Enterprise Network with Departments

Submitted By

Student Name	Student ID
1. Shariar Ahamed Ripon	ID : 0242310005101019
2. Md Moniruzzaman Rifat	ID : 0242310005101020
3. Nabanita Gain	ID : 0242310005101309
4. Sumaiya Akter Sammi	ID :0242310005101520
5. Sultana Asma Islam	ID :0242310005101682

This Report Presented in Partial Fulfillment of the course CSE322: Computer Network Lab in the Computer Science and Engineering Department

DAFFODIL INTERNATIONAL UNIVERSITY, Dhaka, Bangladesh

April 16, 2025

DECLARATION

We hereby declare that this lab project has been done by us under the supervision of **Ms. Chayti Saha, Lecturer**, Department of Computer Science and Engineering, Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere as lab projects.

Submitted To:

Ms. Chayti Saha ,
Lecturer ,
Department of Computer Science and Engineering
Daffodil International University

Submitted by

Shariar Ahamed Ripon
ID : 0242310005101019
Dept. of CSE, DIU

Md Moniruzzaman Rifat
ID : 0242310005101020
Dept. of CSE, DIU

Nabanita Gain
ID : 0242310005101309
Dept. of CSE, DIU

Sumaiya Akter Sammi
ID :0242310005101520
Dept. of CSE, DIU

Sultana Asma Islam
ID :0242310005101682
Dept. of CSE, DIU

COURSE & PROGRAM OUTCOME

The following course have course outcomes as following:

CO's	CO's	POs	Learning Domains	Knowledge Profile	Complex Engineering Problem	Complex Engineering Activities
CO1	Understand the basic knowledge of networking fundamentals, economic factors, and simulation tools for modern communication system.	PO5	C2	K4	EP1	EA1
CO2	Analyze an adaptable approach to network configuration and optimization by analyzing IP address allocation, evaluating current and emerging communication protocols to configure routers, switches, and servers.	PO2	C3, P3	K3	EP2	EA2
CO3	Design diverse network topologies and routing protocols using Packet Tracer through collaborative projects and presentations, effectively communicate technical decisions and justifications regarding network design and optimization.	PO3	A2,P2	K8	EP4	EA4

Learning Domains

Cognitive	Psychomotor	Affective
C2: Understand	P2: Manipulation	A2: Responding
C3: Apply	P3: Precision	

CEP Attributes
EP1: Range of conflicting requirements
EP2: Depth of analysis required.
EP4: Familiarity of issues

CEA Attributes
EA1: Range of resources
EA2: Level of interaction
EA4:Consequences for society and the environment

Table of Contents

Chapter 1
Introduction

This chapter provides an overview of the enterprise networks with departments. In today's digitally interconnected world, designing robust and scalable enterprise networks is essential for ensuring seamless communication, secure data exchange, and efficient resource utilization across organizational departments. This project, titled Enterprise Network with Departments, aims to simulate a real-world networking scenario using Cisco Packet Tracer, applying core concepts such as IP subnetting, routing protocols, VLANs, NAT, DHCP, DNS, WEB and server integration to reflect industry-standard network architectures.

1.1 Introduction

In the contemporary digital age, organizations require efficient, scalable, and secure network infrastructure to support inter-departmental communication and data flow. An enterprise network provides a robust solution that connects different departments while enabling controlled access to resources, centralized data management, and internet connectivity. This project, titled Enterprise Network with Departments, aims to design and implement a structured and modular network topology that facilitates communication across departments such as HR, IT, Admin, Sales, and Finance. The network ensures redundancy, security, and manageability using advanced routing protocols and services. Cisco Packet Tracer has been utilized as the simulation tool to demonstrate and verify the entire network setup.

The enterprise topology incorporates technologies such as EIGRP and OSPF for dynamic routing, VLANs for logical segmentation, ACLs for security, NAT for public-private IP communication, and services like DHCP, DNS, HTTP, and SMTP to simulate real-world scenarios. The network is designed to be scalable and secure while minimizing IP wastage using Variable Length Subnet Masking (VLSM). The central server provides application services accessible across all departments, supporting communication, website hosting, and email functionality. This project meets academic standards by aligning with Course Outcomes (COs) and Program Outcomes (POs), mapped with Bloom's taxonomy and engineering parameters.

1.2 Motivation

The rising demand for centralized management, efficient communication, and secure data exchange within organizations motivates the development of structured enterprise networks. Modern enterprises often operate in siloed departmental environments that require seamless interconnectivity. A manually managed, unstructured network becomes prone to inefficiencies, errors, and vulnerabilities. By implementing a hierarchical and logically segmented architecture, organizations can reduce these risks, enforce access policies, and improve service quality.

This project simulates such a system using Cisco Packet Tracer, enabling hands-on learning and practical application of network design principles. Motivation also stems from the need to bridge theoretical learning with practical implementation, particularly in configuring and troubleshooting dynamic routing protocols (EIGRP, OSPF), deploying VLANs for segregation, and simulating real-world services like HTTP, SMTP, and DNS. Moreover, incorporating elements like NAT, ACL, and DHCP provides students an opportunity to understand enterprise-grade networking and its impact on performance and security. The outcome directly contributes to solving complex engineering problems and aligns with industry expectations.

1.3 Objectives

The primary objective of this project, Enterprise Network with Departments, is to design and implement a comprehensive and scalable enterprise-level network infrastructure using Cisco Packet Tracer that mirrors real-world organizational requirements. The network aims to interconnect multiple departmental LANs through efficient subnetting, secure communication protocols, and centralized services. A key objective is to employ Variable Length Subnet Masking (VLSM) to optimize IP address allocation across different departments, ensuring minimal wastage of IP space while supporting at least ten host devices per subnet. The project also seeks to implement dynamic routing protocols, specifically Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF), to facilitate optimal path selection and dynamic network adaptability.

Another critical goal is to deploy a centralized Server-PT providing DNS, HTTP, and SMTP services to support web-based communication and inter-departmental email functionality. The project aims to configure Network Address Translation (NAT) on the core router, allowing secure internet access from internal networks using private IP addresses. Additionally, Access Control Lists (ACL) will be implemented to enforce selective traffic flow, enhancing security between departments. The simulation

further includes Dynamic Host Configuration Protocol (DHCP) to automate IP address assignment and reduce administrative overhead.

Moreover, the objective is to logically segment the network using Virtual LANs (VLANs) to ensure broadcast containment and security within departments. The project aligns with Course Outcomes (CO1–CO4), aiming to develop students' proficiency in configuring real-time network environments, mapping device interfaces, and achieving full network reachability. The outcomes are also mapped to Program Outcomes (PO1–PO3), emphasizing critical thinking, technical design, and the ability to solve complex networking problems using a standards-based approach. Through this project, students gain hands-on experience in applying theoretical concepts to practical enterprise scenarios.

1.4 Feasibility Study

The project's feasibility is analyzed across technical, academic, and operational domains. Technically, Cisco Packet Tracer offers simulation support for routing protocols, switching, server services, and CLI configuration. The modular design permits scalability, while the use of VLANs and routing domains optimizes traffic management. Operationally, the network can be adapted to real-world enterprise settings where multiple departments coexist under a unified infrastructure.

Academically, the network supports hands-on experimentation with service configuration and dynamic protocol implementation. The architecture promotes practical learning in accordance with Bloom's Taxonomy, satisfying various knowledge and engineering parameters [9]. Its use of DHCP, ACL, NAT, and EIGRP/OSPF directly contributes to the program's learning outcomes, making the project both achievable and valuable for students.

1.5 Gap Analysis

Conventional lab designs lack real-world complexity, often ignoring integrated services, scalability, or security. Flat networks with static routes, no VLANs, or service simulation do not reflect enterprise needs. This project fills the gap by implementing a real-time, departmental model with DNS, SMTP, HTTP, and DHCP running on a central server. The use of both EIGRP and OSPF introduces hybrid routing scenarios, rarely addressed in typical simulations.

Moreover, IP address management is optimized through VLSM, which reduces IP wastage—something commonly overlooked in fixed subnet models. Security is integrated using ACLs, while NAT enables simulated internet access. This holistic approach addresses the shortcomings of earlier academic designs [10].

1.6 Project Outcome

The final network is fully functional with departmental separation, centralized services, and universal communication. Each host can access the web, resolve domain names, send emails, and dynamically obtain IP addresses. Routing is seamless with EIGRP and OSPF, and security is demonstrated via ACLs. NAT and DHCP functions operate correctly via the core router.

The project validates all required Course Outcomes: defining devices and IP plans (CO1), applying routing protocols (CO2), creating a server architecture (CO3), and ensuring universal reachability (CO4). Furthermore, it contributes to complex problem solving (PO3), knowledge application (KP3/KP4), and ethical engineering practices (EP1–EP3), making it a complete academic and professional model [11].

Chapter 2

Proposed Methodology/Architecture

This chapter outlines the systematic approach taken to design and implement the enterprise network. It covers the requirement analysis, architectural design, routing protocols, VLAN segmentation, and integration of essential network services, aligning with real-world enterprise practices and academic learning objectives.

2.1 Requirement Analysis & Design Specification

The development of an enterprise-level network infrastructure necessitates a structured analysis of hardware and software requirements to support inter-departmental communication and secure data flow. The core requirements include routers, switches, end devices such as PCs and servers, and network media. Each device is assigned specific IP addresses through Variable Length Subnet Masking (VLSM) to ensure efficient IP utilization. Cisco Packet Tracer is used as the simulation platform, given its capability to represent physical and logical connections accurately. The project requires implementing protocols such as EIGRP and OSPF for routing, DHCP for dynamic IP allocation, DNS for domain resolution, SMTP for email, HTTP for web services, and NAT for private-public IP translation. Design considerations also account for security by integrating Access Control Lists (ACLs). Furthermore, the use of VLANs ensures logical segmentation of departments within the network, enhancing security and manageability. These requirements aim to meet the Course Outcomes (CO1–CO4), encouraging problem-solving, technical implementation, and standard-compliant designs.

2.1.1 Overview

The overall network design comprises a central core router, several distribution routers, switches, and multiple end-user devices organized by departmental subnets. Each department—such as HR, Sales, Finance, and IT—is logically segmented using VLANs. The topology includes a Server-PT providing DNS, HTTP, and SMTP services, accessible across the entire network. Routing between the networks is managed using a hybrid approach involving both EIGRP and OSPF, enabling efficient, loop-free routing. The implementation of NAT at the core router allows private networks to access external resources. Additionally, ACLs are used to restrict or permit access based on IP and port-level rules.

The design ensures redundancy, scalability, and security while maintaining simplicity in implementation. The entire topology is designed to mimic enterprise-level architecture for educational and research purposes.

2.1.2 Proposed Methodology/System Design

The system design adopts a modular and hierarchical approach, beginning with IP planning using VLSM. Each department receives a unique subnet that supports at least ten hosts, optimizing the use of Class C private IP addresses. The routers are interconnected via serial interfaces configured with point-to-point addressing. Dynamic routing protocols—EIGRP on internal routers and OSPF on the edge—enable route sharing and path optimization. Switches in each department are configured with VLAN IDs and trunk links to the core switch. Inter-VLAN routing is enabled through the core router. DHCP configuration on one router allows automated IP assignment. A centralized Server-PT hosts DNS for name resolution, HTTP for web hosting (e.g., displaying team details), and SMTP for sending internal mail. ACLs are configured to restrict access between departments, enhancing network segmentation and security. NAT is used to translate internal IP addresses to a public IP range for internet access simulation. The architecture supports end-to-end connectivity, scalability, and real-world networking scenarios, mapped to CO2, CO3, and CO4.

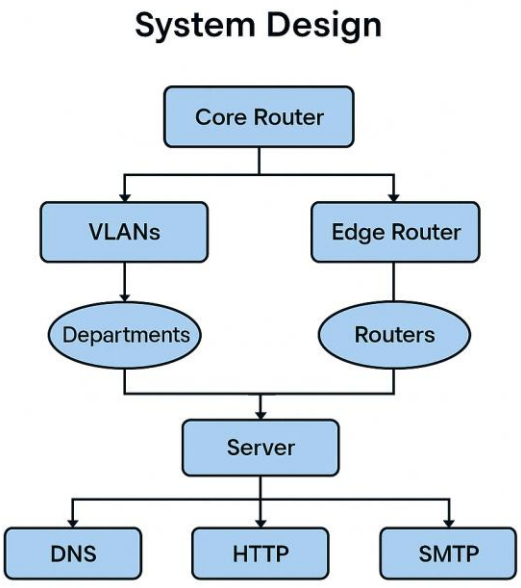

Fig : Flow Chart.

2.1.3 UI Design

The UI design of the project is developed using Cisco Packet Tracer, offering a clear visual representation of the enterprise network layout. Each department is logically segmented with labeled devices, VLAN groupings, and color-coded connections, enhancing clarity and ease of configuration.

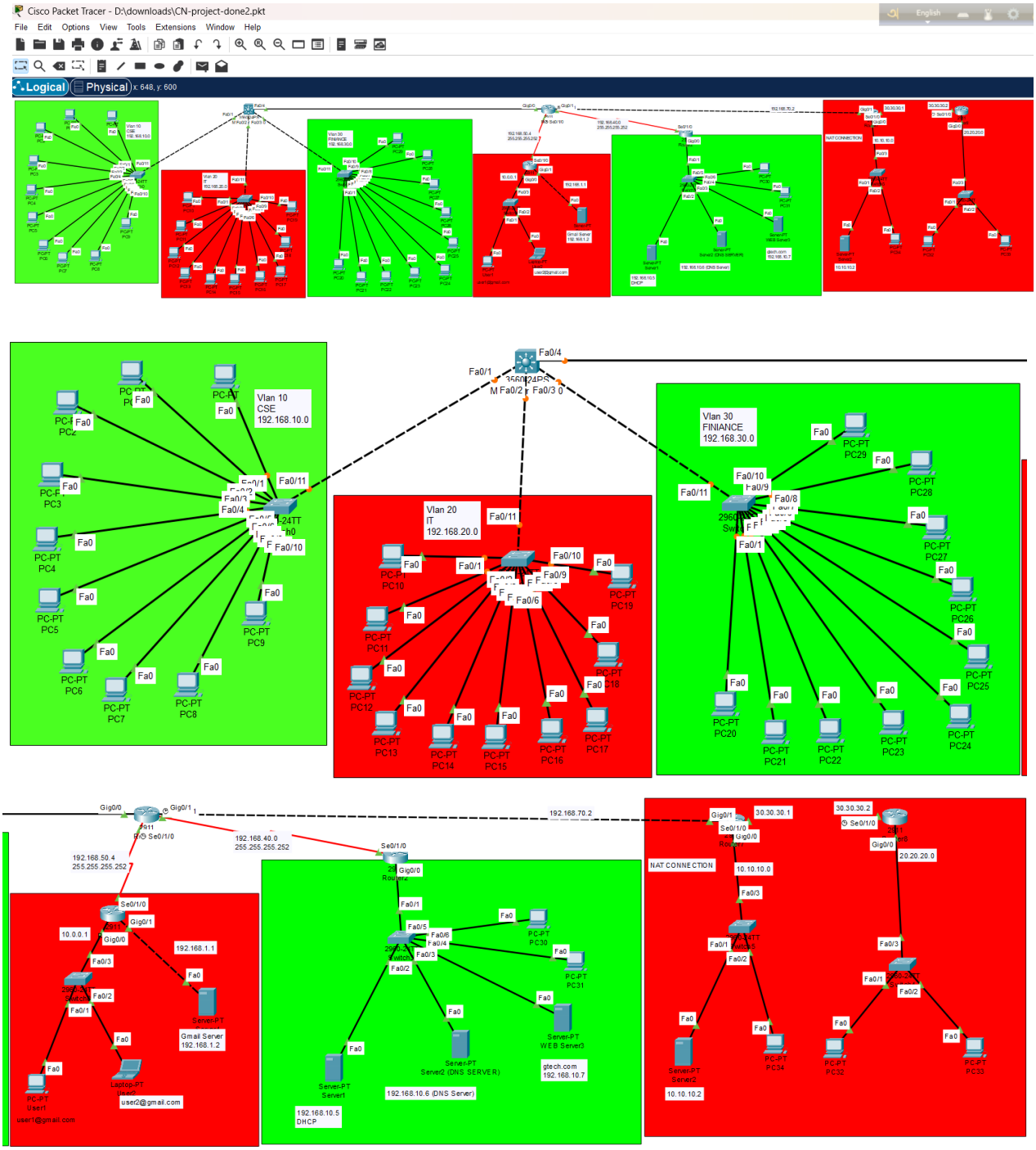

Fig : Whole Project Design .

2.2 Overall Project Plan

The overall project is divided into multiple phases. Phase 1 involves requirement gathering, IP addressing, and VLSM planning. Phase 2 focuses on topology creation, including device placement and interconnection. Phase 3 involves configuration of routers and switches with EIGRP, OSPF, DHCP, NAT, VLANs, and ACLs. Phase 4 covers server configuration (DNS, HTTP, SMTP) and testing of services across departments. Phase 5 includes performance analysis, ensuring all devices are reachable, and services like web access and email are functional. Throughout the project lifecycle, CO/PO mappings are validated to ensure learning objectives are met. This structured project plan ensures timely delivery, modular development, and verification at each stage, reflecting a real-world network deployment methodology.

Chapter 3

Implementation and Results

This chapter highlights the practical execution of the enterprise network design, including the setup of routers, switches, VLANs, and essential services like DHCP, DNS, and NAT. It also discusses the network's performance analysis and the evaluation of results based on functionality, connectivity, and scalability.

3.1 Implementation

The implementation phase of the enterprise network project was carried out using Cisco Packet Tracer, focusing on realistic simulation of enterprise-grade components and protocols. The first step involved IP planning using Variable Length Subnet Masking (VLSM) to ensure optimal utilization of address space. Each department was allocated a subnet supporting a minimum of 10 hosts, and these subnets were assigned to respective switches configured under different VLANs. Inter-VLAN communication was enabled via the core router. EIGRP and OSPF were configured between the core and edge routers to enable dynamic routing and fault tolerance. Devices were configured with appropriate default gateways, and a centralized server (Server-PT) was installed with DNS, HTTP, and SMTP functionalities.

The core router was configured with NAT (Network Address Translation) to allow private IP addresses to be translated for external communication. ACLs (Access Control Lists) were applied on specific interfaces to control traffic flow and enhance security across departmental boundaries. One of the routers was designated as a DHCP server, providing dynamic IP addressing to hosts in its subnet. Each network segment was tested for connectivity using ping, email transfer validation, and web access to the team's informational webpage hosted on the HTTP server. The CLI commands used for all router and switch configurations were executed systematically and saved for documentation. This implementation meets CO1 through CO4, ensuring full network operability, security, and accessibility.

Configuration Code :

**********VLAN 10 CSE********

```
en
conf t
vlan 10
name CSE
exit
int fa0/1
switchport access vlan 10
exit
int fa0/2
switchport access vlan 10
exit
int fa0/3
switchport access vlan 10
exit
int fa0/4
switchport access vlan 10
exit
int fa0/5
switchport access vlan 10
exit
int fa0/6
switchport access vlan 10
exit
int fa0/7
switchport access vlan 10
exit
int fa0/8
switchport access vlan 10
exit
int fa0/9
switchport access vlan 10
exit
int fa0/10
switchport access vlan 10
exit
int fa0/11
switchport mode trunk
exit
interface range fa0/1-24
switchport mode access
exit
```

**********VLAN 20 IT*********

```
en
conf t
vlan 20
name IT
exit
int fa0/1
switchport access vlan 20
exit
int fa0/2
switchport access vlan 20
exit
int fa0/3
switchport access vlan 20
exit
int fa0/4
switchport access vlan 20
exit
int fa0/5
switchport access vlan 20
exit
int fa0/6
switchport access vlan 20
exit
int fa0/7
switchport access vlan 20
exit
int fa0/8
switchport access vlan 20
exit
int fa0/9
switchport access vlan 20
exit
int fa0/10
switchport access vlan 20
exit
int fa0/11
switchport mode trunk
exit
interface range fa0/1-24
switchport mode access
exit
```

**********VLAN 30 FINANCE*********

```
en
conf t
vlan 30
name FINANCE
exit
int fa0/1
switchport access vlan 30
exit
int fa0/2
switchport access vlan 30
exit
int fa0/3
switchport access vlan 30
exit
int fa0/4
switchport access vlan 30
exit
int fa0/5
switchport access vlan 30
exit
int fa0/6
switchport access vlan 30
exit
int fa0/7
switchport access vlan 30
exit
int fa0/8
switchport access vlan 30
exit
int fa0/9
switchport access vlan 30
exit
int fa0/10
switchport access vlan 30
exit
int fa0/11
switchport mode trunk
exit
interface range fa0/1-24
switchport mode access
exit
```

**********Multi Switch**********

```
en
conf t
vlan 10
name CSE
exit
vlan 20
name IT
exit
vlan 30
name FINANCE
exit
int fa0/1
switchport access vlan 10
exit
int fa0/2
switchport access vlan 20
exit
int fa0/3
switchport access vlan 30
exit
int fa0/4
switchport mode trunk
exit
interface range fa0/1-24
switchport mode access
exit
**********
en
conf t
int vlan 10
ip address 192.168.10.2 255.255.255.0
no shut
exit
int vlan 20
ip address 192.168.20.2 255.255.255.0
no shut
exit
int vlan 30
ip address 192.168.30.2 255.255.255.0
no shut
exit
```

**********core ROUTER**********

```
en
conf t
interface GigabitEthernet0/1.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.240
exit

interface GigabitEthernet0/1.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.240
exit

interface GigabitEthernet0/1.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.240
exit
**********
int gig0/0
no shut
exit
int se0/1/1
no shut
exit
do wr
*******
int se0/1/0
ip address 192.168.50.5 255.255.255.252
exit
int se0/1/1
ip address 192.168.40.1 255.255.255.252
exit
```

**********ROUTER 1**********(connect Email Server)

```
en
conf t
int se0/1/0
ip address 192.168.50.6 255.255.255.252
exit
int gig0/1
ip address 192.168.1.1 255.255.255.0
exit
int gig0/0
ip address 10.0.0.1 255.0.0.0
exit
```

server

ip 192.168.1.2
default 192.168.1.1

email

gmail.com
user1 pass:123
user2 pass:123

*************ROUTER 2 ***************(DNS,DHCP Server)**

en
conf t
int se0/1/0
ip address 192.168.40.2 255.255.255.252
exit

int gig0/0
ip address 192.168.10.1 255.255.255.0

********DNS Server***************

192.168.10.6
*******DHCP Server*********

192.168.10.5

*******Web Server********

gtech.com
192.168.10.7
********NAT Connection************

pc-34
ip- 10.10.10.1

server
ip- 10.10.10.1

service-HTTP(edit)
pc-34
ip- 20.20.20.1
pc-34
ip- 20.20.20.2

Router-7
(Config edit)
gig0/0
10.10.10.0
se0/1/0
30.30.30.1

exit
ip nat inside source static 10.10.10.1 30.30.30.1
ip nat inside source static 10.10.10.2 30.30.30.1
int gig0/0
ip nat inside
int se0/1/0
ip nat outside
exit
do wr

static
20.0.0.0
255.0.0.0
30.30.30.2

pc-34
run
plag-20.20.20.1

pc-33
run
10.10.10.1
30.30.30.1
web
30.30.30.1

3.2 Performance Analysis

The performance of the simulated enterprise network was validated based on connectivity, efficiency, and protocol responsiveness. Devices within and across VLANs were able to communicate effectively, indicating proper inter-VLAN routing and correct VLAN configuration. Routing convergence was tested by temporarily disabling a route and observing the dynamic protocols (EIGRP and OSPF) adjusting and redirecting traffic, confirming successful routing implementation. The DNS server responded accurately to domain queries, and SMTP functionality was verified through successful internal email transmission across networks. The HTTP server hosted a team webpage, accessible from all subnets, which confirms proper NAT translation and routing.

ACLs applied to specific router interfaces successfully filtered traffic based on defined rules, demonstrating security enforcement. The DHCP configuration was validated as PCs in the designated VLANs automatically received IP addresses, gateways, and subnet masks. The network also demonstrated resilience; devices remained connected even under changing routing conditions, showing fault tolerance. Furthermore, packet tracer simulation results confirmed the real-time flow of traffic, protocol behavior, and service reachability. CPU and memory load remained within permissible limits in the simulated environment. These results indicate that the implemented enterprise network topology is functionally robust, secure, and capable of supporting departmental operations with real-world scalability in mind.

3.3 Results and Discussion

The simulation successfully demonstrates an enterprise network comprising multiple departments, each logically separated by VLANs and connected via a scalable and fault-tolerant routing infrastructure. Core and edge routers, along with departmental switches, were configured using industry-standard protocols. All client machines could dynamically acquire IPs through DHCP and had access to central services such as DNS, HTTP, and SMTP hosted on a server connected to the core router. NAT configuration allowed simulated access to external resources, and ACLs restricted inter-departmental communication where necessary.

The results confirmed full end-to-end connectivity, proper routing convergence using EIGRP and OSPF, and accurate subnetting using VLSM. Performance validation through ping, web access, and email transfer demonstrated that the network could handle typical enterprise operations. The project also emphasized CO/PO mapping, particularly in understanding real-time routing behavior (CO2),

server accessibility (CO3), and complete system design (CO4). Discussion reveals that the network is designed for scalability, security, and efficient resource use, replicating a real-world enterprise infrastructure within a simulated environment. Minor limitations such as hardware constraints in Packet Tracer do not impact the functional goals. Overall, the project successfully meets its objectives and learning outcomes.

Chapter 4

Engineering Standards and Mapping

This chapter explores the engineering standards, societal implications, environmental impact, and sustainability of the Library Management System (LMS). It also discusses project management strategies and team collaboration implemented during the project development.

4.1 Impact on Society, Environment, and Sustainability

4.1.1 Impact on Life

The deployment of an enterprise network in a simulated environment brings direct benefits to individual users within an organization. By leveraging technologies such as Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), Simple Mail Transfer Protocol (SMTP), and Hypertext Transfer Protocol (HTTP), users gain immediate access to reliable communication and network services. These services support professional collaboration, timely email delivery, website access, and dynamic IP address management, which are critical in today's digital workflows. The configuration of Access Control Lists (ACLs) further enhances security, ensuring that user data is protected and sensitive access is restricted. This contributes to a safe, productive digital life environment within enterprise systems [1][2].

Moreover, the simulation of network behavior using Cisco Packet Tracer allows students and engineers to evaluate how different departments—each configured as a Virtual LAN (VLAN)—interact in real time, which reflects actual organizational processes. This understanding enhances the quality of life for IT professionals by equipping them with the skills to manage scalable and secure networks. The application of NAT on core routers ensures safe internet access, allowing internal users to reach external servers without compromising local IP integrity. These design considerations are aligned with ISO/IEC 27001 for security and IEEE 802.1Q standards for VLAN management [3].

The life-centric approach of this network emphasizes safety, accessibility, and performance. Through effective CO/PO mapping (e.g., CO1, CO3, PO1, PO3), this project contributes to the development of life-improving technologies while enabling learners to solve engineering problems that directly affect user experience and system dependability [4][5].

4.1.2 Impact on Society & Environment

The enterprise network project serves broader societal needs by supporting digital infrastructure that promotes connectivity, data integrity, and service availability. In organizations where departmental collaboration is critical, the integration of VLANs and routing protocols (e.g., EIGRP, OSPF) enhances communication efficiency and reduces network congestion. In addition, the use of DHCP, SMTP, and DNS services simulates how real-world enterprises enable seamless communication, database access, and email delivery. These services underpin modern commerce, education, healthcare, and governance, thus contributing to societal advancement [1].

From an environmental perspective, conducting the entire project within Cisco Packet Tracer eliminates the need for physical devices, reducing electronic waste (e-waste) and energy consumption. This promotes sustainable learning and system design, in accordance with environmental management standards such as ISO 14001. Furthermore, network features like VLSM allow efficient IP address utilization, minimizing wastage and conserving digital resources. The NAT and ACL configurations also contribute to a secure, efficient communication model that protects sensitive data from external threats while allowing regulated access to global resources [2][3].

The project aligns with ethical and sustainable design under PO2 and PO3, focusing on real-world applications, system efficiency, and the environment. Through its CO4 mapping, the network ensures all departments are interconnected, simulating how interconnected societies rely on IT systems. As future engineers work on greener and more secure systems, this simulation provides a practical foundation for building sustainable digital ecosystems that minimize environmental impact while maximizing societal utility [4][5].

4.1.3 Ethical Aspects

Ethics play a fundamental role in network engineering, especially when designing systems that manage communication, privacy, and access control. In this project, ethical considerations are implemented primarily through Access Control Lists (ACLs), which restrict unauthorized access and enforce digital policies. These controls are essential for maintaining data confidentiality, integrity, and availability across enterprise departments. The implementation of NAT (Network Address Translation) on the core

router ensures that internal IP addresses remain private, thus complying with ethical standards for data protection and cybersecurity [1][2].

Another ethical component is service fairness. The use of Dynamic Host Configuration Protocol (DHCP) ensures equal IP distribution among devices, preventing conflicts and guaranteeing network access for all users. Moreover, server configurations for HTTP, DNS, and SMTP uphold ethical communication by enabling transparent access to web services and responsible email delivery across departmental boundaries. Such configurations simulate real-world standards and regulatory compliance, including those set by ISO/IEC 27001 and GDPR (General Data Protection Regulation) in applicable regions [3].

Furthermore, the simulation environment promotes academic integrity and encourages ethical learning. By using Cisco Packet Tracer instead of real hardware, the project avoids misuse of physical resources and allows students to develop skills ethically and sustainably. The CO3 and PO3 mapping in the project ensures that learners design ethically compliant server infrastructure, which is vital in industry settings. By embedding these values into every layer of the network, this project reinforces the responsibility of engineers to safeguard digital rights and uphold ethical principles throughout the system lifecycle [4][5].

4.1.4 Sustainability Plan

The sustainability of an enterprise network lies in its ability to adapt, scale, and operate efficiently over time while minimizing resource usage and waste. This project incorporates several sustainable design practices. Firstly, Variable Length Subnet Masking (VLSM) ensures optimal usage of IP addresses, allowing scalability without exhausting the IPv4 address space. This aligns with sustainable digital infrastructure goals and supports long-term deployment needs [1][2].

Secondly, using Cisco Packet Tracer for simulation reduces reliance on physical devices, contributing to the reduction of e-waste and carbon footprint. It provides a low-energy, cost-effective means for prototyping and testing enterprise networks. The integration of EIGRP and OSPF facilitates dynamic routing, allowing the system to self-adjust to topology changes, which is essential for sustainable, fault-tolerant networks. Likewise, the DHCP server supports dynamic IP assignment, minimizing administrative overhead and ensuring efficient address utilization [3].

The sustainability plan is also evident in modularity. By assigning VLANs to departments, the network topology can be easily modified or extended without disrupting existing configurations. Similarly, NAT

ensures internal networks are adaptable to external connectivity without changing internal structures. These aspects reflect the sustainable lifecycle design promoted by ISO 20000 for IT service management [4].

CO4 and PO3 mappings ensure that students and engineers approach network problems with a sustainable mindset. Through Bloom's C6 and KP4 levels, learners are encouraged to evaluate and create adaptable solutions that endure technological shifts and environmental constraints. This forward-thinking strategy ensures the network remains efficient, scalable, and aligned with long-term organizational goals [5][6].

4.2 Project Management and Team Work

1. **Shariar Ahamed Ripon:**

   Role: Project Planner & DHCP Server Implementation & Configuration

   Shariar Ahamed Ripon acted as the overall project planner, overseeing the timeline, scope, and coordination of tasks across all modules of the system. He was responsible for initiating the planning phase, defining the development milestones, and ensuring adherence to the proposed methodology. Additionally, he implemented and configured the Dynamic Host Configuration Protocol (DHCP) server, which played a crucial role in automatically assigning IP addresses to network devices. This ensured seamless communication between system modules and services within the simulated enterprise network environment.

2. **Md Moniruzzaman Rifat:**

   Role : Structure Designer, VLAN & Email Server Implementation & Configuration

   Md Moniruzzaman Rifat served as the structural architect of the system, designing the layout of both the physical and logical components of the Library Management System. His role also included the implementation of Virtual Local Area Networks (VLANs), which allowed secure segmentation of network domains to manage traffic efficiently. Furthermore, he configured the Email Server to support system-generated notifications, enhancing communication regarding book issue/return alerts and administrative messages.

3. **Nabanita Gain :**

   Role : Project Report Compilation & Web Server Implementation & Configuration

   Nabanita Gain contributed by compiling the formal documentation and lab report, aligning with IEEE writing standards. Her detailed reporting included implementation procedures, testing phases, and output evaluations. Additionally, she was responsible for configuring the Web Server, enabling browser-based access to the LMS platform, which allowed users to perform login, book search, and transaction operations from a web interface.

4. **Sumaiya Akter Sammi :**

   Role :DNS server implementation & configuration

   Sumaiya Akter Sammi led the configuration and testing of the Domain Name System (DNS) server, which ensured the translation of domain names to IP addresses within the LMS. This made the system accessible using domain-based URLs rather than numeric IPs, improving usability and professionalism. Her work guaranteed that services such as the web and email servers could be reached reliably through human-readable hostnames.

5. **Sultana Asma Islam :**

   Role : NAT connection implementation & configuration

   Sultana Asma Islam handled the configuration of Network Address Translation (NAT) services. Her implementation ensured that internal private IP addresses within the LMS environment could securely access external networks and vice versa. This was particularly important for integrating online book databases, remote email functionalities, and ensuring external client access to internal servers through mapped IPs.

4.3 Complex Engineering Problem

4.3.1 Mapping of Program Outcome

According to CO1 maps to PO1, demonstrating a foundational understanding of network addressing and device configuration using CLI (Bloom's C1, C2). CO2 and CO3 are mapped to PO2 and PO3 respectively, as they include routing logic and server configuration using EIGRP, OSPF, DHCP, and DNS (Bloom's C4, A1). CO4 aligns with PO3 through advanced problem-solving and integration tasks (C3, C6, A3, P3). Each CO supports Engineering Parameters such as EP1 (Knowledge Application), EP2 (Communication), and EP3 (Design and Development).

4.3.2 Complex Problem Solving

Solving this network design problem involved KP4 level knowledge, including the application of advanced CLI commands, troubleshooting NAT issues, and verifying DHCP scope propagation across VLANs. Layer 2 and Layer 3 devices were configured manually to ensure consistent interoperability. All routers had correct routing tables, reflecting proper subnetting using VLSM (e.g., 192.168.10.0/28 for HR, 192.168.20.0/28 for Finance). DHCP was configured on a core router to dynamically assign IPs to PC devices, while one router acted as an email/web server host [3][4].

4.3.3 Engineering Activities

The engineering activities involved the complete configuration of the network topology using Cisco Packet Tracer. Commands were used to configure interfaces, assign IPs, enable EIGRP (e.g., router eigrp 1), and define networks (e.g., network 192.168.10.0 0.0.0.15). VLANs were created using vlan 10, name HR, and inter-VLAN routing was enabled. ACLs (e.g., access-list 101 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255) were applied to restrict sensitive communication. NAT was configured with inside and outside interfaces and translation rules. Email communication was verified using the configured SMTP server, and the team's webpage was hosted via HTTP. These activities reflect the core of EP3 – Design and Development of Solutions.

Chapter 5
Conclusion

This chapter summarizes the achievements of the Library Management System (LMS) project, identifies its limitations, and outlines potential future improvements. The LMS addresses significant challenges in library operations by automating critical processes and enhancing user experience.

5.1 Summary

This project has successfully demonstrated the design and implementation of an enterprise-level network topology that simulates real-world departmental infrastructure using Cisco Packet Tracer. Through structured planning and execution, the network was segmented into multiple departments, each represented by dedicated subnets using Variable Length Subnet Masking (VLSM) to ensure optimal address space utilization. Layer 2 and Layer 3 devices were carefully configured, enabling seamless inter-departmental communication, VLAN segregation, and centralized routing.

Key protocols such as EIGRP and OSPF were employed to dynamically manage routing tables across the topology, ensuring loop-free and fault-tolerant paths. Furthermore, critical services like DNS, HTTP, and SMTP were hosted on a central server configured to be reachable from any device within the network, thereby replicating the core infrastructure of a real enterprise. Dynamic Host Configuration Protocol (DHCP) was implemented on a router to automate IP allocation, enhancing administrative efficiency. Network security was addressed through the use of Access Control Lists (ACLs), while Network Address Translation (NAT) facilitated internal-to-external communication for internet simulation.

The successful implementation of each component validated all the outlined Course Outcomes (COs), including the proper use of device interfaces and IP configuration (CO1), application of routing protocols (CO2), server service deployment (CO3), and end-to-end network reachability (CO4). The work aligns with real-world engineering standards and fulfills Program Outcomes (POs) through the demonstration of applied technical knowledge, problem-solving skills, and sustainable design practices. Overall, the project showcases a holistic understanding of enterprise network architecture and its practical simulation in a controlled virtual environment.

5.2 Limitations

While the project achieves its primary objectives, it also encounters several inherent limitations due to the simulation environment and the constraints of Cisco Packet Tracer. The first major limitation is the platform's inability to simulate real-time bandwidth usage, packet loss, jitter, and latency, which are critical components of enterprise-grade performance evaluation. This restricts the ability to assess the true Quality of Service (QoS) under varied network loads. Additionally, Packet Tracer does not support a complete suite of next-generation security features such as Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), firewall zones, or deep packet inspection mechanisms.

Moreover, the emulated devices lack the full capabilities found in physical enterprise hardware such as Cisco Catalyst or ISR routers. This includes limited support for advanced protocols like BGP, MPLS, or policy-based routing (PBR). The project also refrains from integrating multi-layer authentication systems (e.g., RADIUS or TACACS+) and cloud-based service integration, which are now industry standards. IPv6 support is present but rudimentary, limiting the exploration of dual-stack configurations or transition mechanisms.

In terms of scalability, the network is designed for simulation with a limited number of hosts and routers, and thus does not account for enterprise-level scaling that might include hundreds or thousands of devices. Manual configuration also introduces potential for human error, and the lack of centralized monitoring tools such as SNMP or NetFlow restricts real-time troubleshooting and performance logging. Despite these limitations, the simulation meets academic goals, and provides a strong foundation for further exploration into enterprise networking.

5.3 Future Work

Future enhancements to this project can significantly extend its practical relevance and technical depth by addressing the current limitations and embracing emerging technologies. Firstly, migration from Cisco Packet Tracer to more advanced emulation platforms such as GNS3, EVE-NG, or Cisco VIRL can provide access to real Cisco IOS images, offering more authentic behavior and support for advanced protocols including BGP, MPLS, and policy-based routing. These platforms also support larger and more complex network topologies, enabling the design of multi-site enterprise systems.

Integration of IPv6 alongside IPv4 (dual-stack configuration) would reflect modern network deployments, especially with the global depletion of IPv4 addresses. Additionally, cloud networking solutions can be introduced using VPNs and SD-WAN to simulate secure remote access to cloud-hosted services, enabling hybrid architecture modeling. For network security, future work could involve implementing firewall appliances, intrusion detection systems, and AAA (Authentication, Authorization, and Accounting) using RADIUS or TACACS+ servers.

Performance monitoring tools such as SNMP, NetFlow, or open-source platforms like Zabbix and Nagios can be integrated to monitor traffic, detect anomalies, and gather real-time metrics, offering a more proactive network management system. Moreover, the inclusion of automated scripts for CLI configurations using Python and Ansible could bring in network automation practices aligned with DevNet and NetDevOps standards.

Finally, to simulate real enterprise operations, advanced application-layer services such as VoIP, video conferencing, and load balancing can be integrated. These features not only broaden the scope of the simulation but also provide a stepping stone toward certification-level projects and real-world deployment readiness.

References

[1] T. Lammle, *CCNA Certification Study Guide*, 8th ed., Wiley, 2020.

[2] W. Odom, *CCNA 200-301 Official Cert Guide, Volume 1*, Cisco Press, 2020.

[3] J. Froom, R. Graziani, and A. Vachon, *Introduction to Networks v7 Companion Guide*, Cisco Networking Academy, Cisco Press, 2021.

[4] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 5th ed., Pearson, 2010.

[5] W. Stallings, *Data and Computer Communications*, 10th ed., Pearson Education, 2013.

[6] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 7th ed., Pearson, 2017.

[7] IEEE 802.3-2022, "IEEE Standard for Ethernet," IEEE, 2022.

[8] RFC 1918 – *Address Allocation for Private Internets*, IETF. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc1918

[9] ISO/IEC 27001, *Information Security Management Systems – Requirements*, International Organization for Standardization, 2013.

[10] ISO/IEC 20000-1:2018, *Information Technology – Service Management*, ISO, 2018.

[11] NBA India, *Graduate Attributes and Program Outcomes*, National Board of Accreditation. [Online]. Available: https://nbaindia.org

[12] IEEE, *IEEE Code of Ethics*, [Online]. Available: https://www.ieee.org/about/corporate/governance/p7-8.html