National University of Computer and Emerging Sciences
Islamabad Campus

CS-3001

COMPUTER NETWORKS

FINAL PROJECT

Submitted by: Fatima Naeem
Roll number: 23i-2046

Table of Contents

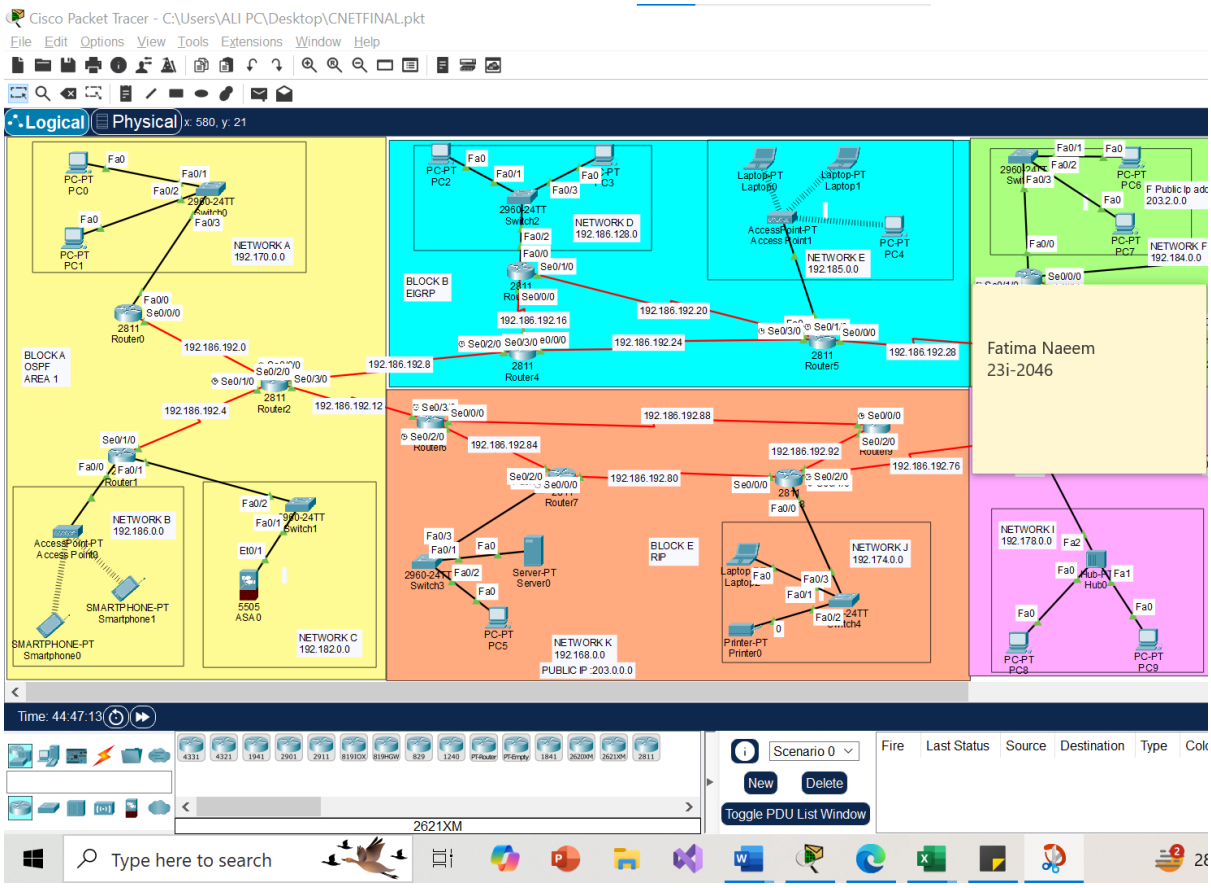
OBJECTIVES

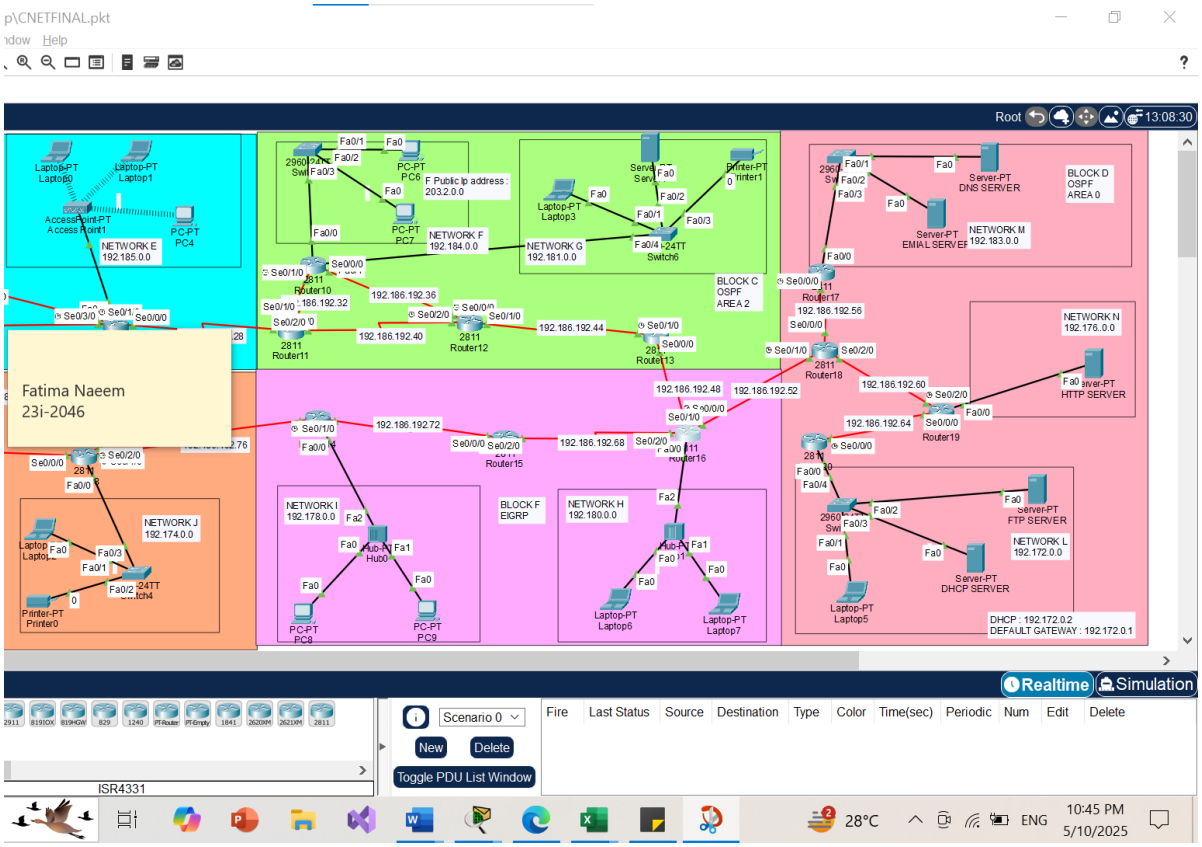
This project is about creating a complete network in Cisco Packet Tracer. I used VLSM for subnetting, set up dynamic routing with EIGRP, OSPF, and RIP, and configured DHCP to assign IPs automatically. NAT was added on two routers for internet access. ACLs were used to block certain devices from accessing the web server as required. I also set up a Mail Server for email between two networks and allowed only one network to use the FTP server. All settings followed the IP details given in the assignment.

Implementation Steps

1. CREATING THE TOPOLOGY

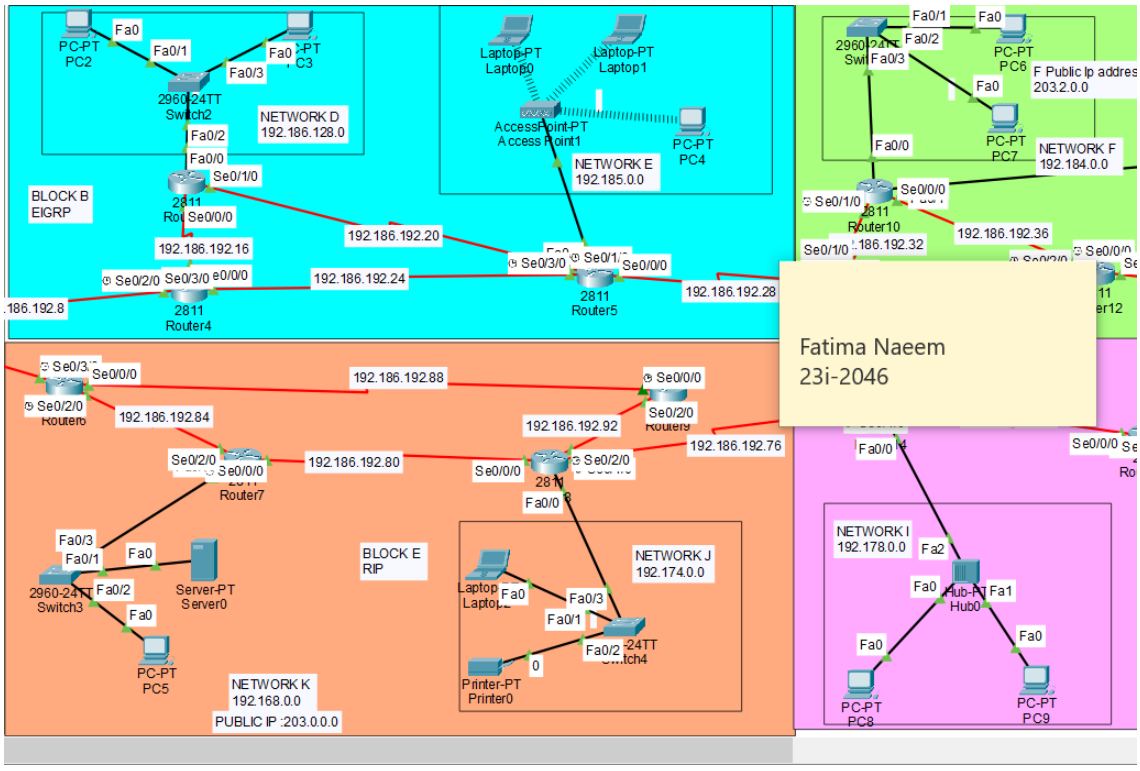
In the implementation, the first step was creating the network topology in Cisco Packet Tracer. I carefully placed the routers, switches, and end devices as per the given layout. Each network block was labeled correctly, and connections were made using the appropriate cables. This provided a clear structure to start configuring IP addresses, routing protocols, and services in the next steps.





2. Planning & VLSM Subnetting

Subnetting was done using Variable Length Subnet Masking (VLSM) to allocate IPs efficiently based on host requirements for each network and connections between routes too. The VLSM helped in assigning Ips to all the subnets and networks and calculate the usable Ip ranges.



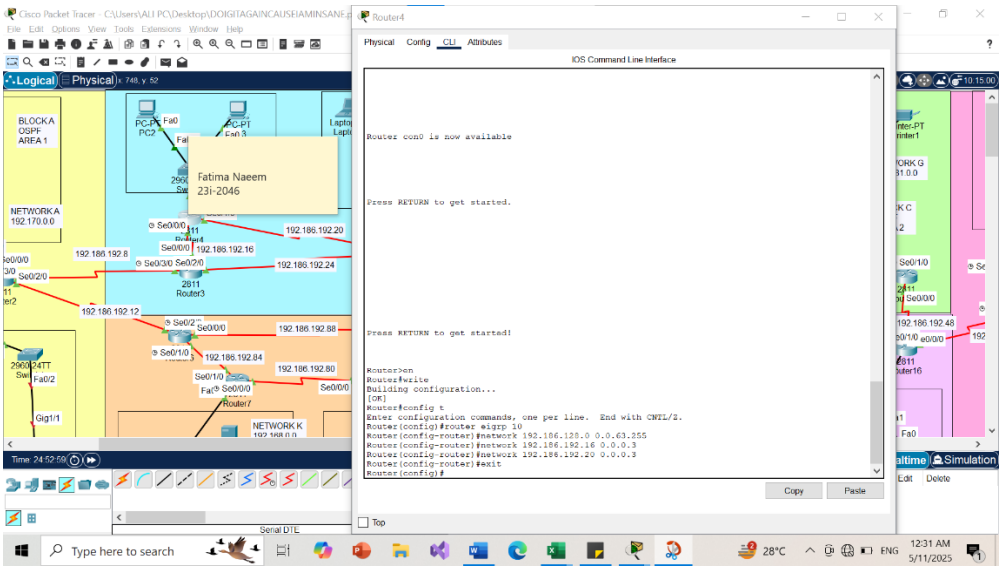
3. ROUTING CONFIGUARATIONS

EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP is a dynamic routing protocol that is used to automatically distribute routing information across routers It was implemented in **BLOCK F** and **BLOCK B**.

STEPS

1. Go to the CLI of routers.
2. En
3. Config t
4. router eigrp 10
5. network <ip address of the network> <wildcard>
6. do this for all the connected networks

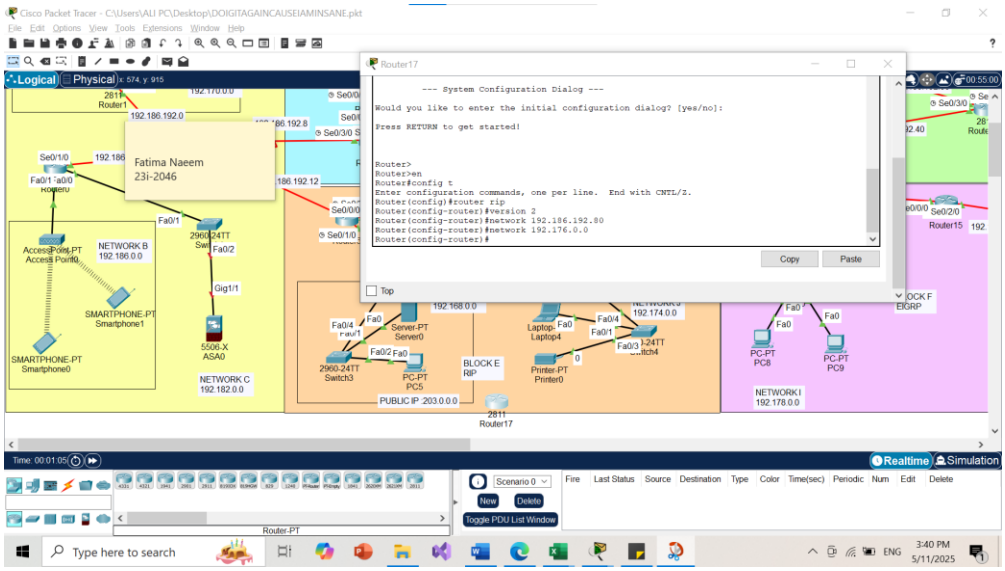


RIP (Routing Information Protocol)

RIP is a distance-vector routing protocol that is easy to configure and suitable for small to medium-sized networks. This was implemented in **BLOCK E** .

STEPS

1. Go to the CLI of router.
2. en
3. config t
4. router rip
5. version 2
6. network <ip address>
7. do for all connected networks.

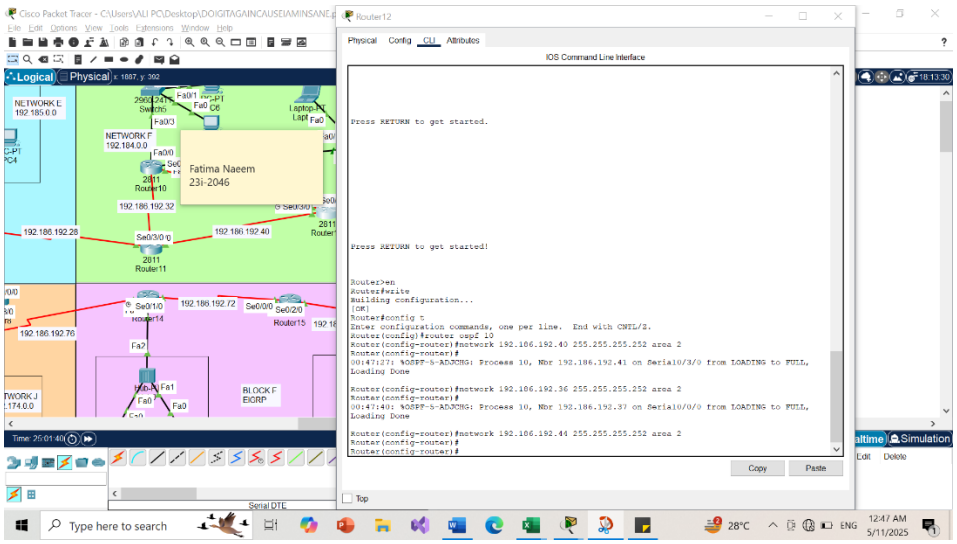


OSPF (Open Shortest Path First)

OSPF is a link-state routing protocol that provides faster convergence and greater scalability compared to RIP. OSPF divides networks into areas for efficient routing and uses the Dijkstra algorithm to compute the best path. It was implemented in **BLOCK A , BLOCK C and BLOCK D.**

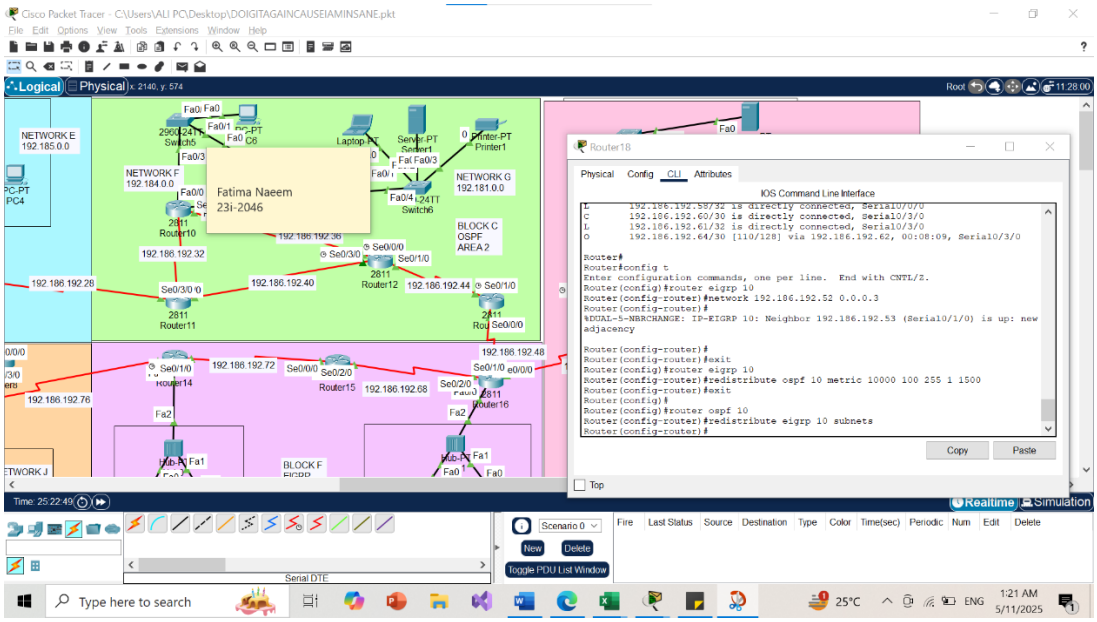
STEPS

1. en
2. config t
3. router ospf 10
4. network <ipaddress of network > <subnet mask > <area # >
5. do for all connected networks



4. REDISTRIBUTION

Redistribution is the process of sharing routing information between different routing protocols, such as EIGRP, RIP, or OSPF. Since each protocol has its own way of calculating the best path, routers that use different protocols may not be aware of each other's routes. By redistributing routes, we allow these different protocols to exchange routing information, so they can work together and make sure all routers in the network know the best paths to reach every destination. In this project, redistribution was done to ensure that all routers, using EIGRP, RIP, or OSPF, could exchange routing information and maintain proper communication between different parts of the network, even if they were running different protocols.

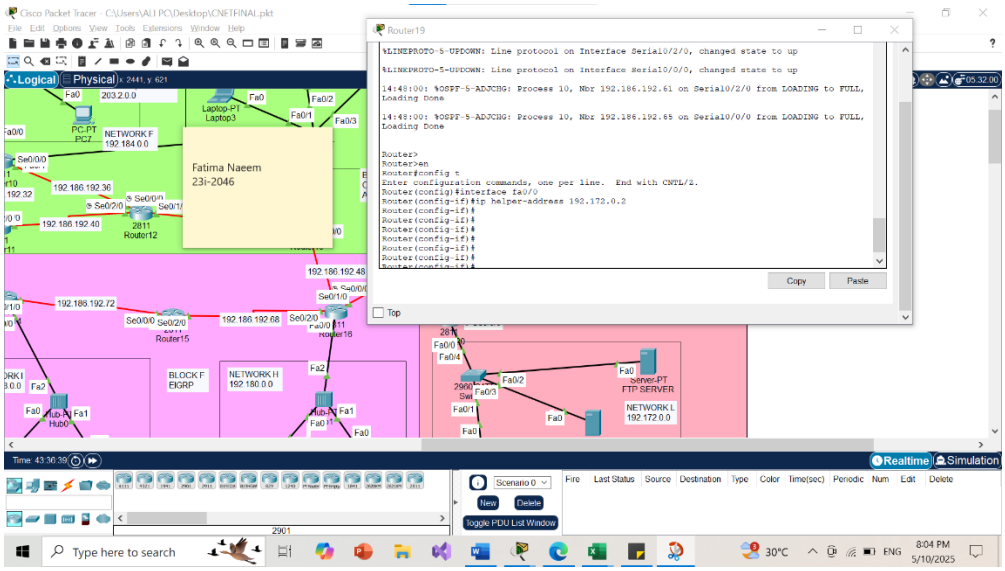


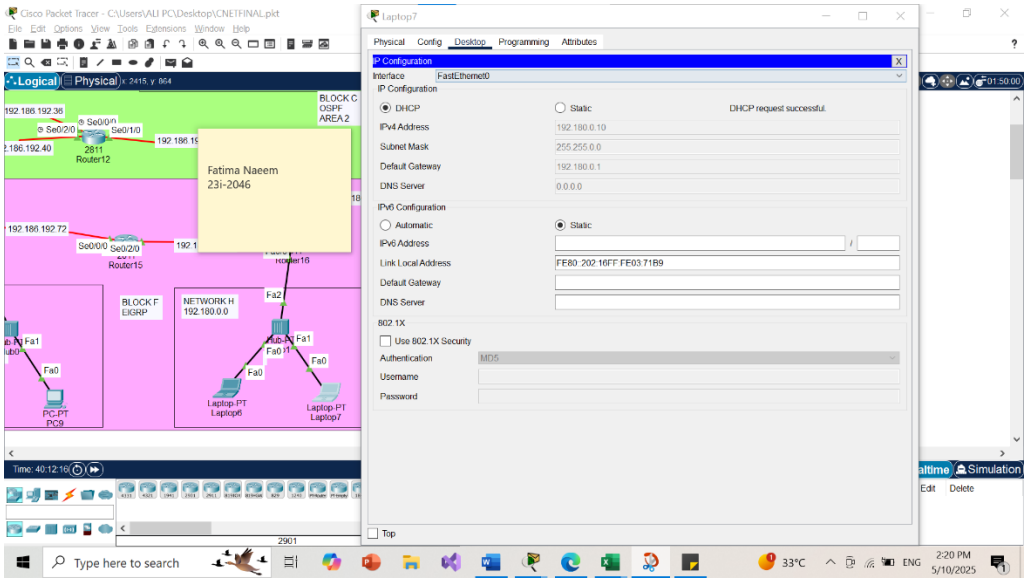
5. DHCP

Then all the devices in Networks A , B , C , D , E, F, G, H, I, J, K, L, M, N were assigned Ip addresses through DHCP from a DHCP server present in Network L with Ip address : 192.172.0.2

Steps

1. Go to device
2. Desktop
3. Ip configuration
4. Change it for static -> DHCP





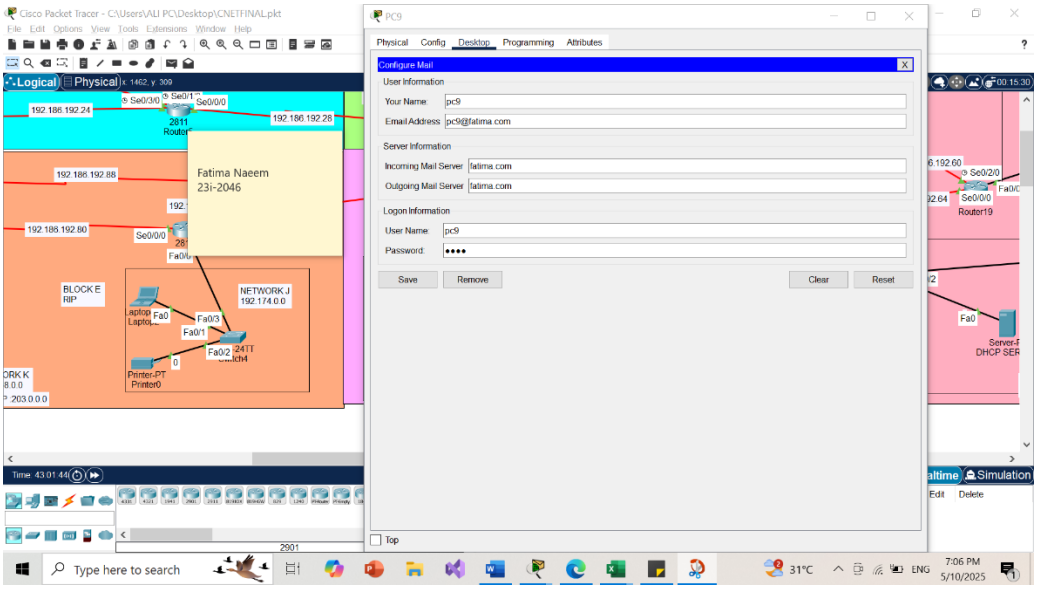
Mail Server Access – Network H and I

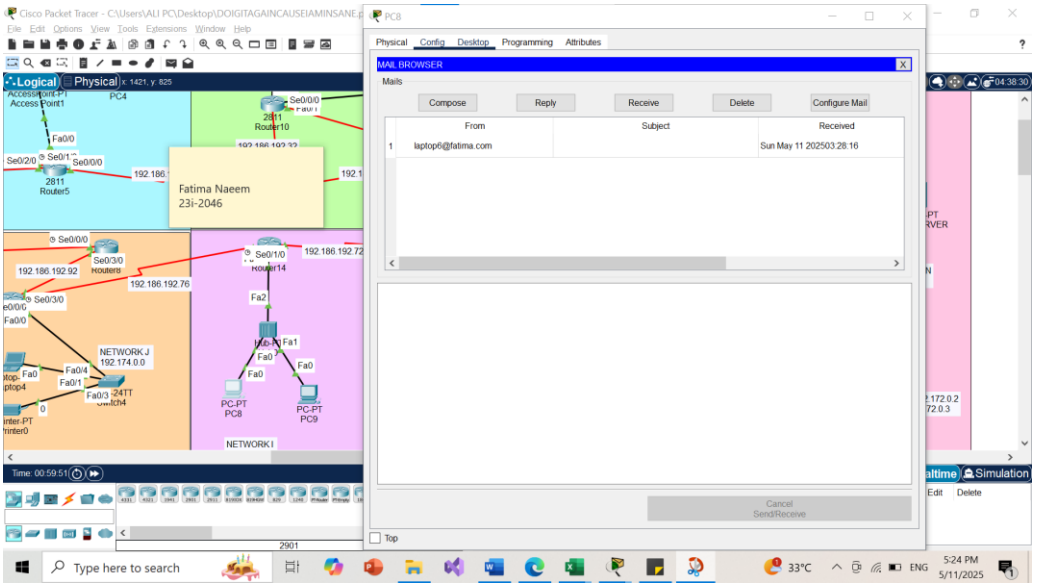
The Mail Server is in Network D. Only computers in **Network H** and **Network I** are allowed to send and receive emails through it. To do this, I configured emails on the devices of network H and I with domain name **fatima.com**.

STEPS

1. **Configure the DNS Server**: Add the IP addresses and corresponding hostnames of all devices to the DNS server, so names can be resolved to IPs.
2. **Set Up Email Accounts**: Configure email settings on each device and create user accounts on the mail server for every user.
3. **Add the Email Domain to DNS**: Register the domain name used for emails (e.g., @yourdomain.com) in the DNS server so devices can locate the mail server.

4. **Test Email Communication**: Send and receive emails between configured devices to confirm everything is working properly.

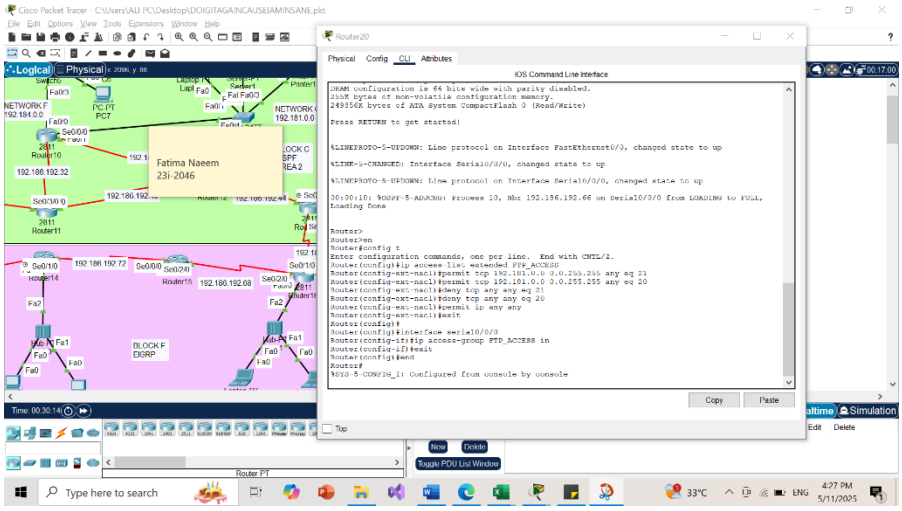




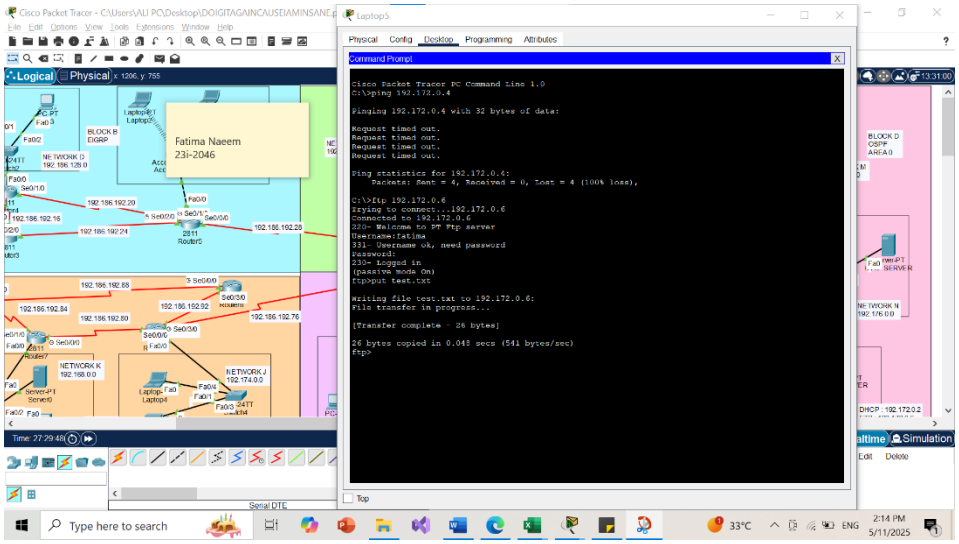
FTP Upload Restriction – Network G

Only devices in Network G should be able to access and upload files to the FTP server. To do this, we use ACLs to **allow traffic from Network G** to the FTP server on **ports 21 and 20** (FTP command and data). The ACL is added to the router interface connected to the FTP server. All other networks are blocked, so only Network G can use FTP.

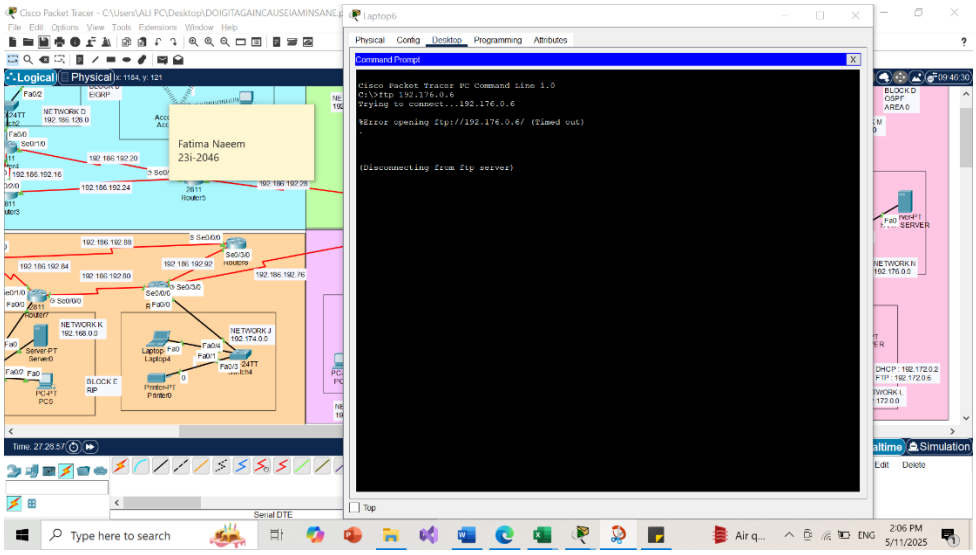
ACL



FTP WORKING CORRECTLY



FTP NOT WORKING



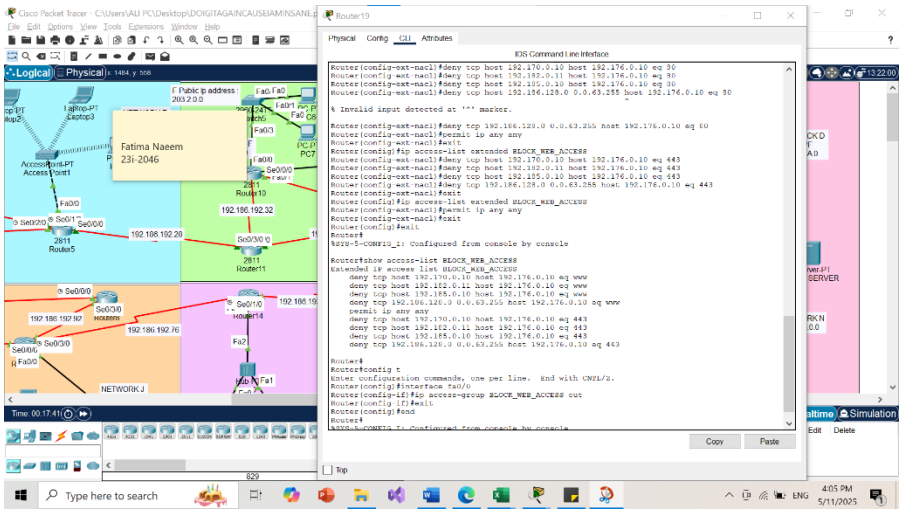
Web Server Access Restrictions using ACLs

Access to the **Web Server (192.176.0.10)** was to be controlled using ACLs on the router it's connected to. Here's what is blocked:

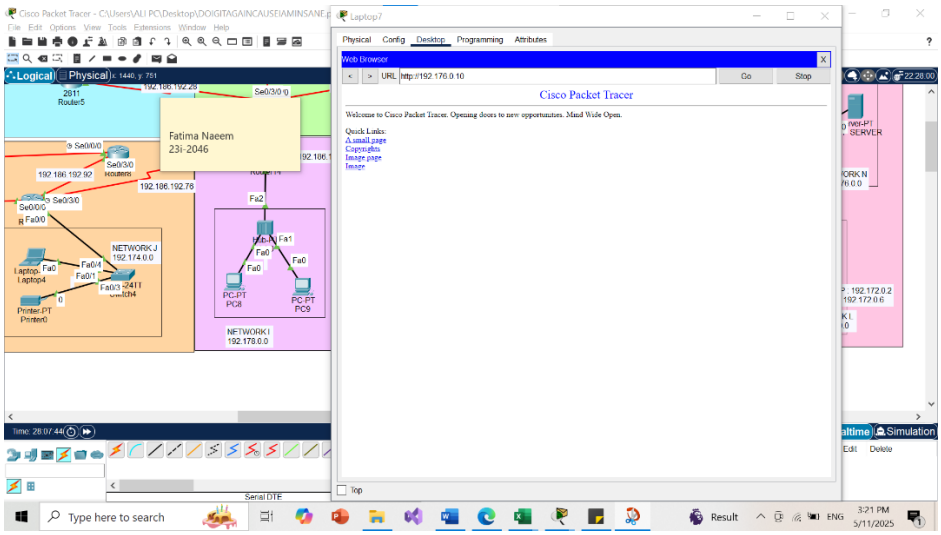
- One PC from **Network A**
- One laptop from **Network E**
- One smartphone from **Network B**
- **All devices in Network D**

Use **extended ACLs** to deny access from these specific devices and subnets to the Web Server's IP on ports **80 (HTTP)** and **443 (HTTPS)**. Used the ACL **inbound** on the router interface facing the Web Server to enforce these restrictions.

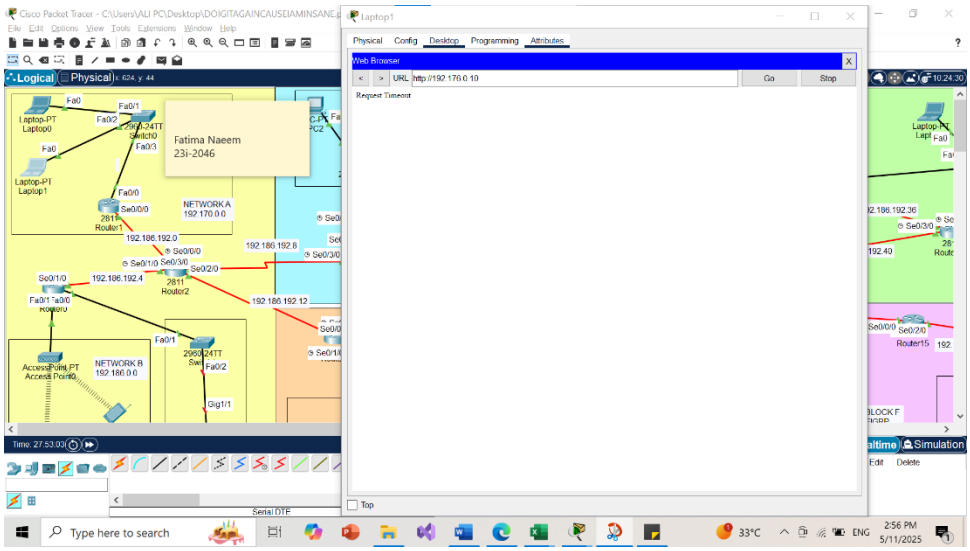
ACL



WEBSERVER ACCESS :



WEB SERVER NOT BEING ACCESSED :



NAT Implementation

configured **NAT on** connected to **Network K** and to **Network F** using the **public IP addresses provided**. On each router, I set up NAT rules to translate the **private IP addresses** of the internal networks to their respective **public IPs**. This allows devices in both networks to access the internet while keeping their internal IPs hidden.