ISSN 2828-9463

Performance Optimization of Virtual Private Network Based on VXLAN VTEP on MikroTik Devices (Case Study: ID-Networkers West Jakarta)

Narendra Dylan Nugraha[1], Ari Ramadhan[2]
Computer Network Engineering Technology Study Program, Politeknik IDN Bogor

This study investigates the performance optimization of a Virtual Private Network (VPN) based on Virtual Extensible LAN (VXLAN) utilizing the VXLAN Tunnel Endpoint (VTEP) mechanism on MikroTik RouterOS version 7.19 devices within the ID-Networkers Jakarta Barat environment. The limitations of traditional Point-to-Point Tunneling Protocol (PPTP)-based VPN in terms of stability and scalability motivate the exploration of overlay technology as an alternative solution. The research method employed is network simulation using the PNETLab platform, applying two testing scenarios: PPTP as a baseline condition and VXLAN VTEP as the optimized solution. Performance evaluation is based on Quality of Service (QoS) parameters comprising throughput, latency, jitter, packet loss, and bandwidth, obtained through ICMP packet transmission and testing with iPerf and Wireshark. Results indicate that VXLAN VTEP produces more consistent latency (±5–8 ms compared to ±6–10 ms for PPTP) and 0% packet loss in both scenarios. Furthermore, VXLAN provides significant advantages in network segmentation flexibility and overlay scalability. Although VXLAN throughput is lower due to encapsulation overhead, bandwidth stability is better maintained compared to PPTP. This study concludes that implementing VXLAN VTEP on MikroTik devices is an effective solution for improving inter-site network service quality, particularly in terms of communication consistency and stability.
Keywords: VPN, VXLAN, VTEP, Mikrotik, QoS, Network Optimization.

This is an open access article under the CC BY-NC license

Corresponding Author:
Narendra Dylan Nugraha
Computer Network Engineering Technology Study Program, Politeknik IDN Bogor, Indonesia
narendradylan46@gmail.com

1. Introduction

The development of computer networking technology demands that organizations provide secure, stable, and high-performance communication services. One commonly used technology to connect networks between locations is a Virtual Private Network (VPN), which enables data transfer over public networks using encrypted and isolated channels [1]. However, traditional VPNs based on Point-to-Point Tunneling Protocol (PPTP) often face performance limitations when dealing with increasingly complex operational requirements, such as increased latency, jitter fluctuations, and limitations in network segmentation and scalability as traffic between locations increases [2].

Virtual Extensible LAN (VXLAN) technology offers a more flexible and scalable solution than traditional tunneling mechanisms. VXLAN enables Layer-2 communications to run over Layer-3 networks through the VXLAN Tunnel Endpoint (VTEP) mechanism for encapsulation and decapsulation. This technology is relevant for network environments that require extensive segmentation, high scalability, and efficient inter-segment management [3].

According to a market report from Global Market Insights, the global VXLAN market value reached USD 1.38 billion in 2022 and is projected to exceed USD 6 billion by 2032, as cloud computing, virtualization, and modern network overlay technologies grow [4]. ID-Networkers West Jakarta is a computer networking training and course institution with two operational locations on Jalan Palmerah and Jalan Anggrek Rosliana. Currently, inter-building connectivity still relies on traditional VPNs, which in practice experience high latency, jitter fluctuations, and increasing overhead as network traffic increases [5].

With VXLAN support in Mikrotik RouterOS version 7 (RouterOS v7), there is an opportunity to improve the quality of inter-building connections by implementing VXLAN-based VPN (VTEP). However, this technology requires in-depth analysis of network conditions, pre- and post-implementation testing, and identification of the most influential parameters for optimization [6]. Several previous studies have shown that VXLAN can provide improved performance compared to traditional tunneling, particularly in terms of scalability and segmentation efficiency [3][7][8]. However, most of this research has focused on enterprise-class devices or data center environments, so studies of VXLAN performance on Mikrotik devices in inter-building network scenarios are still limited [9]. This study aims to compare the performance of traditional VPN (PPTP) with VXLAN-based VPN VTEP on Mikrotik devices using QoS parameters, as well as provide technical recommendations for ID-Networkers and similar institutions.

2. Literature Review

Virtual Private Network (VPN) is widely utilized to provide secure communication over public networks; however, traditional tunneling protocols such as PPTP often face limitations related to scalability, network segmentation, and Quality of Service (QoS) performance as network complexity increases [1], [2]. To address these challenges, Virtual Extensible LAN (VXLAN) was developed as an overlay technology that enables Layer-2 communication over Layer-3 infrastructure through the VXLAN Tunnel Endpoint (VTEP) mechanism [3]. VXLAN offers significant advantages in terms of scalability, supporting millions of virtual segments, while also simplifying network management in distributed environments [3], [5]. Previous studies have demonstrated that VXLAN can improve network flexibility and provide more consistent performance compared to conventional tunneling technologies, particularly in virtualized and multi-site network architectures [7]–[9].

Although previous research has confirmed the benefits of VXLAN, most studies have focused on enterprise networks, cloud infrastructures, or data center environments, while investigations involving MikroTik RouterOS devices in inter-building communication scenarios remain limited [7]–[9]. Furthermore, comparative evaluations between PPTP and VXLAN VTEP based on QoS parameters in educational institution networks are still insufficient. This gap raises the need for further research to determine whether VXLAN VTEP can effectively improve network performance and service quality compared with traditional VPN implementations. Therefore, this study addresses the following research questions: (1) How does the performance of VXLAN VTEP compare with PPTP in terms of throughput, latency, jitter, packet loss, and bandwidth? and (2) To what extent can VXLAN VTEP improve the stability, scalability, and overall quality of inter-site network communication on MikroTik devices?.

3. Methods

This research uses a network simulation method with stages adapted from the Simulation-Based Research approach, including: (1) Problem Formulation, (2) Conceptual Model, (3) Input/Output Data, (4) Modeling, (5) Simulation, and (6) Verification & Validation. The simulation approach was chosen because it allows for controlled experiments with adjustable and replicable parameters without the need for physical hardware [10].

Topology and Testing Scenario

The simulation was conducted on the PNETLab platform version 5.3.11 running on VMware ESXi 9.0. The network topology consisted of three Mikrotik RouterOS version 7.19 routers representing three locations: IDN-Palmerah, IDN-Rosliana, and IDN-Tembalang. The backbone network used the 100.126.0.0/29 subnet with the OSPF dynamic routing protocol. Each location had one virtual server as an end-user to generate and receive test traffic.

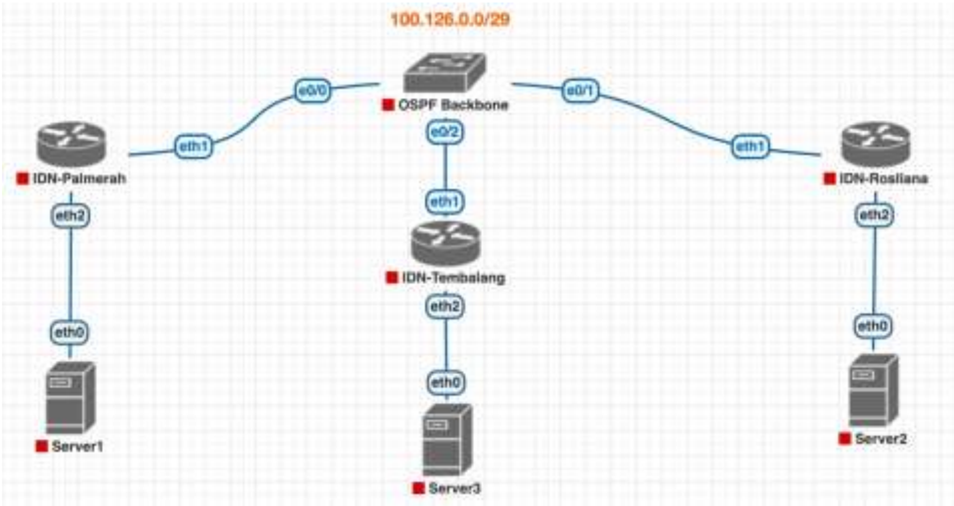

Figure 1. Research Network Topology

Two test scenarios were implemented sequentially:

a. Scenario 1 — Traditional VPN (PPTP): PPTP configuration as the baseline. Each router is configured as a PPTP server/client with MSCHAPv2 authentication. OSPF runs over the PPTP interface as the routing mechanism between the sites. The local networks of each site are on different subnets (192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24).

b. Scenario 2 — VXLAN-Based VPN VTEP: PPTP configuration is disabled and replaced with VXLAN using VNI 100 on UDP port 8472. Each router is configured as a VTEP with the loopback interface as the tunnel source. All sites are connected to a single Layer-2 segment (192.168.1.0/24) via a VXLAN bridge. OSPF runs on top of the underlay network to distribute VTEP routes between routers.

IP Address Configuration

IP addressing is designed according to the needs of each scenario. The main difference lies in the use of a loopback interface as the VTEP source in the VXLAN scenario, replacing the PPTP interface in the baseline scenario.

Table 1. IP Address Mapping — Traditional VPN (PPTP) Scenario

No.	Device	Hostname	Interface	IP Address	Description
1	Router	IDN-Palmerah	ether1	100.126.0.1/29	Backbone
			ether2	192.168.1.1/24	Gateway
			pptp-in	100.127.1.1/32	PPTP
		IDN-Rosliana	ether1	100.126.0.2/29	Backbone
			ether2	192.168.2.1/24	Gateway
			pptp-out	100.127.1.2/32	PPTP
		IDN-Tembalang	ether1	100.126.0.3/29	Backbone
2	Server	Server1	eth0	192.168.1.11/24	LAN
		Server2	eth0	192.168.2.11/24	LAN
		Server3	eth0	192.168.3.11/24	LAN

Table 2. IP Address Mapping — VXLAN VTEP Scenario

No.	Device	Hostname	Interface	IP Address	Description
1	Router	IDN-Palmerah	ether1	100.126.0.1/29	Backbone

No.	Device	Hostname	Interface	IP Address	Description
			loopback	100.127.1.1/32	VTEP
		IDN-Rosliana	ether1	100.126.0.2/29	Backbone
			loopback	100.127.1.2/32	VTEP
		IDN-Tembalang	ether1	100.126.0.3/29	Backbone
			loopback	100.127.1.3/32	VTEP
2	Server	Server1	eth0	192.168.1.11/24	LAN
		Server2	eth0	192.168.1.12/24	LAN
		Server3	eth0	192.168.1.13/24	LAN

Testing Parameters and Instruments

Network performance testing was conducted using three instruments: (1) the ping command to measure latency, jitter, and packet loss through ICMP packet transmission; (2) iPerf3 to measure throughput and bandwidth on TCP and UDP protocols; and (3) Wireshark version 4.6 to capture and analyze VXLAN packets in real time [12]. The QoS parameters measured refer to the standards proposed by Wagiu et al. [13], including:

a. Throughput: The actual data transmission rate (bps or Mbps) generated by the network during the test period.
b. Latency: The delay time (ms) for data packets from sender to receiver, measured by the average RTT value.
c. Jitter: The variation in time between packets (ms) that describes transmission consistency.
d. Packet Loss: The percentage of packets that fail to reach their destination compared to the total packets sent.
e. Bandwidth: The available transmission capacity and its utilization pattern during the test session.

Each scenario was tested using ten iterations of ICMP packets (count=10) to ensure data consistency and TCP/UDP testing using iPerf3. The hardware used included a laptop with an Apple M1 processor, 8GB of RAM, and 256GB of SSD storage.

4. Result And Discussion

Connectivity and Configuration Verification

In the PPTP scenario, all routers successfully established PPTP tunnel connections, and OSPF adjacencies were established over the tunnel interfaces. Inter-router and inter-server connectivity was verified using the ping command and routing table confirmation. In the VXLAN scenario, VTEP configuration was successfully implemented on all three routers, with the bridge host table demonstrating dynamic MAC address learning through the VXLAN interface. OSPF adjacencies were established over the underlying networks (ether1 and loopback), and all servers successfully communicated within a single Layer-2 segment with the 192.168.1.0/24 subnet.

Figure 3. VXLAN traffic capture results using Wireshark

QoS Test Results — PPTP Scenario (Baseline)

Testing in the PPTP scenario between Server 1 (192.168.1.11) and Server 2 (192.168.2.11) produced an average latency of ±4.4 ms (min 3.05 ms; max 5.19 ms) with a standard deviation of ±0.585 ms. The jitter value, derived from the difference in latency between packets, ranged from ±0.5–0.6 ms. Packet loss was recorded at 0% in all ping tests. Throughput testing using iPerf3 TCP showed an average value of ±1.25–1.34 Mbps with a highly fluctuating bandwidth pattern, reaching 5 Mbps in the initial seconds, then dropping to 0 bps at several intervals, and stabilizing at around ±1.03 Mbps. These fluctuations indicate TCP retransmissions caused by PPTP encapsulation overhead and the active PPP connection control mechanism.

QoS Test Results — VXLAN VTEP Scenario

In the VXLAN VTEP scenario, testing between Server1 (192.168.1.11) and Server2 (192.168.1.12) within a single VXLAN VNI 100 segment resulted in an average latency of ±5.6 ms (min 4.32 ms; max 8.85 ms) with a standard deviation of ±1.248 ms. Jitter values ranged from ±0.5–1.2 ms, slightly higher than PPTP but still within the tolerance limits of standard network services. Packet loss was recorded at 0% across all test sessions. TCP throughput testing with iPerf3 showed an average value of approximately ±0.09–0.13 Mbps, which is lower than PPTP, primarily due to the overhead of encapsulating Ethernet frames into UDP packets (50-byte VXLAN header) and the very small Congestion Window (cwnd) (±1.41 KB), indicating a bottleneck at the virtualization layer. However, the resulting bandwidth pattern is more stable than PPTP.

Performance Comparison of PPTP vs. VXLAN VTEP

Table 3. QoS Parameter Comparison: PPTP vs. VXLAN VTEP

No.	Service	Throughput	Latency	Jitter	Packet Loss	Bandwidth
1	PPTP	± 1.25 – 1.34 Mbps	± 6 – 10 ms	± 0.5 – 0.6 ms	0%	Fluctuating (0 – 5 Mbps)
2	VXLAN	± 0.09 – 0.13 Mbps	± 5 – 8 ms	± 0.5 – 1.2 ms	0%	More stable (±100 Kbps – 800 Kbps)

Analysis and Discussion

Based on Table 3, the VXLAN VTEP implementation exhibits several characteristics that differ significantly from PPTP. First, in terms of latency, VXLAN produces more consistent values (±5–8 ms) with a narrower range than PPTP (±6–10 ms). Although the average latency values do not differ dramatically, VXLAN latency stability is higher because the loopback interface, as the VTEP source, provides more deterministic routing than the dynamic PPTP interface. These results align with the findings of Sudrajat et al. [7], which show that VXLAN produces more consistent latency than GRE and L2TP in a virtualized environment.

Second, throughput values in the VXLAN scenario are lower (±0.09–0.13 Mbps) than PPTP (±1.25–1.34 Mbps). This decrease is due to the VXLAN encapsulation overhead, which adds approximately 50 bytes of UDP/IP header per frame, reducing the effective transmittable payload. Furthermore, the 1450-byte MTU configuration on the VXLAN interface in the resource-constrained PNETLab simulation environment (8 GB RAM, Apple M1 processor) contributed to the performance bottleneck. Zhao et al. [8] noted that optimizing the MTU parameters and VXLAN encapsulation mechanisms in a resource-constrained environment requires specific adjustments to maximize throughput.

Third, VXLAN's bandwidth performance exhibits greater stability. In PPTP, bandwidth values fluctuate significantly (0–5 Mbps) due to TCP retransmissions triggered by PPP connection instability. In contrast, VXLAN maintains bandwidth within the range of ±100–800 Kbps with a more predictable pattern. This advantage is relevant for network applications that require consistent data flow, such as real-time services and server-to-server data transfers.

Fourth, VXLAN significantly outperforms in terms of scalability and flexibility. By leveraging 24-bit VNI, VXLAN supports up to 16 million virtual network segments [3], far exceeding the 4096 VLAN limit of traditional infrastructure. All servers at all three locations were successfully placed on a single Layer-2 segment (192.168.1.0/24), eliminating the need for inter-VLAN routing and simplifying topology management. This aligns with the findings of Abdullah et al. [9], who demonstrated the effectiveness of VXLAN for multi-location interconnection at the educational institution scale.

Considering all QoS parameters, it can be concluded that VXLAN VTEP provides improved quality of service in terms of consistency and stability, although raw throughput is lower than PPTP. Given ID-Networkers' needs, which focus on the stability of network-based training services, VXLAN's performance profile is more suitable than PPTP, which is susceptible to high bandwidth fluctuations.

5. Conclusion

This study successfully implemented and evaluated the performance optimization of a VXLAN VTEP-based VPN on a Mikrotik RouterOS version 7.19 device through network simulation using PNETLab. Several conclusions can be drawn as follows:

a. First, traditional PPTP-based VPNs still have limitations in terms of bandwidth stability and segmentation scalability, characterized by significant throughput fluctuations and the limitations of conventional VLAN segments.
b. Second, the implementation of VXLAN VTEP on Mikrotik devices using a loopback interface as the VTEP source and OSPF as the underlying routing protocol resulted in more stable Layer-2 connectivity between sites, with more consistent latency (±5–8 ms) and more predictable bandwidth (±100–800 Kbps).
c. Third, the 0% packet loss rate in both scenarios confirms the reliability of the VXLAN UDP encapsulation mechanism in a controlled simulation environment.
d. Fourth, although VXLAN throughput is lower due to encapsulation overhead, its advantages in scalability (supporting >16 million VNI segments), overlay topology flexibility, and performance consistency make it a more viable solution for long-term inter-premises networking needs.

This study is limited to a simulated network environment and focuses solely on QoS parameters, including throughput, latency, jitter, packet loss, and bandwidth. Therefore, future research is recommended to validate the findings in real-world network deployments and larger-scale environments. Further studies may also compare VXLAN with other tunneling technologies and include security, scalability, and resource utilization analyses to provide a more comprehensive evaluation.

6. References

[1] I. Afrianto and E. B. Setiawan, “Kajian Virtual Private Network (VPN) sebagai Sistem Pengamanan Data pada Jaringan Komputer (Studi Kasus Jaringan Komputer UNIKOM),” *Jurnal Ilmiah Komputer dan Informatika*, 2016.
[2] W. O. Zamalia, L. M. F. Aksara, and M. Yamin, “Analisis Perbandingan Performa QoS PPTP, L2TP, SSTP dan IPSec pada Jaringan VPN Menggunakan Mikrotik,” *Jurnal Teknologi Informasi*, vol. 8, no. 2, pp. 112–120, 2020.
[3] M. Mahalingam et al., “Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks,” *IETF RFC 7348*, Aug. 2014.

[4] Global Market Insights, "Virtual Extensible LAN Market Size, Share & Forecast 2025–2034." [Online]. Available: https://www.gminsights.com/industry-analysis/virtual-extensible-lan-market.

[5] T. Singh, V. Jain, and S. Babu G, "VXLAN and EVPN for Data Center Network Transformation," *Cisco Systems White Paper*, 2017.

[6] Dahnial, "Analisa Perbandingan Quality of Service antara Protokol PPTP dan L2TP pada Virtual Private Network Berbasis Router Mikrotik," *Jurnal Informatika*, vol. 5, no. 1, pp. 45–52, 2018.

[7] M. S. M. Sudrajat, D. Perdana, and R. M. Negara, "Performance Analysis of VXLAN and NVGRE Tunneling Protocol on Virtual Network," *Journal of Network and Computer Applications*, vol. 103, pp. 1–8, 2018.

[8] Z. Zhao, F. Hong, and R. Li, "SDN Based VXLAN Optimization in Cloud Computing Networks," *IEEE Access*, vol. 5, pp. 20011–20021, 2017.

[9] S. D. Abdullah, S. Lutfi, and A. Fuad, "Analisis dan Desain VXLAN untuk Interkoneksi Lokasi yang Berbeda di Universitas Khairun," *Jurnal Informatika dan Jaringan*, vol. 6, no. 2, pp. 89–97, 2021.

[10] I. Dorathy and M. Chandrasekaran, "Simulation Tools for Mobile Ad Hoc Networks: A Survey," *Journal of Applied Research and Technology*, vol. 16, no. 6, pp. 437–445, 2018.

[11] T. Rahman et al., "Analisis Performa RouterOS MikroTik pada Jaringan Internet," *Jurnal Inovtek Polbeng – Seri Informatika*, vol. 5, no. 1, pp. 178–182, 2020.

[12] R. Kaur, "Investigating Network Traffic Using Packet Sniffing Tool–Wireshark," *JETIR*, vol. 6, no. 1, 2019.

[13] E. B. Wagiu, A. Butar-butar, and J. I. Sihotang, "Analisis QoS (Quality of Service) pada Jaringan Internet (Studi Kasus: Universitas Advent Indonesia)," *TEIKA: Journal of Engineering, Informatics and Knowledge Applications*, vol. 9, no. 1, 2019.