

SIMULASI PERANCANGAN DAN IMPLEMENTASI REDUNDANT LINK MULTI PROTOCOL LABEL SWITCHING (MPLS) VIRTUAL PRIVATE NETWORK (VPN) PT. INDONESIA COMNETS PLUS MENGGUNAKAN MIKROTIK ROUTER OS

Radiansyah Akbar¹⁾, Andi Suprianto²⁾

Program Studi Teknik Informatika, Fakultas sains dan Teknologi Informasi
Institut Sains dan Teknologi Nasional

Jl. Moch. Kahfi II, Bhumi Srengseng Indah, Jagakarsa, Jakarta Selatan 12640

Telp.(021).7270090, Fax.(021)7866955

ricardoakbar3@gmail.com, andisuprianto@istn.ac.id

ABSTRAK

Saat ini kebutuhan teknologi informasi dan komunikasi telah berkembang pesat, khususnya di bidang layanan komunikasi dan jaringan. PT. Indonesia Comnets Plus sebagai *service provider* membutuhkan jaringan yang baik untuk pengiriman data dari kantor pusat yaitu kantor Cawang menuju kantor cabang yang berada di Duren Tiga. PT. Indonesia Comnets Plus menginginkan kantor Cawang sebagai pusat memiliki jalur *main* dan *backup* agar ketika jalur *main* nya *mati* kantor Cawang tetap bisa beroperasi menggunakan jalur *backup*. Salah satu konsep yang dapat di terapkan untuk mengatasi permasalahan tersebut adalah menggunakan metode *redundant link* dengan menerapkan sistem *main link* dan *backup link* otomatis. Sistem *main link* dan *backup link* dapat di terapkan pada *MPLS VPN* dengan menggunakan *routing Border Gateway Protocol (BGP)* dengan menambahkan *attribute AS PATH Prepend*. Penelitian ini akan melakukan implementasi *Multi Protocol Label Switching (MPLS) Virtual Private Network (VPN) Redundant Link* dan melakukan pengujian untuk memastikan bahwa *main link* dan *backup link* telah terimplementasi dengan benar

Kata Kunci: *Main Link, Backup Link, Mpls-Vpn, Routing Bgp, Aspath Prepend*

ABSTRACT

Currently the need for information and communication technology has grown rapidly, especially in the field of communication and network services. PT. Indonesia Comnets Plus as a service provider requires a good network for sending data from the head office, namely the Cawang office to the branch office in Duren Tiga. PT. Indonesia Comnets Plus wants the Cawang office as the center to have a main link and backup so that when the main link goes out, the Cawang office can still operate using a backup link. One of the concepts that can be applied to overcome these problems is to use the *redundant link* method by implementing a *main link* system and *automatic backup links*. *Main link* and *backup link* systems can be applied to *MPLS VPN* by using *Border Gateway Protocol (BGP) routing* by adding the *AS PATH Prepend* attribute. This research will implement *Multi Protocol Label Switching (MPLS) Virtual Private Network (VPN) Redundant Link* and conduct tests to ensure that the *main link* and *backup link* have been implemented correctly, and between the Cawang office and Duren Tiga office can communicate using the *main link*. as well as *backup paths* that have been implemented

Kata kunci: *Main Link, Backup Link, Mpls-Vpn, Routing Bgp, Aspath Prepend*.

I. PENDAHULUAN

Saat ini kebutuhan teknologi informasi dan komunikasi telah berkembang pesat, khususnya di bidang layanan komunikasi dan jaringan. Beberapa organisasi memerlukan ketersediaan jaringan untuk melindungi operasi perusahaan dari kerusakan sistem, kehilangan data, dan kesalahan pemrosesan data. Untuk saat ini semakin banyaknya penyelenggara jasa internet atau biasa disebut provider yang sudah banyak menggunakan teknologi yang bernama Multi Protocol Label Switching (MPLS), Virtual Private Network (VPN).

Redundant Link berfungsi untuk menghindari terjadinya kegagalan. Redundant Link merupakan salah satu standar dalam membangun jaringan. Salah satu aspek terpenting untuk memastikan ketersediaan tinggi adalah redundansi. (Adhiwibowo & Irawan, 2019)

Label tersebut berisi tujuan *node* selanjutnya, kemudian paket diteruskan ke *node* yang lain, di setiap proses transit paket di sebuah *node*, maka label tersebut akan dilepas dan diberikan label yang baru yang berisi tujuan berikutnya. Paket-paket tersebut diforward dalam path yang disebut Label Switching Path (LSP). Label ini ditambahkan dan juga dihilangkan oleh LER (Label Edge Router). MPLS juga telah menyiapkan *path* menuju semua kombinasi *node* yang disebut LSP (Label Switching Path). Setiap *router* yang terhubung dalam jaringan MPLS berperan dalam pembuatan LSP. Selanjutnya paket ditransmisikan ke setiap LSR (Label Switching Router) sesuai LSP yang telah ditentukan. MPLS juga memiliki beberapa fitur salah satunya kemampuan membentuk tunnel atau *virtual circuit* pada *networknya*.

Multi Protocol Label Switching (MPLS) adalah teknik penerusan data / paket melalui jaringan dengan menggunakan informasi label yang melekat pada protokol jaringan. Ini memungkinkan *Router* untuk meneruskan paket hanya dengan melihat label paket sehingga anda tidak perlu melihat alamat protokol jaringan tujuan. Jika dengan *Router Cisco* membutuhkan biaya keluar yang lebih tinggi dibandingkan dengan menggunakan *Router Mikrotik* ini bisa menjadi salah satu metode untuk mengoptimalkan jaringan dan meminimalkan biaya keluar. Jadi dengan Multi Protocol Label Switching (MPLS) yang tertanam di Mikrotik, dapat mengoptimalkan kinerja Virtual Private Network Internet Protocol, membuat transmisi data lebih cepat dan lebih

efisien, memudahkan dan juga *custom* yang meningkatkan permintaan, dan meningkatkan kualitas jaringan yang ada (arnita & farid, 2020)

II. TINJAUAN PUSTAKA

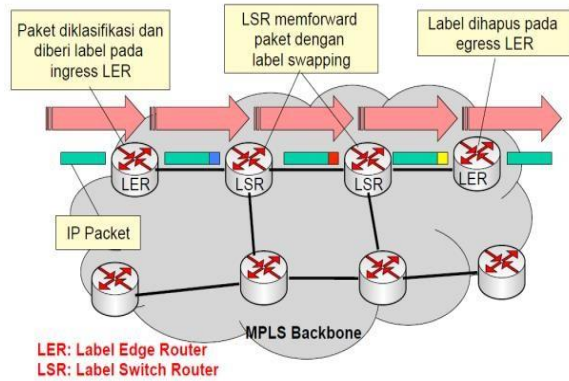
Virtual Private Network (VPN) merupakan suatu teknologi komunikasi yang telah banyak digunakan oleh Perusahaan yang bergerak di bidang jasa dan telekomunikasi, hal ini dikarenakan Virtual Private Network (VPN) menawarkan keamanan yang cukup terjamin dan dapat menghubungkan antara cabang dan pusat.

VPN selalu dikaitkan dengan *tunneling* atau terowongan yang dibangun diatas jalur lain biasanya melalui jaringan publik. Terdapat berbagai macam protokol yang digunakan dalam membangun jaringan VPN diantaranya yaitu Point to Point Protocol (PPTP), Layer 2 VPN (L2VPN) dan Layer 3 VPN (L3VPN)(Watmah, 2020.)

Multi Protocol Label Switching (MPLS) merupakan perkembangan terbaru dari *multi layer switch* yang diusahakan oleh IETF (Internet Engineering Task Force) untuk memadukan mekanisme *multi layer switch* label *swapping* di *layer 2* dengan *routing* di *layer 3* untuk mempercepat pengiriman paket. Arsitektur MPLS dipaparkan dalam RFC-3031. Hal ini dilakukan agar terdapat standar untuk *multi layer switch* dan mendukung interoperabilitas. Disebut *multi* protokol karena tekniknya dapat diterapkan pada semua protokol *layer* jaringan. MPLS adalah suatu teknologi yang mempunyai kemampuan menambah label label yang mengandung informasi jaminan *quality*, *scalability*, *reliability* dan *security* pada paket-paket IP untuk dilewatkan pada suatu jaringan *data*. (Rizkiana 2017.)

Prinsip kerja MPLS yakni dengan menggabungkan kecepatan *switching layer 2* dengan kemampuan *routing* dan *scalability layer 3*.

MPLS akan menyelipkan *label* di antara *layer 2* dan *layer 3* pada paket yang diteruskan. Label dibuat oleh Label- Switching Router (LSR) yang bertindak sebagai penghubung jaringan MPLS ke jaringan luar.



Gambar 1 Cara Kerja MPLS

Cara kerja *MPLS* adalah memberikan label pada header paket. Label *MPLS* berisi jalur yang akan ditempuh paket untuk sampai ke tujuan. Label yang berada pada ujung jaringan *MPLS* disebut Label *Edge Router (LER)*. Label ini berguna untuk mencatat dan menganalisa paket sebelum masuk ke *MPLS*. Setiap paket yang sudah diberi label akan masuk ke router berikutnya. Pada router provider edge (hop) akan dilihat informasi yang dibawa oleh paket mengenai hop berikutnya dan mengganti label paket (*swap*) dengan label baru yang ada pada router provider edge. Paket yang telah diberi label baru akan diteruskan ditujuan berdasarkan informasi routing dari router customer edge. Setelah sampai pada router customer edge tujuan akhir jaringan *MPLS*, label yang telah diteruskan dari provider edge akan dilepaskan dari header paket (*pop*). (Euginia & Ghozali, 2018)

Redundant Link merupakan salah satu standar dalam membangun jaringan. Dengan *Redundant Link*, anda tetap memiliki kesempatan untuk beristirahat dan sarapan dengan tenang walaupun bagian tertentu dari jaringan sedang *down*. Semua karena adanya cadangan. Salah satu aspek terpenting dari *redundant* yaitu memastikan ketersediaan tinggi. Untuk mencapai ketersediaan tinggi, sistem cadangan umumnya dibuat yang akan berfungsi bahkan jika sistem utama gagal dan metode diperlukan untuk menghindari kegagalan. Jika ada perangkat *Internet Service Provider (ISP)* yang tidak berfungsi, maka masih ada perangkat *ISP* yang dapat digunakan sebagai cadangan atau pengganti. (Adhiwibowo & Irawan, 2019)

Packet Loss Ratio (PLR) adalah indikasi paket

hilang yang didapat dari prosentase perbandingan antara kuantitas paket data yang sampai di penerima dengan kuantitas paket yang dikirimkan oleh pengirim. Paket yang hilang harus dikirim kembali, akan menambah total waktu pengiriman dapat disebabkan oleh beberapa kemungkinan, di antaranya yaitu :

1. Terjadinya overload trafik didalam jaringan.
2. Tabrakan (congestion) dalam jaringan.
3. Error yang terjadi pada media fisik.

Tabel 1 Kategori *Packet Loss Rasio*

Kategori	<i>Packet Loss Ratio (%)</i>	Indeks
Sangat Bagus	0 – 3 %	4
Bagus	4 – 15 %	3
Sedang	16 - 25 %	2
Buruk	26% keatas	1

Latency atau *round trip time* merupakan waktu yang dibutuhkan untuk paket mencapai ke tujuan dan kembali lagi ke sumber. Pengukuran *latency* sangat diperlukan dalam sistem yang memerlukan komunikasi interaktif dua arah. Biasanya satuan dari nilai *latency* yang dihasilkan adalah *milisecond (ms)*. Menurut standar *TIPHON*, besarnya *latency* dapat diklasifikasikan pada tabel yang ditunjukkan pada

Tabel 2 Kategori *Latency*

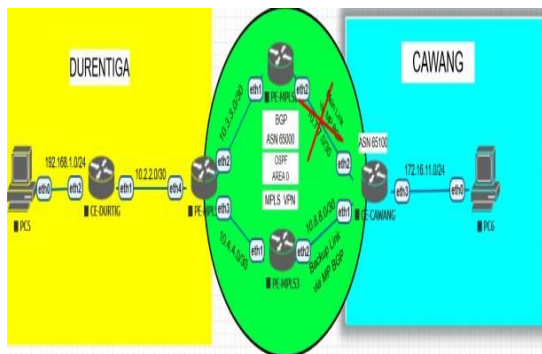
Besar <i>Delay</i>	Kategori <i>Latency</i>	Indeks
<150 ms	Sangat Bagus	4
150 – 300 ms	Bagus	3
300 – 400 ms	Sedang	2
>450 ms	Buruk	1

III. METODE PENELITIAN

Berdasarkan penelitian ini di PT. Indonesia Comnets Plus menerapkan sistem *MPLS VPN* untuk menunjang mempercepat proses *switching*, meningkatkan keamanan dan

memudahkan implementasi jaringan. Dalam penelitian ini diterapkan di kantor PT. Indonesia Comnets Plus Cawang dan PT. Indonesia Comnets Plus Durentiga, dimana kantor Cawang ini menggunakan *Main-Backup (Redundant Link)*. Hal ini dikarenakan kantor Cawang adalah merupakan pusatnya. Metode penelitian yang disajikan berupa flowchart yang tertera pada gambar 2 digunakan penulis sebagai acuan tahapan dalam melakukan penelitian. Terdapat dua metode yang dilakukan untuk penelitian berikut yaitu metode pengumpulan data dan metode simulasi, berikut untuk masing masing penelitian yang di lakukan dengan metode pengumpulan data dan metode simulasi yaitu :

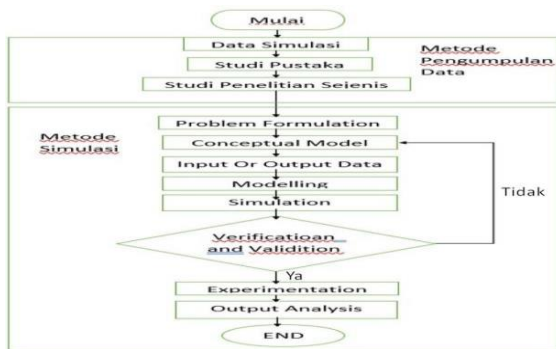
1. Metode Pengumpulan Data



- a. Data Simulasi
- b. Studi Pustaka
- c. Studi Penelitian Sejenis

2. Metode Simulasi

- a. Problem Formulation
- b. Conceptual Model
- c. Input Or Output Data
- d. Modelling
- e. Simulation
- f. Verification and Validation
- g. Experimentation
- h. Output Analysis



Gambar 2 Diagram Alur Penelitian

2.1. Metode Pengumpulan Data

Penulisan penelitian sebagai tugas akhir ini memerlukan data-data sebagai bahan pendukung kebenaran materi uraian dan pembahasan. Karena itu, diperlukannya metode pengumpulan data dan metode pengembangan sistem dalam penyusunan penelitian ini seperti Data Simulasi, Studi Pustaka, dan Studi Penelitian Sejenis

2.2. Metode Simulasi

Metode simulasi yang penulis lakukan pada penelitian ini adalah dengan percobaan sistem *failover link* terhadap *routing protocol BGP* dengan menggunakan system *MPLS-VPN*. Skenario percobaan *redundant link* dengan system *failover* yang akan dianalisis untuk mendapatkan nilai *packet loss*, *latency* dan *response time failover*.

2.3. Rancangan Topologi

Pada penelitian ini terdapat *MPLS*, yang dimana di dalamnya memiliki beberapa device *layer 3* running *MPLS*. *MPLS* berikut dibentuk untuk menghubungkan antar perangkat yang ada di wilayah Jakarta yaitu Cawang sebagai pusat untuk menjalankan sistem *Redundant Link* dan Durentiga sebagai cabang menggunakan kabel *Fiber Optic*.

Gambar 3 Topologi Skenario

Failover

Pada skenario simulasi pada gambar 3 setiap *router* akan di konfigurasi masing masing *ip address*, setelah itu di lanjutkan dengan konfigurasi *routing protocol BGP* dan *routing OSPF* agar setiap *router* dapat berkomunikasi. Selanjutnya konfigurasi di lakukan dengan meng aktifkan *MPLS-VPN* dimasing masing *router PE-MPLS*, dan untuk *redundant link* penulis menggunakan *routing BGP* dengan attribut *ASPATH Prepend* untuk menentukan *main link* dan *backup link*. Simulasi ini dilakukan dengan melakukan percobaan pengiriman paket *ICMP Ping* sebanyak 7 kali dengan mengukur *packet loss ratio* dan *latency*. Kemudian untuk menghitung *response time failover* dimana akan dilakukan pemutusan link antara *PE-MPLS2* dan *CE-CAWANG* dengan

mengukur waktu saat *link* pertama *down* dan berpindah melalui *secondary link*, pengukuran ini untuk mengukur kinerja dari sistem *failover link*. Pengiriman paket data akan dilakukan dengan menggunakan *router CE-Cawang* menuju *IP Lan CE-DURTIG*.

Proses simulasi pengiriman data akan langsung dimonitor dan dapat dihitung nilai *packet loss* dan *latency* setiap detik. Sedangkan untuk mengukur nilai *response time failover* dengan memutuskan koneksi antara PE-MPLS2 dengan CE-CAWANG untuk mengukur seberapa efisiensi waktu *failover link* berjalan. Kemudian di akhir percobaan akan diberikan nilai rata-rata dari setiap parameter yang diukur dan dapat melihat seberapa cepat dan efisiensi waktu *failover link*.

Objek yang digunakan pada perancangan system *failover link* ini adalah:

1. Mikrotik Routerboard CCR1036-12G-4S-EMv2 berjumlah 5 unit 3 unit PC untuk dihubungkan dengan *router*.
2. Optical Distribution Frame sebagai tempat peralihan dari kabel *fiber optic outdoor* dengan kabel *fiber optic indoor* dan sebaliknya
3. Patch Cord

IV. HASIL DAN PEMBAHASAN

Variable yang digunakan untuk mendapatkan *output* pada penelitian simulasi ini berdasarkan permasalahan utama pada analisis kinerja sistem *redundant link* dengan menggunakan *Routing BGP* atribut *ASPATH Prepend*, yaitu. :

a. Packet Loss

Output packet loss ini mengukur persentase kegagalan transmisi paket data yang dikirim dan data yang diterima, yang disebabkan terjadinya *overload* trafik atau tabrakan (*collision*) dalam jaringan, dan *error* yang terjadi pada media fisik.

b. Latency

Output latency atau *Round Trip Time (RTT)* dilakukan untuk mengetahui waktu yang ditempuh oleh paket data dari pengirim ke tujuan kemudian kembali ke pengirim. Pada penelitian ini, pengukuran *latency* dilakukan dengan

melakukan uji *ping* antara *end device* dengan pengalamatan berbasis *IPv4*.

c. Response Time Failover

Pada implementasi pengujian ini ertujuan untuk mengetahui kinerja dari kedua *link* yang telah berhasil dikonfigurasi. Pengujian ini dilakukan dengan menggunakan metode *failover*. *Failover* adalah suatu metode yang digunakan untuk mematikan salah satu jalur utama dengan tujuan untuk menguji jalur lain agar mengetahui kinerja dari jalur tersebut.

Packet Loss Ratio (PLR) adalah indikasi paket hilang yang didapat dari prosentase perbandingan antara kuantitas paket data yang sampai di penerima dengan kuantitas paket yang dikirimkan oleh pengirim. Paket yang hilang harus dikirim kembali, akan menambah total waktu pengiriman. Hilangnya paket tersebut dalam perjalanan tujuan, dapat disebabkan oleh beberapa kemungkinan

Pengukuran *packet loss ratio* dilakukan untuk mengetahui banyaknya paket yang hilang ketika melakukan pengiriman. Pengujian ini dilakukan melalui *test ping* pada *IP Address* 192.168.1.1 dengan melakukan pengiriman 5 kali paket *ICMP* yang masing-masing bernilai 100 *byte*. Pengujian ini dilakukan sebanyak 7 kali dengan melewati jalur *primary link* dan *backup link*.

```
[admin@CE-CAWANG] > ping 192.168.1.1 src-address=172.16.11.1 count=5 size=100
SEQ HOST          SIZE TTL TIME   STATUS
0 192.168.1.1      100 62 5ms
1 192.168.1.1      100 62 5ms
2 192.168.1.1      100 62 4ms
3 192.168.1.1      100 62 4ms
4 192.168.1.1      100 62 5ms
sent=5 received=5 packet-loss=0% min-rtt=4ms avg-rtt=4ms max-rtt=5ms

[admin@CE-CAWANG] > ping 192.168.1.1 src-address=172.16.11.1 count=5 size=100
SEQ HOST          SIZE TTL TIME   STATUS
0 192.168.1.1      100 62 4ms
1 192.168.1.1      100 62 5ms
2 192.168.1.1      100 62 2ms
3 192.168.1.1      100 62 6ms
4 192.168.1.1      100 62 5ms
sent=5 received=5 packet-loss=0% min-rtt=2ms avg-rtt=4ms max-rtt=6ms

[admin@CE-CAWANG] > ping 192.168.1.1 src-address=172.16.11.1 count=5 size=100
SEQ HOST          SIZE TTL TIME   STATUS
0 192.168.1.1      100 62 6ms
1 192.168.1.1      100 62 4ms
2 192.168.1.1      100 62 5ms
3 192.168.1.1      100 62 5ms
4 192.168.1.1      100 62 5ms
sent=5 received=5 packet-loss=0% min-rtt=4ms avg-rtt=5ms max-rtt=6ms

[admin@CE-CAWANG] > ping 192.168.1.1 src-address=172.16.11.1 count=5 size=100
SEQ HOST          SIZE TTL TIME   STATUS
0 192.168.1.1      100 62 5ms
1 192.168.1.1      100 62 5ms
2 192.168.1.1      100 62 5ms
3 192.168.1.1      100 62 5ms
4 192.168.1.1      100 62 5ms
sent=5 received=5 packet-loss=0% min-rtt=2ms avg-rtt=4ms max-rtt=5ms

[admin@CE-CAWANG] > ping 192.168.1.1 src-address=172.16.11.1 count=5 size=100
SEQ HOST          SIZE TTL TIME   STATUS
0 192.168.1.1      100 62 5ms
1 192.168.1.1      100 62 5ms
2 192.168.1.1      100 62 4ms
3 192.168.1.1      100 62 5ms
4 192.168.1.1      100 62 5ms
sent=5 received=5 packet-loss=0% min-rtt=2ms avg-rtt=4ms max-rtt=5ms

[admin@CE-CAWANG] > ping 192.168.1.1 src-address=172.16.11.1 count=5 size=100
SEQ HOST          SIZE TTL TIME   STATUS
0 192.168.1.1      100 62 5ms
1 192.168.1.1      100 62 5ms
2 192.168.1.1      100 62 5ms
3 192.168.1.1      100 62 5ms
4 192.168.1.1      100 62 5ms
sent=5 received=5 packet-loss=0% min-rtt=2ms avg-rtt=4ms max-rtt=5ms
```

Gambar 4 Pengukuran Packet Loss Ratio

Hasil pengukuran *PLR* pada *link* berikut pada gambar 4 menunjukkan angka yang sangat baik, dikarenakan semua nilai dari tujuh pengujian bernilai 0%, yang artinya tidak ada paket yang hilang. Menurut standar TIPHON, apabila nilai rata-rata *packet loss ratio* dari suatu pengujian bernilai 0%, maka dikatakan sangat bagus. Hal ini terjadi karena tidak adanya gangguan dalam melakukan pengujian pengiriman data, gangguan-gangguan tersebut di antaranya tabrakan atau *congestion* dan *overload* trafik.

Pengukuran *latency* atau *Round Trip Time (RTT)* dilakukan untuk mengetahui waktu yang ditempuh oleh paket data dari pengirim ke tujuan kemudian kembali ke pengirim. Pada penelitian ini, pengukuran *latency* dilakukan dengan melakukan uji ping antara *end device* dengan pengalamanan berbasis *IPv4* dengan *IP Address* 192.168.1.1. *End device* yang diuji disini adalah perangkat CE-CAWANG kearah CE-DURTIG. Setiap uji ping dilakukan dengan mengirimkan paket *ICMP* sebanyak 5 kali dengan masing-masing besar nilai paket sebesar 100 byte, sehingga besarnya total paket yang dikirim adalah 500 byte. Test ping dilakukan sebanyak 7 kali dengan melewati jalur *primary link* dan *backup link*.

```
[admin@CE-CAWANG] ~$ nslookup RemoteAddress=10.7.7.1
19:40:51 echo: route,bgp,info Failed to open TCP connection: No route to host
[admin@CE-CAWANG] ~$ nslookup RemoteAddress=10.7.7.1
19:40:51 echo: route,bgp,info RemoteAddress=10.7.7.1
[admin@CE-CAWANG] ~$ ping 192.168.1.1 src-address=172.16.11.1 count=5 size=100
PING 192.168.1.1: 5 bytes from 192.168.1.1: seq=0 ttl=62 time=2.2ms
 0: 192.168.1.1 100 62 2ms
 1: 192.168.1.1 100 62 4ms
 2: 192.168.1.1 100 62 4ms
 3: 192.168.1.1 100 62 4ms
 4: 192.168.1.1 100 62 4ms
---
sent=5 received=5 packet-loss=0% min-rtt=2ms avg-rtt=3ms max-rtt=5ms

[admin@CE-CAWANG] ~$ ping 192.168.1.1 src-address=172.16.11.1 count=5 size=100
PING 192.168.1.1: 5 bytes from 192.168.1.1: seq=0 ttl=62 time=6ms
 0: 192.168.1.1 100 62 6ms
 1: 192.168.1.1 100 62 6ms
 2: 192.168.1.1 100 62 2ms
 3: 192.168.1.1 100 62 4ms
 4: 192.168.1.1 100 62 5ms
---
sent=5 received=5 packet-loss=0% min-rtt=2ms avg-rtt=4ms max-rtt=6ms

[admin@CE-CAWANG] ~$ ping 192.168.1.1 src-address=172.16.11.1 count=5 size=100
PING 192.168.1.1: 5 bytes from 192.168.1.1: seq=0 ttl=62 time=4ms
 0: 192.168.1.1 100 62 5ms
 1: 192.168.1.1 100 62 4ms
 2: 192.168.1.1 100 62 5ms
 3: 192.168.1.1 100 62 5ms
 4: 192.168.1.1 100 62 6ms
---
sent=5 received=5 packet-loss=0% min-rtt=4ms avg-rtt=5ms max-rtt=6ms

19:41:14 echo: route,bgp,info Failed to open TCP connection: No route to host
[admin@CE-CAWANG] ~$ ping 192.168.1.1 src-address=172.16.11.1 count=5 size=100
PING 192.168.1.1: 5 bytes from 192.168.1.1: seq=0 ttl=62 time=5ms
 0: 192.168.1.1 100 62 5ms
 1: 192.168.1.1 100 62 5ms
 2: 192.168.1.1 100 62 3ms
 3: 192.168.1.1 100 62 5ms
 4: 192.168.1.1 100 62 6ms
---
sent=5 received=5 packet-loss=0% min-rtt=3ms avg-rtt=4ms max-rtt=6ms

[admin@CE-CAWANG] ~$ ping 192.168.1.1 src-address=172.16.11.1 count=5 size=100
PING 192.168.1.1: 5 bytes from 192.168.1.1: seq=0 ttl=62 time=8ms
 0: 192.168.1.1 100 62 8ms
 1: 192.168.1.1 100 62 5ms
 2: 192.168.1.1 100 62 8ms
 3: 192.168.1.1 100 62 4ms
 4: 192.168.1.1 100 62 4ms
---
sent=5 received=5 packet-loss=0% min-rtt=2ms avg-rtt=4ms max-rtt=8ms

[admin@CE-CAWANG] ~$
```

Gambar 5 Pengukuran *Latency*

Gambar 5 merupakan hasil rata-rata pengukuran *latency* dari *link* yang sedang digunakan pada saat pengujian. Secara keseluruhan, nilai *latency* yang dihasilkan dari *link* berikut berada di angka

2ms hingga 8 ms. Berdasarkan standar TIPHON, nilai tersebut termasuk ke dalam kategori sangat bagus, karena *latency* dikatakan sangat bagus jika nilai *latency* berada di bawah 150 ms

Pada implementasi pengujian ini bertujuan untuk mengetahui kinerja dari kedua *link* yang telah berhasil dikonfigurasi. Pengujian ini dilakukan dengan menggunakan metode failover. Failover adalah suatu metode yang digunakan untuk mematikan salah satu jalur utama dengan tujuan untuk menguji jalur lain agar mengetahui kinerja dari jalur tersebut. Pada penelitian ini uji failover dilakukan dengan tes ping dengan pengiriman pesan *ICMP* ke *IP address* 192.168.1.1 yang merupakan *IP address* CE-Durentiga. Kemudian selama tes ping berjalan jalur utama (*main link*) dimatikan dan setelah beberapa saat *main Link* dinyalakan kembali.

```
[admin@CE-CAWANG] ~$ ping 192.168.1.1 src-address=172.16.11.1
PING 192.168.1.1: 5 bytes from 192.168.1.1: seq=0 ttl=62 time=5ms
 0: 192.168.1.1 56 62 5ms
 1: 192.168.1.1 56 62 5ms
 2: 192.168.1.1 56 62 7ms
 3: 192.168.1.1 56 62 5ms
 4: 192.168.1.1 56 62 5ms
 5: 192.168.1.1 56 62 5ms
 6: 192.168.1.1 56 62 4ms
 7: 192.168.1.1 56 62 4ms
 8: 192.168.1.1 56 62 5ms
 9: 192.168.1.1 56 62 5ms
10: 192.168.1.1 56 62 5ms
11: 192.168.1.1 56 62 5ms
12: 192.168.1.1 56 62 3ms
13: 192.168.1.1 56 62 2ms
14: 192.168.1.1 56 62 3ms
15: 192.168.1.1 56 62 4ms
16: 192.168.1.1 56 62 2ms
17: 192.168.1.1 56 62 5ms
18: 192.168.1.1 56 62 5ms
19: 192.168.1.1 56 62 6ms
---
sent=20 received=17 packet-loss=15% min-rtt=2ms avg-rtt=4ms max-rtt=7ms

19:00:18 echo: route,bgp,error HoldTimer expired
19:00:18 echo: route,bgp,error RemoteAddress=10.7.7.1
[admin@CE-CAWANG] ~$
```

Gambar 6 Pengujian *Main link* dan *Backup link*

Hasil yang didapat dari pengujian kali ini adalah ketika *main link* dimatikan, terdapat pemberitahuan bahwa sesi *BGP* antar *router border* dan *router neighbor* dengan *IP address* 10.7.7.1 mengalami *down*, hal ini disebabkan karena jalur utama dimatikan. Kemudian pada saat bersamaan tes ping sempat mengalami *time out* dikarenakan sedang terjadinya proses perpindahan *link* menuju *backup link*. Setelah *backup link* berjalan tes ping masih berhasil mengirimkan pesan *ICMP* ke alamat tujuan melalui *backup link*. Dari pengujian ini nilai *success rate* yang dihasilkan yaitu sebesar 85% dengan rincian *sent* = 20, *received* = 17, *packet loss* = 15%, dan nilai rata-rata *latency* yang dihasilkan yaitu 4 ms.

V. PENUTUP

Kesimpulan

Penerapan sistem *MPLS-VPN* dapat diimplementasikan dan bekerja dengan baik pada jaringan PT. Indonesia Comnets Plus. *Redundant link* dengan menerapkan sistem *main link* dan *backup link* secara otomatis dapat berjalan dengan baik pada jaringan PT. Indonesia Comnets Plus. Uji coba performa *link* pada jaringan PT. Indonesia Comnets Plus terpantau sangat baik dari pengukuran performa *packet loss*, *latency* dan *response time failover*.

Saran

Menganalisa lebih dalam untuk mengetahui banyaknya waktu yang diperlukan jalur utama (*main*) beralih menjadi jalur *backup* untuk dijadikan jalur yang digunakan untuk *transmisi data*. Pada penelitian selanjutnya untuk mendapatkan hasil yang berbeda dapat menggunakan jenis *router* dan aplikasi simulasi yang berbeda. Untuk meningkatkan keakuratan hasil penelitian, pada penelitian selanjutnya dapat dilakukan dengan *router* dan komputer secara fisik.

DAFTAR PUSTAKA

- [1] Adhiwibowo, W. and Irawan, A.R. (2019) "IMPLEMENTASI REDUNDANT LINK UNTUK MENGATASI," *Pengembangan Rekayasa dan Teknologi*, 15(1), pp. 48–53. Available at: <http://journals.usm.ac.id/index.php/jprt/index>.
- [2] Adhiwibowo, W. and Irawan, A.R. (2019) "Implementasi Redundant Link Untuk Mengatasi Downtime Dengan Metode Failover," *Jurnal Pengembangan Rekayasa dan Teknologi*, 15(1), p. 48. doi:10.26623/jprt.v15i1.1490.
- [3] Ardianto, F. (2018) PENGGUNAAN MIKROTIK ROUTER SEBAGAI JARINGAN SERVER. Available at: <http://mikrotik.co.id/>.
- [4] arnita, arnita and farid, muhammad (2020) "645-1666- 1-PB," Implementasi jaringan virtual private network dengan teknologi Multi Protocol Label Switching (MPLS) [Preprint].
- [5] Attamimi, S., Oftari, A.D. and Budiyanto, S. (2019) "Analisis QoS (Quality of Service) Pada Implementasi Layanan Broadband IPTV (Internet Protocol Television) di Jaringan Akses PT. Telkom," 10.
- [6] Euginia, B. and Ghozali, T. (2018) Simulasi Multi Protocol Label Switching Virtual Private Network (MPLS VPN) Dengan Virtual Local Area Network (VLAN) Menggunakan Router MIKROTIK.
- [7] Rahmawati, Y., Ikhwan, S. and Hadi, I.P. (2018) "(Mpls Vpn) Dengan Menggunakan Simulator," pp. 367–371.ssss
- [8] Rizkiana, S., Perdana, D. and Negara, R. (2017) DENGAN METODE QOS INTSERV ANALISYS AND IMPLEMENTATION VPN SERVICE PERFORMANCE OF MPLS-TE NETWORK USING BGP PROTOCOL BY INTSERV QOS METODE.
- [9] Sembiring, R. (2019) ANALISA PERBANDINGAN OSPF DAN BGP JARINGAN MPLS UNTUK VIDEO STREAMING.
- [10] Styx Roring, R. and Djumhadi (2020) "PERANCANGAN DAN IMPLEMENTASI JARINGAN FAILOVER MENGGUNAKAN PROTOKOL SPANNINGTREE PADA PT. PLN UP3B KALIMANTAN TIMUR," PERANCANGAN DAN IMPLEMENTASI JARINGAN FAILOVER MENGGUNAKAN PROTOKOL SPANNING TREE PADA PT. PLN UP3B KALIMANTAN TIMUR [Preprint].
- [11] Watmah, S. (2020) Implementasi VPN Menggunakan Point-To-Point Tunneling Protocol (PPTP) Mikrotik Router Pada BPRS Bumi Artha Sampang. Available at: <http://ejournal.bsi.ac.id/ejurnal/index.php/insantek6>.