

## Analisa Jaringan VPN MPLS L3 dan L2 Dimasa Pandemi COVID-2019 untuk Mendukung Work From Home

<sup>1</sup>Haeruddin, <sup>2</sup>Efendi

<sup>1</sup>Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Internasional Batam

<sup>2</sup>Sistem Informasi, Fakultas Ilmu Komputer, Universitas Internasional Batam

Alamat Surat

Email: [haeruddin@uib.ac.id](mailto:haeruddin@uib.ac.id), [1831165.efendi@uib.edu](mailto:1831165.efendi@uib.edu)

Article History:

Diajukan: 27 Maret 2022; Direvisi: 15 April 2022; Accepted: 25 April 2022

### ABSTRAK

Pada akhir tahun 2019 sampai 2021 virus corona (COVID-19) telah melanda sebagian besar negara, penggunaan teknologi informasi dan komunikasi sebagai pedoman dalam pembatasan jarak sosial yang diajukan pemerintah dan departemen kesehatan pada masa pandemi. Tujuan pada penelitian ini yaitu bagaimana mengimplementasikan dan membandingkan penggunaan jaringan MPLS VPN L3 dan L2 pada masa COVID-19 untuk mendukung dunia pendidikan dan industri dengan menggunakan parameter Implementasi, Quality of Service (QoS), Keamanan, dan Skalabiliti. Pada penelitian ini metode yang digunakan adalah *Network Development Life Cycle* (NDLC), dengan menggunakan beberapa tahapan yaitu analisis, desain, penerapan, dan pemantauan. Hasil dari penelitian ini memberikan gambaran pada dunia pendidikan dan industri dalam menentukan dan mengimplementasikan teknologi MPLS yang sesuai dengan kebutuhan.

**Kata kunci:** *Multi Protocol Label Switching; Network Development Life Cycle; Security; Quality of Service; Virtual Private Network*

### ABSTRACT

*From the end of 2019 to 2021 the coronavirus (COVID-19) had hit most countries, the use of information and communication technology as a guide in social distancing restrictions proposed by the government and the health department during the pandemic. The purpose of this study is how to implement and compare the use of MPLS VPN L3 and L2 networks during the COVID-19 period to support the world of education and industry by using implementation parameters, Quality of Service (QoS), security, and scalability. In this research, the method used is the Network Development Life Cycle (NDLC), using several stages, namely analysis, design, implementation, and monitoring. The results of this study provide an overview of the world of education and industry in determining and implementing MPLS technology that suits their needs.*

**Keywords:** *Multi Protocol Label Switching; Network Development Life Cycle; Security; Quality of Service; Virtual Private Network*

### 1. PENDAHULUAN

Pada akhir tahun 2019 sampai 2021 virus corona (COVID-19) telah melanda sebagian besar negara, penggunaan teknologi informasi dan komunikasi sebagai pedoman dalam pembatasan jarak sosial yang diajukan pemerintah dan departemen kesehatan pada masa pandemi. Pembatasan Sosial Berskala Besar (PSBB) diatur pemerintah dalam, Nomor 21 tahun 2020 tentang Pembatasan Sosial Berskala Besar dalam Rangka Percepatan Penanganan *Corona Virus Disease* 2019 (COVID-19)

(Sekretariat kabinet Republik Indonesia, 2020b). Teknik peraturan tersebut dituangkan dalam Peraturan Menteri Kesehatan Republik Indonesia Nomor 9 Tahun 2020 (Biro Hukum dan Organisasi Kementerian Kesehatan Republik Indonesia, 2020). Penutupan sekolah dan sebagian besar industri banyak mengambil tindakan belajar dan bekerja secara daring dan biasa di sebut *Work From Home* (WFH)(Komalasari, 2020; Saragih et al., 2020). Namun setiap organisasi atau perusahaan tidak mempublikasikan datanya secara publik. Untuk menghubungkan akses data internal suatu organisasi atau perusahaan melalui jaringan internet secara aman, membutuhkan teknologi yang disebut dengan *Virtual Private Network* (VPN) (Dahnial, 2019; Firdausi & Wardani, 2020).

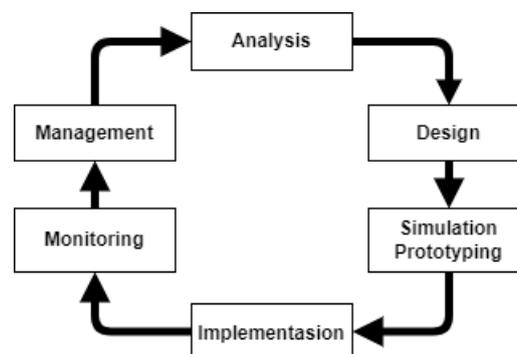
*Virtual Private Network* adalah sebuah jaringan komunikasi *private* menggunakan jaringan publik dengan keamanan *Internet Protocol Security* (IPSec). *Virtual Private Network* yaitu teknologi jaringan *Local Area Network* yang diterapkan pada *Wide Area Network* sehingga memudahkan pengaksesan data asalkan terhubung ke jaringan internet (Hidayatulloh & Wahyudin, 2019; Sari et al., 2020). Dengan teknologi yang terus berkembang, *Internet Service Provider* (ISP) menerapkan teknologi MPLS VPN yang menyediakan layanan *Virtual Private Network* (VPN) yang melewati jaringan *Multi Protocol Label Switching* (MPLS) milik ISP (Mardianto, 2019).

*Multi Protocol Label Switching* (MPLS) yaitu teknologi penyampaian data dengan metode *forwarding* yang meneruskan data informasi dalam label akan dikirimkan sesuai dengan tujuan label. Dengan menggunakan *Multi Protocol Label Switching* (MPLS) router akan melakukan pembacaan label pada tiap data yang dikirimkan dan akan diteruskan ke alamat tujuan, sehingga data yang dikirimkan lebih cepat tanpa harus melewati tabel routing tujuan (Kahfi & Purnawan, 2018). MPLS yaitu gabungan 2 *layer*, dengan memanfaatkan kecepatan *switching* pada *layer 2* dan *routing* pada *layer 3*. Dimana label yang dihasilkan oleh *Label-Switching* router akan menjadi penghubung jaringan *Multi Protocol Label Switching* (MPLS) dengan jaringan luar (Arnita & Farid, 2020; Nurhayati et al., 2020).

Tujuan dari penelitian penulis adalah untuk mengetahui jaringan VPN yang mana paling tepat berdasarkan kelas dunia pendidikan dan industri, serta harga dan keamanan jaringan MPLS.

## 2. METODE

Penelitian ini menggunakan metode *Network Development Life Cycle*, penelitian yang digunakan dari referensi penelitian sebelumnya. Untuk melakukan perbandingan pada jaringan MPLS VPN dengan menggunakan metode ini, penulis akan melakukan konfigurasi untuk menghubungkan jaringan *local* dengan MPLS VPN. Berikut tahapan-tahapan metode penelitian yang penulis gunakan:



Gambar 1. *Network Development Life Cycle*  
(Mardan & Barovich, 2018)

1. *Analysis*: pada tahap ini penulis akan melakukan analisa secara keseluruhan mengenai permasalahan, kebutuhan jaringan, protokol yang digunakan untuk pengujian, maupun parameter yang digunakan, meliputi *hardware* dan *software* yang akan digunakan serta biaya implementasi MPLS VPN.

2. *Design*: dari data analisis yang didapatkan, penulis akan melakukan penggambaran topologi yang akan digunakan untuk penerapan pada jenis jaringan MPLS VPN L2 dan L3
3. *Implementation*: pada tahap ini penulis akan melakukan implementasi jaringan MPLS VPN L2 dan L3 dengan menggunakan Eve-ng.
4. *Monitoring*: setelah melakukan penerapan rancangan jaringan yang telah selesai dilakukan, penulis akan melakukan pemantauan dan pengujian terhadap parameter yang telah ditentukan. Dengan melakukan pemantauan kedua jaringan MPLS VPN yaitu L2 dan L3 yang dimulai dengan *Packet Loss, Throughput, Delay, Jitter*. Hasil pengujian akan dilampirkan menjadi tiga parameter yaitu *Security, Quality of Service, dan Scalability*.

### 3. HASIL DAN PEMBAHASAN

#### 3.1 Analysis

Pada tahap *analysis*, berikut hasil analisis berdasarkan rujukan dan observasi yang telah dibuat:

##### 1. Cara kerja jaringan MPLS VPN L2 dan L3

Jaringan MPLS VPN L2 menggunakan metode *end-to-end* dimana jaringan terhubung langsung melalui jaringan ISP. Jaringan MPLS VPN L2 ini memperluas konektivitas *client* dengan infrastruktur MPLS, sehingga seperti terhubung langsung dengan *switch*. Sedangkan jaringan MPLS VPN L3 menggunakan metode komunikasi *peer-to-peer*, dimana jaringan tersebut dihubungkan dengan menggunakan protokol *routing* untuk menghubungkan jaringan komunikasi yang berjauhan (Aye, 2019; Saraswati et al., 2020).

##### 2. Kelebihan dan kekurangan MPLS VPN L2 dan L3

Kelebihan dari jaringan MPLS VPN L2 yaitu tidak membutuhkan router tambahan dan *packet loss* pada jaringan ini dikategorikan *perfect* sedangkan kekurangan pada jaringan ini yaitu rata-rata *throughput, delay, dan jitter* tidak stabil dibandingkan MPLS VPN L3 dan menggunakan metode komunikasi *end-to-end* dimana perangkat bisa langsung terhubung.

Kelebihan dari jaringan MPLS VPN L3 yaitu keamanan jaringan *local* yang terhubung dapat dikelola, dikarenakan membutuhkan router tambahan untuk menjalankan *routing* serta metode komunikasi yang digunakan *peer-to-peer* dan rata-rata pengukuran *Quality of Service* pada parameter *throughput, packet loss, delay, dan jitter* masuk dalam rata-rata kategori yang bagus, sedangkan kekurangan pada jaringan ini yaitu dari harga untuk menggunakan layanan ini tinggi.

##### 3. Biaya berlangganan MPLS VPN

Dari hasil observasi penulis dengan beberapa provider yang ada, berikut tabel biaya berlangganan MPLS VPN penulis dapatkan dari provider TELKOM:

Tabel 1. Harga Berlangganan MPLS VPN

BANDWIDTH (Kbps)	INSTALASI	Tarif per Bulan					
		PAKET 1	PAKET 2	PAKET 3	PAKET 4	PAKET 5	PAKET 6
128	Rp. 2.250.000	Rp. 3.237.000	Rp. 2.810.800	Rp. 2.734.000	Rp. 2.659.900	Rp. 2.561.100	Rp. 2.487.000
256		Rp. 4.394.000	Rp. 3.683.400	Rp. 3.555.000	Rp. 3.431.700	Rp. 3.267.300	Rp. 3.144.000
512		Rp. 5.603.000	Rp. 4.595.400	Rp. 4.413.000	Rp. 4.238.400	Rp. 4.005.600	Rp. 3.831.000
1.024		Rp. 7.763.432	Rp. 6.225.102	Rp. 5.946.992	Rp. 5.680.170	Rp. 5.324.406	Rp. 5.057.584
2.048		Rp. 11.118.648	Rp. 8.756.282	Rp. 8.329.288	Rp. 7.919.474	Rp. 7.373.054	Rp. 6.963.240
3.072		Rp. 12.978.712	Rp. 10.159.802	Rp. 9.650.208	Rp. 9.161.251	Rp. 8.509.309	Rp. 8.020.352
4.096		Rp. 14.792.248	Rp. 11.527.534	Rp. 10.937.280	Rp. 10.371.043	Rp. 9.616.061	Rp. 9.049.824
5.120		Rp. 16.890.880	Rp. 13.111.100	Rp. 12.477.880	Rp. 11.772.200	Rp. 10.897.960	Rp. 10.242.280
6.144		Rp. 19.321.920	Rp. 14.944.439	Rp. 14.153.032	Rp. 13.393.773	Rp. 12.381.427	Rp. 11.622.168
7.168		Rp. 22.105.216	Rp. 17.057.989	Rp. 16.150.928	Rp. 15.271.702	Rp. 14.099.402	Rp. 13.220.176
8.192		Rp. 25.247.616	Rp. 19.481.317	Rp. 18.464.336	Rp. 17.446.333	Rp. 16.088.995	Rp. 15.070.992
9.216		Rp. 29.165.056	Rp. 22.370.366	Rp. 21.142.368	Rp. 19.963.560	Rp. 18.391.816	Rp. 17.213.008
10.240		Rp. 32.620.000	Rp. 24.976.994	Rp. 23.595.856	Rp. 22.269.750	Rp. 20.501.610	Rp. 19.175.504

##### 4. Kebutuhan MPLS VPN

Perangkat yang perlu disiapkan dalam penerapan MPLS VPN yaitu router sebagai penghubung antara jaringan *local* dengan jaringan ISP. Berlangganan MPLS VPN yang ada berdasarkan kebutuhan. UPS (*Uninterruptable Power Supply*), *Grounding System*, dan perizinan penempatan antena. Penulis juga akan memberikan referensi router mikrotik yang dapat dijadikan sebagai rujukan dalam pengimplementasian jaringan MPLS VPN yaitu, sebagai berikut:

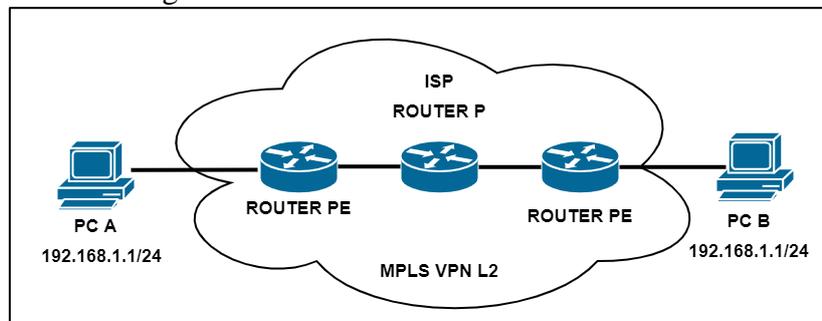
Tabel 2. Rekomendasi *Hardware*

No	Brand	Tipe	Kisaran Harga	Spesifikasi
1	Mikrotik	RB750Gr3(hEX), Router mikrotik RB760iGS (hEX S), RB1100Ahx4	Rp. 860.000-Rp. 4.000.000	10-20 <i>client</i>
2	Mikrotik	RB3011UiAS-RM	Rp. 2.830.000	20-50 <i>client</i>
3	Mikrotik	RB4011iGS+RM, CCR1009-7G-1C-1S+	Rp. 3.147.000-Rp. 7.810.000	50-100 <i>client</i>
4	Cisco	900 Series ISR	Rp. 7.700.000	20-50 <i>client</i>
5	Cisco	1000 Series ISR	Rp. 15.300.000	50-100 <i>client</i>

Pada tahapan ini pengumpulan data terkait jaringan MPLS VPN L2 dan L3 yang meliputi cara kerja, kelebihan dan kekurangan, harga, dan kebutuhan dalam penerapan serta rekomendasi *hardware* untuk penerapan.

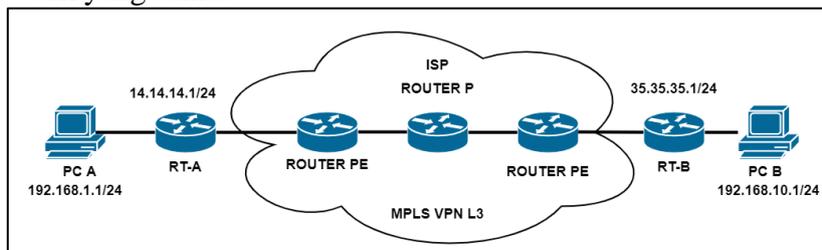
### 3.2 Design

Pada tahap ini melakukan gambaran topologi jaringan MPLS VPN L2 dan L3 yang akan diimplementasikan sebagai berikut:



Gambar 2. Topologi MPLS VPN L2

Dari gambar 2. topologi jaringan MPLS VPN L2 dapat terhubung langsung asalkan berada pada ip network yang sama.



Gambar 3. Topologi MPLS VPN L3

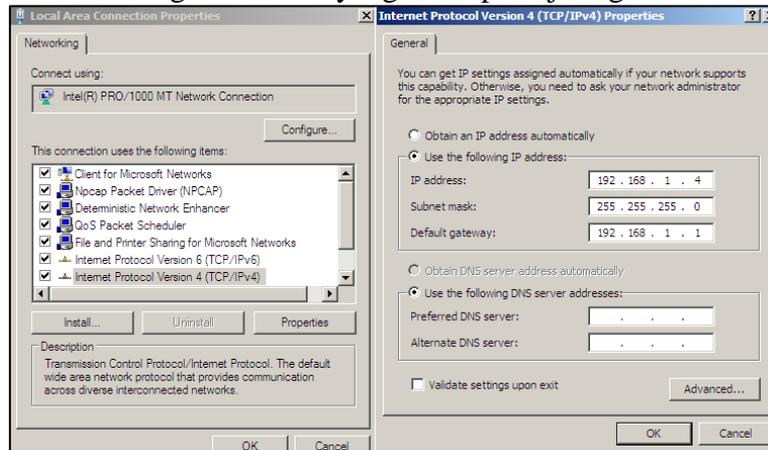
MPLS VPN L3 memiliki jaringan yang harus dihubungkan dengan router dikarenakan perlu menjalankan protokol *routing OSPF* untuk menghubungkan jaringan MPLS pada router PE dengan router local (CE) dengan network yang berbeda.

### 3.3 Implementation

Selanjutnya pada tahapan ini melakukan implementasi MPLS VPN L2 dan L3, dimana hasil konfigurasi ini akan diteruskan ke tahap monitoring. Berikut konfigurasi jaringan MPLS L2 dan L3:

#### 1. Konfigurasi MPLS VPN L2

Tambahkan Alamat IP dengan *network* yang sama pada jaringan MPLS VPN L2.



Gambar 4. Pengecekan IP DHCP

Jaringan MPLS L2 dapat langsung dihubungkan tanpa menggunakan router tambahan, dengan menambahkan alamat *network* MPLS VPN L2 sudah dapat saling berkomunikasi.

#### 2. Konfigurasi MPLS VPN L3

Berikut tahapan konfigurasi jaringan MPLS VPN L3:

Tambahkan ip address untuk jaringan komputer local dan ip address router yang telah diberikan ISP, dan route gateway untuk router seperti di gambar 5.

```
[admin@R4] /ip address> add address=14.14.14.4/24 interface=ether1
[admin@R4] /ip address> add address=192.168.1.1/24 interface=ether2
[admin@R4] /ip address> /ip route
[admin@R4] /ip route> add gateway=14.14.14.1
```

Gambar 5. Tambah Alamat IP

Selanjutnya tambahkan DHCP server untuk memberikan alamat ip langsung ke user seperti berikut ini.

```
[admin@R4] > ip pool add name=dhcp-pool ranges=192.168.1.2-192.168.1.50
[admin@R4] > ip dhcp-server network add address=192.168.1.0/24 gateway=192.168.1.1
[admin@R4] > ip dhcp-server add interface=ether2 address-pool=dhcp-pool lease-time=3d
[admin@R4] > ip dhcp-server print
Flags: D - dynamic, X - disabled, I - invalid
# NAME INTERFACE RELAY ADDRESS-POOL LEASE-TIME ADD-ARP
0 X dhcp1 ether2 dhcp-pool 3d
[admin@R4] > ip dhcp-server enable 0
```

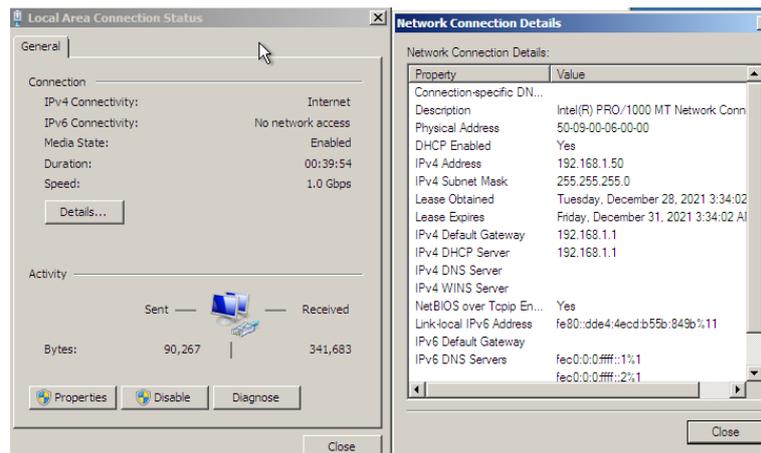
Gambar 6. Tambah DHCP Server

Pada tahap selanjutnya tambahkan routing ospf seperti gambar 7.

```
[admin@R4] /routing> /routing ospf network
[admin@R4] /routing ospf network> add network=14.14.14.0/24 area=backbone
[admin@R4] /routing ospf network> add network=192.168.1.0/24 area=backbone
```

Gambar 7. Penambahan Routing OSPF

Kemudian pada PC *client* dapat dipastikan network pada PC tersebut sudah dhcp. Agar dapat mendapatkan IP jaringan yang telah dibuat.



Gambar 8. Pengecekan IP DHCP

Pada jaringan MPLS VPN L3 menerapkan DHCP server untuk memberikan alamat ip pada jaringan lokal dan *routing* OSPF untuk mendistribusikan routing antar jaringan *network*.

### 3.4 Monitoring

#### 1. Security MPLS VPN

Memiliki tingkat keamanan yang tinggi dikarenakan jaringan MPLS VPN menggunakan fasilitas tunnel dengan jalur jaringan yang dijalankan secara *site-to-site*, jaringan MPLS VPN hanya dapat diakses oleh *user* yang berada pada satu jaringan (*private connection*) (Chairunnisa et al., 2018). Pada penelitian (Saraswati et al., 2020), melakukan penyerangan pada router PE dan CE dengan menggunakan tools LOKI untuk melakukan serangan bruteforce. Dari hasil pengujian serangan algoritma Secure Hash Algorithm (SHA) tidak berhasil meng-cracking key-string yang sudah dikonfirmasi.

Pada penelitian sebelumnya yang dijadikan rujukan keamanan jaringan MPLS VPN memiliki tingkat keamanan yang tinggi dikarenakan fasilitas tunnel dan dijalankan secara *site to site*.

#### 2. Quality of Service

Agar dapat membandingkan jaringan MPLS VPN L2 dan L3 akan melakukan pengujian jaringan QoS untuk dengan *protocol* TCP dan melakukan limitasi *bandwith* 5 MB, 10 MB, 15 MB, dan 20 MB, untuk membandingkan protokol MPLS VPN L2 dan L3 dengan percobaan pengiriman file sebesar 5 MB. Berikut hasil pengujian *Quality of Service* (QoS):

Dari hasil pengukuran nilai pada jaringan MPLS VPN L3 lebih stabil dibandingkan MPLS VPN L2, nilai dari *throughput* MPLS VPN L2 dan L3 dengan menggunakan standar *TIPHON* dapat di kategorikan *good*.

Tabel 3. Hasil Analisa Parameter *Througput*

<i>Througput</i>						
<i>Protocol</i>	<i>Source</i>	<i>Destination</i>	Limit Bandwidth (Megabit)	Jumlah Paket Kirim (Megabyte)	VPN MPLS L2 (Kbps)	VPN MPLS L3 (Kbps)
TCP	<i>Client</i>	<i>Server</i>	5	5	884	843
	<i>Client</i>	<i>Server</i>	10	5	802	832
	<i>Client</i>	<i>Server</i>	15	5	867	803
	<i>Client</i>	<i>Server</i>	20	5	733	841

Dari hasil pengukuran *Quality of Service* pada parameter *packet loss*, untuk jaringan MPLS VPN L2 dan L3 memiliki *packet loss* dengan kategori *perfect* dari standar *TIPHON*.

Tabel 4. Hasil Analisa Parameter *Packet Loss*

<i>Packet Loss</i>						
<i>Protocol</i>	<i>Source</i>	<i>Destination</i>	<i>Limit Bandwidth (Megabit)</i>	<i>Jumlah Paket Kirim (Megabyte)</i>	<i>VPN MPLS L2 (%)</i>	<i>VPN MPLS L3 (%)</i>
TCP	<i>Client</i>	<i>Server</i>	5	5	0	0
	<i>Client</i>	<i>Server</i>	10	5	0	0
	<i>Client</i>	<i>Server</i>	15	5	0	0
	<i>Client</i>	<i>Server</i>	20	5	0	0

Selanjutnya pada parameter *delay*, dari percobaan dengan limitasi *bandwidth* nilai *delay* MPLS VPN L3 lebih stabil dan untuk hasil pengujian jaringan MPLS VPN L2 dan L3 di kategorikan *best* dari standar *TIPHON*.

Tabel 5. Hasil Analisa Parameter *Delay*

<i>Delay</i>						
<i>Protocol</i>	<i>Source</i>	<i>Destination</i>	<i>Limit Bandwidth (Megabit)</i>	<i>Jumlah Paket Kirim (Megabyte)</i>	<i>VPN MPLS L2 (ms)</i>	<i>VPN MPLS L3 (ms)</i>
TCP	<i>Client</i>	<i>Server</i>	5	5	7,6899929	8,05632
	<i>Client</i>	<i>Server</i>	10	5	8,5159397	8,0755
	<i>Client</i>	<i>Server</i>	15	5	7,8125178	8,49011
	<i>Client</i>	<i>Server</i>	20	5	9,2922486	8,06871

Selanjutnya melakukan pengujian pada parameter *jitter* untuk melihat kestabilan *forwarding* data. Dari hasil analisa tabel dibawah, nilai *jitter* pada jaringan MPLS VPN L3 dan L2 masuk dalam kategori *perfect* dari standar *TIPHON*.

Tabel 6. Hasil Analisa Parameter *Jitter*

<i>Jitter</i>						
<i>Protocol</i>	<i>Source</i>	<i>Destination</i>	<i>Limit Bandwidth (Megabit)</i>	<i>Jumlah Paket Kirim (Megabyte)</i>	<i>VPN MPLS L2 (ms)</i>	<i>VPN MPLS L3 (ms)</i>
TCP	<i>Client</i>	<i>Server</i>	5	5	7,671601	8,05361
	<i>Client</i>	<i>Server</i>	10	5	8,4646536	7,98425
	<i>Client</i>	<i>Server</i>	15	5	7,7814285	8,45477
	<i>Client</i>	<i>Server</i>	20	5	9,0212047	8,18876

Pada tahap pengujian *Quality of Service* dapat dilihat jaringan MPLS VPN L3 memiliki hasil rata-rata pengujian yang lebih stabil dibandingkan MPLS VPN L2.

### 3. Scalability

*Scalability* pada jaringan MPLS VPN yaitu hanya jaringan komputer atau smartphone yang terhubung langsung dengan jaringan internet yang berlangganan MPLS VPN sehingga dapat menggunakan layanan MPLS.

## 4. SIMPULAN DAN SARAN

Berdasarkan hasil dari penelitian jaringan MPLS VPN L2 dan L3 yaitu, untuk menggunakan jaringan MPLS harus berlangganan layanan MPLS pada *Internet Service Provider* yang menyediakan layanan tersebut adalah PT Telkom. Serta harga untuk MPLS relatif lebih mahal dibandingkan dengan internet biasa atau *broadband*, untuk *Quality of Service* jaringan MPLS lebih stabil dibandingkan dengan MPLS VPN L2 dan untuk kedua jaringan tersebut memiliki keamanan yang tinggi, di karenakan menggunakan fasilitas tunnel dan dijalankan secara *site to site*.

## 5. DAFTAR PUSTAKA

- Arnita, A., & Farid, M. (2020). Implementasi Jaringan Virtual Private Network dengan Teknologi Multi Protocol Label Switching (MPLS). *JRTI (Jurnal Riset Tindakan Indonesia)*, 5(2), 28–40.
- Aye, T. Z. (2019). Analysis of Multiprotocol Label Switching on Virtual Private Network. *International Journal of Innovative Science Dan Research Technology*, 4(3), 698–702. <https://doi.org/10.1109/I-SMAC.2018.8653745>
- Chairunnisa, S., Munadi, R., & Sanjoyo, D. D. (2018). Analisis Performansi Quality Of Service Inter as MPLS-VPN Back-To-Back VRF pada Layanan IMS. *E-Proceeding of Engineering*, 5(3), 4560–4567. <https://libraryproceeding.telkomuniversity.ac.id/index.php/engineering/article/download/7625/7512>
- Dahnial, D. (2019). Analisa Perbandingan Quality Of Service Antara Protokol PPTP dan L2TP Pada Virtual Private Network Berbasis Router Mikrotik. *Jurnal Ilmiah Informatika Global*, 10(2), 107–113. <https://doi.org/10.36982/jig.v10i2.858>
- Firdausi, A., & Wardani, H. W. (2020). Simulasi dan Analisa QoS dalam Jaringan VPN Site To Site Berbasis IPsec dengan Routing Dynamic. *Jurnal Telekomunikasi Dan Komputer*, 10(2), 49–56. <https://doi.org/10.22441/incomtech.v10i2.8131>
- Hidayatulloh, S., & Wahyudin. (2019). Perancangan Wide Area Network (WAN) dengan Teknologi Virtual Private Network (VPN). *JURNAL TEKNIK KOMPUTER AMIK BSI*, 5(1), 7–14. <https://doi.org/10.31294/jtk.v4i2>
- Kahfi, A., & Purnawan, P. W. (2018). Simulasi dan Analisis Qos Pada Jaringan Mpls Ipv4 dan Ipv6 Berbasis Routing OSPF. *Jurnal Maestro*, 1(1), 73–79.
- Komalasari, R. (2020). Manfaat Teknologi Informasi Dan Komunikasi Di Masa Pandemi Covid 19. *Tematik*, 7(1), 38–50. <https://doi.org/10.38204/tematik.v7i1.369>
- Mardan, Q., & Barovich, G. (2018). Remanajemen Infrastruktur Jaringan dalam Meningkatkan Kinerja pada PT. Jasa Raharja cabang Sumatera Selatan. *Konferensi Nasional Sistem Informasi ...*, 8–9. <http://jurnal.atmaluhur.ac.id/index.php/knsi2018/article/view/399>
- Mardianto. (2019). Analisis Quality Of Service (QoS) pada Jaringan VPN dan MPLS VPN Menggunakan GNS3. *Jurnal Sains Dan Informatika*, 5(2), 98–107. <https://doi.org/10.34128/jsi.v5i2.191>
- Nurhayati, A., Holiyastuta, R. P., & Iskandar, A. R. (2020). Implementasi Virtual Private Network pada Jaringan Multi Protocol Label Switching Traffic Engineering. *Journal of Informatics and Communications Technology (JICT)*, 21(1), 28–40.
- Saragih, N. I., Hartati, V., & Fauzi, M. (2020). Tren, Tantangan, dan Perspektif dalam Sistem Logistik pada Masa dan Pasca (New Normal) Pandemi Covid-19 di Indonesia. *Jurnal Rekayasa Sistem Industri*, 9(2), 77–86. <https://doi.org/10.26593/jrsi.v9i2.4009.77-86>
- Saraswati, M., Iqbal, M., & Irawati, I. D. (2020). Implementasi dan Analisis Jaringan MPLS Menggunakan Algoritma SHA sebagai Keamanan Jaringan pada Komunikasi VOIP. *E-Proceeding of Applied Science*, 6(2), 3754–3774.
- Sari, A. P., Sulistiyono, & Kemala, N. (2020). Perancangan Jaringan Virtual Private Network Berbasis IP Security Menggunakan Router Mikrotik. *Jurnal PROSISKO*, 7(2), 150–164.