Journal of Electrical and Computer Engineering (JEECOM)
Vol. 7, No. 2 (2025), DOI: 10.33650/jeecom.v4i2
p-ISSN: 2715-0410; e-ISSN: 2715-6427

Implementation of VLAN and ACL for Network Security at SDIT Ibnu Hajar Bekasi

Taufik Rahman [1], Qori Aprianto [2]
[1,2] Bina Sarana Informatika University, Jakarta, Indonesia

Article Info

Article history:

Accepted Sept 14, 2025
Revised Okt 30, 2025
Accepted Okt 31, 2025

Keywords:

VLAN
Access Control List
Network Security
Network Segmentation
Cisco Package Tracker
NDLC

ABSTRACT

In the age of modern technology, network security is essential to ensure that educational institutions operate properly. The purpose of this study is to improve the network security of SDIT Ibnu Hajar Bekasi City by applying technologies such as Virtual Local Area Network and Access Control List. This study uses the Network Development Life Cycle (NDLC) approach, which consists of the stages of initiation, planning, design, implementation, testing, and maintenance. Using vlan network segmentation, data traffic is divided into groups, such as administration, computer labs, instructors, and students. For now, ACLs are used to set access rights between network segments according to the user's needs and authorizations. Simulation testing on Cisco Packet Tracer shows that the implementation of vlan and acl improves network stability and security, reduces average latency, and reduces broadcast traffic. The results of the acl configuration indicate that the student cannot access the teacher and administrative network. However, teachers can still access the administration and laboratories. This research shows that the use of vlans and acls can improve the security and effectiveness of network management in schools.

Corresponding authors:
Taufik Rahman,
Bina Sarana Informatika University, Jl. Kramat Raya No. 98, RT.2/RW.9, Kwitang, Senen District, Central Jakarta City, Special Capital Region of Jakarta 10450
Email: taufik@bsi.ac.id

1. INTRODUCTION

The rapid development of information technology has driven the increasing need for reliable, efficient, and secure computer networks in various institutions, including educational institutions. Schools as the center of teaching and learning activities not only need a network to support administration and academic activities, but also to support the technology-based learning process. However, the increasing use of networks and the internet in school environments also poses new challenges, especially in terms of data security, access restrictions, and the efficiency of network traffic management. SDIT Ibnu Hajar Bekasi City is one of the educational institutions that has utilized computer networks to support operational and learning activities. However, the network system used is still open (flat network), where all devices are in the same network segment. This condition results in all users, both students, teachers, and administrative staff, having relatively free access to network resources. As a result, potential security risks such as intrusion, data leakage, and decreased network performance are greater due to the absence of access restrictions between users based on roles and needs.

Based on the problems that have been described, it is necessary to study previous studies that have relevance to the topic of implementing VLANs and Access Control Lists (ACL) in improving network security. The implementation of Access Control List (ACL) on Mikrotik routers in school environments can improve network security and stability. With ACL configuration, internet access can be selectively regulated so that only authorized devices can be connected, so that network usage is more controlled and efficient in supporting teaching and learning activities[1]. The implementation of VLANs and ACLs on school networks has been proven to improve security by limiting communication between network segments. Through simulations in Cisco Packet Tracer, this configuration allows for controlled access rights setting across departments without having to make major changes to the existing network infrastructure[2]. The implementation of VLANs and Access Control Lists (ACLs) in network management is considered effective in regulating the distribution of access rights and improving network security. VLANs allow for virtual cross-network communication, while ACLs play a role in restricting access between devices as per established policies[3]. The application of extended ACL on VLAN networks has been proven to be able to improve network security by restricting user access rights and regulating inter-network connectivity. Through simulation in Cisco Packet Tracer, this configuration helps routers manage access to services such as FTP and web servers in a more controlled and efficient manner[4]. The implementation of VLANs through simulation in Cisco Packet Tracer has proven to be effective in improving network security and efficiency. The configuration results show that network segmentation between VLANs successfully limits communication between different departments, while connectivity within the same VLAN remains optimally run[5]. Schools as educational institutions play an important role in equipping students with various knowledge and skills, including in the field of information and communication technology[1]. The application of the VLAN concept at SMAS Santo Yusup Surabaya was designed using the PPDIOO method and simulated through Cisco Packet Tracer. The results show that the network design is effective, with proper IP allocation and optimal connectivity between devices according to the school's network needs.[6]. The focus of this research is to optimize the computer network at SMK Travina Prima by implementing Inter-VLAN, VLSM, and HSRP. Existing network problems include IP address conflicts, inefficient bandwidth usage, and a high risk of network failure due to reliance on one main router[7]. The focus of this research is a network security strategy that uses Virtual Local Area Networks and Access Control Lists in PT Pegadaian Kalibata Branch[8]. The ACL configuration on the VLAN network successfully restricts access between segments as needed. Student VLANs cannot connect to admin and teacher VLANs, teacher VLANs can access lab VLANs and network management, while admin VLANs have full access. This implementation improves the security, efficiency, and management of the network according to the research objectives.[9]. Network simulation using Cisco Packet Tracer 6.2 plays an important role in designing and visualizing computer network architectures, from topology determination to device configuration, thus aiding in more efficient and targeted planning in network construction[10]. According to research conducted at PT. Cakramedia Indocyber, network resource limitations can be overcome through the implementation of VLAN and port security switches to limit access between users, as well as Access Control List (ACL) on routers to regulate data traffic according to internal communication needs. With observation, interview, and laboratory test methods, the implementation results show an increase in security and effectiveness of network use in the company's environment[11]. The implementation of VLAN-based school networks with Cisco devices is able to increase security and simplify the management of user access rights, so that administrators can manage the network more efficiently (Research at SMK PGRI 11 Ciledug)[12]. The implementation of the Access Control List (ACL) at PT. Hidatech Indonesia has proven to be effective in improving network security and regulating access rights between divisions, so that data traffic can be properly controlled and the risk of cyberattacks can be minimized[13]. The implementation of Access Control List (ACL)-based VLAN on the network of the Serang City Communication and Information Office has been proven to be able to improve network efficiency, stability, and security by minimizing disruption and dividing the network into more managed segments[14]. An Access Control List (ACL)-based network simulation using Cisco Packet Tracer shows that the implementation of ACLs is able to efficiently manage data traffic and improve network security, as well as provide educational benefits in understanding access control concepts in practical terms[15].

Based on the problem, a technical approach is needed that can improve network security while improving the efficiency of data management in the school environment. One of the solutions that can be implemented is to implement a Virtual Local Area Network (VLAN) to segment the network based on user functions, as well as Access Control List (ACL) to manage access rights between VLANs. With network segmentation using VLANs, data traffic between parts such as students, teachers, and admins can be separated, while ACLs are applied to control communication between network segments according to defined security policies. This approach offers two main benefits. First, from a security perspective, VLANs and ACLs can minimize the possibility of unauthorized access between parts of the network to prevent potential internal attacks. Second, in terms of efficiency, the use of VLANs helps reduce excessive data traffic load (broadcast domain) and speeds up the communication process on the network. Through implementation and simulation using Cisco Packet Tracer, this study will analyze how the implementation of VLANs and ACLs can improve network security and performance in elementary school environments. The new value (innovation) of this research lies in the application of a combination of VLAN and Access Control List (ACL) in an integrated manner in the basic education environment which generally still uses a simple network system. This approach not only offers increased security, but also becomes an implementation model that can be replicated by other schools with limited infrastructure. Thus, this research is expected to make practical and theoretical contributions in the field of computer network management and security in the educational environment.

2. METHOD

The design of the research method includes the stages of data collection techniques and network development models. Each stage is described systematically to describe the flow of research implementation from initiation to operation and maintenance.

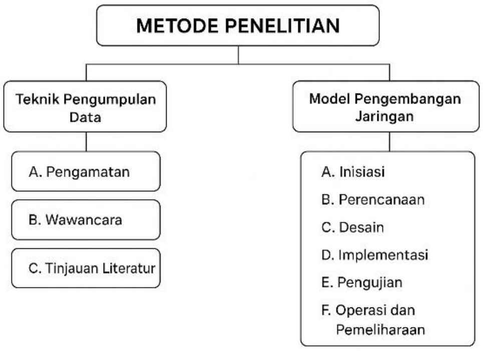


Figure 1. Research Method Design

1. **Data collection techniques**

   A. **Observation**
   The data collection method involves conducting research on the object being studied. The researcher also conducted direct observations at SDIT Ibnu Hajar.

   B. **Interview**
   The researchers conducted a direct interview with Mr. Irfan, the person in charge at SDIT Ibnu Hajar, and discussed this to obtain accurate information about network security issues at SDIT Ibnu Hajar.

   C. **Literature Review**
   The researcher is also supported by a literature review with references from previous research and journal work that addresses issues related to virtual local area networking and access control lists, as well as best practices in network security. This research assists researchers in developing a theoretical foundation and determining the appropriate implementation method.

2. **Network Development Model**
   The network development model used in this study refers to the stages of the Network Development Lifecycle:

   A. **Initiation**: Identify current network needs and security issues at SDIT Ibnu Hajar.

   B. **Planning:** Develop solution designs using VLANs for network segmentation and access control lists for access control, including topology mapping and hardware or software requirements.

   C. **Design:** Designing a new network topology that implements VLANs to separate networks based on functions, as well as designing access control list rules according to access control requirements between segments.

   D. **Implementation:** Configure network devices such as switches and routers to implement vlans and acls according to the design that has been created.

   E. **Testing:** Perform network testing to ensure that vlan segmentation is working properly and that acls are successful in restricting access between network segments.

   F. **Operations and Maintenance:** Post-implementation network monitoring and evaluation to ensure optimal network stability, security, and performance

3. RESULTS AND DISCUSSION

The proposed network schema is simulated using Cisco Packet Tracer, which clearly shows vlan separation, IP address setting, and access grouping by function. Through the implementation of vlan settings and inter-device access, the proposed network scheme aims to support network segmentation and security. One router unit, two switches, and four computer devices are used in this scheme to represent each section: administration, computer lab, teachers, and students. Each part is separated into a specific network of vlans, for example, vlans 10, 20, 30, and 40. In the proposed network, the router-on-a-stick method allows communication between vlans over the router's physical ports. Each sub-interface is configured with the corresponding vlan id and gateway IP address, so that the router can identify and process traffic from each vlan. For example, vlan 10 has a gateway of 192.168.2.1, and vlan 20 has a gateway of 192.168.3.1, and so on. With this configuration, traffic between divisions can be routed in a controlled manner through a single trunk path that connects the router to the main switch. This method is particularly effective for small to medium-sized tissues. It also makes future network development and management easier.

3.1. Network Topology

The proposed network topology uses tree topologies commonly used in educational environments and better supports the implementation of VLANs and ACLs. To create a stable, structured, and manageable network, the proposed network topology uses a tree topology model to connect all devices to the switch. This network has four PCs, one router, two switches, each representing a different section or department: administration, computer lab, teachers, and students. Using the router-on-a-stick method, the router serves as a controller of data traffic between different VLANs by dividing one physical port of the router into several sub-interfaces. To enable a smooth flow of VLAN traffic, this router's port connects to switch 1 via a trunk connection**.**

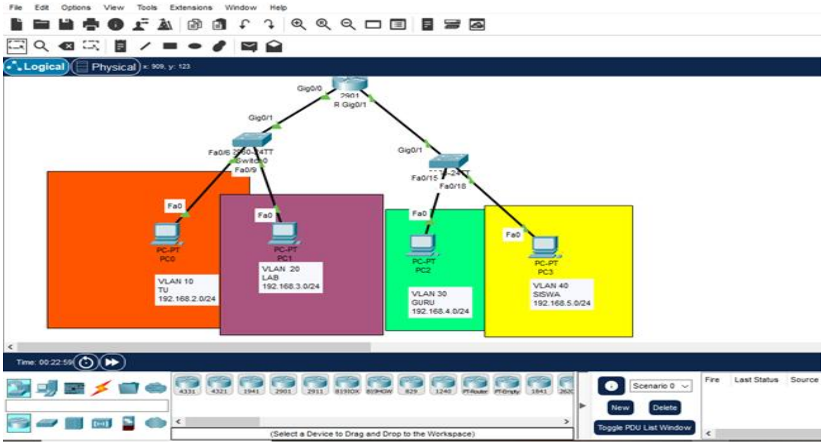


Figure 2. Proposed Network Topology

Each port on the switch is configured to be part of a specific VLAN based on its function, such as VLAN 10 for administration, VLAN 20 for computer labs, and VLAN 30 for computer labs. Switch 1 connects the administration and student PCs with trunk ports, so VLAN traffic from devices on switch 2 can still reach the router through switch 1. The purpose of placing these VLAN-based devices is to separate broadcast domains, improve network security, and facilitate access management between departments. This topological structure makes the network more organized and allows for additional security measures such as Access Control Lists that govern user access rights.

3.2. Network Schema

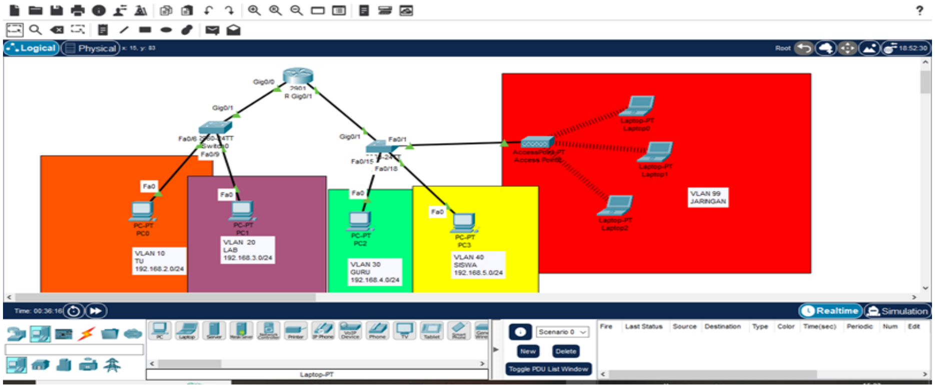


Figure 3. Proposed Network Scheme

The vlan distribution consists of vlan 10 for administration, vlan 20 for computer lab, vlan 30 for office, vlan 40 for students, and vlan 99 for network access management. The proposed network scheme consists of four pcs, two switches, one router, and one access point, each component functioning in a school environment. The structure is simple but effective. To improve the security and efficiency of data traffic, the concept of segmentation of vlan networks is used in this design. The router serves as a traffic controller between vlans, or routing between vlans, and connects to switch 1 via a trunk port that handles all configured vlans. Switch 1 and switch 2 are connected to each other via the trunk port so that all VLANs can pass through both switches without interference. Each pc on this network is placed in a different vlan. The Administration Department uses vlan 10, where pc1 is connected to switch 1 on fastEthernet port 0/6. The administrative staff uses this vlan and has full access to all networks. The computer lab uses vlan 20, where the pc2 is connected to switch 1 on the 0/9 fastEthernet port. These VLANs are only used for computer labs or lessons. In addition, there is a vlan 30 for the teacher, and the pc3 is connected to switch 2 on the 0/15 fastEthernet port. Teachers have limited access, but they can connect to the administration and computer lab vlan, but not to the student vlan. Lastly, there is a vlan 40 for students, with 4 pcs connected to switch 2 on the 0/18 fastEthernet port. Only students have access to their internal network; Students cannot access the administration and teacher network.

Each vlan can be passed through the trunk port on a 1 gigabitEthernet0/0 switch to the router and a 2 gigabitEthernet0/1 switch to the router. This trunk configuration is critical for the router to be able to receive data traffic from various vlans correctly when using the router-on-a-stick method. Each switch can be configured to assign a specific port to the appropriate vlan using the switchport access vlan command on each port. On the other hand, the trunk port can be configured to use the switchport trunk mode. By using structured vlans and acls on routers, these networks can offer security and controlled segmentation.

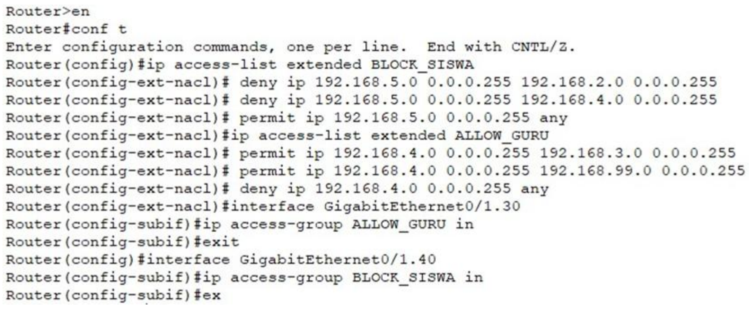
3.3. End-to-End Network Testing

Final testing is done using ping to ensure that an access control list has been implemented. Student computers and computers with other vlans are tested. The results showed that the student's computer (Vlan 40) and the teacher's computer (Vlan 30) were unable to access the administrative network (Vlan 10) and the administrative network (Vlan 30). In contrast, the teacher's computer (Vlan 30) and laboratory (Vlan 20) can still access the administrative network (Vlan 10) and the laboratory (Vlan 20). The router's access control list rules allow this access. This shows that the access control policy successfully divides access rights between divisions.

3.3.1. Enabling Access Control List

An access control list is used on routers to restrict access between predefined vlans. The main purpose of the acl is to ensure that only certain subdivisions can communicate according to established network security rules. In other words, an access control list is used to restrict, allow, or deny access to users from different vlans. In contrast, the access control list configuration results allow access to vlan 10 (Administration) and vlan 20 (Computer Lab) on vlan 30 (Teacher). The ping test from the teacher's computer to the lab computer and the administration was successful, indicating that the destination host responded. This suggests that the acl rule is intended to grant teachers limited access rights to meet their operational needs, such as accessing administrative documents and learning resources in computer labs, but still restricts them from the student's vlan.

Since vlan 10 (Administration) is considered to have full access to the entire network, no access restrictions are applied to this vlan. Computers in the administration vlan can access and ping all other vlans without restrictions. This is very important because the administration department is responsible for managing and supervising the entire school network.



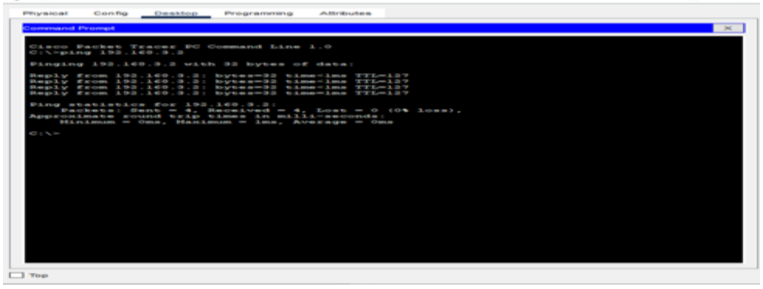
```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended BLOCK_SISWA
Router(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.2.0 0.0.0.255
Router(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.4.0 0.0.0.255
Router(config-ext-nacl)# permit ip 192.168.5.0 0.0.0.255 any
Router(config-ext-nacl)#ip access-list extended ALLOW_GURU
Router(config-ext-nacl)# permit ip 192.168.4.0 0.0.0.255 192.168.3.0 0.0.0.255
Router(config-ext-nacl)# permit ip 192.168.4.0 0.0.0.255 192.168.99.0 0.0.0.255
Router(config-ext-nacl)# deny ip 192.168.4.0 0.0.0.255 any
Router(config-ext-nacl)#interface GigabitEthernet0/1.30
Router(config-subif)#ip access-group ALLOW_GURU in
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/1.40
Router(config-subif)#ip access-group BLOCK_SISWA in
Router(config-subif)#ex
```

Figure 4. Final Testing using the Access Control List

The results of the access control list test show that the vlan has been blocked by the access control list. Vlan 40 (Student) cannot send data to Vlan 30 (Teacher) and Vlan 10 (Administration Room).

3.3.2. Virtual Local Area Network Connectivity Testing

In this test, the ping command is successful, and the teacher's computer receives a response from the lab computer. This indicates that VLAN 30 can access VLAN 20, according to the access control list rules that allow teachers to access computer labs. In addition, successful tests from VLAN 30 to VLAN 10 (administration) show that the teacher has access to the administrative network. This test ensures that the configuration of the access control list does not interfere with allowed communication**.**

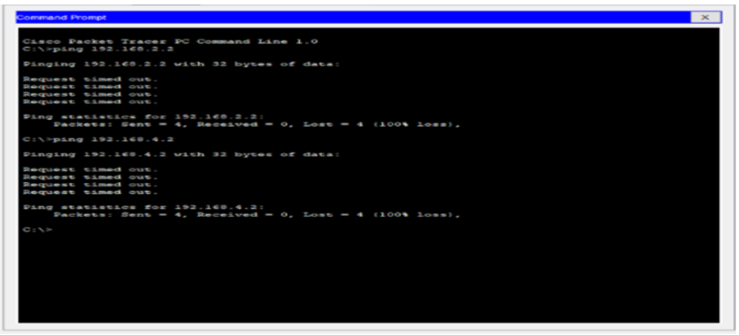


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=1ms TTL=127
Reply from 192.168.3.2: bytes=32 time<1ms TTL=127
Reply from 192.168.3.2: bytes=32 time<1ms TTL=127
Reply from 192.168.3.2: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Figure 5. Ping Results for VLAN 30 and VLAN 20

Network connectivity test results after implementing VLANs and access control lists. In this test, a PC connected to VLAN 30 can access the IP address of a PC connected to VLAN 20. The data communication between the two VLANs is successful, as indicated by the command results. The success of this ping indicates that the router's ACL configuration allows VLAN 30 to access VLAN 20.

Once the access control list configuration is applied to the router, final testing is performed to ensure that the inter-vlan access policy is working correctly. Ping commands are used from each computer to check the connection to other computers in the vlan.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure 6. Ping Test Results

The results of the ping test showed that the network conditions before and after implementation differed significantly. All devices initially had the ability to communicate with each other without limitations. However, after implementing VLANs and ACLs, devices in the student VLAN cannot ping devices in the teacher or administrative VLANs. In contrast, teacher devices can still access administrative VLANs to support work needs, but they can't ping devices in student VLANs. This condition shows that the segmentation and access control mechanisms are working well as planned.

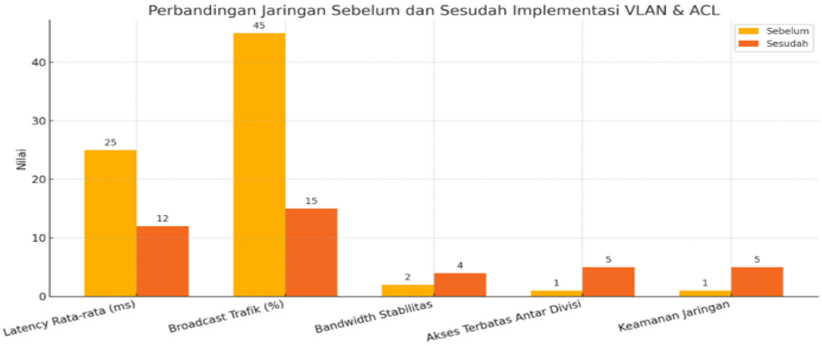


Figure 7. Comparison Before and After Implementation

The vlan implementation and access control list show the results of the network test. The tests conducted showed a decrease in average latency from 25 ms to 12 ms and a decrease in broadcast traffic from 45% to 15%. As unnecessary data is no longer circulating throughout the network, bandwidth stability has improved. Restricting access between divisions also improves the security and control of network traffic. These results show that the new network can meet the requirements of educational institutions that require stable, secure, and manageable systems.

4. CONCLUSION

One of the problems with the current state of the network at SDIT Ibnu Hajar is the lack of clear segmentation between divisions. As a result, all devices are on the same network, or flat network. Unauthorized access, malware distribution, and sensitive data leaks are all highly likely. VLANs have proven to be effective in solving network segmentation problems. This is because they divide the network into sections, such as administration, teachers, computer labs, and students. In addition, the broadcast domain becomes smaller, thus increasing the efficiency of the network. Configuring an access control list on a router can solve access control issues. By applying selective ACL rules, access between VLANs can be controlled according to the needs of each unit. For example, teacher and administrative VLANs cannot be used by students, but laboratory and administrative VLANs can still be used according to their functions.

ACKNOWLEDGEMENTS

Gratitude and praise are offered to Allah for His blessings, grace, and guidance. The authors also express heartfelt thanks to their parents, friends, and lecturers who have provided support and assistance throughout this research.

REFERENCE

[1] Abra, A. Al-furqan, and A. S. Aziz, "IMPLEMENTATION OF ACCESS CONTROL LIST (ACL) IN DESIGNING VIRTUAL LOCAL AREA NETWORK AT SMKN 1 AL-MUBARKEYA," *JATI (Journal of Mhs. Tek. Inform.*, vol. 9, no. 1, pp. 368–373, 2025.

[2] R. Rahman, D. Herlambang, and M. F. Ramadhanu, "IMPLEMENTATION OF VIRTUAL LAN AND ACCESS CONTROL LIST FOR ACCESS SEGMENTATION IN SCHOOL NETWORKS: A SIMULATION STUDY," *J. Syst. Technol.*, vol. 1, no. 1, pp. 20–25, 2025.

[3] U. Hasan, S. Dewi, and Firmansyah, "Application of Access Control List Method on VLAN Networks Using Cisco Routers," *IMTechno J. Ind. Manag. Technol.*, vol. 3, no. 1, p. 5, 2022, [Online]. Available: http://jurnal.bsi.ac.id/index.php/imtechno

[4] O. J. Usior and E. Sediyono, "Simulation of Extended ACL on VLAN Networks Using Cisco Packet Tracer Applications," *AITI J. Teknol. Inf.*, vol. 20, no. 1, pp. 32–47, 2023, doi: 10.24246/aiti.v20i1.32-47.

[5] S. Sitohang and H. Pangaribuan, "Journal of Applied Informatics Science (JSIT) Systematic Study of Learning Analytics Parameters," *J. Science Inform. Apply.*, vol. 4, no. 2, pp. 264–270, 2025.

[6] P. I. O. B. Sipayung, V. Purba2, and Agussalim, "Analysis, Design, and Simulation of VLAN Networks Using the PPDIOO Method (Case Study: SMAS Santo Yusup Surabaya)," *TeknoIS J. Ilm. Technology. Inf. and Science*, vol. 14, no. 1, pp. 110–118, 2024, doi: 10.36350/jbs.v14i1.237.

[7] T. Rahman and E. T. Pamungkas, "OPTIMIZATION OF COMPUTER NETWORKS AT SMK TRAVINA PRIMA WITH THE IMPLEMENTATION OF INTERVLAN, VLSM, AND HSRP," *J. Inform. Univ. Muhammadiyah Tangerang P*, vol. 8, no. 4, pp. 2722–2713, 2024, doi: http://dx.doi.org/10.31000/jika.v8i4.12379.

[8] D. N. Djuanda, "Network Security Strategy with VLANs and Access Control Lists: Case Studies and Implementation," *Inf. Technol. Syst.*, vol. 2, no. 1, pp. 25–31, 2024.

[9] A.-H. Jambak, H. Aspriyono, and A. Al Akbar, "Computer Network Management Using a Mikrotik Router at the Immigration Office Class I TPI Bengkulu City," *J. Media Comput. Sci.*, vol. 1, no. 1, pp. 7–13, 2022, doi: 10.37676/jmcs.v1i1.1909.

[10] A. B. Ivo Colanus Rally Drajana, "NETWORK SIMULATION USING CISCO PACKET TRACER," *J. Sist. Inf. DAN Tek. Computer.*, vol. 6, no. 1, pp. 24–27, 2021, [Online]. Available: https://ejournal.catursakti.ac.id/index.php/simtek/article/view/91/103

[11] F. Fahrizal and B. A. Candra, "Implementation of Access Control List in the Design of Virtual Local Area Network at Pt Cakramedia Indocyber," *Jeis J. Electrical and Inform. Swadharma*, vol. 2, no. 2, pp. 36–43, 2022, doi: 10.56486/jeis.vol2no2.204.

[12] Susilo, S. Hartono, K. Yunan, and B. A. Wardijono, "Implementation of Cisco Vlan for Access Rights Management on School Computer Networks," *Sem. Nas. Technology. Inf. and Commun. STI&K*, vol. 7, no. 1, pp. 192–202, 2023.

[13] M. Rahman and M. Dasuki, "Implementation of access control list (ACL) as a protection and traffic control method in local area network (LAN) network infrastructure," *J. Comput. Sci. Inf. Technol.*, vol. 6, no. 1, pp. 68–76, 2025.

[14] D. P. Agustio and E. R. Nainggolan, "The Implementation of Virtual Local Area Network on the MAN Network with the Access Control List-Based Filtering Method at the Serang City Communication and Information Office," *J. Compute. Antart.*, vol. 1, no. 1, pp. 32–38, 2023.

[15] A. Harmain, M. Guntara, I. G. Ayu, D. Gita, and K. Santi, "Simulation of ACL-Based Network Topology Using Cisco Packet Tracer," *Sem. Nas. CORISINDO*, vol. 1, no. 1 2025, pp. 223–230, 2025.