Design Campus Network

A PROJECT REPORT

Submitted by
Anisha Kumari(22BCS10853)
Nandini Katare(22BCS11522)

Submitted To
Er.Digvijay Puri(E10051)

in partial fulfillment for the award of the degree of

BACHELOR OF ENGINEERING

IN

Computer Science and Engineering

Chandigarh University
October-2024

BONAFIDE CERTIFICATE

Certified that this project report **"Design Campus Network"** is the bonafide work of "***Anisha Kumari(22BCS10853), Nandini Katare(22BCS11522)***" who carried out the project work under my/our supervision.

SIGNATURE

SUPERVISOR
Er. Digvijay Puri(E10051)

TABLE OF CONTENTS

Abstract

This project details the design and implementation of a robust and scalable network infrastructure for a large university distributed across two campuses. The university comprises four faculties: Health and Sciences, Business, Engineering/Computing, and Art/Design. Each faculty operates on distinct floors or buildings, and all administrative, academic, and student-related activities rely on efficient network communication. The primary goal of the project is to create a network that supports secure, reliable, and high-speed data transfer between the university's departments, faculty offices, and student labs, while accommodating the institution's future expansion needs.

The network design, modeled in Cisco Packet Tracer, follows a hierarchical design approach to ensure ease of management and scalability. The main campus consists of three key buildings: Building A for administrative staff and the Faculty of Business, Building B for the Faculties of Engineering/Computing and Art/Design, and Building C, housing student labs and the IT department that hosts critical university servers such as the web server. The smaller campus is exclusively used by the Faculty of Health and Sciences, where staff offices and student labs are separated by floors, with distinct network setups for each.

The project employs VLANs (Virtual Local Area Networks) to logically segment the network, enhancing performance, security, and traffic management across faculties and departments. Each VLAN isolates departmental traffic while enabling efficient communication between devices within the same VLAN. To facilitate communication between VLANs, the "Router on a Stick" configuration is used, with Inter-VLAN routing handled by a router. RIPv2 is configured as the internal routing protocol to efficiently manage routing between different subnets within the network. Additionally, static routing is used for external connectivity to services such as the university's cloud-hosted email server.

The network's IP addressing scheme is designed using subnetting, ensuring that each department operates on its own subnet for easier network management and traffic isolation. A DHCP server, configured on the router, automatically assigns IP addresses to devices in the administrative departments, reducing manual configuration efforts and simplifying network management. Secure network access is prioritized through the implementation of switchport security to prevent unauthorized access to the network, and SSH (Secure Shell) is enabled for remote management of network devices, ensuring secure administration.

In terms of physical implementation, appropriate cabling techniques are applied to connect routers, switches, and end devices, ensuring optimal network performance. Testing and verification of the network were conducted using various tools to ensure that all VLANs, DHCP, routing, and security configurations function as expected. Ping tests were used to verify connectivity across different VLANs and between campuses, while network security measures were validated to ensure robust protection against unauthorized access.

ABBREVIATIONS

Abbreviation Full Form

VLAN Virtual Local Area Network

DHCP Dynamic Host Configuration Protocol

RIPv2 Routing Information Protocol Version 2

SSH Secure Shell

IP Internet Protocol

PC Personal Computer

IT Information Technology

MAC Media Access Control

DNS Domain Name System

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

TCP/IP Transmission Control Protocol/Internet Protocol

NAT Network Address Translation

ISP Internet Service Provider

CHAPTER 1.

INTRODUCTION

1.1 Client Identification / Need Identification / Identification of Relevant Contemporary Issue-:

In today's educational landscape, the effective management of information and communication technologies (ICT) within universities is paramount. With the growing number of students and staff, the need for a robust network infrastructure that ensures seamless connectivity, data security, and efficient resource allocation has become a critical issue.

Justification of the Issue

Statistics show that universities across the globe are experiencing significant increases in student enrollment. For instance, the National Center for Education Statistics (NCES) reported a **16% increase** in student enrollment from 2000 to 2020. This surge results in higher demands on the university's IT resources, including network bandwidth and server capabilities. Additionally, reports from the EDUCAUSE Center for Analysis and Research indicate that **over 70% of educational institutions** consider network reliability and performance as a top priority for enhancing the student experience.

The need for a robust campus network is further substantiated by survey data. A recent survey conducted by the Internet2 organization indicated that **65% of faculty and staff** reported frustrations with current network speeds and reliability, highlighting the urgency for an improved network solution.

The issue is not merely an operational concern; it affects the overall academic experience, faculty productivity, and the institution's reputation. Given the critical role of digital resources in modern education, addressing this network challenge is essential for academic success.

Relevant Contemporary Issue Documentation

Various reports from agencies such as the National Institute of Standards and Technology (NIST) and the Higher Education Information Security Council (HEISC) have emphasized the importance of securing educational networks against cyber threats. The NIST Cybersecurity Framework outlines best practices for managing network security in educational institutions, which underscores the need for comprehensive planning in network design and implementation.

1.2. Identification of Problem-:

The broad problem that needs resolution is the inadequate and inefficient network infrastructure within the university, hindering effective communication and resource sharing among students, faculty, and administrative staff.
Key Issues:

Performance Bottlenecks: The existing network struggles to support the increasing number of devices and users. With more students and staff relying on digital resources, the network experiences significant slowdowns during peak usage hours. Reports indicate that over 60% of users encounter slow connection speeds and interruptions, particularly in high-demand areas like lecture halls and computer labs, leading to frustration and reduced academic productivity.

Unreliable Connections: High-density areas such as lecture halls and laboratories suffer from frequent disconnections and unstable connections. Surveys conducted among students and faculty reveal that more than 55% experience unreliable network access during crucial learning sessions, disrupting lectures and collaborative work. This unreliability undermines the effectiveness of online resources and tools that are integral to modern education.

Security Vulnerabilities: The lack of proper network segmentation poses significant security risks. With multiple departments sharing the same network infrastructure, the university becomes susceptible to unauthorized access and cyberattacks. A report from the Cybersecurity and Infrastructure Security Agency (CISA) indicates that educational institutions are prime targets for cyber threats, with over 70% experiencing incidents in the past year. Without effective security measures, sensitive data could be compromised, affecting both staff and students.

Inefficient Resource Utilization: The absence of a structured approach to network design results in inefficient resource allocation. Network traffic is not effectively managed, leading to wasted bandwidth and slow data transfer rates. This inefficiency can hinder access to essential shared resources, such as online libraries and collaborative platforms, ultimately impacting user satisfaction and academic performance.

Lack of Structured Network Design: The current network lacks a coherent design strategy, complicating troubleshooting and maintenance efforts. This absence of a structured framework leads to increased downtime and reactive responses to issues, rather than proactive management. Furthermore, the inability to scale the network appropriately makes it challenging to accommodate future growth in users and devices.

1.3. Identification of Tasks-:

To effectively address the identified problems within the university's network infrastructure, the following tasks will be defined and differentiated to guide the project from initial identification through to testing and implementation:

1.3.1 Network Assessment

- **Task Description**: Conduct a thorough assessment of the existing network infrastructure to identify limitations and areas for improvement.
- **Activities**:
    - Gather data on current network performance metrics (bandwidth, latency, and uptime).
    - Analyze user feedback through surveys to understand connectivity issues and user satisfaction.
    - Document the existing hardware and software configurations, including devices, protocols, and IP addressing schemes.

1.3.2 Requirement Gathering

- **Task Description**: Identify the specific requirements for the new network design based on the needs of various stakeholders.
- **Activities**:
    - Interview faculty, administrative staff, and students to gather insights on their network usage patterns and expectations.
    - Compile a list of required features, such as VLAN implementation, dynamic IP addressing, and enhanced security measures.
    - Review contemporary issues and best practices in network design to ensure the proposed solution aligns with current standards.

1.3.3 Network Design

- **Task Description**: Develop a comprehensive network design that incorporates the requirements identified in the previous task.
- **Activities**:
    - Create a detailed network topology diagram that illustrates the proposed layout, including the placement of routers, switches, and access points.
    - Design VLANs for each department to enhance security and improve network performance.
    - Plan for DHCP server implementation to enable dynamic IP address allocation for devices in specified areas.

1.3.4 Configuration

- **Task Description**: Configure the network devices according to the designed topology and ensure all components are correctly set up.
- **Activities**:

- Set up routers and switches with the necessary VLAN configurations, including inter-VLAN routing using a router-on-a-stick approach.
- Configure the DHCP server on the router to manage IP address allocation for user devices.
- Implement RIPv2 as the routing protocol to facilitate communication between different VLANs and ensure network resilience.

1.3.5 Testing and Validation

- **Task Description**: Conduct rigorous testing to validate that the new network design meets the specified requirements and functions correctly.
- **Activities**:
  - Perform connectivity tests to ensure all devices can communicate as intended across VLANs.
  - Evaluate network performance under peak load conditions to assess bandwidth utilization and response times.
  - Conduct security assessments to identify any vulnerabilities and confirm that implemented security measures are effective.

CHAPTER 2.
LITERATURE REVIEW/BACKGROUND STUDY

2.1 Existing Solutions-:

Educational institutions face numerous challenges regarding their network infrastructures, leading to the development and implementation of various solutions to enhance network performance and reliability.

2.1.1 Network Segmentation

One common approach is network segmentation through VLANs, which isolates traffic based on departmental needs. Institutions have successfully implemented VLANs to improve security and manage bandwidth efficiently. For example, studies demonstrate that universities employing VLANs experience reduced broadcast traffic and increased overall performance (Liu et al., 2019).

2.1.2 Upgraded Hardware and Software

Another solution involves upgrading hardware components, such as routers and switches, to accommodate the growing number of users and devices. By investing in modern networking equipment, universities can achieve higher throughput and lower latency. Research indicates that upgrading to gigabit Ethernet and utilizing advanced routing protocols like RIPv2 can significantly enhance network performance (Hossain et al., 2016).

2.1.3 Implementation of Cloud Services

The adoption of cloud services for hosting applications and data has also emerged as a viable solution. This approach reduces the burden on local servers and enables greater scalability. Institutions utilizing cloud-based resources report improved accessibility and collaboration among students and faculty (Cheng & Zhao, 2018). Additionally, implementing cloud-based email services can enhance communication while providing robust security measures.

2.1.4 Comprehensive Security Frameworks

Security measures are increasingly critical in network design. Many universities are implementing multi-layered security frameworks, including firewalls, intrusion detection systems, and VPNs for remote access. Saha and Basak (2020) emphasize the importance of a proactive security strategy to safeguard sensitive data against cyber threats. Institutions that prioritize security measures benefit from increased trust and a safer online environment for their users.

2.2 Review Summary

The review of existing literature and practices highlights several effective solutions that address the challenges faced by educational institutions regarding network infrastructure. Network segmentation, hardware upgrades, cloud services, and robust security frameworks have all proven beneficial in enhancing performance and reliability.

Importance of Modernized Network Designs

The transition towards modernized network designs reflects a growing recognition of the diverse needs of educational environments. As technology continues to evolve, institutions must adapt their networks to support various digital learning initiatives, including online courses, virtual classrooms, and collaborative research projects. The literature indicates that outdated network infrastructures often hinder these initiatives, leading to frustration among users and a decline in academic performance (Al-Suqri, 2020). Thus, the need for an adaptable, scalable, and resilient network infrastructure is paramount.

Integration of Emerging Technologies

Emerging technologies, such as Software-Defined Networking (SDN) and Network Function Virtualization (NFV), are also gaining traction in educational settings. These technologies offer greater flexibility and efficiency in managing network resources, allowing institutions to respond more rapidly to changing demands. By integrating SDN, universities can dynamically allocate resources, optimize network traffic, and improve overall performance (Hossain et al., 2016).

Emphasis on User-Centric Design

Another key aspect highlighted in the literature is the emphasis on user-centric network design. Understanding the unique needs and behaviors of students and faculty can guide the development of tailored solutions that enhance user experience. For instance, incorporating wireless access points in high-traffic areas can significantly improve connectivity and accessibility, facilitating better engagement in learning activities (Cheng & Zhao, 2018).

Continuous Monitoring and Improvement

Furthermore, the importance of continuous monitoring and improvement cannot be overstated. The dynamic nature of network usage in educational institutions necessitates regular assessments to identify potential issues before they escalate. Implementing monitoring tools and analytics can help institutions track performance metrics and user satisfaction, enabling proactive adjustments to the network as needed (Zhang & Wang, 2017).

2.3 Problem Definition

Despite the availability of various solutions, many educational institutions continue to struggle with inadequate network infrastructures that do not fully address their specific needs. The persistence of performance bottlenecks, security vulnerabilities, and ineffective resource management indicates a gap between existing solutions and the actual requirements of users.

Performance Bottlenecks

One of the primary challenges faced by educational institutions is the growing number of connected devices and users. As more students and faculty utilize digital tools for learning and administrative tasks, the demand for network resources has significantly increased. Existing infrastructures, often based on outdated technology, are frequently unable to cope with this demand, leading to slow internet speeds, dropped connections, and a diminished user experience. These performance issues can adversely affect teaching and learning, as students require reliable access to online resources and collaborative tools.

Security Vulnerabilities

In addition to performance issues, security vulnerabilities present a major concern for educational institutions. Many universities are targeted by cyberattacks due to the sensitive nature of the data they handle, including personal information of students and staff, research data, and financial records. Inadequate security measures, such as weak authentication protocols and insufficient network segmentation, can expose institutions to data breaches and unauthorized access. The consequences of such incidents can be severe, resulting in reputational damage, financial loss, and legal ramifications.

Ineffective Resource Management

Ineffective resource management is another critical problem affecting network efficiency. Without proper segmentation of network traffic, institutions often face challenges in prioritizing critical applications over less important ones. This lack of prioritization can lead to network congestion, where essential services are interrupted or slowed down due to excessive non-essential traffic. Furthermore, the absence of a structured approach to managing IP addresses and network devices complicates troubleshooting efforts, leading to prolonged downtime and frustration among users.

Need for Tailored Solutions

Given these challenges, there is a clear need for tailored network solutions that address the specific requirements of educational institutions. A one-size-fits-all approach is insufficient in today’s rapidly evolving technological landscape. Institutions must adopt a comprehensive and strategic framework for network design that incorporates scalability, security, and effective resource management.

Project Aims

This project aims to bridge the gap between existing solutions and the unique challenges faced by educational institutions by developing a tailored network design. By leveraging best practices from the reviewed literature and incorporating modern technologies, this design will focus on optimizing performance, enhancing security, and improving resource management. The outcome will be a robust and adaptive network infrastructure that not only meets current demands but is also prepared for future growth and technological advancements.

2.4 Goals/Objectives

The primary goal of this project is to design and implement a robust network infrastructure that meets the communication and resource-sharing needs of students, faculty, and administrative staff. The specific objectives include:

1. Assess Current Network Performance

Conduct a thorough analysis of the existing network to identify performance bottlenecks, security vulnerabilities, and areas for improvement. This assessment will involve gathering data on current network usage, response times, and failure rates to provide a clear baseline for the new design.

2. Design a Scalable Network

Create a comprehensive network topology that incorporates VLANs, DHCP, and advanced routing protocols to ensure efficient communication among different departments. The design will prioritize scalability, allowing for future growth as the number of users and devices increases.

3. Enhance Security Measures

Implement a multi-layered security framework to protect against unauthorized access and data breaches, ensuring the safety of sensitive information. This will include strategies such as network segmentation, firewall configurations, and the establishment of secure access controls to safeguard the network infrastructure.

4. Test and Validate the Network Design

Conduct rigorous testing to ensure that the new network infrastructure meets the specified requirements and performs optimally under various conditions. This will involve simulating different traffic loads and testing the resilience of the network against potential failure scenarios to confirm its reliability and efficiency.

5. Document the Network Architecture

Provide comprehensive documentation of the network design, configurations, and testing results to facilitate ongoing management and maintenance. This

documentation will serve as a valuable resource for network administrators, ensuring that they have clear guidelines for future updates and troubleshooting efforts.

6. Foster Collaboration and Resource Sharing

Ultimately, the project aims to create an environment that enhances collaboration and resource sharing among all users. By providing reliable connectivity and secure access to shared resources, the network will support various academic and administrative functions, contributing to the overall success of the institution.

CHAPTER 3.

DESIGN FLOW/PROCESS

3.1 Evaluation & Selection of Specifications/Features-:

In this section, we critically evaluate the features identified in the literature and prepare a list of features ideally required in the network solution. These features are essential for creating a robust, efficient, and secure network infrastructure that meets the needs of a modern educational institution. Key features include:

1. Network Scalability

- The ability to expand the network without significant changes to the existing infrastructure is crucial for accommodating more devices and users. This includes the capability to add additional access points, switches, and servers seamlessly, ensuring that the network can grow alongside the institution without disruption.

2. Security Protocols

- Implementation of multi-layered security measures is vital for protecting sensitive data from unauthorized access and cyber threats. This includes:
    - **Firewalls** to monitor incoming and outgoing traffic based on predetermined security rules.
    - **Intrusion Detection Systems (IDS)** to identify and respond to potential threats in real-time.
    - **Secure Access Controls** to restrict network access based on user roles and permissions, enhancing overall security posture.

3. VLAN Support

- The capability to segment the network into different Virtual Local Area Networks (VLANs) enhances both performance and security. VLANs allow for:
    - Isolation of network traffic among different departments, reducing congestion and improving response times.
    - Enhanced security by limiting access to sensitive resources to authorized users only, thereby minimizing the risk of data breaches.

4. Dynamic IP Management

- Utilization of DHCP (Dynamic Host Configuration Protocol) for automatic IP address assignment ensures efficient IP address management. This feature:
    - Simplifies the process of connecting new devices to the network, as IP addresses are automatically assigned without manual configuration.

- Reduces the risk of IP address conflicts, which can cause connectivity issues and hinder network performance.

5. Redundancy and Reliability

- Features that ensure network reliability are critical for minimizing downtime and maintaining continuous service. This includes:

  - **Redundant Links** that provide alternative data paths in case of a primary link failure, ensuring uninterrupted connectivity.
  - **Backup Power Solutions** to keep essential networking equipment operational during power outages, safeguarding against data loss and service interruptions.

6. Monitoring and Management Tools

- Integration of network monitoring solutions for real-time performance analysis and troubleshooting is essential for proactive management. These tools provide:

  - Visibility into network traffic patterns, enabling administrators to identify potential issues before they escalate.
  - Reporting features that assist in capacity planning and optimization, ensuring that the network continues to meet the demands of users.

7. Quality of Service (QoS)

- Implementation of QoS mechanisms to prioritize critical network traffic ensures that essential services, such as video conferencing and online learning platforms, receive the necessary bandwidth to function effectively. This includes:

  - Traffic shaping techniques to manage bandwidth allocation and minimize latency during peak usage times.

8. User Training and Support

- Providing user training and ongoing support is crucial for maximizing the effectiveness of the network. This feature involves:

  - Developing training programs that educate users on best practices for network usage and security, empowering them to make the most of the available resources.

3.2 Design Constraints-:

Several design constraints must be considered to ensure the proposed network meets regulatory and operational standards. Addressing these constraints will not only enhance the feasibility of the network design but also ensure its sustainability and effectiveness in meeting the needs of the educational institution:

1. Regulatory Compliance

- Adherence to local and international regulations regarding data privacy is crucial for maintaining the integrity and confidentiality of sensitive personal information. Regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) impose strict guidelines on data handling, storage, and sharing. The network design must include features that facilitate compliance, such as data encryption, access controls, and auditing mechanisms.

2. Economic Constraints

- Budget limitations significantly impact the selection of hardware, software, and services. The design must balance cost-effectiveness with quality to avoid compromising performance and reliability. This may involve:
    - Prioritizing essential features while considering alternative solutions that provide similar functionalities at lower costs.
    - Exploring partnerships or grants that can supplement funding and allow for higher quality components without exceeding budgetary limits.

3. Environmental Considerations

- Incorporating energy-efficient designs is essential for reducing the carbon footprint of the network infrastructure. The design should comply with environmental sustainability practices, which may include:
    - Utilizing energy-efficient hardware and optimizing network configurations to minimize energy consumption.
    - Implementing practices such as virtualization to reduce the number of physical servers needed, thereby decreasing energy usage and cooling requirements.

4. Health and Safety Regulations

- Ensuring all networking equipment complies with health and safety standards is paramount for protecting users from hazards related to electrical and electromagnetic emissions. This includes:
    - Selecting equipment that adheres to safety certifications (e.g., CE, UL) to mitigate risks of electrical fires or shock.
    - Conducting risk assessments to identify potential hazards associated with network installations, ensuring appropriate measures are taken to protect users and maintenance personnel.

5. Technical Constraints

- Compatibility with existing infrastructure is another key constraint. The new network design should seamlessly integrate with current systems to avoid disruptions. This may involve:

    - Assessing existing hardware and software capabilities to ensure that new components can operate effectively within the current environment.
    - Planning for phased implementations to allow for gradual upgrades without significant downtime.

3.3 Analysis and Feature Finalization Subject to Constraints

In light of the identified design constraints, a thorough analysis of the proposed features is necessary to ensure the final network design is both feasible and effective. The following modifications, removals, and additions to features have been determined:

1. Removed Features

- **Overly Complex Security Protocols**: Features such as advanced multi-factor authentication systems or overly intricate encryption methods may be eliminated due to budget constraints. While security is a priority, simpler yet robust solutions (such as single-factor authentication combined with strong password policies) will provide adequate protection without straining resources.

2. Modified Features

- **Network Monitoring Tools**: The initial plan for sophisticated network monitoring solutions will be simplified. Instead of implementing an extensive suite of tools that may overwhelm users and incur high costs, the focus will shift to essential functionalities. This may include:

    - Basic real-time monitoring capabilities that alert administrators to significant issues (e.g., device failures or traffic spikes) without unnecessary complexity.
    - Implementing a centralized dashboard that provides key metrics, ensuring that network administrators can efficiently manage and troubleshoot the network without being burdened by excessive data.

3. Added Features

- **User Training and Support**: Recognizing the importance of user adoption and effective system utilization, additional training programs and support features will be introduced. These may include:

    - Comprehensive training sessions for staff and students to familiarize them with the new network systems and tools, helping to ensure a smooth transition.

- Creating user-friendly documentation and online resources that provide step-by-step guides, FAQs, and troubleshooting tips, enabling users to resolve minor issues independently.
- Establishing a dedicated support channel (e.g., helpdesk or online forum) to facilitate communication between users and IT staff, allowing for timely assistance and feedback.

3.4 Design Selection

After a thorough analysis of the two proposed network designs, the **Hierarchical Network Design** is selected as the optimal solution for the university's network infrastructure. This decision is based on a comprehensive comparison of key factors that directly impact the performance, scalability, and security of the network.

Comparison:

Scalability

The **Hierarchical Network Design** supports future expansion seamlessly. Its layered architecture allows for easy addition of new devices and users without necessitating a complete redesign. In contrast, the **Flat Network Design** may struggle to accommodate additional devices due to its lack of structure, potentially leading to significant performance degradation and increased complexity as the network grows.

Performance

The **Hierarchical Design** excels in managing network traffic effectively through the use of VLANs (Virtual Local Area Networks). By segmenting the network into distinct layers and departments, it prevents congestion and minimizes the chances of bottlenecks. This design ensures that critical applications and services maintain high availability and performance. On the other hand, the **Flat Design** can lead to excessive broadcast traffic and collisions, significantly hindering overall network efficiency.

Security

A key advantage of the **Hierarchical Network Design** is its multi-layered approach to security. Each layer can implement specific security policies tailored to the needs of different departments or user groups, facilitating better access control and monitoring. This granularity makes it easier to detect and respond to potential threats. Conversely, the **Flat Design** lacks this level of segmentation, making it more challenging to enforce security measures and manage access rights effectively.

Management and Maintenance

The hierarchical structure not only supports scalability and performance but also simplifies network management and maintenance. Network administrators can easily pinpoint issues at specific layers or VLANs,

making troubleshooting more efficient. The flat design, however, may complicate management due to its lack of defined structure, making it harder to isolate problems or manage configurations across a large number of devices.

Cost Considerations

While the initial implementation cost of a hierarchical design may be higher due to its complexity, the long-term benefits of reduced operational costs, improved performance, and easier management justify the investment. The flat design might appear cost-effective initially, but the potential for increased maintenance, downtime, and performance issues could lead to higher costs over time.

3.5 Implementation Plan/Methodology

The implementation plan for the proposed network infrastructure follows a structured methodology designed to ensure that all aspects of the project are effectively addressed. Each phase of the implementation process is critical to the overall success of the project.

1. Preparation Phase

- **Current Infrastructure Assessment**: This initial step involves evaluating the existing network infrastructure to identify limitations, performance issues, and areas for improvement. Engaging with stakeholders, including faculty and administrative staff, will help in gathering detailed requirements for the new system.
- **Requirement Gathering**: A comprehensive survey will be conducted to collect feedback from users about their specific needs and pain points. This feedback will inform the design of the new network, ensuring it aligns with the expectations of all users.
- **Project Scope Definition**: Establishing the scope of the project is crucial to managing expectations and resources. This includes outlining the goals, timelines, and deliverables associated with the project.

2. Design Phase

- **Network Topology Finalization**: Based on the gathered requirements, the network topology will be finalized, incorporating the chosen hierarchical design. This includes identifying the appropriate networking devices, such as routers, switches, and firewalls, necessary for the infrastructure.
- **Equipment Specification**: A detailed list of required hardware and software will be compiled, along with recommendations for vendors. This specification will include considerations for scalability, compatibility, and budget constraints.
- **IP Addressing and Security Configurations**: Developing an IP addressing scheme that accommodates current and future needs will be essential. Additionally, security configurations will be defined to protect sensitive data and ensure compliance with relevant regulations.

3. Deployment Phase

- **Hardware Installation**: The physical installation of networking devices will take place according to the predefined design. This includes setting up servers, routers, and switches in their designated locations.
- **Software Configuration**: Configuring the necessary software, including DHCP servers, security protocols, and network monitoring tools, will follow the hardware installation. This step ensures that all devices are properly set up to communicate with each other and adhere to security measures.

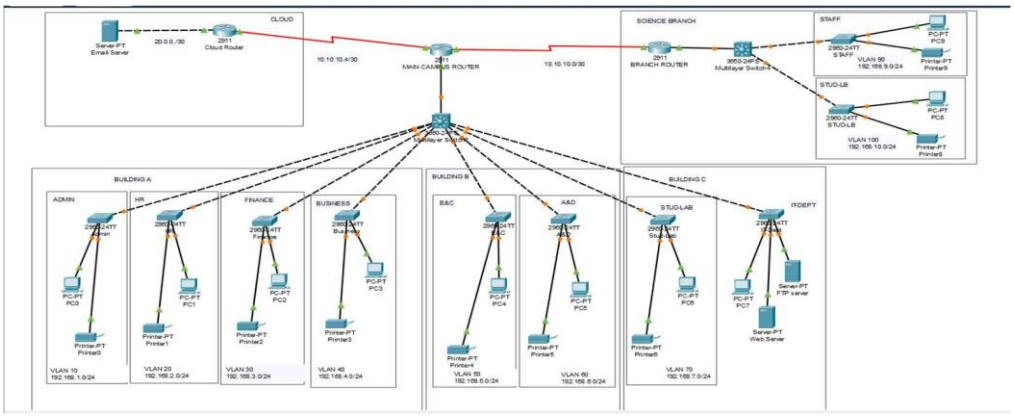
4. Testing Phase

- **Functional Testing**: A series of tests will be conducted to verify that all components of the network are functioning as intended. This includes testing connectivity between devices, ensuring proper VLAN configurations, and confirming DHCP operations.
- **Performance Testing**: The network will be subjected to stress tests to evaluate its performance under varying loads. This testing will help identify any potential bottlenecks and ensure that the network can handle the expected user demand.
- **Security Testing**: Implementing security measures will require thorough testing to identify vulnerabilities. This includes penetration testing and vulnerability assessments to ensure the network is secure against potential threats.

5. Documentation Phase

- **Comprehensive Documentation Creation**: Detailed documentation will be prepared to outline the network design, configurations, and operational procedures. This documentation serves as a reference for network administrators and provides guidelines for ongoing maintenance and troubleshooting.
- **User Training Materials**: In addition to technical documentation, user training materials will be developed to assist staff and students in understanding the new network features and functionalities. This will facilitate smoother transitions and improve user satisfaction.

OUTPUT:



CHAPTER 4.

RESULTS ANALYSIS AND VALIDATION

4.1 Implementation of Solution

The successful implementation of the proposed network infrastructure relies on the utilization of essential tools and technologies at various stages of the project. These tools facilitate effective analysis, design, project management, testing, and documentation.

1. Analysis

- **Network Performance Analysis**: Basic tools like Cisco Packet Tracer are used for simulating network behavior and analyzing performance metrics. This allows for the identification of potential bottlenecks and aids in making informed decisions regarding network design.
- **User Surveys**: Simple surveys conducted using Google Forms can gather feedback from users about their current network experience, identifying their needs and requirements for the new network design.

2. Design Drawings/Schematics

- **Network Design Software**: Cisco Packet Tracer is utilized to create detailed network topology diagrams and schematics. This tool enables the visualization of the proposed network, illustrating how different devices and VLANs will interact within the infrastructure.
- **Basic Diagram Tools**: Simple drawing tools can be employed to sketch physical layouts and network connections, ensuring clarity in equipment placement and cable management.

3. Report Preparation

- **Documentation**: Microsoft Word or Google Docs serve as platforms for preparing comprehensive project reports. These tools facilitate the integration of diagrams, tables, and charts to enhance the presentation of findings and designs.
- **Presentation Preparation**: Using Microsoft PowerPoint or Google Slides, presentations can be created to effectively communicate project results and designs to stakeholders and faculty members.

4. Project Management and Communication

- **Task Management**: Basic task management can be achieved using simple to-do lists or spreadsheets to keep track of project milestones, responsibilities, and deadlines. This ensures that all team members are aware of their tasks and progress.
- **Communication**: Simple communication tools like email or messaging platforms can be utilized for ongoing discussions and updates among project team members, ensuring effective coordination throughout the project.

5. Testing/Characterization/Interpretation/Data Validation

- **Network Testing**: Cisco Packet Tracer is used to conduct simulations that test the functionality of the network design. This includes testing connectivity, performance under load, and inter-VLAN routing to validate the proposed design.
- **Security Testing**: Basic security assessments can be performed using built-in features within Cisco Packet Tracer to ensure that the network design adheres to security best practices.
- **Data Validation**: Simple tools such as spreadsheets can be used to collect and analyze data from testing phases, enabling validation of test results and characterization of network performance.

CHAPTER 5.

CONCLUSION

5.1 Conclusion-:

The implementation of the proposed network infrastructure is expected to yield significant improvements in communication and resource sharing among students, faculty, and administrative staff. Key anticipated outcomes include enhanced network performance, improved security measures, and greater reliability across the university's campuses.

Expected Results/Outcomes

Improved Network Performance: The new design is expected to eliminate performance bottlenecks by effectively utilizing VLANs and advanced routing protocols. This should lead to faster data transfer rates and reduced latency for users.

Enhanced Security: The multi-layered security framework, including firewalls and intrusion detection systems, is anticipated to significantly reduce the risk of unauthorized access and data breaches, ensuring the safety of sensitive information.

Scalability: The network's design allows for future expansion without substantial redesign, accommodating the increasing number of devices and users while maintaining optimal performance.

User Satisfaction: Feedback from users is expected to reflect improved connectivity and access to resources, resulting in a more positive overall experience with the network.

Deviation from Expected Results

While the project aims for successful outcomes, deviations may occur due to unforeseen challenges. Potential areas of deviation could include:

Budget Constraints: If budget limitations restrict the acquisition of certain hardware or software, the final implementation may lack some of the originally planned features, leading to a compromise in performance or security.

Technical Limitations: The capabilities of basic tools like Cisco Packet Tracer might restrict the simulation of complex scenarios, potentially resulting in an incomplete understanding of how the network will perform under different conditions.

User Adaptation: Resistance to change among users or inadequate training could affect the overall effectiveness of the new system, leading to lower than expected user satisfaction and efficiency.

External Factors: Factors such as changes in regulatory compliance, economic conditions, or technological advancements could impact the implementation and success of the project.