DOI: https://doi.org/10.33197/justinfo.v3i1.3379 ISSN: 3031-3449

Implementation of Virtual LANs (VLANs) for Academic Network Isolation Between Lecturer and Students

[1]Nathasa Rowen Frederika Abarua, [2]Ramadhan Alvito Alfian, [3]Rosa Putri Almaira, [4]Johannes Siregar
[1]Program Studi Sistem Informasi, Universitas Pembangunan Jaya, Tangerang Selatan, Indonesia, nathasa.rowenfrederika@student.upj.ac.id
[2]Program Studi Sistem Informasi, Universitas Pembangunan Jaya, Tangerang Selatan, Indonesia, ramadhan.alvitoalfian@upj.ac.id
[3]Program Studi Sistem Informasi, Universitas Pembangunan Jaya, Tangerang Selatan, Indonesia, rosa.putrialmaira@upj.ac.id
[4]Program Studi Sistem Informasi, Universitas Pembangunan Jaya, Tangerang Selatan, Indonesia, johannes.siregar@upj.ac.id

ABSTRACT

Network security is a critical aspect in academic environments where multiple user groups with different access privileges coexist within the same infrastructure. Inadequate network segmentation between lecturers and students can increase the risk of unauthorized access, data leakage, and disruption of academic services. This study aims to implement Virtual Local Area Network (VLAN) as a mechanism to isolate academic networks between lecturers and students in order to enhance network security. The research adopts an experimental approach using Cisco Packet Tracer to design and simulate VLAN-based network segmentation. VLAN 10 is assigned to the student network, while VLAN 20 is assigned to the lecturer network, each configured with distinct IP address ranges. Connectivity testing is conducted using ICMP ping to evaluate communication within the same VLAN and across different VLANs. The results show that communication within the same VLAN operates successfully, whereas communication between different VLANs is blocked, indicating effective network isolation. Furthermore, the implementation of VLAN supports the principles of Confidentiality, Integrity, and Availability (CIA Triad) by protecting sensitive academic data, preventing unauthorized data manipulation, and maintaining network service availability for authorized users. These findings demonstrate that VLAN-based segmentation is an effective and scalable solution for securing academic networks in higher education institutions.

Keywords: Virtual LAN, Network Security, Academic Network, Cisco Packet Tracer, Network Segmentation.

Corresponding Author:

Ramadhan Alvito Alfian
Program Studi Sistem Informasi, Universitas Pembangunan Jaya
Tangerang Selatan, Indonesia
ramadhan.alvitoalfian@upj.ac.id

INTRODUCTION

The advancement of information technology has compelled universities to rely on computer networks as the backbone of their academic systems, including online learning services, academic information systems, and the management of faculty and student data [1]–[5]. This high dependency necessitates adequate security management to protect academic data and services from diverse cyber threats [6]–[9]. Studies indicate that campus environments are particularly vulnerable to network attacks due to the high volume of users with varying access privileges and a lack of proper network segmentation (Seguela & Littlewood, 2020). Consequently, network security within university settings has become a critical issue that must be addressed systematically.

An academic network that lacks clear separation between faculty and students poses significant security risks, such as unauthorized access to sensitive data, leakage of academic information, and disruptions to system integrity. Faculty members typically require access to high-value data, including grades and evaluative materials, whereas students possess more restricted access rights [10]–[12]. This condition directly relates to potential violations of the core principles of information security:

Confidentiality, Integrity, and Availability (the CIA Triad). Confidentiality ensures that data is only accessible to authorized parties, Integrity maintains data accuracy, and Availability guarantees that network services remain accessible to legitimate users [13]–[16]. These three principles serve as the primary foundation for modern network security design.

One effective approach to enhancing network security without expanding physical infrastructure is the utilization of Virtual Local Area Networks (VLANs) [17]–[20]. A VLAN enables logical network separation on a single physical network device, allowing data traffic between user groups to be isolated according to established security policies. Prior research demonstrates that VLAN implementation can mitigate cross-network access risks, limit broadcast domains, and improve overall network efficiency and security [21], [22]. In a university context, VLANs can be employed to separate faculty and student networks, ensuring each group accesses only the resources appropriate to their roles. This approach aligns with segmentation-based security principles recommended in modern network management practices [23], [24].

Based on these issues, this study aims to implement a Virtual LAN (VLAN) as a mechanism for academic network isolation between faculty and students and to analyze its effectiveness in enhancing network security. Simulations are conducted using Cisco Packet Tracer to test communication between devices within the same and different VLANs [25]. This research is expected to provide empirical evidence regarding the role of VLANs in supporting the CIA Triad and serve as a reference for educational institutions in designing secure, efficient, and controlled academic networks [26].

METHODOLOGY

This study employs an experimental approach based on network simulation to implement and analyze Virtual Local Area Networks (VLANs) as a mechanism for academic network isolation between faculty and students. The simulation was conducted using Cisco Packet Tracer software to model network configurations and support a controlled testing process.

1) Topology Design and VLAN Schematics

At this stage, an academic network topology was designed to represent two primary user groups: students and faculty. The topology utilized a single distribution switch as the central hub, with each user group assigned to a distinct VLAN to ensure data traffic isolation.

VLAN 10 was designated for the student network, while VLAN 20 was assigned to the faculty network. Each VLAN utilized a different IP address segment to facilitate network identification and management. This design aimed to logically restrict communication between user groups without requiring additional physical infrastructure.

2) VLAN Configuration and IP Addressing

The configuration phase was performed via the Command Line Interface (CLI) on the switch within Cisco Packet Tracer. The configuration involved creating VLANs, assigning VLAN names, and grouping switch ports according to their respective VLAN assignments. The CLI command procedures were documented as evidence of the research implementation.

```
Switch>enable
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#do show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
10   Mahasiswa                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10
20   Dosen                             active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch(config)#
```

Figure 1. VLAN Configuration via CLI

Subsequently, each PC was configured with a static IP address corresponding to its assigned VLAN and network segment. This IP addressing scheme served as the foundation for testing network isolation in the following phase. Table 1 details the IP address configuration for each device used in the simulation.

Table 1. Device IP Address Configuration

PC	Department	VLAN	IP Address	Subnet Mask
PC-0	Students	10	192.168.10.1	255.255.255.0
PC-1	Students	10	192.168.10.2	255.255.255.0
PC-2	Students	10	192.168.10.3	255.255.255.0
PC-3	Lecturer	20	192.168.20.1	255.255.255.0
PC-4	Lecturer	20	192.168.20.2	255.255.255.0
PC-5	Lecturer	20	192.168.20.3	255.255.255.0

This configuration ensures that each device can only communicate within its respective VLAN segment, thereby supporting the research objective of creating academic network isolation.

RESULTS AND DISCUSSIONS

1) Lecturer and Student VLAN Configuration Results

In the implementation phase, the Virtual Local Area Network (VLAN) configuration was successfully deployed within the Cisco Packet Tracer simulation to segregate the academic network. Two VLANs were configured on the switch: VLAN 10 for students and VLAN 20 for faculty. Each switch port was assigned to its respective VLAN, ensuring that connected devices could only communicate within the same network segment.

The configuration output confirms that the VLANs are correctly registered and all switch ports are associated according to the designed network topology. This indicates that the logical network segmentation was executed successfully, and the system is ready for connectivity testing.

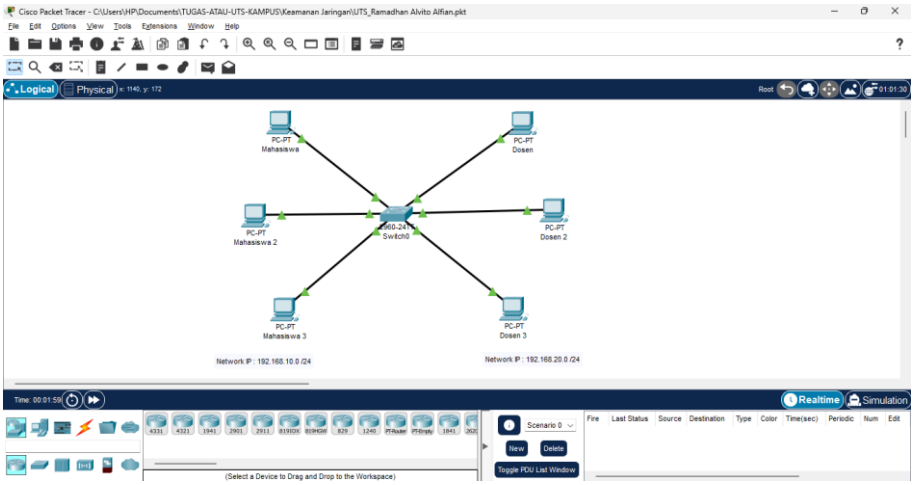

Figure 2. Faculty and Student VLAN Configuration Results in Cisco Packet Tracer

2) Network Connectivity Test Results

Connectivity testing was performed using the ping command to verify communication both within the same VLAN (Intra-VLAN) and across different VLANs (Inter-VLAN). This test aimed to ensure that the network remains functional within its segment while remaining properly isolated from other segments.

Intra-VLAN Communication (Student to Student) The initial test involved sending ICMP packets from a Student PC (192.168.10.1) to another Student PC (192.168.10.2) within VLAN 10. The results showed successful communication, indicated by the "Reply received" message.

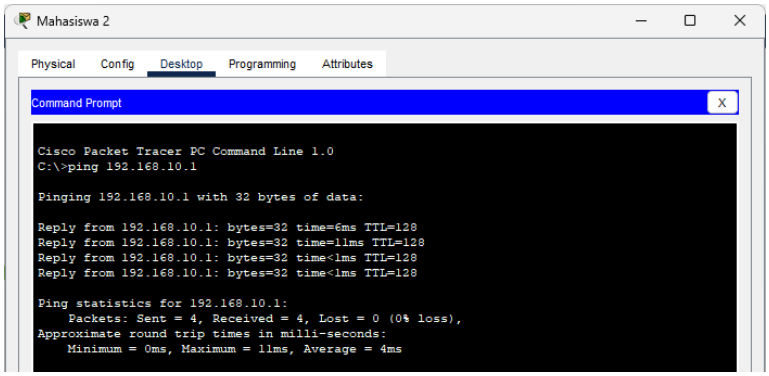

Figure 3. Successful ping result: Student to Student

These results demonstrate that VLAN segmentation does not interfere with internal communication within a user group.

Inter-VLAN Communication (Student to Faculty) The subsequent test involved sending ICMP packets from a Student PC (192.168.10.1) to a Faculty PC (192.168.20.1) on a different VLAN. The test resulted in a "Request timed out" message.

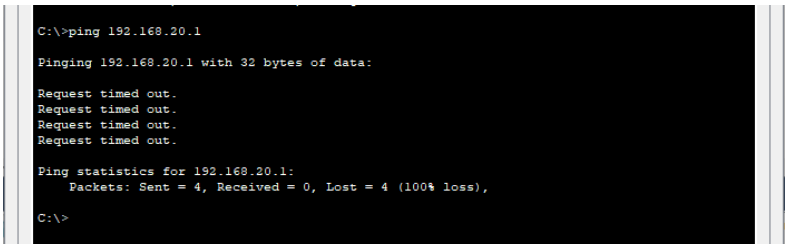

Figure 4. Failed ping result: Student to Faculty.

This communication failure confirms that devices on the Student VLAN cannot access the Faculty VLAN, validating that the network isolation aligns with the design objectives.

3) Analysis of Network Isolation Effectiveness

Based on the connectivity results, it can be concluded that the VLAN implementation effectively established network isolation between faculty and students. Successful intra-VLAN communication confirms the system supports internal network activities, while the failure of inter-VLAN communication signifies that cross-network access has been logically restricted. This isolation is a key performance indicator of successful segmentation, as data traffic cannot bypass these boundaries without additional mechanisms such as inter-VLAN routing.

4) Alignment with CIA Triad Principles

The simulation results directly correspond to the Confidentiality, Integrity, and Availability (CIA Triad) framework:

1) Confidentiality: Network isolation ensures that sensitive faculty data, such as grades and academic records, remain inaccessible to students. The failed inter-VLAN communication serves as empirical evidence of data privacy.
2) Integrity: By blocking unauthorized cross-VLAN access, the potential for unauthorized data manipulation is mitigated, maintaining the accuracy and authenticity of data within each segment.
3) Availability: Successful intra-VLAN communication proves that network services remain available and functional for authorized users. Segmentation also optimizes traffic load and reduces potential network disruptions.

5) Final Evaluation of VLAN Configuration

The final evaluation indicates that the network segmentation system was implemented in a secure and controlled manner. Increasing the number of devices (three student PCs and three faculty PCs) did not affect the isolation's effectiveness, suggesting that the VLAN configuration is scalable. Consequently, this model serves as a robust foundation for designing secure and efficient academic networks in modern educational institutions.

CONCLUSION

This research successfully demonstrates that the implementation of Virtual Local Area Networks (VLANs) effectively segregates academic networks for faculty and students within a simulated environment. By utilizing Cisco Packet Tracer, the study established distinct logical segments that maintain functional intra-VLAN communication while strictly prohibiting unauthorized inter-VLAN access. This isolation serves as empirical evidence that VLAN-based segmentation enhances academic network security by minimizing the risk of unauthorized exposure of sensitive data. Furthermore, the simulation results validate the system's alignment with the CIA Triad framework, where confidentiality and integrity are preserved through robust isolation, and availability remains consistent for authorized users. Given that the configuration remained stable despite an increased number of devices, it can be concluded that this model offers a scalable and reliable foundation for designing secure, controlled, and efficient university network infrastructures.

Looking forward, there are several avenues for expanding this research to address more complex institutional requirements. Future studies should consider integrating advanced security layers, such as inter-VLAN routing combined with Access Control Lists (ACLs) or dedicated firewalls, to achieve more granular access management between segments. Such enhancements would allow for a more flexible policy-driven architecture beyond simple logical isolation. Additionally, future work could increase the topological complexity by incorporating multiple switches, DHCP services, and centralized academic servers. Transitioning from a controlled simulation to a high-fidelity environment or a real-world campus pilot would provide deeper insights into the performance, reliability, and long-term security of VLAN configurations in supporting large-scale, network-based academic systems.

REFERENCES

[1] L. Qing, "Research on the Innovation of Student Education and Management in Colleges and Universities under Network Environment," *Int. J. New Dev. Educ.*, vol. 6, no. 5, pp. 242–247, 2024, doi: 10.25236/ijnde.2024.060538.

[2] M. N. Habib, W. Jamal, U. Khalil, and Z. Khan, "Transforming universities in interactive digital platform: case of city university of science and information technology," *Educ. Inf. Technol.*, vol. 26, no. 1, pp. 517–541, 2021, doi: 10.1007/s10639-020-10237-w.

[3] S. M. Saif, S. I. Ansarullah, M. T. Ben Othman, S. Alshmrany, M. Shafiq, and H. Hamam, "Impact of ICT in Modernizing the Global Education Industry to Yield Better Academic Outreach," *Sustainability*, vol. 14, no. 11. p. 6884, 2022. doi: 10.3390/su14116884.

[4] U. Matthew, J. Kazaure, and N. Okafor, "Contemporary Development in E-Learning Education, Cloud Computing Technology & Internet of Things," *EAI Endorsed Trans. Cloud Syst.*, vol. 7, no. 20, p. 169173, 2018, doi: 10.4108/eai.31-3-2021.169173.

[5] M. Alenezi, "Digital Learning and Digital Institution in Higher Education," *Education Sciences*, vol. 13, no. 1. p. 88, 2023. doi: 10.3390/educsci13010088.

[6] D. B. Rawat, R. Doku, and M. Garuba, "Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security," *IEEE Trans. Serv. Comput.*, vol. 14, no. 6, pp. 2055–2072, 2021, doi: 10.1109/TSC.2019.2907247.

[7] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Networks*, vol. 169, p. 107094, 2020, doi: https://doi.org/10.1016/j.comnet.2019.107094.

[8] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey," *Electronics*, vol. 11, no. 1. p. 16, 2022. doi: 10.3390/electronics11010016.

[9] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electronics*, vol. 12, no. 6. p. 1333, 2023. doi: 10.3390/electronics12061333.

[10] Christian Fischer *et al.*, "Mining Big Data in Education: Affordances and Challenges," *Rev. Res. Educ.*, vol. 44, no. 1, pp. 130–160, Mar. 2020, doi: 10.3102/0091732X20903304.

[11] L. Cohen-Vogel, M. Little, and C. Fierro, "Evidence-Based Staffing in High Schools: Using Student Achievement Data in Teacher Hiring, Evaluation, and Assignment," *Leadersh. Policy Sch.*, vol. 18, no. 1, pp. 1–34, Jan. 2019, doi: 10.1080/15700763.2017.1326146.

[12] Brendan Bartanen, "Principal Quality and Student Attendance," *Educ. Res.*, vol. 49, no. 2, pp. 101–113, Jan. 2020, doi: 10.3102/0013189X19898702.

[13] V. Rajkumar, M. Prakash, and V. Vennila, "Secure data sharing with confidentiality, integrity and access control in cloud environment," *Comput. Syst. Sci. Eng.*, vol. 40, no. 2, pp. 779–793, 2021, doi: 10.32604/CSSE.2022.019622.

[14] O. Mitchell and C. Osazuwa, "Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature," *Int. J. Innov. Sci. Res. Technol.*, vol. 8, no. 12, 2023.

[15] L. Kim, "Cybersecurity: Ensuring Confidentiality, Integrity, and Availability of Information BT - Nursing Informatics : A Health Informatics, Interprofessional and Global Perspective," U. H. Hübner, G. Mustata Wilson, T. S. Morawski, and M. J. Ball, Eds. Cham: Springer International Publishing, 2022, pp. 391–410. doi: 10.1007/978-3-030-91237-6_26.

[16] B. Hazela, S. K. Gupta, N. Soni, and C. N. Saranya, "Securing the Confidentiality and Integrity of Cloud Computing Data," *ECS Trans.*, vol. 107, no. 1, p. 2651, 2022, doi: 10.1149/10701.2651ecst.

[17] H. A. Saeed, S. Askar, Z. Soran, and D. Khoshnaw, "Comparative Evaluation of VXLAN with

Traditional Overlay Network Protocols," *Indones. J. Comput. Sci.*, vol. 12, no. 2, pp. 284–301, 2023, [Online]. Available: http://ijcs.stmikindonesia.ac.id/ijcs/index.php/ijcs/article/view/3135

[18] D. Li, Z. Yang, S. Yu, M. Duan, and S. Yang, "A Micro-Segmentation Method Based on VLAN-VxLAN Mapping Technology," *Future Internet*, vol. 16, no. 9. p. 320, 2024. doi: 10.3390/fi16090320.

[19] Y. A. Makeri, G. T. Cirella, F. J. Galas, H. M. Jadah, and A. O. Adeniran, "Network Performance Through Virtual Local Area Network (VLAN) Implementation & Enforcement On Network Security For Enterprise," *Int. J. Adv. Netw. Appl.*, vol. 12, no. 06, pp. 4750–4762, 2021, doi: 10.35444/ijana.2021.12604.

[20] S. W. Nourildean, Y. A. Mohammed, and H. A. Attallah, "Virtual Local Area Network Performance Improvement Using Ad Hoc Routing Protocols in a Wireless Network," *Computers*, vol. 12, no. 2. p. 28, 2023. doi: 10.3390/computers12020028.

[21] T. Zhang, G. Wang, C. Xue, J. Wang, M. Nixon, and S. Han, "Time-Sensitive Networking (TSN) for Industrial Automation: Current Advances and Future Directions," *ACM Comput. Surv.*, vol. 57, no. 2, 2024, doi: 10.1145/3695248.

[22] W. Lei, M. Li, Y.-H. Kuo, and G. Q. Huang, "Converged Address Resolution Protocol for Traceability and Visibility in Cyber–Physical Internet," *IEEE Internet Things J.*, vol. 12, no. 14, pp. 27322–27338, 2025, doi: 10.1109/JIOT.2025.3562803.

[23] N. E. Cicek and N. Shafae, "Zero Trust Micro-Segmentation in Cloud Environments: A Systematic Literature Review of Strategies, Challenges, and Future Trends." p. 29, 2025.

[24] A. Brännström and T. Vandermaesen, "The Role of Network Segmentation in Enhancing Cybersecurity in Substation Communication Networks." p. 35, 2025.

[25] G. Mwansa, M. R. Ngandu, and Z. S. Dasi, "Enhancing Practical Skills in Computer Networking: Evaluating the Unique Impact of Simulation Tools, Particularly Cisco Packet Tracer, in Resource-Constrained Higher Education Settings," *Education Sciences*, vol. 14, no. 10. p. 1099, 2024. doi: 10.3390/educsci14101099.

[26] O. Erukayenure, H. A. Bashir, A. Adekunbi, O. S. Esan, and O. Idris, "IoT Device Security in Modern Healthcare : Addressing Cyber Threats to Connected Medical Equipment," *Int. J. Med. All Body Heal. Res.*, vol. 06, no. 04, pp. 49–57, 2025, doi: 10.54660/IJMBHR.2025.6.4.49-57 Keywords: