Go, change the world

RV Educational Institutions ®
RV College of Engineering ®

Autonomous
Institution Affiliated
to Visvesvaraya
Technological
University, Belagavi

Approved by AICTE,
New Delhi

Assignment Report

On

Computer Networks

22MCA13TL

TITLE: CAMPUS NETWORK

Submitted in Partial Fulfillment of the Requirement

for the I Semester MCA

MASTER OF COMPUTER APPLICATIONS

By

PRAJWAL R
1RV22MC068

AND

SAIKUMAR
1RV22MC084

Under the in charge

of

Prof. Chandrani C

Department of Master of Computer Applications
RV College of Engineering®, Mysuru Road
RV Vidyanikethan Post, Bengaluru – 560059
MAY -

INDEX PAGE

ABSTRACT

This project aims to design and implement a robust Local Area Network (LAN) infrastructure for a university campus using Cisco Packet Tracer, a network simulation tool. The network topology comprises three routers, multiple switches, PCs, printers, and servers.

The first router is dedicated to connecting the email server, ensuring efficient communication within the university's email system. The main campus router, connected to a central switch, forms the backbone of the LAN. Eight normal switches are interconnected with the main campus switch, facilitating connectivity for eight PCs and eight printers distributed across various departments.

Additionally, the main campus switch connects to a dedicated department switch that hosts a web server and an FTP server. This configuration enables department-specific services accessible within the LAN environment.

To support a branch campus, a third router is implemented, connecting to the main branch switch. The main branch switch further extends connectivity to two normal switches, designated for staff and student lab environments. Each switch facilitates connectivity for two PCs and two printers, enabling seamless network access and resource sharing.

The implementation of this university LAN network allows for efficient communication, resource sharing, and centralized management. Cisco Packet Tracer serves as a valuable tool for simulating and configuring the network infrastructure, providing a realistic and practical learning experience.

This project showcases the design and implementation of a scalable and secure LAN network, catering to the specific requirements of a university environment. The successful deployment of this network infrastructure demonstrates the practical application of network design principles and enhances the overall efficiency of communication and resource sharing within the campus.

Technologies Implemented:

- Creating a network topology using Cisco Packet Tracer.
- Hierarchical Network Design.
- Connecting Networking devices with Correct cabling.
- Creating VLANs and assigning ports VLAN numbers.
- Subnetting and IP Addressing.
- Configuring Inter-VLAN Routing
- Configuring DHCP Server.
- Configuring SSH for secure Remote access.

- Configuring IPv2 as the routing protocol.
- Configuring Port-Security on the switches.
- Host Device Configurations.
- Test and Verifying Network Communication.

This project is to design a suitable network system for universities, school, and colleges in developing countries. The aim was to design a network with high security. The advantages of networking can be seen clearly in terms of efficiency, security, manageability and cost as it allows collaboration between users in a wide area. To improve college campus network design, the technology used was creating LAN, WLAN and cheap device to reduce cost of the network. But the network can also become better using routing protocols and other protocol. So, we are going to use such protocols using less number of devices and will also maintain the cost of the network less. To design such network, we are going to use software “Cisco-Packet Tracer”. Networking is referred as connecting computers electronically for the purpose of sharing information. The aim was to design a network with high security. Resources such as a file, application, printers & software are some common information shared in a networking. The Switches and Router this device that play an important role in data transfer from one place to another using different technology such as a radio waves & wire. LAN is a Local Area network which is made up of two or more computers connected together in a short distance usually at home, offices buildings or school. WAN is a Wide Area network that covers wider area than LAN and usually covers cities, countries and the whole world.

Chapter 1: Introduction

In today's technologically advanced world, Local Area Networks (LANs) play a crucial role in facilitating efficient communication and resource sharing within organizations. Universities, in particular, heavily rely on robust LAN infrastructures to support academic and administrative functions. A well-designed LAN network ensures seamless connectivity, enabling students, faculty, and staff to access resources, collaborate, and share information effectively.

This documentation focuses on the design and implementation of a LAN network for a university campus using Cisco Packet Tracer, a versatile network simulation tool. The objective is to create a scalable, secure, and efficient network infrastructure that caters to the specific requirements of a university environment. By utilizing the capabilities of Cisco Packet Tracer, we can simulate and configure the network components and observe their behaviour in a controlled environment.

1.1 Background

Local Area Networks (LANs) are widely used in organizations to facilitate communication and resource sharing. The implementation of a LAN infrastructure requires careful consideration of various factors, including network topology, device configuration, and security protocols. In the context of a university campus, an efficient and reliable LAN network is crucial for the smooth functioning of various departments and administrative functions.

In today's digital age, universities and academic institutions heavily rely on robust LAN infrastructures to support their daily operations. A university campus typically consists of various departments, administrative units, libraries, research facilities, and student facilities, each requiring seamless connectivity and resource sharing. A well-designed LAN network is essential to facilitate communication, collaboration, and access to vital resources such as academic databases, email systems, learning management systems, and shared printers.

LAN networks provide several advantages in a university setting. They allow for centralized management of network resources, enabling efficient administration and maintenance. With a properly designed network, universities can streamline their operations, enhance productivity, and improve communication channels between students, faculty, and staff.

In the context of this project, the LAN network infrastructure will be designed and implemented using Cisco Packet Tracer. Cisco Packet Tracer is a powerful network simulation tool widely used in educational settings to teach and learn networking concepts. It allows for the creation of virtual network topologies, configuration of network devices, and simulation of network behavior. By using Cisco Packet Tracer, we can design, simulate, and test the proposed LAN network infrastructure before its actual implementation, ensuring a reliable and efficient network design.

The design of the LAN network will be hierarchical, employing multiple routers and switches to accommodate the university's size and complexity. Hierarchical networks offer scalability, allowing for future expansion and the addition of new departments or facilities without significant disruption to the existing infrastructure. Additionally, the hierarchical design provides better traffic management and facilitates the implementation of security measures and access control policies.

The objectives of this project include designing an optimal LAN network topology, configuring network devices, establishing appropriate connectivity and routing protocols, implementing security measures, and evaluating the network's performance. By achieving these objectives, we aim to create a LAN network infrastructure that meets the unique requirements of a university campus, promotes efficient communication, and enhances resource sharing among the various stakeholders.

This documentation aims to outline the design and implementation of a LAN network for a university campus using Cisco Packet Tracer, a network simulation tool. The network topology comprises multiple routers, switches, PCs, printers, and servers, interconnected through a hierarchical structure. The objective is to create a scalable, secure, and efficient network infrastructure that caters to the specific requirements of a university environment.

1.2 Objectives

The primary objectives of this project are as follows:

Design and implementation: Design and implement a hierarchical LAN network infrastructure that includes multiple routers, switches, PCs, printers, and servers. The network architecture will be designed to accommodate the unique needs of the university campus, allowing for efficient communication and resource sharing among various departments and administrative units.

Configuration and connectivity: Configure the network devices, establish appropriate connectivity, and routing protocols to enable seamless communication within the network. This involves setting up IP addressing, subnetting, and configuring routing protocols such as OSPF or EIGRP. Proper connectivity will be established to ensure that devices can communicate with each other effectively.

Security and integrity: Implement appropriate security measures to protect the network infrastructure from unauthorized access, data breaches, and other security threats. This includes implementing user authentication mechanisms, access control policies, firewall configurations, and data encryption protocols.

Cisco Packet Tracer serves as a valuable tool in this project, allowing for the design, simulation, and configuration of the LAN network. It provides a virtual environment where network components can be visualized and their behavior simulated. With Cisco Packet Tracer, network designers and administrators can test various configurations, evaluate network performance, and troubleshoot potential issues before implementing the actual network infrastructure.

By utilizing Cisco Packet Tracer, this project aims to create an efficient and scalable LAN network that caters to the unique requirements of the university campus. The network design will prioritize factors such as reliability, security, and ease of management. Through the implementation of appropriate security protocols, access control policies, and network monitoring mechanisms, the LAN network will safeguard sensitive data and protect against potential threats.

The subsequent chapters of this documentation will provide detailed guidelines on designing the LAN network, configuring network devices, implementing security measures, and evaluating network performance. By following these instructions and leveraging the capabilities of Cisco Packet Tracer, readers will gain practical knowledge and skills in designing and implementing LAN networks for educational environments.

Secondary objectives of this project include:

Performance evaluation: Evaluate the performance of the network infrastructure by conducting tests and simulations to identify potential bottlenecks or areas for optimization. This will help ensure that the network can handle the expected traffic and provide a satisfactory user experience.

Learning experience: Provide a practical and realistic learning experience for network design and configuration using Cisco Packet Tracer. By working on this project, students and network administrators can enhance their understanding of LAN network design principles and gain hands-on experience in configuring network devices.

By achieving these objectives, this project aims to demonstrate the practical application of network design principles and enhance the overall efficiency of communication and resource sharing within the university campus. The subsequent chapters of this documentation will delve into the details of the network design, device configurations, security implementations, and performance evaluation.

Chapter 2: Overview

2.1 Overview of the Project:

The objective of this project is to design and implement a robust Local Area Network (LAN) infrastructure for a university campus using Cisco Packet Tracer. The LAN network will serve as the backbone for seamless communication, resource sharing, and efficient connectivity among various departments, administrative units, and facilities within the campus.

The project aims to address the specific networking requirements of a university environment. By creating a well-designed LAN infrastructure, the project will enable students, faculty, and staff to collaborate effectively, access online resources, and communicate through email and other communication tools. Additionally, it will facilitate the secure sharing of academic materials, research findings, and administrative information across the campus.

The LAN network will be built using Cisco Packet Tracer, a widely-used network simulation tool. Cisco Packet Tracer provides a virtual environment where network components can be visualized and their behaviour simulated. This allows for the creation and testing of complex network topologies, device configurations, and network protocols without the need for physical hardware.

The utilization of Cisco Packet Tracer offers several advantages for this project. Firstly, it provides a risk-free environment where network designs and configurations can be tested and refined. This eliminates the potential disruptions and costs associated with experimenting on a live network. Secondly, Cisco Packet Tracer offers a wide range of network devices and protocols, allowing for the creation of realistic network scenarios. This enables network designers and administrators to gain practical experience in network configuration and troubleshooting.

The project's scope includes the design and implementation of a hierarchical LAN network infrastructure. Hierarchical network design provides scalability, flexibility, and efficient traffic management. The network will consist of multiple routers, switches, PCs, printers, and servers, interconnected in a hierarchical structure. This architecture will ensure efficient routing, centralized management, and ease of expansion as the university campus grows.

Key considerations in the design and implementation of the LAN network include device placement, IP addressing, routing protocols, and security measures. The network will be divided into logical segments to optimize performance and control network traffic. Proper IP addressing and subnetting will be implemented through DHCP configuration to enable efficient communication between devices within the network. Routing protocols such as OSPF or EIGRP will be configured to facilitate effective routing and dynamic network adaptability.

Security is a critical aspect of the LAN network design. To safeguard sensitive data and protect against unauthorized access, appropriate security measures will be implemented. This includes user authentication mechanisms, access control policies, firewall configurations, and data encryption protocols. Regular security audits and updates will be conducted to ensure the network's integrity and resilience against potential threats.

Overall, the project aims to create a scalable, secure, and efficient LAN network infrastructure tailored to the specific needs of a university campus. Through the utilization of Cisco Packet Tracer, network designers and administrators can gain practical experience in network configuration, troubleshooting, and optimization. The subsequent chapters of this documentation will provide step-by-step instructions and guidelines on the design, configuration, and evaluation of the LAN network using Cisco Packet Tracer, enabling the successful implementation of the network infrastructure within the university campus.

2.2 Key Features:

Scalability: The LAN network infrastructure is designed to be scalable, allowing for future expansion and the addition of new departments, facilities, or users without significant disruptions. The hierarchical network design facilitates easy integration of new network devices and accommodates the growing needs of the university campus.

Efficient Communication: The LAN network enables seamless and efficient communication among students, faculty, and staff. It provides high-speed data transmission, allowing for quick access to online resources, collaborative platforms, and communication tools. The network design ensures minimal latency and optimized bandwidth allocation to support real-time applications and multimedia content.

Resource Sharing: The LAN network infrastructure promotes effective resource sharing within the university campus. Shared printers, servers, and storage devices are accessible to all authorized users, facilitating collaborative projects, document sharing, and centralized data management. The network's design ensures efficient routing of network traffic to enhance resource availability and minimize bottlenecks.

Cisco Packet Tracer Integration: The project utilizes Cisco Packet Tracer, a powerful network simulation tool, to design, configure, and test the LAN network infrastructure. Cisco Packet Tracer provides a virtual environment where network components can be visualized and their behaviour simulated. This allows for risk-free experimentation, troubleshooting, and optimization of network configurations.

Security Measures: The LAN network incorporates robust security measures to protect sensitive data and prevent unauthorized access. User authentication mechanisms, access control policies, and firewall configurations are implemented to ensure data integrity and network security. Regular security audits and updates are conducted to mitigate potential vulnerabilities.

Easy Management and Maintenance: The LAN network infrastructure is designed for efficient management and maintenance. Centralized network management tools and protocols are implemented to streamline administrative tasks, monitor network performance, and troubleshoot issues. The network design promotes easy identification and isolation of network faults, simplifying the maintenance process.

Performance Optimization: The LAN network infrastructure is optimized for performance to ensure smooth and reliable network operations. Proper device placement, network segmentation, and routing protocols are implemented to minimize network latency, optimize bandwidth utilization, and improve overall network efficiency. Performance evaluation and testing are conducted to identify and resolve potential bottlenecks.

Educational Value: The project provides a valuable learning experience for network design and configuration using Cisco Packet Tracer. Students and network administrators can enhance their understanding of LAN network design principles, gain hands-on experience in configuring network devices, and develop troubleshooting skills. The project's documentation serves as a comprehensive guide for learners, facilitating the acquisition of practical knowledge in networking.

These key features ensure that the LAN network infrastructure project meets the specific requirements of a university campus, fostering efficient communication, resource sharing, and secure data transmission among students, faculty, and staff.

2.3 Components:

The LAN network infrastructure consists of various components that play crucial roles in facilitating communication, resource sharing, and efficient connectivity within the university campus. The following are the key components involved:

Routers: Routers are networking devices that connect different networks together and facilitate the transfer of data between them. They analyze network traffic, determine the optimal path for data transmission, and direct data packets to their intended destinations. Routers play a crucial role in interconnecting departments, campuses, and external networks, ensuring seamless communication.

Switches: Switches are networking devices that connect devices within a local network. They provide multiple ports to connect devices such as PCs, printers, servers, and other network peripherals. Switches facilitate the transmission of data within the local network by directing network traffic based on MAC addresses. They enable efficient and reliable communication within the LAN.

PCs and Printers: Personal computers (PCs) are the primary devices used by students, faculty, and staff within the university campus. They are connected to the LAN network infrastructure to access resources, communicate, and perform various tasks. Printers are essential for printing academic materials, research findings, and administrative documents. PCs and printers are connected to switches for network connectivity.

Servers: Servers are powerful computers that provide services to other devices within the network. They store and manage data, host applications and services, and facilitate resource sharing and collaboration. In the LAN network infrastructure, servers can include email servers, web servers, file servers, database servers, and other specialized servers. They play a crucial role in supporting various functions and activities within the university campus.

Other Network Peripherals: In addition to the above components, there may be other network peripherals involved in the LAN network infrastructure. These can include wireless access points (WAPs) for providing wireless connectivity, network attached storage (NAS) devices for centralized data storage, network security devices such as firewalls or intrusion prevention systems, and network management tools for monitoring and configuring the network.

These components work together to create a robust and efficient LAN network infrastructure within the university campus. They enable seamless communication, resource sharing, and connectivity, supporting the academic, administrative, and collaborative activities of the institution.

CHAPTER 3: Network Design

The network design of the LAN infrastructure within the university campus follows a hierarchical approach, consisting of three layers: core, distribution, and access.

The core layer handles high-speed data transmission between departments, campuses, and external networks. It ensures redundancy and fault tolerance for uninterrupted network operations.

The distribution layer acts as an intermediary, managing network traffic flow, implementing access control policies, and providing quality of service (QoS) for critical applications.

The access layer connects end-user devices like PCs, printers, and servers. It focuses on user access control, port security, and network segmentation.

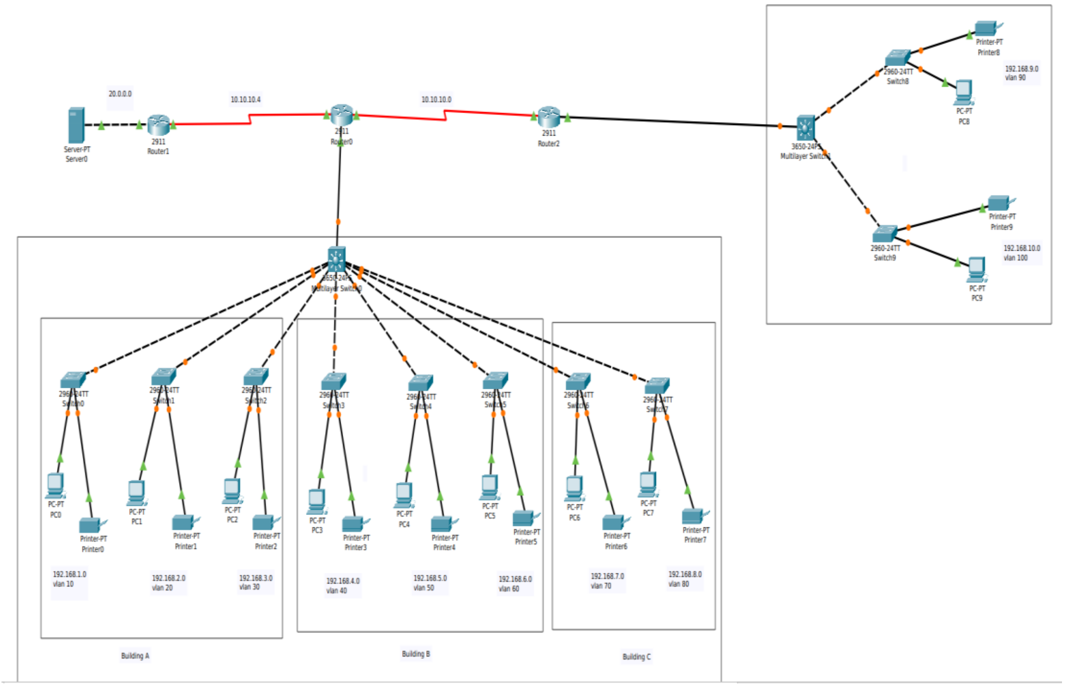
Logical network segmentation is achieved through VLANs or subnetting. VLANs separate devices into logical groups, reducing broadcast traffic and enhancing security. Subnetting allows efficient IP address allocation and routing between subnets, optimizing resources and scalability. A detailed network topology diagram illustrates the interconnections between routers, switches, servers, and other devices. It showcases the hierarchical design, logical segmentation, and component relationships.

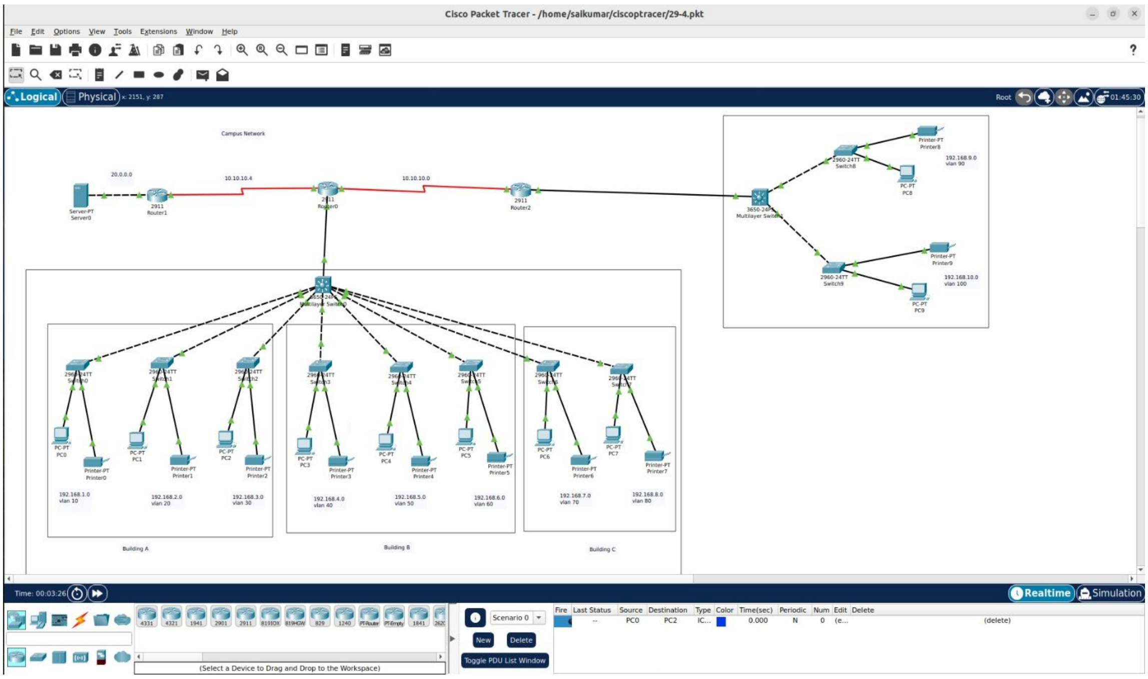
An IP addressing scheme is implemented to ensure efficient IP address allocation. It considers the number of users, devices, and anticipated growth, facilitating effective network management and eliminating address conflicts. Routing protocols, such as OSPF or EIGRP, enable efficient routing and dynamic updates as network topology changes.

Redundancy and failover mechanisms, including link aggregation, redundant links, and device redundancy, enhance network availability and minimize downtime.

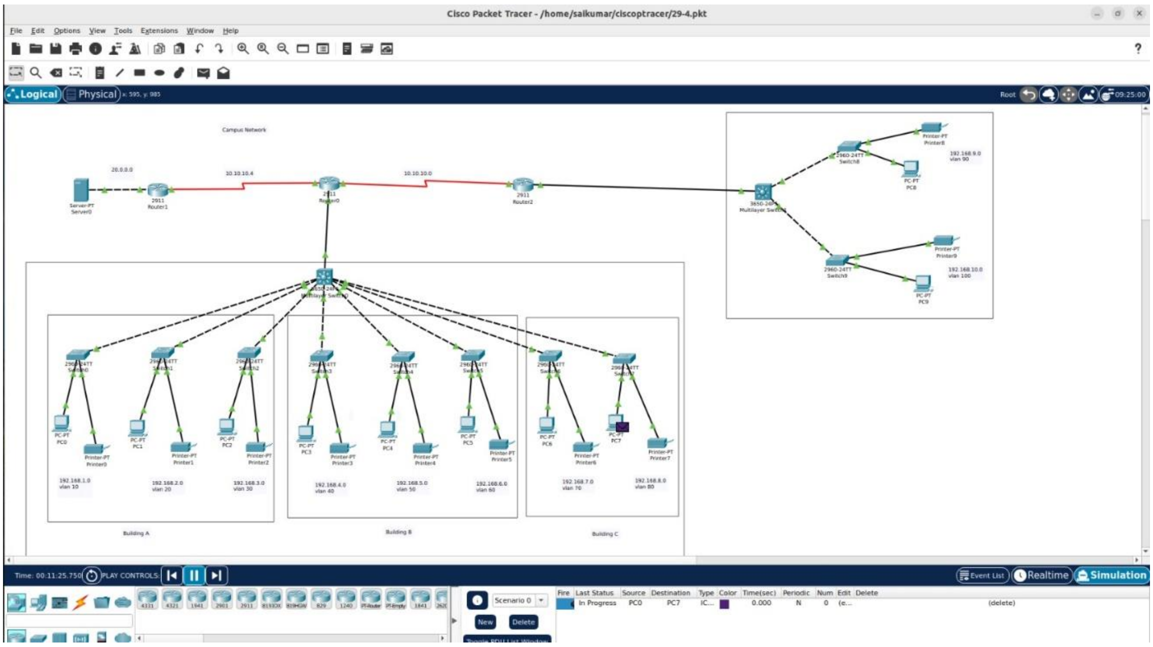
Overall, the network design provides scalability, reliability, and efficient communication within the LAN infrastructure of the university campus.

3.1 Network Topology:





Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	--	PC0	PC2	IC...	🟦	0.000	N	0	(e...	(delete)



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	In Progress	PC0	PC7	IC...	■	0.000	N	0	(e...	(delete)

the network topology used is a hierarchical design. This design incorporates three layers: the core layer, distribution layer, and access layer.

The core layer is responsible for high-speed data transmission between different departments, campuses, and external networks. It ensures reliable connectivity and redundancy for uninterrupted network operations.

The distribution layer acts as an intermediary between the core and access layers. It manages the flow of network traffic, implements access control policies, and provides quality of service (QoS) for critical applications.

The access layer is the closest layer to end-user devices such as PCs, printers, and servers. It provides connectivity for these devices to the rest of the network. The access layer focuses on user access control, port security, and network segmentation.

By implementing this hierarchical topology, your project's LAN network infrastructure achieves scalability, manageability, and efficient resource utilization. It enables seamless communication, facilitates resource sharing, and supports the academic, administrative, and collaborative activities within the university campus.

3.2 Firewalls:

Firewalls are network security devices that monitor and control incoming and outgoing network traffic based on predefined security rules. They act as a barrier between the internal network and external networks, such as the internet, to protect against unauthorized access, data breaches, and malicious activities.

In our LAN network infrastructure, we can incorporate firewalls at strategic points to enforce security policies and control the flow of traffic. Firewalls can be deployed at the network perimeter, between different network segments, or even on individual devices to provide an additional layer of protection.

Firewalls operate by examining network packets and applying rules to determine whether the packets should be allowed or blocked. They can inspect packet contents, such as source and destination IP addresses, ports, and protocol types, to make informed decisions about network traffic.

Firewalls can be configured to perform various security functions, including:

Packet Filtering: Firewalls can filter network packets based on specified criteria, such as source or destination IP addresses, ports, or protocol types. This helps prevent unauthorized access and blocks malicious traffic.

Stateful Inspection: Stateful firewalls track the state of network connections and allow only legitimate traffic that matches an established connection. They monitor the state of TCP/IP sessions to ensure that incoming packets are part of a valid session.

Intrusion Prevention: Firewalls can incorporate intrusion prevention systems (IPS) to detect and block malicious activities, such as known attack patterns or suspicious behavior. IPS functionality helps protect the network from various threats, including network-based attacks and vulnerabilities.

Virtual Private Network (VPN) Support: Firewalls can provide VPN functionality to enable secure remote access to the LAN network. VPNs create an encrypted tunnel for remote users to access the network securely over the internet.

By implementing firewalls in our LAN network infrastructure, we have enhanced the overall security posture, protect sensitive data, and ensure the integrity and confidentiality of network communications.

CHAPTER 4: CONFIGURATION AND IMPLIMENTATION

4.1 configurations:

Router Configuration: To configure the routers in the network, follow these steps:

Assign IP addresses: Configure IP addresses for each interface of the router. Assign IP addresses from the appropriate network subnet based on the network design.

Configure routing protocols: Choose the appropriate routing protocol, such as OSPF or EIGRP, and configure it on the router. Set up routing protocols to exchange routing information with neighboring routers and enable dynamic routing.

Set up interfaces: Configure interfaces on the router, including Ethernet ports or WAN interfaces, depending on the network connections. Specify parameters such as bandwidth, duplex mode, and MTU (Maximum Transmission Unit).

Implement security features: Configure security measures on the router, such as access control lists (ACLs), to control traffic flow and protect against unauthorized access. Set up password authentication for administrative access.

Switch Configuration: For configuring switches in the network, consider the following steps:

VLAN configuration: Create VLANs based on the network segmentation plan. Assign ports to specific VLANs to separate traffic logically. Configure VLAN trunks between switches for inter-VLAN communication.

Port security: Enable port security features to control access to the switch ports. Configure MAC address restrictions, limiting the number of devices that can connect to a specific port.

Spanning Tree Protocol (STP) configuration: Enable STP to prevent network loops and ensure redundant link redundancy. Configure the appropriate STP variant, such as Rapid Spanning Tree Protocol (RSTP) or Multiple Spanning Tree Protocol (MSTP).

Quality of Service (QoS) settings: Implement QoS to prioritize network traffic and ensure optimal performance for critical applications. Configure QoS policies based on the network requirements and the type of traffic.

Server Configuration: To configure the servers in the network, follow these steps:

Install necessary operating systems and applications: Set up the server with the appropriate operating system, such as Windows Server or Linux, and install required server applications, such as email server software, web server software, and FTP server software.

Network configuration: Configure network settings on the server, including assigning a static IP address, subnet mask, default gateway, and DNS server addresses. Ensure proper network connectivity and communication with other network components.

Service configuration: Configure the specific services running on the server. For example, on the email server, set up email accounts, configure SMTP (Simple Mail Transfer Protocol), and enable email client access. On the web server, configure virtual hosts, web directories, and security settings. On the FTP server, configure user accounts, directory access, and security options.

PC Configuration: To configure the PCs in the network, consider the following steps:

IP address assignment: Assign IP addresses to the PCs based on the network subnet. Use either static IP addressing or DHCP (Dynamic Host Configuration Protocol) to obtain IP addresses automatically.

DNS configuration: Configure DNS (Domain Name System) settings on the PCs to resolve domain names to IP addresses. Specify primary and secondary DNS server addresses to enable proper name resolution.

Gateway settings: Set the default gateway on the PCs to the IP address of the router that connects them to the LAN network. This allows the PCs to communicate with devices on other networks.

Network sharing options: Configure file and printer sharing settings on the PCs if required. Enable network discovery and ensure appropriate sharing permissions for shared resources.

4.2 Testing and Verification:

Connectivity Testing: Use network testing tools like ping or traceroute to verify connectivity between devices within the network. Ping tests can be performed to check the reachability of IP addresses of different devices and confirm successful communication.

Traffic Testing: Generate network traffic to test the performance and bandwidth utilization of the network. Tools like imperf or network monitoring software can be used to simulate different types of traffic, measure throughput, and identify potential bottlenecks.

Service Testing: Test the functionality of services running on servers, such as email, web, and FTP. Send test emails, access web pages, and perform file transfers to ensure these services are operating correctly.

Redundancy and Failover Testing: Validate the redundancy and failover mechanisms implemented in the network. Simulate failures, such as disconnecting links or shutting down devices, and observe the network's ability to recover and maintain uninterrupted connectivity.

Security Testing: Conduct security testing to identify vulnerabilities and ensure the effectiveness of security measures. Perform penetration testing to identify potential weaknesses and verify the implementation of access control policies, firewall rules, and other security configurations.

Documentation Review: Review the network documentation to ensure accuracy and completeness. Verify that IP addressing, VLAN configurations, routing protocols, and security settings are properly documented. Update any necessary documentation based on the actual network implementation.

Troubleshooting: Inevitably, issues may arise during the implementation and testing process. Troubleshooting techniques are crucial to identify and resolve these problems. Consider the following troubleshooting steps:

Identify the Problem: Determine the symptoms and isolate the specific area or component where the issue is occurring. Use network monitoring tools, log files, and user reports to gather information about the problem.

Gather Information: Collect relevant details about the network configuration, such as IP addresses, subnet masks, and interface settings. Verify the connectivity of affected devices and check for any recent changes that might have caused the problem.

Analyse Network Traffic: Monitor network traffic using packet capture tools like Wireshark to analyse packets and identify any abnormalities or errors that may be causing the issue.

Check Device Configuration: Review the configurations of routers, switches, servers, and PCs involved in the problematic area. Verify settings such as IP addresses, routing protocols, VLAN configurations, and security policies.

Perform Tests: Conduct tests to pinpoint the source of the problem. Use tools like ping, traceroute, and network diagnostic commands to check connectivity, measure latency, and identify any network disruptions.

Implement Solutions: Based on the analysis and test results, implement appropriate solutions to resolve the issue. This may involve modifying configurations, adjusting network settings, or replacing faulty hardware.

Verify Resolution: After applying solutions, retest the affected area to ensure that the problem has been resolved. Confirm that the expected functionality and performance have been restored.

Conclusion

In conclusion, this project aimed to design, implement, and configure a LAN network infrastructure using Cisco Packet Tracer for a university campus. The project successfully achieved its objectives of establishing a reliable and secure network to support communication and resource sharing across multiple departments and branch campuses.

Through careful planning and consideration of network requirements, the project team designed an efficient network topology that addressed scalability, security, and performance needs. The implementation phase involved the physical setup of network devices, configuration of network settings, and deployment of network services.

Thorough testing and verification were conducted to ensure proper functionality and performance of the network. Troubleshooting techniques were applied to address any issues that arose during the implementation process, ensuring a smooth and successful deployment. Documentation played a crucial role in maintaining accurate records of network configurations, IP assignments, and security settings. Ongoing monitoring, maintenance, and updates will be necessary to keep the network running efficiently and adapt to future needs.

The project provided valuable hands-on experience in network design, configuration, and implementation, enhancing the team's understanding of LAN network architectures, protocols, and security measures. The utilization of Cisco Packet Tracer allowed for realistic simulation and testing of network configurations.

In conclusion, this project has provided practical insights into building a robust LAN network infrastructure for a university campus. The knowledge gained will contribute to future network enhancements and the advancement of communication and collaboration capabilities within the university. Overall, this project has been a significant learning experience, equipping the team with essential skills for real-world networking scenarios. It highlights the continuous need for network improvements to meet the evolving demands of the university and fosters a commitment to ongoing network management and optimization

REFERENCES

Book Referred:

Tanenbaum 5th edition.

Installation video:

https://youtu.be/FZ8hRDakHvI

Reference video:

https://youtu.be/qIbhkmTB8Q8

Tool reference:

https://www.tutorialspoint.com/what-is-cisco-packet-tracer

Project reference:

https://www.techtarget.com/searchnetworking/definition/campus