Jurnal Edik Informatika
Penelitian Bidang Komputer Sains dan Pendidikan Informatika
Website: ejournal.stkip-pgri-sumbar.ac.id/index.php/eDikInformatika

ANALISA PERFORMA INTERKONEKSI VPN MENGGUNAKAN METODE L2TPV3

Andry Maulana[1]
[1]Universitas Nusa Mandiri
andry.ayz@nusamandiri.ac.id

INFO ARTIKEL

Diterima:
18 Oktober 2023
Direview:
26 Oktober 2023
Disetujui:
28 Maret 2024

Kata Kunci:

L2TPv3, VPN, Tunnel

Abstract

Information security and privacy is a major concern. One popular way to keep data safe while accessing the internet is by using a Virtual Private Network (VPN). VPNs allow users to create a secure encrypted channel through a public network, thus securing their data from potential threats. In this research, the author analyzes a computer network between two locations (sites) with each location having a router connected to the internet and having a client under it. By using the Mikrotik router board device and the development method of L2TP, namely L2TPv3, the authors implemented on each router and conducted tests between clients. From the test results, it was found that data transmission was successfully carried out (connected). Based on several trials, the test results also show an average of 0.004751 ms using ICMP packets from source IP 192.168.30.10 to destination IP 192.200.10.50. L2TPv3 is a good protocol for securely connecting networks using public networks.

INTRODUCTION

Dalam era digital yang semakin berkembang, Setiap generasi membutuhkan jaringan internet, seperti yang terlihat di kantor, sekolah, universitas, dan tempat lainnya (Maulana et al., 2022). Meskipun internet adalah salah satu layanan jaringan yang paling praktis dan cepat untuk berbagi informasi secara global, belum ada standar keamanan yang memastikan bahwa informasi tersebut aman, dan orang-orang yang tidak bertanggung jawab dapat dengan mudah mengaksesnya (Pamungkas et al., 2021). Keamanan dan privasi informasi menjadi perhatian utama. Salah satu cara yang populer untuk menjaga keamanan data saat mengakses internet adalah dengan menggunakan Virtual Private Network (VPN) (Sari et al., 2020).

Dalam penelitiannya, Sri Fatimah mendevinisikan metode dasar VPN untuk membuat jaringan private melalui internet adalah dengan membuat tunnel sehingga jaringan yang terpercaya dapat terhubung dengan jaringan di luar melalui internet (Watmah, 2020). VPN memungkinkan pengguna untuk membuat saluran terenkripsi yang aman melalui jaringan publik, sehingga mengamankan data mereka dari ancaman potensial (Purwanto & Fikriadi, 2020). Sejak 1993, VPN sudah

ada. Ini dimulai dengan swIPe yang ditemukan oleh John Ioannidis sebagai PPTP (Point to Point Tunnelling Protocol), kemudian IPsec, dan kemudian berkembang lagi sampai OpenVPN tersedia (Alviendra et al., 2022).

Salah satu protokol VPN yang masih relevan hingga saat ini adalah Layer 2 Tunneling Protocol (L2TP) (Syahputra et al., 2023). Protokol L2TP memliki fungsimembuat transfer data lebih aman digunakan oleh user karena saat mengirim data, data dienkripsi, sehingga orang yang ingin menjebol jaringan tidak bisa mengaksesnya (Nugraha & Ranius, 2022). Namun saat ini, L2TP mengalami perkembangan menjadi L2TPv3. L2TPv3 adalah pengembangan dari protokol L2TP yang awalnya diciptakan oleh Microsoft dan Cisco. Protokol ini memungkinkan pengguna untuk membuat koneksi jaringan yang aman melalui jaringan IP (Internet Protocol) dengan menggunakan enkripsi dan tuneling data (Sumarna & Maulana, 2021).

L2TPv3 secara khusus dirancang untuk mengatasi beberapa keterbatasan yang ada dalam versi sebelumnya. Protokol ini memungkinkan pengguna untuk mengirimkan lalu lintas data jaringan Layer 2 (seperti Ethernet) melalui jaringan IP, yang membuatnya sangat berguna dalam pengaturan jaringan yang kompleks dan heterogen. L2TPv3 berfungsi untuk memungkinkan lalu lintas data dikirim melalui jaringan Layer 2 (seperti Ethernet, Frame Relay, dan ATM) melalui jaringan IP (Internet Protocol). Teknik ini membentuk saluran terenkripsi yang aman di atas jaringan publik seperti internet, yang memungkinkan komunikasi yang aman dan pribadi antara lokasi atau jaringan yang terpisah geografis.

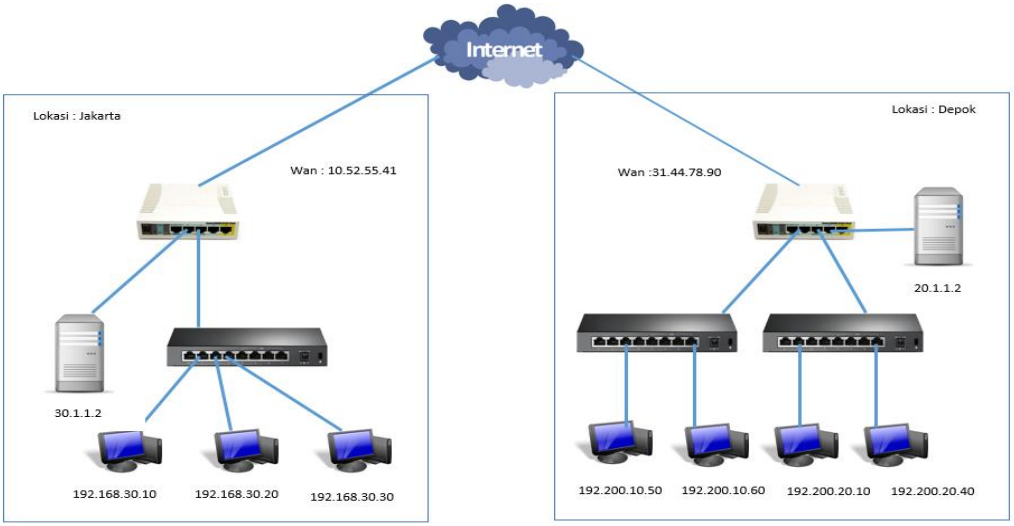
Selain itu, L2TPv3 mendukung enkripsi data yang dikirimkan melalui saluran VPN. Ini berarti bahwa data yang melewati saluran L2TPv3 terlindungi dengan aman dari ancaman potensial atau pihak-pihak yang tidak berwenang. Enkripsi ini menjaga kerahasiaan dan integritas data yang dikirimkan, sehingga menjadikan L2TPv3 sebagai pilihan yang kuat untuk mengamankan komunikasi secara online.

Berdasarkan penelitian yang telah dilakukan oleh Adji Putra Pamungkas pada Diskominfo Kabupaten Muko-muko didapatkan hasil bahwa pengujian yang dilakukan dengan kedua protokol L2TP dan PPTP menunjukkan bahwa L2TP dengan IPSec memberikan keamanan berlapis untuk menjamin keamanan data yang dikirimkan. Nilai penundaan, bandwidth, dan kehilangan paket pada protokol PPTP dan L2TP-VPN tidak terlalu berbeda dan terlihat sama. Keduanya beroperasi melalui cloud Internet, hanya format header L2TP lebih besar daripada format PPTP sundulan. Menurut parameter latency, PPTP memiliki waktu tunggu yang lebih pendek daripada L2TP. PPTP unggul atas L2TP dalam pengujian throughput. Ketika paket hilang, baik PPTP maupun tidak. Menurut pengujian kualitas layanan (QoS), VPN L2TP bekerja lebih baik daripada PPTP(Pamungkas et al., 2021).

Dalam penelitian ini, kami akan menjelaskan lebih dalam tentang protokol VPN L2TPv3, bagaimana cara kerjanya, manfaatnya dalam mengamankan komunikasi online, serta tantangan dan pertimbangan yang perlu diperhatikan ketika mengimplementasikan L2TPv3 dalam lingkungan jaringan. Kami juga akan membahas contoh penggunaan nyata dari L2TPv3 dan bagaimana protokol ini dapat membantu organisasi atau individu dalam menjaga keamanan dan privasi data mereka dalam dunia digital yang terus berkembang.

METODE

Metode penelitian ini menggunakan eksperimental. Metode penelitian ini bertujuan untuk mengukur dan mengevaluasi kinerja jaringan dengan menggunakan perangkat MikroTik sebagai pusat penelitian (Firmansyah et al., 2023).



Gambar 1. Skema Jaringan Berjalan

Dengan menggunakan perangkat routerboard mikrotik untuk menginvestigasi kinerja jaringan komputer dalam skenario VPN Dengan Menggunakan L2TPv3. Cara ini memungkinkan peneliti untuk membuat model jaringan yang realistis dan mengamati bagaimana jaringan tersebut merespons situasi tertentu, sehingga dapat memberikan wawasan tentang faktor-faktor yang memengaruhi kinerja jaringan .

Gambar 1. menggambarkan skema jaringan yang terjadi saat penulis membuat rancangan. Terdapat dua buah router yang berbeda lokasi yaitu Jakarta dan Depok yang masing masing terhubung ke internet. Dalam konsep jaringan diatas maka penulis mendapatkan permasalahan antara lain : (1) Masing masing client pada segment network tidak dapat terhubung satu sama lain. Hal ini dikarenakan tidak mungkin terjadi proses routing terhadap penyedia layanan internet (provider). (2) Lapisan keamanan data saat data dikirimkan via internet dari source ke destination tidak memiliki keamanan data yang baik. Data yang dikirimkan melalui jaringan dapat rentan terhadap pencurian oleh pihak yang tidak berwenang. Informasi pribadi, seperti kata sandi, nomor kartu kredit, dan data sensitif lainnya, dapat dicuri oleh peretas atau pengguna jaringan yang tidak sah. sebagai langkah yang tepat untuk menemukan solusi untuk masalah di atas, penulis memulai dengan melakukan pengumpulan data dengan tahapan sebagai berikut:

1. Observasi

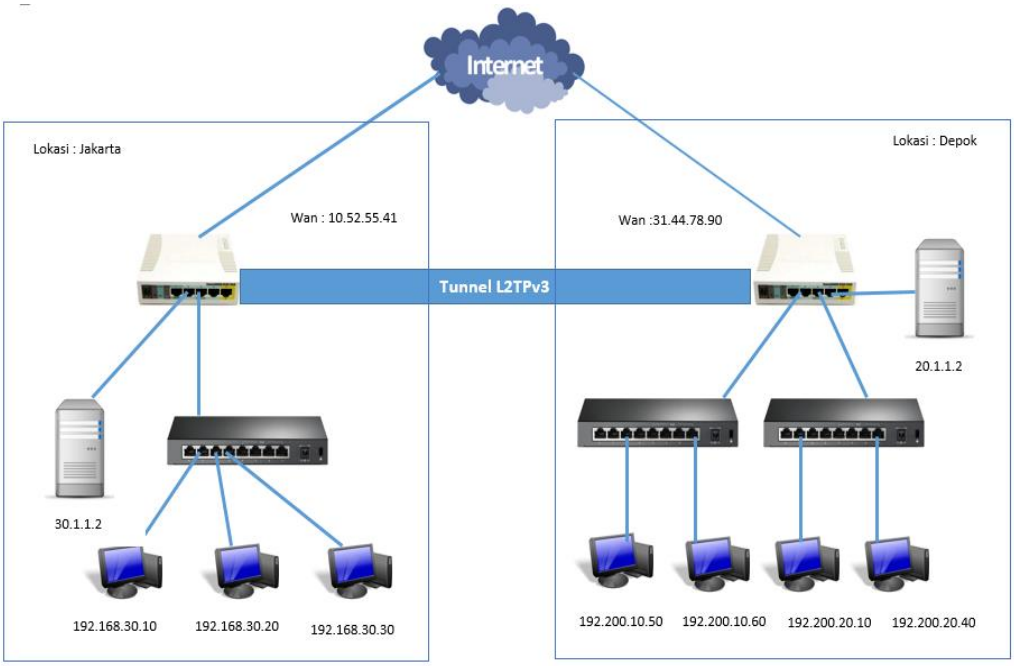
Tahapan ini penulis mulai dengan mengumpulkan data secara pengamatan langsung. Mencatat semua kebutuhan yang diperlukan untuk pembuatan jaringan seperti routerboard mikrotik, PC, Switch hingga media transmisi kabel

2. Eksperiment

Tahapan selanutnya, penulis mulai dengan mengumpulkan data secara eksperimen dasar. Jaringan yang dibuat dengan menggunakan perangkat routerboard mikrotik rb951ui dilakukan beberapa kali pengujian koneksi antar client dalam segmen jaringan yang berbeda dan mencatat hasil pengujian.

3. Studi Pustaka

Mengumpulkan data dengan membaca dan meneliti pengetahuan teoritis yang diperoleh dari buku, artikel, dan media online. Buku, artikel, dan media online ini membahas atau memuat materi yang berkaitan dengan masalah yang dibahas, memberikan informasi tambahan kepada penulis, dan memberikan analisis komparatif.



Gambar 2. Skema Jaringan Usulan

HASIL DAN PEMBAHASAN

Topologi Jaringan

Dari hasil analisa topologi jaringan yang ada dan permasalahan yang penulis dapatkan serta data yang berhasil dikumpulkan, maka penulis membuat sebuah topologi jaringan sebagaimana yang terlihat pada Gambar 2. Rancangan topologi jaringan dibuat dengan menggunakan VPN L2TPv3. L2TPv3 ini yang nanti akan menghubungkan jaringan yang berbeda segmen dan dilokasi yang berbeda dapat saling tehubung satu sama lain. Rancangan jaringan yang diusulkan ini dirancang untuk memenuhi kebutuhan dan menyelesaikan masalah yang ada. Ini juga merupakan alternatif yang dapat digunakan untuk mengurangi masalah jaringan perusahaan yang sering terjadi.

Spesifikasi Ip Address

Penjabaran IP Adrees berdasarkan usulan topologi jaringan (Gambar 2) dapat dilihat pada Tabel 1. Penjabaran ini sangat perlu dilakukan dalam penelitian karena termasuk dari salah satu metode pengumpulan data dalam bentuk observasi. Pencatatanan ip address ini juga penting karena menjelaskan sumber (*source*) jaringan dan tujuan (*destination*) paket data dalam jaringan dikirim.

Pada usulan jaringan masing masing router memiliki ip address yang didapatkan dari ISP yang berbeda. Keduanya sudah saling terhubung ke internet. Kemudian masing masing router tersebut memiliki alamat jaringan private yang digunakan oleh user untuk bekerja.

Tabel 1. Spesifikasi IP Address Router

Ip Address	Router Site A (Jakarta)	Router Site B (Depok)
Ip Public	10.52.55.41	31.44.78.90
Ip Local Client	192.168.30.1	192.200.10.1
Ip Local Server	30.1.1.1	20.1.1.1
Ip Tunnel	10.10.10.1/30	10.10.10.2/30

Tabel 2. Spesifikasi Ip Address Client

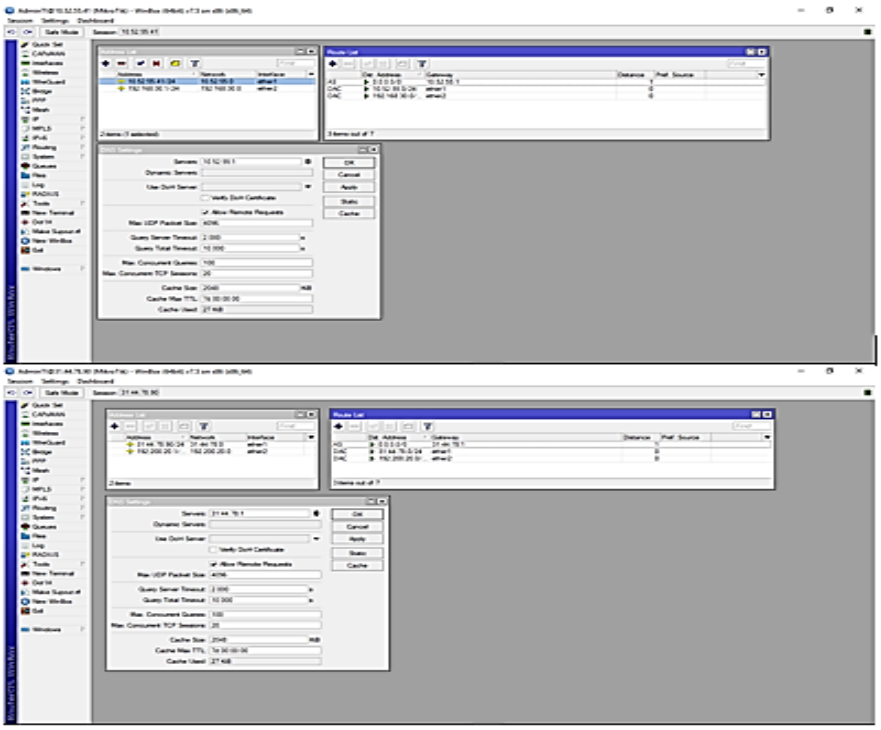
Ip Address	Site A (jakarta)	Site B (Depok)
network	192.168.30.0	192.200.10.0
Gateway	192.168.30.1	192.200.10.1
DNS	192.168.30.1	192.200.10.1
Start Ip	192.168.30.10	192.200.10.50
End IP	192.168.30.20	192.200.10.80
subnetmask	255.255.255.0	255.255.255.0
Server	30.1.1.2	20.1.1.2

Karena ip lokal tidak bisa terhubung satu sama lain pada router tersebut. Maka penulis menyiapkan ip tunnel yang nanti akan penulis terapkan dalam L2TPv3.

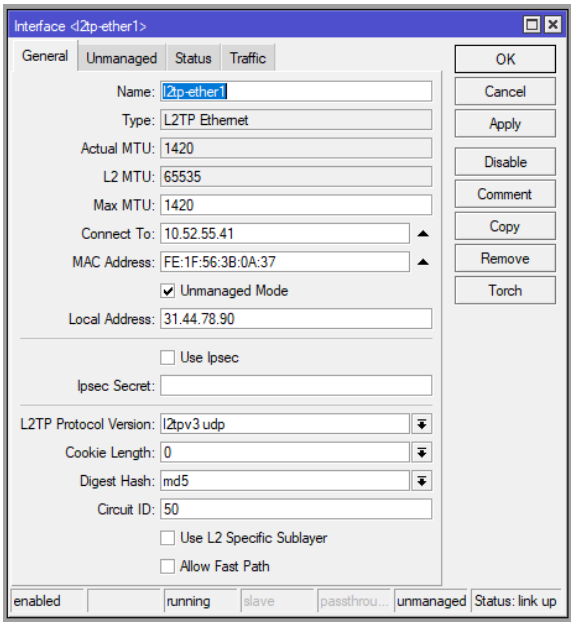
Sedangkan tabel dibawah ini adalah penjabaran ip address yang digunakan oleh masing masing user di jaringan lokal. Tujuannya adalah setelah L2TPv3 terbentuk maka masing masing user pada Site A dan B dapat saling berkomunikasi.

Penerapan L2TPv3

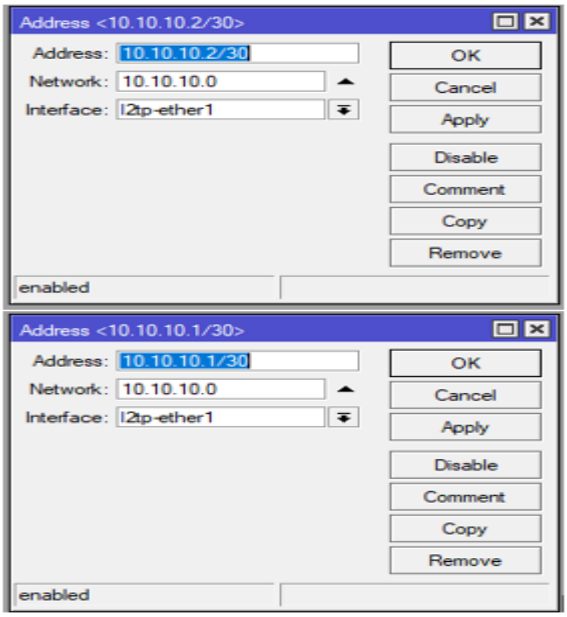
Sebelum melakukan menerapkan L2TPv3, konfigurasi dasar seperti ip address yang telah dijabarkan pada Tabel 1. harus dimasukan kedalam router. Selain itu, agar router dapat terbuhung dengan internet maka harus ditambahkan pengaturan DNS dan Gateway. Konfigurasi L2TPv3 dilakukan di menu PPP pada tab L2TP Ethernet. Tambahkan sebuah rule baru dengan mesukan ip public yang dituju pada kolom Connect To. Ceklist juga pada bagian Unmanage Mode. Selanjutnya masukan IP Public router tersebut pada kolom Local Address. (Gambar 2)



Gambar 3. Konfigurasi Ip, DNS dan Gateway

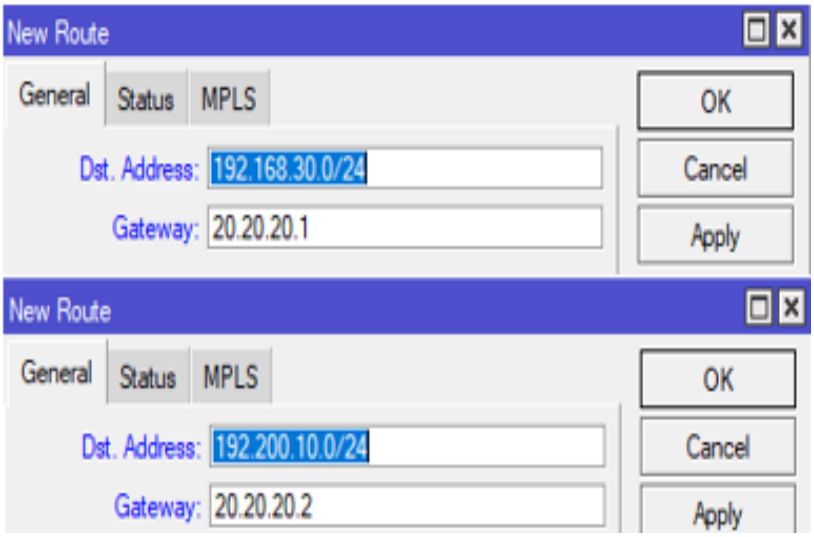


Gambar 4. Konfigurasi L2TPv3



Gambar 5. Ip Address L2TPv3

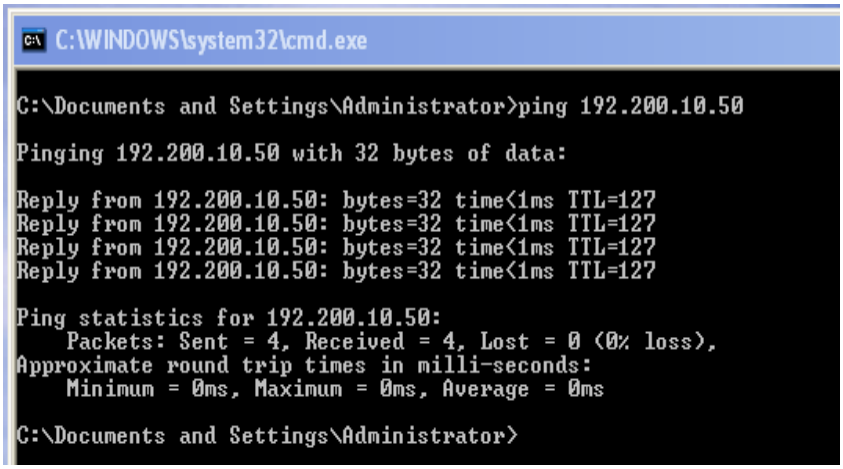
Konfigurasi pada Gambar 4. dapat dilakukan pada masing masing Site Router. Setelah jalur L2TP terbentuk, maka dibutuhkan alamat protocol. Penulis perikan Ip Address 10.10.10.1 untuk interface l2tp-ether1 di Site A dan 10.10.10.2 Untuk untuk interface l2tp-ether1 di Site B. IP Address dibuat untuk masing masing interface L2tpv3 (Gambar 5). Ip Address inlah yang akan menghubungkan antar router seolah olah kedua router tersebut terhubung secara Point To Point. Selanjutnya adalah proses mengatur bagaimana perangkat MikroTik yang akan mengarahkan lalu lintas data antara berbagai jaringan atau subnet. Konfigurasi yang digunakan adalah routing statik yang dilakukan secara manual menentukan rute-rute yang spesifik untuk lalu lintas (Gambar 6). Langkah ini hanya memasukan alamat tujuan yaitu 192.168.30.0/24 dengan gateway 20.20.20.1 dan 192.200.10.0/24 dengan gateway 20.20.20.2.



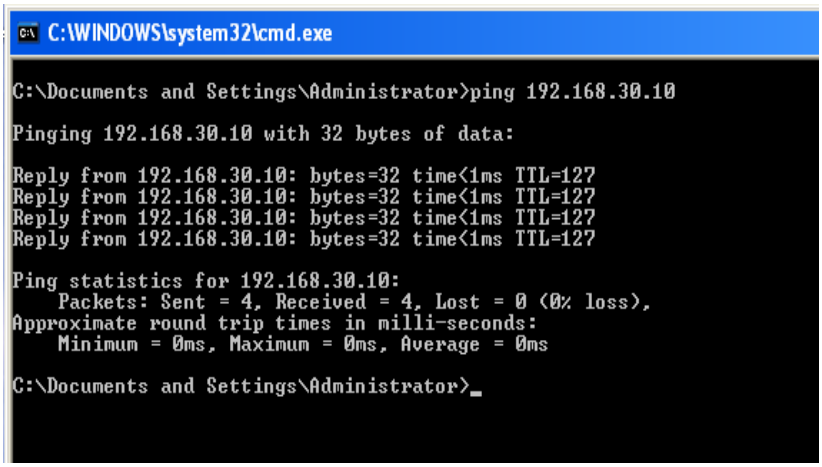
Gambar 6. Routing Statis Dengan L2TPv3

Pengujian jaringan

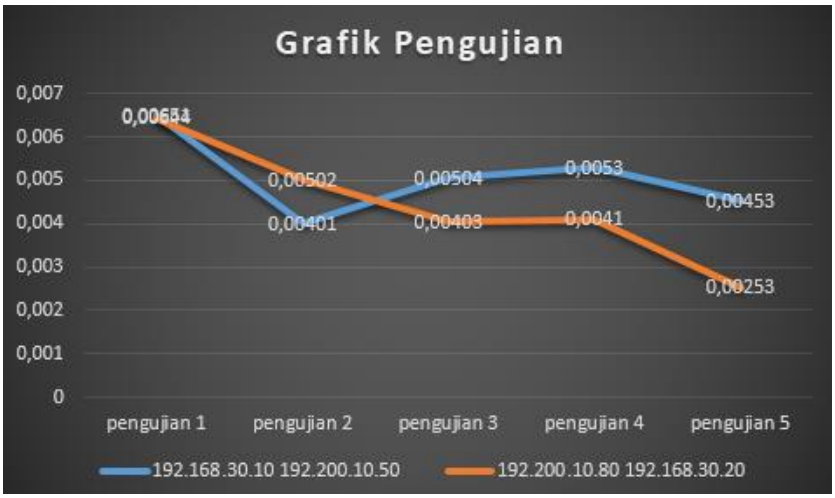
L2TPv3 secara khusus dirancang untuk mengatasi beberapa keterbatasan yang ada dalam versi sebelumnya. Dalam pengujian ini di buat sebuah prototype jaringan yang kompleks dan heterogen dengan menggunakan 2 buah router dengan masing masing router terhubung kejaringan internet. Masing masing router mengatur lalu litas jaringan lokal. Proses pengiriman data dari lapisan dua Ethernet ke lapisan tiga IP address melibatkan beberapa langkah dalam proses pengiriman data pada jaringan komputer. Alamat IP tujuan diperoleh dari hasil tabel routing di dalam perangkat jaringan atau dari proses resolusi nama seperti DNS. Data yang akan dikirim harus dibungkus dengan header dan trailer yang sesuai dengan protokol lapisan dua (biasanya protokol Ethernet) dan lapisan tiga (biasanya protokol IP) . Setelah data dibungkus dengan header IP, sistem harus menentukan alamat MAC (Media Access Control) dari perangkat jaringan tujuan. Pengujian akhir ini mencoba tes ping (ICMP) antar client di berbagai segment jaringan untuk memastikan bahwa jaringan telah stabil dan dapat digunakan dengan baik. Komputer yang berada di segment jaringan jakarta mencoba berkomunikasi dengan komputer yang berada di segmen jaringan depok. (Gambar 7)



Gambar 7. Hasil Pengujian Jaringan

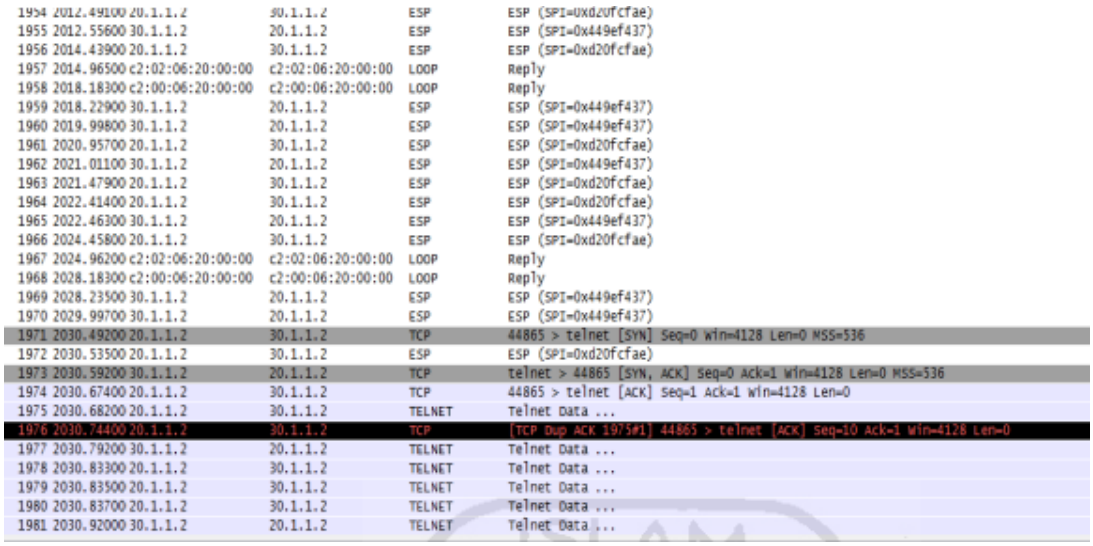


Gambar 8. Hasil Pengujian Jaringan



Gambar 9. Grafik Hasil Pengujian Jaringan

Gambar 7 adalah hasil pengujian antar client yang berada di site A dengan source ip 192.168.30.10 ke destination 192.200.10.50. untuk hasil yang lebih baik dilakukan pengujian dengan cara sebaliknya dan didapatkan hasil yang sama yaitu koneksi terhubung dengan baik dengan menggunakan L2TPv3. (Gambar 8). Berdasarkan pengujian yang penulis lakukkan maka penulis merangkum dan menganalisis percobaan antar client dan didapatkan hasil grafik pengujian seperti pada Gambar 9. Selain itu juga dilakukan pengujian melalui aplikasi *wireshark*, diamana hasil dari pengecekan ping memperlihtakan data (Gambar 10) yang dikirim saat ini tidak lagi terlihat menggunkanan protokol L2TPv3 dikarenakan adanya enskripsi keamanan saat melewati internet. Ini menandakan bahwa data yang melewati saluran L2TPv3 terlindungi dengan aman dari ancaman potensial atau pihak-pihak yang tidak berwenang. Enkripsi ini menjaga kerahasiaan dan integritas data yang dikirimkan, sehingga menjadikan L2TPv3 sebagai pilihan yang kuat untuk mengamankan komunikasi secara online.



Gambar 10. Grafik Hasil Pengujian Jaringan

Tabel 3 Spesifikasi Ip Address Client

Source	Destination	Test	Result
192.168.30.10	192.168.30.1	ICMP	Success
	10.52.55.41	ICMP	Success
	20.20.20.1	ICMP	Success
	20.20.20.2	ICMP	Success
	192.200.10.1	ICMP	Success
	192.200.10.50	ICMP	Success
	192.200.10.80	ICMP	Success
192.200.10.50	192.200.10.1	ICMP	Success
	20.20.20.2	ICMP	Success
	20.20.20.1	ICMP	Success
	192.168.30.1	ICMP	Success
	192.168.30.10	ICMP	Success
	192.168.30.120	ICMP	Success
30.1.1.1	20.1.1.1	ICMP	Success

Tabel 3. memperlihatkanhasil pengujian mengguakan L2TPv3 kejaringan lokal antar tempat menggunakan media internet.

KESIMPULAN DAN SARAN

Berdasarkan pengumpulan data dan analisis penulis lakukan, serta teori yang ada yang penulis dapat dari berbagai sumber penelitian, dapat disimpulkan bahwa konfigurasi L2TPv3 adalah pengembangan dari teknik L2TP pada router mikrotik. Konfigurasi ini dimaksudkan untuk menghubungkan dua lokasi yaitu jakarta dan Depok yang memiliki segmen jaringan yang berbeda. Penerapat L2TPv3 dan routing berdasarkan pengujian yang penulis lakukan sangatlah baik. Hasil pengujian jaringan menunjukkan rata-rata 0,004751 ms pengiriman paket ICMP dari sumber IP 192.168.30.10 ke destination IP 192.200.10.50. L2TPv3 protokol yang baik untuk menghubungkan jaringan dengan aman menggunakan jaringan publik. Selain itu penggunaan L2TPv3 menjadikan data yang dikirim memiliki keamanan karena

adanya enskripsi data . Enkripsi ini menjaga kerahasiaan dan integritas data yang dikirimkan, sehingga menjadikan L2TPv3 sebagai pilihan yang kuat untuk mengamankan komunikasi secara online dari ancaman potensial atau pihak-pihak yang tidak berwenang.

DAFTAR PUSTAKA

Alviendra, I. M., Setijadi, E., & Kusrahardjo, G. (2022). Pengembangan dan Penerapan Sistem Virtual Private Network (VPN) pada Internet Of Things (IOT) Menggunakan Simulasi. *Jurnal Teknik ITS*, *11*(1). https://doi.org/10.12962/j23373539.v11i1.81278

Firmansyah, F., Alfian Armawan Sandi, T., Fauzi, A., & Septian Anwar, R. (2023). Analisis Performa Redundancy Link Menggunakan Metode Spanning Tree Protocol Dan Per VLAN Spanning Tree. *Jurnal Infortech*, *5*(1), 47–52. https://doi.org/10.31294/infortech.v5i1.15629

Maulana, A., Novarian, F., & Fauzi, A. (2022). Penerapan Manajemen Network Router on Stick (ROS) Pada PT. Bank Rakyat Indonesia. *Jurnal Teknik Komputer AMIK BSI*, *8*(2), 174–180. https://doi.org/10.31294/jtk.v4i2

Nugraha, M. D., & Ranius, A. Y. (2022). Perbandingan Metode Pptp Dengan L2Tp Pada Jaringan Vpn Pt. Pertamina Bagian Pemasaran Plaju Palembang. *Prosiding Seminar Hasil …*, 82–90. https://conference.binadarma.ac.id/index.php/semhavok/article/view/3190%0Ahttps://conference.binadarma.ac.id/index.php/semhavok/article/download/3190/1432

Pamungkas, A. P., Muhammad Reza Putra, & M. Hafizh. (2021). Analisis Jaringan VPN Menggunakan PPTP dan L2TP Berbasis Mikrotik pada Diskominfo Kabupaten Muko-muko. *Jurnal KomtekInfo*, *8*, 189–194. https://doi.org/10.35134/komtekinfo.v8i3.143

Purwanto, T. D., & Fikriadi. (2020). Implementasi ftp server dengan memanfaatkan vpn mikrotik sebagai keamanan jaringan di bnnp sumsel 1. *Semhavok Universitas Bina Darma*, *1*, 48–53.

Sari, A. P., Sulistiyono, & Kemala, N. (2020). Perancangan Jaringan Virtual Private Network IP Security Router Mikrotik. *Jurnal PROSISKO*, *7*(2), 150–164.

Sumarna, S., & Maulana, A. (2021). Implementasi Virtual Private Network Menggunakan L2TP/IPsec pada BBPK Jakarta. *EXPERT: Jurnal Manajemen Sistem Informasi Dan Teknologi*, *11*(2), 90. https://doi.org/10.36448/expert.v11i2.1829

Syahputra, A., Indriyani, F., Alfian, T., & Sandi, A. (2023). *Perancangan Sistem Keamanan VoIP Server Randomize number PT Mulia Persada Indonesia Menggunakan VPN L2TP*. *3*(1), 1–10.

Watmah, S. (2020). Implementasi VPN Menggunakan Point-To-Point Tunneling Protocol (PPTP) Mikrotik Router Pada BPRS Bumi Artha Sampang. *INSANTEK - Jurnal Inovasi Dan Sains Teknik Elektro*, *1*(1), 6–12. https://ejournal.bsi.ac.id/ejurnal/index.php/insantek/article/view/8145