National University of Computer and Emerging Sciences
Islamabad Campus

CS3001

Computer Networks

Project

Design and Simulation of a Multi-Protocol(OSPF,EIGRP,RIP), Multiple kind of Servers ,ACL and NAT-Enabled Network Using Cisco Packet Tracer

Submitted by: Abdullah Noman
Roll number: 23i-2012
Date: 5/12/2025

Table of Contents

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.
- 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**: IP addresses were assigned to all router interfaces and devices as per subnetting plans.
4. **Routing Protocols**:
    - EIGRP configured in Block A and Block E.
    - OSPF Area 1 and 2 are configured in Blocks B and C.
    - RIP configured in Block G.
5. **Route Redistribution**: Applied between routers connecting different blocks (e.g., EIGRP-OSPF, OSPF-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 Router21 (connected to Network K).
    - Configured on Router10 (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**:
    - Mail Server in Block D allows email exchange between Network H and Network I.
    - FTP Server in Network G allows only hosts from Network G to upload files.
10. **Testing & Validation**:

- Verified IP addressing.
- Confirmed routing tables and redistribution.
- Checked ACL effectiveness.
- Validated DHCP, NAT translations, FTP and mail delivery.

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 /30 subnets (4 IPs) 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 A and E for its fast convergence and support for VLSM.
    - Configured using AS numbers and relevant networks.
- **OSPF (Open Shortest Path First):**
    - Used in Blocks B and C, with Area 1 and Area 2.
    - Hierarchical, link-state protocol suitable for larger domains.
- **RIP (Routing Information Protocol):**
    - Used in Block G.
    - Simple distance vector protocol with 15-hop limit.

3.3 DHCP Configuration

What is DHCP?
Dynamic Host Configuration Protocol (DHCP) automates the assignment of IP addresses to hosts.

Why use DHCP?

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

Where it is used?

- A centralized DHCP Server is placed in Block D.
- It serves hosts in Blocks A (EIGRP), B & C (OSPF), and G (RIP).

3.4 NAT Configuration

What is NAT?
Network Address Translation (NAT) converts private IP addresses into public IP addresses before packets are sent to the internet.

Why use NAT?

- Allows multiple private IP devices to access the internet using a single public IP.
- Enhances security by hiding internal IPs.

Where NAT is used in the project?

- **Router7 (connected to Network K)**: NAT is used to translate internal addresses for internet access.
- **Router11 (connected to Network F)**: Performs NAT for outbound traffic using public IP.

3.5 ACL Configuration

What are ACLs?
Access Control Lists (ACLs) control network traffic by filtering packets based on criteria like IP, protocol, or port.

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 for Network D.

3.6 Mail Server Configuration

Purpose: To allow communication via email.

Location: Block D

Configuration:

- Mail Server IP: 192.168.12.10
- Email clients on Network H and I.
- SMTP and IMAP protocols used.
- ACLs and firewall rules ensure only those networks can communicate with the mail server.

3.7 FTP Server Configuration

Purpose: To allow file uploads.

Location: Network G

Access Restricted to: Only devices in Network G.

Configuration:

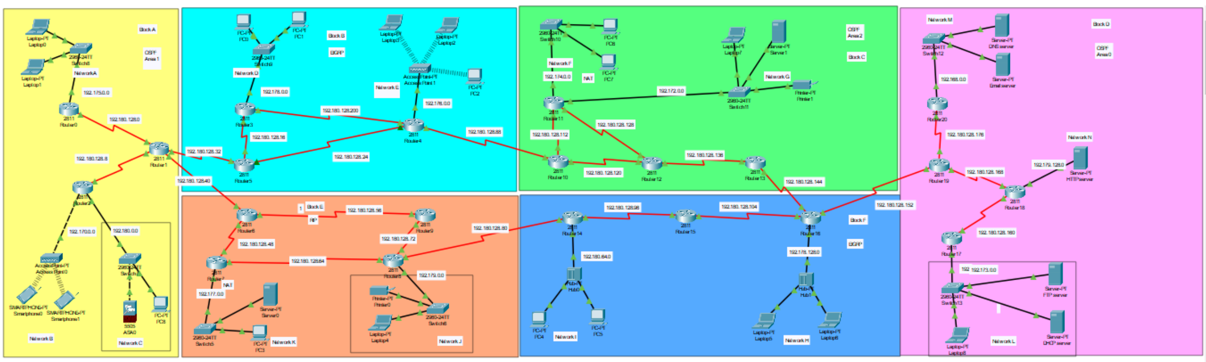
- FTP Server IP: 192.173.0.4
- Username/password set up for clients.
- ACL restricts access to the FTP server.

4. Observations and Results

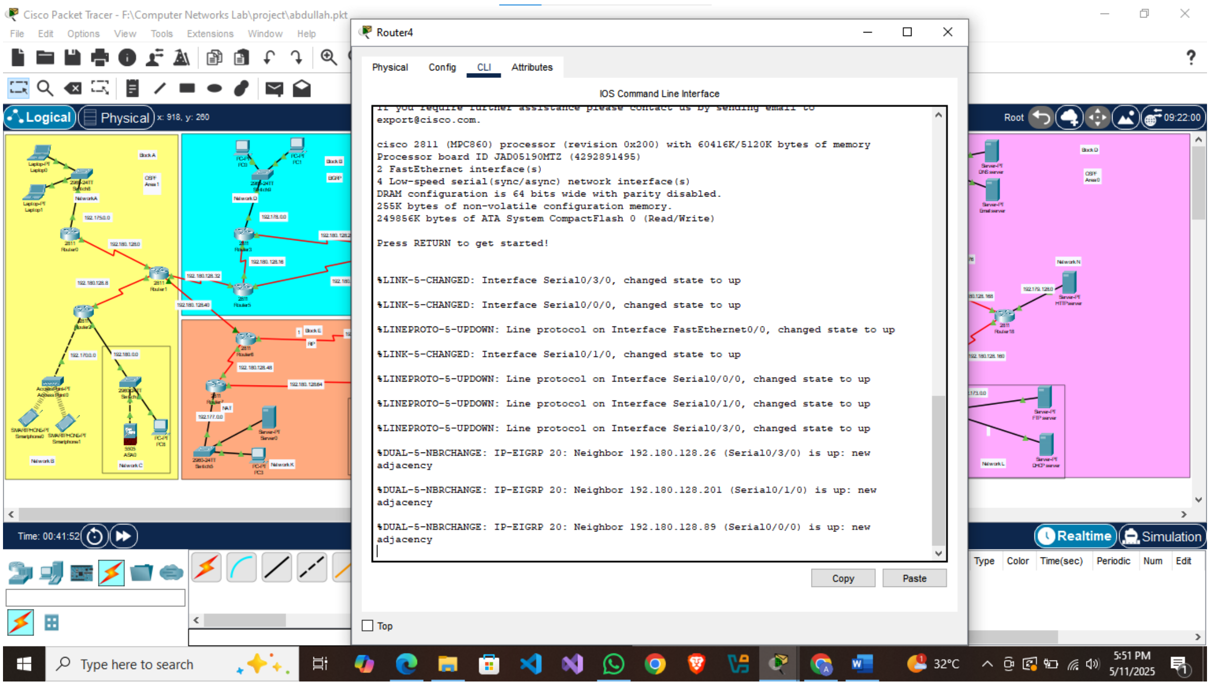
- All DHCP-configured hosts received IPs.
- Routing tables correctly propagated through redistribution.
- NAT translation verified using show ip nat translations.
- ACLs effectively blocked traffic from restricted hosts.
- Email services between Network H and I were successful.
- FTP upload from Network G was functional.

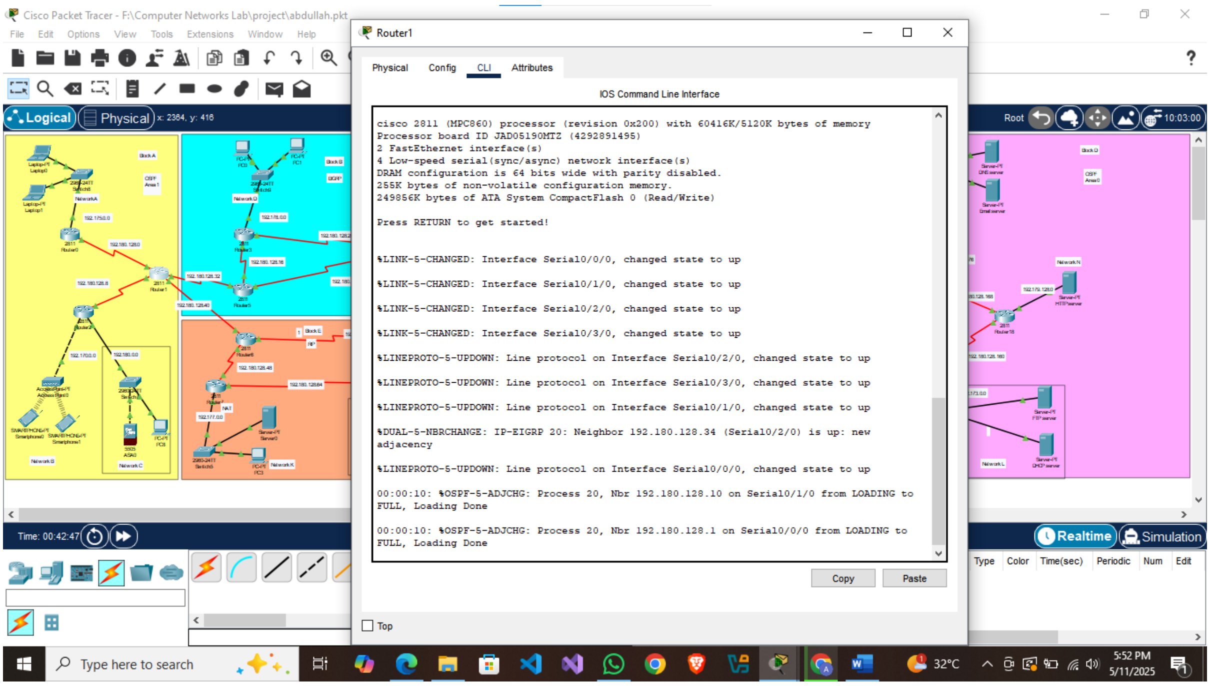
5. Screenshots

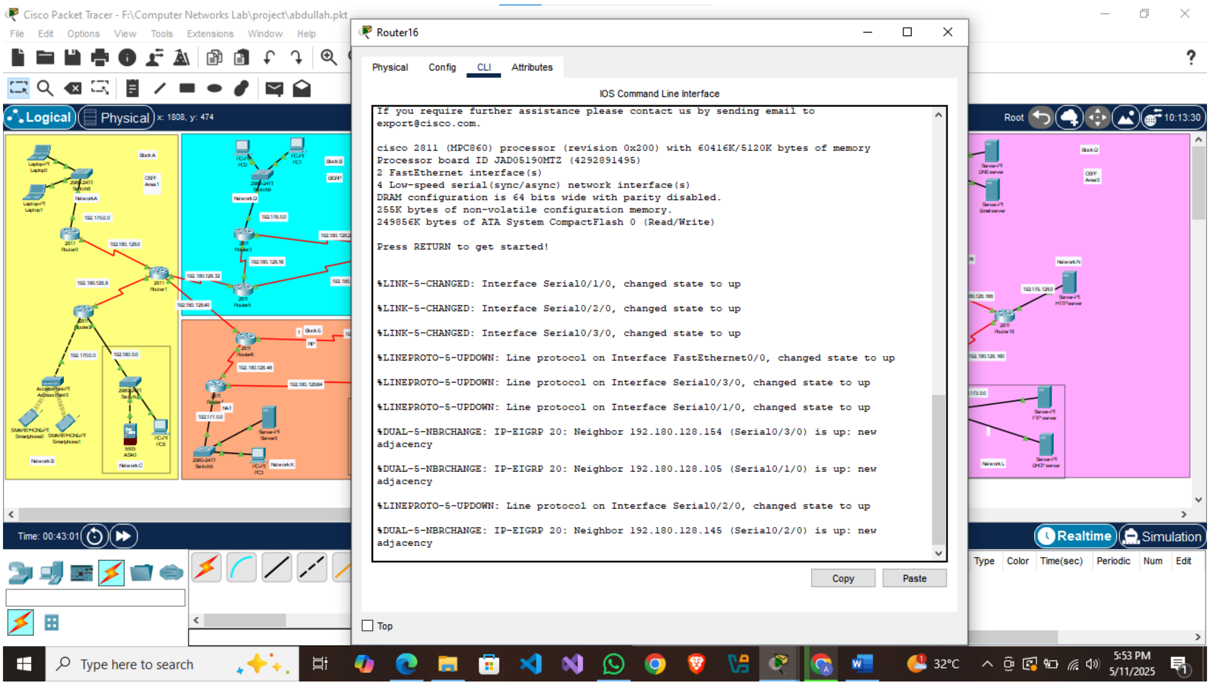
- Full topology diagram.



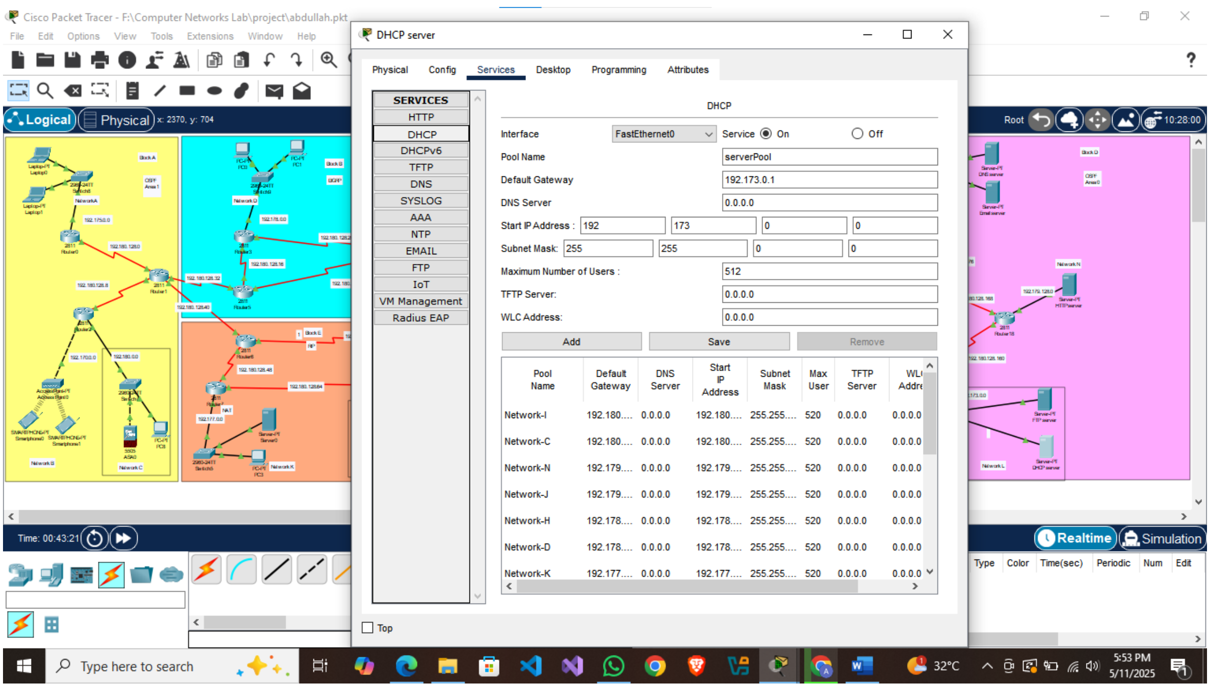
- Router and switch interface settings.



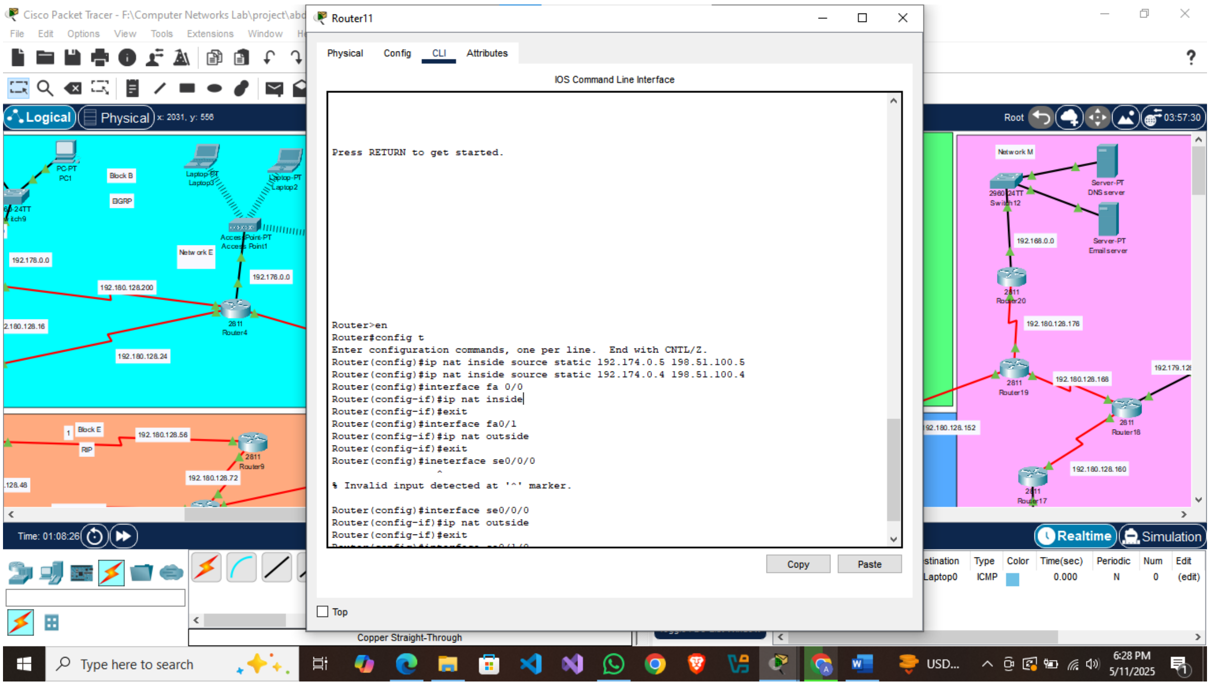


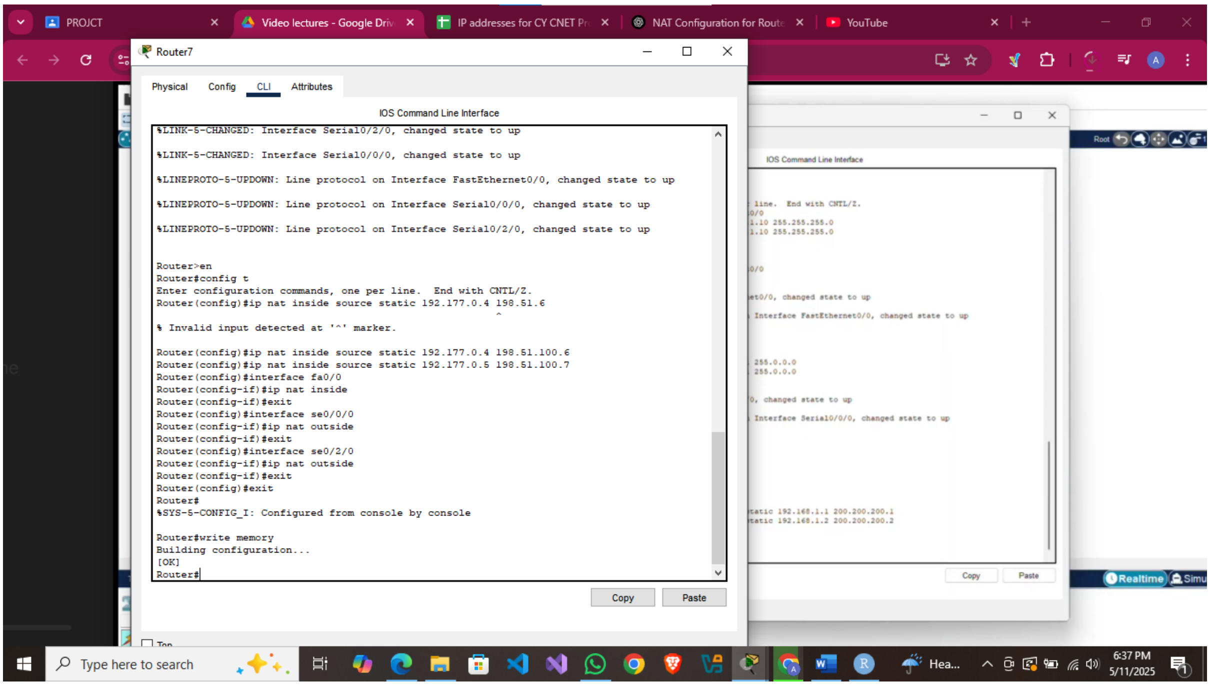


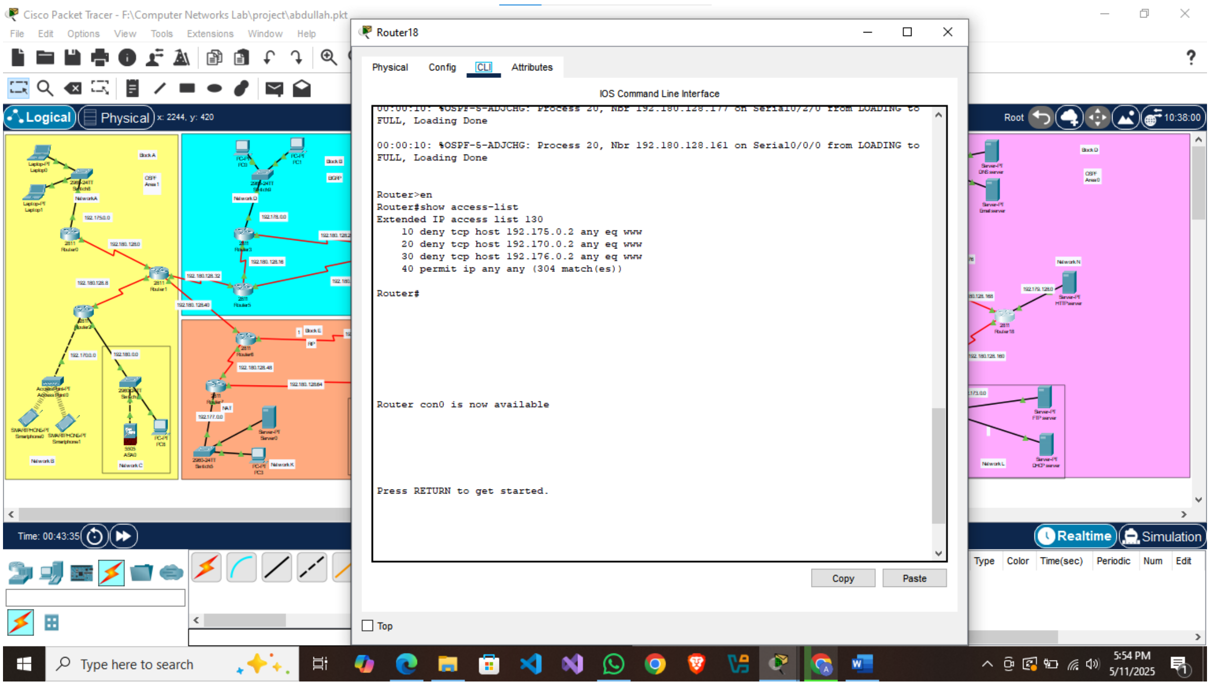
- DHCP pool output.



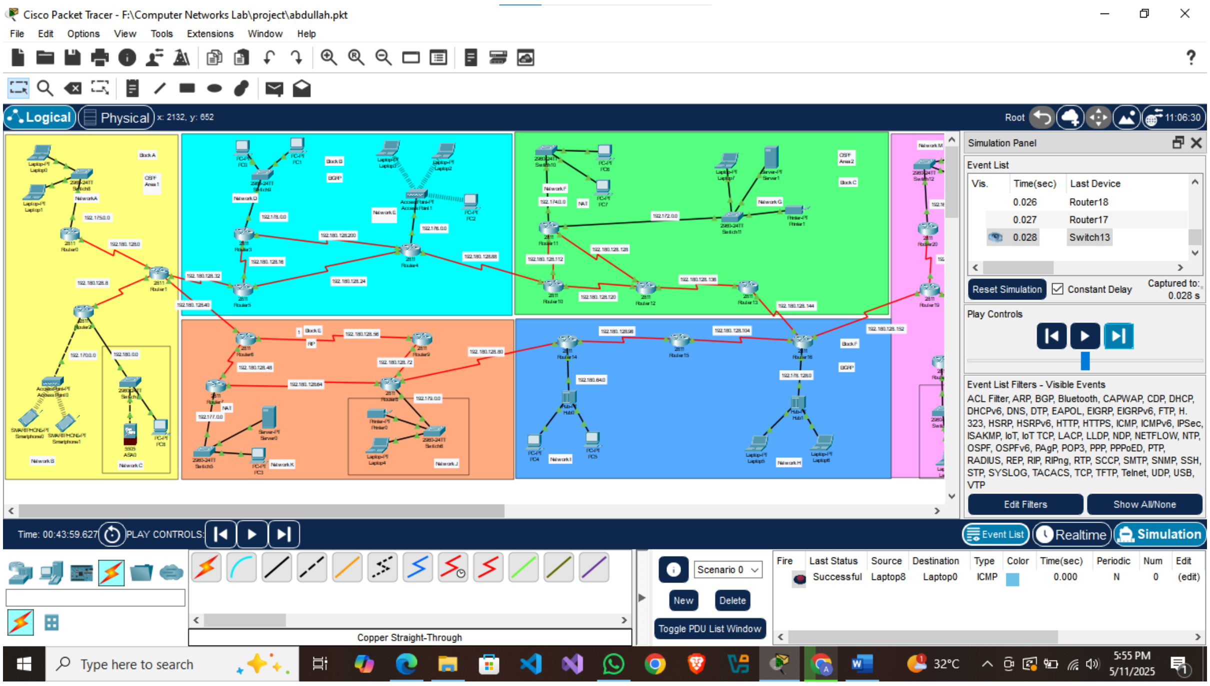
- NAT and ACL verification outputs.


Router11
Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started.
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip nat inside source static 192.174.0.5 198.51.100.5
Router(config)#ip nat inside source static 192.174.0.4 198.51.100.4
Router(config)#interface fa 0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface fa0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ineterface se0/0/0
% Invalid input detected at '^' marker.
Router(config)#interface se0/0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Copy
Paste
Top
Copper Straight-Through
Type here to search
6:28 PM
5/11/2025

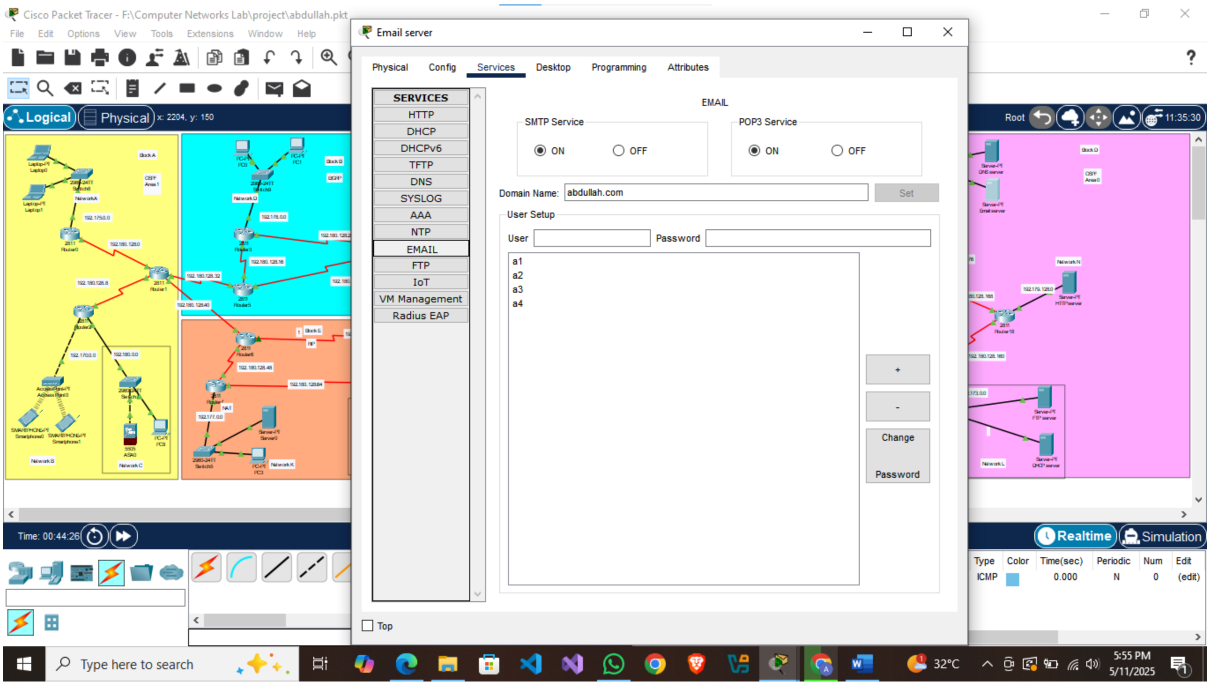

Router7
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface Serial0/2/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip nat inside source static 192.177.0.4 198.51.6
% Invalid input detected at '^' marker.
Router(config)#ip nat inside source static 192.177.0.4 198.51.100.6
Router(config)#ip nat inside source static 192.177.0.5 198.51.100.7
Router(config)#interface fa0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface se0/0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#interface se0/2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#write memory
Building configuration...
[OK]
Router#
Copy
Paste
Type here to search
6:37 PM
5/11/2025



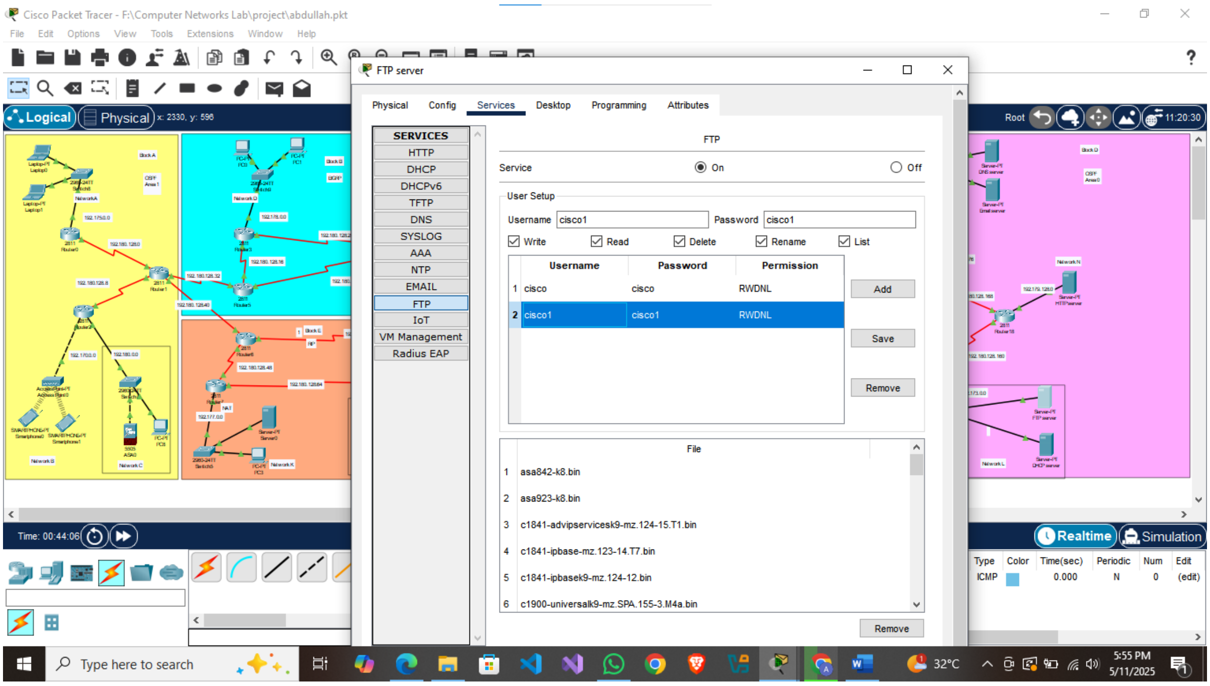
- Ping results for testing connectivity and restrictions.



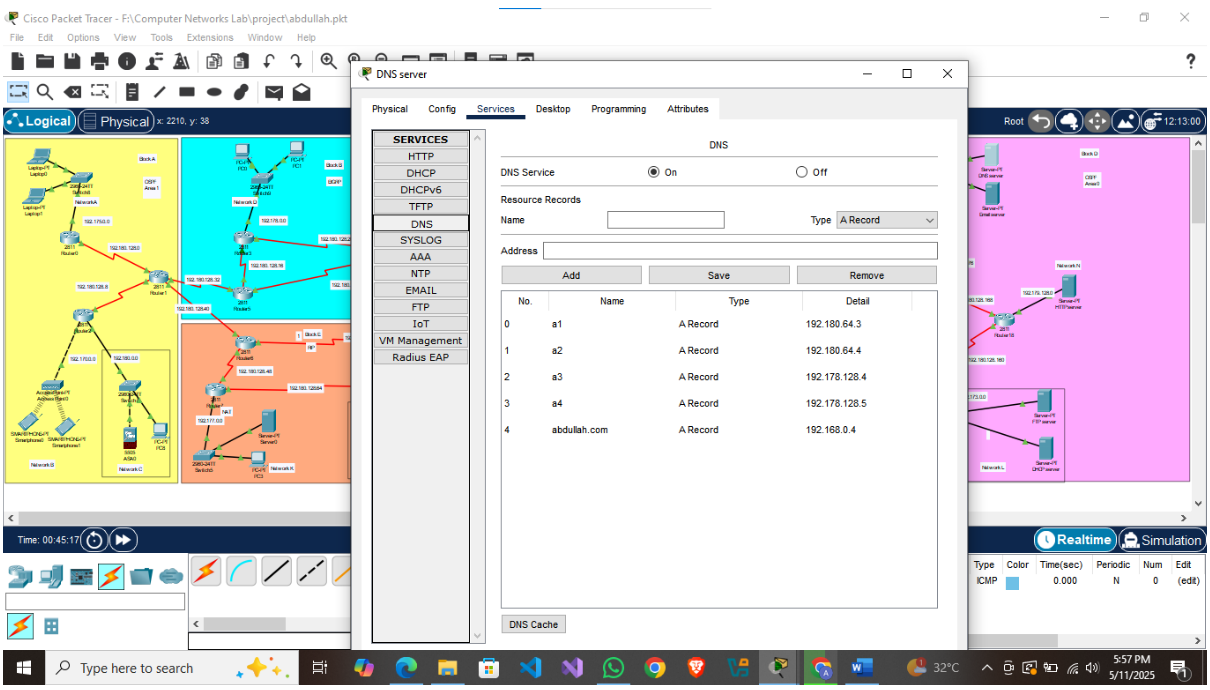
- Mail client send/receive window.



- FTP client upload interface.



- DNS interface



6. Conclusion

This project successfully 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 service configurations were all verified and met the project's requirements.