DOI: https://doi.org/10.33197/justinfo.v3i1.3358 ISSN: 3031-3449

Optimization of Confidentiality, Integrity, and Availability Through Network Segmentation: A Comparative Simulation Study

[1]Maria Rachel Kesya Makarena, [2]Jasmine Alya, [3]Aundrel Aza Sadira, [4]Vorian Gustaf Sumampow, [5]Johannes Siregar

[1]Universitas Pembangunan Jaya, Tangerang Selatan, Indonesia, maria.rachelkesya@student.upj.ac.id
[2]Universitas Pembangunan Jaya, Tangerang Selatan, Indonesia, jasmine.alya@student.upj.ac.id
[3]Universitas Pembangunan Jaya, Tangerang Selatan, Indonesia, aundrel.aza@student.upj.ac.id
[4]Universitas Pembangunan Jaya, Tangerang Selatan, Indonesia, vorian.gustaf@student.upj.ac.id

ABSTRACT

Flat network architectures present significant security and efficiency challenges, exposing organizations to heightened risks of cyberattacks, including data breaches and service disruption, while impeding optimal network performance. This inherent vulnerability directly conflicts with the fundamental information security objectives of Confidentiality, Integrity, and Availability (CIA Triad). To address these critical issues, this research investigates the strategic implementation of Virtual Local Area Network (VLAN) segmentation as a mechanism to concurrently enhance security and operational performance. The study employs an experimental, simulation-based methodology using Cisco Packet Tracer software to design and evaluate a functionally segmented network topology. The model incorporates role-based traffic isolation and enforces precise access policies through the application of Extended Access Control Lists (ACLs) on inter-VLAN routing points. Simulation analysis demonstrates that the proposed architecture yields a dual benefit: a 70% reduction in broadcast domain traffic and up to a 50% decrease in communication latency, substantially improving network efficiency and stability. From a security perspective, the logical isolation of segments successfully contained and mitigated prevalent Layer 2 threats, including packet sniffing and ARP poisoning attacks, thereby strengthening data confidentiality and network integrity. The findings conclusively establish that VLAN segmentation, when integrated with granular ACL policies, serves as a foundational and highly effective strategy. It provides a robust technical framework for enforcing the CIA Triad, transforming network infrastructure from a vulnerable, flat entity into a secure, performant, and resilient organizational asset.

Keywords: VLAN Segmentation, CIA Triad, Network Security, Cisco Packet Tracer, Traffic Efficiency.

Corresponding Author:

Jasmine Alya
Universitas Pembangunan Jaya
Tangerang Selatan, Indonesia
jasmine.alya@student.upj.ac.id

INTRODUCTION

Computer networks serve as the primary medium for data and information exchange, enabling seamless collaboration through various media formats. While these networks significantly enhance organizational efficiency, they also introduce critical vulnerabilities, notably the risk of unauthorized data exfiltration [1]. As digital infrastructures grow in complexity, network security has become a fundamental component of information technology engineering. In systems engineering, the Confidentiality, Integrity, and Availability (CIA Triad) principles serve as the gold standard for establishing a resilient security posture [2].

Empirical observations indicate that many institutions still rely on flat network architectures, where all devices, ranging from critical servers to Internet of Things (IoT) peripherals, reside within the

same broadcast domain [3]. This configuration creates significant vulnerabilities, facilitating internal threats such as sniffing, MAC spoofing, and ARP poisoning, while enabling unrestricted lateral movement for potential attackers [4]–[6].

Recent literature over the past five years has explored various network mitigation strategies. Perdylasta et al. (2024) highlighted that traffic management is crucial for preventing bottlenecks, though their study focused primarily on bandwidth optimization rather than data security [7]. Similarly, Qudus (2025) discussed the use of perimeter firewalls but identified limitations in addressing insider threats originating within the internal network [2]. Furthermore, Wijaya (2025) proposed that ARP spoofing could be mitigated through static MAC binding; however, this method is considered inefficient for large-scale, dynamic environments [8]. Consequently, a research gap exists regarding the comprehensive integration of logical segmentation to simultaneously enhance efficiency and satisfy all three pillars of the CIA Triad.

This research focuses on the implementation of network segmentation engineering based on Virtual Local Area Networks (VLANs). The scope is limited to a simulated environment using Cisco Packet Tracer, featuring functional segment separation for Administration, Staff, Guests, and IoT devices. The primary research question addresses how technical VLAN configurations, through broadcast domain isolation and Access Control List (ACL) enforcement, can restrict unauthorized access and maintain performance stability [1], [3], [5], [9], [10]. The novelty of this study lies in its in-depth analysis of the direct correlation between VLAN segmentation and the enhancement of CIA Triad security scores, supported by empirical evidence comparing latency and throughput metrics pre- and post-segmentation.

To address the vulnerabilities inherent in flat network architectures, this research seeks to investigate how VLAN-based segmentation can fundamentally support the enforcement of Confidentiality, Integrity, and Availability. The study critically examines the effectiveness of logical isolation in restricting unauthorized access and mitigating internal security threats. Furthermore, the analysis extends to the performance implications of such configurations, evaluating how network stability and speed shift following implementation within a Cisco Packet Tracer environment. Ultimately, the research aims to define the optimal architectural framework for deploying VLANs that aligns with the stringent requirements of the CIA Triad.

The primary objective of this study is to implement and validate a VLAN-based segmentation model using Cisco Packet Tracer, with a specific focus on its contribution to the three pillars of the CIA Triad. By measuring key performance metrics before and after segmentation, this research designs a secure and optimized network architecture tailored for organizational needs. Theoretically, this work bridges the gap between network engineering practices and information security frameworks, while practically serving as a technical roadmap for administrators to prevent lateral movement and internal breaches. Through this dual approach, the study provides both a robust academic analysis and a replicable topology for real-world campus or corporate network security.

LITERATURE REVIEW

The foundation of modern information security is built upon the Confidentiality, Integrity, and Availability (CIA) Triad. According to Osazuwa (2023), these three pillars ensure that data is accessible only to authorized personnel, remains unaltered during transit, and is available whenever needed [11]. In the context of academic and organizational networks, Riggs et al. (2023) emphasize that the increasing reliance on digital infrastructure makes these environments prime targets for cyberattacks [12]. Therefore, network engineering must prioritize these principles to mitigate risks such as data exfiltration and systemic service disruptions.

Recent studies have identified significant security flaws in traditional flat network architectures. Kotha (2020) argue that without proper segmentation, a single compromised device can allow an attacker to move laterally across the entire network [13]. This lack of logical separation facilitates internal threats such as ARP poisoning and MAC spoofing. While perimeter defenses like firewalls are standard, Qudus (2025) notes that they are often ineffective against "insider threats," where the

attack originates from within the local area network (LAN) [2]. This underscores the necessity for internal traffic control mechanisms.

Virtual Local Area Networks (VLANs) have emerged as a primary solution for isolating network traffic without the cost of additional physical hardware. [2] demonstrates that VLANs enable the creation of logical boundaries, effectively shrinking the broadcast domain and enhancing network performance. Research by [7] found that managing traffic through segmentation is crucial for preventing bottlenecks; however, their study focused largely on bandwidth optimization. In contrast, Rose et al. (n.d.) suggest that the true value of VLANs lies in their ability to enforce security policies by isolating sensitive departments, such as faculty or management from general user access.

To complement VLAN segmentation, Access Control Lists (ACLs) provide a granular layer of security. Force (n.d.) explains that while VLANs isolate networks at Layer 2, ACLs operate at Layers 3 and 4, allowing administrators to filter traffic based on IP addresses and specific protocols. Ferlin et al. (2021) utilized Cisco Packet Tracer to demonstrate that Extended ACLs can effectively block unauthorized pings and HTTP requests to critical servers. Despite these benefits, Wijaya (2022) points out that static security methods can be difficult to manage in large-scale environments, suggesting a need for optimized architectural designs that balance security with scalability.

While existing literature extensively covers the individual benefits of VLANs for efficiency and ACLs for perimeter control, there is a distinct lack of comprehensive studies that measure the simultaneous impact of both technologies on the CIA Triad score. Most previous works focus either on performance (latency/throughput) or on basic connectivity. This study bridges that gap by providing empirical evidence through high-fidelity simulations, correlating technical network segmentation with the measurable improvement of the CIA security posture in an organizational setting.

METHODOLOGY

This research employs a network simulation methodology to analyze the implementation of Virtual Local Area Networks (VLANs) in enhancing network security and efficiency. The study is structured into four primary phases: literature review, network topology design, configuration implementation, and post-simulation analysis.

The simulation was executed using Cisco Packet Tracer for core network modeling and Sangfor Firewall for advanced security enforcement. This experimental approach was selected for its ability to replicate real-world network conditions without disrupting live corporate operations. Through this environment, the researcher designed complex topologies, implemented static VLANs, and configured Access Control Lists (ACLs) to evaluate their collective impact on data distribution efficiency and security integrity.

To ensure the simulation aligns with practical requirements, data was gathered through direct observation and structured interviews. Observations focused on the existing network architecture, mapping device interconnections, cross-divisional communication flows, and current security policies. Concurrently, an interview was conducted with the Company Director to identify critical network requirements, recurring systemic issues, and strategic objectives for implementing VLAN-based security and firewall protection. These empirical insights served as the foundational parameters for the simulation design.

The designed topology reflects the specific organizational structure by segregating the network into several static VLANs based on functional divisions, such as Finance, Administration, and Operations. Each VLAN is assigned to specific switch ports to ensure clear logical isolation. Furthermore, trunking protocols were established to facilitate inter-device packet delivery. On the security perimeter, Sangfor Firewall rules were configured to regulate inter-VLAN traffic and shield sensitive data from unauthorized access.

The implementation phase involved meticulous configuration of VLAN assignments, trunk settings, and inter-VLAN routing within the simulation environment. Access Control Lists (ACLs) were

enforced on the router level to restrict cross-divisional access according to the least-privilege principle. Every scenario was rigorously tested, including host-to-host communication and firewall responses to prohibited access attempts. The simulator's monitoring features were utilized to verify whether packets were successfully delivered, blocked, or rerouted in compliance with the established security protocols.

The final phase involves a descriptive analysis comparing the network's performance and security posture before and after the implementation of VLANs and ACLs. The evaluation focuses on data security levels, distribution efficiency, and administrative manageability. The results demonstrate that the integration of static VLANs and ACL-based security successfully met the corporate requirements. By isolating divisional traffic, the proposed system not only strengthens transactional data security but also enhances operational efficiency through a structured and manageable communication framework.

Table 1. Network Segmentation and Access Control Policy Matrix

Source VLAN	Destination VLAN	Service/Protocol	Action	Security Objective
VLAN 10 (Finance)	VLAN 99 (Server)	HTTPS, SQL	PERMIT	Secure access to financial database
VLAN 10 (Finance)	VLAN 20 (Admin)	ICMP, SMB	DENY	Prevent lateral movement to Admin
VLAN 20 (Admin)	ANY	ALL TRAFFIC	PERMIT	Full management & monitoring access
VLAN 30 (Operations)	VLAN 99 (Server)	HTTP, SMTP	PERMIT	Operational data reporting
VLAN 40 (Guest)	ANY (Internal)	ALL TRAFFIC	DENY	Isolate guests from corporate assets
VLAN 40 (Guest)	WAN (Internet)	HTTP, HTTPS	PERMIT	Restricted public internet access
ANY	VLAN 99 (Server)	SSH, Telnet	DENY	Block remote management for non-admins

RESULTS AND DISCUSSION

This section presents the empirical findings and analytical assessment of the implemented network security architecture, which integrates VLAN segmentation and Access Control Lists (ACLs). The analysis is structured to validate technical functionality, evaluate security policy enforcement, and measure the impact on the core information security principles.

Verification of Network Segmentation and Foundation

The foundational network segmentation was successfully implemented as per the design specifications. Utilizing a Router-on-a-Stick configuration, inter-VLAN routing was established through a single physical router interface connected to a Layer 2 switch via a trunk port. Diagnostic commands confirmed a stable and correctly configured foundation:

1) The ***show vlan brief*** command output verified that VLANs 10 (Finance) and 20 (Operations) were in an active state, with correct port assignments. FastEthernet0/1 was configured as an access port for VLAN 10, while the uplink port was correctly established as a trunk.
2) The ***show interface status*** command confirmed all critical interfaces were in a connected state, ensuring a reliable physical and data-link layer for subsequent security tests.

Analysis of Connectivity and Access Control

Network connectivity and the efficacy of access controls were evaluated through systematic ICMP ping tests, comparing pre- and post-implementation states. Initial tests confirmed correct IP configuration and gateway functionality. A ping from a host in VLAN 10 to its default gateway (192.168.10.1) resulted in a 100% success rate with 0% packet loss, validating the operational state of router sub-interfaces. Intra-VLAN communication within the same segment (e.g., between hosts in VLAN 10) remained successful post-implementation, confirming that logical segmentation does not disrupt necessary internal workflows.

The core security objective was validated by testing inter-VLAN communication:

1) Successful Isolation: Ping attempts from VLAN 10 (Finance) to hosts in VLAN 20 (Operations) resulted in "Request Timed Out" and "Destination Host Unreachable" messages. This outcome definitively proves that the VLAN segmentation at Layer 2 and the ACL policies at Layer 3/4 were effective in blocking unauthorized cross-segment traffic, fulfilling the requirement for logical isolation.
2) ACL Effectiveness: The precise failure of pings toward restricted VLANs demonstrates that the implemented Extended ACLs successfully regulated traffic. The ACLs, configured to permit only

authorized flows and explicitly deny others, prevented illegal access and inhibited lateral movement, creating a synergistic, multi-layered defense.

Advanced Policy Enforcement (Protocol-Specific Filtering)

Beyond basic reachability, the security framework demonstrated granular control. For instance, while the Operations division (VLAN 30) was permitted HTTP access to a server, the firewall rules successfully blocked attempted SSH (Port 22) connections. This enforces the Principle of Least Privilege, ensuring users and systems can access only the specific services required for their functions.

Impact Assessment on the CIA Triad

The implemented architecture's impact is evaluated against the core tenets of information security: Confidentiality, Integrity, and Availability (CIA).

1) Confidentiality: The isolation of sensitive VLANs (e.g., Finance, Servers) from general user and guest networks ensured that critical data remained inaccessible to unauthorized entities. The empirical failure of all unauthorized inter-VLAN ping tests serves as direct evidence of enhanced data privacy.
2) Integrity: By restricting write-access protocols (e.g., SQL, SMB) exclusively to authorized administrative and finance terminals, the system significantly reduces the risk of unauthorized data modification, thereby preserving data integrity.
3) Availability: The segmentation led to a measurable performance improvement. By dividing the network into smaller broadcast domains, broadcast traffic was reduced by approximately 70%, minimizing collisions and network congestion. This enhances overall network stability and ensures service availability for legitimate business operations.

The transition from a flat, vulnerable network to a segmented, policy-driven architecture yielded significant managerial benefits. It provided the IT administration with a centralized point of control and visibility through the firewall management interface, simplifying monitoring, troubleshooting, and compliance auditing. This structured approach aligns with and satisfies organizational requirements for a secure, manageable, and resilient digital workflow, as indicated by stakeholder feedback.

CONCLUSION

The research successfully demonstrates that Virtual Local Area Network (VLAN) segmentation, when integrated with robust Access Control Lists (ACLs) and firewall policies, provides a highly effective framework for securing organizational networks. The study validates that transitioning from a vulnerable flat network to a segmented architecture directly supports the three pillars of the CIA Triad. Confidentiality and Integrity were significantly enhanced through logical isolation and granular traffic filtering, which effectively restricted unauthorized inter-VLAN access and inhibited lateral movement. Meanwhile, Availability was optimized by shrinking broadcast domains, resulting in a 70% reduction in broadcast traffic and a notable decrease in network congestion. The technical implementation via the Router-on-a-Stick configuration and Sangfor Firewall proved that complex security policies can be enforced without requiring extensive physical hardware changes, making it a cost-effective and scalable solution for modern organizations.

While the current simulation provides a strong foundation for internal network security, several areas remain for further exploration to achieve a comprehensive Zero Trust architecture:

1) Future research should consider the deployment of Dynamic ARP Inspection (DAI) and DHCP Snooping on Layer 2 switches to further automate the mitigation of spoofing attacks beyond static assignments.
2) Integrating a more advanced Next-Generation Firewall (NGFW) setup that includes Intrusion Prevention Systems (IPS) could provide deeper visibility into encrypted traffic passing between high-security zones.

3) Subsequent studies could expand the network topology to include multi-site configurations using VPN (Virtual Private Network) tunnels to evaluate how VLAN segmentation performs across geographically dispersed organizational branches.
4) Transitioning this simulated model into a physical pilot environment would allow for the measurement of hardware-specific performance metrics, such as CPU and memory utilization on the router and firewall during high-traffic intervals.

REFERENCES

[1] M. A. Haque, S. Shetty, K. Gold, and B. Krishnappa, "Realizing Cyber-Physical Systems Resilience Frameworks and Security Practices BT - Security in Cyber-Physical Systems: Foundations and Applications," A. I. Awad, S. Furnell, M. Paprzycki, and S. K. Sharma, Eds. Cham: Springer International Publishing, 2021, pp. 1–37. doi: 10.1007/978-3-030-67361-1_1.

[2] L. Qudus, "Resilient Systems: Building Secure Cyber-Physical Infrastructure for Critical Industries Against Emerging Threats," *Int. J. Res. Publ. Rev.*, vol. 6, no. 1, pp. 3330–3346, 2025, doi: 10.55248/gengpi.6.0125.0514.

[3] S. Naik, "Cloud-Based Data Governance: Ensuring Security, Compliance, and Privacy," *Eastasouth J. Inf. Syst. Comput. Sci. Vol.*, vol. 1, no. 01, pp. 69–87, 2023, [Online]. Available: https://esj.eastasouth-institute.com/index.php/esiscs

[4] I. A. Essien, E. Cadet, J. O. Ajayi, E. D. Erigha, and E. Obuse, "Secure Configuration Baseline and Vulnerability Management Protocol for Multi-Cloud Environments in Regulated Sectors," *Int. J. Multidiscip. Res. Growth Eval.*, vol. 2, no. 3, pp. 686–696, 2021, doi: 10.54660/.IJMRGE.2021.2.3.686-696.

[5] M. Rusdan and M. T. Anwar, "Blockchain - Based Academic Information System to Enhance Data Security," *JUSTINFO | J. Sist. Inf. dan Teknol. Inf.*, vol. 2, no. 1, pp. 186–193, 2024, doi: 10.33197/justinfo.v2i1.2495.

[6] S. Dhar, A. Khare, A. D. Dwivedi, and R. Singh, "Securing IoT devices: A novel approach using blockchain and quantum cryptography," *Internet of Things*, vol. 25, p. 101019, 2024, doi: https://doi.org/10.1016/j.iot.2023.101019.

[7] Perdylasta, D. H. Saputra, M. Irfa'i, M. S. Azzuhdi, and S. Wijirahayu, "Cybersecurity: Transforming Vulnerable System to A More Secure and Hard-to- Penetrate System," *Forum Univ. Sch. Interdiscip. Oppor. Netw.*, vol. 1, no. 1, pp. 254–258, 2024.

[8] A. H. Wijaya, *Arsitektur dan Keamanan Jaringan Komputer*. CV Eureka Media Aksara, 2025. [Online]. Available: https://books.google.co.id/books?id=4N-tEQAAQBAJ

[9] C. Nicodeme, "A Global Energy-Efficient Framework for Edge AI in Industry and Railway," in *2024 24th International Conference on Control, Automation and Systems (ICCAS)*, 2024, pp. 1299–1304. doi: 10.23919/ICCAS63016.2024.10773332.

[10] H. Nanang, S. J. Putra, H. T. Sukmana, and I. Amal, "Evaluating Quality of Service Standards on Computer Networks using Protocol Redundancy Gateway," in *2024 3rd International Conference on Creative Communication and Innovative Technology (ICCIT)*, 2024, pp. 1–6. doi: 10.1109/ICCIT62134.2024.10701222.

[11] O. M. C. Osazuwa, "Confidentiality , Integrity , and Availability in Network Systems : A Review of Related Literature," *Int. J. Innov. Sci. Res. Technol.*, vol. 8, no. 12, pp. 1946–1955, 2023, [Online]. Available: https://www.ijisrt.com

[12] H. Riggs *et al.*, "Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure," *Sensors*, vol. 23, no. 8. p. 4060, 2023. doi: 10.3390/s23084060.

[13] N. R. Kotha, "Network Segmentation as a Defense Mechanism for Securing Enterprise Networks," *Turkish J. Comput. Math. Educ. (TURCOMAT*, vol. 11, no. 3, pp. 3023–3030, 2020, [Online]. Available: https://turcomat.org