DESIGN & IMPLEMENTATION

SECURE LAN SYSTEM DESIGN FOR BUSINESS

ANISHA KAMILA	2141011002
ASHUTOSH DAS	2141004162
BISHNUPRIYA NAYAK	2141014140

Institute of Technical Education and Research

SIKSHA ‘O’ ANUSANDHAN DEEMED TO BE UNIVERSITY
Bhubaneswar, Odisha, India

Abstract

We live in age of modern science. Computer Network is the best innovation of Modern science. A local area network (LAN) is a computer network within a small geographical area such as a home, school, computer laboratory, office building or group of buildings. A LAN is composed of interconnected workstations and personal computers which are each capable of accessing and sharing data and devices, such as printers, scanners and data storage devices, anywhere on the LAN. LANs are characterized by higher communication and data transfer rates and the lack of any need for leased communication lines. A high-quality and correctly dimensioned network infrastructure is essential for all well-functional IT system. A Local Area Network based network can ensure high speed as well as high quality network.

In today's digital age, small businesses face increasing threats to their network security. This project focuses on designing and implementing a secure Local Area Network (LAN) tailored for small business environments. The primary objective is to ensure the confidentiality, integrity, and availability of data while maintaining cost-effectiveness and scalability.

The design phase involves a thorough analysis of network requirements, including the selection of appropriate hardware and software components. Key security measures such as firewalls, intrusion detection systems, and encryption protocols are integrated to protect against internal and external threats. The implementation phase covers the configuration of network devices, establishment of secure communication channels, and deployment of access controls to restrict unauthorized access.

The proposed LAN system is tested for vulnerabilities and performance, ensuring it meets the security and operational needs of small businesses. The results demonstrate a robust and secure network infrastructure capable of supporting business operations while safeguarding sensitive information.

Key words: Secure LAN, Operating Wavelength, Route Planning, Planning & Deployment, Network Design for small business.

Table of Contents

Introduction

1.1 Introduction

We live in age of modern science. Computer Network is the best innovation of Modern science. A local area network (LAN) is a computer network within a small geographical area such as a home, school, computer laboratory, office building or group of buildings. A LAN is composed of interconnected workstations and personal computers which are each capable of accessing and sharing data and devices, such as printers, scanners and data storage devices, anywhere on the LAN. LANs are characterized by higher communication and data transfer rates and the lack of any need for leased communication lines. A high-quality and correctly dimensioned network infrastructure is essential for all well-functional IT system. A Local Area Network based network can ensure high speed as well as high quality network.

In the modern business landscape, small businesses are increasingly reliant on digital infrastructure to manage their operations, communicate with clients, and store sensitive information. However, this reliance also exposes them to various cybersecurity threats, ranging from data breaches to malware attacks. Unlike larger enterprises, small businesses often lack the resources and expertise to implement comprehensive security measures, making them attractive targets for cybercriminals.

1.2 Project Overview

The objective of this project is to design and implement a secure Local Area Network (LAN) system specifically tailored for small businesses. The proposed system aims to provide a robust and scalable network infrastructure that ensures the confidentiality, integrity, and availability of business data. By integrating advanced security features such as firewalls, intrusion detection systems, and encryption protocols, the system seeks to protect against both internal and external threats.

This project will cover the entire lifecycle of the LAN system, from initial requirement analysis and design to implementation and testing. The ultimate goal is to empower small businesses to operate securely and efficiently in an increasingly digital world.The scope of the project for designing and implementing a secure Local Area Network (LAN) system for small businesses includes the following key areas.

- **Network Requirements Analysis:**

  Assess the specific needs of the small business, including the number of users, types of devices, and data flow requirements.

  Identify any existing network infrastructure and determine compatibility with new components.

- **Network Design:**

  Develop a detailed network topology that includes all necessary hardware (routers, switches, access points) and software components.

  Plan for network scalability to accommodate future growth.

Introduction

- **Security Measures:**
  Integrate security features such as firewalls, Virtual Private Networks (VPNs), intrusion detection/prevention systems (IDS/IPS), and encryption protocols.
  Implement secure authentication methods and access controls to protect sensitive data.

- **Implementation:**
  Install and configure network devices and software according to the designed topology.
  Establish secure communication channels and network segmentation to isolate sensitive areas.

- **Conduct Vulnerability Assessments:**
  Perform security audits and penetration testing to identify potential vulnerabilities.
  Implement necessary patches and updates to mitigate identified risks.

- **Cisco Network Assistant:**
  A tool for managing Cisco network devices, including configuration and troubleshooting.
  Simplifies the management of small to medium-sized networks.

- **Testing and Validation:**
  Conduct thorough testing to ensure the network operates as intended and meets performance standards.
  Perform security audits and penetration testing to identify and mitigate vulnerabilities.

- **Training and Support:**
  Provide training for staff on network security best practices and the proper use of network resources.
  Establish a support plan for ongoing network maintenance and troubleshooting.

- **Monitoring and Maintenance:**
  Implement continuous monitoring tools to detect and respond to security incidents.
  Regularly update and patch network components to address emerging threats & vulnerabilities.

By covering these areas, the project aims to create a secure, reliable, and scalable network infrastructure that meets the operational needs of small businesses while protecting against cyber threats.

1.3. Project Management:-

According to the PMBOK Guide (Project Management Body of Knowledge), a project management life cycle consists of 5 distinct phases including initiation, planning, execution,review, and closure that combine to turn a project idea into a working product. The project initiation phase is the first stage of turning an abstract idea into a meaningful goal.In this stage, we need to develop a business case and define the project on a broad level. The project planning stage requires complete diligence as it lays out the project's roadmap.

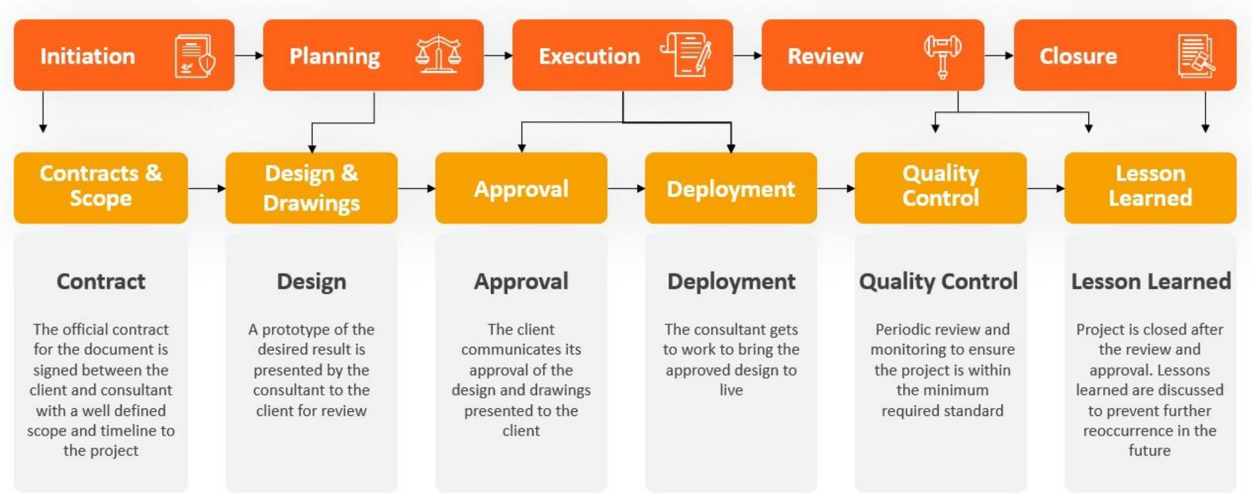

Initiation
Planning
Execution
Review
Closure
Contracts & Scope
Design & Drawings
Approval
Deployment
Quality Control
Lesson Learned
Contract
The official contract for the document is signed between the client and consultant with a well defined scope and timeline to the project
Design
A prototype of the desired result is presented by the consultant to the client for review
Approval
The client communicates its approval of the design and drawings presented to the client
Deployment
The consultant gets to work to bring the approved design to live
Quality Control
Periodic review and monitoring to ensure the project is within the minimum required standard
Lesson Learned
Project is closed after the review and approval. Lessons learned are discussed to prevent further reoccurrence in the future

Fig.1. Model of phases in project management.

The project execution stage is where the project team does the actual work. The job of a project manager is to establish efficient workflows and carefully monitor the progress of the team.In the project management process, the third and fourth phases are not sequential in nature. The project monitoring and controlling phase run simultaneously with project execution.

1.4. Organization of the Report:-

The report is organized into the following chapters. Each chapter is unique on its own and is described with the necessary theory to comprehend it.

Chapter 2 deals with Background Study, Chapter 3 has the literature Survey and review, techniques and Architecture description of the theoretical aspects,Chapter 4 has the Proposed solution and lastly Chapter 5 Result and Analysis , that have been acquired to commence the project work.

1.5. Background Study

To Understand the background theory and Modeling of Secure Local Area Network System(LAN) for small business, let’s explore the key concepts involved:

1.5.1. Secure Local Area Network(LAN) System:-

A Local Area Network (LAN) is a network that connects computers and other devices within a limited area, such as a home, office, school, or laboratory.

✧ **Types:**

Client/Server LAN: Devices (clients) are connected to a central server that manages resources and network traffic.

Peer-to-Peer LAN: Devices communicate directly with each other without a central server.

✧ **Benefits:**

Improved resource sharing and communication.Centralized management and security.Cost-effective for small to medium-sized environments.

✧ **Technologies:**

Common technologies used in LANs include Ethernet and Wi-Fi1.Virtual LANs (VLANs) allow network administrators to logically segment networks without changing the physical layout.

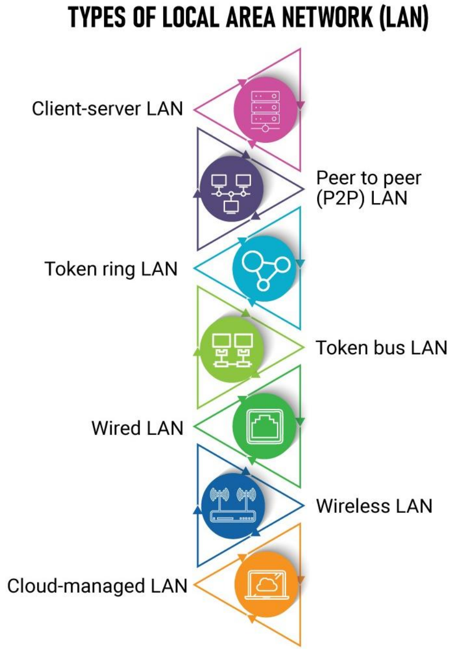


Fig2. Types of LAN

1.5.2. Different Type Of Cyber Attacks :-

- **Phishing:** Deceptive emails or messages designed to trick individuals into revealing sensitive information.
- **Ransomware**: Malicious software that encrypts data and demands payment for the decryption data.
- **Password Cracking:** Techniques used to guess or crack passwords to gain unauthorized access.Brute-force Attack: Trying all possible combinations to crack passwords or encryption keys.
- **MITM(Man-in-the-Middle)Attacks:** Intercepting and altering communication between two parties.
- **SQL Injection Attack:** Exploiting vulnerabilities in web applications to execute malicious SQL code.
- **XSS(Cross-Site-Scripting) Attacks:** Injecting malicious scripts into web pages viewed by other users.
- **Malware Attack:** General term for malicious software designed to harm or exploit systems

1.6.Motivation(s)

The motivation behind designing a Local Area Network (LAN) system for small businesses includes several key factors:Enhanced Communication and Collaboration,Resource Sharing:(LANs allow multiple users to share resources such as printers, scanners, and internet connections, reducing costs and improving efficiency).Data Security,Cost-Effectiveness,Improved Network Performance,Compliance with Standards,Business Continuity,Centralized Management,Support for Modern Technologies(A modern LAN supports, IoT, and cloud computing, enabling businesses to leverage these innovations for improved operations) etc.

1.7. Uniqueness of the Work

- The uniqueness of designing and implementing a secure Local Area Network (LAN) system for small businesses lies in several key aspects. The design is specifically tailored to meet the unique needs and constraints of small businesses, which often differ significantly from larger enterprises.

- By focusing on cost-effective security, the project integrates advanced security measures within a limited budget, making high-level security accessible to small businesses. The LAN system is designed to be scalable, allowing for easy expansion as the business grows, ensuring long-term usability and adaptability.

- The secure LAN system design incorporates cutting-edge technologies like virtualization, cloud integration, and IoT support to ensure future-proofing. It features multi-layered defense mechanisms, real-time monitoring, and proactive threat management to cyber threats.

Literature Review

2.1 Existing System

- ✧ **Mokhaled N. A. Al-Hamadani [1]**

Title: Designing a Secure Campus Network and Simulating it Using Cisco Packet Tracer

Existing System: This paper discusses the design and simulation of a secure campus network (SCN) using Cisco Packet Tracer. The existing system includes multiple networks and VLANs to ensure secure data transfer among high-security end-users. The system employs various protocols and security configurations to protect the network from unauthorized access and cyber threats.

- ✧ **B. Midhun Krishna Yadav, Akhilendranath Mummadi, Vishnu Vardhan Ciripuram, and Dr. R Uma Mageswari [2]**

Title: Secure Campus Area Network in Cisco Packet Tracer

Existing System: This research focuses on designing a secure campus area network (CAN) using Cisco Packet Tracer. The existing system is designed to enhance security and limit threats by using VLANs, Access Control Lists (ACLs), and IoT monitoring systems. The architecture includes various departments within a college, each housed in different buildings, and is secured through the use of VLANs and ACLs.

- ✧ **Tarkaa, Nathaniel S., Paul I. Iannah, and Isaac T. Iber [3]**

Title: Design and Simulation of Local Area Network Using Cisco Packet Tracer

Existing System: This paper focuses on the design and simulation of a local area network (LAN) for a small to medium-sized enterprise using Cisco Packet Tracer. The existing system includes a detailed network layout with switches, routers, and access points to ensure seamless connectivity and data transfer. The design also incorporates security measures such as firewalls and ACLs to protect the network from potential threats.

- ✧ **David B. Green and Mohammad S. Obaidat [4]**

Title: An Accurate Line of Sight Propagation Performance Model for Ad-Hoc 802.11 Wireless LAN (WLAN) Devices

Existing System:.The existing system involves a detailed propagation model that accurately predicts the performance of wireless LAN devices. This model is particularly useful for designing and optimizing wireless networks in environments where line-of-sight conditions are prevalent.

Literature Review

2.2 Problem Identification

- **Tamirat Atsemegiorgis: [1]**

Complexity in Implementation: The proposed security measures might be too complex for small businesses to implement without specialized knowledge or resources1.

Scalability Issues: As the network grows, the initial design may not efficiently handle increased traffic and user authentication, requiring significant redesign.

- **B. Midhun Krishna Yadav, Akhilendranath Mummadi, Vishnu Vardhan Ciripuram, and Dr. R Uma Mageswari: [2]**

Simulation Limitations: The use of Cisco Packet Tracer for simulation may not fully capture real-world network behavior and performance.

Generalization: The design might be too generalized, lacking specific adaptations for unique campus environments or varying security needs.

- **Tarkaa, Nathaniel S., Paul I. Iannah, and Isaac T. Iber: [3]**

Simulation Limitations: Cisco Packet Tracer may not fully capture the complexities of real-world network environments, leading to potential discrepancies between simulated and actual performance.

Cost Inefficiency: The design may rely heavily on routers instead of switches, increasing costs and potential security risks due to misconfigurations.

- **David B. Green and Mohammad S. Obaidat: [4]**

Focus on Line-of-Sight: Their model primarily addresses line-of-sight propagation, which may not be applicable in many real-world scenarios where obstacles are present.

Technical Complexity: The proposed model might be too technically complex for practical implementation without advanced expertise.

- **Authors of "Campus Network Architecture Using Cisco Packet Tracer": [5]**

Troubleshooting Limitations: Simulated troubleshooting might not fully replicate real-world scenarios, potentially leading to gaps in practical problem-solving skills.

Proposed Solution

3.1. Solution And Recommendation

To design a secure LAN system for a business using Cisco Packet Tracer, implement VLANs for network segmentation, configure robust access controls, and deploy continuous monitoring tools like IDS/IPS for real-time threat detection1. Regularly update and patch all network devices and software to protect against vulnerabilities1. Additionally, provide comprehensive training programs for employees to foster a culture of security awareness and readiness.

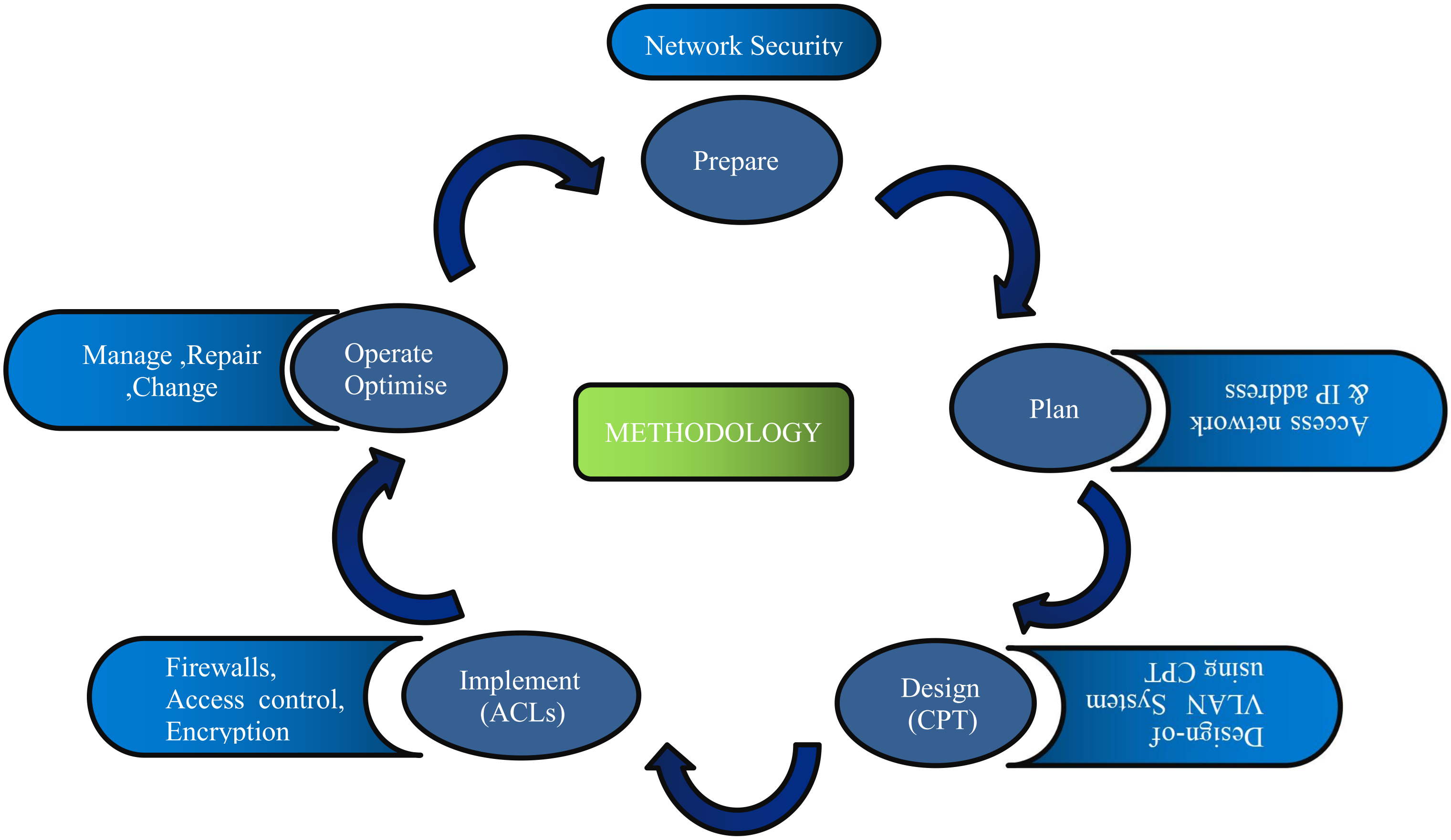


Fig2. PPDIO Methodology Used in LAN System

3.2. Model Architecture and Methods

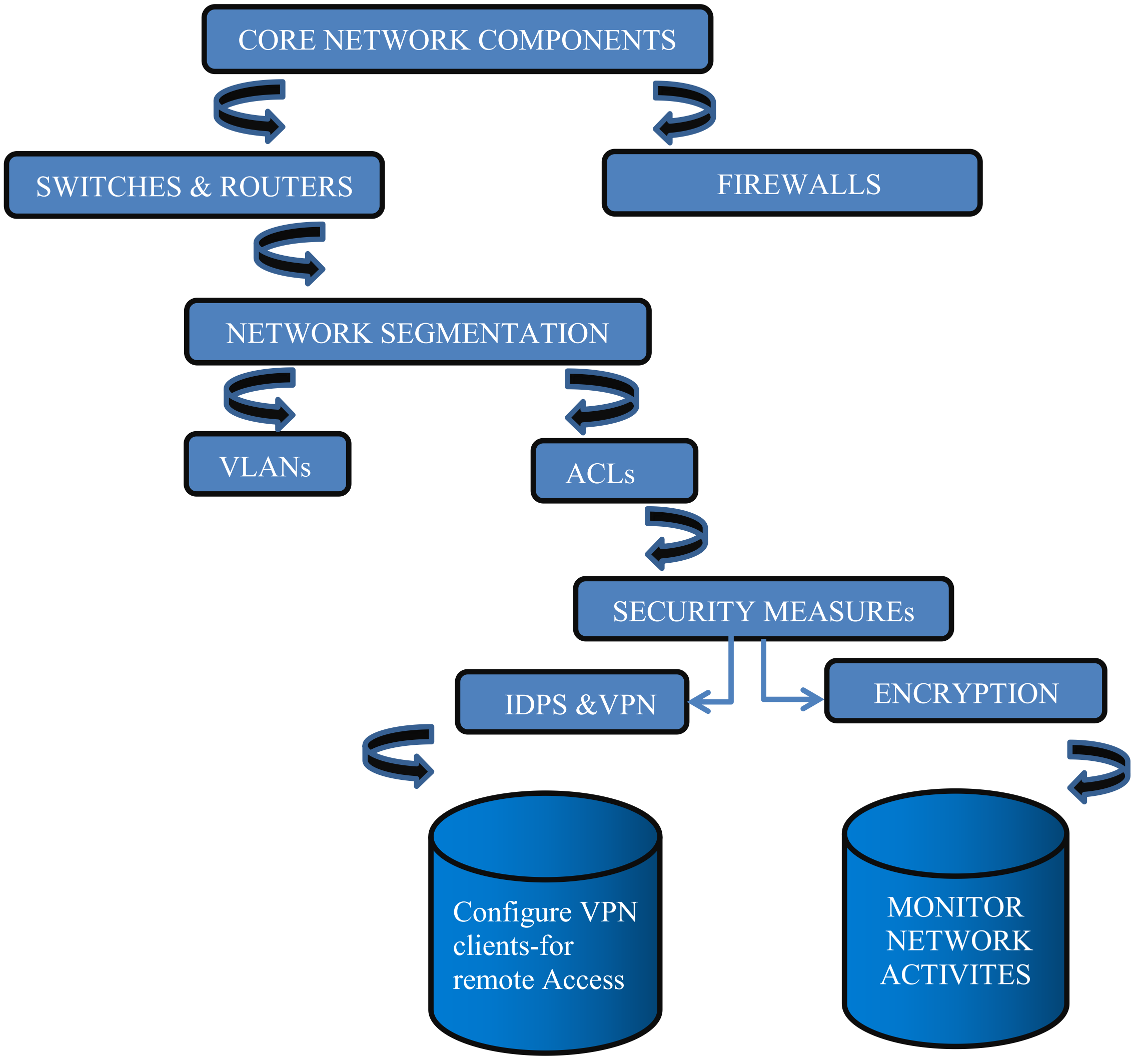
Designing a secure Local Area Network (LAN) system for small businesses involves creating a model architecture that ensures robust security, scalability, and efficient performance. Here's a detailed model architecture for such a system:

Proposed Solution

- **Network Segmentation:**
  Create VLANs: Segment the network into different VLANs based on departments, functions, or security levels. This isolates sensitive data and reduces the attack surface by limiting broadcast domains.

- **Access Control:**
  Implement ACLs: Apply Access Control Lists (ACLs) to each VLAN to restrict access based on user roles and responsibilities. This ensures that only authorized users can access specific network segments.

- **Monitoring and Management:**
  Deploy IDS/IPS: Use Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor VLAN traffic for suspicious activities and potential threats. This helps in real-time threat detection and response


CORE NETWORK COMPONENTS

SWITCHES & ROUTERS

FIREWALLS

NETWORK SEGMENTATION

VLANs

ACLs

SECURITY MEASUREs

IDPS &VPN

ENCRYPTION

Configure VPN clients-for remote Access

MONITOR NETWORK ACTIVITES

Implementation Plan

4.1 Datasets(s) Description

Designing a Local Area Network (LAN) system for a business involves several key steps and considerations. Here are some useful datasets and descriptions to guide you through the process:

- **Network Requirements Dataset:**

  Description: This dataset includes information on the specific needs of the business, such as the number of users, types of devices, data flow requirements, and existing network infrastructure.

  Example Data Points: Number of employees, types of applications used, bandwidth requirements, existing hardware and software.

- **Office Floor Plan Dataset:**

  Description: This dataset contains the physical layout of the office, including the locations of workstations, meeting rooms, and network equipment.

  Example Data Points: Floor dimensions, workstation locations, cabling routes, access point placements.

- **Network Performance Metrics Dataset:**

  Description: This datasets tracks the performance of the existing network, including metrics such as throughput, latency, and uptime.

  Example Data Points: Average bandwidth usage, peak traffic times, latency measurements, downtime incidents.

- **Security Requirements Dataset:**

  Description: This dataset outlines the security needs of the business, including compliance requirements, types of data handled, and potential threats.

  Example Data Points: Required encryption standards, access control policies, compliance regulations (e.g., GDPR, HIPAA).

- **Cost Analysis Dataset:**

  Description: This datasets includes the budget constraints and cost estimates for network components and implementation.

  Example Data Points: Hardware costs, software licensing fees, installation and maintenance expenses.

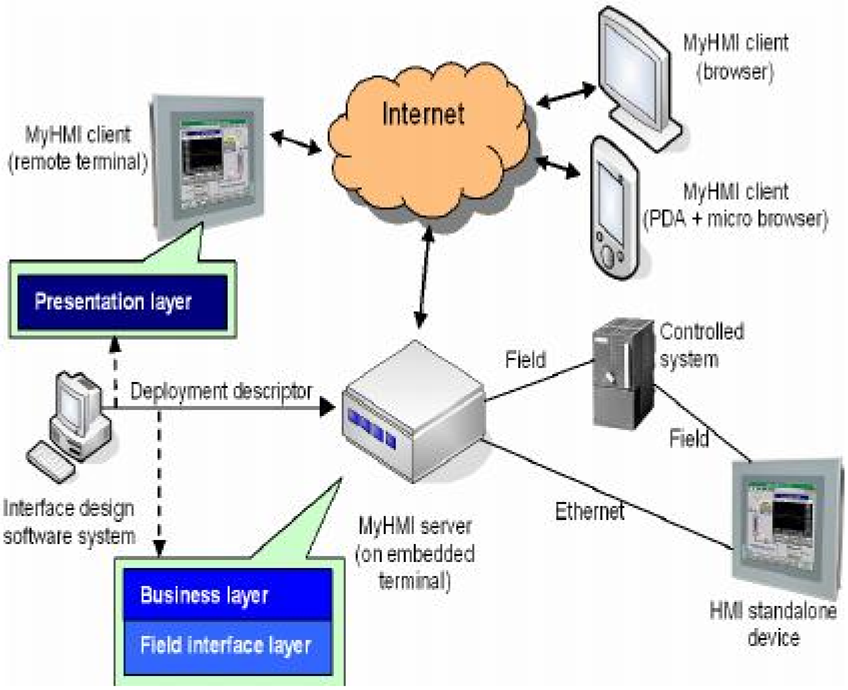


Fig.3 Model Architecture of LAN System

4.2 Tools/Technologies

Cisco Packet Tracer (CPT) is a powerful network simulation tool widely used in the design and implementation of Local Area Network (LAN) systems. Here are some key uses of CPT in LAN systems:

✧ **Network Design and Simulation:**

Topology Creation: CPT allows users to create detailed network topologies, including various devices like routers, switches, and end devices, to simulate real-world network environments.

Configuration Testing: Users can configure network devices and test different configurations to ensure optimal performance and security before actual deployment.

✧ **Troubleshooting and Analysis:**

Problem Simulation: CPT can simulate network issues, allowing users to practice troubleshooting and develop problem-solving skills.

Performance Analysis: Users can analyze network performance, identify bottlenecks, and optimize configurations to improve efficiency.

4.3. Evaluation Measures

When evaluating the security of a Local Area Network (LAN), consider the following measures:

- **Network Segmentation**: Divide your LAN into separate segments or VLANs to limit the impact of security breaches. This helps contain threats and prevents lateral movement within the network.

- **Access Control**: Implement strict access controls to restrict who can connect to the LAN. Use technologies like 802.1X for port-based authentication and Network Access Control (NAC) solutions.

- **Visibility**: Ensure you have visibility into network traffic. Use tools like Intrusion Detection Systems (IDS) and network monitoring to detect anomalies and potential security incidents.

- **Policy Enforcement**: Enforce security policies consistently across the LAN. This includes firewall rules, access control lists (ACLs), and other security policies.

- **Vulnerability Assessment**: Regularly scan the LAN for vulnerabilities. Identify weaknesses in devices, configurations, and software, and address them promptly.

- **Documentation and Reporting**: Maintain documentation of your LAN’s security posture. Create assessment reports that summarize findings, risks, and recommended actions.

5. SYSTEM DESIGN AND OUTPUTS

5.1 System Specification

Operating System:

Microsoft Windows 8.1, 10, 11 (64-bit)
Ubuntu 20.04 LTS (64-bit)
macOS 10.14 or newer

Hardware Requirements:

Processor: amd64 (x86-64) CPU
Memory: 4 GB of RAM
Storage: 1.4 GB of free disk space

5.2 Parameters Used (if any)

When configuring a secure LAN in Cisco Packet Tracer, we need to consider several parameters and features. Here are some key aspects:

- **VLANs (Virtual LANs)**:
  Create separate VLANs for each department to segment network traffic. Assign specific ports or interfaces to each VLAN.

✧ **IP Addressing & Security Measures**:

Decide on IP address ranges for each VLAN (floor). Use private IP addresses.
Implement subnetting to efficiently allocate IP addresses within each VLAN.
IPv4 Address Structure An IPv4 address is a 32-bit address.example 192.168.23.100.which bits refer to the network and which bits refer to the host is called subnet mask. An example of a subnet mask is 255.255.255.0.

5.3 Results With Subneting

Multiple VLANs are created. Network traffic is segmented, improving security and performance. IP addresses are assigned to each VLAN. Devices within each VLAN can communicate using their assigned IP addresses. ACLs, port security, and DHCP snooping are configured. Unauthorized access is restricted, and DHCP-related attacks are mitigated.

Sl.no	Network Address	Firstvalid Host	LastValidHost	Broadcast
1	172.168.0.2	172.168.0.1	172.168.0.254	172.168.0.255
2	172.168.1.0	172.168.1.1	172.168.1.254	172.168.1.255
3	172.168.2.0	172.168.2.1	172.168.2.254	172.168.2.255
4	172.168.3.0	172.168.3.1	172.168.3.254	172.168.3.255
5	172.168.4.0	172.168.4.1	172.168.4.254	172.168.4.255
6	172.168.5.0	172.168.5.1	172.168.5.254	172.168.5.255
7	172.168.6.0	172.168.6.1	172.168.6.254	172.168.6.255

Table.1. : Subnets obtained from the Subnetting Scheme

5.3 Result Analysis and Validation

✧ **VLAN Configuration:**

Check that each switch has the correct VLANs configured.
Verify that devices within the same VLAN can communicate with each other.

✓ **Trunk-to-Router**

To create a trunk port on the switch that will connect to the router, and all other access ports, we login to the switch and using the command Line interface (CLI), use the following commands.

```
 Switch(config)# int fastethernet 0/1
 Switch(config-if)#switchport mode trunk
 Switch(config-if)#spanning-tree portfast trunk
 Switch(config-if)#interface range fa0/2 – 24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#end
```

Implementation Plan

- ✓ **Assigning Switch Ports to VLANs**

The VLANs have been created and even though active, they don't have switch ports associated with them. This makes the switch still just a single broadcast domain. To assign switch ports to the VLANs, the following commands are used:

```
Switch(config)#interface [interface type] [interface identifier]
Switch(config-if)#switchport access vlan [vlan id]
Switch(config)#interface fastethernet0/2
Switch(config-if)#switchport access vlan 10
Switch(config-if)#interface fastethernet0/3
Switch(config-if)#switchport access vlan 10
```

- ✧ **IP Addressing:**

Use the show ip interface brief command on routers or Layer 3 switches to verify IP addresses.

Ping devices within the same VLAN to ensure connectivity.

- ✓ **Configuring Default-Gateway**

The switches in the departments need to have a gateway for packets that are destined outside the network (VLAN), and this can be configured using the command below:

```
Switch(config)#ip default-gateway [ip address]
EEESW(config)#ip default-gateway 172.168.0.1
FOR VLAN 20: Account Section
AGRICSW(config)#ip default-gateway 172.168.1.1
For VLAN 30: Exam Section
 CIVSW(config)#ip default-gateway 172.168.2.1
For VLAN 40: Academic Section
MECHSW(config)#ip default-gateway 172.168.3.1
```

- ✧ **Security Measures:**

Access Control Lists (ACLs): Define rules to control traffic between VLANs. Restrict access based on source/destination IP addresses or port numbers.

Port Security: Limit the number of MAC addresses allowed on a switch port to prevent unauthorized devices.

DHCP Snooping: Protect against rogue DHCP servers by allowing only trusted DHCP servers on the networks.

Where: "interface type" is either a gigabitethernet port or a fastethernet port and "interface identifier break" starts the creation of the sub-interfaces e.g. 0/1.1 to create the first sub-interface. The set of commands below configures the router sub-interfaces, enables DHCP relay, also it implements NAT and finally inter-VLAN routing.

```
 Admin_router#configure terminal
Admin_router(config)# interface gig0/1
Admin_router(config-if)#no ip address
Admin_router(config-if)#duplex auto
Admin_router(config-if)#speed auto
Admin_router(config-if)#interface gig0/1.1
Admin_router(config-subif)#description VLAN10_interface
Admin_router(config-subif)#encapsulation dot1q 10
Admin_router(config-subif)#ip address 172.168.0.1 255.255.255.0
Admin_router(config-subif)#ip nat inside
Admin_router(config-subif)#ip helper-address 172.168.4.3
 Admin_router(config-subif)#end
```

5.4. Analysis:-

Sl no	Parameter	Description	Accuracy Measure
1.	Router configuration	Setting up routers to manage traffic between subnets and external networks.	Success rate of routing configurations and connectivity between subnets..
2.	IP Addressing	Assigning unique IP addresses to devices within each subnet.	Percentage of IP addresses correctly assigned and utilized
3.	Access Control	Implementing ACLs to restrict access based on user roles and policies.	Percentage of unauthorized access attempts blocked.
4.	Network Performance	Ensuring efficient data flow and minimal latency across the network.	Average network latency and throughput.
5.	Security Measures	Deploying IDS/IPS to monitor and prevent suspicious activities.	Detection rate of potential threats and response time.
6.	Monitoring-and Management	Utilizing SIEM and network monitoring tools for real-time threat detection.	Number of security incidents detected and resolved.
7.	Policy Enforcement	Developing and enforcing security policies across the network.	Compliance rate with security policies and audit results.
8.	User-Training-and Awareness	Conducting training sessions to educate employees on security best practices.	Number of training sessions conducted and employee participation rate.

6. Conclusions

- In this paper, we have explored the possibility of using VLANs for network segmentation and management. The simulation of the same on Cisco Packet Tracer provides a ‘proof of concept’ for the proposed solution

- A Local Area Network (LAN) that uses both wired and wireless topology have been implemented with some important concepts like DHCP, DNS, Email, VLANs in a single network using Cisco.

- VLANs have been used to logically group clients on the network, and with the aid of a router and switch configurations, data packets routed from one device to another. It is also noteworthy that, the configuration and specifications are for the initial prototype and can further be developed and additional functionality as AI/ML can be added to increase support and coverage. The procedures provide a veritable approach for the design of LANs for end-to-end IP network connectivity for next generation network (NGN) architecture implementations

- Secure LAN System design suites typically implement the aforementioned design methods and algorithms.By following these methods, we can design a LAN that is robust, secure, and capable of meeting the evolving needs of a small business.

- A robust Network Infrastructure Design is essential for modern businesses. It ensures smooth operations, security, and scalability.

7. References

[1] Green, David B., and Mohammad S. Obaidat. "An accurate line of sight propagation performance model for ad-hoc 802.11 wireless LAN (WLAN) devices." 2002 IEEE International Conference on Communications. Conference Proceedings. ICC 2002 (Cat. No. 02CH37333). Vol. 5. IEEE, 2002.

[2] Tarkaa, Nathaniel S., Paul I. Iannah, and Isaac T. Iber. "Design and simulation of local area network using cisco packet tracer." *The International Journal of Engineering and Science* 6.10 (2017): 63-77.

[3] Annigeri, Shubham, Anushka Chauhan, and Jaikishin Chhatlani. "Use of Virtual LANs for Network Segmentation and Organization."

[4] Kim, H. (2010, October). Business models for the free public wireless LAN service. In *2010 14th International Conference on Intelligence in Next Generation Networks* (pp. 1-5). IEEE.

[5] Lam, K. Y., Ng, J. K., & Wang, J. T. (2013, March). A business model for personalized promotion systems on using wlan localization and nfc techniques. In *2013 27th International Conference on Advanced Information Networking and Applications Workshops* (pp. 1129-1134). IEEE.

[6] Mummadi, Akhilendranath, B. Midhun Krishna Yadav, Vishnu Vardhan Ciripuram, and R. Uma Mageswari. "Secure Campus Area Network in Cisco Packet Tracer."

[7] Mummadi, Akhilendranath, et al. "Secure Campus Area Network in Cisco Packet Tracer."