Analisis *Quality of Service* Protokol VPN Berbasis Mikrotik RouterOS pada Lingkungan GNS3 dengan Standar TIPHON dan Model ITU-T G-107 pada IPv6 Menggunakan *Tunneling* 6to4

Saca Ilmare Dinbiru[1)], Nanang Trianto[2)]

(1) Jurusan Keamanan Siber, Politeknik Siber dan Sandi Negara, saca.ilmare@student.poltekssn.ac.id

(2) Jurusan Keamanan Siber, Politeknik Siber dan Sandi Negara, nanang@poltekssn.ac.id

Abstrak

Penggunaan IPv6 sebagai penerus IPv4 mengatasi masalah kehabisan alamat IP dan meningkatkan keamanan komunikasi. Namun, pada tahun 2022, sebanyak 12,7 juta akun mengalami kebocoran data, menjadikan VPN solusi utama bagi pengguna internet. Sebanyak 35% pengguna VPN mengharapkan komunikasi internet yang aman dan berkualitas, meskipun terdapat prinsip dasar bahwa keamanan sering kali berbanding terbalik dengan kenyamanan, yang menjadi tantangan bagi teknologi VPN. Penelitian ini mengevaluasi performa tiga protokol VPN pada MikroTik RouterOS yaitu WireGuard, L2TP/IPsec, dan SSTP dalam lingkungan IPv6 dengan tunneling 6to4 di GNS3. Pengujian dilakukan melalui tiga skenario: pengukuran bandwidth menggunakan iPerf3, serta evaluasi QoS melalui WinSCP dan HTML5 Video. Hasil pengujian menunjukkan bahwa WireGuard memiliki performa terbaik dalam kecepatan transfer data dan bandwidth, menjadikannya pilihan utama untuk transfer data yang tinggi. L2TP/IPsec unggul dalam pengiriman berkas audio dan video dengan performa stabil. SSTP memberikan kualitas streaming video yang sangat baik, tercermin dari nilai Mean Opinion Score (MOS) dan R-Faktor yang tinggi. Parameter delay dan jitter menunjukkan performa yang baik dengan nilai konsisten, sementara packet loss tidak terdeteksi selama pengujian. Secara keseluruhan, meskipun WireGuard tidak unggul dalam streaming video, perbedaannya dengan SSTP sangat kecil. Oleh karena itu, penelitian ini merekomendasikan WireGuard sebagai protokol VPN terbaik untuk berbagai kebutuhan transfer data, sehingga pengguna tidak perlu berganti-ganti protokol untuk transfer data dan streaming video.

Kata kunci: GNS3 (1), IPv6 (2), Mikrotik RouterOS (3), Model ITU-T G.107 (4), Quality of Service (5), TIPHON (6), Tunneling 6to4 (7), dan VPN (8).

Abstract

The use of IPv6 as a successor to IPv4 addresses the problem of IP address exhaustion and improves communication security. However, by 2022, as many as 12.7 million accounts experienced data breaches, making VPNs the ultimate solution for internet users. As many as 35% of VPN users expect secure and quality internet communication, despite the basic principle that security is often inversely proportional to convenience, which poses a challenge for VPN technology. This study evaluates the performance of three VPN protocols on MikroTik RouterOS namely WireGuard, L2TP/IPsec, and SSTP in an IPv6 environment with 6to4 tunneling in GNS3. Tests were conducted through three scenarios: bandwidth measurement using iPerf3, as well as QoS evaluation through WinSCP and HTML5 Video. The test results show that WireGuard has the best performance in data transfer speed and bandwidth, making it the first choice for high data transfer. L2TP/IPsec excels in sending audio and video files with stable performance. SSTP provides excellent video streaming quality, reflected by high Mean Opinion Score (MOS) and R-Factor values. The delay and jitter parameters performed well with consistent values, while packet loss was not detected during the test. Overall, although WireGuard does not excel in video streaming, the difference with SSTP is very small. Therefore, this study recommends WireGuard as the best VPN protocol for various data transfer needs, so that users do not need to switch protocols for data transfer and video streaming.

Keywords: GNS3 (1), IPv6 (2), Mikrotik RouterOS (3), Model ITU-T G.107 (4), Quality of Service (5), TIPHON (6), Tunneling 6to4 (7), and VPN (8).

1. PENDAHULUAN

Internet Protocol version 6 atau biasa dikenal dengan IPv6 merupakan hasil pengembangan dari IPv4 yang ditetapkan oleh Internet Engineering Task Force (IETF) [1]. IETF menetapkan IPv6 sebagai penerus dari IPv4 yang berguna untuk mengatasi permasalahan habisnya alamat dari IPv4, meningkatkan jumlah alamat dari IP. IPv6 menawarkan fitur-fitur baru yang dijadikan keunggulan, seperti ruang alamat yang besar, peningkatan keamanan, *multicasting*, dan keunggulan lainnya [1]. Berdasarkan data dari perusahaan keamanan siber yaitu Surfshark pada tahun 2022, Indonesia berada di dalam urutan ketiga dengan jumlah kasus kebocoran data terbanyak yaitu 12,7 juta akun walaupun sudah menggunakan IPv6 [2]. Salah satu kerawanan jaringan yaitu adanya pencurian data yang disebabkan *intercept* pada jaringan komputer yang terhubung dengan internet karena penyadapan data jaringan komputer yang mengarah pada pencurian data memiliki risiko yang signifikan terhadap keamanan informasi. Perkembangan teknologi menciptakan adanya *Virtual Private*

Network (VPN) yang mampu mengamankan komunikasi dalam jarak yang jauh karena VPN merupakan bentuk jaringan yang sifatnya privat tetapi dapat diakses melalui jaringan publik yang dapat memungkinkan pengguna untuk masuk ke dalam jaringan privat serta juga dapat melakukan *remote* di dalam jaringan tersebut [3]. Berdasarkan data dari *We Are Social* pada Juli 2023, sebanyak 35% pengguna internet di Indonesia dengan rentang umur 16 – 64 tahun menggunakan layanan VPN dengan harapan mendapatkan keamanan dan kenyaman dalam berselancar di dunia maya [4]. Namun seperti prinsip keamanan informasi, keamanan berbanding terbalik dengan kenyamanan. VPN bukan tanpa kekurangan, walaupun dapat mengamankan informasi pribadi saat menggunakan internet, kecepatan yang termasuk dalam kenyamanan bagi pengguna dalam menggunakan internet juga menjadi kekurangannya. VPN berjalan dengan dukungan protokol VPN yang berbeda-beda untuk mengamankan datanya yang mana tiap protokol VPN memiliki kualitas kenyamanan yang berbeda-beda. Terdapat beberapa protokol pendukung dalam mengamankan dan juga mendukung jalur komunikasi, di antaranya terdapat protokol SSTP, L2TP/IPsec, dan WireGuard.

Beberapa jenis *router* menyediakan layanan VPN yang berbeda-beda, contohnya seperti Mikrotik RouterOS. Mikrotik RouterOS merupakan salah satu *router* ternama yang diciptakan untuk membangun jaringan, baik dari skala yang kecil maupun yang besar. Jaringan yang dibentuk dari Mikrotik RouterOS dapat disimulasikan secara virtual dan dapat digunakan di lingkungan *Graphical Network Simulator* 3 (GNS3). GNS3 merupakan sebuah aplikasi simulator jaringan berbasis grafis yang dapat berjalan di sistem operasi Windows dan Linux. Kecepatan protokol VPN yang berbeda sangat bervariasi, dengan masing-masing protokol menawarkan karakteristik kinerja yang berbeda sehingga akan berpengaruh kepada performa dari *Quality of Service* (QoS). QoS merupakan salah satu cara perhitungan kuantitatif untuk memperlihatkan kualitas dari layanan protokol VPN. Perhitungan dan pengelolaan hasil dari pengukuran dapat menggunakan standar TIPHON dan Model ITU-T G.107.

TIPHON merupakan standar yang dikeluarkan oleh badan standar ETSI (*European Telecommunications Standards Institue*) yang merupakan standar perhitungan, penilaian parameter QoS, dan penyedia hasil parameter serta penyedia standar persentase dari nilai QoS yang dihasilkan [5]. TIPHON digunakan dalam penelitian ini dikarenakan dengan pendekatan standar. Selain TIPHON, Model ITU-T G.107 merupakan standar yang digunakan pada penelitian ini karena standar ini diterima secara luas untuk mengevaluasi kinerja sistem komunikasi suara di berbagai jenis jaringan. Keduanya harus digunakan karena standar ini memiliki saling keterkaitan pada penelitian ini walaupun keduanya memiliki kegunaan yang berbeda. Standar TIPHON berguna untuk mendukung penilaian QoS terhadap parameter *delay, jitter, throughput,* dan *packet loss.* Sedangkan standar Model ITU-T G.107 berguna untuk mendukung penilaian QoS terhadap parameter *Mean Opinion Score* (MOS). Pada penelitian ini, kedua standar memiliki perbedaan namun saling melengkapi untuk menentukan kategorisasi penilaian terhadap parameter yang diuji.

Pada penelitian ini, penulis akan melakukan Uji QoS dengan menggunakan standar perhitungan TIPHON dan Model ITU-T G.107 pada layanan protokol VPN yang berada pada Mikrotik RouterOS yaitu L2TP/IPsec, SSTP, dan WireGuard pada lingkungan GNS3 dengan menggunakan IPv6 dan dengan bantuan *tunneling* 6to4. Hasil dari analisis komparasi ini dapat dijadikan rekomendasi dalam pemilihan protokol VPN yang aman, namun tetap memiliki kualitas kenyamanan yang baik bagi individu maupun organisasi sesuai dengan kebutuhannya yang diukur berdasarkan hasil pengujian dari proses kirim dan terima berkas serta akses jaringan lokal.

2. LANDASAN TEORI

2.1 IPv6

IP merupakan singkatan dari *Internet Protocol* yang merupakan protokol berbasis tanpa koneksi dan berguna untuk mendefinisikan sebuah alamat agar paket dapat dikirimkan atau diterima dari komputer satu ke komputer lainnya. IP ini merupakan sebuah protokol yang bekerja pada *layer* 3 OSI *Layer* yaitu Internet *Layer* atau *Network Layer* [6].

IPv6 merupakan versi terbaru dari IPv4 yang dikeluarkan oleh IETF. IPv6 menggunakan 128-bit alamat sehingga memungkinkan adanya lebih dari 7,9 x 1028 kali lebih banyak dari IPv4 yang mana IPv4 ini menggunakan 32-bit untuk alamat. Bentuk dari pengalamatan IPv6 juga berbentuk *unicast, multicast,* dan *anycast* dengan *loopback address*-nya yaitu ::1 [1].

2.2 *Tunneling* 6to4

Tunneling IPv4 ke IPv6 merupakan sebuah mekanisme yang digunakan dengan tujuan memfasilitasi transisi antara IPv4 dan IPv6 dengan cara mengenkapsulasi paket IPv6 ke dalam paket IPv4 agar memungkinkan untuk adanya transmisi melalui jaringan IPv6. Transisi dibutuhkan karena habisnya alamat IPv4 yang menyebabkan transisi dari IPv4 ke IPv6 tidak bisa dihindari sehingga IPv6 dapat menjadi solusi untuk mengatasi keterbatasan pengalamatan pada IPv4 [7].

2.3 VPN

Jaringan ada yang bersifat lokal atau privat dan juga ada yang sifatnya publik. Jaringan lokal atau privat ini adalah jaringan yang menghubungkan

antara *host* ke *host* namun dengan konteks di dalam wilayah yang sama, seperti contohnya di perkantoran. Jaringan publik merupakan jaringan yang menghubungkan antar *host* secara luas atau global [8]. Protokol VPN memiliki tujuan utama yaitu mengubah jaringan publik menjadi privat atau secara aman dapat mengakses jaringan privat di publik.

2.3.1 SSTP

Secure Socket Tunneling Protocol (SSTP) merupakan protokol yang dirancang untuk pengumpulan data yang aman dalam jaringan [9] serta merupakan protokol yang mendukung VPN dan didukung dengan keamanan SSL untuk beroperasi melalui TCP [10]. SSTP berjalan pada *port* 443 dalam pengiriman dan penerimaan paket datanya.

2.3.2 L2TP/IPsec

Layer 2 *Tunneling Protocol*/IP *Security* biasa disebut L2TP/IPsec merupakan salah satu protokol VPN [11] yang digunakan untuk menghubungkan satu *router* ke *router* lain dan dari klien ke *host gateway* melalui *server* NAS ISP. Di sisi lain, IPsec menawarkan layanan keamanan untuk jaringan IP, seperti enkripsi dan otentikasi yang kuat.

2.3.3 WireGuard

WireGuard diciptakan oleh Jason Donenfeld pada tahun 2018, seseorang yang menciptakan Edge Security [12]. WireGuard merupakan VPN yang mendukung *host-to-host* dan bekerja pada *layer* 3 OSI *Layer*. WireGuard diklaim dapat menggantikan SSL VPN karena lebih aman, lebih mudah digunakan, dan memiliki kinerja yang lebih mumpuni. WireGuard juga memberikan kinerja yang baik karena memiliki latensi yang rendah namun dengan *throughput* yang tinggi.

2.4 Mikrotik RouterOS

Mikrotik RouterOS merupakan sebuah sistem operasi yang diadopsi dari Mikrotik Routerboard yang berbasis Linux v2.6. Mikrotik RouterOS ini memiliki banyak kelebihan, di antaranya semua fitur yang ada dapat dipasang dengan mudah dan cepat [13].

2.5 *Graphical Network Simulator* 3 (GNS3)

GNS3 merupakan sebuah perangkat lunak gratis yang digunakan untuk melakukan simulasi, meniru, mengonfigurasi, menguji, dan memecahkan permasalahan pada jaringan, baik di lingkungan nyata maupun di lingkungan virtual [14].

2.6 Model ITU-T G.107

Standar ITU-T G.107 menawarkan beberapa keuntungan untuk penelitian, terutama dalam konteks MOS untuk penilaian kualitas sedangkan G.107 adalah standar untuk mengevaluasi kinerja berbagai layanan telekomunikasi [15]. MOS termasuk pada jenis QoS. Penggunaan standar model ITU-T G.107 dikarenakan parameter yang dikeluarkan hanya parameter MOS. Oleh karena itu, pada penelitian ini, Model ITU-T G.107 yang dipilih untuk mengukur MOS.

Faktor-R, yang merupakan jumlah dari faktor penurunan kualitas, digunakan untuk menentukan nilai kualitas secara keseluruhan. Kemudian diterjemahkan ke dalam MOS untuk menunjukkan kualitas yang dirasakan dari sinyal yang diterima [16]. E-model memetakan metrik jaringan ke estimasi nilai MOS.

2.7 TIPHON

TIPHON merupakan standar yang digunakan untuk menilai QoS dari suatu jaringan. TIPHON dikeluarkan oleh suatu badan standar bernama *European Telecommunications Standards Institue* atau biasa dikenal dengan badan standar ETSI [17]. Terdapat beberapa jenis QoS, yaitu *delay, throughput, jitter, packet loss,* MOS, *echo cancellation, error rate*, PDD, dan lainnya. Namun TIPHON hanya mengeluarkan parameter kualitas jaringan yang disesuaikan dengan standar dari QoS, yaitu *delay, throughput, jitter,* dan *packet loss* [18]. Sehingga pada pengujian ini untuk pengukuran parameter *delay, jitter, packet loss,* dan *throughput* diukur dan dikategorisasikan berdasarkan standar TIPHON.

2.8 QoS

QoS merupakan suatu cara untuk mengukur kualitas jaringan dengan menerapkan parameter seberapa baik jaringan tersebut dengan melihat nilai dari parameter yang ditetapkan, seperti *delay, throughput, jitter, packet loss,* MOS, *echo cancellation,* dan PDD [19]. Tujuan QoS salah satunya yaitu dirancang sebagai salah satu cara untuk membantu pengguna atau klien mendapatkan kinerja yang baik dari layanan jaringan.

2.8.1 *Delay*

Delay atau bisa disebut juga dengan *latency*. *Delay* merupakan waktu tunda yang terjadi ketika suatu paket dikirimkan dari titik pengiriman ke titik tujuannya [18], [19], [20]. Berikut adalah rumusan dan penilaian kategori yang disediakan oleh standar TIPHON untuk parameter *delay* dengan mengacu pada [21].

Perhitungan nilai *delay* ditentukan dari persamaan berikut:

$$Delay = \frac{Total\ Delay}{Total\ Paket\ yang\ Diterima}$$

Penilaian kategori *delay* ditentukan berdasarkan tabel berikut:

Tabel 1. Parameter Penilaian *Delay*

Kategori *Delay*	Besar *Delay* (ms)	Indeks
Sangat Baik	< 150	4
Baik	150 s/d 300	3
Sedang	300 s/d 450	2
Buruk	> 450	1

2.8.2 *Jitter*

Jitter merupakan salah satu jenis dari *delay*. *Jitter* disebabkan oleh adanya variasi dari panjang antrian paket, waktu pengolahan paket atau data, dan juga besarnya tumbukan antar paket yang ada [18], [19], [20]. Jika beban pada antrian paket semakin besar kemungkinan terjadinya tumbukan semakin besar pula, maka nilai dari *jitter* juga semakin besar sedangkan nilai QoS semakin turun dari jaringan tersebut [20]. Berikut adalah rumusan dan penilaian kategori yang disediakan oleh standar TIPHON untuk parameter *jitter* dengan mengacu pada [21].

Perhitungan nilai *jitter* ditentukan dari persamaan berikut:

$$Jitter = \frac{Total\ Variasi\ Delay}{Total\ Packet\ yang\ Diterima - 1}$$

Penilaian kategori *jitter* ditentukan berdasarkan tabel berikut:

Tabel 2. Parameter Penilaian *Jitter*

Kategori *Jitter*	Peak *Jitter* (ms)	Indeks
Sangat Baik	0 s/d 74	4
Baik	75 s/d 124	3
Sedang	125 s/d 224	2
Buruk	> 225 ms	1

2.8.3 *Throughput*

Throughput merupakan kecepatan (laju) transfer data yang efektif, yang diukur dalam bps (bit per detik) atau bisa juga disebutkan dengan jumlah paket yang berhasil tiba di tujuan yang ditunjukkan dengan interval waktu [18], [19].

Perhitungan nilai *throughput* ditentukan dari persamaan berikut:

$$Throughput = \frac{Jumlah\ Data\ yang\ Dikirim}{Waktu\ Pengiriman\ Paket}$$

Penilaian kategori *throughput* ditentukan berdasarkan tabel berikut:

Tabel 3 Parameter Penilaian *Throughput*

Kategori *Throughput*	Nilai (Kbps)	Indeks
Sangat Baik	> 2100 Kbps	4
Baik	1200 Kbps – 2100 Kbps	3
Normal	700 Kbps – 1200 Kbps	2
Kurang	338 Kbps – 700 Kbps	1
Buruk	0 – 338 Kbps	0

2.8.4 *Packet loss*

Packet loss merupakan sebuah parameter QoS yang merepresentasikan kondisi persentase jumlah paket yang hilang saat pengiriman paket yang disebabkan oleh *overload*-nya trafik pada jaringan yang menyebabkan *congestion* [19], [20].

Perhitungan nilai *packet loss* ditentukan dari persamaan berikut:

$$Packet\ Loss = \frac{Paket\ Data\ Terkirim - Paket\ Data\ Diterima}{Paket\ Data\ Terkirim} \times 100\%$$

Penilaian kategori *packet loss* ditentukan berdasarkan tabel berikut:

Tabel 4. Parameter Penilaian *Packet loss*

Kategori *Packet loss*	Persentase (%)	Indeks
Sangat Baik	0 %	4
Baik	3 %	3
Sedang	15 %	2
Buruk	25 %	1

2.8.5 MOS

Mean Opinion Score atau MOS merupakan satuan parameter kualitas suara. Perhitungan MOS dilakukan dengan pendekatan matematis yaitu dengan E-Model yang didasari oleh nilai *delay* dan juga *packet loss* [22]. R-Faktor dihitung dengan menggunakan rumus yang ditunjukkan pada Persamaan (1). Faktor kualitas transmisi ditandai dengan variable R, dan I_d adalah faktor penurunan kualitas yang disebabkan oleh *delay* atau d. I_{ef} adalah faktor penurunan kualitas yang disebabkan oleh *codec* atau *packet loss.*

$$R = 94.2 - I_d - I_{ef} \quad (1)$$

Nilai I_d ditampilkan dalam Persamaan (2). H merupakan sebuah fungsi bernama *heavyside*.

$$I_d = 0.024d + 0.11(d - 177.3)\,H\,(d - 177.3) \quad (2)$$

Syarat nilai H berada pada persamaan (3). Rumus I_{ef} ada pada persamaan (4) dan besar kemungkinan *packet loss* disimbolkan dengan "e" dalam desimal. Rumus R-Faktor secara keseluruhan terdapat pada persamaan (5).

$$H = \begin{cases} 0, & x < 0 \\ 1, & x \geq 0 \end{cases} \quad (3)$$

$$I_{ef} = 7 + 30 \ln(1 + 15e) \quad (4)$$

$$R = 94.2 - 0.024d + 0.11(d - 177.3)\,H\,(d - 177.3) - 7 + 30 \ln(1 + 15e) \quad (5)$$

Perhitungan nilai MOS ditentukan dari persamaan berikut dengan ketentuan R mengacu pada Tabel 2.7.

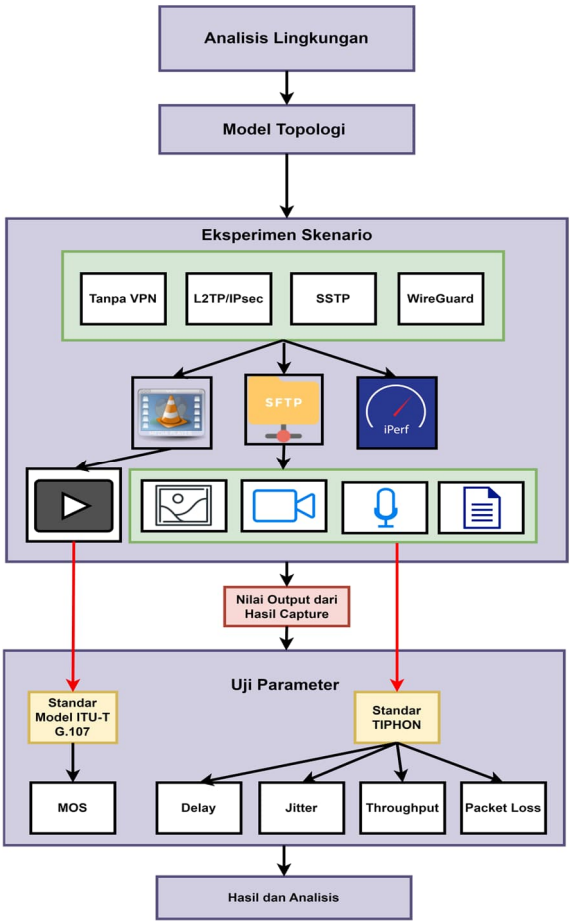
$$MOS = \begin{cases} 1, & Jika\ R < 0 \\ 4.5, & Jika\ R > 100 \\ 1 + 0.035R + 7 \times 10^{6}\,R\,(R - 60)(100 - R), & Jika\ 0 < R < 100 \end{cases}$$

Tabel 5. Parameter Penilaian MOS

R-Faktor	Nilai MOS	Index	Kategori
89 ≥ R ≥ 100	4,2 ≥ M ≥ 5	A	*Excellent*
79 ≥ R ≥ 89	3,9 ≥ M ≥ 4,2	B	*Very Good*
70 ≥ R ≥ 79	3,5 ≥ M ≥ 3,9	C	*Acceptable*
59 ≥ R ≥ 70	3 ≥ M ≥ 3,5	D	*Concerning*
49 ≥ R ≥ 59	2,5 ≥ M ≥ 3	E	*Poor*
0 ≥ R ≥ 49	0 ≥ M ≥ 2,5	F	*Very Poor*

3. METODE PENELITIAN

Penelitian ini berfokus pada tiga fitur VPN di MikroTik, yaitu L2TP/IPsec, SSTP, dan WireGuard, yang diimplementasikan pada IPv6 menggunakan *Tunneling* 6to4 untuk mentransisikan IPv6 dari IPv4 publik. Penelitian komparatif ini bertujuan membandingkan kinerja ketiga protokol VPN. Pendekatan kuantitatif digunakan untuk mengumpulkan dan menganalisis data yang diperoleh melalui iPerf3, SFTP, dan HTML5 Video.



Gambar 1. Desain Penelitian

Pada Gambar 1 ditampilkan alur penelitian yang dilakukan sebagai metode penelitian.

3.1 Analisis Lingkungan

Analisis Lingkungan yaitu menjelaskan *software* dan *hardware* apa saja yang digunakan beserta alasannya. Pada penelitian ini menggunakan *software* GNS3, VirtualBox, MikroTik RouterOS, dan *tools* seperti iPerf3, SFTP, HTML5 Video untuk simulasi dan pengujian.

3.2 Model Topologi

Pada tahap ini mendesain dan menjelaskan topologi jaringan yang digunakan dengan melibatkan dua *router*, *cloud*, *switch*, dan *host* dengan komunikasi IPv4 dan transisi ke IPv6 melalui *Tunneling* 6to4.

3.3 Eksperimen Skenario

Eksperimen Skenario menentukan dan menjalankan skenario eksperimen yang sudah ditetapkan sesuai dengan topologi yang dibuat, melakukan konfigurasi atau persiapan pengujian, dan melakukan pengujian. Pada eksperimen ini menguji tiga skenario yang melibatkan komunikasi tanpa VPN dan dengan tiga protokol VPN (L2TP/IPsec, SSTP, WireGuard). Skenario I: dengan mengirimkan paket menggunakan iPerf3, Skenario II dengan mengirimkan berkas dengan ekstensi berbeda (dokumen, gambar, audio, video) menggunakan WinSCP Protokol Transmisi SFTP, Skenario III dengan *streaming* video berdurasi 10 detik dan 30 detik menggunakan HTML5 Video Web Server. Seluruh hasil Data di-*capture* dengan Wireshark pada *Network Layer.*

3.4 Uji Parameter

Uji Parameter melakukan perhitungan terhadap hasil dari pengujian dengan menggunakan standar tertentu, dan pengambilan data dengan Wireshark. Perhitungan nilai *delay*, *jitter*, *packet loss*, *throughput*, dan MOS berdasarkan standar TIPHON dan E-Model dari hasil pengujian.

3.5 Hasil dan Analisis

Hasil dan Analisis yang merupakan penentuan kualitas dari protokol VPN juga perbandingan ketiga protokol VPN, analisis hasil, dan penulisan hasil akhir. Analisis dan perbandingan protokol VPN dilakukan berdasarkan hasil pengujian serta menentukan kualitas protokol VPN berdasarkan standar. Hasil disajikan dalam bentuk tabel dan grafik, dengan rekomendasi penggunaan protokol VPN berdasarkan hasil QoS.

4. HASIL DAN ANALISIS

Berdasarkan Tabel 6, ditampilkan lingkungan yang dipilih untuk simulasi dan pengujian jaringan dirancang untuk menyediakan platform yang komprehensif dan serbaguna untuk mengevaluasi kinerja, keamanan, dan fungsionalitas jaringan.

Topologi jaringan ini menggunakan *site-to-site* VPN, atau *router-to-router* VPN, untuk menghubungkan dua lokasi terpisah secara aman melalui internet menggunakan *tunnel* VPN. Jaringan dibangun di lingkungan virtual GNS3 dengan komponen berupa satu NAT awan, satu switch, dua Mikrotik RouterOS, dan dua PC virtual dengan Windows 10. Kedua router terhubung ke switch melalui *interface* eth0, sementara eth1 pada tiap router terhubung ke PC virtual. IPv4 diatur dengan DHCP dari NAT awan, sedangkan IPv6 dikonfigurasi statik pada router. Setiap router memiliki MAC *address* unik yang memungkinkan akses ke WebFig melalui WinBox.

Tabel 6. Spesifikasi *Hardware* dan *Software*

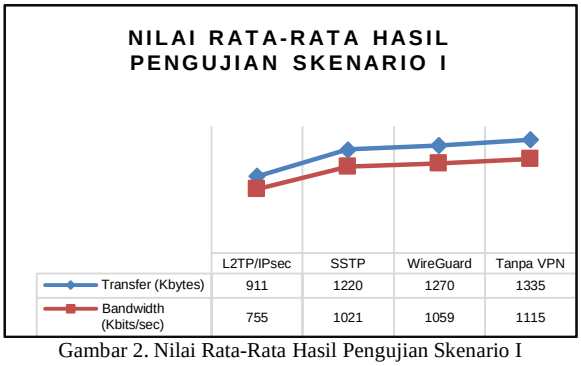
No	Kategori	Perangkat	Spesifikasi
1	*Software*	Lingkungan Simulasi	GNS3 2.2.46
		Virtual Machine	VirtualBox 7.0.14
		Tools Pengujian	Wireshark 4.2.2
			WinSCP 6.3.1
			iPerf3 3.1.3
			HTML5 Video
			Apache XAMPP 8.2.12
			WinBox64
		Router 1 dan *Router* 2	Mikrotik RouterOS CHR 7.14
		PC 1 dan PC 2	Windows 10 Home 64-Bit
2	*Hardware*	Sistem Manufaktur	ASUSTek Computer Inc
		Sistem Model	ROG Strix G513RC
		BIOS	G513RC.327
		Processor	AMD Ryzen 7 6800HS with Radeon Graphics, 3.2 Ghz (16 Cpus)
		Sistem Operasi	Windows 11 Home Single Language 64-Bit
		Memory	16384 MB RAM
		Hardisk	1 TB
3	Pengaturan Jaringan pada GNS3	NAT	Running pada Server GNS3 dengan *port* 80
		Switch	Running pada Server Laptop dengan *port* 3080
		Router 1 dan *Router* 2	Running pada Server GNS3 VM pada *port* 80
			Terhubung dengan QEMU VM
			Jaringan dengan settingan *default* GNS3
		PC 1 dan PC 2	Running pada Server Laptop dengan *port* 3080
			Terhubung dengan VirtualBox VM
			Network adapter 1: terhubung dengan *Generic Driver*
			Network adapter 2: terhubung dengan *Generic Driver*

Tabel 7. IP Perangkat

Device	*Interface*	IPv4 / IPv6 *Address*	*Gateway*
NAT	nat0	192.168.122.1 /24	N/A
Router 1	eth1	2001:db8:ac10:1::2 /64	N/A
	eth0 (6to4)	2:2:2:2::1 /64	N/A
	IPv4 DHCP	192.168.122.9 /24	192.168.122.1 /24
Router 2	eth1	2001:db8:ac10:3::2 /64	N/A
	eth0 (6to4)	2:2:2:2::2 /64	N/A
	IPv4 DHCP	192.168.122.43 /24	192.168.122.1 /24
PC 1	N/A	2001:db8:ac10:1::1 /64	2001:db8:ac10:1::2 /64
PC 2	N/A	2001:db8:ac10:3::1 /64	2001:db8:ac10:3::2 /64

4.1 Hasil Pengujian dan Perhitungan Skenario I

Hasil pengujian pada Skenario I terhadap protokol VPN dan tanpa protokol VPN dapat menampilkan dua sisi, yaitu dari server dan klien. Pada pengujian ini, sisi server dan klien berperan penting dalam mengukur berbagai parameter kinerja, seperti kecepatan dan besar paket yang ditransfer, serta *bandwidth* yang digunakan untuk kirim dan terima paket. Pengujian ini memungkinkan untuk mengevaluasi dan memberikan gambaran yang lebih baik tentang tingkat keandalan dan kestabilan koneksi yang disediakan oleh VPN tersebut serta bertujuan menghilangkan rasa penasaran dari pengguna. Pengujian tanpa menggunakan VPN dapat dijadikan pembanding terkait kualitas VPN yang dilihat dari segi transfer dan *bandwidth.*



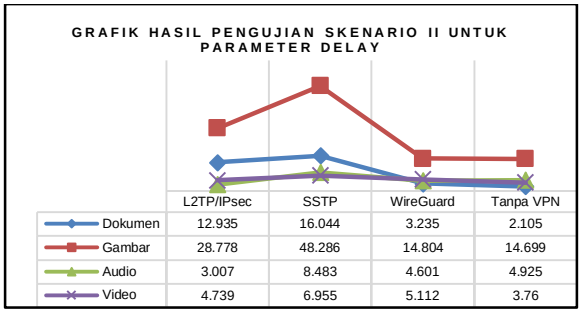
Gambar 2. Nilai Rata-Rata Hasil Pengujian Skenario I

Pada skenario pengujian ini, dilakukan pengiriman paket selama 10 detik dengan interval satu detik, mengukur transfer data dan *bandwidth*. Hasil menunjukkan bahwa VPN WireGuard unggul dengan rata-rata *bandwidth* 1059 Kbits/sec dan transfer data sebesar 1270 Kbytes (10160 Kbits). WireGuard menunjukkan perbedaan yang signifikan dibandingkan L2TP/IPsec, yang memiliki rata-rata *bandwidth* 755 Kbits/sec dan transfer data 911 Kbytes (7288 Kbits). SSTP berada di antara keduanya dengan *bandwidth* rata-rata 1021 Kbits/sec dan transfer data 1220 Kbytes (9760 Kbits).

Pengujian ini mengindikasikan bahwa WireGuard memiliki kinerja yang lebih stabil dan konsisten, dibandingkan L2TP/IPsec. Meskipun pengujian tanpa VPN menunjukkan transfer data dan *bandwidth* yang lebih tinggi (1335 Kbytes atau 10680 Kbits dan 1115 Kbits/sec), penggunaan VPN tetap lebih aman. Secara keseluruhan, WireGuard mendominasi dalam pengujian ini dengan performa yang lebih baik dibandingkan L2TP/IPsec dan SSTP.

4.2 Hasil Pengujian dan Perhitungan Skenario II

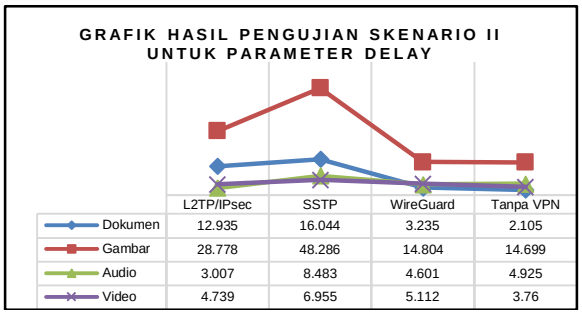
Hasil pengujian pada Skenario II yaitu transmisi berkas menggunakan protokol kirim dan terima berkas SFTP dan aplikasi WinSCP dengan mengirimkan dokumen, gambar, suara, dan video, terdapat hasil perhitungan parameter QoS berupa *delay*, *jitter*, *packet loss*, dan *throughput*. Dari hasil pengujian yang ada, berikut pengkategorian parameter QoS berdasarkan standar TIPHON.



	L2TP/IPsec	SSTP	WireGuard	Tanpa VPN
Dokumen	12.935	16.044	3.235	2.105
Gambar	28.778	48.286	14.804	14.699
Audio	3.007	8.483	4.601	4.925
Video	4.739	6.955	5.112	3.76

Gambar 3. Nilai Rata-Rata Hasil Pengujian Skenario II Parameter *Delay*

Pada Gambar 3 yang merepresentasikan hasil pengujian transmisi dokumen, gambar, audio, dan video dalam menguji parameter *delay* dapat dilakukan analisis yaitu dalam pengujian *delay*, L2TP/IPsec unggul pada berkas audio dan video, sementara WireGuard unggul pada berkas dokumen dan gambar. SSTP tidak menunjukkan keunggulan dibandingkan dengan VPN lainnya maupun tanpa VPN di semua jenis berkas. Pengujian tanpa VPN memberikan hasil terbaik untuk semua transmisi berkas. Semua nilai *delay* dalam pengujian ini dikategorikan "sangat baik" menurut standar TIPHON karena seluruhnya kurang dari 150 ms.

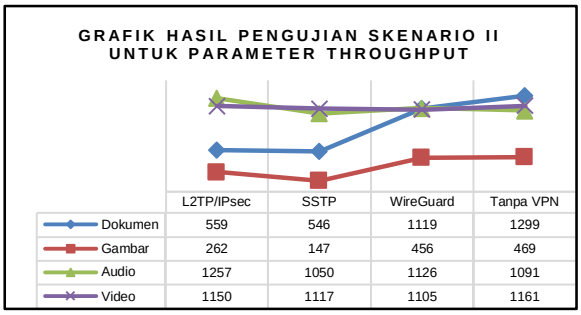


	L2TP/IPsec	SSTP	WireGuard	Tanpa VPN
Dokumen	12.935	16.044	3.235	2.105
Gambar	28.778	48.286	14.804	14.699
Audio	3.007	8.483	4.601	4.925
Video	4.739	6.955	5.112	3.76

Gambar 4. Nilai Rata-Rata Hasil Pengujian Skenario II Parameter *Jitter*

Pada Gambar 4 yang merepresentasikan hasil pengujian transmisi dokumen, gambar, audio, dan video dalam menguji parameter *jitter* dapat dilakukan analisis yaitu Protokol L2TP/IPsec menunjukkan keunggulan dalam parameter *jitter* pada berkas audio, gambar, dan video, sementara WireGuard unggul pada berkas dokumen. Sebaliknya, SSTP tidak lebih unggul dibandingkan dengan protokol VPN lainnya atau tanpa VPN di semua jenis berkas. Pengujian tanpa VPN memberikan hasil terbaik dalam transmisi dokumen, gambar, dan video. Secara keseluruhan, nilai *jitter* pada seluruh pengujian ini dikategorikan "sangat baik" menurut standar TIPHON dengan nilai *jitter* di bawah 75 ms.

Dalam melakukan pengujian *packet loss* menunjukkan hasil sebesar 0% pada seluruh pengujian, yang berarti seluruh paket terkirim dan diterima secara lengkap dan menurut standar TIPHON berkategorikan “Sangat Baik”. Hal ini disebabkan oleh beberapa faktor, yaitu pengujian dilakukan di lingkungan virtual yang menyebabkan kestabilan transmisi data dan tidak adanya interferensi jaringan fisik. Selain itu, mesin *host* atau perangkat keras yang menjalankan GNS3 memiliki sumber daya yang memadai, baik CPU maupun RAM, sehingga mendukung pengiriman paket dengan baik. Pada pengujian ini juga, topologi pengujian yang dirancang tidak kompleks atau hanya menggunakan satu hop, tanpa melibatkan *multiple hops*, sehingga mendukung pengiriman seluruh paket secara sempurna.



	L2TP/IPsec	SSTP	WireGuard	Tanpa VPN
Dokumen	559	546	1119	1299
Gambar	262	147	456	469
Audio	1257	1050	1126	1091
Video	1150	1117	1105	1161

Gambar 5. Nilai Rata-Rata Hasil Pengujian Skenario II Parameter *Throughput*

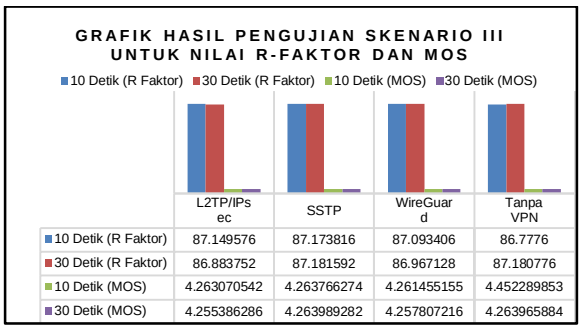
Pada Gambar 5 yang merepresentasikan hasil pengujian transmisi dokumen, gambar, audio, dan video dalam menguji parameter *throughput* dapat dilakukan analisis sebagai berikut. Hasil pengujian menunjukkan bahwa L2TP/IPsec unggul dalam *throughput* untuk berkas audio dan video, sementara WireGuard unggul dalam *throughput* untuk berkas dokumen dan gambar. SSTP tidak menunjukkan keunggulan dalam *throughput* dibandingkan dengan protokol VPN lainnya atau tanpa VPN pada semua jenis berkas. Pengujian tanpa VPN unggul dalam *throughput* untuk transmisi dokumen, gambar, dan video. Berdasarkan standar TIPHON, *throughput* untuk dokumen dan gambar bervariasi dari kategori "Buruk" hingga "Baik", sementara audio dan video sebagian besar berada dalam kategori "Normal" hingga "Baik".

Hasil pengujian menunjukkan bahwa *delay* dan *jitter* memiliki pengaruh yang berbeda terhadap kualitas jaringan. Meskipun *delay* yang tinggi namun stabil tidak selalu menyebabkan *jitter* tinggi, *jitter* lebih terkait dengan ketidakstabilan waktu pengiriman paket daripada besar-kecilnya *delay*. Dalam pengujian ini, ditemukan bahwa *delay* tinggi dapat disertai *jitter* rendah jika variasi antar *delay* paket kecil. *Jitter* yang tinggi dapat menyebabkan *packet loss* karena variasi dalam pengiriman paket, namun dalam pengujian ini, semua nilai *delay* dan *jitter* berkategori "Sangat Baik," sehingga *packet loss* mencapai 0% dan semua paket terkirim dengan sempurna. Meskipun demikian, *packet loss* dapat mempengaruhi *throughput*, karena paket yang hilang perlu dikirim ulang, yang dapat mengurangi efisiensi jaringan. Meskipun *delay*, *jitter*, dan *packet loss* berkategori "Sangat Baik," *throughput* tidak selalu optimal karena keterbatasan GNS3 sebagai lingkungan virtual yang tidak dapat mereplikasi performa perangkat keras sebenarnya. Dalam konteks ini, protokol L2TP/IPsec terbukti unggul dalam

transmisi berkas berukuran besar, seperti audio dan video, sesuai dengan penelitian lain yang mendukung hasil ini.

Namun, ketika dibandingkan dengan transmisi berkas tanpa VPN, hasil menunjukkan kinerja yang lebih cepat dan *throughput* yang lebih tinggi tanpa VPN, meskipun aspek keamanan menjadi lebih rentan tanpa adanya enkripsi. Dari pengujian ini, dapat disimpulkan bahwa protokol VPN yang direkomendasikan untuk transmisi dokumen dan gambar adalah WireGuard, diikuti oleh L2TP/IPsec, dan kemudian SSTP. Sementara itu, untuk audio dan video, L2TP/IPsec lebih unggul, diikuti oleh WireGuard, dan kemudian SSTP. Secara keseluruhan, WireGuard dan L2TP/IPsec menunjukkan hasil yang hampir sebanding, dengan WireGuard menunjukkan sedikit keunggulan dalam beberapa aspek. Penelitian ini menegaskan bahwa pemilihan protokol VPN harus disesuaikan dengan jenis berkas yang dikirim untuk mencapai performa yang optimal.

4.3 Hasil Pengujian dan Perhitungan Skenario III



	L2TP/IPsec	SSTP	WireGuard	Tanpa VPN
10 Detik (R Faktor)	87.149576	87.173816	87.093406	86.7776
30 Detik (R Faktor)	86.883752	87.181592	86.967128	87.180776
10 Detik (MOS)	4.263070542	4.263766274	4.261455155	4.452289853
30 Detik (MOS)	4.255386286	4.263989282	4.257807216	4.263965884

Gambar 6. Hasil Pengujian Skenario III Untuk Nilai R Faktor dan Nilai MOS

Berdasarkan pengujian *streaming* video menggunakan Web Server HTML5 Video dengan dan tanpa VPN, seluruh hasil pengujian masuk dalam kategori "Sangat Baik" dengan indeks "B" menurut standar Model ITU-T G.107. Nilai R-Faktor berada antara 79 dan 89, serta nilai MOS berkisar antara 3,9 dan 4,2. Protokol VPN SSTP unggul dibandingkan dengan protokol lainnya, baik pada video berdurasi 10 detik maupun 30 detik, dengan nilai R-Faktor dan MOS tertinggi. Pengujian menunjukkan bahwa meskipun nilai MOS dan R-Faktor tanpa VPN lebih rendah daripada dengan VPN, SSTP tetap unggul. Hasil pengujian ini didukung oleh penelitian sebelumnya yang menunjukkan keunggulan SSTP dalam *streaming* video. Dengan *delay* dan *packet loss* yang sangat rendah menghasilkan nilai R-Faktor dan MOS yang tinggi. Kesimpulannya, semakin besar nilai MOS dan R-Faktor, semakin baik kualitas video dan suara yang dirasakan pengguna, dengan SSTP sebagai protokol VPN yang paling unggul dalam pengujian ini.

4.4 Rekomendasi

Berdasarkan penelitian, rekomendasi penggunaan protokol VPN pada skenario II dan skenario III.

Tabel 8. Rekomendasi Penggunaan VPN Untuk Pengiriman Berkas dan Pemutaran Video

Protokol VPN	Dokumen	Gambar	Audio	Video	Pemutaran Video
L2TP/IPsec			☑	☑	
SSTP					☑
WireGuard	☑	☑			

Tabel 8 adalah rekomendasi penggunaan protokol VPN yang menunjukkan bahwa protokol L2TP/IPsec direkomendasikan untuk transmisi berkas berjenis audio dan video. Protokol SSTP direkomendasikan untuk pemutaran video atau *streaming* video. Terakhir, protokol WireGuard direkomendasikan untuk transmisi berkas berjenis dokumen dan gambar.

Namun sangat tidak efektif apabila pengguna melakukan pergantian protokol VPN disetiap kali ingin mengirimkan berkas yang berbeda atau ingin melakukan *streaming* video. Maka, rekomendasi untuk *streaming* video dipilih WireGuard karena perbedaan antara SSTP dan WireGuard untuk nilai R-Faktor 10 dan 30 detik yaitu 0,08041 dan 0.214464. Untuk nilai MOS 10 detik dan 30 detik yaitu 0.002311119 dan 0.006182066. Dilihat dari perbedaan selisihnya hal ini tidak signifikan atau hanya sedikit perbedaannya sehingga untuk merekomendasikan pengguna agar penggunaan protokol VPN lebih efektif dan efisien maka direkomendasikan protokol WireGuard untuk transmisi dan *streaming* video. Sehingga para pengguna tidak perlu mengkhawatirkan terkait dengan keamanan dan kenyamanan karena protokol WireGuard sudah mendukung keduanya.

5. KESIMPULAN

Berikut adalah kesimpulan yang diambil sebagai jawaban dari rumusan masalah dalam penelitian ini:

a. Pada Skenario I, WireGuard unggul dalam kecepatan transfer data dan *bandwidth*. Skenario II, L2TP/IPsec menunjukkan performa terbaik dalam transmisi audio dan video, sementara WireGuard unggul dalam transmisi dokumen dan gambar. Skenario III, SSTP mendominasi dalam streaming video dengan nilai MOS dan R-Faktor yang tinggi, menunjukkan kualitas *streaming* yang sangat baik.
b. *Delay* yang konsisten namun stabil dapat menjaga *jitter* tetap rendah, sementara *packet loss* yang rendah mendukung *throughput* tinggi. *Delay* dan *packet loss* yang rendah mendukung nilai R-Faktor dan MOS yang tinggi, menghasilkan kualitas *streaming* yang sangat baik dalam lingkungan pengujian yang stabil.
c. WireGuard direkomendasikan sebagai protokol

VPN utama karena kinerjanya yang konsisten dan efisien dalam berbagai skenario, meskipun terdapat perbedaan kinerja yang tidak signifikan dibandingkan SSTP dalam aspek R-Faktor dan MOS.

REFERENSI

[1] Z. Hamid, S. Daud, I. S. Abd. Razak, and N. Abd. Razak, "A Comparative Study between IPv4 and IPv6," *ANP Journal Of Social Sciences And Humanities*, vol. 2, no. 1, pp. 68–72, Feb. 2021, doi: 10.53797/anpjssh.v2i1.9.2021.

[2] A. Cindy, "Indonesia Masuk 3 Besar Negara dengan Kasus Kebocoran Data Terbanyak Dunia," Databoks.

[3] A. Purnama Sari and N. Kemala, "Perancangan Jaringan Virtual Private Network Berbasis IP Security Menggunakan Router Mikrotik," *Jurnal PROSISKO*, vol. 7, no. 2, 2020.

[4] gabby.kenny@wearesocial.net, "Social media use reaches new milestone," We Are Social, Jul. 2023. Available: https://wearesocial.com/us/blog/2023/07/social-media-use-reaches-new-milestone/. [Accessed: Dec. 04, 2024].

[5] P. R. Utami, "Analisis Perbandingan Quality Of Service Jaringan Internet Berbasis Wireless Pada Layanan Internet Service Provider (Isp) Indihome Dan First Media," *Jurnal Ilmiah Teknologi dan Rekayasa*, vol. 25, no. 2, pp. 125–137, 2020, doi: 10.35760/tr.2020.v25i2.2723.

[6] G. K. Ordabayeva, M. Othman, B. Kirgizbayeva, Z. D. Iztaev, and A. Bayegizova, "A systematic review of transition from IPV4 to IPV6," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Sep. 2020. doi: 10.1145/3410352.3410735.

[7] G. Lencse and Y. Kadobayashi, "Comprehensive Survey of IPv6 Transition Technologies: A Subjective Classification for Security Analysis," 2019, doi: 10.1587/transcom.E0.B.1.

[8] W. Zamalia, L. M. Aksara, and M. Yamin, "Analisis Perbandingan Performa Qos, Pptp, L2tp, Sstp Dan Ipsec Pada Jaringan Vpn Menggunakan Mikrotik," *semanTIK*, vol. 4, no. 2, pp. 29–36, 2018, doi: 10.5281/zenodo.1444898.

[9] T. T. Khoei, H. O. Slimane, and N. Kaabouch, "Cyber-Security of Smart Grids: Attacks, Detection, Countermeasure Techniques, and Future Directions," *Communications and Network*, vol. 14, no. 04, pp. 119–170, 2022, doi: 10.4236/cn.2022.144009.

[10] I. Ruslianto and U. Ristian, "Perancangan dan Implementasi Virtual Private Network (VPN) Menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Mikrotik di Fakultas MIPA Universitas Tanjungpura," *CESS (Journal of Computer Engineering System and Science)*, vol. 4, no. 1, 2019.

[11] B. Febrianto, "Perancangan dan Implementasi Jaringan VPN Dengan Metode L2TP/IPSec pada Kantor Cabang dan Kantor Pusat," *OKTAL : Jurnal Ilmu Komputer dan Science*, vol. 1, no. 7, pp. 879–885, 2022.

[12] A. M. Abdulazeez, B. W. Salim, D. Q. Zeebaree, and D. Doghramachi, "Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol," *International Journal of Interactive Mobile Technologies*, vol. 14, no. 18, pp. 157–177, 2020, doi: 10.3991/ijim.v14i18.16507.

[13] MikroTik, "MikroTik RouterOS," 2010. [Online]. Available: www.mikrotik.com

[14] GNS3, "Getting Started With GNS3." Accessed: Jan. 14, 2024. [Online]. Available: https://docs.gns3.com/docs/

[15] P. Pérez, J. Ruiz, I. Benito, and R. López, "A parametric quality model to evaluate the performance of tele-operated driving services over 5G networks," *Multimed Tools Appl*, vol. 81, no. 9, pp. 12287–12303, Apr. 2022, doi: 10.1007/s11042-021-11251-x.

[16] International Telecommunication Union, "ITU-T Series G: Transmission Systems And Media, Digital Systems And Networks International telephone connections and circuits-Transmission planning and the E-model The E-model: a computational model for use in transmission planning," 2015. [Online]. Available: http://handle.itu.int/11.1002/1000/11

[17] M. Y. Simargolang and A. Widarma, "Quality Of Service (QoS) Untuk Analisis Performance Jaringan Wireless Area Network (WLAN) Quality Of Service (QoS) For Network Performance Analysis Wireless Area Network (WLAN)," *Journal of Computing Engineering, System and Science)*, vol. 7, no. 1, pp. 162–171, 2022, [Online]. Available: www.jurnal.unimed.ac.id

[18] A. Charisma, A. D. Setiawan, G. M. Rahmatullah, and M. R. Hidayat, "Analysis Quality of Service (QoS) on 4G Telkomsel Networks In Soreang," in *IEEE*, 2019.

[19] A. Mikola, A. Sistem, J. Berbasis…, M. Sari, and K. S. Wacana, "Analisis Sistem Jaringan Berbasis QoS untuk Hot-Spot Di Institut Shanti Bhuana," *JIFOTECH (JOURNAL OF INFORMATION TECHNOLOGY*, vol. 2, no. 1, 2022, [Online]. Available: http://noc.eepis-its.edu/hotspot.php

[20] Fatoni, "Analisis Kualitas Layanan Jaringan

Intranet (Studi Kasus Universitas Bina Darma)," 2022.

[21] European Telecommunications Standards Institute, "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); General aspects of Quality of Service (QoS)," 1999. [Online]. Available: http://www.etsi.org

[22] R. FITRIYANTI, L. LINDAWATI, and A. ARYANTI, "Analisis Perbandingan Mean Opinion Score Aplikasi VoIP Facebook Messenger dan Google Hangouts menggunakan Metode E-Model pada Jaringan LTE," *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika*, vol. 6, no. 3, p. 379, Oct. 2018, doi: 10.26760/elkomika.v6i3.379.