ENTERPRISE OFFICE NETWORK DESIGN AND IMPLEMENTATION USING CISCO PACKET TRACER

NAME: Gagandeep Kaur

COURSE : Cybersecurity

INSTITUTION NAME: Cognimab

MENTOR : Yashmit

TITLE OF CONTENT

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my mentor, Yashmit, for continuous guidance, support, and valuable suggestions throughout the development of this project. Their technical insights and feedback played a crucial role in improving the overall design and implementation of the enterprise network.

I also thank my institution and faculty members for providing the required learning resources and environment that supported the successful completion of this work.

Finally, I acknowledge everyone who directly or indirectly contributed to this project and helped enhance my understanding of enterprise networking concepts.

ABSTRACT

This report presents the design and implementation of a simulated enterprise office network using Cisco Packet Tracer. The objective of the project is to build a scalable and functional network infrastructure capable of supporting multiple subnetworks, automated configuration, remote administration, and internal web services.

The network includes nine routers and sixteen switches interconnected in a chained topology to represent different enterprise departments or office locations. Dynamic routing is implemented using Enhanced Interior Gateway Routing Protocol (EIGRP) to ensure efficient communication between networks. Automated IP address assignment is achieved through DHCP configured on routers, allowing end devices to obtain configuration parameters without manual intervention.

Additionally, DNS and HTTP services are deployed on a server to simulate real-world enterprise services, enabling users to access hosted websites through domain names. Remote management of routers is configured using Telnet through VTY lines, allowing administrators to manage network devices from remote locations.

Testing procedures including connectivity verification, DNS resolution, web browsing, and remote login confirm successful network deployment. The project demonstrates practical understanding of enterprise networking principles and highlights the importance of automation, routing protocols, and centralized services in modern networks.

1. INTRODUCTION

Enterprise networks are designed to support communication across multiple departments, users, and services while maintaining scalability and efficient management. Organizations rely on structured network architectures to enable seamless connectivity, automated configuration, and centralized services such as web hosting and domain resolution.

This project focuses on designing an enterprise office network using Cisco Packet Tracer to simulate real-world networking scenarios. The network consists of multiple routers interconnected through WAN links, with each router supporting its own LAN environment connected through switches and end devices. Key goals include implementing dynamic routing, automating IP address allocation, enabling domain-based website access, and providing remote administrative capabilities. The project demonstrates how multiple networking technologies work together to create a functional enterprise environment.

Modern enterprise networks require flexible design and efficient resource management to support growing infrastructure demands. Technologies such as dynamic routing protocols, automated IP configuration, and centralized services help reduce manual configuration and improve network scalability. By implementing EIGRP routing, DHCP-based IP allocation, DNS resolution, and HTTP web hosting, this project reflects core enterprise networking practices. The use of simulation tools allows safe testing, configuration validation, and practical understanding of real-world network deployment strategies.

2. METHODOLOGY AND BACKGROUND CONCEPTS

The design and implementation of an enterprise office network require understanding both theoretical networking concepts and practical configuration methodologies. This project integrates fundamental networking technologies with hands-on implementation using Cisco Packet Tracer to simulate a realistic enterprise environment.

Enterprise networks are structured to ensure reliable connectivity, scalability, and efficient management across multiple departments or locations. In this project, a chain topology of routers was implemented to simulate interconnected enterprise branches communicating through Wide Area Network (WAN) links. Each router represents an individual network segment connected to local devices through switches.

Dynamic routing was implemented using Enhanced Interior Gateway Routing Protocol **(EIGRP)**. EIGRP is a widely used routing protocol designed to automate route exchange between routers while maintaining fast convergence and efficient bandwidth utilization. By combining characteristics of distance-vector and link-state routing concepts, EIGRP allows routers to dynamically learn and update routing information without requiring manual static route configuration. This improves scalability and simplifies network expansion.

Automatic IP address management was achieved using Dynamic Host Configuration Protocol **(DHCP)**. DHCP plays a critical role in enterprise environments by assigning IP addresses and network configuration parameters automatically to client devices. Separate DHCP pools were configured on individual routers to ensure logical separation between subnets and to prevent address conflicts. This approach reduces administrative overhead and improves deployment efficiency when adding new devices to the network.

Domain Name System **(DNS)** and Hypertext Transfer Protocol **(HTTP)** services were deployed to simulate real-world enterprise applications. DNS converts domain names into corresponding IP addresses, enabling users to access network services using human-readable URLs instead of numeric addresses. In this implementation, domain entries such as www.aot.com and www.jjk.com were configured to demonstrate internal web service accessibility. HTTP services allowed hosting of web pages accessible through client browsers across different networks.

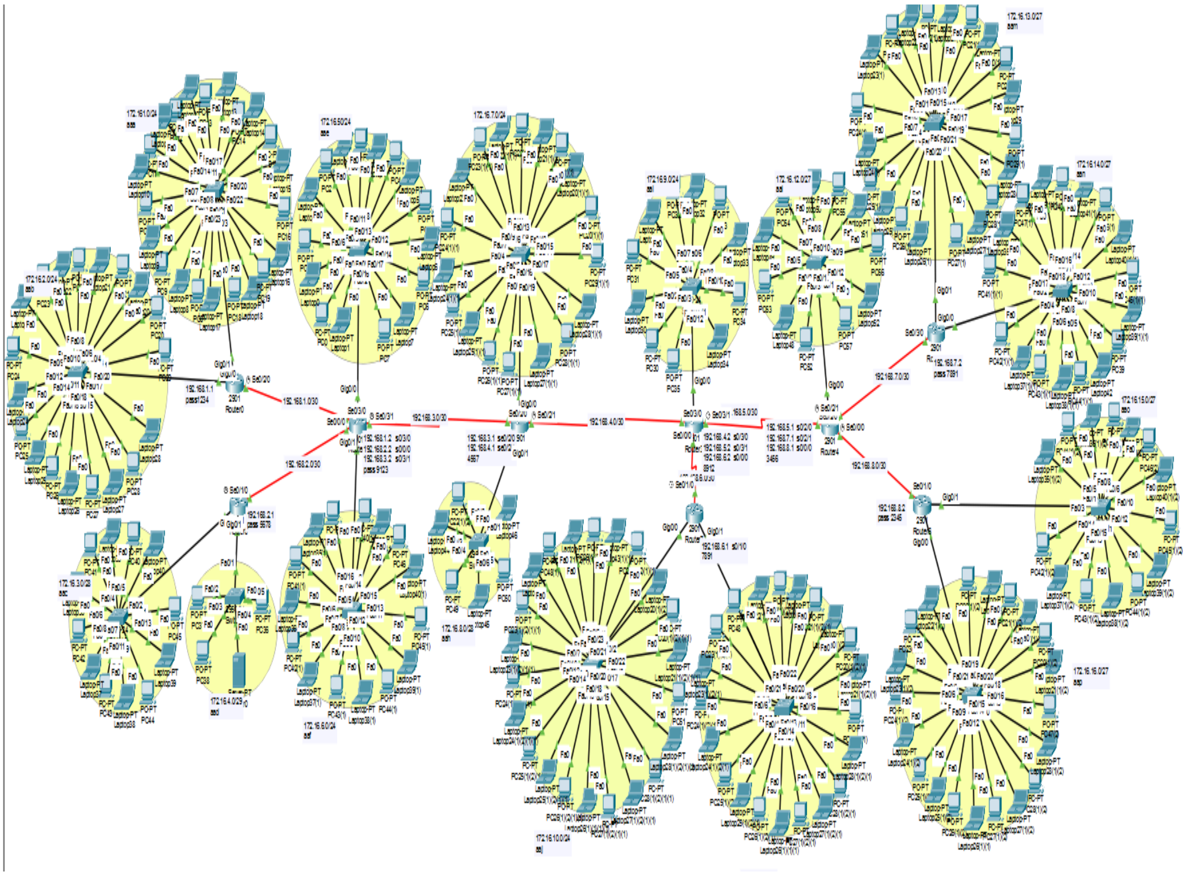
Remote device management is an important aspect of enterprise networking. **Telnet** was configured on all routers to enable remote command-line access via Virtual Terminal **(VTY)** lines. This allows administrators to monitor and configure devices from remote locations within the network. Although Telnet lacks encryption and is not recommended for production environments, it is useful for learning purposes and network simulation.

Switches were deployed as Layer 2 devices responsible for connecting end-user devices within local networks. They provide efficient frame forwarding and device aggregation, while routers operate at Layer 3 to manage traffic between different networks and maintain routing tables.

The practical implementation followed a structured methodology. First, the physical topology was created using routers, switches, and end devices within Cisco Packet Tracer. WAN and LAN addressing schemes were assigned using separate IP ranges to distinguish inter-router connections from local networks. EIGRP was then configured across all routers to establish dynamic routing relationships. DHCP pools were created to automate IP allocation, followed by configuration of DNS and HTTP services on the server. Finally, Telnet access was enabled to allow remote administration, and comprehensive testing was performed to validate connectivity, domain resolution, web access, and remote login functionality.
This combined approach of theoretical understanding and practical configuration ensures that the network design reflects core enterprise networking principles while demonstrating real-world implementation skills.

3. IMPLEMENTATION / WORK DONE

NETWORK TOPOLOGY



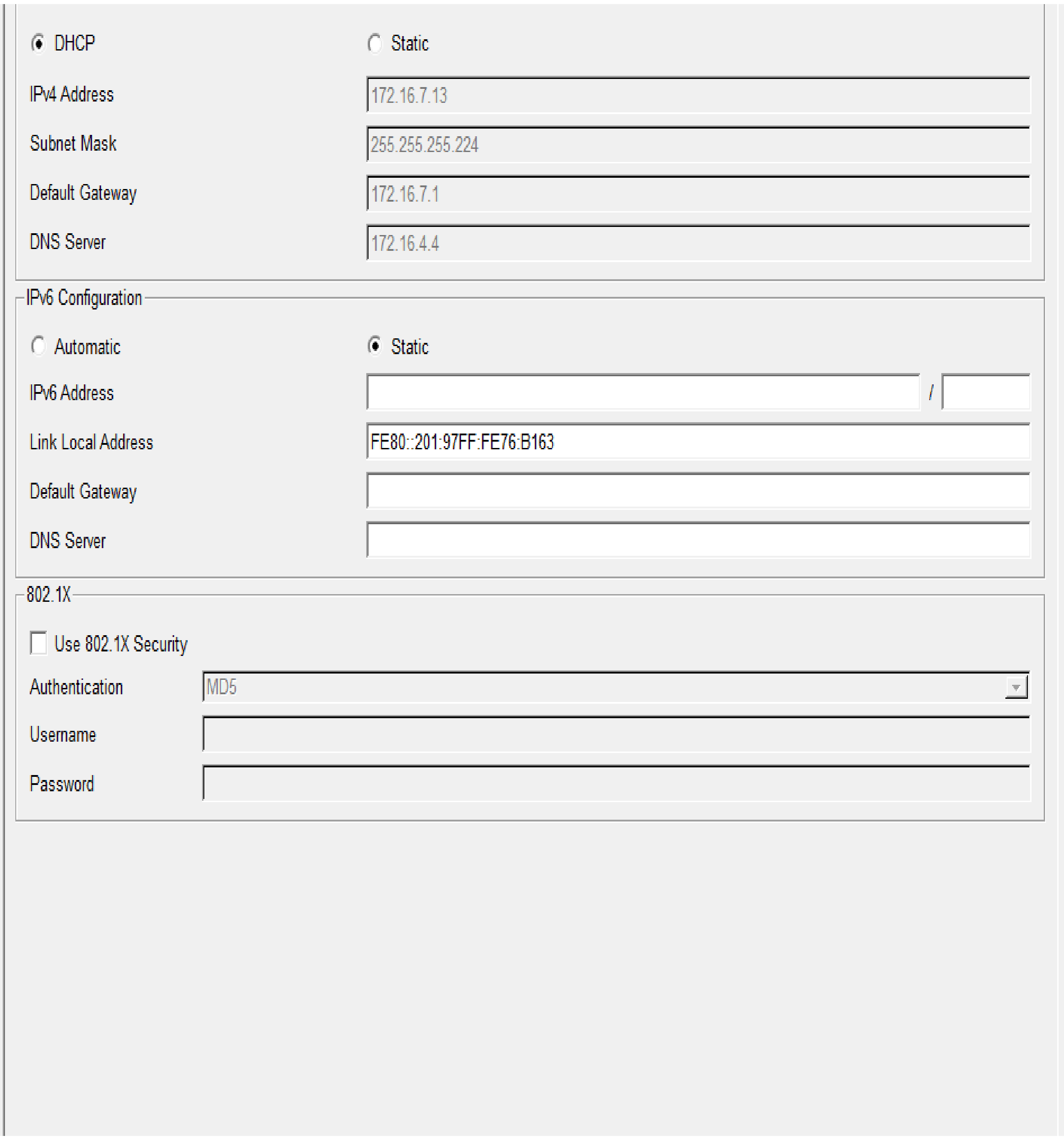
Nine routers are interconnected using WAN networks ranging from 192.168.1.0 to 192.168.8.0. Each router connects to a local LAN network using the address range 172.16.1.0 to 172.16.16.0.

EIGRP CONFIGURATION

EIGRP was enabled on all routers to dynamically share route information and ensure connectivity between LANs.

DHCP CONFIGURATION

Each router contains a dedicated DHCP pool corresponding to its LAN subnet. End devices receive IP addresses automatically upon enabling DHCP.

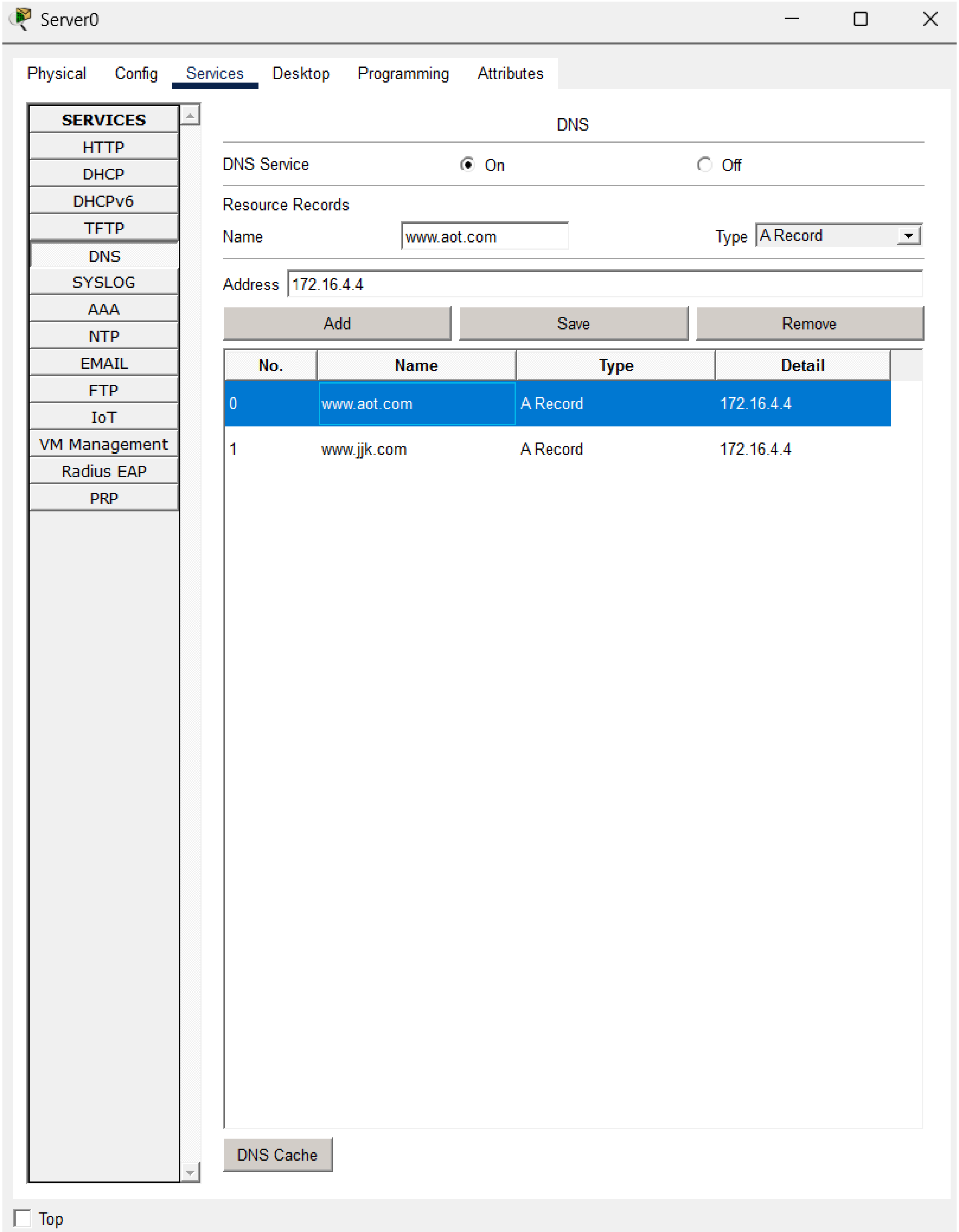


DNS AND HTTP SERVER

The server hosts DNS entries for:

- www.aot.com
- www.jjk.com

HTTP services allow users to access web pages through browsers.



TELNET CONFIGURATION

Remote management is enabled through line VTY configuration including login password and enable password settings.

Router1

Physical Config CLI Attributes

IOS Command Line Interface

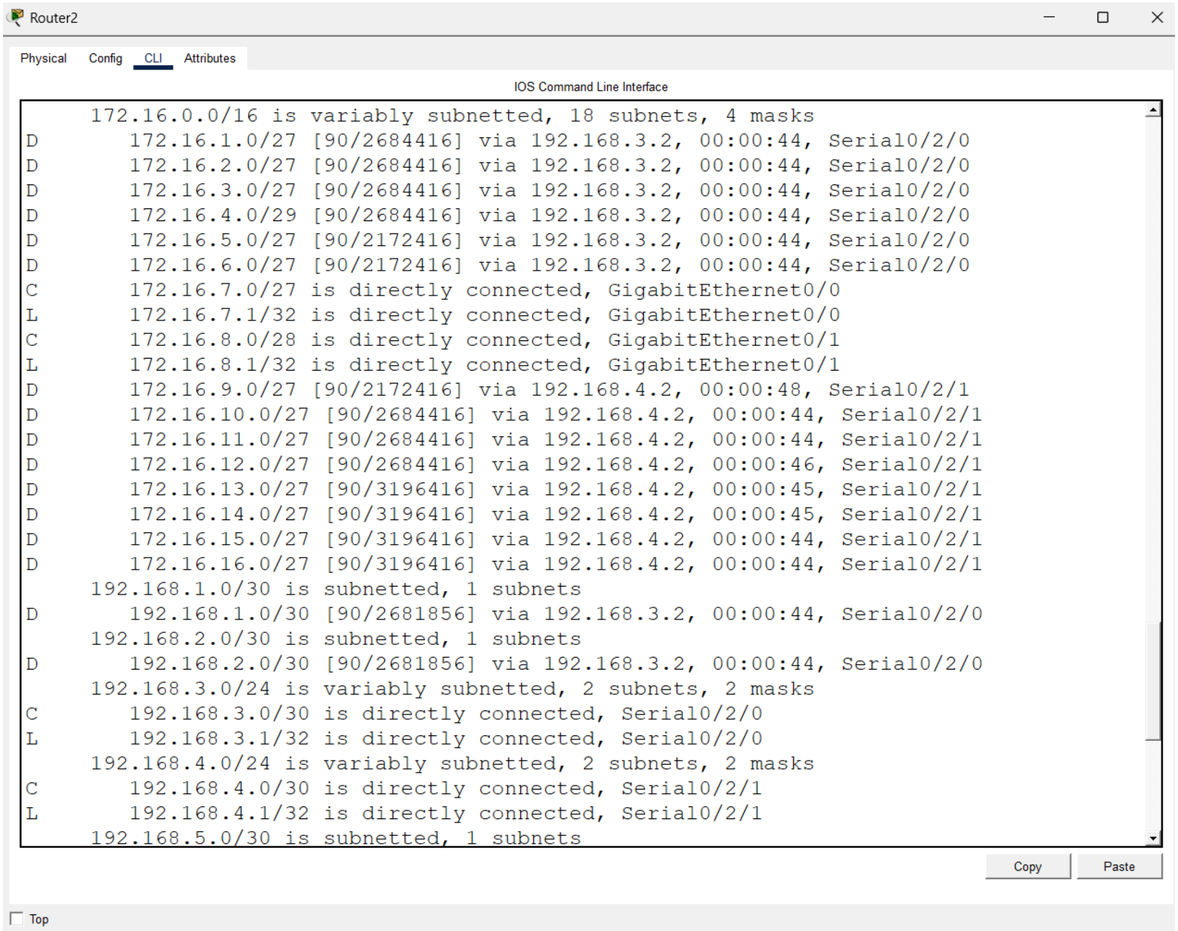
```
Router>telnet 192.168.2.1
Trying 192.168.2.1 ...Open


User Access Verification

Password:
Router>en
Password:
Router#ex

[Connection to 192.168.2.1 closed by foreign host]
Router>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Password:
Router>en
Password:
Router#ex

[Connection to 192.168.1.1 closed by foreign host]
Router>telnet 192.168.3.1
Trying 192.168.3.1 ...Open


User Access Verification

Password:
```

Top

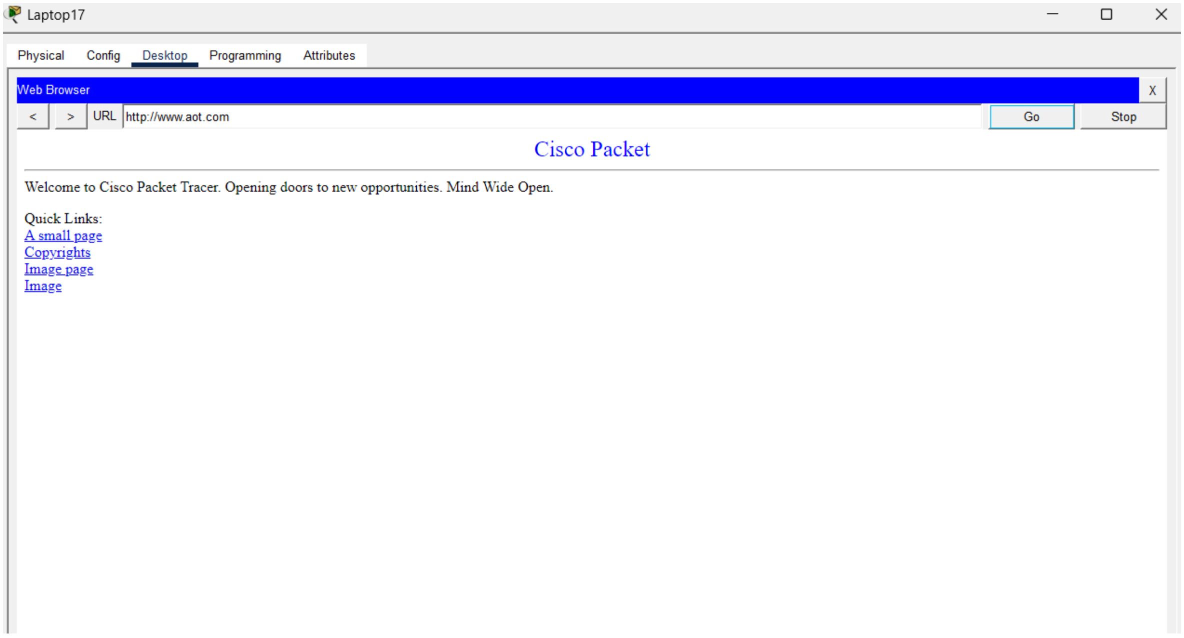
4. RESULTS AND ANALYSIS

RESULT:

- All routers successfully exchanged routing information through EIGRP.
- Client devices received IP configuration automatically via DHCP.
- DNS resolution successfully converted domain names into IP addresses.
- HTTP websites loaded correctly through browser testing.
- Remote Telnet login allowed management of routers across the network.




```
     172.16.0.0/16 is variably subnetted, 18 subnets, 4 masks
D       172.16.1.0/27 [90/2684416] via 192.168.3.2, 00:00:44, Serial0/2/0
D       172.16.2.0/27 [90/2684416] via 192.168.3.2, 00:00:44, Serial0/2/0
D       172.16.3.0/27 [90/2684416] via 192.168.3.2, 00:00:44, Serial0/2/0
D       172.16.4.0/29 [90/2684416] via 192.168.3.2, 00:00:44, Serial0/2/0
D       172.16.5.0/27 [90/2172416] via 192.168.3.2, 00:00:44, Serial0/2/0
D       172.16.6.0/27 [90/2172416] via 192.168.3.2, 00:00:44, Serial0/2/0
C       172.16.7.0/27 is directly connected, GigabitEthernet0/0
L       172.16.7.1/32 is directly connected, GigabitEthernet0/0
C       172.16.8.0/28 is directly connected, GigabitEthernet0/1
L       172.16.8.1/32 is directly connected, GigabitEthernet0/1
D       172.16.9.0/27 [90/2172416] via 192.168.4.2, 00:00:48, Serial0/2/1
D       172.16.10.0/27 [90/2684416] via 192.168.4.2, 00:00:44, Serial0/2/1
D       172.16.11.0/27 [90/2684416] via 192.168.4.2, 00:00:44, Serial0/2/1
D       172.16.12.0/27 [90/2684416] via 192.168.4.2, 00:00:46, Serial0/2/1
D       172.16.13.0/27 [90/3196416] via 192.168.4.2, 00:00:45, Serial0/2/1
D       172.16.14.0/27 [90/3196416] via 192.168.4.2, 00:00:45, Serial0/2/1
D       172.16.15.0/27 [90/3196416] via 192.168.4.2, 00:00:44, Serial0/2/1
D       172.16.16.0/27 [90/3196416] via 192.168.4.2, 00:00:44, Serial0/2/1
     192.168.1.0/30 is subnetted, 1 subnets
D       192.168.1.0/30 [90/2681856] via 192.168.3.2, 00:00:44, Serial0/2/0
     192.168.2.0/30 is subnetted, 1 subnets
D       192.168.2.0/30 [90/2681856] via 192.168.3.2, 00:00:44, Serial0/2/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/30 is directly connected, Serial0/2/0
L       192.168.3.1/32 is directly connected, Serial0/2/0
     192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.4.0/30 is directly connected, Serial0/2/1
L       192.168.4.1/32 is directly connected, Serial0/2/1
     192.168.5.0/30 is subnetted, 1 subnets
```



ANALYSIS:

The chained topology allowed simulation of distributed enterprise branches while maintaining manageable configuration complexity. Dynamic routing simplified network expansion and reduced manual route configuration.

Automated IP assignment improved scalability and minimized configuration errors. DNS and HTTP integration demonstrated application-layer services within enterprise environments. However, the current implementation lacks advanced security features such as encrypted remote access and traffic filtering mechanisms.

5. CONCLUSION AND FUTURE SCOPE

CONCLUSION:

The project successfully demonstrates the design and implementation of an enterprise office network integrating dynamic routing, automated IP management, centralized services, and remote administration. The use of EIGRP ensures efficient communication across multiple networks, while DHCP and DNS improve usability and management efficiency.

This project enhances practical understanding of enterprise networking concepts and provides a foundation for advanced network design and security implementations.

FUTURE SCOPE:

Implement SSH instead of Telnet for secure remote management.
Introduce Access Control Lists (ACL) for traffic filtering.
Add VLAN segmentation for improved network organization.
Design hierarchical network architecture.
Implement redundancy and fault tolerance.

6. REFERENCES

- Cisco Networking Academy Materials
- Computer Networking Concepts and Protocols textbooks
- RFC documentation for DHCP, DNS, and HTTP protocols
- Cisco Packet Tracer official documentation