Abstract

This project focuses on the design and implementation of a secure university network connecting two campuses located in separate areas. The network is built using a three-tier hierarchical topology in Cisco Packet Tracer, which is a proven framework for improving efficiency, scalability, and manageability of complex network infrastructures. The primary objective of this project is to establish a robust network structure that meets the diverse needs of the university while demonstrating the practical application of networking concepts in a simulated environment. Each phase of the project, from planning and design to actual implementation, highlights key aspects of network architecture, including security, routing, and management of wired and wireless devices. The significance of this research lies not only in its immediate applicability but also in its contribution to the broader understanding of how well-designed networks can support secure, efficient, and reliable communication in academic institutions. By simulating a realistic campus network, this project provides a model for future-ready university networks that can adapt to evolving technological demands and academic requirements.

Acknowledgments

We would like to express our deepest gratitude to all those who have supported and guided us throughout the completion of this project. Their assistance and encouragement have been invaluable in shaping our work. We are profoundly thankful to our project supervisor, Syeda Alisha Noor, for her unwavering guidance, insightful feedback, and continuous support, which have been instrumental in steering this project towards successful completion.

We also extend our sincere appreciation to the faculty members of the Computer Science & Engineering Department for providing an academic environment that nurtures creativity, critical thinking, and collaborative learning. Their dedication to education and research has greatly enriched our experience throughout this project.

This project was completed collaboratively by our team members Nahian Subah (C223286), Rehnuma Tasneem (C223288), Saima Kawsar (C223297), Sakaratul Ara Tasmia (C223298), and Tahsin Islam Nafisa (C223311). The project would not have been possible without the collective efforts and support of all these individuals, and for that, we are sincerely thankful.

Table of Contents

1. Introduction

The objective of this project is to design and replicate a Campus Area Network (LAN) in order to demonstrate practical understanding of computer networking concepts. The project aims to simulate a real-world campus network environment by implementing a scalable, reliable, and secure LAN infrastructure.

The designed network supports multiple essential services, including Domain Name System (DNS), IP Telephony, and wireless connectivity, which are commonly required in modern educational institutions. To ensure efficient communication and management, the network incorporates VLAN-based segmentation, dynamic IP addressing, secure device access, and appropriate routing mechanisms. This project applies core CCNA concepts such as IP addressing and subnetting, routing protocols, switching technologies, network security, and wireless LAN configuration. Various networking tools and configurations were used to build, test, and verify the functionality of the network.

2. Background

A Campus Area Network (LAN) is a very important part of any large educational institution. It provides connectivity between different locations within the campus such as the male campus, female campus, academic departments, hostels, and administrative offices. A properly designed campus network ensures fast communication, secure data transfer, and efficient resource sharing among users.

In a campus environment, each department depends on the network for teaching, learning, research, and administrative activities. The IT division is responsible for managing the entire network infrastructure, including routers, switches, servers, security, and maintenance. Therefore, a reliable and scalable LAN design is essential to support the daily operations of the institution.This project focuses on designing a campus LAN that connects the male campus, female campus, different academic departments, and the IT division under a single network architecture. The network is designed to support approximately 200 network devices, including routers, switches, servers, IP phones, wired computers, and wireless clients. To manage this number of devices efficiently, proper IP addressing, VLAN segmentation, and routing mechanisms are required.

The importance of this project lies in gaining practical knowledge of how real-world campus networks are planned and implemented. CCNA-level networking concepts such as IP addressing and subnetting, VLAN configuration, routing protocols, network services, and basic security features are applied in this design. Various tools and methods are used in this project to design and test the network. Network simulation tools such as Cisco Packet Tracer used to configure and analyze routers, switches, servers, and wireless devices. These tools help in understanding network behavior and verifying that the campus LAN operates efficiently, securely, and reliably.

3. Literature Review

A literature review explains the important networking concepts and technologies that are related to campus area network design. Many studies and networking guidelines show that a well-planned campus LAN is necessary for providing reliable communication, security, and efficient network management in large organizations such as universities and colleges.

3.1 Campus LAN Design Concepts

A Campus Area Network is designed to connect different buildings, departments, and user groups within the same campus. In large campuses, networks usually follow a hierarchical design model that includes core, distribution, and access layers. This type of design helps to improve network performance, reduce traffic congestion, and make the network easier to manage and expand in the future.

VLANs are commonly used in campus LANs to separate departments and user groups. VLAN segmentation reduces unnecessary broadcast traffic and improves network security by isolating different parts of the network. These design concepts are widely used in educational institutions to support a large number of users efficiently.

3.2 Routing, Switching, and Network Services

Routing and switching technologies form the backbone of a campus network. Switches are mainly used to connect end devices such as computers, IP phones, and access points. Routers or multilayer switches are used to enable communication between different VLANs. Dynamic routing protocols like OSPF are commonly preferred in campus networks because they support scalability and provide fast route convergence.

Campus networks also depend on various network services. DNS is used for resolving domain names, DHCP provides automatic IP addresses to devices, and NTP helps in time synchronization across network devices. IP Telephony is also widely used to allow voice communication using the same data network.

3.3 Network Security and Wireless Technologies

Security is a very important part of campus network design. Techniques such as port security, Access Control Lists (ACLs), DHCP snooping, and secure remote access using SSH are used to protect the network from unauthorized access and attacks. These security methods help ensure safe and stable network operation.

Wireless technologies are essential in modern campus networks to provide mobility for users. Access Points (APs) are deployed across the campus to offer wireless connectivity. In large networks, these APs are centrally managed using a Wireless LAN Controller (WLC) for better control and performance. Security mechanisms like WPA2-PSK are used to protect wireless communication. From the reviewed concepts and practices, it is clear that an effective campus LAN must combine proper network design, routing, switching, security, and wireless technologies. These concepts provide the theoretical foundation for the design and implementation of the campus LAN in this project.

4. Problem Statement

The rapid growth of academic departments and users in a campus environment creates the need for a well-planned and secure network infrastructure. Different departments require reliable connectivity for academic, administrative, and communication purposes. Managing such a large number of users and services without proper network design can lead to performance issues, security risks, and poor network management.

4.1 Problem Identification

In a large educational campus, multiple academic departments such as CSE, EEE, CCE, ETE, Pharmacy, ELL, and BBA operate along with different campus areas like the male campus, female campus, and IT division. Without a properly designed campus network, communication between these areas becomes slow and unreliable. Separate or unstructured networks create difficulties in data sharing, internet access, and service availability. Network congestion, poor scalability, and weak security further affect academic and administrative activities. The lack of centralized servers and proper monitoring also makes network management complex and inefficient.

4.2 Objectives of the Project

The main objective of this project is to design and implement a Campus Area Network that efficiently connects all academic departments and campus areas, including separate male and female campuses, through a unified and reliable network. The project aims to support data, voice, and wireless communication while ensuring security, scalability, and easy management. Another objective is to integrate centralized services such as DNS, Web, Email, and Syslog servers to simplify administration and improve service availability. Overall, the project focuses on creating a realistic campus network using Cisco technologies to demonstrate practical CCNA-level networking skills.

4.3 Proposed System / Solution

To address the identified problems, a Cisco-based Campus Area Network is proposed using a hierarchical network design model consisting of core, distribution, and access layers. Cisco routers and switches are used to interconnect different departments and campus areas. VLANs are implemented to logically separate departments and improve security and traffic control. Inter-VLAN routing ensures proper communication between departments when required. Centralized servers such as DNS, Web, Email, DHCP, NTP, and Syslog are configured to provide essential network services. The entire network is designed and tested using Cisco Packet Tracer to replicate a real-life campus LAN environment.

4.4 Scope of the Project

The scope of this project includes the design and simulation of a campus area network connecting multiple departments and campus areas such as the male campus, female campus, and IT division. The project covers basic routing, switching, VLAN configuration, inter-VLAN communication, and centralized server integration using Cisco devices. It also includes support for wired and wireless communication within the campus. The project is limited to simulation-based implementation and focuses on CCNA-level networking concepts to analyze connectivity, functionality, and basic performance of the campus network.

4.5 Limitations

Despite providing a realistic campus network design, this project has certain limitations. The entire network is implemented in a simulation environment, so real-world hardware failures and physical issues are not considered. Additionally, configuring a large-scale network involves many devices and complex settings, where configuration mistakes can easily occur and require significant time to identify and correct. Managing IP addressing, VLANs, routing, and multiple servers in a large network can be time-consuming and error-prone. Advanced enterprise-level features such as high availability, redundancy, and advanced security mechanisms are also beyond the scope of this project, as the design focuses mainly on CCNA-level concepts.

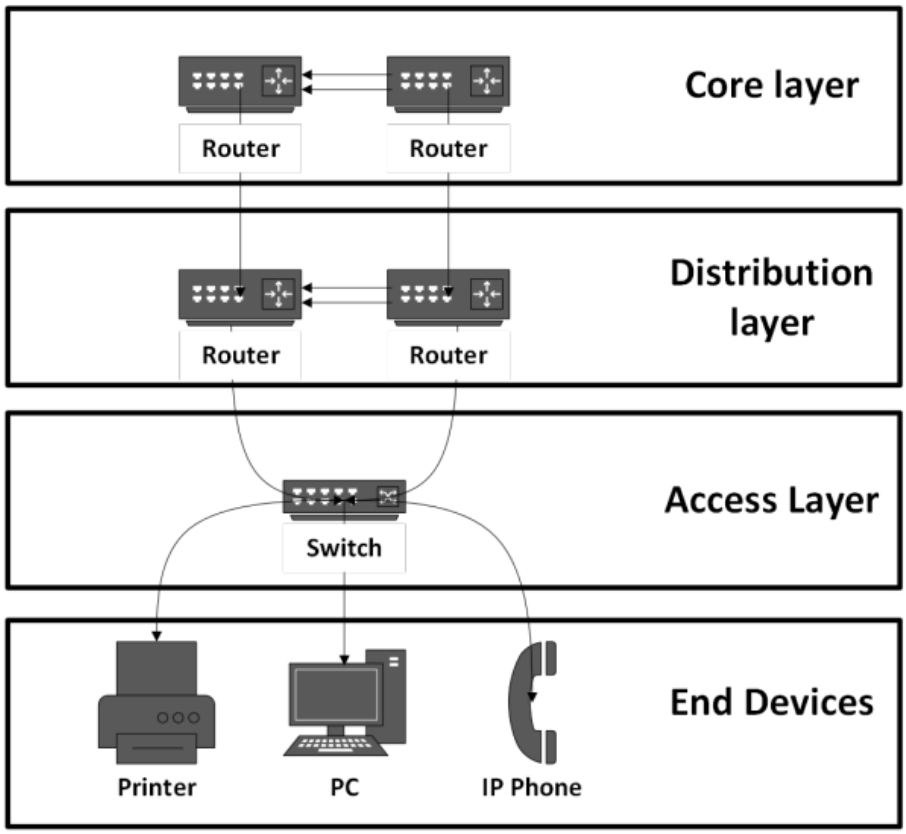

Fig- Hierarchical Network

5. Implementation

This chapter explains how the Campus LAN network was implemented using Cisco Packet Tracer, covering installation, project setup, module design, network design, configurations, and simulation.

5.1 Install Cisco Packet Tracer

At first, Cisco Packet Tracer must be installed on the system to begin designing the campus network. This software is essential because it allows simulation of different network devices such as routers, switches, PCs, laptops, IP phones, printers, and wireless access points. Installing Packet Tracer ensures that all network components can be configured, tested, and monitored virtually before implementing them in a real campus environment. It also allows experimenting with routing protocols, VLANs, NAT, and security features without affecting a live network. Proper installation is the first step toward creating a realistic, functional, and manageable campus LAN.

5.2 Setup the Project

After installing Cisco Packet Tracer, a new project was created to replicate the IIUC campus network. Devices were placed logically based on the IIUC campus layout. The main devices used include:

- **Routers:** To route traffic between different departments and provide internet gateway access.
- **Multilayer Switches:** To handle routing between VLANs and connect core and distribution layers.
- **Access Switches:** To connect wired end devices like PCs and printers.
- **PCs and Laptops:** Representing wired users in departments, hostels, and labs.
- **IP Phones:** Providing telephony services for each department.
- **Printers:** Shared printing services for users in different modules.
- **Lightweight Access Points (APs):** Providing wireless connectivity to laptops, mobile phones, and tablets.
- **Servers:** Hosting essential services such as DNS, Web, Email, Syslog, and DHCP.

This setup allows visualization of all devices, logical connection paths, and realistic traffic flow, helping to test and troubleshoot the network efficiently.

5.3 Module Design

To simplify management and improve scalability, the network was divided into **three main modules**:

- **Male Campus:** Includes all departments, labs, offices, and end devices located in the male campus.
- **Female Campus:** Includes all departments, labs, offices, and end devices located in the female campus.
- **IT Division:** Centralized servers, routers, switches, and wireless management devices.

Dividing the network into modules allows administrators to manage resources efficiently, isolate problems to specific areas, and expand the network in future if required. Each module contains a mix of wired and wireless devices to provide full coverage to students, faculty, and staff.

5.4 Device Description

Device Name	Description
PC (Personal Computer)	PCs are used by students and staff for academic and administrative tasks. They access internet, email, web servers, and internal network resources through wired connections.
Laptop	Laptops provide portable computing for users within the campus. They connect to the network using wired or wireless connections to access internet and campus services.
Smartphone	Smartphones connect to the campus network via wireless access points. They allow users to access internet, email, and internal resources securely over Wi-Fi.
IP Telephone	IP telephones are used for voice communication inside the campus. They enable internal calling between departments using IP telephony services.
Cloud / Internet	The cloud represents external internet connectivity. It allows users to access online services and resources through NAT-enabled routers.
Access Point (AP)	Access points provide wireless network coverage across the campus. They are managed by a Wireless LAN Controller and secured using WPA2 authentication.
Printer	Network printers allow multiple users to print documents over the LAN. They are assigned IP addresses and shared among departments.
Cisco Switch 3560 (Multilayer Switch)	Cisco 3560 switches operate at both Layer 2 and Layer 3. They support VLANs, inter-VLAN routing, and efficient traffic control.
Access Switch	Access switches connect end devices such as PCs, laptops, printers, and IP phones. They provide secure access and forward traffic to higher network layers.
Server	Servers provide essential services such as DNS, DHCP, email, web hosting, and syslog. They ensure centralized management of network resources.
Router	Routers connect different networks and provide internet access. They handle routing, NAT, and secure inter-campus communication.

Fig- Used Devices

5.5 Network Design

The network follows a hierarchical structure with three layers: Core, Distribution, and Access. This design ensures better performance, scalability, and easier troubleshooting.

- **Core Layer:** High-speed backbone connecting different campus modules and providing internet access.
- **Distribution Layer:** Connects core to access switches, implements routing between VLANs, and enforces security policies.
- **Access Layer:** Connects all end devices such as PCs, laptops, IP phones, printers, and APs to the network.

The private IP range 10.0.0.0/8 was used for all devices to maintain internal addressing and security. Subnet masks were assigned based on network requirements:

- **/24 (255.255.255.0)** for end hosts (PCs, laptops, phones)
- **/30 (255.255.255.252)** for point-to-point links between routers
- **/29 (255.255.255.248)** for point-to-multipoint connections

VLANs were configured on multilayer switches to separate departments and support multiple SSIDs for wireless users. This ensures traffic segregation, better performance, and enhanced security across the campus network.

5.5 Configurations

Key configurations implemented in the network include:

- **NAT** for internet access
- **OSPF** dynamic routing with default route
- Hostnames and domain names configured as IIUC on all devices
- **DNS Server:** 10.10.10.10 for local domain resolution; Google DNS (8.8.8.8) for recursive queries
- **Web Server:** 10.9.10.9 hosting the official university website
- **Email Server:** *@iiuc.ac.bd* domain with 70+ accounts
- **Syslog Server:** Collects logs from all network devices
- **DHCP:** Configured on nearby routers for automatic IP assignment to wired and wireless hosts
- **IP Telephony:** Functional IP phones in each department using telephone-service and dial-peerings
- **Switch Security Features:** Port Security, DHCP Snooping, Dynamic ARP Inspection, PortFast
- Unused switch ports were shut down and assigned to an Unused VLAN
- **SSH:** Remote login enabled but restricted to server room devices via ACLs
- **Device Credentials:**
  - Username: admin
  - Password: deepk
  - Enable password: passwd (MD5 encrypted)
- **Wireless Network:** Lightweight APs with WLC in FlexConnect mode
  - WLC login: admin / Wifi@123
  - SSID password: iiuc123

- Security: WPA2-PSK
- VLAN trunking configured to support multiple SSIDs

5.6 Run the Simulation

After completing all configurations, the network was tested in both simulation and real-time modes. Connectivity between all departments, servers, PCs, laptops, IP phones, printers, and wireless clients was verified.

Overall, the project successfully replicated the IIUC campus LAN**,** providing a secure, scalable, and fully functional network environment that supports wired and wireless users, multiple modules, and centralized services.

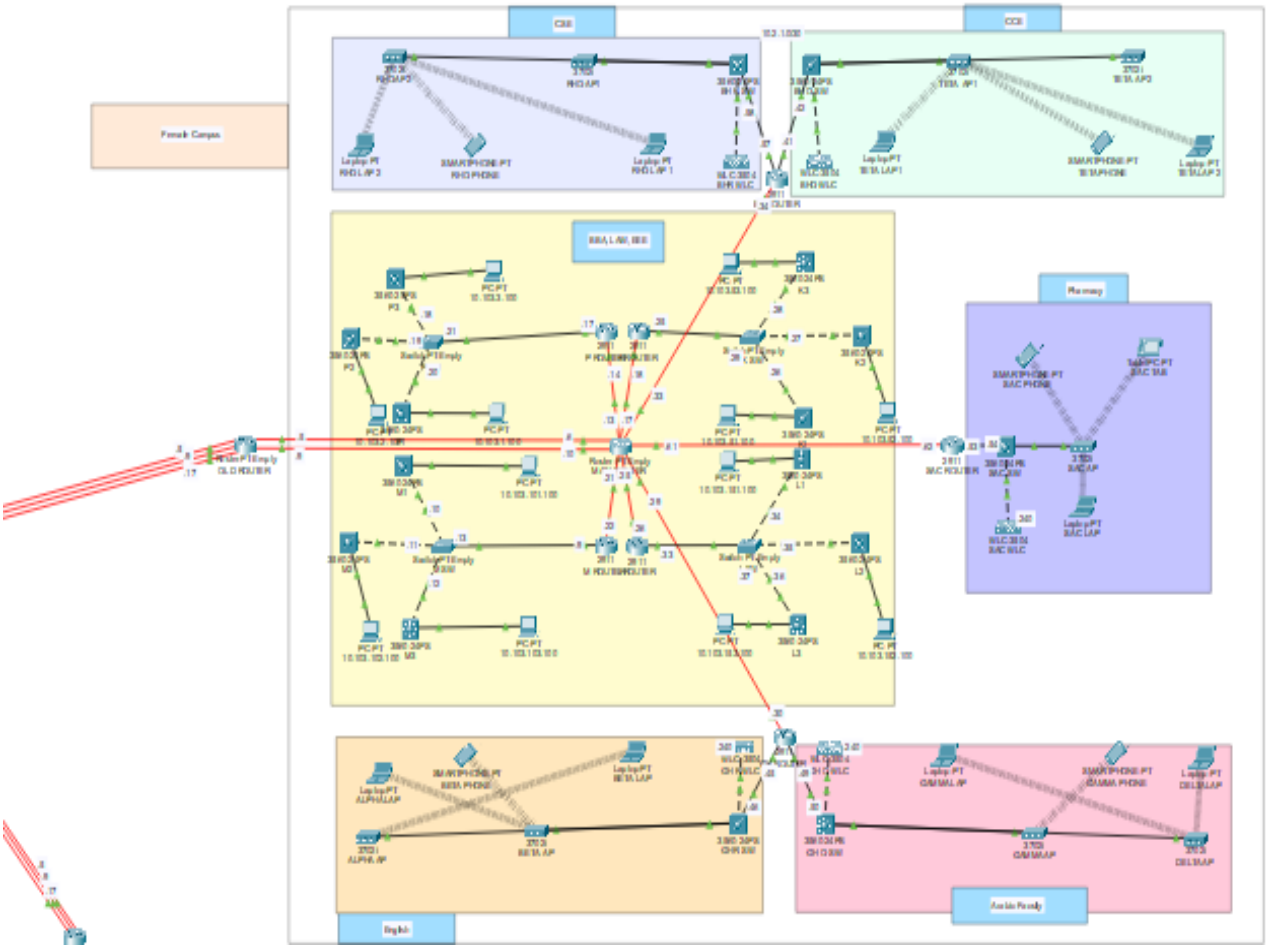

Fig- Female Campus Network

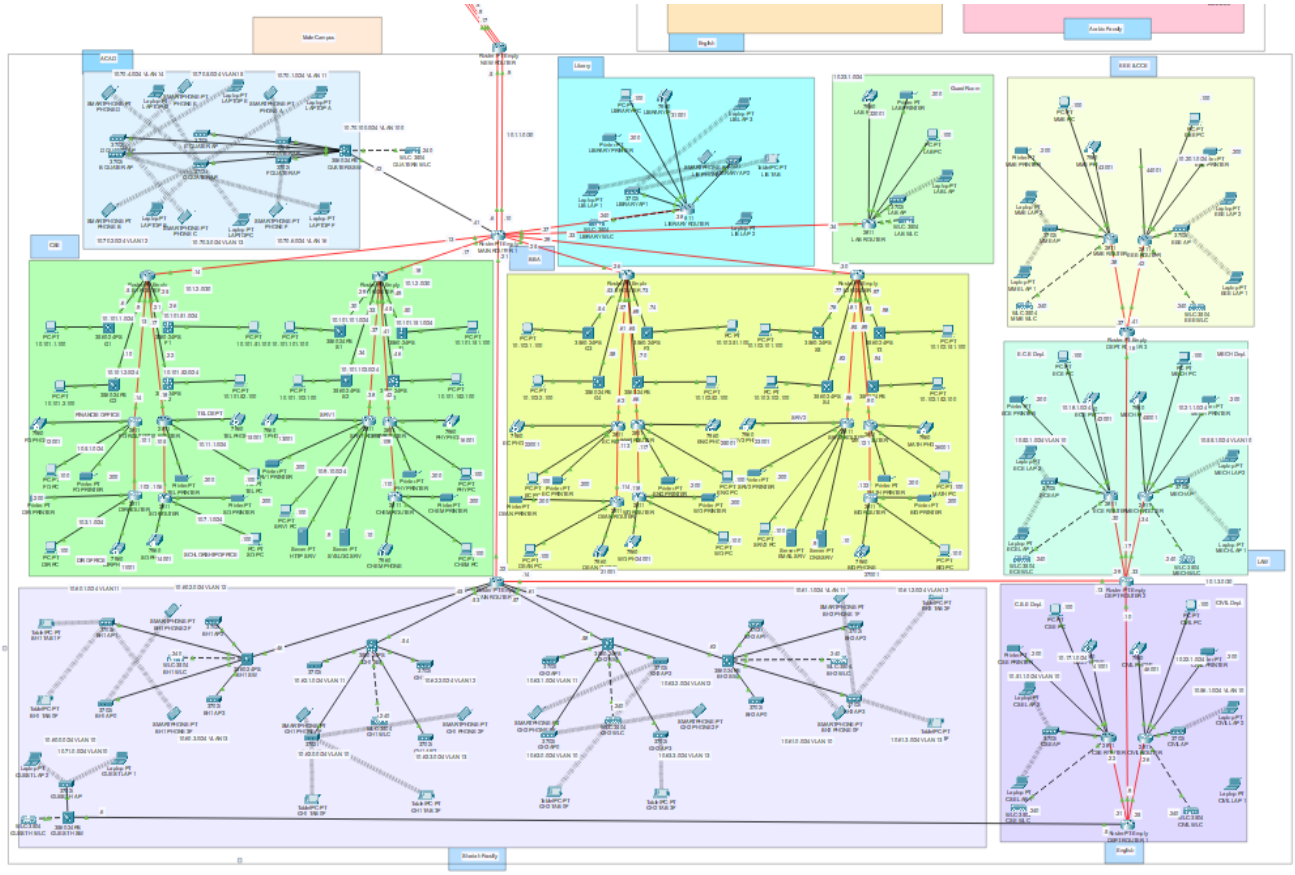

Fig- Male Campus Network

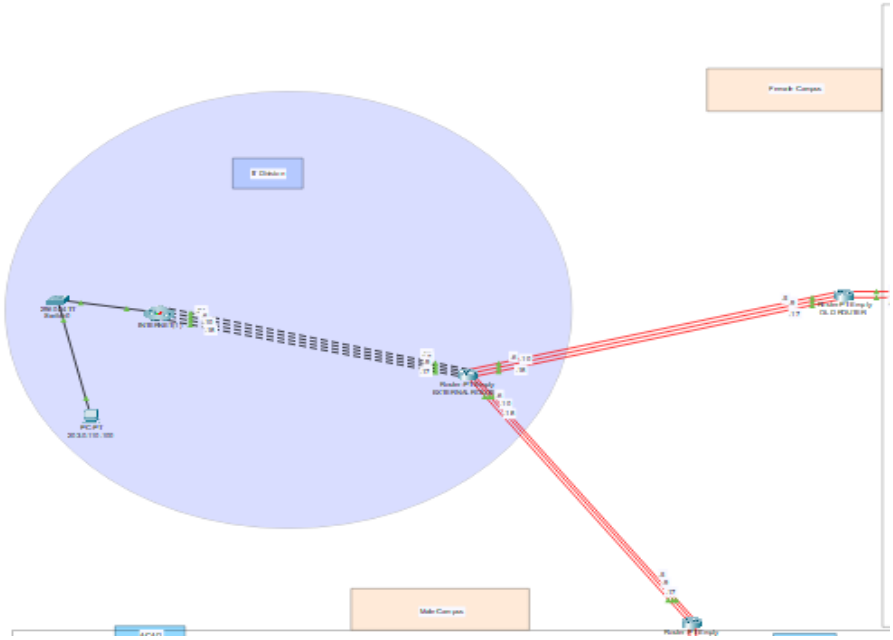

Fig- Main IT Division

6. Future Work

Although the current IIUC campus LAN network is fully functional, it can be further enhanced in the following areas:

1. **Security and Monitoring:** Implement advanced security features like intrusion detection and prevention systems (IDS/IPS) and deploy network monitoring tools to detect faults and prevent unauthorized access.
2. **Wireless and IoT Expansion:** Increase wireless coverage by adding more access points and implementing Wi-Fi 6, and integrate IoT devices such as smart classrooms, automated lighting, and environmental sensors.
3. **Cloud Services and Scalability:** Introduce cloud-based services for email, file storage, and backup, and design the network to handle future expansions, including new buildings and additional academic blocks.

7. Conclusion

The design and implementation of the IIUC campus LAN network has provided a comprehensive understanding of both theoretical and practical aspects of modern network architecture. The project demonstrates how a hierarchical network structure with clearly defined core, distribution, and access layers can ensure scalability, reliability, and efficient management of campus connectivity. Secure site-to-site IPSec connections between different campuses enable safe data transfer and communication, while the integration of multiple devices including routers, multilayer and access switches, PCs, laptops, IP phones, printers, servers, and wireless access points ensures seamless connectivity for both wired and wireless users. Throughout the project, challenges such as maintaining security without compromising performance, configuring devices correctly, and managing the complexity of a large network were successfully addressed. While the current implementation focuses on the main campus network, further enhancements such as adding individual academic departments, implementing advanced security measures, monitoring tools, and backup servers are planned for future work. Overall, this project effectively combines theoretical knowledge with practical execution, resulting in a robust, efficient, and future-ready network that can meet the growing demands of students, faculty, and staff.

8. References

1. *Maris Trops*, Designing and Deploying a Campus Wide Wireless Network with MikroTik. *https://mikrotik.com/download/pdf/Campus_WiFi_with_MikroTik.pdf*
2. *Saadat Malik*, Network Security Principles and Practices. *https://www.cisco.com/c/dam/en/us/about/security-center/network-security-principles-practices.pdf*
3. *Microsoft*, Windows Server 2019 Security Features and Best Practices. *https://docs.microsoft.com/en-us/windows-server/security/windows-server-2019-security-features*
4. *Cisco*, Cisco Campus Network Design Basics. *https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-campus/campus-network-design-basics.html*
5. *MikroTik*, MikroTik RouterOS Security Guide. *https://wiki.mikrotik.com/wiki/MikroTik_RouterOS_Security_Guide*
6. *Lakshmi Deepak*, Campus LAN Network Design RGUKT RKV. *https://github.com/LakshmiDeepak9653/Campus-Lan-Network-Design-RGUKT-RKV/blob/main/README.md*