OPEN ACCESS

Volume 10 (2), April 2026, 694-701

E-ISSN:2580-1643

Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)

DOI: https://doi.org/10.35870/jtik.v10i2.5561

Analisis dan Penerapan VPN *Site to Site* Jaringan Antargedung Universitas Bina Darma

Muhammad Faiz Nabil [1*], Aan Restu Mukti [2], Suryayusra [3], Dedi Irawan [4]

[1*,2,3,4] *Program Studi Teknik Informatika, Falkutas Sains Teknologi, Universitas Bina Darma, Kota Palembang, Provinsi Sumatera Selatan, Indonesia.*

a r t i c l e i n f o

Article history:
Received 19 September 2025
Received in revised form
20 October 2025
Accepted 20 November 2025
Available online April 2026.

Keywords:
VPN Site-to-Site; PPTP; L2TP; Mikrotik; QoS; Throughput; Delay; Packet Loss; Jitter; Universitas Bina Darma.

Kata Kunci:
VPN Site-to-Site; PPTP; L2TP; Mikrotik; QoS; Throughput; Delay; Packet Loss; Jitter; Universitas Bina Darma.

a b s t r a c t

This research analyzes the implementation of a site-to-site Virtual Private Network (VPN) between buildings at Universitas Bina Darma using two protocols: Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP). The objective is to evaluate network performance based on Quality of Service (QoS) parameters, including delay, throughput, packet loss, and jitter. The study employs an experimental method by configuring VPN connections on MikroTik devices installed in each building and conducting tests using the iperf3 application. The results show that L2TP provides a lower average delay (6 ms) compared to PPTP (18 ms) and achieves higher throughput, reaching 95.8 Mbps at 100 Mbps bandwidth. In contrast, PPTP records lower throughput, with an average of 71.9 Mbps and TCP throughput of only 3.8 Mbps, but demonstrates better stability in terms of packet loss (0–0.0046%) and jitter (0.8–1.4 ms). In conclusion, PPTP is more suitable for stable data transmission, while L2TP is preferable for high-speed communication, and the choice of protocol should be adjusted to specific network requirements.

a b s t r a k

Penelitian ini membahas implementasi Virtual Private Network (VPN) site-to-site antar gedung di Universitas Bina Darma dengan membandingkan dua protokol, yaitu Point-to-Point Tunneling Protocol (PPTP) dan Layer 2 Tunneling Protocol (L2TP). Tujuannya adalah mengevaluasi kinerja jaringan berdasarkan parameter Quality of Service (QoS) yang mencakup delay, throughput, packet loss, dan jitter. Metode yang digunakan adalah penelitian eksperimental dengan konfigurasi VPN pada perangkat MikroTik di masing-masing gedung, serta pengujian menggunakan aplikasi iperf3. Hasil pengujian menunjukkan bahwa L2TP memiliki rata-rata delay lebih rendah (6 ms) dibanding PPTP (18 ms) dan throughput lebih tinggi, mencapai 95,8 Mbps pada bandwidth 100 Mbps. Sebaliknya, PPTP hanya mencapai 71,9 Mbps dengan throughput TCP rendah (3,8 Mbps), tetapi lebih stabil dari sisi packet loss (0–0,0046%) dan jitter (0,8–1,4 ms). Kesimpulannya, PPTP lebih sesuai untuk kebutuhan stabilitas transmisi, sedangkan L2TP lebih unggul untuk kecepatan tinggi, sehingga pemilihan protokol harus disesuaikan dengan kebutuhan jaringan.

Corresponding Author. Email: muhammadfaiznabil030104@gmail.com [1].

1. Pendahuluan

Internet telah menjadi infrastruktur krusial bagi institusi pendidikan dalam mendukung komunikasi, kolaborasi, dan pertukaran data. Namun, pemanfaatan jaringan publik menimbulkan risiko keamanan yang berpotensi mengancam integritas data. Salah satu solusi yang banyak diterapkan adalah *Virtual Private Network* (VPN), khususnya tipe site-to-site yang memungkinkan penghubungan jaringan antar lokasi secara aman melalui jaringan publik. Universitas Bina Darma memiliki tiga gedung kampus yang membutuhkan konektivitas andal dan aman guna menunjang aktivitas akademik dan administratif. Saat ini, koneksi antar gedung belum menggunakan VPN site-to-site, sehingga aspek keamanan dan efisiensi pertukaran data masih kurang optimal. Penelitian ini merancang dan menganalisis penerapan VPN site-to-site dengan dua protokol, yakni *Point-to-Point Tunneling Protocol* (PPTP) dan *Layer 2 Tunneling Protocol* (L2TP), menggunakan perangkat MikroTik sebagai infrastruktur jaringan. Evaluasi dilakukan berdasarkan parameter *Quality of Service* (QoS), meliputi throughput, delay, packet loss, dan jitter, untuk menentukan protokol yang paling sesuai digunakan pada jaringan antar gedung Universitas Bina Darma. Jaringan komputer merupakan kumpulan perangkat yang saling terhubung untuk berbagi data, sumber daya, dan layanan. Berdasarkan cakupannya, jaringan terbagi menjadi LAN, MAN, dan WAN (Mananggel *et al.*, 2021).

Dalam universitas, koneksi antar gedung termasuk dalam kategori WAN skala kecil yang memerlukan infrastruktur handal dan aman. Fungsi utama jaringan mencakup pertukaran informasi, pemanfaatan sumber daya bersama, komunikasi antar pengguna, dan manajemen sistem terpusat, dengan perangkat utama seperti server, client, switch, router, modem, dan media transmisi. Topologi jaringan dapat berupa bus, star, ring, mesh, atau hybrid, yang masing-masing memiliki kelebihan dan keterbatasan. Aspek keamanan menjadi prioritas sehingga diperlukan penerapan firewall, VPN, enkripsi, autentikasi, dan segmentasi jaringan. Secara luas, jaringan komputer telah menjadi fondasi penting dalam sektor pendidikan, bisnis, kesehatan, dan rumah tangga, sekaligus menjadi pendorong utama transformasi digital global. Internet adalah jaringan global yang menghubungkan jutaan perangkat komputer melalui protokol standar TCP/IP, memungkinkan pertukaran data dan komunikasi lintas sistem secara cepat dan efisien (Martin *et al.*, 2022). Fungsi utamanya meliputi akses informasi, komunikasi jarak jauh, bisnis digital, dan layanan berbasis cloud, meskipun menghadirkan tantangan terkait keamanan, privasi, dan ketergantungan teknologi. Akses internet diperoleh melalui ISP dengan perangkat seperti modem dan router, yang menggunakan alamat IP statis atau dinamis. Efisiensi layanan didukung oleh teknologi tambahan seperti DNS, caching server, dan HTTPS. Internet berperan sebagai infrastruktur vital yang menopang komunikasi global, ekonomi digital, inovasi teknologi, serta transformasi sosial di berbagai bidang. VPN merupakan teknologi jaringan yang memungkinkan koneksi aman melalui jaringan publik dengan memanfaatkan teknik tunneling dan enkripsi untuk menjaga kerahasiaan serta integritas data (Dewi, 2020). Teknologi ini banyak digunakan oleh perusahaan, lembaga pendidikan, dan pemerintahan, baik dalam bentuk *Remote Access VPN* untuk akses individu maupun *Site-to-Site VPN* yang menghubungkan jaringan antar lokasi, seperti antar gedung kampus. Berbagai protokol mendukung implementasi VPN, antara lain PPTP yang sederhana dan kompatibel, L2TP/IPSec dengan tingkat keamanan lebih tinggi, OpenVPN yang fleksibel dan aman, serta IKEv2/IPSec yang stabil untuk perangkat mobile.

VPN tidak hanya melindungi identitas pengguna dengan menyembunyikan alamat IP, tetapi juga membantu mengatasi pembatasan geografis dan memungkinkan akses ke sumber daya internal. Namun demikian, penggunaan VPN dapat menurunkan kecepatan koneksi akibat proses enkripsi serta sangat bergantung pada kualitas server, sehingga pemilihan protokol dan konfigurasi yang tepat menjadi faktor kunci dalam mengoptimalkan performa. Jenis VPN site-to-site menghubungkan dua atau lebih jaringan lokal (LAN) di lokasi berbeda melalui internet dengan perangkat seperti router atau firewall sebagai titik akhir (Usanto, 2021). Teknologi ini memungkinkan komunikasi antar jaringan berjalan otomatis tanpa interaksi langsung dari pengguna, sehingga sesuai untuk organisasi dengan cabang atau gedung terpisah, termasuk Universitas Bina Darma.

Implementasi VPN site-to-site memudahkan pertukaran data antar gedung secara aman, efisien, dan terintegrasi, serta memberikan akses terpusat ke server, sistem informasi, dan aplikasi internal. Protokol yang umum digunakan meliputi PPTP, L2TP, IPSec, dan OpenVPN. Walaupun konfigurasi teknisnya memerlukan ketelitian, VPN site-to-site menawarkan solusi hemat biaya, aman, dan efektif bagi institusi yang memerlukan konektivitas jaringan skala besar. *Quality of Service* (QoS) merupakan mekanisme pengelolaan lalu lintas jaringan yang menjamin kualitas layanan transmisi data dengan mengatur prioritas trafik agar aplikasi real-time seperti VoIP dan video conference tetap berjalan optimal (Budiman *et al.*, 2020). QoS mengukur parameter penting seperti delay, jitter, packet loss, dan throughput, serta bekerja melalui klasifikasi dan pengendalian trafik pada perangkat jaringan seperti router atau switch. Metode yang digunakan meliputi *traffic shaping*, *policing*, dan *scheduling* untuk memastikan distribusi bandwidth sesuai kebutuhan layanan. Penerapan QoS sangat penting pada jaringan skala besar atau antar lokasi, termasuk VPN antar gedung, guna mencegah gangguan seperti suara terputus, buffering video, atau keterlambatan akses aplikasi kritis. Oleh karena itu, QoS menjadi faktor utama dalam menjaga efisiensi, stabilitas, dan keandalan sistem jaringan modern.

MikroTik adalah perusahaan asal Latvia yang mengembangkan perangkat keras jaringan dan sistem operasi RouterOS, banyak dipakai oleh institusi pendidikan, perusahaan, dan ISP karena harga terjangkau, kemudahan konfigurasi, dan fitur lengkap (Bahtiar *et al.*, 2021). Perangkat MikroTik mendukung fungsi routing, firewall, NAT, DHCP, DNS, proxy, hotspot, load balancing, VLAN, monitoring, hingga VPN site-to-site dengan berbagai protokol seperti PPTP, L2TP, SSTP, dan IPsec. Konfigurasi dapat dilakukan melalui CLI, WebFig, maupun aplikasi Winbox yang populer. Dukungan komunitas yang luas dan dokumentasi lengkap menjadikan MikroTik pilihan utama untuk pembelajaran maupun implementasi nyata. Produk seperti RouterBOARD dan seri wireless hAP, RB, serta CCR semakin memperkuat fleksibilitasnya. Kombinasi harga terjangkau, fitur lengkap, dan kemudahan penggunaan menjadikan MikroTik solusi praktis untuk membangun infrastruktur jaringan yang handal, aman, dan mudah dikelola. Router adalah perangkat jaringan yang menghubungkan dua atau lebih jaringan dan meneruskan paket data dengan menentukan jalur terbaik melalui tabel routing dan protokol tertentu (Rismawati & Mulya, 2020). Selain menghubungkan LAN dan WAN, router juga berfungsi mengatur lalu lintas data, termasuk manajemen bandwidth, NAT, firewall, DHCP, VLAN, hingga sebagai VPN gateway pada perangkat seperti MikroTik, Cisco, atau Ubiquiti. Router terbagi menjadi hardware router dan software router, serta diklasifikasikan berdasarkan skala penggunaan mulai dari rumah hingga enterprise. Dengan peran vital tersebut, router menjadi komponen inti dalam membangun infrastruktur jaringan yang andal, aman, dan efisien, baik untuk skala kecil maupun besar. PPTP merupakan salah satu protokol VPN tertua yang dikembangkan Microsoft dan memungkinkan transmisi data terenkripsi melalui internet sehingga perangkat di lokasi berbeda dapat terhubung seolah dalam jaringan lokal (Satryawati *et al.*, 2022). Secara teknis, PPTP menggunakan PPP untuk autentikasi dan GRE untuk enkapsulasi, berjalan pada port TCP 1723, serta didukung oleh berbagai sistem operasi dan perangkat jaringan. Keunggulan PPTP terletak pada konfigurasi sederhana, kompatibilitas tinggi, dan kecepatan relatif baik karena overhead enkripsi rendah.

Namun, kelemahannya terdapat pada aspek keamanan, karena enkripsi MPPE yang digunakan dianggap rentan dibandingkan protokol modern seperti L2TP/IPSec atau OpenVPN. Oleh sebab itu, PPTP lebih sesuai untuk jaringan skala kecil, eksperimen, atau implementasi yang tidak memerlukan tingkat keamanan tinggi. L2TP adalah protokol VPN hasil kolaborasi Cisco dan Microsoft yang menggabungkan L2F dan PPTP untuk membangun koneksi aman melalui internet dengan membuat "terowongan" antar jaringan (Pamungkas *et al.*, 2021). L2TP bekerja pada lapisan data link dan mendukung enkapsulasi berbagai protokol, namun tidak menyediakan enkripsi bawaan sehingga biasanya dipadukan dengan IPSec (*L2TP/IPSec*) untuk menghadirkan autentikasi kuat, enkripsi AES/3DES, serta integritas data tinggi. Secara teknis, L2TP menggunakan UDP port 1701 untuk inisialisasi serta port 500 dan 4500 untuk keamanan dan NAT traversal, serta mendukung multiple tunneling

sessions di berbagai sistem operasi maupun perangkat jaringan seperti MikroTik dan Cisco. Jika dibandingkan dengan PPTP, *L2TP/IPSec* menawarkan konfigurasi lebih kompleks namun jauh lebih aman, sehingga menjadi pilihan tepat untuk VPN site-to-site pada perusahaan maupun institusi pendidikan yang membutuhkan koneksi antar lokasi dengan tingkat keamanan tinggi. Kajian terhadap penelitian terdahulu memberikan dasar dan acuan penting dalam penelitian ini. Beberapa studi yang dijadikan referensi antara lain: penelitian berjudul "Implementasi Virtual Private Network Menggunakan Point-to-Point Tunneling Protocol" oleh Satryawati *et al.* (2022); penelitian "Interkoneksi Site-to-Site dan Remote Access Menggunakan Virtual Private Network dan IP Security" oleh Arif dan Budiman (2020); serta penelitian "Rancang Bangun Jaringan Site to Site VPN dengan Protokol OpenVPN" oleh Usanto (2021).

2. Metodologi Penelitian

Pendekatan Penelitian

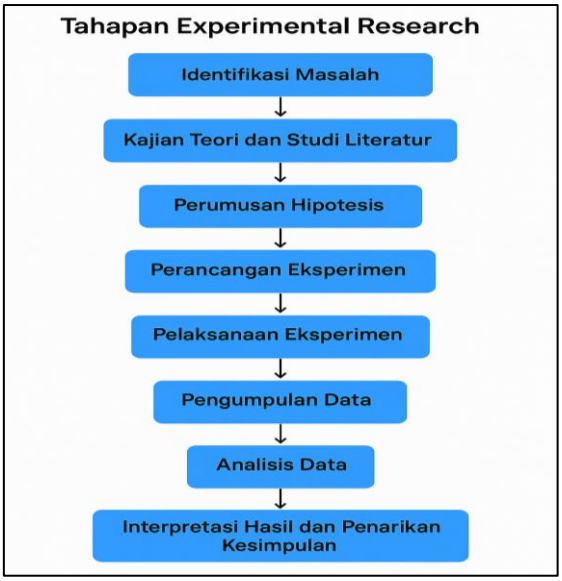
Penelitian ini menggunakan metode *experimental research* dengan pendekatan kuantitatif untuk mengevaluasi performa VPN site-to-site antar gedung Universitas Bina Darma. Objek penelitian adalah tiga gedung, yaitu BR1, BR2, dan BR3, yang masing-masing dihubungkan menggunakan perangkat MikroTik RouterOS sebagai endpoint VPN (Tasrif *et al.*, 2020).

Experimental Research

Konfigurasi dilakukan dengan dua protokol berbeda, yakni *Point-to-Point Tunneling Protocol* (PPTP) dan *Layer 2 Tunneling Protocol* (L2TP). Pada tahap awal, router dikonfigurasi dengan alamat IP dan routing dasar, kemudian dibangun koneksi VPN site-to-site menggunakan PPTP. Setelah dilakukan pengujian, konfigurasi diganti ke L2TP dan diuji kembali dengan parameter yang sama. Pengujian performa dilakukan menggunakan tools bawaan MikroTik seperti *ping* dan *bandwidth test*, dengan parameter *Quality of Service* (QoS) yang meliputi:

1) *Throughput* – jumlah data yang berhasil ditransmisikan per detik,
2) Delay (latency) – waktu tempuh rata-rata paket,
3) Packet loss – persentase paket yang hilang,
4) Jitter – variasi waktu keterlambatan antar paket.

Data hasil pengujian dicatat dan dibandingkan antara PPTP dan L2TP untuk menilai kelebihan dan kekurangannya. Analisis dilakukan secara deskriptif kuantitatif guna menentukan protokol yang lebih optimal dalam mendukung konektivitas antar gedung secara aman, stabil, dan efisien.



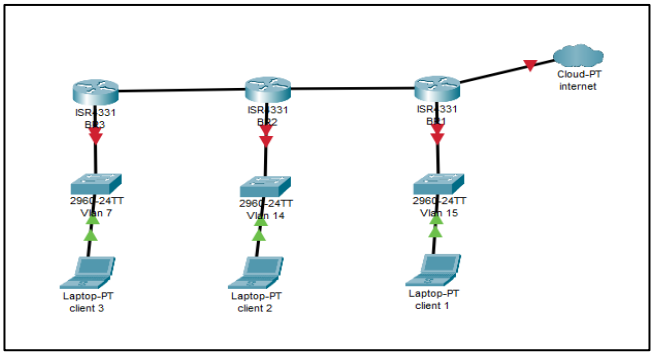
Gambar 1. Tahapan *Experimental Research*

3. Hasil dan Pembahasan

Hasil

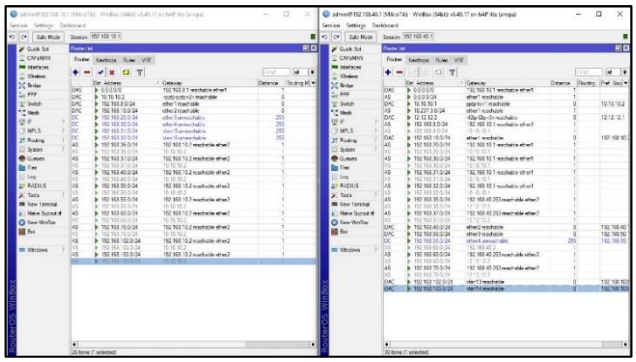
Evaluasi

Pada tahap ini dilakukan evaluasi kinerja VPN menggunakan protokol PPTP dan L2TP berbasis MikroTik dengan dukungan perangkat keras dan lunak. Pengujian dilakukan saat client melakukan *dial* VPN ke server untuk membangun tunnel sebelum data ditransmisikan. Data yang dikumpulkan bertujuan untuk mengamati performa kedua protokol dalam proses pembentukan koneksi serta menilai kelayakannya sebagai saluran komunikasi yang aman antar jaringan. Di bawah ini disajikan gambar topologi VPN site-to-site.



Gambar 2. Topologi VPN Site To Site

Peneliti mengambil data menggunakan aplikasi winbox saat pptp client membuat koneksi ke pptp server, hasil di dapatkan seperti gambar 3.



Gambar 3. Koneksi PPTP Dan L2TP

1) PPTP
   Proses pembentukan tunnel diamati menggunakan aplikasi Winbox. Pertukaran pesan dimulai ketika client mengirim *Start-Control-Connection-Request* ke server untuk memulai sesi. Server kemudian membalas dengan *Start-Control-Connection-Reply* sebagai tanda persetujuan. Selanjutnya, client mengirim *Outgoing-Call-Request* untuk melakukan koneksi, yang dijawab oleh server dengan *Outgoing-Call-Reply*. Proses dilanjutkan dengan pengiriman *Set-Link-Info* oleh client untuk menyesuaikan parameter koneksi. Setelah seluruh tahap ini selesai, tunnel berhasil terbentuk dan siap digunakan untuk transmisi data.
2) L2TP
   Proses pembentukan tunnel diamati melalui *Command Prompt* (CMD). Client mengirim pesan inisialisasi (*SCCRQ*) ke server, yang kemudian dibalas dengan *Start-Control-Connection-Reply* (*SCCRP*) sebagai indikasi bahwa proses pembentukan tunnel dapat dilanjutkan. Setelah itu, client kembali mengirim pesan konfirmasi untuk memastikan sinkronisasi. Tahapan ini menandakan bahwa tunnel L2TP berhasil terbentuk dan siap digunakan untuk komunikasi data antar jaringan dengan tingkat keamanan lebih tinggi apabila dipadukan dengan IPSec.

Hasil Perbandingan Protokol PPTP dan L2TP

Pada hasil penelitian ini, peneliti mengevaluasi dan membahas hasil analisis perbandingan antara dua protokol, yaitu PPTP dan L2TP, dengan membangun tunnel VPN melalui jaringan Universitas Bina Darma. Parameter yang diukur adalah besaran bandwidth pada jaringan server dan client, kemudian dianalisis berdasarkan *Quality of Service* (QoS) seperti delay, throughput, dan packet loss untuk menilai kinerja kedua protokol tersebut. Berikut disajikan hasil rekaman dari CMD:

```
Reply from 192.168.102.254: bytes=32 time=3ms TTL=126
Reply from 192.168.102.254: bytes=32 time=4ms TTL=126
Reply from 192.168.102.254: bytes=32 time=4ms TTL=126
Reply from 192.168.102.254: bytes=32 time=2ms TTL=126
Reply from 192.168.102.254: bytes=32 time=2ms TTL=126
Reply from 192.168.102.254: bytes=32 time=2ms TTL=126
Reply from 192.168.102.254: bytes=32 time=2ms TTL=126
Reply from 192.168.102.254: bytes=32 time=2ms TTL=126
Reply from 192.168.102.254: bytes=32 time=2ms TTL=126
Reply from 192.168.102.254: bytes=32 time=1ms TTL=126
Reply from 192.168.102.254: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.102.254:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 13ms, Average = 2ms
```

Gambar 4. Hasil Rekam Test Ping

Dari hasil tersebut, kemudian dilakukan penyaringan file header hasil rekaman PPTP. Berikut disajikan perhitungan delay, throughput, dan packet loss.

Analisis Hasil QoS

Berdasarkan pengujian *Quality of Service* (QoS) dengan parameter delay, throughput, jitter, dan packet loss menggunakan aplikasi *iperf3* pada protokol VPN PPTP dan L2TP, analisis dilakukan untuk menjelaskan kelebihan dan kekurangan masing-masing protokol.

Tabel 1. Tabel Perbandingan PPTP Dan L2TP

Parameter / Metode	PPTP	L2TP
QoS *Delay*	- Min: 1 ms - Avg: 18 ms (sangat baik) - Max: 186 ms (ada delay spike) - *Packet loss*: 1%	- Min: 1 ms - Avg: 6 ms (sangat baik) - Max: 105 ms - *Packet loss*: 0%
Throughput TCP	- *Sender*: 45,4 MB - *Receiver*: 45,3 MB - Rata-rata: 3,8 Mbps	- *Sender*: 1009 MB - *Receiver*: 1009 MB - Rata-rata: 84,6 Mbps
Throughput UDP 10 Mbps	- Total: 119 MB - Avg: 9,99 Mbps - Stabil, mendekati target	- Total: 119 MB - Avg: 9,99 Mbps - Stabil, mendekati target
Throughput UDP 50 Mbps	- Total: 595 MB - Avg: 49,9 Mbps - Stabil, mendekati target	- Total: 596 MB - Avg: 50,0 Mbps - Stabil, mendekati target
Throughput UDP 100 Mbps	- Total: 857 MB - Avg: 71,9 Mbps (tidak tercapai)	- Total: 1,11 GB - Avg: 95,8 Mbps (mendekati target)
Packet Loss UDP 10 Mbps	0% (baik sekali)	23% (buruk)
Packet Loss UDP 50 Mbps	0% (baik sekali)	8,2% (kurang baik)
Packet Loss UDP 100 Mbps	0,0046% (sangat kecil, dapat diabaikan)	27% (sangat tinggi, buruk)
Jitter UDP 10 Mbps	1,006 ms	1,000 ms
Jitter UDP 50 Mbps	0,876 ms	1,155 ms
Jitter UDP 100 Mbps	1,419 ms	368 ms (sangat tinggi)

1) Penjelasan Tabel Perbandingan PPTP dan L2TP
   Hasil pengujian menunjukkan bahwa L2TP memiliki delay rata-rata yang lebih rendah, yakni sekitar 6 ms, dibandingkan dengan PPTP yang mencapai 18 ms, sehingga L2TP lebih responsif untuk aplikasi real-time. Dari sisi throughput, L2TP menunjukkan keunggulan signifikan dengan rata-rata capaian 84,6 Mbps pada TCP dan 95,8 Mbps pada UDP dengan bandwidth 100 Mbps, sementara PPTP hanya mencapai 3,8 Mbps untuk TCP dan 71,9 Mbps untuk UDP. Namun, PPTP menawarkan kestabilan yang lebih baik dengan packet loss yang hampir nihil serta jitter yang rendah di seluruh skenario pengujian. Sebaliknya, L2TP mengalami packet loss yang cukup tinggi berkisar antara 8 hingga 27 persen serta jitter ekstrem hingga 368 ms pada bandwidth 100 Mbps.
2) Keunggulan dan Kelemahan
   PPTP unggul dalam hal stabilitas QoS, terbukti dari packet loss yang hampir nol, jitter yang rendah antara 0,8 hingga 1,4 ms, konfigurasi yang sederhana, serta kompatibilitas yang luas. Delay rata-rata sebesar 18 ms masih termasuk kategori sangat baik menurut standar ITU-T. Namun, kelemahan PPTP terletak pada throughput TCP yang rendah (3,8 Mbps), throughput UDP yang tidak maksimal pada bandwidth 100 Mbps (71,9 Mbps), delay maksimum yang cukup tinggi mencapai 186 ms, serta tingkat keamanan yang relatif lemah dibandingkan protokol VPN modern.

Sementara itu, L2TP unggul dalam hal throughput dengan nilai TCP sebesar 84,6 Mbps dan UDP yang mendekati target 100 Mbps, serta delay rata-rata yang sangat rendah yaitu 6 ms, menjadikannya efisien untuk transfer data besar dan aplikasi real-time. Namun, L2TP menghadapi kelemahan berupa packet loss yang tinggi (8–27%), jitter yang ekstrem pada bandwidth 100 Mbps (368 ms), konfigurasi yang lebih kompleks, serta kebutuhan sumber daya perangkat yang lebih besar.

Pembahasan

Hasil pengujian menunjukkan bahwa protokol L2TP memberikan performa throughput dan delay yang lebih baik dibandingkan PPTP, dengan rata-rata delay 6 ms dan throughput mencapai 95,8 Mbps pada bandwidth 100 Mbps. Temuan ini sejalan dengan penelitian Pamungkas *et al.* (2021) yang juga melaporkan keunggulan L2TP dalam hal kecepatan dan responsivitas jaringan pada implementasi VPN berbasis MikroTik. Namun, peningkatan kecepatan yang ditawarkan L2TP diimbangi oleh tingginya nilai packet loss dan jitter, khususnya pada bandwidth maksimum, yang menandakan potensi masalah stabilitas. Kondisi ini berbeda dengan PPTP yang meskipun memiliki throughput TCP yang lebih rendah, mampu menjaga kestabilan koneksi dengan packet loss yang hampir nihil dan jitter rendah, sebagaimana diamati oleh Satryawati *et al.* (2022) dalam studi mereka mengenai VPN PPTP. Kelebihan PPTP dalam hal stabilitas juga didukung oleh konfigurasi yang lebih sederhana dan kompatibilitas yang luas, meskipun aspek keamanannya lebih lemah jika dibandingkan dengan L2TP/IPSec. Perbedaan karakteristik ini menunjukkan bahwa pemilihan protokol VPN harus mempertimbangkan kebutuhan spesifik jaringan, apakah lebih mengutamakan kecepatan transfer data atau kestabilan transmisi. Selain itu, hasil ini menguatkan rekomendasi Arif dan Budiman (2020) yang menyarankan penyesuaian protokol VPN berdasarkan kondisi trafik dan prioritas aplikasi yang digunakan dalam jaringan. Oleh karena itu, meskipun L2TP menawarkan performa yang lebih tinggi, keandalan PPTP dalam menjaga kualitas koneksi tetap menjadi pilihan yang relevan dalam lingkungan yang menuntut stabilitas tinggi.

4. Kesimpulan dan Saran

Hasil pengujian *Quality of Service* (*QoS*) mengindikasikan bahwa protokol *L2TP* unggul dalam hal *throughput*, mencapai hingga 95,8 Mbps, serta memiliki *delay* rata-rata yang rendah sebesar 6 ms, sehingga lebih responsif untuk aplikasi dengan kebutuhan kecepatan tinggi. Sebaliknya, protokol *PPTP* menunjukkan kestabilan yang lebih baik dengan *packet loss* yang hampir nihil dan *jitter* rendah antara 0,8 hingga 1,4 ms, meskipun *throughput TCP*-nya terbatas pada 3,8 Mbps dan *throughput UDP* tidak mencapai maksimal pada bandwidth 100 Mbps, yaitu sebesar 71,9 Mbps. Oleh karena itu, *PPTP* lebih sesuai digunakan pada aplikasi yang mengutamakan kestabilan transmisi data, sementara *L2TP* lebih tepat untuk kebutuhan transfer data dalam volume besar dengan kecepatan tinggi, walaupun berisiko mengalami kehilangan paket yang lebih signifikan. Pemilihan protokol *VPN* hendaknya disesuaikan dengan prioritas kebutuhan jaringan, yakni *PPTP* untuk kestabilan dan *L2TP* untuk performa tinggi. Untuk penelitian lanjutan, disarankan melakukan perbandingan dengan protokol lain seperti *OpenVPN*, *WireGuard*, atau *IPSec*, serta menguji pada kondisi jaringan yang beragam, termasuk trafik tinggi, koneksi *wireless* versus kabel, dan jarak antar lokasi yang berbeda. Selain itu, perlu dilakukan investigasi lebih mendalam terkait penyebab tingginya *packet loss* pada *L2TP* dan penambahan analisis aspek keamanan agar evaluasi protokol dapat memberikan gambaran yang lebih menyeluruh dan aplikatif.

5. Daftar Pustaka

Arif, M., & Budiman, A. S. (2020). Interkoneksi site-to-site dan remote access menggunakan virtual private network dan IP security. *JSI: Jurnal Sistem Informasi, 12*(1), 1856–1866.

Bahtiar, D., *et al.* (2021). Pengenalan dasar instalasi jaringan komputer menggunakan MikroTik. *Jurnal Kreatif Mahasiswa Informatika, 2*(3), 507–518.

Budiman, A., Duskarnaen, M. F., & Ajie, H. (2020). Analisis Quality of Service (QoS) pada jaringan internet SMK Negeri 7 Jakarta. *PINTER: Jurnal Pendidikan Teknik Informatika dan Komputer, 4*(2), 32–36.

Dewi, S. (2020). Keamanan jaringan menggunakan VPN (Virtual Private Network) dengan metode PPTP (Point To Point Tunneling Protocol) pada kantor Desa Kertaraharja Ciamis. *EVOLUSI: Jurnal Sains dan Manajemen, 8*(1).

Firdausi, A., & Wardani, H. W. (2020). Simulasi dan Analisa QoS dalam Jaringan VPN Site To Site

Berbasis IPSec dengan Routing Dynamic. *InComTech: Jurnal Telekomunikasi dan Komputer*, *10*(2), 49-56.

Jackie, J. (2022). Analisa dan Penerapan Pencadangan Pusat Data Antar Site dengan Teknologi VPN. *Journal of Information System and Technology (JOINT)*, *3*(2), 257-269. https://doi.org/10.37253/joint.v3i2.6764.

Mananggel, A. V., Mewengkang, A., & Djamen, A. C. (2021). Perancangan jaringan komputer di SMK menggunakan Cisco Packet Tracer. *Edutik: Jurnal Pendidikan Teknologi Informasi dan Komunikasi, 1*(2), 119–131.

Martin, Y., Montessori, M., & Nora, D. (2022). Pemanfaatan internet sebagai sumber belajar. *Ranah Research: Journal of Multidisciplinary Research and Development, 4*(3), 242–246.

Pamungkas, A. P., Putra, M. R., & Hafizh, M. (2021). Analisis jaringan VPN menggunakan PPTP dan L2TP berbasis MikroTik pada Diskominfo Kabupaten Muko-muko. *Jurnal KomtekInfo, 8*(3), 189–194.

Rismawati, N., & Mulya, M. F. (2020). Analisis dan perancangan simulasi jaringan MAN (Metropolitan Area Network) dengan dynamic routing EIGRP (Enhanced Interior Gateway Routing Protocol) dan algoritma DUAL (Diffusing Update Algorithm) menggunakan Cisco Packet Tracer. *Jurnal SISKOM-KB (Sistem Komputer dan Kecerdasan Buatan), 3*(2), 55–62.

Satryawati, E., Pangestu, D. A., & Budiman, A. S. (2022). Implementasi virtual private network menggunakan point-to-point tunneling protocol. *JEIS: Jurnal Elektro dan Informatika Swadharma, 2*(1), 36–42.

Tasrif, E., Mubai, A., Huda, A., & Rukun, K. (2020). Pemanfaatan media pembelajaran berbasis augmented reality menggunakan aplikasi Ar_Jarkom pada mata kuliah instalasi jaringan komputer. *Jurnal Konseling dan Pendidikan, 8*(3), 217–223.

Usanto, U. (2021). Rancang bangun jaringan site to site VPN (Virtual Private Network) dengan protocol OpenVPN. *JEIS: Jurnal Elektro dan Informatika Swadharma, 1*(2), 55–65.