2026 Volume: 02 Issue: 06 www.ijrpa.com ISSN 2456-9995 Research Article

International Journal Research Publication Analysis

Page: 01-13

VIRTUAL LOCAL AREA NETWORK IN A SIMULATED CAMPUS NETWORK

***Muhammad Auwal Ibrahim**

Department of Computer Studies College of Science and Technology Hassan Usman Katsina Polytechnics.

Article Received: 13 May 2026
Article Revised: 03 June 2026
Published on: 23 June 2026

***Corresponding Author: Muhammad Auwal Ibrahim**
Department of Computer Studies College of Science and Technology Hassan Usman Katsina Polytechnics.

DOI: https://doi-doi.org/101555/ijrpa.2363

ABSTRACT

The implementation of Virtual Local Area Networks (VLANs) is essential for optimizing performance, security, and management in campus networks. Many campus networks operate on a single broadcast domain where all users share the same network. This causes congestion, security issues, and poor performance. Managing such networks becomes harder as the number of users increases. This research focuses on designing and implementing VLANs in a simulated campus environment using Cisco Packet Tracer. The study analyzed typical network challenges, including congestion, broadcast traffic, and security risks in flat network structures. A hierarchical network design was adopted, with VLANs assigned to three departments: Administration, Staff, and Students. Inter-VLAN routing, IP addressing, trucking, and cloud service integration were implemented and tested. The results demonstrated improved traffic management, secure communication between departments, and enhanced network scalability. This project confirms the effectiveness of VLANs in educational institutions and provides a practical framework for future network expansion, security enhancement, and performance optimization.

KEYWORDS: Inter-Vlan, Czmpus, simulation, Packet Tracer.

1. INTRODUCTION

Computer networks are vital in today's educational and business environments. They allow sharing of resources such as printers, files, and internet connections among multiple users. However, as the number of connected devices increases in a campus setting, managing a single flat network becomes challenging. Large networks without segmentation often suffer from congestion, security risks, and broadcast storms that slow down communication (Al-Khaffaf& Al-Hamiri, 2021). To overcome these issues, network administrators use **Virtual Local Area Networks (VLANs)**, which allow logical grouping of users and devices based on function or department rather than physical location.

A VLAN divides a single physical network into multiple logical networks. Each VLAN functions as an independent broadcast domain, meaning that network traffic from one VLAN does not affect another. This helps reduce unnecessary traffic, enhances performance, and increases network security by controlling access between groups *(Makeri et al., 2021).* For instance, in a campus network, students, lecturers, and administrative staff can be placed in different VLANs to limit unauthorized access to sensitive information. VLANs also make it easier to manage users when they move from one department or building to another since their network policies can move with them.

In recent years, the use of VLANs has become an important topic in both education and research. Simulation tools like Cisco Packet Tracer and OPNET Modeler have made it possible to design, configure, and analyze VLAN networks in a safe virtual environment *(Ingale&Bakhtar, 2024).* These tools help students understand how VLANs work and how they can be applied in real-world networks. Through simulation, one can test the effects of VLANs on network performance by measuring factors such as delay, throughput, and packet loss. This provides valuable insight into how VLANs improve efficiency without requiring expensive hardware.

Moreover, VLANs improve network security by isolating traffic between different groups. For example, students in a university network should not have direct access to the finance or staff networks. By separating them into VLANs, administrators can apply access control and firewall rules to protect sensitive data *(Madavarapu et al., 2023)*. VLANs also support features like **Quality of Service (QoS)**, which ensures that important applications such as online classes or video conferences get priority bandwidth over less critical traffic. This makes VLANs suitable for modern campus networks that depend heavily on cloud-based and multimedia services.

Finally, implementing VLANs in a simulated campus network provides a practical way to study and understand network segmentation, security, and performance improvement. It allows learners to test configurations, identify design errors, and analyze the results before applying the design to real equipment. This project, therefore, aims to design and implement VLANs in a simulated campus network to demonstrate how VLAN technology can improve efficiency, security, and scalability in academic institutions *(Zainol et al., 2024).*

2. Review of Related Literature

One of the key concept guiding thisresearch is the **Hierarchical Network Model**, which divides the network into core, distribution, and access layers. In this model, VLANs are usually implemented at the access layer to segment end devices, while inter-VLAN routing occurs at the distribution layer. This structure improves network efficiency by reducing bottlenecks and helping administrators apply security policies at different layers of the hierarchy (Ingale&Bakhtar, 2024). The combination of VLANs and hierarchical design supports scalability, which is essential in campus networks where user populations frequently grow.

The framework further incorporates the concept of **broadcast domain control**, which is central to VLAN functionality. A broadcast domain is a part of the network where devices receive broadcast messages from one another. Large broadcast domains often lead to traffic congestion, reduced performance, and security risks. VLANs address this by dividing a single physical network into multiple logical broadcast domains. This segmentation isolates traffic and improves network stability, making it especially valuable in campus environments with many users (Al-*Khaffaf& Al-Hamiri, 2021).*

Another theoretical component is **network segmentation for security enhancement**. VLANs allow administrators to separate users based on roles or departments, ensuring that sensitive systems—such as administrative or financial units—are isolated from general student traffic. This segmentation limits unauthorized access and protects confidential information. Research shows that VLAN-based segmentation is one of the simplest and most cost-effective methods of improving network security in educational institutions *(Madavarapu et al., 2023).*

The framework also draws from **routing and switching theories**, which explain the interaction between Layer 2 VLANs and Layer 3 routing devices. VLANs require a routing mechanism, commonly known as inter-VLAN routing, to enable communication between network segments. Devices such as routers-on-a-stick or Layer 3 switches make this possible by directing traffic across VLAN boundaries. Understanding this theoretical foundation allows network designers to plan addressing schemes and routing tables that match the needs of each VLAN (Zainol et al., 2024).

Furthermore, the conceptual framework includes the idea of **Quality of Service (QoS)**, which ensures efficient handling of different types of traffic in VLAN-based networks. For instance, classrooms relying on video conferencing or online learning platforms require higher priority compared to casual student browsing. VLAN segmentation supports QoS policies by grouping users with similar needs and controlling traffic more effectively. Studies demonstrate that VLANs enable network administrators to apply differentiated services that enhance performance for critical applications *(Makeri et al., 2021).*

Another important concept is the **client-server model**, which explains how network services (such as DHCP, DNS, and web servers) operate inside VLAN environments. VLANs often require servers to respond to clients across different subnets, which means DHCP relay and inter-VLAN routing must be properly configured. Researchers argue that understanding the client-server interaction is crucial for designing campus networks that depend on multiple servers for authentication, internet services, and academic platforms *(Ingale&Bakhtar, 2024).*

The conceptual framework also integrates the principles of **logical vs. physical network design**. A VLAN network shows that logical architecture can differ significantly from physical wiring. Devices connected to the same switch may belong to different VLANs, while devices in the same VLAN may be located in different buildings. This flexibility improves mobility and simplifies network management in environments where users frequently change locations. Scholars emphasize that this separation of logical and physical concepts is one of the major advantages of VLAN-based design *(Al-Khaffaf& Al-Hamiri, 2021).*

Finally, modern network architecture includes the concept of **simulation-based design**, which frames how VLAN structures are studied before real-world implementation. Simulation tools such as Packet Tracer and OPNET allow designers to test topologies, evaluate performance, and identify weaknesses without deploying physical hardware. This aligns with constructivist learning theories that emphasize hands-on practice and iterative design. Researchers support simulation as a valid conceptual approach for teaching and analyzing network behavior

2.1 Networking Protocols and Addressing (IPv4 vs. IPv6)

Networking protocols play an essential role in how VLANs operate and communicate within a campus network. Most VLAN implementations still rely heavily on **IPv4**, the traditional addressing system used in computer networks for decades. IPv4's simplicity and widespread adoption make it the default choice for configuring VLAN interfaces, subnetting, and inter-VLAN routing in many institutions. Because of its compatibility with older and newer devices, IPv4 remains the standard option in simulation tools like Packet Tracer, which makes it useful for academic projects and training environments

Although IPv4 remains dominant, **IPv6** has become increasingly relevant due to the exhaustion of IPv4 addresses. IPv6 offers a larger address space, improved routing efficiency, and enhanced security features. However, IPv6 adoption has been slower in educational networks because many campuses rely on legacy infrastructure that does not yet support full IPv6 deployment. Studies show that while IPv6 offers long-term scalability, IPv4 is still preferred in practical VLAN configurations because it is easier to teach, configure, and troubleshoot (Madavarapu et al., 2023).

Another important aspect of networking protocols is the use of **subnetting** when assigning IP addresses to VLANs. Each VLAN typically requires its own subnet to ensure proper segmentation and routing. Subnetting simplifies network management by allowing administrators to allocate address ranges based on the size and needs of user groups. Proper IPv4 subnetting reduces address wastage and improves routing performance, making it ideal for campus networks with multiple departments *(Makeri et al., 2021).*

Furthermore, networking protocols determine how inter-VLAN traffic flows. Inter-VLAN routing uses protocols such as **Static Routing**, **RIPv2**, **OSPF**, or simple router-on-a-stick configurations. Research indicates that for small or medium-sized campus networks, static routing is often sufficient due to its simplicity and predictability. Larger networks benefit from dynamic routing protocols like OSPF, which automatically adjust to changes in the topology and ensure faster convergence. The choice of protocol affects overall performance and reliability.

Both IPv4 and IPv6 rely on **address resolution mechanisms**, but they operate differently. IPv4 uses ARP (Address Resolution Protocol), while IPv6 uses NDP (Neighbor Discovery Protocol). In VLAN-based networks, ARP broadcasts can create unnecessary traffic if not properly segmented. VLANs reduce this overhead by limiting ARP broadcasts to specific broadcast domains. Researchers emphasize that broadcast control is one of the primary ways VLANs improve performance in large campus environments (Al-Khaffaf& Al-Hamiri, 2021).

In addition, DHCP (Dynamic Host Configuration Protocol) plays a fundamental role in managing IP address assignments within VLANs. DHCP servers must be configured with separate pools for each VLAN, and DHCP relay must be enabled to allow devices in different VLANs to communicate with the DHCP server via Layer 3 devices. Studies show that misconfigured DHCP settings are one of the most common causes of network failure in instructional labs, highlighting the importance of understanding IPv4/IPv6 addressing within VLANs (Zainol et al., 2024).

Network security is another factor influenced by addressing protocols. IPv6 includes built-in features such as IPsec, which strengthens authentication and encryption. However, security studies show that many institutions still rely on IPv4-based security policies, VLAN ACLs (Access Control Lists), and port security features to safeguard traffic between departments. VLAN-based segmentation combined with IPv4 ACLs has proven highly effective in limiting unauthorized access to sensitive campus resources (Madavarapu et al., 2023). This demonstrates that a secure VLAN design depends on both proper addressing and well-configured protocols.

Finally, the choice between IPv4 and IPv6 influences network scalability. For educational institutions that plan significant future expansion, IPv6 offers a more sustainable addressing structure. However, because simulation tools and coursework still focus predominantly on IPv4, most student projects—including this one—use IPv4 for VLAN addressing. Researchers agree that IPv4 remains practical for teaching foundational networking skills, while IPv6 continues to gain attention for advanced training and large-scale deployments (Makeri et al., 2021)

2.2 Design-Based Approach to Network Implementation

Empirical research methods are widely used in networking studies to measure the performance of specific technologies, including VLANs. These methods involve collecting data through experiments, simulations, or real-world observations. In VLAN-related research, empirical methods may include measuring latency, throughput, packet loss, or broadcast traffic before and after VLAN deployment. Scholars state that empirical methods help researchers evaluate how VLAN segmentation improves network efficiency under controlled conditions (Al-Khaffaf& Al-Hamiri, 2021).

Another important research method used in VLAN implementations is the **experimental approach**, which involves testing different network configurations to observe their behavior. For example, experiments may compare the performance of a flat network to that of a VLAN-segmented network using tools like Packet Tracer or GNS3. Researchers emphasize that experimental methods provide reliable insights because they rely on systematic manipulation of variables such as routing protocols, switching modes, and trunking configurations (Madavarapu et al., 2023).

The **design-based approach** is especially relevant to network implementation projects. This approach focuses on developing a structured network design that includes topology planning, IP addressing schemes, VLAN grouping, trunk configuration, and security policies. Unlike empirical methods that primarily measure performance, the design-based method aims to create an optimized solution that meets user requirements. Literature shows that design-based approaches are particularly effective in campus network environments because they support scalability and ease of management

In addition to empirical and design methodologies, some studies adopt a **comparative analysis method**. This method involves evaluating multiple network designs or protocols to determine which performs better under specific conditions. For example, a study may compare the use of static versus dynamic VLAN assignment, or analyze the effect of different routing protocols on inter-VLAN communication. Comparative analysis allows researchers to choose the most effective configuration for a given environment, enhancing the decision-making process for networkdesigners .

Finally, the use of **simulation-based methodology** supports both empirical analysis and design validation. Simulation tools allow researchers to create realistic network environments where VLANs can be implemented, tested, and analyzed without deploying physical devices. Studies from recent years confirm that simulation offers a controlled and cost-effective way to test multiple scenarios, making it ideal for academic institutions and training programs. This method is particularly useful for evaluating how VLANs enhance security, reduce congestion, and improve network performance (Zainol et al., 2024).

3. Research Method Adopted

This research adopts a **simulation-based design methodology**, which is widely recognized as effective for teaching and evaluating computer networks. Simulation tools provide a safe and controlled environment for testing configurations without the cost of physical devices. Researchers support simulation as a feasible approach for analyzing VLAN performance because it allows repeated testing, controlled traffic generation, and visualization of packet flow

The method is also chosen because it aligns with the recommendations of prior studies that emphasize hands-on learning and the ability to analyze different configurations quickly. Furthermore, simulation facilitates accurate measurement of metrics such as throughput, delay, and packet delivery ratio, which are essential for evaluating the effectiveness of VLAN implementation (Zainol et al., 2024).

Finally, this methodology supports flexibility and iterative refinement, enabling adjustments to be made based on testing outcomes. As VLAN designs often require tuning—for example, modifying IP addressing, trunking, or access control—the ability to test and adjust configurations is essential. Using a simulation-driven design method, the project aligns with contemporary research practices that emphasize adaptability, cost-effectiveness, and hands-on experimentation in network studies (Zainol et al., 2024).

The research design adopted for this research is a design-based and simulation-focused study. This structure allows the network to be planned, designed, and implemented within a virtual environment using tools such as Cisco Packet Tracer. A design-based research design is appropriate because it focuses on constructing a practical solution, in this case a VLAN-segmented campus network, and then analyzing its behavior and performance. Scholars note that design-based approaches support hands-on experimentation and are ideal for networking studies that require testing of configurations without physical equipment (Ingale&Bakhtar, 2024).

The research method used is a practical, simulation-based implementation method. Rather than collecting data through surveys or questionnaires, this study relies on creating a fully functional simulated network environment. The method involves designing network topologies, assigning VLANs, configuring switches, implementing trunking protocols, and establishing inter-VLAN routing. This approach is commonly used in technical research where the emphasis is on demonstrating system functionality and evaluating the effects of configuration decisions (Madavarapu et al., 2023).

The simulation environment offers a realistic platform where network behavior can be observed under controlled conditions. This allows for testing different configurations such as access ports, trunk links, and routing protocols without the cost and complexity of physical devices. Researchers support simulation-based methods because they provide flexibility, repeatability, and safe experimentation with complex network scenarios (Zainol et al., 2024).

The chosen method is appropriate because the objective of the project is to design and implement VLANs within a controlled network environment**,** which is best achieved using simulation. This method provides the ability to model real-world network behavior and identify potential issues before applying the design in a physical setting. Using simulations ensures cost-effectiveness, as all configurations can be tested without purchasing actual switches, routers, or cables (Makeri et al., 2021).

Furthermore, simulation-based research reduces risks and enables iterative improvement. Errors in configuration can be easily identified and corrected, leading to a more stable and secure network design. Simulation also supports visual learning and enhances understanding of abstract networking concepts, making it an effective research method for academic and training purposes (Al-Khaffaf& Al-Hamiri, 2021).

4. Implementation of the Adopted Method

The first stage involved designing the network topology. A hierarchical structure was chosen, consisting of a core layer, distribution layer, and access layer. Devices such as switches, routers, and end-user systems were arranged to represent departments in a campus network such as Administration, Students, and Staff.

VLANs were assigned to each department, and an IP addressing scheme was created. For example, separate subnets were created for Student VLAN, Staff VLAN, and Admin VLAN, ensuring clear segmentation and improved traffic management.

4.1 Equipment Selection

Cisco Packet Tracer was selected as the simulation tool due to its accessibility, reliability, and wide use in networking research and training. Switches supporting VLAN and trunking configurations were chosen within the software environment.

Switches were configured with access ports, trunk ports (802.1Q), and VLAN assignments. Inter-VLAN routing was implemented using a router-on-a-stick method to enable communication between different VLANs when necessary.

4.2 Testing and Validation

Connectivity tests were conducted using tools like **ping**, **traceroute**, and Packet Tracer's simulation mode. Testing verified that devices within the same VLAN could communicate, while communication between different VLANs followed defined routing rules.

5. RESULT AND DISCUSSION

A system analysis was conducted to understand the networking needs of a typical campus environment. Most educational institutions rely on multiple user groups, including administrators, lecturers, and students, who access the network for different purposes. In many existing networks, devices are often placed in a single broadcast domain, which leads to unnecessary traffic, reduced performance, and potential security vulnerabilities. As a result, network segmentation using VLANs becomes essential to improve traffic flow control, safeguard sensitive information, and enhance overall network efficiency.

Performance analysis shows that student networks typically generate the highest traffic load because of online learning activities, multimedia usage, and internet browsing. Administrative networks, however, require stronger security and controlled access due to confidential data such as staff records, financial files, and examination processing. The system therefore must separate these traffic flows using VLANs while still maintaining controlled and secure inter-VLAN communication through routing.

Security needs are also a major consideration. Without segmentation, unauthorized access to administrative systems becomes more likely, and broadcast storms can disrupt the entire network. The proposed VLAN-based network must address these risks by ensuring proper isolation, minimizing broadcast domains, and enabling monitoring through authentication and access control mechanisms. This analysis highlights the necessity of adopting a structured and secure VLAN architecture in the campus network.

5.1 Design

The system design process involves developing both a physical and logical representation of the network. The **physical design** includes the layout of networking devices such as switches, routers, servers, and end-user systems across different departments. In this simulation, each department—Administration, Staff, and Students is assigned dedicated access switches connected to a central distribution switch, which in turn connects to a core router. This hierarchical design enhances scalability and simplifies VLAN management.

The **logical design** specifies how VLANs are assigned and how traffic flows between them. Each department is assigned a unique VLAN ID (e.g., VLAN 10 for Admin, VLAN 20 for Staff, VLAN 30 for Students). Trunk links using IEEE 802.1Q tagging are used between switches to ensure VLAN propagation across the network. Inter-VLAN routing is enabled through a router-on-a-stick configuration, allowing controlled communication between VLANs while maintaining isolation.

An IP addressing scheme was developed using private IPv4 addressing. Each VLAN receives its own subnet for example:

- VLAN 10 (Admin): 192.168.10.0/24
- VLAN 20 (Staff): 192.168.20.0/24
- VLAN 30 (Students): 192.168.30.0/24

This addressing plan ensures efficient traffic management and simplifies troubleshootingadditionally, a cloud service deployment plan is included to support functions such as online storage, backup, and e-learning platforms. Cloud services are logically integrated into the core network using simulated cloud connectors available in Packet Tracer.

This design allows users from different VLANs to securely access cloud resources based on defined access rules.

5.2 Implementation

The implementation stage involved building the network in Cisco Packet Tracer according to the system design. All switches were configured with VLAN assignments, access ports, and trunk ports. The router was configured with subinterfaces to support inter-VLAN routing using 802.1Q encapsulation. DHCP services were configured to dynamically assign IP addresses to devices within each VLAN. The cloud service components were connected through static routes, allowing controlled access.

Testing was conducted to ensure the system works as expected. Connectivity tests such as **ping**, **traceroute**, and Packet Tracer's real-time simulation mode were used to validate communication within each VLAN. Devices in the same VLAN successfully communicated, while devices in different VLANs required routing, confirming correct segmentation and routing policies. Security tests were also performed by attempting unauthorized access from one VLAN to another, verifying that access control configurations were effective.

5.3 Testing and Validation Procedures

1. **Broadcast Control Test:** Ensured that broadcast traffic remained contained within each VLAN.
2. **Inter-VLAN Routing Test:** Verified that only authorized departments could communicate through routing policies configured on the router.
3. **Cloud Access Test:** Confirmed that all VLANs could reach cloud services without breaching security rules.
4. **Performance Check:** Monitored network responsiveness to confirm improved traffic management after segmentation.

These procedures validated that the implemented VLAN network met the performance, security, and design requirements.

6. CONCLUSION

The research successfully demonstrated the design and implementation of VLANs within a simulated campus network environment using Cisco Packet Tracer. Through detailed system analysis, the study identified the major challenges associated with flat network structures, including excessive broadcast traffic, weak security, and limited scalability. These challenges were effectively addressed through VLAN segmentation, inter-VLAN routing, and hierarchical network design.

All project objectives were achieved. A functional VLAN-based network was designed, configured, and tested across multiple departments, illustrating improved performance and enhanced data security. The network design included clear VLAN assignments, logical addressing schemes, and the implementation of trunking and routing protocols. Testing confirmed that devices within the same VLAN could communicate efficiently while communication between different VLANs was securely controlled. The deployment of simulated cloud services further demonstrated how modern campuses can integrate online learning tools and storage platforms into their network architecture.

Overall, the simulated environment provided a practical and cost-effective platform for understanding VLAN concepts and validating the advantages of network segmentation in a campus setting. The results confirm that VLANs are essential for improving network structure, controlling broadcast domains, and enhancing security in modern educational environments.

REFERENCES

1. Makeri, Y. A., Cirella, G. T., Galas, F. J., Jadah, H. M., &Adeniran, A. O. (2021).Network performance through virtual local area network (VLAN) implementation & enforcement on network security for enterprise. *International journal of advanced networking and applications*, *12*(6), 4750-4762.
2. Makeri, Y. A., Cirella, G. T., Galas, F. J., Jadah, H. M., &Adeniran, A. O. (2021).Network performance through virtual local area network (VLAN) implementation & enforcement on network security for enterprise. *International journal of advanced networking and applications*, *12*(6), 4750-4762.
3. Madavarapu, J. B., Yalamanchili, R. K., &Mandhala, V. N. (2023, September).An ensemble data security on cloud healthcare systems.In *2023 4th International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 680-686).IEEE.
4. Zainol, D. A., Anuar, N. S., Halim, N. S. S. A., Kaur, M., Noordin, R., &Rahumatullah, A. (2024). Systematic review of strongyloidesstercoralis infection diagnosis in Southeast Asia: insights from parasitological, molecular, and serological approaches. *The American Journal of Tropical Medicine and Hygiene*, *111*(4), 724.
5. Al-Khaffaf, D. A. J., & Al-Hamiri, M. G. (2021).Performance evaluation of campus network involving VLAN and broadband multimedia wireless networks using OPNET

modeler. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *19*(5), 1490-1497.

6. Madavarapu, J. B., Yalamanchili, R. K., &Mandhala, V. N. (2023, September).An ensemble data security on cloud healthcare systems.In *2023 4th International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 680-686).IEEE.
7. Makeri, D., Odoki, M., Eilu, E., &Agwu, E. (2023). Update on prevalence and antimicrobial resistance of Staphylococcus aureus and Pseudomonas aeruginosa isolated from diabetic foot ulcers in Africa: a systematic review and meta-analysis. *Bulletin of the National Research Centre*, *47*(1), 145.
8. Roach, S. N. (2023). *Local and systemic innate immunity in viral infection and transmission at barrier surfaces* (Doctoral dissertation, University of Minnesota).
9. Al-Khaffaf, D. A. J., & Al-Hamiri, M. G. (2021).Performance evaluation of campus network involving VLAN and broadband multimedia wireless networks using OPNET modeler. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *19*(5), 1490-1497.
10. Makeri, Y. A., Cirella, G. T., Galas, F. J., Jadah, H. M., &Adeniran, A. O. (2021).Network performance through virtual local area network (VLAN) implementation & enforcement on network security for enterprise. *International journal of advanced networking and applications*, *12*(6), 4750-4762.