Computer Networks Semester Project

Submitted by:

Mahrukh Wahidi
Roll Number: 21i-1765

Instructor:

Mr. Atif Khurshid

December 7, 2024

Abstract

This report presents the design, implementation, and configuration of a comprehensive computer network for a semester project in the field of Computer Networks. The project involves the creation of a scalable and efficient topology, assignment of IP addresses using Variable Length Subnet Masking (VLSM), and the configuration of routing protocols such as RIP, OSPF, and EIGRP to enable seamless communication across multiple networks. Advanced network functionalities such as Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP) were implemented to ensure efficient IP address management and secure internet access. Access Control Lists (ACLs) were employed to enhance network security by restricting access to sensitive resources, such as the web server. Additionally, an SMTP server was configured to enable email communication among devices in the network, demonstrating the integration of application-level services. The project showcases a practical understanding of network design, configuration, and testing while adhering to best practices for scalability, security, and efficiency. Each component was tested and verified to ensure reliability and functionality, providing a robust solution for real-world networking challenges.

Contents

Chapter 1

Topology Creation

Abstract

.

1.1 Overview

The topology for this project has been meticulously designed to meet the requirements outlined in the project objectives. It includes all necessary components, such as routers, switches, and hosts, interconnected to enable seamless communication and effective routing. Below is the topology created for the project.

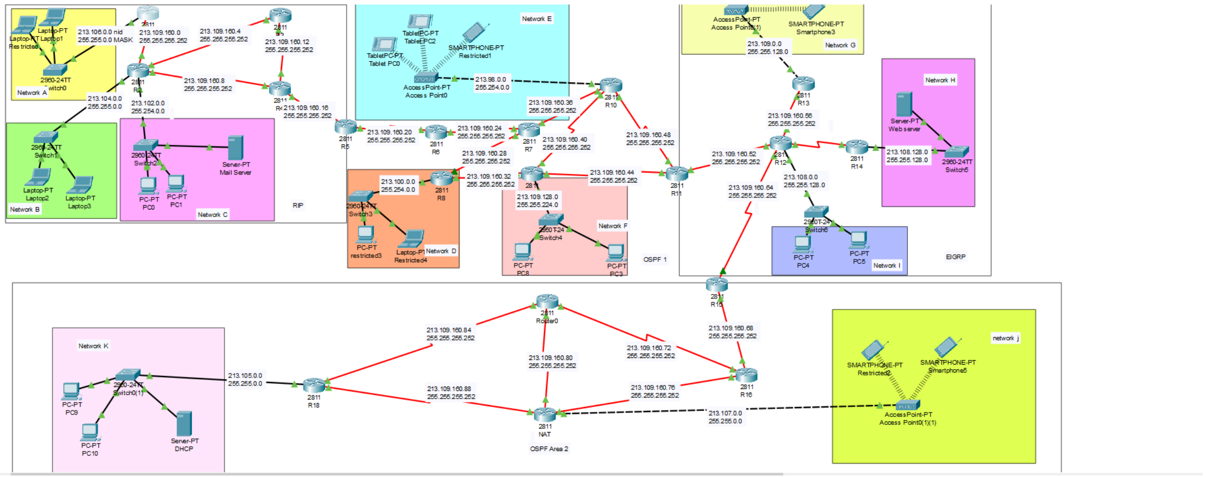


Figure 1.1: Network Topology

Figure 2.1 shows the network topology designed for this project. Each device and its connections have been configured according to the project requirements.

1.2 Components

The topology includes:

- Routers for inter-network communication.

- Switches for connecting hosts and managing local networks.
- Hosts to simulate end-user devices.
- A DHCP server for dynamic IP assignment.
- NAT for translating private IP addresses to public IPs.
- An SMTP server for email communication.

1.3 Tools Used

To create and configure the network topology, the following tool was used:

- **Cisco Packet Tracer:** A network simulation tool used for designing and testing the topology.

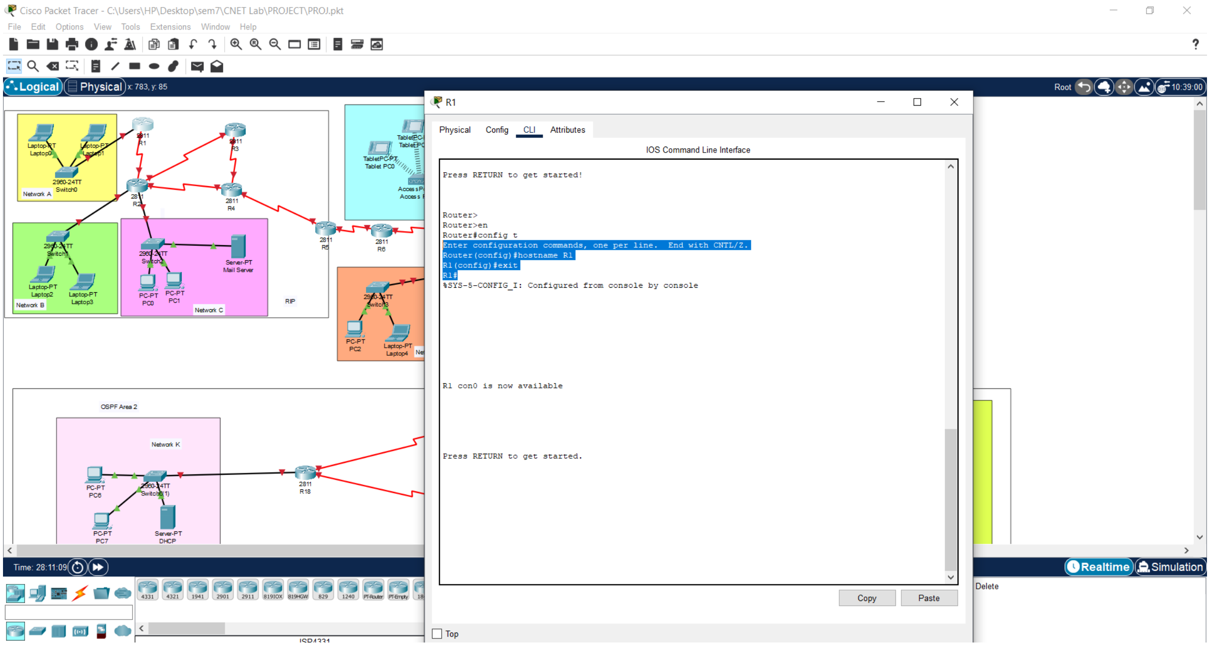
Chapter 2

IP Addressing

This chapter discusses the assignment of IP addresses using VLSM and subnet mask calculations to ensure efficient use of the IP address space. Each device and interface is assigned a proper IP address for seamless communication.

2.1 Hostname Configuration

For simplicity and ease of identification, the hostname of each router was changed to reflect its role in the network. This was achieved using the following commands in the router configuration mode.
Below is an example of how the hostname was changed to ”R1”:


Cisco Packet Tracer - C:\Users\HP\Desktop\sem7\CNET Lab\PROJECT\PROJ.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Copy
Paste
Top
Realtime
Simulation

```
Press RETURN to get started!



Router>
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console









R1 con0 is now available






Press RETURN to get started.
```

Figure 2.1: Hostname Configuration

Similarly, the router responsible for NAT configuration was renamed to ”NAT” using the following commands:
Changing the hostname simplifies the identification of routers in both the CLI and the network topology.

2.2 Adherence to VLSM and Subnet Mask Calculations

To ensure efficient use of IP addresses, I used private IP addresses for VLSM calculations. The calculations were performed manually and verified with the help of [SubnettingPractice.com](https://subnettingpractice.com/vlsm.html). This allowed the proper allocation of IP addresses to each subnet and ensured optimal resource utilization.

Below is the table summarizing the calculated IP addresses, subnets, and related information:

Name	Hosts Needed	Hosts Available	Unused Hosts	Network Address	Slash	Mask
Network E	96890	131070	34180	213.98.0.0	/15	255.254.0.
Network D	85789	131070	45281	213.100.0.0	/15	255.254.0.
Network C	74678	131070	56392	213.102.0.0	/15	255.254.0.
Network B	63567	65534	1967	213.104.0.0	/16	255.255.0.
Network K	53456	65534	12078	213.105.0.0	/16	255.255.0.
Network A	52456	65534	13078	213.106.0.0	/16	255.255.0.
Network J	42345	65534	23189	213.107.0.0	/16	255.255.0.
Network I	31234	32766	1532	213.108.0.0	/17	255.255.128
Network H	20123	32766	12643	213.108.128.0	/17	255.255.128
Network G	19012	32766	13754	213.109.0.0	/17	255.255.128
Network F	7901	8190	289	213.109.128.0	/19	255.255.224

Table 2.1: VLSM and Subnet Mask Calculations

I've used 4 ip address for each router.
This table ensures all networks have been assigned the proper IP range and subnet mask while minimizing wasted IP space.

2.3 Static IP Allocation and Interface Configuration

In the initial phase of network setup, I configured static IP addresses on each router interface. This ensured precise control over IP allocation and allowed for testing the basic functionality of the network before implementing other configurations. Each interface was assigned an appropriate IP address and subnet mask to establish connectivity.

2.3.1 Steps for Static IP Configuration

The static IP configuration was performed on all router interfaces using the following steps:

1. Access the router's configuration mode.
2. Enter the interface configuration for each required port (e.g., serial or Ethernet interfaces).
3. Assign the IP address and subnet mask for the interface.
4. Enable the interface using the 'no shutdown' command to ensure it is operational.

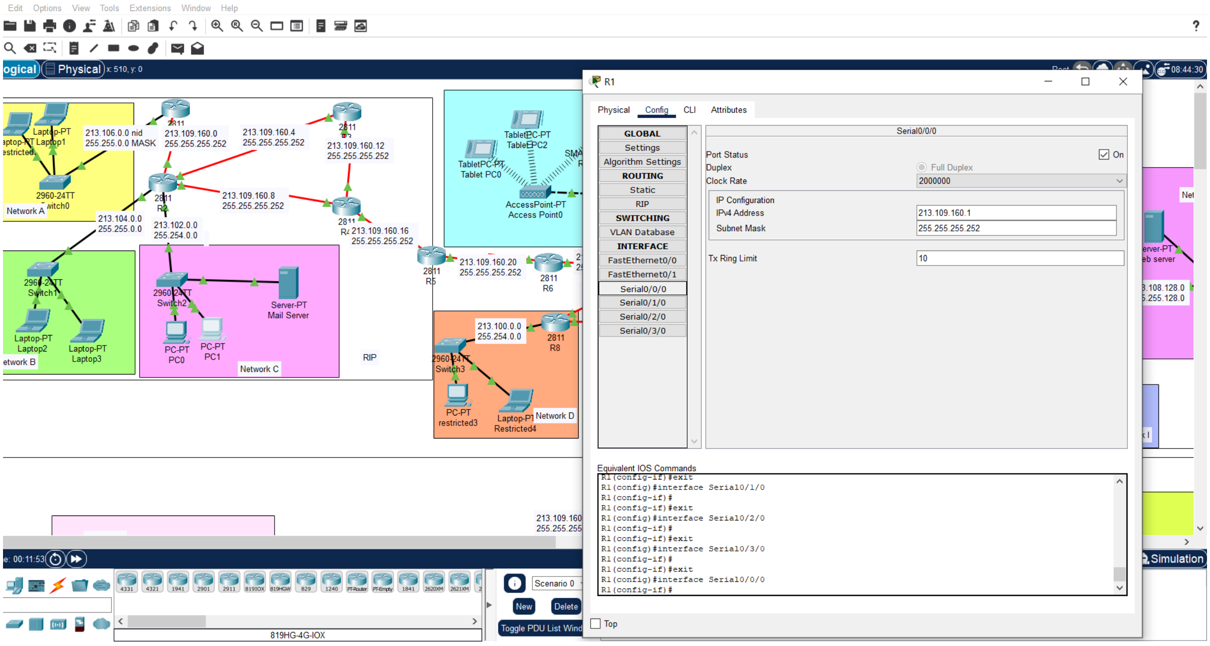
Below is an example of how a static IP address was configured for a router's interface:

```
Router> enable
Router# configure terminal
Router(config)# interface serial0/0/0
Router(config-if)# ip address 213.109.160.1 255.255.255.252
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
Router#
```

2.3.2 Configured Interfaces

Each router in the network was configured with static IP addresses for its interfaces. The IP allocation followed the VLSM plan to ensure efficient utilization of the address space. The configured interfaces allowed seamless communication between routers, ensuring all connections in the topology were functional.

The figure below provides an example of static IP allocation and interface configuration on a router:



Serial0/0/0

Port Status ☑ On
Duplex ○ Full Duplex
Clock Rate 2000000

IP Configuration
IPv4 Address 213.109.160.1
Subnet Mask 255.255.255.252

Tx Ring Limit 10

Equivalent IOS Commands

```
R1(config-if)#exit
R1(config)#interface Serial0/1/0
R1(config-if)#
R1(config-if)#exit
R1(config)#interface Serial0/2/0
R1(config-if)#
R1(config-if)#exit
R1(config)#interface Serial0/3/0
R1(config-if)#
R1(config-if)#exit
R1(config)#interface Serial0/0/0
R1(config-if)#
```

□ Top

Figure 2.2: Example of Static IP Allocation and Interface Configuration

Figure 2.2 demonstrates the configuration process of assigning a static IP address and subnet mask to a router interface.

Chapter 3

Routing Protocol Configuration

This chapter outlines the configuration of various routing protocols for different networks to ensure seamless communication between devices. The protocols used are:

- RIP for Networks A, B, and C.
- OSPF1 for Networks D, E, and F.
- EIGRP for Networks G, H, and I.
- OSPF2 for Networks J and K.

Each protocol is configured with specific commands tailored to the requirements of the corresponding network.

3.1 RIP Configuration for Networks A, B, and C

Routing Information Protocol (RIP) was configured for Networks A, B, and C to facilitate dynamic routing. RIP was chosen due to its simplicity and ability to handle smaller networks effectively. Below are the steps and commands used:

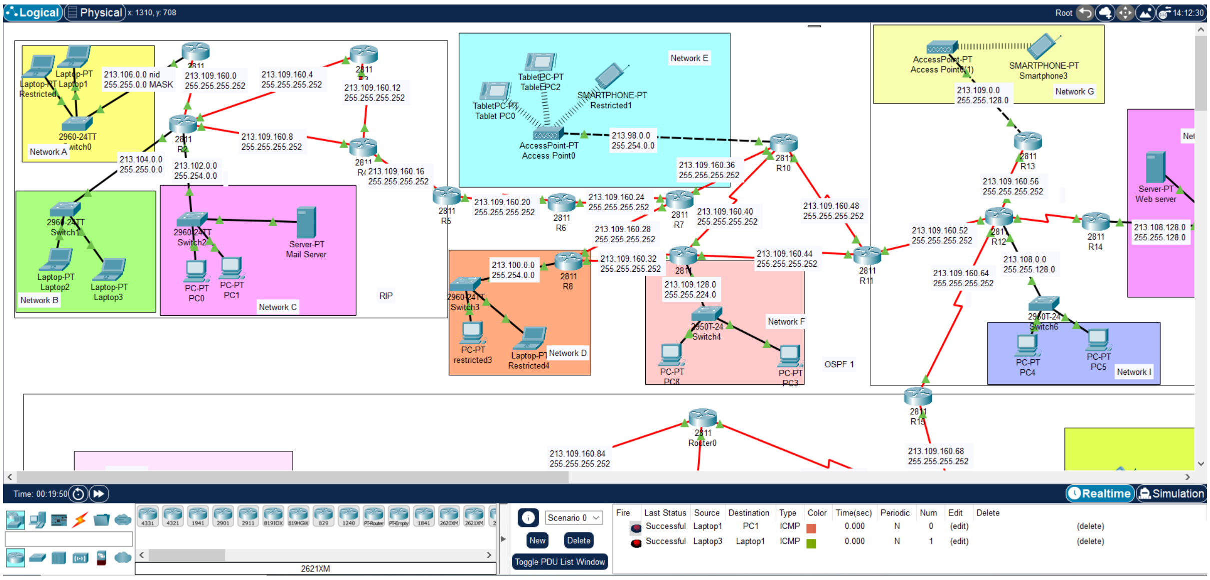
3.1.1 Commands for RIP Configuration

The following commands were used to configure RIP on the routers:

```
Router> enable
Router# configure terminal
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 213.104.0.0
Router(config-router)# network 213.102.0.0
Router(config-router)# network 213.100.0.0
Router(config-router)# exit
Router(config)# exit
Router#
```

These commands enable RIP version 2 and specify the networks that need to exchange routing information dynamically.

PDU Success in RIP



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	Laptop1	PC1	ICMP	🟥	0.000	N	0	(edit)	(delete)
●	Successful	Laptop3	Laptop1	ICMP	🟩	0.000	N	1	(edit)	(delete)

Figure 3.1: PDU Success in RIP

Figure ?? demonstrates the successful PDU delivery using RIP routing between devices in Networks A, B, and C.

3.2 OSPF1 Configuration for Networks D, E, and F

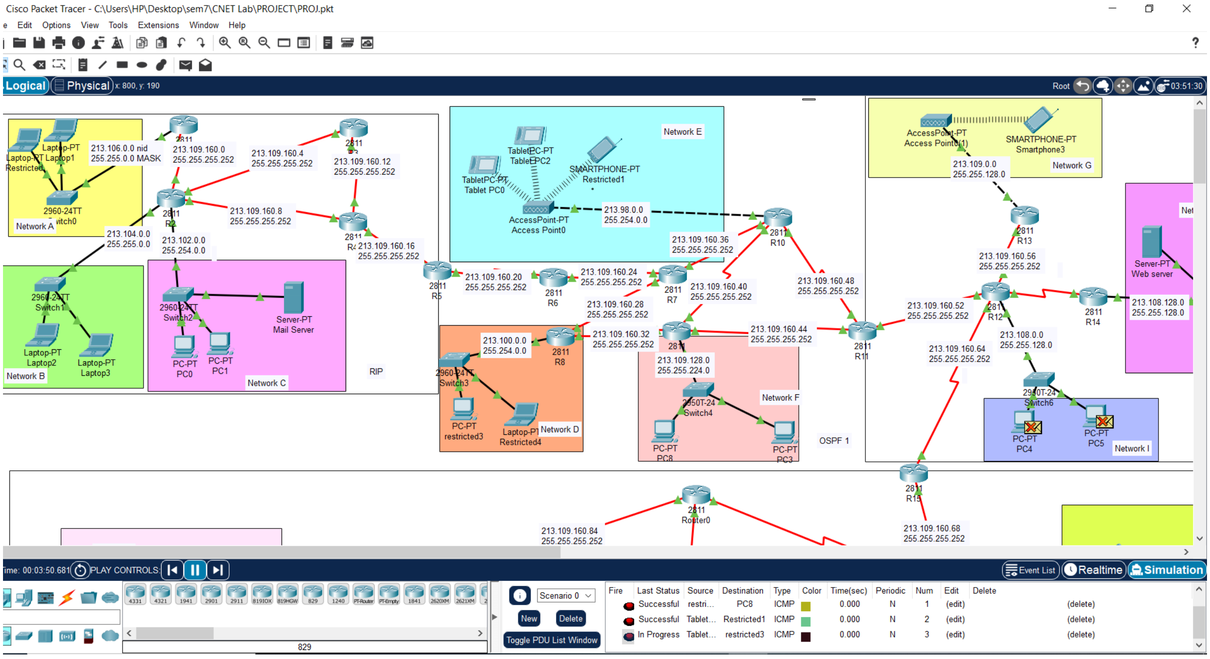
Open Shortest Path First (OSPF) was chosen for Networks D, E, and F due to its efficiency and scalability. OSPF Area 1 was created for these networks.

3.2.1 Commands for OSPF1 Configuration

```
Router> enable
Router# configure terminal
Router(config)# router ospf 1
Router(config-router)# network 213.100.0.0 0.0.1.255 area 1
Router(config-router)# network 213.98.0.0 0.1.255.255 area 1
Router(config-router)# network 213.109.128.0 0.0.31.255 area 1
Router(config-router)# exit
Router(config)# exit
Router#
```

PDU Success in OSPF Area 1

The above commands assign Networks D, E, and F to OSPF Area 1.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	restri...	PC8	ICMP	🟨	0.000	N	1	(edit)	(delete)
●	Successful	Tablet...	Restricted1	ICMP	🟩	0.000	N	2	(edit)	(delete)
●	In Progress	Tablet...	restricted3	ICMP	■	0.000	N	3	(edit)	(delete)

Figure 3.2: PDU Success in OSPF Area 1

3.3 EIGRP Configuration for Networks G, H, and I

Enhanced Interior Gateway Routing Protocol (EIGRP) was configured for Networks G, H, and I due to its advanced features and fast convergence.

3.3.1 Commands for EIGRP Configuration

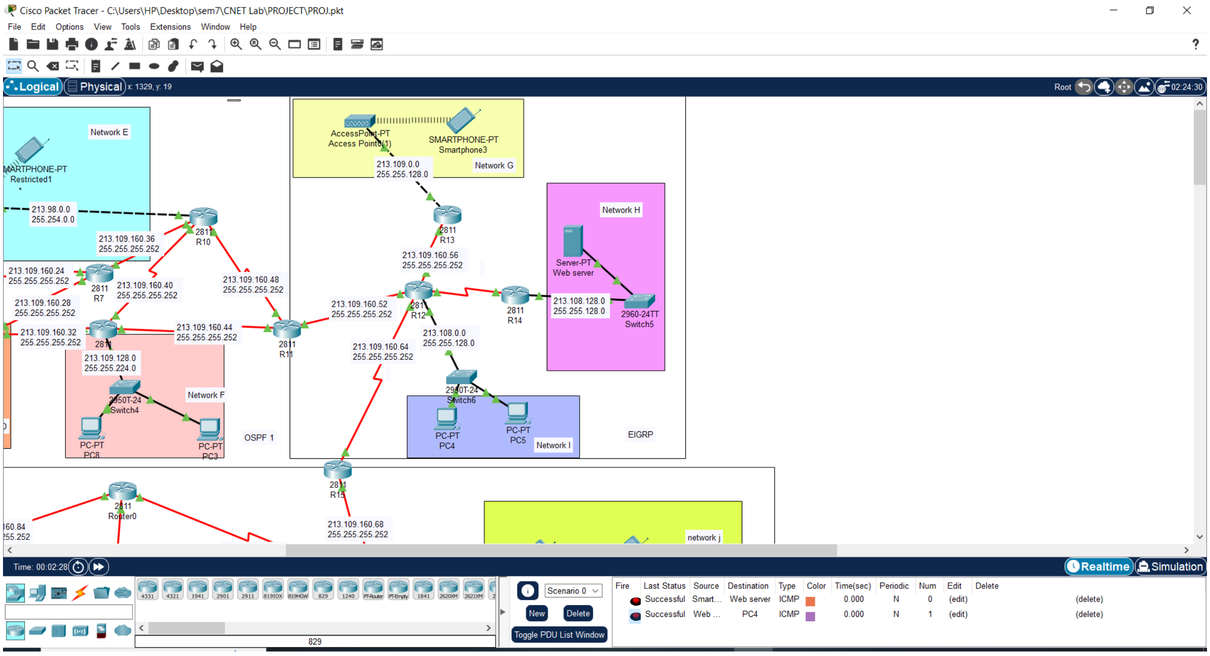
```
Router> enable
Router# configure terminal
Router(config)# router eigrp 100
Router(config-router)# network 213.109.0.0 0.0.127.255
Router(config-router)# network 213.108.128.0 0.0.127.255
Router(config-router)# network 213.108.0.0 0.0.127.255
Router(config-router)# no auto-summary
Router(config-router)# exit
Router(config)# exit
Router#
```

PDU Success in EIGRP

These commands enable EIGRP with an Autonomous System (AS) number of 100 and include the networks for dynamic routing.

3.4 OSPF2 Configuration for Networks J and K

Open Shortest Path First (OSPF) was also used for Networks J and K under a different area, OSPF Area 2.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	Smart...	Web server	ICMP	🟧	0.000	N	0	(edit)	(delete)
●	Successful	Web ...	PC4	ICMP	🟪	0.000	N	1	(edit)	(delete)

Figure 3.3: PDU Success in EIGRP

3.4.1 Commands for OSPF2 Configuration

```
Router> enable
Router# configure terminal
Router(config)# router ospf 2
Router(config-router)# network 213.107.0.0 0.0.255.255 area 2
Router(config-router)# network 213.105.0.0 0.0.255.255 area 2
Router(config-router)# exit
Router(config)# exit
Router#
```

PDU Success in OSPF Area 2

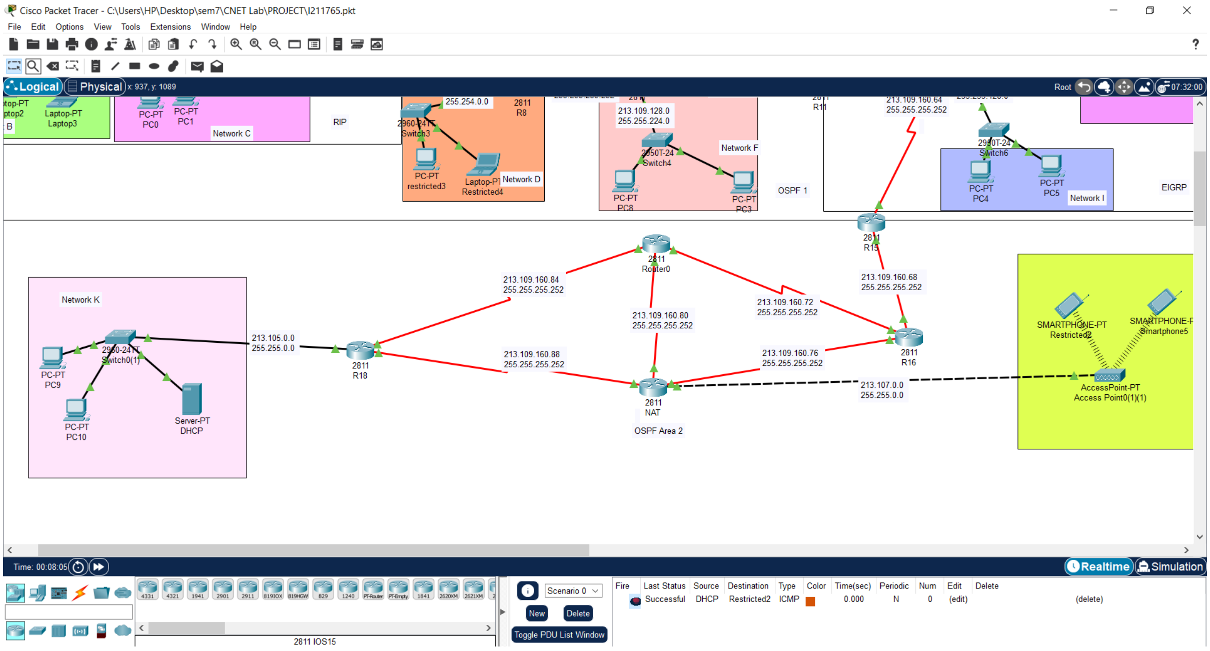
The above commands configure OSPF Area 2 and include Networks J and K.

3.5 Redistribution Between Routing Protocols

To enable communication between different routing protocol domains, redistribution was implemented on specific routers that connect these domains. Redistribution allows routes learned from one protocol to be advertised into another, ensuring seamless communication across the entire network.

In this topology, redistribution was configured on the following routers:

- **R5:** Redistribution between EIGRP and RIP.
- **R11:** Redistribution between OSPF Area 1 and OSPF Area 2.
- **R15:** Redistribution between OSPF Area 2 and EIGRP.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	DHCP	Restricted2	ICMP	🟧	0.000	N	0	(edit)	(delete)

Figure 3.4: PDU Success in OSPF Area 2

3.5.1 Redistribution Between EIGRP and OSPF

To enable redistribution between EIGRP and OSPF, the following commands were used on the router responsible for connecting the two protocols:

```
Router> enable
Router# configure terminal
Router(config)# router eigrp 10
Router(config-router)# redistribute ospf 10 metric 1000 1 255 1 1500
Router(config-router)# router ospf 10
Router(config-router)# redistribute eigrp 10 subnets
```

3.5.2 Redistribution Between RIP and OSPF

For redistribution between RIP and OSPF, the following commands were executed:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 10
Router(config-router)# redistribute rip subnets
Router(config-router)# router rip
Router(config-router)# version 2
Router(config-router)# redistribute ospf 10 metric 2
```

3.5.3 Topology Overview with Redistribution

The figure below illustrates the topology with the redistribution points highlighted: *Figure 3.5 highlights the routers (R5, R11, and R15) where redistribution between different routing protocols was implemented.*

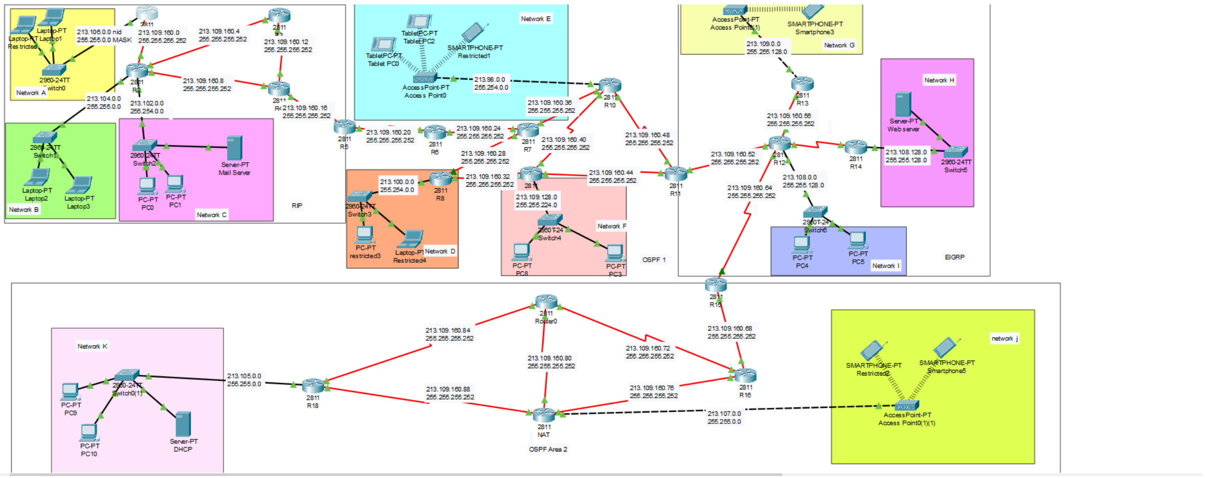


Figure 3.5: Network Topology with Redistribution Points on R5, R11, and R15

The configured redistribution ensures seamless communication between the different routing protocol blocks, enabling devices in all networks to communicate effectively.

Chapter 4

DHCP Server Configuration

4.1 DHCP Configuration in Network K

The DHCP server was configured in Network K to dynamically assign IP addresses to devices within its pool. The configuration included specifying the default gateway, subnet mask, and a range of IP addresses for allocation.

4.1.1 Steps for DHCP Server Configuration

The following steps were performed to configure the DHCP server:

1. Accessed the DHCP server device in Network K.
2. Enabled the DHCP service from the server settings.
3. Defined the IP address pool, subnet mask, and default gateway for the network.
4. Saved the configuration to ensure the DHCP server was ready to assign IP addresses to devices dynamically.

4.1.2 DHCP Server Configuration Screenshot

The screenshot below shows the configuration of the DHCP server in Network K, including the IP address pool and related parameters.

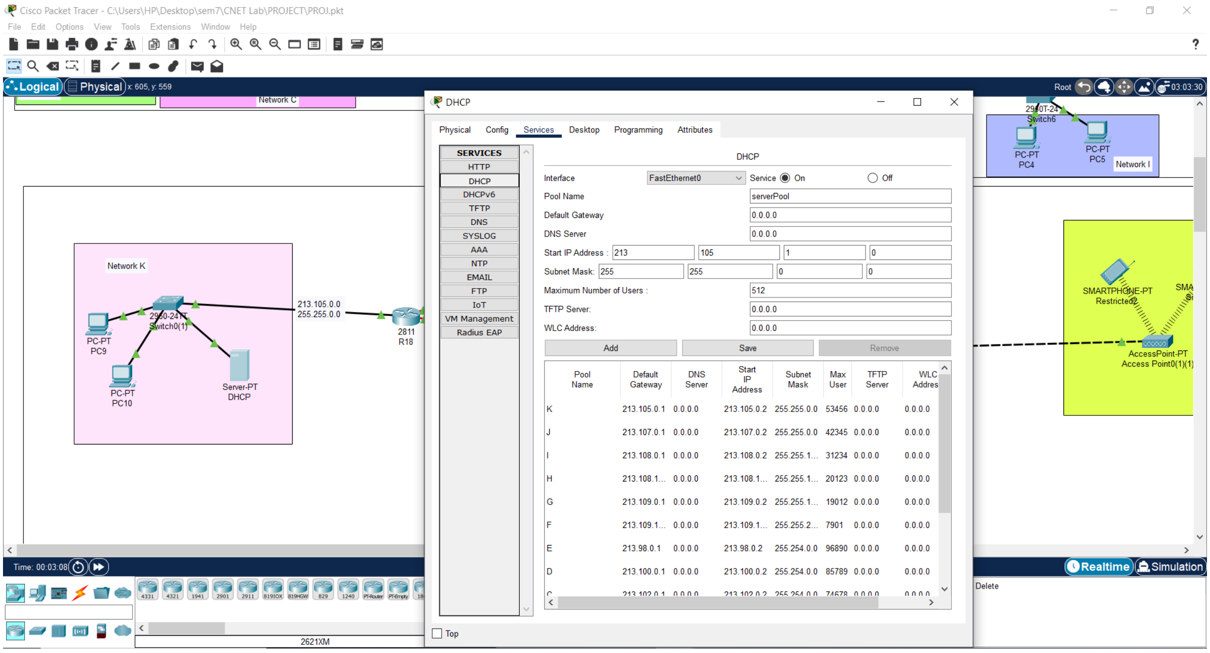
4.2 Verification of DHCP Configuration

To verify the DHCP configuration, devices in the network, such as smartphones and PCs, were configured to obtain IP addresses dynamically. Successful dynamic IP allocation confirmed the correctness of the DHCP server configuration.

4.2.1 Smartphone with Dynamically Assigned IP

The following figure demonstrates a smartphone in the network receiving an IP address dynamically from the DHCP server:

By configuring DHCP on the server in Network K, dynamic IP allocation was successfully implemented, simplifying the management of IP addresses across the network.



DHCP

Physical | Config | Services | Desktop | Programming | Attributes

SERVICES: HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, FTP, IoT, VM Management, Radius EAP

DHCP

Interface: FastEthernet0 Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address : 213 | 105 | 1 | 0

Subnet Mask: 255 | 255 | 0 | 0

Maximum Number of Users : 512

TFTP Server: 0.0.0.0

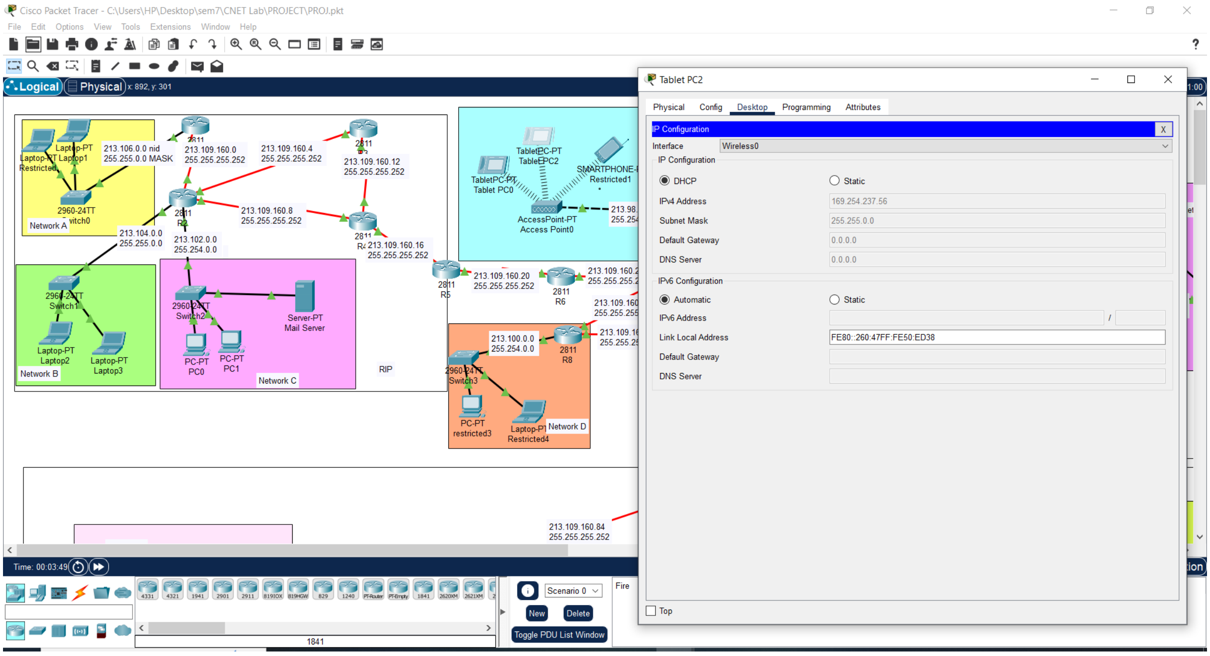
WLC Address: 0.0.0.0

Add | Save | Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Addres
K	213.105.0.1	0.0.0.0	213.105.0.2	255.255.0.0	53456	0.0.0.0	0.0.0.0
J	213.107.0.1	0.0.0.0	213.107.0.2	255.255.0.0	42345	0.0.0.0	0.0.0.0
I	213.108.0.1	0.0.0.0	213.108.0.2	255.255.1...	31234	0.0.0.0	0.0.0.0
H	213.108.1...	0.0.0.0	213.108.1...	255.255.1...	20123	0.0.0.0	0.0.0.0
G	213.109.0.1	0.0.0.0	213.109.0.2	255.255.1...	19012	0.0.0.0	0.0.0.0
F	213.109.1...	0.0.0.0	213.109.1...	255.255.2...	7901	0.0.0.0	0.0.0.0
E	213.98.0.1	0.0.0.0	213.98.0.2	255.254.0.0	96890	0.0.0.0	0.0.0.0
D	213.100.0.1	0.0.0.0	213.100.0.2	255.254.0.0	85789	0.0.0.0	0.0.0.0
C	213.102.0.1	0.0.0.0	213.102.0.2	255.254.0.0	74678	0.0.0.0	0.0.0.0

□ Top

Figure 4.1: DHCP Server Configuration in Network K



Tablet PC2

Physical | Config | Desktop | Programming | Attributes

IP Configuration

Interface: Wireless0

IP Configuration

● DHCP ○ Static

IPv4 Address: 169.254.237.56

Subnet Mask: 255.255.0.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

● Automatic ○ Static

IPv6 Address: /

Link Local Address: FE80::260:47FF:FE50:ED38

Default Gateway:

DNS Server:

□ Top

Figure 4.2: Smartphone with Dynamically Assigned IP Address

Chapter 5

NAT Configuration

This chapter focuses on configuring Network Address Translation (NAT) for Network J and Network E. NAT is used to translate private IP addresses to public IP addresses, ensuring internet access for devices within these networks. Dynamic NAT was implemented for both networks to handle multiple devices using limited public IP addresses.

5.1 NAT Configuration for Network J

For Network J, dynamic NAT was configured on the router to translate private IP addresses in the range ‘213.107.0.0/16‘ to public IPs. The configuration details are as follows:

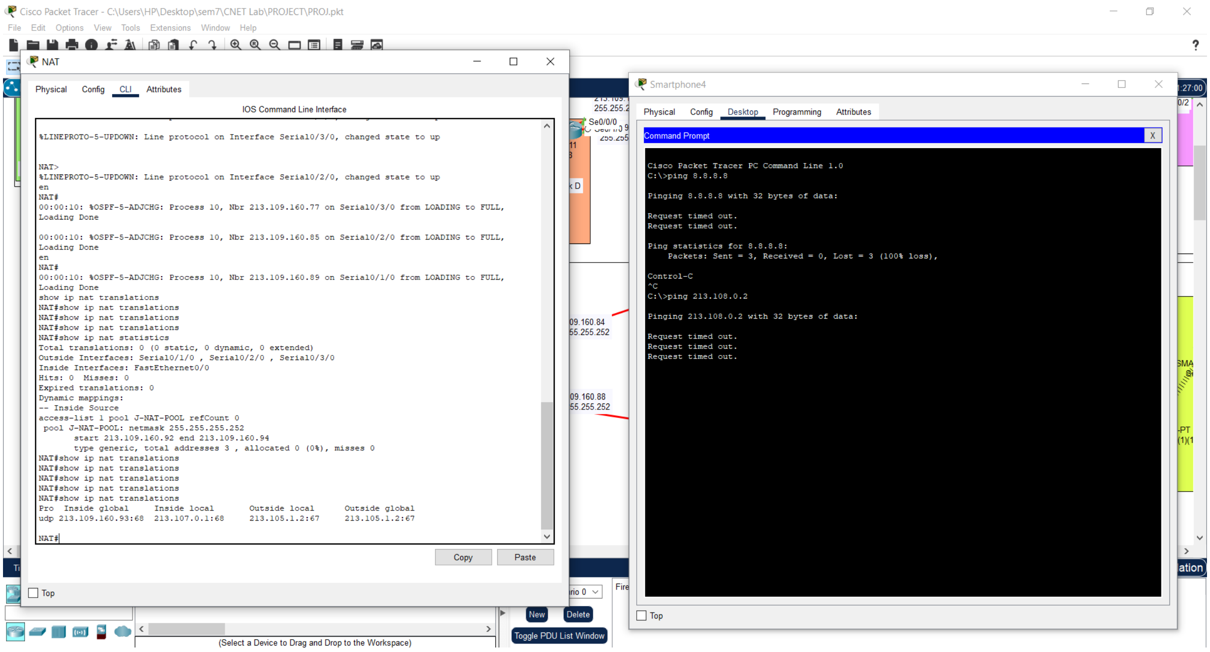
5.1.1 Commands for Network J NAT Configuration

The following commands were used to configure NAT for Network J:

```
NAT(config)#ip nat pool J-NAT-POOL 213.109.160.92 213.109.160.94 netmask 255.255.255.
NAT(config)#access-list 1 permit 213.107.0.0 0.0.255.255
NAT(config)#ip nat inside source list 1 pool J-NAT-POOL overload
NAT(config)#interface FastEthernet0/0
NAT(config-if)#ip nat inside
NAT(config-if)#exit

NAT(config)#interface Serial0/1/0
NAT(config-if)#ip nat outside
NAT(config-if)#exit

NAT(config)#interface Serial0/2/0
NAT(config-if)#ip nat outside
NAT(config-if)#exit

NAT(config)#interface Serial0/3/0
NAT(config-if)#ip nat outside
NAT(config-if)#exit
```

5.1.2 Verification for Network J NAT

The configuration was verified by sending traffic from devices in Network J. The following image demonstrates successful NAT operation:



Cisco Packet Tracer - C:\Users\HP\Desktop\sem7\CNET Lab\PROJECT\PROJ.pkt
File Edit Options View Tools Extensions Window Help
NAT
Physical Config CLI Attributes
IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up


NAT>
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up
en
NAT#
00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr 213.109.160.77 on Serial0/3/0 from LOADING to FULL,
Loading Done

00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr 213.109.160.85 on Serial0/2/0 from LOADING to FULL,
Loading Done
en
NAT#
00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr 213.109.160.89 on Serial0/1/0 from LOADING to FULL,
Loading Done
show ip nat translations
NAT#show ip nat translations
NAT#show ip nat translations
NAT#show ip nat translations
NAT#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/1/0 , Serial0/2/0 , Serial0/3/0
Inside Interfaces: FastEthernet0/0
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool J-NAT-POOL refCount 0
 pool J-NAT-POOL: netmask 255.255.255.252
       start 213.109.160.92 end 213.109.160.94
       type generic, total addresses 3 , allocated 0 (0%), misses 0
NAT#show ip nat translations
NAT#show ip nat translations
NAT#show ip nat translations
NAT#show ip nat translations
NAT#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
udp 213.109.160.93:68  213.107.0.1:68     213.105.1.2:67     213.105.1.2:67

NAT#
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),

Control-C
^C
C:\>ping 213.108.0.2

Pinging 213.108.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
```

Figure 5.1: NAT Verification for Network J

5.2 NAT Configuration for Network E

For Network E, dynamic NAT was configured to translate private IP addresses in the range ‘213.98.0.0/15‘ to public IPs. The configuration details are as follows:

5.2.1 Commands for Network E NAT Configuration

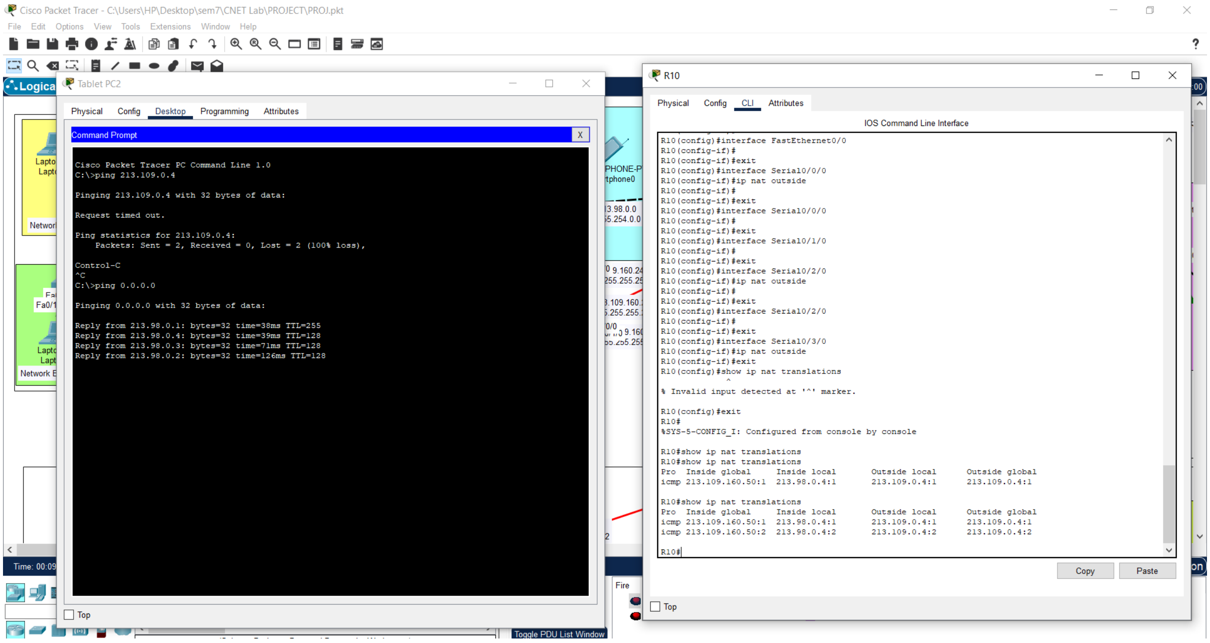
The following commands were used to configure NAT for Network E:

```
R10(config)#ip nat pool R10-NAT-POOL 213.109.160.50 213.109.160.55 netmask 255.255.25
R10(config)#access-list 1 permit 213.98.0.0 0.1.255.255
R10(config)#ip nat inside source list 1 pool R10-NAT-POOL overload
R10(config)#interface FastEthernet0/0
R10(config-if)#ip nat inside
R10(config-if)#exit

R10(config)#interface Serial0/0/0
R10(config-if)#ip nat outside
R10(config-if)#exit

R10(config)#interface Serial0/2/0
R10(config-if)#ip nat outside
R10(config-if)#exit
```

```
R10(config)#interface Serial0/3/0
R10(config-if)#ip nat outside
R10(config-if)#exit
```

5.2.2 Verification for Network E NAT

The configuration was verified by sending traffic from devices in Network E. The following image demonstrates successful NAT operation:



Cisco Packet Tracer - C:\Users\HP\Desktop\sem7\CNET Lab\PROJECT\PROJ.pkt
File Edit Options View Tools Extensions Window Help
Tablet PC2
Physical Config Desktop Programming Attributes
Command Prompt
Top
R10
Physical Config CLI Attributes
IOS Command Line Interface
Copy Paste
Top
Toggle PDU List Window

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 213.109.0.4

Pinging 213.109.0.4 with 32 bytes of data:

Request timed out.

Ping statistics for 213.109.0.4:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
^C
C:\>ping 0.0.0.0

Pinging 0.0.0.0 with 32 bytes of data:

Reply from 213.98.0.1: bytes=32 time=38ms TTL=255
Reply from 213.98.0.4: bytes=32 time=39ms TTL=128
Reply from 213.98.0.3: bytes=32 time=71ms TTL=128
Reply from 213.98.0.2: bytes=32 time=126ms TTL=128
```

```
R10(config)#interface FastEthernet0/0
R10(config-if)#
R10(config-if)#exit
R10(config)#interface Serial0/0/0
R10(config-if)#ip nat outside
R10(config-if)#
R10(config-if)#exit
R10(config)#interface Serial0/0/0
R10(config-if)#
R10(config-if)#exit
R10(config)#interface Serial0/1/0
R10(config-if)#
R10(config-if)#exit
R10(config)#interface Serial0/2/0
R10(config-if)#ip nat outside
R10(config-if)#
R10(config-if)#exit
R10(config)#interface Serial0/2/0
R10(config-if)#
R10(config-if)#exit
R10(config)#interface Serial0/3/0
R10(config-if)#ip nat outside
R10(config-if)#exit
R10(config)#show ip nat translations
                ^
% Invalid input detected at '^' marker.

R10(config)#exit
R10#
%SYS-5-CONFIG_I: Configured from console by console

R10#show ip nat translations
R10#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 213.109.160.50:1  213.98.0.4:1       213.109.0.4:1      213.109.0.4:1

R10#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 213.109.160.50:1  213.98.0.4:1       213.109.0.4:1      213.109.0.4:1
icmp 213.109.160.50:2  213.98.0.4:2       213.109.0.4:2      213.109.0.4:2

R10#
```

Figure 5.2: NAT Verification for Network E

Chapter 6

ACL Implementation

This chapter covers the creation and application of Access Control Lists (ACLs) to restrict access to the web server for specified devices while allowing access to other resources. The ACLs were configured on the router connected to the web server to enforce these restrictions effectively.

6.1 ACL Requirements

The following restrictions were implemented using ACLs:

- A laptop named ”Restricted” from Network A is not allowed to access the web server.
- A smartphone named ”Restricted1” from Network E is not allowed to access the web server.
- A smartphone named ”Restricted2” from Network J is not allowed to access the web server.
- All hosts connected to Network D (a laptop named ”Restricted4” and a PC named ”Restricted3”) are not allowed to access the web server.

The restrictions ensure selective access control to the web server while maintaining accessibility for other devices.

6.2 Commands for ACL Configuration

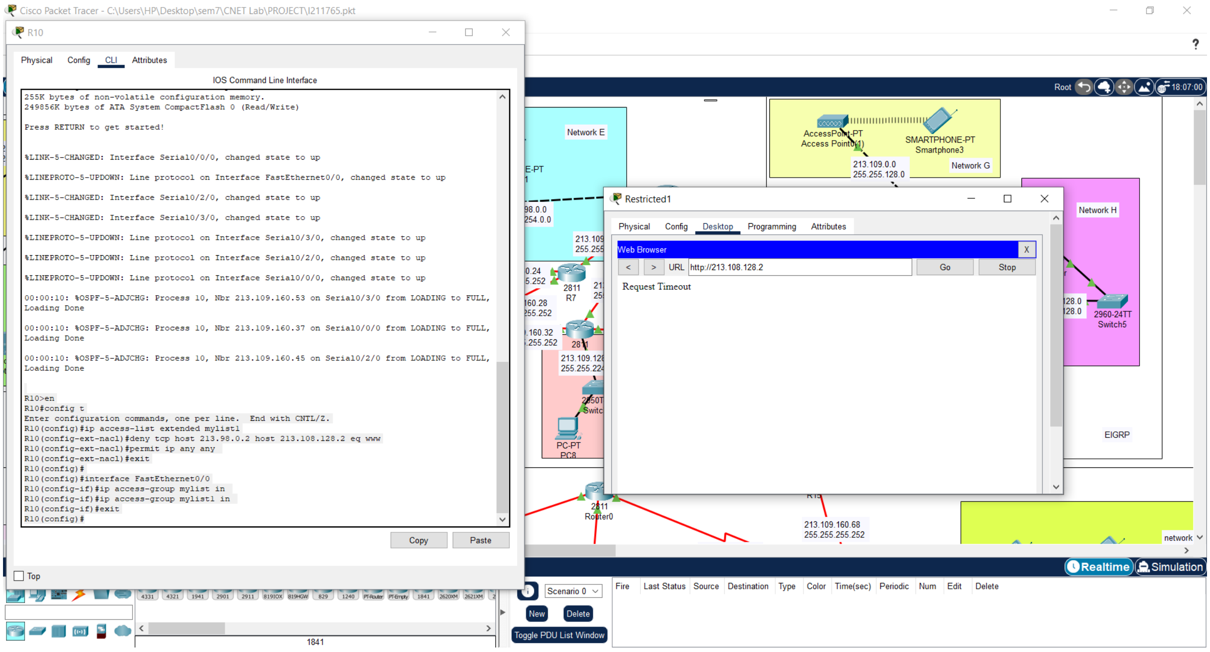
The following commands were used to configure the ACLs on Router R1, R10, R8 and NAT, which is connected to the web server:

```
R8(config)#ip access-list extended mylist3
R8(config-ext-nacl)#deny tcp host 213.100.0.2 host 213.108.128.2 eq www
R8(config-ext-nacl)#permit ip any any
R8(config-ext-nacl)#EXIT
R8(config)#interface FastEthernet0/0
R8(config-if)#ip access-group mylist3 iN
R8(config-if)#
R8(config-if)#exit
```

These commands deny specific hosts from accessing the web server (‘213.108.128.2‘) on port 80 (HTTP) while permitting all other traffic.

6.3 Verification of ACL Configuration

To verify the ACL implementation, tests were performed using the restricted devices to ensure they could not access the web server, while other devices retained access.

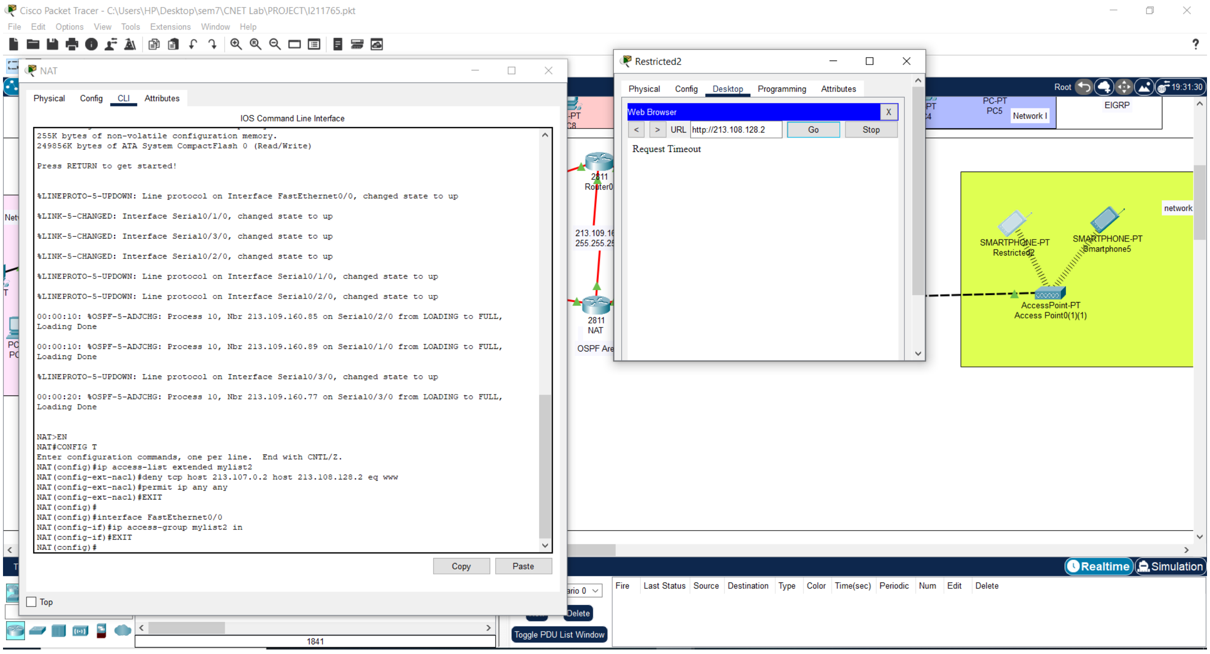


```
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface Serial0/2/0, changed state to up

%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr 213.109.160.53 on Serial0/3/0 from LOADING to FULL,
Loading Done

00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr 213.109.160.37 on Serial0/0/0 from LOADING to FULL,
Loading Done

00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr 213.109.160.45 on Serial0/2/0 from LOADING to FULL,
Loading Done


R10>en
R10#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R10(config)#ip access-list extended mylist1
R10(config-ext-nacl)#deny tcp host 213.98.0.2 host 213.108.128.2 eq www
R10(config-ext-nacl)#permit ip any any
R10(config-ext-nacl)#exit
R10(config)#
R10(config)#interface FastEthernet0/0
R10(config-if)#ip access-group mylist in
R10(config-if)#ip access-group mylist1 in
R10(config-if)#exit
R10(config)#
```

URL http://213.108.128.2

Request Timeout

Figure 6.1: Verification of Web Server ACL Configuration

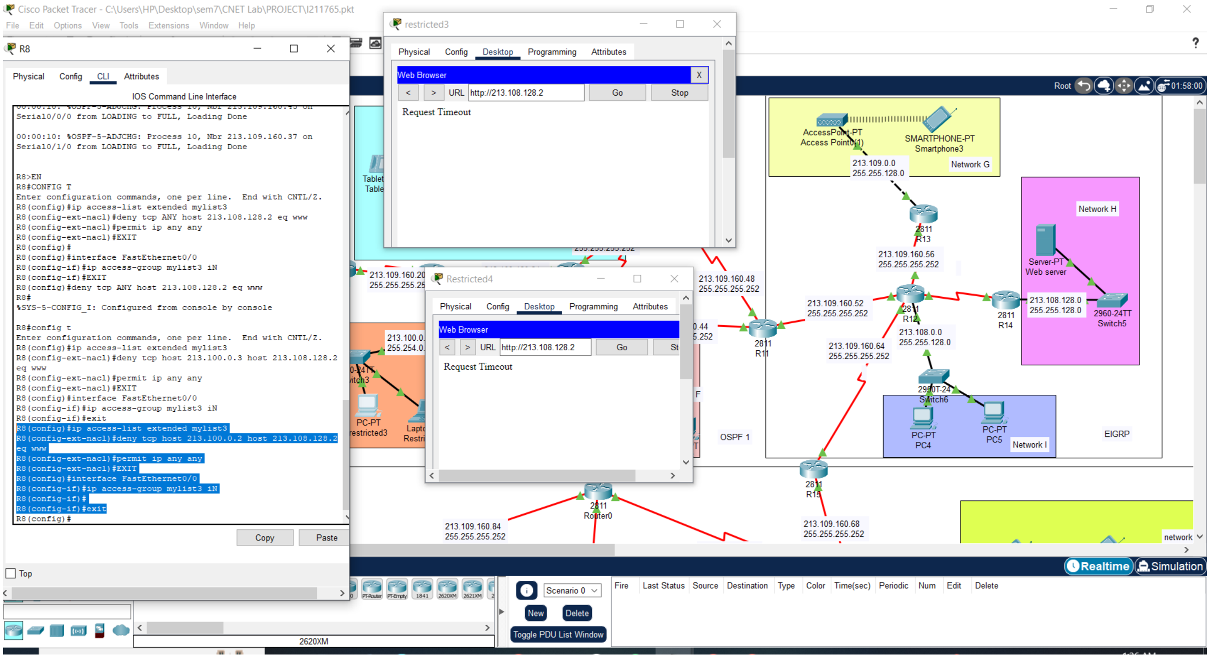


```
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up

%LINK-5-CHANGED: Interface Serial0/2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up

00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr 213.109.160.85 on Serial0/2/0 from LOADING to FULL,
Loading Done

00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr 213.109.160.89 on Serial0/1/0 from LOADING to FULL,
Loading Done

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

00:00:20: %OSPF-5-ADJCHG: Process 10, Nbr 213.109.160.77 on Serial0/3/0 from LOADING to FULL,
Loading Done


NAT>EN
NAT#CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
NAT(config)#ip access-list extended mylist2
NAT(config-ext-nacl)#deny tcp host 213.107.0.2 host 213.108.128.2 eq www
NAT(config-ext-nacl)#permit ip any any
NAT(config-ext-nacl)#EXIT
NAT(config)#
NAT(config)#interface FastEthernet0/0
NAT(config-if)#ip access-group mylist2 in
NAT(config-if)#EXIT
NAT(config)#
```

URL http://213.108.128.2

Request Timeout

Figure 6.2: Verification of Web Server ACL Configuration



Cisco Packet Tracer - C:\Users\HP\Desktop\sem7\CNET Lab\PROJECT\I211765.pkt

R8 — IOS Command Line Interface

```
00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr 213.109.160.45 on
Serial0/0/0 from LOADING to FULL, Loading Done

00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr 213.109.160.37 on
Serial0/1/0 from LOADING to FULL, Loading Done


R8>EN
R8#CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
R8(config)#ip access-list extended mylist3
R8(config-ext-nacl)#deny tcp ANY host 213.108.128.2 eq www
R8(config-ext-nacl)#permit ip any any
R8(config-ext-nacl)#EXIT
R8(config)#
R8(config)#interface FastEthernet0/0
R8(config-if)#ip access-group mylist3 iN
R8(config-if)#EXIT
R8(config)#deny tcp ANY host 213.108.128.2 eq www
R8#
%SYS-5-CONFIG_I: Configured from console by console

R8#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R8(config)#ip access-list extended mylist3
R8(config-ext-nacl)#deny tcp host 213.100.0.3 host 213.108.128.2
eq www
R8(config-ext-nacl)#permit ip any any
R8(config-ext-nacl)#EXIT
R8(config)#interface FastEthernet0/0
R8(config-if)#ip access-group mylist3 iN
R8(config-if)#exit
R8(config)#ip access-list extended mylist3
R8(config-ext-nacl)#deny tcp host 213.100.0.2 host 213.108.128.2
eq www
R8(config-ext-nacl)#permit ip any any
R8(config-ext-nacl)#EXIT
R8(config)#interface FastEthernet0/0
R8(config-if)#ip access-group mylist3 iN
R8(config-if)#
R8(config-if)#exit
R8(config)#
```

restricted3 — Web Browser

URL http://213.108.128.2

Request Timeout

Restricted4 — Web Browser

URL http://213.108.128.2

Request Timeout

Figure 6.3: Verification of Web Server ACL Configuration

Figure 6.3 demonstrates the ACL configuration and successful enforcement of restrictions on Router R14.

Chapter 7

Email Configuration

This chapter explains the configuration of an SMTP server to enable successful email communication between hosts in the network. A mail server was configured in the first block of the network, and all hosts were set up to use email services. The configuration ensures seamless email exchange between devices in the network.

7.1 Mail Server Configuration

The mail server was configured to provide SMTP and POP3 services to the network. The following steps were performed:

1. Accessed the ”Mail Server” in the network.
2. Enabled SMTP and POP3 services under the server settings.
3. Added user accounts for all hosts in the network, specifying usernames and passwords.
4. Verified that the server was operational and ready to handle email communication.

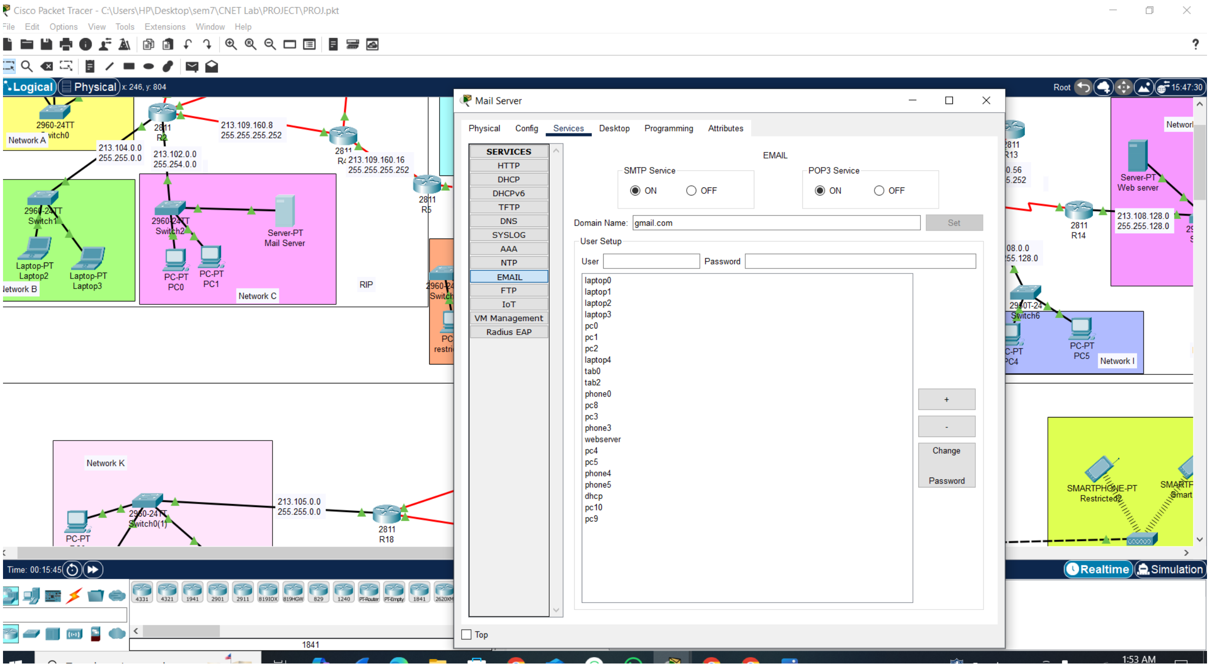
7.2 Email Verification

To verify the configuration, an email was sent from Laptop3 in Network B to a smartphone in Network J. The email was successfully delivered, confirming the functionality of the mail server and proper configuration of email services on the devices.

7.2.1 Verification Screenshot

The following image demonstrates the email sent from Laptop3 to the smartphone in Network J, showing successful email delivery:

The email configuration was successfully implemented, allowing hosts in the network to communicate via email. The SMTP server was able to handle multiple users, and the verification process confirmed the reliability and functionality of the email services.



EMAIL

SMTP Service: ● ON ○ OFF

POP3 Service: ● ON ○ OFF

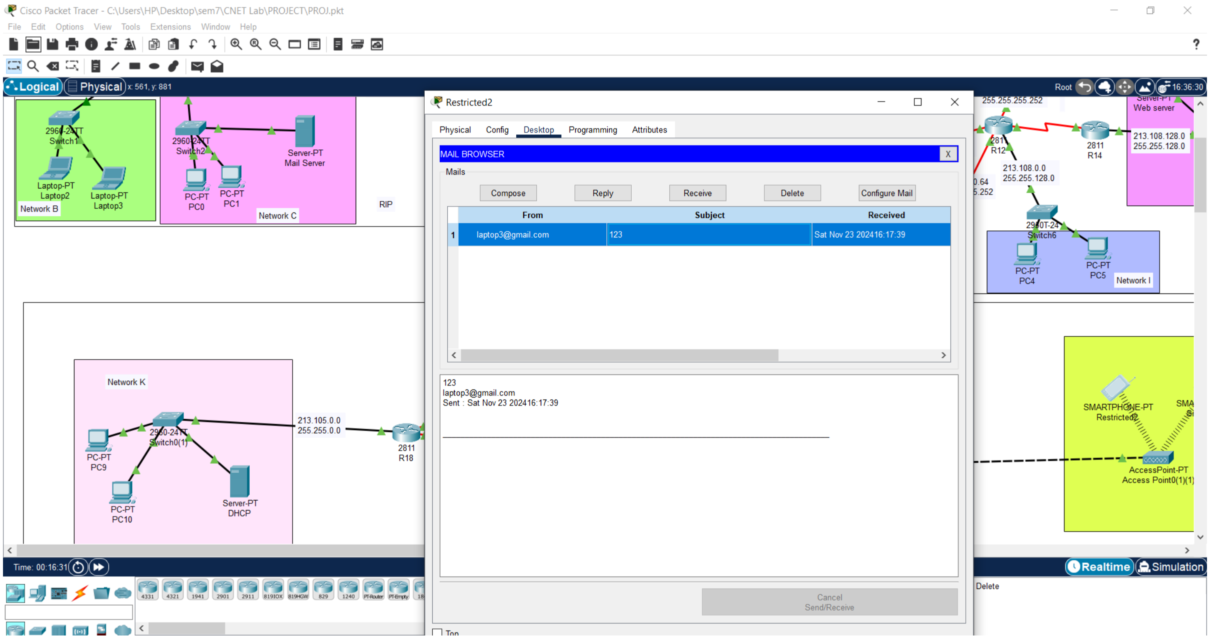
Domain Name: gmail.com

User Setup

User: Password:

laptop0
laptop1
laptop2
laptop3
pc0
pc1
pc2
laptop4
tab0
tab2
phone0
pc8
pc3
phone3
webserver
pc4
pc5
phone4
phone5
dhcp
pc10
pc9

Figure 7.1: Mail Server Configuration



	From	Subject	Received
1	laptop3@gmail.com	123	Sat Nov 23 202416:17:39

123
laptop3@gmail.com
Sent : Sat Nov 23 202416:17:39

Figure 7.2: Email Verification: Email from Laptop3 to Smartphone in Network J

PDUs Verification

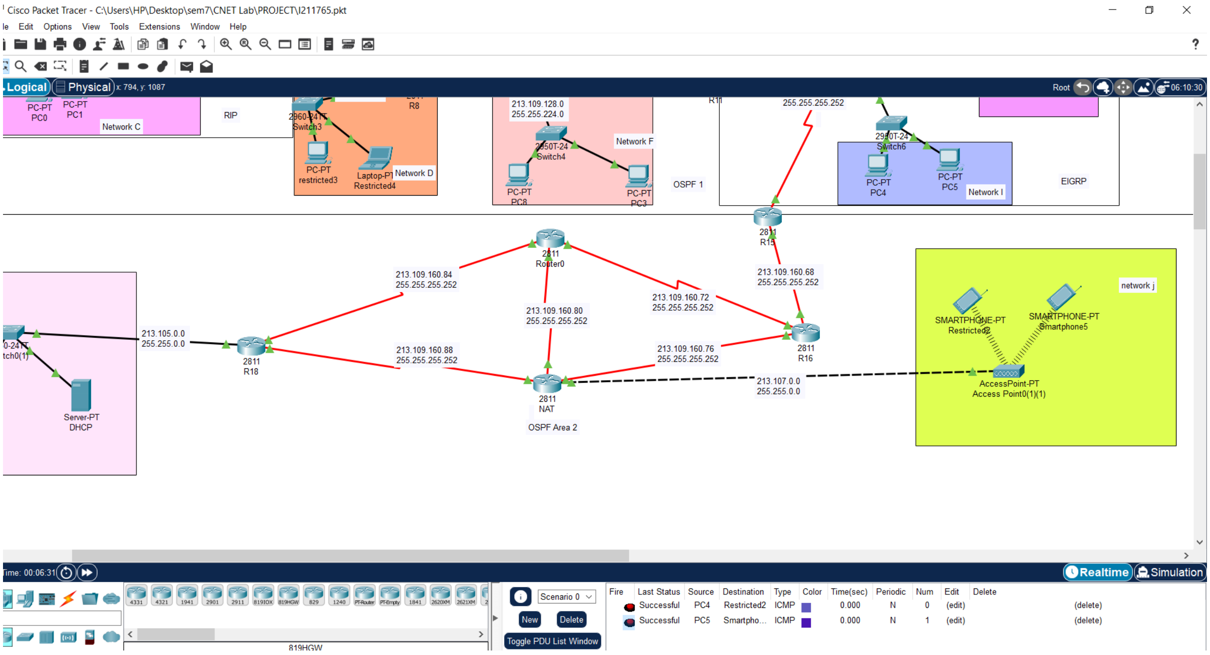
Successful PDUs in EIGRP and OSPF Area 2

Successful PDUs in OSPF Area 1 and Area 2

Successful PDUs in OSPF Area 1 and EIGRP

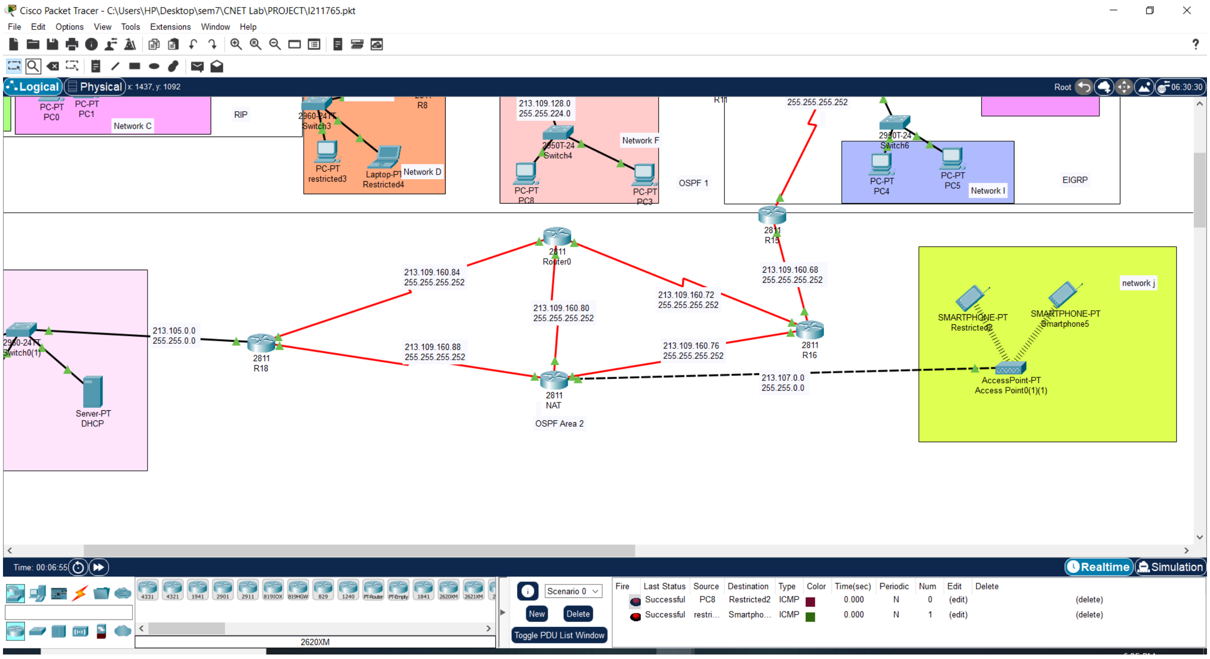
Successful PDUs in RIP and OSPF Area 2

Successful PDUs in RIP and EIGRP



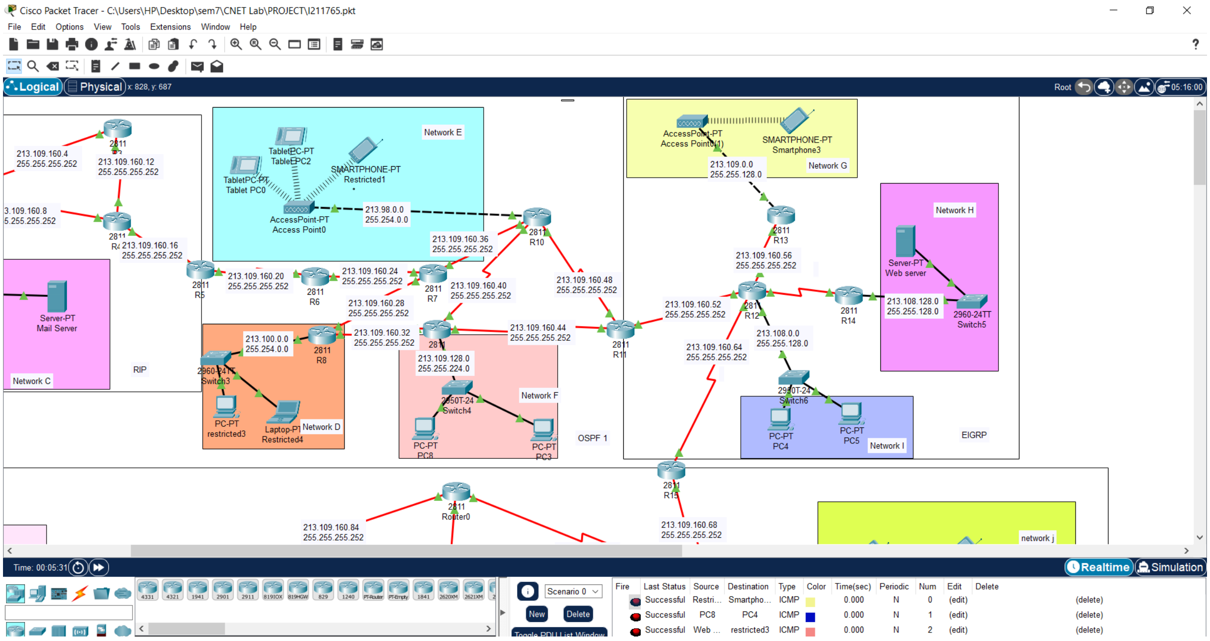
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC4	Restricted2	ICMP	🟪	0.000	N	0	(edit)	(delete)
●	Successful	PC5	Smartpho...	ICMP	🟪	0.000	N	1	(edit)	(delete)

Figure 7.3: Successful PDUs in EIGRP and OSPF Area 2



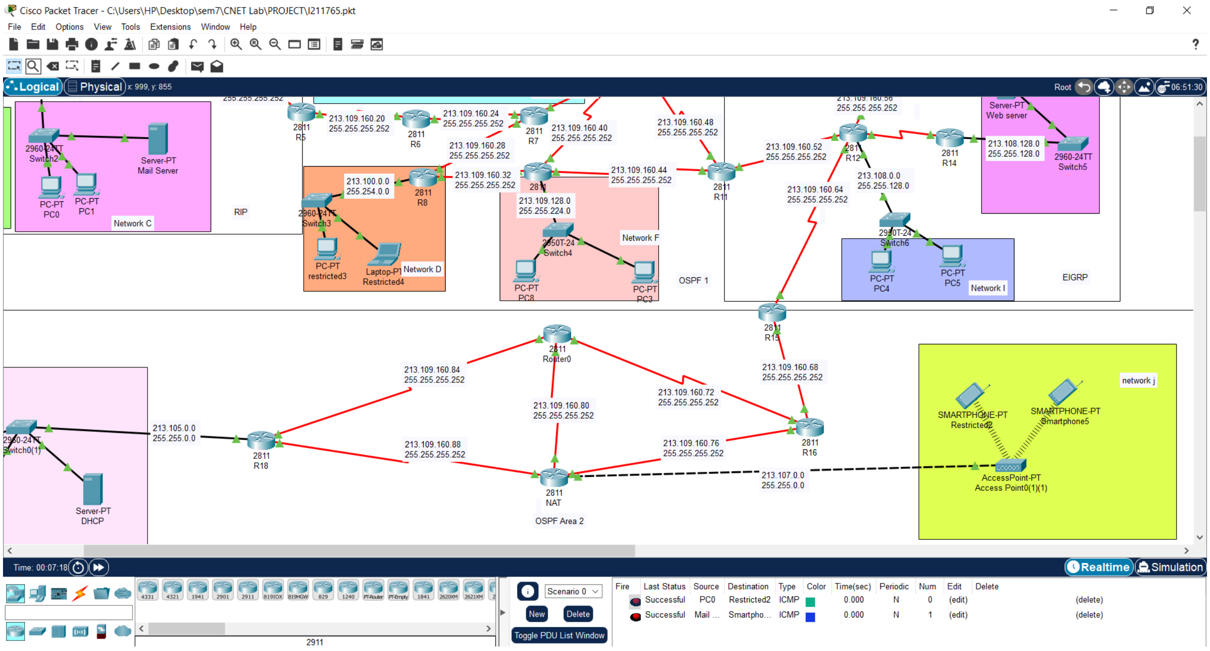
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC8	Restricted2	ICMP	🟥	0.000	N	0	(edit)	(delete)
●	Successful	restri...	Smartpho...	ICMP	🟩	0.000	N	1	(edit)	(delete)

Figure 7.4: Successful PDUs in OSPF Area 1 and Area 2



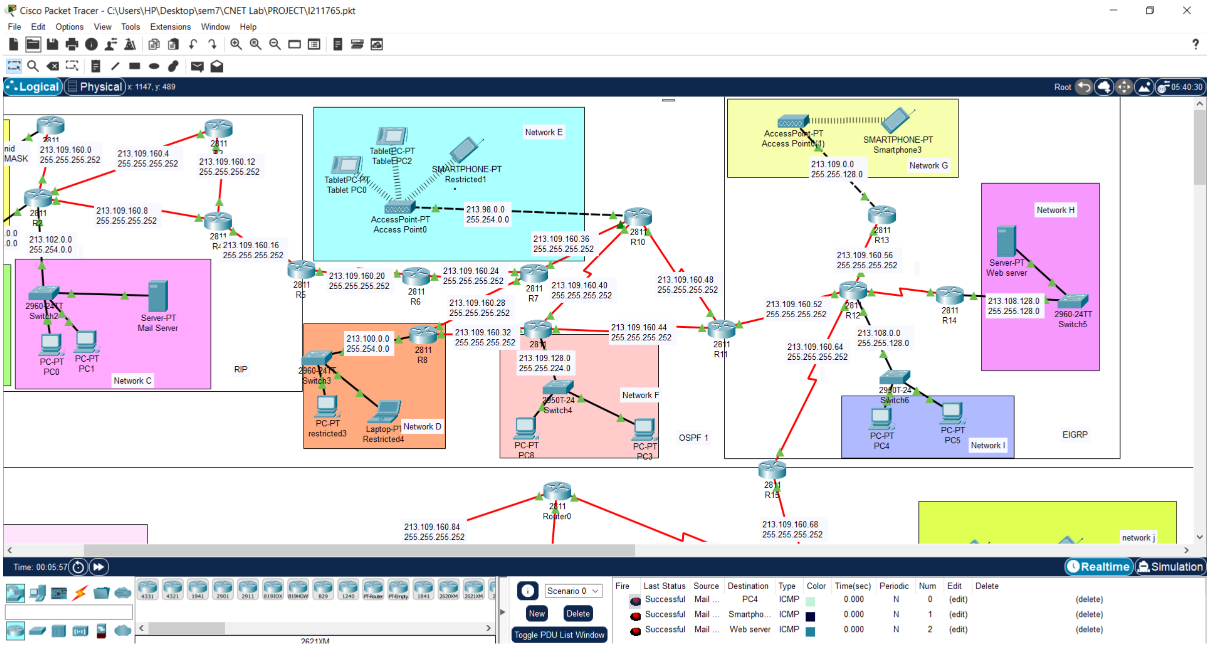
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	Restri...	Smartpho...	ICMP	🟨	0.000	N	0	(edit)	(delete)
●	Successful	PC8	PC4	ICMP	🟦	0.000	N	1	(edit)	(delete)
●	Successful	Web ...	restricted3	ICMP	🟥	0.000	N	2	(edit)	(delete)

Figure 7.5: Successful PDUs in OSPF Area 1 and EIGRP



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC0	Restricted2	ICMP	🟩	0.000	N	0	(edit)	(delete)
●	Successful	Mail ...	Smartpho...	ICMP	🟦	0.000	N	1	(edit)	(delete)

Figure 7.6: Successful PDUs in RIP and OSPF Area 2



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	Mail ...	PC4	ICMP	■	0.000	N	0	(edit)	(delete)
●	Successful	Mail ...	Smartpho...	ICMP	■	0.000	N	1	(edit)	(delete)
●	Successful	Mail ...	Web server	ICMP	■	0.000	N	2	(edit)	(delete)

Figure 7.7: Successful PDUs in RIP and EIGRP

Conclusion

This Computer Networks Semester Project successfully demonstrated the design, implementation, and configuration of a robust and scalable network infrastructure. Through careful planning and execution, key networking concepts such as topology creation, efficient IP addressing using VLSM, dynamic routing protocols (RIP, OSPF, and EIGRP), and DHCP server configuration were implemented effectively. Network Address Translation (NAT) was configured to enable secure and efficient internet access for private IP addresses, while Access Control Lists (ACLs) were applied to enforce security policies and restrict unauthorized access to the web server. Additionally, an SMTP server was set up to facilitate email communication across the network, showcasing application-level functionality. Each network component was tested and verified to ensure proper connectivity and functionality, highlighting a comprehensive understanding of computer networking principles. This project serves as a practical demonstration of integrating various networking technologies to solve real-world challenges while ensuring scalability, security, and efficiency.

The project showcased the integration of various networking technologies and their practical application. Through detailed configuration and verification, the project achieved all objectives, demonstrating a comprehensive understanding of computer networks.

References

1. Cisco Networking Academy. ”Introduction to Networks.” Cisco Press.

2. SubnettingPractice.com. ”VLSM Subnetting Tool.” Available at https://subnettingpractice.com/vlsm.htm

3. Packet Tracer Official Documentation. ”Cisco Packet Tracer User Guide.”