Jurnal Teknologi Informasi dan Pendidikan
Volume 18, No. 2, September 2025
https://doi.org/10.24036/jtip.v18i2.1056

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

Implementation of Mikrotik Firewall and QoS for Secure and Efficient Internet Networking

Seyhan[1], Joko Triloka[1*]✉
[1] Faculty of Computer Science, Informatics & Business Institute Darmajaya, Bandar Lampung, Indonesia
**Corresponding Author: joko.triloka@darmajaya.ac.id*

Article Information

Article history:

No. 1056
Rec. September 07, 2025
Rev. November 04, 2025
Acc. November 05, 2025
Pub. November 06, 2025
Page. 1097 – 1109

Keywords:

- *Network administration*
- *Traffic management*
- *Bandwidth control*
- *Educational infrastructure*
- *Access control*

ABSTRACT

Effective network management in school environments is an ongoing challenge as the demand for internet access among students, teachers, and staff continues to grow. This study aims to design and implement a Mikrotik-based network management solution. The research was conducted at SMK Negeri 1 Bandar Lampung, with the objectives of improving network service quality, optimizing bandwidth allocation, and ensuring network security. This research adopts the Network Development Life Cycle (NDLC) model as the framework for system development, which includes analysis, design, simulation, implementation, monitoring, and evaluation stages. Mikrotik was chosen due to its flexibility in network management at a relatively affordable cost. The research methods included analyzing the school's network requirements, designing the network topology, and configuring Mikrotik devices based on Quality of Service (QoS), firewall, and user access control implemented through Hotspot with user profiles and MAC address filtering. The results show that the implementation of Mikrotik successfully enhanced network stability, reduced latency, and restricted access to non-relevant websites. Unlike previous studies that mainly focused on general QoS testing, this research integrates NDLC-based systematic development with granular access control and bandwidth management tailored to educational environments. These findings highlight that Mikrotik provides an effective and efficient solution for network management, particularly in small to medium-scale settings. This study is expected to serve as a reference for other schools facing similar challenges in network management.

How to Cite:

Seyhan & Triloka, J. (2025). Analysis of QoS and Security Mechanisms of Internet Networks Using Mikrotik Firewall and Access Control. Jurnal Teknologi Informasi Dan Pendidikan, 18(2), 1097-1109. https://doi.org/10.24036/jtip.v18i2.1056

1. INTRODUCTION

An internet network can be defined as a collection of interconnected computers that communicate and share resources on a large scale. According to [1], a system qualifies as a network when devices can exchange information effectively. In Indonesia, the internet has become an essential medium for communication since it overcomes the limitations of distance and time [2]. Its rapid growth has influenced many sectors of life, including education. Reliable internet access in educational institutions supports learning activities by enabling students and lecturers to obtain literature and references for academic purposes [3]. Moreover, schools and universities depend on stable networks to conduct administrative processes, making effective network management a critical requirement.

To ensure optimal network performance, institutions must not only provide sufficient connectivity but also maintain Quality of Service (QoS). QoS represents the overall effectiveness of service performance in meeting user expectations [4]. It is described as crucial for ensuring optimal network performance, particularly in terms of bandwidth allocation, jitter reduction, and minimizing delay [5], and is measured through other parameters such as packet loss and throughput [6, 7]. Variations in these metrics usually result from congestion, which occurs when the volume of incoming traffic exceeds a router's capacity, leading to excessive queuing and degraded performance [8, 9]. Congestion can be reduced through flow control mechanisms [10], which regulate data transmission rates to ensure efficient processing [11]. Among these mechanisms, traffic shaping with the token bucket algorithm is widely applied. The Token Bucket Filter (TBF) regulates packet transmission based on token availability, thereby maximizing bandwidth usage and improving QoS [12]. Previous studies have employed various approaches, including traffic prioritization mechanisms for narrow-band IoT services in 4G/5G networks [13], quality of the internet network in a university using Hierarchical Token Bucket (HTB) [14] [15] [16] [17], and bandwidth allocation and distribution algorithm using OpenFlow meters [18], all of which demonstrate the importance of QoS optimization in computer networks.

However, maintaining high QoS alone is insufficient to ensure reliable and secure internet services. Network security mechanisms, particularly firewall configurations and access control policies, play a crucial role in securing networks. A firewall acts as a barrier that monitors and filters incoming and outgoing traffic based on predefined security rules, thereby preventing unauthorized access and mitigating potential threats. Similarly, access control mechanisms regulate user privileges within the network, ensuring that only authorized individuals can utilize specific resources. When properly configured, firewall and access control policies not only strengthen security but also contribute to the stability of QoS by reducing the risk of malicious traffic that may cause congestion or packet loss.

Mikrotik routers provide an integrated platform for managing both QoS and security mechanisms cost-effectively. Their flexible configuration allows administrators to implement traffic shaping through token bucket methods while simultaneously enforcing

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

firewall rules and user-based access control. This dual approach ensures that educational institutions, such as vocational schools, can maintain stable internet performance, optimize bandwidth allocation, and protect their networks from security threats. Consequently, Mikrotik offers a practical and efficient solution for small- to medium-scale networks seeking to balance performance quality and security.

In line with these prior works, this study focuses on evaluating the Quality of Service (QoS) of internet networks using parameters such as delay, jitter, packet loss, and throughput. Additionally, the research utilizes the token bucket mechanism for traffic shaping while integrating firewall and access control policies in Mikrotik, aiming to enhance both network performance and security.

2. RESEARCH METHOD

This research adopts the Network Development Life Cycle (NDLC) model as the framework for system development. NDLC is a structured methodology used to design and build network infrastructures [19]. The proposed model generally consists of five sequential stages: baseline analysis, network topology design, firewall implementation and configuration, post-firewall QoS measurement, evaluation and optimization.

2.1. Baseline Analysis Stage

At this stage, an assessment of the existing network conditions at SMK Negeri 1 Bandar Lampung was conducted. The analysis involved two main activities:

a) Field study: Direct observations and interviews were carried out with network administrators at the school to examine the current condition of the network infrastructure.
b) Existing performance measurement: Internet performance was evaluated by monitoring activities such as downloading and uploading.

The results of the analysis indicated that access points with high numbers of users experienced noticeable declines in internet speed. In contrast, access points with fewer users showed no significant performance degradation. These findings suggest that the main issue lies in the varying quality and capacity of the access points in use.

To evaluate the initial quality of the school's internet network, a series of performance measurements was conducted using the TIPHON standard as the reference. The assessment focused on four key Quality of Service (QoS) parameters: throughput, delay, packet loss, and jitter. These parameters were measured at different workstations and websites to capture the actual performance of the network under typical usage conditions. The TIPHON classification was then applied to determine the service quality category for each parameter.

Jurnal Teknologi Informasi dan Pendidikan
Volume 18, No. 2, September 2025
https://doi.org/10.24036/jtip.v18i2.1056

2.2. Network Topology Design

At this stage, the network topology for SMK N 1 Bandar Lampung is designed to illustrate the placement and interconnection of network devices. The topology consists of an ISP modem connected to a Mikrotik router, which functions as the firewall. The router is then linked to a 16-port hub that distributes the network connection to several laboratory computers (PC Lab 1, PC Lab 2, PC Lab 3, up to PC Lab n). Additionally, a wireless access point (Tenda N301) is connected to the hub to provide wireless connectivity for mobile devices, such as smartphones. This topology, as shown in Figure 1, ensures that all traffic passes through the Mikrotik router for monitoring, filtering, and security management.

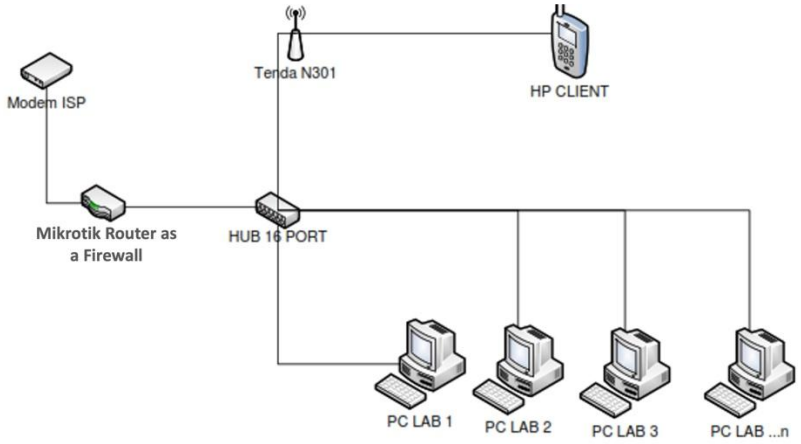

Figure 1. Firewall design of SMK Negeri 1 Bandar Lampung

2.3. Firewall Implementation and Configuration

At this stage, the security requirements of the network are identified, which involves configuring the MikroTik firewall and defining security rules, including filtering and access control. The firewall design is then aligned with the existing network topology of SMK Negeri 5 Bandar Lampung to ensure compatibility and effectiveness as designed in Figure 1. The logical process of packet filtering is illustrated in Figure 2. It shows how the system decides whether to block, drop, or forward packets based on predefined firewall rules. The configuration results are documented in the form of graphical representations of the Mikrotik settings, which illustrate the applied rules, as shown in Figure 3.

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

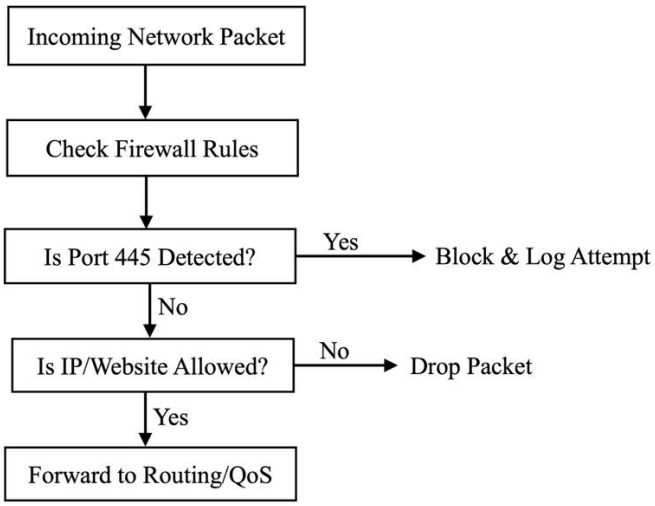

Figure 2. Flowchart of Mikrotik firewall filters packets

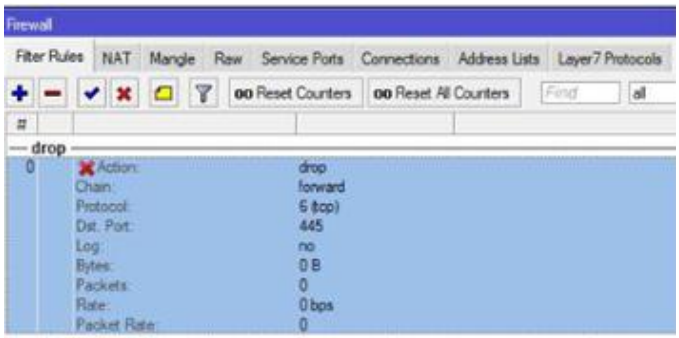

Figure 3. Graphical representations of configuration results

Additionally, a bandwidth management mechanism is incorporated using the Simple Queue feature in MikroTik. This configuration is intended to regulate traffic flow, prevent congestion, and ensure fair bandwidth allocation among users, as shown in Figure 4. The bandwidth allocation logic applied through Mikrotik's Simple Queue is summarized in Algorithm 1, which defines the bandwidth limit and priority levels for each user group. To enhance network security, port 445 is blocked since it is commonly used by the Server Message Block (SMB) service and Microsoft Active Directory [19]. This port is not required in the laboratory environment and is known to have critical security vulnerabilities, such as Remote Code Execution (RCE). Therefore, a MikroTik firewall rule is applied to block port 445 to prevent potential exploitation and unauthorized access [20]. Authenticated users are automatically assigned bandwidth limitations to prevent excessive consumption of internet resources. This mechanism ensures fair distribution of bandwidth among all users and mitigates the risk of bandwidth monopolization by a single client.

Jurnal Teknologi Informasi dan Pendidikan
Volume 18, No. 2, September 2025
https://doi.org/10.24036/jtip.v18i2.1056

Figure 4. Graphical representations of a simple queue configuration

Algorithm 1. Bandwidth Allocation Procedure (Pseudocode)

```
Input: User_Group ∈ {Principal, Teacher, Student}
Output: Assigned_Bandwidth
Begin
  if User_Group = Principal then
     Assigned_Bandwidth ← 3 Mbps
  else if User_Group = Teacher then
     Assigned_Bandwidth ← 1 Mbps
  else if User_Group = Student then
     Assigned_Bandwidth ← 0.5 Mbps
  end if
  Apply Simple_Queue(Assigned_Bandwidth)
  Monitor throughput, delay, packet loss, and jitter
  if congestion_detected then
     Adjust bandwidth dynamically using a priority queue
  end if
End
```

2.4. Post-Firewall QoS Measurement

Following the deployment of the firewall, Quality of Service (QoS) measurements are carried out to assess the impact of the firewall configuration on network performance. The testing process involves re-evaluating QoS parameters such as delay, jitter, packet loss, and throughput. This step provides a comparative analysis of network performance before and after firewall implementation.

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

2.5. Evaluation and Optimization

The results of the QoS measurements are analyzed to compare pre- and post-firewall performance. This analysis highlights the trade-offs between enhanced network security and potential performance degradation. Based on the findings, optimization of firewall rules and configurations is conducted to minimize negative impacts on QoS while maintaining adequate security levels.

3. RESULTS AND DISCUSSION

3.1. Firewall System Performance Evaluation

Based on the implementation and testing process, several findings from the experiment provide conclusions for this study. During the attack simulation stage, the researcher tested network traffic using port 445 to observe whether the router was capable of detecting and blocking the attempted intrusion. As shown in Figure 5, the router successfully blocked access to port 445 traffic passing through it. This action effectively terminated client PCs from performing file-sharing or printer-sharing activities. However, this did not pose any issues since such activities are not required within the laboratory environment.

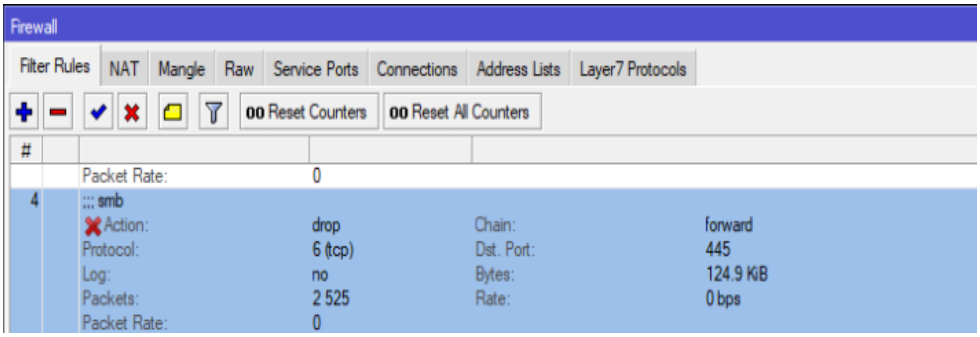

Figure 5. Blocking port 445 with a firewall rule

3.2. QoS Measurement Post-Firewall

After the firewall was implemented, the Quality of Service (QoS) of the network was re-evaluated to compare performance before and after firewall deployment. The measurements focused on four main parameters: delay, jitter, packet loss, and throughput.

The QoS measurements were conducted separately in three different laboratories; the QoS measurement results for the Adm. Room are presented in Figure 6. The bar chart compares throughput, delay, packet loss, and jitter values before and after the firewall implementation.

Jurnal Teknologi Informasi dan Pendidikan
Volume 18, No. 2, September 2025
https://doi.org/10.24036/jtip.v18i2.1056

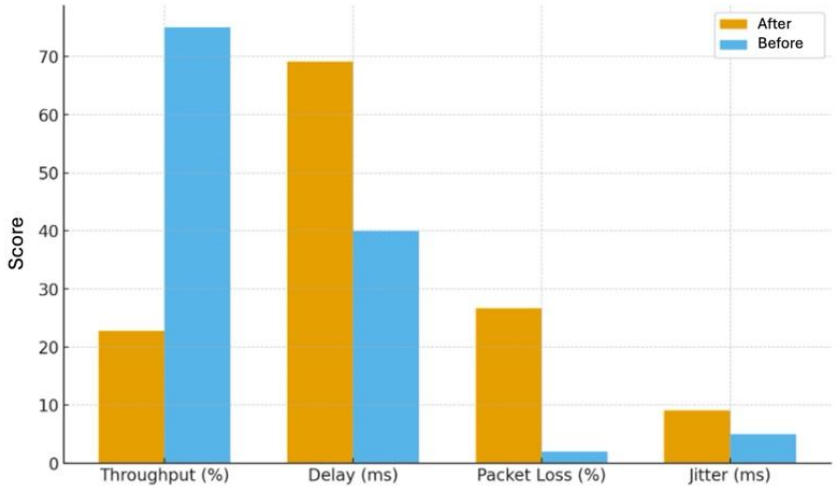

Figure 6. The QoS measurement results for the Adm. Room

The QoS measurement results for TKJ3 Lab. are shown in Figure 7, illustrating the differences in throughput, delay, packet loss, and jitter between the pre-firewall and post-firewall conditions.

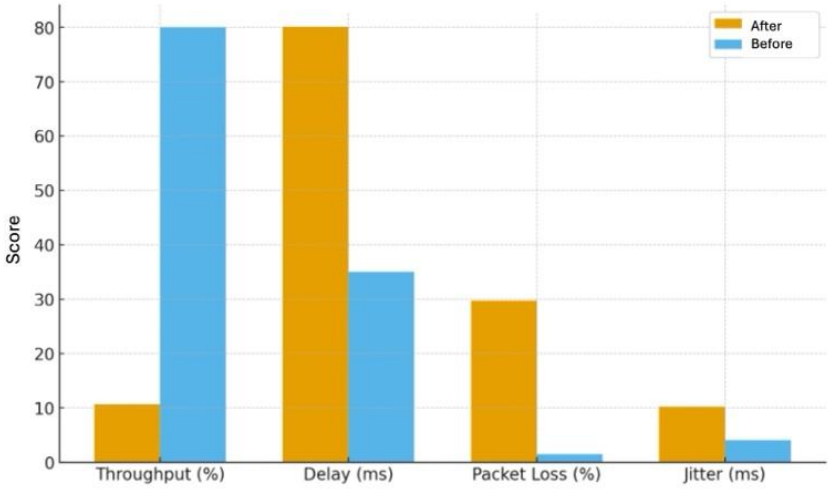

Figure 7. The QoS measurement results for the TKJ3 Lab.

The QoS measurement results for MM2 Lab. are displayed in Figure 8. Like the previous results, the graph highlights the changes in QoS parameters before and after the firewall deployment.

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

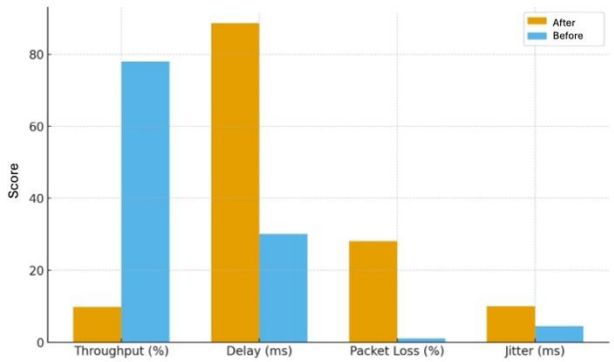

Figure 8. The QoS measurement results for the MM2 Lab.

The results showed that, although the firewall introduced a slight increase in delay and jitter due to the filtering and inspection process, the overall network performance remained within acceptable limits for the laboratory environment. To clearly demonstrate the impact of the implemented firewall, Table 1 provides a comparative summary of QoS parameters measured before and after the firewall deployment. The comparison includes key metrics such as delay, jitter, packet loss, and throughput, enabling a direct evaluation of performance changes.

Table 1. Comparison of QoS Parameters Before and After Firewall & Bandwidth Management Configuration

Parameters	Before Firewall & Bandwidth Management	After Firewall & Bandwidth Management	TIPHON Category
Throughput	9–23% (± 294–463 kbps) – Poor	Stable > 1000 kbps	Before: Poor After: Good/Very Good
Delay	66–99 ms – Very Good	< 300 ms (stable)	Remains Very Good
Packet Loss	26–30% – Poor	0–2% (maximum)	Before: Poor After: Very Good-
Jitter	9–10 ms – Good	0.001–2297 ms	Still Good (although variable)
QoS Index	2.14 – Fair	> 3.0 (significant improvement)	From Fair to Good

According to Table 1, it can be observed that the implementation of firewall rules and bandwidth management significantly improved the overall Quality of Service (QoS) on the network. The throughput, which was previously in the poor category (9–23% or approximately 294–463 kbps), increased to a stable rate of more than 1000 kbps, falling into the good to very good category according to TIPHON standards.

In terms of delay, the network performance remained consistent in the very good category, with average values below 300 ms both before and after the configuration. Packet loss experienced the most notable improvement, decreasing drastically from 26–30% (poor) to only 0–2% (very good). Jitter performance was relatively stable, still categorized as good, although post-configuration values varied more widely.

Finally, the overall QoS index improved from 2.14 (fair) to above 3.0, which places the network performance into the good category. These results clearly demonstrate that the combined firewall configuration and bandwidth management strategy not only enhanced security by blocking unnecessary or vulnerable ports but also optimized bandwidth distribution, leading to more stable and reliable network performance.

In addition to the QoS comparison results, a series of internet speed tests was conducted to further validate the improvements in throughput performance. The speed test trials were conducted five times, where devices 1 through 10 simultaneously performed speed tests. The speed test results are presented in Table 2, showing that the post-firewall configuration consistently achieved higher download and upload speeds compared to the pre-configuration condition. These outcomes support the findings from the QoS measurements, confirming that the firewall and bandwidth management setup not only optimized traffic distribution but also provided more stable and reliable internet access for end users.

Table 2. The speed tests result

No	Device	Download Speed Average (kbps)	Upload Speed Average (kbps)
1	Device 1	732	97
2	Device 2	706	89
3	Device 3	718	96
4	Device 4	700	95
5	Device 5	728	98
6	Device 6	720	92
7	Device 7	714	94
8	Device 8	721	97
9	Device 9	716	93
10	Device 10	726	96

3.3. Bandwidth Allocation Analysis

In addition to the speed test evaluation, the analysis of bandwidth allocation was carried out to examine how effectively the firewall and bandwidth management rules distribute network resources among different user groups. Table 3 presents the bandwidth allocation scheme implemented in the network, which categorizes users into three groups: School Principal, Teachers, and Students, each with different levels of bandwidth capacity. This allocation ensures fairness, prevents bandwidth monopolization, and reflects the prioritization of network usage according to institutional needs.

Table 3. Bandwidth allocation

No	User Categories	Bandwidth
1	School Principal	3 Mbps
2	Teachers	1 Mbps
3	Students	0,5 Mbps

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

The bandwidth allocation scheme divides network capacity into three main categories of users: the School Principal, Teachers, and Students. The School Principal is allocated the highest bandwidth capacity of 3 Mbps, reflecting the need for uninterrupted access to administrative systems, online meetings, and critical decision-making tools. Teachers are assigned 1 Mbps, which provides sufficient capacity for accessing online learning resources, managing digital classrooms, and supporting instructional activities. Meanwhile, Students are allocated 0.5 Mbps per user, which is adequate for essential tasks such as browsing, accessing e-learning platforms, and submitting assignments.

This hierarchical allocation ensures that bandwidth distribution aligns with organizational priorities. By prioritizing higher bandwidth for administrative and teaching functions while still providing fair access to students, the system achieves both efficiency and fairness. As shown in the bandwidth allocation algorithm (Algorithm 1), the applied rule set ensured proportional bandwidth distribution. Evaluation results confirmed that throughput stability improved accordingly. Moreover, this approach prevents bandwidth monopolization by any single group, supporting balanced network utilization across the institution.

4. CONCLUSION

The implementation of the MikroTik RouterBoard RB1100AHx4 as the main router server at SMK Negeri 1 Bandar Lampung has not yet reached optimal performance. Bandwidth capacity remains limited at 200 Mbps, resulting in poor throughput and significant packet loss under heavy traffic, even though delay performance was categorized as very good, and jitter results were generally satisfactory according to TIPHON standards. The overall QoS index reached 2.14, which falls under the "fair" category, indicating that the network has not yet achieved the expected "very good" level (3.8–4.0). These findings highlight the need for both infrastructure improvements and traffic management strategies to address instability and congestion.

On the other hand, the implementation of firewall and Access Control List (ACL) mechanisms demonstrated positive results. The firewall successfully detected and blocked malicious attempts on port 445, while ACL-based bandwidth allocation ensured fair distribution among user groups (Principal: 3 Mbps, Teacher: 1 Mbps, Student: 0.5 Mbps). Speed test results confirmed that bandwidth distribution was balanced, preventing monopolization. Furthermore, QoS performance after applying ACL improved significantly, with stable throughput above 1000 kbps, packet loss reduced to 0–2%, delay maintained under 300 ms, and jitter within acceptable limits. Additional access control through address lists further enhanced network management by restricting unwanted website access.

This study's novelty lies in the integration of the NDLC development framework with fine-grained access control and QoS optimization, specifically adapted to the dynamic

environment of a vocational school network. Such integration provides a structured and replicable approach that bridges the gap between theoretical QoS implementation and real-world educational settings.

For future work, it is recommended to expand the system by integrating centralized authentication using a RADIUS server to improve scalability and security in user management. Additionally, upgrading the bandwidth capacity and hardware specifications would be beneficial to handle higher traffic demands. Future studies could also explore the use of automated monitoring and adaptive QoS algorithms to dynamically adjust bandwidth allocation based on real-time usage patterns, ensuring more stable and intelligent network performance across different user groups.

REFERENCES

[1] L. N. Das Monu, "Optimal packet routing with multiple demands and link lines," *Lecture Notes in Networks and Systems*, vol. 321, pp. 177–185, 2022, doi: 10.1007/978-981-16-5987-4_19.

[2] M. K. R. E. Atmawijaya, D. E. Siringoringo, F. Ricoras, R. D. Nainggolan, and S. B. G. Putra, "Criminal liability for the provision of illegal wifi telecommunications services," *Indonesian Journal of Criminal Law Studies*, vol. 8, no. 1, pp. 135–164, 2023, doi: 10.15294/ijcls.v8i1.43273.

[3] J. F. Ariza, J. P. Saldarriaga, K. Y. Reinoso, and C. D. Tafur, "Information and communication technologies and academic performance in high school in Colombia," *Lecturas de Economía*, no. 94, pp. 47–86, 2021, doi: 10.17533/UDEA.LE.N94A338690.

[4] J. Yu, A. Y. Alhilal, T. Zhou, P. Hui, and D. H. K. Tsang, "Attention-Based QoE-Aware digital twin empowered edge computing for immersive virtual reality," *IEEE Transactions on Wireless Communications*, vol. 23, no. 9, pp. 11276–11290, Sept. 2024, doi: 10.1109/TWC.2024.3380820.

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

[6] K. K. Saleh, H. P. A. Tjahyaningtijas, N. Nurhayati, and L. Rakhmawati, "Quality of service (qos) comparative analysis of wireless network," *INAJEEE (Indonesian Journal of Electrical and Electronics Engineering*, vol. 5, no. 2, pp. 30–37, 2022.

[7] I. S. N. Nisa, M. R. Saputro, T. F. Nugroho, and A. R. Lahitani, "Analisis Quality of Service (QoS) menggunakan standar parameter tiphon pada jaringan internet berbasis wi-fi Kampus 1 Unjaya," *Teknomatika: Jurnal Informatika dan Komputer*, vol. 17, no. 1, pp. 1–9, 2024, doi: 10.30989/teknomatika.v17i1.1307.

[8] C. Pan, X. Cui, C. Zhao, Y. Wang, and Y. Wang, "An adaptive network congestion control strategy based on the change trend of average queue length," *Computer Networks*, vol. 250, 110566, 2024, doi: 10.1016/j.comnet.2024.110566.

[9] M. Sharafat and B. Kulambayev, "The role of QoS at the OSI model layers," in Quality of Service (QoS) – Challenges and Solutions. London, U.K.: IntechOpen, Oct. 2024, doi: 10.5772/intechopen.1007182.

[10] A. M. Altameemi and K. A. Nassar, "Congestion control mechanisms and techniques in computer network: a review," *in Proc. 2022 Int. Conf. Data Sci. Intell. Comput*. (ICDSIC), Karbala,

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

Iraq, 2022, pp. 46–51, doi: 10.1109/ICDSIC56987.2022.10076206.

[11] T. Mazhar, M. A. Malik, S. A. H. Mohsan, Y. Li, I. Haq, S. Ghorashi, F. K. Karim, and S. M. Mostafa, "Quality of Service (QoS) performance analysis in a traffic engineering model for next-generation wireless sensor networks," *Symmetry*, vol. 15, no. 2, p. 513, 2023, doi: 10.3390/sym15020513.

[12] Z. Wu, H. Qin, X. Song, G. Fu, and J. Li, "The improvement of scheduling algorithm based on token bucket and weighted fair queue," *in Proc. 2023 12th Int. Conf. Inf. Commun. Technol. (ICTech)*, 2023, pp. 66–72, doi: 10.1109/ICTech58362.2023.00024.

[13] M. Beshley, N. Kryvinska, M. Seliuchenko, H. Beshley, E. M. Shakshuki, and A.-U.-H. Yasar, "End-to-end QoS 'smart queue' management algorithms and traffic prioritization mechanisms for narrow-band internet of things services in 4G/5G networks," *Sensors*, vol. 20, no. 2324, 2020.

[14] Y. B. Pello and R. Efendi, "Analisis Quality of Service Menggunakan metode hierarchical token bucket (Studi Kasus: FTI UKSW)," *JIKO (Jurnal Informatika dan Komputer)*, vol. 4, no. 3, pp. 193–198, 2021, doi: 10.33387/jiko.

[15] T. O. Sidqi, I. Fitri, and N. D. Nathashia, "Implementasi manajemen bandwidth menggunakan metode HTB (Hierarchical Token Bucket) pada jaringan mikrotik," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 6, no. 1, pp. 132–138, Jun. 2021.

[16] R. K. Abdullah, S. P. Wibowo, and T. P. Fiqar, "Analisis QoS jaringan internet ITK dengan metode Hierarchical Token Bucket," *Progresif: Jurnal Ilmiah Komputer*, vol. 20, no. 1, pp. 280–293, Feb. 2024.

[17] H. Kusbandono, T. Lestariningsih, and T. Septianto, "Comparative analysis of Quality of Service (QoS) on WLAN network bandwidth management using HTB method with PCQ," *East Asian Journal of Multidisciplinary Research*, vol. 3, no. 10, pp. 4797–4810, 2024, doi: 10.55927/eajmr.v3i10.11675.

[18] K. Deo, K. Chaudhary, and M. Assaf, "Adaptive quality of service for packet loss reduction using OpenFlow meters," *PeerJ Computer Science*, vol. 10, Art. no. e1848, 2024, doi: 10.7717/peerj-cs.1848.T.

[19] F. H. P. Prasetyo, E. Infitharina, and M. Febriyansyah, "Penerapan Metode Network Development Life Cycle (NDLC) dalam Pengembangan Jaringan Komputer," *Journal of Informatics and Communication Technology (JICT)*, vol. 7, no. 1, pp. 80–87, 2025.

[20] H. M. Zangana, M. Omar, J. N. Al-Karaki, and D. Mohammed. "Comprehensive review and analysis of network firewall rule analyzers: Enhancing security posture and efficiency," Redefining Security with Cyber AI, pp. 15 – 36, 2024. doi: 10.4018/979-8-3693-6517-5.ch002.