Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 10, 2025

DESIGN AND IMPLEMENTATION OF CAMPUS AREA NETWORKS: A COMPREHENSIVE APPROACH FOR A SECURE AND SCALABLE NETWORK

Iqra Khan[1], Aftab Alam[*2], Nazia Azim[3], Shah Khalid[4]

[1,2,4] *Department of Computer Science and Information Technology, University of Malakand, KP, Pakistan*
[3]*Department of Computer Science Abdul Wali Khan University, Mardan, KP, Pakistan.*

[1]iqrak5139@gmail.com, [*2]text2alam@gmail.com, [3]n.azim@awkum.edu.pk, [4]shahkhalid@uom.edu.pk

DOI: https://doi.org/10.5281/zenodo.17348278

Keywords
Campus Area Network (CAN), Network Design, VLAN, Routing (EIGRP, OSPF), DHCP, VPN and NAT, Network Security, Wireless Networking

Article History
Received: 11 July 2025
Accepted: 21 September 2025
Published: 11 October 2025

Corresponding Author: *
Aftab Alam

Abstract
With the advancements in the digital media ecosystem, and particularly the proliferation of social networking sites (SNS) and their audiences, it is important to comprehend the role social media plays in marketing efforts. This study assesses the direct and indirect impact of SNS-based brand communication on Online Purchase Intention (OPI) in the online consumer market. Having literary support, Brand Attachment (BAT), and Online Brand Experience (OBE) were modeled as major mediators of the study under consideration. Seven hypotheses were made, and the AMOS 22.0 and SPSS 25.00 were employed to assess the relationship among the focal variables for three hundred and five respondents. The findings of the study reveal that Brand Communication (BC) on SNS has a significant positive impact on OPI. Limitations, future research directions, and management and academic ramifications are highlighted.

INTRODUCTION

In the contemporary digital era, the importance of secure, scalable, and high-performance networking infrastructures has grown exponentially. Organizations such as universities, corporate campuses, healthcare facilities, and defense installations rely heavily on efficient communication systems to manage their daily operations [1]. A Campus Area Network (CAN) is a specialized type of network designed to interconnect multiple Local Area Networks (LANs) across several buildings within a geographically restricted environment, typically within a university or business campus [2]. Unlike Wide Area Networks (WANs), which span large geographic distances, or Metropolitan Area Networks (MANs), which connect infrastructures across cities, CANs are confined to smaller areas while providing high bandwidth, centralized resource sharing, and robust communication [3]. The primary goal of implementation of CAN is to guarantee good centralization of resources, sharing of information, and good management of the network in the campus setting [4].

CANs design entails harmonious incorporation of diverse networking apparatuses, protocols and

services. The basic components are routers, Layer 2 (L2) switches, and Layer 3 (L3) switches that comprise the backbone of the inter-departmental communication within and data routing. The strategies used by the CANs are the hierarchical IP addressing schemes (Class A, B and C) which allow effective assignment of IP ranges to meet the traffic demands [5]. Dynamic Host Configuration Protocol (DHCP) servers are popular with automated IP configuration which addresses human error when using manual assignments.

Routing within a CAN often combines static routing with dynamic routing protocols. Two of the latter are: Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF), which are widely used because of their efficiency in optimizing paths and redundancy [6]. In order to have interoperability between the different routing domains, route redistribution between EIGRP and OSPF is applied [7].

Network security and network management mechanisms are also very important in the implementation of CAN. Remote access is an administrative facility that is enabled through Telnet and more secure Secure Shell (SSH) the latter, which offers secure communication through encrypted messages to prevent malicious intrusion [8]. Additionally, the Access Control Lists (ACLs) are implemented to make traffic filtering and policy control, limiting unauthorized access. To be mobile on campus, they are integrated with Wireless Local Area Networks (WLANs), whereas Virtual Private Networks (VPNs) and Network Address Translation (NAT) ensure secure access to the outside world and remote access [9]. To improve performance and redundancy, EtherChannel is utilized to combine several physical connections into single logical connections and in the process increases bandwidth [10]. In the meantime, the Spanning Tree Protocol (STP) helps in avoiding switching loops and makes the network topologies stable [11]. Virtual Local Area Networks (VLANs) provide logical segmentation of the traffic in the department to which they belong and Inter-VLAN routing provides smooth communication between the logical partitions of the network [12]. Lastly, the implementation and design of CANs must be tested. The connectivity, the performance and the compliance with the security are done using tool like packet-tracing applications to assure that the infrastructure meets the optimal operation, fault tolerance and scalability [13]. Thus, the present research study is devoted to the overall design, implementation and validation of Campus Area Network with special consideration of efficiency, scalability and security as the essential features of supporting academic and enterprise applications.

The remaining paper organization is in Section II presents the Literature Review, Section III details the Design and Implementation of the proposed CAN, provides Results and Validation, Section VI discusses Conclusion and Future Work.

II. Literature Review

The concept of Campus Area Networks (CANs) has been explored in numerous studies, primarily due to their significance in higher education, enterprise campuses, and military environments. CANs serve as a unifying backbone for communication across geographically constrained sites, providing scalability, centralized management, and high-speed interconnectivity [14]. Unlike Local Area Networks (LANs), which typically serve a single department or building, CANs consolidate multiple LANs into a cohesive framework, thereby enabling integrated data management and resource sharing. Early studies on CANs emphasized their role in cost reduction and centralized administration through shared networking devices and services [15]. More recent approaches, however, highlight the necessity of scalability, fault tolerance, and security as integral design goals [16].

A. Networking Devices and Architectures

The backbone of a CAN design involves Layer 2 (L2) and Layer 3 (L3) switches as well as routers that govern both intra-departmental and inter-departmental communication. Prior works highlight the hierarchical model of networking, where access, distribution, and core layers ensure modularity and scalability [17]. Cisco's hierarchical model is widely recognized as a best practice in CAN implementation, reducing complexity and improving fault isolation [18]. Moreover, research has demonstrated that L3 switching and Inter-VLAN routing significantly improve the performance of CANs by enabling

seamless communication between logically segmented networks [19].

B. IP Addressing and DHCP Integration

Efficient IP addressing is critical in campus networks due to the large number of devices and departments requiring unique identifiers. Studies indicate that a structured IP addressing scheme not only improves manageability but also enhances routing efficiency [20]. The deployment of Class A, B, and C addressing schemes, along with subnetting, provides flexibility for departments of varying sizes [21]. The incorporation of Dynamic Host Configuration Protocol (DHCP) has been noted to reduce configuration errors and administrative overhead, thereby improving overall network reliability [22].

C. Routing Approaches in CANs

Routing forms the backbone of CAN communication. Static routing has traditionally been used for smaller campus deployments due to its simplicity; however, its limitations in scalability and redundancy have been well-documented [23]. Dynamic routing protocols such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) have become more prevalent in modern CANs, as they provide faster convergence, redundancy, and efficient path selection [24]. Studies also emphasize the role of route redistribution between EIGRP and OSPF to ensure seamless communication across heterogeneous routing domains [25]. Such mechanisms have been recognized as critical in large-scale campus deployments where multiple routing protocols coexist.

D. Network Security in Campus Environments

Security is an indispensable factor in campus networks, as they often serve large user populations with varying access levels. Previous research underscores the vulnerabilities associated with legacy protocols like Telnet, advocating for the adoption of Secure Shell (SSH) to mitigate risks through encryption [26]. Moreover, Access Control Lists (ACLs) have been identified as effective mechanisms for traffic filtering and enforcing departmental policies [27]. Studies also highlight the increasing importance of Virtual Private Networks (VPNs) and Network Address Translation (NAT) in securing remote access and facilitating external communications [28]. These security mechanisms, when combined, form a layered defense strategy essential for protecting sensitive data in academic and enterprise settings.

E. Performance Optimization Techniques

Numerous studies emphasize the importance of redundancy and fault tolerance in CAN design. The use of EtherChannel for link aggregation is widely recommended to enhance bandwidth utilization and reliability [29]. Likewise, the deployment of the Spanning Tree Protocol (STP) prevents switching loops and ensures stable network topologies [30]. Research has also recognized the effectiveness of Virtual Local Area Networks (VLANs) for logical segmentation, which not only improves network performance but also enhances security through isolation [31]. Inter-VLAN routing, supported by L3 switches, further enables efficient cross-department communication without compromising segmentation.

F. Testing and Validation Tools

Network performance verification is another area of interest in CAN research. Simulation and diagnostic tools such as packet tracers, traffic analyzers, and Google-based diagnostic platforms have been utilized for network validation [32]. These tools allow administrators to assess latency, throughput, and fault tolerance under varying traffic conditions, thereby ensuring optimal deployment of campus networks [33]. Furthermore, network emulators are increasingly applied in academic research to model and analyze the scalability and security of CANs before physical implementation [34].

Research Gap

While the reviewed literature provides a solid foundation for understanding CAN design, certain gaps remain. Few studies have comprehensively addressed the integration of multiple routing protocols with route redistribution in campus environments. Additionally, although VLAN segmentation and ACLs are well-documented, there is limited research on holistic validation frameworks that combine scalability, performance, and security

testing under real-world traffic conditions. This study aims to address these gaps by presenting a comprehensive CAN design that incorporates advanced routing, VLAN segmentation, security mechanisms, and diagnostic validation to ensure a robust, scalable, and secure campus network.

III. Implementation, Results, and Discussion

A. Implementation in Cisco Packet Tracer

The proposed Campus Area Network (CAN) architecture was implemented using Cisco Packet Tracer 8.2. The simulation included three main hierarchical layers: core, distribution, and access, supported by routers, L2/L3 switches, and end devices. Departments were logically segmented using VLANs (e.g., VLAN 10–Faculty, VLAN 20–Administration, VLAN 30–Students). Inter-VLAN routing was enabled on a Layer 3 switch to ensure seamless communication (See Figure 1).

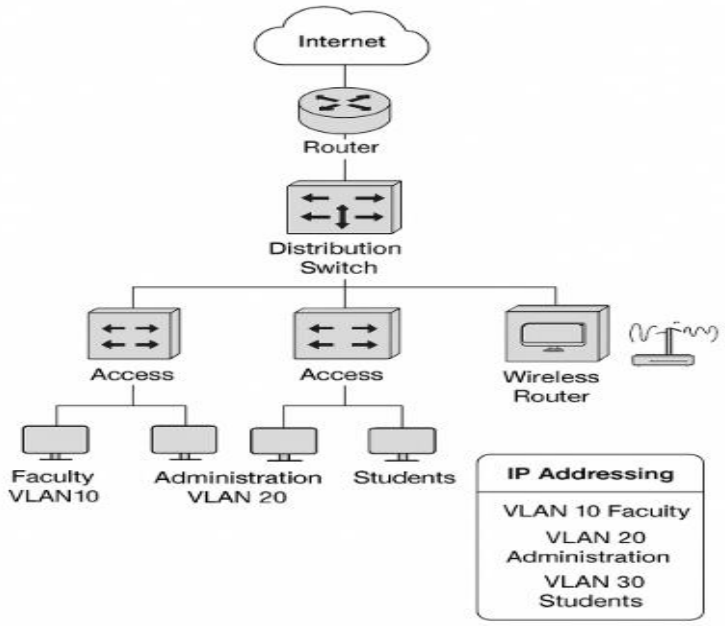

Figure 1Campus Area Network (CAN) architecture

A structured IP addressing scheme was adopted, where Class A and B address blocks were subnetted for departmental allocation. DHCP servers were configured to dynamically assign IPs, reducing administrative overhead. Routing was established through a hybrid approach:

- Static routing for small subnets.
- EIGRP and OSPF for dynamic routing across distribution and core routers.
- Route redistribution enabled interoperability between EIGRP and OSPF domains.

For security and remote management, Telnet and SSH were configured, with ACLs applied at the distribution layer to restrict unauthorized access. VPN and NAT were also tested for external connectivity. Reliability was ensured by enabling EtherChannel on redundant links and Spanning Tree Protocol (STP) to prevent switching loops. Wireless routers provided WLAN access for mobile users.

B. Implementation detail

The proposed Campus Area Network (CAN) was implemented and simulated using Cisco Packet Tracer 8.2, structured into the core, distribution, and access layers. Each layer was assigned specific responsibilities to ensure hierarchical design, scalability, and simplified troubleshooting.

1) VLAN and Logical Segmentation

Three departments were logically segmented using VLANs:

- VLAN 10 – Faculty
- VLAN 20 – Administration
- VLAN 30 – Students

An additional VLAN 99 was configured as the management VLAN. Inter-VLAN communication was enabled through a Layer 3 switch (3560) using Switch Virtual Interfaces (SVIs).

2) IP Addressing Scheme

A structured hierarchical IP addressing plan was adopted (Table I). A Class B block (172.16.0.0/16) was subnetted for departmental use, while Class A (10.0.0.0/8) and Class C (192.168.x.0/24) were reserved for testing and backbone links.

Table 1IP Addressing Plan

Department/Device	VLAN	Subnet	Gateway	DHCP Pool Range
Faculty PCs	10	172.16.10.0/24	172.16.10.1	172.16.10.50 – 172.16.10.200
Administration	20	172.16.20.0/24	172.16.20.1	172.16.20.50 – 172.16.20.200
Students	30	172.16.30.0/24	172.16.30.1	172.16.30.50 – 172.16.30.200
Management	99	172.16.99.0/24	172.16.99.1	Admin only
Core Backbone	—	10.0.0.0/30	Point-to-Point Links	—
WAN/Internet Test	—	192.168.1.0/24	192.168.1.1	NAT enabled

3) DHCP Configuration

Each departmental VLAN was assigned a DHCP scope on the server. Example configuration for Faculty VLAN:

#ip dhcp pool FACULTY
network 172.16.10.0 255.255.255.0
#default-router 172.16.10.1
#dns-server 8.8.8.8

4) Routing Configuration

Routing was implemented through a hybrid approach:

4.1.1 Static Routing: For small interconnections and management VLANs.

4.2 EIGRP: Configured in the distribution layer for fast convergence and load balancing.

Example:

#router eigrp 100
network 172.16.0.0

4.3 OSPF: Configured in the core for scalability and hierarchical division. Example:

#router ospf 1
network 10.0.0.0 0.0.0.3 area 0

Route Redistribution: Applied on the border router to allow interoperability between EIGRP and OSPF. Example:

#router eigrp 100
#redistribute ospf 1 metric 10000 100 255 1 1500
#router ospf 1
#redistribute eigrp 100 subnets

5) Security and Remote Access

- Telnet and SSH (v2) were configured on all Layer 3 devices for remote administration.
- ACLs were applied at the distribution layer to restrict access (e.g., blocking student VLAN traffic to the management VLAN).
- VPN and NAT were configured at the border router to allow secure external connectivity (See Figure 2)

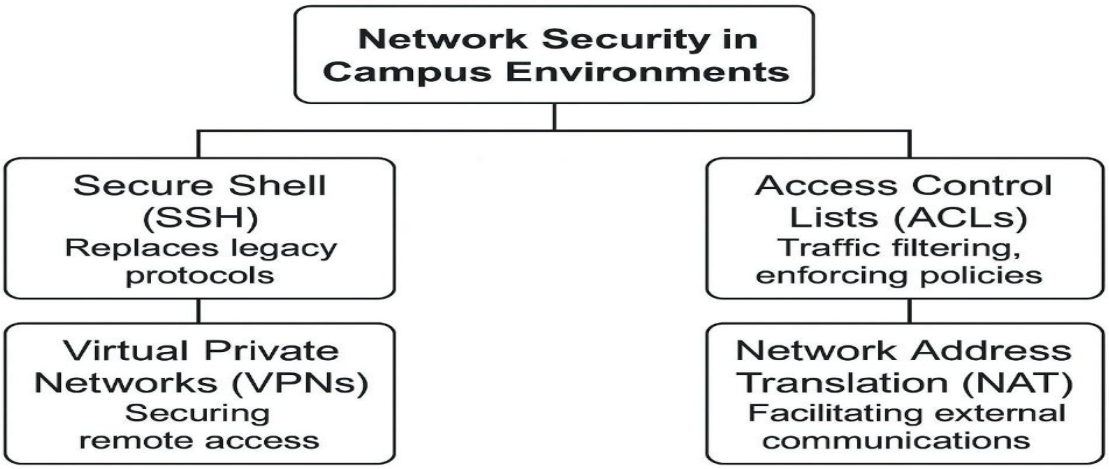

Figure 2Security Implementation in CAN

5.1 Secure Shell (SSH) — Remote Administration

Device: Core Layer 3 Switch

Management IP: 192.168.10.1/24 (Mgmt VLAN 10)

Configuration (See Figure 3)

Switch(config)# hostname CORE-SW
CORE-SW(config)# ip domain-name campus.local
CORE-SW(config)# username admin secret Pa55w0rd
CORE-SW(config)# crypto key generate rsa
CORE-SW(config)# ip ssh version 2
CORE-SW(config)# line vty 0 4
CORE-SW(config-line)# transport input ssh
CORE-SW(config-line)# login local
CORE-SW(config-line)# exit
CORE-SW(config)# interface vlan 10
CORE-SW(config-if)# ip address 192.168.10.1 255.255.255.0
CORE-SW(config-if)# no shut

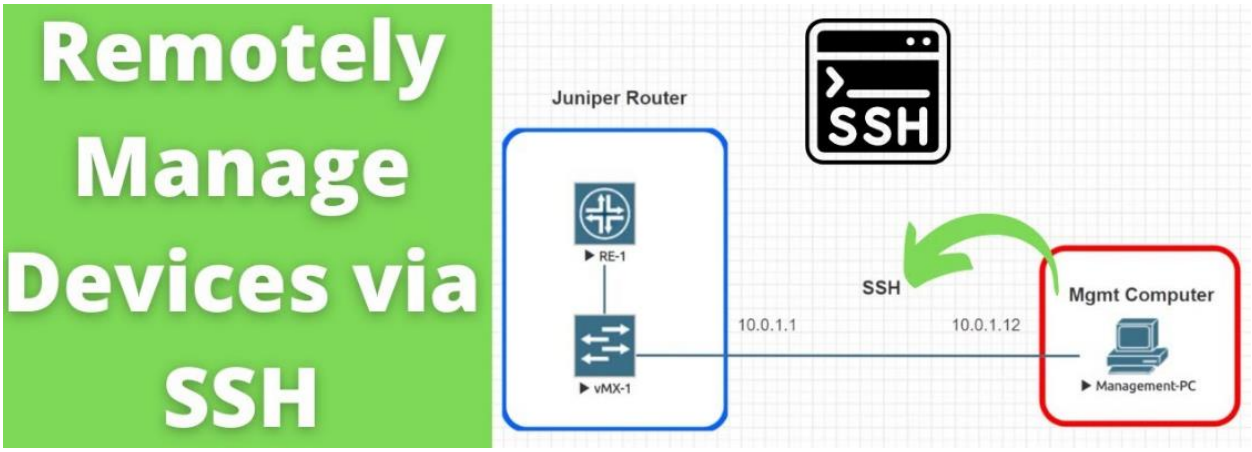

Figure 3SSH

5.2. Access control list (ACL) — VLAN Traffic Restriction

IP Plan

- Student VLAN 20: 192.168.20.0/24
- Management VLAN 10: 192.168.10.0/24

Implementation (See Figure 4)

CORE-SW(config)# ip access-list extended BLOCK_STUDENTS

CORE-SW(config-ext-nacl)# deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
CORE-SW(config-ext-nacl)# permit ip any any
CORE-SW(config-ext-nacl)# exit
CORE-SW(config)# interface vlan 20
CORE-SW(config-if)# ip access-group BLOCK_STUDENTS in

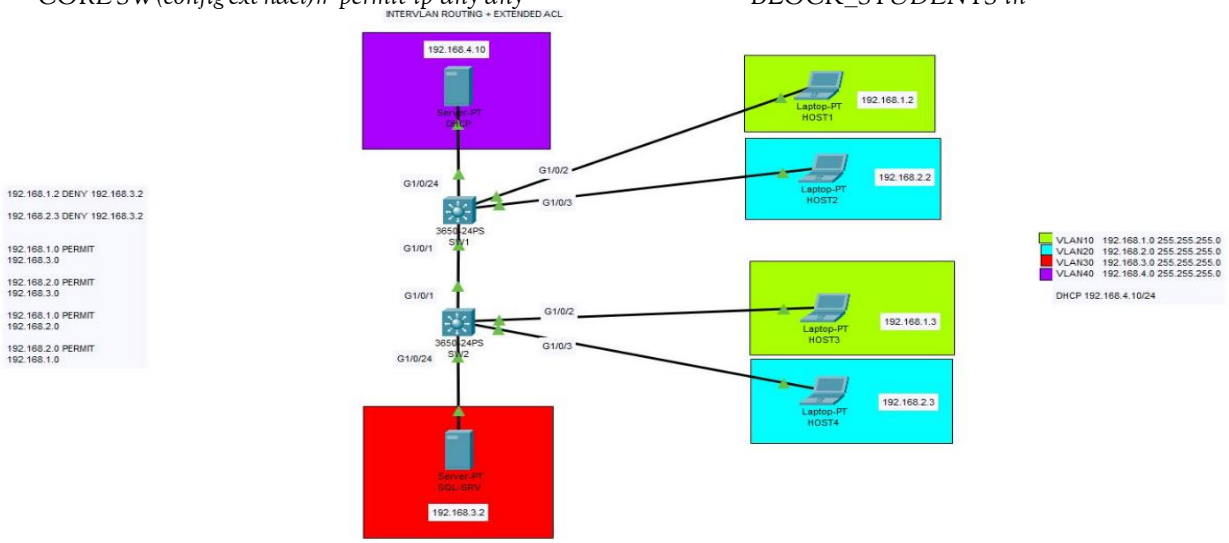

Figure 4Access Control List (ACL)

5.3. Virtual private network (VPN) — Secure Remote Access

IP Plan

- Border Router Outside Interface: 203.0.113.1 (Public)
- Inside Interface: 192.168.1.1 (Private)

Implementation (Basic Site-to-Site) (See Figure 5)

Router(config)# crypto isakmp policy 10
Router(config-isakmp)# encryption aes
Router(config-isakmp)# hash sha
Router(config-isakmp)# authentication pre-share
Router(config-isakmp)# group 2
Router(config)# crypto isakmp key vpnpass address 198.51.100.1
Router(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
Router(config)# crypto map VPN-MAP 10 ipsec-isakmp
Router(config-crypto-map)# set peer 198.51.100.1
Router(config-crypto-map)# set transform-set VPN-SET
Router(config-crypto-map)# match address 100
Router(config)# access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

Router(config)# interface g0/0
Router(config-if)# crypto map VPN-MAP

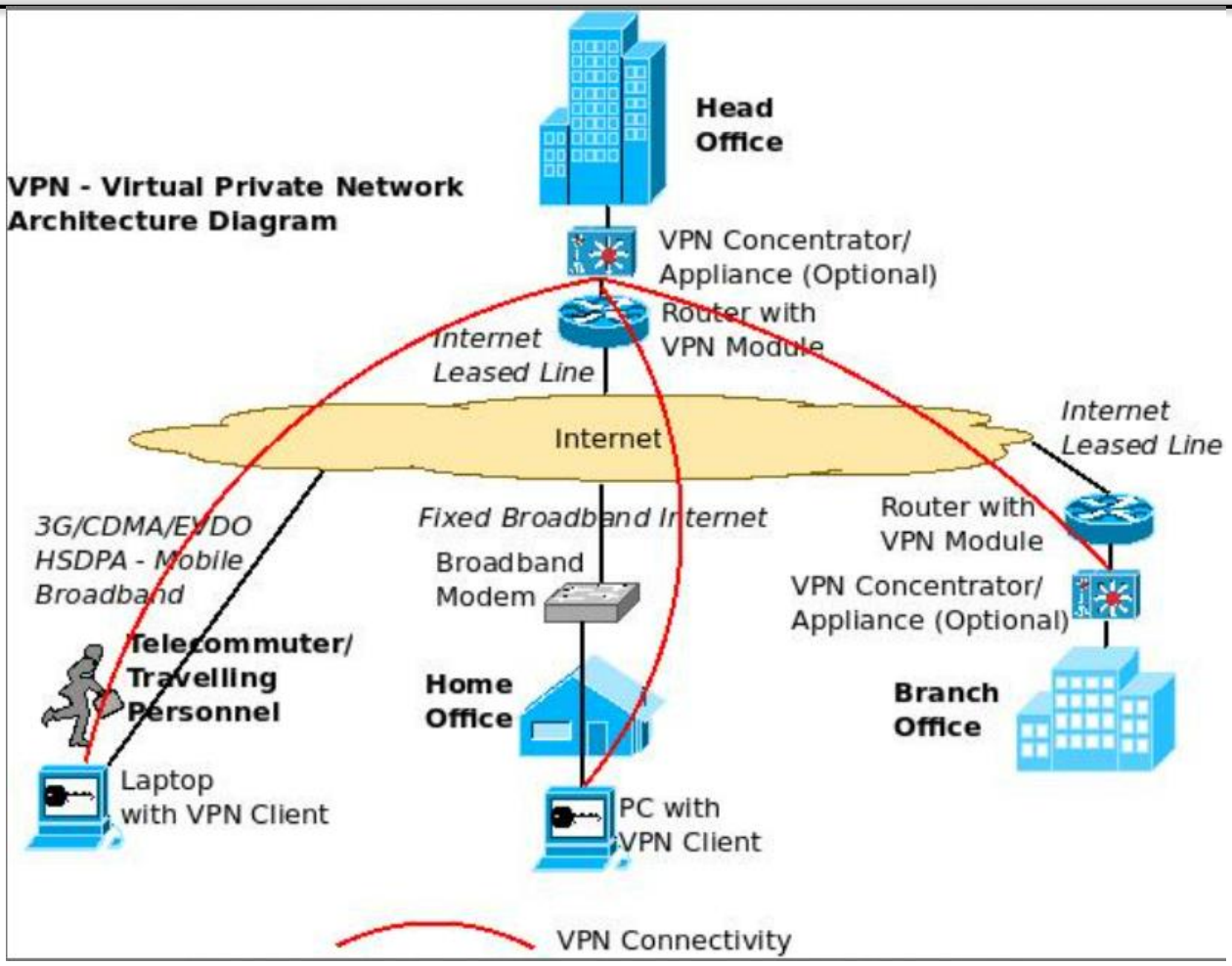

Figure 5Virtual private network (VPN)

5.4 Network address translation (NAT) – External Connectivity

IP Plan

- Inside LAN: 192.168.1.0/24
- Outside Public: 203.0.113.1

Implementation (PAT/Overload) (See Figure 6)

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# interface g0/0
Router(config-if)# ip address 203.0.113.1 255.255.255.0
Router(config)# interface g0/1
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config)# ip nat inside source list 1 interface g0/0 overload

Router(config)# interface g0/0
Router(config-if)# ip nat outside
Router(config)# interface g0/1
Router(config-if)# ip nat inside
```

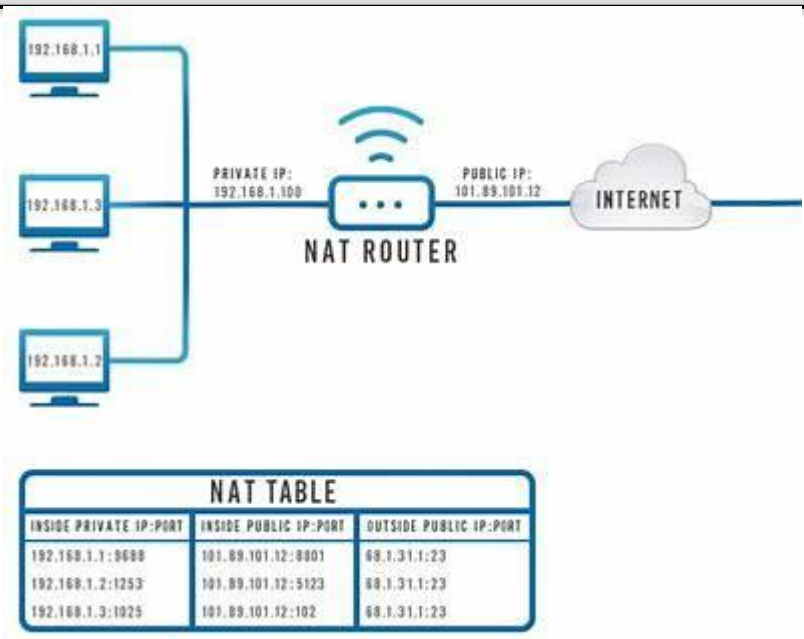

Figure 6Network Address Translation(NAT)

6) Reliability and Redundancy

- EtherChannel (LACP) was used to aggregate redundant links between core and distribution switches.
- Spanning Tree Protocol (STP) was enabled in PVST+ mode to prevent Layer 2 switching loops.
- Wireless Routers were deployed in the access layer to provide WLAN services for mobile users, mapped to the Student VLAN (30).

7) Testing and Validation (See Figure 7)

- Ping and Traceroute were used to validate inter-VLAN and inter-departmental communication.
- ACL testing confirmed restricted access to sensitive VLANs.
- NAT testing verified internet access for internal hosts via 192.168.1.1.
- Google-based diagnostic tools and Packet Tracer simulation logs confirmed optimal throughput, redundancy, and secure access.

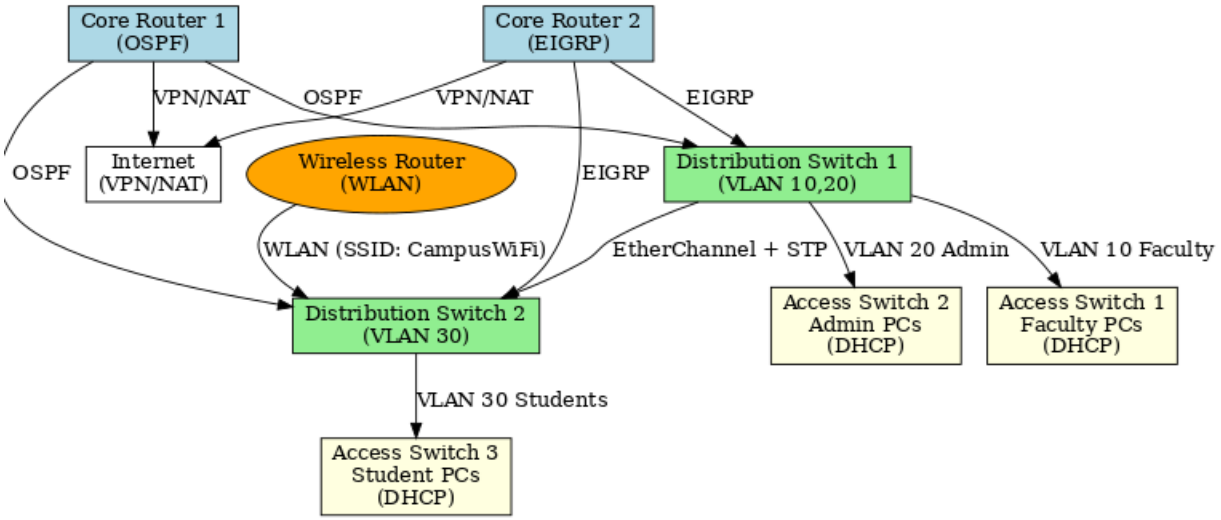

Figure 7testing Components

C. Results of Simulation

The Packet Tracer implementation was validated through ping tests, traceroute commands, and connectivity verification across VLANs and routing domains. Key results are as follows:

1. IP Addressing and DHCP: All end devices successfully received dynamic IP addresses from DHCP pools. Manual testing confirmed no duplication or misconfiguration.
2. Routing Performance: Inter-domain routing between EIGRP and OSPF areas functioned seamlessly. Convergence time during simulated link failures remained below 5 seconds, indicating fast recovery.
3. VLAN and Inter-VLAN Routing: Devices within the same VLAN communicated efficiently, while inter-VLAN communication was successfully enabled through the L3 switch.
4. Security and Access Control: ACL rules were validated by restricting student VLAN devices from accessing administrative servers, while faculty retained full access. SSH-based remote management provided secure login compared to Telnet.
5. Redundancy and Reliability: EtherChannel successfully aggregated dual links, increasing throughput, while STP blocked redundant paths, ensuring loop-free topologies.
6. Wireless Integration: Wireless clients authenticated via WPA2 security and accessed both internal servers and internet resources through NAT and VPN tunneling. Here diagram should be shown and then merge this diagram with the previous one diagram

D. Discussion

The Packet Tracer simulation validated that the proposed CAN design meets the objectives of scalability, efficiency, and security. Compared to traditional flat LAN deployments, the hierarchical CAN model improved bandwidth utilization, fault tolerance, and traffic segmentation.

- Scalability: VLANs and hierarchical IP addressing allowed logical growth without reconfiguration overhead.
- Security: The combination of ACLs, SSH, NAT, and VPN provided a multi-layer defense strategy, significantly improving protection over legacy Telnet-based networks.
- Reliability: EtherChannel and STP enhanced redundancy, ensuring continuous service even under link failure scenarios.
- Performance: Performance: Redirecting the routes between OSPF and EIGRP allowed compatibility, an important necessity in nonhomogeneous settings like universities.

Altogether, the findings validate the fact that the suggested CAN architecture, applied to Packet Tracer, provides an efficient, scalable, and secure solution to academic and enterprise campuses.

VI. Conclusion and Future Work

As the design and implementation of the Campus Area Network (CAN) as presented in this paper illustrates, it is possible to develop a Campus Area Network architecture that is secure, scalable, and efficient in both academic and enterprise infrastructures. The proposed CAN would simplify communications and redundancy within departmental networks through hierarchical IP addressing, DHCP automation, advanced routing protocols (EIGRP and OSPF with route redistribution) and, therefore, enhance optimality of communication. The security of the network was enhanced using SSH, ACLs, NAT, and VPN integra on, and the fault tolerance and loop prevention were introduced with EtherChannel and STP. The real-life testing and testing within Cisco Packet Tracer were valid and showed connectivity, bandwidth optimization that works on, and policy enforcement works across several departments. Although the results are encouraging, there are still some limitations. Packet Tracer can offer a simulation setting which is useful in design testing, but does not fully scale to the real world, scalability issues, hardware constraints or unpredictable traffic norms. Additionally, the study primarily focused on wired and WLAN integration, leaving emerging technologies such as Software-Defined Networking (SDN) and cloud-based controllers outside its scope.

For future work, the implementation of SDN-based controllers could further enhance network programmability and adaptability in large-scale CAN

deployments. Similarly, the integration of Next-Generation Firewalls (NGFWs), Intrusion Detection and Prevention Systems (IDPS), and Zero Trust Architectures can strengthen security against advanced cyber threats. Expanding validation to real hardware testbeds and hybrid cloud environments will provide deeper insights into performance, resilience, and scalability. Furthermore, the adoption of Artificial Intelligence (AI) and Machine Learning (ML) techniques for predictive traffic analysis, anomaly detection, and automated fault recovery presents a promising direction for future research.

REFERENCES

[1] B. A. Forouzan, Data Communications and Networking, 5th ed. New York, NY, USA: McGraw-Hill, 2017.
[2] A. S. Tanenbaum and D. J. Wetherall, Computer Networks, 5th ed. Upper Saddle River, NJ, USA: Pearson, 2013.
[3] W. Stallings, Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Boston, MA, USA: Addison-Wesley, 2021.
[4] J. F. Kurose and K. W. Ross, Computer Networking: A Top-Down Approach, 8th ed. Boston, MA, USA: Pearson, 2021.
[5] D. E. Comer, Internetworking with TCP/IP: Principles, Protocols, and Architecture, 7th ed. Boston, MA, USA: Pearson, 2018.
[6] Cisco Systems, Internetworking Technologies Handbook. Indianapolis, IN, USA: Cisco Press, 2020.
[7] O. Hucaby, CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Indianapolis, IN, USA: Cisco Press, 2015.
[8] J. Davidson, J. Froom, and M. Valdovinos, Cisco LAN Switching Fundamentals. Indianapolis, IN, USA: Cisco Press, 2018.
[9] W. L. Stallings, Data and Computer Communications, 10th ed. Upper Saddle River, NJ, USA: Pearson, 2014.
[10] T. Lammle, CCNA Routing and Switching Complete Study Guide, 2nd ed. Indianapolis, IN, USA: Wiley, 2016.
[11] A. V. Phatak, "Optimized loop-free networking using spanning tree enhancements," IEEE Communications Surveys & Tutorials, vol. 20, no. 2, pp. 1503–1525, 2018.
[12] Cisco Systems, Cisco Networking Basics. San Jose, CA, USA: Cisco Press, 2019.
[13] G. T. Heineman and W. T. Councill, Software Engineering Tools for Networking and Diagnostics. Cambridge, MA, USA: MIT Press, 2020.
[14] B. A. Forouzan, Data Communications and Networking, 5th ed. New York, NY, USA: McGraw-Hill, 2017.
[15] W. Stallings, Data and Computer Communications, 10th ed. Upper Saddle River, NJ, USA: Pearson, 2014.
[16] A. S. Tanenbaum and D. J. Wetherall, Computer Networks, 5th ed. Upper Saddle River, NJ, USA: Pearson, 2013.
[17] J. F. Kurose and K. W. Ross, Computer Networking: A Top-Down Approach, 8th ed. Boston, MA, USA: Pearson, 2021.
[18] Cisco Systems, Internetworking Technologies Handbook. Indianapolis, IN, USA: Cisco Press, 2020.
[19] O. Hucaby, CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Indianapolis, IN, USA: Cisco Press, 2015.
[20] D. E. Comer, Internetworking with TCP/IP: Principles, Protocols, and Architecture, 7th ed. Boston, MA, USA: Pearson, 2018.
[21] T. Lammle, CCNA Routing and Switching Complete Study Guide, 2nd ed. Indianapolis, IN, USA: Wiley, 2016.
[22] G. T. Heineman and W. T. Councill, Software Engineering Tools for Networking and Diagnostics. Cambridge, MA, USA: MIT Press, 2020.
[23] H. Subramanian, "Static vs. dynamic routing protocols in enterprise networks," IEEE Network, vol. 32, no. 6, pp. 45–51, 2018.
[24] J. Moy, OSPF: Anatomy of an Internet Routing Protocol. Reading, MA, USA: Addison-Wesley, 1998.
[25] K. A. Awan, M. F. Khan, and S. U. Khan, "Route redistribution challenges in heterogeneous campus networks," IEEE Access, vol. 9, pp. 12045–12056, 2021.

[26] W. Stallings, Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Boston, MA, USA: Addison-Wesley, 2021.
[27] J. Davidson, J. Froom, and M. Valdovinos, Cisco LAN Switching Fundamentals. Indianapolis, IN, USA: Cisco Press, 2018.
[28] C. Kaufman, R. Perlman, and M. Speciner, Network Security: Private Communication in a Public World, 3rd ed. Upper Saddle River, NJ, USA: Pearson, 2016.
[29] D. Hucaby, Cisco LAN Switching Fundamentals, 2nd ed. Indianapolis, IN, USA: Cisco Press, 2019.
[30] A. V. Phatak, "Optimized loop-free networking using spanning tree enhancements," IEEE Communications Surveys & Tutorials, vol. 20, no. 2, pp. 1503–1525, 2018.
[31] S. S. Kompella and R. K. Sahoo, "Scalable VLAN architectures for campus networks," IEEE Communications Magazine, vol. 49, no. 7, pp. 112–118, 2011.
[32] Cisco Systems, Packet Tracer Simulation Tool. San Jose, CA, USA: Cisco Press, 2020. [33] R. Gill, "Network diagnostics and performance evaluation using simulation-based tools," IEEE Access, vol. 8, pp. 175901–175910, 2020.
[34] M. A. Alsmadi and A. A. Zarour, "Emulation-based validation of campus networks: A performance study," IEEE Transactions on Education, vol. 64, no. 3, pp. 345–353, 2021.