National University of Computer and Emerging Sciences
Islamabad Campus

CS-3001
COMPUTER NETWORKS

Semester Project

Network Infrastructure on Cisco Packet Tracer

Submitted by: Sarita Sangrez
Roll number: 23i-2088
Section : CY-A
Submission Date: 9th May 2025

Project Objectives

The objective of this project is to design and configure a multi-block enterprise network in Cisco Packet Tracer using advanced networking concepts. The tasks were structured to help us learn and apply key networking principles, including subnetting with VLSM, assigning IPs based on host requirements, and configuring dynamic routing protocols (EIGRP, OSPF Area 1 & 2, and RIP) along with route redistribution across blocks. A centralized DHCP server in Block D was used to dynamically assign IP addresses to designated networks.

Additionally, the project included implementing NAT on the routers with Network F and Network K using a provided public IP and a private IP to enable internet access for internal hosts. Access Control Lists (ACLs) were used to restrict web server access for specified devices (in Network A and B) and all hosts in network D. A Mail Server was configured to allow email communication between specific networks, and FTP Server access was restricted to authorized systems. These tasks reinforced our understanding of network segmentation, IP management, routing protocols, NAT, ACLs, and network service configuration.

Steps Followed During Implementation

1. Initial IP Address Planning and Network Design

Began by analyzing the assigned host requirements for each network from the provided file. Using Variable Length Subnet Masking (VLSM), appropriate IP addresses and subnet masks were allocated. The main allocations included:

Network L: 192.168.0.0/16 (supports 65,000 hosts)

Network N: 192.169.0.0/18 (supports 16,000 hosts)

Network M: 192.169.64.0/18

Network G: 192.169.128.0/18

Network F: 172.16.0.0/18 (private)

Network H: 192.170.0.0/16

Network I: 192.171.0.0/16

Network J: 192.172.0.0/15

Network K: 172.18.0.0/15 (private)

Network A: 192.174.32.0/19

Network B: 192.174.64.0/18

Network C: 192.174.128.0/23

2. Design and Configuration of Block D (Core Block)

- Designed Block D first, as it included the centralized DHCP Server.
- Configured the DHCP server to serve dynamic IP addresses to all networks in EIGRP, RIP, and OSPF Area 1 & 2.
- Implemented the required IP addressing for all internal devices and router interfaces based on the subnetting scheme.

3. Routing Configuration by Block

For each block, appropriate routing protocols were configured based on the instructions:

- EIGRP for designated Block F and Block B
- RIP for Block E
- OSPF Area 0, Area 1 and Area 2 in Block D, A and C respectively

Routing was configured first for each block before any other services were implemented.

4. Stepwise Block Connectivity and Redistribution

- After completing a block's routing configuration, the next connected block was designed.
- Redistributed routes between blocks where different routing protocols were used, ensuring full interconnectivity.

- After establishing routing within and between blocks, DHCP pools were added to the server for all networks using dynamic IP assignment.

5. Access Control List (ACL) Implementation

Configured ACLs on the router connected to the Web Server to enforce restrictions and deny access to the web server from:

- One PC in Network A
- One Laptop in Network E
- Smart Phone in Network B
- All hosts in Network D

6. Network Address Translation (NAT) Configuration

Implemented NAT on:

- Router with the Network F
- Router with the Network K
- Used 192.168.2.26 as the public IP address (assigned)
- Used 172.16.254.30 as the private IP address for NAT translation.

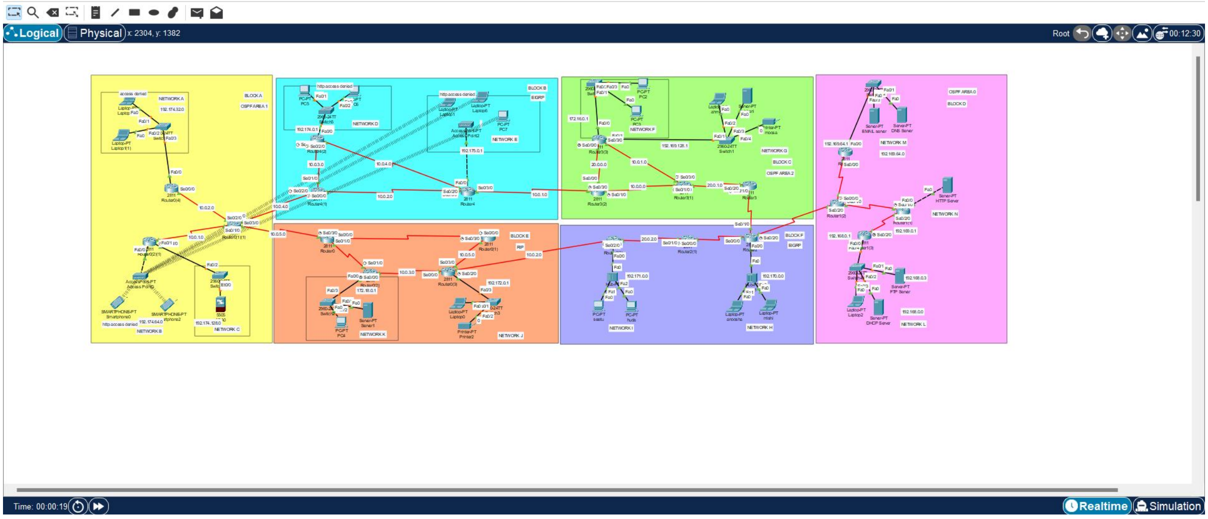
7. Service Configuration

Configured the following services toward the end after completing the above configurations:

- Web Server for general HTTP access (except for the end systems whichss were restricted)
- Mail Server in Block D to allow email communication between Network H and Network I
- FTP Server, with access and upload permissions restricted exclusively to Network G

Network Design and Configuration Details

The network was designed using Cisco Packet Tracer based on the provided scenario and assigned IP address resources. The design followed modular block-based topology, with each block using a specific routing protocol and interconnecting through redistribution where needed. All subnets were calculated using VLSM (Variable Length Subnet Masking) to optimize IP usage.

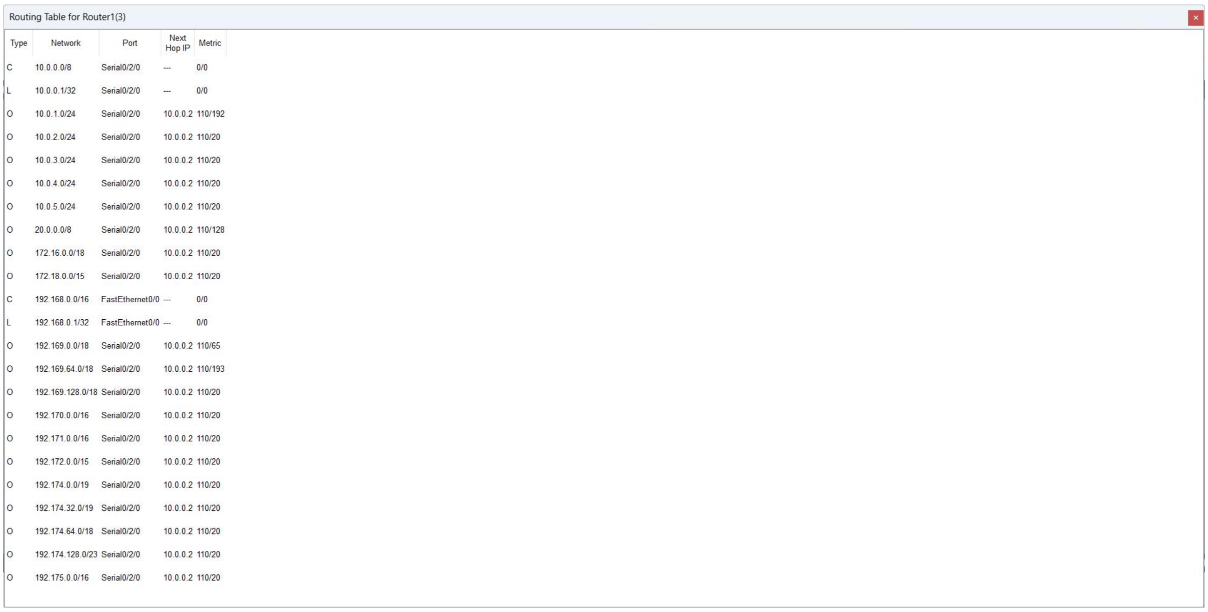


1. IP Address Allocation (VLSM-Based)

Each network was assigned an IP range based on the number of required hosts. The following addresses and subnet masks were used:

Network	IP Address	Subnet Mask	CIDR	Description
L	192.168.0.0	255.255.0.0	/16	~65,000 hosts
N	192.169.0.0	255.255.192.0	/18	~13,000 hosts
M	192.169.64.0	255.255.192.0	/18	~11,000 hosts
G	192.169.128.0	255.255.192.0	/18	~9,000 hosts
F	172.16.0.0	255.252.0.0	/18	~9,000 hosts

H	192.170.0.0	255.255.0.0	/16	~65,000 hosts
I	192.171.0.0	255.255.0.0	/16	~65,000 hosts
J	192.172.0.0	255.254.0.0	/15	~75,000 hosts
K	172.18.0.0	255.254.0.0	/15	~85,000 hosts
A	192.174.32.0	255.255.224.0	/19	~7,000 hosts
B	192.174.64.0	255.255.192.0	/18	~10,000 hosts
C	192.174.128.0	255.255.254.0	/23	~500 hosts



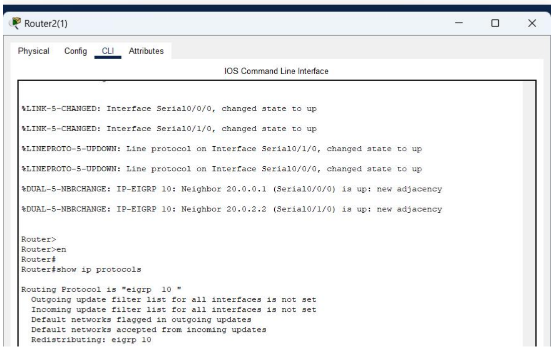
Routing Table for Router1(3)

Type	Network	Port	Next Hop IP	Metric
C	10.0.0.0/8	Serial0/2/0	---	0/0
L	10.0.0.1/32	Serial0/2/0	---	0/0
O	10.0.1.0/24	Serial0/2/0	10.0.0.2	110/192
O	10.0.2.0/24	Serial0/2/0	10.0.0.2	110/20
O	10.0.3.0/24	Serial0/2/0	10.0.0.2	110/20
O	10.0.4.0/24	Serial0/2/0	10.0.0.2	110/20
O	10.0.5.0/24	Serial0/2/0	10.0.0.2	110/20
O	20.0.0.0/8	Serial0/2/0	10.0.0.2	110/128
O	172.16.0.0/18	Serial0/2/0	10.0.0.2	110/20
O	172.18.0.0/15	Serial0/2/0	10.0.0.2	110/20
C	192.168.0.0/16	FastEthernet0/0	---	0/0
L	192.168.0.1/32	FastEthernet0/0	---	0/0
O	192.169.0.0/18	Serial0/2/0	10.0.0.2	110/65
O	192.169.64.0/18	Serial0/2/0	10.0.0.2	110/193
O	192.169.128.0/18	Serial0/2/0	10.0.0.2	110/20
O	192.170.0.0/16	Serial0/2/0	10.0.0.2	110/20
O	192.171.0.0/16	Serial0/2/0	10.0.0.2	110/20
O	192.172.0.0/15	Serial0/2/0	10.0.0.2	110/20
O	192.174.0.0/19	Serial0/2/0	10.0.0.2	110/20
O	192.174.32.0/19	Serial0/2/0	10.0.0.2	110/20
O	192.174.64.0/18	Serial0/2/0	10.0.0.2	110/20
O	192.174.128.0/23	Serial0/2/0	10.0.0.2	110/20
O	192.175.0.0/16	Serial0/2/0	10.0.0.2	110/20

2. Routing Protocols Used

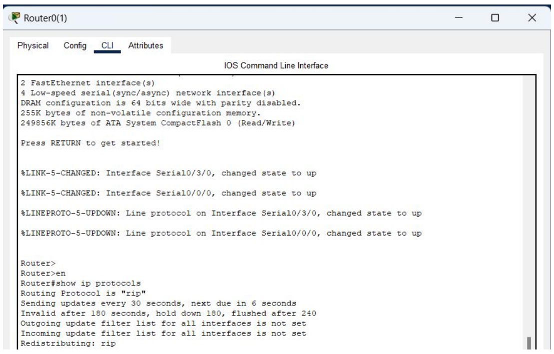
Each block was configured with a specific routing protocol as follows:

- EIGRP for selected blocks e.g The protocol shown on a router in Block F is “eigrp 10”



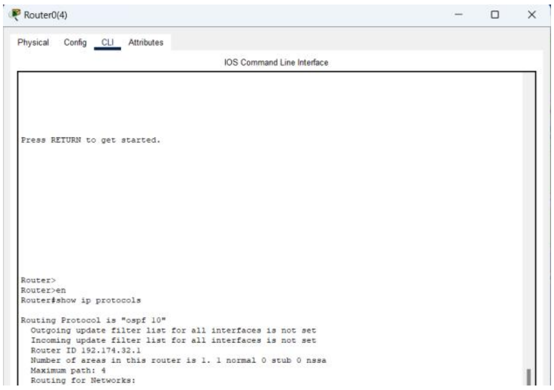
```
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

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

%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 20.0.0.1 (Serial0/0/0) is up: new adjacency

%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 20.0.2.2 (Serial0/1/0) is up: new adjacency


Router>
Router>en
Router#
Router#show ip protocols

Routing Protocol is "eigrp  10 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  Redistributing: eigrp 10
```

- RIP for other assigned blocks e.g the The protocol shown on a router in Block E is “rip”



```
2 FastEthernet interface(s)
4 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
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 Serial0/3/0, changed state to up

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


Router>
Router>en
Router#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 6 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
```

- OSPF Area 0, 1 and 2 where specified e.g The protocol shown on a router in Block A is “ospf 10”

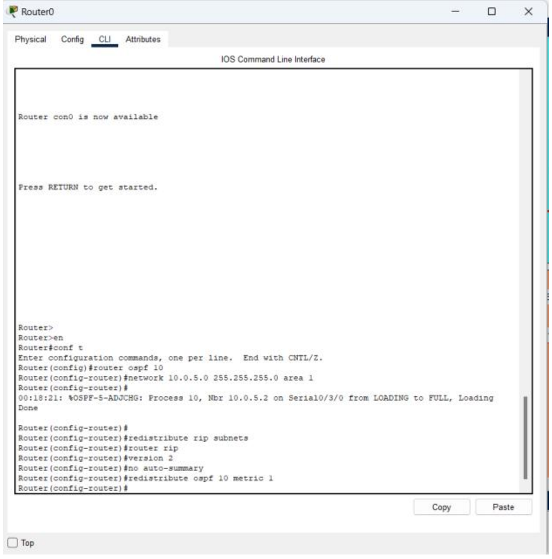


```
Press RETURN to get started.


Router>
Router>en
Router#show ip protocols

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.174.32.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
```

Routers connecting blocks with different routing protocols were configured with route redistribution to ensure connectivity.

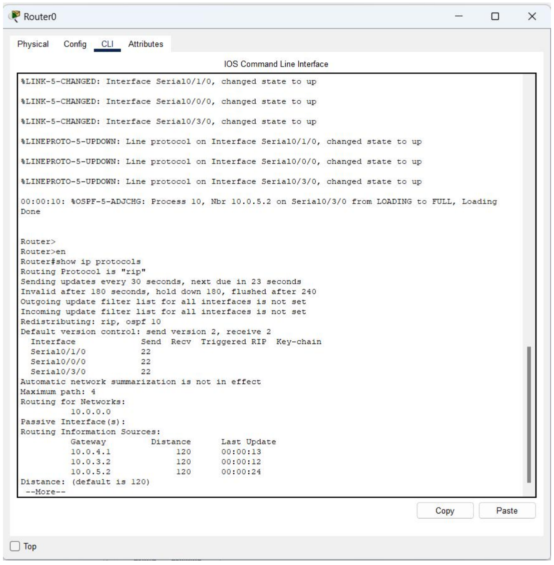
The following boundary router in Block E is part of RIP and is redistributed over OSPF 10:

Implementation:



```
Router con0 is now available



Press RETURN to get started.







Router>
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 10
Router(config-router)#network 10.0.5.0 255.255.255.0 area 1
Router(config-router)#
00:18:21: %OSPF-5-ADJCHG: Process 10, Nbr 10.0.5.2 on Serial0/3/0 from LOADING to FULL, Loading
Done

Router(config-router)#
Router(config-router)#redistribute rip subnets
Router(config-router)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary
Router(config-router)#redistribute ospf 10 metric 1
Router(config-router)#
```

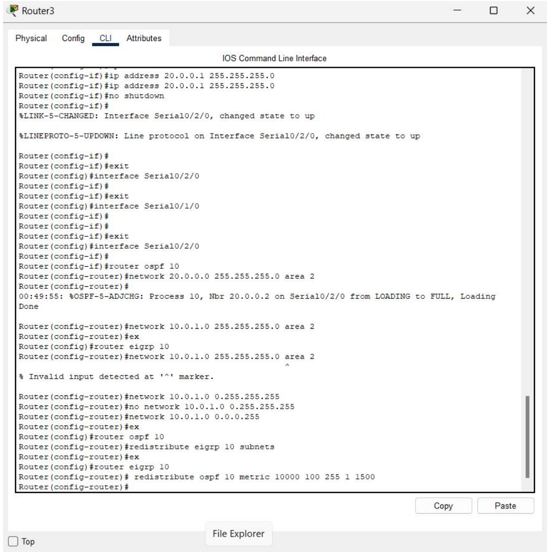
After redistribution:



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

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

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

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

00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr 10.0.5.2 on Serial0/3/0 from LOADING to FULL, Loading
Done


Router>
Router>en
Router#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 23 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip, ospf 10
Default version control: send version 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial0/1/0           22
  Serial0/0/0           22
  Serial0/3/0           22
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
          10.0.0.0
Passive Interface(s):
Routing Information Sources:
          Gateway         Distance      Last Update
          10.0.4.1             120      00:00:13
          10.0.3.2             120      00:00:12
          10.0.5.2             120      00:00:24
Distance: (default is 120)
 --More--
```

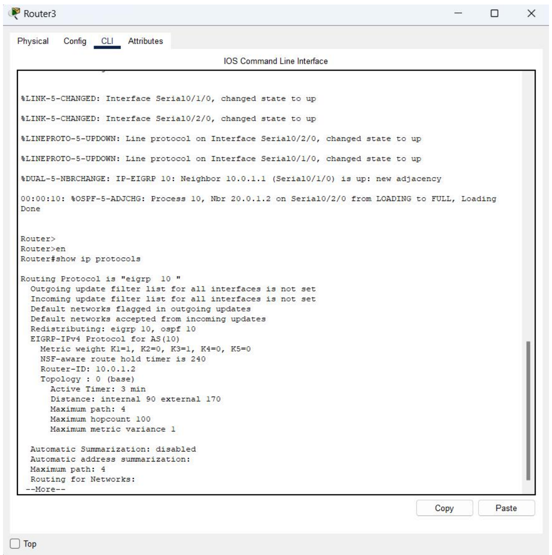
The following boundary router in Block C is part of OSPF and is redistributed over EIGRP 10:

Implementation :



```
Router(config-if)#ip address 20.0.0.1 255.255.255.0
Router(config-if)#ip address 20.0.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/2/0, changed state to up

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

Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/2/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/2/0
Router(config-if)#
Router(config-if)#router ospf 10
Router(config-router)#network 20.0.0.0 255.255.255.0 area 2
Router(config-router)#
00:49:55: %OSPF-5-ADJCHG: Process 10, Nbr 20.0.0.2 on Serial0/2/0 from LOADING to FULL, Loading
Done

Router(config-router)#network 10.0.1.0 255.255.255.0 area 2
Router(config-router)#ex
Router(config)#router eigrp 10
Router(config-router)#network 10.0.1.0 255.255.255.0 area 2
                                                      ^
% Invalid input detected at '^' marker.

Router(config-router)#network 10.0.1.0 0.255.255.255
Router(config-router)#no network 10.0.1.0 0.255.255.255
Router(config-router)#network 10.0.1.0 0.0.0.255
Router(config-router)#ex
Router(config)#router ospf 10
Router(config-router)#redistribute eigrp 10 subnets
Router(config-router)#ex
Router(config)#router eigrp 10
Router(config-router)# redistribute ospf 10 metric 10000 100 255 1 1500
Router(config-router)#
```

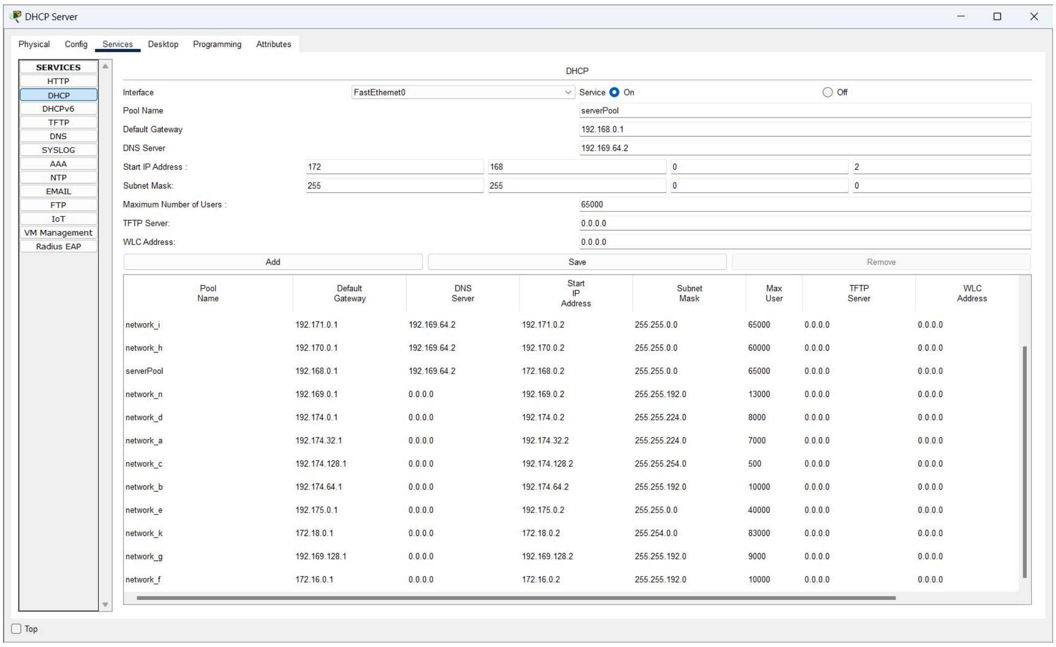
After redistribution :



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

%LINK-5-CHANGED: Interface Serial0/2/0, 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 Serial0/1/0, changed state to up

%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 10.0.1.1 (Serial0/1/0) is up: new adjacency

00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr 20.0.1.2 on Serial0/2/0 from LOADING to FULL, Loading
Done


Router>
Router>en
Router#show ip protocols

Routing Protocol is "eigrp  10 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  Redistributing: eigrp 10, ospf 10
  EIGRP-IPv4 Protocol for AS(10)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 10.0.1.2
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
 --More--
```

3. DHCP Server Setup

A centralized DHCP Server was placed in Block D.
All devices in EIGRP, RIP, OSPF Area 1, and Area 2 received IP addresses dynamically from this server.
DHCP pools were created for each subnet based on their address and mask.



Interface: FastEthernet0
Service ● On ○ Off
Pool Name: serverPool
Default Gateway: 192.168.0.1
DNS Server: 192.169.64.2
Start IP Address : 172 168 0 2
Subnet Mask: 255 255 0 0
Maximum Number of Users : 65000
TFTP Server: 0.0.0.0
WLC Address: 0.0.0.0

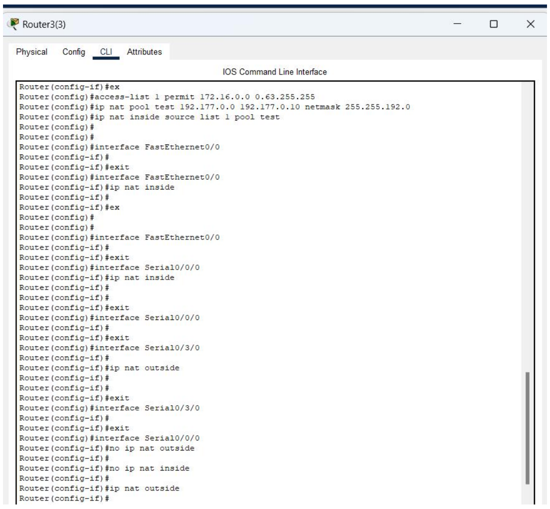
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
network_i	192.171.0.1	192.169.64.2	192.171.0.2	255.255.0.0	65000	0.0.0.0	0.0.0.0
network_h	192.170.0.1	192.169.64.2	192.170.0.2	255.255.0.0	60000	0.0.0.0	0.0.0.0
serverPool	192.168.0.1	192.169.64.2	172.168.0.2	255.255.0.0	65000	0.0.0.0	0.0.0.0
network_n	192.169.0.1	0.0.0.0	192.169.0.2	255.255.192.0	13000	0.0.0.0	0.0.0.0
network_d	192.174.0.1	0.0.0.0	192.174.0.2	255.255.224.0	8000	0.0.0.0	0.0.0.0
network_a	192.174.32.1	0.0.0.0	192.174.32.2	255.255.224.0	7000	0.0.0.0	0.0.0.0
network_c	192.174.128.1	0.0.0.0	192.174.128.2	255.255.254.0	500	0.0.0.0	0.0.0.0
network_b	192.174.64.1	0.0.0.0	192.174.64.2	255.255.192.0	10000	0.0.0.0	0.0.0.0
network_e	192.175.0.1	0.0.0.0	192.175.0.2	255.255.0.0	40000	0.0.0.0	0.0.0.0
network_k	172.18.0.1	0.0.0.0	172.18.0.2	255.254.0.0	83000	0.0.0.0	0.0.0.0
network_g	192.169.128.1	0.0.0.0	192.169.128.2	255.255.192.0	9000	0.0.0.0	0.0.0.0
network_f	172.16.0.1	0.0.0.0	172.16.0.2	255.255.192.0	10000	0.0.0.0	0.0.0.0

4. NAT Configuration

NAT was implemented to allow private IP address translation for internet access:

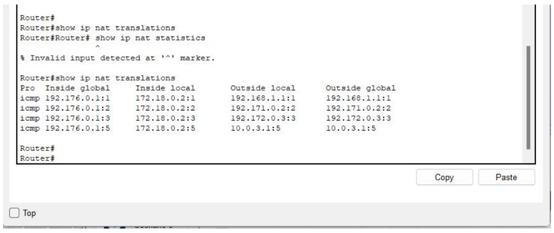
Router with the Network F and Router with Network K were configured with NAT. The following shows the router in Network K :

Implementation :



```
Router(config-if)#ex
Router(config)#access-list 1 permit 172.16.0.0 0.63.255.255
Router(config)#ip nat pool test 192.177.0.0 192.177.0.10 netmask 255.255.192.0
Router(config)#ip nat inside source list 1 pool test
Router(config)#
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#ip nat inside
Router(config-if)#
Router(config-if)#ex
Router(config)#
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#ip nat inside
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/3/0
Router(config-if)#
Router(config-if)#ip nat outside
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/3/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#no ip nat outside
Router(config-if)#
Router(config-if)#no ip nat inside
Router(config-if)#
Router(config-if)#ip nat outside
Router(config-if)#
```

After implementation :



```
Router#
Router#show ip nat translations
Router#Router# show ip nat statistics
              ^
% Invalid input detected at '^' marker.

Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 192.176.0.1:1     172.18.0.2:1       192.168.1.1:1      192.168.1.1:1
icmp 192.176.0.1:2     172.18.0.2:2       192.171.0.2:2      192.171.0.2:2
icmp 192.176.0.1:3     172.18.0.2:3       192.172.0.3:3      192.172.0.3:3
icmp 192.176.0.1:5     172.18.0.2:5       10.0.3.1:5         10.0.3.1:5

Router#
Router#
```

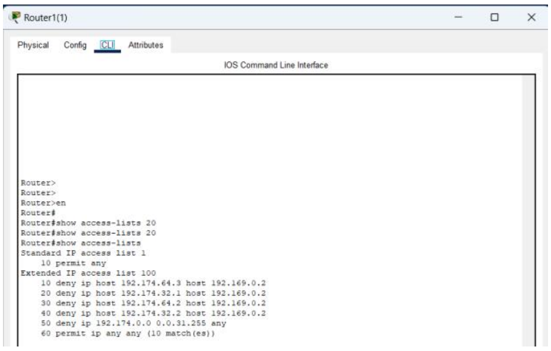
5. Access Control Lists (ACLs)

To secure access to the Web Server, the following ACLs were configured:

Denied access from:

One PC in Network A, One Laptop in Network E, Smart Phone in Network B, All devices in Network D

ACLs were applied inbound on the router connected to the Web Server. The access-list on the router connected to the HTTP server is shown below :

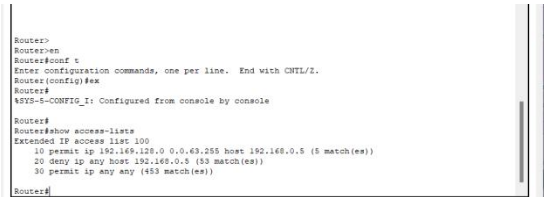


```
Router>
Router>
Router>en
Router#
Router#show access-lists 20
Router#show access-lists 20
Router#show access-lists
Standard IP access list 1
    10 permit any
Extended IP access list 100
    10 deny ip host 192.174.64.3 host 192.169.0.2
    20 deny ip host 192.174.32.1 host 192.169.0.2
    30 deny ip host 192.174.64.2 host 192.169.0.2
    40 deny ip host 192.174.32.2 host 192.169.0.2
    50 deny ip 192.174.0.0 0.0.31.255 any
    60 permit ip any any (10 match(es))
```

6. FTP and Mail Configuration

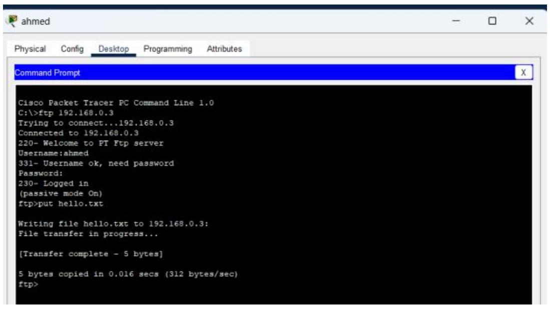
FTP Server: Configured to only allow access and file uploads from devices in Network G. The access-list on the router connected to FTP server and a successful file upload from a host in Network G is shown below :

- **Access-list :**



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

Router#
Router#show access-lists
Extended IP access list 100
    10 permit ip 192.169.128.0 0.0.63.255 host 192.168.0.5 (5 match(es))
    20 deny ip any host 192.168.0.5 (53 match(es))
    30 permit ip any any (453 match(es))

Router#
```

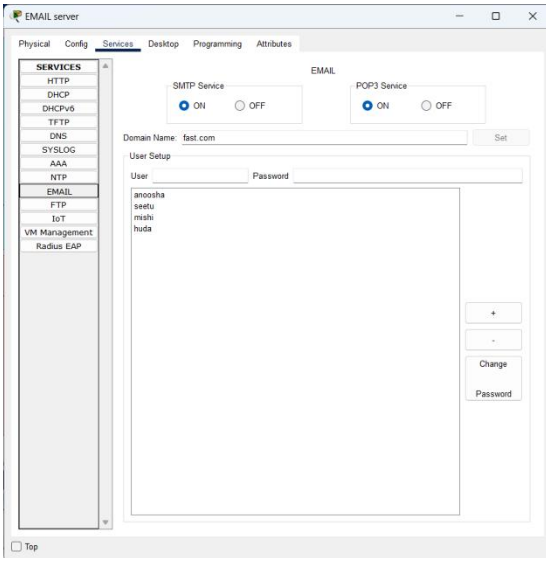
- **Writing File :**



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.0.3
Trying to connect...192.168.0.3
Connected to 192.168.0.3
220- Welcome to PT Ftp server
Username:ahmed
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put hello.txt

Writing file hello.txt to 192.168.0.3:
File transfer in progress...

[Transfer complete - 5 bytes]

5 bytes copied in 0.016 secs (312 bytes/sec)
ftp>
```

Mail Server: The DNS server was also configured for the hosts to be able to access the mail server. Only devices in Network H and Network I were configured with email client settings to exchange emails.

- **Mail Server :**



EMAIL

SMTP Service: ● ON ○ OFF

POP3 Service: ● ON ○ OFF

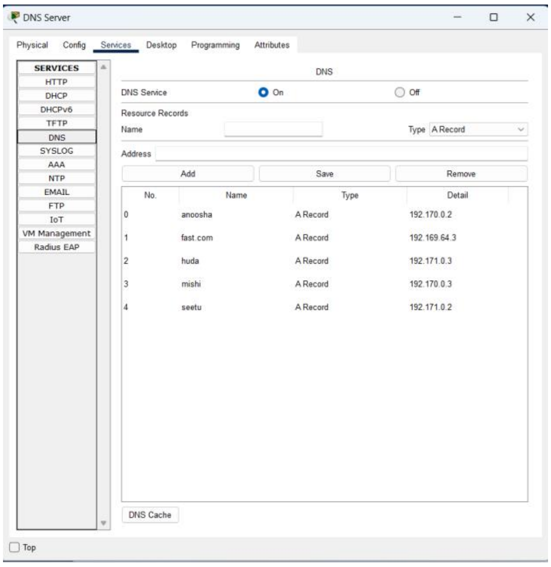
Domain Name: fast.com

User Setup

User | Password

anoosha
seetu
mishi
huda

- **DNS Server :**



DNS

DNS Service ● On ○ Off

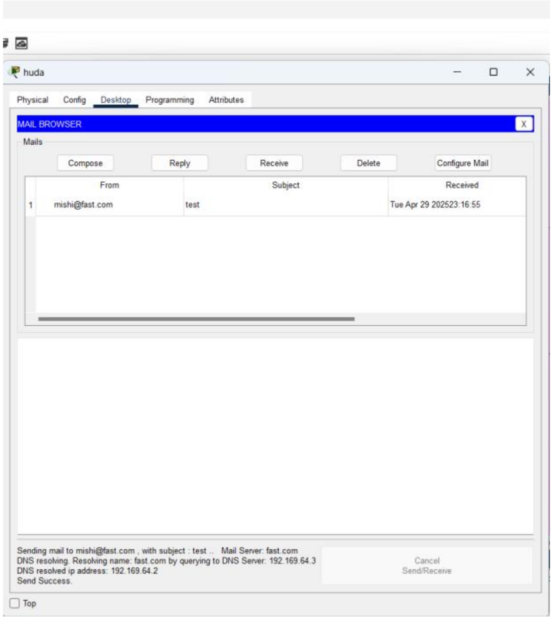
Resource Records

Name | Type: A Record

Address

No.	Name	Type	Detail
0	anoosha	A Record	192.170.0.2
1	fast.com	A Record	192.169.64.3
2	huda	A Record	192.171.0.3
3	mishi	A Record	192.170.0.3
4	seetu	A Record	192.171.0.2

- **Sending Mail :**



	From	Subject	Received
1	mishi@fast.com	test	Tue Apr 29 202523:16:55

```
Sending mail to mishi@fast.com , with subject : test ..  Mail Server: fast.com
DNS resolving. Resolving name: fast.com by querying to DNS Server: 192.169.64.3
DNS resolved ip address: 192.169.64.2
Send Success.
```

7. Device Configuration

Each router and switch was configured with:

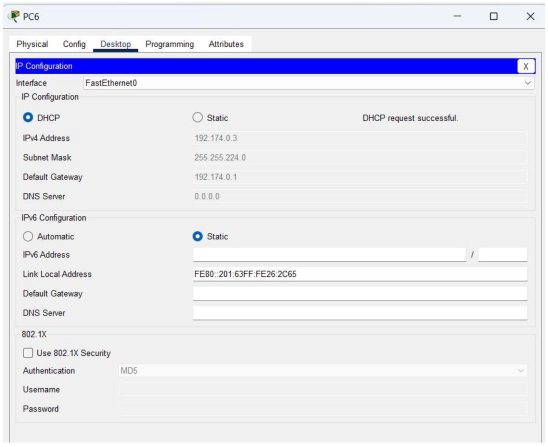
- Appropriate interface IPs
- Routing settings
- DHCP relay (ip helper-address) where required
- NAT and ACL rules
- Service configurations (FTP, HTTP, Mail)

Relevant Observations and Results

During the simulation and testing of the network, several observations were made that confirmed the correct implementation and functionality of the design:

1. Successful IP Assignment via DHCP

- All end devices across EIGRP, RIP, and OSPF areas successfully received IP addresses from the central DHCP server in Block D.
- IP address allocation matched the subnet ranges configured using VLSM.



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address	192.174.0.3
Subnet Mask	255.255.224.0
Default Gateway	192.174.0.1
DNS Server	0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address	/
Link Local Address	FE80::201:63FF:FE26:2C65
Default Gateway	
DNS Server	

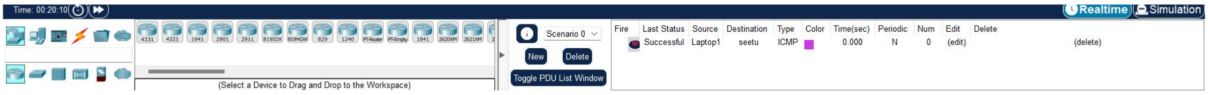
802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	

2. End-to-End Connectivity

- Devices across different networks and blocks were able to ping each other successfully after proper routing and redistribution.
- Inter-block communication confirmed that routing protocols and redistribution were correctly configured.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	Laptop1	seetu	ICMP	🟪	0.000	N	0	(edit)	(delete)

3. NAT Functionality

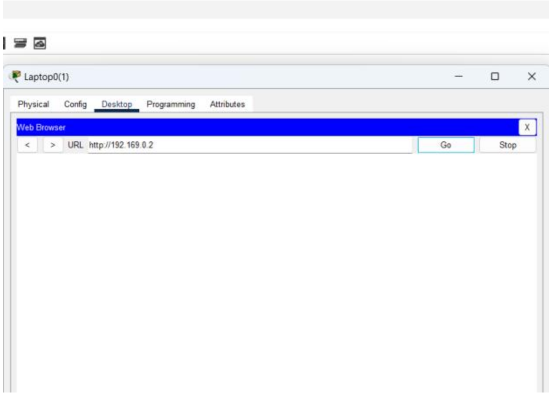
- Devices behind Router in Network F and Router21 Network K could access external services via NAT, using the public IP.
- NAT translations were verified through the **show ip nat translations** command on the routers.

4. Access Control Lists

The configured ACLs correctly blocked access to the Web Server from:

- A specific PC in Network A
- A specific Laptop in Network E
- A Smartphone in Network B
- All hosts in Network D

PC in Network A showed the following upon accessing web server **failed** :

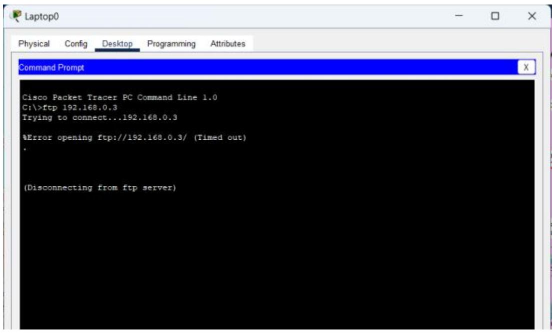


URL http://192.169.0.2

All other devices could access the Web Server as expected, validating precise ACL configuration.

Only the devices in **Network G** could connect to and upload files to the FTP Server. Devices from other networks were denied access, demonstrating correct ACL and FTP configuration.

A PC in Network J upon accessing the FTP server **failed**:



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.0.3
Trying to connect...192.168.0.3

%Error opening ftp://192.168.0.3/ (Timed out)
.



(Disconnecting from ftp server)
```

5. Mail Server Functionality

- Devices in Network H and Network I were able to send and receive emails from each other.
- Other networks could not access the mail server, confirming correct restrictions.

6. Service Availability

- The Web, Mail, and FTP servers responded appropriately when accessed from authorized networks.
- Testing via web browsers and FTP clients in Cisco Packet Tracer showed successful connections.

7. Performance

- Network performance remained stable and efficient even with large subnets (e.g., Network G with /14).
- No IP conflicts or broadcast issues occurred due to correct subnetting and DHCP management.

Conclusion

This project provided a hands-on understanding of designing and implementing a complex computer network using Cisco Packet Tracer. By configuring IP addressing with VLSM, applying routing protocols like RIP, OSPF, and EIGRP, and managing inter-protocol communication through redistribution, we simulated a real-world scalable network. The integration of DHCP, NAT, ACLs, and server configurations (FTP, Mail, HTTP) further enhanced our practical networking skills. Overall, this project deepened our knowledge of enterprise-level network planning, implementation, and security enforcement, making us better equipped to tackle professional networking challenges.