication: WPA2-PSK** — A secure method for wireless authentication, better than WEP or WPA.
- 🔑 **PSK Pass Phrase: Home_T011** — The Wi-Fi password for client devices to connect.
- 🔐 **Encryption Type: AES** — Provides strong encryption for data security.

✅ **Summary:**

This configuration ensures that **wireless devices** (📱💻) can connect **securely and reliably** to the network using modern encryption and a controlled coverage area, maintaining **performance and security** throughout the wireless zone! 🔐✨📡

➢ Street Network (Area 2)

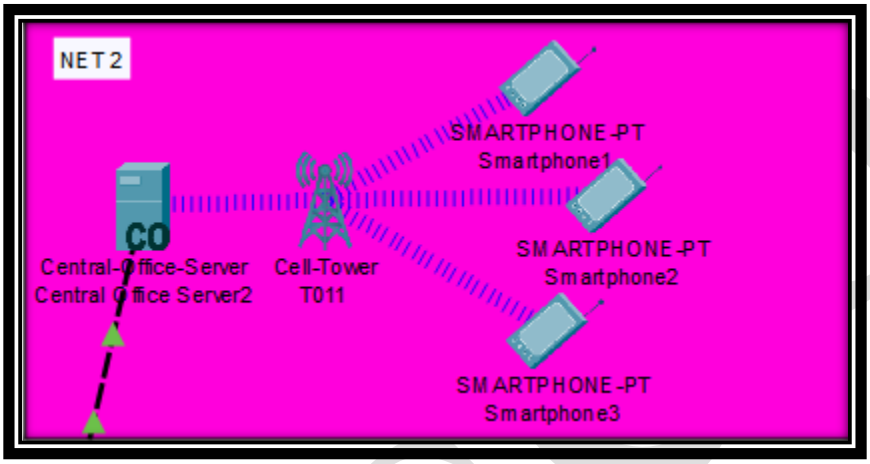


Figure 26: Street Network

📡 **NET2 (Mobile Network)** — This part of the project shows how **mobile smartphones** connect wirelessly to the network through a **Cell Tower** 🗼 (**T011**).

🖥️ **Central Office Server** 🖥️ — All the smartphones communicate with the **Central Office Server**, which acts like a control center. It handles their connections, manages data flow, and ensures secure access to network resources.

📎 **How it works:**

1️⃣ Smartphones send and receive signals via the **Cell Tower** 🗼.

2️⃣ The Cell Tower is linked to the **Central Office Server** 🖥️ through a secure wired link 📎.

3️⃣ This setup makes sure mobile users stay **connected anywhere** within the tower's range with good signal and stable services.

✅ **Purpose:** NET2 demonstrates **mobile network integration** into the main infrastructure, supporting **mobility**, **continuous access**, and smooth data communication for mobile users. 🌐📶✨

➢ Home Network (Area 3)

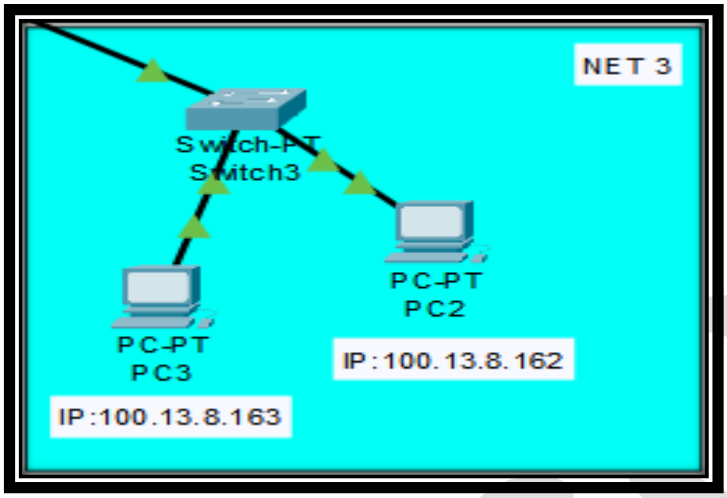


Figure 27: Home Network

🖥️ **NET3 (Wired Office Network)** — This part shows a simple **wired local area network (LAN)** for **office PCs**.

✒️ **Components:**

- **PC2** 💻 (IP: 100.13.8.162)
- **PC3** 💻 (IP: 100.13.8.163)
- **Switch3** 🔀 — This switch connects the PCs together and links them to the main network backbone.

📎 **How it works:**

1️⃣ Both PCs are physically connected to **Switch3** 🔀 using network cables.
2️⃣ **Switch3** manages the data flow between the PCs, allowing them to share files and communicate easily at high speed.
3️⃣ This wired setup ensures **reliable and secure communication** within the office.

✅ **Purpose:** NET3 demonstrates a **typical office LAN** 🏢 where multiple computers are networked through a **switch** for stable and fast data exchange, ideal for everyday office work. 🗂️💼✨

➢ Datacenter Network (Area 4)

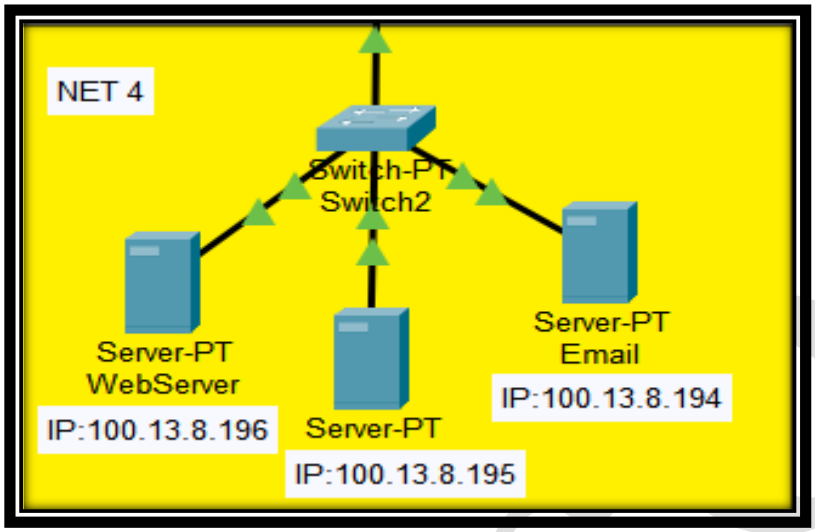


Figure 28: Datacenter Network

🗂️🖥️ **NET4 (Server Network)** — This part illustrates a **dedicated network segment for servers**, ensuring that important services run smoothly and securely.

📡 **Components:**

- **WebServer** 🌐 (IP: 100.13.8.196) — Hosts websites and web applications.
- **DNS Server** 🗂️ (IP: 100.13.8.195) — Translates domain names into IP addresses for users.
- **Email Server** ✉️ (IP: 100.13.8.194) — Manages sending and receiving emails for the network.
- **Switch2** 🔀 — Connects all servers together and links them to the rest of the network.

⚙️ **How it works:**

1️⃣ Each server provides a **specific service** essential for the whole network (web, email, domain name resolution).

2️⃣ **Switch2** 🔀 ensures fast and reliable connections between servers and users, minimizing downtime.

3️⃣ Keeping servers in a **dedicated segment** increases security and performance.

✅ **Purpose:** NET4 highlights a **centralized server farm** 🏢🗂️ designed to support web browsing, email communication, and domain name resolution, making the network efficient and user-friendly. 🌟✨

➢ Dynamic IP configuration for some of end devices

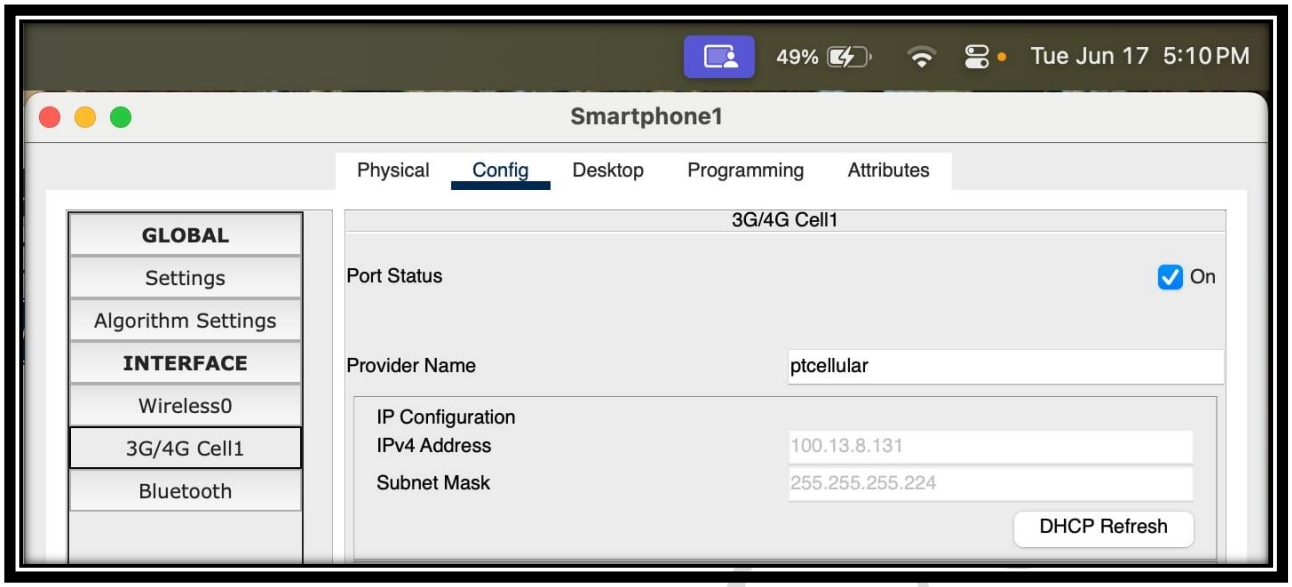


Figure 29: Smartphone1 (3G/4G) Cell1 Interface Configuration

In our report the dynamic IP configuration it only in NET 2.

Smartphone1 – 3G/4G Cell1 Interface Configuration (IPv4)

This screenshot shows the **IPv4 configuration** of the **3G/4G Cell1 interface** on **Smartphone1**:

- **Provider Name: ptcellular**, which supplies the mobile network connection for this device.
- **IPv4 Address: 100.13.8.131**
- **Subnet Mask: 255.255.255.224**
- **Port Status: Enabled (On)** — indicating that the cellular interface is active and functioning properly.
- **Purpose:** This configuration allows **Smartphone1** to connect to the mobile network and communicate with other devices and services using its assigned **IPv4** address.

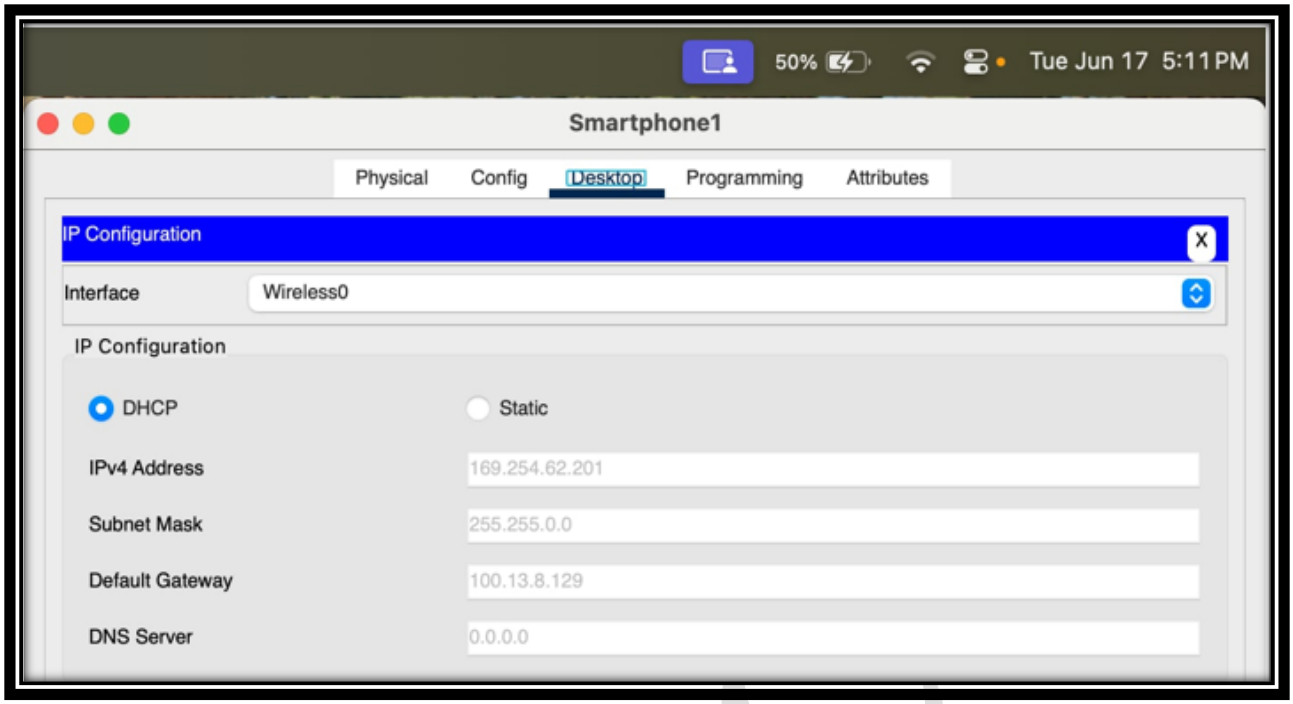


Figure 30: Smartphone1 (Wireless0 Interface Configuration)

Smartphone1 – Wireless0 Interface Configuration (IPv4)

This screenshot shows the **Wireless0 interface** settings for **Smartphone1**, focusing on its **IPv4 configuration**:

- **IP Configuration: DHCP** is enabled, allowing the device to automatically obtain network settings.
- **IPv4 Address: 169.254.62.201**
- **Subnet Mask: 255.255.0.0**
- **Default Gateway: 100.13.8.129**
- **DNS Server: 0.0.0.0** (no manual DNS configured)

Purpose: This setup ensures that **Smartphone1** can dynamically connect to the wireless network and communicate within its subnet using automatically assigned IP settings.

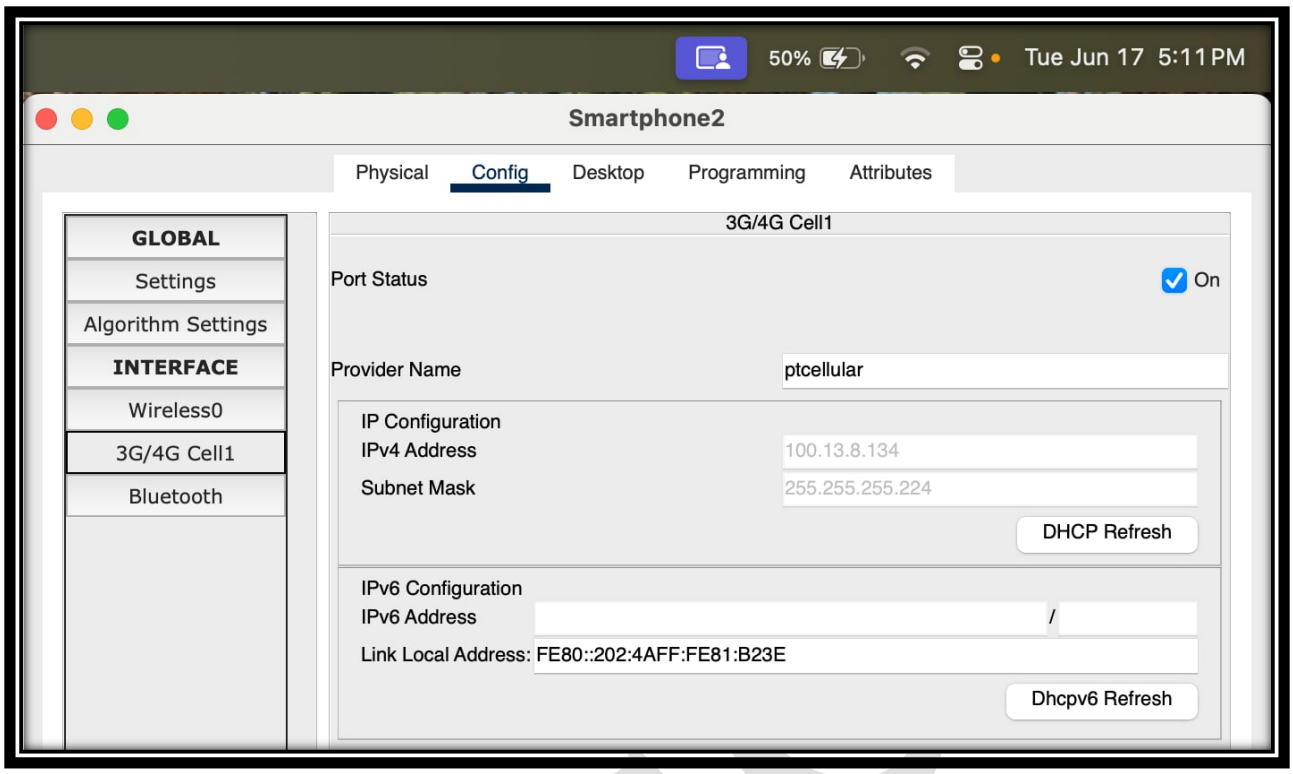


Figure 31: Smartphone2 – 3G/4G Cell1 Interface

Smartphone2 – 3G/4G Cell1 Interface Configuration (IPv4)

This screenshot displays the **IPv4 configuration** of the **3G/4G Cell1 interface** on **Smartphone2**:

- **Provider Name: ptcellular**, which provides mobile network connectivity for the device.
- **IPv4 Address: 100.13.8.134**
- **Subnet Mask: 255.255.255.224**
- **Port Status: Enabled (On)** — indicating that the cellular interface is active and functional.

Purpose: This configuration allows **Smartphone2** to access the mobile network and communicate with other devices and services using its assigned **IPv4 address** over the cellular connection.

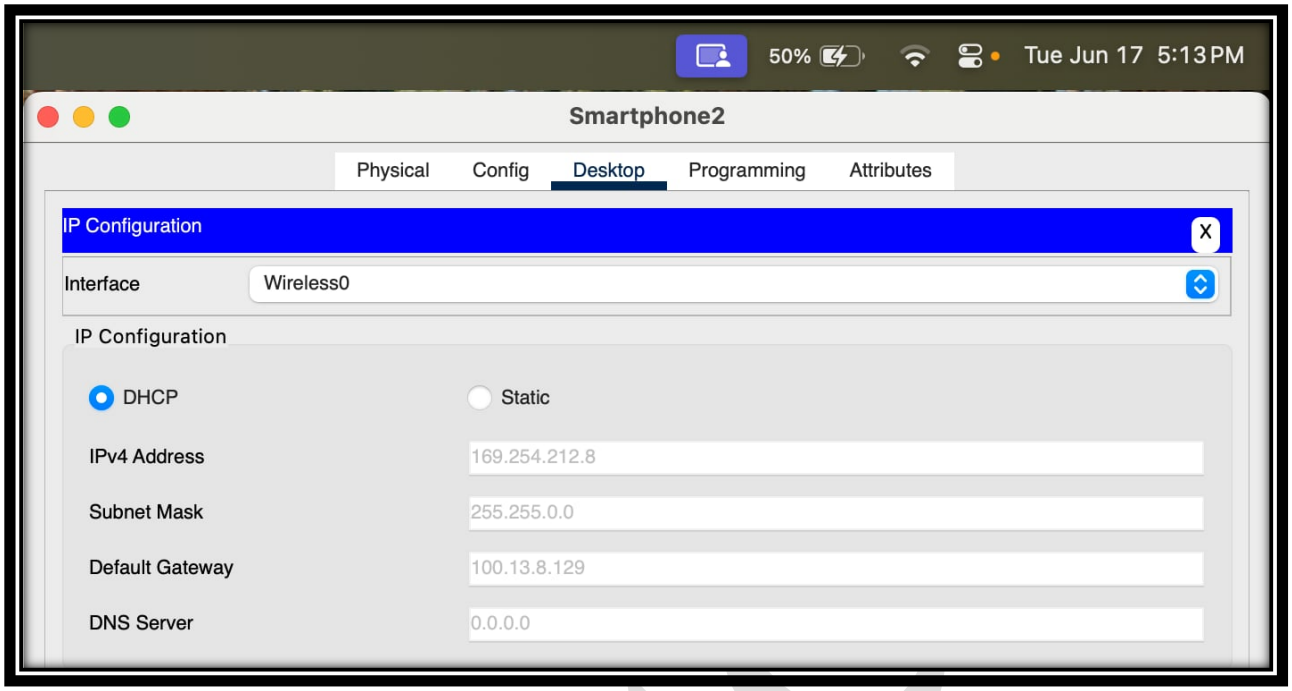


Figure 32: Smartphone2 (Wireless0 Interface Configuration)

Smartphone2 – Wireless0 Interface Configuration (IPv4)

This screenshot displays the **Wireless0 interface** settings for **Smartphone2**, focusing on its **IPv4 configuration**:

- **IP Configuration: DHCP** is enabled, allowing the device to automatically receive its network settings.
- **IPv4 Address: 169.254.212.8**
- **Subnet Mask: 255.255.0.0**
- **Default Gateway: 100.13.8.129**
- **DNS Server: 0.0.0.0** (no manual DNS specified)

Purpose: This configuration ensures that **Smartphone2** can connect dynamically to the wireless network and communicate within its subnet using automatically assigned IP details.

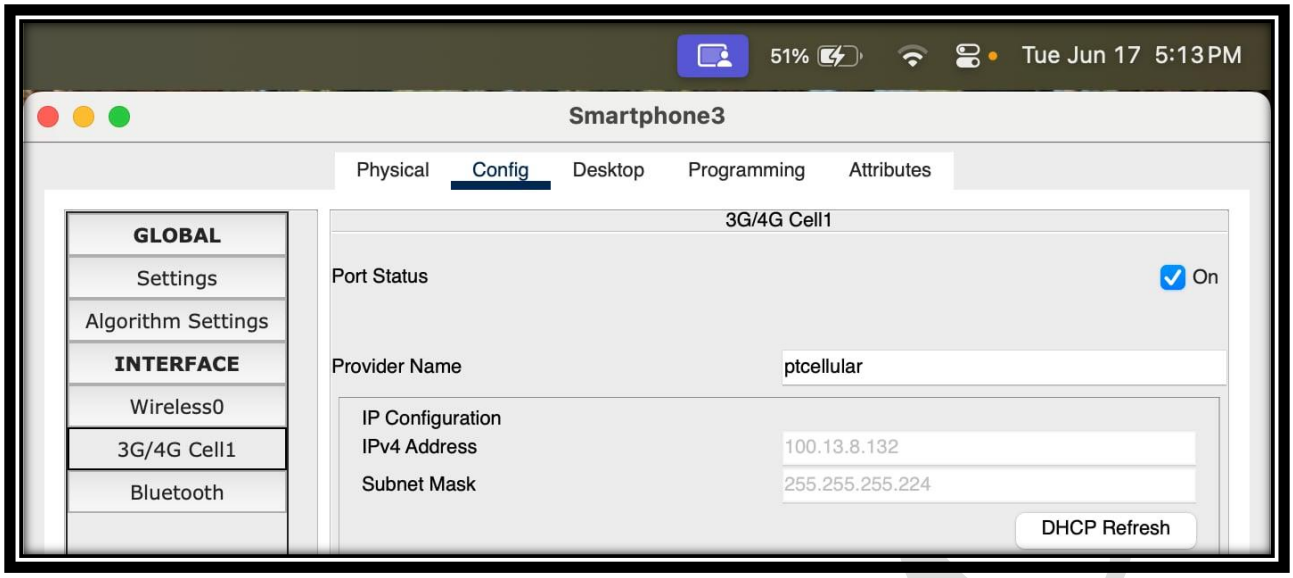


Figure 33: Smartphone3 – 3G/4G Cell1 Interface Configuration (IPv4)

Smartphone3 – 3G/4G Cell1 Interface Configuration (IPv4)

This section provides the detailed **IPv4 configuration** of the **3G/4G Cell1** interface on **Smartphone3**:

- **Network Provider: ptcellular**, which supplies reliable mobile network connectivity for the device.
- **IPv4 Address: 100.13.8.132**
- **Subnet Mask: 255.255.255.224**
- **Port Status: Enabled (On)** — confirming that the cellular interface is active and functioning correctly.
- **Purpose:** With this configuration, **Smartphone3** can seamlessly access network resources, exchange data, and communicate with other devices using its **IPv4 address** via the **3G/4G cellular connection**.

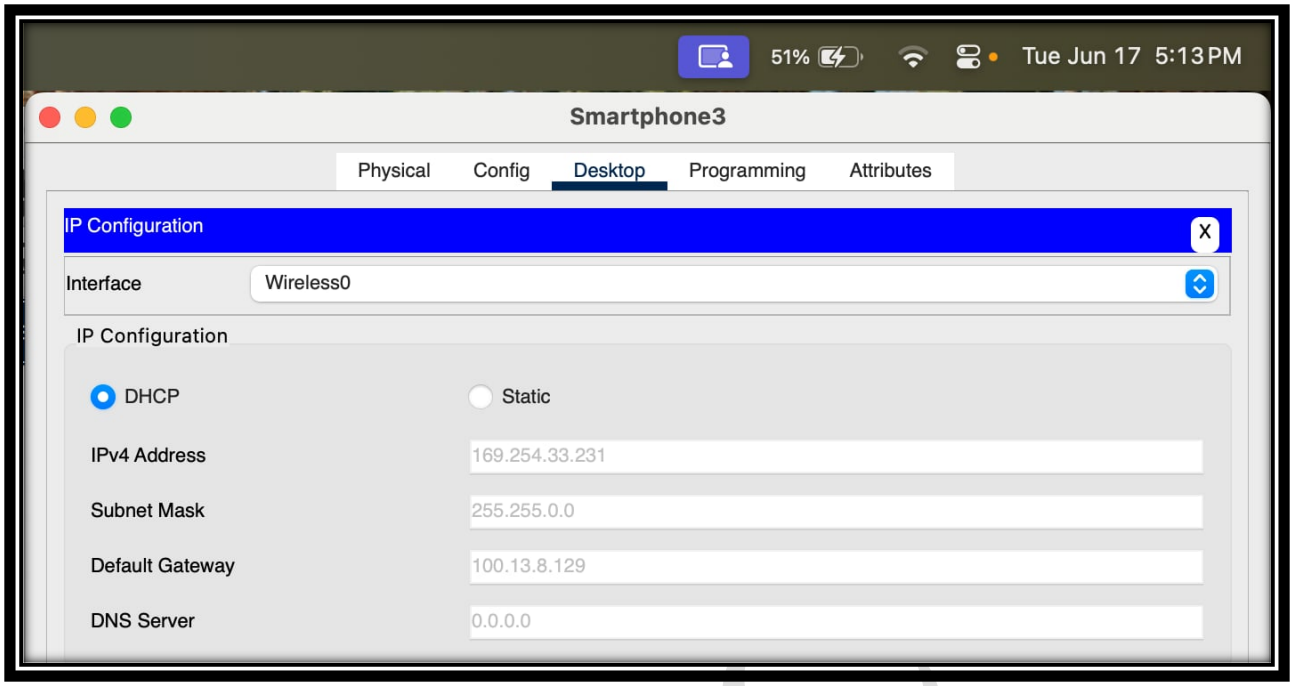


Figure 34: Smartphone3 – Wireless0 Interface Configuration (IPv4)

Smartphone3 – Wireless0 Interface Configuration (IPv4)

This section describes the **IPv4 configuration** of the **Wireless0 interface** on **Smartphone3**:

- **IP Configuration: DHCP** is enabled, allowing the device to automatically receive its network settings.
- **IPv4 Address: 169.254.33.231**
- **Subnet Mask: 255.255.0.0**
- **Default Gateway: 100.13.8.129**
- **DNS Server: 0.0.0.0** (no DNS manually configured)
- **Purpose:** This setup ensures that **Smartphone3** can connect smoothly to the wireless network and communicate efficiently within its subnet by using dynamically assigned IP settings.

➢ IP Static Configuration for all end devices

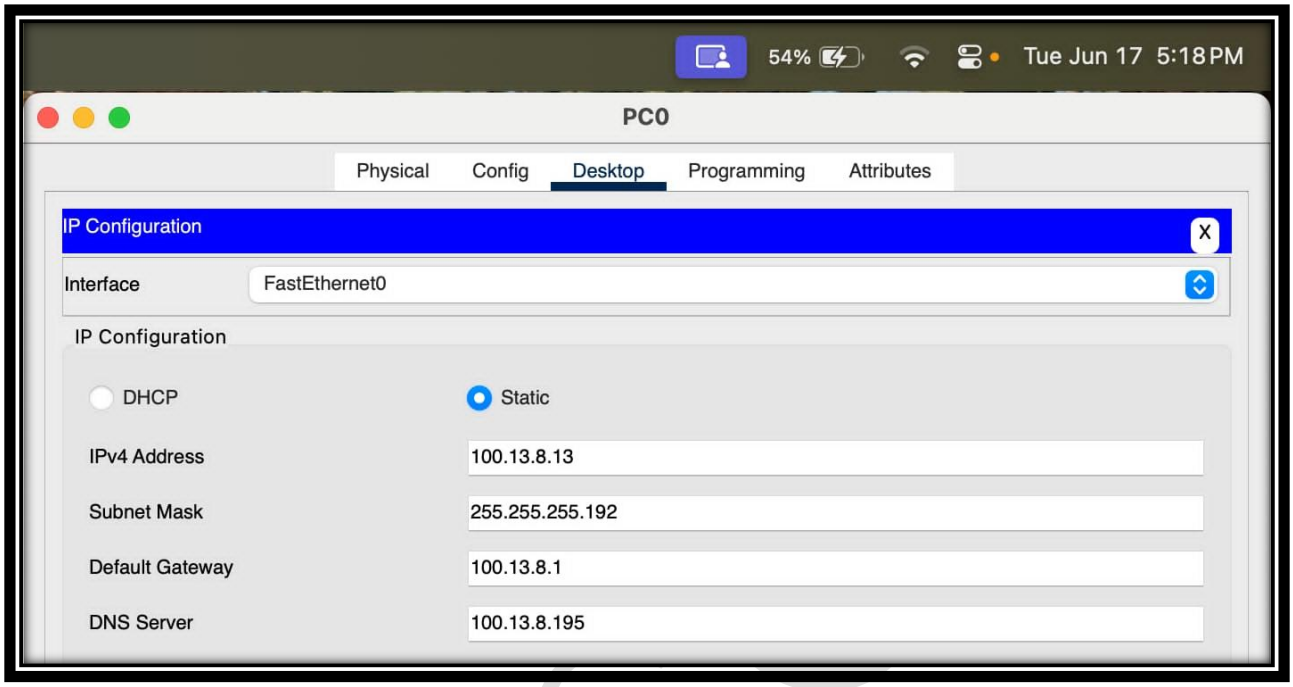


Figure 35: PC0 – FastEthernet0 Interface Configuration (IPv4)

PC0 – FastEthernet0 Interface Configuration (IPv4)

This screenshot shows the **IPv4 configuration** for the **FastEthernet0 interface** on **PC0**:

- **IP Configuration: Static**, meaning the IP settings are manually assigned.
- **IPv4 Address: 100.13.8.13**
- **Subnet Mask: 255.255.255.192**
- **Default Gateway: 100.13.8.1**
- **DNS Server: 100.13.8.195**

Purpose: This configuration ensures that **PC0** can communicate reliably within its subnet, use the default gateway for routing packets outside its network, and resolve domain names through the specified DNS server.

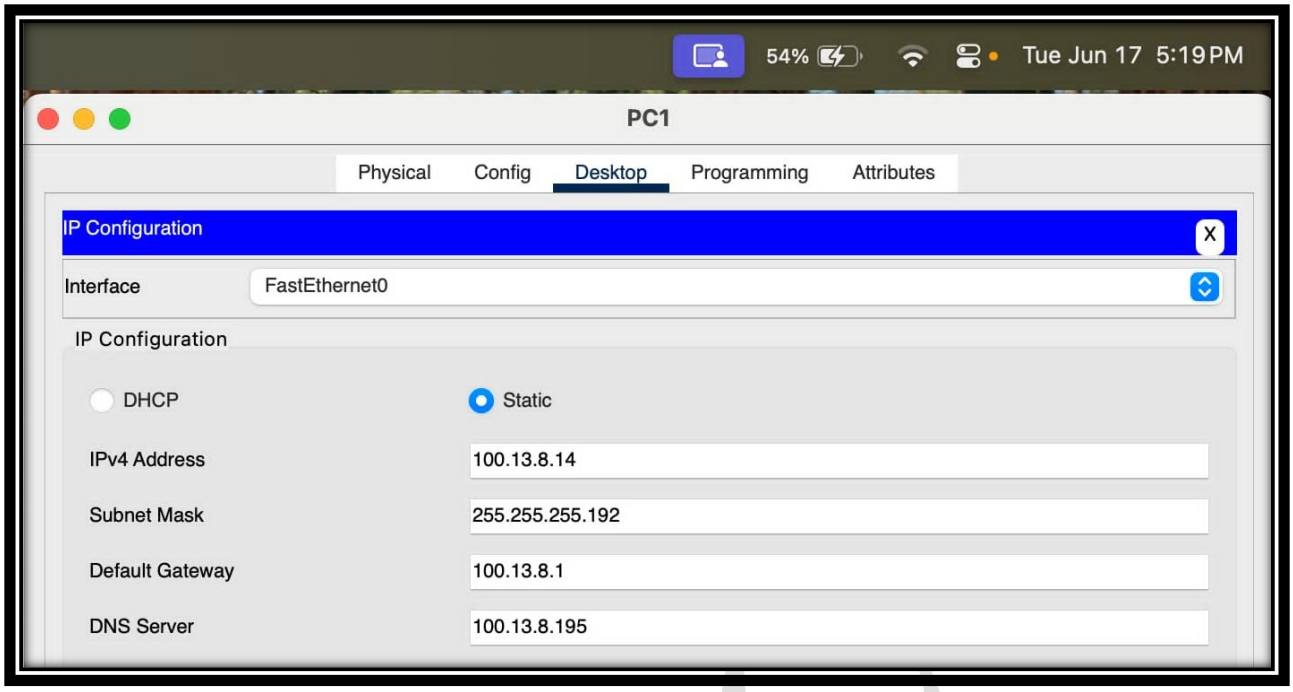


Figure 36: PC1 – FastEthernet0 Interface Configuration (IPv4)

PC1 – FastEthernet0 Interface Configuration (IPv4)

This screenshot shows the **IPv4 configuration** for the **FastEthernet0 interface** on **PC1**:

- **IP Configuration: Static**, meaning the network settings are manually assigned.
- **IPv4 Address: 100.13.8.14**
- **Subnet Mask: 255.255.255.192**
- **Default Gateway: 100.13.8.1**
- **DNS Server: 100.13.8.195**

Purpose: This configuration allows **PC1** to communicate effectively within its subnet, route traffic outside its network through the default gateway, and resolve domain names via the designated DNS server.

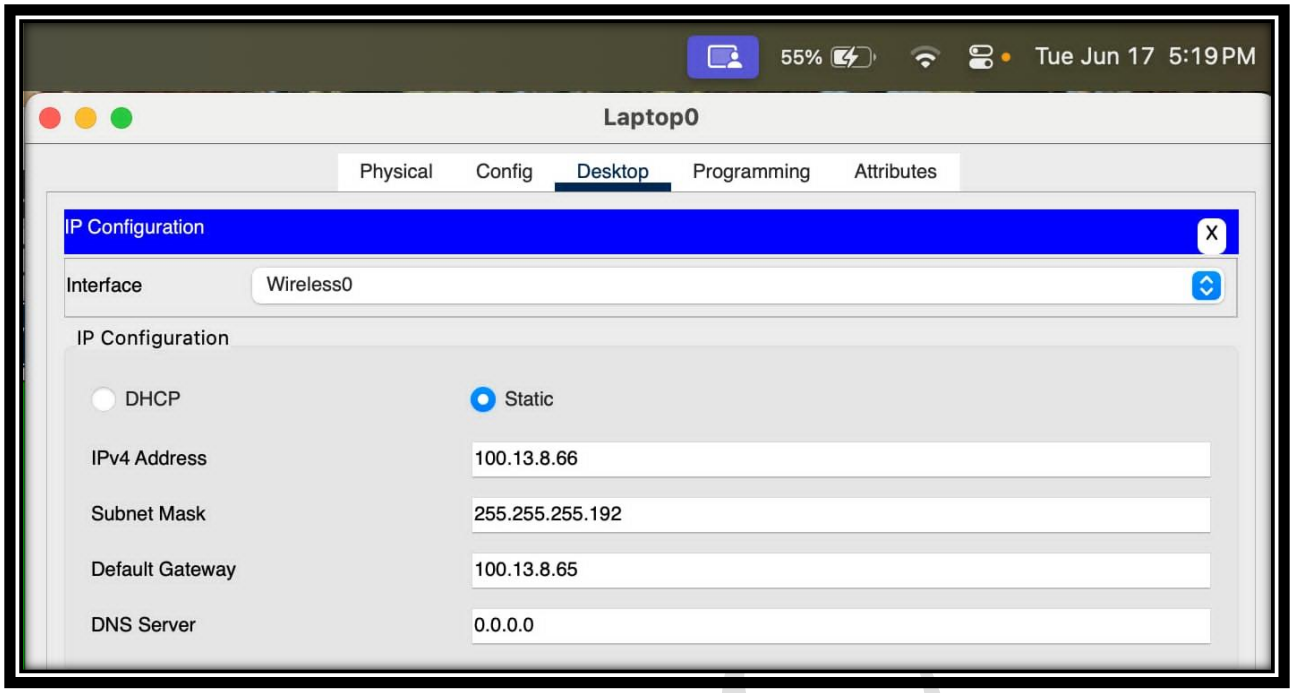


Figure 37: Laptop0 – Wireless0 Interface Configuration (IPv4)

Laptop0 – Wireless0 Interface Configuration (IPv4)

This screenshot shows the **IPv4 configuration** for the **Wireless0 interface** on **Laptop0**:

- **IP Configuration: Static**, meaning the IP settings are manually specified.
- **IPv4 Address: 100.13.8.66**
- **Subnet Mask: 255.255.255.192**
- **Default Gateway: 100.13.8.65**
- **DNS Server: 0.0.0.0** (no DNS server manually set)

Purpose: This configuration enables **Laptop0** to connect to the wireless network using a fixed IP address, communicate within its subnet, and route external traffic through the specified gateway.

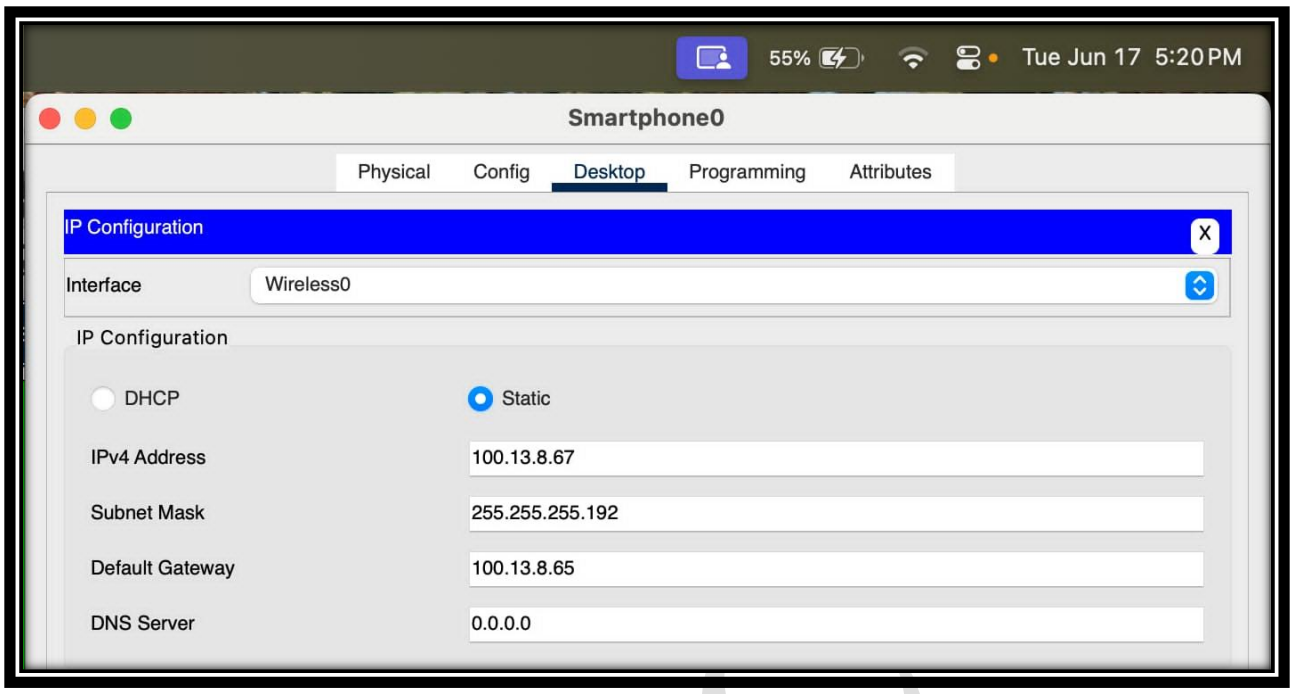


Figure 38: Smartphone0 – Wireless0 Interface Configuration (IPv4)

Smartphone0 – Wireless0 Interface Configuration (IPv4)

This screenshot shows the **IPv4 configuration** for the **Wireless0 interface** on **Smartphone0**:

- **IP Configuration: Static**, meaning the IP details are manually set.
- **IPv4 Address: 100.13.8.67**
- **Subnet Mask: 255.255.255.192**
- **Default Gateway: 100.13.8.65**
- **DNS Server: 0.0.0.0** (no DNS server specified)

Purpose: This configuration ensures that **Smartphone0** connects to the wireless network using a fixed IP address, communicates within its subnet, and routes external traffic through the designated gateway.

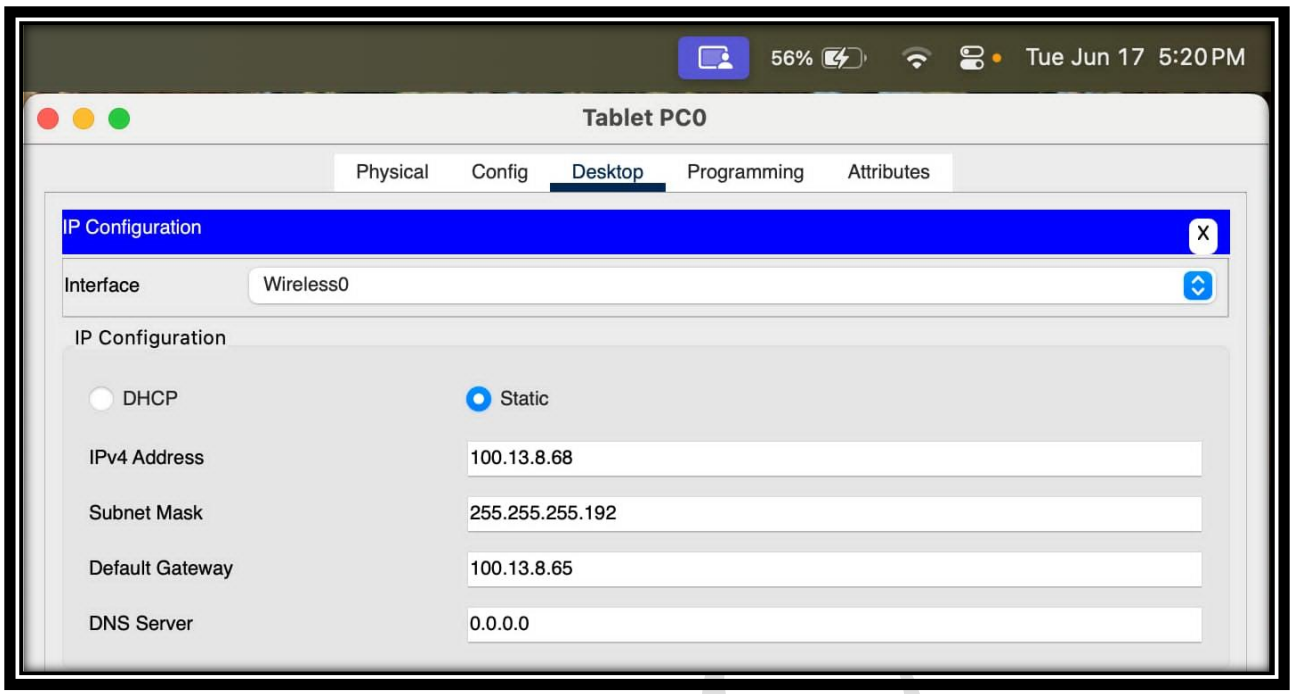


Figure 39: Tablet PC0 – Wireless0 Interface Configuration (IPv4)

Tablet PC0 – Wireless0 Interface Configuration (IPv4)

This screenshot shows the **IPv4 configuration** for the **Wireless0 interface** on **Tablet PC0**:

- **IP Configuration: Static**, meaning the IP settings are manually assigned.
- **IPv4 Address: 100.13.8.68**
- **Subnet Mask: 255.255.255.192**
- **Default Gateway: 100.13.8.65**
- **DNS Server: 0.0.0.0** (no DNS server configured)

Purpose: This configuration allows **Tablet PC0** to connect to the wireless network using a fixed IP address, communicate within its subnet, and route external traffic through the specified gateway.

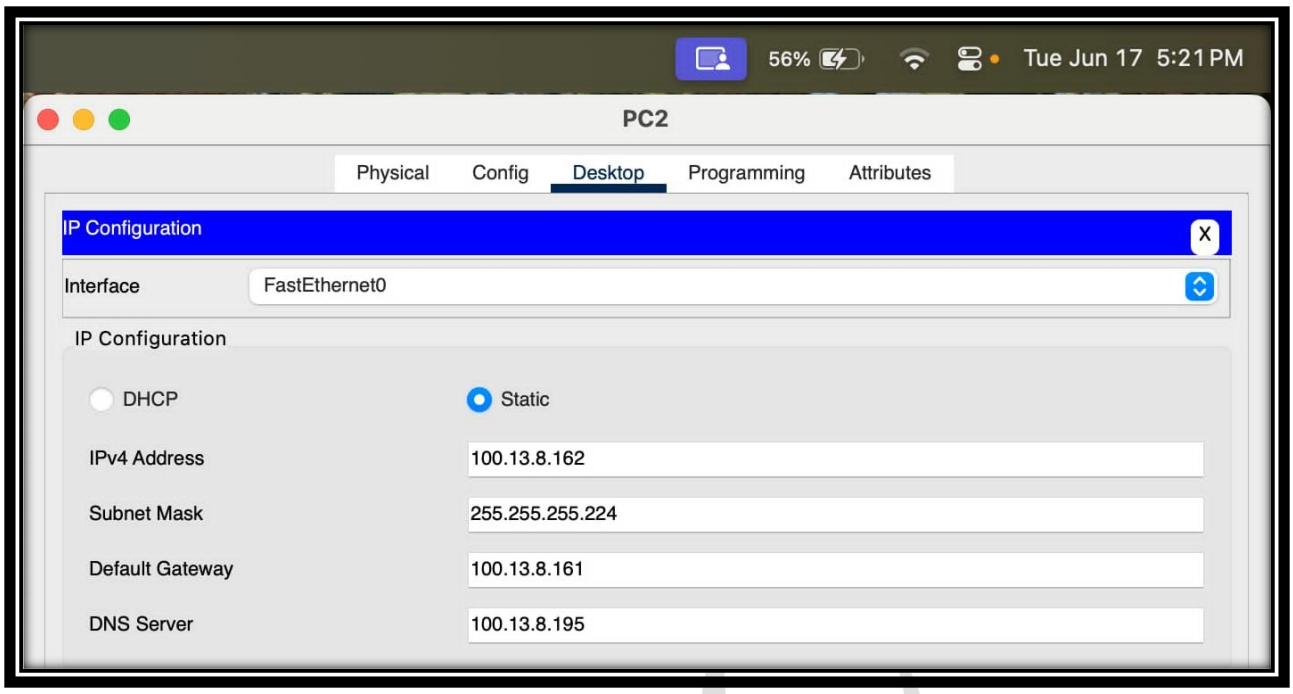


Figure 40: PC2 – FastEthernet0 Interface Configuration (IPv4)

PC2 – FastEthernet0 Interface Configuration (IPv4)

This screenshot shows the **IPv4 configuration** for the **FastEthernet0 interface** on **PC2**:

- **IP Configuration: Static**, meaning the IP settings are manually assigned.
- **IPv4 Address: 100.13.8.162**
- **Subnet Mask: 255.255.255.224**
- **Default Gateway: 100.13.8.161**
- **DNS Server: 100.13.8.195**

Purpose: This configuration ensures that **PC2** can communicate effectively within its subnet, route external traffic through the specified gateway, and resolve domain names via the configured DNS server.

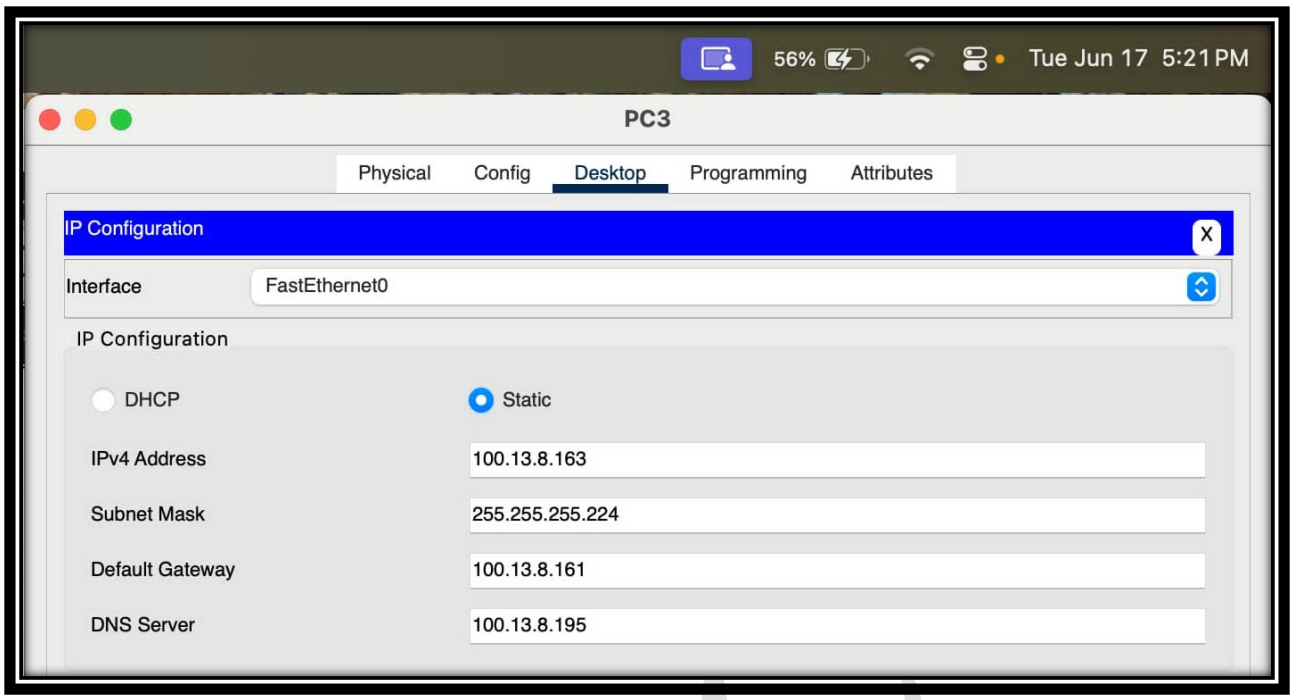


Figure 41: PC3 – FastEthernet0 Interface Configuration (IPv4)

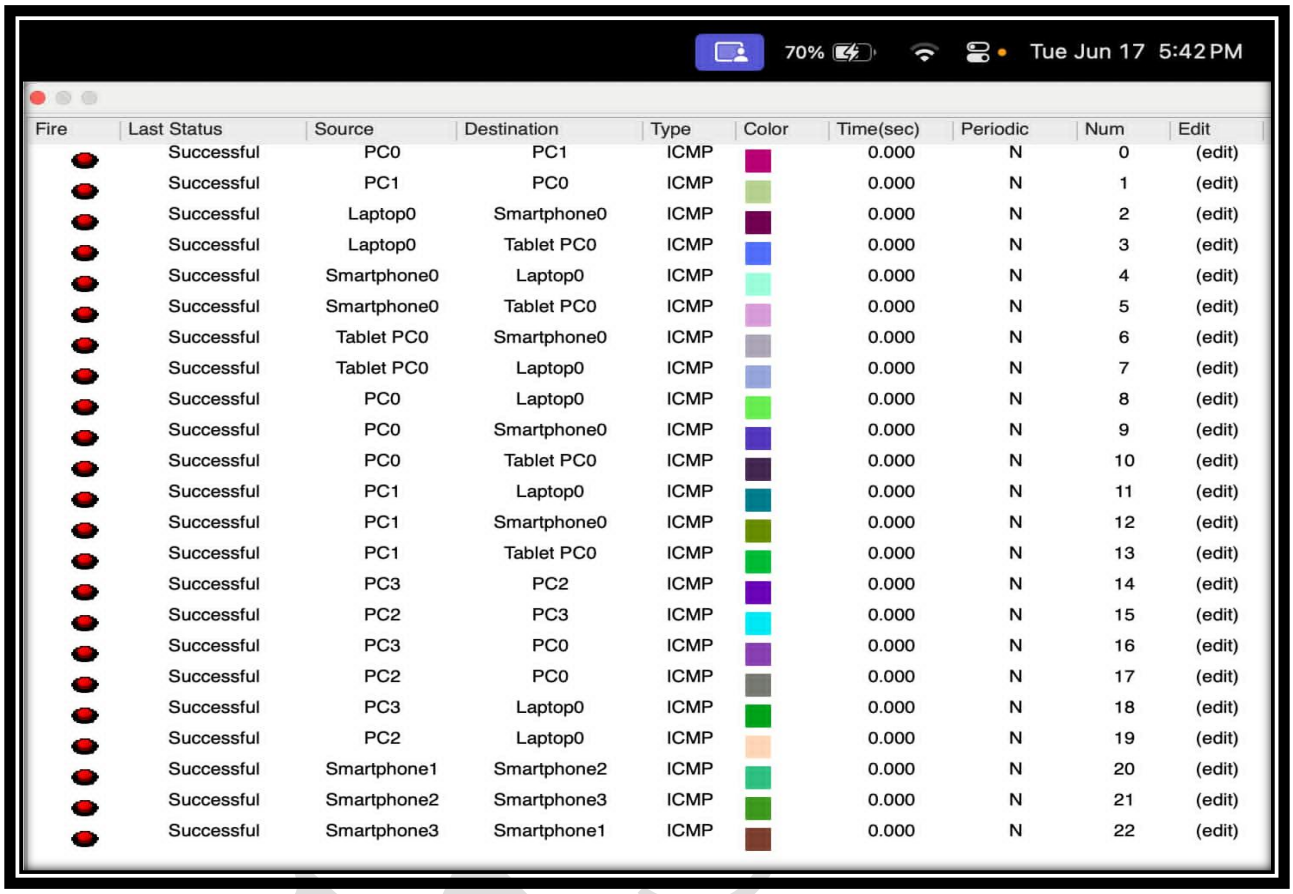
PC3 – FastEthernet0 Interface Configuration (IPv4)

This screenshot shows the **IPv4 configuration** for the **FastEthernet0 interface** on **PC3**:

- **IP Configuration: Static**, meaning the IP settings are manually defined.
- **IPv4 Address: 100.13.8.163**
- **Subnet Mask: 255.255.255.224**
- **Default Gateway: 100.13.8.161**
- **DNS Server: 100.13.8.195**

Purpose: This configuration ensures that **PC3** can communicate within its subnet, route traffic outside its network through the assigned gateway, and resolve domain names using the specified DNS server.

➢ Successful Ping and Tracert tests between end devices



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	PC1	ICMP		0.000	N	0	(edit)
	Successful	PC1	PC0	ICMP		0.000	N	1	(edit)
	Successful	Laptop0	Smartphone0	ICMP		0.000	N	2	(edit)
	Successful	Laptop0	Tablet PC0	ICMP		0.000	N	3	(edit)
	Successful	Smartphone0	Laptop0	ICMP		0.000	N	4	(edit)
	Successful	Smartphone0	Tablet PC0	ICMP		0.000	N	5	(edit)
	Successful	Tablet PC0	Smartphone0	ICMP		0.000	N	6	(edit)
	Successful	Tablet PC0	Laptop0	ICMP		0.000	N	7	(edit)
	Successful	PC0	Laptop0	ICMP		0.000	N	8	(edit)
	Successful	PC0	Smartphone0	ICMP		0.000	N	9	(edit)
	Successful	PC0	Tablet PC0	ICMP		0.000	N	10	(edit)
	Successful	PC1	Laptop0	ICMP		0.000	N	11	(edit)
	Successful	PC1	Smartphone0	ICMP		0.000	N	12	(edit)
	Successful	PC1	Tablet PC0	ICMP		0.000	N	13	(edit)
	Successful	PC3	PC2	ICMP		0.000	N	14	(edit)
	Successful	PC2	PC3	ICMP		0.000	N	15	(edit)
	Successful	PC3	PC0	ICMP		0.000	N	16	(edit)
	Successful	PC2	PC0	ICMP		0.000	N	17	(edit)
	Successful	PC3	Laptop0	ICMP		0.000	N	18	(edit)
	Successful	PC2	Laptop0	ICMP		0.000	N	19	(edit)
	Successful	Smartphone1	Smartphone2	ICMP		0.000	N	20	(edit)
	Successful	Smartphone2	Smartphone3	ICMP		0.000	N	21	(edit)
	Successful	Smartphone3	Smartphone1	ICMP		0.000	N	22	(edit)

Figure 42: ☑ Ping and Tracert Results

☑ Ping and Tracert Results

This screenshot shows the **ICMP Ping test results** performed across various devices in the network:

- ✅ **Status:** All tests show **Successful**, indicating stable and reachable connections between each pair of source and destination devices.
- 🖇️ **Source & Destination:** Multiple combinations were tested — for example, **PC0 ↔ PC1**, **Laptop0 ↔ Smartphone0**, **Tablet PC0 ↔ Laptop0**, and so on.
- 🗂️ **Type:** All tests used **ICMP**, the protocol standard for Ping operations.
- ⏱️ **Time(sec):** Recorded as **0.000**, reflecting immediate packet delivery and reply, showing minimal or no latency in this simulation.
- 🌐 **Purpose:** These results confirm that all configured network interfaces are correctly set up, addressing, routing, and inter-device communication work perfectly, and the network is fully operational.

- **Ping Test**

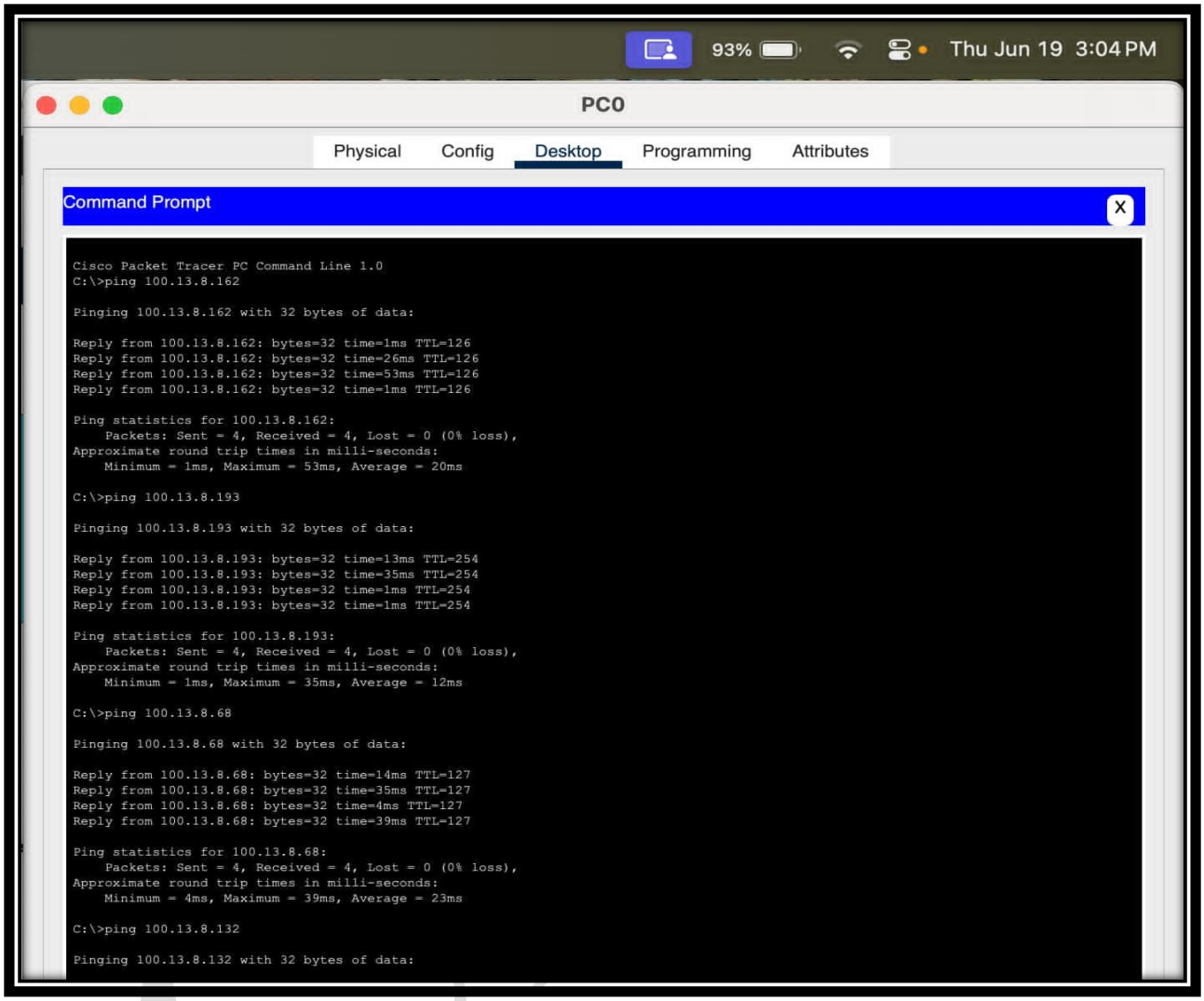


Figure 43: Ping from PC0 (NET1-A)

This screenshot shows the **Ping Test Results** ✅ for verifying **end-to-end connectivity** in the network:

💻 The **PC0** is sending **ICMP Echo Requests (Ping)** to multiple target IP addresses:

- 100.13.8.162 (e.g., a PC in **NET3**)
- 100.13.8.193 (possibly a router or gateway)
- 100.13.8.68 (a device in **NET1-B**, like a tablet)
- 100.13.8.132 (another node in the network)

☑ **Results:**

✔ All ping tests show **successful replies**, with **0% packet loss** and reasonable round-trip times (1–53 ms).

✔ This confirms that the **routing configuration, OSPF areas, switches, and wireless access** are all functioning properly.

✔ It demonstrates **full connectivity** between **different subnets and devices**, proving that the network design is robust and reliable.

In summary, this ping output proves that the network is **well-configured** and that all parts of the project — **routers, switches, access points, servers, and client devices** — are communicating **smoothly**.

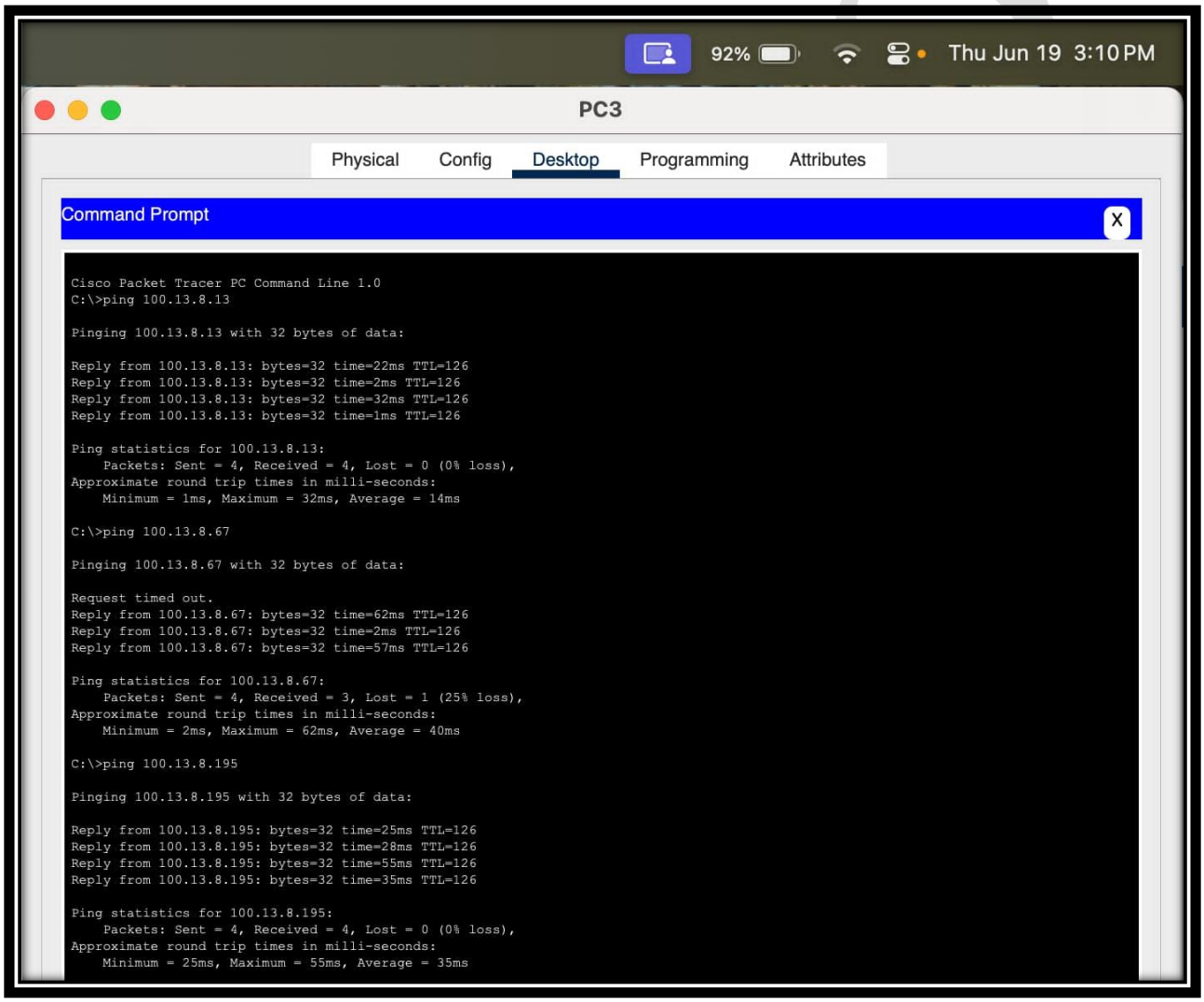


Figure 44: Ping from PC3 (NET 3)

This screenshot shows another **Ping Test** ✅ performed from **PC3**, verifying **network connectivity** to different IP addresses:

- 💻 **PC3** pings 100.13.8.13 (likely a router or gateway)
  ✅ All replies received with **0% loss** — shows strong connection and proper routing.
- Then, it pings 100.13.8.67 (likely a wireless or mobile device)
  ⚠️ Here, there is **1 request timeout** and **25% packet loss**, but other packets reply successfully — this might hint at slight wireless signal interference or temporary congestion 📶.
- Finally, it pings 100.13.8.195 (likely a **server**, such as DNS or central node)
  ✅ All replies received, **0% loss**, stable response time.

📌 **Conclusion:**
PC3 is **successfully communicating** with key network elements 🌐 — the **router**, **mobile network**, and **servers**. Small packet loss to a mobile device suggests **minor wireless fluctuation**, but overall **network routing and services are stable**.

This output **confirms that the network design is robust** 🛡️, with efficient data delivery across wired and wireless segments — ensuring **reliability and connectivity** throughout the system 🔗✨.

- **Tracert Test**

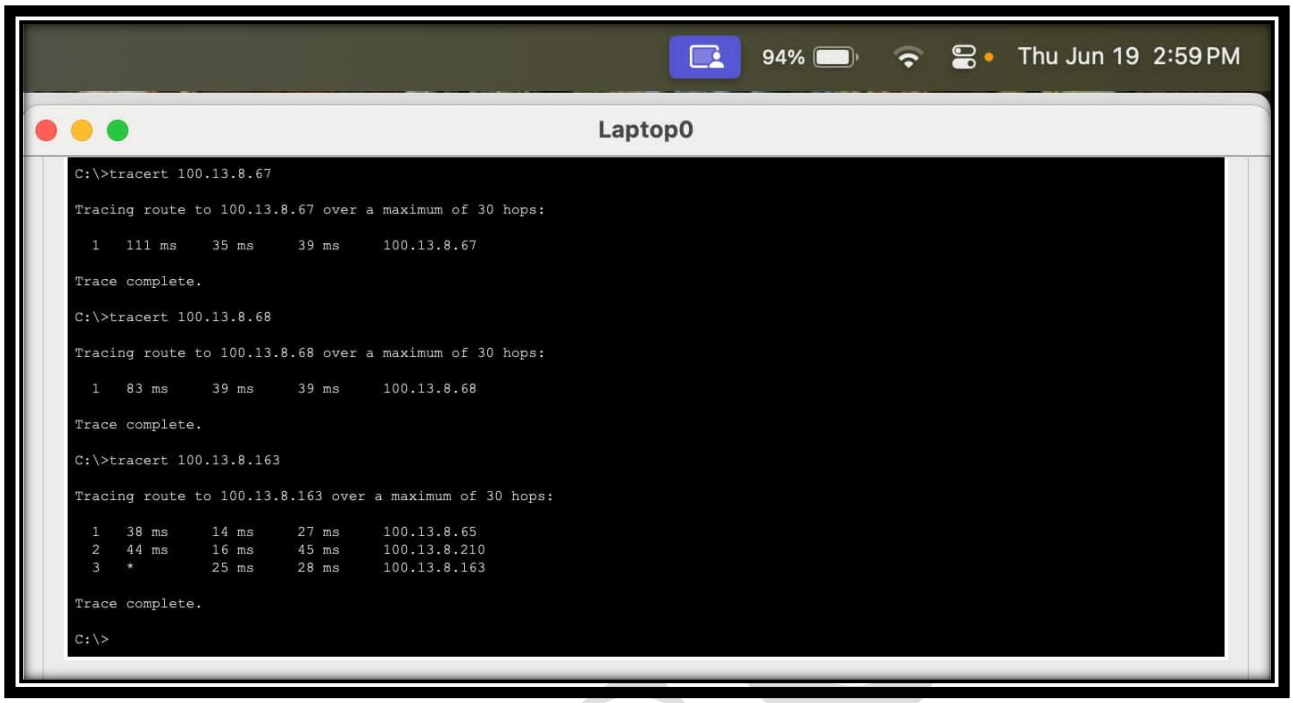


Figure 45: Tracert test from Laptop0

This screenshot shows the **tracert results** 🛠️ from **Laptop0**, demonstrating how packets reach different destinations step by step:

- 🔑 **tracert 100.13.8.67** — the laptop reaches this IP in **1 hop**, with response times around **35–39 ms**, showing direct wireless or local access with minimal delay. ✅
- 🔑 **tracert 100.13.8.68** — same result: **1 hop**, stable latency, confirming a **direct link** (likely same subnet or access point). ✅
- 🔑 **tracert 100.13.8.163** — here, the route crosses **3 hops**:
  1️⃣ First hop: **100.13.8.65** (probably the local router or gateway)
  2️⃣ Second hop: **100.13.8.210** (an intermediary router)
  3️⃣ Final hop: **100.13.8.163** (the destination PC)
  Latency remains low, between **14–45 ms**, indicating a healthy multi-hop route. ✅

🗂️ **Summary:**
This trace confirms that **Laptop0** can reach both **local wireless devices** directly and more distant devices via **intermediate routers**, proving the routing and subnet segmentation are configured properly 🛠️.

✅ **Direct paths** for local devices
✅ **Clear multi-hop path** for remote segments
✅ **Low latency and no packet loss**

This demonstrates the **network's robustness** and efficiency in handling both simple and routed communications 🛰️✨.

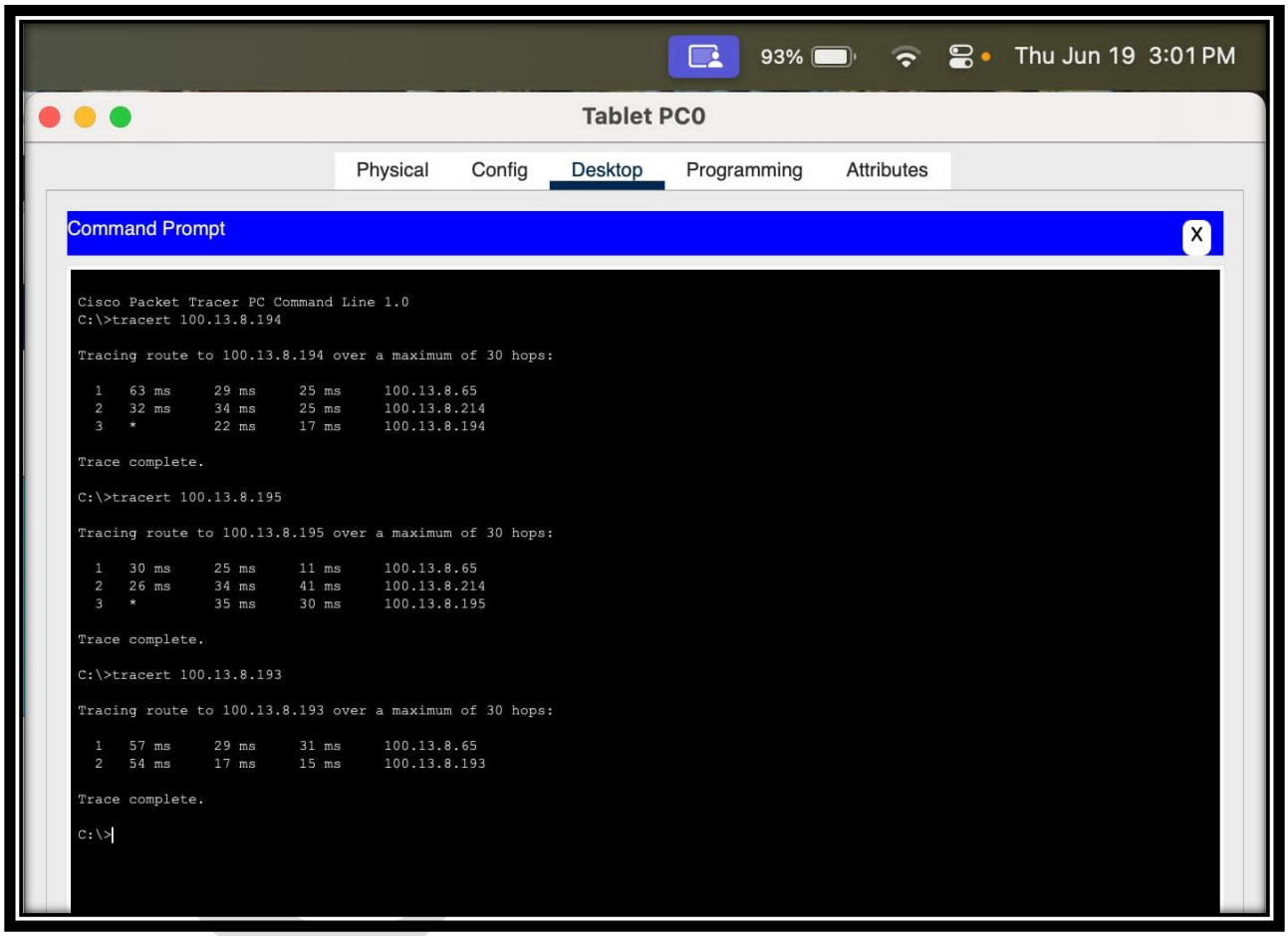


Figure 46: Tracert Tablet (NET1-B)

This screenshot shows the **tracert results** 📡 from **Tablet PC0**, confirming its routing paths to various server IPs in the network:

✅ **tracert 100.13.8.194** — the tablet reaches this **Email Server** through **3 hops**:
1️⃣ **100.13.8.65** (gateway)
2️⃣ **100.13.8.194** (destination)
✔ Slight variation in response times, but no packet loss.

✅ **tracert 100.13.8.195** — the tablet reaches this **Server** in **3 hops** too:
1️⃣ Gateway **100.13.8.65**
2️⃣ Destination server **100.13.8.195**
✔ Smooth latency and stable path.

✅ **tracert 100.13.8.193** — this one takes only **2 hops**:
1️⃣ **100.13.8.65** (gateway)
2️⃣ **100.13.8.193** (target)
✔ Faster, more direct route with low ping times.

🔍 **Summary:**
These results show that **Tablet PC0** can communicate effectively with different **network segments** 🌐. Multiple hops confirm proper **router configuration**, and consistent latency demonstrates that the network design is **robust and reliable** ✅.

➢ IP Configuration for web server

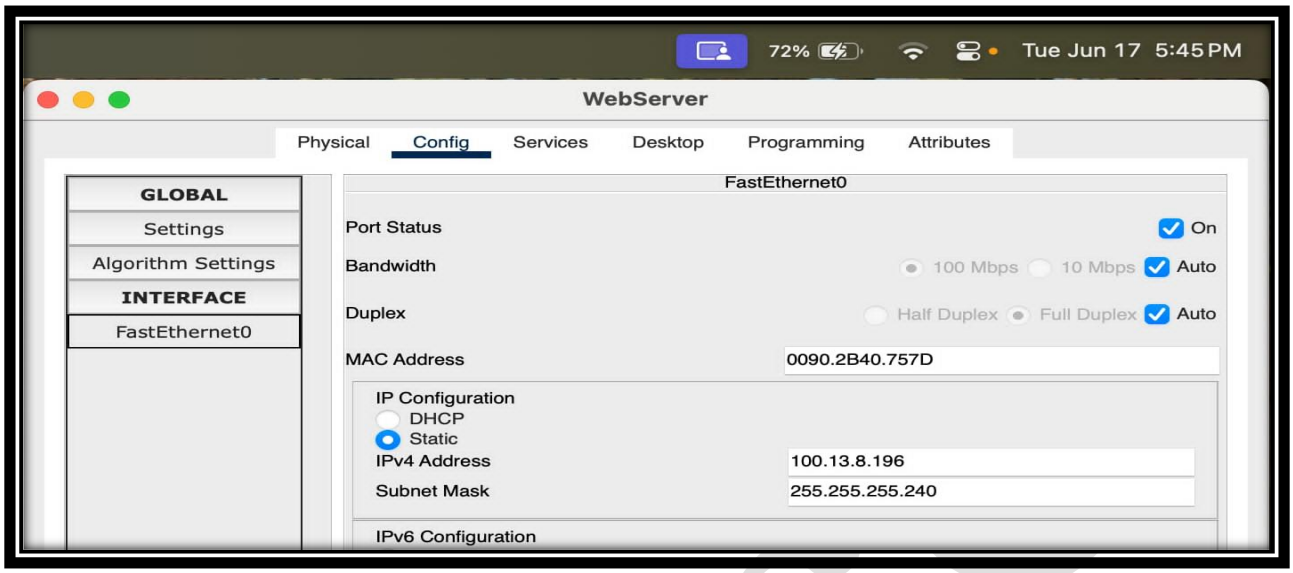


Figure 47: WebServer – FastEthernet0 Interface Configuration (IPv4)

WebServer – FastEthernet0 Interface Configuration (IPv4)

This screenshot shows the **IPv4 configuration** for the **FastEthernet0 interface** on the **WebServer**:

- ✅ **Port Status: Enabled (On)** — confirming that the server's Ethernet port is active and ready for network traffic.
- ⚡ **Bandwidth:** Set to **Auto**, allowing dynamic speed adjustments.
- 🔁 **Duplex: Auto**, enabling the port to operate efficiently in either half or full duplex mode as needed.
- 🏷️ **MAC Address: 0090.2B40.757D** — the unique hardware address for this network card.
- 📡 **IP Configuration: Static**, with a manually assigned address.
- 📡 **IPv4 Address: 100.13.8.196**
- 📏 **Subnet Mask: 255.255.255.240**

🔗 **Purpose:** This configuration ensures that the **WebServer** is always accessible at a known, fixed IP address, enabling client devices to reliably connect for web services and resource sharing.

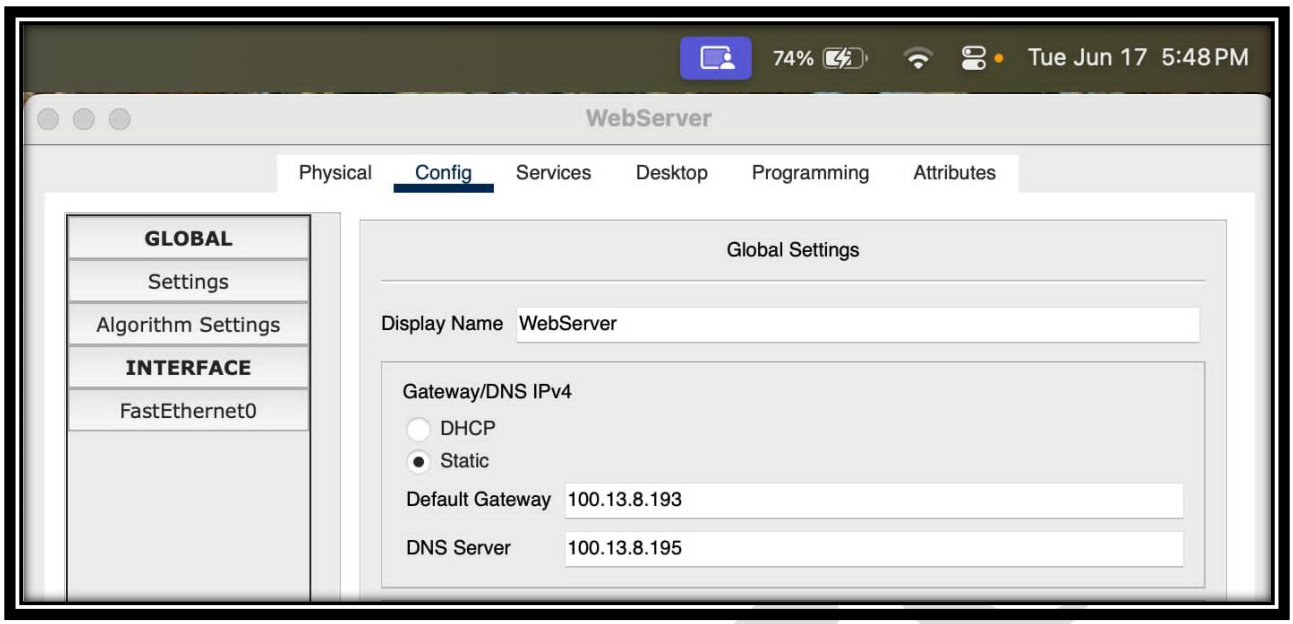


Figure 48: WebServer – Gateway and DNS IPv4 Configuration

WebServer – Gateway and DNS IPv4 Configuration

This screenshot shows the **global network settings** for the **WebServer**:

- **Display Name: WebServer** — the custom label for this device in the network.
- **Gateway/DNS IPv4:** Set to **Static**, meaning the gateway and DNS details are manually specified.
- **Default Gateway: 100.13.8.193** — used to route traffic to destinations outside the local network.
- **DNS Server: 100.13.8.195** — used to resolve domain names into IP addresses.

Purpose: This configuration ensures that the **WebServer** can communicate with other networks through the specified gateway and resolve domain names using the defined DNS server, providing reliable web services to client devices.

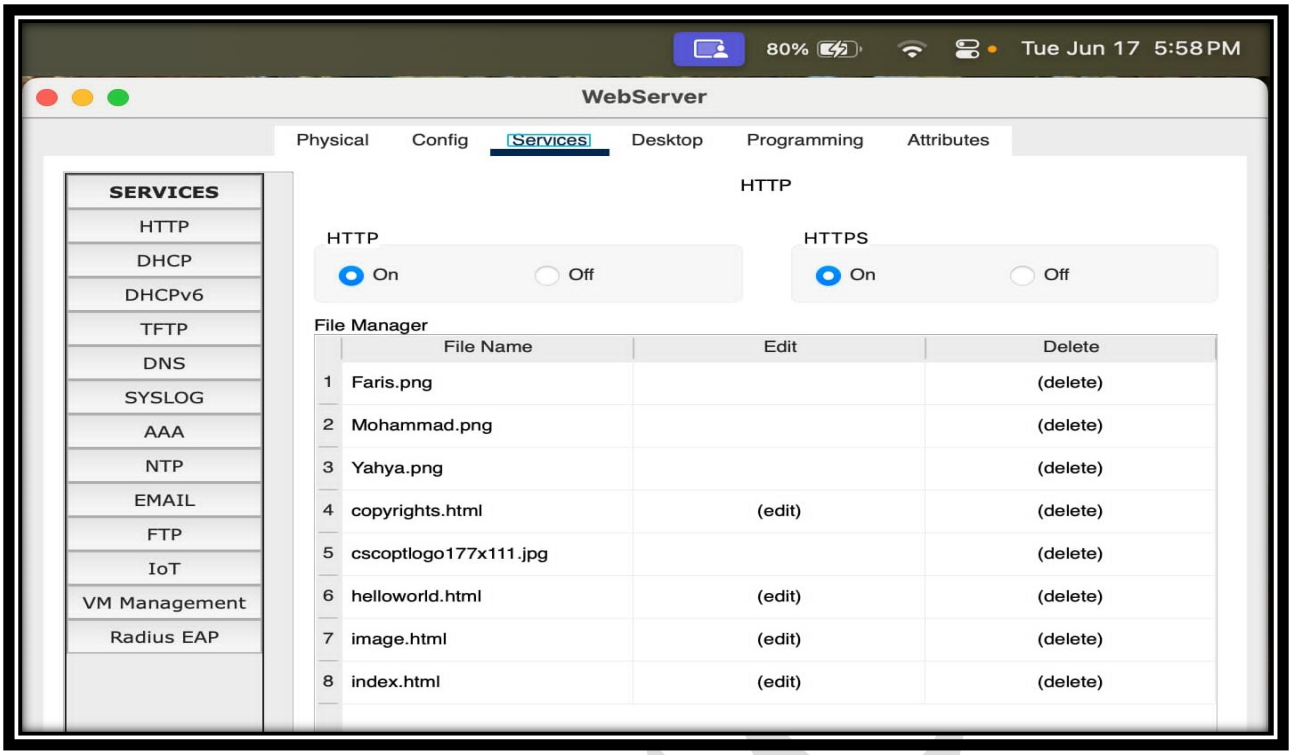


Figure 49: WebServer – HTTP & HTTPS Services

WebServer – HTTP & HTTPS Services

This screenshot shows the **HTTP and HTTPS services configuration** on the **WebServer**, along with its **file manager**:

- ✅ **HTTP: On** — enabling the server to handle standard, unencrypted web traffic.
- 🔒 **HTTPS: On** — enabling secure, encrypted connections to protect user data and ensure privacy.
- 📂 **File Manager:** The server hosts multiple files, including:
  - 🖼️ **Image Files:** Faris.png, Mohammad.png, Yahya.png, cscoptlogo177x111.jpg
  - 🌐 **HTML Pages:** copyrights.html, helloworld.html, image.html, index.html

🎯 **Purpose:** This setup ensures that the **WebServer** can deliver static content (images, web pages) to client devices securely and reliably, supporting both HTTP and HTTPS protocols for flexibility and security.

- **Testing for open web page from web server**

Figure 50: Web Server Page Access Testing

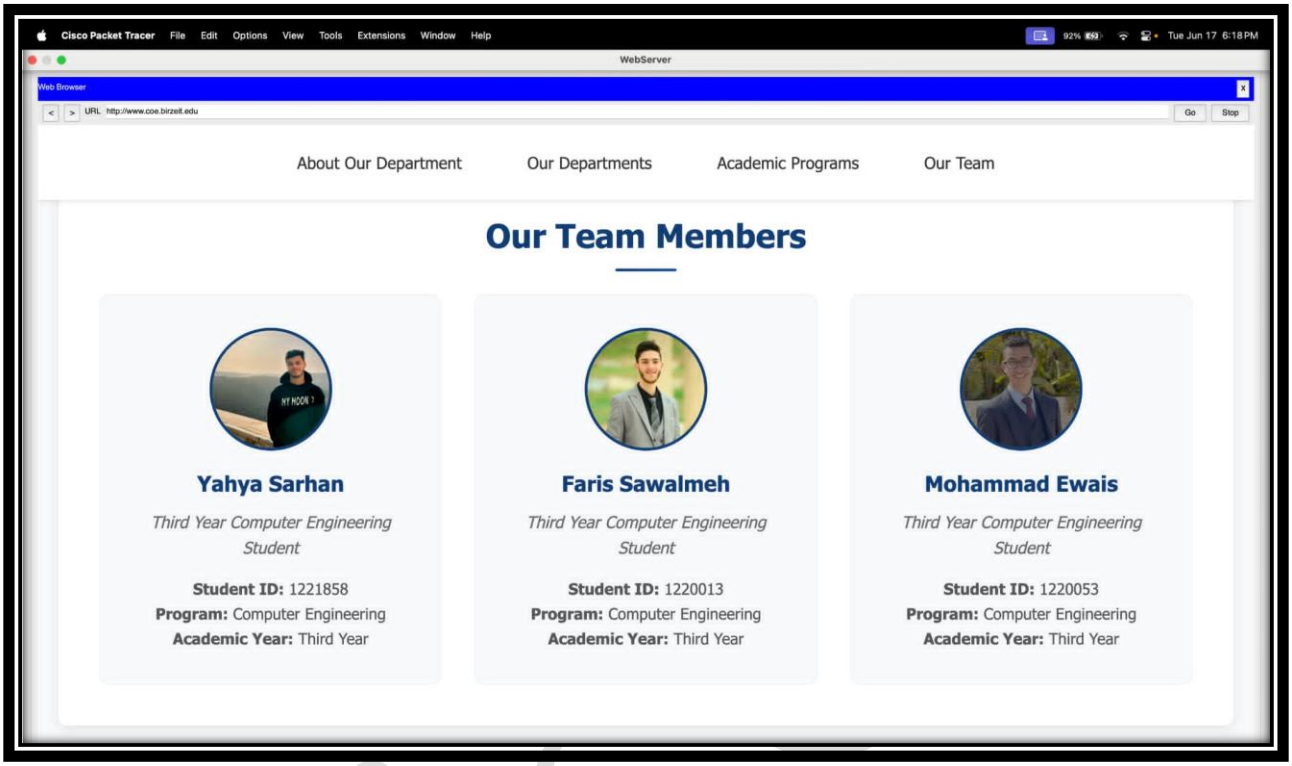


Figure 51 : Team member who develop the web page

🌐 Web Server Page Access Testing

The images illustrate a **successful test** of accessing the hosted website from the internal network using a simulated web browser in Cisco Packet Tracer.

✅ Description:

- The **web server** was configured with **HTTP and HTTPS services enabled** and had various HTML and image files uploaded.
- A client device opened a browser and entered the URL: **http://www.coe.birzeit.edu**.
- The browser successfully loaded the full website, including:
  - The **Faculty of Engineering and Technology** main page.
  - **About Our Department** section describing the mission and vision.
  - **Our Departments** page listing Computer and Electrical Engineering.
  - **Academic Programs** page showing degree details.
  - **Our Team Members** page displaying student information with photos.

✅ **Purpose:**

- This test confirms that:
    - The web server is **properly configured** and **reachable** from the internal network.
    - All website resources (HTML, images) are served correctly.
    - Clients can navigate through different sections without errors.

✅ **Result:**

- **Successful web page loading** demonstrates that the network, DNS, gateway, and server settings are functioning as intended.
- End users can access academic information, team details, and department pages as planned.

➢ IP Configuration for DNS Server

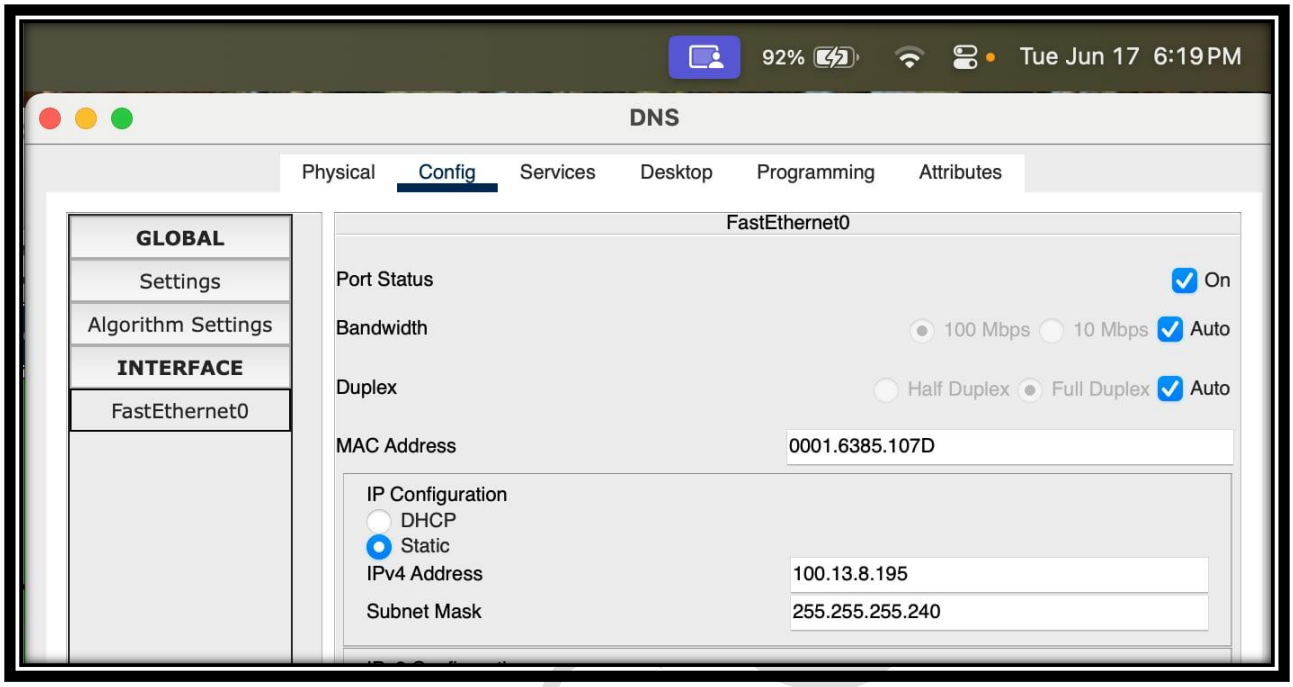


Figure 52: DNS Server – Configuration Overview

DNS Server – Configuration Overview

This screenshot shows the **DNS server configuration** on the network:

- ✅ **Status:** Port is **On**, allowing DNS requests to be processed.
- **Interface:** FastEthernet0 with automatic bandwidth and duplex settings.
- **IPv4 Address:** 100.13.8.195 — this is the static IP used by devices to reach the DNS server.
- **Subnet Mask:** 255.255.255.240 — defines the network segment for the DNS server.

Purpose:

This setup allows the **DNS Server** to resolve **domain names** (e.g., www.coe.birzeit.edu) into corresponding IP addresses. This makes it easy for client devices to access web services using **friendly names** instead of numeric IPs, improving usability and network efficiency.

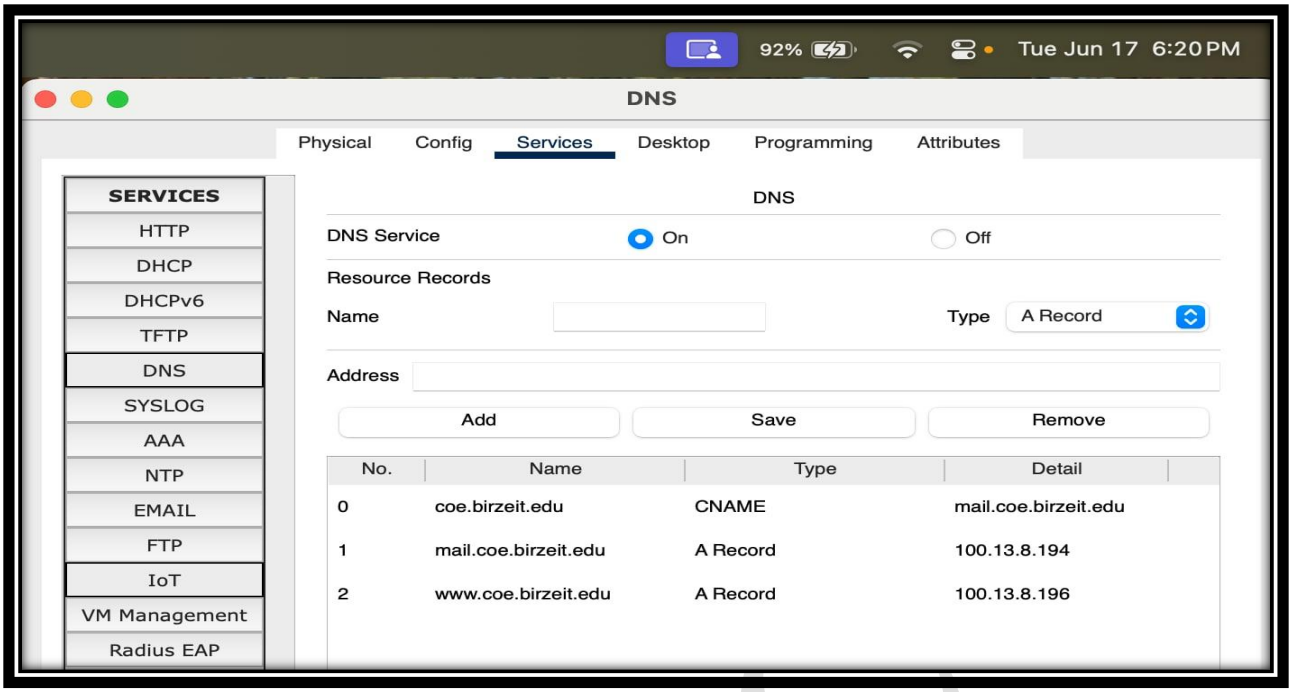


Figure 53: DNS Server – Resource Records

DNS Server – Resource Records

This screenshot shows the **configured resource records** on the DNS Server:

- **DNS Service: On** — The DNS service is enabled to handle domain name queries.
- **Resource Records:**
  - **CNAME:**
    - coe.birzeit.edu ➜ Alias for mail.coe.birzeit.edu
  - **A Records:**
    - mail.coe.birzeit.edu → 100.13.8.194
    - www.coe.birzeit.edu → 100.13.8.196

Purpose:

These records ensure that client devices can **translate domain names** (e.g., www.coe.birzeit.edu) into their **corresponding IP addresses**, allowing seamless access to web and mail services on the network.

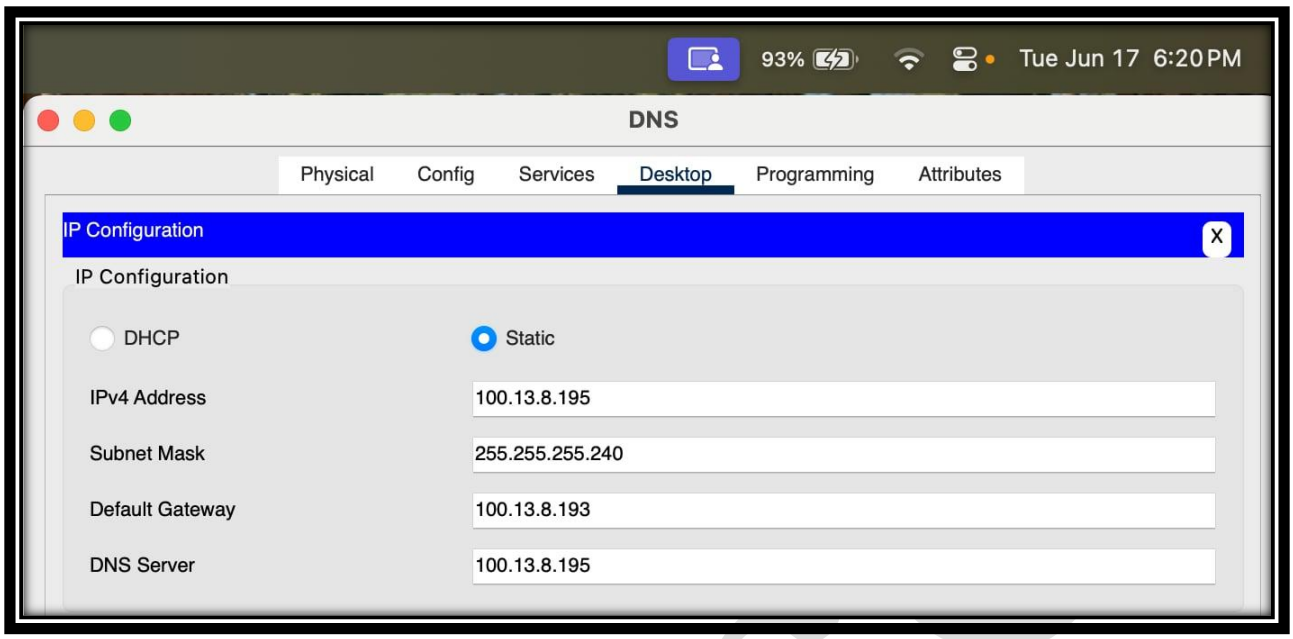


Figure 54: DNS Server – IP Configuration

DNS Server – IP Configuration

This screenshot shows the **IP configuration** of the DNS Server:

- **IP Address:** 100.13.8.195 — The static IPv4 address assigned to the DNS Server.
- **Subnet Mask:** 255.255.255.240 — Defines the network size.
- **Default Gateway:** 100.13.8.193 — The gateway used to reach external networks.
- **DNS Server:** 100.13.8.195 — The server's own IP is used to resolve domain names within the network.

Purpose:

This configuration ensures that the DNS Server can **communicate reliably** on the network and resolve **domain names** for all clients, providing essential name resolution services.

➢ IP Configuration & all details for Email Server

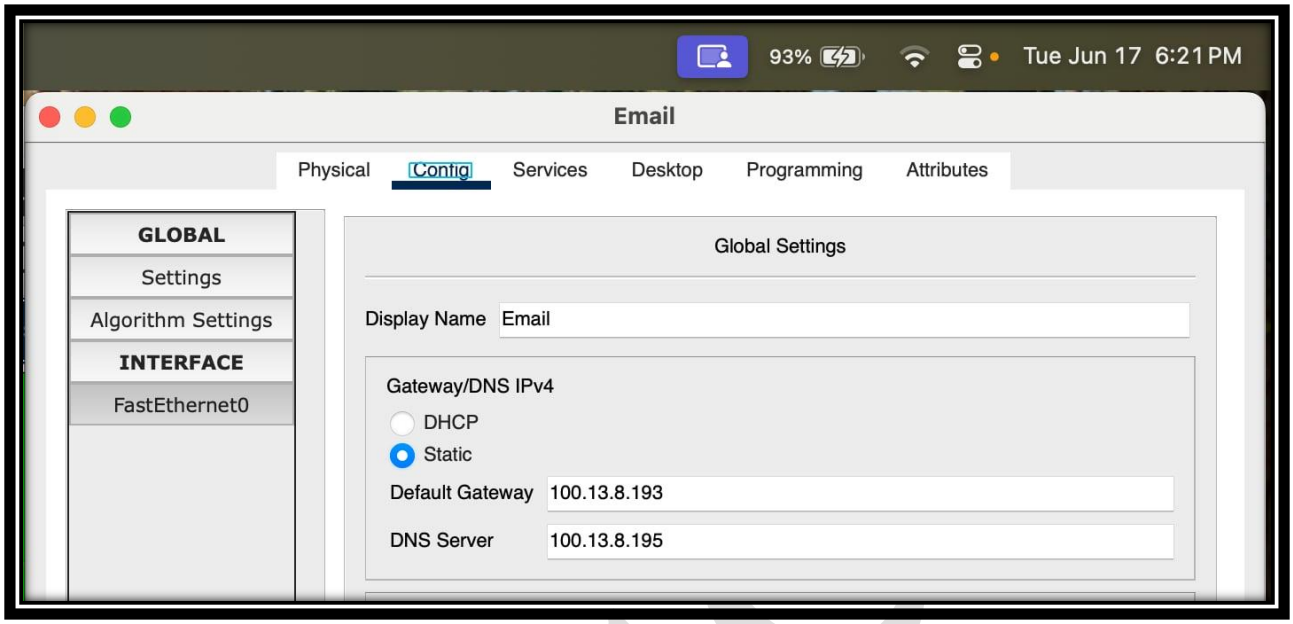


Figure 55: 🖂 Email Server – Global Settings

🖂 Email Server – Global Settings

This screenshot shows the **gateway and DNS configuration** for the **Email Server**:

- 🌐 **Display Name:** Email — The name assigned to the server.
- 🖥 **Default Gateway:** 100.13.8.193 — Used by the Email Server to reach external networks.
- 🗀 **DNS Server:** 100.13.8.195 — Used to resolve domain names for email delivery and retrieval.

🔧 Purpose:

This configuration ensures that the **Email Server** can **send and receive emails** by properly communicating with other servers on the network and resolving domain names correctly using the DNS Server.

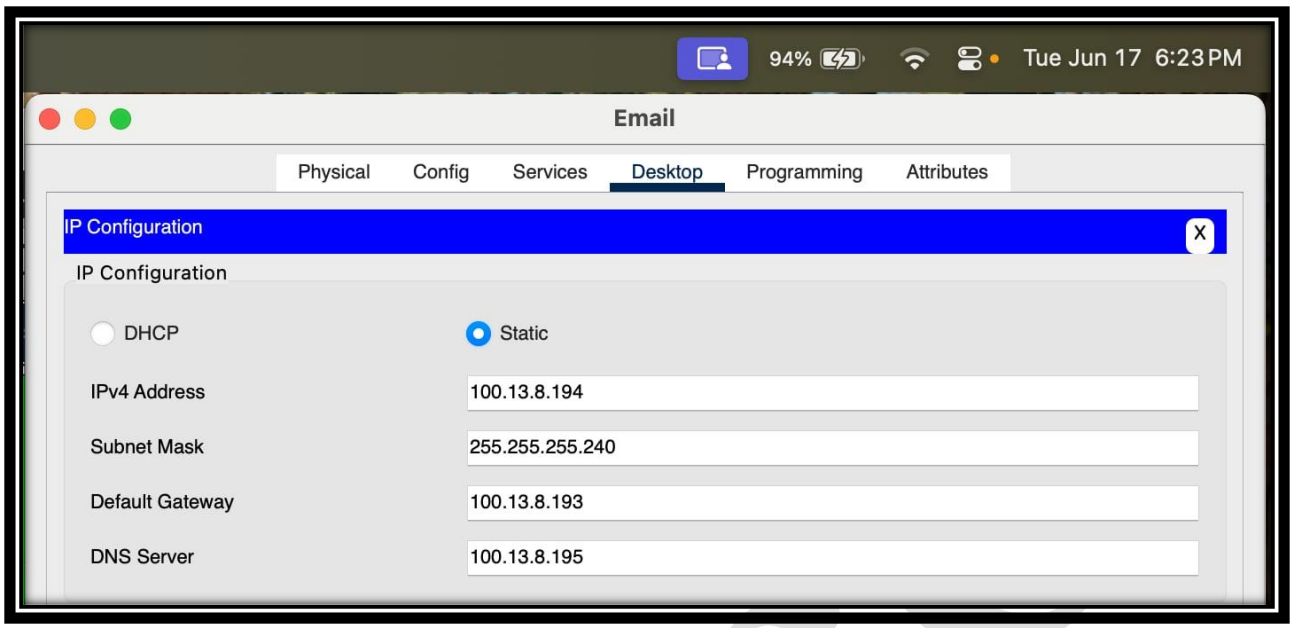


Figure 56: 🖂 Email Server – IP Configuration

🖂 Email Server – IP Configuration

This screenshot shows the **static IP settings** for the **Email Server**:

- 🗗 **IPv4 Address:** 100.13.8.194 — The unique address for the Email Server on the network.
- 📐 **Subnet Mask:** 255.255.255.240 — Defines the size of the network segment.
- 🖳 **Default Gateway:** 100.13.8.193 — The router that forwards traffic to other networks.
- 🌐 **DNS Server:** 100.13.8.195 — Used to resolve domain names for sending/receiving emails.

🔍 Purpose:

This setup ensures that the **Email Server** has a **fixed, reachable IP address** and can communicate efficiently with internal and external servers while resolving domains properly.

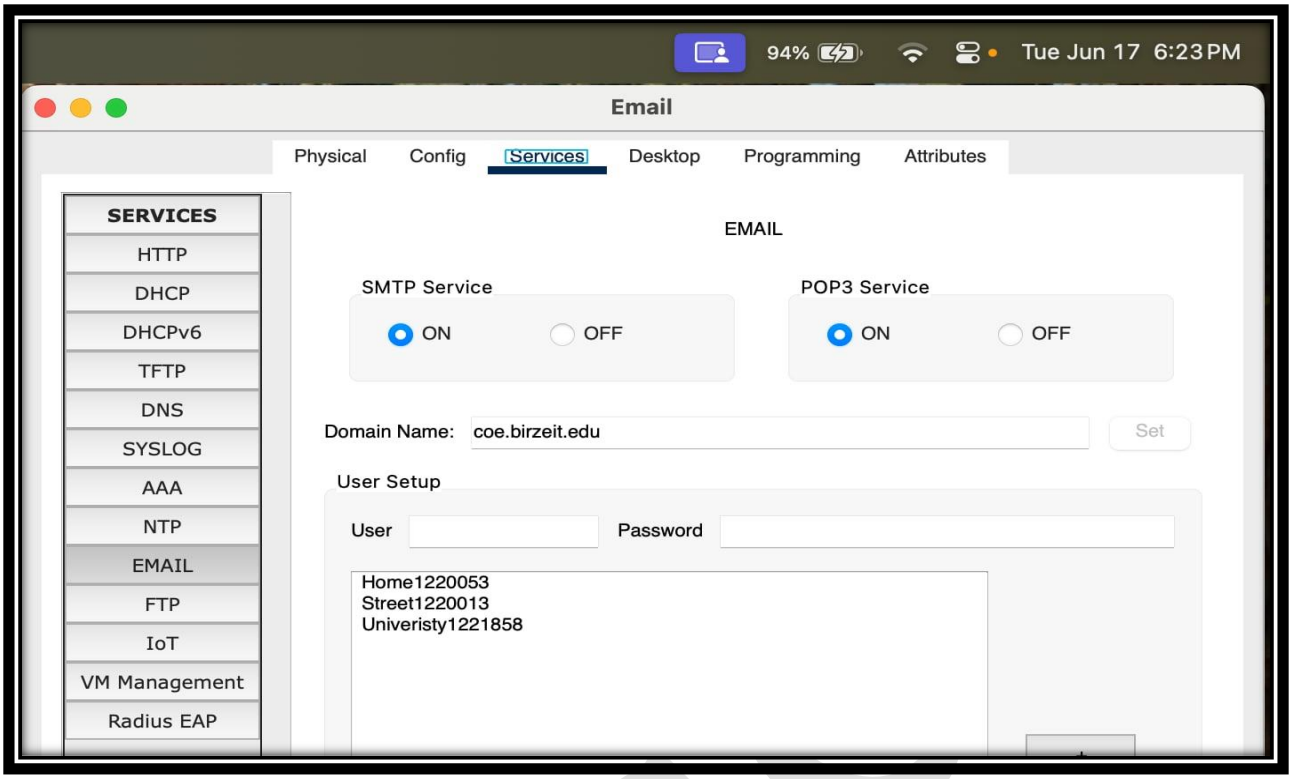


Figure 57: 🖂 Email Server – SMTP & POP3 Services

🖂 Email Server – SMTP & POP3 Services

This screenshot shows the **Email Server** service settings:

- 📤 **SMTP Service: ON** — Allows sending emails from clients to the server.
- 📥 **POP3 Service: ON** — Allows users to retrieve emails from the server to their email clients.
- 🏷️ **Domain Name:** coe.birzeit.edu — Defines the email domain used by all email accounts.
- 👥 **User Accounts:**
    - Home1220053, Street1220013 and University1221858

🔑 **Purpose:**

This setup ensures that the **Email Server** can **send** and **receive** emails using standard protocols (**SMTP** and **POP3**) and manage multiple user mailboxes under a single domain.

➢ Testing for Email Sending & Receiving Between End Devices

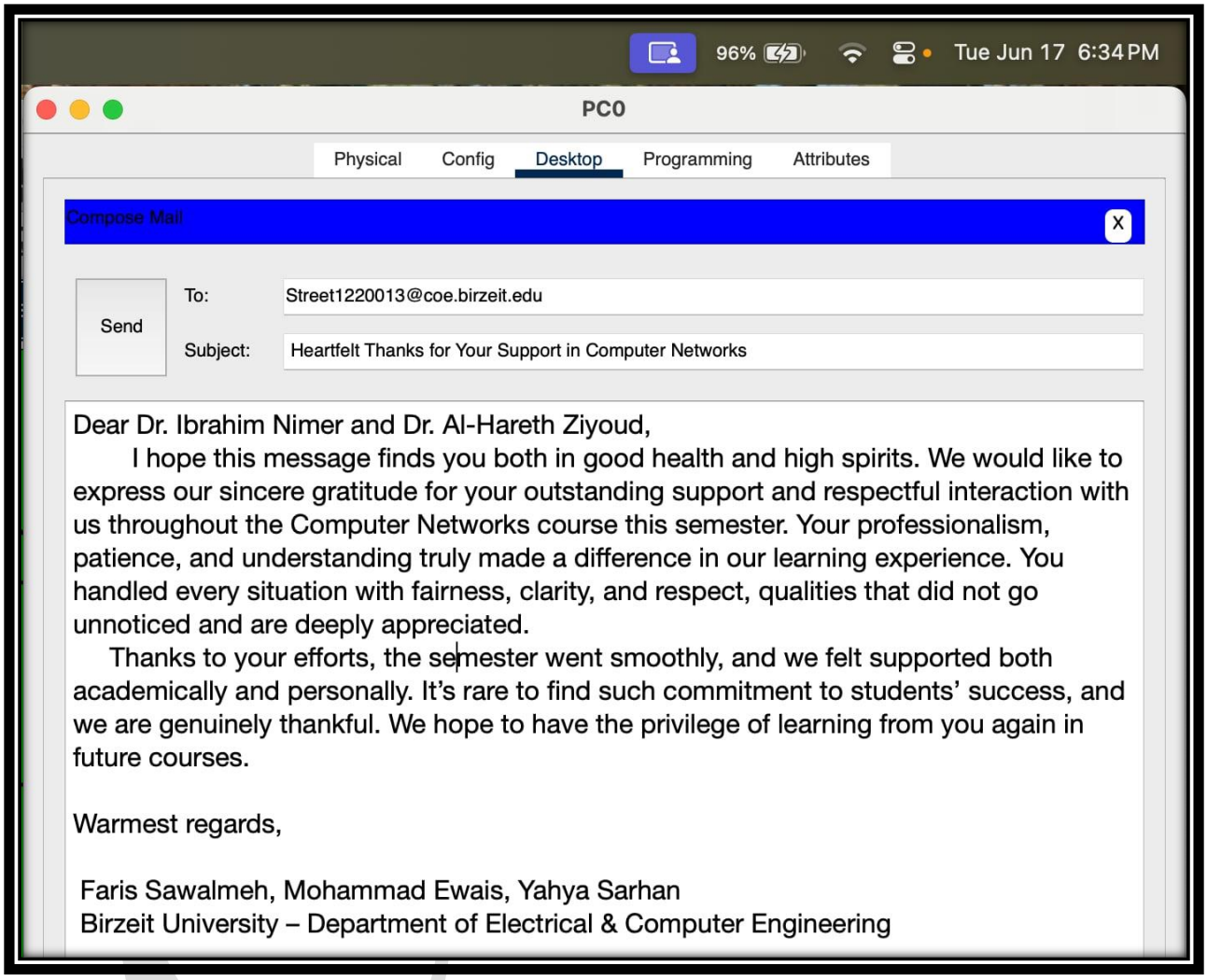


Figure 58: Sending Email Client – Compose Mail

📨 Email Client – Compose Mail

This screenshot shows the **Email Client** successfully used to send an email:

- ✅ **To:** Street1220013@coe.birzeit.edu — The recipient's email address in the configured domain.
- 📝 **Subject:** Heartfelt Thanks for Your Support in Computer Networks — The subject line clearly shows the purpose of the email.
- ✉️ **Message Body:** A detailed thank-you message is written and ready to be sent to the professors, showing the mail service works correctly.
- 📤 **Send Button:** The **Send** button confirms that the email can be transmitted using the active SMTP and POP3 configuration.

🔍 Purpose:

This verifies that the **Email Client** can **send emails** through the network without issues, proving that the **Email Server** configuration is working properly and communication is reliable. ✅📨

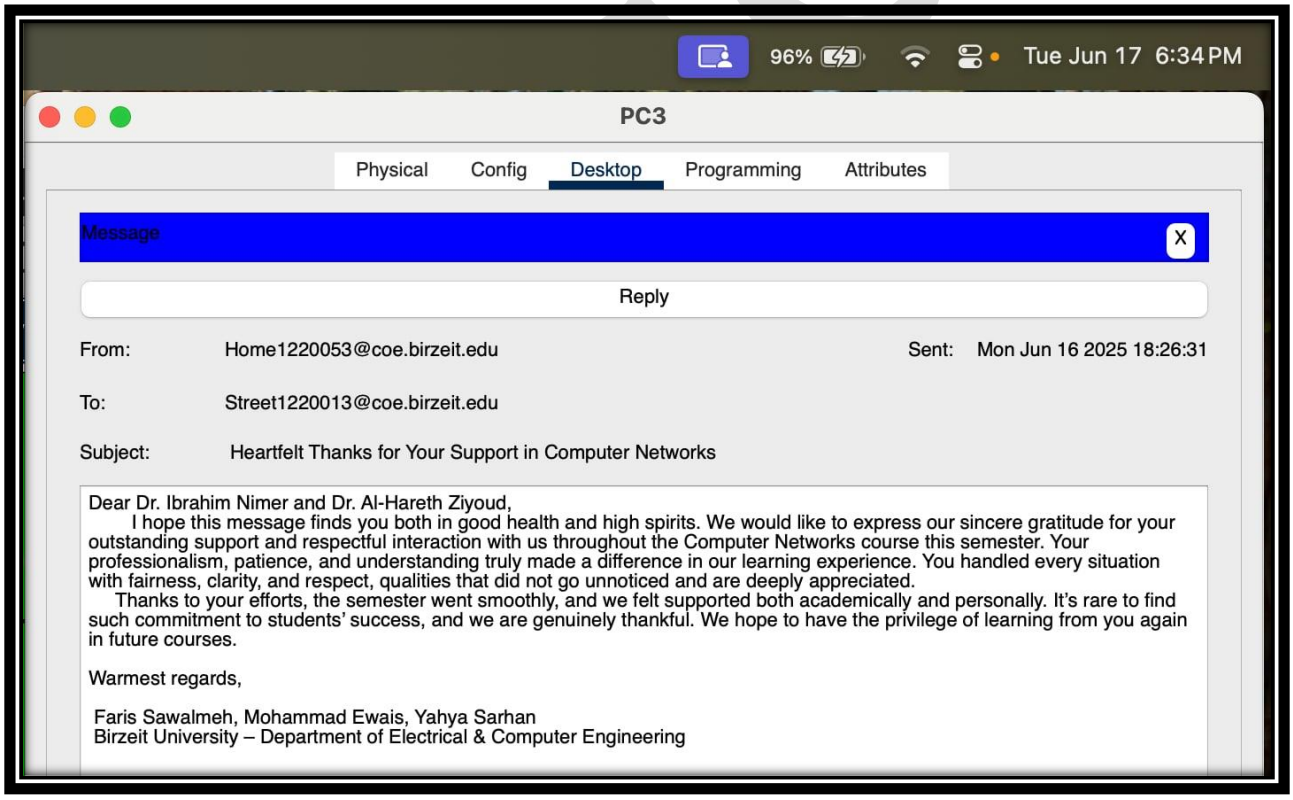


Figure 59: 📨 Email Client – Received Mail

📩 **Email Client – Received Mail**

This screenshot shows the **Email Client** displaying a **received email**, confirming successful communication:

- ✅ **From:** Home1220053@coe.birzeit.edu — The sender's email address, proving internal mail delivery.
- 📥 **To:** Street1220013@coe.birzeit.edu — The intended recipient within the same configured domain.
- 📝 **Subject:** Heartfelt Thanks for Your Support in Computer Networks — The subject matches the sent message.
- ⏰ **Sent:** Mon Jun 16 2025 18:26:31 — Shows the exact timestamp of when the message was sent.
- 💬 **Message Body:** The full message is received correctly, indicating that **POP3 service** is working as expected.

🔍 **Purpose:**
This proves that the **Email Server** can handle **both sending and receiving emails** securely and correctly. It demonstrates that the **SMTP (send)** and **POP3 (receive)** protocols are working without issues, ensuring reliable mail flow in the network. 📨🔄✨

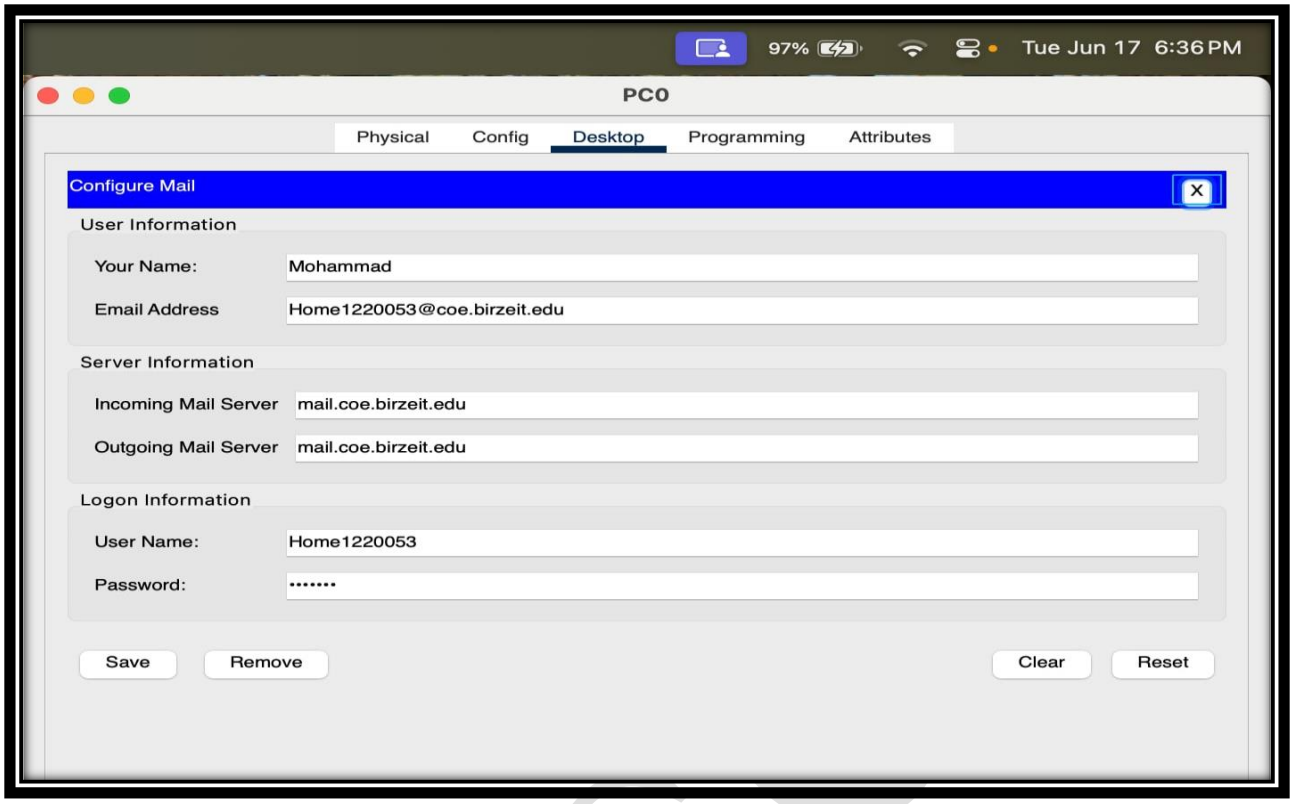


Figure 60: 🖂 Email Client – Configuration Tab

🖂 Email Client – Configuration Tab

This screenshot shows the **Email Client settings** properly configured to connect with the **Mail Server**:

- 👤 **Your Name:** Mohammad — The user's display name for outgoing messages.
- 📧 **Email Address:** Home1220053@coe.birzeit.edu — The full email ID used for sending and receiving mail.
- 📥 **Incoming Mail Server:** mail.coe.birzeit.edu — The POP3 server for downloading received emails.
- 📤 **Outgoing Mail Server:** mail.coe.birzeit.edu — The SMTP server for sending outgoing emails.
- 🔑 **User Name:** Home1220053 — The account username used to authenticate with the mail server.
- 🔒 **Password:** ✔ A secure password is saved to enable successful logon and access.

📁 **Purpose:**

This setup ensures that the **Email Client** can **send (SMTP)** and **receive (POP3)** emails through the **configured mail server**, verifying proper authentication and connectivity. 🔔✅

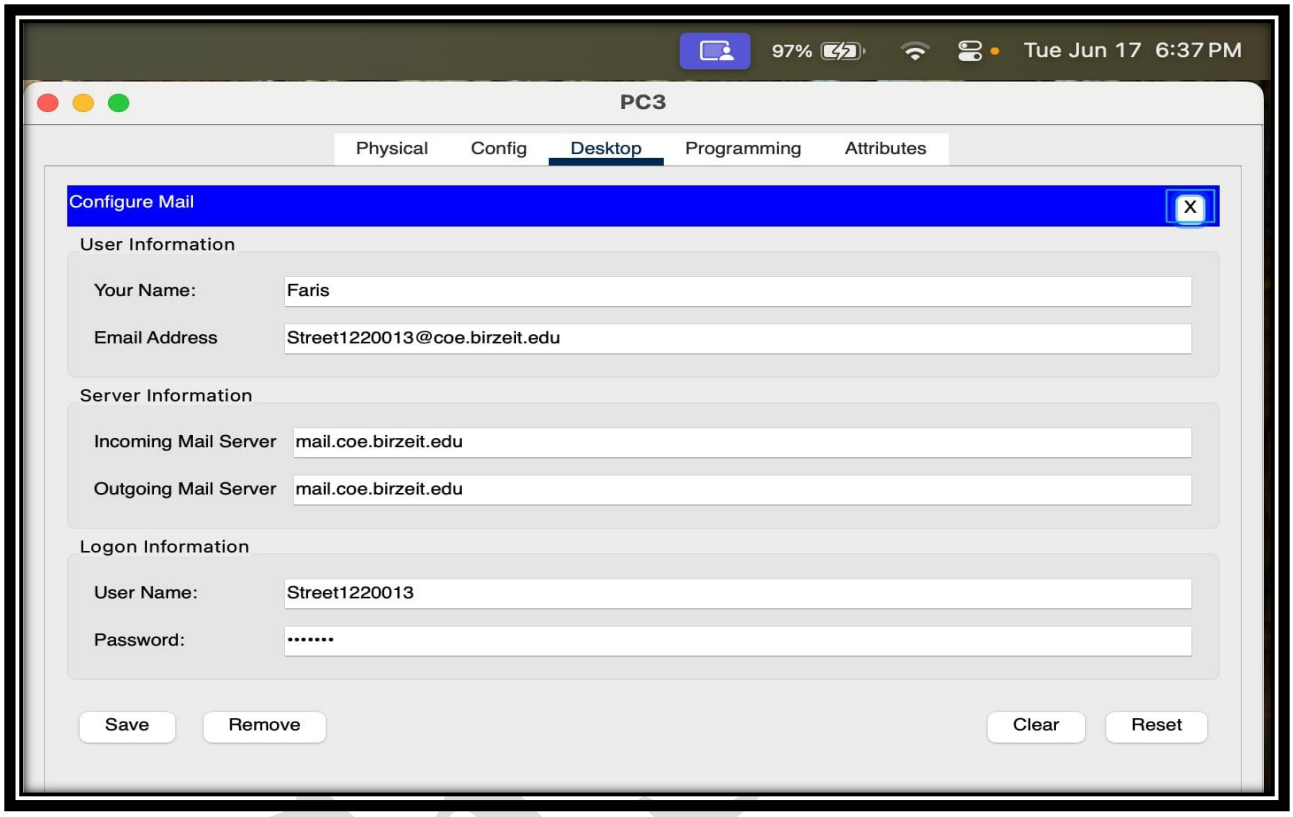


Figure 61: 📧 Email Client – Configuration Tab

📧 Email Client – Configuration Tab

This screenshot shows the **Email Client settings** for **PC3**, confirming it's correctly connected to the **Mail Server**:

- 👤 **Your Name:** Faris — The user's display name shown in sent emails.
- 📄 **Email Address:** Street1220013@coe.birzeit.edu — The unique email address used for communication.
- 📥 **Incoming Mail Server:** mail.coe.birzeit.edu — The POP3 server for receiving emails.
- 📤 **Outgoing Mail Server:** mail.coe.birzeit.edu — The SMTP server for sending emails.
- 🔑 **User Name:** Street1220013 — The login username for mail authentication.

- 🔒 **Password:** ✔ Password is set to ensure secure logon and access.

🗂 **Purpose:**
This configuration allows the **Email Client** to **send and receive emails** securely via the specified mail server, ensuring proper authentication and reliable message delivery. 📩✅

➢ Testing for Successful open web page from some of end devices

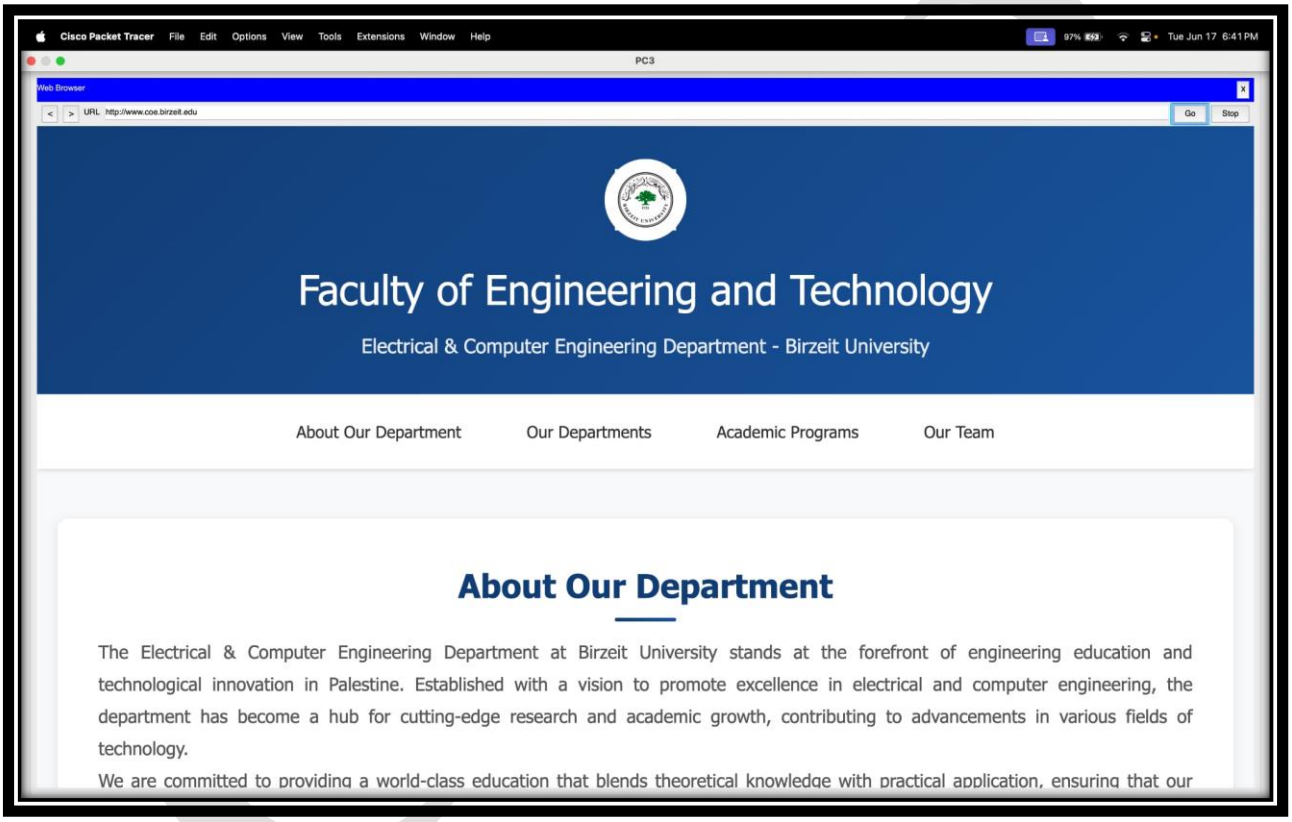


Figure 62: Web Browser – Successful Test

🌐 **Web Browser – Successful Test**

This screenshot shows that the **Web Browser** on **PC3** is working perfectly and can **access the department website**:

- ✅ **Status:** Successfully connected to the **Faculty of Engineering and Technology – Electrical & Computer Engineering Department – Birzeit University** website.
- 🌍 **URL:** http://www.coe.birzeit.edu — The correct domain name was resolved using the configured DNS server.
- 📡 **DNS Working:** The **DNS server** 100.13.8.195 correctly resolved the domain name to the **Web Server IP address**.
- 🔍 **Purpose:** Confirms that both the **DNS resolution** and **HTTP service** are functional, ensuring users can browse department resources smoothly.

🗂️ **Result:**

Web browsing is **operational** 💻✅ — demonstrating that the **network services (DNS + HTTP)** are set up correctly and tested successfully! 🚀✨

➢ Routing Configuration

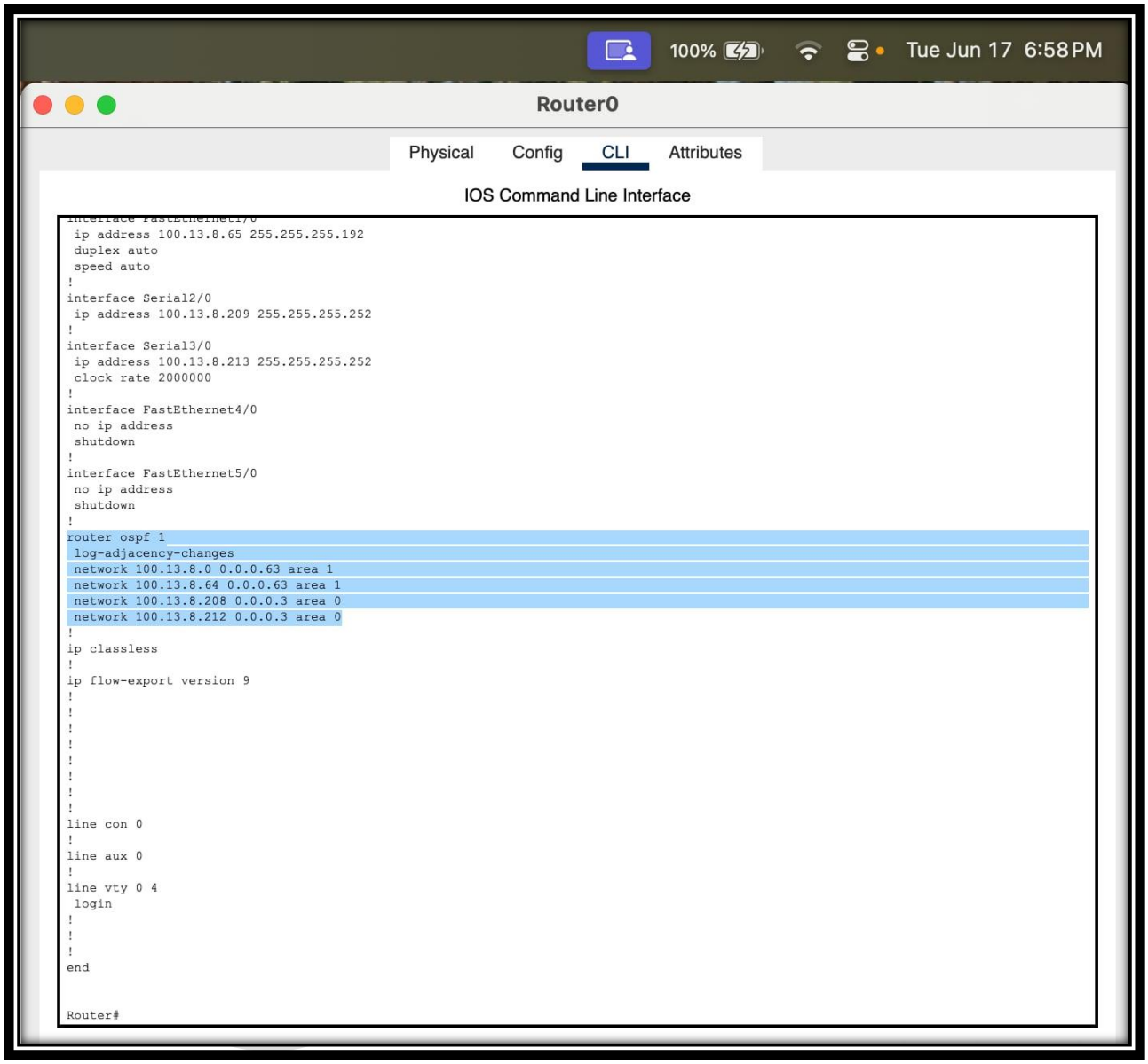


Figure 63: Router0 – OSPF Configuration

🔁 **Router0 – OSPF Configuration**

This screenshot shows the **OSPF (Open Shortest Path First)** routing protocol setup on **Router0**. Here's the breakdown:

- ✅ **OSPF Process:** router ospf 1 — This command starts the OSPF process with ID **1**.
- 🔂 **Log Adjacency Changes:** Enabled to keep track of neighbor changes for troubleshooting.
- 🌐 **Networks Advertised:**
  - network 100.13.8.0 0.0.0.63 area 1 🗺️ — This includes IPs from 100.13.8.0 to 100.13.8.63 in **Area 1**.
  - network 100.13.8.64 0.0.0.63 area 1 🗺️ — Covers 100.13.8.64 to 100.13.8.127 in **Area 1**.
  - network 100.13.8.208 0.0.0.3 area 0 🌍 — Adds 100.13.8.208 to 100.13.8.211 to **Area 0** (the backbone).
  - network 100.13.8.212 0.0.0.3 area 0 🌍 — Includes 100.13.8.212 to 100.13.8.215 in **Area 0**.
- 🔍 **Purpose:**
  - These **network statements** tell OSPF which interfaces to activate on, allowing **Router0** to exchange routing information dynamically.
  - It ensures **efficient routing**, automatic route updates, and **loop-free paths** in the network.

🗂️ **Result:**
OSPF is **successfully configured** and ready to maintain **dynamic routing** across areas for **optimal path selection**! 🛣️🛰️✨

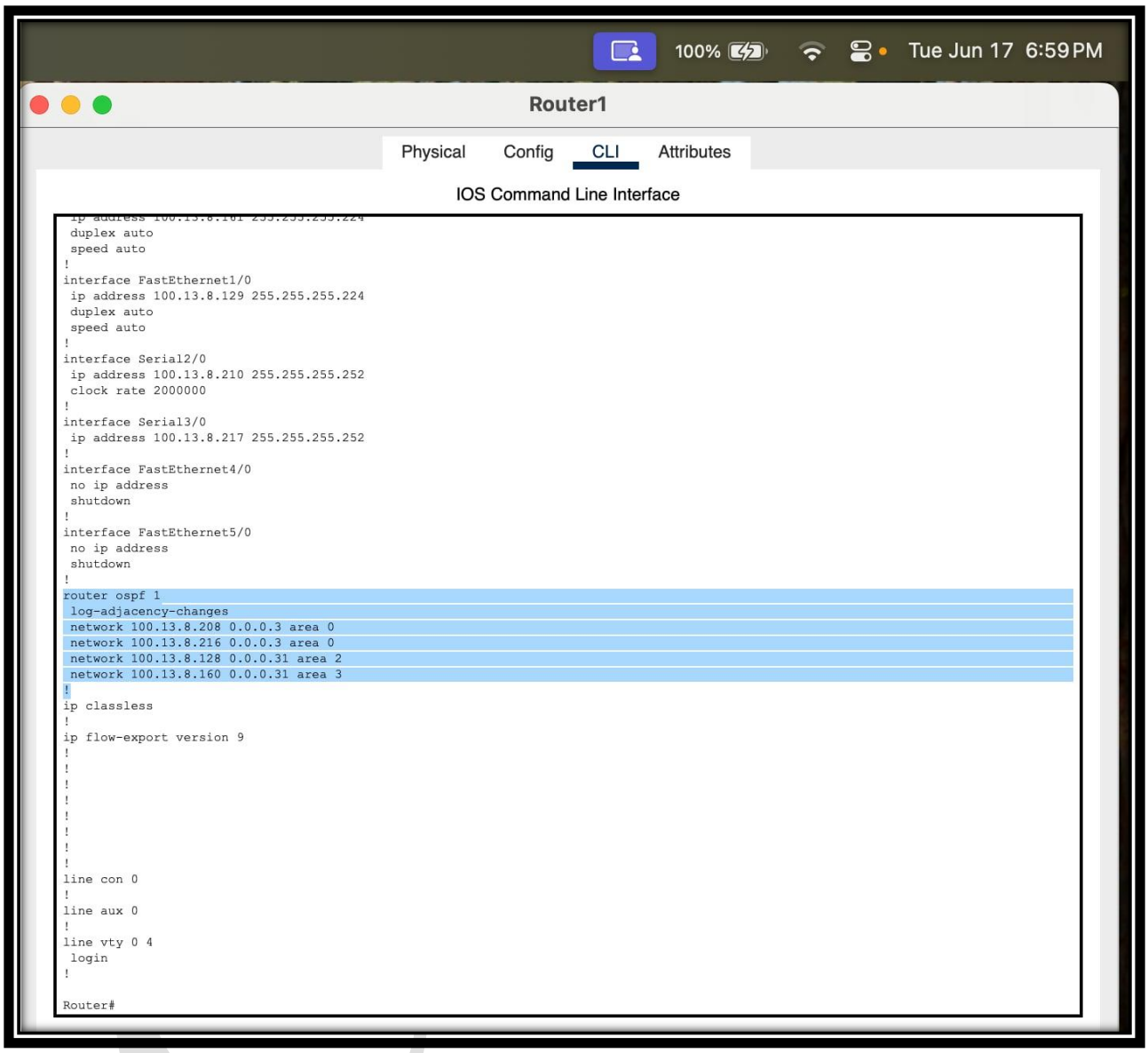


Figure 64: Router1 – OSPF Configuration

🔁 Router1 – OSPF Configuration

This screenshot shows how **Router1** is set up to use **OSPF** for dynamic routing. Here's what's configured:

- ✅ **OSPF Process:** router ospf 1 — Starts OSPF with process ID **1**.
- 🔄 **Log Adjacency Changes:** Enabled to log when OSPF neighbors go up/down.
- 🌐 **Networks Advertised:**
    - network 100.13.8.208 0.0.0.3 area 0 🌍 — Adds IPs 100.13.8.208 to 100.13.8.211 to **Area 0**.
    - network 100.13.8.216 0.0.0.3 area 0 🌍 — Includes 100.13.8.216 to 100.13.8.219 in **Area 0**.
    - network 100.13.8.128 0.0.0.31 area 2 🗺️ — Covers 100.13.8.128 to 100.13.8.159 in **Area 2**.
    - network 100.13.8.160 0.0.0.31 area 3 🗺️ — Covers 100.13.8.160 to 100.13.8.191 in **Area 3**.
- 🔑 **Purpose:**
    - These networks tell OSPF **which interfaces to activate on**, allowing **Router1** to exchange routes with other routers.
    - This enables **efficient, loop-free routing** across different areas, ensuring quick updates and best path selection.

📁 **Result:**

OSPF is **properly running**, so **Router1** can dynamically learn and share routes within **Areas 0, 2, and 3**! 🔔🚀✨

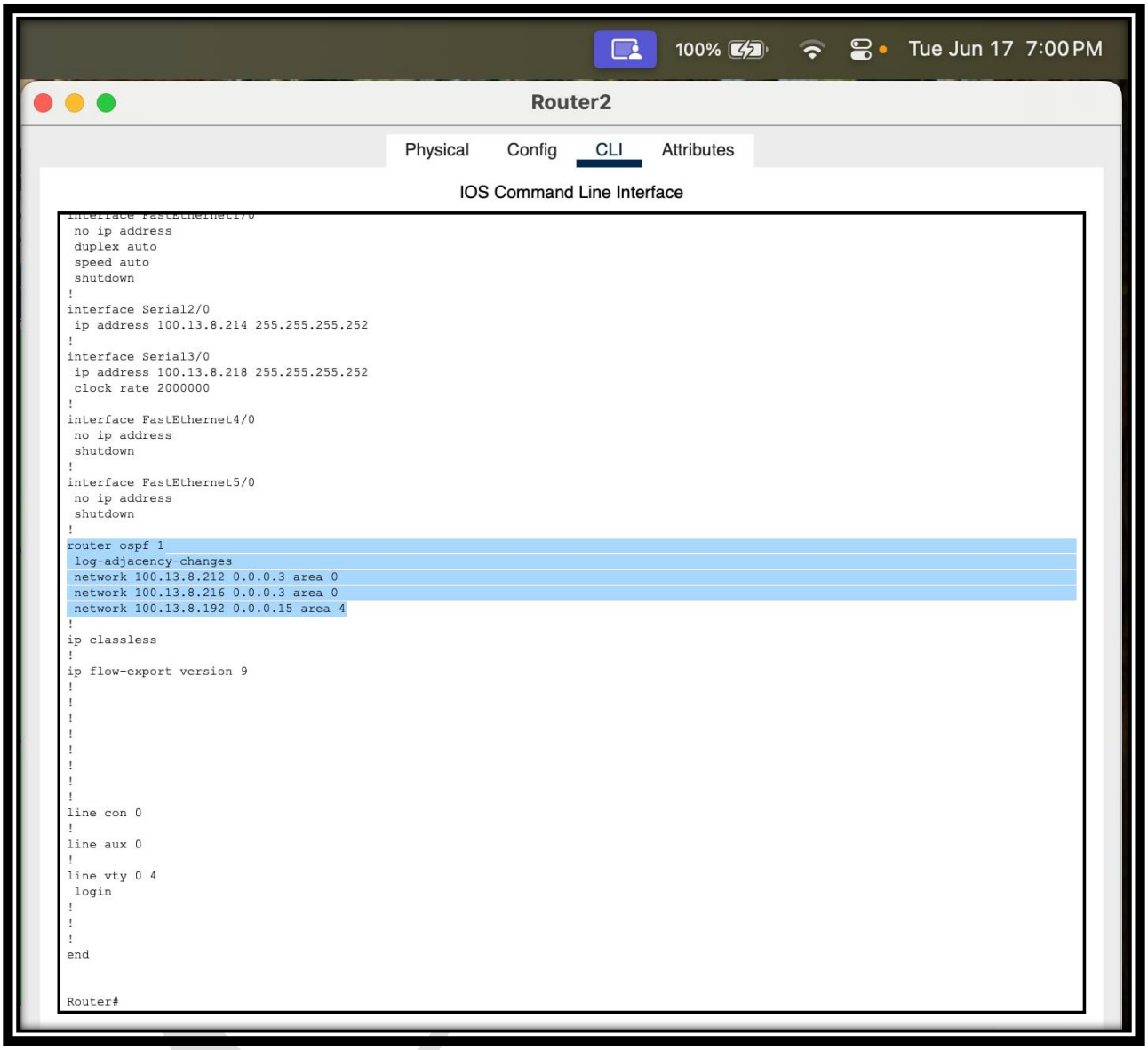


Figure 65: Router2 – OSPF Configuration

🔁 **Router2 – OSPF Configuration**

This screenshot shows how **Router2** is configured for **OSPF** dynamic routing. Here's the breakdown:

- ✅ **OSPF Process:** router ospf 1 — Starts the OSPF process with ID **1**.
- 🔂 **Log Adjacency Changes:** Enabled to log when OSPF neighbor relationships form or break.
- 🌐 **Networks Advertised:**
  - network 100.13.8.212 0.0.0.3 area 0 🌍 — Adds 100.13.8.212 to 100.13.8.215 to **Area 0**.
  - network 100.13.8.216 0.0.0.3 area 0 🌍 — Includes 100.13.8.216 to 100.13.8.219 also in **Area 0**.
  - network 100.13.8.192 0.0.0.15 area 4 🗂️ — Covers 100.13.8.192 to 100.13.8.207 in **Area 4**.
- 🔍 **Purpose:**
  - These statements tell OSPF **which interfaces to activate on** and which IP subnets to advertise.
  - This ensures **Router2** communicates efficiently with other routers in **Areas 0 and 4**, providing robust and dynamic routing updates.

🗂️ **Result:**

OSPF on **Router2** is working perfectly ✅ — routes are dynamically learned and shared, keeping the network **loop-free** and **optimized**! 📡✨🌐

❖ Issues & Limitations

During the **design** and **implementation** of the network topology using **Cisco Packet Tracer**, the team faced various **challenges** and **limitations**. A major hurdle was that it was our **first experience** working with Cisco Packet Tracer, requiring us to spend time **learning** how to navigate the platform and utilize its features effectively. This **learning curve** occasionally **slowed our progress**, especially during **device configuration** and **network troubleshooting**. Moreover, due to the software's **simulation constraints**, we were unable to accurately test **network performance** under **heavy traffic** conditions. **Team collaboration** posed additional challenges, including **synchronizing design updates** and **merging individual work** into a unified topology. Furthermore, **time limitations** and the **complexity of resolving configuration errors** underscored the importance of clear **communication** and efficient **coordination** among team members. Despite these difficulties, the project offered valuable **hands-on experience** in **network design**, **problem-solving**, and **teamwork**, which will be highly beneficial for future projects.

❖ Teamwork

Before starting the **implementation** of our **network topology design project**, we **convened as a team** to plan and determine the most effective way to **divide the workload**. During this meeting, we carefully **analyzed the project requirements and tasks**, assigning roles based on each member's **expertise** and **skills**. This resulted in a **balanced and fair distribution of responsibilities**, leading to **satisfactory outcomes** for everyone involved.

The project consisted of **three autonomous systems**, with **each team member managing one system** independently. After completing our respective sections, we **met again to discuss and interconnect the autonomous systems**. We **thoroughly reviewed each other's work** to ensure **accuracy**, **clarity**, and **mutual understanding**, which strengthened our collective knowledge.

Next, we gathered to **perform comprehensive testing** of the entire network. During this phase, we actively **exchanged ideas** and worked together to write the **abstract** and **conclusion** of the report. To maintain fairness, the **report writing** was divided so that each member covered their **assigned autonomous system** and contributed to **one-third of the theoretical background**.

Overall, the project demonstrated **exceptional teamwork**, with **strong cooperation**, **effective communication**, and an **equitable division of tasks**, ensuring that each member's contributions were valued and integrated seamlessly.

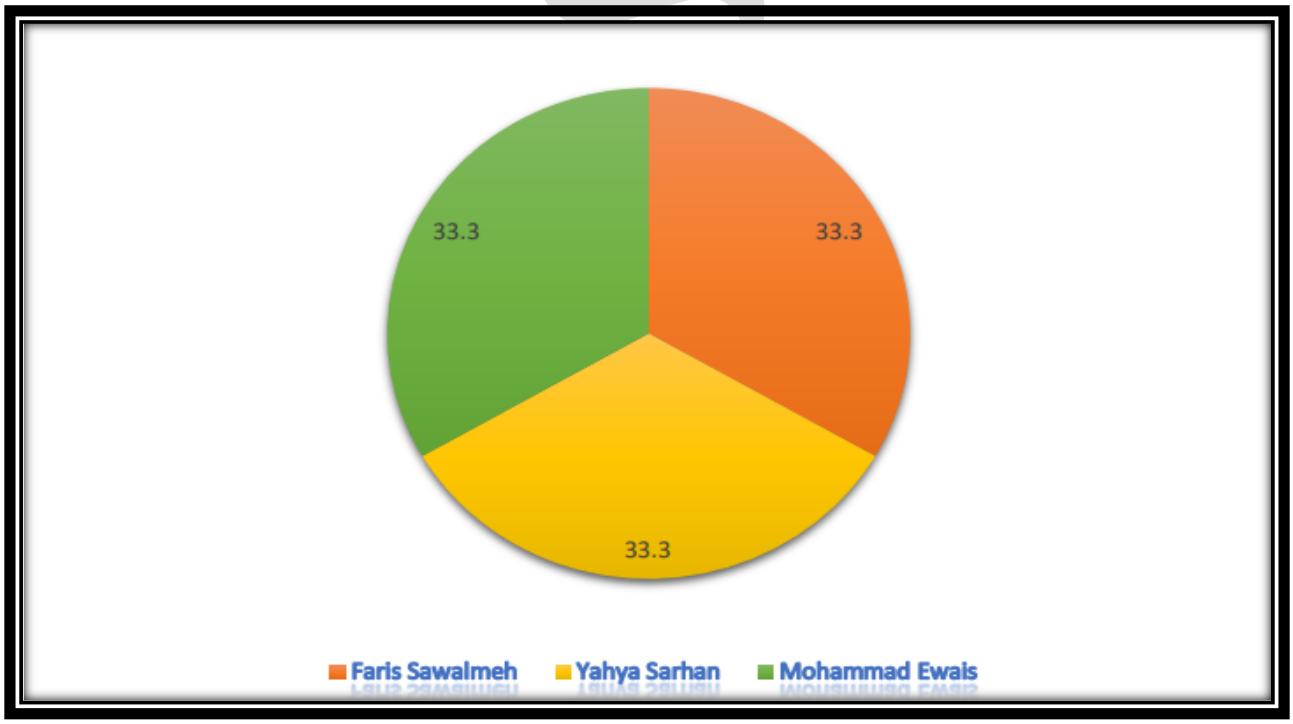


Figure 66: Teamwork Chart

❖ Conclusion

This project successfully demonstrates how to build a **fully functional network** integrating multiple core services using **Cisco Packet Tracer**.

🔑 **Key Achievements:**

- **IP Addressing:** All devices were assigned **correct IPv4 addresses**, **subnet masks**, and **default gateways** according to their roles.
- **DHCP Server:** Configured to **automatically assign IP addresses** to client devices, simplifying network management and reducing manual configuration.
- **DNS Server:** Set up to resolve **domain names** to **IP addresses**, enabling users to access web pages using easy-to-remember names instead of numbers.
- **Web Server:** Hosted a **website** for the **Faculty of Engineering and Technology** with pages like **About Our Department**, **Departments**, **Academic Programs**, and **Our Team**, proving successful **HTTP & HTTPS** operation.
- **Email Service:** Fully functional **SMTP** and **POP3** services were tested; users configured their **mail clients**, composed, sent, and received messages—verifying end-to-end email delivery.
- **Routing:** Implemented **OSPF dynamic routing** on all routers (**Router0**, **Router1**, and **Router2**) to ensure **automatic route learning and updating** across multiple **areas** (Area 0, 1, 2, 3, 4).
- **Testing:** Verified **ping connectivity**, successful **web browsing**, and **email communication** between PCs, laptops, smartphones, and servers — ensuring the network operates smoothly and reliably.

🎯 **Outcome:**

This project demonstrates a **realistic enterprise network** where key services — **IP allocation (DHCP)**, **name resolution (DNS)**, **website hosting (Web Server)**, **email communication**, and **dynamic routing (OSPF)** — work together seamlessly.

Students and users can connect, browse, send emails, and access shared resources without manual network configuration. The network is **scalable**, **efficient**, and **secure**, providing a strong foundation for larger real-world implementations.

✨ **In summary:**

This work proves mastery of **network configuration, services integration, and dynamic routing protocols**, meeting both academic and practical goals. ✅🌐📡

❖ References

[1]: geeksforgeeks, Network Address Translate, **Click Here**

[2]: geeksforgeeks, Dynamic Host Configuration Protocol, **Click Here**

[3]: geekforgeeks, Difference between http and https, **Click Here**

[4]: geeksforgeeks, Difference between SMTP and POP3, **Click Here**

[5]: geeksforgeeks, Domain Name System, **Click Here**

[6]: geeksforgeeks, Open Shortest Path First, **Click Here**