Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th October 2025. Vol. 5. No. 1; e-ISSN: 2808-4519

Implementation of Bandwidth Management Using Website-Based Hierarchical Token Bucket (HTB) Method at PT. Fatih Amanah Sejahtera

Farchan Maulidhin[1*], Jafar Shadiq[2]

[1,2]*Informatics engineering, Universitas Bina Insani, Indonesia*
farchanmaulidhin@gmail.com[1*], jafarshadiq@binainsani.ac.id[2]

Abstract

PT. Fatih Amanah Sejahtera, a sharia property company, faced uneven internet bandwidth distribution and a lack of centralized monitoring, impacting productivity. This research aimed to implement effective bandwidth management and develop a web-based monitoring system for near real-time monitoring. The method used was the Network Development Life Cycle (NDLC) up to the monitoring stage, with PPPoE authentication for PCs/Laptops and Hotspot for mobile devices, and bandwidth management using Queue tree with Hierarchical Token Bucket (HTB). A web application was developed using Laravel for monitoring and management via Mikrotik API. The results demonstrated even and proportional bandwidth allocation, significant improvements in Quality of Service (QoS) parameters, and a functional web monitoring system for efficient network management, thereby enhancing company productivity.

Keywords: *Bandwidth Management, Mikrotik, NDLC, Queue tree, Web Monitoring.*

1. Introduction

PT. Fatih Amanah Sejahtera (Fatih Group) is a sharia property company whose daily operations are highly dependent on internet access. Divisions such as Marketing, Sales, Content Creation, Finance, Human Resources, and Production rely on the internet for communication, data processing, and other essential tasks. With the internet's unlimited reach, employees can easily exchange information, collaborate, and establish partnerships. However, the increasing reliance on internet connectivity also raises the importance of bandwidth management to ensure smooth and stable operations across the organization [1].The intensity of internet usage across all divisions often results in problems with connection stability, particularly in bandwidth distribution. Some divisions may experience smooth and uninterrupted access, while others encounter slow or limited connectivity. This inequality in access directly impacts work productivity and efficiency [2]. Moreover, the absence of a web-based system capable of near real-time bandwidth monitoring further complicates the situation, often leading to inefficient use of network resources. Without proper monitoring and control, the company faces challenges in maintaining an equitable and reliable internet experience for all users [3].

To solve these issues, this research proposes a structured and comprehensive network management solution. Authentication methods will be tailored according to the type of device: Point-to-Point Protocol over Ethernet (PPPoE) will be applied for laptops and PCs to create separate connection sessions for each device, making it easier to monitor and control usage [4]. Meanwhile, authentication for smartphones will be managed through a Hotspot system. This distinction ensures that all users can be properly identified, controlled, and allocated bandwidth according to their needs [5].In addition, bandwidth management will be enhanced using the Queue Tree mechanism with the Hierarchical Token Bucket (HTB) method. This approach provides dynamic, fair, and proportional bandwidth allocation across divisions. Complementing this setup, a web-based management application will be developed, offering real-time traffic monitoring, simplified configuration, and efficient policy enforcement [6]. With this solution, network administrators can manage resources more effectively without direct access to Mikrotik devices, ensuring structured, transparent, and efficient network management that supports the company's operational goals [7].

2. Research Methodology

2.1. Network Development Life Cycle (NDLC)

The development model used in this research is the Network Development Life Cycle (NDLC). It is a method applied in the development or creation of a network infrastructure that enables the monitoring of network statistics and performance. The Network Development Life Cycle consists of six stages: analysis, design, simulation prototyping, implementation, monitoring, and management [8].

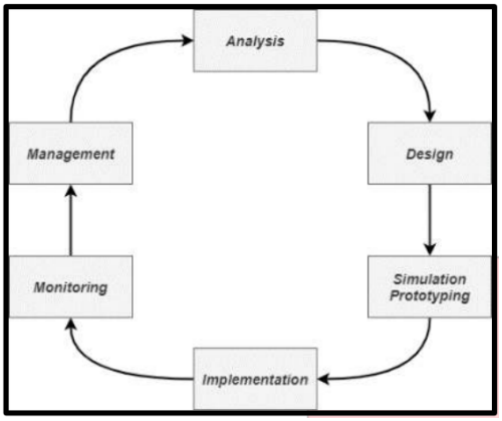

Fig. 1: Network Development Life Cycle (NDLC)

The stages of the NDLC method are explained as follows:

1. Analysis:
   Identification of network problems and requirements based on observations and interviews, consisting of:
   Problems: Unequal bandwidth distribution across divisions and the absence of a centralized monitoring system.
   Hardware Requirements: Mikrotik RB750Gr3 router as the main gateway, PPPoE & Hotspot server, and Queue Tree/HTB manager.
   Software Requirements: A Laravel-based web application to monitor and manage the network through API integration with Mikrotik.
   Bandwidth Needs: 10 Mbps for standard divisions (Marketing, Sales, Finance, HR) and 30 Mbps for high-demand divisions (Content and Production).
2. Design:
   Creation of a detailed network and system design, consisting of:
   Network Topology: Hybrid model combining star and wireless extensions, with Mikrotik as the center.
   Monitoring Website: Web interface design to display traffic statistics, manage users, and apply site-blocking policies.
3. Simulation Prototyping:
   Testing configurations and applications before real implementation, consisting of:
   Router Simulation: Using VirtualBox to run Mikrotik RouterOS for PPPoE, Hotspot, and bandwidth management testing.
   Web Application: Developing the Laravel-based monitoring system on localhost and integrating it with the Mikrotik virtual router via API.
4. Implementation:
   Applying the validated prototype in the real environment, consisting of:
   Network Setup: Installation and configuration of Mikrotik Router and Access Points, implementing IP, NAT, PPPoE, Hotspot, and Queue Tree.
   Website Deployment: Migrating the Laravel application to production hosting, configuring the database, adjusting API connections, and performing final testing.
5. Monitoring:
   Continuous observation of bandwidth usage and network performance using the web dashboard. This includes Quality of Service (QoS) testing and real-time traffic monitoring.
6. Management:
   Ongoing administration of the implemented system, consisting of:
   User Management: Adding/removing PPPoE and Hotspot accounts.
   Policy Control: Applying site-blocking rules and adjusting bandwidth allocation as needed.
   Efficiency: Ensuring fair, dynamic, and proportional bandwidth distribution using PPPoE, Hotspot, Queue Tree, and HTB methods.

3. Result and Discussion

The current network topology at PT. Fatih Amanah Sejahtera distributes internet connections directly to each division without structured bandwidth management. This approach results in unequal access among users, particularly when multiple divisions are active simultaneously, leading to unstable connectivity. The existing network architecture also lacks user authentication and prioritization mechanisms, which causes uncontrolled bandwidth usage and performance degradation during peak traffic [9].

To address these issues, a new hybrid topology was designed, combining a star model with wireless extensions. In this proposed system, the internet connection from the Internet Service Provider (ISP) is routed through a Mikrotik device that serves as the central controller. The Mikrotik router manages bandwidth, network security, and IP allocation, while distributing connections evenly across two floors using Wireless Routers configured with PPPoE for laptops and PCs, and Hotspot authentication for mobile devices [10]. Supported by a 100 Mbps ISP connection from MyRepublic with a 1:1 upload/download ratio, this architecture ensures efficient bandwidth management and real-time monitoring through the integration of a web-based system with Mikrotik, resulting in more stable and controlled network performance [11].

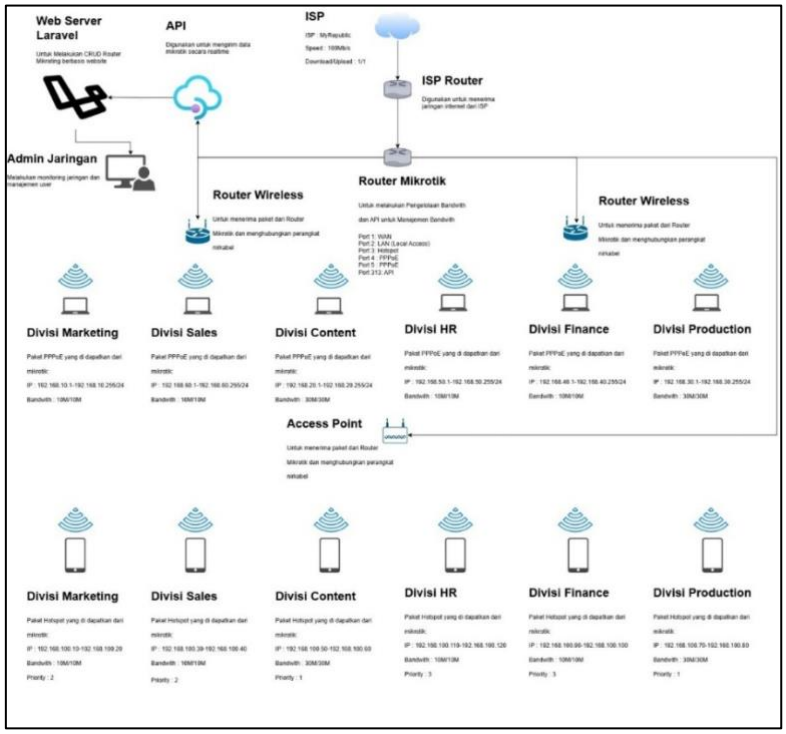

Fig. 2: Proposed Network Architecture

3.1. Network Hardware and Software Specifications Requirements

The hardware and software specifications used in the proposed network design are essential to support effective bandwidth management and monitoring. The hardware includes a Mikrotik router as the central network manager, an ISP modem as the main internet gateway, and access points for connection distribution. The software consists of the operating system, Winbox for Mikrotik configuration, and a web-based application developed for monitoring and management [12]. The complete proposed hardware and software specifications are as follows:

Table 1: Proposed Hardware and Software Specifications

No	Hardware	Model	Function
1	Mikrotik Router	RB750Gr3 (hEX)	Functions as the central network management device, handling bandwidth allocation using Queue Tree and HTB. It also serves as the PPPoE and Hotspot server for user authentication, as well as the main gateway in the network system.
2	TP-Link Access Point	TL-WR840N	Used as an access point for Wi-Fi distribution. Operated in Access Point mode to broadcast the Hotspot network, allowing client devices to connect and authenticate through the Hotspot feature on Mikrotik.
3	ZTE Access Point	F609	Used as an access point for Wi-Fi distribution. Operated in Access Point mode to provide connections for PPPoE users, where authentication is handled through the PPPoE server on Mikrotik.
4	LAN / UTP Cable	Cat6 UTP	Connects network devices.
5	RJ-45 Connector	RJ-45 Standard	Serves as the connector for LAN cables to plug into network ports.
6	Crimping Tool	Standar RJ-45 Crimping Tool	Used to attach RJ-45 connectors to UTP cables.
7	LAN Tester	LAN Cable Tester	Used to test LAN cable connections to ensure proper wiring.
8	Mikrotik Power Adapter	12V DC 1A	Provides power to the Mikrotik router.
9	Extension Power Socket	4 Outlets	Provides additional power sources for network devices.

3.2. Mikrotik Router Configuration

The first step in configuring the Mikrotik RB750r2 router as the central network manager is setting up the basic configuration, IP addresses, and NAT for internet access. The router is reset to default to avoid conflicts, and interfaces are renamed for clarity: "WAN-Ether1" (receiving IP from ISP via DHCP Client), "LAN-Ether2" (10.10.10.1/24 for the local network), "Hotspot-Ether3" (192.168.100.1/24 for

the Hotspot network), and "PPPoE-Ether5." This setup provides unique identities for each network segment, enabling proper routing, gateway functionality, and easier traffic management for administrators. DHCP servers are configured to automatically assign IP addresses: dhcp1 for LAN (10.10.10.2–10.10.10.254) and dhcp2 for Hotspot (192.168.100.2–192.168.100.14), along with DNS servers (8.8.8.8, 1.1.1.1) and appropriate gateways to ensure smooth connectivity [13].

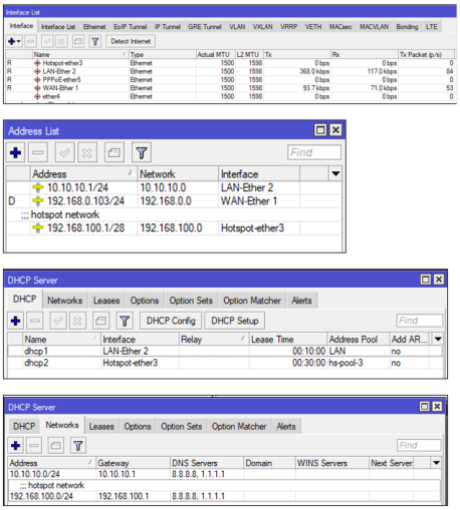

Fig. 3: Mikrotik Router Configuration Part 1

For internet access, NAT (Network Address Translation) is applied using masquerade on "WAN-Ether1," allowing private IP addresses in the local network to be translated into a public IP for outbound traffic. A specific NAT masquerade rule is also configured for the Hotspot network (192.168.100.0/28), ensuring Hotspot clients can access the internet as well. This configuration enables seamless connectivity for both LAN and Hotspot users, with automatic IP management and internet access through the public IP provided by the ISP [14].

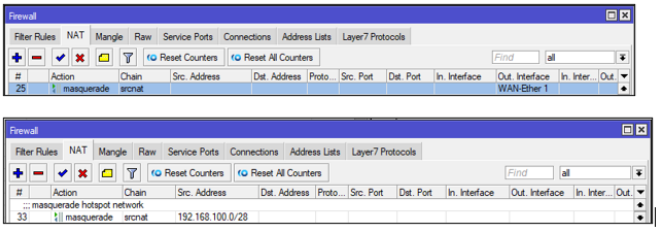

Fig. 4: Mikrotik Router Configuration Part 2

3.3. User Authentication Implementation

The user authentication implementation on the MikroTik router distinguishes and manages internet access based on device type and division needs: PPPoE for laptops/PCs and Hotspot for mobile devices. A PPPoE Server is configured on ether4 and ether5 with division-based profiles. Divisions like Marketing, Sales, Content, and Production use standard DNS servers (8.8.8.8, 1.1.1.1), while Finance and HR divisions are filtered via NextDNS through DNS-over-HTTPS. Each profile includes specific IP address pools, and PPPoE Secrets ensure that only registered users with unique usernames and passwords can establish connections, providing structured IP allocation and controlled access [15].

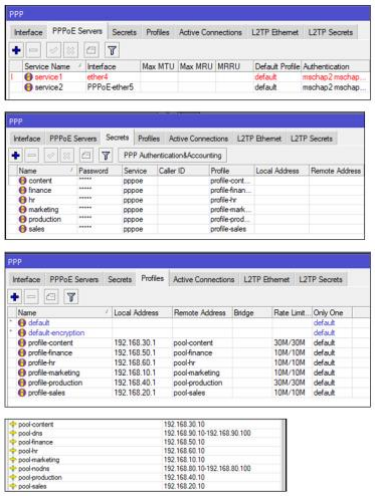

Fig. 5: User Authentication Implementation Part 1

DNS configuration integrates NextDNS filtering for selected divisions. The router is set to allow remote DNS requests with standard servers, while Finance and HR traffic is redirected to NextDNS using firewall NAT rules for content filtering. Other divisions bypass this

redirection and use standard DNS without restrictions. This setup enables domain name resolution and enforces tailored filtering policies per division, simplifying the application of firewall rules for targeted IP groups [16].

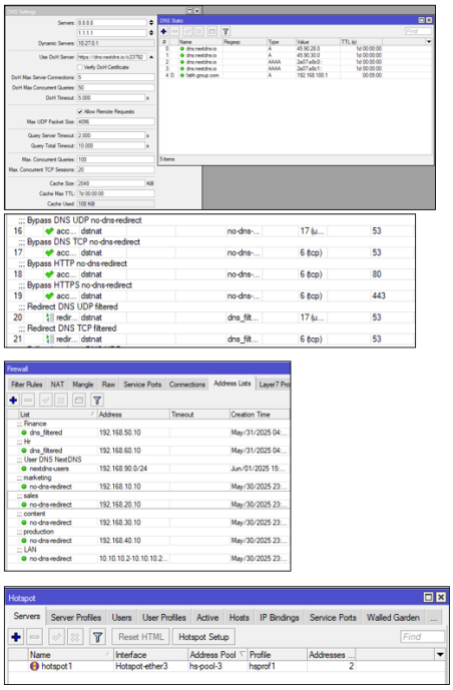

Fig. 6: User Authentication Implementation Part 2

For mobile devices, a Hotspot Server is implemented on the Hotspot-ether3 interface with a custom login page (fatih.group.com). A dedicated Wi-Fi SSID broadcasts the Hotspot network, redirecting connected users to the login portal for authentication. Each division has its own Hotspot user profile with separate IP address pools and optional rate limits. This ensures that only authorized users with valid credentials can access the network, while maintaining clear segmentation and control across different user groups.

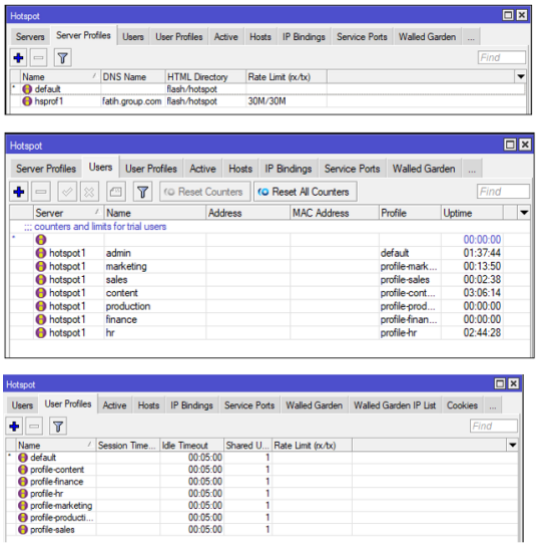

Fig. 7: User Authentication Implementation Part 3

3.4. Bandwidth Management Implementation (Queue Tree, Hierarchical Token Bucket (HTB), and PPPoE)

The bandwidth management is optimized through the combined use of Queue Tree with the Hierarchical Token Bucket (HTB) method for Hotspot users and Rate Limit on PPPoE profiles for laptop and PC users. For Hotspot traffic, Firewall Mangle rules are applied to mark packets based on the IP range of each division (e.g., Marketing, Sales, Finance, etc.). These marks are then used in a Queue Tree configuration, where a parent queue limits the total Hotspot bandwidth, and child queues distribute it across divisions. Each division receives a defined maximum bandwidth and priority level, ensuring fair allocation and traffic prioritization during congestion.

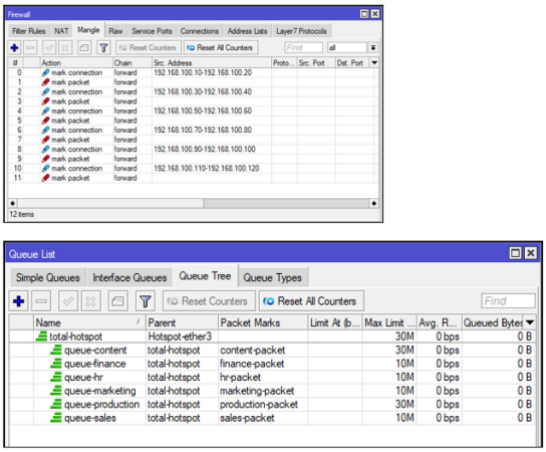

Fig. 8: Bandwidth Management Implementation Part 1

For PPPoE users, bandwidth is controlled directly through Rate Limits defined in each PPP profile. Divisions such as Marketing, Sales, Finance, and HR are assigned 10 Mbps, while Content and Production divisions receive 30 Mbps. This setup guarantees consistent upload and download speeds per division, ensuring structured bandwidth distribution across both Hotspot and PPPoE connections.

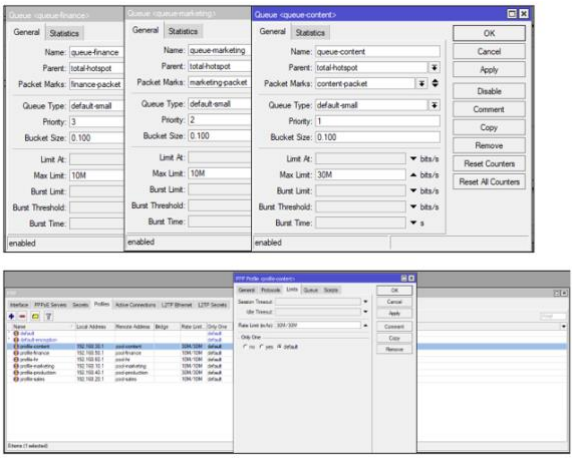

Fig. 9: Bandwidth Management Implementation Part 2

3.5. Web-Based Monitoring System Implementation

The web-based network monitoring system was developed as a centralized platform for administrators to oversee bandwidth usage and manage Mikrotik configurations without direct device access. Built using the Laravel V9.52.20 framework with PHP V8.1.25 and MySQL managed via phpMyAdmin, the application integrates database design, user interface development, and Mikrotik API interaction to provide effective monitoring and control.

Fig. 10: Web-Based Monitoring System

3.6. Network Performance Testing (Quality of Service – QoS) and Bandwidth Allocation

The QoS testing aimed to verify that bandwidth was distributed according to the configured max-limit on the Queue Tree for Hotspot users with HTB and the Rate Limit applied to PPPoE profiles for laptops and PCs. Priority settings in the Queue Tree ensured fair bandwidth allocation during network congestion. Testing was conducted over three days with three sessions per day (morning, afternoon, and evening), totaling nine tests to capture accurate performance data under varying conditions. The summarized results demonstrate stable and effective bandwidth management using HTB and Queue Tree for both PPPoE and Hotspot authentication, confirming that bandwidth allocation across divisions was fair, proportional, and supportive of overall company productivity.

Table 2: Bandwidth Testing Results for PPPoE and Hotspot

Division	Device Type	Planned Download (Mbps)	Average Download Result (Mbps)	Planned Upload (Mbps)	Average Upload Result (Mbps)	Priority (*Hotspot*)	Remarks
Marketing	*Hotspot*	10	9.07	N/A	N/A	2	Optimal
Sales	*Hotspot*	10	9.17	N/A	N/A	2	Optimal
Content	*Hotspot*	30	27.97	N/A	N/A	1	Optimal
Production	*Hotspot*	30	28.08	N/A	N/A	1	Optimal
Finance	*Hotspot*	10	9.08	N/A	N/A	3	Optimal
HR	*Hotspot*	10	9.06	N/A	N/A	3	Optimal
Marketing	PPPoE	10	9.38	10	9.15	N/A	Optimal
Sales	PPPoE	10	9.16	10	8.98	N/A	Optimal
Content	PPPoE	30	28.32	30	28.37	N/A	Optimal
Production	PPPoE	30	28.43	30	28.52	N/A	Optimal
Finance	PPPoE	10	8.97	10	9.1	N/A	Optimal
HR	PPPoE	10	9.06	10	8.94	N/A	Optimal

4. Conclusion

Based on the research and implementation of bandwidth management using the Hierarchical Token Bucket (HTB) method with a web-based system at PT. Fatih Amanah Sejahtera, two main conclusions can be drawn. First, the system successfully allocated bandwidth evenly and efficiently by combining PPPoE for laptop/PC users and Hotspot with Queue Tree and HTB for mobile users. Rate Limits in PPPoE profiles and max-limit with priority in Queue Tree ensured proportional bandwidth distribution across divisions. QoS testing results—covering delay, jitter, throughput, and packet loss—were all in the "Very Good" or "Optimal" category, proving stable internet access and improved productivity by solving previous issues of unequal distribution and connection instability. Second, the web-based system developed with the Laravel framework and integrated with the Mikrotik API provided a centralized platform for near real-time monitoring and management. It enabled administrators to view bandwidth statistics, manage PPPoE and Hotspot users, and control blocked sites via DNS filtering, significantly improving efficiency and simplifying network management.

Given the time limitations of this study, several aspects remain unexplored and can be considered for future development. Suggested improvements include adding client application and website monitoring, implementing automatic site blocking based on categories or blacklists, enabling WAN disconnection notifications via email or messaging apps, logging internet speed history for trend analysis, and enhancing the reporting module for detailed historical data per division or user. These enhancements would provide deeper insights, faster response to connectivity issues, and more effective long-term network capacity planning.

References

[1] S. Aminah, "Manajemen Bandwidth dalam Mengoptimalkan Penggunaan Router Mikrotik terhadap Pelayanan Koneksi Jaringan," *Jurnal Informatika Ekonomi Bisnis*, vol. 4, no. 3, pp. 102–106, 2022, doi: 10.37034/infeb.v4i3.144.

[2] L. O. Sari, H. A. Suri, E. Safrianti, and F. Jalil, "Rancang Bangun Sistem Monitoring Bandwidth Server pada PT. Industri Kreatif Digital," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 3, no. 2, pp. 168–179, 2023, doi: 10.57152/malcom.v3i2.914.

[3] M. A. Sabara and A. Prayogi, "Konfigurasi Manajemen Bandwidth Menggunakan Router Mikrotik RB2011UIAS-RM Untuk Mengontrol Penggunaan Internet Di Pt Rekan Usaha Mikro Anda Tegal," *Jurnal POLEKTRO: Jurnal Power Elektronik*, vol. 9, no. 2, pp. 43–46, 2020.

[4] L. O. Sari, E. Safrianti, and D. Wahyuningtias, "Analisis Keamanan Jaringan Berbasis Point to Point Protocol Over Ethernet (PPPoE) Menggunakan Mikrotik," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 4, no. 3, pp. 943–954, 2024, doi: 10.57152/malcom.v4i3.1301.

[5] A. I. Santoso and J. Eriyanto, "Implementasi Fitur Queue Tree, Nat, Mangle Dan Hotspot Pada Router Mikrotik RB1100AHX4 Untuk Mengatur Bandwidth Internet Pada Kampus AMIK Polibisnis Perdagangan," *Gudang Jurnal Multidisiplin Ilmu*, vol. 2, no. 8, pp. 102–109, 2024, doi: 10.59435/gjmi.v2i8.793.

[6] N. Dimas Mahendra and L. Sugiarto, "Seminar Nasional Amikom Surakarta (Semnasa) 2024 Implementasi Dan Optimalisasi Manajemen Bandwidth Pada Mikrotik Berbasis Queue Tree Dan Htb Untuk Stabilitas Jaringan," 2024.

[7] M. J. Komputer *et al.*, "Computer Network Management Using a Mikrotik Router at the Immigration Office Class I TPI Bengkulu City," *Jurnal Media Computer Science*, vol. 1, no. 1, pp. 7–13, 2022.
[8] A. Averian, A. Budiono, and U. Y. K. S. Hediyanto, "Analisis dan Pengoptimalisasi Jaringan Wireless Local Area Network (WLAN) Pada PT.XYZ Dengan Menggunakan Metode Network Development Life Cycle (NDLC)," *e-Proceeding of Engineering*, vol. 10, no. 2, pp. 1325–1330, 2023.
[9] M. S. Anwar, "Analisis QoS (Quality of Service) Manajemen Bandwidth menggunakan Metode Kombinasi Simple Queue dan PCQ (Per Connection Queue) pada Fakultas Teknik Universitas Islam Sumatera Utara," *sudo Jurnal Teknik Informatika*, vol. 1, no. 2, pp. 82–97, 2022, doi: 10.56211/sudo.v1i2.24.
[10] T. Ariyadi, T. Dali Purwanto, and M. M. Fajar, "Tamsir Ariyadi Implementasi Desain Jaringan Hotspot Implementasi Desain Jaringan Hotspot Berbasis Mikrotik Dengan Metode NDLC (Network Development Life Cycle) Pada PT Kirana Permata," *JURNAL ILMIAH INFORMATIKA (JIF)*, vol. 11, no. 2, pp. 189–195, 2023.
[11] N. Asyifah and D. Ramayanti, "Optimasi Kinerja Jaringan Di Smk Al Fudhola Bekasi: Pengaturan Bandwidth Dengan Mikrotik Rb 951ui-2hnd Dan Penerapan Algoritma Simple Queue," *Jurnal Ilmiah ILKOMINFO - Jurnal Ilmu Komputer dan Informatika*, vol. 7, no. 1, pp. 33–46, 2024.
[12] D. Bahtiar *et al.*, "Pengenalan Dasar Instalasi Jaringan Komputer Menggunakan Mikrotik," *Jurnal Kreativitas Mahasiswa Informatika (JATIMIKA)*, vol. 2, pp. 507–518, 2021.
[13] A. Mei Candra and S. Samsugi, "Perancangan Dan Implementasi Controller Access Point System Manager (Capsman) Mikrotik Menggunakan Aplikasi Winbox," *TELEFORTECH : Journal of Telematics and Information Technology*, vol. 2, no. 2, pp. 26–32, 2021.
[14] E. Eben, M. Mukramin, and H. Abduh, "Pengembangan Manajemen Keamanan Jaringan Nirkabel (Wifi) Menggunakan Routerboard Mikrotik Dan Firewall Pada Smk Kristen Palopo," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 12, no. 3, pp. 2229–2238, 2024, doi: 10.23960/jitet.v12i3.4716.
[15] R. Aditya, Y. Rezwan, and A. Walad Mahfuzhi, "Perancangan Hotspot Dan Manajemen Bandwidth Berbasis Mikrotik Dengan Metode Otentikasi Pengguna (User) Menggunakan Mikhmon Server," *Jurnal Mahasiswa Teknik Informatika (JATI)*, vol. 8, no. 4, pp. 10920–10926, 2024.
[16] B. K. Sihotang, S. Sumarno, and B. E. Damanik, "Implementasi Access Control List Pada Mikrotik dalam Mengamankan Koneksi Internet Koperasi Sumber Dana Mutiara," *JURIKOM (Jurnal Riset Komputer)*, vol. 7, no. 2, pp. 229–234, 2020, doi: 10.30865/jurikom.v7i2.2010.