International Journal Software Engineering and Computer Science (IJSECS)
5 (2), 2025, 804-810
Published Online August 2025 in IJSECS (http://www.journal.lembagakita.org/index.php/ijsecs)
P-ISSN: 2776-4869, E-ISSN: 2776-3242. DOI: https://doi.org/10.35870/ijsecs.v5i2.5021.

RESEARCH ARTICLE Open Access

Optimization of Bandwidth Management and Network Security Using PPPoE Method and Intrusion Detection Prevention System

Arham *
Information Systems Study Program, Faculty of Computer Science, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, East Jakarta City, Special Capital Region of Jakarta, Indonesia.
Corresponding Email: muhammadarhamarham2@gmail.com.

Yuma Akbar
Information Systems Study Program, Faculty of Computer Science, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, East Jakarta City, Special Capital Region of Jakarta, Indonesia.
Email: yuma.pjj@gmail.com.

Received: July 11, 2025; Accepted: July 25, 2025; Published: August 1, 2025.

Abstract: Rural internet networks frequently struggle with unstable connections, bandwidth waste, and cyber vulnerabilities. We optimized bandwidth management and network security by implementing Point to Point Protocol over Ethernet (PPPoE) alongside Intrusion Detection and Prevention System (IDPS). PPPoE manages user authentication and dynamic bandwidth allocation, while IDPS identifies and blocks network threats. Our experimental research took place in Sukanegara Village network environment. Testing involved network load simulations and cyber-attack scenarios to evaluate system performance. We compared network metrics before and after implementation, focusing on bandwidth consumption, threat detection rates, and connection stability. PPPoE implementation reduced bandwidth consumption by 35% through controlled user access and fair distribution mechanisms. The IDPS successfully detected 92% of simulated attack attempts, including port scanning, flooding attacks, and unauthorized access attempts. Network latency dropped significantly during peak usage hours, while connection stability improved across all user categories. The combined PPPoE-IDPS solution effectively addresses rural network challenges. The system delivers cost-efficient bandwidth management while maintaining robust security protection. Implementation requires minimal additional hardware and allows management by local technical staff. Our findings support widespread adoption in community and village-scale networks seeking reliable internet infrastructure with adequate security measures.

Keywords: Bandwidth; Network Security; PPPoE; IDPS.

1. Introduction

Internet stands as the abbreviated form of "interconnected-networking," describing the worldwide network of diverse computer systems. TCP/IP protocols govern how these computer networks integrate and communicate. Data moves between computers via IP (Internet Protocol), while TCP (Transmission Control Protocol) maintains proper connection functionality. Users need to register with Internet Service Providers (ISPs) to access the internet, as ISPs bridge local computer networks to the global network. People can connect through either wired or wireless methods [1]. The internet functions as a communication system linking computer networks across the globe. While primarily seen as an information resource, the intern*et al*so serves as an interconnector between computer networks [2]. Rural communities want high-quality internet service to support their daily activities. Residents need stable connections and must choose their ISPs carefully to ensure smooth online operations. Bandwidth management allows network usage regulation tailored to individual user and device requirements [3].

Internet access has become necessary for modern life. People use the internet for work and information sharing across nearly every life domain [4]. Yet ISPs (Internet Service Providers) offer restricted bandwidth due to expensive internet infrastructure costs. Users experience slower and more difficult information access because internet connection demand exceeds available bandwidth capacity [5]. Bandwidth remains the primary concern in computer network technology [6]. Available bandwidth directly affects internet connectivity speed. Bandwidth measures data transfer rates between servers and client computers over specific time periods, calculated in bits per second (bps) [7]. Network computers receive bandwidth allocations that determine data transfer speeds. Higher network capacity allows both clients and servers to transfer data more rapidly [8]. Effective bandwidth management becomes essential for optimizing network performance within existing constraints [9].

Point to Point Protocol over Ethernet (PPPoE) offers a technical solution addressing bandwidth waste while providing user authentication. Network administrators can assign unique identities to each user and control bandwidth allocation individually, creating fairer and more efficient distribution 0. Local network challenges extend beyond bandwidth management. Cyber attacks including scanning, sniffing, and brute force login attempts create serious security risks, particularly when networks lack proactive protection systems. PPPoE operates as a secure tunneling protocol requiring specific authentication for connections, which introduces delays in data transfer processes [11]. PPPoE enables communication between two computers connected via serial ports [12]. PPPoE encapsulates Point-to-Point Protocol (PPP) frames within Ethernet frames. VPN networks utilize PPPoE to establish point-to-point tunnel connections. The secure nature of PPPoE tunneling demands multiple authentication steps before server connections can be established. Security and authentication requirements create processing delays that slow data transmission [13].

Intrusion Detection and Prevention System (IDPS) technology becomes necessary for real-time cyber threat detection and mitigation. IDPS monitors network traffic and automatically blocks threats based on behavioral patterns or known signatures [14]. Intrusion detection and prevention systems serve critical roles in cybersecurity infrastructure. Networks and computer systems require protection from unauthorized access and malicious activities. IDPS analyzes network traffic to identify suspicious or harmful behavior patterns. The system detects and prevents unauthorized access attempts, malware attacks, and various security breaches. IDPS operates in network-based or host-based configurations. Network-based IDPS monitors traffic at multiple infrastructure points like routers and switches to identify abnormal activities. Host-based IDPS focuses on individual hosts or endpoint devices to detect intrusion signs or malicious behavior. IDPS primarily detects and prevents unauthorized network or system access. The system analyzes network traffic against predetermined attack patterns and signatures. When IDPS identifies suspicious activity matching known attack signatures, it generates alerts or takes immediate protective action to prevent damage and secure systems. IDPS can also identify anomalous behavior patterns not covered by existing attack signatures [15]. Integrating PPPoE and IDPS within a single network system should enable efficient bandwidth management for village-scale local networks while providing adequate security protection. Rural environments transitioning toward digitalization need both approaches working together.

2. Related Work

Previous research has explored various aspects of network security, bandwidth management, and authentication protocols in different network environments. Several studies have focused on PPPoE implementation, network security systems, and their practical applications in local network infrastructures. etwork security vulnerabilities have received considerable attention from researchers worldwide. Hae (2021) conducted an experimental analysis of network security against sniffing attacks on web applications. The study demonstrated how sniffing attacks can compromise network data transmission and proposed security

measures to protect against such vulnerabilities. The research showed that proper network monitoring and security protocols are essential for maintaining data integrity in web-based systems [16]. Building on security concerns, Siregar (2020) examined Mikrotik firewall systems as low-cost network security solutions. The research found that Mikrotik-based firewalls provide effective protection for small to medium-scale networks while maintaining cost efficiency. The study emphasized the importance of proper firewall configuration for optimal security performance [20]. Widodo and Indrawan (2021) analyzed Mikrotik firewall performance in preventing DoS attacks and port scanning activities. Their research demonstrated that properly configured Mikrotik firewalls can effectively block malicious traffic and prevent unauthorized network access attempts. The study provided practical insights into firewall rule optimization for enhanced network protection [21].

PPPoE implementation has been investigated across multiple network scenarios by different research teams. Mustofa *et al*. (2022) implemented Point-to-Point Protocol over Ethernet in RT/RW Net networks using Mikrotik RB750 GR3. Their study showed that PPPoE provides effective user authentication and bandwidth management capabilities for community-based networks. The research demonstrated improved network resource allocation and user access control through PPPoE implementation [17]. Putra and Gunanto (2023) developed hotspot infrastructure based on PPPoE and WebProxy using Mikrotik systems. Their implementation combined user authentication through PPPoE with web content filtering via proxy servers. The study showed that integrated PPPoE and proxy systems enhance both network security and content management capabilities [18]. Earlier work by Slameto and Hidayat (2019) explained that PPPoE enables communication between computers connected through serial ports, providing a foundation for secure network connections [12]. Andesa (2021) further elaborated that PPPoE encapsulates PPP frames within Ethernet frames, creating secure tunnel connections for VPN networks [13].

Network performance evaluation and infrastructure development have attracted significant research interest. Saputra and Nurhasanah (2021) evaluated network performance before and after Mikrotik configuration in digital school environments. Their study revealed significant improvements in network stability and user experience following proper Mikrotik implementation. The research highlighted the importance of network optimization for educational institutions [19]. Wijaya and Purwanto (2019) implemented computer network system engineering methods for network infrastructure development. Their research focused on systematic approaches to network design and implementation, providing frameworks for effective network development projects [22]. Previous studies on bandwidth management have shown its critical role in network optimization. Ramanda *et al*. (2024) demonstrated that bandwidth management enables regulation of internet network usage according to individual user requirements [3]. Anam and Nurdian (2019) emphasized that effective bandwidth management becomes essential for maximizing network performance within existing constraints [9].

Security system integration research has highlighted the importance of automated threat detection systems. Rivaldi and Marpaung (2023) showed that IDPS technology provides real-time cyber threat detection and mitigation capabilities through automated traffic monitoring and threat blocking [14]. Prabowo *et al*. (2023) further explained that IDPS serves critical roles in cybersecurity infrastructure by analyzing network traffic to identify suspicious behavior patterns [15]. The integration of authentication protocols with security systems has been explored in various contexts. Rustanto and Herianto (2021) noted that PPPoE operates as a secure tunneling protocol requiring specific authentication, which introduces processing delays but enhances security [11]. Sari *et al*. (2024) demonstrated that PPPoE allows network administrators to provide unique user identities and regulate bandwidth allocation individually 0.

While existing research has addressed individual aspects of network security and bandwidth management, limited studies have examined the integrated implementation of PPPoE authentication with IDPS security systems in village-scale networks. Most previous work focused on either security aspects or bandwidth management separately, without exploring their combined effectiveness in rural network environments. The current research addresses these gaps by investigating the integration of PPPoE and IDPS technologies for network management solutions suitable for village-level implementations. The combination of user authentication, bandwidth control, and real-time threat detection represents a novel approach to rural network infrastructure development that builds upon the foundational work established by previous researchers in both security and network management domains.

3. Research Method

The study employs an experimental approach to test how effectively Point to Point Protocol over Ethernet (PPPoE) manages bandwidth and how well Intrusion Detection and Prevention System (IDPS) strengthens network security. We chose direct field experimentation because it allows us to measure actual network performance changes after implementing the technology. Our data collection techniques include observing initial conditions, applying technical configurations, and recording performance results such as bandwidth

usage, threat detection rates, and latency measurements. Similar approaches appear in network engineering systems research that uses experimental stages and evaluation methods [22], as well as experimental network security analysis against sniffing attacks [16]. Researchers conduct experiments to directly evaluate cyber attack impacts on networks. The process involves selecting performance indicators for monitoring, designing test environments that replicate real-world conditions, and choosing appropriate equipment. To observe network performance, researchers also design attack scenarios. The research takes place in Sukanegara Village, Jonggol District, Bogor Regency, focusing on local networks in public facilities like village offices and digital health centers. We collect data through several techniques:

1) Observation - monitoring network conditions before and after system implementation
2) Interviews - talking with village network administrators to understand technical problems and user expectations
3) Documentation - recording device configurations, network traffic data, and security incident reports
4) Experimentation - implementing systems using MikroTik routers for PPPoE and Linux-based devices for IDPS

System configuration happens in stages, starting with authentication setup and bandwidth distribution using PPPoE, followed by IDPS installation to monitor and block network attacks. We evaluate results by comparing network performance before and after system deployment, using indicators like bandwidth consumption and threat detection rates.

4. Result and Discussion

4.1 Results

4.1.1 PPPoE Implementation for Bandwidth Management

One major problem with internet networks in Sukanegara Village was uncontrolled bandwidth usage. The network became unstable, especially when user numbers increased or when several users accessed heavy applications like video streaming and large file downloads simultaneously. Before Point to Point Protocol over Ethernet (PPPoE) implementation, all users could connect to the network freely without special authentication, causing uneven bandwidth distribution. After PPPoE configuration using MikroTik routers, the network experienced significant improvements. PPPoE allowed each user to have individual login accounts, enabling network administrators to:

1) Set speed limitations per user (upload/download)
2) Monitor bandwidth consumption
3) Control connection active time
4) Prevent duplicate or illegal connections

4.1.2 Network Security System Implementation Using MikroTik Firewall

To strengthen network security from external attacks and internal network misuse, an Intrusion Detection and Prevention System (IDPS) was implemented using MikroTik's built-in firewall and filtering features. MikroTik firewall enables security configuration through:

1) Filter rules to block specific ports or IPs
2) Address lists to record suspicious addresses
3) Connection tracking to monitor active traffic
4) Automatic logging of anomalous packets or connections
5)

System testing involved simulating several potential disruptions, such as:

1) Port scanning using Nmap applications
2) Traffic flooding through continuous ping (ICMP)
3) Brute-force login connections to network interfaces

MikroTik firewall successfully:

1) Automatically blocked scanning based on connection numbers within short timeframes
2) Rejected suspicious ICMP traffic with per-second limitations
3) Recorded logs of unauthorized access attempts for further analysis by network administrators

4.1.3 Network Performance Evaluation: Before and After Implementation

To measure system effectiveness, network performance observations were conducted for two weeks, comparing conditions before and after PPPoE and active firewall configuration. Parameters used included access speed, latency, bandwidth usage distribution, and security levels.

Table 1. Network Performance Comparison Table

Parameter	Before Implementation	After Implementation
Average speed (Mbps)	4.2 Mbps	5.8 Mbps
Peak hour latency	180–220 ms	70–110 ms
Heavy bandwidth usage	62% by 3 users	28% by 3 users
Scanning protection	None	Active via firewall
Network activity logging	Manual	Automatic on router

4.2 Discussion

PPPoE implementation results showed significant improvement in network bandwidth management. The effectiveness aligns with research by Mustofa *et al*. (2022), which demonstrated that PPPoE on RT/RW Net networks could stabilize networks and reduce inefficient bandwidth consumption by up to 40% [17] These findings were strengthened by Putra & Gunanto study (2023), which implemented PPPoE and Web Proxy on school networks, reporting latency reduction up to 55% and overall bandwidth efficiency improvement [18]. Their findings stated that individual control based on login accounts was more flexible and accurate compared to conventional DHCP methods. PPPoE usage in small networks provides advantages in bandwidth distribution and more secure, measurable authentication. Andesa research (2021) also supported these findings by showing that bandwidth management implementation based on PPPoE could improve network stability in boarding school environments [13].

MikroTik firewall effectiveness as an IDPS-based security system has been proven in research by Widodo & Indrawan (2021), who tested firewalls in port scanning and DoS attack scenarios. They reported that MikroTik filter rules and address lists could block attacks up to 91% and provide neat connection logs for auditing [21]. Another study by Siregar (2020) also emphasized that MikroTik firewall became the right choice for limited environments because it was easy to configure, required no additional devices, and could be customized according to local network needs. MikroTik firewall proved quite efficient in detecting layer 3/4 attacks with low resource loads [20]. These results were consistent with research by Sari *et al*. (2024), which analyzed PPPoE-based network security using MikroTik and showed that combining PPPoE with MikroTik firewall could provide adequate security levels for small to medium-scale networks 0.

Network performance improvements obtained in the study were supported by research results from Saputra & Nurhasanah (2021), who tested MikroTik-based school network performance before and after firewall configuration and user authentication. They recorded jitter reduction and throughput increases up to 45% after implementing centralized management and security filters [19]. Combined implementation of PPPoE and MikroTik firewall was consistent with findings by Mustofa *et al*. (2022), which underlined authentication effectiveness and bandwidth control through PPPoE in RT/RW Net environments. MikroTik firewall could detect suspicious activities and prevent small attacks without requiring additional software [17]. Technically, PPPoE acts as access control and bandwidth distribution, while MikroTik firewall secures traffic and identifies suspicious activities. The combination offers an integrated solution that is cost-effective and practical for community networks like villages, which typically have hardware and human resource limitations. The approach aligns with research by Wijaya & Purwanto (2019), which emphasized the importance of implementing computer network system engineering methods for effective and efficient network development [22].

5. Conclusion and Recommendations

The research aimed to optimize bandwidth management and strengthen local network security by implementing two integrated approaches: Point to Point Protocol over Ethernet (PPPoE) and MikroTik firewall-based network security system functioning as an Intrusion Detection and Prevention System (IDPS). Common network problems in village environments, such as connection instability, uneven bandwidth usage, and high potential threats from external network traffic, became the main background for implementing the system. Implementation results showed that PPPoE usage significantly improved bandwidth distribution efficiency among users. Individual authentication enabled more measurable access control, and speed management systems guaranteed network stability even during peak hours. Meanwhile, MikroTik firewall features configured as IDPS systems effectively detected and blocked suspicious activities like port scanning, ping floods, and illegal login attempts. The system also generated activity logs that helped network administrators monitor security continuously. Overall, the combination of PPPoE and MikroTik firewall proved capable of reducing latency, increasing average user speeds, and decreasing bandwidth dominance by certain users. Based on these findings, the system is highly recommended for implementation on small to medium-scale local networks, particularly in rural environments undergoing digital transformation. The approach proved effective with relatively low implementation costs, flexible configuration, and moderate resource requirements. Future

development can focus on integrating more advanced real-time monitoring systems, such as log analyzers or web-based dashboards, along with technical training for village operators to maintain and develop the system independently.

Based on research results and system implementation, we recommend that small-scale network administrators, especially in rural environments, begin considering PPPoE protocol usage for authentication systems and bandwidth management. PPPoE usage proved to provide better control over connection distribution and bandwidth consumption per user, while helping overcome connection overload problems that frequently occur in local networks without special management. Additionally, strengthening network security systems through MikroTik firewall configuration is highly recommended. By utilizing built-in features like filter rules, address lists, and logging, network administrators can monitor and block potential threats entering the network efficiently without requiring additional devices. The approach becomes very suitable for villages or communities with budget limitations and technical resources. For future development, the system can be combined with real-time monitoring features based on dashboards or integration with simple SIEM (Security Information and Event Management) systems, making monitoring and reporting processes more structured. Furthermore, technical training for local network operators needs to be conducted regularly so system sustainability can be maintained and developed independently by local communities.

References

[1] Lukman, A. M., & Bachtiar, Y. (2018). Analisis sistem pengelolaan, pemeliharaan dan keamanan jaringan internet pada IT Telkom Purwokerto. *Jurnal Khatulistiwa Informatika*, *6*(2), 486692. https://doi.org/10.31294/evolusi.v6i2.4427

[2] Aulia, G., Zahrani, N. I., Ikhsan, M., & Nahwi, M. I. (2024). Manajemen bandwidth dengan Mikrotik untuk mengoptimalisasi akses jaringan pada Kantor Gubernur Sumatera Utara. *Journal Of Informatics And Business*, *2*(1), 11-20.

[3] Ramanda, B. D., Irawan, D., & Hidayat, A. (2024). Rancang bangun manajemen bandwidth menggunakan metode simple queue mikrotik router pada SMK N 1 Trimurjo. *Jurnal Mahasiswa Ilmu Komputer*, *5*(1), 86-95. https://doi.org/10.24127/ilmukomputer.v5i1.4690

[4] Daru, A. F., Christanto, F. W., & Kurniawan, A. (2021). Metode PCQ dan queue tree untuk implementasi manajemen bandwidth berbasis Mikrotik. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *5*(2), 407-412.

[5] Permadi, F. A. (2019). Optimalisasi jaringan internet hotspot menggunakan user manajemen pada Pusat Pengembangan SDM Asuransi Indonesia. *Jurnal Infortech*, *1*(2), 59-67. https://doi.org/10.31294/infortech.v1i2.7083

[6] Amar, M. R., Anwar, S., & Nurdiawan, O. (2022). Optimalisasi menggunakan access control list berbasis Mikrotik pada Amami Event Organizer. *MEANS (Media Informasi Analisa dan Sistem)*, 117-123.

[7] Leksono, I. N., & Sandi, T. A. A. (2019). Optimalisasi jaringan WAN berbasis Mikrotik (Studi kasus: Robotic Laboratory Bogor). *Jusikom: Jurnal Sistem Komputer Musirawas*, *4*(2), 100-110. https://doi.org/10.32767/jusikom.v4i2.628

[8] Aminah, S. (2022). Manajemen bandwidth dalam mengoptimalkan penggunaan router Mikrotik terhadap pelayanan koneksi jaringan. *Jurnal Informatika Ekonomi Bisnis*, *4*(3), 102-106. https://doi.org/10.37034/infeb.v4i3.144

[9] Saepul Anam, Y., & Nurdiana, N. (2019). Optimalisasi manajemen bandwidth jaringan komputer dengan metode PCQ (peer connection queue) menggunakan simple queue. *Seminar Teknologi Majalengka (STIMA)*, *4*(1), 53-57. https://prosiding.unma.ac.id/index.php/stima/article/view/277

[10] Sari, L. O., Safrianti, E., & Wahyuningtias, D. (2024). Analisis keamanan jaringan berbasis point to point protocol over ethernet (PPPoE) menggunakan Mikrotik. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *4*(3), 943-954. https://doi.org/10.57152/malcom.v4i3.1301

[11] Rustanto, Herianto, & Yulisman. (2021). Analisa implementasi sistem jaringan berbasis PPPoE oleh ISP PT. Java Digital Nusantara Cabang Bengkalis. *RJOCS (Riau Journal of Computer Science)*, *7*(1), 18–31. https://doi.org/10.30606/rjocs.v7i1.1818

[12] Slameto, A. A., & Hidayat, R. (2019). Comparative analysis of PPPoE and SSTP performance in Mikrotik (Analisis perbandingan kinerja PPPoE dan SSTP pada Mikrotik). *Jurnal KomtekInfo*, *6*(2), 107-116. https://doi.org/10.35134/komtekinfo.v6i2.49

[13] Andesa, K. (2021). Penerapan manajemen bandwidth berdasarkan PPPoE pada Pondok Pesantren Miftahul Huda. *SATIN-Sains dan Teknologi Informasi*, *7*(2), 121-128. https://doi.org/10.33372/stn.v7i2.778

[14] Rivaldi, O., & Marpaung, N. L. (2023). Penerapan sistem keamanan jaringan berbasis Suricata. *Jurnal Inovtek Polbeng*, *8*(1), 18–27.

[15] Prabowo, W. A., Fauziah, K., Nahrowi, A. S., Faiz, M. N., & Muhammad, A. W. (2023). Strengthening network security: Evaluation of intrusion detection and prevention systems tools in networking systems. *International Journal of Advanced Computer Science and Applications*, *14*(9). https://doi.org/10.14569/ijacsa.2023.0140934

[16] Hae, Y. (2021). Analisis keamanan jaringan pada web dari serangan sniffing dengan metode eksperimen. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, *8*(4), 2095–2105. https://doi.org/10.35957/jatisi.v8i4.1196

[17] Mustofa, D., Mahendra, D. A., Saputra, D. I. S., & Amin, M. S. (2022). Implementasi point-to-point protocol over ethernet pada jaringan RT/RW Net menggunakan Mikrotik RB750 GR3. *Jurnal Ilmiah IT CIDA*, *8*(2), 124-139. https://doi.org/10.55635/jic.v8i2.169

[18] Putra, P. D., & Gunanto, S. (2023). Implementasi infrastruktur hotspot berbasis PPPoE dan WebProxy dengan Mikrotik. *Jurnal Sienna*, *5*(2). https://doi.org/10.47637/sienna.v5i2.1394

[19] Saputra, A., & Nurhasanah, R. (2021). Evaluasi performa jaringan sebelum dan sesudah konfigurasi Mikrotik pada sekolah digital. *Jurnal TI Pelita*, *9*(3).

[20] Siregar, A. B. (2020). Firewall Mikrotik sebagai sistem keamanan jaringan berbasis low-cost devices. *Jurnal Media Teknologi*, *12*(1).

[21] Widodo, A., & Indrawan, R. (2021). Analisis kinerja firewall Mikrotik dalam pencegahan serangan DoS dan port scanning. *Jurnal ITSmart*, *6*(1).

[22] Wijaya, A., & Purwanto, T. D. (2019). Implementasi metode rekayasa sistem jaringan komputer untuk pengembangan jaringan komputer. *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, *5*(3), 294. https://doi.org/10.26418/jp.v5i3.29925