**VISVESVARAYA TECHNOLOGICAL UNIVERSITY**

**“Jnana Sangama”, Belagavi-560014**

****

**Computer Networks**

**Mini Project Report**

**On**

**Secure Campus Area Network Design**

**Submitted in partial fulfillment of the requirement of V Semester**

**Computer Networks Laboratory (21CS52)**

Submitted by,

|  |  |
| --- | --- |
| **Abhyudith M** | **1RF21IS005** |
| **Ezekiel David** | **1RF21IS023** |

**Under the guidance of**

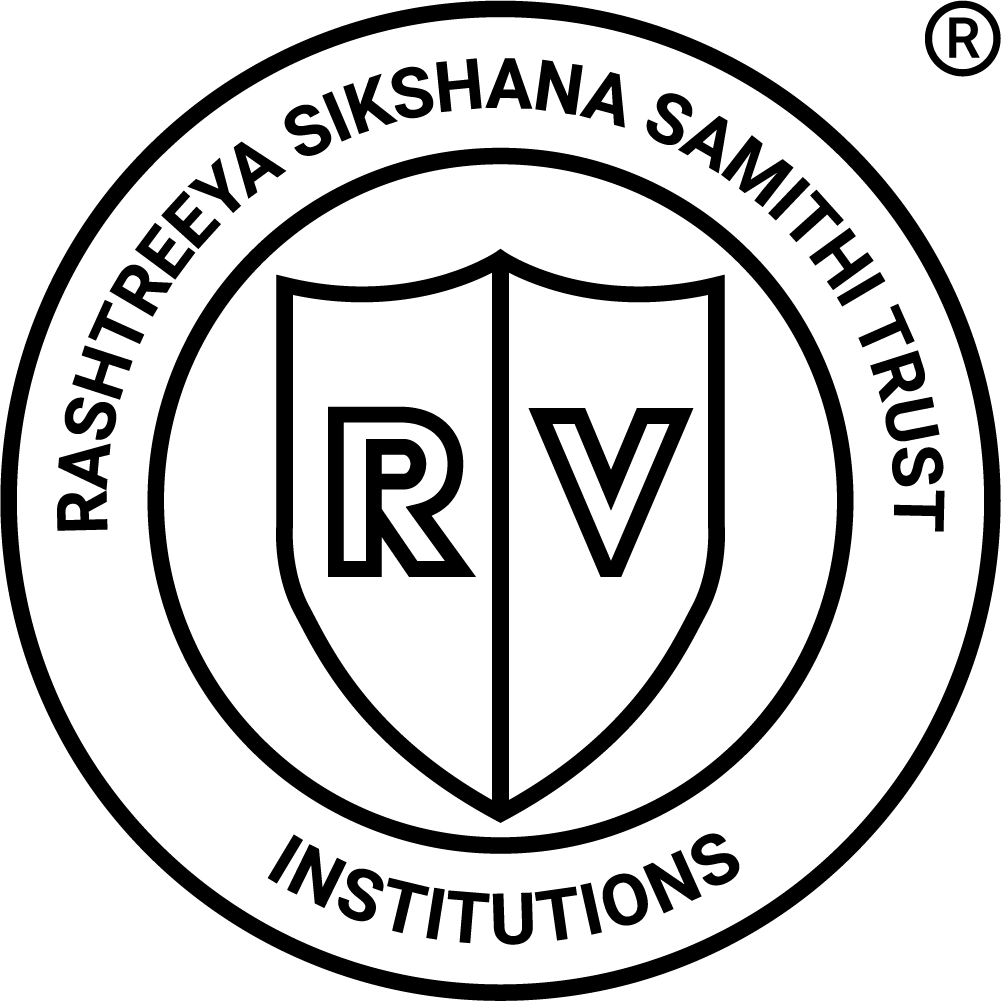
### 

**Dr. Niharika P. Kumar**

Associate Professor

Dept. of ISE

RVITM, Bangalore.



**DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING**

**RV INSTITUTE OF TECHNOLOGY AND MANAGEMENT®**

**Chaitanya Layout, JP Nagar 8th Phase, Kothanur, Bengaluru-560076**

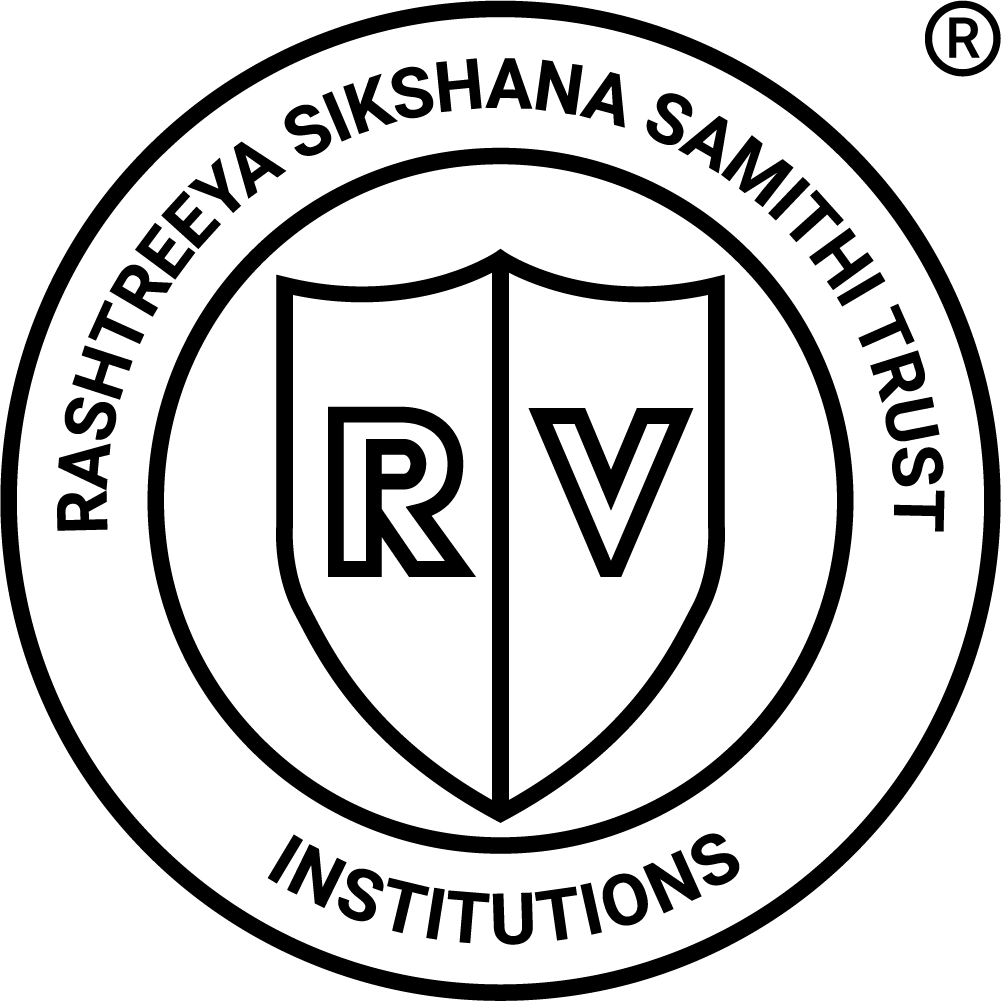
**2023-2024**

**RV INSTITUTE OF TECHNOLOGY AND MANAGEMENT®**

**(Affiliated to Visvesvaraya Technological University, Belagavi & Approved by AICTE, New Delhi)**

**Chaitanya Layout, JP Nagar 8th Phase, Kothanur, Bengaluru-560076**

**DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING**



**Certificate**

This is to certify that the mini-project work entitled **Secure Campus Area Network Design** is carried out by **Abhyudith M (1RF21IS005) and Ezekiel David (1RF21IS023)** in partial fulfillment for the requirement of V Semester Computer Networks Lab with (21CS52) in **Information Science and Engineering** of the **Visvesvaraya Technological University, Belagavi** during the year 2023-2024. It is certified that all the corrections/ suggestions indicated for the given internal assessment have been incorporated in the report. This report has been approved as it satisfies the academic requirements with respect to the mini-project work.

|  |  |  |
| --- | --- | --- |
| **Signature of the Guide** |  | **Signature of the HoD** |
| **Dr. Niharika P. Kumar**  Asso. Professor, Dept. of ISE  RVITM, Bangalore. |  | **Dr. Latha CA**  Dept. of ISE,  RVITM, Bangalore. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |
|  |

**ACKNOWLEDGEMENT**

We express our profound gratitude to **Dr. Jayapal R, Principal, RVITM, Bangalore,** for providing the necessary facilities and an ambient environment to work.

We are grateful to **Dr. Latha C A, Head of Department, Information Science and Engineering, RVITM, Bangalore,** for her valuable suggestions and advice throughout my/our work period.

We would like to express our deepest gratitude and sincere thanks to our guide, **Dr. Niharika P. Kumar**, for their keen interest and encouragement in the project, whose guidance made the project into reality.

We would like to thank all the staff members of **Department** **of Information Science and Engineering** for their support and encouragement during the course of this project.

**ABSTRACT**

In an era marked by escalating cybersecurity threats and stringent data protection regulations, the imperative for designing resilient and secure network infrastructures has become paramount. This abstract delves into the conceptualization and design of a robust Campus Area Network (CAN) tailored for an enterprise spanning two pivotal locations, A and B. Emphasizing stringent access controls and fortified security measures, the proposed CAN architecture aims to safeguard critical assets while facilitating seamless communication between designated user devices and a central server.

The focal point of this endeavor lies in crafting a secure CAN environment that effectively compartmentalizes network traffic and restricts unauthorized access to the central server stationed at Location B. Through meticulous subnet design and VLAN segmentation, the network is structured to ensure isolation between user devices at Location A and the server, thereby curtailing the risk of unauthorized infiltration.

While this abstract provides a high-level overview of the CAN design strategy, it underscores the dynamic nature of network security, necessitating continuous vigilance and adaptation to emerging threats. By prioritizing access controls, subnet segmentation, and meticulous ACL configurations, the proposed CAN framework offers a robust defense mechanism against unauthorized access attempts and potential security breaches. As organizations navigate the evolving landscape of cybersecurity challenges, the design principles outlined in this abstract serve as a foundational blueprint for constructing resilient and secure network architectures tailored to the needs of modern enterprises.

**TABLE OF CONTENTS**

| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
| --- | --- | --- |
|  | **ACKNOWLEDGEMENT** | **i** |
|  | **ABSTRACT** | **ii** |
|  | **TABLE OF CONTENTS** | **iii** |
| **1** | **INTRODUCTION** |  |
| **2** | **IMPLEMENTATION** |  |
| **3** | **SNAPSHOTS** |  |
| **4** | **CONCLUSION AND FUTURE ENHANCEMENTS** |  |
| **5** | **REFERENCES** |  |

**CHAPTER 1**

**INTRODUCTION**

In today's interconnected business landscape, the significance of a secure and dependable network infrastructure cannot be overstated. As enterprises expand their operations across multiple locations, the necessity for a resilient Campus Area Network (CAN) becomes increasingly apparent. This introduction serves as a precursor to an in-depth exploration of the design and implementation of a secure CAN tailored to the specific requirements of an enterprise with two pivotal locations, A and B.

The rapid advancement of technology has revolutionized the way organizations conduct their business, enabling seamless communication and collaboration across dispersed teams. However, this heightened connectivity also brings about new challenges, as cyber threats continue to evolve and data breaches pose significant risks to organizational security. Against this backdrop, the development of a secure CAN emerges as a critical strategic endeavor, providing the foundation for digital operations while safeguarding sensitive information and critical assets.

This introduction lays the groundwork for the ensuing discussion, which delves into the intricacies of constructing a secure and resilient Campus Area Network for an enterprise spanning multiple locations. By examining key principles of network design, access control mechanisms, and security protocols, this endeavor aims to offer valuable insights into mitigating risks, fortifying defenses, and upholding the integrity of digital infrastructures in an ever-evolving threat landscape. As organizations navigate the complexities of modern cybersecurity challenges, the principles outlined herein provide a framework for building robust and adaptable network architectures tailored to the needs of today's interconnected enterprises.

**CHAPTER 2**

**IMPLEMENTATION**

The implementation of the secure Campus Area Network (CAN) involves a series of steps aimed at establishing a robust and resilient network infrastructure that effectively safeguards critical assets while facilitating seamless communication between locations A and B. Below, we outline key components of the implementation process along with relevant pseudocode snippets and descriptions:

1. **Subnet Design and VLAN Configuration**:

// Define subnets for locations A and B

subnet\_A = 192.168.1.0/24

subnet\_B = 192.168.2.0/24

// Configure VLANs for segmentation

VLAN\_A = VLAN1

VLAN\_B = VLAN2

// Assign subnets to VLANs

Assign subnet\_A to VLAN\_A

Assign subnet\_B to VLAN\_B

Description: This pseudocode snippet illustrates the initial steps in subnet design and VLAN configuration. Subnets are defined for each location (A and B), and VLANs are configured to segment the network traffic accordingly. Each subnet is then assigned to its respective VLAN, ensuring proper isolation and traffic control.

1. **Access Control Lists (ACLs) Configuration**:

// Configure ACLs on the router interface connecting locations A and B

AccessControlList ACL\_Location\_B

Deny any traffic from subnet\_A to subnet\_B

Permit traffic from PCs PC0 to PC5 to the server's web service port

Deny ping requests from subnet\_A to the server

Apply ACL\_Location\_B to router interface connecting subnet\_A and subnet\_B

Description: In this pseudocode snippet, ACLs are configured on the router interface connecting locations A and B to enforce access control policies. The ACL denies any traffic from subnet\_A to subnet\_B, except for authorized PCs (PC0 to PC5) accessing the server's web service port. Additionally, ping requests from subnet\_A to the server are denied to restrict unauthorized access attempts.

1. **Firewall Rules Configuration:**

// Configure firewall rules on the network firewall device

FirewallRule Location\_B\_Server\_Rules

Allow incoming traffic to the server's web service port from subnet\_A

Deny all other incoming traffic to the server

Apply Location\_B\_Server\_Rules to network firewall device

Description: This pseudocode snippet demonstrates the configuration of firewall rules on the network firewall device to further enhance security. The rules allow incoming traffic to the server's web service port from subnet\_A while blocking all other incoming traffic to the server, thereby restricting access exclusively to authorized users.

By following these implementation steps and configuring network devices accordingly, the secure Campus Area Network (CAN) can be effectively deployed to ensure robust security and seamless communication between locations A and B.

**2.1 SOFTWARE REQUIREMENTS:**

1. **Network Operating System (NOS)**:

The network devices (routers, switches) should run a reliable network operating system capable of supporting advanced security features such as VLANs, ACLs, and encryption.

1. **Firewall Software**:

Deploy firewall software capable of implementing access control policies to restrict traffic flow between network segments (subnets) and enforce security policies for incoming and outgoing traffic.

1. **Intrusion Detection and Prevention System (IDPS)**:

Implement IDPS software to monitor network traffic for suspicious activities, detect potential security threats, and take appropriate actions to prevent security breaches.

1. **Remote Access Software**:

Utilize remote access software to enable secure remote management of network devices, allowing administrators to configure and monitor the network from remote locations while maintaining security.

1. **Network Management Software:**

Deploy network management software for centralized monitoring, configuration, and administration of network devices, facilitating efficient network operation and troubleshooting.

**2.2 HARDWARE REQUIREMENTS**

1. **Routers:**

High-performance routers capable of handling routing between different network segments (subnets), implementing access control lists (ACLs), and supporting virtual private network (VPN) connections for secure remote access.

1. **Switches:**

Managed switches with support for VLANs, spanning tree protocol (STP), and quality of service (QoS) features to efficiently manage network traffic, segment the network, and prioritize critical data flows.

1. **Firewalls:**

Next-generation firewalls (NGFW) with intrusion prevention system (IPS) capabilities, deep packet inspection (DPI), and application-aware filtering to enforce security policies, block unauthorized access attempts, and protect against advanced threats.

1. **Authentication Servers:**

Authentication servers such as RADIUS (Remote Authentication Dial-In User Service) or LDAP (Lightweight Directory Access Protocol) servers to manage user authentication, authorization, and accounting for secure access control.

1. **Server:**

A robust server located in Location B to host critical network services and applications, such as web services, databases, and file servers, requiring sufficient processing power, memory, and storage capacity to handle enterprise-level workloads.

**CHAPTER 3**

**SNAPSHOTS**

**CHAPTER 4**

**CONCLUSION AND FUTURE ENHANCEMENTS**

In conclusion, the design of a secure campus area network (CAN) for the enterprise with two locations, A and B, is crucial for ensuring the confidentiality, integrity, and availability of network resources and services. By implementing a robust network architecture, access control mechanisms, and security measures, the CAN can effectively restrict access to critical assets while facilitating secure communication and collaboration within the organization.

Key components of the secure CAN design include subnet segmentation, VLAN implementation, access control lists (ACLs), firewalls, intrusion detection and prevention systems (IDPS), authentication servers, and encryption technologies.

While the initial design lays the foundation for a secure CAN, there are several future enhancements that can further strengthen the network's security

1. **Advanced Threat Detection**: Implement advanced threat detection technologies such as machine learning-based anomaly detection and behavior analysis to proactively identify and mitigate emerging cyber threats.
2. **Zero Trust Architecture**: Transition towards a zero trust security model where access to network resources is granted based on strict verification of user identity, device health, and contextual factors, regardless of the user's location.
3. **Software-Defined Networking (SDN)**: Explore the adoption of SDN principles to centralize network management, automate security policy enforcement, and improve network agility and scalability.
4. **Cloud Integration:** Integrate cloud-based security services and solutions to extend the perimeter of the secure CAN, enable secure access to cloud resources, and enhance data protection and resilience.

**CHAPTER 5**

**REFERENCES**

* https://www.cisco.com/
* https://www.researchgate.net/publication/
* https://www.semanticscholar.org/paper/
* https://www.academia.edu/