Institut Riset dan Publikasi Indonesia (IRPI)
MALCOM: Indonesian Journal of Machine Learning and Computer Science
Journal Homepage: https://journal.irpi.or.id/index.php/malcom
Vol. 4 Iss. 4 October 2024, pp: 1496-1504
ISSN(P): 2797-2313 | ISSN(E): 2775-8575

Virtual Private Network Implementation Using Mikrotik Based Layer 2 Tunneling Protocol

Implementasi Virtual Private Network MenggunakanLayer 2 Tunneling Protocol Berbasis Mikrotik

Linna Oktaviana Sari[1], Helena[2*]

[1,2]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Riau, Indonesia

E-Mail: [1]linnaosari@lecturer.unri.ac.id, [2]helena5109@student.unri.ac.id

Received Aug 7th 2024; Revised Sept 17th 2024; Accepted Sept 20th 2024
Corresponding Author: Helena

Abstract

The rapid development of technology has made the need for an internet network increasing, including in the education sector. SDS IT Friends of Muslim Duri uses the internet network as a medium for learning and storing important data online. However, network management by admins can only be done within the school's local network. This research aims to implement a VPN network using Mikrotik-based L2TP protocol so that devices in schools can be configured and monitored remotely securely. The methods used include problem identification, literature study, data collection, L2TP VPN implementation, and testing. The results show that the implementation of L2TP VPN successfully allows admins to access and manage school networks from public networks securely. Testing using ping, traceroute, and device remote shows good connectivity. This implementation improves the efficiency of network management and school data security.

Keyword: L2TP, Mikrotik, SDS IT Sahabat Muslim, VPN

Abstrak

Perkembangan teknologi yang semakin pesat membuat kebutuhan akan jaringan internet semakin meningkat, termasuk di sektor pendidikan. SDS IT Sahabat Muslim Duri menggunakan jaringan internet sebagai media pembelajaran dan penyimpanan data penting secara online. Namun, pengelolaan jaringan oleh admin hanya dapat dilakukan dalam jaringan lokal sekolah. Penelitian ini bertujuan untuk mengimplementasikan jaringan VPN menggunakan protokol L2TP berbasis Mikrotik agar perangkat di sekolah dapat dikonfigurasi dan dimonitor dari jarak jauh secara aman. Metode yang digunakan meliputi identifikasi masalah, studi literatur, pengumpulan data, implementasi VPN L2TP, dan pengujian. Hasil penelitian menunjukkan bahwa implementasi VPN L2TP berhasil memungkinkan admin untuk mengakses dan mengelola jaringan sekolah dari jaringan publik secara aman. Pengujian menggunakan ping, *traceroute*, dan *remote* perangkat menunjukkan konektivitas yang baik. Implementasi ini meningkatkan efisiensi pengelolaan jaringan dan keamanan data sekolah.

Kata Kunci: L2TP, Mikrotik, SDS IT Sahabat Muslim, VPN

1. PENDAHULUAN

Perkembangan teknologi saat ini berkembang semakin cepat membuat tingkat kebutuhannya semakin meningkat, khususnya pada jaringan internet. Jaringan internet merupakan faktor penting bagi perusahaan maupun instansi yang menggunakan teknologi komputerisasi untuk operasionalnya, serta penggunaan komputer 1 dengan komputer lainnya yang saling terhubung di dalam sebuah jaringan, baik secara intranet (lokal) maupun internet. Jaringan juga sangat diperlukan didalam dunia pendidikan, karena jaringan internet memberikan kemudahan untuk mengakses berbagai informasi mengenai pendidikan secara langsung [1].

Pada Sekolah Dasar Swasta (SDS) IT Sahabat Muslim Duri memiliki jumlah murid 70 dan jumlah guru 7. Jaringan yang ada disekolah tersebut dikelola oleh admin yang berjumlah 1 orang. Admin bertugas untuk mengelola jaringan, memastikan jaringan berfungsi dengan baik, serta menjaga dan meningkatkan kualitas jaringan. SDS IT Sahabat Muslim memiliki beberapa perangkat jaringan dan layanan akses jaringan agar dapat menghubungkan penguna yang ada disekolah, adapun perangkat jaringannya yaitu terdiri dari *Router*, *Acces Point*, *Switch* serta *Closed Circuit Television* (CCTV) disetiap sudutnya. Perangkat tersebut terhubung dengan modem Telkom sebagai sumber jaringan utama, dari modem tersambung ke *router* dan didistribusikan melalui

switch sebagai penyebar jaringan yang dihubungkan ke *access point*, CCTV, serta terhubung ke komputer admin.

Virtual Private Network (VPN) merupakan inovasi dalam teknologi jaringan yang memungkinkan koneksi aman antar jaringan melalui infrastruktur internet public [2]. Teknologi ini menciptakan terowongan terenkripsi, menjamin privasi dan keamanan data saat berkomunikasi melintasi jaringan yang berbeda, memungkinkan pengguna untuk terhubung secara aman dari jarak jauh seolah-olah berada dalam jaringan lokal yang sama [3]. Menurut [1] VPN adalah teknologi yang memungkinkan koneksi aman antar jaringan lokal melalui internet. Sistem ini mengenkapsulasi data dalam terowongan virtual, memastikan kerahasiaan informasi saat ditransmisikan melalui jaringan publik. Metode ini menjamin keamanan dan integritas data, melindunginya dari akses tidak sah selama perjalanan melalui infrastruktur komunikasi umum. VPN memungkinkan pengguna untuk mengakses sumber daya jaringan dari jarak jauh seolah-olah mereka terhubung langsung ke jaringan lokal. Selain itu, teknologi ini juga dapat digunakan untuk melewati pembatasan geografis dan sensor internet, memberikan kebebasan dan privasi yang lebih besar dalam mengakses konten online [4].

L2TP adalah protokol tunneling yang menggabungkan teknologi dari Cisco dan Microsoft (PPTP). Protokol ini dirancang untuk mendukung operasi VPN, memanfaatkan kelebihan dari kedua sistem tersebut untuk menciptakan koneksi yang aman dan efisien [5]. Penerapan jaringan VPN L2TP dan *port forwarding* dengan mikrotik agar dapat dilakukan *remote* secara jarak jauh atau secara publik.

Penelitian yang dilakukan oleh [6] menghasilkan implementasi jaringan VPN dengan protokol *Layer 2 Tunneling Protocol* (L2TP) di Balai Besar Pelatihan Kesehatan (BBPK) Jakarta memungkinkan terjalinnya konektivitas antara dua lokasi penting, yaitu kantor pusat BBPK Jakarta yang berlokasi di Cilandak dan kantor cabangnya di Hang Jebat. Melalui pemanfaatan teknologi VPN dengan metode L2TP ini, para pegawai yang bekerja baik di gedung pusat maupun di cabang dapat menjalin komunikasi secara efektif dan terjamin keamanannya. Sistem ini menjembatani kedua lokasi kerja tersebut, menciptakan lingkungan komunikasi yang lancar dan terlindungi bagi seluruh staf BBPK Jakarta. Sementara itu penelitian dari [5] implementasi rancangan jaringan interkoneksi VPN yang mengintegrasikan protokol L2TP/ IPSec dengan routing OSPF telah menunjukkan hasil yang memuaskan. Sistem ini, yang terhubung ke internet, beroperasi secara efisien sesuai dengan desain yang direncanakan. Lebih lanjut, serangkaian pengujian yang dilakukan untuk mengevaluasi kinerja sistem menghasilkan data yang menggembirakan. Performa jaringan yang diukur melalui berbagai parameter uji menunjukkan tingkat kehandalan dan efektivitas yang tinggi, memvalidasi keberhasilan rancangan dan implementasi jaringan tersebut. Selain itu, penelitian yang dilakukan oleh [7] Penerapan VPN dengan protokol PPTP menghasilkan perlindungan data yang efektif, mencegah akses tidak sah. PPTP meningkatkan keamanan jaringan melalui enkapsulasi jalur komunikasi, membentuk terowongan data yang terlindungi.

Maka penelitian ini berfokus untuk melakukan penghubungan jaringan atau disebut juga interkoneksi jaringan dengan cara mengimplementasikan VPN untuk menghubungkan sekolah dengan admin secara jarak jauh, mengingat banyak nya data yang bersifat sensitif pada sekolah yang hanya boleh diketahui atau digunakan oleh orang yang berkepentingan dalam jaringan lokal. Oleh karena itu VPN sangat dibutuhkan di SDS IT Sahabat Muslim. Pada penelitian ini menerapkan protokol L2TP yang memiliki kelebihan memberikan perlindungan ganda, enkapsulasi dan verifikasi dua kali, dikonfigurasinya tidak terlalu konfleks, serta mendukung disemua perangkat operasi *Windows, Mac, Android*, IOS, maupun *Linux*. Berdasarkan permasalahan yang terjadi, maka pada penelitian ini mengimplementasikan jaringan VPN menggunakan protokol L2TP berbasis mikrotik pada SDS IT Sahabat Muslim Duri.

2. METODOLOGI PENELITIAN

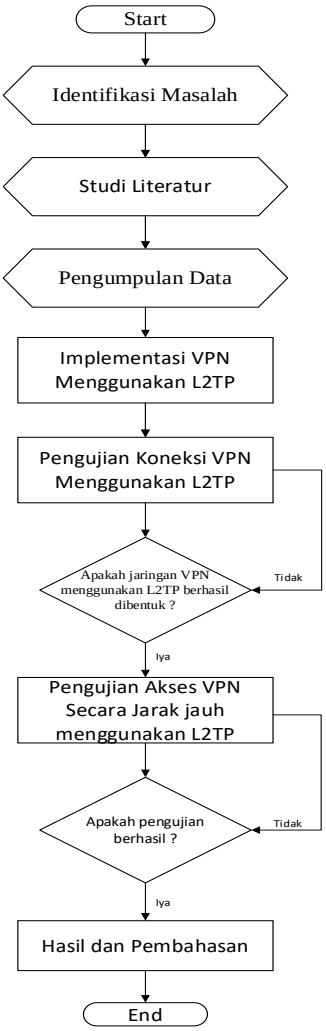
Penelitian ini menggunakan metode implemetasi dengan pendekatan kualitatif. Tahapan metodologi penelitian dimulai dengan identifikasi masalah melalui observasi dan wawancara untuk mengidentifikasi permasalahan jaringan yang ada di SDS IT Sahabat Muslim Duri, serta merumuskan masalah terkait keterbatasan admin dalam memonitoring jaringan secara jarak jauh. Adapun tahapan penelitian ini dapat dilihat pada Gambar 1.

2.1. Identifikasi Masalah

Identifikasi masalah yang terjadi ketika admin sedang berada pada jaringan publik atau tidak berada dalam ruang lingkup sekolah, maka tidak dapat mengakses *router* ataupun perangkat *Access Point* secara langsung, karena tidak adanya akses untuk masuk kejaringan lokal dikarenakan admin berada jauh dari sekolah.

2.2. Studi Literatur

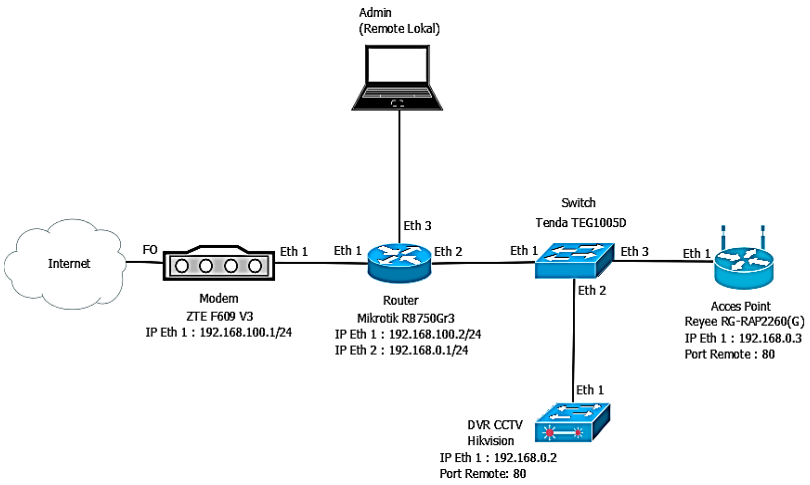
Studi loiteratur melakukan serangkaian kegiatan yang berkaitan dengan metode pengumpulan data dengan mencari referensi dari berbagai sumber seperti buku, jurnal, karya tulis, penelitian terdahulu yang berkaitan dengan VPN.



Gambar 1. Tahapan Penelitian

2.3. Pengimpulan Data

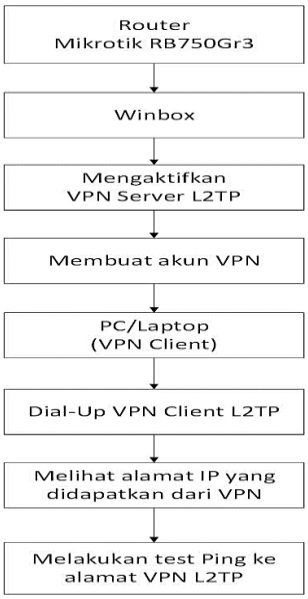
Pengumpulan data dilakukan untuk mengumpulkan berbagai data yang akan digunakan untuk mengamati permasalahan yang terjadi serta mengetahui kondisi jaringan yang ada pada SDS IT Sahabat Muslim . Pada pengumpulan data ini dilakukan observasi serta wawancara terhadap admin sekolah dilakukan guna mendapat informasi tentang perangkat jaringan yang ada dan kebutuhan informasi untuk pembuatan VPN menggunakan L2TP di SDS IT Sahabat Muslim Duri. Tahapan ini juga untuk menganalisis dan mengetahui bagaimana topologi jaringan yang ada pada SDS IT Sahabat Muslim [8]. Detail topologi ditunjukan pada Gambar 2.



Gambar 2. Topologi SDS IT Sahabat Muslim

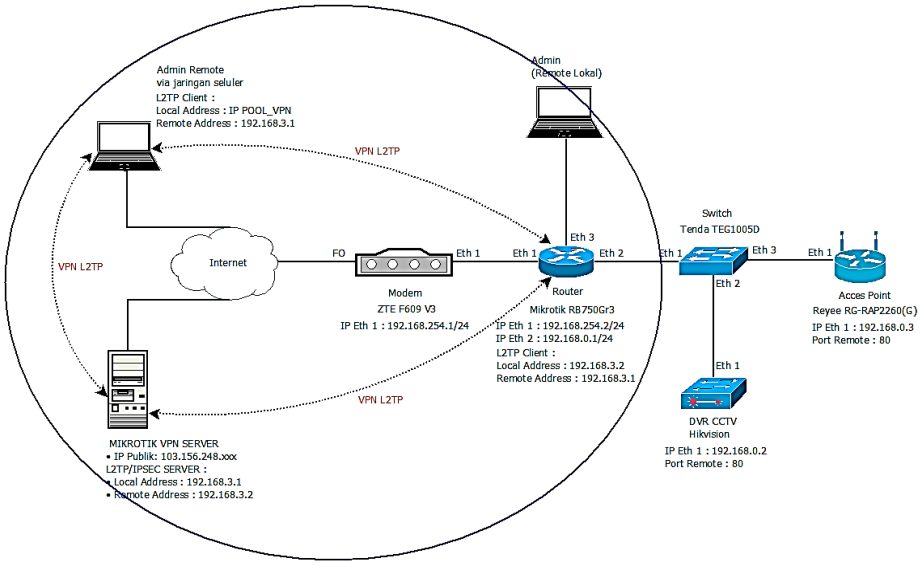
2.4. Implementasi VPN Menggunakan L2TP

Tahapan ini dilakukan pembuatan topologi sistem dengan menggunakan beberapa tahapan proses dalam perancangan jaringan VPN [9]. Adapun tahapan rancangan jaringan VPN dengan menggunakan L2TP dapat dilihat pada Gambar 3.



Gambar 3. Tahapan Rancangan Jaringan VPN

Setelah melakukan tahapan rancangan jaringan VPN menggunakan L2TP, selanjutnya dilakukan pembuatan Topologi menggunakan protokol VPN L2TP. Topologi jaringan menggunakan VPN L2TP dapat dilihat pada Gambar 4.



Gambar 4. Topologi Jaringan Menggunakan VPN L2TP

2.5. Skenario Pengujian

Pada tahap pengujian dilakukan skenario pengujian untuk mengetahui konektivitas pada VPN menggunakan L2TP . Adapun macam-macam pengujian yang dilakukan adalah sebagai berikut.

1. Pengujian Jaringan Menggunakan Ping di Command Prompt (CMD)
   Pengujian Ping ini dilakukan secara jarak jauh menggunakan *command prompt* dengan memberikan perintah ping pada IP *Router*, IP CCTV dan IP *Access Point* yang ada di sekolah, jika hasil ping menunjukan hasil reply maka konfigurasi VPN L2TP pada sekolah berhasil [10].

2. Pengujian Jaringan Menggunakan *Traceroute* di *Command Prompt* (CMD)
   Pengujian *Traceroute* ini dilakukan secara jarak jauh menggunakan *command prompt* dengan memberikan perintah "tracert" pada IP *Router*, IP CCTV dan IP *Access Point* yang ada di sekolah, jika hasil *traceroute* hop pertama adalah IP Server VPN maka konfigurasi VPN L2TP pada sekolah berhasil.

3. Pengujian *Remote* Jaringan Menggunakan Browser
   Pengujian *Remote* Perangkat ini dilakukan secara jarak jauh melalui browser dengan IP *Router*, IP CCTV dan IP *Access Point* yang ada di sekolah, jika hasil *remote* pada browser terbuka maka konfigurasi VPN L2TP pada sekolah berhasil.

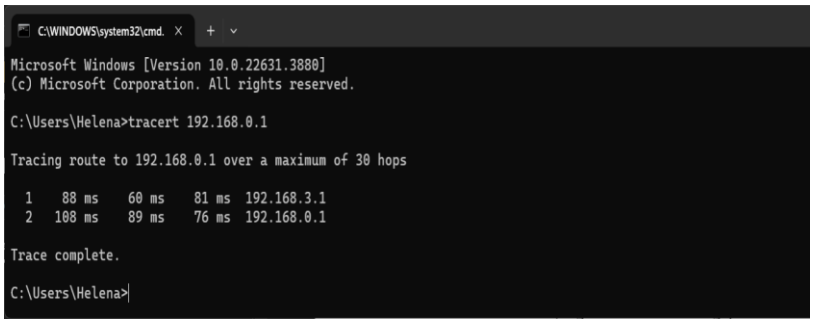
3. HASIL DAN PEMBAHASAN

3.1. Hasil Pengujian Jaringan Menggunakan L2TP

Tahapan ini, akan dijelaskan serangkaian pengujian yang akan dilakukan menggunakan VPN L2TP, pengujian tersebut dilakukan agar mengetahui apakah sistem yang telah dirancang dapat berfungsi dan dijalankan dengan baik. Pada pengujian jaringan dilakukan dengan beberapa tahap yaitu ping, *traceroute* dan *remote*.

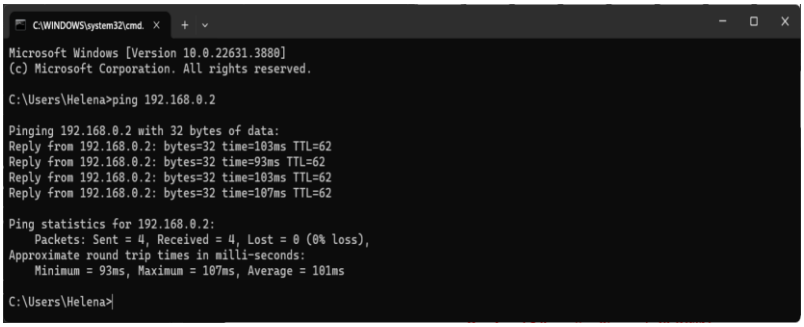
3.1.1. Pengujian jaringan menggunakan ping di *Command Prompt* (CMD)

Pengujian ping ini dilakukan secara jarak jauh menggunakan *command prompt* bertujuan untuk mengetahui konektivitas jaringan dengan memberikan perintah ping pada IP *Router*, IP CCTV dan IP *Access Point* yang ada di sekolah [10]. Pengujian Ping pada IP *Router* dapat dilihat pada gambar 5.



Gambar 5. Pengujuan jaringan menggunakan ping pada IP *Router*

Untuk *Router* (IP 192.168.0.1), pengujian ping pada jaringan publik memberikan respon berupa reply dengan status 0% Packet Loss. Ini membuktikan bahwa koneksi sudah terbentuk dan jaringan di sekolah berjalan normal., ditunjukkan pada gambar 6.

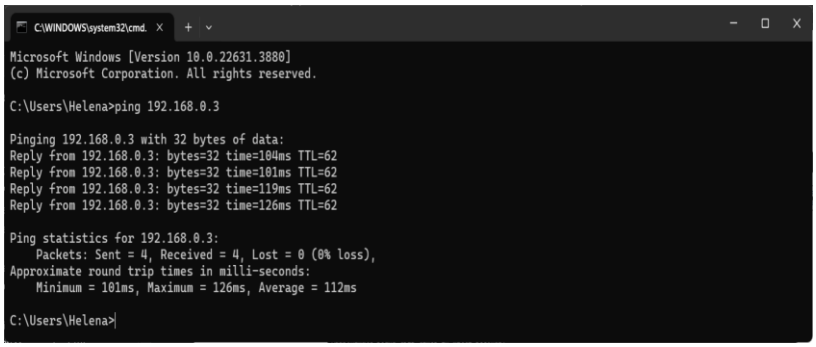


Gambar 6. Pengujuan jaringan menggunakan ping pada IP CCTV

Pada CCTV (IP 192.168.0.2), hasil pengujian ping juga menunjukkan respon berupa reply dengan status 0% Packet Loss. Hal ini memverifikasi bahwa koneksi ke CCTV sudah terbentuk dan jaringan berjalan normal. Pengujuan jaringan menggunakan ping pada IP *Access Point* ditunjukkan pada gambar 7.

Pengujian terhadap *Access Point* (IP 192.168.0.3) menghasilkan respon serupa, yaitu reply dengan status 0% Packet Loss. Ini mengkonfirmasi bahwa koneksi ke *Access Point* juga sudah terbentuk dan jaringan sekolah berjalan normal. Hasil ini menunjukkan bahwa implementasi VPN L2TP berhasil membuat koneksi yang stabil antara admin di jaringan publik dan perangkat jaringan sekolah. Tidak adanya packet loss pada semua perangkat yang diuji menandakan kualitas koneksi yang baik dan reliable.

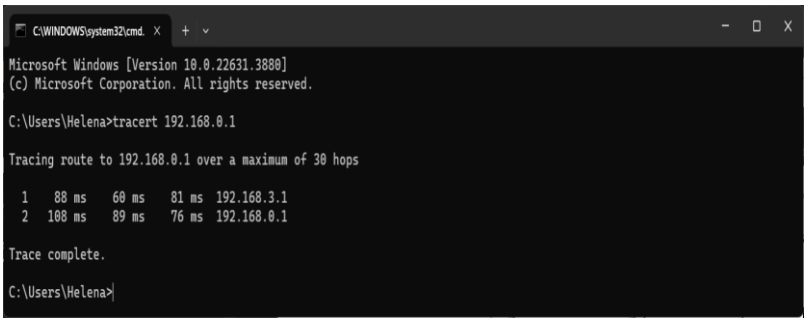
Konsistensi hasil 0% Packet Loss pada semua perangkat membuktikan kehandalan implementasi VPN L2TP dalam menyediakan akses jarak jauh yang stabil dan efisien. Hal ini memungkinkan admin untuk melakukan monitoring dan manajemen jaringan sekolah dari lokasi *remote* dengan tingkat keandalan yang tinggi [11]. Hasil pengujian ping ini memverifikasi keberhasilan implementasi VPN L2TP dalam memungkinkan konektivitas yang handal antara admin di jaringan publik dan perangkat jaringan di SDS IT Sahabat Muslim Duri. Koneksi yang stabil ini mendukung efektivitas pengelolaan jaringan jarak jauh dan meningkatkan responsivitas dalam menangani masalah jaringan yang mungkin timbul [12].



Gambar 7. Pengujuan jaringan menggunakan ping pada IP *Access Point*

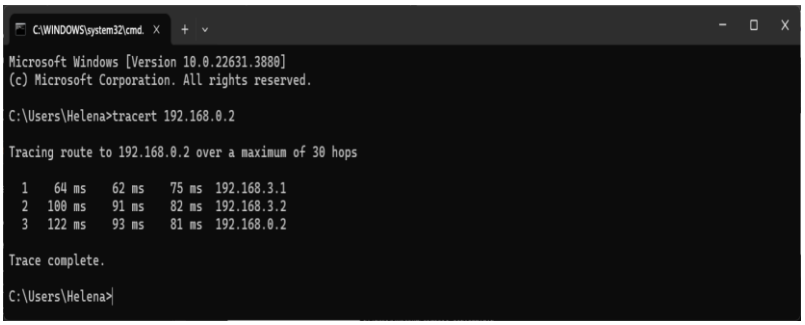
3.1.2. Pengujian jaringan menggunakan *Traceroute* di *Command Prompt* (CMD)

Pengujian *Traceroute* ini dilakukan secara publik menggunakan *command prompt* dengan tujuan untuk mengetahui waktu yang dibutuhkan untuk mencapai setiap hop menggunakan jaringan publik, dengan memberikan perintah "tracert" pada IP *Router*, IP CCTV dan IP *Access Point* yang ada di sekolah. Pengujian *traceroute* pada IP *Router* dapat dilihat pada gambar 8.



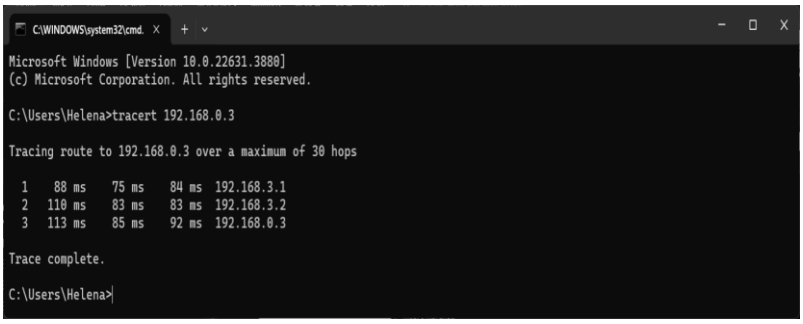
Gambar 8. Pengujian jaringan menggunakan *Traceroute* pada IP *Router*

Untuk *Router* (IP 192.168.0.1), *traceroute* menunjukkan 2 hop dengan waktu tempuh total 108 ms. Paket data melewati IP 192.168.3.1 dengan kecepatan 88 ms sebelum mencapai tujuan akhir, ditunjukkan pada gambar 9.



Gambar 9. Pengujuan jaringan menggunakan *Traceroute* pada IP CCTV

Pada CCTV (IP 192.168.0.2), *traceroute* mencatat 3 hop dengan waktu tempuh total 122 ms. Rute paket melewati IP 192.168.3.1 (64 ms) dan IP 192.168.3.2 (100 ms) sebelum mencapai CCTV. Pengujuan jaringan menggunakan *Traceroute* pada IP *Access Point* ditunjukkan pada gambar 10.



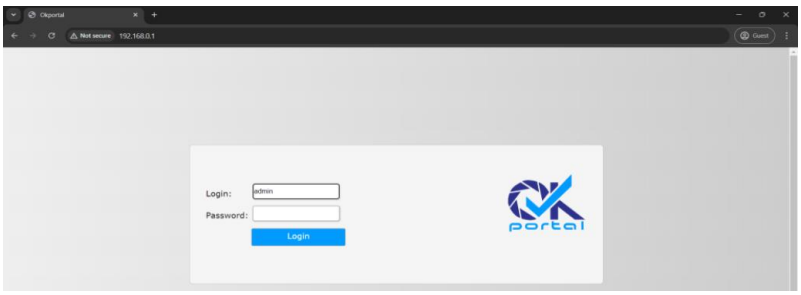
Gambar 10. Pengujuan jaringan menggunakan *Traceroute* pada IP *Access Point*

Pengujian terhadap *Access Point* (IP 192.168.0.3) juga menunjukkan 3 hop dengan waktu tempuh total 113 ms. Paket data melewati IP 192.168.3.1 (88 ms) dan IP 192.168.3.2 (110 ms) sebelum mencapai *Access Point*. Hasil pengujian jaringan jarak jauh menggunakan *traceroute* pada SDS IT Sahabat Muslim menunjukkan konektivitas yang baik antara perangkat admin dan jaringan sekolah melalui VPN L2TP. Pengujian dilakukan terhadap tiga perangkat utama: *Router*, CCTV, dan *Access Point*.

Hasil ini menunjukkan bahwa implementasi VPN L2TP berhasil membuat tunnel yang memungkinkan admin untuk mengakses perangkat jaringan sekolah dari jaringan publik. Waktu tempuh yang relatif singkat (di bawah 150 ms untuk semua perangkat) menunjukkan latensi yang dapat diterima untuk manajemen jarak jauh. Perbedaan jumlah hop antara *Router* (2 hop) dengan CCTV dan *Access Point* (3 hop) mencerminkan topologi jaringan internal sekolah, di mana CCTV dan *Access Point* mungkin berada pada segmen jaringan yang berbeda dari *Router* utama. Kesimpulannya, hasil *traceroute* ini memverifikasi keberhasilan implementasi VPN L2TP dalam memungkinkan akses jarak jauh yang efisien terhadap perangkat jaringan SDS IT Sahabat Muslim Duri.

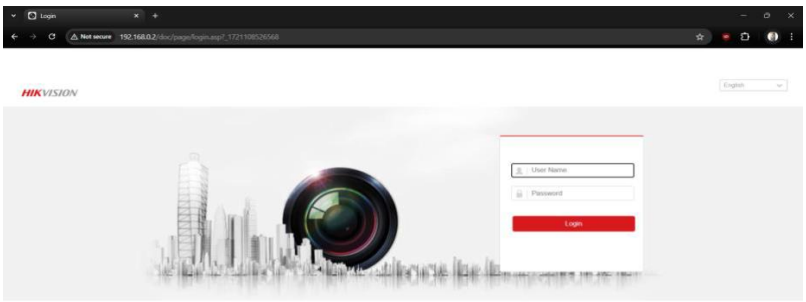
3.2. Pengujian *Remote* Perangkat Menggunakan Browser

Pengujian *remote* perangkat ini dilakukan secara jarak jauh (jaringan publik) dengan tujuan apakah jaringan VPN L2TP sudah terkoneksi dan apakah dapat digunakan untuk melakukan *remote* perangkat secara jarak jauh, dengan membuka website melalui browser pada IP *Router*, IP CCTV dan IP *Access Point* yang ada di sekolah [13]. Pengujian Remote pada IP *Router* dapat dilihat pada gambar 11.



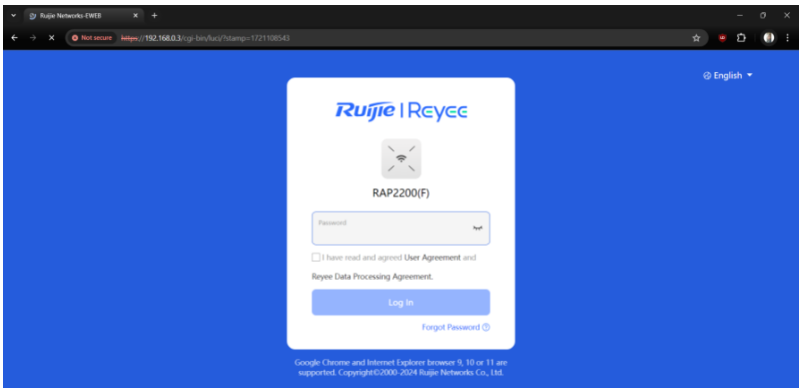
Gambar 11. Pengujian Remote pada IP *Router*

Untuk *Router* (IP 192.168.0.1), hasil pengujian menunjukkan bahwa admin berhasil mengakses perangkat ini dari jaringan publik. Keberhasilan ini membuktikan bahwa konfigurasi VPN L2TP telah berhasil membuat tunnel yang aman antara lokasi *remote* admin dan jaringan sekolah, memungkinkan akses langsung ke *router* utama [14]. Pengujian Remote pada IP CCTV ditunjukkan pada gambar 12.



Gambar 12. Pengujian Remote pada IP CCTV

Pada CCTV (IP 192.168.0.2), pengujian *remote* juga menunjukkan hasil yang positif. Admin dapat mengakses CCTV dari jaringan publik, mengkonfirmasi bahwa koneksi VPN L2TP tidak hanya memungkinkan akses ke *router*, tetapi juga ke perangkat lain dalam jaringan sekolah [15]. Pengujian *Remote* pada IP *Access Point* ditunjukkan pada gambar 13.



Gambar 13. Pengujian *Remote* pada IP *Access Point*

Pengujian terhadap *Access Point* (IP 192.168.0.3) juga menunjukkan hasil yang memuaskan. Admin berhasil mengakses *Access Point* dari jaringan publik, membuktikan bahwa konektivitas VPN L2TP mencakup seluruh perangkat utama dalam jaringan sekolah. Keberhasilan akses *remote* ke ketiga perangkat ini mendemonstrasikan efektivitas implementasi VPN L2TP dalam menyediakan konektivitas yang aman dan handal antara jaringan publik dan jaringan sekolah. Ini memungkinkan admin untuk melakukan berbagai tugas manajemen jaringan, termasuk konfigurasi *router*, monitoring CCTV, dan pengelolaan *Access Point*, dari lokasi *remote* tanpa kompromi keamanan [16].

Hasil pengujian ini juga mengindikasikan bahwa konfigurasi firewall dan routing pada jaringan sekolah telah diatur dengan tepat untuk memungkinkan akses *remote* melalui VPN L2TP, sambil tetap menjaga keamanan jaringan internal. Pengujian *remote* jaringan ini memverifikasi keberhasilan implementasi VPN L2TP dalam memungkinkan manajemen jarak jauh yang efektif terhadap perangkat jaringan di SDS IT Sahabat Muslim. Kemampuan untuk mengakses dan mengelola perangkat-perangkat kritis seperti *Router*, CCTV, dan *Access Point* dari jaringan publik meningkatkan fleksibilitas dan responsivitas dalam pengelolaan infrastruktur jaringan sekolah, memungkinkan pemantauan dan pengelolaan yang lebih efisien.

4. KESIMPULAN

Implementasi *Virtual Private Network* (VPN) menggunakan L2TP berbasis mikrotik di SDS IT Sahabat Muslim telah berhasil dilaksanakan, dengan jaringan VPN yang berfungsi sesuai konfigurasi, dapat diakses dari jarak jauh, dan menjamin keamanan data melalui enkripsi tunnel. Meskipun demikian, penelitian ini memiliki keterbatasan dalam hal pengujian keamanan komprehensif, analisis skalabilitas, dan evaluasi dampak terhadap kinerja operasional sekolah. Untuk penelitian selanjutnya, disarankan melakukan analisis keamanan yang lebih mendalam, termasuk pengujian penetrasi dan evaluasi ancaman keamanan, melakukan studi komparatif dengan protokol VPN lainnya seperti OpenVPN atau IPSec, mengoptimalkan performa jaringan VPN terutama dalam hal kecepatan transfer data dan latensi, serta mengeksplorasi integrasi dengan sistem manajemen identitas dan akses untuk meningkatkan keamanan dan kemudahan pengelolaan pengguna dalam konteks penerapan di lingkungan pendidikan.

REFERENSI

[1] S. Ikhwan and A. Amalina, "Analisis Jaringan VPN Menggunakan PPTP dan L2TP," *JURNAL INFOTEL*, vol. 9, no. 3, Aug. 2017, doi: 10.20895/infotel.v9i3.274.

[2] R. Watrianthos and M. Nasution, "Analisa Kemampuan Transver Data VPN Berbasis Open Source Pada Kondisi Encripsi-Dekscripsi dan Komprensi-Dekomprensi," 2018.

[3] M. Badrul, S. Informasi, S. Tinggi Manajemen Informatika dan Komputer, J. No, and W. Jati Barat Jakarta Selatan, "Open VPN-Access Server Dengan Enskripsi SSL/TI Open SSL," *Informatics For Educators And Professionals*, vol. 1, no. 1, p. 12, 2016.

[4] A. Rachmawan, A. Prihanto, and M. Kom, "Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet di Atas VPN 53 Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet Di atas VPN."

[5] A. Imran and A. Rustianto, "Jurnal Informatika Terpadu," *Jurnal Informatika Terpadu*, vol. 7, no. 1, pp. 33–38, 2021, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[6] S. Sumarna and A. Maulana, "Implementasi Virtual Private Network Menggunakan L2TP/IPsec pada BBPK Jakarta," *EXPERT: Jurnal Manajemen Sistem Informasi dan Teknologi*, vol. 11, no. 2, p. 90, Dec. 2021, doi: 10.36448/expert.v11i2.1829.

[7] S. Sinurat and J. Simarmata, "Pemanfaatan Protokol Pppt Dan L2tp Dalam Membangun Virtual Private Network (Vpn) Pada Mikrotik Os," *Juril Amik MBP*, vol. II, 2014.

[8] L. Umaroh and M. Rifauddin, "Implementasi Virtual Private Network (Vpn) Di Perpustakaan Universitas Islam Malang," *Baca: Jurnal Dokumentasi Dan Informasi*, vol. 41, no. 2, p. 193, Dec. 2020, doi: 10.14203/j.baca.v41i2.531.

[9] B. Sutara, "Layanan Jaringan Internet Pada Virtual Private Network (VPN) Menggunakan L2TP Untuk Peningkatan Keamanan Jaringan," vol. 16, no. 1, 2017.

[10] M. Suprianty, "Identifikasi Domain Name System (DNS) menggunakan Command Prompt (CMD) dan Traceroute (Tracert)," 2014.

[11] Prayogi Wicaksana, F. Hadi, and Aulia Fitrul Hadi, "Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan," *Jurnal KomtekInfo*, pp. 169–175, Aug. 2021, doi: 10.35134/komtekinfo.v8i3.128.

[12] A. Rachmawan, A. Prihanto, and M. Kom, "Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet di Atas VPN 53 Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet Di atas VPN."

[13] A. Putra, P. 1∗, M. R. Putra, and M. Hafizh, "Jurnal KomtekInfo Analisis Jaringan VPN Menggunakan PPTP dan L2TP Berbasis Mikrotik pada Diskominfo Kabupaten Muko Muko," 2021, doi: 10.37034/komtekinfo.v8i3.143.

[14] A. Habibi and S. Arifin, "Membangun Jaringan Virtual Private Network (Vpn) Dengan Metode Tunneling Menggunakan Mikrotik Untuk Komunikasi Lokal Di Stmik Ppkia Pradnya Paramita Malang."

[15] M. N. R. Maja, "Implementasi Dan Analisa L2tpipsec Menggunakan Router Cisco Seri 2900," 2019.

[16] A. W. Rahman and M. M. Sigalingging, "Network Security & Interkoneksi Jaringan Dengan L2tp+Ipsec."