

Penggunaan Layer2 Tunneling Protocol untuk Remote Access Maintenance dan Monitoring CCTV pada Dinas Kominfo Kabupaten Magetan

Muhammad Nurfian Aziz¹, Agus Prihanto²

^{1,2} Teknik Informatika/Teknik Informatika, Universitas Negeri Surabaya

¹muhammadnurfian.23399@mhs.unesa.ac.id

²agusprihanto@unesa.ac.id

Abstrak— Sistem pengawasan menggunakan CCTV telah menjadi elemen penting dalam mendukung keamanan dan monitoring di lingkungan pemerintahan. Namun, keterbatasan dalam mengakses perangkat CCTV secara langsung dari luar jaringan lokal masih menjadi kendala, terutama bagi tim teknis yang perlu melakukan pemeliharaan jarak jauh. Akses yang terbatas ini dapat menghambat responsivitas dan efektivitas pengelolaan jaringan, terlebih jika lokasi perangkat berada di area yang jauh dan perlu waktu untuk perjalanan menuju lokasi. Dalam penelitian ini, dilakukan perancangan dan konfigurasi jaringan menggunakan *router* MikroTik yang berfungsi sebagai *server* dan *client* VPN L2TP. Selain itu, dilakukan pengujian parameter *Quality of Service* (QoS) seperti *delay*, *jitter*, *throughput*, dan *packet loss* berdasarkan rekomendasi ITU-T G.1010. Protokol RTSP juga berhasil diimplementasikan melalui koneksi VPN menggunakan metode *port-forwarding* untuk mengakses *video-streaming* secara langsung dari kamera CCTV.

Hasil pengujian menunjukkan bahwa koneksi L2TP memiliki performa yang baik dengan nilai *delay* rata-rata sebesar 63 ms, *jitter* sebesar 1,125 ms, *packet loss* 0%, serta *throughput upload* dan *download* masing-masing sebesar 48,2 Mbps dan 94,9 Mbps. Nilai-nilai tersebut berada dalam kategori sangat baik dan mendukung kebutuhan operasional *remote access* maupun *live-view* CCTV. Hasil tersebut menunjukkan bahwa implementasi L2TP dan RTSP mampu memberikan solusi yang efektif terhadap permasalahan keterbatasan akses jarak jauh dalam pengelolaan CCTV. Dengan demikian, sistem ini layak diadopsi sebagai alternatif solusi untuk instansi dengan kebutuhan serupa.

Kata Kunci— VPN, L2TP, RTSP, NVR, CCTV, QoS.

I. PENDAHULUAN

Dinas Komunikasi dan Informatika Kabupaten Magetan mengelola sistem pengawasan CCTV guna menunjang keamanan wilayah secara real-time dan menyeluruh. Namun, keterbatasan fitur bawaan dari perangkat *Network Video Recorder* (NVR), seperti tidak tersedianya akses langsung ke masing-masing kamera serta terbatasnya dukungan terhadap protokol *streaming*, menjadi kendala yang signifikan. Selain itu, kebutuhan *monitoring* CCTV melalui protokol *Real Time Streaming Protocol* (RTSP) juga belum dapat terpenuhi. Masalah lain yaitu sulitnya tim teknis dalam melakukan *troubleshooting* dan konfigurasi ulang perangkat dari luar jaringan lokal secara efisien.

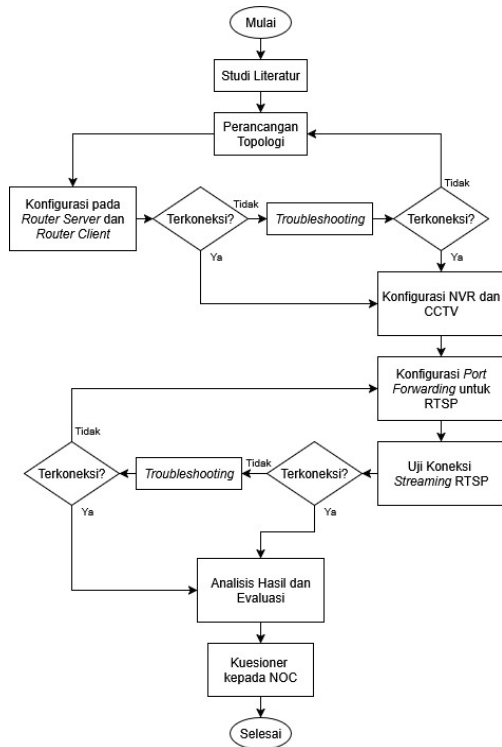
Untuk menjawab tantangan tersebut, penelitian ini memanfaatkan *Layer2 Tunneling Protocol* (L2TP) sebagai protokol VPN yang aman dan kompatibel dengan perangkat MikroTik, serta mengintegrasikan RTSP melalui teknik *port forwarding* untuk memungkinkan akses langsung ke video kamera CCTV dari jarak jauh. Penelitian ini juga merujuk pada

beberapa studi terdahulu, seperti penelitian oleh Pratama & Puspitasari (2020) yang membahas penerapan L2TP/IPSec dan *port forwarding* untuk remote akses MikroTik, serta menunjukkan efektivitas kombinasi tersebut dalam menyediakan akses yang stabil[1]. Sari & Helena (2024) juga menemukan bahwa penggunaan L2TP pada MikroTik mampu meningkatkan efisiensi dan keamanan koneksi jaringan untuk kebutuhan akses jarak jauh[2]. Selain itu, penelitian oleh Kariyamin et al. (2023) mengungkap bahwa RTSP memiliki performa lebih baik dibandingkan protokol sejenis dalam transmisi *video streaming*, khususnya dari sisi *delay*, *packet loss*, dan *throughput*[3]. Dengan merujuk pada studi tersebut, tujuan dari penelitian ini adalah menyediakan sistem *remote access* yang aman, andal, dan efisien untuk keperluan *maintenance* maupun *monitoring* CCTV menggunakan protokol RTSP di lingkungan pemerintah secara jarak jauh, serta mengevaluasi performanya berdasarkan parameter *Quality of Service* (QoS) sesuai standar rekomendasi.

II. METODE PENELITIAN

A. Metodologi Penelitian

Metodologi penelitian yang digunakan adalah melalui beberapa tahapan sebagaimana *flowchart* berikut.



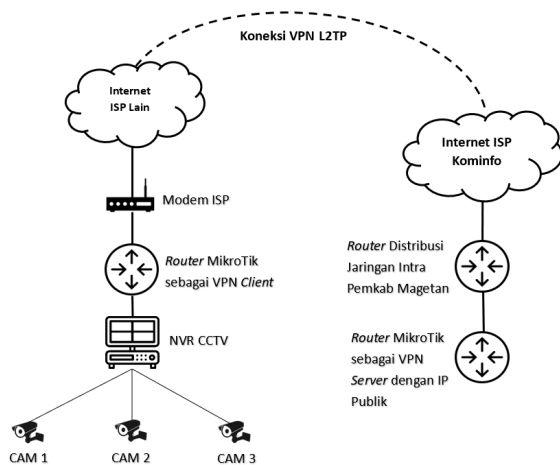
Gbr 1. Flowchart

1. Studi Literatur

Penelitian dimulai dengan melakukan studi literatur untuk memahami konsep dasar *Layer2 Tunneling Protocol* (L2TP) dan kebutuhan *remote access*. Literatur yang relevan, seperti jurnal, buku, dan dokumentasi teknis, akan digunakan sebagai acuan.

2. Perancangan Topologi

Setelah memahami konsep, dilakukan perancangan topologi jaringan yang akan diterapkan. Perancangan mencakup konfigurasi perangkat jaringan seperti *router*, *server*, dan perangkat CCTV, serta integrasi dengan protokol L2TP.



Gbr 2. Topologi Jaringan

3. Pengaplikasian pada Perangkat

Implementasi dilakukan dengan mengonfigurasi perangkat jaringan sesuai topologi yang telah dirancang. Tahapan ini melibatkan pengaturan L2TP pada *router* dan pengujian koneksi dengan *ping* dan untuk memastikan fungsi *remote access* dan *video-stream* menggunakan RTSP dapat berjalan dengan baik.

4. Analisis dan Evaluasi

Data hasil implementasi dianalisis untuk mengevaluasi kinerja jaringan, seperti *latency*, dan *throughput*. Evaluasi juga dilakukan terhadap kemudahan penggunaan dan efisiensi pengelolaan oleh personel teknis di Dinas Kominfo Kabupaten Magetan.

B. Desain Penelitian

Desain penelitian pada penelitian ini adalah desain eksperimen terapan, karena penelitian ini berfokus pada pengujian efektivitas L2TP dalam konteks tertentu (*remote access maintenance* dan *monitoring CCTV*). Pendekatan yang digunakan dapat berupa *mixed methods*:

- Kualitatif untuk memahami kebutuhan Dinas Kominfo Kabupaten Magetan.
- Kuantitatif untuk mengukur performa protokol L2TP (*bandwidth*, QoS) dan trafik *bandwidth* ketika berjalan protokol RTSP.

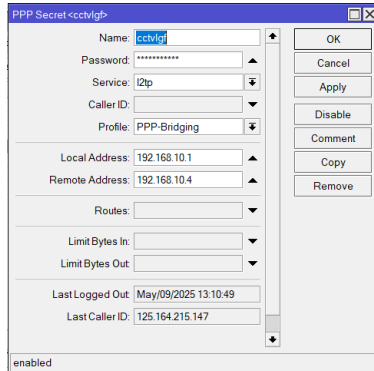
III. HASIL DAN PEMBAHASAN

A. Hasil Penelitian

1) Konfigurasi Router Server

Perangkat *router server* yang digunakan yaitu MikroTik dengan seri RB760iGS hEX S dengan *firmware* RouterOS versi 6.49.8 yang terkoneksi dengan internet melalui ISP Diskominfo Kabupaten Magetan.

Router server yang dilengkapi IP publik dari Diskominfo Kabupaten Magetan dikonfigurasi sebagai server VPN dengan aktivasi layanan L2TP. Kamera CCTV dan NVR menggunakan IP privat 192.168.1.xxx/24. Setelah membuat profil *client* dengan *username*, *password*, dan *remote address*, ditambahkan pula profil VPN menggunakan protokol PPTP untuk tim administrator.

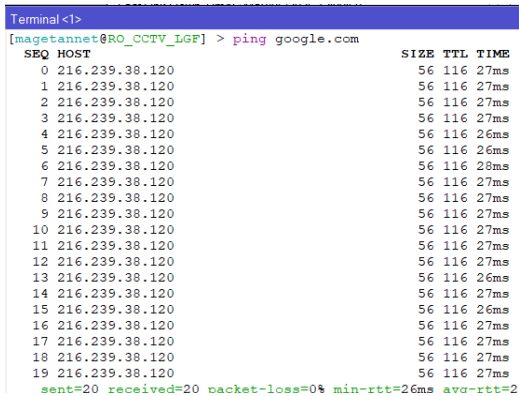


Gbr 3. Konfigurasi router server

Selain itu, dibuat pula profil VPN tambahan dengan protokol PPTP untuk digunakan oleh tim *network administrator* Diskominfo. Untuk alasan keamanan, setelah seluruh konfigurasi selesai, semua *service* MikroTik yang tidak digunakan dinonaktifkan dan *port default router* diubah.

2) Konfigurasi Router Client

Router client ini berfungsi untuk mengkoneksikan *service* VPN menuju ke *router server*. Perangkat yang digunakan pada sisi *client* yaitu *router* MikroTik seri RB760iGS HEX S dengan *firmware* RouterOS versi 6.46.6.



Gbr 4. Uji ping pada router client

Pada sisi *router client*, langkah pertama adalah memastikan koneksi internet dari ISP tersedia, yang dalam hal ini menggunakan layanan Indihome di lokasi Lawu Green Forest, Plaosan, Magetan. Setelah koneksi aktif dan terverifikasi melalui uji *ping* ke Google, dilakukan penambahan koneksi L2TP *Client* di Winbox dengan isian *name* dan *password* sesuai konfigurasi *router server*.

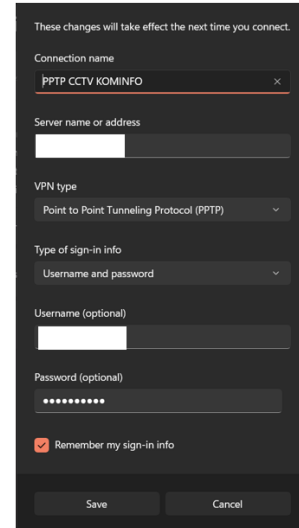
X	ether1	Ethernet
RS	ether2-SWITCH PoE KAMERA	Ethernet
RS	ether3-NVR LGF	Ethernet
R	ether4-INTERNET	Ethernet
	ether5	Ethernet
RS	l2tp-out1	L2TP Client
X	sfp1	Ethernet

Gbr 5. Daftar interface pada router client

Konfigurasi *port* pada *router client* meliputi *ether2* untuk kamera CCTV, *ether3* untuk NVR, dan *ether4* sebagai sumber internet dari *modem* Indihome, sementara *port* lainnya disesuaikan sesuai kebutuhan.

3) Konfigurasi VPN pada PC untuk remote-access

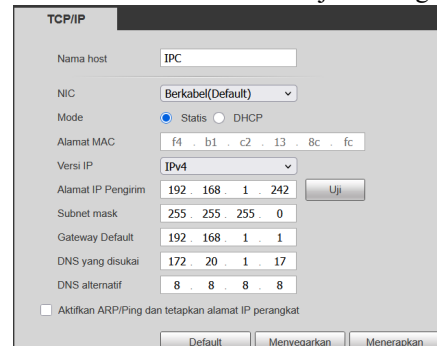
Penulis melakukan konfigurasi VPN *client* pada laptop berbasis Windows 11 untuk keperluan *remote-access*. Pengaturan VPN dilakukan menggunakan fitur bawaan Windows, kemudian dilanjutkan dengan proses koneksi ke *server* VPN. Hasilnya, koneksi berhasil terhubung antara laptop dan VPN *server*.



Gbr 6. Konfigurasi VPN client pada laptop

4) Konfigurasi Kamera CCTV

Kamera CCTV yang digunakan pada penelitian ini adalah Dahua dengan seri DH-IPC-HFW626S-G2 dengan versi *firmware* V2.840.0000000.12.R dan berjumlah tiga buah.



Gbr 7. Konfigurasi IP address pada kamera

Konfigurasi IP, *subnet*, *gateway*, dan DNS pada tiga kamera CCTV disesuaikan dengan jaringan *router server*, masing-masing menggunakan alamat 192.168.1.241, 192.168.1.242, dan 192.168.1.243. Setelah seluruh kamera dikonfigurasi, perangkat dihubungkan ke NVR dan dilakukan proses inisialisasi.

5) Konfigurasi NVR

Pada penelitian ini, perangkat *Network Video Recorder* (NVR) yang digunakan adalah NVR merk Dahua seri DHI-NVR2208-8P-4KS2 yang berjalan pada versi *firmware* V4.001.0000005.0.

Perangkat yang ditambahkan					Info Terkait Kamera		
	Saluran	Edit	Menghapus	Status	Alamat IP	Port	Nama peranti
☐	1				192.168.1.241	37777	9B0946...
☐	2				192.168.1.242	37777	9C0B40...
☐	3				192.168.1.243	37777	9F07400...

Gbr 8. Inisialisasi kamera pada NVR

Perangkat NVR yang digunakan mendukung hingga 8 *channel* kamera dan dilengkapi *harddisk* berkapasitas 1 TB. Konfigurasi dimulai dengan pengaturan IP statis melalui *web interface* NVR, mencakup IP, *subnet*, dan *gateway*. Selanjutnya, dilakukan inisialisasi kamera melalui menu deteksi otomatis atau dengan memasukkan IP kamera secara manual.

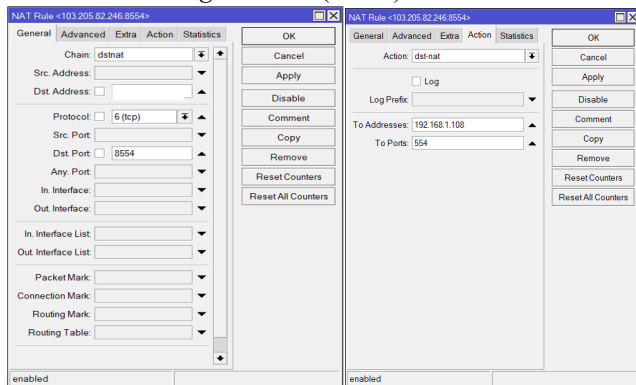


Gbr 9. Tampilan *live-view* pada NVR

Hasil tayangan langsung (*live view*) menunjukkan bahwa semua kamera telah terhubung dan melakukan perekaman ke NVR.

6) Konfigurasi *Port-Forwarding*

Setelah konfigurasi topologi VPN dan perangkat CCTV selesai, tahap selanjutnya adalah mengatur *port-forwarding* untuk memungkinkan akses *live-view* CCTV melalui protokol *Real-Time Streaming Protocol* (RTSP).



Gbr 10. Konfigurasi NAT rule

Konfigurasi dilakukan dengan membuat NAT Rule baru pada menu *firewall* di *router* MikroTik *server* VPN. Pada bagian *General*, alamat IP publik *router* diisikan sebagai *Dst. Address* dan port 8554 digunakan sebagai *Dst. Port*. Sementara itu, pada tab *Action*, jenis aksi diset ke *dst-nat* dan diarahkan ke IP lokal NVR (192.168.1.108) dengan *To Port* 554. Rule ini berfungsi untuk meneruskan permintaan dari luar menuju NVR secara langsung.



Gbr 11. Tampilan kamera pada VLC

Pengujian koneksi RTSP dilakukan menggunakan aplikasi VLC *Media Player*, yang mendukung *streaming* video secara *realtime*. Melalui fitur *Open Media*, penulis memasukkan alamat RTSP sesuai dengan format standar perangkat NVR Dahua. Hasilnya, seluruh kamera berhasil diakses dan menampilkan tayangan langsung (*live-view*) secara *realtime* menggunakan protokol RTSP.

7) Kuesioner Tim Teknis

Sebagai bagian dari pengumpulan data kualitatif, dilakukan survei terhadap enam staf teknis Dinas Kominfo Kabupaten Magetan yang terlibat langsung dalam pengelolaan dan pemeliharaan jaringan CCTV. Survei ini bertujuan untuk mengevaluasi implementasi sistem remote access VPN L2TP. Kuesioner terdiri dari sembilan pernyataan yang mencakup aspek kebutuhan, efektivitas teknis, dan evaluasi umum, dengan penilaian menggunakan skala Likert sebagaimana disadur dalam penelitian Raharja et al. (2018)[4].

- 1 = Sangat tidak setuju (STS)
- 2 = Tidak setuju (TS)
- 3 = Cukup setuju (CS)
- 4 = Setuju (S)
- 5 = Sangat setuju (SS)

Total respon yang terkumpul sebanyak 54, dengan nilai maksimal 270 (9 pernyataan $\times$ 6 responden $\times$ 5). Hasil rekapitulasi penilaian disajikan pada tabel berikut.

TABEL I
HASIL KUESIONER

Aspek	Jumlah Pernyataan	Skala Jawaban	Skala x Jumlah Jawaban	Skor
Kebutuhan Akses dan Monitoring	3	STS	1 x 0	0
		TS	2 x 0	0
		CS	3 x 0	0
		S	4 x 1	4
		SS	5 x 17	85
Efektivitas Teknis	4	STS	1 x 0	0
		TS	2 x 0	0
		CS	3 x0	0
		S	4 x 3	12
		SS	5 x 21	105
Evaluasi Umum dan Rekomendasi	2	STS	1 x 0	0
		TS	2 x 0	0
		CS	3 x 0	0
		S	4 x 2	8
		SS	5 x 10	50
Total Skor				264

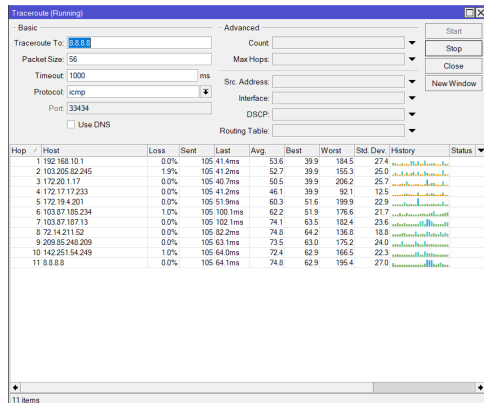
Berdasarkan hasil rekapitulasi kuesioner, diperoleh total skor sebesar 264 dari nilai maksimal 270. Hasil ini kemudian dihitung menggunakan rumus indeks persentase: $(264 \div 270) \times 100\% = 97,78\%$. Mengacu pada kriteria interpretasi skala Likert, nilai tersebut berada pada rentang 80%–100%, yang termasuk dalam kategori **Sangat Setuju**.

B. Pembahasan

Dalam implementasi Quality of Service (QoS), terdapat sejumlah parameter utama yang digunakan untuk mengukur dan mengevaluasi kinerja jaringan. Parameter-parameter ini berperan penting dalam menentukan sejauh mana jaringan mampu memberikan layanan yang andal, stabil, dan sesuai dengan kebutuhan aplikasi yang berjalan di atasnya. Berikut ini adalah nilai rekomendasi dari parameter QoS yang diambil dari penelitian Darmawan et al. (2022)[5].

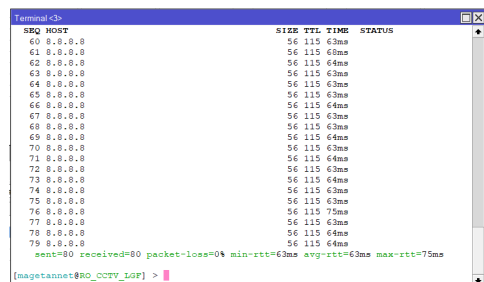
1) Pengujian Delay

Pengukuran delay dilakukan melalui fitur *ping* ICMP pada router MikroTik di sisi *client* dengan mengirimkan 80 paket ICMP ke Google, lalu menghitung nilai minimum, maksimum, dan rata-rata RTT (*Round Trip Time*) untuk mendapatkan estimasi *delay* aktual. Pengujian dilakukan setelah memastikan bahwa trafik berjalan melalui koneksi VPN L2TP menggunakan fitur *traceroute*.



Hop	Host	Loss	Sent	Last	Avg	Best	Worst	Std Dev	History	Status
1	192.168.10.1	0.0%	105	41.4ms	53.6	39.9	194.5	27.4		
2	103.205.82.245	1.9%	105	41.2ms	52.7	38.9	155.3	25.0		
3	172.201.1.7	0.0%	105	40.7ms	50.5	38.9	286.2	26.7		
4	172.17.17.233	0.0%	105	41.2ms	46.1	39.9	92.1	12.5		
5	172.194.201	0.0%	105	51.3ms	60.3	51.6	199.9	22.9		
6	103.87.185.234	1.0%	105	100.1ms	62.2	51.9	176.5	21.7		
7	103.87.187.13	0.0%	105	102.1ms	74.1	63.5	182.4	23.6		
8	72.14.21.52	0.0%	105	82.2ms	74.8	64.2	136.0	18.8		
9	209.85.248.209	0.0%	105	63.1ms	73.5	63.0	175.2	24.0		
10	142.251.54.249	1.0%	105	64.0ms	72.4	62.9	166.5	22.3		
11	8.8.8.8	0.0%	105	64.1ms	74.6	62.9	195.4	27.0		

Gbr 12. Uji *traceroute* VPN L2TP



Seq	Host	Size	TTL	Time	Status
60	8.8.8.8	56	115	63ms	
61	8.8.8.8	56	115	60ms	
62	8.8.8.8	56	115	64ms	
63	8.8.8.8	56	115	63ms	
64	8.8.8.8	56	115	63ms	
65	8.8.8.8	56	115	63ms	
66	8.8.8.8	56	115	64ms	
67	8.8.8.8	56	115	63ms	
68	8.8.8.8	56	115	63ms	
69	8.8.8.8	56	115	64ms	
70	8.8.8.8	56	115	63ms	
71	8.8.8.8	56	115	64ms	
72	8.8.8.8	56	115	63ms	
73	8.8.8.8	56	115	64ms	
74	8.8.8.8	56	115	63ms	
75	8.8.8.8	56	115	63ms	
76	8.8.8.8	56	115	75ms	
77	8.8.8.8	56	115	63ms	
78	8.8.8.8	56	115	64ms	
79	8.8.8.8	56	115	64ms	

sent=80 received=80 packet-loss=0% min-rtt=63ms avg-rtt=63ms max-rtt=75ms

[magnet@net80_OCTV_L2TP] >

Gbr 13. Uji *delay* pada router *client*

Berikut adalah rekomendasi nilai *delay* yang diberikan.

TABEL II
NILAI REKOMENDASI DELAY

Kategori	Nilai Delay (ms)
----------	------------------

Sangat Baik	<150
Baik	150 - 300
Sedang	300 - 450
Buruk	≥ 450

Berdasarkan hasil pengujian *ping* pada router MikroTik *client*, diperoleh 80 paket terkirim dan seluruhnya diterima kembali. Nilai minimum RTT tercatat 63 ms, rata-rata 63 ms, dan maksimum 75 ms. Dengan rata-rata *delay* sebesar **63 ms**, koneksi VPN L2TP berada dalam kategori **Sangat Baik** sesuai nilai rekomendasi.

2) Pengujian Jitter

Pengukuran *jitter* dalam penelitian ini menggunakan rumus: *Jitter* = (Total variasi *delay*) ÷ (Jumlah paket diterima). Berdasarkan data variasi *delay* yang diperoleh dari hasil *capture* MikroTik *router client*, total variasi sebesar 90 ms dibagi dengan 80 paket yang diterima menghasilkan nilai *jitter* sebesar 1,125 ms. Dan berikut adalah Tabel rekomendasi untuk nilai *Jitter*.

TABEL III
NILAI REKOMENDASI JITTER

Kategori	Nilai Jitter (ms)
Sangat Baik	0
Baik	1 - 75
Sedang	75 - 125
Buruk	125 - 225

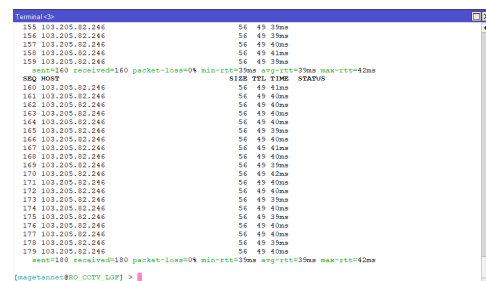
Berdasarkan hasil tersebut didapatkan besar *jitter* yaitu **1,125ms** atau bernilai **Baik**.

3) Pengujian Packet Loss

Untuk menilai kualitas jaringan berdasarkan nilai *packet loss*, digunakan acuan rekomendasi nilai *packet loss* pada Tabel berikut.

TABEL IV
NILAI REKOMENDASI PACKET-LOSS

Kategori	Nilai Packet Loss (%)
Sangat Baik	0
Baik	3
Sedang	15
Buruk	25



Seq	Host	Size	TTL	Time	Status
155	103.205.82.246	56	49	39ms	
156	103.205.82.246	56	49	39ms	
157	103.205.82.246	56	49	40ms	
158	103.205.82.246	56	49	41ms	
159	103.205.82.246	56	49	39ms	

sent=160 received=160 packet-loss=0% min-rtt=39ms avg-rtt=39ms max-rtt=42ms

Seq	Host	Size	TTL	Time	Status
160	103.205.82.246	56	49	41ms	
161	103.205.82.246	56	49	40ms	
162	103.205.82.246	56	49	40ms	
163	103.205.82.246	56	49	40ms	
164	103.205.82.246	56	49	40ms	
165	103.205.82.246	56	49	39ms	
166	103.205.82.246	56	49	40ms	
167	103.205.82.246	56	49	41ms	
168	103.205.82.246	56	49	40ms	
169	103.205.82.246	56	49	39ms	
170	103.205.82.246	56	49	42ms	
171	103.205.82.246	56	49	40ms	
172	103.205.82.246	56	49	40ms	
173	103.205.82.246	56	49	39ms	
174	103.205.82.246	56	49	40ms	
175	103.205.82.246	56	49	39ms	
176	103.205.82.246	56	49	40ms	
177	103.205.82.246	56	49	40ms	
178	103.205.82.246	56	49	39ms	
179	103.205.82.246	56	49	40ms	

sent=180 received=180 packet-loss=0% min-rtt=39ms avg-rtt=39ms max-rtt=42ms

[magnet@net80_OCTV_L2TP] >

Gbr 14. Uji *packet-loss* menggunakan *ping*

Berdasarkan pengujian *ping* dari *router client* ke IP publik VPN *server* selama tiga menit menggunakan fitur *terminal*

pada MikroTik, diperoleh nilai *packet loss* sebesar **0%**. Hasil ini menunjukkan bahwa koneksi berada pada kategori **Sangat Baik** sesuai dengan kategori pada tabel rekomendasi.

4) Pengujian *Bandwidth* dan *Throughput*

Pada bagian ini dilakukan pengujian *bandwidth* dari ISP yang tersedia di lokasi *client* serta pengukuran *throughput* saat koneksi menggunakan VPN L2TP. Pengujian dilakukan langsung di lokasi CCTV menggunakan laptop yang terhubung melalui kabel LAN. *Speedtest* dilakukan menggunakan situs *nperf.com*, dengan hasil pengujian pertama merepresentasikan *bandwidth* murni dari ISP tanpa melalui koneksi VPN.



Gbr 15. Pengujian bandwidth



Gbr 16. Pengujian throughput

Berdasarkan hasil *speedtest*, didapatkan kecepatan *download* sebesar **94,74 Mbps** dan *upload* sebesar **51,09 Mbps** sebagai *bandwidth* ISP. Setelah terkoneksi menggunakan VPN L2TP, dilakukan pengujian kembali dan diperoleh nilai *throughput* sebesar **55,54 Mbps** untuk *download* dan **28,33 Mbps** untuk *upload*.

5) Pengujian Trafik RTSP dan *Maintenance*

Pengujian trafik *playback* video realtime menggunakan protokol RTSP dilakukan melalui fitur *Graph* pada aplikasi Winbox. Pengujian dilakukan pada siang dan malam hari untuk melihat perbedaan beban trafik berdasarkan pencahayaan. Setiap kamera dikonfigurasi dengan spesifikasi video sebagai berikut: *encode mode* H.264, resolusi 1280×720 (720p), frame rate 25 FPS, dan bitrate 2048 Kbps. Hasil pengamatan trafik ditampilkan dalam bentuk tabel berikut untuk masing-masing kondisi siang dan malam.

TABEL V
PENGUNAAN BANDWIDTH PADA KAMERA

Jumlah Kamera	Penggunaan Bandwidth (Mbps)
---------------	-----------------------------

	Siang Hari	Malam Hari
1 Kamera	1.88 Mbps	1.78 Mbps
2 Kamera	4.19 Mbps	4.38 Mbps
3 Kamera	6.21 Mbps	6.93 Mbps

Pengujian trafik saat proses *maintenance* dilakukan dengan menangkap data pada interface *l2tp-cctvlgf* di *router server* selama sepuluh menit. Aktivitas yang dilakukan mencakup perubahan konfigurasi kamera, pengaturan NVR, dan pemutaran *live-view*. Hasil capture menunjukkan rata-rata *upload* dari sisi *client* sebesar **6,15 Mbps** dan *download* sebesar **226,14 Kbps**, yang menunjukkan bahwa *throughput* VPN mencukupi untuk kebutuhan *maintenance* CCTV secara *remote*.

TABEL VI
PEMBAHASAN QUALITY OF SERVICE

Parameter	Hasil	Nilai Rekomendasi	Kategori	Interpretasi
Delay	63 ms	≤ 150 ms	Sangat Baik	Koneksi responsif dan sesuai standar komunikasi <i>real-time</i>
Jitter	1.125 ms	< 30 ms	Baik	Variasi <i>delay</i> sangat rendah dan stabil
Packet Loss	0%	< 1%	Sangat Baik	Tidak ada paket yang hilang, koneksi sangat stabil
Throughput Upload	28.33 Mbps	> 6 Mbps (estimasi kebutuhan 3 kamera RTSP)	Sangat Baik	Cukup untuk <i>streaming</i> 3 kamera resolusi HD
Throughput Download	55.54 Mbps	—	-	Cukup untuk kebutuhan <i>remote access</i>

IV. KESIMPULAN

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, dapat disimpulkan bahwa:

- Implementasi VPN L2TP dengan menggunakan perangkat MikroTik berhasil menyediakan koneksi *remote access* dengan performa yang memenuhi standar QoS berdasarkan ITU-T G.1010 dan memenuhi kebutuhan *maintenance* dan *monitoring* CCTV.
- Penerapan protokol RTSP melalui koneksi VPN berhasil dilakukan menggunakan metode *port-forwarding*, yang memungkinkan akses langsung ke *video stream* tiap kamera dari luar jaringan lokal.
- Pengujian parameter QoS menunjukkan performa jaringan yang sangat baik, dengan nilai *delay* 63 ms, *jitter* 1.125 ms, *packet loss* 0%, dan *throughput* yang mencukupi untuk *streaming* video CCTV secara *real-time*.

REFERENSI

- [1] H. Pratama and N. F. Puspitasari, "Penerapan Protokol L2TP/IPSec dan Port-Forwarding untuk Remote Mikrotik pada Jaringan Dynamic IP," *Creative Information Technology Journal*, pp. 51-62, 2020.
- [2] L. O. Sari and H. , "Implementasi Virtual Private Network Menggunakan Layer2 Tunneling Protocol Berbasis Mikrotik," *Indonesian Journal of Machine Learning and Computer Science*, pp. 1496-1504, 2024.
- [3] K. I. Riadi and H. , "Analisis Kinerja Real Time Streaming Protocol (RTSP) dan Real Time Transport (RTP) Menggunakan Aplikasi VLC pada Live Video Streaming," *Jurnal Teknik Informatika Vol. 4 No. 4*, pp. 769-778, 2023.
- [4] U. Raharja, E. P. Harahap and R. E. C. Devi, "Pengaruh Pelayanan dan Fasilitas pada Raharja Internet Cafe terhadap Kegiatan Perkuliahan pada Perguruan Tinggi," *Jurnal Teknoinfo Vol. 12 No. 2*, pp. 62-64, 2018.
- [5] E. Darmawan, S. Budiyanto and L. M. Silalahi, "QoS Analysis on VoIP with VPN using SSL and L2TP IPSec Method," in *International Conference on Communication, Networks and Satellite (COMNETSAT)*, Solo, 2022.