Green University of Bangladesh

Department of Computer Science and Engineering (CSE)
Semester: (Summer, Year: 2025), B.Sc. in CSE (Day)

Corporate Office Network Infrustructure

Course Title: Computer Networking Lab
Course Code: CSE 318
Section: 231 D2

Students Details

Name	ID
Promod Chondra Das	231002005
Chinmoy Debnath	231902029

Submission Date: 25/08/2025
Course Teacher's Name: Fatema Akter

[For teachers use only: Don't write anything inside this box]

Lab Project Status	
Marks:	**Signature:**
Comments:	**Date:**

Contents

Chapter 1

Introduction

1.1 Overview

This project focuses on the design and implementation of a corporate office network infrastructure that ensures secure, reliable, and efficient communication across the organization. The network connects different departments through a structured topology, enabling smooth data transfer, centralized resource sharing, and controlled access. It is designed to support everyday business operations such as internet connectivity, file sharing, and internal communication while maintaining flexibility for future growth. By combining practical design with real-world considerations, the project demonstrates how a well-planned network can improve productivity, enhance security, and provide a strong foundation for corporate IT operations.

1.2 Motivation

The motivation for developing this project came from the need to design a corporate office network that reflects how real-world enterprises operate and manage their IT infrastructure. In a modern office environment, efficient communication, secure data transfer, and reliable connectivity are essential for maintaining productivity. Without a proper network structure, organizations face difficulties such as unmanaged IP addressing, poor scalability, security vulnerabilities, and inefficient resource utilization. This project was designed to overcome these limitations by creating a topology divided into functional zones, each serving a specific purpose to ensure smooth operations. The use of centralized IP allocation, secure external connectivity, controlled traffic management, and inter-zone communication makes the network practical and realistic. Working on this design allowed us to apply classroom knowledge in a simulated enterprise environment, giving us the opportunity to understand how theoretical concepts translate into real implementations.

The ultimate motivation was not only to build a functioning network but also to gain hands-on experience with enterprise-level practices. By designing a scalable and secure infrastructure, we learned how modern organizations address networking challenges, which will be valuable for both academic growth and future professional work. [1].

1.3 Problem Definition

1.3.1 Problem Statement

In a corporate office without a well-structured network, several issues arise, including inefficient IP address management, weak security, poor scalability, and limited communication between departments. Static IP allocation leads to conflicts and management overhead, while the absence of proper routing protocols results in slower or unreliable data transmission. Furthermore, without NAT and ACLs, internal networks remain vulnerable to external threats and unauthorized access. To overcome these challenges, it becomes essential to design a network that integrates automated IP allocation, dynamic routing, secure external communication, and controlled access policies. This project addresses these issues by developing a structured and scalable corporate office network infrastructure.

1.3.2 Complex Engineering Problem

The following Table 1.1 must be completed according to your above discussion in detail. The column on the right side should be filled only on the attributes you have chosen to be touched by your own project.

Table 1.1: Summary of the attributes touched by the mentioned projects

Name of the P Attributess	Explain how to address
P1: Depth of knowledge required	Addressed through applying core networking concepts such as IP addressing, routing, and security configurations.
P2: Range of conflicting requirements	Managed by balancing performance, scalability, and security in the design.
P3: Depth of analysis required	Ensured by testing and validating connectivity, routing, and access policies in the simulation.
P4: Familiarity of issues	Tackled by using well-known networking challenges like address allocation, packet loss, and access control.
P5: Extent of applicable codes	Followed standard networking practices and protocols supported within Cisco Packet Tracer.
P6: Extent of stakeholder involvement and conflicting requirements	Considered by simulating real-world needs of users, administrators, and external connections.
P7: Interdependence	Handled by ensuring all services (DHCP, NAT, ACLs, routing) work together seamlessly without conflict.

1.4 Design Goals/Objectives

The primary goal of this project is to design and implement a corporate office network infrastructure that ensures secure, reliable, and efficient communication across the organization. The project aims to create a structured topology that connects different zones within the office while supporting centralized resource sharing and seamless internal as well as external communication. One of the key objectives is to establish proper IP address management through automated allocation, ensuring that devices are configured correctly and network conflicts are avoided. Another important objective is to enhance security by segmenting the network into zones and controlling access to sensitive resources, which mirrors the standards of enterprise-level networking. At the same time, the network has been designed with scalability in mind so that additional departments, devices, or services can be integrated in the future without major restructuring. By simulating real-world networking practices, the project also seeks to provide practical learning outcomes, allowing us to apply theoretical knowledge in a hands-on environment and better understand how organizations manage and secure their IT infrastructure.

1.5 Application

The corporate office network infrastructure designed in this project has wide applications in real-world enterprise and institutional environments. In a corporate setting, the network ensures seamless connectivity between different departments, allowing employees to share resources such as files, printers, and application servers without interruption. By segmenting the network into Access, Core, and Distribution zones, the design supports efficient traffic flow, minimizes congestion, and provides an organized framework for scaling as the company grows. A key application of this design is in ensuring secure and reliable internet access. With NAT configured on edge routers, internal devices can communicate with external networks while still protecting private IP addresses, thereby improving overall security. ACLs further enhance this by restricting unauthorized access and enforcing company policies on which types of traffic are allowed. In addition, the DHCP configuration automates IP address assignment across the network, which reduces manual workload, prevents address conflicts, and ensures smooth onboarding of new devices. This network model can also be applied to other organizations beyond corporate offices, such as universities, banks, hospitals, or government institutions, where multiple departments require interconnectivity with controlled access. For instance, in a university, the Access Zone could connect student labs, while the Core Zone manages faculty networks, and the Distribution Zone hosts servers for academic resources. Similarly, in banks or government offices, this design can provide both secure internal communication and controlled external connectivity. [1] also.

Chapter 2

Design/Development/Implementation of the Project

2.1 Introduction

In today's world, computer networks have become the backbone of every modern organization, enabling communication, resource sharing, and secure access to information. A corporate office relies heavily on its network infrastructure to maintain smooth operations, whether it is for internal communication, connecting different departments, or providing secure access to external services. Without a well-structured network, organizations face problems such as poor connectivity, unmanaged resources, and vulnerabilities that can disrupt daily activities. To address these needs, this project focuses on the design and implementation of a corporate office network infrastructure using Cisco Packet Tracer. The design mirrors a real-world enterprise setup by dividing the topology into functional zones, ensuring that communication remains reliable, security is maintained, and resources are efficiently managed. By incorporating practical networking concepts into a simulated corporate environment, the project demonstrates how a properly planned infrastructure can improve organizational productivity and provide a foundation for future growth. [2] [3] [4].

2.2 Project Details

The project is centered on the design and implementation of a corporate office network infrastructure in Cisco Packet Tracer. The network has been built to reflect the requirements of a real enterprise environment, focusing on secure communication, efficient resource management, and reliable connectivity across all zones of the office. The design ensures that departments are interconnected, resources are accessible, and external communication is enabled without compromising security.

Network Topology

The network topology is divided into three main zones: Access, Core, and Distribution. The Access Zone contains end devices such as PCs and laptops along with DHCP servers that dynamically assign IP addresses, ensuring smooth and automated configuration for all users. The Core Zone acts as the backbone of the entire network, linking the Access and Distribution zones and providing redundancy to maintain high availability. The Distribution Zone hosts application servers and services required by the organization while also handling secure external communication through NAT. This structured segmentation improves manageability, security, and performance of the network.

Device Configuration

A range of devices is used in this project to emulate a corporate setup. Routers are responsible for interconnecting the zones and ensuring efficient routing of traffic, while switches provide Layer 2 connectivity within each zone. Servers are deployed to run critical functions such as DHCP, NAT, and enterprise applications. End devices such as desktops and laptops represent the employees of the organization, showcasing how users interact with the network. Each device has been configured according to an addressing scheme that uses private IP ranges internally and translates them into public IPs when accessing external resources.

Network Services

Several important services have been integrated into the design. DHCP is configured to automate IP address allocation across the zones, ensuring conflict-free and efficient address management. NAT is implemented on the edge routers to allow internal devices to communicate with external networks securely, protecting the internal addressing scheme from exposure. Access Control Lists (ACLs) are applied to regulate traffic, ensuring that only authorized communication is permitted. Additionally, VPN functionality is simulated to demonstrate secure inter-zone connectivity, which is a common requirement in real-world corporate networks.

Routing and Communication

Dynamic routing is configured to enable reliable communication between different parts of the network. Each zone uses appropriate routing mechanisms to ensure efficient data transfer, scalability, and optimized path selection. Routing tables have been carefully designed to support connectivity between devices while also maintaining flexibility for future expansion. To validate the design, connectivity tests such as ping and traceroute were conducted, showing that devices can communicate across zones, obtain IP addresses dynamically, and securely access external resources.

Results and Verification

The final network demonstrates all the intended functionalities of a corporate office setup. End devices are able to communicate within and across zones, servers provide centralized services, and the external connection is established without compromising internal security. Dynamic IP assignment works correctly, NAT ensures safe public access, and ACLs enforce traffic policies effectively. The network operates smoothly, confirming that the design goals have been achieved.

2.2.1 Subsection_name

You can fix the height, width, position, etc., of the figure accordingly.

Figure 2.1: Figure name

2.3 Implementaion

The workflow

The workflow of this project followed a systematic approach, starting with the planning and analysis of how a corporate office network should be structured to meet the requirements of a real enterprise environment. The first stage involved designing the topology in Cisco Packet Tracer, where the network was divided into three zones—Access, Core, and Distribution—to ensure that devices, servers, and services were properly organized. Once the layout was complete, routers, switches, servers, and end devices were placed and interconnected according to the design. After the physical arrangement, the logical configuration began with the assignment of IP addresses and the setup of DHCP servers, which automated the allocation of IPs across different subnets and ensured that devices were connected without conflicts.

With the addressing scheme in place, routing configurations were applied so that communication between the zones could take place efficiently, and the flow of data could adapt to different paths in the network. Network Address Translation was then configured on the edge routers to allow internal devices to access external networks securely while hiding private IP addresses. To strengthen security, Access Control Lists were implemented, restricting unauthorized traffic and enforcing access rules based on organizational needs. Once the core configurations were completed, the workflow moved into the testing phase, where tools like ping and traceroute were used within Packet Tracer to validate connectivity, verify DHCP functionality, and check secure communication across all zones. Each stage of the workflow built upon the previous one, moving logically from planning and design to configuration, implementation, and testing. This structured process ensured that the final network was not only functional but also secure, scalable, and aligned with real-world corporate networking practices.

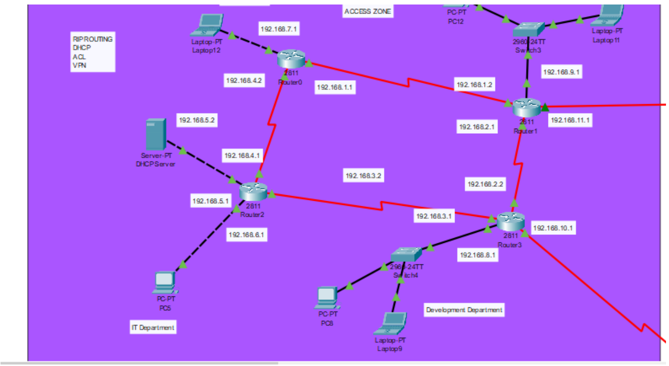


Figure 2.2: Figure 1: Access part

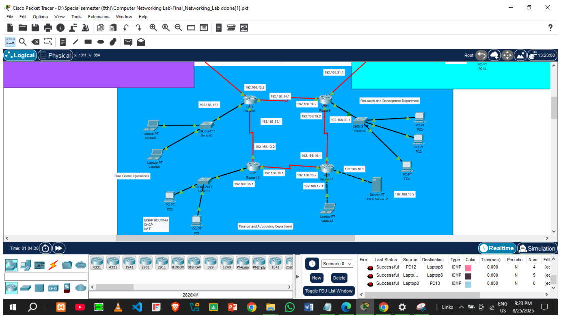


Figure 2.3: Core Part

Tools and libraries

The primary tool used for this project is Cisco Packet Tracer, a powerful simulation software that allows the design, configuration, and testing of network topologies in a virtual environment. Packet Tracer was used to create the corporate office infrastructure, configure devices such as routers, switches, servers, and end-user systems, and verify communication across different zones of the network. Within this environment, built-in configuration options and command-line interfaces provided the necessary functions to implement services like DHCP, NAT, ACLs, and routing. No external programming libraries were required, as the entire project was developed and tested within Packet Tracer's simulation platform. This made it possible to replicate real-world enterprise networking features in a controlled and flexible virtual setup, providing both accuracy and ease of learning.

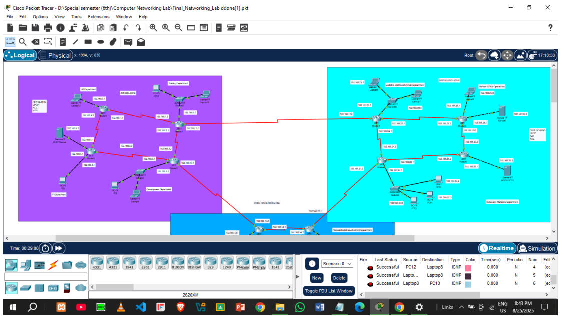
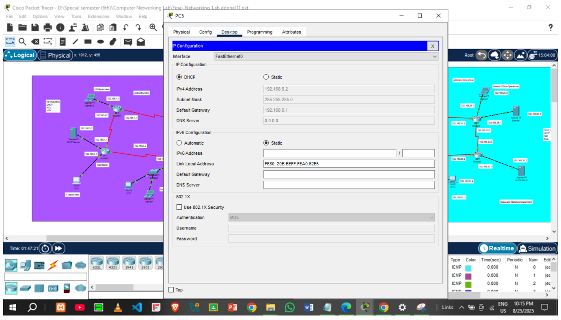


Figure 2.4: Figure1:Network Design

Implementation details (with screenshots and programming codes)



PC5 — Desktop — IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.6.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.6.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

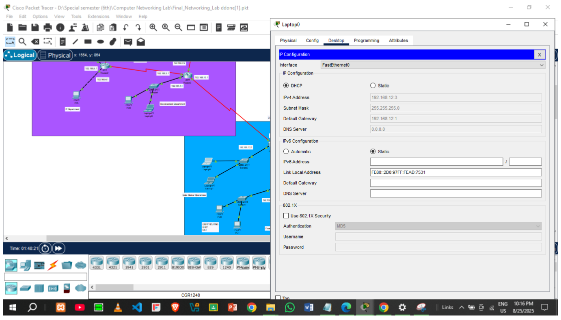
Link Local Address: FE80::20B:BEFF:FEA0:62E5

802.1X

□ Use 802.1X Security

Authentication: MD5

Figure 1: Ip setup



Laptop0 — Desktop — IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.12.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.12.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

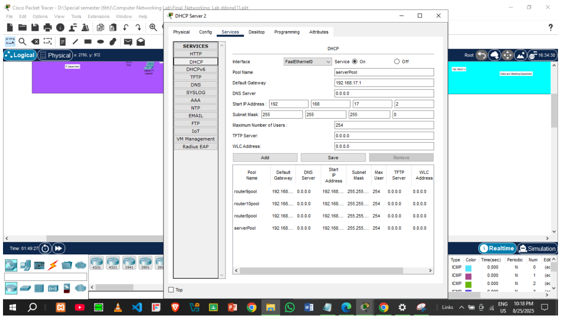
Link Local Address: FE80::2D0:97FF:FEAD:7531

802.1X

□ Use 802.1X Security

Authentication: MD5

Figure 2: Initial Pc setup



DHCP Server 2 — Services — DHCP

Interface: FastEthernet0 Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 192.168.17.1

DNS Server: 0.0.0.0

Start IP Address : 192 168 17 2

Subnet Mask: 255 255 255 0

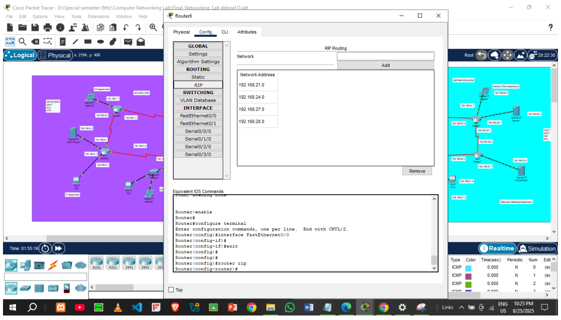
Maximum Number of Users : 254

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
router9pool	192.168....	0.0.0.0	192.168....	255.255....	254	0.0.0.0	0.0.0.0
router10pool	192.168....	0.0.0.0	192.168....	255.255....	254	0.0.0.0	0.0.0.0
router8pool	192.168....	0.0.0.0	192.168....	255.255....	254	0.0.0.0	0.0.0.0
serverPool	192.168....	0.0.0.0	192.168....	255.255....	254	0.0.0.0	0.0.0.0

Figure 3: DHCP



Router6 — Config — RIP Routing

Network Address

192.168.21.0

192.168.24.0

192.168.27.0

192.168.28.0

Equivalent IOS Commands

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#router rip
Router(config-router)#
```

Figure 4: Dynamic Setup

Kindly, check the workflow, tools and library part for more information. Screenshots have been attached there.

2.4 Algorithms

Design the Topology: Divide the corporate network into three zones — Access Zone, Core Operations Zone, and Distribution Zone — and place routers, switches, servers, and end devices accordingly.

Assign IP Addressing: Allocate private IP ranges for each zone and configure addressing on routers and end devices following the subnet design.

Configure Routing Protocols: Enable and configure routing protocols (EIGRP in the core, OSPF in the distribution, and RIP where applicable) to ensure dynamic path selection and full connectivity between zones.

Setup DHCP Servers: Configure centralized DHCP servers with pools for each subnet, enabling automatic and conflict-free IP allocation to client devices.

Implement NAT: Configure NAT on edge routers to allow internal devices to access external networks while maintaining security with private IP addressing.

Apply ACLs: Define and apply Access Control Lists to control traffic flows, enforce security policies, and restrict unauthorized access between zones.

Verify Connectivity: Use testing tools like ping and traceroute within Packet Tracer to confirm correct routing, DHCP assignments, NAT functionality, and ACL restrictions.

-

Algorithm 1: Sample Algorithm

```
Input: Your Input
Output: Your output
Data: Testing set $x$
$\sum_{i=1}^{\infty} := 0$                          // this is a comment
/* Now this is an if...else conditional loop               */
if Condition 1 then
    Do something                                // this is another comment
    if sub-Condition then
        Do a lot
else if Condition 2 then
    Do Otherwise
    /* Now this is a for loop                              */
    for sequence do
        loop instructions
else
    Do the rest
/* Now this is a While loop                                */
while Condition do
    Do something
```

Chapter 3

Performance Evaluation

3.1 Simulation Environment/ Simulation Procedure

The project was simulated using Cisco Packet Tracer, which provided the required environment to design, configure, and test the corporate office network.

The simulation included routers, switches, DHCP servers, NAT configuration, ACLs, and client devices, all arranged into Access, Core, and Distribution zones.

Private IP ranges were used internally, with NAT enabled at the edge routers for external connectivity.

The environment setup was done on a standard workstation capable of running the latest Packet Tracer version without additional tools or libraries.

Simulation Procedure

The network topology was first designed and organized into three zones with appropriate devices placed in each.

IP addressing was configured for all routers, switches, servers, and client devices based on the chosen addressing scheme.

DHCP servers were set up to dynamically allocate IP addresses to hosts, ensuring conflict-free configuration.

Dynamic routing protocols were enabled and verified to ensure smooth connectivity between the zones.

NAT configuration was applied on the edge routers to translate private addresses for secure external access.

ACL rules were defined and implemented to control the flow of traffic and restrict unauthorized communication.

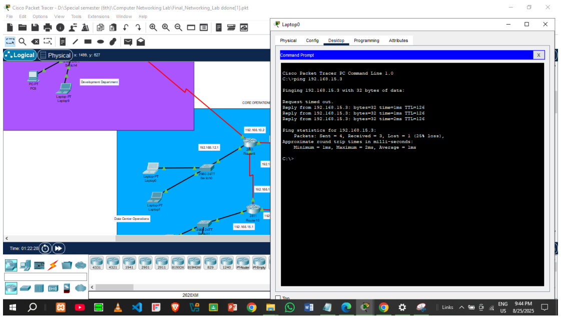
Connectivity testing was performed using ping and traceroute to validate routing, DHCP, NAT, and ACL functionalities.

Simulation Mode was used to trace packet movements and verify the accuracy of routing tables, address assignments, and access policies.

3.2 Results Analysis/ Testing

3.2.1 Result_portion_1

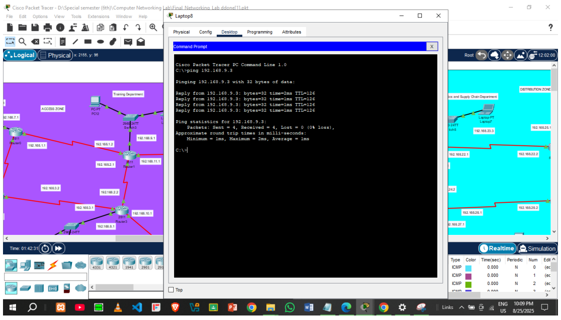
The results of the network simulation are shown below. The image demonstrates connectivity, DHCP assignment, and routing between zones.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.15.3

Pinging 192.168.15.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.15.3: bytes=32 time=1ms TTL=126
Reply from 192.168.15.3: bytes=32 time=1ms TTL=126
Reply from 192.168.15.3: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.15.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Figure 5: Connection Successful from both side

3.2.2 Result_portion_2



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.9.3

Pinging 192.168.9.3 with 32 bytes of data:

Reply from 192.168.9.3: bytes=32 time=2ms TTL=126
Reply from 192.168.9.3: bytes=32 time=1ms TTL=126
Reply from 192.168.9.3: bytes=32 time=1ms TTL=126
Reply from 192.168.9.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.9.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Figure 6: perfect ping response

3.2.3 Result_portion_3

3.3 Results Overall Discussion

The implemented corporate office network demonstrates that the design meets all intended objectives and performs as expected in a simulated environment. All end devices in the Access Zone successfully receive dynamic IP addresses from the DHCP servers, eliminating configuration conflicts and ensuring smooth onboarding of new devices. Inter-zone communication through the Core and Distribution zones is fully operational, with routing tables reflecting correct path selection and redundancy. The NAT configuration at the edge routers allows secure external connectivity while protecting internal IP addressing, and Access Control Lists effectively restrict unauthorized access, confirming that security policies are enforced correctly. Connectivity tests, including ping and traceroute, show reliable data transfer between all zones and proper access to external resources. Overall, the simulation validates that the network is scalable, secure, and efficient, reflecting the design principles outlined in the project and providing a strong foundation for real-world corporate networking scenarios.

3.3.1 Complex Engineering Problem Discussion

[OPTIONAL] In this subsection, if you want, you can discuss in details the attributes that have been touched by your project problem in details. This has already been mentioned in the Table **??**.

Chapter 4

Conclusion

4.1 Discussion

This project successfully demonstrates the design and implementation of a corporate office network infrastructure that reflects the requirements of a real-world enterprise. The network is organized into three main zones—Access, Core, and Distribution—to ensure structured connectivity, efficient resource management, and secure communication across the organization. End devices in the Access Zone receive dynamic IP addresses through DHCP, simplifying configuration and preventing address conflicts. The Core Zone functions as the backbone, maintaining reliable inter-zone communication and redundancy, while the Distribution Zone hosts essential servers and manages external connectivity through NAT. Access Control Lists are strategically applied to regulate traffic and enforce security policies, ensuring that only authorized communication occurs between different parts of the network. Dynamic routing protocols facilitate efficient path selection and scalability, allowing the network to adapt to growing organizational needs. Simulation tests including ping, traceroute, and packet inspection confirm that all components operate as intended, demonstrating seamless internal communication, secure external access, and correct enforcement of access policies. Overall, the project highlights how a carefully planned and implemented network can enhance productivity, maintain security, and provide a solid foundation for future expansion, making it a practical learning experience and a realistic model of enterprise networking practices.

4.2 Limitations

Although the project successfully demonstrates the design of a corporate office network infrastructure, there are certain limitations that restrict its real-world application. Since the implementation has been carried out in Cisco Packet Tracer, it only provides a simulated environment and cannot fully replicate the performance of actual hardware devices under real traffic conditions. Important aspects such as bandwidth consumption, latency, packet loss, and fault tolerance are not tested in this setup. The security of the network is limited as well, because advanced protective measures like firewalls, intrusion detection systems, and monitoring tools have not been included. Another limitation is that the design is built entirely on IPv4 addressing, which reduces its long-term adaptability given that many organizations are now transitioning to IPv6 to meet modern networking standards. These factors highlight the gap between the simulated environment and the challenges faced in deploying a real enterprise-level infrastructure.

4.3 Scope of Future Work

There is significant potential to expand and improve this project in the future. One of the key enhancements would be the integration of IPv6 addressing to ensure better scalability, efficiency, and global compatibility. The design could also be extended to include more departments and users, as well as wireless networks, to create a more comprehensive office environment. Advanced security mechanisms such as firewalls, intrusion detection and prevention systems, and strict access policies could be implemented to strengthen protection against external and internal threats. Future versions of the network could also adopt redundancy features like backup routers and failover links to maintain high availability during failures. In addition, the project could be enhanced with cloud integration, virtualization, and remote office connectivity to reflect the hybrid and distributed networks commonly used in modern organizations. These improvements would make the infrastructure more practical, secure, and aligned with the evolving demands of enterprise networking.

References

[1] Omid C Farokhzad and Robert Langer. Impact of nanotechnology on drug delivery. *ACS nano*, 3(1):16–20, 2009.

[2] Uthayasankar Sivarajah, Muhammad Mustafa Kamal, Zahir Irani, and Vishanth Weerakkody. Critical analysis of big data challenges and analytical methods. *Journal of Business Research*, 70:263–286, 2017.

[3] Douglas Laney. 3d data management: controlling data volume, velocity and variety. gartner, 2001.

[4] MS Windows NT kernel description. `http://web.archive.org/web/20080207010024/http://www.808multimedia.com/winnt/kernel.htm`. Accessed Date: 2010-09-30.