# Computer Networks

## Final Project Report

Anas Bin Rashid
22I-0907 CS-5A

# Table of Contents

# OBJECTIVE

The objective of this project was to design and implement a complex enterprise network topology using Cisco Packet Tracer. The project aimed to demonstrate the integration of various network protocols and technologies, including RIP, DHCP, NAT, ACL, and VPN. The goal was to ensure seamless connectivity, security, and efficient resource management across different network sections.

# NETWORK ZONES OVERVIEW

## 1. Access Zone

This zone serves as the entry point for end-user devices like PCs, laptops, and servers. It provides dynamic IP addresses through DHCP and ensures secure, controlled access to network resources.

### Key Features

- **DHCP Server:** Configured to assign IPs dynamically to devices in this zone.
- **Security:** ACLs restrict unauthorized access to the Core Operations and Distribution Zones.
- **VPN:** A VPN tunnel between Router 1 and Router 8 provides secure communication between the Core Operations and Distribution Zones

## 2. Core Operations Zone

This zone acts as the backbone of the enterprise network, interconnecting the Access and Distribution Zones. EIGRP is implemented for efficient routing, and redundancy ensures minimal downtime.

### Key Features

- **EIGRP Routing:** Provides dynamic and efficient routing for interconnectivity.
- **VPN Tunnel:** Configured between Router 1 and Router 8 for secure communication.

- **DHCP Server:** Configured to assign IPs dynamically to devices in this zone.
- **NAT Configuration:** Translates private IP addresses to public IPs for internet access.

### 3. Distribution Zone

This zone connects remote branches and other departments to the Core Operations Zone using OSPF. It also includes a secure VPN connection between remote routers.

### Key Features

- **OSPF Routing:** Ensures link-state-based dynamic routing for scalability.
- **DHCP Server:** Configured to assign IPs dynamically to devices in this zone.
- **NAT Configuration:** Translates private IP addresses to public IPs for internet access.
- **ACL:** Ensures access restrictions for local devices.

# TECHNOLOGIES USED

## *Cisco Packet Tracer*

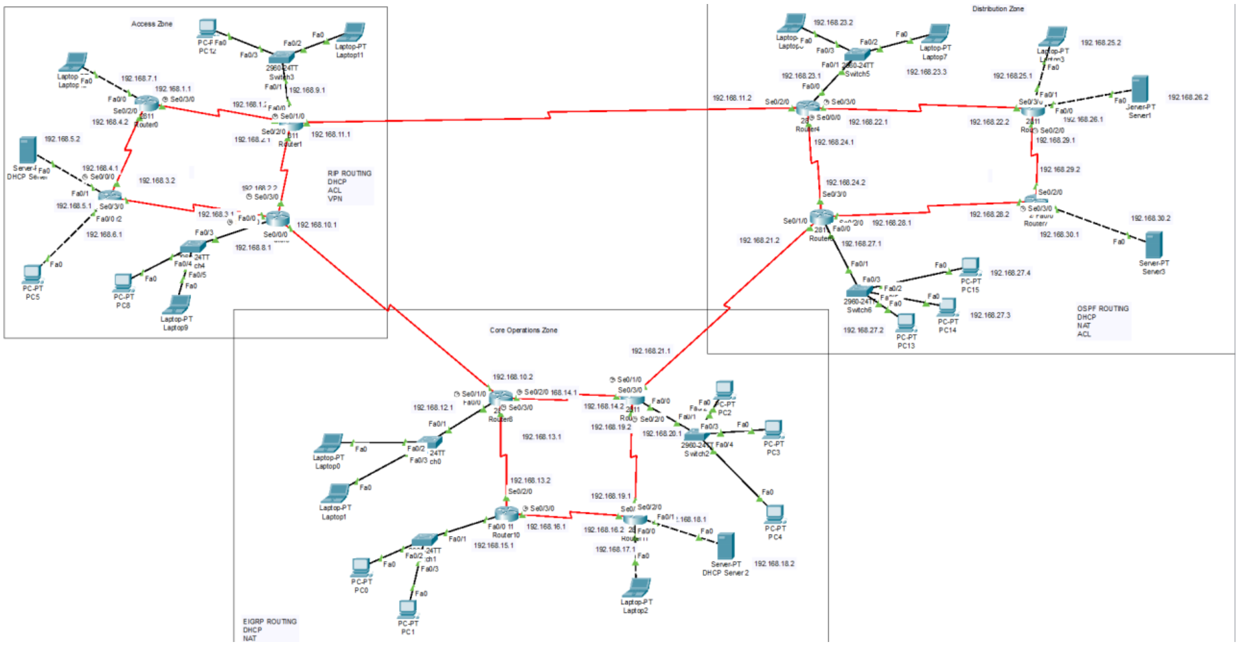
# CISCO USAGE

Cisco Packet Tracer was utilized to design, simulate, and implement the enterprise network. It provided a virtual environment for creating and configuring devices like routers, switches, and servers while testing their functionality. Key applications included:

- ***Network Design***: Created a logical topology with clusters for operations, access, and distribution zones.
- ***Dynamic Routing*** (EIGRP): Configured routers for efficient routing and verified using commands like *show ip eigrp neighbors*.

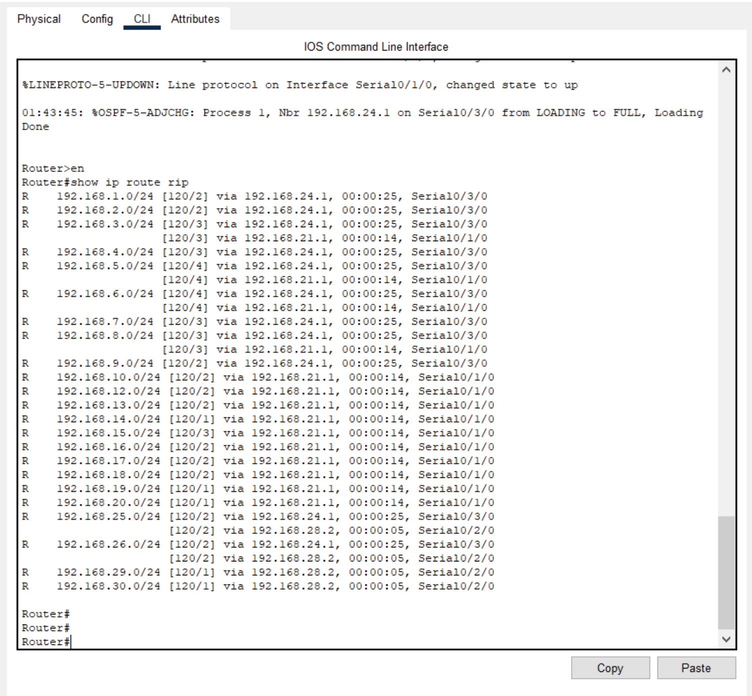
- ***NAT Implementation***: Enabled secure communication between private and public networks through dynamic IP translation.
- ***DHCP Configuration***: Automated IP assignment to devices.
- ***ACL Application***: Enforced security by filtering traffic and blocking unauthorized access.
- ***End-to-End Testing***: Validated communication, security, and routing efficiency using Packet Tracer's simulation tools. This ensured a scalable, secure, and functional network design.

# TOPOLOGY



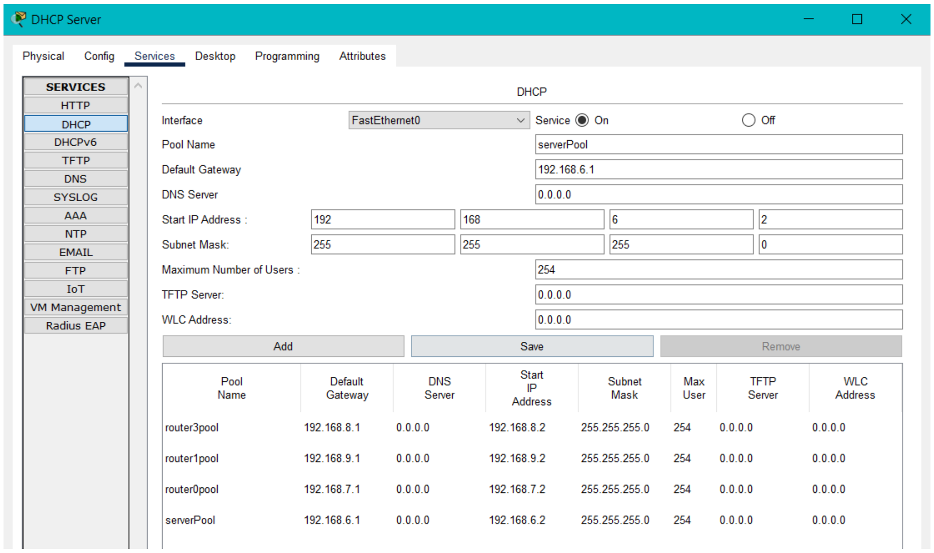
# CONFIGURATION, RESULTS & TESTING

## 1. RIP



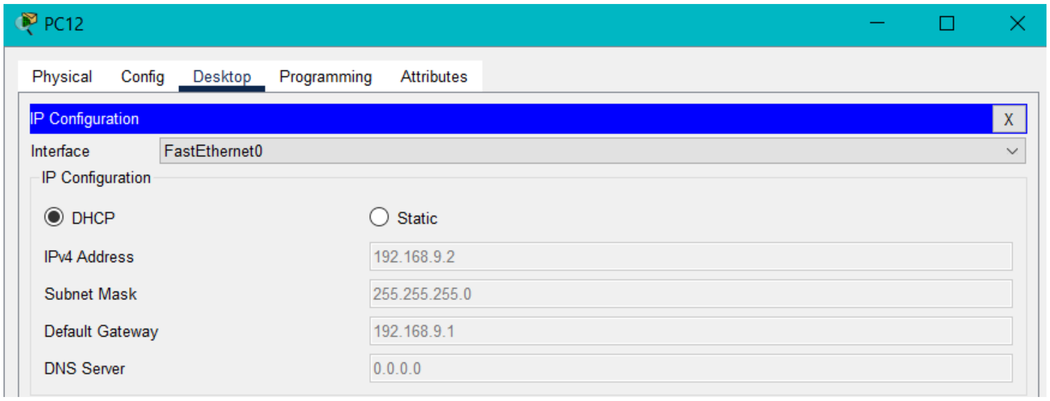
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

01:43:45: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.24.1 on Serial0/3/0 from LOADING to FULL, Loading
Done


Router>en
Router#show ip route rip
R    192.168.1.0/24 [120/2] via 192.168.24.1, 00:00:25, Serial0/3/0
R    192.168.2.0/24 [120/2] via 192.168.24.1, 00:00:25, Serial0/3/0
R    192.168.3.0/24 [120/3] via 192.168.24.1, 00:00:25, Serial0/3/0
                    [120/3] via 192.168.21.1, 00:00:14, Serial0/1/0
R    192.168.4.0/24 [120/3] via 192.168.24.1, 00:00:25, Serial0/3/0
R    192.168.5.0/24 [120/4] via 192.168.24.1, 00:00:25, Serial0/3/0
                    [120/4] via 192.168.21.1, 00:00:14, Serial0/1/0
R    192.168.6.0/24 [120/4] via 192.168.24.1, 00:00:25, Serial0/3/0
                    [120/4] via 192.168.21.1, 00:00:14, Serial0/1/0
R    192.168.7.0/24 [120/3] via 192.168.24.1, 00:00:25, Serial0/3/0
R    192.168.8.0/24 [120/3] via 192.168.24.1, 00:00:25, Serial0/3/0
                    [120/3] via 192.168.21.1, 00:00:14, Serial0/1/0
R    192.168.9.0/24 [120/2] via 192.168.24.1, 00:00:25, Serial0/3/0
R    192.168.10.0/24 [120/2] via 192.168.21.1, 00:00:14, Serial0/1/0
R    192.168.12.0/24 [120/2] via 192.168.21.1, 00:00:14, Serial0/1/0
R    192.168.13.0/24 [120/2] via 192.168.21.1, 00:00:14, Serial0/1/0
R    192.168.14.0/24 [120/1] via 192.168.21.1, 00:00:14, Serial0/1/0
R    192.168.15.0/24 [120/3] via 192.168.21.1, 00:00:14, Serial0/1/0
R    192.168.16.0/24 [120/2] via 192.168.21.1, 00:00:14, Serial0/1/0
R    192.168.17.0/24 [120/2] via 192.168.21.1, 00:00:14, Serial0/1/0
R    192.168.18.0/24 [120/2] via 192.168.21.1, 00:00:14, Serial0/1/0
R    192.168.19.0/24 [120/1] via 192.168.21.1, 00:00:14, Serial0/1/0
R    192.168.20.0/24 [120/1] via 192.168.21.1, 00:00:14, Serial0/1/0
R    192.168.25.0/24 [120/2] via 192.168.24.1, 00:00:25, Serial0/3/0
                     [120/2] via 192.168.28.2, 00:00:05, Serial0/2/0
R    192.168.26.0/24 [120/2] via 192.168.24.1, 00:00:25, Serial0/3/0
                     [120/2] via 192.168.28.2, 00:00:05, Serial0/2/0
R    192.168.29.0/24 [120/1] via 192.168.28.2, 00:00:05, Serial0/2/0
R    192.168.30.0/24 [120/1] via 192.168.28.2, 00:00:05, Serial0/2/0

Router#
Router#
Router#
```

## 2. DHCP



| | | | | |
|---|---|---|---|---|
| Interface | FastEthernet0 | Service ● On | ○ Off | |
| Pool Name | serverPool | | | |
| Default Gateway | 192.168.6.1 | | | |
| DNS Server | 0.0.0.0 | | | |
| Start IP Address : | 192 | 168 | 6 | 2 |
| Subnet Mask: | 255 | 255 | 255 | 0 |
| Maximum Number of Users : | 254 | | | |
| 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 |
|---|---|---|---|---|---|---|---|
| router3pool | 192.168.8.1 | 0.0.0.0 | 192.168.8.2 | 255.255.255.0 | 254 | 0.0.0.0 | 0.0.0.0 |
| router1pool | 192.168.9.1 | 0.0.0.0 | 192.168.9.2 | 255.255.255.0 | 254 | 0.0.0.0 | 0.0.0.0 |
| router0pool | 192.168.7.1 | 0.0.0.0 | 192.168.7.2 | 255.255.255.0 | 254 | 0.0.0.0 | 0.0.0.0 |
| serverPool | 192.168.6.1 | 0.0.0.0 | 192.168.6.2 | 255.255.255.0 | 254 | 0.0.0.0 | 0.0.0.0 |



Interface FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address 192.168.9.2

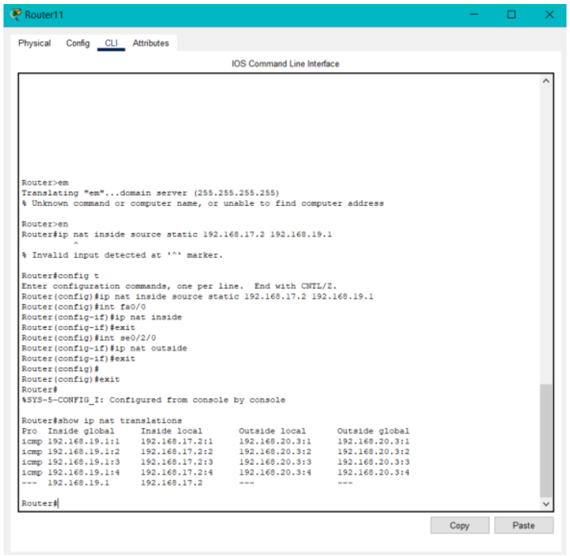
Subnet Mask 255.255.255.0

Default Gateway 192.168.9.1

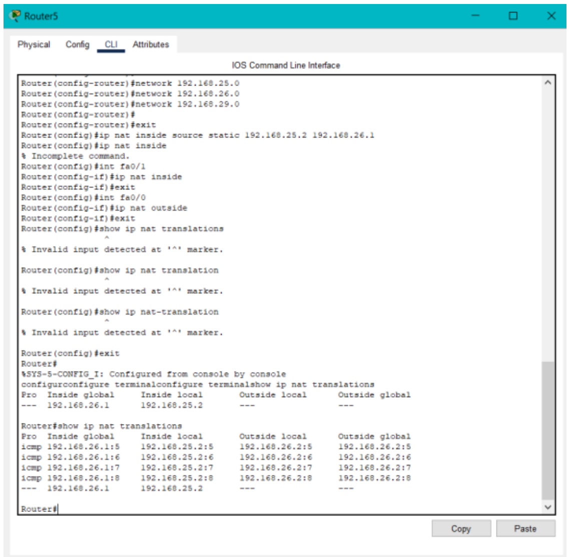
DNS Server 0.0.0.0

## 3. NAT

For NAT, the following image shows, this was done in the area 3 the right upmost with router 5 as shown below.



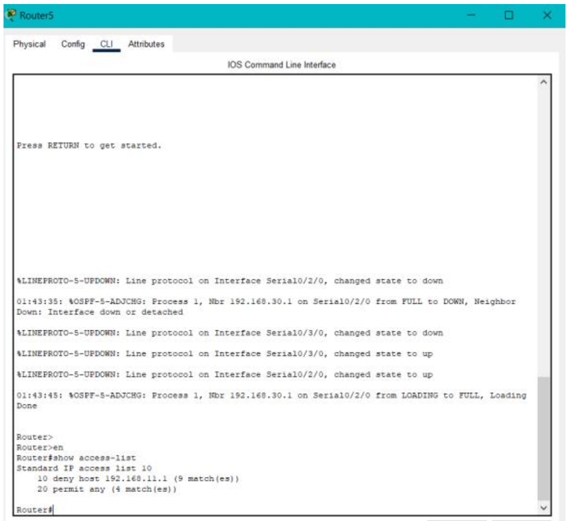
```
Router>em
Translating "em"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

Router>en
Router#ip nat inside source static 192.168.17.2 192.168.19.1
          ^
% Invalid input detected at '^' marker.

Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip nat inside source static 192.168.17.2 192.168.19.1
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int se0/2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 192.168.19.1:1    192.168.17.2:1     192.168.20.3:1     192.168.20.3:1
icmp 192.168.19.1:2    192.168.17.2:2     192.168.20.3:2     192.168.20.3:2
icmp 192.168.19.1:3    192.168.17.2:3     192.168.20.3:3     192.168.20.3:3
icmp 192.168.19.1:4    192.168.17.2:4     192.168.20.3:4     192.168.20.3:4
---  192.168.19.1      192.168.17.2       ---                ---

Router#
```



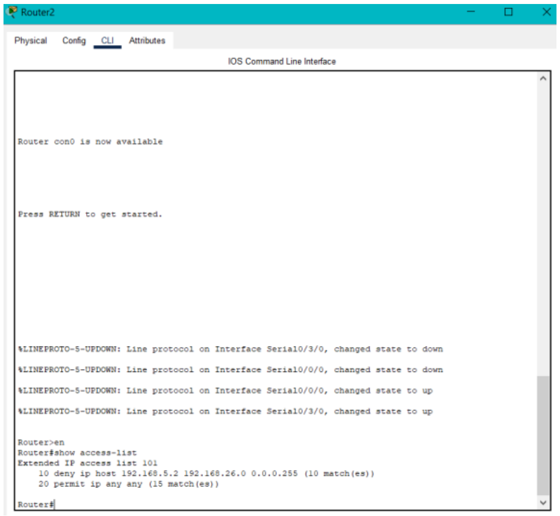
```
Router(config-router)#network 192.168.25.0
Router(config-router)#network 192.168.26.0
Router(config-router)#network 192.168.29.0
Router(config-router)#
Router(config-router)#exit
Router(config)#ip nat inside source static 192.168.25.2 192.168.26.1
Router(config)#ip nat inside
% Incomplete command.
Router(config)#int fa0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int fa0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#show ip nat translations
                ^
% Invalid input detected at '^' marker.

Router(config)#show ip nat translation
                ^
% Invalid input detected at '^' marker.

Router(config)#show ip nat-translation
                ^
% Invalid input detected at '^' marker.

Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
configurconfigure terminalconfigure terminalshow ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  192.168.26.1      192.168.25.2       ---                ---

Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 192.168.26.1:5    192.168.25.2:5     192.168.26.2:5     192.168.26.2:5
icmp 192.168.26.1:6    192.168.25.2:6     192.168.26.2:6     192.168.26.2:6
icmp 192.168.26.1:7    192.168.25.2:7     192.168.26.2:7     192.168.26.2:7
icmp 192.168.26.1:8    192.168.25.2:8     192.168.26.2:8     192.168.26.2:8
---  192.168.26.1      192.168.25.2       ---                ---

Router#
```

## 4. ACL

The ACL has been implemented on the server of router 7. It cannot send or receive a message from the servers of another area, but its corresponding pc's can as well as it can send a packet to server.



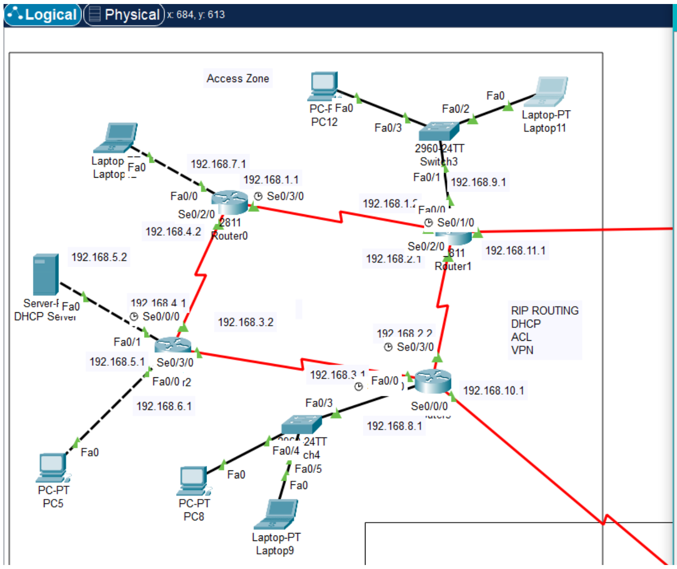
```
Press RETURN to get started.




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

01:43:35: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on Serial0/2/0 from FULL to DOWN, Neighbor
Down: Interface down or detached

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

%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

01:43:45: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on Serial0/2/0 from LOADING to FULL, Loading
Done


Router>
Router>en
Router#show access-list
Standard IP access list 10
    10 deny host 192.168.11.1 (9 match(es))
    20 permit any (4 match(es))

Router#
```

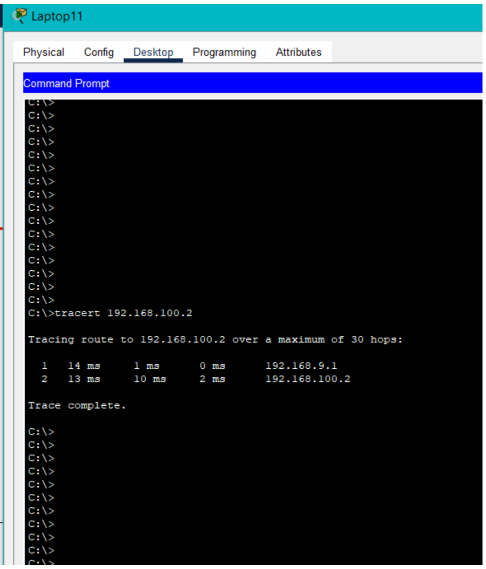


```
Router con0 is now available



Press RETURN to get started.




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

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

%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


Router>en
Router#show access-list
Extended IP access list 101
    10 deny ip host 192.168.5.2 192.168.26.0 0.0.0.255 (10 match(es))
    20 permit ip any any (15 match(es))

Router#
```

## 5. VPN

The VPN tunnel has been implemented between Router 1 and Router 8.





```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>tracert 192.168.100.2

Tracing route to 192.168.100.2 over a maximum of 30 hops:

  1   14 ms     1 ms      0 ms      192.168.9.1
  2   13 ms     10 ms     2 ms      192.168.100.2

Trace complete.

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```

## MAJOR COMMANDS USED

1. *RIP: router rip <address>*
2. *DHCP: ip helper-address <address>*
3. *ACL: access-list 100 deny ip host <address> <address> <wildcardmask>*
4. *NAT: ip nat inside source static*
5. *VPN: tunnel source <interface>, tunnel destination <address>*

# CHALLENGES & LEARNING

## CHALLENGES FACED

- Configuration Errors: Initial misconfigurations in DHCP, NAT, and ACL settings led to communication failures between devices, requiring careful debugging and testing.
- RIP Routing Loops: In early stages, improper RIP configuration caused routing loops, resulting in inefficient data flow and delays in network convergence.
- Access Control Lists : Crafting effective ACL rules was challenging, as overly restrictive rules initially blocked legitimate traffic.
- NAT Complexity: Understanding and implementing NAT for bidirectional communication between private and public networks was complex and required thorough testing.
- Device Interconnections: Ensuring all devices were properly connected in the topology while avoiding redundancy or inefficiencies was time-consuming.

## LESSONS LEARNED

- Thorough Planning: Proper network design and planning are critical before implementation to minimize errors during configuration.
- Protocol Understanding: Deep understanding of protocols like DHCP, RIP, NAT, and ACL is essential for efficient implementation and troubleshooting.
- Troubleshooting Skills: Learned the importance of methodical troubleshooting using tools like Packet Tracer's simulation and real-time monitoring features.
- Configuration Documentation: Maintaining detailed documentation of configurations helps in revisiting and resolving issues efficiently.
- Patience and Precision: Network design requires attention to detail and patience, as small errors can significantly impact functionality.

This project provided hands-on experience with networking protocols, enhanced problem-solving skills, and emphasized the importance of systematic configuration and testing.

# CONCLUSION

This project successfully demonstrated the design and implementation of a functional and scalable network using Cisco Packet Tracer. By incorporating DHCP for dynamic IP allocation, efficient routing, NAT for enabling communication between private and public networks, and ACL for traffic filtering, the network achieved its intended objectives. The topology was tested thoroughly, ensuring proper connectivity, data flow, and adherence to security policies.

## OUTCOMES

- A fully operational network that automates key processes such as IP assignment and routing.
- Enhanced understanding of networking protocols and their practical applications.
- Successful implementation of NAT and ACL to address real-world requirements like internet access and security.

## FUTURE RECOMMENDATIONS

1. **Scalability Testing**: Expand the network to include more devices and subnets to test scalability and performance under higher traffic loads.

2. **Security Enhancements**: Implement additional security measures, such as firewalls, to further protect the network from external threats.