**EASTERN INTERNATIONAL UNIVERSITY**

**SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY**

**DEPARTMENT OF COMPUTER NETWORKS AND DATA COMMUNICATIONS**



**PROJECT**

**LOAD BALANCING, MULTIPATH ROUTING, AND PACKET FILTERING TECHNIQUES**

**Students**

PHAM NGUYEN BAO TRANG-2131220034

NGUYEN VU PHUONG TRANG-2131220008

HA QUANG MINH-1931220012

**Supervisor**

DR. PHAN VAN VINH

**Binh Duong, December, 2024**

Abstract

This project focuses on the implementation of OSPF and EIGRP routing protocols in enterprise networks, highlighting their individual strengths in improving network resilience and performance. OSPF’s multipath backup feature is utilized to enhance network redundancy, while EIGRP’s load balancing capabilities are employed to optimize traffic distribution across multiple paths. The configurations are implemented on real Cisco devices to ensure a practical and scalable solution for real-world enterprise networks.

By using OSPF multipath backup, the network ensures high availability through multiple equal-cost paths, providing an effective failover mechanism in case of link failures. EIGRP, on the other hand, offers efficient load balancing, distributing traffic evenly across available links to prevent congestion and improve overall network performance.

In addition, the project incorporates NAT (Network Address Translation) and packet filtering to secure the network and manage external connections effectively. These configurations contribute to a secure, efficient, and fault-tolerant network infrastructure.

In conclusion, this project demonstrates how OSPF and EIGRP can independently enhance network reliability, performance, and security in enterprise environments. The result is a robust network solution that ensures both network redundancy and optimal resource utilization.

Acknowledgement

We would like to express our sincere gratitude to Dr. Phan Van Vinh, a lecturer at the Department of Computer Networking at Eastern International University, for his continuous support and guidance throughout the course of this project. His expert advice and encouragement were essential in helping us understand and implement the OSPF and EIGRP protocols for optimizing network performance and redundancy. His assistance in navigating complex configurations, including multipath backup, load balancing, NAT, and packet filtering, was invaluable. We are truly grateful for his time, dedication, and commitment to our academic and professional development.

**Table of contents**

**LIST OF FIGURES**

[Figure 1. Packet Filtering Firewalls and the OSI Reference Mdel 13](#_heading=h.2jxsxqh)

[Figure 2. Packet-Filtering Firewall Example 13](#_heading=h.z337ya)

[Figure 3. Stateful Firewalls and the OSI Reference Model 14](#_heading=h.3j2qqm3)

[Figure 4. Packet-Filtering Firewall Example?Initiating Connections 14](#_heading=h.1y810tw)

[Figure 5. Application Gateway Firewalls and the OSI Reference Model 14](#_heading=h.4i7ojhp)

[Figure 6. Application Gateway Firewalls Authentication Process 15](#_heading=h.2xcytpi)

[Figure 7. Address-translation firewalls model 15](#_heading=h.1ci93xb)

[Figure 8. NAT firewall process 15](#_heading=h.3whwml4)

[Figure 9. Personal Firewall model 15](#_heading=h.2bn6wsx)

[Figure 10. Host firewall process 16](#_heading=h.qsh70q)

[Figure 11. Hybrid firewalls model 16](#_heading=h.3as4poj)

[Figure 12. Firewall categories 17](#_heading=h.1pxezwc)

[Figure 13. Example of a firewall (pfsense) with orther devices 18](#_heading=h.23ckvvd)

[Figure 14. Download pfSense Installer 20](#_heading=h.1hmsyys)

[Figure 15. pfSense console interface 20](#_heading=h.41mghml)

[Figure 16. Copyright and distribution notice 20](#_heading=h.2grqrue)

[Figure 17. Install option 21](#_heading=h.vx1227)

[Figure 18. Disk partitioning 21](#_heading=h.3fwokq0)

[Figure 19. Fetching distribution 21](#_heading=h.1v1yuxt)

[Figure 20. Reboot notice 22](#_heading=h.4f1mdlm)

[Figure 21. pfSense Console Menu 22](#_heading=h.2u6wntf)

[Figure 22. pfSense login interface 22](#_heading=h.19c6y18)

[Figure 23. pfSense Wizard interface 23](#_heading=h.3tbugp1)

[Figure 24. General information menu 23](#_heading=h.28h4qwu)

[Figure 25. Time Server information menu 24](#_heading=h.nmf14n)

[Figure 26. WAN interface configuration 24](#_heading=h.37m2jsg)

[Figure 27. Successful configuration 24](#_heading=h.1mrcu09)

[Figure 28. pfSense dashboard interface 25](#_heading=h.46r0co2)

[Figure 29. pfSense interface assignments 26](#_heading=h.3l18frh)

[Figure 30. Example of setting up a rule 27](#_heading=h.4k668n3)

[Figure 31. Creating the firewall rules in pfSense 28](#_heading=h.2zbgiuw)

[Figure 32. Examples of successful configuration of captive portal 29](#_heading=h.3ygebqi)

[Figure 33. Example of configuraion of OpenVPN 30](#_heading=h.sqyw64)

[Figure 34. Example of installation of IPSec in pfSense 31](#_heading=h.3cqmetx)

[Figure 35. Example of installation of L2TP in pfSense 31](#_heading=h.1rvwp1q)

[Figure 36. Example of configuration of L2TP in pfSense 32](#_heading=h.2r0uhxc)

[Figure 37. Example of pfblockerng package 34](#_heading=h.3q5sasy)

[Figure 38. Example of Configuration pfblockerNG 35](#_heading=h.25b2l0r)

[Figure 39. Example of General Settings of pfBlockerNG 35](#_heading=h.kgcv8k)

[Figure 40. Example of General Settings of IP FILTERING 36](#_heading=h.34g0dwd)

[Figure 41. Example of General Settings of DNSBL 37](#_heading=h.43ky6rz)

[Figure 42. Example of Configuration DNSBL 37](#_heading=h.3hv69ve)

[Figure 43. Example of Blacklist 39](#_heading=h.1x0gk37)

[Figure 44. Example of Whitelist 39](#_heading=h.4h042r0)

[Figure 45. An example of setting rules to block traffic from LAN 40](#_heading=h.3vac5uf)

[Figure 46. Example of blocked accessing to a specific website. 41](#_heading=h.2afmg28)

[Figure 47. Example of captive portal for Wifi service 41](#_heading=h.39kk8xu)

[Figure 48. Example of VPN service 42](#_heading=h.48pi1tg)

[Figure 49. Example of Snort deployment 43](#_heading=h.1302m92)

[Figure 50. Example of Blocking a website 43](#_heading=h.2250f4o)

[Figure 51. Example of IP Blocking configuration 44](#_heading=h.haapch)

[Figure 52. Example of Whilelisting configuration 44](#_heading=h.319y80a)

[Figure 53. Example of AdBlock configuration 44](#_heading=h.1gf8i83)

LIST OF ABBREVIATIONS

| **Abbreviation** | **Full word** |
| --- | --- |
| ASN | Autonomous System Number |
| BGP | Border Gateway Protocol |
| CIDR | Classless Inter-Domain Routing |
| CPU | Central Processing Unit |
| DHCP | Dynamic Host Configuration Protocol |
| DMZ | Demilitarized Zone |
| DNS | Domain Name System |
| DNSBL | Domain Name System-based Blackhole List |
| GUI | Graphical User Interface |
| HA | High Availability |
| HDD | Hard Disk Drive |
| ICMP | Internet Control Message Protocol |
| IDS | Intrusion Detection System |
| IP | Internet Protocol address |
| IPS | Intrusion Prevention System |
| ISP | Internet Service Provider |
| IT | Information Technology |
| L2TP | Layer Two Tunneling Protocol |
| LAN | Local Area Network |
| NAT | Network Address Translation |
| NGFW | Next-Generation Firewall |
| OSI | Open Systems Interconnection |
| OSPF | Open Shortest Path First protocol |
| PC | Personal Computer |
| PPTP | Point-to-Point Tunneling Protocol |
| QoS | Quality of Service |
| RAM | Random-Access Memory |
| SSD | Solid State Drive |
| TLD | Top-Level Domain |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |

# CHAPTER 1. INTRODUCTION

## Motivation

In modern networking, ensuring efficient traffic distribution, optimal routing paths, and robust security is crucial for maintaining high performance and reliability. Our project, titled *"Load Balancing, Multipath Routing, and Packet Filtering Techniques,"* aims to address these requirements through the implementation of advanced networking techniques. The motivation for this project stems from several key factors:

* **Efficient Resource Utilization:** Load balancing ensures that network traffic is evenly distributed across available paths, preventing any single resource from becoming a bottleneck. This improves overall network performance and reliability.
* **Enhanced Redundancy and Fault Tolerance:** Multipath routing provides backup routes, ensuring network continuity even in the event of link failures. This is particularly vital for mission-critical applications that require uninterrupted connectivity.
* **Cost-Effectiveness:** By utilizing dynamic routing protocols like OSPF and EIGRP and implementing NAT, we can maximize existing network infrastructure without significant additional investment.
* **Improved Security:** Packet filtering enhances network security by blocking access to unauthorized or harmful websites, protecting sensitive data and resources.
* **Real-World Applications:** These techniques are widely used in enterprise networks to meet demands for scalability, security, and performance. Mastery of these methods provides valuable skills applicable to various networking roles.

In an era where organizations heavily rely on interconnected systems, understanding and implementing such networking techniques are vital for maintaining robust, efficient, and secure infrastructures.

## Project Objectives

The primary objectives of this project are as follows:

1. **Develop Expertise in Routing Protocols:** Implement and analyze OSPF and EIGRP for efficient routing in enterprise networks.
2. **Configure Load Balancing:** Set up mechanisms to distribute traffic across multiple paths, enhancing network performance and reducing latency.
3. **Establish Multipath Backup:** Ensure network resilience by configuring redundant paths that activate in case of link failures.
4. **Implement NAT:** Enable internal devices to access external networks securely while conserving public IP addresses.
5. **Apply Packet Filtering:** Demonstrate security features by blocking access to specific websites and monitoring traffic flow.

## Organization of the project

The project is structured as follows:

* Chapter 1: Introduction
* Chapter 2: Load Balancing and Multipath Routing
* Chapter 3: NAT and Packet Filtering Techniques
* Chapter 4: Results of implementation
* Chapter 5: Conclusion

Through this project, we aim to provide a practical demonstration of integrating advanced networking techniques into a cohesive and functional model, showcasing their impact on network performance, security, and reliability.

# CHAPTER 2. LOAD BALANCING AND MULTIPATH ROUTING

## 2.1 Introduction to Unequal-Cost Load Balancing with EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing protocol that enables routers to share information and calculate the best path to network destinations. Unlike other routing protocols, EIGRP supports unequal-cost load balancing, allowing traffic distribution across multiple paths with different metrics. This feature provides greater flexibility in network traffic management and ensures optimal use of available bandwidth.

### 2.1.1 What is Load Balancing?

Load balancing is the capability of a router to distribute traffic over all the router network ports that are the same distance from the destination address. Load balancing increases the utilization of network segments, and so increases effective network bandwidth. There are two types of load balancing:

* Equal cost path – Applicable when different paths to a destination network report the same routing metric value. The **maximum-paths** command determines the maximum number of routes that the routing protocol can use.
* Unequal cost path – Applicable when different paths to a destination network report are of different routing metric values. The **variance** command determines which of these routes is used by the router.

### 2.1.2 How does Unequal Cost Path Load Balancing (Variance) work in EIGRP?

Every routing protocol supports equal cost path load balancing. In addition, Interior Gateway Routing Protocol (IGRP) and EIGRP also support unequal cost path load balancing. Use the variance n command in order to instruct the router to include routes with a metric of less than n times the minimum metric route for that destination. The variable n can take a value between 1 and 128. The default is 1, which means equal cost load balancing. Traffic is also distributed among the links with unequal costs, proportionately, with respect to the metric.

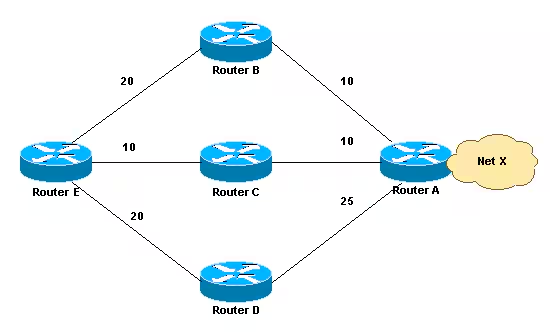


Figure 1. Network Diagram

**Variance**

This section provides an example. In the network diagram, there are three ways to get to Network X:

E-B-A with a metric of 30

E-C-A with a metric of 20

E-D-A with a metric of 45

Router E chooses the path E-C-A with a metric of 20 because 20 is better than 30 and 45. In order to instruct EIGRP to select the path E-B-A as well, configure variance with a multiplier of 2:

router eigrp 1

network x.x.x.x

variance 2

This configuration increases the minimum metric to 40 (2 \* 20 = 40). EIGRP includes all routes that have a metric of less than or equal to 40 and satisfy the feasibility condition. In the configuration in this section, EIGRP now uses two paths to get to Network X, E-C-A and E-B-A, because both paths have a metric of under 40. EIGRP does not use path E-D-A because that path has a metric of 45, which is not less than the value of the minimum metric of 40, because of the variance configuration. Also, the reported distance of neighbor D is 25, which is greater than the feasible distance (FD) of 20 through C. This means that, even if variance is set to 3, the E-D-A path is not selected for load balancing because Router D is not a feasible successor.

**Traffic Sharing**

EIGRP not only provides unequal cost path load balancing, but also intelligent load balancing, such as traffic sharing. In order to control how traffic is distributed among routes when there are multiple routes for the same destination network that have different costs, use the traffic-share balanced command. With the keyword balanced, the router distributes traffic proportionately to the ratios of the metrics that are associated with different routes. This is the default setting:

router eigrp 1

network x.x.x.x

variance 2

traffic-share balanced

The traffic share count for this example is:

For path E-C-A: 30/20 = 3/2 = 1

For path E-B-A: 30/30 = 1

Because the ratio is not an integer, round down to the nearest integer. In this example, EIGRP sends one packet to E-C-A and one packet to E-B-A.

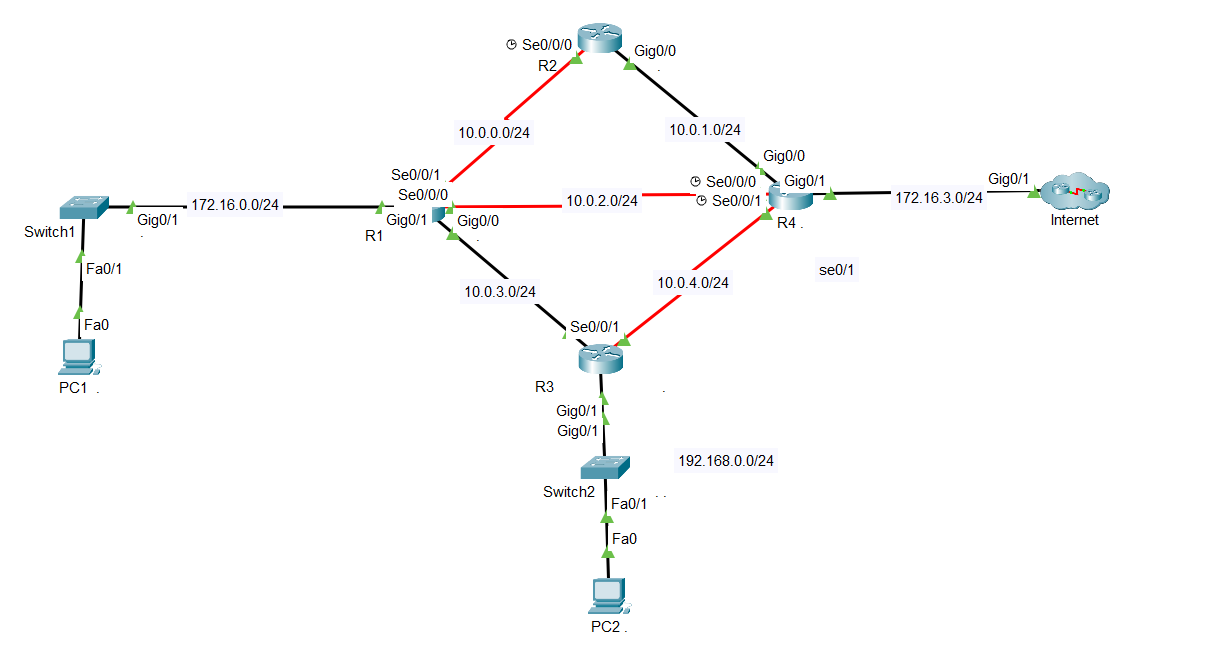
Now, assume that the metric between E-B is 25 and the metric between B-A is 15. In this case, the E-B-A metric is 40. However, this path will not be selected for load balancing because the cost of this path, 40, is not less than (20 \* 2 ), where 20 is the FD and 2 is the variance. In order to include this path also in load sharing, the variance should be changed to 3. In this case, the traffic share count ratio is:

For path E-C-A: 40/20 = 2

For path E-B-A: 40/40 = 1

In this situation, EIGRP sends two packets to E-C-A and one packet to E-B-A. In this way, EIGRP provides both unequal cost path load balancing and intelligent load balancing

## 2.2 Model 2 – OSPF Routing and Multipath Backup



### 2.2.1 Routing with OSPF

**Overview of OSPF (Open Shortest Path First) protocol:** OSPF is an Interior Gateway Protocol (IGP) that uses the Dijkstra algorithm (SPF - Shortest Path First) to find the shortest path between routers. OSPF supports many features such as dividing the routing domain into Areas, reducing CPU load and increasing security.

**Benefits of OSPF:**

* Fast routing: Automatically update paths when there is a problem.
* Support large networks: With division into areas for optimization.
* Support load balancing: On paths with equal costs.

Basic configuration steps on network devices:

1. **Router ID configuration:**

Command to start OSPF

| router ospf [process-id] |
| --- |

Assign router ID using command

| router-id [id] |
| --- |

1. **Area Configuration:**

Assign interfaces to Area using the command

| network [IP] [wildcard-mask] area [area-id] |
| --- |

For example:

| router ospf 1  network 172.16.0.0 0.0.0.255 area 0  network 10.0.0.0 0.0.7.255 area 0 |
| --- |

### 2.2.2 Multipath Backup

Meaning and Role of Multipath Backup:

Meaning of Multipath Backup:

* Providing redundancy: Redundant paths enhance network availability.
* Continuous connectivity: Ensuring no interruptions when the primary path fails.

Role of Multipath Backup:

* Enhancing reliability: Secondary paths ensure network availability.
* Optimizing network resources: Minimizing the risk of overloading a single path.

How to configure multiple redundant routes on OSPF:

* Use the cost or parameter metric to prioritize different routes.
* For example, on R1:

| interface se0/0/1  ip ospf cost 10  interface g0/0  ip ospf cost 50  interface se0/0/0  ip ospf cost 50 |
| --- |

Main route: R1 → R2 → R4.

Backup routes:

* 1. R1 → R4 directly .
  2. R1 → R3 → R4.

**Why Not Combine Load Balancing with Multipath Backup?**

* Different Purposes:

Load balancing: Distributes traffic across equal-cost paths (ensuring maximum bandwidth efficiency).

Multipath backup: Increases redundancy to ensure connectivity when the primary path fails.

* Potential Conflicts:

Backup paths are set to a higher cost (so they are not used when the primary path is available).

Load balancing will divide traffic between paths, including the primary and backup paths, which does not meet the original purpose.

* Design Complexity:

Combining these two features can increase the complexity of installation and management, especially in large networks.

Consumes additional CPU and energy during network operation, especially in large networks

In this model, Multipath Backup is chosen as a solution to increase redundancy and ensure connectivity instead of Load Balancing, helping to maintain network stability when problems occur.

### 2.2.3 Implement NAT

NAT is a networking technique that allows converting the source (or destination) IP address in a packet when the packet passes through a router. NAT helps connect devices in the internal network using private IP to the Internet using one or more public IPs.

* Role and Meaning of NAT

Save IP address resources: NAT allows many internal devices to share one or more public IP addresses.

Enhance security: Private IP addresses are not directly displayed on the Internet, reducing the risk of external attacks.

Flexibility: Supports management and changes to the internal network address structure without affecting the Internet connection.

* NAT Configuration

In this model, NAT is used to provide Internet connection to internal networks through routers 4 (R4)

Example:

| access-list 1 permit 10.0.0.0 0.0.7.255  access-list 1 permit 172.16.0.0 0.0.0.255  access-list 1 permit 192.168.0.0 0.0.0.255  int se 0/0/0  ip nat inside  ex  int gi0/0  ip nat inside  ex  int se 0/0/1  ip nat inside  ex  int gi0/1  ip nat outside  ex  ip nat inside source list 1 int gi0/1 overload |
| --- |

Interface se0/0/0, se0/0/1, gi0/0 are set as inside to handle packets from the internal network.

Interface g0/1 is set as outside to connect to the Internet.

The ip nat inside source command enables NAT, using overload (PAT) to share a single public IP.

### 2.2.4 Packet Filtering

Packet Filtering is a network security mechanism that allows or denies traffic based on predefined rules such as IP address, protocol, or port number.

Role and Meaning of Packet Filtering:

* Protect internal network: Prevent unauthorized access or attacks from outside.
* Control traffic: Filter and limit unwanted traffic types.
* Enhanced security: Reduce the risk of exploits and attacks from malicious sources.

**Performance Evaluation**

Stability: Using Multipath Backup ensures uninterrupted connectivity.

Scalability: OSPF model is easily expanded with new Areas.

Security: Combining NAT and Packet Filtering reduces the risk of external attacks.

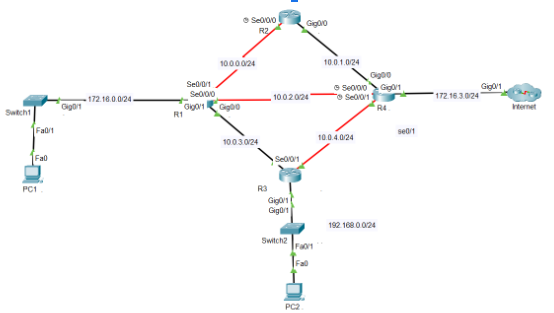
**Recommendations**

Cost Optimization: Use load balancing on OSPF links when traffic is high.

Additional Security: Implement OSPF Authentication to protect routing information exchange.

Network Monitoring: Combine with monitoring tools (such as SNMP) to monitor network traffic and performance.

**2.2.5 Implement Packet Filtering into OSPF**



Before implementing Packet Filtering in a real network, it was first applied in the packet tracer diagram. This is the code that was applied:

Select the router where packet filtering will be applied.

Choose the interface where the ACL will be implemented.

Block network **10.0.4.0/24** from communicating with network **192.168.0.0/24**.

Configure **R3**: **g0/1**.

| en  conf t  access-list 100 deny ip 10.0.4.0 0.0.0.255 192.168.0.0 0.0.0.255  access-list 100 permit ip any any  int g0/1  ip access-group 100 out  exit |
| --- |

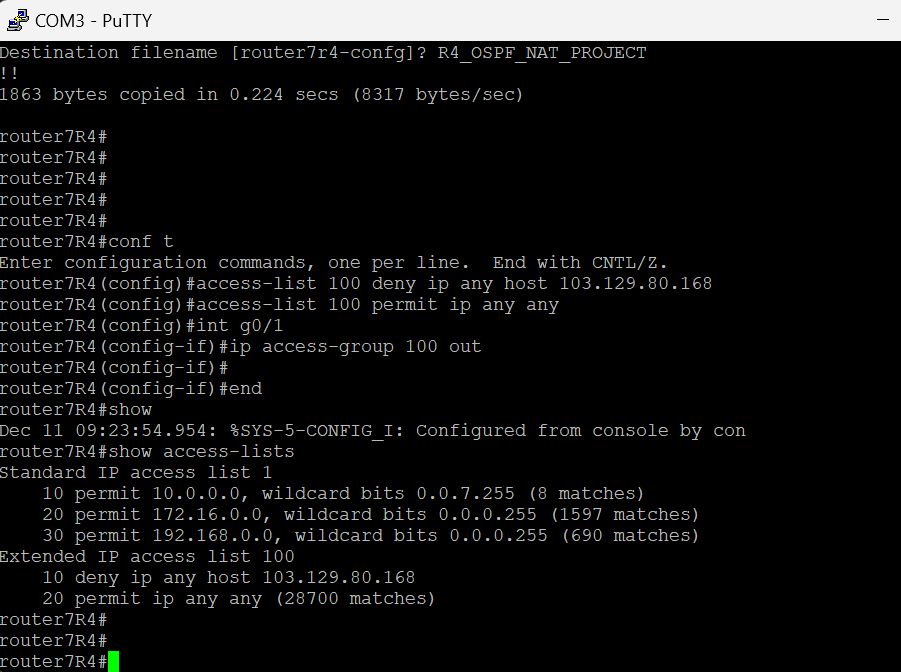
Verification commands.

| show access-lists |
| --- |

remove or delete the ACL entirely.

| no access-list 100 deny ip 10.0.4.0 0.0.0.255 192.168.0.0 0.0.0.255 |
| --- |

**Next, I will apply it in a real-world scenario.**



| conf t  access-list 100 deny ip any host 103.129.80.168  access-list 100 permit ip any any  int g0/1  ip access-group 100 out  show access-lists |
| --- |

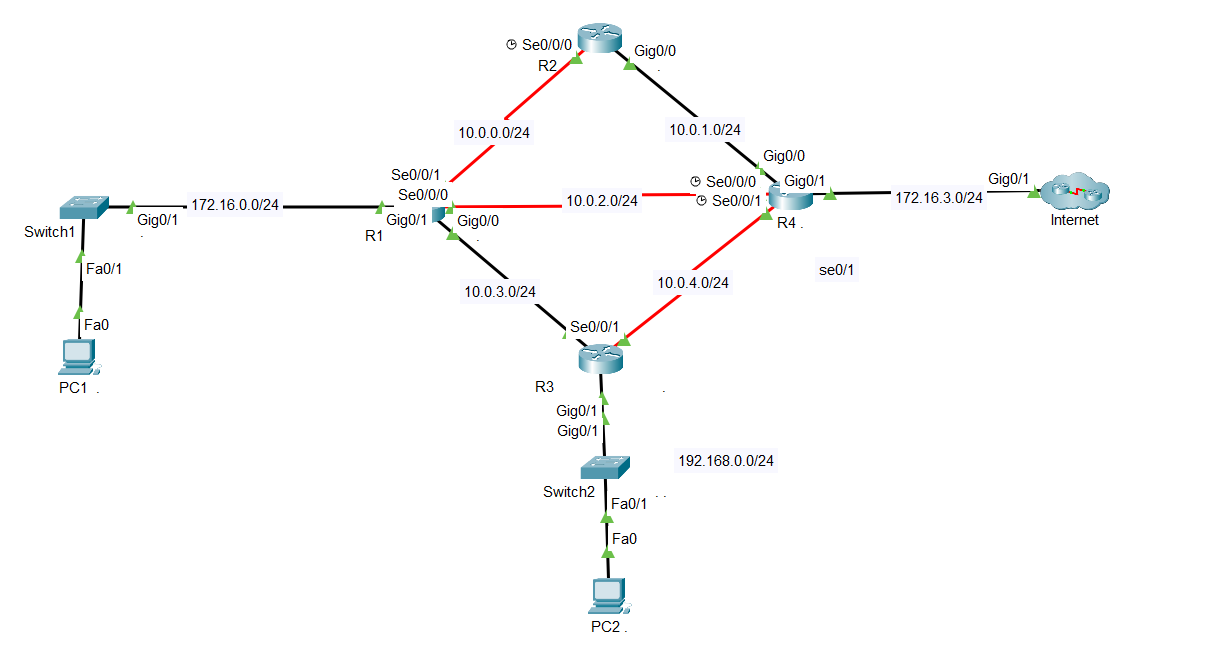
Remove or delete the ACL entirely.

| int g0/1  no ip access-group 100 out  no access-list 100 |
| --- |

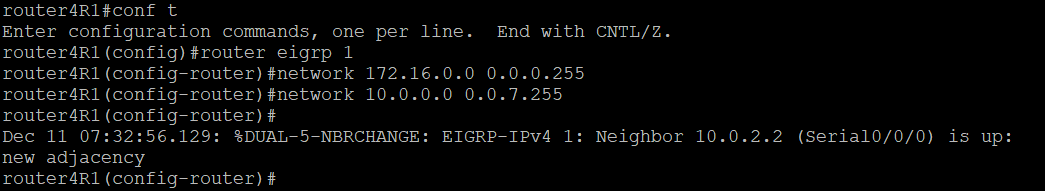
# 

# CHAPTER 3. RESULTS OF IMPLEMENTATION

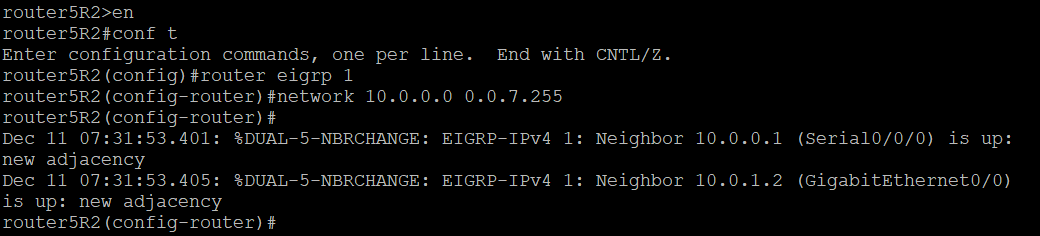
# 3.1 EIGRP



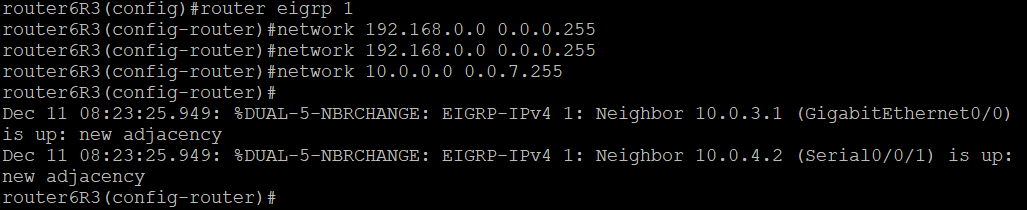
#### R1



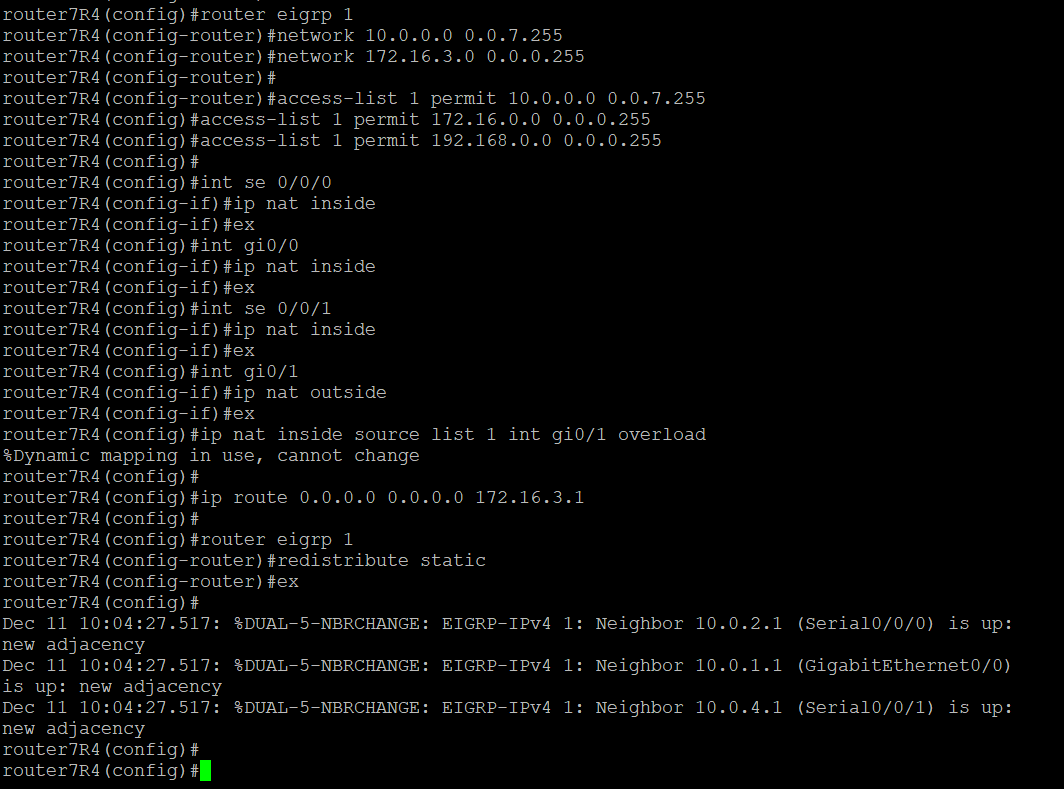
#### R2



#### R3



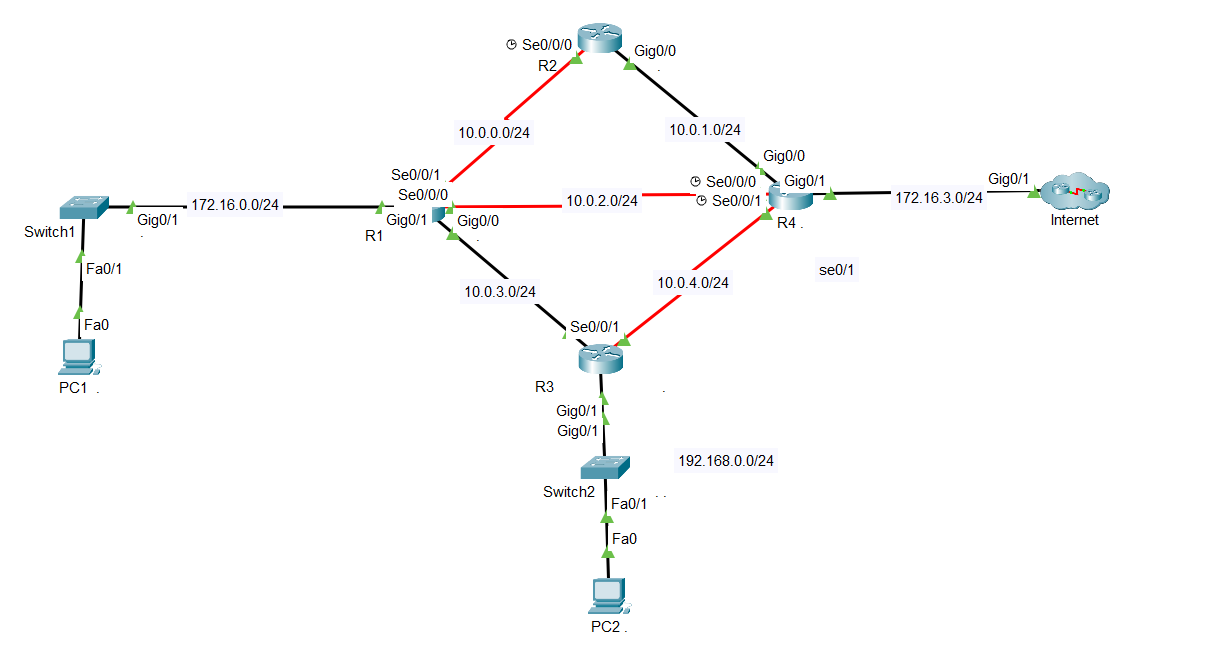
#### R4





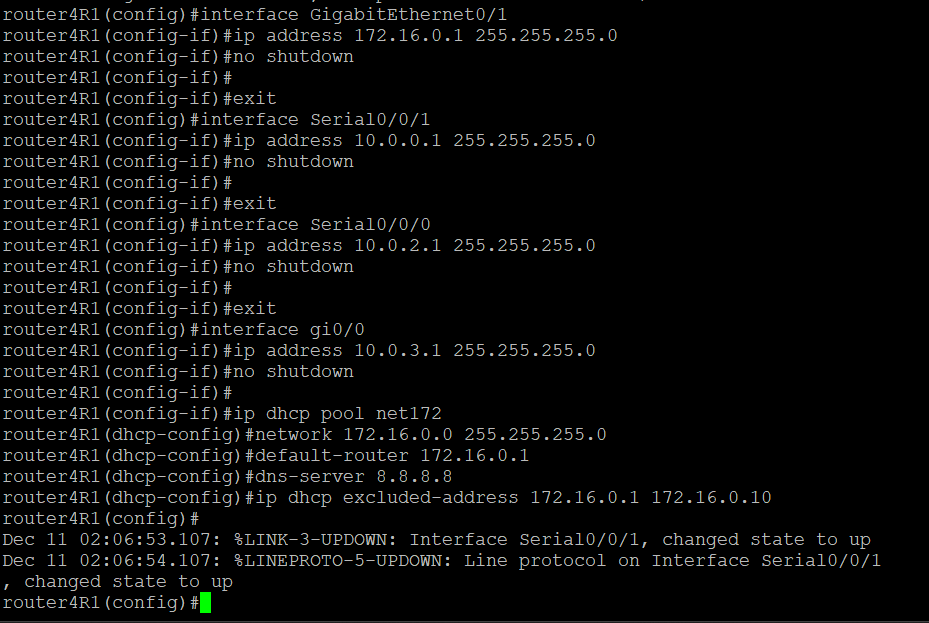
*Figure routing table*

## 3.2 OSPF

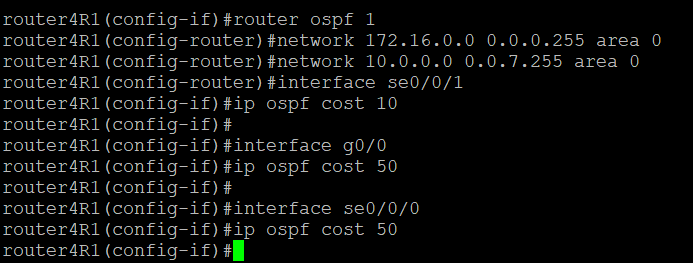


### Configure

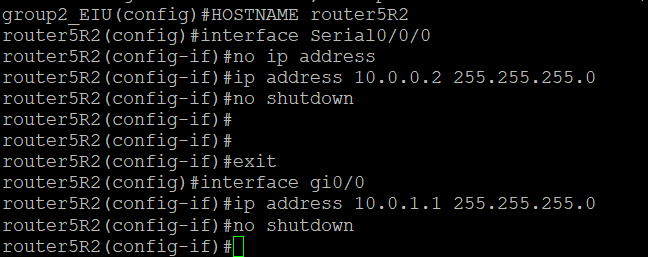
#### R1



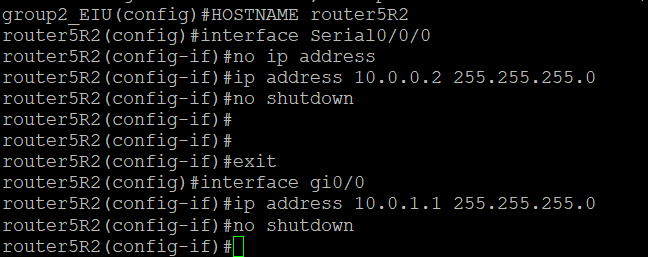
*Figure . Example of basic configure R1*

**

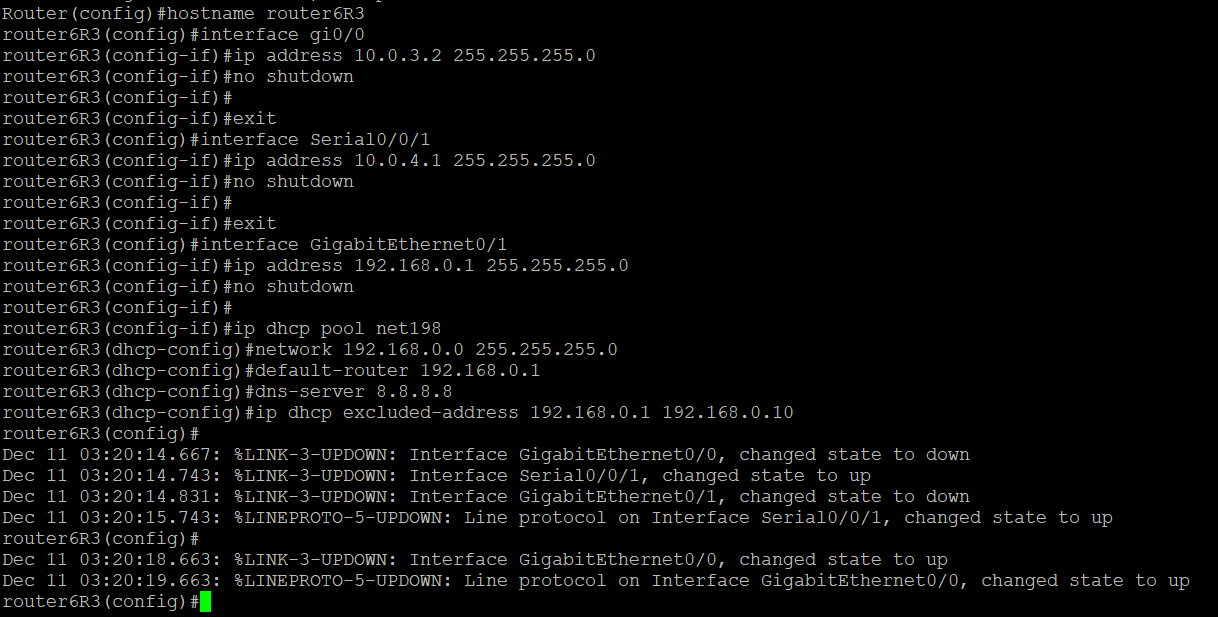
#### R2

**

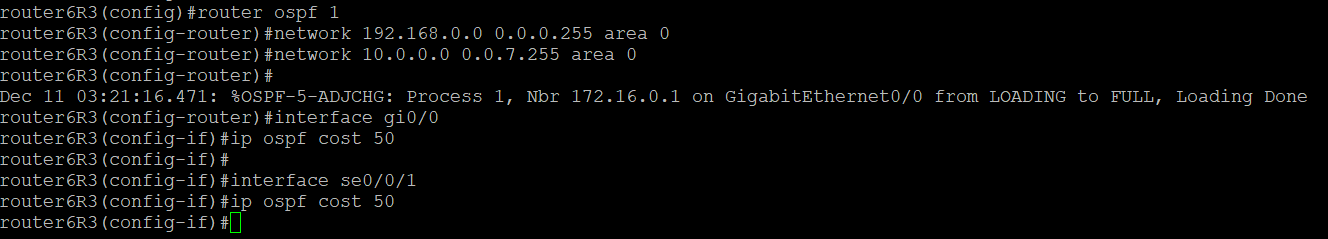
*Figure . Example of basic configure R2*

**

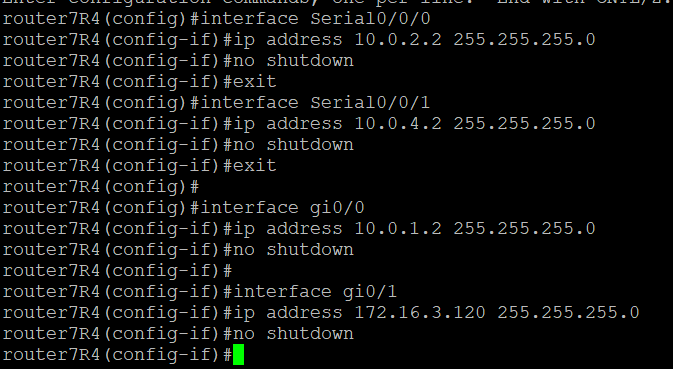
#### R3



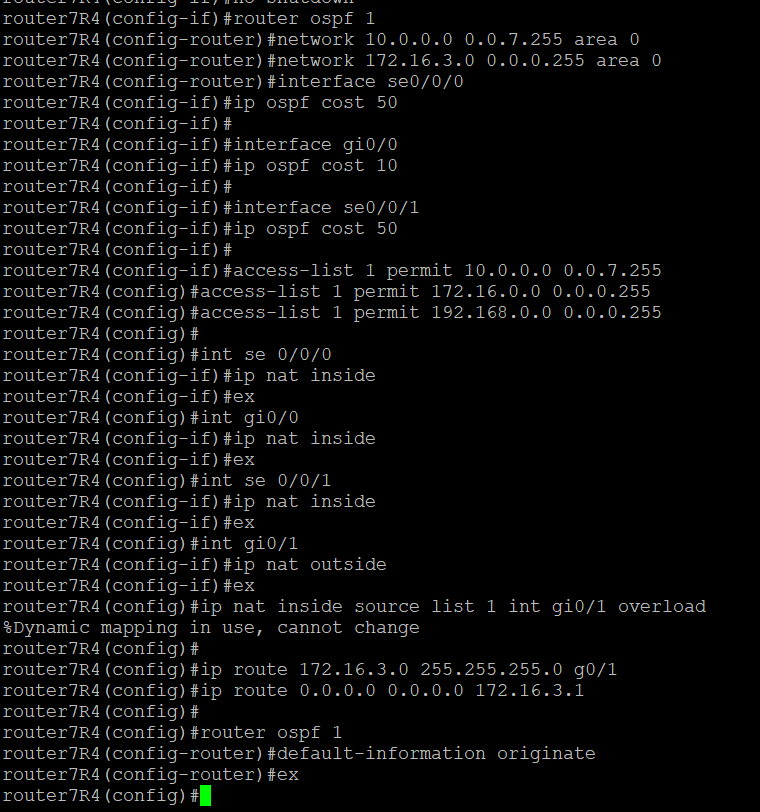
*Figure . Example of basic configure R3*



#### R4



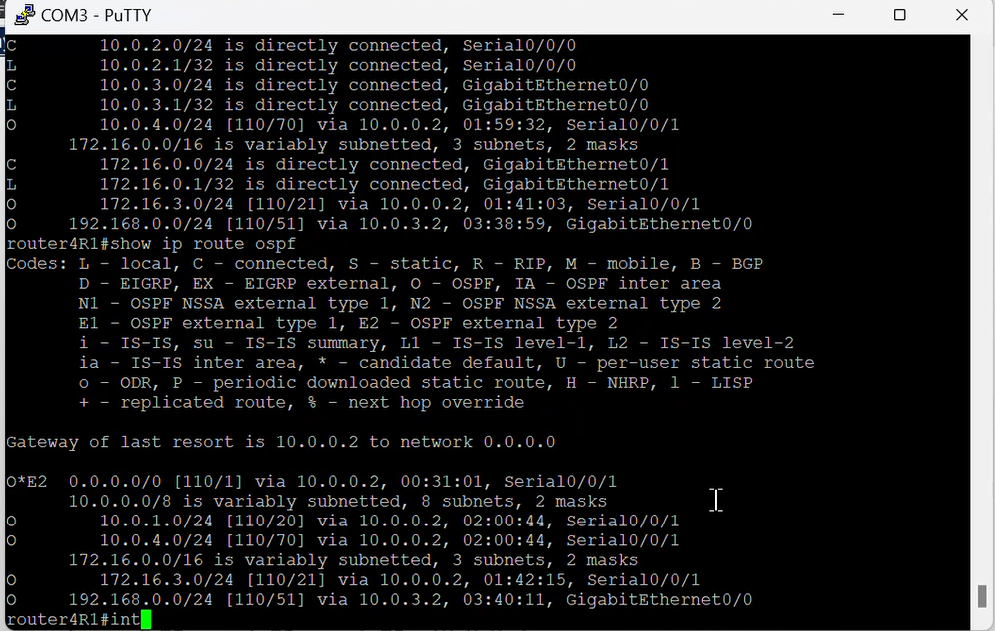
*Figure . Example of basic configure R4*



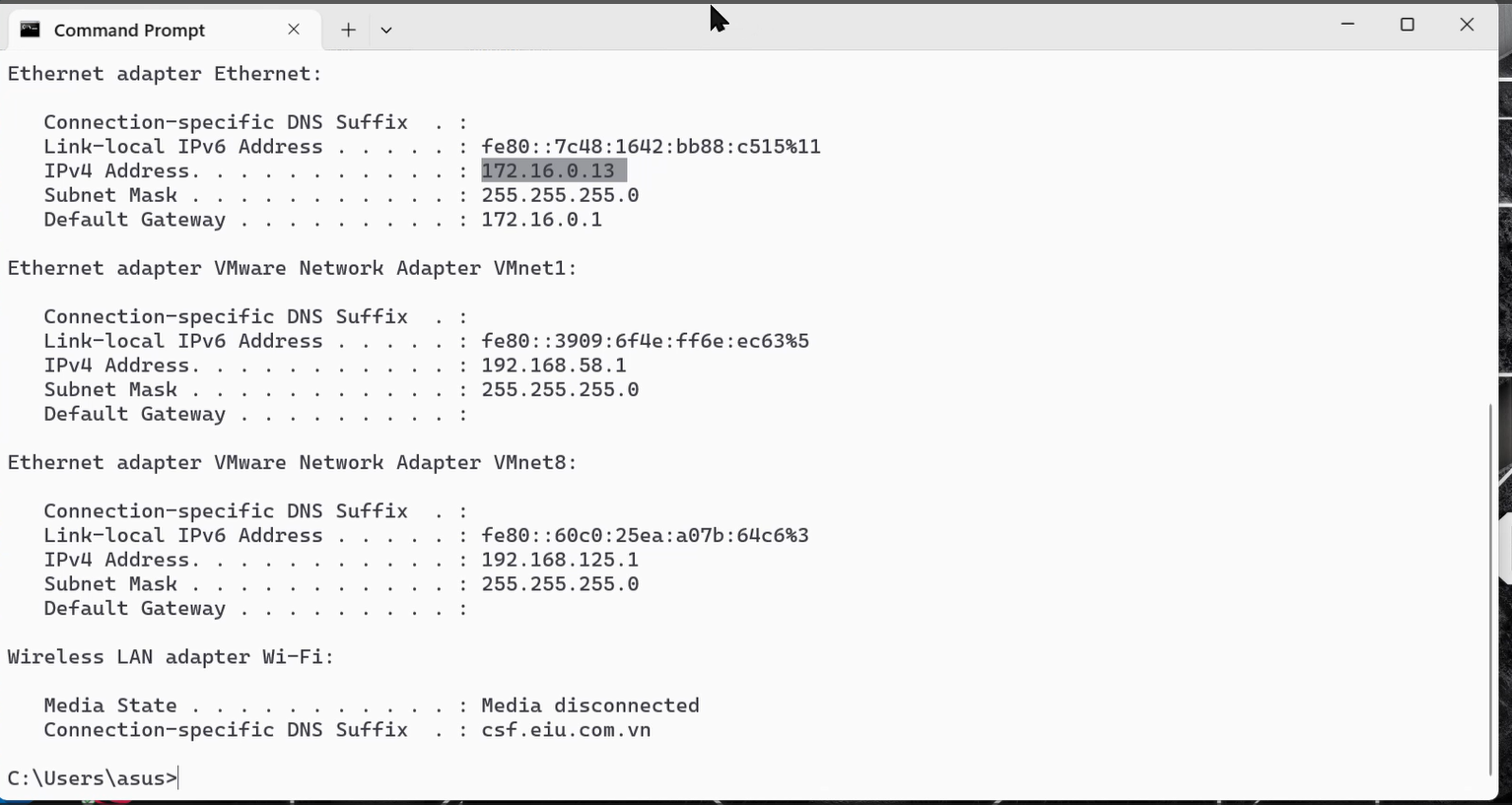
### Result

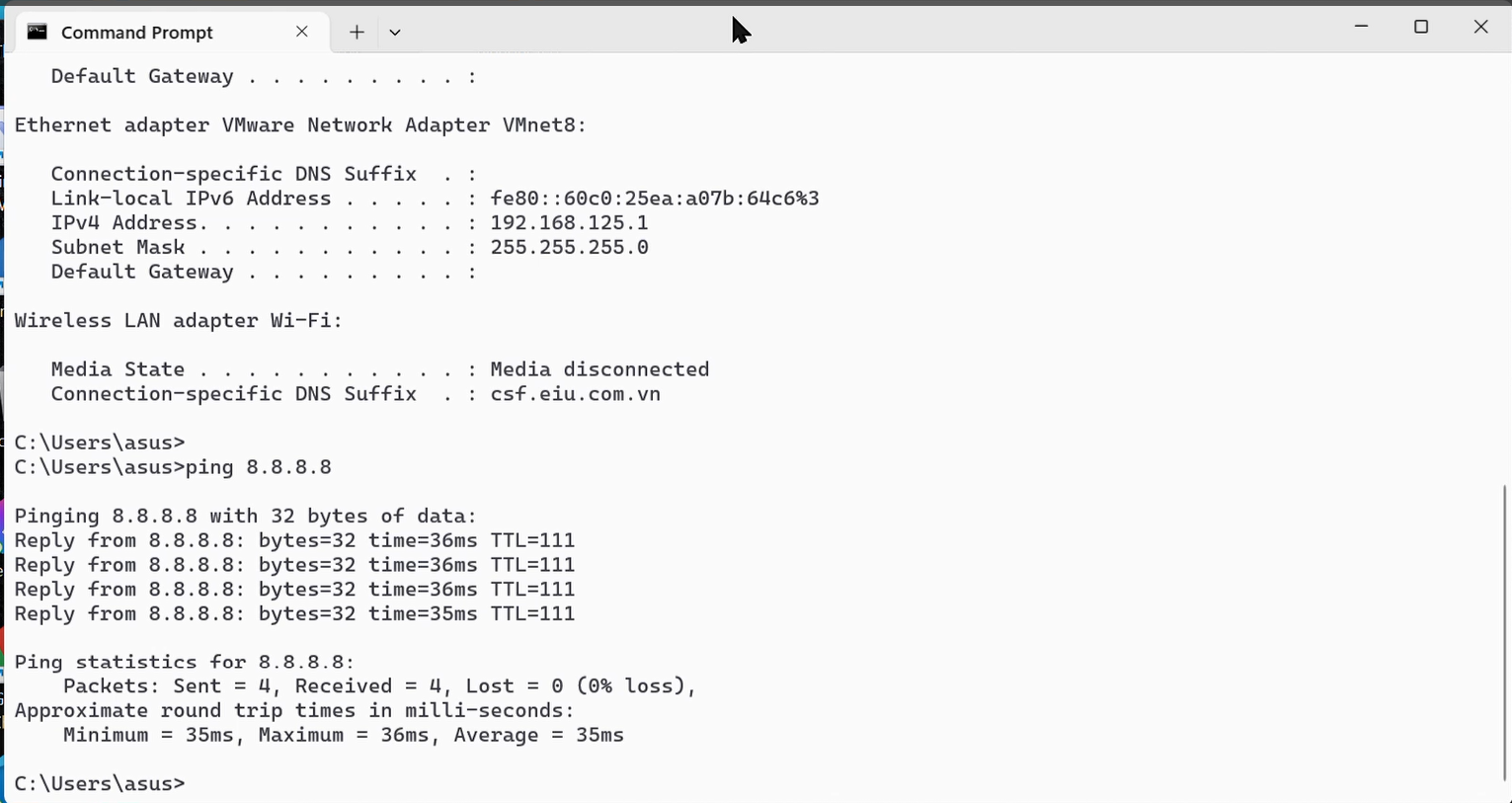
#### OSPF Routing

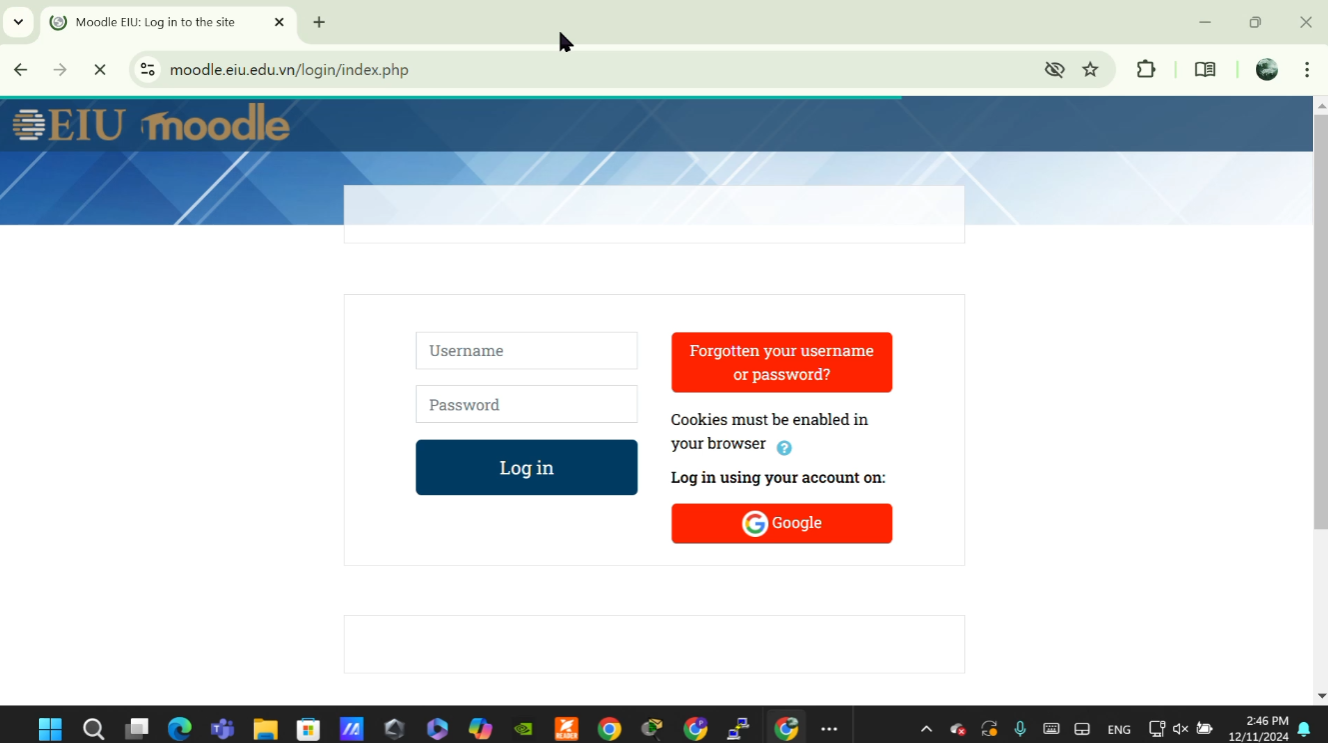
R1



#### NAT



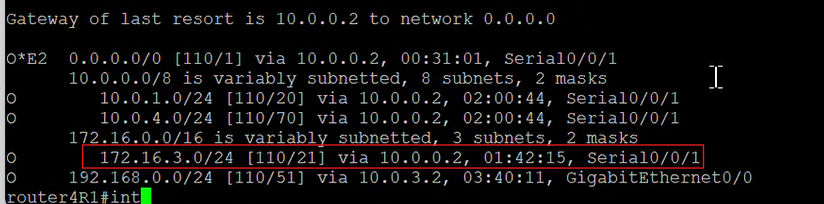




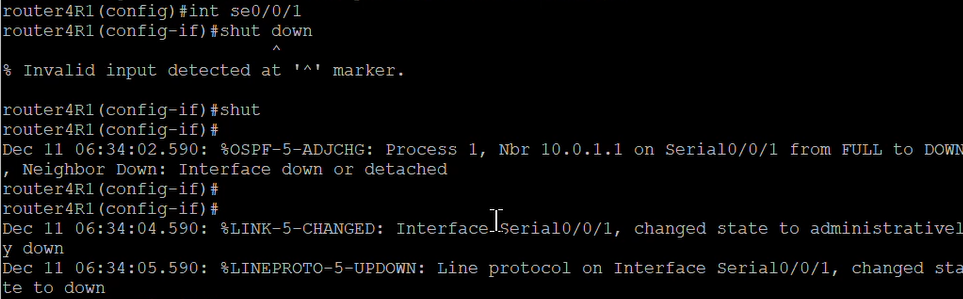
#### Multipath backup

initially, data will go to 172.16.3.0. Via 10.0.0.2 (R2 - se0/0/1) to R4

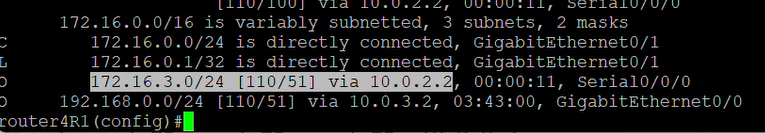
R1 -> R2 -> R4

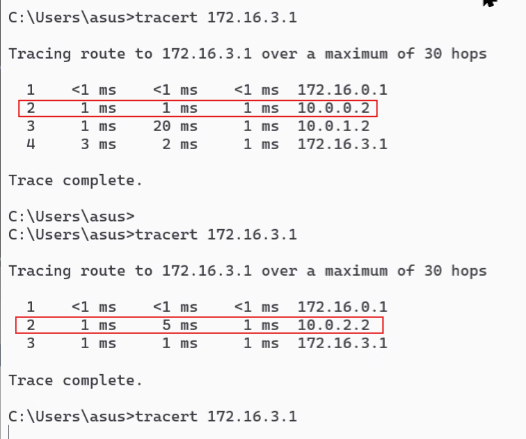


next, shut down se0/0/1

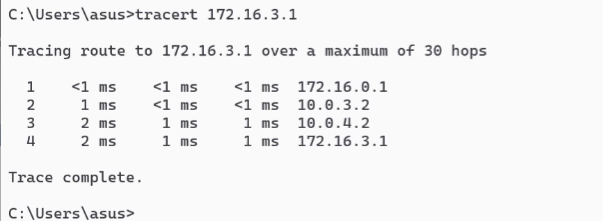


change path from se0/0/1 to se0/0/0 (10.0.0.2 to 10.0.2.2)

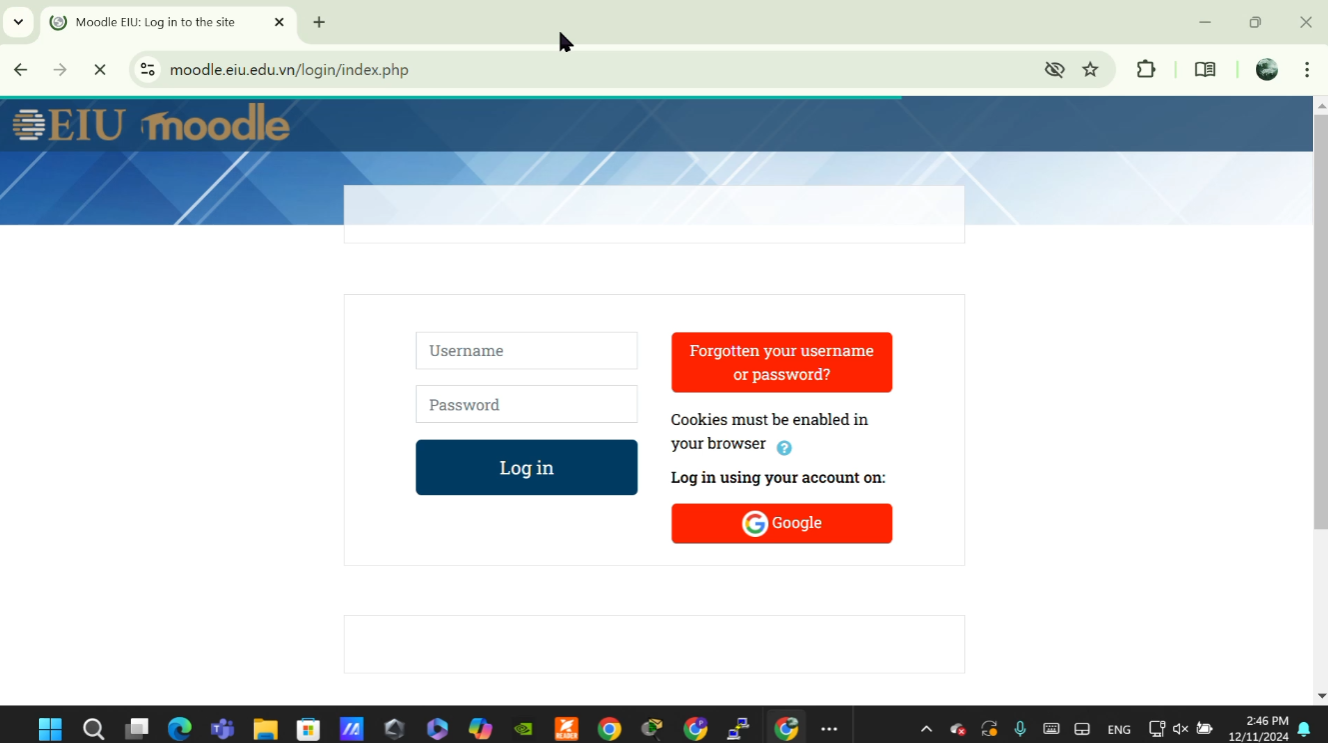




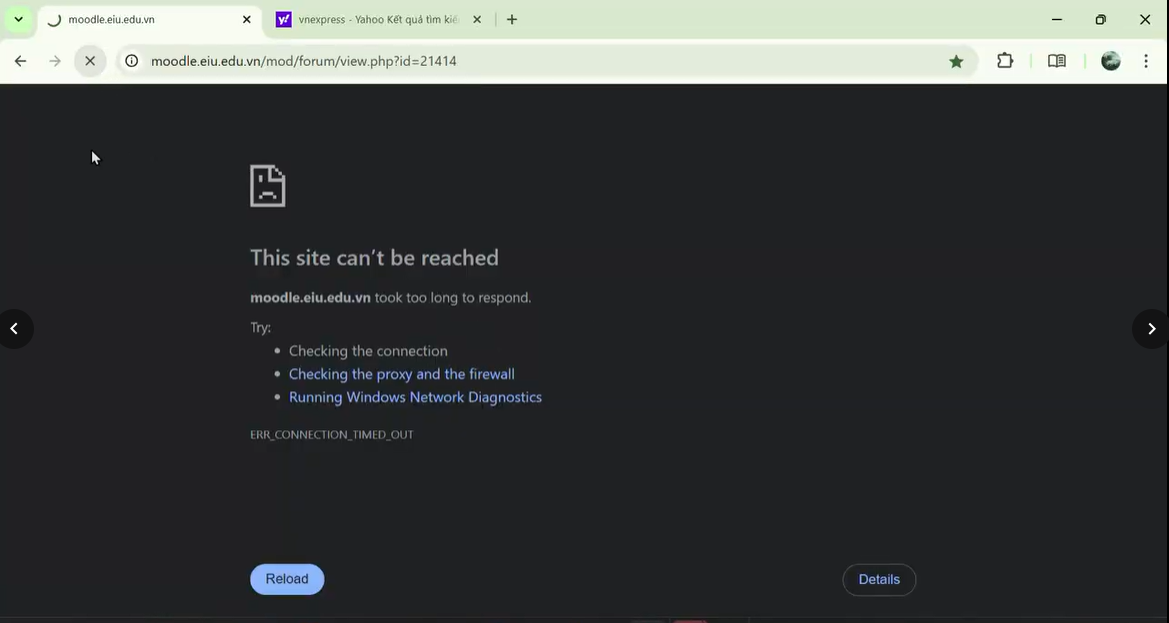
next, shut down se0/0/0, change path from se0/0/0 to gi0/0 (10.0.2.2 to 10.0.3.2)



**Packet Filtering**



**After packet filtering applied**



# 

# CHAPTER 4. CONCLUSION

## Conclusion

The deployed model not only ensures stable and secure connection but is also easy to expand. This is a suitable solution for small and medium-sized enterprises that need to optimize network resources.

## Future Works

* Enhancing Security:

Implementing more advanced security measures such as IPSec or Firewalls to increase network protection against new threats.

* Improving Load Balancing:

Apply load balancing across multiple routing protocols to improve traffic management efficiency.

* Implementing Monitoring Tools:

Integrate monitoring tools such as Zabbix or PRTG to monitor performance and detect faults early.

* Expanding Scenarios:

Extend the model with other routing protocols such as BGP or MPLS to serve larger enterprise networks

# REFERENCES

1. How Does Unequal Cost Path Load Balancing (Variance) Work in IGRP and EIGRP? - Cisco: [How Does Unequal Cost Path Load Balancing (Variance) Work in IGRP and EIGRP? - Cisco](https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13677-19.html?form=MG0AV3)
2. What Is a Virtual Private Network (VPN)? (2023): https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html
3. B., & B. (2022). Deploy pfSense VMware step-by-step: https://www.virtualizationhowto.com/2022/03/deploy-pfsense-vmware-step-by-step/
4. Packages — IDS / IPS — Configuring the Snort Package, pfSense Documentation. (2023): https://docs.netgate.com/pfsense/en/latest/packages/snort/setup.html
5. Zoltan, M., & Zoltan, M. (2023). How to Set Up IP Filtering &amp; DNS Blackholing on pfSense. Privacy Affairs: <https://www.privacyaffairs.com/ip-filtering-pfsense>
6. PfblockerNG Guide : <https://www.zenarmor.com/docs/network-security-tutorials/pfblockerng>
7. Introduction to firewall : https://etutorials.org/Networking/Router+firewall+security/Part+I+Security+Overview+and+Firewalls/Chapter+2.+Introduction+to+Firewalls/Firewall+Categories/