Design and Simulation of a Secure Campus Network Using Cisco Packet Tracer

Anand Mahadevan SM
Dept. of ECE
Amrita Vishwa Vidyapeetham
AM.EN.U4ECE22008
anandmahadevan2004@gmail.com

Aiswarya Santhosh
Dept. of ECE
Amrita Vishwa Vidyapeetham
AM.EN.U4ECE22007
aiswarya44044@gmail.com

Devarsh MD
Dept. of ECE
Amrita Vishwa Vidyapeetham
AM.EN.U4ECE22015
devarshmd@gmail.com

Nived G Unni
Dept. of ECE
Amrita Vishwa Vidyapeetham
AM.EN.U4ECE22031
nivedgunni@gmail.com

Muhammed Basil K
Dept. of ECE
Amrita Vishwa Vidyapeetham
AM.EN.U4ECE22025
muhammedbasil2415@gmail.com

***Abstract*—As modern institutions grow increasingly reliant on digital infrastructure, the need for secure, scalable, and high-performance networks becomes paramount. Campus Area Networks (CANs), which interconnect computing resources within educational or enterprise environments, must be designed with a strong emphasis on security, accessibility, and resilience.**

This project presents the design and simulation of a Secure Campus Area Network tailored for a dual-location enterprise setup. Utilizing Cisco Packet Tracer, we implemented a network architecture employing VLAN segmentation, subnetting, Access Control Lists (ACLs), and firewalls to regulate traffic flow and protect critical resources. Specific network zones were defined using subnet ranges and associated with VLANs to isolate broadcast domains and manage inter-device communication securely. ACLs enforced tight access rules allowing only authorized nodes to interact with central services such as web servers.

The project demonstrates that with strategic use of network segmentation, administrative control, and security protocols, a robust CAN can be built to prevent lateral threats, enforce access discipline, and support seamless communication between distributed network entities. The proposed design not only secures the infrastructure but also lays the groundwork for future scalability and integration with modern technologies such as SDN and cloud computing.

***Index Terms*—Campus Area Network, VLAN, Subnetting, Network Security, Access Control Lists, Cisco Packet Tracer, Firewalls**

I. Introduction

In the era of digital transformation, networks serve as the foundation of all organizational communication and services. Educational institutions and enterprises alike rely on robust network infrastructures to support operations ranging from resource sharing and collaboration to data security and remote access. Within this context, a Campus Area Network (CAN) plays a critical role in connecting systems across buildings or locations within a confined geographic space.

Despite the benefits of connectivity, increased exposure to cyber threats and system vulnerabilities necessitates that these networks be secure by design. Conventional flat network models are ill-equipped to address today's sophisticated threat landscape. Thus, there is a strong demand for segmented, policy-driven, and resilient network structures that reduce the attack surface and improve control over data flows.

This project aims to design and simulate a secure and scalable CAN architecture for an organization operating across two locations, A and B. The network employs best practices in modern network design, including:

- Logical segmentation using Virtual LANs (VLANs)
- Subnetting for traffic management and isolation
- Access Control Lists (ACLs) to define and enforce communication policies
- Deployment of firewalls to prevent unauthorized access

The use of Cisco Packet Tracer enables visualization and validation of the network design. Through simulation, it becomes possible to observe traffic behaviors, verify policy enforcement, and ensure that security objectives are achieved before real-world deployment. This paper details the implementation methodology, simulation results, and potential for future enhancements to meet evolving network demands.

II. Implementation

A. Subnet and VLAN Configuration

To ensure logical separation and efficient traffic control, the network is divided into two main subnets and VLANs:

- Location A Subnet: 192.168.1.0/24 assigned to VLAN1
- Location B Subnet: 192.168.2.0/24 assigned to VLAN2

These VLANs provide isolation between user devices in different physical locations, reducing the risk of broadcast storms and minimizing exposure in case of an internal compromise. Switches are configured to associate specific ports with the corresponding VLANs, and inter-VLAN routing is managed through the core router.

B. Access Control Lists (ACLs)

ACLs are used to enforce traffic filtering at the router level. The configurations include:

- Denying general traffic from Subnet A to Subnet B to protect critical assets.
- Explicitly permitting HTTP/HTTPS traffic from only PC0 to PC5 to the web server located in Location B.
- Blocking ICMP echo requests (ping) to prevent reconnaissance from potential intruders.

The ACLs are applied to the appropriate router interfaces using inbound/outbound filters to strictly manage permitted communication paths, thus enhancing internal security.

C. Firewall Rules

A network-based firewall is deployed at the perimeter of Location B, enforcing application-layer inspection and policy-based controls. The firewall is configured with rules to:

- Allow only HTTP and HTTPS traffic to the web server from authorized IP addresses.
- Block all other protocols and traffic types not explicitly permitted.

This setup adds another layer of protection, reducing the attack surface and improving compliance with best security practices.

D. Tools Used

- Cisco Packet Tracer: A powerful network simulation tool used to design, configure, and test the entire CAN topology.
- Router CLI: Used to apply ACLs, configure interfaces, and enable routing protocols.
- Managed Switches: Configured with VLAN settings and trunk/access port definitions.
- Network Devices: Including servers, access points, and PCs were virtually deployed and configured within Packet Tracer to simulate real-world scenarios.

III. Results and Observations

Through the Packet Tracer simulation, several observations were recorded:

- Unauthorized PCs located in VLAN1 (Subnet A) were unable to reach the server in VLAN2 due to correctly configured ACLs and firewall rules.
- Designated PCs (PC0–PC5) successfully accessed the server's web service, verifying the correct ACL application.
- Attempted ICMP traffic was blocked as expected, demonstrating effective reconnaissance prevention.
- VLAN segmentation was confirmed to reduce inter-VLAN broadcast traffic and ensure clear logical separation between user zones.
- The simulation displayed a scalable architecture that can easily be expanded to support additional VLANs, subnets, and services.

These outcomes validate the security and performance of the designed network and its ability to enforce strict access policies while maintaining necessary communication.

IV. Conclusion and Future Work

The secure Campus Area Network (CAN) designed and simulated in this project illustrates a strong foundation for implementing enterprise-level network security. The integration of Virtual LANs (VLANs), Access Control Lists (ACLs), and firewalls ensures controlled communication, network segmentation, and resilience against common cyber threats.

The simulation demonstrated that the system effectively prevents unauthorized access, restricts lateral movement within the network, and supports structured communication among designated devices. Furthermore, the modularity of the architecture makes it adaptable for future scaling and integration.

To further enhance this architecture, the following future improvements are proposed:

- Zero Trust Architecture (ZTA): Implement continuous identity verification and least-privilege access controls to enhance security posture.
- Cloud Integration: Employ cloud-based Identity and Access Management (IAM) solutions to enable flexible, centralized authentication services.
- Advanced Intrusion Detection and Prevention: Integrate next-generation Intrusion Prevention Systems (IPS) and security analytics to identify and mitigate sophisticated threats.
- AI-Based Traffic Monitoring: Leverage machine learning algorithms for real-time anomaly detection and proactive threat response.
- Software Defined Networking (SDN): Adopt SDN to provide dynamic, policy-driven control and improve network flexibility and scalability.

These enhancements will align the CAN infrastructure with evolving cybersecurity requirements and future-proof it for next-generation enterprise needs.

Acknowledgment

We would like to express our sincere gratitude to our faculty mentor and guide, Aswathy K Nair, for their invaluable support, expert guidance, and constant encouragement throughout the course of this mini project. We are also grateful to the Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, for providing access to essential tools and resources, including Cisco Packet Tracer and laboratory infrastructure.

References

[1] Cisco Networking Academy, *CCNA Curriculum*. [Online]. Available: https://www.cisco.com/

[2] *ResearchGate Publications on Network Security*. [Online]. Available: https://www.researchgate.net/

[3] *Secure Network Design*. Semantic Scholar. [Online]. Available: https://www.semanticscholar.org/

[4] *Computer Networking Reports*. Academia.edu. [Online]. Available: https://www.academia.edu/