

OPTIMALISASI KINERJA JARINGAN WAN PADA PENYEDIA JASA LAYANAN *INTERNET* MENGUNAKAN TEKNOLOGI EVPN-MPLS

Fernanda Adhipramana^{1*}, Yuma Akbar²

^{1*2} Program Studi Teknik Informatika, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika,
Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta, Indonesia.

Email: fernandaadhipr11@gmail.com^{1*}

Histori Artikel:

Dikirim 20 Juli 2023; *Diterima dalam bentuk revisi* 22 Agustus 2023; *Diterima* 25 Agustus 2023; *Diterbitkan* 10 September 2023. Semua hak dilindungi oleh Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) STMIK Indonesia Banda Aceh.

Abstrak

Jaringan WAN yang efisien dan handal adalah kunci sukses untuk bisnis modern. Dengan meningkatnya kompleksitas jaringan dan tantangan dalam memantau trafik BUM (Broadcast, Unkown Unicast, Multicast), dibutuhkan solusi yang lebih canggih. Penelitian ini berfokus pada penggunaan EVPN-MPLS sebagai opsi teknologi L2VPN yang lebih baik. Dengan menggunakan metode Network Development Life Cycle (NDLC). Penelitian ini mengimplementasikan EVPN-MPLS menggunakan perangkat Juniper dan melakukan uji kinerja menggunakan aplikasi simulasi PNET-LAB. Hasil penelitian menunjukkan bahwa EVPN-MPLS memiliki performa yang unggul dalam hal latency, jitter, dan pemantauan trafik BUM. Pada skenario pengujian dimana salah satu PE router mati, EVPN mengalami packetloss sebesar 4%, sementara VPLS mencapai 12-16%. Selain itu, fitur active-active multihoming pada EVPN-MPLS juga menawarkan peningkatan kapasitas dan penyeimbangan beban yang efisien. Meski memerlukan sumber daya control plane routing yang signifikan, EVPN-MPLS menjanjikan peningkatan kinerja jaringan WAN, khususnya bagi penyedia layanan internet. Penelitian ini diharapkan dapat memberikan wawasan dan rekomendasi praktis bagi mereka yang ingin mengoptimalkan pengelolaan jaringan WAN mereka.

Kata Kunci: MPLS; MPLS VPN; EVPN.

Abstract

An efficient and reliable WAN network is the key to success for modern businesses. With the increasing complexity of the network and the challenges in monitoring BUM traffic (Broadcast, Unkown Unicast, Multicast), a more sophisticated solution is needed. This research focuses on the use of EVPN-MPLS as a superior option for L2VPN technology. Using the Network Development Life Cycle (NDLC) method, this research implements EVPN-MPLS using Juniper devices and conducts performance testing using the PNET-LAB simulation application. The results show that EVPN-MPLS outperforms in terms of latency, jitter, and BUM traffic monitoring. In a testing scenario where one of the PE routers is down, EVPN experiences a packet loss of 4%, while VPLS reaches 12-16%. In addition, the active-active multihoming feature in EVPN-MPLS also offers efficient load balancing and capacity enhancement. Although it requires significant control plane routing resources, EVPN-MPLS promises to improve WAN network performance, especially for internet service providers. This research is expected to provide insights and practical recommendations for those who want to optimize their WAN network management.

Keyword: MPLS; MPLS VPN; EVPN.

1. Pendahuluan

Latar belakang penggunaan teknologi informasi dan komunikasi, khususnya dalam hal jaringan WAN (*Wide Area Network*), telah menjadi komponen kritis dalam keberhasilan operasional banyak bisnis modern. Keandalan dan efisiensi jaringan WAN berperan penting dalam mendukung pertukaran data dan informasi yang cepat dan aman antar lokasi yang jauh secara geografis. Namun, dengan peningkatan kompleksitas jaringan dan tantangan dalam memantau trafik *Broadcast*, *Unknown Unicast*, dan *Multicast* (BUM), solusi jaringan yang lebih maju menjadi kebutuhan mendesak. *Virtual Private Network* (VPN) dengan *Multi-Protocol Label Switching* (MPLS) merupakan salah satu teknologi yang banyak digunakan dalam membangun jaringan pribadi *virtual*. Teknologi ini menghubungkan lokasi yang jauh secara geografis dengan aman dan efektif seolah-olah mereka adalah bagian dari jaringan lokal yang sama. Sementara itu, *Virtual Private LAN Service* (VPLS) juga memanfaatkan MPLS untuk menghubungkan beberapa lokasi pada *Layer 2*, menciptakan jaringan lokal yang luas.

Namun, keterbatasan dari teknologi MPLS VPN dan VPLS, khususnya dalam hal skalabilitas dan efisiensi distribusi alamat MAC, mendorong penelitian ini untuk mempertimbangkan penggunaan teknologi *Ethernet VPN* (EVPN). EVPN, yang dapat beroperasi pada lingkungan *VPN Layer 2* dan *Layer 3*, menawarkan solusi yang lebih fleksibel dan scalable. Teknologi ini juga menonjol dengan fitur *multi-homing* aktif-aktifnya, yang memungkinkan penyeimbangan beban yang efisien sambil mempertahankan redundansi jaringan. Dengan mempertimbangkan kelebihan dan keterbatasan dari masing-masing teknologi tersebut, penelitian ini bertujuan untuk memanfaatkan EVPN-MPLS sebagai alternatif teknologi L2VPN yang lebih baik. Diharapkan, hasil penelitian ini dapat memberikan rekomendasi dan wawasan praktis bagi mereka yang ingin mengoptimalkan pengelolaan jaringan WAN mereka. Meskipun penelitian ini memerlukan sumber daya kontrol plane routing yang signifikan, penelitian ini menjanjikan peningkatan kinerja jaringan WAN, khususnya bagi penyedia layanan internet.

Menurut Forouzan dan Fegan dalam buku "*Data Communications and Networking*", Jaringan Area Luas (*Wide Area Network* atau WAN) adalah jaringan komunikasi yang mencakup area geografis yang besar, seperti Kota, negara, atau bahkan benua. WAN umumnya digunakan untuk menghubungkan perangkat jaringan seperti komputer dan server yang berada jauh satu sama lain. WAN memungkinkan pertukaran data dan informasi antara pengguna di berbagai lokasi, baik melalui koneksi kabel maupun nirkabel. Beberapa teknologi yang digunakan dalam WAN termasuk sistem telepon, kabel serat optik, dan link satelit. WAN berbeda dari Jaringan Area Lokal (*Local Area Network* atau LAN) yang biasanya mencakup area yang lebih kecil, seperti sebuah gedung atau kampus. Jaringan LAN biasanya memiliki kecepatan data yang lebih tinggi dibandingkan dengan WAN, tetapi memiliki jangkauan yang lebih terbatas. Jaringan WAN memainkan peran penting dalam organisasi dan bisnis yang memiliki cabang atau Kantor di berbagai lokasi, memungkinkan mereka untuk berkomunikasi dan berbagi sumber daya secara efisien dan aman [1].

Menurut William Stallings dalam bukunya berjudul "*Data and Computer Communications*", kinerja jaringan didefinisikan sebagai ukuran efektivitas sebuah sistem komunikasi. Kinerja jaringan mencakup berbagai aspek, termasuk kecepatan transmisi data, *latency* atau *delay*, *jitter*, keandalan, dan kapasitas jaringan [2]. *Multi-Protocol Label Switching* (MPLS) adalah teknologi jaringan yang digunakan untuk memudahkan proses *routing* dan *switching* data dalam jaringan [3]. MPLS digunakan untuk mempercepat proses transfer data dengan mengalokasikan jalur yang optimal untuk setiap paket data. Dalam MPLS, setiap paket data diberikan label atau *tag* yang digunakan untuk menentukan jalur yang optimal untuk paket tersebut. Label ini dipasang pada paket data oleh router pertama yang ditemui dalam jaringan dan dilepas oleh router terakhir yang dituju [4]–[18].

Virtual Private LAN Service (VPLS) adalah teknologi jaringan yang memungkinkan untuk menghubungkan beberapa lokasi secara *Layer 2*, sehingga lokasi tersebut akan terhubung seperti satu jaringan lokal yang besar [19]. Dalam VPLS, setiap lokasi akan terhubung ke satu atau lebih *Provider Edge* (PE) router yang mengambil paket data dari lokasi tersebut, kemudian meneruskannya ke PE router lainnya untuk mencapai lokasi tujuan. VPLS dapat digunakan untuk menghubungkan beberapa Kantor atau cabang yang berada di lokasi yang berbeda secara efektif dan efisien. VPLS menggunakan

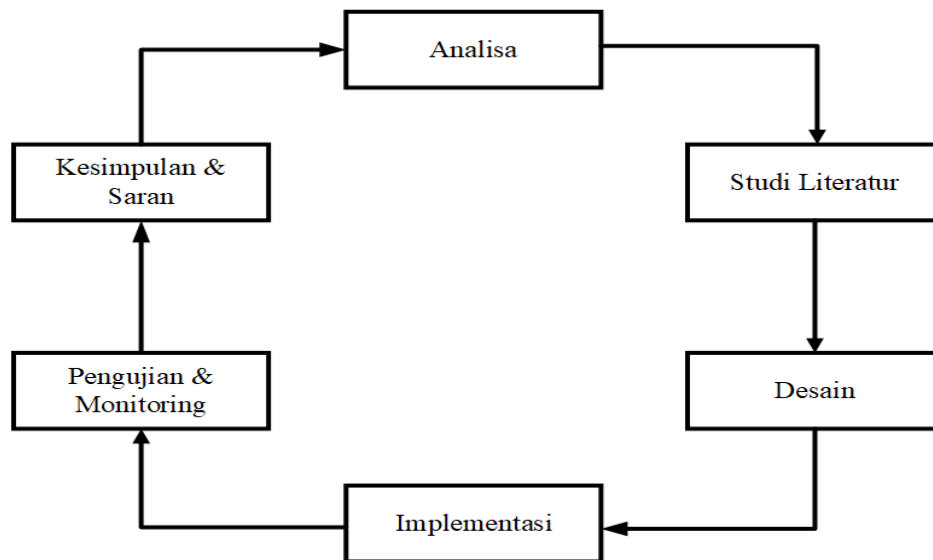
teknologi Multiprotocol Label Switching (MPLS) sebagai teknologi inti yang memungkinkan pengiriman data yang efisien. Pada VPLS, setiap lokasi Akan memiliki identitas unik yang disebut sebagai *Virtual Private LAN Service Identifier* (VPLS-ID). VPLS-ID digunakan untuk mengidentifikasi setiap lokasi dan memastikan bahwa setiap paket data yang diterima oleh PE router hanya dikirimkan ke lokasi yang tepat [20]–[25].

Ethernet VPN (EVPN) adalah teknologi yang menyediakan solusi yang fleksibel dan *scalable* untuk membangun jaringan VPN [26]. EVPN dapat beroperasi di lingkungan *Layer 2 VPN* ataupun di lingkungan *Layer 3 VPN*. EVPN didasarkan pada BGP dan menggunakan MP-BGP untuk mendistribusikan alamat MAC dan prefiks IP di seluruh jaringan. Keuntungan utama dari menggunakan EVPN dibandingkan teknologi *Layer 2 VPN* tradisional seperti VPLS adalah penggunaan BGP untuk mendistribusikan alamat MAC, yang memungkinkan pembelajaran alamat MAC yang lebih efisien dan *scalable*. EVPN juga memberikan dukungan untuk trafik *multicast* dan memungkinkan distribusi informasi *routing Layer 3* di seluruh VPN yang ada. Salah satu manfaat utama EVPN adalah kemampuannya untuk menyediakan fitur *active-active multi-homing* [27], yang memungkinkan lalu lintas trafik untuk *load-balance* di seluruh koneksi yang tersedia, sambil tetap mempertahankan redundansi dalam jaringan. EVPN juga mendukung integrasi yang *seamless* dengan teknologi lain, seperti MPLS dan VXLAN. EVPN telah mendapatkan popularitas dalam beberapa tahun terakhir karena kemampuannya untuk mengatasi skalabilitas dan masalah operasional yang terkait dengan teknologi *Layer 2 VPN* tradisional. Diharapkan Akan terus meningkatkan popularitasnya saat lebih banyak penyedia layanan dan perusahaan mengadopsi teknologi ini.

2. Metode Penelitian

Data dalam penelitian ini diperoleh melalui studi literatur terhadap jurnal-jurnal ilmiah terindeks, buku-buku teks terkait jaringan dan teknologi EVPN MPLS, serta referensi lainnya yang relevan dan akurat. Studi literatur ini dilakukan secara sistematis dan mencakup berbagai aspek EVPN MPLS, *active-active multihoming* dan penanganan trafik BUM untuk mendapatkan pemahaman yang mendalam. Kriteria penyeleksian sumber meliputi relevansi dengan topik penelitian, kualitas dan keandalan sumber, serta tanggal publikasi untuk memastikan informasi yang paling terkini.

Selain itu, dalam penelitian ini, peneliti mengimplementasikan dan mensimulasikan jaringan EVPN MPLS dengan menggunakan aplikasi simulasi PNET-LAB dan *platform* Juniper Networks. PNET-LAB adalah perangkat lunak simulasi jaringan yang dipilih karena kemampuannya untuk mensimulasikan berbagai topologi jaringan secara akurat, kemudahan penggunaan, dan fitur-fitur canggih lainnya. Dalam penelitian ini, peneliti merancang topologi jaringan yang sesuai dengan skenario yang dipelajari, mengatur konfigurasi sesuai dengan praktek terbaik, dan melakukan simulasi pengujian untuk mengukur kinerja dan efektivitas EVPN MPLS dan penanganan trafik BUM. Metode yang digunakan dalam penelitian ini adalah metode *Network Development Life Cycle* (NDLC). Metode NDLC terdiri dari beberapa tahapan yang meliputi Analisa, Studi Literatur, Desain, Implementasi, Pengujian dan Monitoring, Kesimpulan dan Saran. Penjelasan mengenai masing-masing tahapan adalah sebagai berikut:

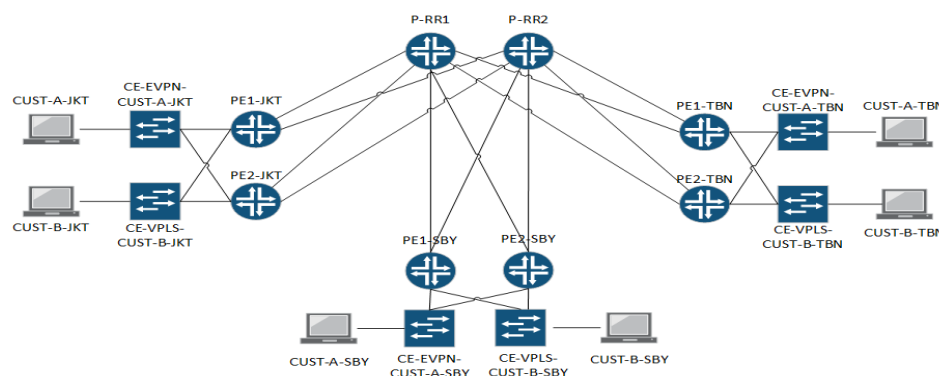


Gambar 1. Metode Penelitian

Analisa, pada tahap ini identifikasi dan analisa masalah untuk optimasi jaringan WAN melalui EVPN-MPLS dan kontrol trafik BUM, termasuk penjelasan solusi. Studi Literatur, tahap ini melibatkan pengumpulan data dan informasi terkait masalah dari berbagai referensi seperti jurnal, *website*, dan buku. Desain, pada tahap ini, desain jaringan EVPN MPLS dibuat termasuk topologi jaringan, alokasi sumber daya, dan konfigurasi jaringan. Implementasi, disini desain jaringan diwujudkan menjadi sistem jaringan yang berfungsi pada tahap ini. Pengujian & Monitoring, setelah implementasi, jaringan diuji dan dimonitor untuk memastikan fungsionalitas, performa, dan fitur khusus dari EVPN MPLS serta mengidentifikasi dan mengatasi masalah. Kesimpulan & Saran, tahap akhir meliputi evaluasi, ringkasan temuan, dan saran untuk penelitian selanjutnya.

2.1 Analisa Topologi Jaringan

Topologi jaringan untuk pengujian EVPN MPLS melibatkan 3 *site*, masing-masing dengan 2 router PE yang terhubung ke 2 router P dan perangkat CE. Tujuannya adalah menciptakan koneksi redundan, mengimplementasikan *active-active multiboming*, dan memberikan jalur beragam untuk transmisi data, meningkatkan ketersediaan jaringan dan ketahanan terhadap kegagalan. Topologi ini juga dirancang untuk memantau dan mengendalikan trafik BUM secara efisien. Router P berfungsi mendistribusikan *route* dari router PE ke PE lain, router PE menyimpan informasi dari perangkat CE, dan perangkat CE mengatur konfigurasi di sisi pelanggan.



Gambar 2. Topologi EVPN-MPLS

2.2 Parameter Pengujian

Penelitian ini melakukan pengujian pada tiga aspek utama:

- 1) Pengujian *Active-active multihoming* pada EVPN, untuk mengevaluasi manajemen lalu lintas data dan respon terhadap kegagalan jaringan.
- 2) Perbandingan *latency*, *jitter*, dan *packet loss* antara EVPN dan VPLS, untuk mengetahui efisiensi dan kinerja kedua teknologi tersebut.
- 3) Perbandingan kemampuan EVPN dan VPLS dalam memantau dan mengelola trafik BUM (*Broadcast, Unknown unicast, dan Multicast*).

Pengujian dilakukan dengan simulasi jaringan menggunakan aplikasi PNET-LAB, bertujuan memberikan pemahaman mendalam tentang kinerja EVPN dibandingkan dengan VPLS.

2.3 Alat Penelitian

Alat-alat yang digunakan untuk mendukung penelitian ini meliputi *hardware* berupa server dan juga aplikasi PNET-LAB yang terinstal di dalamnya. Berikut adalah detail alat yang digunakan dalam penelitian ini:

Tabel 1. Spesifikasi *Hardware*

No	Jenis Hardware	Spesifikasi
1	Server	HP ProLiant DL360P Gen8
2	CPU	Intel Xeon Processor E5-2651 V2 @1,8Ghz x 2 (24Core, 48Thread)
3	RAM	128GB
4	HDD	600GB

Tabel 2. Spesifikasi *Software*

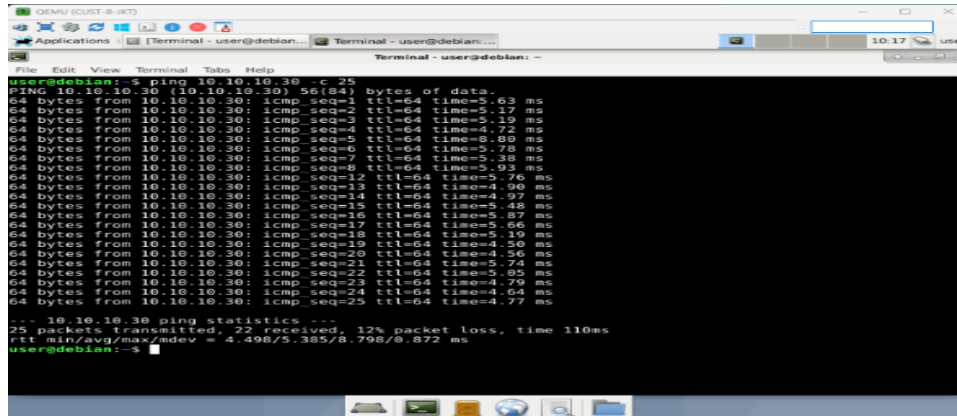
No	Jenis Hardware	Jumlah	Spesifikasi
1	Ubuntu Server 20.04.6 LTS	1	Sistem operasi pada server yang digunakan
2	PNET-LAB 6.0.0-76	1	Aplikasi simulasi jaringan
3	Juniper vMX 22.3R1.11	8	Digunakan sebagai perangkat PE dan P
4	Juniper vEX 23.1R1.8	6	Digunakan sebagai perangkat CE
5	Debian 10	6	Digunakan sebagai client untuk verifikasi pengujian
6	SecureCRT	1	Aplikasi untuk remote access SSH
7	MTR	1	Aplikasi untuk menganalisa paket

3. Hasil dan Pembahasan

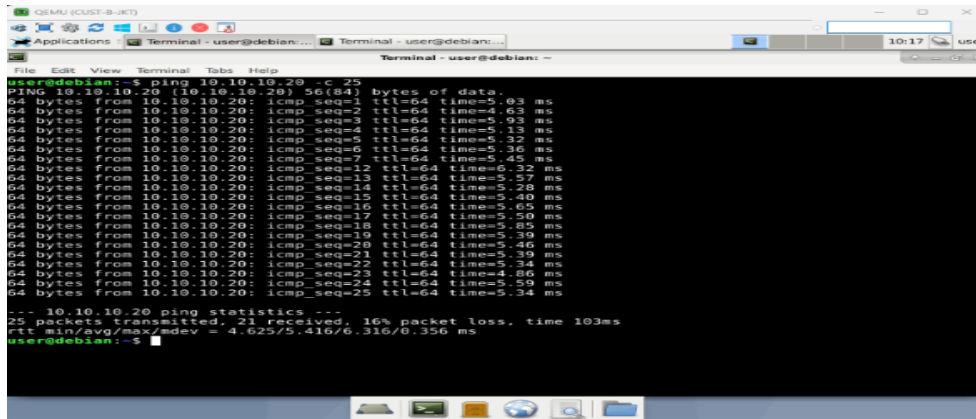
Setelah melakukan tahapan implementasi, selanjutnya akan dilakukan pengujian. Ada tiga jenis pengujian yang akan dilakukan. Pengujian pertama adalah pengujian *active-active multihoming*, pengujian kedua adalah perbandingan *latency*, *jitter*, dan *packet loss*, pengujian ketiga adalah perbandingan pemantauan/*monitoring* trafik BUM antara EVPN dan VPLS.

3.1 Pengujian Active-Active Multihoming

Pengujian ini bertujuan untuk memeriksa kinerja jalur *uplink* saat salah satunya tidak berfungsi. Dalam pengujian ini, Peneliti akan mematikan jalur *uplink* pada salah satu PE yang sedang meneruskan trafik. Kami akan memantau *packetloss* pada protokol EPVN dan VPLS untuk melihat mana yang lebih optimal dalam menangani situasi ini. Optimal di sini berarti mengalami *packetloss* yang lebih sedikit. Berikut merupakan hasil pengujiannya masing-masing protokol dengan skenario mematikan *uplink* pada PE1-JKT.

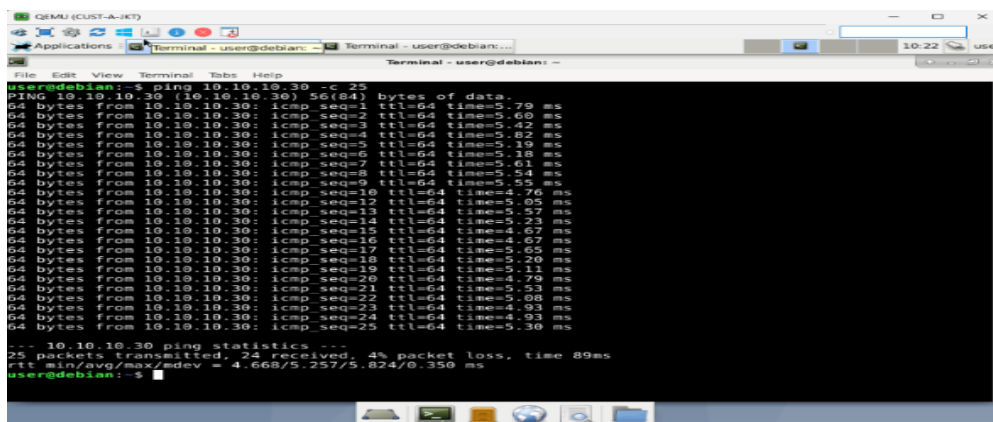


Gambar 3. *Packetloss* VPLS CUST-B-JKT ke CUST-B-TBN

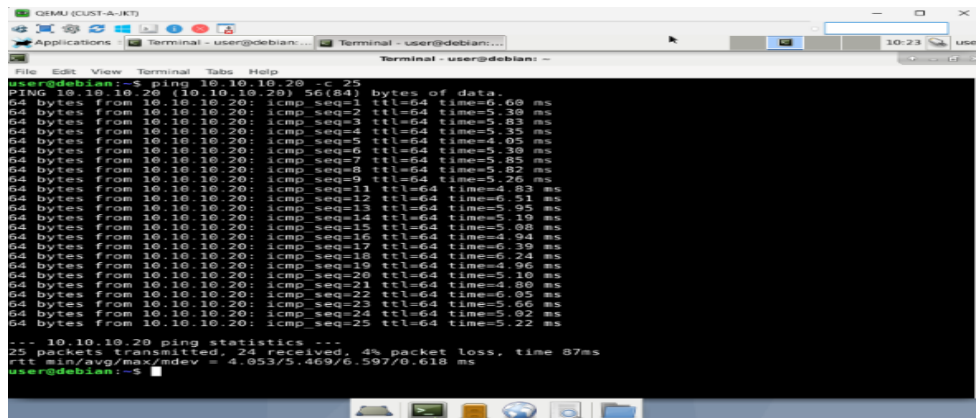


Gambar 4. *Packetloss* VPLS CUST-B-JKT ke CUST-B-SBY

Dari gambar diatas Peneliti dapat memperoleh informasi bahwa *packetloss* pada teknologi VPLS saat salah satu PE mati, dalam kasus ini adalah PE1-JKT yang mati, *packetloss* yang di dapatkan pada trafik ke site Tabanan (TBN) adalah 12%, dari 25 paket yang dikirim, 22 paket diterima, dan 3 paket hilang. Kemudian *packetloss* yang di dapatkan pada trafik ke site Surabaya (SBY) adalah 16%, dari 25 paket yang dikirim, 21 paket diterima, dan 4 paket hilang.



Gambar 5. *Packetloss* EVPN CUST-A-JKT ke CUST-A-TBN

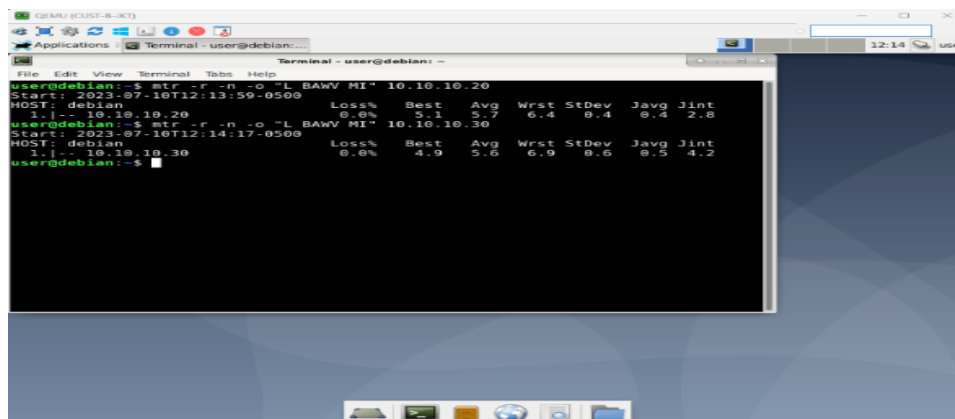


Gambar 6. Packetloss EVPN CUST-A-JKT ke CUST-A-SBY

Dari gambar diatas Peneliti dapat memperoleh informasi bahwa *packetloss* pada teknologi EVPN saat salah satu PE mati, dalam kasus ini adalah PE1-JKT yang mati, *packetloss* yang di dapatkan pada trafik ke masing masing *site* adalah 4%. Dari 25 paket yang dikirim, 24 paket diterima, dan 1 paket hilang. Dapat disimpulkan bahwa EVPN bekerja lebih optimal dibandingkan VPLS dalam skenario pengujian *Active-Active Multihoming* ini. EVPN menunjukkan *packetloss* yang lebih sedikit, yang berarti bahwa teknologi ini lebih efisien dalam menangani situasi dimana salah satu PE menjadi non-fungsional.

3.2 Perbandingan Latency, Jitter, dan Packet Loss

Dalam pengujian ini, kami melakukan transfer data antara lokasi yang berbeda menggunakan aplikasi MTR (*My Traceroute*). Kami melakukan transfer data dari Jakarta ke Tabanan dan Surabaya, kemudian membandingkan performa protokol EVPN dan VPLS dalam hal *Latency*, *Jitter*, dan *Packet Loss*. Kami menentukan mana yang lebih optimal berdasarkan nilai yang lebih rendah untuk ketiga parameter tersebut.



Gambar 7. Hasil uji *latency*, *jitter*, *packetloss* VPLS menggunakan MTR

Dari gambar di atas didapatkan hasil pengujian dari VPLS Jakarta ke Surabaya dan Tabanan. Untuk rute Jakarta ke Surabaya, hasil pengujian sebagai berikut:

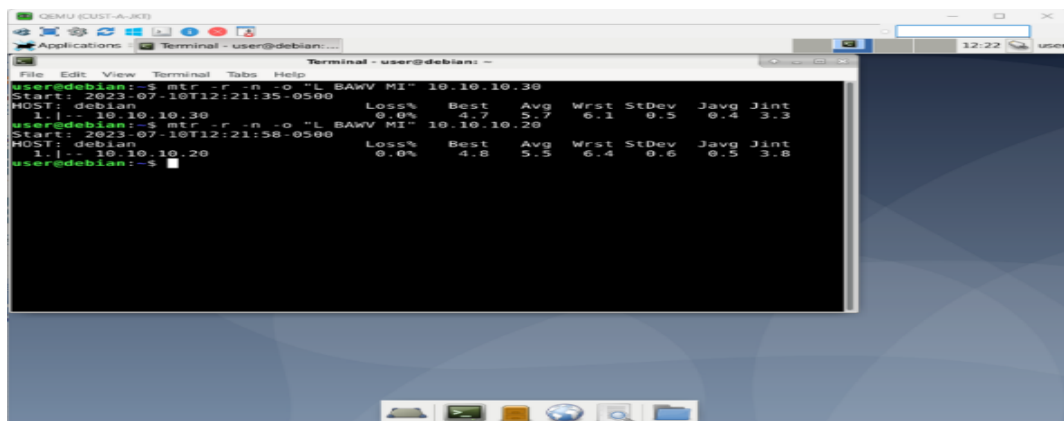
Tabel 3. Hasil Tes VPLS Jakarta – Surabaya

Parameter	Nilai
<i>Packetloss</i>	0%
<i>Best latency</i>	5.1 ms
<i>Average latency</i>	5.7 ms
<i>Worst latency</i>	6.7 ms
<i>Standard Deviation</i>	0.4
<i>Jitter average</i>	0.4 ms
<i>Jitter interarrival</i>	2.8 ms

Sedangkan untuk rute Jakarta ke Tabanan, hasil pengujian adalah:

Tabel 4. Hasil tes VPLS Jakarta – Tabanan

Parameter	Nilai
<i>Packetloss</i>	0%
<i>Best latency</i>	4.9 ms
<i>Average latency</i>	5.6 ms
<i>Worst latency</i>	6.9 ms
<i>Standard Deviation</i>	0.6
<i>Jitter average</i>	0.5 ms
<i>Jitter interarrival</i>	4.2 ms



Gambar 8. Hasil uji *latency*, *jitter*, *packetloss* EVPN menggunakan MTR

Dari gambar di atas, didapatkan hasil pengujian dari EVPN Jakarta ke Tabanan dan Surabaya. Untuk rute Jakarta ke Tabanan, hasil pengujian sebagai berikut:

Tabel 5. Hasil Tes EVPN Jakarta – Tabanan

Parameter	Nilai
<i>Packetloss</i>	0%
<i>Best latency</i>	4.7 ms
<i>Average latency</i>	5.7 ms
<i>Worst latency</i>	6.1 ms
<i>Standard Deviation</i>	0.5
<i>Jitter average</i>	0.4 ms
<i>Jitter interarrival</i>	3.3 ms

Untuk rute Jakarta ke Surabaya, hasil pengujian adalah:

Tabel 6. Hasil tes EVPN Jakarta – Surabaya

Parameter	Nilai
Packetloss	0%
Best latency	4.8 ms
Average latency	5.5 ms
Worst latency	6.4 ms
Standard Deviation	0.6
Jitter average	0.6 ms
Jitter interarrival	3.8 ms

Dari hasil pengujian di atas, dapat disimpulkan bahwa EVPN memiliki performa yang lebih baik dalam hal *latency* dan *jitter* dibandingkan dengan VPLS. Nilai *latency* terbaik dan rata-rata EVPN lebih rendah dibandingkan VPLS, serta *Jitter interarrival* pada EVPN lebih rendah dibandingkan VPLS. *Jitter interarrival* adalah variasi dalam interval waktu antara kedatangan dua paket berturut-turut. Jika paket data tiba dengan interval waktu yang tidak konsisten, ini bisa berarti ada *jitter* dalam jaringan. Hal ini menunjukkan bahwa EVPN memberikan kualitas jaringan yang lebih baik dalam konteks ini.

3.3 Perbandingan pemantauan trafik BUM antara EVPN dan VPLS

Dalam pengujian ini, kami membandingkan bagaimana protokol EVPN dan VPLS memantau dan mengatur trafik BUM, dan melihat mana yang lebih efisien dalam hal ini. Efisiensi dinilai berdasarkan seberapa lengkap masing-masing protokol menyajikan informasi terkait dengan trafik BUM, alamat MAC, dan alamat IP yang disimpan dari masing-masing *site*.

```

root@PE1-JKT> show vpls statistics
VPLS statistics:
Instance: CUST-B
Local interface: ge-0/0/3.0, Index: 341
Broadcast packets: 870
Broadcast bytes: 52200
Multicast packets: 6754
Multicast bytes: 2367049
Flooded packets: 2
Flooded bytes: 148
Unicast packets: 719135
Unicast bytes: 362500781
Current MAC count: 2 (Limit 1024)
Local interface: lsi.1048576, Index: 348
Remote PE: 172.16.1.2
Broadcast packets: 0
Broadcast bytes: 0
Multicast packets: 0
Multicast bytes: 0
Flooded packets: 0
Flooded bytes: 0
Unicast packets: 0
Unicast bytes: 0
Current MAC count: 0
    
```

Gambar 9. Statistik VPLS

Dari gambar diatas, dapat Peneliti ketahui statistik VPLS dari masing-masing site, berapa banyak paket yang sudah dikirim. Di sini Peneliti bisa melihat juga bahwa di masing-masing *site*, ada satu perangkat yang total dikirim 0 karena dia merupakan perangkat pasif, karena VPLS ini single-active.

```

root@PE1-JKT> show vpls mac-table
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
O -OVSDB MAC, SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC, P -Pinned MAC)
Routing instance : CUST-B
Bridging domain : CUST-B, VLAN : NA
MAC address MAC flags Logical interface NH Index MAC property active source
50:21:fc:00:86:01 D lsi.1048599
50:a1:43:00:84:01 D ge-0/0/3.0
50:ad:c8:00:30:00 D lsi.1048599
50:b9:19:00:85:01 D lsi.1048597
50:ee:5d:00:2c:00 D ge-0/0/3.0
50:ef:7f:00:2e:00 D lsi.1048597
    
```

Gambar 10. VPLS MAC-Table

Selanjutnya, Peneliti bisa melihat bahwa Peneliti bisa memantau alamat MAC dari masing-masing *site* menggunakan VPLS dengan mengecek parameter LSI yang ada di bagian *logical interface*.

```

root@PE1-JKT> show evpn arp-table
INET          MAC          Logical      Routing      Bridging
address       address      interface    instance     domain
10.10.10.30   50:73:73:00:31:00 ae1.100     CUST-A       _CUST-A_
10.10.10.10   50:bf:6d:00:2b:00 ae1.100     CUST-A       _CUST-A_
10.10.10.20   50:d0:f2:00:2f:00 ae1.100     CUST-A       _CUST-A_

root@PE1-JKT> show evpn statistics instance CUST-A
Name: CUST-A
Local interface: ae1.100, Index: 332, VLAN ID: 100
Broadcast packets: 1336
Broadcast bytes : 398928
Multicast packets: 8206
Multicast bytes : 2799338
Flooded packets : 11
Flooded bytes   : 954
Unicast packets : 29410
Unicast bytes   : 14772697
Current MAC count: 3 (Limit 1024)

root@PE1-JKT>

```

Gambar 11. EVPN Statistik & ARP-Table

Dari gambar diatas, dapat diketahui statistik EVPN, berapa banyak paket yang sudah dikirim, dan Peneliti juga bisa memantau IP dan alamat MAC yang ada di masing-masing lokasi.

```

root@PE1-JKT> show evpn mac-ip-table
MAC IP flags (S - Static, D - Dynamic, L - Local, R - Remote, Lp - Local Proxy,
Rp - Remote Proxy, K - Kernel, RT - Dest Route, (N)AD - (Not) Advt to remote,
RE - Re-ARP/ND, RO - Router, OV - Override, Ur - Unresolved,
RTS - Dest Route Skipped, RGW - Remote Gateway)
Routing instance: CUST-A
Bridging domain: _CUST-A_
IP          MAC          Flags      Logical      Active
address     address      interface  source
10.10.10.30 50:73:73:00:31:00 DR,K       ae1.100     00:00:00:00:00:00:00:00:30
10.10.10.10 50:bf:6d:00:2b:00 DL,K,AD    ae1.100     00:00:00:00:00:00:00:00:30
10.10.10.20 50:d0:f2:00:2f:00 DR,K       ae1.100     00:00:00:00:00:00:00:00:20

root@PE1-JKT> show evpn database
Instance: CUST-A
VLAN DomainID MAC address Active source Timestamp IP address
100 50:40:65:00:5b:01 00:00:00:00:00:00:00:00:30 Jul 10 15:24:15
100 50:40:65:00:5b:02 00:00:00:00:00:00:00:00:30 Jul 10 15:24:15
100 50:73:73:00:31:00 00:00:00:00:00:00:00:00:30 Jul 10 18:08:28 10.10.10.30
100 50:bf:6d:00:2b:00 00:00:00:00:00:00:00:00:10 Jul 10 18:08:27 10.10.10.10
100 50:c9:5e:00:5c:01 00:00:00:00:00:00:00:00:20 Jul 10 15:24:15
100 50:c9:5e:00:5c:02 00:00:00:00:00:00:00:00:20 Jul 10 15:24:15
100 50:d0:f2:00:2f:00 00:00:00:00:00:00:00:00:20 Jul 10 18:08:20 10.10.10.20
100 50:f8:ba:00:5a:01 00:00:00:00:00:00:00:00:10 Jul 10 15:24:26
100 50:f8:ba:00:5a:02 00:00:00:00:00:00:00:00:10 Jul 10 15:24:15

```

Gambar 12. EVPN Statistik & ARP-Table

Kemudian, Peneliti bisa melihat bahwa di EVPN tidak hanya alamat MAC dari masing-masing *site* saja yang bisa dipantau atau dimonitor, tetapi alamat IP dari masing-masing lokasi juga bisa Peneliti pantau.

```

root@PE1-JKT> show evpn instance CUST-A extensive
Instance: CUST-A
Route Distinguisher: 172.16.1.1:100
VLAN ID: 100
Per-Instance MAC route label: 299776
Duplicate MAC detection threshold: 5
Duplicate MAC detection window: 180
MAC database status
MAC advertisements: Local 2 Remote 0
MAC-IP advertisements: Local 1 Remote 3
Default gateway MAC advertisements: 0
Number of local interfaces: 2 (2 up)
Interface name ESI Mode single-homed Status AC-Role
ae1.100 00:00:00:00:00:00:00:00:00:10 all-active Up Up Root
Number of IRB interfaces: 0 (0 up)
Number of protect interfaces: 0
Number of bridge domains: 1
VLAN Domain-ID Intfs/up IRB-Intf Mode MAC-sync v4-SG-sync v6-SG-sync
Extended Enabled Disabled Disabled
Number of neighbors: 5
Address MAC MAC+IP AD IM ES Leaf-label Remote-DCI-Peer
172.16.1.2 2 1 0 1 0 0
172.16.2.1 1 1 0 1 0 0
172.16.2.2 2 1 0 1 0 0
172.16.3.1 1 1 0 1 0 0
172.16.3.2 1 1 0 1 0 0
Number of ethernet segments: 3
ESI: 00:00:00:00:00:00:00:00:10
Status: Resolved by IFL ae1.100
Local interface: ae1.100, Status: Up/Forwarding
Number of remote PEs connected: 1
Remote-PE MAC-label Aliasing-label Mode
172.16.1.2 299824 299824 all-active
DR Election Algorithm: Preference based
Designated forwarder: 172.16.1.1, Preference: 2
Backup forwarder: 172.16.1.2, Preference: 1
Last designated forwarder update: Jul 10 15:24:25
Advertised MAC label: 299824
Advertised aliasing label: 299824
Advertised split horizon label: 299840
ESI: 00:00:00:00:00:00:00:00:20
Status: Resolved by RH 1048592
Number of remote PEs connected: 2
Remote-PE MAC-label Aliasing-label Mode
172.16.2.1 299824 299824 all-active
172.16.2.2 299824 299824 all-active
ESI: 00:00:00:00:00:00:00:00:30
Status: Resolved by RH 104855
Number of remote PEs connected: 2
Remote-PE MAC-label Aliasing-label Mode
172.16.1.2 299824 299824 all-active
172.16.3.1 299824 299824 all-active
SMET Forwarding: disabled

```

Gambar 13. EVPN Instance

Terakhir, Peneliti dapat memantau kondisi masing-masing PE yang menjalankan EVPN. Peneliti bisa melihat berapa banyak informasi MAC & IP address yang ada di PE tersebut, kemudian Peneliti juga bisa melihat apakah di lokasi tersebut menjalankan *active-active multihoming* atau tidak dengan melihat parameter *all-active* yang tertera. Dan juga Peneliti bisa melihat router DF (*Designated Forwarder*), yang mana router ini bertugas untuk meneruskan trafik BUM dari satu lokasi ke lokasi lainnya. Kesimpulannya, EVPN menawarkan pemantauan yang lebih komprehensif dibandingkan VPLS. EVPN memungkinkan pemantauan alamat MAC dan IP di setiap lokasi, serta menampilkan statistik pengiriman paket. Selain itu, EVPN juga memungkinkan pemantauan terhadap PE yang menjalankan protokol tersebut dan menampilkan informasi apakah lokasi tersebut menjalankan *active-active multihoming* atau tidak. Dengan kata lain, EVPN memberikan visibilitas yang lebih baik terhadap jaringan dan memudahkan proses pemantauan dan pengaturan trafik BUM.

4. Kesimpulan

Berdasarkan hasil penelitian dan analisis data yang telah dilakukan, dapat disimpulkan bahwa protokol EVPN memiliki kinerja yang lebih baik dibandingkan dengan protokol VPLS dalam sejumlah aspek. Pertama, dalam hal *latency* dan *jitter*, EVPN menunjukkan kinerja yang lebih baik dengan nilai *latency* terbaik dan rata-rata yang lebih rendah, serta *Jitter interarrival* yang lebih rendah. Ini menunjukkan bahwa EVPN dapat menyediakan kualitas jaringan yang lebih baik dalam konteks ini. Kedua, dalam aspek pemantauan atau monitoring trafik BUM, EVPN juga menunjukkan keunggulan dengan kemampuan pemantauan yang lebih komprehensif. EVPN memungkinkan pemantauan alamat MAC dan IP di setiap lokasi, serta menampilkan statistik pengiriman paket. Selain itu, EVPN juga memungkinkan pemantauan terhadap PE yang menjalankan protokol tersebut dan menampilkan informasi apakah lokasi tersebut menjalankan *active-active multihoming* atau tidak. Ketiga, fitur *active-active multihoming* pada EVPN memberikan keuntungan signifikan dalam hal peningkatan kapasitas, penyeimbangan beban, dan ketahanan. Fitur ini memungkinkan semua jalur uplink pada suatu PE untuk aktif secara bersamaan dan berbagi beban lalu lintas, sehingga dapat meningkatkan kapasitas dan efisiensi penggunaan jalur. Selain itu, jika satu jalur uplink mengalami kegagalan, trafik dapat dengan cepat dialihkan ke jalur lain tanpa mengganggu layanan.

5. Daftar Pustaka

- [1] Forouzan, B. A. (2007). 4.1 Digital to Digital conversion.”. *Data communications and networking, 4th ed., McGraw Hill New York*, 118.
- [2] Stallings, W. (2007). *Data and computer communications*. Pearson Education India.
- [3] N. Kanoi, “Day One: MPLS Up and Running with Junos,” 2018. [Online]. Available: www.juniper.net/books.
- [4] Dewi, S., & Sulistiyah, S. (2022). Analisa Virtual Private Network (VPN) IP Multi Protocol Label Switching (MPLS) Untuk Jaringan Wide Area Network (WAN). *JISAMAR (Journal of Information System, Applied, Management, Accounting and Research)*, 6(1), 16-25. DOI: 10.52362/jisamar.v6i1.662.
- [5] Nurdiansyah, Y., Pratama, N., Putra, M. I., & Sya’roni, M. A. (2020). Analisis Perbandingan Metode Interior Gateway Protocol RIP Dengan OSPF Pada Jaringan MPLS-VPLS. *INFORMAL: Informatics Journal*, 5(2), 49-56. DOI: <https://doi.org/10.19184/isj.v5i2.18668>.

- [6] Nugita, N. R. (2022). Analisis QoS Streaming Video Jaringan MPLS dan VPLS. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, 9(2), 1053-1067. DOI: <https://doi.org/10.35957/jatisi.v9i2.1915>.
- [7] Sllame, A. M. (2022, May). Performance Evaluation of Multimedia over MPLS VPN and IPSec Networks. In *2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)* (pp. 32-37). IEEE. DOI: 10.1109/MI-STA54861.2022.9837572.
- [8] Mardianto, M. (2019). Analisis Quality Of Service (QoS) pada Jaringan VPN dan MPLS VPN Menggunakan GNS3. *Jurnal Sains Dan Informatika*, 5(2), 98-107. DOI: 10.34128/jsi.v5i2.191.
- [9] Saraswati, M., Iqbal, M., & Irawati, I. D. (2020). Implementasi Dan Analisis Jaringan Mpls Menggunakan Algoritma Sha Sebagai Keamanan Jaringan Pada Komunikasi Voip. *eProceedings of Applied Science*, 6(3).
- [10] Sariana, N., & Suharta, T. (2019). IMPLEMENTATION NETWORK WITH IP/MPLS VPN IN INFORMATION TECHNOLOGY DIVISION IN PERUM JAMKRINDO. *Jurnal Kesejahteraan Sosial*, 6(01). DOI: 10.31326/jks.v6i01.
- [11] Dwiartanto, D. B., Pranindito, D., & Iryani, N. Analisa Perbandingan Performansi Jaringan IPv4 dan IPv6 pada MPLS VPN menggunakan Server IMS Core. *InComTech: Jurnal Telekomunikasi dan Komputer*, 11(2), 85-99. DOI: 10.22441/incomtech.v11i2.10195.
- [12] Sllame, A. M., AboJreeda, A., & Hasaneen, M. (2022, May). Evaluating the Fast Rerouting with MPLS Networks as a Fault Tolerance Mechanism with OSPF and IS-IS routing protocols. In *2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)* (pp. 53-58). IEEE. DOI: 10.1109/MI-STA54861.2022.9837598.
- [13] Raj, L. D. W., Megala, G., Shree, J. M., Preetha, J., & Rashmika, V. (2021). Implementation of Traffic Engineering in MPLS Networks by Creating TE Tunnels Using RSVP and Implementing Fast Reroute Mechanism for Back up Paths.
- [14] Arnita, A., & Farid, M. (2020). Implementasi jaringan virtual private network dengan teknologi Multi Protocol Label Switching (MPLS). *vol. 5*, 28-39. DOI: 10.29210/3003645000.
- [15] Fathurrahmad, F., & Yusuf, S. (2019). Implementasi Jaringan VPN dengan Routing Protocol terhadap Jaringan Multiprotocol Label Switching (MPLS). *Jurnal JTik (Jurnal Teknologi Informasi dan Komunikasi)*, 3(1), 29-33. DOI: 10.35870/jtik.v3i1.83.
- [16] Damanik, M. B. (2022). Perancangan Jaringan Menggunakan Mpls Untuk Layanan Video Streaming. *Jurnal Pendidikan Sains dan Komputer*, 2(02), 301-307. DOI: 10.47709/jpsk.v2i2.1756.
- [17] Fathurrahmad, S. Y., Iqbal, T., & Salam, A. (2019). Virtual Private Network (VPN) Network Design For Multiprotocol Label Switching (MPLS) Networks. *International Journal of Scientific and Technology Research*, 8(11), 2653-2656.
- [18] R. Akbar and A. Suprianto, "SIMULASI PERANCANGAN DAN IMPLEMENTASI REDUNDANT LINK MULTI PROTOCOL LABEL SWITCHING (MPLS) VIRTUAL PRIVATE NETWORK (VPN) PT. INDONESIA COMNETS PLUS MENGGUNAKAN MIKROTIK ROUTER OS," *Jurnal Rekamaya Informasi*, vol. 11, no. 2, pp. 153–159, Oct. 2022.

- [19] Juniper Networks, "MPLS VPN Overview," 2023. https://www.juniper.net/documentation/en_US/junos/topics/concept/mpls-security-vpn-overview.html (accessed May 03, 2023).
- [20] Tulloh, R., & Irawati, I. D. (2020). Implementasi Vpls Pada Jaringan Software Defined Network (sdn) Dengan Menggunakan Onos Controller Berbasis Raspberry-pi 3. *eProceedings of Applied Science*, 6(3).
- [21] Fakhri, G., & Setiyadi, A. (2019). IMPLEMENTASI IPv6 DENGAN METODE MIGRASI NAT64 DAN VPLS UNTUK Mendukung IPv6 MOBILE DI SEBUAH INSTITUSI PENDIDIKAN. *Komputa: Jurnal Ilmiah Komputer dan Informatika*, 8(2), 86-93.
- [22] Syafrinal, S., & Salam, A. (2021). Network Security to Protect Negative Web: A Case Study of the Government of Aceh. *Jurnal Mantik*, 5(3), 1584-1590. [Online]. Available: www.ijstr.org
- [23] Arifin, R. M. A., Wardhani, E. D., & Samuel, B. E. T. A. (2021). Implementasi Tunnel GRE pada Jaringan Ring dan Mesh Perangkat Metro-E Nokia. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, 10(3), 204-213.
- [24] Pangestu, P., & Yusuf, R. (2021). Implementasi Metode QINQ Pada Jaringan Metro Ethernet Untuk Memaksimalkan Penggunaan VLAN Menggunakan Teknologi GPON Studi Kasus: PT. Telkom Indonesia. *Technomedia Journal*, 6(1 Agustus), 82-98. DOI: <https://doi.org/10.33050/tmj.v6i1.1551>.
- [25] Attari, A., Negara, R. M., & Sanjoyo, D. D. (2019). Analisis Performansi High Availability Jaringan pada Virtual Private LAN Service Legasi dan Berbasis Software Defined Network. *Prosiding SENLATI*, 5(3), 99-104. DOI: <https://doi.org/10.36040/seniati.v5i3.960>.
- [26] Monge, A. S., & Szarkowicz, K. G. (2015). *MPLS in the SDN Era: Interoperable Scenarios to Make Networks Scale to New Services*. " O'Reilly Media, Inc."
- [27] Sajassi, A., Aggarwal, R., Bitar, N., Isaac, A., Uttaro, J., Drake, J., & Henderickx, W. (2015). *Bgp mpls-based ethernet vpn* (No. rfc7432).