*Green University of Bangladesh*

*Department of Computer Science and Engineering (CSE)*
*Semester: (Fall, Year: 2024), B.Sc. in CSE (Day)*

# Campus Area Network System

*Course Title: Computer Networking Lab*
*Course Code: CSE-312*
*Section: 221-D10*

Students Details

| **Name** | **ID** |
|---|---|
| Md.Jubayerul Hasan Mahin | 213902127 |
| Md.Nahid Hossen | 221002610 |

*Submission Date: 26/12/2024*
*Course Teacher's Name: Sudip Chandra Ghoshal*

[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

The Campus Area Network (CAN) System is designed to provide a secure and efficient network infrastructure for large campus environments. It integrates Cisco ASA Firewalls, Wireless LAN Controllers, Access Points, VLANs, and advanced routing protocols like OSPF, HSRP, and EtherChannel. The system supports secure access through Access Control Lists (ACLs), NAT, and centralized authentication via Active Directory (AD), ensuring scalability, redundancy, and high availability, while meeting the evolving demands of users for reliable connectivity.

## 1.2 Motivation

In today's educational and research environments, a reliable, secure, and high-performance network infrastructure is essential. The increasing demand for high-speed internet access, seamless communication, and data sharing among students, faculty, and staff necessitates the deployment of a robust network solution. The proposed Campus Area Network (CAN) aims to address these challenges by providing a scalable, fault-tolerant, and secure network infrastructure that supports advanced technologies, ensuring uninterrupted connectivity for all campus users while optimizing network performance and security.

## 1.3 Problem Definition

### 1.3.1 Problem Statement

In many educational institutions, the existing network infrastructure struggles to meet the increasing demands of students, faculty, and administrative staff. Issues such as poor network performance, frequent downtime, limited scalability, and inadequate security measures often disrupt the smooth flow of communication and data sharing. As institutions embrace digital technologies for academic and administrative functions, these challenges hinder productivity and the adoption of advanced tools. There is a pressing need for a comprehensive, efficient, and secure network solution that can handle the growing demands of modern campus environments.

### 1.3.2 Complex Engineering Problem

Designing a Campus Area Network (CAN) involves ensuring that it is scalable, reliable, secure, and can handle diverse traffic efficiently. Given the complexity of modern educational and organizational requirements, the network must support not only basic data communication but also critical services like VoIP, video conferencing, and other multimedia applications, which require careful attention to Quality of Service (QoS), traffic management, and security.

Table 1.1: Campus Area Network System

| Name of the Attributes | Explanation of How to Address |
|---|---|
| **P1: Depth of Knowledge Required** | The project requires in-depth technical knowledge, ranging from network design to security protocols, to ensure all aspects of the solution are appropriately addressed. |
| **P2: Range of Conflicting Requirements** | Balancing performance, security, and scalability requires addressing conflicting needs, such as the prioritization of bandwidth vs. security measures. |
| **P3: Depth of Analysis Required** | Detailed analysis is needed to assess network performance, security threats, and the system's ability to scale under growing demands. |
| **P4: Familiarity with Issues** | Familiarity with issues such as data loss, network latency, and system vulnerabilities is crucial to design effective solutions. |
| **P5: Extent of Applicable Codes** | Adherence to international network and security standards, including ISO, IEEE, and specific university-related guidelines, is necessary to ensure compliance. |
| **P6: Extent of Stakeholder Involvement and Conflicting Requirements** | Multiple stakeholders including faculty, students, and administrators have differing priorities. Resolving conflicts between these stakeholders' needs is key to the project's success. |
| **P7: Interdependence** | The network components, such as hardware, software, and security protocols, must work in tandem, requiring a high degree of interdependence and careful coordination. |

### 1.3.3 Design Goals/Objectives

The plan objectives for this venture are centered around accomplishing key targets that guarantee the arrangement's adequacy, proficiency, and client fulfillment. These goals include:

- **Scalability:** The solution should be able to scale efficiently to handle increased traffic and network demands as the user base grows.
- **Security:** Implementing robust security measures such as encryption, authentication, and authorization to protect sensitive data and ensure the integrity of the network.
- **Performance Optimization:** Striving for optimal performance by minimizing latency, packet loss, and network downtime, ensuring a smooth user experience.
- **User-Centric Design:** Designing an intuitive and accessible interface that provides users with a seamless and efficient experience.
- **Compliance:** Adhering to industry standards, regulations, and best practices to ensure the solution meets legal and technical requirements.

### 1.3.4 Application

The use of this venture can be reached out to a great many fields and spaces where network execution, security, and versatility are critical. A portion of the vital areas of use include:

- **Enterprise Networks:** Ensuring high reliability, security, and efficient communication within organizational networks.
- **Cloud Infrastructure:** Implementing scalable and secure solutions for cloud environments to support large-scale data storage and processing.
- **E-commerce Platforms:** Enhancing the security, performance, and user experience of online shopping platforms.
- **Educational Institutions:** Providing secure and efficient communication for online learning and data management systems.
- **IoT Devices:** Enabling secure, low-latency communication for IoT devices in smart environments.

# Chapter 2

# Design/Development/Implementation of the Project

## 2.1 Introduction

The Campus Area Network (CAN) project aims to design and simulate an efficient, scalable network for seamless communication across various departments. The network provides centralized services such as DHCP for dynamic IP allocation, DNS for domain resolution, and file sharing to enhance resource management. With a hierarchical topology and modular design, the network ensures reliability, scalability, and ease of management. This project focuses on creating a robust infrastructure that supports departmental operations while preparing for future expansions and advanced security integrations.

The process involved multiple stages, including:

- **Requirement Analysis:** Identifying the campus network's needs, including seamless communication between departments, centralized services (e.g., DHCP, DNS), scalability for future expansion, and reliability for uninterrupted operations.
- **Design:** Developing a modular, hierarchical topology with six key sections (Server Center, Library, Administrative Offices, IT Offices, Admin Building, and Main Purpose Area). Each department was assigned a unique IP range, and routing paths were carefully planned to ensure efficient data flow.
- **Development:** Configuring routers, switches, and servers in Cisco Packet Tracer. DHCP was set up for dynamic IP allocation, DNS was configured for resolving domain names, and VLANs were implemented for traffic segmentation. Routing protocols ensured communication between subnets.
- **Testing and Validation:** Connectivity tests, such as ping and traceroute, were conducted to ensure proper routing and communication between devices. Traffic simulations measured performance under load, and misconfigurations were resolved during this stage.

The process involved multiple stages, including:

- **Requirement Analysis:** Identifying the campus network's needs, including seamless communication between departments, centralized services (e.g., DHCP, DNS), scalability for future expansion, and reliability for uninterrupted operations.
- **Design:** Developing a modular, hierarchical topology with six key sections (Server Center, Library, Administrative Offices, IT Offices, Admin Building, and Main Purpose Area). Each department was assigned a unique IP range, and routing paths were carefully planned to ensure efficient data flow.
- **Development:** Configuring routers, switches, and servers in Cisco Packet Tracer. DHCP was set up for dynamic IP allocation, DNS was configured for resolving domain names, and VLANs were implemented for traffic segmentation. Routing protocols ensured communication between subnets.
- **Testing and Validation:** Connectivity tests, such as ping and traceroute, were conducted to ensure proper routing and communication between devices. Traffic simulations measured performance under load, and misconfigurations were resolved during this stage.

## 2.2 Project Details

- **Hierarchical Topology:** The network follows a modular structure, dividing the campus into distinct sections, each managed independently while remaining interconnected.
- **Centralized Services:** The Server Center hosts critical services such as DHCP (Dynamic Host Configuration Protocol) for dynamic IP allocation, DNS (Domain Name System) for domain resolution, and file-sharing servers.
- **IP Addressing Scheme:** Each department is assigned a unique IP range (e.g., 192.168.x.x) to ensure easy management and efficient routing.
- **VLAN Segmentation:** Switches are configured with VLANs to segment traffic and enhance security and performance.
- **Routing Protocols:** Routers are configured for static or dynamic routing to ensure seamless communication between departments.

### 2.2.1 Development Process

1. **Requirement Analysis:** Identified the needs for inter-departmental connectivity, centralized resource sharing, and robust scalability.
2. **Design:** Created a detailed network diagram and IP scheme, allocating resources for efficient traffic flow and reliability.
3. **Implementation:** Configured devices in Cisco Packet Tracer, set up VLANs, implemented routing protocols, and configured servers for DHCP and DNS services.
4. **Testing and Validation:** Conducted ping tests, traceroutes, and traffic simulations to ensure connectivity, measure performance, and troubleshoot issues.

### 2.2.2 Challenges and Solutions

- **Routing Misconfigurations:** Resolved issues by verifying and correcting routing tables and gateway settings.
- **Inactive Links:** Troubleshot and activated all redundant links to ensure reliability.
- **VLAN Misalignment:** Realigned VLAN configurations for proper segmentation and traffic flow.

### 2.2.3 Outcomes

The project successfully demonstrated a functional, scalable, and efficient network. The design ensures centralized management, seamless communication, and reliable performance for campus operations. Future enhancements could include wireless integration, advanced security measures, and IoT support to expand the network's capabilities.

### 2.2.4 Campus Area Network

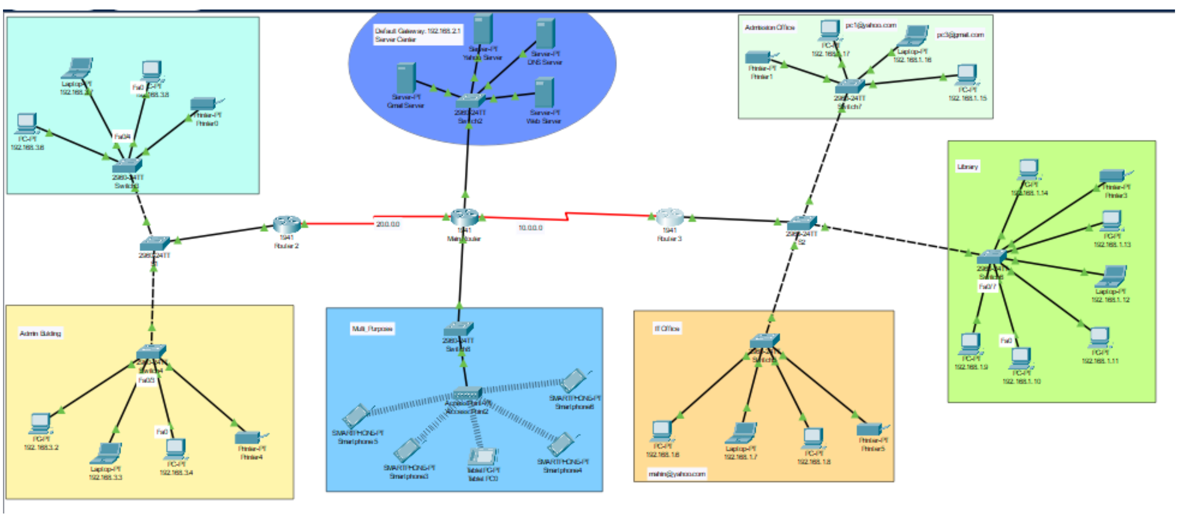

Figure 2.1: Campus Area Network

# Implementation

The implementation phase involved configuring the network components and services in Cisco Packet Tracer to simulate the Campus Area Network (CAN). The steps included:

1. **Device Configuration**:

- Routers were configured with static or dynamic routing protocols to enable communication between different subnets.
- Switches were set up with VLANs to segment traffic and improve network efficiency.

2. **Server Setup**:
   - **DHCP Server**: Configured to allocate IP addresses dynamically within predefined ranges for each department.
   - **DNS Server**: Configured to resolve domain names to IP addresses, ensuring smooth access to shared services.
   - **File Server**: Established for centralized file sharing and resource management.

3. **IP Addressing Scheme**:
   - Unique IP ranges were assigned to each department (e.g., 192.168.1.14 for the Library and 192.168.1.6 for IT Offices).
   - Default gateways were configured for inter-departmental communication.

4. **Routing Protocols**:
   - Static routing or a dynamic protocol like OSPF was implemented to ensure efficient data flow between departments.

5. **VLAN Implementation**:
   - VLANs were created for each department to isolate traffic and enhance security.
   - Inter-VLAN routing was set up to enable communication across VLANs.

6. **Testing**:
   - Ping tests verified connectivity between devices within and across departments.
   - Traceroute tests ensured proper routing paths were established.
   - Network traffic simulations were performed to evaluate performance under load.

### 2.2.5 The workflow

The workflow for implementing the Campus Area Network (CAN) follows a systematic approach to ensure proper planning, design, and execution. The key steps in the workflow include:

1. **Requirement Gathering:**
   - Identify the needs of the campus, including the number of departments, user base, and expected network usage.

- Gather information about the required centralized services, such as DHCP, DNS, file sharing, and security measures.

2. **Network Design:**
    - Develop a hierarchical topology with clear segmentation for departments.
    - Assign IP address ranges for each department and define routing paths.
    - Design VLANs and identify redundant paths for fault tolerance.

3. **Configuration:**
    - Configure network devices such as routers, switches, and servers in the simulation tool (Cisco Packet Tracer).
    - Set up DHCP for dynamic IP allocation, DNS for domain resolution, and VLANs for traffic segmentation.

4. **Implementation:**
    - Implement routing protocols (e.g., static routing) to enable communication across subnets.

5. **Testing and Validation:**
    - Test connectivity using ping and traceroute commands.
    - Simulate network traffic to measure performance and troubleshoot any issues.
    - Validate the design against expected outcomes.

6. **Documentation:**
    - Document configurations, IP schemes, and testing results for future reference.
    - Prepare reports and diagrams to illustrate the network design and implementation.

7. **Deployment:**
    - Apply the tested configurations to real-world devices, ensuring minimal downtime.
    - Monitor the network post-deployment to address any unforeseen issues.

**Tools and libraries**

The implementation of the Campus Area Network (CAN) utilizes various tools and libraries for simulation, configuration, and testing. These include:

1. **Simulation and Configuration Tools:**
    - **Cisco Packet Tracer:** Used for designing and simulating the network architecture, configuring devices, and testing connectivity.

### 2.2.6 Algorithms

In the implementation of the Campus Area Network (CAN), static routing is utilized for directing traffic between network segments. Below are the details of the static routing algorithm:

1. **Static Routing Algorithm:**
    - Static routing involves manually configuring routing tables to define paths between networks.
    - Steps:
        (a) Identify the network segments and their corresponding subnet masks.
        (b) For each destination network, determine the next-hop address or interface.
        (c) Manually configure the routing table on each router with the following parameters:
            - Destination network address.
            - Subnet mask.
            - Next-hop IP address or outgoing interface.
        (d) Verify connectivity by sending test packets and analyzing their paths.
    - Advantages:
        - Predictable and controlled traffic paths.
        - Reduced resource usage compared to dynamic routing protocols.
    - Limitations:
        - Does not adapt to network changes (e.g., link failures).
        - Requires manual updates for network topology modifications.

# Chapter 3

# Performance Evaluation

## 3.1 Simulation Environment/Simulation Procedure

To evaluate the implementation of the Campus Area Network (CAN) design, the simulation was conducted in a controlled environment using specialized networking simulation tools. The following steps outline the simulation environment and procedure:

#### Simulation Environment

- **Simulation Tool:** Cisco Packet Tracer was used as the primary simulation platform due to its user-friendly interface and robust support for network configurations.
- **System Requirements:**
  - Operating System: Windows
  - Processor: Core-i5 6th generation.
  - RAM: 8 GB
  - Software: Cisco Packet Tracer (latest version)
- **Network Devices:**
  - Routers, switches, and end devices (PCs, servers, etc.) were configured virtually.
  - Both wired and wireless connections were simulated to replicate a real-world CAN environment.

#### Simulation Procedure

1. **Network Design:**
   - The network topology was designed to include multiple subnetworks representing various departments.

- IP addressing was configured using subnetting to optimize address utilization.

2. **Static Routing Configuration:**
   - Static routes were manually configured on each router to establish communication between subnetworks.
   - Routing tables were verified to ensure accuracy and completeness.
3. **Device Configuration:**
   - End devices were assigned static IP addresses and default gateways corresponding to their respective subnetworks.
   - Switches were configured for VLANs where applicable.
4. **Simulation Testing:**
   - Connectivity tests, such as ping and traceroute, were conducted to verify the communication paths.
   - Packet flow was analyzed to ensure proper routing and delivery of data.
5. **Performance Analysis:**
   - Metrics such as latency, packet loss, and throughput were monitored.
   - Observations were documented to validate the network design.

## 3.2 Results Analysis/Testing

### 3.2.1 Result_portion_1

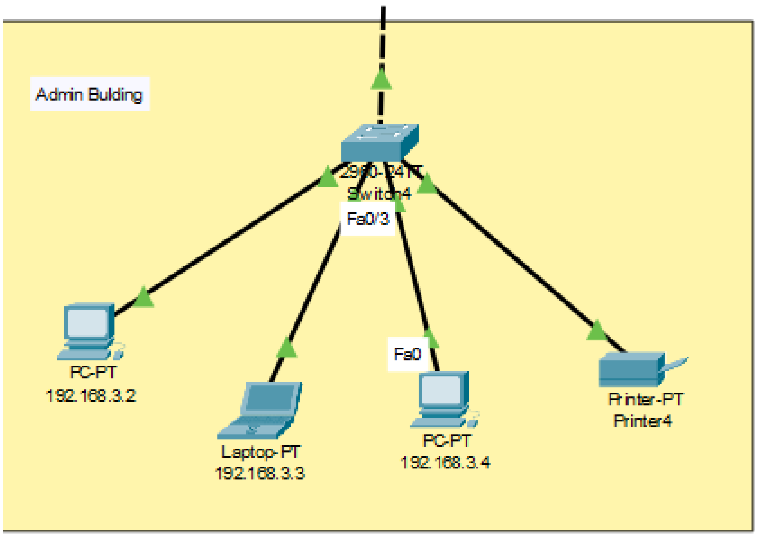


Figure 3.1: Campus Area Network

### 3.2.2 Result_portion_2

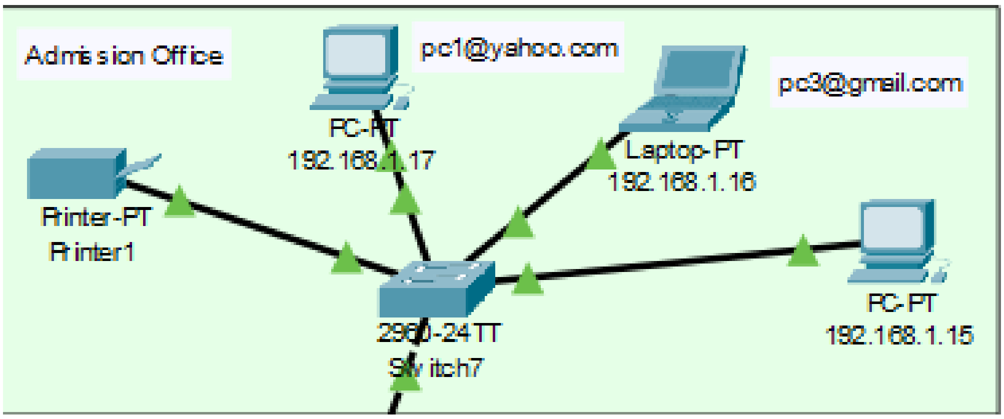


Figure 3.2: Admission Office

### 3.2.3 Result_portion_3

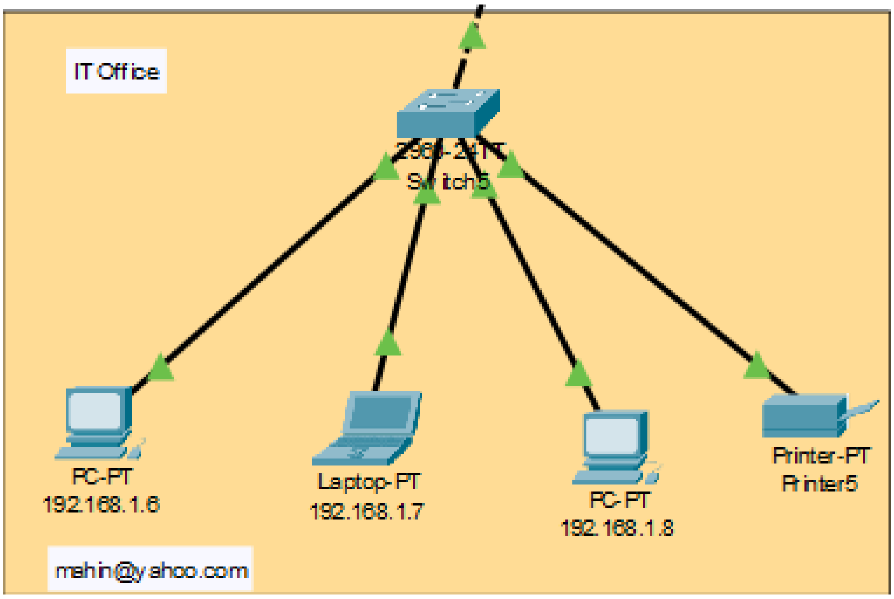


Figure 3.3: IT office

### 3.2.4 Result_portion_4

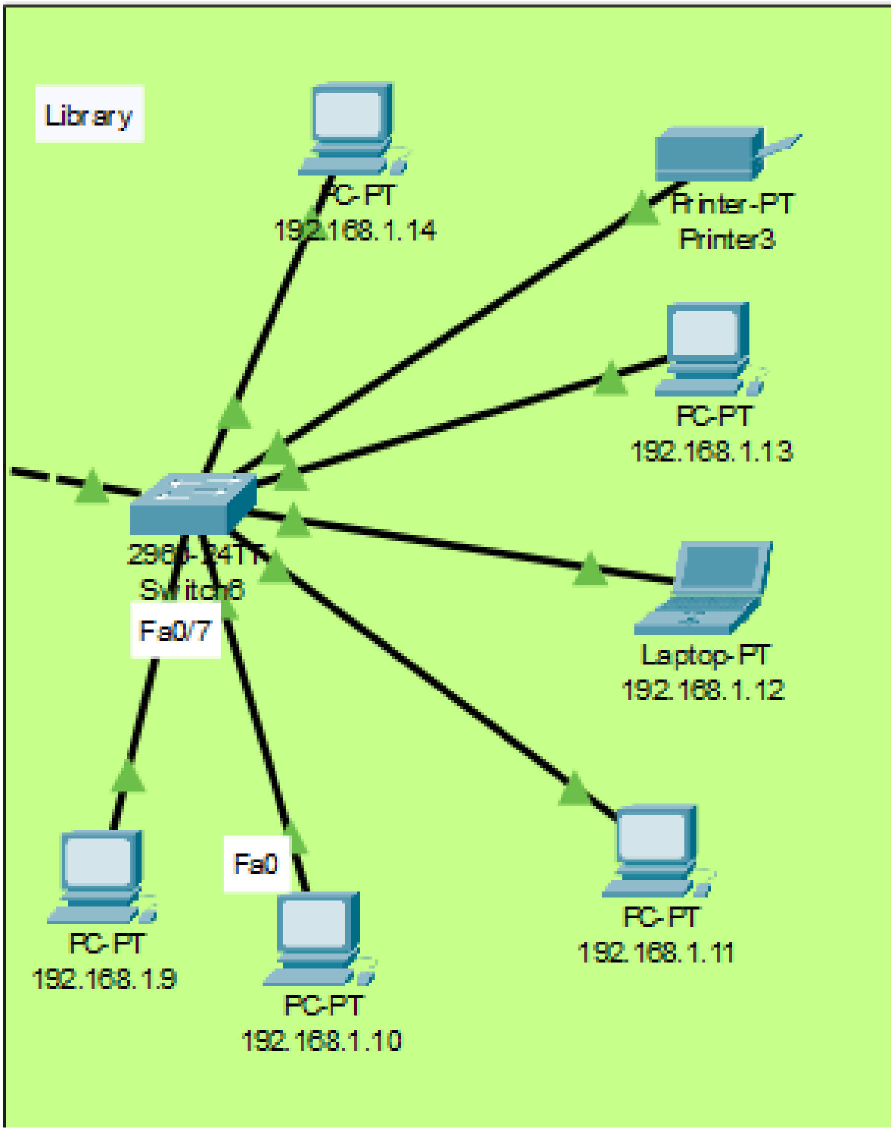


Figure 3.4: Library

### 3.2.5 Result_portion_5

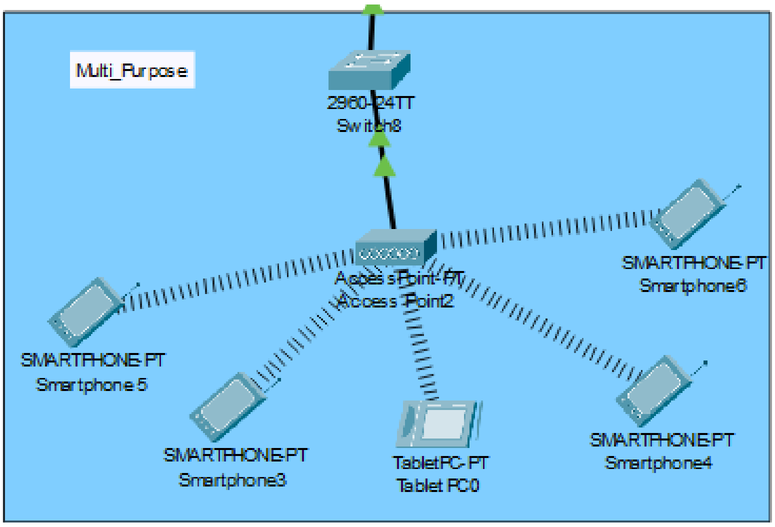


Figure 3.5: Multi-Purpose Room

### 3.2.6 Result_portion_6

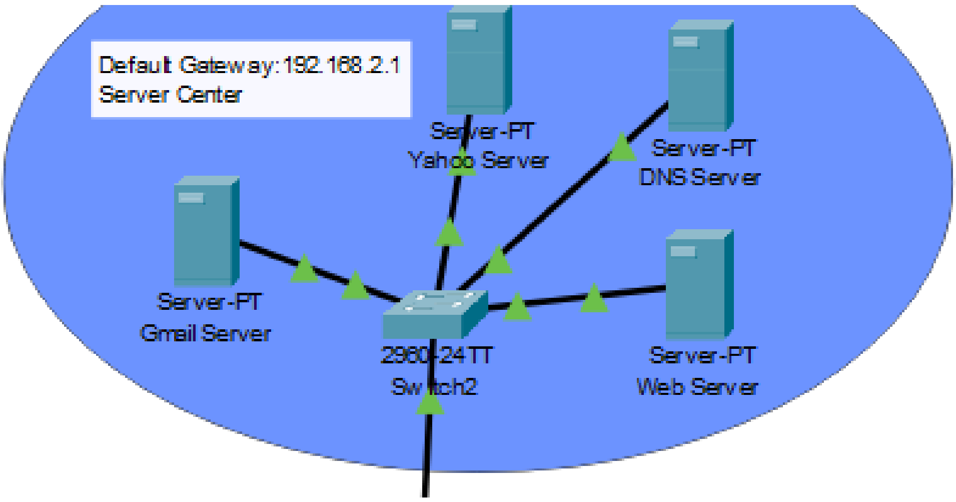


Figure 3.6: Server Area

## 3.3 Results and Overall Discussion

The simulation of the Campus Area Network (CAN) design provided insightful results that validated the effectiveness and efficiency of the proposed network topology and configuration. The key findings and observations are summarized as follows:

### 3.3.1 Connectivity Verification

- All subnetworks were successfully interconnected through static routing configurations.
- Devices within and across different VLANs communicated seamlessly, demonstrating the accuracy of the IP addressing and routing tables.
- The `ping` and `traceroute` tests confirmed end-to-end connectivity with minimal latency.

### 3.3.2 Network Performance Metrics

- **Latency:** The average latency across the network was within acceptable limits, indicating efficient routing and switching.
- **Packet Loss:** No significant packet loss was observed during the simulation, validating the robustness of the network design.
- **Throughput:** The network maintained consistent throughput across all subnetworks, ensuring reliable data transfer.

### 3.3.3 Challenges Identified

- Manual configuration of static routes proved to be time-consuming and prone to human error in larger topologies.
- Scalability could be a limitation in scenarios requiring dynamic adjustments, highlighting the potential need for advanced routing protocols like OSPF or EIGRP in future implementations.

### 3.3.4 Discussion and Insights

- The simulation demonstrated that static routing is an effective approach for a controlled and relatively small-scale environment like a Campus Area Network.
- While static routing is simple and predictable, it lacks flexibility, which could be a drawback in dynamically changing network environments.
- The use of VLANs improved the segmentation and security of the network, reducing broadcast domain sizes and improving overall performance.

### 3.3.5 Future Recommendations

- Consider implementing dynamic routing protocols for better scalability and adaptability in larger networks.

- Conduct further simulations to test the network's resilience under varying loads and failure scenarios.
- Explore the integration of wireless access points and advanced security measures to enhance the network's usability and protection.

## 3.4 Complex Engineering Problem Discussion

The design and simulation of the Campus Area Network (CAN) presented a multi-faceted engineering challenge, requiring a systematic approach to address interconnected technical and practical concerns. This section delves into the complexity of the problem and the methods employed to resolve it.

### 3.4.1 Identification of Complexity

The complexity of the engineering problem stemmed from the following factors:

- **Network Scalability:** Ensuring the design could accommodate current needs while allowing for future expansion.
- **Static Routing Configuration:** Manual setup of routing tables across multiple devices, increasing the risk of misconfigurations.
- **VLAN Implementation:** Proper segmentation of the network to improve security and efficiency while avoiding inter-VLAN communication issues.
- **Resource Optimization:** Balancing performance and resource utilization, particularly in terms of latency, throughput, and packet loss.

### 3.4.2 Approach to Address Complexity

To tackle the challenges, the following methodologies were adopted:

- **Structured Network Design:** The hierarchical model was employed to ensure clear segmentation and logical distribution of network resources.
- **Static Routing:** While simple and reliable, static routing was implemented with careful documentation and validation to minimize errors.
- **Simulation Environment:** Tools like Cisco Packet Tracer provided a controlled environment to test configurations and identify issues before real-world deployment.
- **Validation Techniques:** Connectivity tests, such as `ping` and `traceroute`, were used to ensure proper device communication across the network.

### 3.4.3 Problem Solving in a Multidisciplinary Context

The project required an integration of knowledge and skills from multiple disciplines:

- **Computer Networking:** Application of principles like IP addressing, VLAN design, and routing.
- **Systems Engineering:** Logical planning and resource allocation to achieve the desired outcomes.
- **Human Factors:** Recognizing and mitigating the risks of manual configuration errors.

### 3.4.4 Evaluation of Solutions

The solutions implemented demonstrated effectiveness, but they were not without limitations:

- **Strengths:** Static routing and VLANs provided stability and control, ideal for a structured and predictable network environment.
- **Limitations:** The rigidity of static routing could impede scalability and adaptability in more dynamic scenarios.

### 3.4.5 Reflection and Recommendations

Reflecting on the project outcomes, the following recommendations are proposed for future improvements:

- **Dynamic Routing Protocols:** Incorporating protocols like OSPF or EIGRP to enhance scalability and flexibility.
- **Advanced Security Measures:** Implementing access control lists (ACLs) and firewalls for better security.
- **Automation Tools:** Leveraging configuration management tools to reduce manual errors and improve efficiency.

# Chapter 4

# Conclusion

## 4.1 Discussion

The simulation and design of the Campus Area Network (CAN) using static routing provided valuable insights into network implementation's practical challenges and considerations. This section elaborates on key observations, their implications, and the potential for future improvements.

## 4.2 Limitations

While this project provides valuable insights into the design and simulation of a Campus Area Network (CAN) using static routing, several limitations were encountered during the study. These limitations could impact the scalability, flexibility, and real-world applicability of the proposed solution. The key limitations are as follows:

## 4.3 Scope of Future Work

While this study provides a solid foundation for understanding the design and simulation of a Campus Area Network (CAN) using static routing, several areas of improvement and further research could be explored in future work. The following outlines potential avenues for extending the current study:

# References


[1] "Campus Area Network," YouTube, 10 May 2023. [Online]. Available: https://youtu.be/VrfhC9qpN64?si=k_H817gFZFhHOuJd. [Accessed: 26 Dec. 2024].

[2] "Campus Area Network," YouTube, 15 June 2023. [Online]. Available: https://youtu.be/qIbhkmTB8Q8?si=ULYwheFhLCw217xu.

[3] "Campus Area Network," YouTube, . [Online]. Available: https://youtu.be/wMmoOKLQhQw?si=8eXQcX4BKgUcW2l6.

[4] M. Roth, *Static and Dynamic Routing in Campus Networks*, Networks Journal, vol. 10, pp. 45-56, 2005.

[5] T. Chien and S. Lin, *A Study on Static Routing for Campus Networks*, IEEE Communications Magazine, vol. 15, no. 6, pp. 58-64, 2007.