**CS3001**

**Computer Networks**

**Project**

**Design and Simulation of a Multi-Protocol(OSPF,EIGRP,RIP) along with redistribution, Multiple kind of Servers with services ACL, NAT, FTP**

**Submitted by:** Habib Ahmed

**Roll number:** 23i-2078

**Date:** 5/12/2025

**Table of Contents**

[**1. Project Objectives** 3](#_Toc197977383)

[**2. Methodology & Steps Followed During Implementation** 3](#_Toc197977384)

[**3. Network Design and Configuration Details** 4](#_Toc197977385)

[**4. Observations and Results** 5](#_Toc197977386)

[**5. Screenshots** 6](#_Toc197977387)

[**6. Conclusion** 9](#_Toc197977388)

# **1. Project Objectives**

The primary objectives of this Computer Networks project are:

* To simulate a complex network topology using Cisco Packet Tracer.
* To apply subnetting using Variable Length Subnet Masking (VLSM).
* To configure and implement routing protocols: EIGRP, OSPF (Areas 1 & 2), and RIP v2.
* To enable communication between these protocols through route redistribution.
* To set up and configure a centralized DHCP Server for dynamic IP addressing.
* To implement NAT (Network Address Translation) for external network access.
* To restrict access to the Web Server using Access Control Lists (ACLs).
* To configure Mail and FTP servers with access limited to specific network segments.

# **2. Methodology & Steps Followed During Implementation**

1. **Topology Design**: The given logical network layout was replicated precisely using routers, switches, servers, and end devices categorized by color-coded network blocks (A to N).
2. **VLSM Subnetting**: Calculated subnets based on host requirements provided. Applied VLSM to efficiently allocate IP ranges.
3. **Router and Interface Configuration**: Given IP addresses were assigned to all router interfaces and devices as per subnetting plans.
4. **Routing Protocols**:
   * EIGRP configured in Block B and Block F.
   * OSPF Area 1 and 2 configured in Blocks A and C.
   * RIP configured in Block E.
5. **Route Redistribution**: Applied between routers connecting different blocks (e.g., EIGRP-OSPF, OSPF-RIP, EIGRP-RIP).
6. **DHCP Configuration**: Central DHCP server configured in Block D to assign IPs dynamically to devices in DHCP-enabled blocks.
7. **NAT Implementation**:
   * Configured on Router7 (connected to Network K).
   * Configured on Router11 (connected to Network F).
   * Used public IPs provided in IP address file.
8. **ACL Configuration**:
   * Blocked one PC from Network A from accessing the Web Server.
   * Blocked a laptop from Network E and smartphone from Network B.
   * Blocked all devices in Network D from accessing the Web Server.
9. **Server Configuration**:
   * FTP Server in Network L allows only hosts to upload files.
10. **Testing & Validation**:

* Verified IP addressing.
* Confirmed routing tables and redistribution.

# **3. Network Design and Configuration Details**

**3.1 VLSM and IP Address Planning**

Variable Length Subnet Masking (VLSM) was used to allocate IP addresses efficiently based on the number of hosts required in each network. Point-to-point links between routers were assigned /24 subnets (4 IPs – 2 Hosts) to minimize address waste.

Each subnet is planned to ensure that host and network communication requirements are met with minimum wastage.

**3.2 Routing Protocols**

Routing protocols were used to manage the dynamic exchange of routing information between routers.

* **EIGRP (Enhanced Interior Gateway Routing Protocol):**
  + Used in Blocks B and F.
* **OSPF (Open Shortest Path First):**
  + Used in Blocks A, C and D, with Area 1, 2, 0.
* **RIP (Routing Information Protocol):**
  + Used in Block E.

**3.3 DHCP Configuration**

* Reduces manual IP configuration errors.
* Simplifies network management.

**Where it is used?**

* A centralized DHCP Server is placed in Block D.
* It serves hosts B & H(EIGRP), A, C & D (OSPF), and E (RIP).

**3.4 NAT Configuration**

**What is NAT?**  
Network Address Translation (NAT) converts private IP addresses into public IP addresses.

**Why use NAT?**

* Enhance security by hiding internal IPs.

**Where NAT is used in the project?**

* Router7 (connected to Network K)
* Router11 (connected to Network F)

**3.5 ACL Configuration**

**What are ACLs?**  
Access Control Lists (ACLs) control network traffic by filtering packets based on IP.

**Why use ACLs?**

* To enhance security.
* To restrict specific devices or networks from accessing services.

**Where ACLs were applied?**

* Router connected to the Web Server:
  + Denied one PC from Network A.
  + Denied one Laptop from Network E.
  + Denied one Smartphone from Network B.
  + Denied complete access to Network D.

**3.6 FTP Server Configuration**

**Purpose:** To allow file uploads.

**Location:** Network G

**Access Restricted to:** Only devices in Network G.

**Configuration:**

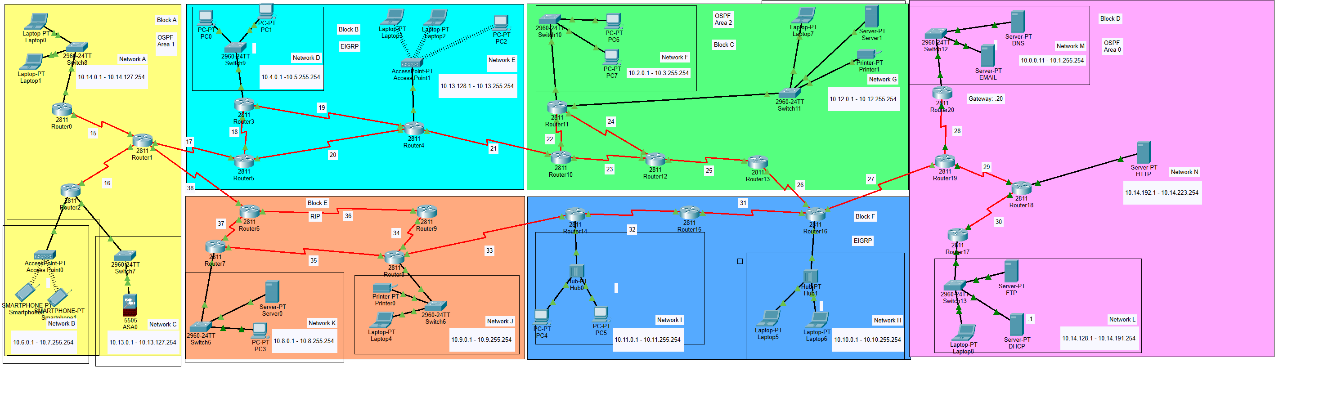
* FTP Server IP: 10.14.128.1
* Username/password set up for clients.

# **4. Observations and Results**

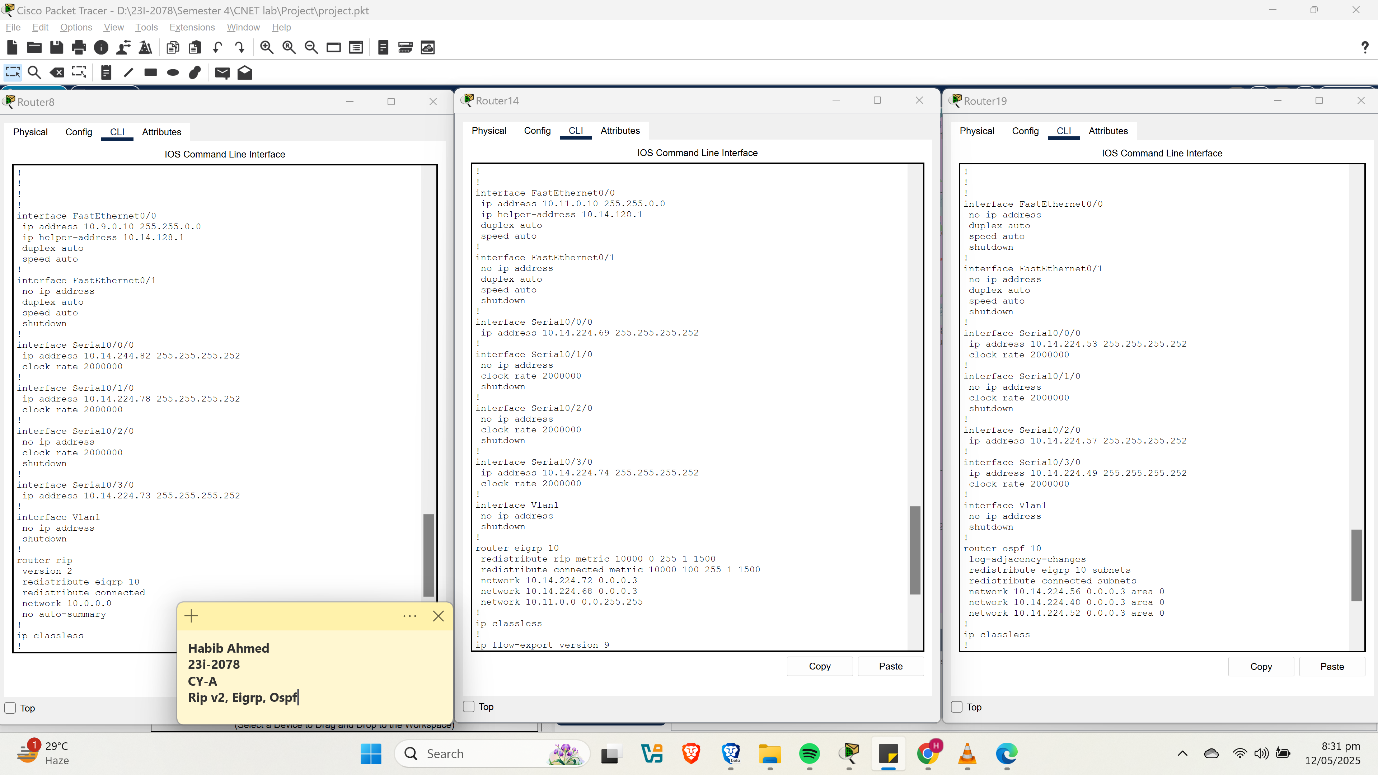
* Routing tables correctly propagated through redistribution.
* Router interfaces correctly configured.
* DHCP records correctly maintained.
* NAT configured on routers through commands.
* FTP turned ON, username and password set.

# **5. Screenshots**

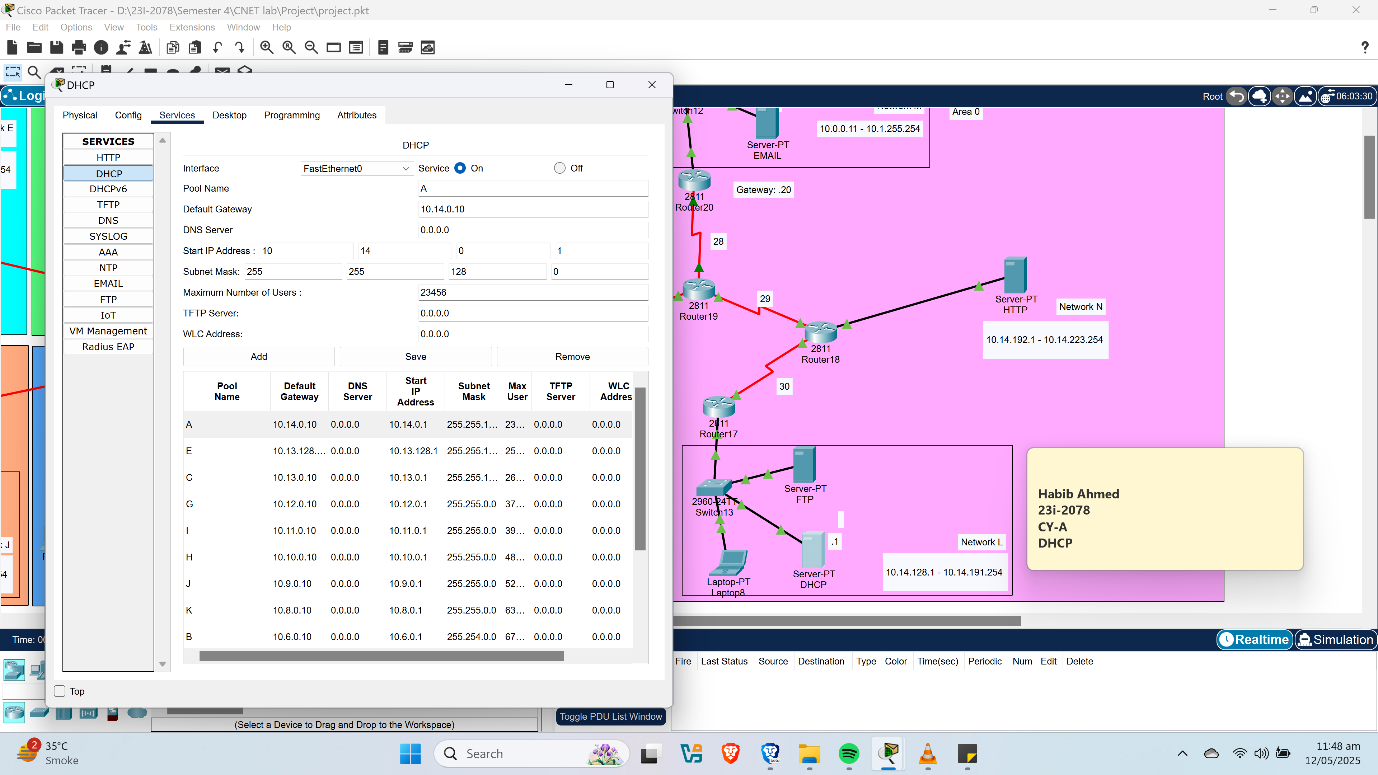
* Full topology diagram.



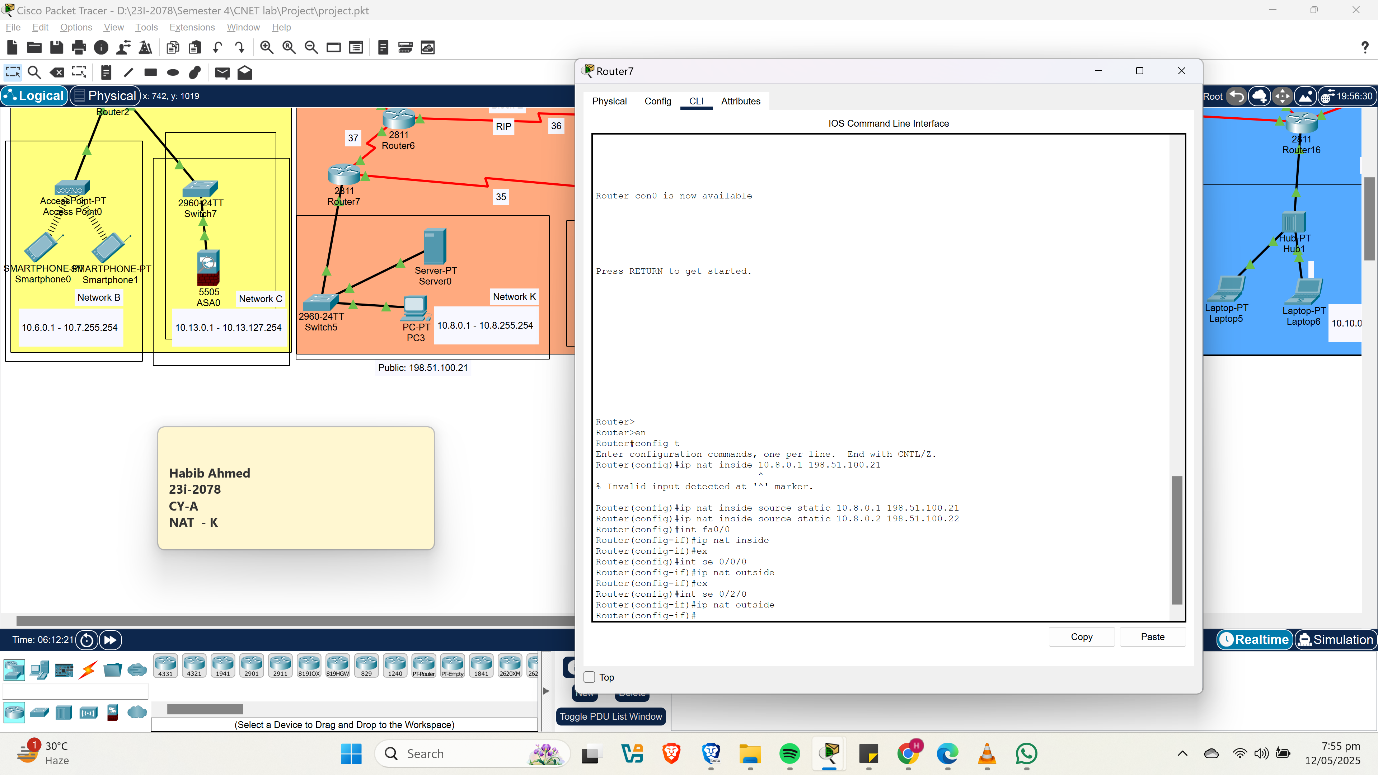
* Router and switch interface settings.

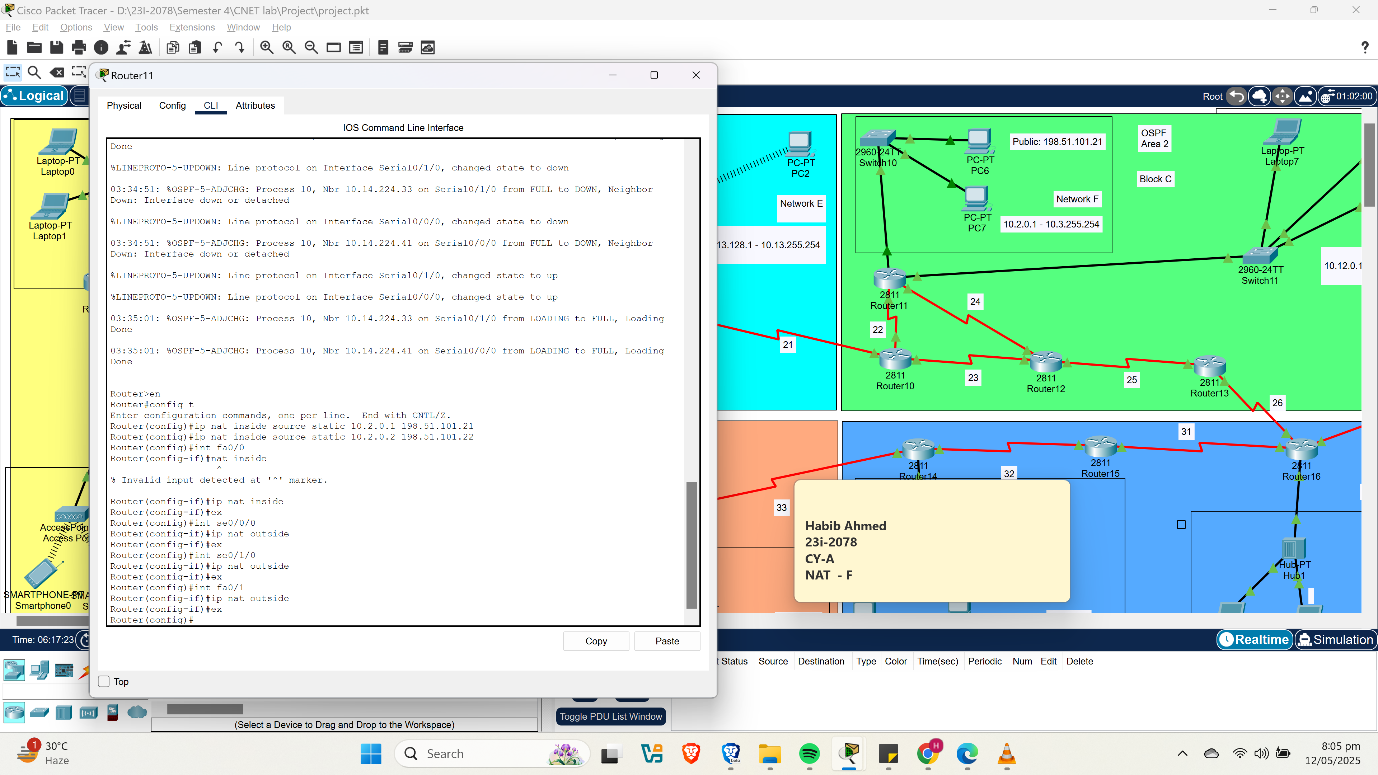


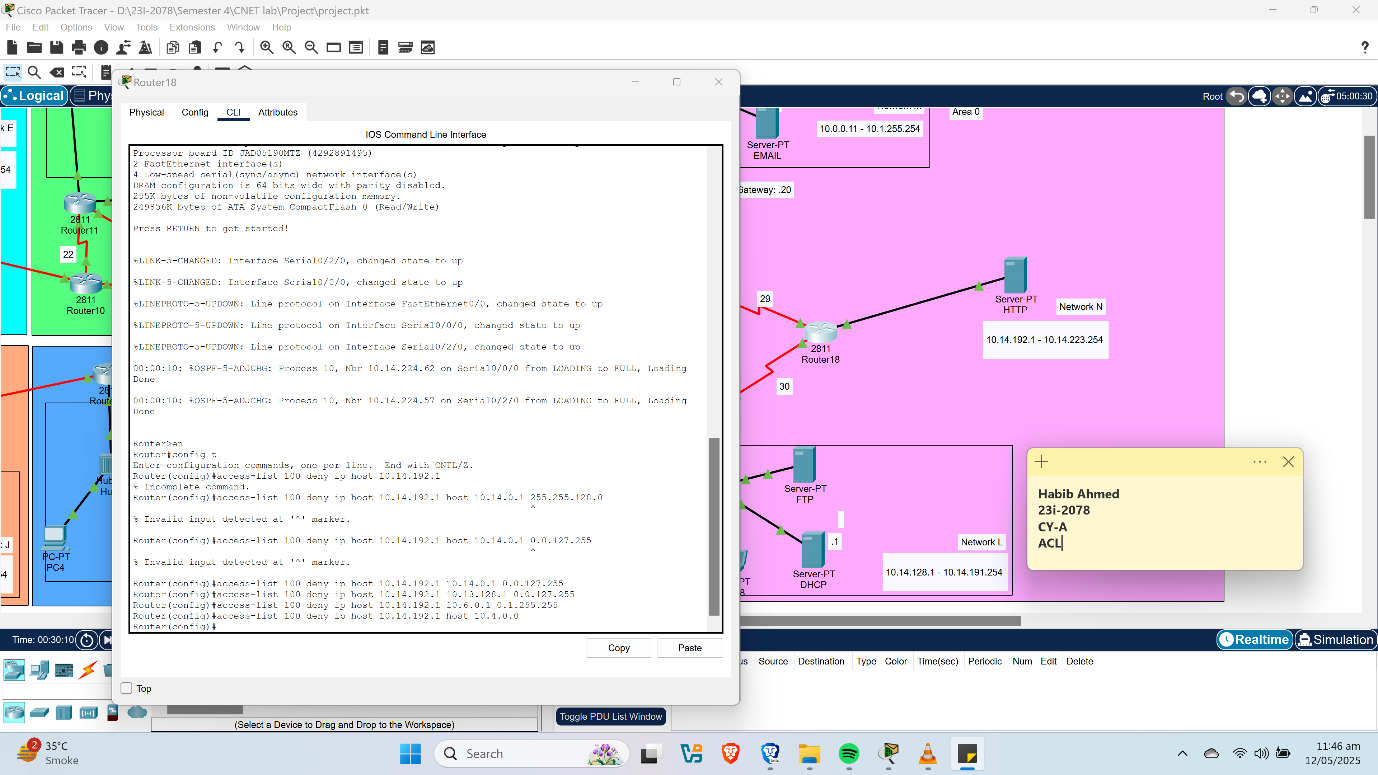
* DHCP pool output.



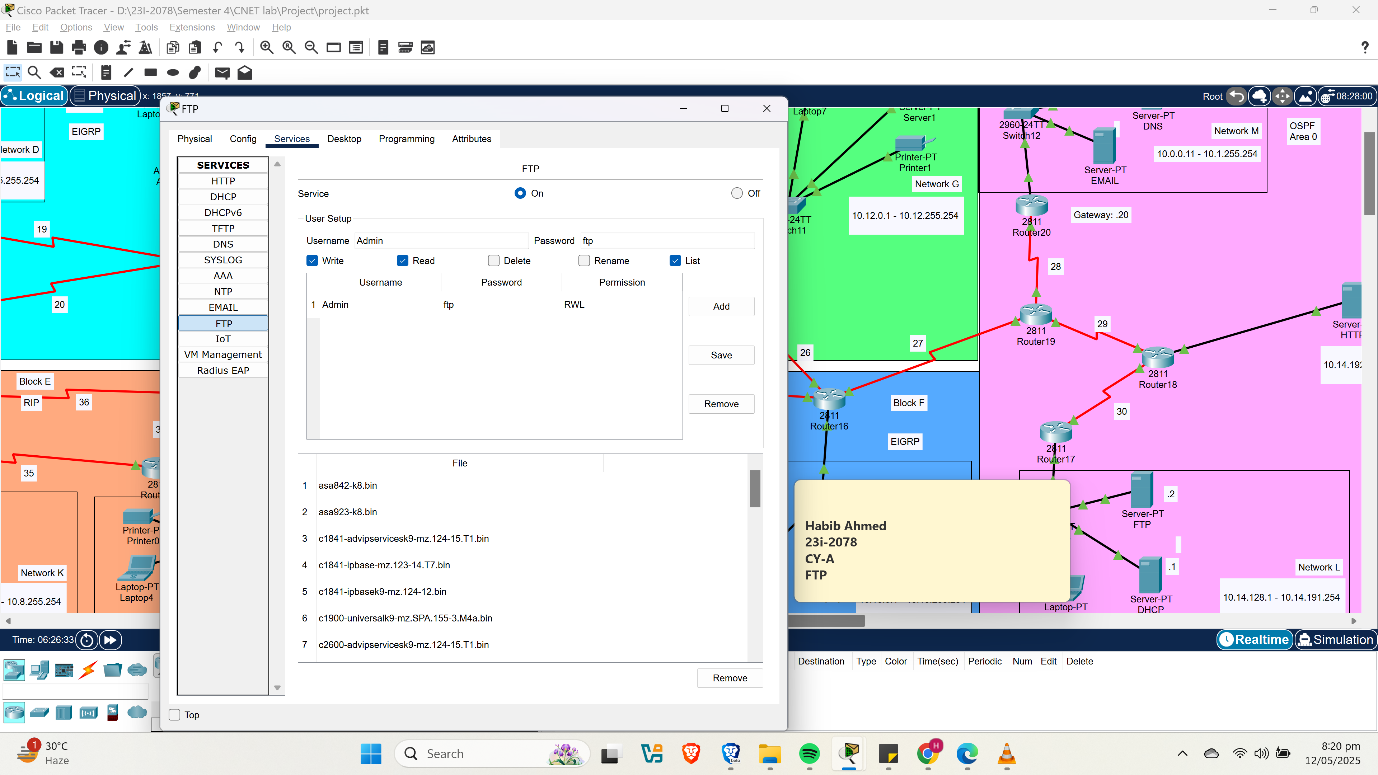
* NAT and ACL verification outputs.







* FTP client upload interface.



# **6. Conclusion**

This project demonstrated the planning, configuration, and deployment of a scalable and secure network using Cisco Packet Tracer. Key protocols and technologies including EIGRP, OSPF, RIP, DHCP, NAT, and ACLs were integrated in a functional topology. Access control, address translation, and other services were all configured and met the project’s requirements.