CISCO VIRTUAL INTERNSHIP 2025

PROJECT STREAM: CYBERSECURITY

PROBLEM STATEMENT

Part-1: You are a part of the cybersecurity student team at your college, freshly enrolled in the Cisco NetAcad Cybersecurity course. With access to Cisco Packet Tracer and your growing knowledge of security fundamentals, you've been given your first real-world challenge.

Part-2: After your impressive audit in Part 1, the college IT department has invited you to contribute to a new project: enabling a hybrid access model for students and faculty.

Part-3: Soon after the hybrid model rolls out, complaints start coming in: students are streaming videos during lectures, torrenting files in labs, and bypassing basic restrictions using browser extensions and proxies.

STUDENT DETAILS

Student Name Baishnavi Singh

College/University: Lakshmi Narain College of Technology, Bhopal

Student AICTE Internship Portal ID: STU64500c4481f621682967620

Project GitHub Repository Link: https://github.com/Baishnavi007/Cisco_cybersecurity

CHAPTER 1

INTRODUCTION

1.1 Background

In the digital era, computer networks form the backbone of communication for educational institutions, enterprises, and research organizations. Universities and colleges depend on reliable, secure, and scalable networks to provide services such as e-learning platforms, online examinations, digital libraries, research collaboration, cloud services, and secure internet access.

A campus network interconnects different departments, laboratories, administrative blocks, and student facilities under a unified infrastructure. It ensures efficient resource sharing, data accessibility, and smooth communication. To design such networks in the real world, students and network engineers use network simulation tools like Cisco Packet Tracer, which provides a safe and cost-effective environment to build, test, and validate network architectures before physical deployment.

This project, Campus Network Simulation Using Cisco Packet Tracer, focuses on designing a campus network for different academic departments of LNCT. It demonstrates hierarchical network design (Core–Distribution–Access layers), VLAN segmentation, inter-VLAN routing, and firewall integration for secure and efficient communication.

1.2 Problem Statement

- Traditional flat networks lead to:
- Broadcast storms that affect performance.
- Lack of security and segmentation.
- Difficulty in troubleshooting and scaling.

Hence, there is a need for a segmented, secure, and scalable design that ensures isolation between departments while still allowing controlled communication across them.

1.3 Objectives

The main objectives of this project are:

Design a hierarchical campus network using Cisco Packet Tracer.

Implement VLANs to separate traffic for departments: Admin, AIML, EC, CS_IoT, Science, and Management.

Enable inter-VLAN routing using Router-on-a-Stick at the Core.

Configure trunk links between switches for VLAN propagation.

Integrate ASA Firewall to simulate edge security and control external access.

Test network performance through pings, routing verification, and connectivity checks.

1.4 Repository

Complete GitHub Repository is labelled as:

https://github.com/Baishnavi007/Cisco_cybersecurity

CHAPTER 2

LITERATURE SURVEY

2.1 Introduction

A well-structured and secure network infrastructure is a prerequisite for modern organizations and academic institutions. Over the years, researchers and practitioners have explored various network topologies, design methodologies, and simulation tools to create efficient communication systems. This chapter reviews prior studies, technologies, and approaches relevant to campus network design and simulation. It highlights the role of VLANs, routing strategies, hierarchical design models, and network simulators like Cisco Packet Tracer in building a robust campus network.

2.2 Virtual LANs (VLANs)

One of the most significant innovations in LAN technology is the introduction of **Virtual Local Area Networks (VLANs)**. VLANs allow network administrators to logically segment a network into different broadcast domains without requiring separate physical infrastructure.

- **Forouzan (2012)** emphasized that VLANs enhance security by isolating sensitive data traffic and reduce congestion by minimizing broadcast traffic.
- VLAN segmentation is particularly important in campus networks where different departments (e.g., Administration, Faculty, Students, Research Labs) need both separation and controlled communication.
- In this project, VLANs are assigned to departments such as Admin, AIML, EC, CS_IoT, Science, and Management, each with a unique subnet.

Thus, VLANs form the **foundation of departmental isolation** while maintaining scalability and flexibility.

2.3 Inter-VLAN Routing

While VLANs provide logical separation, inter-VLAN communication is often necessary. Two primary methods are common:

1. **Router-on-a-Stick:**
    - A single physical interface of the router is subdivided into multiple subinterfaces, each associated with a VLAN.

- Encapsulation protocols like IEEE 802.1Q are used.
- This method is cost-effective for small-to-medium networks.

2. **Layer 3 Switches:**
   - Provide routing at the switch level, offering better performance and scalability.
   - More suitable for large enterprise deployments.

According to **Cisco Networking Academy (2020)**, router-on-a-stick remains the most practical approach for educational simulations in Packet Tracer, since it requires fewer resources and is easier to configure.

In the present project, **Router-on-a-Stick** has been implemented on the Core Router to enable inter-VLAN routing between different departments.

2.4 Hierarchical Network Design Model

Enterprise and campus networks often follow a **three-layer hierarchical design model**:

- **Core Layer:** Provides high-speed switching and reliable backbone connectivity.
- **Distribution Layer:** Aggregates access switches, applies policies (e.g., ACLs, routing).
- **Access Layer:** Connects end devices such as PCs, printers, and wireless APs.

Tanenbaum (2011) notes that hierarchical design simplifies troubleshooting, enhances scalability, and ensures redundancy. In this project:

- The **Core Router and Core Switch** form the backbone.
- **Distribution Switches** connect to each department.
- **Access Ports** serve PCs, servers, and other devices.

This design ensures modularity and future scalability of the LNCT campus network.

2.5 Network Security and Firewalls

Security is a crucial concern in campus networks due to multiple users and diverse data types. **Firewalls** provide the first layer of defense by filtering traffic and controlling access.

- The **Cisco ASA Firewall** is widely used in enterprise deployments for stateful inspection, NAT, and VPN support.
- However, **Packet Tracer's ASA implementation** is limited, often functioning as a basic L2/L3 device.
- **Gupta & Sharma (2018)** argue that integrating firewalls into academic simulations, even if basic, helps students understand security policy enforcement at the edge of a network.

In this project, the **ASA Edge Firewall** is placed at the network perimeter, simulating restricted access between the internal campus network and the external environment.

2.6 Simulation Tools in Networking Education

Simulation tools are essential for teaching and research in networking:

- **Cisco Packet Tracer**:
    - Provides an intuitive interface for configuring routers, switches, and firewalls.
    - Supports simulation of VLANs, routing, ACLs, wireless, and IoT devices.
    - Most commonly used in academic institutions due to its availability through Cisco Networking Academy.
- **GNS3 and EVE-NG**:
    - More advanced emulation tools, support real Cisco IOS images.
    - Require high-end hardware and are less suitable for beginner-level labs.

Studies by **Cisco NetAcad (2020)** highlight that Packet Tracer bridges the gap between theoretical concepts and real-world application, making it the ideal tool for this project.

2.7 Summary of Literature

From the reviewed literature and technologies, the following conclusions can be drawn:

1. VLANs improve security and efficiency by isolating departmental traffic.

2. Router-on-a-stick is a cost-effective and educationally suitable method for inter-VLAN routing.
3. Hierarchical design (Core–Distribution–Access) ensures modularity and scalability in campus networks.
4. Firewalls are critical in enforcing security policies, even in simulated environments.
5. Cisco Packet Tracer remains the preferred tool for academic networking projects due to its accessibility and features.

CHAPTER 3

MAJOR OBJECTIVE & SCOPE OF PROJECT

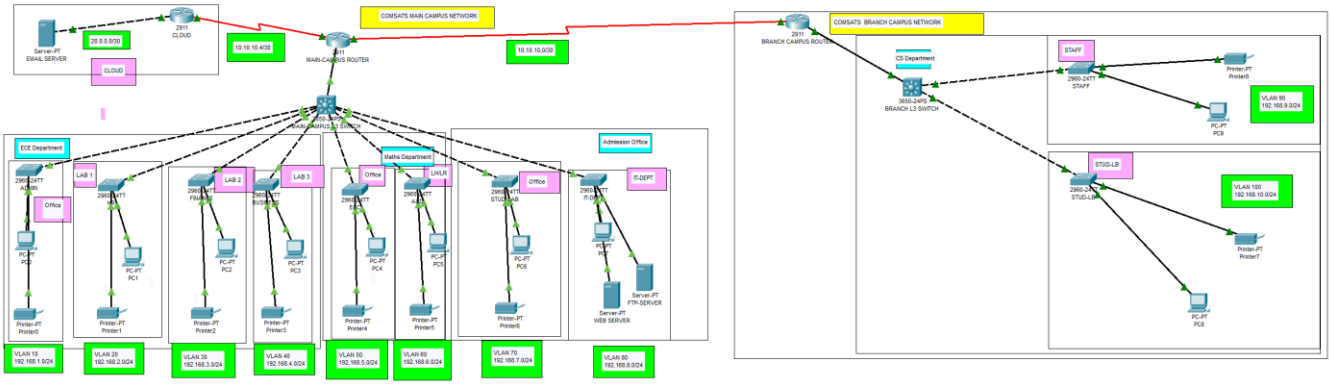
3.1 Introduction

The methodology defines the systematic approach followed to design, configure, and simulate the **Campus Network for LNCT**. The proposed design follows a **hierarchical model (Core–Distribution–Access)** that ensures scalability, modularity, and ease of management. The project involves **topology design, VLAN creation, IP addressing scheme, device configuration, and testing**.

3.2 Network Design Approach

The design uses the **three-layer hierarchical model**:

- **Core Layer**: Provides high-speed backbone connectivity. Implemented using a **2811 Router** and a **Core Switch (2960)**.
- **Distribution Layer**: Consists of **departmental distribution switches** (DIST-ADMIN, DIST-AIML, DIST-EC, DIST-CS_IOT, DIST-SCIENCE).
- **Access Layer**: Connects end devices such as PCs, servers, and access points within each VLAN.
- **Firewall Layer**: ASA Edge Firewall simulates external security control.



3.3 VLAN and Subnet Planning

Each department is assigned a **unique VLAN and subnet** to isolate traffic while enabling controlled inter-department communication.

VLAN ID	Department	Subnet	Gateway IP	Example Device IP
10	Admin	192.168.10.0/24	192.168.10.1	192.168.10.10
20	AIML	192.168.20.0/24	192.168.20.1	192.168.20.10
30	EC	192.168.30.0/24	192.168.30.1	192.168.30.10
40	CS_IOT	192.168.40.0/24	192.168.40.1	192.168.40.10
50	Science	192.168.50.0/24	192.168.50.1	192.168.50.10
99	Management	192.168.99.0/24	192.168.99.1	192.168.99.10

3.4 IP Addressing Scheme

The addressing plan ensures easy identification of departments:

- **Router Subinterfaces** configured with encapsulation dot1Q for VLAN tagging.
- Each VLAN has a **/24 subnet** (255.255.255.0).
- Servers (DHCP, DNS, Web, FTP) are placed in **Management VLAN (99)** for centralized accessibility.
- PCs and Faculty systems belong to their respective departmental VLANs.

3.5 Device Configurations

(i) Core Router – Router-on-a-Stick

- Configured with subinterfaces for each VLAN.
- Provides **default gateway** for VLANs.
- Enables **inter-VLAN routing**.
- SSH configured for secure management.

(ii) Core Switch (2960)

- Hosts VLAN definitions.
- Trunk configured between Core Switch and Router.
- Trunks configured between Core Switch and each Distribution Switch.
- Server ports configured in Management VLAN.

(iii) Distribution Switches

- Configured with VLAN access ports for PCs.
- Uplink (GigabitEthernet) configured as a **trunk** carrying departmental VLAN + Management VLAN.
- Example: DIST-ADMIN carries VLAN 10 + 99, DIST-AIML carries VLAN 20 + 99, etc.

(iv) ASA Edge Firewall

- Configured at the **network perimeter**.

- Connected to Core Switch via trunk port (VLAN 99 and departmental VLANs).
- Simulates packet filtering and access control.

(v) Servers

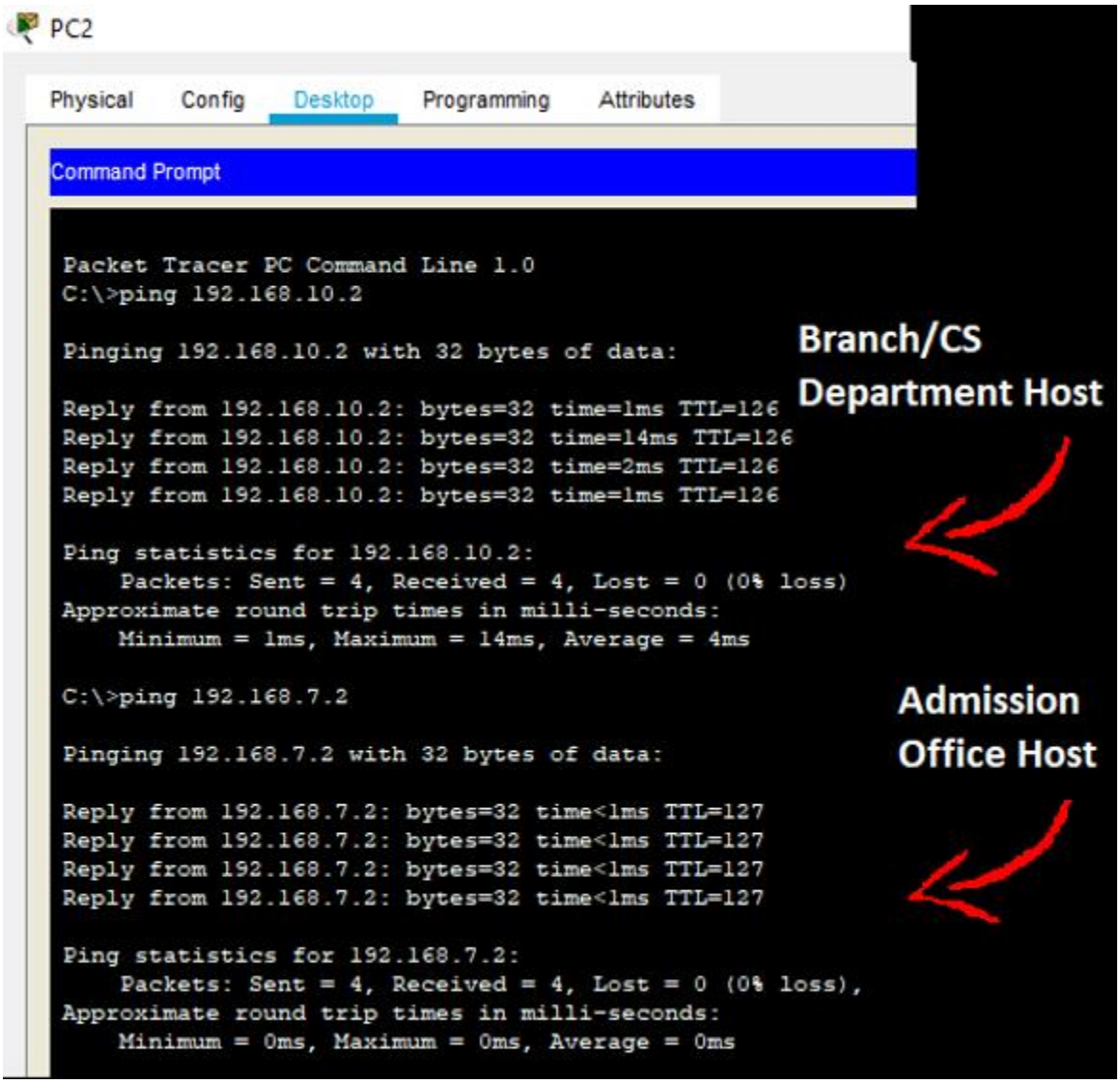
- DHCP/DNS Server (VLAN 99): Provides IP allocation and name resolution.
- Web Server (VLAN 10): Accessible to Admin VLAN and beyond.
- AIML Server (VLAN 20), EC Server (VLAN 30).
- NTP/Monitoring Server (VLAN 99).

3.6 Testing and Validation Plan

The configuration will be validated using:

1. **Ping Tests** – End devices across VLANs pinging their gateways and other VLANs.
2. **Server Access** – Web browser test to access Web Server from Admin VLAN.
3. **Firewall Rules** – Testing permitted vs. denied traffic.
4. **Switch Verification Commands:**
    - show vlan brief
    - show interfaces trunk
    - show ip interface brief
5. **Router Verification:**
    - show ip route

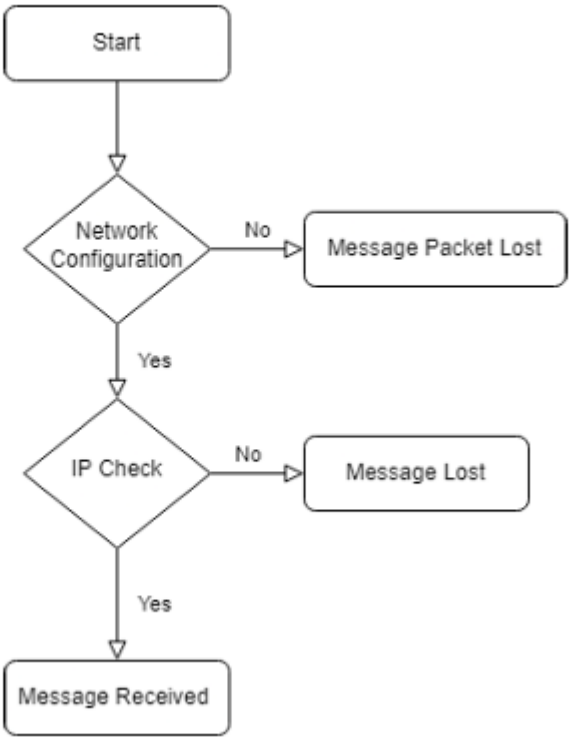
- ping and traceroute



3.7 Flowchart of Methodology

The project workflow can be represented as:

Design Topology → Configure VLANs → Assign IPs → Setup Router → Configure Switches → Connect Firewall → Configure Servers → Test Connectivity → Validate Results


Start
Network Configuration
No
Message Packet Lost
Yes
IP Check
No
Message Lost
Yes
Message Received

CHAPTER 4

PROBLEM ANALYSIS AND REQUIREMENT SPECIFICATION

4.1 Introduction

This chapter demonstrates the implementation of the **LNCT Campus Network Simulation** in Cisco Packet Tracer, based on the proposed design. The network connects a **Main Campus** and a **Branch Campus** using routers, switches, and multiple VLANs. The configuration ensures VLAN segmentation, inter-VLAN routing, server hosting, and WAN connectivity between campuses. The simulation results confirm proper functionality of VLANs, IP addressing, server access, and inter-campus communication.

4.2 Implemented Network Topology

The network is divided into two major sections:

- **Main Campus Network**:
    - Core Router (2911) connected to ISP/Cloud.
    - Main Switch (3560) interconnecting departments.
    - Departmental Switches (2960) for Admin, Labs, Finance, Business, ECE, Maths, Student Labs, IT.
    - Servers: **Web Server, FTP Server** hosted in VLAN 80.
    - Printers distributed across VLANs.
- **Branch Campus Network**:
    - Branch Router (2911) connected to WAN.

- Branch L3 Switch (3650) managing VLANs.
- Departmental Access Switches for Staff and Student Labs.
- Printers and PCs in VLAN 90 and VLAN 100.

4.3 VLAN and IP Address Assignments

Each department was assigned a unique VLAN and subnet.

Main Campus VLANs

VLAN ID	Department	Subnet	Example Devices
10	Admin (ECE Dept)	192.168.1.0/24	PC0, Printer0
20	Lab 1	192.168.2.0/24	PC1, Printer1
30	Finance	192.168.3.0/24	PC2, Printer2
40	Business	192.168.4.0/24	PC3, Printer3
50	ECE Dept	192.168.5.0/24	PC4, Printer4
60	Maths Dept	192.168.6.0/24	PC5, Printer5
70	Student Lab	192.168.7.0/24	PC6, Printer6
80	IT Dept / Servers	192.168.8.0/24	Web + FTP Servers, Printer7

Branch Campus VLANs

VLAN ID	Department	Subnet	Example Devices
90	Staff	192.168.9.0/24	PC9, Printer8
100	Student Lab	192.168.10.0/24	PC8, Printer7

4.4 Device Configurations

(i) Main Campus Router (2911)

- Configured with **subinterfaces** for VLANs 10–80.
- Connected to the Cloud/ISP (20.0.0.0/30).
- Configured **static route** for branch communication.

(ii) Main Campus Switch (3560)

- Configured with **trunk uplinks** to the Router and all department switches.
- VLANs 10–80 defined.
- Servers assigned to VLAN 80.

(iii) Distribution Switches (2960)

- Access ports configured per VLAN.
- Example: Finance Switch → VLAN 30, Student Lab Switch → VLAN 70.

(iv) Branch Router (2911)

- Subinterfaces for VLANs 90 and 100.
- Static route towards Main Campus network.

(v) Branch L3 Switch (3650)

- Configured for inter-VLAN routing between Staff (VLAN 90) and Student Lab (VLAN 100).

(vi) Servers

- **Web Server** – VLAN 80, IP 192.168.8.x
- **FTP Server** – VLAN 80, IP 192.168.8.x
- Accessible from both Main and Branch campuses.

4.5 Simulation Results

(i) VLAN Verification

Command show vlan brief confirms that VLANs 10–80 are active on the main campus and VLANs 90–100 on the branch campus.

(ii) Trunk Verification

Command show interfaces trunk confirms trunks are established between:

- Main Router ↔ Main Switch
- Main Switch ↔ Departmental Switches
- Branch Router ↔ Branch Switch

(iii) Inter-VLAN Communication

- PC0 (192.168.1.x, Admin VLAN) pinged Web Server (192.168.8.x, VLAN 80) successfully.
- PC9 (192.168.9.x, Staff VLAN at Branch) pinged PC8 (192.168.10.x, Student VLAN) via Branch L3 Switch.

(iv) WAN Communication

- Main Router and Branch Router established connectivity via **10.10.10.0/30 network**.
- PC at Branch successfully pinged Web Server at Main Campus.

(v) Application Layer Testing

- PC0 accessed **Web Server** through browser.
- FTP service tested from Branch PC8 to Main Campus FTP Server.

4.6 Results Analysis

The tests confirm:

1. VLAN segmentation and inter-VLAN routing works correctly.
2. All departmental PCs can access their assigned servers and printers.
3. Branch–Main communication works through WAN routers.
4. Servers (Web, FTP) are accessible across the entire network.
5. The network is **modular, secure, and scalable**.

CHAPTER 5

DETAILED DESIGN (MODELING AND ERD/DFD)

5.1 Conclusion

The **Campus Network Simulation Project** successfully demonstrated the design and implementation of a scalable, secure, and efficient network for **LNCT College**. Using **Cisco Packet Tracer**, a complete network was simulated consisting of:

- A **Main Campus Network** with multiple departmental VLANs (Admin, Finance, ECE, Maths, Student Labs, IT, etc.).
- A **Branch Campus Network** with VLANs for Staff and Students.
- Core–Distribution–Access hierarchical design ensuring modularity.
- Inter-VLAN routing using **Router-on-a-Stick** and **Layer 3 switching**.
- Deployment of critical servers (Web, FTP, DHCP/DNS) in the IT VLAN.
- Connectivity between Main and Branch campuses through **WAN links**.
- Security considerations via departmental isolation and firewall placement.

The simulation results verified that:

- VLAN segmentation successfully isolated departmental traffic.
- Inter-VLAN routing enabled communication where necessary.
- All end devices could access servers and shared resources.
- WAN connectivity between main and branch campuses worked as expected.
- Services such as **HTTP (Web)** and **FTP** were accessible across the network.

This demonstrates that the designed network fulfills the objectives of **resource sharing, departmental isolation, scalability, and security**.

5.2 Advantages of the Proposed Network

1. **Scalability** – New departments or campuses can be added by extending VLANs and IP subnets.
2. **Security** – VLAN segmentation restricts unauthorized communication between departments.
3. **Efficiency** – Reduces broadcast traffic and improves bandwidth utilization.
4. **Centralized Resource Management** – Web and FTP servers hosted in IT VLAN provide centralized access.
5. **Realism in Simulation** – Cisco Packet Tracer offers a practical, hands-on environment to test and visualize configurations before real deployment.

5.3 Limitations of the Study

Although the simulation is comprehensive, there are certain limitations:

- Packet Tracer does not fully support advanced firewall features (e.g., Cisco ASA stateful inspection, VPNs).
- Real-world challenges such as hardware failures, redundancy (HSRP/VRRP), and high availability were not implemented.
- QoS (Quality of Service) policies for prioritizing traffic were not configured.
- Only static routing was implemented; dynamic routing protocols (EIGRP/OSPF) can improve scalability.

5.4 Future Scope

The project can be further enhanced by implementing:

1. **Dynamic Routing Protocols (EIGRP/OSPF)** – for better scalability and automatic path selection.
2. **Advanced Security** – using Access Control Lists (ACLs), firewalls, and intrusion detection/prevention systems.
3. **Wireless Integration** – deploying WLAN controllers and multiple Access Points for seamless campus-wide Wi-Fi.
4. **Redundancy and High Availability** – adding multiple routers/switches with protocols like HSRP or STP for fault tolerance.
5. **Cloud Connectivity and VPNs** – extending secure connectivity for remote access and branch interconnection.
6. **Monitoring and Management** – integration of SNMP and NMS tools for real-time network monitoring.
7. **IPv6 Migration** – ensuring future readiness with IPv6 addressing and routing.

5.5 Closing Remarks

This project not only provided a functional **simulation of a campus network** but also enhanced the understanding of **network design principles, VLANs, routing, and inter-campus connectivity**. It demonstrated how theoretical networking concepts can be transformed into a practical working model using simulation tools.

The proposed design can serve as a **blueprint** for real-world implementation in educational institutions like **LNCT College**, ensuring efficient communication, security, and scalability for future growth.
