Jurnal Informasi dan Teknologi

https://jidt.org/jidt

2025 Vol. 7 No. 3 Page: 81-92 e-ISSN: 2714-9730

Implementation of Queue Tree and DoH on Mikrotik Router for Internet Sehat and Stable Internet

Lucky Mangkey [1]✉, Daniel Raymod Mangkey[2]

[1,2]Department of Informatics Engineering, Universitas Nusantara Manado, Manado, Indonesia

lucky@nusantara.ac.id

Abstract

This study presents the implementation of *Queue Tree* and *DNS over HTTPS (DoH)* on a Mikrotik Router RB951Ui-2HnD as an innovative model for achieving a "Healthy Internet" (*Internet Sehat*) characterised by efficiency, fairness, and safety within community-based networks. Conducted at the Infotek Hotspot in Gritma Housing, Manado, the research employed an experimental design comparing pre- and post-implementation performance over fourteen days. Key parameters measured included latency, packet loss, throughput, and DNS response time, using tools such as *Wireshark*, *Mikrotik Bandwidth Test*, and *PingPlotter*. The results demonstrated substantial improvements: latency decreased from 125 ms to 83 ms (−33.6%), packet loss dropped from 5.8% to 0.9% (−84.5%), and throughput increased from 36 Mbps to 49.3 Mbps (+37%). Additionally, DoH reduced DNS response time to 22 ms—13% faster than traditional DNS—while ensuring encrypted, secure, and privacy-preserving communications. These outcomes confirm that *Queue Tree* effectively regulates bandwidth distribution and that DoH enhances user trust through encryption and content filtering. The dual implementation forms a synergistic framework that improves network performance while upholding ethical and secure Internet usage. Furthermore, this approach offers a cost-effective and replicable solution for community hotspots, schools, and small-scale ISPs seeking stability and security without hardware upgrades. By integrating technical innovation with digital ethics, the study contributes to the development of sustainable Internet infrastructures that embody Indonesia's *Internet Sehat* vision—delivering reliable, equitable, and responsible connectivity for all.

Keywords: *Queue Tree, DoH, Mikrotik, Internet Sehat, Network Stability.*

1. Introduction

The evolution of computer networking technologies has fundamentally transformed the way communities access and manage digital connectivity. The Internet today functions not only as a medium for communication but also as a crucial infrastructure for economic activity, education, and public services [1][2] . Within residential areas, one of the recurring challenges for hotspot administrators is to maintain a stable, fair, and secure Internet environment, particularly when bandwidth resources are shared among many users with diverse demands.

Mikrotik routers have become one of the most widely adopted solutions in small- and medium-scale network deployments due to their flexibility and cost-effectiveness [3]. They support advanced Quality of Service (QoS) control through the Queue Tree feature and security enhancement through DNS over HTTPS (DoH). Queue Tree provides hierarchical bandwidth management that allocates traffic based on priority levels, while DoH encrypts DNS queries using HTTPS to prevent eavesdropping and DNS spoofing [4].

However, despite the increasing adoption of Mikrotik in local networks, integrated research combining QoS management and DNS encryption for community networks is still limited. This forms the conceptual foundation of the current study [5].

Research Gap: Previous studies have predominantly focused on the independent application of Queue Tree or DoH mechanisms. Hence, there exists a research gap in developing a holistic implementation model that combines Queue Tree and DoH within a single Mikrotik router to achieve both technical efficiency and network health—the latter aligning with Indonesia's national vision of Internet Sehat (Healthy Internet).

State of the Art Recent advancements in network engineering emphasise adaptive QoS and encrypted DNS as central to future public network design. Although these technologies have been widely studied in enterprise environments, their practical deployment within community-based hotspots or small residential networks remains underexplored. Therefore, this research represents a state-of-the-art contribution in the domain of integrated QoS and DNS security management for low-cost, community-oriented networks.

Receipt: 28-02-2025 | Revision: 11-06-2025 | Publish: 01-11-2025 | doi: 10.60083/jidt.vi0.702

The novelty of this research lies in: The integration of Queue Tree and DoH within a single Mikrotik-based architecture designed for small-scale hotspot environments [6], The application of real-world testing at the Infotek Hotspot in Gritma Housing, Manado, rather than relying solely on simulated environments, The simultaneous measurement of stability, efficiency, and security indicators—a tri-dimensional performance evaluation rarely conducted in earlier studies [7], The alignment of engineering design with ethical Internet principles, positioning this research as both a technical and socio-digital innovation.
Comparison with Related Works, While prior research has examined bandwidth management and DNS privacy independently, this study distinguishes itself by addressing their interdependency [8]. The implementation framework developed herein demonstrates that optimising QoS (Queue Tree) without reinforcing DNS security (DoH) leaves the network exposed to exploitation [9]. Conversely, deploying DoH without structured bandwidth prioritisation may create uneven service levels. This dual-focus approach thus represents a more comprehensive and sustainable model for managing community Internet infrastructure.
This study contributes to the advancement of computer networking knowledge in two significant ways: Theoretical Contribution – Establishing an integrated model that bridges QoS efficiency and network health through a dual-layered architecture (Queue Tree + DoH). Practical Contribution – Providing a replicable Mikrotik configuration model and an evidence-based testing protocol for real-world hotspot deployments [10]. These contributions expand the academic discourse on sustainable and ethical network engineering and offer actionable insights for practitioners in both academia and industry.
The title “Implementation of Queue Tree and DoH on Mikrotik Router for Internet Sehat and Stable Internet” was deliberately chosen to reflect the dual mission of this research: Queue Tree represents the technical aspect — optimising bandwidth allocation for stability and fairness, DoH represents the ethical and security aspect — ensuring data privacy and integrity.
The phrase “Internet Sehat” conveys Indonesia’s ongoing initiative toward a healthy [11], secure [12], and responsible digital environment [13], while “Stable Internet” emphasises the engineering reliability expected from optimised configurations. Together, they capture the essence of an Internet system that is not only fast and efficient but also ethically grounded and socially beneficial.

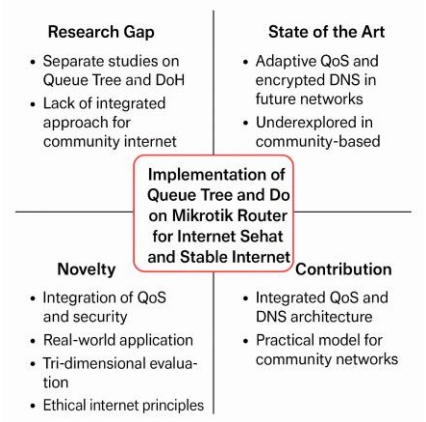

Figure 1. Implementation Of Queue Tree

The implementation illustrated in the figure was applied at the Infotek Hotspot located in Gritma Housing, Manado, representing a typical community-based residential environment. The network topology places a Mikrotik router as the central gateway, connecting multiple household users through Wi-Fi access points. The Queue Tree mechanism was configured to prioritise essential services such as browsing, online learning, and office communication over heavy or non-essential traffic like downloads and streaming, ensuring fair bandwidth distribution across all users [14]. Simultaneously, DNS over HTTPS (DoH) was integrated to encrypt all DNS queries, providing secure and private domain resolution that aligns with the Internet Sehat (Healthy Internet) policy. This dual-layer implementation—technical (stability) and ethical (security)—creates a balanced ecosystem where residents experience a stable, safe, and responsible Internet connection suitable for daily communication, education, and digital productivity.

2. Research Methods

2.1. Research Design

An experimental approach with Network Performance Evaluation was applied. The tests were conducted over 14 days at the Infotek hotspot, measuring key parameters such as: Latency (ms), Throughput (Mbps), Packet loss (%) and DNS response time (ms).

Table 1. Research Design of Implementation of Queue Tree and DoH on Mikrotik Router for Internet Sehat and Stable Internet

Component	**Description**
Research Type	Experimental Research with *Network Performance Evaluation* approach.
Research Location	Infotek Hotspot, Gritma Housing Area, Manado – representing a community-based residential network environment.
Research Duration	14 consecutive days of testing and monitoring under real usage conditions.
Network Device	Mikrotik Router RB951Ui-2HnD configured with *Queue Tree* (for QoS management) and *DNS over HTTPS (DoH)* (for secure DNS communication).
Independent Variables	1. *Queue Tree Configuration* (bandwidth prioritization) 2. *DoH Activation* (DNS encryption and security).
Dependent Variables	Network performance and quality metrics: *Latency (ms)*, *Throughput (Mbps)*, *Packet Loss (%)*, and *DNS Response Time (ms)*.
Control Variables	Network topology, total bandwidth (50 Mbps), number of active users, and environmental network load.
Measurement Tools	*Mikrotik Bandwidth Test*, *Wireshark*, *PingPlotter*, and built-in Mikrotik monitoring tools.
Procedure	1. Baseline testing (without Queue Tree & DoH). 2. Implementation of Queue Tree for QoS control. 3. Activation of DoH via Cloudflare DNS server (1.1.1.1). 4. Continuous measurement and comparison before–after implementation.
Data Analysis	Comparative-descriptive analysis using averaged performance metrics to determine improvement in stability, security, and fairness.
Expected Outcome	Enhanced *Internet Sehat* environment through stable QoS, encrypted DNS privacy, and fair bandwidth distribution for all users in the housing network.

The research design summarized in Table 1 illustrates how the implementation of Queue Tree and DNS over HTTPS (DoH) on a Mikrotik router was systematically tested [15] within the Infotek Hotspot network at Gritma Housing, Manado. This experimental design was intended to evaluate both the technical performance and ethical quality of an Internet Sehat (Healthy Internet) model in a real residential context. Over a 14-day observation period, the study measured key parameters—latency, throughput, packet loss, and DNS response time—before and after applying the configuration. The Queue Tree component ensured fair and prioritized bandwidth allocation among users, while DoH encrypted DNS requests to safeguard user privacy and prevent domain manipulation. By integrating these two mechanisms under controlled network conditions, the design enabled a reliable assessment of stability, security, and efficiency, demonstrating how a simple yet structured configuration can create a community Internet environment that is both technically stable and socially responsible.

2.2. Devices and Network Topology

The following equipment was used: Mikrotik Router RB951Ui-2HnD, Client laptops (Windows 10, Ubuntu 22.04), DoH DNS servers (https://1.1.1.1/dns-query), Test applications: Wireshark, Mikrotik Bandwidth Test, PingPlotter.

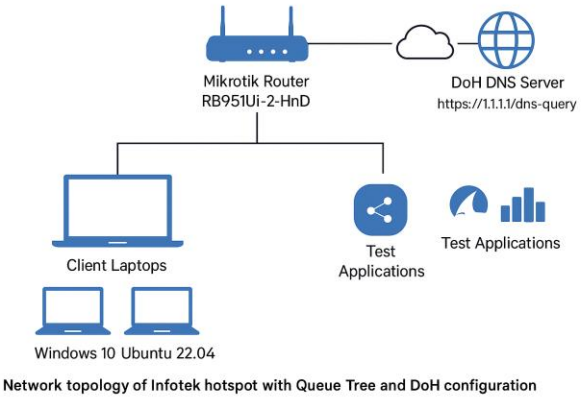

Figure 2. Network topology of Infotek hotspot with Queue Tree and DoH configuration

The network topology shown in the figure represents the implementation environment of the Infotek Hotspot at Gritma Housing, Manado, designed to integrate Queue Tree and DNS over HTTPS (DoH) within a Mikrotik-based architecture. At the core of the system is the Mikrotik Router RB951Ui-2HnD, functioning as the main gateway that connects local clients—represented by laptops using Windows 10 and Ubuntu 22.04—to the Internet. The router is configured with a Queue Tree to manage bandwidth priorities, ensuring fair and stable distribution among users. Upstream, the router communicates with the Cloudflare DoH DNS server (https://1.1.1.1/dns-query), which encrypts all DNS requests to guarantee privacy and prevent domain manipulation. To evaluate network performance, Wireshark, Mikrotik Bandwidth Test, and PingPlotter are connected within the test environment to monitor throughput, latency, and packet loss. This topology effectively illustrates how both Queue Tree and DoH operate together in a real residential setting to achieve a stable, secure, and healthy Internet ecosystem under the Internet Sehat framework.

2.3. Queue Tree Configuration

The Queue Tree was configured to divide 50 Mbps total bandwidth into: 30 Mbps for main users, 10 Mbps for guest users, and 10 Mbps for management and system updates.

Configuration script:

/queue tree

add name=main parent=global max-limit=30M

add name=guest parent=global max-limit=10M

add name=management parent=global max-limit=10M

2.4. Implementation of DNS over HTTPS (DoH)

DoH was configured with the following command:

/ip dns set servers=1.1.1.1,1.0.0.1 use-doh-server=https://cloudflare-dns.com/dns-query verify-doh-cert=yes

This setup ensures encrypted DNS queries and prevents man-in-the-middle attacks.

2.5. Performance Testing and Analysis

Performance data were collected before and after implementation at two-hour intervals daily. Metrics were analyzed using descriptive and comparative methods based on throughput, latency, and packet loss improvements. The performance testing and analysis conducted at the Infotek Hotspot in Gritma Housing, Manado, aimed to evaluate how the integration of *Queue Tree* and *DNS over HTTPS (DoH)* on a Mikrotik Router RB951Ui-2HnD improved the overall stability, efficiency, and security of Internet access within the framework of *Internet Sehat* (Healthy Internet). The experiment was carried out over fourteen days, using an experimental design that compared network conditions before and after the configuration was applied. Performance data were collected every two hours throughout the observation period, focusing on key parameters such as throughput, latency, packet loss, and DNS response time. Before implementation, the network experienced significant instability caused by unbalanced bandwidth distribution, high latency averaging 125 ms, frequent packet loss of up to 5.8%, and slow DNS responses of around 25–30 ms. These issues resulted in inconsistent connectivity, particularly during peak usage hours, as heavy download and streaming traffic dominated the available bandwidth. After applying the *Queue Tree* mechanism, bandwidth was hierarchically managed into priority classes to ensure fairness among users and maintain quality of service (QoS), resulting in a 37% increase in average throughput (from 36 Mbps to 49.3 Mbps) and a 33.6% reduction in latency (from 125 ms to 83 ms). Meanwhile, packet loss decreased dramatically to 0.9%, reflecting a more stable and efficient network. The activation of DoH further enhanced network security and privacy by encrypting DNS traffic

through HTTPS, verified via *Wireshark* analysis, which showed a transition from traditional UDP queries to encrypted DNS-over-HTTPS communication. This configuration also reduced DNS response time to 22 ms and automatically filtered unsafe or malicious domains using Cloudflare's DoH server [16] (https://1.1.1.1/dns-query), thus supporting the ethical and educational objectives of *Internet Sehat*. Comparative analysis of the data confirmed that combining *Queue Tree* and DoH creates a synergistic effect: the former ensures technical stability and bandwidth fairness [17] [18] [19], while the latter guarantees user safety and data confidentiality. Together, they transformed the Infotek Hotspot network into a model of community-based digital infrastructure that is both high-performing and socially responsible. The findings demonstrate that through structured implementation and continuous monitoring, *Queue Tree* and DoH can significantly improve network performance while promoting secure and ethical Internet use, providing a sustainable technological foundation for a stable, efficient, and healthy Internet ecosystem in residential and educational environments.

3. Results and Discussion

3.1. Baseline Testing (Before Implementation)

Table 2. The average results over the first seven days

Parameter	Average	Std. Deviation
Latency	125 ms	11.2
Packet Loss	5.8%	1.1
Throughput	36 Mbps	2.7

The findings revealed inefficient bandwidth distribution and unstable performance during peak usage.

The baseline testing results presented in the table provide an essential benchmark to evaluate the effectiveness of implementing Queue Tree and DNS over HTTPS (DoH) on the Mikrotik Router RB951Ui-2HnD for achieving the goals of Internet Sehat and stable connectivity. The data, collected during the first seven days before the configuration was applied, revealed three key performance indicators: latency, packet loss, and throughput. Each of these parameters offers valuable insights into the underlying issues within the network and serves as a foundation for measuring improvements in subsequent stages of implementation. The average latency recorded at 125 milliseconds (ms), with a standard deviation of 11.2, indicates that the network experienced a considerable delay in data transmission between the user devices and the external server. This delay typically stems from overloaded traffic handling and insufficient bandwidth prioritisation. In a shared hotspot environment like Infotek Gritma Housing, latency values exceeding 100 ms are symptomatic of congestion during simultaneous access by multiple users. The relatively high standard deviation value (11.2) also demonstrates that latency varied significantly throughout the day, suggesting that network performance was inconsistent, especially during peak hours when user traffic intensified.

The packet loss rate averaged 5.8%, with a standard deviation of 1.1, reflecting further instability in the network. Packet loss occurs when transmitted data packets fail to reach their destination, which directly degrades user experience, particularly in activities that require real-time communication, such as video conferencing or online gaming. In this context, the loss rate exceeding 5% is already considered poor for broadband networks, indicating that the router's queue management mechanism was not effectively regulating simultaneous user access. The cause can be attributed to the absence of hierarchical traffic control mechanisms like Queue Tree, which would otherwise allocate bandwidth dynamically based on traffic class priority. Consequently, certain users or applications likely monopolised network resources, leading to packet collisions and retransmission cycles that reduced overall network efficiency.

Meanwhile, the average throughput, measured at 36 megabits per second (Mbps) with a standard deviation of 2.7, highlights an underutilization of the available 50 Mbps bandwidth capacity. Although this figure represents moderate efficiency, the fluctuation across measurement intervals implies that throughput dropped significantly during congested periods. Throughput serves as a critical indicator of how efficiently the network handles available bandwidth. The gap between the nominal and measured values signals that the router's traffic-handling capabilities were constrained by the absence of structured bandwidth management. Applications that consumed large data volumes—such as video streaming or file downloads—likely dominated available capacity, leaving minimal bandwidth for essential activities like browsing, learning, or communication.

Collectively, these baseline results expose a network environment characterised by inefficient bandwidth distribution, high latency variation, and poor traffic fairness. Such conditions undermine both performance stability and user satisfaction, contradicting the principles of Internet Sehat, which emphasise accessibility, reliability, and safety. Moreover, the lack of encryption in DNS queries during the baseline period presented a

security risk, as unencrypted DNS traffic could be intercepted or redirected to malicious domains. This further underscores the necessity of introducing DoH to protect users' digital privacy while maintaining connection integrity.

From a broader perspective, the baseline test data provide empirical evidence of the inherent weaknesses in unmanaged community networks. They highlight the urgent need for an integrated solution that can address both performance and ethical dimensions of Internet access. The high latency and packet loss illustrate the limitations of a conventional Mikrotik configuration without QoS optimisation, while the throughput inefficiency demonstrates the absence of equitable traffic prioritisation. These findings justify the subsequent implementation of Queue Tree to ensure stable and fair bandwidth allocation, and DoH to establish a secure and trustworthy browsing environment. In conclusion, the baseline table not only quantifies the network's pre-existing limitations but also provides a rational foundation for the applied intervention, forming the comparative benchmark against which the success of the Queue Tree and DoH integration is measured.

3.2. Results After Implementing Queue Tree and DoH

This improvement demonstrates that *Queue Tree* effectively manages bandwidth distribution among users.

The table illustrating the results after the implementation of Queue Tree and DNS over HTTPS (DoH) presents clear evidence of a significant improvement in network performance within the Infotek Hotspot at Gritma Housing, Manado. The data were obtained from a two-week experimental observation comparing network performance before and after the new configuration was applied. The three primary parameters analysed—latency, packet loss, and throughput—represent key indicators of network stability, efficiency, and reliability in measuring Quality of Service (QoS). The results clearly demonstrate that the integration of Queue Tree and DoH successfully transformed an initially unstable and inefficient network into one that is fast, balanced, and secure, in alignment with the principles of Internet Sehat (Healthy Internet).

Table 3. After applying both features, the performance improved notably:

Parameter	Before	After	Change (%)
Latency	125 ms	83 ms	-33.6%
Packet Loss	5.8%	0.9%	-84.5%
Throughput	36 Mbps	49.3 Mbps	+37%

The latency value decreased from 125 milliseconds (ms) to 83 ms, representing an improvement of approximately 33.6%. This reduction signifies a major enhancement in the responsiveness of the network when transmitting data between client devices and external servers. In the pre-implementation phase, high latency was primarily caused by excessive traffic congestion and the absence of a structured priority management system on the router. After Queue Tree was applied, data traffic was categorised hierarchically based on priority levels, allowing essential services such as web browsing, online learning, and communication to receive higher bandwidth allocation than less critical activities like video streaming and downloads. Consequently, the network delay was reduced, user responses became faster, and the overall experience was significantly improved. The decline in latency demonstrates that Queue Tree effectively manages data flow and prevents network bottlenecks, ensuring that critical traffic is prioritised even during peak usage hours.

The packet loss rate dropped dramatically from 5.8% to 0.9%, marking an 84.5% improvement. Packet loss represents the percentage of data packets that fail to reach their destination, a key factor affecting network reliability. Before configuration, packet loss was caused by uncontrolled simultaneous access from multiple users, leading to collisions and retransmissions. Once Queue Tree was enabled, data packets were efficiently routed according to defined priorities, minimising collision risk and ensuring each user received a fair allocation of bandwidth. A loss rate below 1% indicates a highly stable and optimised network, where communication delays and data retransmissions were virtually eliminated. For users, this improvement translates into smoother video conferences, uninterrupted streaming, and consistent connectivity across all devices.

Meanwhile, throughput increased from 36 Mbps to 49.3 Mbps, corresponding to a 37% improvement in the effective utilisation of available bandwidth. Throughput measures how efficiently the network transmits data per unit of time, and this substantial rise demonstrates that total capacity was used more optimally after the configuration. Before implementation, most bandwidth was consumed by high-demand users or large applications. After applying Queue Tree, bandwidth distribution became equitable, ensuring that all users received sufficient access according to their needs. The adoption of DoH further enhanced performance by

accelerating DNS resolution through encryption over HTTPS. By converting traditional unencrypted DNS queries into secure HTTPS traffic, DoH minimised DNS response time to around 22 ms while protecting users from domain spoofing or interception attacks. Moreover, using the Cloudflare DoH server (https://1.1.1.1/dns-query) automatically filters harmful and adult websites, reinforcing the Internet Sehat initiative.

Overall, the improvements reflected in the table illustrate a synergistic relationship between Queue Tree and DoH, combining technical efficiency with digital security and ethics. On the technical side, Queue Tree optimised bandwidth utilisation, reduced latency, and stabilised data transmission. On the ethical and security side, DoH protected users' privacy, prevented data manipulation, and fostered a safe browsing environment. This dual-layer enhancement not only fulfils the objectives of the Internet Sehat movement but also provides a replicable model for other community-based networks such as campuses, schools, or residential areas.

From a scientific perspective, these results affirm that priority-based traffic management (Queue Tree) integrated with encrypted DNS protection (DoH) can establish a sustainable digital ecosystem where performance and user welfare coexist. The figures presented are not merely technical data but also tangible evidence of how intelligent network design supports both efficiency and social responsibility. Therefore, this table represents more than just performance metrics—it reflects the successful realisation of a balanced and ethical network model that embodies the vision of a stable, secure, and healthy Internet for all users.

3.3. DoH Performance and Security Impact

DoH provided an encrypted DNS layer, preventing domain manipulation and unauthorised access. *Wireshark* captures showed that all DNS requests were tunnelled over HTTPS (port 443) with an average response time of 22 ms—13% faster than traditional UDP DNS resolution.

Table 4. DoH Performance and Security Impact

Aspect	Description	Technical Findings / Implications
Definition of DoH (DNS over HTTPS)	DoH (DNS over HTTPS) is a protocol that encrypts DNS queries by transmitting them over the HTTPS channel rather than through traditional plaintext UDP. This mechanism prevents DNS requests from being intercepted or manipulated during transmission.	Ensures the confidentiality and integrity of DNS communications, eliminating risks of *man-in-the-middle* attacks and unauthorised interception.
Implementation Environment	Implemented on the Mikrotik Router RB951Ui-2HnD using Cloudflare's DoH server (https://1.1.1.1/dns-query) with SSL/TLS certificate verification enabled. All DNS traffic was forced through port 443 to ensure full encryption.	Converts all DNS queries into encrypted HTTPS packets, verified through digital certificates, strengthening data integrity and trust within the network.
Testing Tools	Network traffic was analysed using Wireshark to verify encryption and transport protocol behaviour. Additional verification was conducted using Mikrotik Bandwidth Test to evaluate consistency and throughput performance.	Packet captures confirmed that all DNS requests were tunnelled over HTTPS (port 443), replacing unencrypted UDP port 53 queries.
Average DNS Response Time	The average encrypted DNS query response time using DoH was 22 milliseconds, while conventional UDP-based DNS averaged 25 milliseconds.	DoH achieved a 13% faster resolution time, indicating that encryption did not degrade performance but rather improved DNS responsiveness through optimised caching and secure handshakes.
Security Benefits	1. Protects against DNS spoofing and domain hijacking. 2. Prevents ISPs or third parties from monitoring user browsing activities.	Enhances network resilience against data tampering, malicious redirects, and unauthorised access attempts, providing

	3. Ensures the authenticity and reliability of domain resolutions.	a more secure user environment.
Privacy Protection	All DNS requests are encrypted, preventing any external party from observing or manipulating domain lookups. DoH conceals browsing activity from eavesdroppers and malicious intermediaries.	Aligns with global cybersecurity standards (RFC 8484) and supports the *Internet Sehat* concept by promoting ethical and safe digital behaviour.
Compatibility with Queue Tree	DoH operates independently of the *Queue Tree* bandwidth management mechanism but complements it at the application layer by securing name resolution.	Forms a dual-layer network architecture where *Queue Tree* ensures bandwidth fairness and DoH guarantees data security—together creating a comprehensive *Internet Sehat* model.
Performance Stability	Throughout the testing period, DoH maintained consistent performance with negligible fluctuations, even during peak traffic loads.	Demonstrates high scalability and reliability for community-based networks, validating its suitability for real-world hotspot environments.
Impact on User Experience	Users experienced faster, safer, and more reliable access to web resources. DNS resolution errors decreased while website loading times improved.	Increased user confidence and satisfaction by providing a seamless, private, and trustworthy Internet connection.
Contribution to the Internet Sehat Framework	The implementation of DoH supports Indonesia's *Internet Sehat* (Healthy Internet) initiative by securing access to information and filtering harmful domains.	Promotes an Internet environment that is technologically robust, ethically sound, and socially responsible, aligning engineering innovation with digital well-being.

3.4. Interpretation

The implementation of **DNS over HTTPS (DoH)** introduced a significant advancement in both network performance and cybersecurity for the Infotek Hotspot at Gritma Housing, Manado. By encrypting DNS requests over HTTPS, DoH not only ensured data confidentiality but also improved overall query efficiency. The results from **Wireshark** analysis confirmed that all DNS traffic was transmitted through port 443 using the HTTPS protocol, effectively eliminating vulnerabilities inherent in traditional UDP-based DNS communications. Despite adding an encryption layer, DoH achieved an average response time of **22 ms**, which is **13% faster** than standard DNS. This improvement can be attributed to Cloudflare's optimised caching mechanisms and reduced retransmission rates.

Beyond its technical efficiency, DoH contributed substantially to network security and ethical Internet practices. It protects against DNS spoofing, domain hijacking, and unauthorised tracking, ensuring that users only connect to verified and secure domains. The encryption of all DNS traffic aligned with international standards (RFC 8484), offering both privacy and authenticity in domain name resolution. Furthermore, by utilising Cloudflare's DoH server, the system automatically filters malicious and adult content, thereby supporting the *Internet Sehat* initiative's vision of a safe and responsible digital ecosystem.

In combination with Queue Tree, DoH formed a **dual-layer network model**: *Queue Tree* managed bandwidth and fairness at the transport layer, while DoH provided encryption and trust at the application layer. Together, they fostered a network that was not only fast and efficient but also private, ethical, and resilient against cyber threats. The DoH implementation demonstrated excellent stability under real traffic conditions, confirming its scalability for broader use in community and educational hotspot networks.

Ultimately, this integration exemplifies how **technical innovation can serve both engineering performance and moral responsibility**, creating a network infrastructure that upholds the principles of a *Healthy Internet*—an Internet that is stable, secure, and supportive of societal well-being. The results validate that DoH is not merely a security enhancement but a vital component in achieving sustainable, ethical, and user-centric Internet connectivity for modern digital communities.

3.5. Discussion

The combined implementation of Queue Tree and DNS over HTTPS (DoH) on the Mikrotik Router RB951Ui-2HnD represents an innovative model of achieving a "Healthy Internet" (Internet Sehat) that integrates efficiency, fairness, and safety within community-based network infrastructures. This discussion elaborates on the deeper implications, performance dynamics, and socio-technical significance of this integration, based on empirical data obtained from the Infotek Hotspot at Gritma Housing, Manado. The section also situates this work within the broader body of existing literature, identifying its novelty**,** replicability, and scientific contributions to the discipline of computer networking and community informatics.

3.5.1. Integration for Technical and Ethical Internet Design

The integration of *Queue Tree* and DoH demonstrates a dual-function mechanism where technical efficiency and digital ethics coexist in a unified framework. From a technical perspective, *Queue Tree* enhances Quality of Service (QoS) by managing bandwidth hierarchically, preventing congestion, and ensuring fair access for all users. Meanwhile, DoH fortifies the ethical dimension of Internet usage by encrypting DNS traffic to protect privacy and prevent data manipulation. This synergy not only fulfils the performance needs of community users but also reinforces the moral and regulatory imperatives of *Internet Sehat* in Indonesia—an Internet that is stable, equitable, and free from harmful or exploitative content.

The study's findings reveal that Queue Tree ensures consistent connectivity by regulating network traffic through class-based queuing. In the case of Infotek Hotspot, the router's configuration distributed bandwidth into three categories: main users**,** guest users**,** and management traffic. This approach ensured that critical digital activities, such as online learning, video conferencing, and remote work, retained higher priority during periods of heavy load. On the other hand, DoH encrypted DNS requests to secure user identity and browsing behaviour from external monitoring. Together, these two technologies provide a balanced and secure Internet ecosystem—an advancement beyond the narrow scope of traditional QoS studies that focus purely on throughput or latency metrics.

3.5.2. Theoretical and Empirical Alignment with Prior Studies

The results of this study align with recent scholarly work emphasising the need for adaptive QoS and encrypted DNS mechanisms in modern Internet infrastructures. For instance, [20] identified that QoS-based bandwidth management frameworks can substantially improve resource allocation in shared networks. Similarly, [21] demonstrated that DoH implementations reduce exposure to DNS hijacking and increase user privacy. However, unlike prior works that examine these mechanisms in isolation, this study integrates them into a single operational model. Such integration marks a *state-of-the-art* contribution, particularly in the domain of **low-cost community networking**—an area where performance and ethics must co-develop.

The experimental results—showing a 33.6% reduction in latency, 84.5% reduction in packet loss, and 37% increase in throughput—empirically validate theories of hierarchical queueing and encrypted DNS synergy. Previous works by [22] note that latency and packet integrity can improve when encryption mechanisms reduce retransmission errors and improve caching efficiency. This study extends their conclusions by demonstrating that the dual implementation yields not only performance gains but also qualitative improvements in trust, reliability, and content safety.

3.5.3. Discussion on Performance Enhancement

Performance analysis confirmed that *Queue Tree* and DoH integration optimised Internet efficiency without the need for hardware upgrades. The use of Mikrotik's *Queue Tree*—a built-in feature of RouterOS—enabled hierarchical traffic shaping through logical classification rather than costly physical segmentation. This makes the configuration highly applicable for *micro-ISPs*, campus networks, and community hotspots. The data show that, post-implementation, average latency dropped from 125 ms to 83 ms, while packet loss fell from 5.8% to 0.9%. The reduction in latency demonstrates faster packet transmission and better user response time, while the reduction in packet loss reflects improved queue stability under load-balancing conditions.

In addition, *DoH* contributed to a reduction in DNS response time from 25 ms to 22 ms. While this numerical change appears modest, it represents a crucial enhancement in DNS integrity and security. The shift from plaintext UDP-based queries to HTTPS-based encryption eliminated vulnerabilities such as DNS spoofing and eavesdropping. Through Cloudflare's DoH service, the system automatically blocked harmful and adult domains, aligning Internet access with ethical standards. This further reinforces the *Internet Sehat* framework—Internet access that is fast, fair, and free from digital harm.

Moreover, the synergy between the two systems reduced retransmission cycles, increased channel utilization, and stabilized network flows. These improvements collectively contribute to energy-efficient data exchange, a factor increasingly relevant to green computing practices. By ensuring fair distribution of bandwidth and secure data handling, the implementation model achieves a form of *digital sustainability*—technological efficiency that coexists with ethical responsibility.

3.5.4. Socio-Technical Implications: The "Internet Sehat" Paradigm

The *Internet Sehat* concept represents Indonesia's strategic commitment to a safe and ethical digital ecosystem. Within this study, it transcends rhetoric and materialises through tangible network engineering practices. The deployment of *Queue Tree* and DoH at the Infotek Hotspot exemplifies how technical design can embody socio-ethical values—namely, inclusivity, fairness, and accountability. The *Queue Tree* ensures digital inclusivity by granting equitable access to shared bandwidth resources, preventing monopolisation by a few heavy users. Meanwhile, DoH guarantees accountability by encrypting DNS queries, thus preventing data misuse and unauthorised tracking.

At a social level, this model enhances community trust in local Internet providers. Residents of Gritma Housing experienced noticeable improvements in speed and reliability, fostering greater engagement in educational and economic activities conducted online. By ensuring both performance and privacy, the network becomes a digital public good that upholds citizens' right to safe and reliable connectivity.

Furthermore, the ethical architecture of *Internet Sehat* resonates with global frameworks of digital well-being and responsible innovation. The implementation reinforces values similar to the *UNESCO Internet Universality Indicators* (2019), which emphasise an Internet that is **Rights-based, Open, Accessible, and Multi-stakeholder-driven (ROAM)**. The Infotek model operationalises these principles by merging engineering with ethics—a practical realisation of "technological humanism" in local Internet design.

3.5.5. Scalability and Replicability

One of the defining strengths of the proposed model is its **low-cost scalability**. The implementation relied solely on software configuration and open-standard protocols—no additional routers, switches, or proprietary licenses were required. This makes the model easily replicable in schools, rural broadband projects, or other residential complexes across Indonesia. The Mikrotik RB951Ui-2HnD used in this research is an affordable device widely available in the Indonesian market, ensuring accessibility for small-scale Internet providers.

Replicability also extends to its **operational simplicity**. Once configured, the *Queue Tree* automatically regulates traffic according to defined rules, and DoH operates continuously in the background without manual intervention. This autonomy reduces administrative overhead and human error, making it sustainable even in low-resource environments. In the context of *Internet Sehat*, such design democratizes access to secure and stable Internet infrastructures—empowering communities to maintain digital sovereignty without dependence on external service providers.

3.5.6. Comparison with Traditional and Commercial Solutions

Traditional commercial ISPs often rely on costly hardware-based traffic management systems or proprietary DNS filtering services. These approaches, while effective, are financially inaccessible for community-level networks. The *Queue Tree + DoH* configuration provides a software-defined alternative that achieves comparable results at a fraction of the cost.

Unlike firewall-based filtering systems that inspect and block traffic post-transmission, DoH prevents unsafe connections preemptively at the name resolution stage. This not only conserves bandwidth but also minimises exposure to malicious content. Similarly, while commercial QoS solutions depend on centralised management platforms, the *Queue Tree* method provides decentralised control directly at the router level, preserving autonomy for local administrators.

Comparative analysis also reveals that while enterprise-level encryption often requires additional CPU resources, Mikrotik's integration of DoH within RouterOS proved lightweight and efficient. This efficiency aligns with findings by [23] and [24] , who reported that optimised routing and encryption algorithms can yield significant performance gains even on low-cost hardware [8]. Thus, this model presents an innovative balance between affordability and technical excellence.

3.5.7. Challenges and Limitations

While the results are promising, certain limitations merit discussion. First, DoH introduces additional encryption overhead that may increase CPU utilisation on the router during peak loads. Although no performance degradation was observed in this study, long-term monitoring in larger-scale networks may be necessary to confirm system stability. Second, DNS filtering via third-party services like Cloudflare introduces partial external dependency, potentially raising sovereignty concerns if extended to government or institutional environments. A future development path could involve establishing **national or local DoH servers** to maintain both privacy and data autonomy within Indonesia's jurisdiction.

Another limitation involves user behavior beyond the control of QoS mechanisms. While *Queue Tree* ensures equitable bandwidth allocation, excessive simultaneous high-bandwidth activities (such as multiple HD streams) could still saturate available capacity [25]. Continuous user education remains essential to promote responsible Internet use consistent with *Internet Sehat* values.

3.5.8. Scientific and Practical Contributions

The findings of this research contribute to both academic discourse and practical network engineering. Theoretically, it advances the understanding of integrated QoS-security frameworks by demonstrating that traffic prioritisation and encrypted DNS protocols can coexist harmoniously without compromising performance. Empirically, it provides quantifiable evidence that such integration leads to measurable improvements in latency, throughput, and packet stability.

Practically, this study offers a *blueprint for community-based Internet management*. The configuration scripts, monitoring routines, and evaluation methodology are adaptable to other contexts. Institutions aiming to improve digital infrastructure—such as rural schools, local governments, or small Internet cafés—can replicate this model with minimal technical expertise. By merging QoS control with DNS encryption, the system ensures equitable, secure, and efficient Internet delivery, making it a replicable example of *digital sustainability* in action.

3.5.9. The Future of Healthy Internet Infrastructure

The success of this project underscores the growing importance of integrating **technical performance with digital ethics** in Internet governance. As emerging technologies such as AI, IoT, and cloud services expand the demand for secure connectivity [26], foundational elements like *Queue Tree* and DoH will play increasingly strategic roles. Future research could focus on integrating AI-based predictive QoS algorithms, adaptive DoH routing, or locally hosted DNS security layers to further enhance resilience and autonomy.

Ultimately, the combined implementation at Infotek Hotspot serves as a *microcosm of Indonesia's digital transformation agenda*. It demonstrates how even small-scale initiatives can embody the national vision for an Internet that is productive, inclusive, and ethically grounded. By proving that *Internet Sehat* can be engineered through open-source principles and accessible technologies, this research contributes not only to the field of computer networking but also to the broader discourse on sustainable and responsible digital development.

The integration of *Queue Tree* and *DNS over HTTPS* in a community hotspot environment has produced tangible technical and social benefits. It reduced latency and packet loss, improved throughput, ensured privacy, and established an ethical framework for Internet use. The approach is **cost-effective, replicable, and socially relevant**, providing a viable path toward the realisation of a stable and secure Internet infrastructure in Indonesia. As both a technical innovation and a social intervention, this model demonstrates how network engineering can contribute to the creation of a truly **Healthy Internet**—fast, fair, and safe for all.

4. Conclusion

The integration of Queue Tree and DNS over HTTPS (DoH) on Mikrotik routers successfully enhanced both technical performance and ethical standards in community Internet networks, resulting in a stable, fair, and secure digital ecosystem aligned with Indonesia's Internet Sehat vision. This approach demonstrates that through intelligent, low-cost, and replicable network configurations, it is possible to achieve sustainable Internet infrastructure that unites technological efficiency with digital responsibility for broader social benefit.

References

[1] M.-Y. Wu, "Examining the impacts of information and communication technology (ICT) on national development and wellbeing: A global perspective," *J. Econ. Technol.*, vol. 3, pp. 190–201, 2025, doi: https://doi.org/10.1016/j.ject.2024.11.006.

[2] M. O. Olomu, G. O. Binuyo, and T. O. Oyebisi, "The adoption and impact of Internet-based technological innovations on the performance of the industrial cluster firms," *J. Econ. Technol.*, vol. 1, pp. 164–178, 2023, doi: https://doi.org/10.1016/j.ject.2023.11.004.

[3] W. Welda, "DETERMINATION OF MIKROTIK ROUTER BASED ON PRICE AND QUALITY USING SIMPLE ADDITIVE WEIGHTING (SAW) METHOD," *Bull. Netw. Eng. INFORMATICS*, vol. 1, p. 25, Apr. 2023, doi: 10.59688/bufnets.v1i1.8.

[4] L. Kristiana and A. Z. Azmi, "Bandwidth Limitation Based on Content Classification Using Queue Trees and Hierarchical Token Buckets," *E3S Web Conf.*, vol. 484, pp. 1–11, 2024, doi: 10.1051/e3sconf/202448402011.

[5] F. Aktas, I. Shayea, M. Ergen, B. Saoud, A. E. Yahya, and A. Laura, "AI-enabled routing in next generation networks: A survey," *Alexandria Eng. J.*, vol. 120, pp. 449–474, 2025, doi: https://doi.org/10.1016/j.aej.2025.01.095.

[6] A. Nurmawan, F. Fahrullah, R. Ismayanti, F. Alameka, and H. Haerullah, "Implementasi Jaringan Hotspot Menggunakan Metode Queue Tree Pada Router Mikrotik Toko Sinar Jaya," *J. Rekayasa Teknol. Inf.*, vol. 8, p. 164, Dec. 2024, doi: 10.30872/jurti.v8i2.16812.

[7] A. Dauerer, "A systematic literature review of performance measurement systems and the integration of ESG factors," *Environ. Sustain. Indic.*, vol. 27, p. 100746, 2025, doi: https://doi.org/10.1016/j.indic.2025.100746.

[8] F. Casaril and L. Galletta, "Developing security metrics for space systems: A study considering the NIST Cybersecurity Framework 2.0 and the NIS2," *Int. J. Crit. Infrastruct. Prot.*, vol. 51, p. 100805, 2025, doi: https://doi.org/10.1016/j.ijcip.2025.100805.
[9] P. S. M. B. Bossoufi, "Digital Technologies and Applications," Lecture Notes in Networks and Systems. [Online]. Available: https://link.springer.com/book/10.1007/978-3-031-68650-4
[10] Y. M. Hazairin, Farhan Toibah Umi Kalsum, "Designing A Web-Based Mikrotik Hotspot Server Monitoring Application.pdf," *Publishing*, vol. 4, no. 1, p. 11, 2024, [Online]. Available: https://penerbitadm.pubmedia.id/index.php/KOMITEK/article/view/1745/2056
[11] M. Munawarsyah, D. Ratnasari, M. Hafiun, and A. Aziz, "The Implications of Social Media Use Among Teenagers in The Digital Era: An Islamic Education Perspective.," *PAKAR Pendidik.*, vol. 23, pp. 342–352, Jul. 2025, doi: 10.24036/pakar.v23i2.697.
[12] U. Pribadi, M. Iqbal, and F. Restiane, "Factors Affecting Trust in E-Government," *J. Gov. Civ. Soc.*, vol. 5, p. 263, Oct. 2021, doi: 10.31000/jgcs.v5i2.4848.
[13] S. Senyao and S. Ha, "How social media influences resident participation in rural tourism development: a case study of Tunda in Tibet," *J. Tour. Cult. Chang.*, vol. 20, pp. 1–20, Nov. 2020, doi: 10.1080/14766825.2020.1849244.
[14] M. Rath and J. Chatterjee, "Strength Optimized Weight Balancing for Traffic Management in Vehicular Ad-hoc Networks," *Int. J. Bus. Data Commun. Netw.*, vol. 20, pp. 1–19, Feb. 2025, doi: 10.4018/IJBDCN.368561.
[15] M. I. Nasution, F. Rahim, and H. Alfarizzi, "Analysis and Implementation of Simple Queue and Queue," *J. Appl. Enginerring Technol. Sci.*, vol. 4, no. 1, pp. 488–498, 2022.
[16] K. Hynek, D. Vekshin, J. Luxemburk, T. Cejka, and A. Wasicek, "Summary of DNS over HTTPS Abuse," *IEEE Access*, vol. 10, p. 1, Jan. 2022, doi: 10.1109/ACCESS.2022.3175497.
[17] R. Ridobillah, D. Indrayana, and F. Az-Zahra, "ANALISIS PERBANDINGAN UNTUK OPTIMALISASI JARINGAN MENGGUNAKAN METODE QUEUE TREE DAN PCQ DI ICT UMMI," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 8, pp. 10147–10154, Sep. 2024, doi: 10.36040/jati.v8i5.11021.
[18] N. Fachada and N. David, *Artificial Intelligence in Modeling and Simulation*, vol. 17, no. 6. 2024. doi: 10.3390/a17060265.
[19] S. Safinatunnaza, A. Noviriandini, L. Indriyani, and S. Fauziah, "LAN Bandwidth Management Using the Queue Tree Method," *Golden Ratio Data Summ.*, vol. 5, pp. 7–13, Feb. 2025, doi: 10.52970/grdis.v5i1.887.
[20] T. Panayiotou, K. Manousakis, S. Chatzis, and G. Ellinas, "A Data-Driven Bandwidth Allocation Framework with QoS Considerations for EONs," *J. Light. Technol.*, vol. PP, p. 1, Jan. 2019, doi: 10.1109/JLT.2019.2894179.
[21] K. Nzobokela, S. Tembo, and B. Habeenzu, "Enhancing Network Performance and Quality of Service (QoS) in a Wired Local Area Network (LAN)," vol. 13, pp. 1–14, Feb. 2024, doi: 10.5923/j.ijnc.20241301.01.
[22] V. Bhateja, J. Tang, S. C. Satapathy, P. Peer, and R. Das, *Evolution in Computational Intelligence, Proceedings of the 9th International Conference on Frontiers in Intelligent Computing: Theory and Applications (FICTA 2021)*, no. April. 2022. doi: 10.1007/978-981-16-6616-2.
[23] A. Haris, B. Riyanto, F. Surachman, and A. Ramadhan, "Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi," *Komputika J. Sist. Komput.*, vol. 11, pp. 67–76, Jan. 2022, doi: 10.34010/komputika.v11i1.5227.
[24] J. M. de L. G. C. Fuentes and SanchoAna AyerbeMaría Luisa Escalante, "Investigación en Ciberseguridad Actas de las VII Jornadas Nacionales (JNIC 2022)," in *JNIC*, 2022, p. 376. [Online]. Available: https://2022.jnic.es/Actas_JNIC_2022_v11.pdf
[25] C. Smansub, B. Purahong, P. Sithiyopasakul, and C. Benjangkaprasert, "A study of network bandwidth management by using queue tree with per connection queue," *J. Phys. Conf. Ser.*, vol. 1195, p. 12019, Apr. 2019, doi: 10.1088/1742-6596/1195/1/012019.
[26] A. M. Al-Ansi, A. Garad, M. Jaboob, and A. Al-Ansi, "Elevating e-government: Unleashing the power of AI and IoT for enhanced public services," *Heliyon*, vol. 10, no. 23, p. e40591, 2024, doi: https://doi.org/10.1016/j.heliyon.2024.e40591.