

**ANALISIS KUALITAS LAYANAN VPN DENGAN
PROTOCOL L2TP MENGGUNAKAN METODE QOS
DI PT. ROYAL ASSETINDO**

TUGAS AKHIR

Oleh:

Yudista Rahadian 4311411012

Disusun untuk memenuhi syarat kelulusan Program Diploma IV



**PROGRAM STUDI TEKNIK MULTIMEDIA JARINGAN
JURUSAN TEKNIK INFORMATIKA
POLITEKNIK NEGERI BATAM
BATAM
2021**

HALAMAN PENGESAHAN
ANALISIS KUALITAS LAYANAN VPN DENGAN PROTOCOL
L2TP MENGGUNAKAN METODE QOS DI PT. ROYAL
ASSETINDO

Oleh:
Yudista Rahadian 4311411012

Telah dikonsultasikan dengan dosen pembimbing sebagai persyaratan untuk
melaksanakan sidang Tugas Akhir I
di

PROGRAM DIPLOMA IV
PROGRAM STUDI TEKNIK MULTIMEDIA JARINGAN
JURUSAN TEKNIK INFORMATIKA
POLITEKNIK NEGERI BATAM

Batam, 1 April 2021

Disetujui oleh:

Pembimbing ,

Supardianto, S.ST., M.Eng

NIK. 113105

Abstraksi

Salah satu cara untuk mengantisipasi adanya penambahan kasus Covid-19 dan juga sebagai bukti kepedulian pihak manajemen terhadap kesehatan dan keselamatan karyawannya adalah dengan memberlakukan penerapan bekerja dari rumah atau *Work From Home* (WFH). Ketika diberlakukannya penerapan ini maka yang harus diperhatikan adalah bagaimana proses pertukaran data dapat berjalan dengan aman, sehingga dirancanglah *Virtual Private Network* (VPN) dengan membangun *tunnel Layer Two Tunneling Protocol* (L2TP) dimana setelahnya akan dilakukan analisa dan evaluasi apakah teknologi ini berjalan sesuai dengan tujuan yang telah ditetapkan sebelumnya atau tidak.

Keywords: IPSec, L2TP, Tunneling, VPN, WFH

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Pada tanggal 2 Maret 2020, Presiden Republik Indonesia mengumumkan kasus pertama terjadinya penularan virus Corona (Covid-19) di Indonesia. Hal ini kemudian berdampak pada setiap kegiatan masyarakat. Untuk mencegah terjadinya penularan lebih banyak, maka hampir semua kegiatan yang berhubungan dengan kegiatan di luar ruangan terpaksa dihentikan sementara waktu. Begitu juga dengan semua pekerjaan yang seharusnya dilakukan di kantor atau di tempat bekerja, sebagai bentuk kepedulian pihak manajemen terhadap kesehatan dan keselamatan karyawannya, maka kegiatan tersebut dilakukan di rumah masing-masing atau penerapan sistem *Work From Home* (WFH).

Selama penerapan WFH, perlu bagi karyawan untuk mengakses program internal *backoffice*. Program *backoffice* yang digunakan di PT. Royal Assetindo, hanya dapat diakses melalui jaringan intranet. Selain itu, selama proses pekerjaan tentu ada pertukaran data antara karyawan satu dengan yang lain, namun harus dipastikan pertukaran data tersebut aman.

Untuk menunjang kegiatan karyawan selama WFH agar karyawan yang bekerja dari rumah dapat mengakses program *backoffice* kantor, maka perlu adanya teknologi *Virtual Private Network* (VPN). Sesuai dengan namanya, teknologi ini merupakan perancangan jaringan pribadi dengan memanfaatkan jaringan public. Biasanya teknologi ini banyak digunakan untuk komunikasi kantor pusat dengan kantor cabang dengan membangun *tunnel* di antara kantor-kantor tersebut. Berdasarkan salah satu jurnal ilmiah berjudul Perancangan Virtual Private Network Dengan Server Linux Pada PT. Dharma Guna Sakti yang ditulis oleh Siswa Trihadi, Frenky Budianto dan Wirriyanto Arifin, dijelaskan bahwa dengan adanya VPN, komunikasi antar kantor pusat dan kantor cabang menjadi lebih ekonomis, selain itu juga memberikan jaminan keamanan yang tinggi karena koneksi dengan VPN dilakukan dengan peralatan yang menerapkan metode autentikasi, dimana berfungsi untuk memberikan

identitas kepada pemakai dan data yang dikirimkan lewat VPN dienkripsikan. Sebagai contoh, pada perusahaan PT. Royal Assetindo menggunakan intranet antara kantor pusat dan kantor cabang, untuk bisa mengakses program *back-office* dari server yang berada pada kantor pusat. Dikarenakan adanya pandemi maka karyawan yang menerapkan WFH, terpaksa harus mengakses program *back-office* dari luar. Untuk itu, karyawan harus terhubung ke jaringan intranet karena akses program *back-office* tersebut tidak dibuka untuk publik, sehingga dibutuhkan akses yang dapat menghubungkan langsung perangkat karyawan ke jaringan intranet dari luar melalui VPN.

Tunneling yang digunakan nantinya adalah *Layer Two Tunneling Protokol* (L2TP). Salah satu protokol VPN ini sebenarnya adalah pengembangan dari *Point to Point Tunneling Protokol* (PPTP), dengan tingkat keamanan yang lebih baik. L2TP ini biasanya menggunakan IPSec sebagai sistem keamanannya dimana data yang nantinya melewati *tunneling* sangat dijaga kerahasiaannya.

Unuk mengetahui apakah kualtias dari jaringan VPN ini sudah stabil dan layak digunakan, perlu dilakukan adanya pengujian dengan mengkaji parameter apa saja yang menjadi kendala dalam proses implementasi tersebut. Maka, setelah proses implementasi nanti akan dilakukan analisa terhadap QoS (*Quality of Service*). QoS ini menjadi acuan dari kemampuan sebuah jaringan unuk menyediakan layanan yang lebih baik.

Berdasarkan hal di atas, maka dilakukanlah perancangan dan analisa QoS terhadap jaringan VPN dengan protokol L2TP sebagai penunjang pekerjaan karyawan selama penerapan WFH.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka identifikasi rumusan masalah adalah sebagai berikut :

1. Bagaimana merancang jaringan VPN dengan protokol L2TP agar karyawan yang bekerja dari rumah dapat mengakses program *backoffice* kantor
2. Bagaimana menganalisa aspek dari efektivitas perancangan jaringan

VPN dengan protokol L2TP bagi karyawan yang menerapkan program WFH dengan melakukan pengujian menggunakan sistem *Quality of Service* (QoS)

1.3 Batasan Masalah

Berdasarkan rumusan masalah di atas, maka perlu ada batasan masalah agar ruang lingkup penelitian ini tidak terlalu luas dan tetap pada jalurnya. Maka untuk batasan masalah dari Tugas Akhir ini adalah sebagai berikut :

1. Penelitian ini untuk merancang jaringan VPN dengan protokol L2TP
2. Penelitian ini hanya menganalisa QoS dengan parameter *latency*, *jitter*, *packet loss* dan *throughput* dari perancangan jaringan VPN dengan protokol L2TP sebagai penunjang kegiatan karyawan selama WFH

1.4 Tujuan Penelitian

Adapun tujuan dari implementasi dan analisis pada Tugas Akhir ini adalah sebagai berikut :

1. Merancang merancang jaringan VPN dengan protokol L2TP agar karyawan yang bekerja dari rumah dapat mengakses program *backoffice* kantor
2. Menganalisa aspek dari efektivitas perancangan jaringan VPN dengan protokol L2TP bagi karyawan yang menerapkan program WFH dengan melakukan pengujian menggunakan sistem *Quality of Service* (QoS)

1.5 Manfaat Penelitian

Adapun manfaat dari implementasi dan analisis pada Tugas Akhir ini adalah sebagai berikut :

1. Untuk merancang jaringan VPN dengan protokol L2TP agar karyawan yang bekerja dari rumah dapat mengakses program *backoffice* kantor

2. Untuk mengetahui hasil pengujian QoS pada lingkungan PT. Royal Assetindo

1.6 Sistematika Penulisan

Adapun sistematika penulisan dalam laporan Tugas Akhir ini adalah sebagai berikut :

Bab I Pendahuluan

Pada Bab ini dipaparkan mengenai latar belakang, rumusan masalah, batasan masalah, tujuan penelitian dan manfaat penelitian.

Bab II Landasan Teori

Pada Bab ini berisi tinjauan pustaka yang berkaitan dengan penelitian terdahulu dan berbagai dasar-dasar teori untuk dijadikan acuan dalam penelitian ini.

Bab III Analisis dan Perancangan

Bab ini berisi penjelasan deskripsi umum dari sistem yang dibangun, kebutuhan fungsional, kebutuhan non-fungsional, serta perancangan dari sistem yang dibangun.

BAB II LANDASAN TEORI

2.1 Tinjauan Pustaka

Untuk menunjang kegiatan karyawan selama bekerja dari rumah agar dapat mengakses program *backoffice* kantor, maka perlu adanya teknologi *Virtual Private Network* (VPN). Sesuai dengan namanya, teknologi ini merupakan perancangan jaringan pribadi dengan memanfaatkan jaringan publik. Biasanya teknologi ini banyak digunakan untuk komunikasi kantor pusat dengan kantor cabang dengan membangun *tunnel* di antara kantor-kantor tersebut.

Karyawan harus terhubung ke jaringan intranet karena akses program *back-office* tersebut tidak dibuka untuk publik, sehingga dibutuhkan akses yang dapat menghubungkan langsung perangkat karyawan ke jaringan intranet dari luar melalui VPN.

Tunneling yang digunakan adalah *Layer Two Tunneling Protokol* (L2TP). Salah satu protokol VPN ini sebenarnya adalah pengembangan dari *Point to Point Tunneling Protokol* (PPTP), dengan tingkat keamanan yang lebih baik. L2TP ini biasanya menggunakan IPSec sebagai sistem keamanannya dimana data yang nantinya melewati *tunneling* sangat dijaga kerahasiaannya.

QoS atau *Quality of Service* merupakan mekanisme pada sebuah jaringan yang mengidentifikasi bahwa sebuah aplikasi ataupun layanan dapat berjalan sesuai dengan standar kualitas yang ditetapkan.

Berikut adalah beberapa penelitian terdahulu yang berhubungan dengan topik penelitian Analisis Kualitas Layanan VPN Dengan Protokol L2TP Menggunakan Metode QoS di PT. Royal Assetindo :

1. Analisa Perbandingan Protokol PPTP dan L2TP Menggunakan Video Call Melalui Jaringan *Virtual Private Network* (VPN), jurnal ini ditulis oleh Raisul Azhar dan Ezra Romliyanto, pada jurnal ini dilakukan pengujian untuk mengetahui kinerja yang lebih baik antara PPTP dan L2TP dimana hasilnya adalah kualitas QoS jaringan VPN yang menggunakan protokol L2TP

lebih baik daripada jaringan VPN yang menggunakan protokol PPTP karena paket data yang diterima pada waktu yang sama lebih besar pada jaringan VPN L2TP dengan codec H-263 sehingga nilai *throughput*-nya lebih besar.

2. Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet di atas VPN, hasil dari jurnal yang ditulis oleh Akbar Rachmawan dan Agus Prihanto ini menjelaskan bahwa keamanan yang digunakan oleh *tunneling* L2TP lebih unggul daripada keamanan yang digunakan oleh PPTP karena dipadukan dengan IPSec.
3. Perancangan Virtual Private Network Dengan Server Linux Pada PT. Dharma Guna Sakti karya Siswa Trihadi, Frenky Budianto, dan Wirriyanto Arifin, menjelaskan VPN dapat menghubungkan jaringan lokal perusahaan dengan jaringan yang terdapat di luar perusahaan, yaitu antara jaringan kantor pusat dengan kantor cabang.

2.2 Dasar Teori

2.2.1 IPSec (IP Security)

Menurut Syarif Hidayatulloh dalam jurnal yang berjudul Analisis dan Optimalisasi Keamanan Jaringan Menggunakan Protokol IPSec, IPSec merupakan sekumpulan standard dan protokol yang bertujuan untuk menyediakan keamanan dan kerahasiaan dalam pertukaran data di layer *network*.

2.2.2 L2TP (Layer 2 Tunneling Protocol)

L2TP merupakan *tunneling* yang bekerja pada layer 2 hanya saja biasanya ditambahkan sistem keamanan yang lebih baik, yaitu menggunakan IPSec.

Menurut Akbar Rachmawan dalam jurnal berjudul Perbandingan Protokol L2TP dan PPTP Untuk Membangun

Jaringan Intranet Di Atas VPN, L2TP merupakan protokol *tunneling* yang digunakan untuk mendukung *Virtual Private Network*.

L2TP merupakan *tunnel* standard dari satu router ke router lain atau dari *client* ke *host gateway* melewati *Network Access Server* (NAS) ISP yang dianalisa terlebih dahulu oleh *server* NAS ISP dan jika proses autentikasi berhasil, maka ISP akan membuat saluran dari *client* ke *host gateway* secara *point to point*. L2TP merupakan basis dan kombinasi dari protokol L2F dari Cisco System dan PPTP dari Microsoft.

2.2.3 *Virtual Private Network (VPN)*

VPN adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terhubung ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Sehingga akan didapatkan hak dan pengaturan yang sama seperti halnya berada di dalam LAN walaupun sebenarnya menggunakan jaringan milik publik.

2.2.4 *Quality of Service (QoS)*

QoS didefinisikan sebagai suatu alat ukur untuk menguji seberapa baik jaringan yang ada dan merupakan suatu usaha untuk menentukan karakteristik dan sifat dari suatu layanan. Tujuan dari QoS adalah untuk memenuhi kebutuhan-kebutuhan layanan yang berbeda, yang menggunakan infrastruktur yang sama. Ada beberapa parameter QoS di antaranya adalah *delay*, *jitter*, *throughput*, dan *packet loss*.

Throughput merupakan kecepatan mengirim data efektif, yang diukur dalam bps, dimana hasilnya merupakan jumlah total kedatangan paket yang sukses diamati pada *destination* selama interval waktu dibagi oleh durasi interval waktu tersebut. Persamaan perhitungan *throughput* adalah jumlah data yang dikirim dibagi

waktu pengamatan.

Berikut adalah tabel *throughput* yang diambil dari jurnal berjudul Analisis QoS (*Quality of Service*) Pada Jaringan Internet (Studi Kasus : UPT Loka Uji Teknik Penambangan Jampang Kulon-LIPI).

Table 1 Kategori Throughput

Kategori <i>Throughput</i>	<i>Throughput</i>	Indeks
Sangat Bagus	100	4
Bagus	75	3
Sedang	50	2
Jelek	<25	1

Packet loss merupakan parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang. Persamaan perhitungannya adalah sebagai berikut :

$$\text{Packet loss} : \frac{\text{Paket Data Dikirim} - \text{Paket Data Diterima}}{\text{Paket Data Dikirim}} \times 100\%$$

Berikut adalah tabel *packet loss* yang diambil dari jurnal berjudul Analisis QoS (*Quality of Service*) Pada Jaringan Internet (Studi Kasus : UPT Loka Uji Teknik Penambangan Jampang Kulon-LIPI).

Table 2 Kategori *Packet Loss*

Kategori Degradasi	<i>Packet Loss</i> (%)	Indeks
Sangat Bagus	0	4
Bagus	3	3
Sedang	15	2
Jelek	25	1

Delay atau *latency* merupakan waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, dan juga waktu yang lama. Untuk menghitung *delay* dapat dilakukan dengan persamaan berikut :

$$Delay : \frac{Packet\ Length}{Link\ Bandwidth}$$

Berikut adalah tabel kategori *delay* yang diambil dari jurnal berjudul Analisis QoS (*Quality of Service*) Pada Jaringan Internet (Studi Kasus : UPT Loka Uji Teknik Penambangan Jampang Kulon-LIPI).

Table 3 Kategori *Delay*

Kategori Latensi	Besar <i>Delay</i> (ms)	Indeks
Sangat Bagus	<150	4
Bagus	150 s/d 300	3
Sedang	300 s/d 450	2
Jelek	>450	1

Jitter berhubungan dengan latensi, dimana menunjukkan banyaknya variasi *delay* pada transmisi data di jaringan. Persamaan perhitungan *jitter* adalah sebagai berikut :

$$Jitter : \frac{Total\ Variasi\ Delay}{Total\ Paket\ yang\ Diterima}$$

Berikut adalah tabel kategori *jitter* yang diambil dari jurnal

berjudul Analisis QoS (*Quality of Service*) Pada Jaringan Internet (Studi Kasus : UPT Loka Uji Teknik Penambangan Jampang Kulon-LIPI).

Table 4 Kategori Jitter

Kategori Jitter	Jitter (ms)	Indeks
Sangat Bagus	0	4
Bagus	0 s/d 75	3
Sedang	75 s/d 125	2
Jelek	125 s/d 225	1

Menurut rekomendasi ITU-T G.114 (ITU-T Recommendation, 2003: No Page), batasan *delay* adalah sebagai berikut :

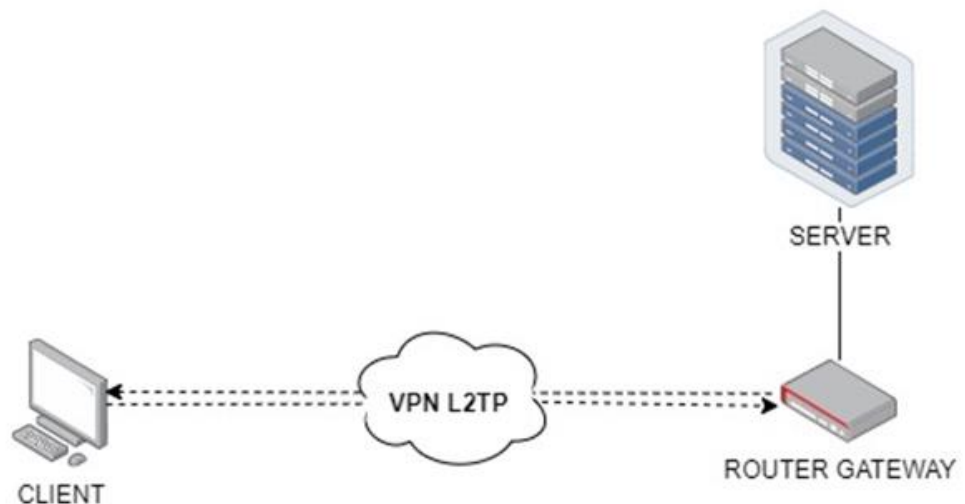
Table 5 Batasan Delay

<i>Delay Range</i>	ITU-T Recommendation
0 to 150 ms	<i>Recommended range for transmission delay</i>
150 to 400 ms	<i>Recommended if the designers are aware of reduced quality</i>
400 ms and greater	<i>Not recommended, although it may be necessary in some extraordinary cases</i>

BAB III PERANCANGAN

3.1 Deskripsi Umum Sistem

Secara umum, proses komunikasi L2TP adalah sebagai berikut :

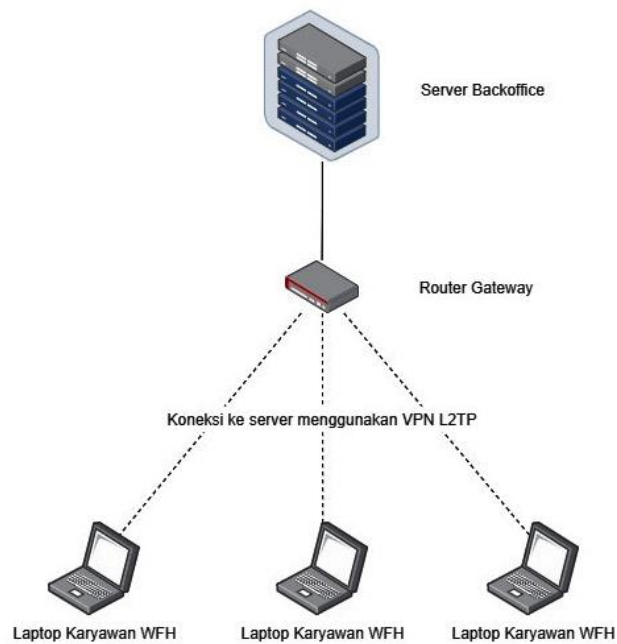


Gambar 1 Proses Komunikasi L2TP

1. *Client* melakukan koneksi ke router via VPN L2TP menggunakan IP Publik router
2. *Client* melakukan konfigurasi L2TP pada perangkatnya dengan menginput IP Publik, IPSec *presared key*, *username* dan *password*, kemudian setelah itu mulai menginisiasi *tunnel* L2TP ke router *gateway*
3. Jika router *gateway* menerima koneksi, *client* kemudian mengenkapsulasi PPP dengan L2TP dan dikirimkan ke router *gateway* melalui koneksi *tunnel*
4. Router kemudian menerima *frame incoming* PPP, kemudian melakukan validasi *user* dan menetapkan alamat IP *client*

3.2 Perancangan Topologi L2TP di PT. Royal Assetindo

Berikut adalah topologi jaringan yang dirancang pada PT. Royal Assetindo :



Gambar 2 Topologi Jaringan PT. Royal Assetindo

3.3 Spesifikasi *Client*

3.3.1 Spesifikasi *Hardware*

Spesifikasi *hardware* yang digunakan adalah sebagai berikut

:

Table 6 Spesifikasi *Hardware*

Processor	Ryzen 3 3200U 2,6 GHz
RAM	8 GB
SSD	500 GB
OS	Windows 10

3.3.2 Spesifikasi Router

Router yang digunakan adalah Mikrotik CCR1009-7G-1C dengan spesifikasi sebagai berikut :

Table 7 Spesifikasi Router

CPU Nominal Frequency	1.2 GHz
CPU Core Count	9
RAM	2 GB
10/100/1000 Ethernet Ports	7

3.4 Winbox

Untuk proses remote mikrotik aplikasi yang akan digunakan adalah Winbox.



Gambar 3 Winbox

3.5 Wireshark

Aplikasi ini digunakan pada saat pengujian QoS. Dimana pada saat pengujian QoS akan dilihat angka dari parameter-parameter yang diuji untuk diolah nantinya, sehingga dapat diketahui hasil apakah L2TP yang telah dirancang mempunyai kualitas yang baik atau tidak.

3.6 Cara Menghitung *Quality of Service* (QoS)

Pada bagian ini akan dijelaskan bagaimana menghitung hasil dari parameter-parameter yang telah diuji.

1. *Throughput*

Cara untuk mencari nilai dari parameter *throughput* ini adalah sebagai berikut :

Statistics			
Measurement	Captured	Displayed	Marked
Packets	3404	3043 (89.4%)	—
Time span, s	70.034	60.779	—
Average pps	48.6	50.1	—
Average packet size, B	217	214	—
Bytes	740094	651202 (88.0%)	0
Average bytes/s	10 k	10 k	—
Average bits/s	84 k	85 k	—

Gambar 4 Tampilan Capture File Properties

Dari tampilan ini diketahui jumlah data dikirim adalah 740094, angka tersebut dapat dilihat dari data *Bytes*. Kemudian untuk waktu dapat dilihat dari data *Time span* yaitu 70.034 s, sehingga nilai *throughput*-nya adalah “jumlah data dikirim” dibagi dengan “waktu pengamatan”.

$740094 : 70.034 = 10567$ hasil ini masih dalam satuan *Bytes/s*, kemudian dirubah ke dalam satuan *Mbit/s* = 0.08062 dibulatkan menjadi 0.80 *Mbit/s*.

2. Jitter

Dalam Wireshark, *jitter* dapat diketahui dengan melihat data yang ada pada kategori “Mean Jitter”.

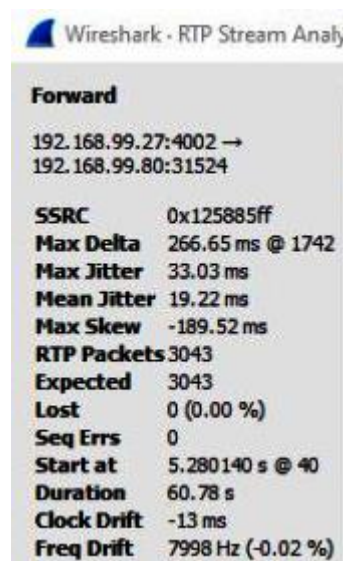
Wireshark · RTP Stream Analy	
Forward	
192.168.99.27:4002 → 192.168.99.80:31524	
SSRC	0x125885ff
Max Delta	266.65 ms @ 1742
Max Jitter	33.03 ms
Mean Jitter	19.22 ms
Max Skew	-189.52 ms
RTP Packets	3043
Expected	3043
Lost	0 (0.00 %)
Seq Errs	0
Start at	5.280140 s @ 40
Duration	60.78 s
Clock Drift	-13 ms
Freq Drift	7998 Hz (-0.02 %)

Gambar 5 Tampilan RTP Stream Analysis

Pada tampilan di atas, dapat diketahui bahwa nilai *jitter* adalah sebesar 19.22 ms.

3. *Packet Loss*

Untuk *packet loss*, dapat dilihat langsung dari hasil Wireshark, atau bisa juga menggunakan rumus paket data yang dikirim dikurang paket data yang diterima kemudian hasilnya dibagi dengan paket data yang dikirim lalu dikali dengan seratus persen (100%).



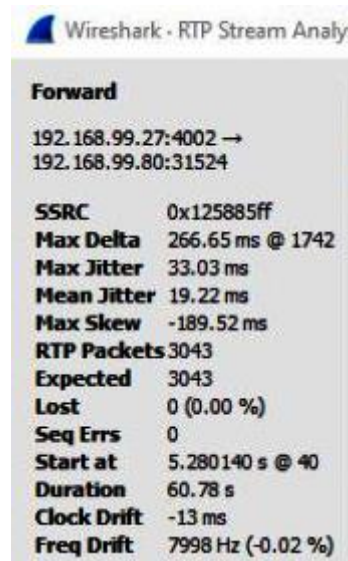
Wireshark · RTP Stream Analysis	
Forward	
192.168.99.27:4002 → 192.168.99.80:31524	
SSRC	0x125885ff
Max Delta	266.65 ms @ 1742
Max Jitter	33.03 ms
Mean Jitter	19.22 ms
Max Skew	-189.52 ms
RTP Packets	3043
Expected	3043
Lost	0 (0.00 %)
Seq Errs	0
Start at	5.280140 s @ 40
Duration	60.78 s
Clock Drift	-13 ms
Freq Drift	7998 Hz (-0.02 %)

Gambar 6 Tampilan RTP Stream Analysis

Paket data yang dikirim apabila dilihat dari tampilan di atas adalah 3043 ms, paket data yang diterima adalah 3043 ms, sehingga $((3043 - 3043) / 3043) \times 100\%$ sama dengan 0%.

4. *Delay*

Untuk mencari *delay*, dapat digunakan rumus jarak waktu antara paket awal dan akhir lalu dibagi dengan paket yang diterima.



Gambar 7 Tampilan RTP Stream Analysis

Jarak waktu dapat dilihat pada bagian “Duration” yaitu 60.78 s dibagi dengan paket data sebesar 3043 hasilnya menjadi 0.019 s.