

3.1. Analisis Kebutuhan dan Parameter Pengujian

3.1.1. Penetapan Parameter Kinerja

Parameter kinerja yang digunakan untuk mengevaluasi kedua teknologi (SD-WAN *ZeroTier* dan VPN Konvensional) difokuskan pada aspek *Quality of Service* (QoS) dan *routing*. Parameter ini adalah:

- 1) *End-to-End Delay* merupakan waktu yang dibutuhkan paket data untuk bergerak dari sumber ke tujuan. *End-to-End Delay* diukur dalam milidetik (ms).
- 2) *Delay Variation* merupakan variasi atau fluktuasi waktu tunda antara kedatangan paket yang berurutan. *Delay Variation (Jitter)* dalam satuan milidetik yang diperoleh dari menganalisis perhitungan waktu total variation delay dengan banyak paket (Nadarajah & Ba, 2025).

$$Delay Variation = \frac{total\ variation\ delay = \sum_{i=1}^n variation\ delay(delay^{i+1} - delay^i)}{total\ packet\ received} \quad (1)$$

- 3) *Packet loss Rasio* merupakan persentase paket data yang hilang atau gagal mencapai tujuan selama transmisi. Persentase kehilangan dihitung dan dibandingkan dengan ambang batas. *Packet loss Rasio* dapat dirumuskan:

$$Packet Loss Ratio = \frac{Packet\ drop}{Packet\ send} \times 100\% \quad (2)$$

- 4) *Hop count* merupakan Jumlah node atau router yang dilewati oleh paket data dari sumber ke tujuan, digunakan untuk menilai jalur terpendek *routing* kedua arsitektur.

- 5) Parameter kinerja yang digunakan untuk mengevaluasi kedua teknologi (SD-WAN *ZeroTier* dan VPN Konvensional) difokuskan pada aspek *Quality of Service* (QoS) dan *routing*. Selain itu, penelitian ini juga mengukur Beban *remote* (*traffic Utilization*) dan Penggunaan CPU (*CPU Utilization*) pada Mikrotik.

3.1.2. Standar Acuan Kinerja

Untuk memberikan penilaian objektif terhadap kinerja yang diukur, hasil penelitian akan dibandingkan dengan standar sebagai berikut:

- 1) Standar *Quality of Service* dengan menggunakan rekomendasi ITU-T Y.1541 (ITU-T, 2019) dengan kriteria Class 0 sebagai standar acuan untuk mengklasifikasikan kinerja layanan. Berdasarkan parameter pada Tabel 3.1.

Tabel 3.1 Parameter QoS (ITU-T Y.1541)

Parameter	Hasil Uji	Standar Y.1541	Keterangan
<i>End-to-End Delay</i>	- ms	≤ 100 ms (Class 0)	OK/Tidak OK
<i>Delay Variation</i>	- ms	≤ 50 ms (Class 0)	OK/Tidak OK
<i>Packet loss Ratio</i>	- %	$\leq 0.05\%$ (Class 0)	OK/Tidak OK

- 2) Standar Khusus Hop Count, karena tidak ada standar baku internasional untuk hop count, evaluasi dilakukan secara komparatif dengan membandingkan nilai yang dihasilkan oleh SD-WAN *ZeroTier* dengan VPN Konvensional. Nilai hop count yang lebih rendah dianggap menunjukkan arsitektur *routing* yang lebih pendek.

3.1.3. Alat dan Bahan Sistem *Remote*

Alat dan bahan yang digunakan dalam sistem *remote* dikelompokkan menjadi dua bagian utama: Perangkat Keras (Hardware) sebagai komponen fisik dan Perangkat Lunak (Software) sebagai sistem operasi dan tools pengujian.

3.1.4. Perangkat Keras

Perangkat keras yang digunakan berfungsi sebagai *gateway*, *router* utama RT/RW Net, dan perangkat *client* untuk simulasi akses jarak jauh dan pengujian kinerja.

Tabel 3.2 Perangkat Keras

No	Perangkat	Spesifikasi	Fungsi
1	Gateway SD-WAN	TP-Link TL-WDR4300	Bertindak sebagai gateway jaringan utama yang menjalankan firmware OpenWRT dan <i>ZeroTier</i> One untuk koneksi SD-WAN.
2	Router Utama	MikroTik RB941-2nD	Berfungsi sebagai router utama RT/RW Net untuk mengelola traffic lokal dan pembandingan (baseline) VPN Konvensional.
3	Perangkat Klien (PC)	Laptop Dell	Digunakan untuk menjalankan <i>client ZeroTier</i> , <i>client</i> VPN, dan menjalankan <i>tools</i> pengujian QoS (HTTP-Ping, Tracert).
4	Perangkat Klien (Mobile)	Redmi 14C	Digunakan untuk simulasi koneksi <i>remote access</i> melalui jaringan seluler atau Wi-Fi publik.
5	Media Transmisi	Kabel UTP Kategori 5e/6	Media penghubung fisik antar router utama dan Gateway SD-WAN.

3.1.5. Perangkat Lunak

Perangkat lunak yang digunakan mencakup sistem operasi pada gateway, aplikasi SD-WAN, dan tools yang krusial untuk pengukuran metrik kinerja.

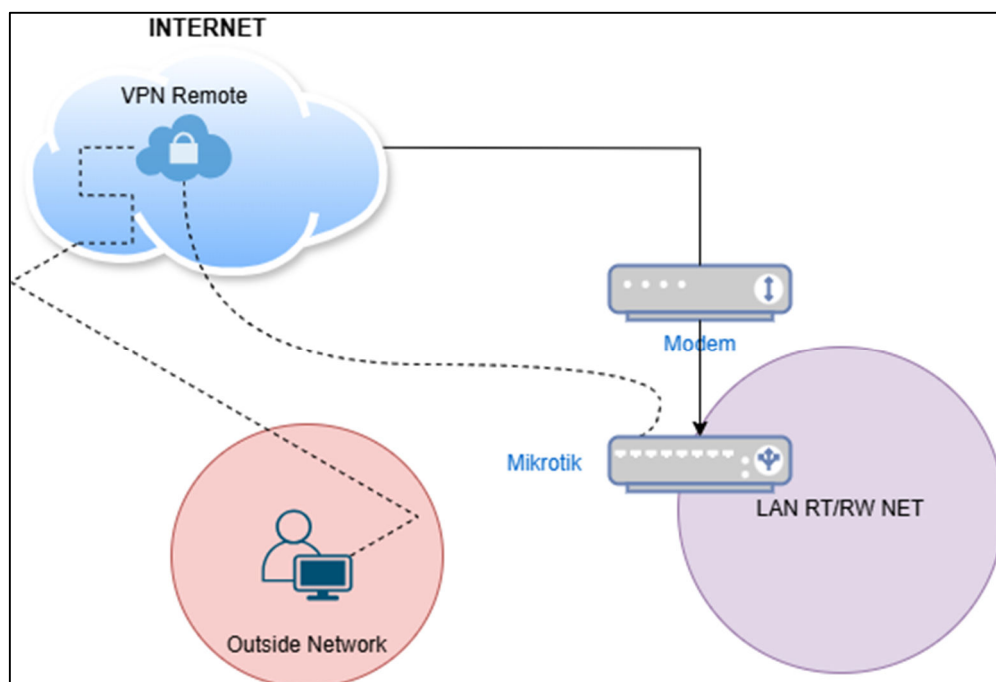
Tabel 3.3 Perangkat Lunak

No	Perangkat Lunak	Spesifikasi	Fungsi
1	Firmware Router	OpenWRT 19.07.10	Firmware dipasang pada <i>Gateway</i> TP-Link WDR4300 untuk mendukung <i>ZeroTier</i> .
2	Akun VPN <i>Remote</i>	FreeDDNS	Akun untuk layanan vpn <i>remote</i> konvensional
2	Platform SD-WAN	<i>ZeroTier</i>	Klien utama yang diinstal pada <i>gateway</i> dan <i>client</i> untuk SD-WAN virtual <i>Peer-to-peer</i> .
3	Pengukur QoS	HTTP-Ping	Digunakan untuk mengukur metrik <i>End-to-End Delay</i> (EED) dan <i>Packet loss Ratio</i> (PLR).
4	Peng analisis Jaringan	Wireshark	Digunakan untuk menganalisis dan menghitung variasi waktu antar paket (<i>Jitter</i>) serta mengamati paket data yang hilang.
5	Pengukur Hop Count	Tracert (<i>Traceroute</i>)	Digunakan untuk membandingkan jalur <i>routing</i> dengan menghitung jumlah <i>hop</i> yang dilewati oleh paket.
6	Management Network	Winbox	Digunakan manajemen jaringan, konfigurasi monitoring cpu, interface dan lain-lain untuk meremote sistem operasi RouterOS

7	Sistem Operasi Klien	Windows 11 dan Android/iOS	Platform operasi pada perangkat <i>client</i> yang digunakan untuk koneksi dan pengujian.
---	----------------------	----------------------------	---

3.2. Perancangan Sistem *Remote*

Dalam tahap ini, dilakukan perancangan dua topologi jaringan yang menjadi objek penelitian: topologi jaringan yang sedang beroperasi berbasis Layanan VPN *remote* konvensional dan topologi jaringan usulan dengan implementasi SD-WAN berbasis *ZeroTier*. Kedua desain ini dibuat untuk mencerminkan kondisi nyata jaringan RT/RW Net dan perbandingan mekanisme akses jarak jauhnya.

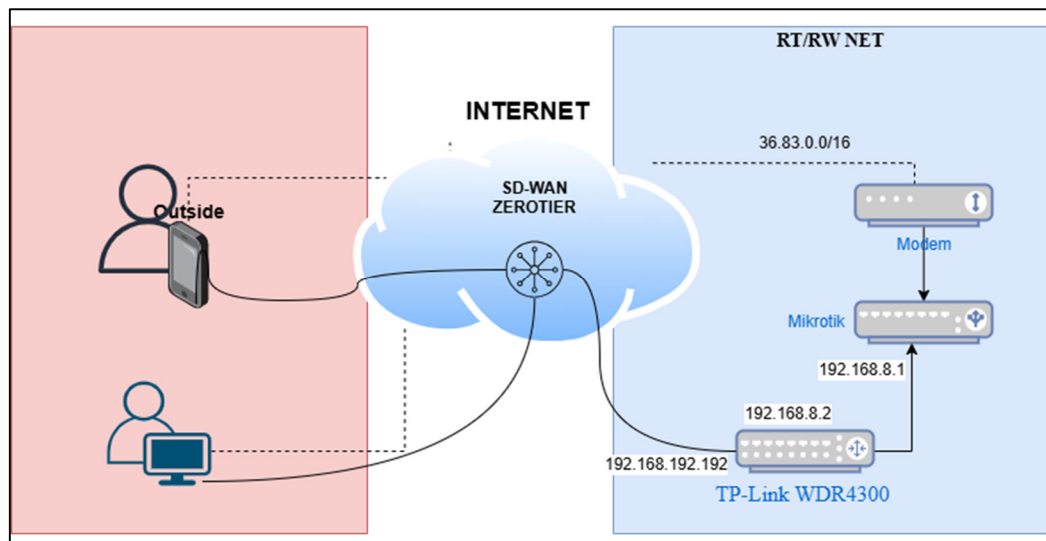


Gambar 3.2 Topologi *Remote* Layanan VPN Konvensional

Pada jaringan RT/RW Net yang sedang beroperasi saat ini, terdapat dua sumber utama layanan internet, yakni satu dari *Internet Service Provider* (ISP) berbasis kabel. Terlihat pada Gambar 3.2 untuk mengakses perangkat jaringan inti secara jarak jauh, jaringan ini memanfaatkan mekanisme *VPN Remote access* menggunakan protokol OpenVPN yang dikonfigurasi pada router utama

(MikroTik). Mekanisme ini digunakan sebagai solusi terhadap keterbatasan akses langsung akibat tidak tersedianya IP Publik Statis dari pihak ISP.

Konfigurasi jaringan ini cukup fleksibel dalam mengakomodasi berbagai kebutuhan pengguna, namun menuntut pengelolaan supaya stabil dan kualitas layanan tetap terjaga. Penggunaan VPN konvensional di sisi lain juga membawa keterbatasan dalam aspek skalabilitas dan kemudahan manajemen, terutama bagi pengelola RT/RW Net dengan sumber daya teknis terbatas.



Gambar 3.3 Topologi SDWAN ZeroTier

Sebagai solusi alternatif terhadap keterbatasan VPN konvensional, penelitian ini mengusulkan desain jaringan baru (Gambar 3.3) dengan implementasi SD-WAN berbasis *ZeroTier*. Dalam desain ini, SD-WAN *Gateway* diinstal pada perangkat TP-Link WDR4300 yang menggunakan sistem operasi OpenWRT dan diintegrasikan langsung ke jaringan lokal. Perangkat SD-WAN *Gateway* dihubungkan dengan *router* utama MikroTik menggunakan satu segmen jaringan, dengan konfigurasi alamat IP sebagai berikut:

- 1) *Router Hotspot* (RB941-2nD): 192.168.8.1/30
- 2) *SD-WAN Gateway* (TP-Link WDR4300): 192.168.8.2/30

Konfigurasi ini memungkinkan pengelola jaringan RT/RW Net untuk mengakses *router* utama tidak hanya dari dalam jaringan lokal, tetapi juga secara *remote* (jarak jauh) melalui jaringan *overlay ZeroTier* tanpa bergantung pada IP publik statis. *ZeroTier* bekerja sebagai jaringan virtual terenkripsi (virtual SD-WAN) yang membentuk konektivitas *peer-to-peer* langsung antar perangkat dengan pengalamatan jaringan privat. Implementasi ini tidak hanya menyederhanakan proses konfigurasi akses jarak jauh, tetapi juga menghadirkan fleksibilitas dalam pengelolaan jaringan, termasuk dari sisi pemantauan performa dan keamanan. Selain itu, desain ini memungkinkan evaluasi langsung terhadap kualitas layanan jaringan melalui parameter QoS, serta perbandingan mekanisme *remote access* terhadap desain Layanan VPN *Remote* yang telah ada.

3.2.1. Tahapan Konfigurasi Sistem *Remote*

3.2.1.1. Konfigurasi VPN Konvensional

Implementasi arsitektur *remote* akses teknologi VPN Konvensional menggunakan akun vpn *remote* seperti OpenVPN dari FreeDDNS, dengan layanan *port forwarding* ke port HTTP. Pada penelitian ini Mikrotik yang digunakan adalah seri RB941-2nD.

3.2.1.2. Konfigurasi SD-WAN *SaaS ZeroTier*

Implementasi arsitektur *remote* akses teknologi SD-WAN *SaaS* menggunakan *custom firmware* pada perangkat TP-Link WDR4300, karena secara bawaan perangkat ini tidak mendukung teknologi *Software-Defined Networking* (SDN).

Oleh karena itu, digunakan OpenWRT sebagai *firmware* alternatif yang memungkinkan penerapan fitur-fitur jaringan yang lebih fleksibel. Firmware yang dipilih untuk implementasi ini adalah OpenWRT versi 19.07.10 r11427-9ce6aa9d8d, yang dipilih karena stabilitasnya serta dukungannya terhadap fitur-fitur yang diperlukan dalam penerapan SD-WAN berbasis *ZeroTier*. Langkah selanjutnya adalah instalasi, konfigurasi, autentikasi dan *routing ZeroTier*. supaya dapat berfungsi sebagai SD-WAN *Gateway* dalam jaringan RT/RW Net

3.2.1.3. Konfigurasi *Client*

Untuk VPN Konvensional tidak memerlukan konfigurasi disisi *Client* dan langsung bisa diakses melalui web browser. Sedangkan SD-WAN *SaaS ZeroTier* memerlukan aplikasi *ZeroTier* atau *ZeroTier One* do smartphone dan pengaturan di sisi *client* terlebih dahulu, supaya terhubung di dalam jaringan SD-WAN *SaaS ZeroTier*.

3.3. Prosedur pengujian dan analisis data

Prosedur pengujian kinerja dalam penelitian ini diimplementasikan melalui pendekatan eksperimental yang dieksekusi pada kondisi jaringan stabil selama masa *off-peak hours* untuk memastikan lingkungan pengujian yang bersifat deterministik dan bebas dari interferensi trafik eksternal. untuk mendapatkan data kuantitatif kinerja. Pengujian dilakukan secara komparatif pada dua arsitektur yang telah diimplementasikan, yaitu SD-WAN *ZeroTier* dan VPN Konvensional.

3.3.1. Skenario Pengujian

1. Titik Pengukuran, data dikumpulkan dari *Client* Jarak Jauh menuju *Router* utama berupa paket data HTTP berkapasitas 7062 *bytes/paket*.

2. Jumlah Pengulangan, setiap metrik kinerja diukur sebanyak 10 kali pengulangan dengan jumlah transmisi 100 paket data untuk setiap arsitektur. Pengulangan ini bertujuan untuk mendapatkan data yang valid dan mewakili variasi kondisi jaringan yang mungkin terjadi.
3. Data Representatif, Hasil dari 10 kali pengulangan akan diolah untuk mendapatkan nilai rata-rata (*mean*) yang digunakan sebagai data representatif akhir.

Prosedur Pengambilan Data *Hop count*

Pengambilan data *Hop count* bertujuan untuk membandingkan jalur *routing* antara teknologi *Peer-to-peer* SD-WAN *ZeroTier* dan *Client-Server* VPN Konvensional.

1. Client dihubungkan ke internet publik dan dikoneksikan ke *ZeroTier* Network (Skenario A).
2. *Tool* Tracert atau Traceroute dijalankan pada *client* dengan tujuan alamat web server RT/RW Net yang diakses melalui koneksi *ZeroTier*.
3. Jumlah lompatan (*hop*) yang dicatat oleh tool dicatat sebagai hasil.
4. Langkah 1 sampai 3 diulangi dengan client terhubung ke VPN Konvensional (Skenario B).
5. Proses ini diulang total 10 kali, 5 kali di PC melalui jaringan publik dan 5 kali di smartphone melalui jaringan seluler untuk mendapatkan nilai rata-rata Hop Count pada kedua arsitektur.

3.3.1.4. Prosedur Pengambilan Data *End-to-End Delay* dan *Packet loss Rasio*

Pengambilan data dilakukan secara simultan menggunakan *tool* HTTP-Ping atau perintah *ping* standar pada *client* PC yang terhubung melalui *remote access*.

1. Koneksi *remote access ZeroTier* diaktifkan pada client.
2. Client menjalankan perintah *http-ping* ke alamat IP Mikrotik di jaringan RT/RW Net. Pengaturan *ping* disesuaikan untuk mengirimkan paket data dalam jumlah yang cukup selama durasi tertentu.
3. Data nilai waktu tunda dan jumlah paket yang hilang (*lost*) dicatat untuk diolah.
4. Langkah 1 sampai 3 diulangi dengan koneksi VPN Konvensional diaktifkan.
5. Proses ini diulang sebanyak 10 kali pada kedua arsitektur untuk mendapatkan nilai rata-rata.

3.3.1.5. Prosedur Pengambilan Data *Delay Variation*

Pengambilan data *Jitter* dilakukan dengan menganalisis waktu kedatangan paket yang berurutan menggunakan *tool* Wireshark untuk akurasi yang lebih tinggi dalam kondisi jaringan berbeban.

1. Wireshark diaktifkan pada perangkat client dan server untuk menangkap paket yang dikirimkan melalui koneksi *remote access* (baik *ZeroTier* maupun VPN).
2. Data atau traffic dari HTTP-ping dikirimkan dari client ke server.
3. Proses *capture* dihentikan, dan diekspor sebagai CSV untuk dianalisis menggunakan spreadsheet lebih lanjut.
4. *Jitter* dihitung berdasarkan selisih waktu tunda antar paket yang berurutan.
5. Pengukuran ini diulang 10 kali untuk setiap arsitektur, dan nilai *Jitter* rata-rata dicatat.

3.3.1.6. Prosedur Pengambilan Data CPU dan *Traffic Winbox*

Pengambilan data *CPU Utilization* dan *Traffic Utilization* diamati selama 30 detik terhitung sejak inisiasi kondisi, dilakukan untuk menganalisis total *Overhead* pemrosesan yang ditimbulkan oleh masing-masing teknologi pada *Router MikroTik*. Pengukuran dilakukan dengan mencatat rata-rata *CPU Load* dan *Traffic* dengan kondisi pengujian pada Tabel 3.4.

Tabel 3.4 Kondisi Pengujian CPU dan *Traffic*

No.	Kondisi Pengujian	Tujuan Pengukuran
1.	IDLE (<i>Baseline</i>)	Layanan VPN & SD-WAN dimatikan, tidak ada klien lokal maupun <i>remote</i> aktif. Menentukan CPU <i>Baseline</i> , <i>Overhead</i> minimum sistem operasi.
2.	VPN Aktif (Tidak Ada <i>Traffic</i>)	Layanan VPN Konvensional dihidupkan (<i>listening</i>), tetapi tidak ada klien yang terhubung secara <i>remote</i> . Mengukur <i>Overhead</i> saat service hanya berjalan (<i>running service Overhead</i>).
3.	SD-WAN Aktif (Tidak Ada <i>Traffic</i>)	Layanan SD-WAN <i>ZeroTier</i> dihidupkan (<i>running</i>), tetapi tidak ada klien yang terhubung secara <i>remote</i> . Mengukur <i>Overhead</i> saat service hanya berjalan (<i>running service Overhead</i>).
4.	VPN Aktif & <i>Loaded</i>	Layanan VPN Konvensional aktif, dan klien <i>remote</i> terhubung serta mengirim traffic pengukuran (<i>ping</i>). Mengukur Total <i>Overhead</i> saat pemrosesan <i>remote</i> traffic saja.
5.	SD-WAN Aktif & <i>Loaded</i>	Layanan SD-WAN <i>ZeroTier</i> aktif, dan klien <i>remote</i> terhubung serta mengirim traffic pengukuran (<i>ping</i>). Mengukur Total <i>Overhead</i> saat pemrosesan <i>remote</i> traffic saja.

3.3.2. Metode Analisis Data

Metode analisis data yang digunakan dalam penelitian ini adalah pendekatan Analisis Kuantitatif Komparatif. Data mentah yang dikumpulkan dari 10 kali

pengulangan pengujian pada kedua arsitektur akan diproses melalui tiga tahapan utama: Pengolahan Matematis, Klasifikasi Standar, dan Analisis Komparatif Kritis.

3.3.2.1. Pengolahan Data Kuantitatif

Tahap awal analisis adalah pengolahan data mentah menjadi nilai representatif.

Proses ini meliputi:

1. Perhitungan Nilai Rata-Rata (*Mean*), Untuk setiap metrik kinerja pada setiap arsitektur, data dari 10 kali pengulangan akan dihitung nilai rata-rata (*mean*) untuk mendapatkan angka yang stabil dan representatif. Perhitungan rata-rata ini bertujuan untuk meminimalisir noise atau anomali data yang mungkin terjadi pada satu kali pengujian.

$$Rata - Rata \text{ Metrik} = \frac{\sum_{i=1}^{10} \text{Nilai Metrik}^{ke-i}}{10} \quad (3)$$

2. Perhitungan *Packet loss Ratio*, Nilainya akan dihitung berdasarkan perbandingan jumlah paket yang hilang dengan jumlah total paket yang dikirimkan, kemudian dikalikan 100% untuk mendapatkan persentase.

3.3.2.2. Analisis Klasifikasi Standar Kinerja

Setelah diperoleh nilai rata-rata dari masing-masing metrik QoS, nilai tersebut akan dianalisis dan diklasifikasikan menggunakan standar acuan kinerja:

1. Klasifikasi ITU-T Y.1541: Nilai rata-rata EED, *Jitter*, dan PLR dari implementasi *ZeroTier* akan dibandingkan dengan kriteria Tabel 3.1 Hasil perbandingan ini akan digunakan untuk menentukan kelas layanan yang dicapai oleh teknologi SD-WAN pada *remote* jaringan.

2. Penentuan Mutu Layanan: Hasil klasifikasi akan mengindikasikan apakah kinerja *ZeroTier* sudah memenuhi persyaratan ketat layanan real-time sesuai standar, atau hanya memenuhi kriteria layanan yang lebih rendah.

3.3.2.3. Analisis Komparatif

Tahap akhir adalah analisis mendalam yang mengintegrasikan semua temuan kuantitatif dan kualitatif untuk menjawab seluruh tujuan penelitian.

1. Perbandingan Kinerja QoS (Kuantitatif): Melakukan perbandingan secara langsung nilai rata-rata metrik kinerja antara arsitektur SD-WAN *ZeroTier* dan VPN Konvensional.
2. Analisis *Routing* (Hop Count): Hasil pengukuran Hop Count akan dibahas secara kritis. Perbedaan Hop Count antara *ZeroTier* dan VPN Konvensional akan dianalisis, menghubungkan temuan jalur dengan prinsip arsitektur *Peer-to-peer* dan Client-Server (VPN).
3. Evaluasi Implementasi Sistem (Kualitatif): Menganalisis temuan selama tahap Implementasi mengenai kemudahan instalasi, kompleksitas konfigurasi, dan fleksibilitas yang ditawarkan oleh kedua teknologi. Hal ini sangat relevan untuk konteks *remote* jaringan yang memerlukan solusi yang mudah dikelola.
4. Sintesis Kesimpulan: Menggabungkan semua hasil dari analisis QoS, Hop Count, dan faktor implementasi untuk menarik kesimpulan akhir mengenai kelayakan dan rekomendasi penggunaan SD-WAN *ZeroTier* untuk *remote* jaringan.

BAB 4

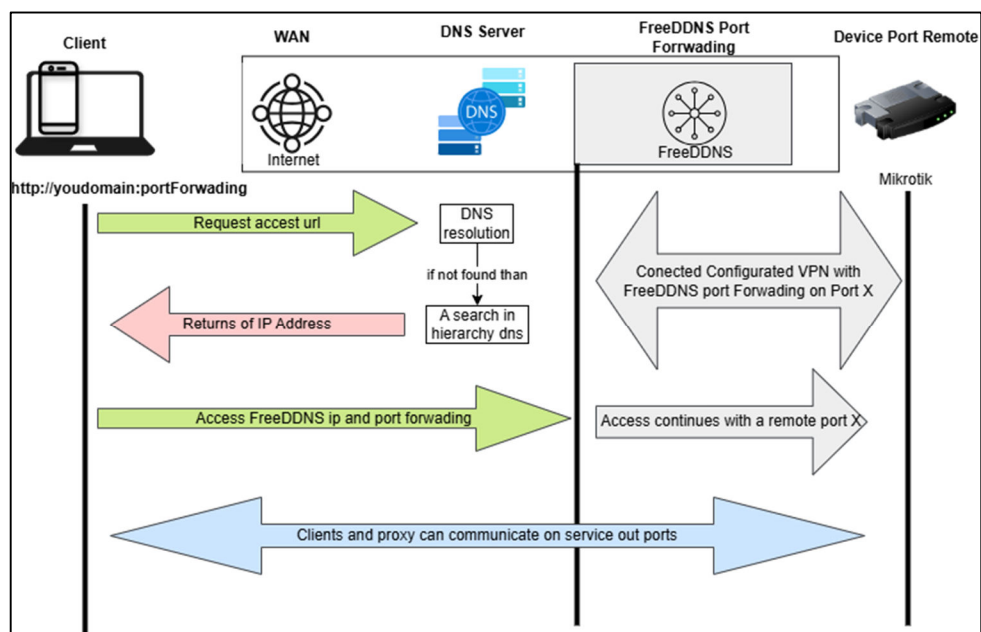
HASIL DAN PEMBAHASAN

4.1. Realisasi Sistem *Remote*

4.1.1. Arsitektur Sistem *Remote*

A. Arsitektur VPN Konvensional

Arsitektur VPN Konvensional diimplementasikan menggunakan Router MikroTik RB941-2nD sebagai VPN Server utama. Koneksi *remote access* jenis ini memerlukan pengikatan IP dinamis dengan layanan DDNS (*Dynamic Domain Name System*) dan konfigurasi NAT (*Network Address Translation*) atau *Port forwarding* pada firewall untuk mengizinkan client dari luar mengakses server. Alur koneksi pada sistem ini bersifat Client-Server, di mana semua traffic wajib melewati VPN Server terpusat.



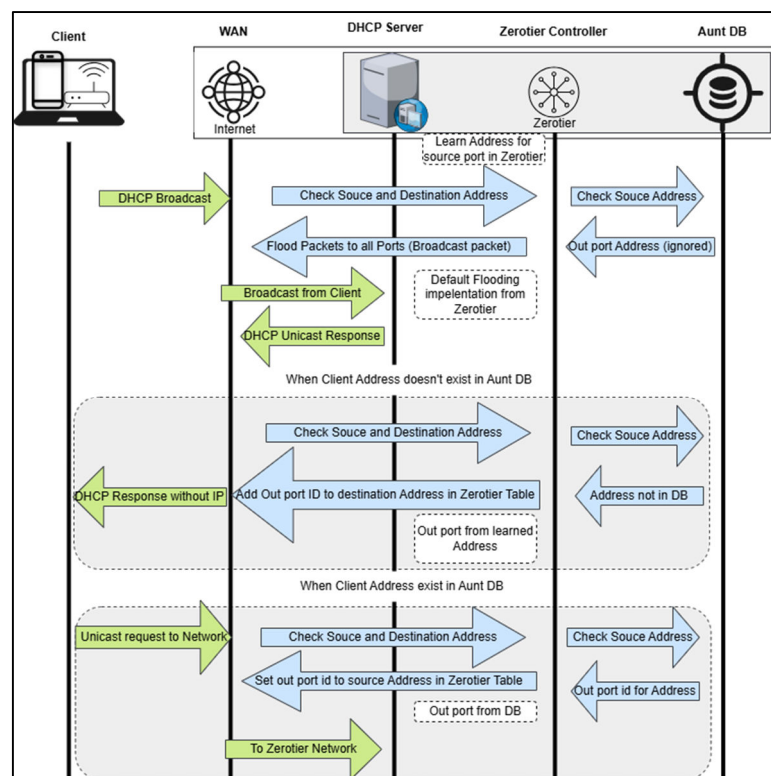
Gambar 4.1 Alur Koneksi *Remote access* Layanan VPN Konvensional

Seperti terlihat pada Gambar 4.1, paket data dari Client Jarak Jauh (Internet Publik) harus melalui banyak node (termasuk router ISP) dan VPN *Remote* sebelum

mencapai jaringan RT/RW Net. Jalur yang panjang dan terpusat ini merupakan karakteristik utama dari *routing* VPN Konvensional yang akan dievaluasi kinerjanya.

B. Arsitektur SD-WAN *ZeroTier*

Implementasi SD-WAN menggunakan platform *ZeroTier* One dengan *Gateway* berbasis *firmware* OpenWRT yang terpasang pada *router* TP-Link TL-WDR4300. *Gateway* ini berfungsi sebagai jembatan yang menghubungkan jaringan fisik RT/RW Net ke *ZeroTier Network* virtual. *ZeroTier* menggunakan arsitektur *Peer-to-peer* (P2P) yang memungkinkan *client* Jarak Jauh untuk membangun koneksi langsung ke *Gateway* tanpa memerlukan DDNS atau *Port forwarding*.



Gambar 4.2 Alur Koneksi *Remote access* Layanan SDWAN *ZeroTier*

Gambar 4.2 mengilustrasikan mekanisme yang ringkas pada *ZeroTier*, di mana *client* terhubung ke *ZeroTier* Controller hanya untuk *handshake* awal dan

otentikasi. Setelah otentikasi berhasil, koneksi data selanjutnya berusaha mencari jalur terpendek (P2P) untuk langsung terhubung dengan *Gateway* RT/RW Net. Mekanisme inilah yang diharapkan dapat mengurangi jalur *routing* (*Hop count*) dan mengurangi *latency*

4.1.2. Konfigurasi Sistem *Remote*

A. Konfigurasi VPN Konvensional

Konfigurasi VPN Konvensional diimplementasikan pada Router MikroTik RB941-2nD terlihat pada Tabel 4.1 . Konfigurasi ini memerlukan penyiapan *VPN Server*, integrasi DDNS, dan konfigurasi penerusan *port* (*Port forwarding*) untuk memastikan *server* dapat dijangkau dari internet publik.

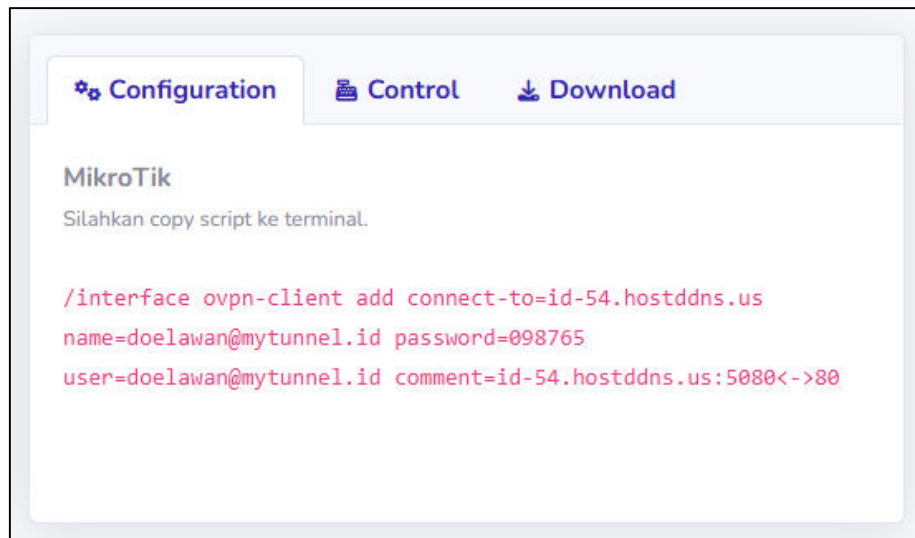
Table 4.1 Tahap Konfigurasi VPN Konvensional

No	Perangkat	Deskripsi	keterangan
1	Layanan FreeDDNS	Registrasi dan <i>Setup</i> VPN <i>Remote</i>	Membuat akun <i>remote</i> OpenVPN di FreeDDNS untuk mendapatkan nama <i>domain</i> tetap (<i>hostname</i>) dan <i>port Forwarding</i> .
2	Mikrotik	Konfigurasi untuk koneksi Interface OpenVPN Client, dan <i>Port forwarding</i>	Konfigurasi untuk koneksi OpenVPN Client ke layana FreeDDNS dan <i>port forwarding</i> ke port 80

Keberhasilan konfigurasi ini sangat bergantung pada integrasi yang tepat antara layanan pihak ketiga (FreeDDNS) dan Konfigurasi pada MikroTik. Proses yang melibatkan OpenVPN, *Port forwarding* ke Port 80.

Proses implementasi akses jarak jauh menggunakan metode VPN konvensional dilakukan dengan mengonfigurasi layanan OpenVPN pada perangkat MikroTik. Tahap pertama dimulai dengan pendefinisian kredensial pengguna agar otentikasi keamanan dapat berjalan. Gambar 4.3 menunjukkan bukti pembuatan

akun VPN *Remote* pada menu FreeDDNS, yang meliputi pengaturan username, password, serta penentuan *profil port forwarding* layanan yang digunakan.



Gambar 4.3 Bukti Pembuatan Akun VPN *Remote* Konvensional

Interface List

Interface

Interface List

Ethernet

EoIP Tunnel

IP Tunnel

GRE Tunnel

VLAN

VRRP

Bonding

LTE

+

-

✓

✗

Detect Internet

	Name	Type	Actual MTU	L2 MTU	Tx	Rx
R	WAN	Ethernet	1500	1598	910.4 kbps	21.9 Mbps
	::: id-54.hostddns.us:5080<->80					
R	doelawan@my...	OVPN Client	1500		0 bps	0 bps

Gambar 4.4 Bukti Penerapan Interface VPN *Remote* Konvensional

Setelah akun didefinisikan, dilakukan pengaktifan layanan pada sisi server agar dapat menerima permintaan koneksi dari klien. Keberhasilan penerapan konfigurasi ini dibuktikan pada Gambar 4.4, yang menampilkan status *interface VPN Remote* dalam kondisi aktif (*running*) pada perangkat MikroTik. Munculnya *interface* virtual ini memverifikasi bahwa jalur *tunneling* telah terbentuk dan siap digunakan untuk proses transmisi data. Detail parameter teknis mengenai kredensial dan alamat IP yang dialokasikan dalam tahap ini kemudian dirangkum secara sistematis pada Tabel 4.1.

B. Konfigurasi SD-WAN *ZeroTier*

Konfigurasi kunci pada arsitektur *ZeroTier* pada tabel 4.2 berfokus pada pemasangan *package* dan pengaturan *routing* pada *Gateway* TP-Link TL-WDR4300 yang menjalankan OpenWRT. Keberhasilan instalasi dan *join* ke jaringan virtual merupakan prasyarat utama.

Table 4.2 Tahap Konfigurasi SDWAN

No	Perangkat	Deskripsi	Keterangan/Nilai
1	<i>ZeroTier</i> Network ID	ID Jaringan Virtual (dibuat via <i>ZeroTier Central</i>)	network-id
2	Gateway OpenWRT	Instalasi Package Join Network dan firewall	opkg install <i>ZeroTier</i> dan <i>ZeroTier-cli</i> join network-id rules <i>ZeroTier</i> firewall
3	<i>ZeroTier Central</i>	Otorisasi dan Pemberian IP Managed, <i>Routing</i>	Otorisasi Node ID <i>Gateway</i> dan pemberian IP <i>virtual</i> statis. <i>Routing</i> ke Mikrotik



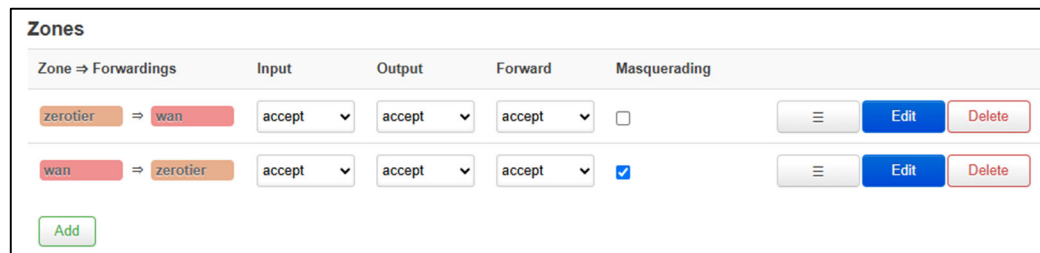
Gambar 4.5 Bukti Pembuatan *Network ID*

Implementasi SD-WAN menggunakan *ZeroTier* dilakukan melalui beberapa tahapan integrasi antara *cloud controller* dan perangkat *gateway*. Gambar 4.5 menunjukkan bukti pembuatan jaringan virtual pada panel *dashboard ZeroTier Central*, di mana *Network ID* unik dihasilkan sebagai identitas jalur komunikasi.

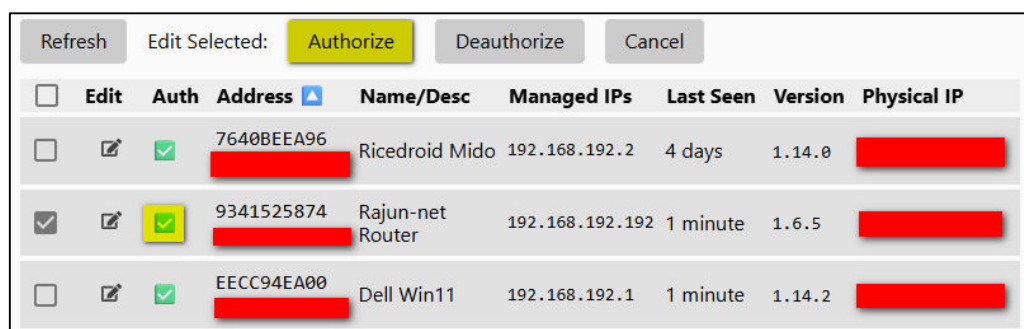


Gambar 4.6 Bukti status *ZeroTier* terinstall dan terkoneksi pada *Gateway*

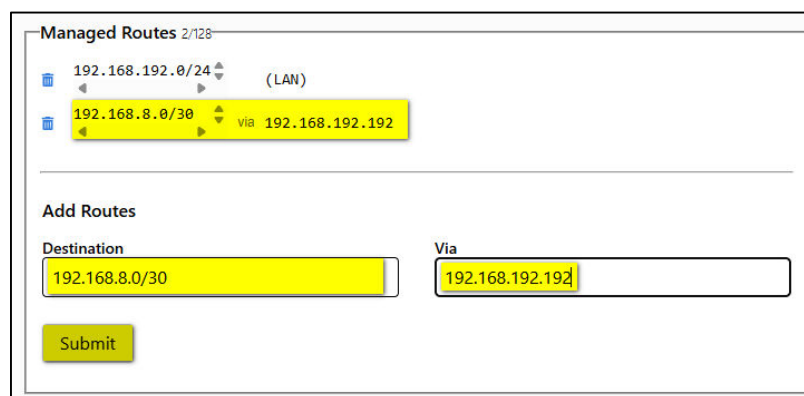
Selanjutnya, pada Gambar 4.6, terlihat proses penambahan *Network ID* tersebut ke dalam sistem Gateway Openwrt agar perangkat dapat mengenali jaringan *overlay* yang telah dibuat.

Gambar 4.7 Bukti Konfigurasi *Firewall SD-WAN Gateway*

Untuk menjamin keamanan dan kelancaran trafik, dilakukan konfigurasi pada sisi *firewall* Gateway sebagaimana ditampilkan pada Gambar 4.7. Pengaturan ini berfungsi untuk mengizinkan paket data *ZeroTier* melewati *gateway* tanpa hambatan keamanan.

Gambar 4.8 Bukti Otorisasi dan mengalamatkan *Node Gateway* dan *Client*

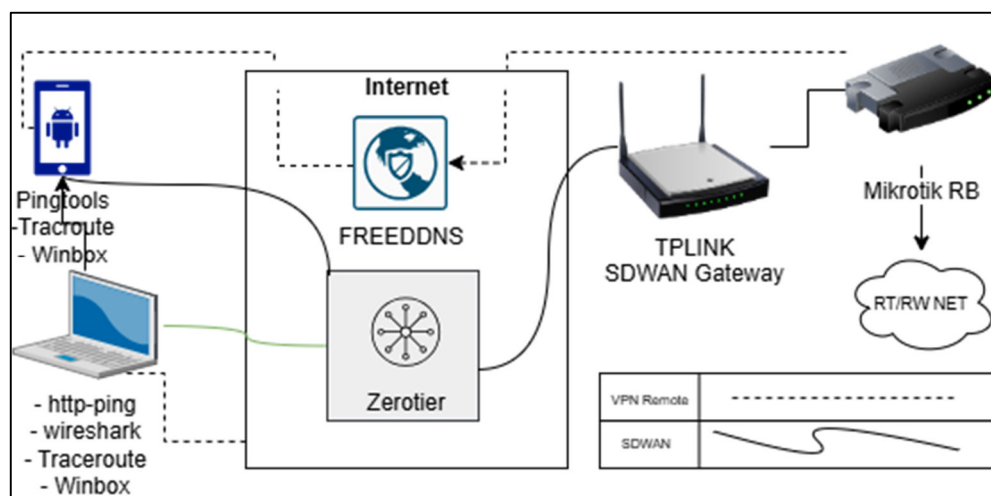
Setelah jalur terbuka, Gambar 4.8 memberikan bukti proses otorisasi serta pengalamanan IP secara dinamis bagi *node gateway* dan klien melalui *controller ZeroTier*, guna memastikan setiap simpul memiliki identitas logis yang valid.

Gambar 4.9 Bukti *Routing* ke *Network Mikrotik*

Tahap konfigurasi diakhiri dengan verifikasi jalur *routing* menuju jaringan MikroTik pada Gambar 4.9. Gambar tersebut membuktikan bahwa tabel *routing* telah terbentuk secara otomatis, sehingga komunikasi antar-jaringan lokal dapat terjalin melalui infrastruktur SD-WAN. Seluruh parameter teknis dari rangkaian bukti visual ini kemudian dirangkum secara mendalam pada Tabel 4.2.

4.2. Realisasi Pengujian

Pengujian direalisasikan pada kondisi jaringan stabil (*off-peak hours*) dengan mekanisme sebagaimana ditunjukkan pada alur topologi berikut, yang merinci titik asal koneksi hingga kondisi jaringan RT/RW Net sebagai *gateway*..



Gambar 4.10 Topologi Alur Pengujian Komparatif Kinerja SD-WAN dan VPN

Gambar 4.10 memperlihatkan bahwa:

1. Titik asal pengujian adalah Perangkat Klien Jarak Jauh (di luar jaringan RT/RW Net).
2. Target pengukuran adalah MikroTik di jaringan RT/RW Net.
3. Perbedaan utama berada pada jalur koneksi *remote access* yang diuji (garis putus-putus untuk VPN Konvensional dan garis kurva untuk *ZeroTier*).

4. Yang diukur *End-to-End Delay*, *Delay Variation*, *Packet loss* Rasio, Hop Count, Penggunaan CPU dan *Traffic Remote*.

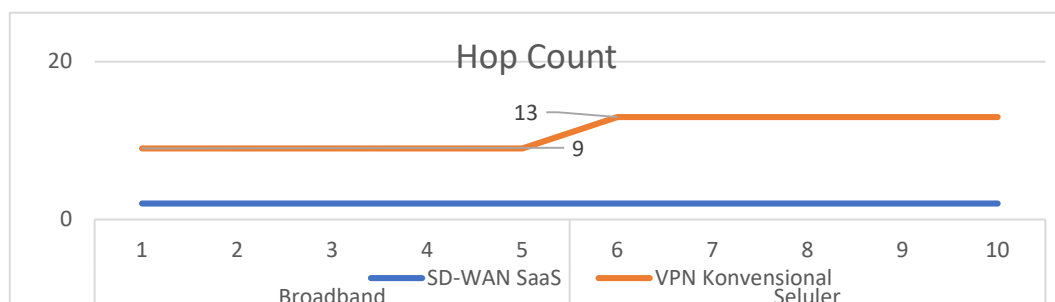
Hasil parameter disajikan berupa nilai rata-rata (*mean*) dari 10 kali pengulangan pengujian, membandingkan kinerja SD-WAN *ZeroTier* dan VPN Konvensional pada kondisi jaringan terkontrol sesuai dengan kondisi pengujian.

4.2.1. Hop count

Analisis *Hop count* dilakukan untuk mengevaluasi efisiensi jalur *routing* dengan mengalkulasi jumlah simpul (*node*) yang dilintasi oleh paket data. Kuantitas *hop count* ini menjadi indikator fundamental terhadap potensi latensi yang dihasilkan selama proses transmisi. Data hasil pengujian yang divisualisasikan pada Gambar 4.11 diolah lebih lanjut untuk mendapatkan nilai rata-rata menggunakan perhitungan matematis yang merujuk pada Persamaan 3.3. Hasil akhir dari pengolahan data tersebut kemudian dirangkum secara sistematis pada Tabel 4.1.

Tabel 4.1 Perbandingan Rata-Rata *Hop count*

No.	<i>Hop count</i>	Rata-Rata	Keterangan
1	SD-WAN <i>ZeroTier</i>	2 hop	Jalur <i>Peer-to-peer</i> (P2P)
2	VPN Konvensional	11 hop	Jalur <i>Client-Server</i> melalui <i>backbone</i> ISP



Gambar 4.11 Grafik Pengujian *Hop count*

Hasil Pengujian pada Gambar 4.11 menunjukkan perbedaan drastis pada perutean jalur. SD-WAN *ZeroTier* menghasilkan rata-rata 2 Lompatan, yang

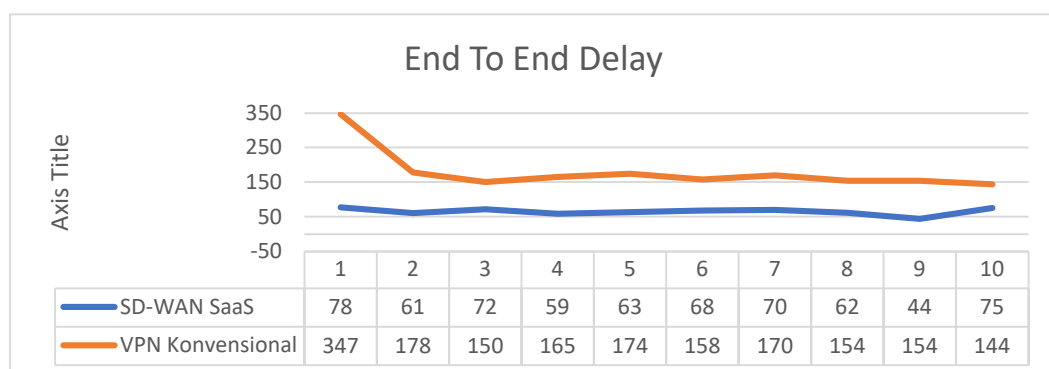
merepresentasikan pengurangan jalur sebesar 81.82% dibandingkan VPN Konvensional rata-rata 11 Lompatan. Pengurangan *hop count* yang ekstrem ini membuktikan keunggulan arsitektur *routing* P2P *ZeroTier* dalam membentuk jalur terpendek, sekaligus menjadi faktor utama penurunan *latency* akibat perbedaan mekanisme kedua teknologi yang diuraikan pada Gambar 4.1 dan Gambar 4.2.

4.2.2. End-to-End Delay

Pengujian *End-to-End Delay* (EED) mengukur total waktu transmisi paket data melalui jalur *remote access* sesuai dengan skenario. Visualisasi hasil pada Gambar 4.12 diolah lebih lanjut untuk mendapatkan nilai rata-rata menggunakan perhitungan matematis yang merujuk pada Persamaan 3.3. Hasil akhir dari pengolahan data tersebut kemudian dirangkum secara sistematis pada Tabel 4.2. Data ini menjadi dasar klasifikasi mutu layanan menurut standar ITU-T Y.1541 untuk membandingkan responsivitas antara SD-WAN dan VPN konvensional.

Tabel 4.2 Perbandingan Rata-Rata *End to end delay*

No.	<i>End-to-End Delay</i>	Rata-Rata	Standar Class 0 (≤ 100 ms)	Keterangan
1	SD-WAN <i>ZeroTier</i>	65,2 ms	Memenuhi	Mutu Sangat Baik
2	VPN Konvensional	179,4 ms	Tidak memenuhi	Mutu Class 1



Gambar 4.12 Grafik Pengujian *End to end delay*

Hasil Pengujian pada Gambar 4.12, SD-WAN *ZeroTier* berhasil memenuhi standar *End to end delay* Class 0 dengan rata-rata 65.2 ms. Sebaliknya, VPN

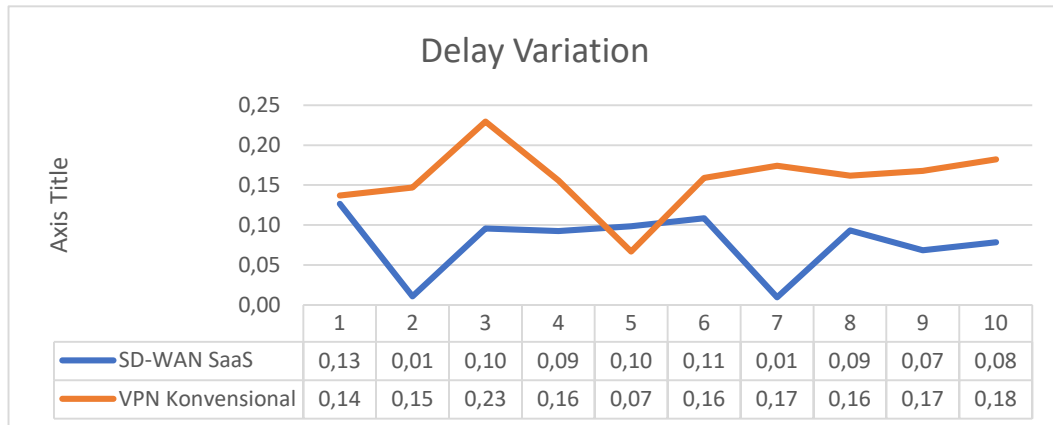
Konvensional mencatatkan rata-rata 179.4 ms, yang gagal memenuhi standar Class 0 dan hanya berada di kriteria Class 1 (≤ 150 ms) atau Class 2 (≤ 400 ms). Secara komparatif, *End to end delay* yang dihasilkan SDWAN adalah 63.66% lebih rendah daripada VPN Konvensional. Selisih yang signifikan ini membuktikan adanya korelasi langsung antara jumlah *hop count* yang rendah (dua lompatan) dengan penurunan *latency* pada mekanisme *virtual network* yang diilustrasikan pada Gambar 4.2.

4.2.3. *Delay Variation*

Analisis terhadap variabel *Delay Variation* atau yang secara teknis dikenal sebagai *Jitter* dilakukan guna mengobservasi sejauh mana fluktuasi waktu kedatangan paket data terjadi saat melintasi jalur *remote access* sesuai dengan skenario, dengan memberikan perhatian khusus pada stabilitas transmisi di tengah kondisi beban trafik jaringan yang dinamis. Visualisasi dari hasil pengukuran tersebut dipaparkan secara komprehensif melalui grafik pada Gambar 4.13, diolah lebih lanjut untuk mendapatkan nilai rata-rata menggunakan perhitungan matematis yang merujuk pada Persamaan 3.1 dan 3.3. Hasil akhir dari pengolahan data tersebut kemudian dirangkum secara sistematis pada Tabel 4.3. Parameter-parameter ini menjadi instrumen krusial dalam mengevaluasi tingkat konsistensi performa komparatif antara arsitektur SD-WAN dan VPN konvensional berdasarkan ambang batas standar ITU-T Y.1541. Hal ini dilakukan demi menjamin reliabilitas infrastruktur jaringan, terutama dalam menangani jenis trafik *real-time* yang memiliki sensitivitas tinggi terhadap ambiguitas variasi *delay* demi menjaga integritas komunikasi data.

Tabel 4.3 Perbandingan Rata-Rata *Delay Variation*

No.	<i>Delay Variation</i>	Rata-Rata	Standar Class 0 (≤ 50 ms)	Keterangan
1	SD-WAN <i>ZeroTier</i>	0,08 ms	Memenuhi	Mutu Sangat Baik
2	VPN Konvensional	0,16 ms	Memenuhi	Mutu Sangat Baik

Gambar 4.13 Grafik Pengujian *Delay Variation*

Pada grafik pengujian Gambar 4.13 Kedua arsitektur menunjukkan kinerja *Delay Variation* yang luar biasa baik, dengan keduanya berhasil memenuhi standar Class 0 (≤ 50 ms). Namun, *ZeroTier* mencapai 0.08 ms, yang 50.00% lebih stabil daripada VPN Konvensional (0.16 ms). Nilai *Jitter* yang mendekati nol pada kedua teknologi tersebut mengindikasikan bahwa pengiriman paket data berlangsung konsisten, meskipun jalur yang dilalui oleh VPN konvensional jauh lebih panjang.

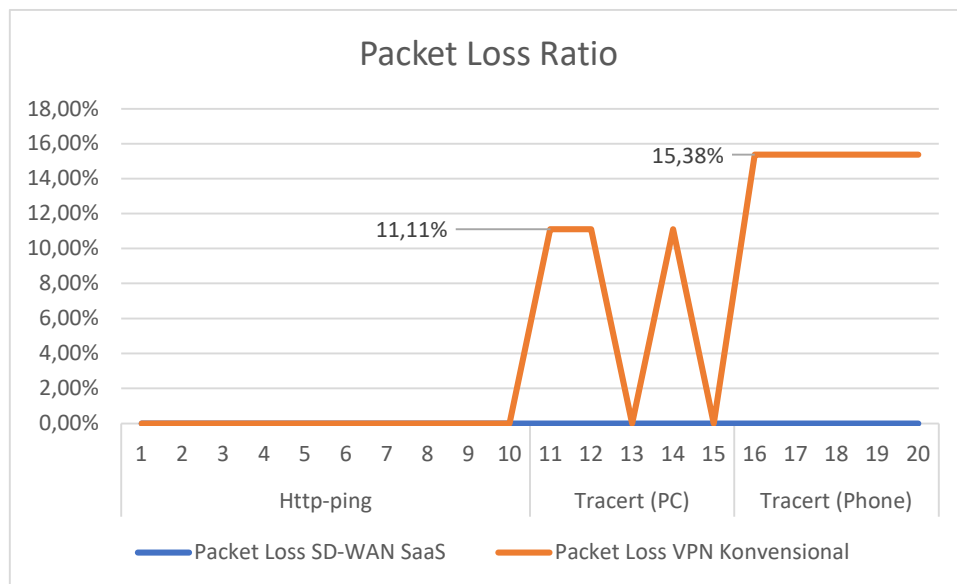
4.2.4. *Packet loss Ratio*

Pengujian *Packet loss Ratio* (PLR) mengukur persentase paket data yang hilang selama proses transmisi pada jalur *remote access*. Pengambilan data dilakukan berdasarkan skenario pada Sub-bab 3.4, yang mensimulasikan kondisi beban jaringan untuk menguji ketahanan protokol dalam menjaga integritas data. Hasil pengujian yang ditampilkan pada grafik Gambar 4.14 diolah lebih lanjut untuk mendapatkan nilai rata-rata menggunakan perhitungan matematis yang merujuk pada Persamaan 3.2 dan 3.3. Hasil akhir dari pengolahan data tersebut

kemudian dirangkum secara sistematis pada Tabel 4.4. Nilai PLR ini menjadi indikator utama untuk menentukan klasifikasi keandalan jaringan berdasarkan standar ITU-T Y.1541, guna membandingkan efisiensi mekanisme *error handling* antara teknologi SD-WAN dan VPN konvensional dalam mencegah kegagalan pengiriman paket.

Tabel 4.4 Perbandingan Rata-Rata *Packet loss Ratio*

No.	<i>Packet loss Ratio</i>	Rata-Rata	Standar Class 0 ($\leq 0.05\%$)	Keterangan
1	SD-WAN <i>ZeroTier</i>	0,00%	Memenuhi	Mutu Sangat Baik
2	VPN Konvensional	5,51%	Tidak memenuhi	Mutu (Class 4)



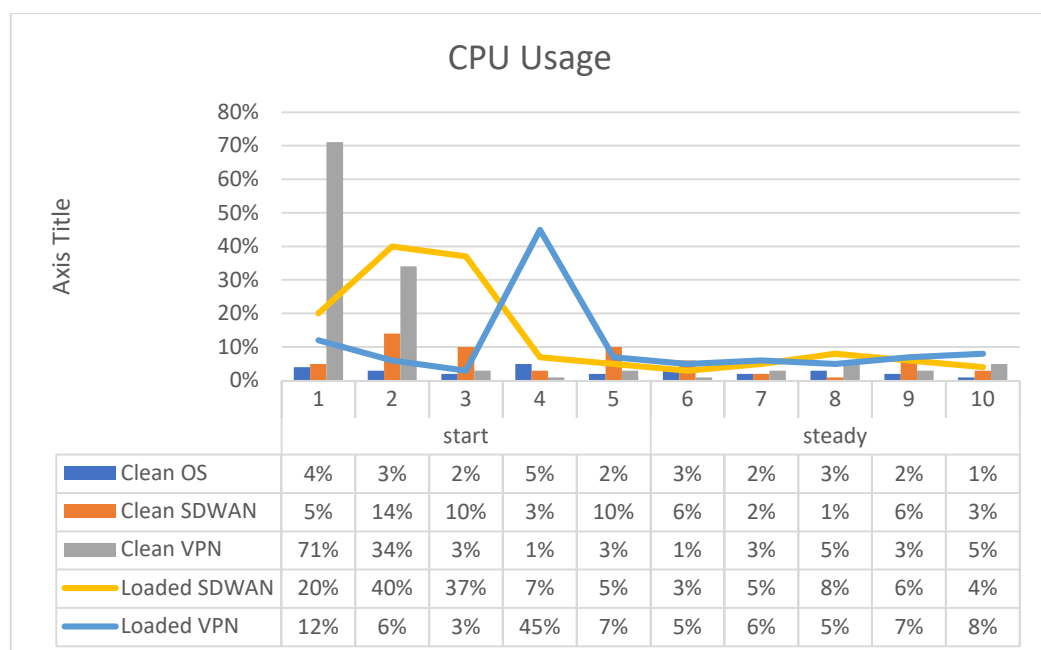
Gambar 4.14 Grafik Pengujian *Packet loss Ratio*

Hasil pengujian pada Gambar 4.14 menunjukkan perbedaan performa yang signifikan. *ZeroTier* berhasil mencapai nilai ideal 0,00%, yang secara mutlak memenuhi standar Class 0. Sebaliknya, VPN konvensional mencatatkan *packet loss* sebesar 5,51%, yang jauh melampaui batas toleransi Class 0 (0,05%) maupun Class 3 (1%). Angka kehilangan paket yang tinggi ini mengklasifikasikan kinerja VPN konvensional ke dalam Class 4. Fenomena ini membuktikan bahwa arsitektur client-server tradisional sangat rentan terhadap packet dropping akibat adanya

bottleneck pada server pusat saat jaringan mengalami kongesti. Di sisi lain, teknologi P2P pada *ZeroTier* mampu menjaga integritas data dengan membentuk jalur langsung yang lebih pendek dan efisien, sehingga meminimalisir risiko paket hilang selama proses transmisi.

4.2.5. CPU Utilization

Analisis penggunaan unit pemrosesan pusat (*CPU Utilization*) pada *router* MikroTik dilakukan melalui lima kondisi pengujian sebagaimana ditampilkan pada Gambar 4.15. Hasil rata-rata Persamaan 3.3, observasi tersebut kemudian dirangkum dalam Tabel 4.5.



Gambar 4.15 Perbandingan *Overhead* CPU: Kontribusi OS, VPN Konvensional, dan SD-WAN *ZeroTier* pada Kinerja Router

Tabel 4.5 Hasil Pengukuran Rata-Rata CPU Utilization

No.	Kondisi Uji	Rata-rata CPU
1.	IDLE	3%
2.	VPN Aktif	13%
3.	SD-WAN Aktif	6%
4.	VPN Aktif dan Loaded	10%
5.	SDWAN Aktif dan Loaded	14%

Hasil Rata CPU Usage pada Tabel 4.5 kemudian Analisis dilakukan dengan mengisolasi *Overhead* CPU Bersih yaitu beban CPU tambahan yang hanya ditimbulkan oleh proses *routing* dan enkripsi *remote access*, di luar beban *baseline* sistem operasi.

Tabel 4.6 Perbandingan *Overhead* CPU Bersih

No	Arsitektur	Rata-Rata CPU Aktif	CPU IDLE	<i>Overhead</i> CPU Bersih (%)
1.	SDWAN	14%	3%	11%
2.	VPN-Konvensional	10%	3%	7%

Data pada Tabel 4.6 menunjukkan bahwa *Overhead* CPU yang dihasilkan oleh SD-WAN *ZeroTier* sebesar 11%, secara kuantitatif lebih tinggi dibandingkan VPN konvensional yang hanya mencapai 7%. Secara persentase, beban kerja *ZeroTier* 57,14% lebih berat bagi *router* daripada VPN konvensional. Temuan ini akan dibahas lebih mendalam pada sub-bab analisis dengan mengintegrasikannya pada hasil *Traffic utilization* untuk menentukan efisiensi pemanfaatan sumber daya perangkat secara keseluruhan.

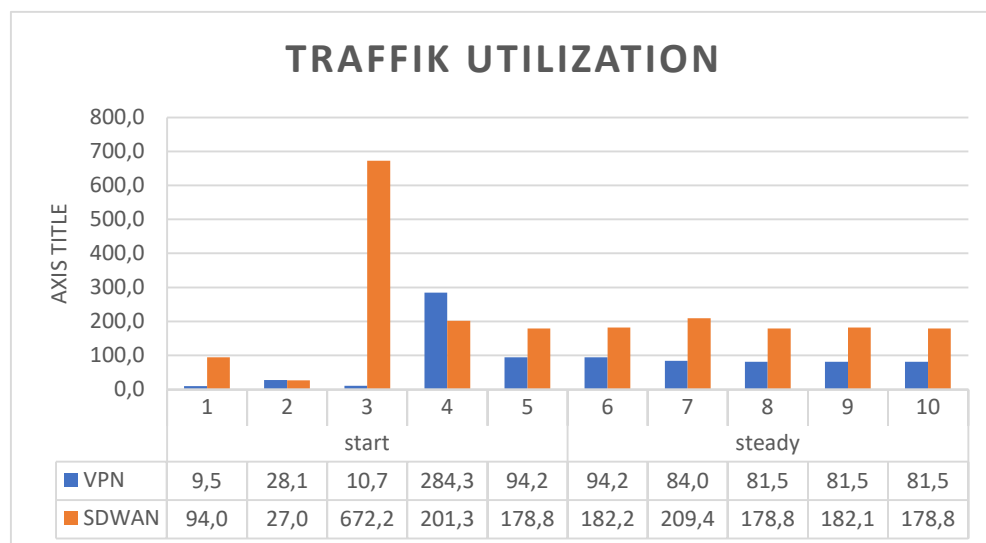
4.2.6. *Traffic utilization*

Pengukuran *Traffic utilization* dilakukan untuk memvalidasi bahwa pengujian QoS dan *Overhead* CPU berlangsung di bawah beban data yang sebanding antara VPN Konvensional dan SD-WAN *ZeroTier*. Pengambilan data dilakukan melalui fitur Traffic Monitor/Graph pada WinBox, terfokus pada *interface* virtual yang memproses koneksi *remote* di Router MikroTik melalui Winbox. Data *traffic utilization* rata-rata yang dicatat dari pengujian Net Processing *Overhead* CPU Usage terlihat pada Gambar 4.16. Data *traffic utilization* yang

dicatat (Total Tx + Rx) pada kedua kondisi awal dan stady untuk kedua arsitektur dihitung dengan Persamaan 3.3, kemudian disajikan pada Tabel 4.7.

Tabel 4.7 Hasil Pengujian *Traffic utilization*

No	Arsitektur	Start Awal	Posisi Stady	Selisih
1	SD-WAN <i>ZeroTier</i>	234.7 kbps	186.3 kbps	48.4 kbps
2	VPN Konvensional	85.4 kbps	84.5 kbps	0.82 kbps



Gambar 4.16 Perbandingan *Traffic utilization* Total: Kinerja *Peak* (Posisi *Start*) dan Rata-Rata (Posisi *Stady*) *ZeroTier* vs. VPN

Pada Gambar 4,16 Rata-rata Keseluruhan Traffic VPN Konvensional 85 kbps dan SDWAN 210,5 kbps . sedangkan pada saat inisiasi koneksi (*Start Awal*), Pada Tabel 4.7 *traffic utilization* SD-WAN *ZeroTier* mencapai *peak* 234.7 kbps, jauh lebih tinggi dibandingkan *peak* VPN Konvensional 85.4 kbps. Selisih internal antara *Start Awal* dan *Posisi Stady* pada *ZeroTier* mencapai 48.4 kbps. Selisih *traffic* yang besar ini mengindikasikan bahwa proses *path discovery* dan *handshake Peer-to-peer* (P2P) *ZeroTier* menghasilkan volume *control traffic* yang signifikan selama fase *transient* untuk menemukan jalur koneksi terpendek. Meskipun menghasilkan *Overhead* data awal yang besar, mekanisme ini efektif dalam membentuk jalur *routing* terpendek (dua *hop count*) yang berdampak pada

rendahnya *latency* . Sebaliknya, trafik VPN konvensional cenderung stabil sejak awal dengan selisih hanya 0,82 kbps. Saat mencapai kondisi operasional stabil (*steady state*), *traffic utilization* pada *ZeroTier* mencapai 186,3 kbps, sedangkan VPN konvensional hanya 84,5 kbps. Data ini menunjukkan bahwa pengujian *Quality of Service* (QoS) dan *Overhead* CPU pada *ZeroTier* dilakukan saat memproses *throughput* 2,2 kali lebih besar dibandingkan VPN konvensional. Fakta ini memperkuat argumen bahwa performa Class 0 pada *ZeroTier* dicapai di bawah beban trafik yang signifikan lebih berat. Hal ini terjadi karena *ZeroTier* mampu melayani seluruh layanan jaringan secara transparan, berbeda dengan VPN konvensional yang dalam pengujian ini hanya meneruskan satu *port* layanan tertentu.

4.3. Ringkasan Perbandingan dan Analisis Akhir

4.3.1. Kualifikasi Mutu Jaringan Berdasarkan Standar ITU-T Y.1541

Analisis ini menyajikan evaluasi gabungan semua metrik QoS yang dicapai oleh implementasi SD-WAN *ZeroTier* dan VPN Konvensional di bawah kondisi jaringan berbeban normal, dibandingkan dengan standar ITU-T Y.1541 Class 0 yang merupakan kriteria layanan *real-time* tertinggi.

Tabel 4.8 Klasifikasi Kinerja Arsitektur Berdasarkan ITU-T Y.1541 Class 0

No	Arsitektur	EED (≤ 100 ms)	Jitter (≤ 50 ms)	PLR ($\leq 0.05\%$)	QoS Class
1	SD-WAN <i>ZeroTier</i>	65.2 ms	0.08 ms	0.00%	Class 0 (Sangat Baik)
2	VPN Konvensional	179.4 ms	0.16 ms	5.51%	Hanya Class 4 (Toleran)

Klasifikasi pada Tabel 4.8 SD-WAN *ZeroTier* berhasil memenuhi seluruh kriteria Class 0. Ini membuktikan bahwa *ZeroTier* adalah solusi ideal dan layak

untuk mendukung aplikasi *real-time* yang sangat sensitif seperti VoIP dan *Video Conference* di lingkungan *remote access* RT/RW Net.

Sebaliknya, VPN Konvensional gagal total dalam memenuhi kriteria Class 0. Nilai PLR 5.51% sangat kritis karena angka ini hanya berada di kriteria Class 4 (Layanan Toleran), menjadikannya tidak andal untuk *traffic* yang membutuhkan jaminan pengiriman paket. Kegagalan ini menunjukkan bahwa mekanisme *Client-Server* tradisional kurang handal dalam menangani *traffic remote* saat jaringan RT/RW Net berada dalam kondisi berbeban.

4.3.2. Mekanisme Akses Jarak Jauh

Analisis ini berfokus pada *mengapa* SD-WAN *ZeroTier* dapat menghasilkan kinerja yang jauh lebih unggul dibandingkan VPN Konvensional.

1. Analisis terhadap korelasi *routing* dan *latency* menunjukkan bahwa perbedaan *hop count* sebesar 81,82% menjadi faktor penentu utama disparitas nilai *End-to-End Delay* (EED) antara kedua teknologi. Berdasarkan mekanisme yang diilustrasikan pada Gambar 4.1 dan Gambar 4.2, *ZeroTier* yang berbasis arsitektur *Peer-to-peer* (P2P) mampu mengeliminasi ketergantungan pada server sentral melalui proses *hole punching*. Hal ini memungkinkan *ZeroTier* membentuk jalur terpendek (2 *hop*) secara langsung antar *node*, sehingga meminimalisir *propagation delay* di setiap titik perantara. Sebaliknya, pada VPN konvensional, terjadi fenomena *hairpinning* atau *tromboning* di mana trafik dipaksa melewati 11 *hop* untuk mencapai server pusat terlebih dahulu sebelum diteruskan ke tujuan. Akumulasi *queuing delay* dan pemrosesan paket di setiap *node* perantara tersebut menyebabkan EED melonjak hingga 179,4

ms. Angka ini secara tegas berada di luar batas toleransi standar komunikasi *real-time*, membuktikan bahwa efisiensi jalur pada mekanisme P2P *ZeroTier* jauh lebih unggul dalam menjaga stabilitas transmisi data dibandingkan arsitektur *client-server* tradisional.

2. Stabilitas dan Keandalan Koneksi (*Packet loss Ratio*): Perbedaan nilai PLR yang sangat kontras antara *ZeroTier* (0,00%) dan VPN konvensional (5,51%) menjadi bukti nyata keunggulan mekanisme distribusi paket secara *Peer-to-peer* (P2P). Tingginya angka kehilangan paket pada VPN konvensional disebabkan oleh ketergantungan pada satu titik akses pusat (*centralized gateway*) yang menjadi *bottleneck* utama. Saat infrastruktur RT/RW Net mengalami kongesti atau beban trafik tinggi, server VPN pusat mengalami saturasi pada antrean paket (*buffer overflow*), yang memicu terjadinya *tail drop* atau pembuangan paket data. Sebaliknya, *ZeroTier* menggunakan mekanisme *hole punching* untuk membangun jalur komunikasi langsung antar simpul, sehingga beban trafik tidak terpusat pada satu server melainkan terdistribusi ke seluruh *node*. Melalui optimalisasi jalur L2 *overlay* ini, *ZeroTier* berhasil mengeliminasi titik kegagalan tunggal (*single point of failure*) dan menjaga integritas transmisi data tetap pada standar Class 0, bahkan dalam kondisi jaringan yang tidak stabil.
3. Efisiensi Operasional dan Fleksibilitas Akses Layanan: *ZeroTier* menawarkan keunggulan operasional yang signifikan melalui pendekatan *Zero-Configuration* dibandingkan VPN konvensional yang mengandalkan konfigurasi statis. Secara teknis, VPN konvensional dalam pengujian ini

bekerja pada *Application Layer* melalui mekanisme *Port forwarding*, yang membatasi akses klien hanya pada layanan tertentu (seperti Port 80). Hal ini menciptakan kompleksitas administratif karena setiap layanan baru memerlukan pembuatan *firewall rule* baru secara manual pada *router* MikroTik. Sebaliknya, *ZeroTier* beroperasi sebagai *Network Overlay* pada Layer 2 yang menciptakan *virtual switch* transparan, sehingga memungkinkan klien mengakses seluruh rentang alamat IP dan layanan di jaringan lokal RT/RW Net tanpa batasan *port*. Dengan mengabstraksi kerumitan *routing* fisik dan eliminasi kebutuhan pengelolaan NAT (*Network Address Translation*), *ZeroTier* memberikan skalabilitas yang jauh lebih tinggi serta mengurangi risiko *human error* dalam manajemen keamanan jaringan.

4. Analisis terhadap penggunaan sumber daya perangkat menunjukkan bahwa karakteristik operasional *ZeroTier* dan VPN konvensional memiliki perbedaan yang signifikan. Berdasarkan Tabel 4.6, *Overhead* CPU pada *ZeroTier* tercatat sebesar 11%, atau secara kuantitatif lebih tinggi dibandingkan VPN konvensional yang hanya sebesar 7%. Tingginya penggunaan CPU ini merupakan konsekuensi logis dari mekanisme *encapsulation* dan proses *encryption/decryption* P2P yang dilakukan secara terdesentralisasi oleh *router* untuk setiap *node*. Meskipun aktivitas *network overlay* dan *hole punching* ini mengonsumsi siklus CPU lebih besar, hal tersebut merupakan *trade-off* yang sepadan untuk menghasilkan *packet loss* sebesar 0,00% (Gambar 4.14). Dari sisi penggunaan *bandwidth*, *traffic utilization* *ZeroTier* mencapai 186,3 kbps, yang membuktikan kemampuannya menjalankan virtualisasi L2/L3 untuk

seluruh layanan jaringan. Fakta bahwa *ZeroTier* tetap mempertahankan standar Class 0 meskipun menangani beban trafik 2,2 kali lebih besar daripada VPN konvensional menunjukkan efisiensi penggunaan sumber daya yang jauh lebih unggul dalam menjaga integritas data di bawah beban kerja yang berat..

4.3.3. Sintesis Hasil dan Evaluasi Kinerja Komparatif

Evaluasi kinerja membuktikan bahwa arsitektur SD-WAN memberikan performa yang lebih superior, terutama dalam meminimalkan latensi dan *packet loss*. Terkait penggunaan sumber daya, *overhead* CPU SDWAN yang mencapai 11% (lebih tinggi 57,14% dari VPN konvensional) serta pemakaian trafik yang lebih besar merupakan konsekuensi logis dari kapabilitas layanan yang ditawarkan. Berbeda dengan VPN Konvensional yang terbatas pada akses *port* spesifik melalui *port forwarding*.. Beban ekstra tersebut merupakan investasi teknis yang sebanding untuk menjamin integritas transmisi data serta fleksibilitas operasional pada kondisi jaringan yang dinamis. Perbandingan menyeluruh dari parameter yang diuji disajikan dalam Tabel 4.9 berikut:

Tabel 4.9 Sintesis Hasil Pengujian dan Matriks Kinerja Komparatif

No.	Kriteria Perbandingan	SD-WAN <i>ZeroTier</i>	VPN Konvensional
1	Arsitektur Jaringan	<i>Peer-to-peer</i> (P2P)	Client-Server
2	QoS - EED	65.2 ms	179.4 ms
3	QoS - <i>Jitter</i>	0.08 ms	0.16 ms
4	QoS - PLR	0.00%	5.51%
5	QoS - ITU-T Y.1541	Class 0	Class 4
6	Hop Count	2 <i>Hop</i>	11 <i>Hop</i>
7	<i>Traffic Remote</i>	210,5 kbps	85 kbps
8	<i>Overhead</i> CPU	11%	7%
9	Mekanisme Akses	IP Virtual <i>ZeroTier</i> (Akses hanya di jaringan <i>ZeroTier</i>)	<i>Domain</i> DDNS dan Port Publik (Akses terbuka di publik)
10	Lingkup Layanan Akses	Akses semua layanan Network	Layanan Spesifik Terbatas (Hanya yang di Forward)

Berdasarkan data komparatif pada Tabel 4.9, dapat dianalisis bahwa perbedaan performa yang signifikan antara kedua teknologi berakar pada efisiensi arsitektur jaringan yang digunakan. Keunggulan SD-WAN ZeroTier dalam mencapai klasifikasi *Class 0* (Excellent) menurut standar ITU-T Y.1541 merupakan implikasi langsung dari mekanisme *hole punching* yang membentuk jalur *peer-to-peer* (P2P). Jalur ini secara drastis mereduksi jumlah lompatan (*hop count*) hingga 81,82%, sehingga meminimalkan probabilitas terjadinya kongesti dan *packet loss* yang sering ditemukan pada arsitektur tersentralisasi seperti VPN Konvensional.

Lebih lanjut, analisis terhadap penggunaan sumber daya menunjukkan bahwa *overhead* CPU sebesar 11% pada SD-WAN merupakan investasi performa. Meskipun secara angka lebih tinggi dibandingkan VPN konvensional, beban kerja tersebut dialokasikan untuk manajemen *virtual switch* Layer 2 dan enkripsi yang jauh lebih komprehensif. Hal ini memberikan nilai tambah berupa fleksibilitas akses seluruh layanan jaringan (bukan sekadar *port* spesifik) serta stabilitas transmisi data yang 2,2 kali lebih andal. Dengan demikian, SD-WAN ZeroTier membuktikan efektivitasnya sebagai solusi *remote access* yang superior untuk infrastruktur jaringan dengan sumber daya terbatas namun membutuhkan kualitas layanan yang terjaga.

BAB 5

SIMPULAN DAN SARAN

5.1. Simpulan

Berdasarkan hasil implementasi, pengujian, dan analisis kinerja komparatif antara teknologi SD-WAN dan VPN konvensional untuk akses jarak jauh (*remote access*), dapat ditarik tiga simpulan utama sebagai berikut:

1. SD-WAN memenuhi kriteria mutu layanan *real-time* tertinggi (ITU-T Y.1541 Class 0), sedangkan VPN konvensional gagal memenuhi standar tersebut. Seluruh metrik QoS SDWAN menunjukkan performa superior dengan rata-rata EED 65,2 ms, *Jitter* 0,08 ms, dan PLR 0,00%. Sebaliknya, VPN konvensional hanya mencapai kriteria Class 2 untuk EED (179,4 ms) dan Class 4 untuk PLR (5,51%). Secara teknis, pencapaian Class 0 pada SDWAN dimungkinkan oleh pengiriman paket yang meminimalkan *queuing delay* dan *packet dropping* melalui arsitektur yang tidak terpusat pada satu *gateway*.
2. SD-WAN *ZeroTier* secara mutlak lebih unggul dalam efisiensi *routing* dan stabilitas koneksi dibandingkan VPN konvensional. SDWAN hanya memerlukan 2 *hop* untuk mencapai tujuan, jauh lebih efisien dibandingkan VPN konvensional yang menempuh 11 *hop*. Keunggulan ini didasari oleh mekanisme *hole punching* yang membentuk jalur langsung antar simpul, sehingga berhasil mengeliminasi fenomena *hairpinning* (jalur memutar ke server pusat) yang menjadi penyebab

utama lonjakan *latency* dan kerentanan koneksi pada VPN tradisional saat jaringan RT/RW Net mengalami kongesti.

3. Penggunaan sumber daya CPU pada SD-WAN SDWAN terbukti lebih efektif dalam menjamin mutu layanan meskipun memiliki *Overhead* yang lebih tinggi. Walaupun *Overhead* CPU bersih SDWAN (11%) secara kuantitatif 57,14% lebih tinggi dari VPN konvensional (7%), beban ini merupakan investasi teknis yang produktif karena SDWAN 28,7% lebih handal dalam memproses *throughput* per alokasi siklus CPU. Beban ekstra tersebut digunakan untuk menjalankan fungsi *virtual switch* Layer 2 dan enkripsi P2P yang lebih intensif, yang secara teknis terbukti mampu menjaga stabilitas layanan pada beban trafik 2,2 kali lebih besar tanpa mengorbankan integritas data.

Secara keseluruhan, penelitian ini menyimpulkan bahwa teknologi SD-WAN merupakan solusi yang sangat layak dan direkomendasikan untuk implementasi akses jarak jauh. Keunggulannya terbukti melalui kemampuan menyediakan jalur transmisi yang andal dengan efisiensi *routing* sebesar 81,82% melalui jalur *peer-to-peer*. Meskipun memerlukan *overhead* CPU yang sedikit lebih tinggi, teknologi ini secara superior mampu menjamin mutu layanan pada klasifikasi *Class 0 (Excellent)* sesuai standar ITU-T Y.1541, menjadikannya infrastruktur yang jauh lebih stabil dan adaptif dibandingkan solusi konvensional dalam menghadapi kondisi jaringan yang dinamis.

5.2. Saran

Berdasarkan penelitian yang telah dilakukan, terdapat beberapa saran yang dapat diajukan sebagai masukan untuk pengembangan lebih lanjut di masa mendatang:

1. Pengujian dengan Beban Jaringan yang Berbeda: Penelitian selanjutnya dapat mengevaluasi kedua teknologi ini pada kondisi jaringan yang bervariasi, seperti kondisi *idle* (tanpa beban), beban sangat tinggi (misalnya, saat *video streaming* masal), atau saat terjadi kemacetan (*congestion*) yang signifikan.
2. Evaluasi Kinerja pada Jaringan dengan Jarak Geografis yang Lebih Jauh: Pengujian dapat dilakukan dengan titik klien yang berada di luar kota atau bahkan di luar negeri untuk melihat bagaimana kinerja kedua teknologi dipengaruhi oleh *latency* dan hop count yang jauh lebih tinggi.
3. Analisis Skalabilitas: Penelitian dapat mengevaluasi bagaimana kinerja *ZeroTier* dipengaruhi oleh penambahan jumlah *node* atau klien yang sangat besar, untuk melihat batas skalabilitas dari arsitektur *Peer-to-peer* pada lingkungan RT/RW Net yang terus berkembang.
4. Studi Komparatif dengan Teknologi SD-WAN Lain: Penelitian dapat membandingkan *ZeroTier* dengan teknologi SD-WAN lain yang memiliki fitur serupa, seperti Twingate atau Tailscale, untuk memberikan analisis yang lebih komprehensif.

DAFTAR PUSTAKA

- Akinsanya, M. O., Ekechi, C. C., & Okeke, C. D. (2024). Theoretical Underpinnings and Practical Implications of Sd-Wan Technologies in Telecommunications. *Computer Science & IT Research Journal*, 5(4), 950–971. <https://doi.org/10.51594/csitrj.v5i4.1082>
- Al Mukasyah, M. B., & Yulianton, H. (2024). Analisa Penggunaan *ZeroTier* pada Jaringan RT/RW Net dengan Metode *Quality of Service*. *Progresif: Jurnal Ilmiah Komputer*, 20(1), 477. <https://doi.org/10.35889/progresif.v20i1.1784>
- Ausavarungnirun, R., & Mutlu, O. (2022). The design of an energy-efficient deflection-based on-chip network. *Advances in Computers*, 124, 257–318. <https://doi.org/10.1016/BS.ADCOM.2021.12.002>
- FreeDDNS*. (2025). Mexious Teknologi Indonesia. <https://www.hostddns.us/vpn-remote>
- Govender, P., Ogudo, K. A., & Chabalala, C. (2023). EXPLORING THE POTENTIAL OF DYNAMIC *QUALITY OF SERVICE* CLOUD-BASED NETWORK SLICING IN 5G AND NEXT GENERATION VIRTUALIZED NETWORKS: A SIMULATION-BASED STUDY. *ITU Journal on Future and Evolving Technologies*, 4(2). <https://www.itu.int/en/journal/jfet/Pages/default.aspx>
- Hadinata, F., Prasetyo, S. E., & Haeruddin, H. (2022). Analisa Penggunaan Jaringan *ZeroTier* di Masa Pandemi Covid-2019. *Jurnal Ilmu Komputer dan Bisnis*, 13(1), 85–93. <https://doi.org/10.47927/jikb.v13i1.276>

- ITU-T. (2019). *Network performance objectives for IP-based services*. ITU-T Publications. https://www.itu.int/rec/T-REC-Y.1541/?utm_source=chatgpt.com
- Marsela, A., Khairil, & Aspriyono, H. (2024). Penerapan *ZeroTier* Dalam Membangun File Server Pada Kantor Desa Dusun Baru II Kabupaten Bengkulu Tengah. *Jurnal Penelitian Rumpun Ilmu Teknik*, 3(1), 111–120. <https://doi.org/10.55606/juprit.v3i1.3183>
- Martín, & Josué. (2024). An Assessment of Voice Quality and QoS in Real VoIP Calls Using Multiple Voice Codecs. *Proceedings IMCIC - International Multi-Conference on Complexity, Informatics and Cybernetics, 2024–March*(Imcic), 79–88. <https://doi.org/10.54808/IMCIC2024.01.79>
- Nadarajah, S., & Ba, A. (2025). *On the analytical model for Jitter*. July, 1–4. <https://doi.org/10.3389/frcmn.2025.1602095>
- OpenWRT Project. (2023). *[OpenWRT Wiki] Welcome to The OpenWRT Project*. [Https://Openwrt.Org/](https://Openwrt.Org/). <https://openwrt.org/start>
- Putra, T. G. S., & Wideasari, I. R. (2022). Rancangan Virtual Private Server Pada Kantor Kelurahan Menggunakan *ZeroTier*. *Building of Informatics, Technology and Science (BITS)*, 4(2), 352–360. <https://doi.org/10.47065/bits.v4i2.1810>
- Rad, F., Reshadi, M., & Khademzadeh, A. (2020). A survey and taxonomy of congestion control mechanisms in wireless network on chip. *Journal of Systems Architecture*, 108, 101807.

<https://doi.org/10.1016/J.SYSARC.2020.101807>

ZeroTier. (2025). ZeroTier | Global Networking Solution for IoT, SD-WAN, and VPN. <https://www.ZeroTier.com/>

LAMPIRAN

Lampiran 1 Surat Keterangan Tugas Akhir



KEMENTERIAN PENDIDIKAN TINGGI, SAINS,
DAN TEKNOLOGI
UNIVERSITAS SILIWANGI

Jalan Siliwangi Nomor 24 Kota Tasikmalaya Kode Pos 46115
Jalan Mugarasari Kecamatan Tamansari 46146
Telepon (0265) 330634, 333092 Faksimile (0265) 325812
Laman: www.unsil.ac.id Posel: info@unsil.ac.id

KEPUTUSAN REKTOR UNIVERSITAS SILIWANGI
NOMOR : 3721/UN58/P.TA/2025
TENTANG
PEMBIMBING SKRIPSI/TUGAS AKHIR
MAHASISWA PROGRAM STUDI INFORMATIKA FAKULTAS TEKNIK UNIVERSITAS SILIWANGI

REKTOR UNIVERSITAS SILIWANGI,

Menimbang : a. Bahwa untuk kelancaran dalam pelaksanaan penyusunan dan penulisan Skripsi/Tugas Akhir bagi mahasiswa Program Studi Informatika Fakultas Teknik Universitas Siliwangi, perlu menunjuk Dosen Pembimbing.
b. bahwa untuk kepentingan tersebut diatas, perlu mempertimbangkan Keputusan Rektor Universitas Siliwangi tentang Pembimbing Skripsi/Tugas Akhir Mahasiswa Program Studi INFORMATIKA FAKULTAS TEKNIK Universitas Siliwangi;

Mengingat : 1. Undang-Undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 78, Tambahan Lembaran Negara Republik Indonesia Nomor 4301);
2. Undang-Undang Nomor 12 Tahun 2012 tentang Pendidikan Tinggi (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 158, Tambahan Lembaran Negara Republik Indonesia Nomor 5336);
3. Peraturan Pemerintah Nomor 4 Tahun 2014 tentang Penyelenggaraan Pendidikan Tinggi dan Pengelolaan Perguruan Tinggi (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 16, Tambahan Lembaran Negara Republik Indonesia Nomor 5500);
4. Peraturan Presiden Nomor 24 Tahun 2014 tentang Pendirian Universitas Siliwangi (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 64);
5. Peraturan Menteri Pendidikan, Kebudayaan, Riset, dan Teknologi Nomor 19 Tahun 2023 tentang Organisasi dan Tata Kerja Universitas Siliwangi (Berita Negara Republik Indonesia Tahun 2023 Nomor 153);
6. Peraturan Menteri Pendidikan, Kebudayaan, Riset, dan Teknologi Nomor 27 Tahun 2024 tentang Statuta Universitas Siliwangi (Berita Negara Republik Indonesia Tahun 2024 Nomor 391);

MEMUTUSKAN

Menetapkan : KEPUTUSAN REKTOR UNIVERSITAS SILIWANGI TENTANG PEMBIMBING SKRIPSI/TUGAS AKHIR MAHASISWA PROGRAM STUDI INFORMATIKA FAKULTAS TEKNIK UNIVERSITAS SILIWANGI.

KESATU : Menunjuk kepada yang namanya tersebut di bawah ini,
Pembimbing I : **Rohmat Gunawan, 7941758659131162**
Pembimbing II : **Firmansyah Maulana Sugiartana Nursuwars, 8537761662130203**

Sebagai Pembimbing dalam penyusunan Skripsi/Tugas Akhir, untuk mahasiswa tersebut dibawah ini,

Nama : **Doel Awan Nuri Suryadi**
NPM : **207006071**

KEDUA : Pelaksanaan bimbingan penyusunan Skripsi/Tugas Akhir dilaksanakan sesuai jadwal yang telah ditentukan

KETIGA : Dalam melaksanakan tugasnya Pembimbing bertanggung jawab kepada Dekan.

KEEMPAT : Keputusan ini berlaku sejak tanggal 18 Desember 2025 s.d 18 April 2026.

KELIMA : Apabila terdapat kekeliruan dalam Keputusan ini akan diadakan perbaikan sebagaimana mestinya.

Ditetapkan di Tasikmalaya
Pada tanggal : 4 Desember 2025
a.n Rektor
Dekan FAKULTAS TEKNIK


ARIPIN
NIP 196708161996031004

Tembusan. :
Ketua Program Studi Informatika Fakultas Teknik Universitas Siliwangi



Lampiran 2 Lembar Konsultasi Tugas Akhir



KEMENTERIAN PENDIDIKAN TINGGI, SAINS,
DAN TEKNOLOGI
UNIVERSITAS SILIWANGI
Jalan Siliwangi No.24 Kota Tasikmalaya Kode Pos 46115
Telepon (0265) 330634, 333092 Faksimili (0265) 325812
Laman : www.unsil.ac.id Posel : info@unsil.ac.id

PROGRAM STUDI INFORMATIKA
LEMBAR KONSULTASI TUGAS AKHIR/SKRIPSI

Tgl Mulai TA : 18-12-2025
Tgl Batas Akhir TA : 18-04-2026

Nama : DOEL AWAN NURI SURYADI
NPM : 207006071
Judul Tugas Akhir : EVALUASI KINERJA TEKNOLOGI SD-WAN
PADA JARINGAN RT/RW NET BERDASARKAN PENDEKATAN
QUALITY OF SERVICE

Dosen Pembimbing : Rohmat Gunawan, ST., M.T.
NIP/NIDN : 198006092021211007 / 0409058007

A. Konsultasi TA

No	Tanggal	Hasil Pemeriksaan	Perbaikan yang perlu dilakukan	Paraf Pembimbing
1	30-4-2025	BAB I	Terlampir	
2	9-5-2025	BAB I & BAB II	Terlampir	
3	3-6-2025	BAB II	Terlampir	
4	13-6-2025	BAB II & III	Terlampir	
5	9-9-2025	BAB III & IV	Terlampir	
6	22-9-2025	BAB IV	Terlampir	
7	6-10-2025	BAB IV & V	Terlampir	
8	8-10-2025	BAB V	Terlampir	

B. Siap Sidang TA :
C. Tanggal Sidang TA :

Tasikmalaya,
Dosen Pembimbing,

Rohmat Gunawan, ST., M.T.
198006092021211007

Keterangan : Lembar Konsultasi Tugas Akhir/Skripsi ini dilampirkan dalam laporan akhir Tugas Akhir



KEMENTERIAN PENDIDIKAN TINGGI, SAINS,
DAN TEKNOLOGI
UNIVERSITAS SILIWANGI
Jalan Siliwangi No.24 Kota Tasikmalaya Kode Pos 46115
Telepon (0265) 330634, 333092 Faksimil (0265) 325812
Laman : www.unsil.ac.id Posel : info@unsil.ac.id

PROGRAM STUDI INFORMATIKA
LEMBAR KONSULTASI TUGAS AKHIR/SKRIPSI

Tgl Mulai TA : 18-12-2025
Tgl Batas Akhir TA : 18-04-2026

Nama : DOEL AWAN NURI SURYADI
NPM : 207006071
Judul Tugas Akhir : EVALUASI KINERJA TEKNOLOGI SD-WAN
PADA JARINGAN RT/RW NET BERDASARKAN PENDEKATAN
QUALITY OF SERVICE

Dosen Pembimbing : Ir. Firmansyah MSN, S.T., M.Kom.
NIP/NIDN : 198312052021211001 / 0405128301

A. Konsultasi TA

No	Tanggal	Hasil Pemeriksaan	Perbaikan yang perlu dilakukan	Paraf Pembimbing
1	20-5-2025	BAB I	Tertampir	SA
2	13-6-2025	BAB I dan II	Tertampir	SA
3	23-9-2025	BAB III dan IV	Tertampir	SA
4	3-10-2025	BAB IV	Tertampir	SA
5	24-12-2025	BAB V dan VI	Tertampir	SA
6	11-12-2025	BAB VI	Tertampir	SA

B. Siap Sidang TA :
C. Tanggal Sidang TA :

Tasikmalaya,
Dosen Pembimbing,

Ir. Firmansyah MSN, S.T., M.Kom
198312052021211001

Keterangan : Lembar Konsultasi Tugas Akhir/Skripsi ini dilampirkan dalam laporan akhir Tugas Akhir

Lampiran 3 Revisi Laporan Sidang Usulan Penelitian Tugas Akhir



KEMENTERIAN PENDIDIKAN TINGGI, SAINS,
DAN TEKNOLOGI
UNIVERSITAS SILIWANGI
FAKULTAS TEKNIK
Jalan Siliwangi Nomor 24 Kota Tasikmalaya Kode Pos 46115
Telepon (0265) 330634, 333092 Faksimil (0265) 325812
Laman: www.ft.unsil.ac.id Posel: ft@unsil.ac.id

REVISI LAPORAN SIDANG USULAN PENELITIAN TUGAS AKHIR
Tasikmalaya, 18 Juni 2025

Nama : Doel Awan Nuri Suryadi
NPM : 207006071
Prodi : Informatika

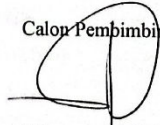
JUDUL USULAN PENELITIAN :

EVALUASI KINERJA TEKNOLOGI SD-WAN PADA JARINGAN RT/RW NET BERDASARKAN
PENDEKATAN QUALITY OF SERVICE

NO.	KETERANGAN REVISI
1	Tata tulis
2	Tujuan harus jelas & terukur
3	Seragamkan parameter yang akan di diukur pada kedua metode yang akan dicoba / diteliti.

Lembar ini diserahkan
kepada Mahasiswa

Calon Pembimbing 1,


Rohmat Gunawan, S.T., M.T., MCE.
NIPPPK. 198005092021211007



KEMENTERIAN PENDIDIKAN TINGGI, SAINS,
DAN TEKNOLOGI
UNIVERSITAS SILIWANGI
FAKULTAS TEKNIK

Jalan Siliwangi Nomor 24 Kota Tasikmalaya Kode Pos 46115
Telepon (0265) 330634, 333092 Faksimil (0265) 325812
Laman: www.ft.unsil.ac.id Posel: ft@unsil.ac.id

REVISI LAPORAN SIDANG USULAN PENELITIAN TUGAS AKHIR
Tasikmalaya, 18 Juni 2025

Nama : Doel Awan Nuri Suryadi
NPM : 207006071
Prodi : Informatika

JUDUL USULAN PENELITIAN :

EVALUASI KINERJA TEKNOLOGI SD-WAN PADA JARINGAN RT/RW NET BERDASARKAN
PENDEKATAN QUALITY OF SERVICE

NO.	KETERANGAN REVISI
	Perbaiki Aya yang sudah

Lembar ini diserahkan
kepada Mahasiswa

Calon Pembimbing 2,

Ir. Firmansyah Maulana SN., S.T., M.Kom., IPM., AER.
NIPPPK. 198312052021211001



KEMENTERIAN PENDIDIKAN TINGGI, SAINS,
DAN TEKNOLOGI
UNIVERSITAS SILIWANGI
FAKULTAS TEKNIK

Jalan Siliwangi Nomor 24 Kota Tasikmalaya Kode Pos 46115
Telepon (0265) 330634, 333092 Faksimil (0265) 325812
Laman: www.ft.unsil.ac.id Posel: ft@unsil.ac.id

REVISI LAPORAN SIDANG USULAN PENELITIAN TUGAS AKHIR
Tasikmalaya, 18 Juni 2025

Nama : Doel Awan Nuri Suryadi
NPM : 207006071
Prodi : Informatika

JUDUL USULAN PENELITIAN :

EVALUASI KINERJA TEKNOLOGI SD-WAN PADA JARINGAN RT/RW NET BERDASARKAN
PENDEKATAN QUALITY OF SERVICE

NO.	KETERANGAN REVISI
1	penelitian di sarankan parameter yang di uji kurang.
2	penelitian diperbaiki.
3	istilah penelitian Bahasa yang ring.

Lembar ini diserahkan
kepada Mahasiswa

Penguji I,

Ir. Rianto, S.T., M.T.
NIPPPK. 198412242021211001



KEMENTERIAN PENDIDIKAN TINGGI, SAINS,
DAN TEKNOLOGI
UNIVERSITAS SILIWANGI
FAKULTAS TEKNIK

Jalan Siliwangi Nomor 24 Kota Tasikmalaya Kode Pos 46115
Telepon (0265) 330634, 333092 Faksimil (0265) 325812
Laman: www.ft.unsil.ac.id Posel: ft@unsil.ac.id

REVISI LAPORAN SIDANG USULAN PENELITIAN TUGAS AKHIR
Tasikmalaya, 18 Juni 2025

Nama : Doel Awan Nuri Suryadi
NPM : 207006071
Prodi : Informatika

JUDUL USULAN PENELITIAN :

EVALUASI KINERJA TEKNOLOGI SD-WAN PADA JARINGAN RT/RW NET BERDASARKAN
PENDEKATAN QUALITY OF SERVICE

NO.	KETERANGAN REVISI
1.	Tambahkan penelitian ss berhubungan dgn. ITG-T 1571.
2.	Penulisan perbaikan sesuai pedoman.

Lembar ini diserahkan
kepada Mahasiswa

Penguji 2,

Hen Hen Lukmana, M.Kom.
NIP. 199401292022031006

Lampiran 4 Rekap Seminar Hasil



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS SILIWANGI
FAKULTAS TEKNIK
Jalan Siliwangi Nomor 24 Kota Tasikmalaya Kode Pos 46115
Telepon (0265) 330634, 333092 Faksimil (0265) 325812
Laman: www.ft.unsil.ac.id Posel: ft@unsil.ac.id

REKAP PERBAIKAN SEMINAR HASIL TUGAS AKHIR

Nama : Doel Awan Nuri Suryadi
NPM : 207006071
Jurusan : Informatika

JUDUL PENELITIAN :

EVALUASI KINERJA TEKNOLOGI SD-WAN PADA JARINGAN RT/RW NET BERDASARKAN
PENDEKATAN QUALITY OF SERVICE

No	Catatan Pembimbing dan Penguji	Catatan Perbaikan	Validasi Pembimbing
1	Rohmat Gunawan, S.T., M.T.		
	A. Tata Tulis	Sudah diperbaiki	
	B. Rumusan Masalah	Sudah diperbaiki	
	C. Tujuan Penelitian harus jelas dan terukur	Sudah diperbaiki	
	D. Metode Penelitian	Sudah diperbaiki	
	E. Kesimpulan menjawab sejauh mana tujuan tercapai	Sudah diperbaiki	
2	Ir. Firmansyah MSN, S.T., M.Kom.		
	A. Tata tulis	Sudah diperbaiki	
3	Ir. RANDI RIZAL, Ph.D.		
	A. Perbaiki tata penulisan Laporan TA!	Sudah diperbaiki	
	B. Latar belakang perbaiki sesuai dengan kondisi existing dan justifikasi kemudian perkuat research gapnya di sebelah mana.	Sudah diperbaiki	
	C. Perbaiki rumusan masalah penelitian yang diambil dari latar belakang.	Sudah diperbaiki	
	D. Tabel matriks penelitian tambahkan bagian parameter pengujiannya.	Sudah diperbaiki	
	E. Kesimpulan harus menjawab dan koheren dengan rumusan masalah.	Sudah diperbaiki	
	F. Daftar pustaka pastikan referensinya 5 tahun	Sudah diperbaiki	



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS SILIWANGI
FAKULTAS TEKNIK

Jalan Siliwangi Nomor 24 Kota Tasikmalaya Kode Pos 46115
Telepon (0265) 330634, 333092 Faksimil (0265) 325812
Laman: www.ft.unsil.ac.id Posel: ft@unsil.ac.id

	terakhir. Gunakan mendeley dan pastikan sesuai.		
4	Hen Hen Lukmana S.Pd., M.Kom.		
	A. Perbaiki tata penulisan Laporan TA!	Sudah diperbaiki	
	B. Perbaiki Manfaat Penelitian sesuaikan dengan Rumusan dan Tujuan	Sudah diperbaiki	
	C. Tambahkan Landasan Teori terkait penelitian	Sudah diperbaiki	
	D. Tambahkan Gambar Tahapan penelitian	Sudah diperbaiki	
	E. Tambahkan Penjelasan Gambar Konfigurasi 4.1.2.	Sudah diperbaiki	
	F. Tambahkan Penjelasan Analisa Pengujian Kinerja 4.2.1-4	Sudah diperbaiki	
	G. Kesimpulan harus menjawab dan koheren dengan rumusan masalah.	Sudah diperbaiki	

Pembimbing 1,

Rohmat Gunawan, S.T., M.T.
NIDN. 0409058007

Tasikmalaya,
Pembimbing 2,

Ir. Firmansyah MSN, S.T., M.Kom.
NIDN. 0405128301

Lampiran 5 Rekap Tugas Akhir



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS SILIWANGI
FAKULTAS TEKNIK
Jalan Siliwangi Nomor 24 Kota Tasikmalaya Kode Pos 46115
Telepon (0265) 330634, 333092 Faksimil (0265) 325812
Laman: www.ft.unsil.ac.id Posel: ft@unsil.ac.id

REKAP PERBAIKAN TUGAS AKHIR

Nama : Doel Awan Nuri Suryadi
NPM : 207006071
Jurusan : Informatika

JUDUL PENELITIAN:

EVALUASI KINERJA TEKNOLOGI SD-WAN PADA JARINGAN RT/RW NET BERDASARKAN PENDEKATAN QUALITY OF SERVICE

No	Catatan Pembimbing dan Penguji	Catatan Perbaikan	Validasi Pembimbing
1	Rohmat Gunawan, S.T., M.T.		
	-	-	
2	Ir. Firmansyah MSN, S.T., M.Kom.		
	-	-	
3	Ir. Rianto, S.T., M.T.		
	A. Perbaiki Penulisan Laporan TA	Sudah direvisi (Cover, hal vii - I-4)	
	B. Tambahkan penjelasan terkait hasil komparasi setelah tabel 4.9	Sudah direvisi (IV-46)	
4	Hen Hen Lukmana S.Pd., M.Kom.		
	A. Dimanfaat tambahkan keilmuan	Sudah direvisi (hal I-4)	
	B. Jelaskan jaringan berbeban seperti jelaskan secara rinci sesuai catatan pada draft	Sudah direvisi (hal III-20, III-32,33)	
	C. Perbaiki freeddns bagian batasan dan lainnya	Sudah direvisi (hal I-4, II-5)	
	D. Sesuaikan Subab dengan rangkaian metode penelitian	Sudah direvisi (hal subab III dan IV)	

Pembimbing 1,

Rohmat Gunawan, S.T., M.T.
NIDN. 0409058007

Tasikmalaya,

Pembimbing 2,

Ir. Firmansyah MSN, S.T., M.Kom.
NIDN. 0405128301

Lembar ini dibuat oleh
Mahasiswa

Lampiran 6 Submit Jurnal

The screenshot displays the JATISI Submissions interface. The top navigation bar includes the JATISI logo, a Tasks dropdown with a count of 0, and links for English, View Site, and a user profile named doelawan. The left sidebar shows the Submissions menu. The main content area is titled 'Submissions' and features tabs for 'My Queue' and 'Archives'. A 'Help' button is located in the top right corner of the main area. Below the tabs, there is a 'My Assigned' section with a search bar and a 'New Submission' button. A single submission is listed with the ID 13557, the author Doel Awan Nuri Suryadi, and the title 'New era Remote connectivity: Evaluation of SD-Wan's superiority over conventiona...'. The submission status is indicated by a red circle with a white 'O' and the word 'Submission'. A dropdown arrow is visible to the right of the submission entry. At the bottom right of the submission list, it says '1 of 1 submissions'. The footer of the page mentions 'Platform & workflow by OJS / PKP'.

JATISI Tasks 0 English View Site doelawan

Submissions

My Queue Archives Help

My Assigned Search New Submission

13557 Doel Awan Nuri Suryadi
New era Remote connectivity: Evaluation of SD-Wan's superiority over conventiona... Submission

1 of 1 submissions

Platform & workflow by
OJS / PKP