JTERA (Jurnal Teknologi Rekayasa), Vol. 6, No. 1, Juni 2021, Hal. 61-66
Terakreditasi "**Peringkat 3"** oleh Kemenristek/BRIN, Nomor SK: 85/M/KPT/2020
DOI: 10.31544/jtera.v6.i1.2021.61-66
p-ISSN 2548-737X
e-ISSN 2548-8678

Analisis Performansi *Dynamic Multipoint Virtual Private Network* pada *Routing Protocol BGP* dengan *FRRouting*

Nanda Iryani[#], Dyas Dendi Andika
Jurusan Teknik Telekomunikasi, Institut Teknologi Telkom Purwokerto
Jl. DI Panjaitan No. 128, Purwokerto Kidul, Kec. Purwokerto Sel., Jawa Tengah, Indonesia
[#]nanda@ittelkom-pwt.ac.id

Abstrak

Dynamic Multipoint Virtual Private Network (DMVPN) merupakan salah satu jenis teknologi VPN. Berbeda dengan model VPN lain yang mengharuskan terjalin koneksi *point to point* di jalur *tunnel*, pada DMVPN jalur komunikasi *tunnel*-nya bisa terbentuk secara *point to multipoint*, artinya untuk menghubungkan beberapa *site* yang jumlahnya banyak pada jaringan DMVPN hanya memerlukan satu buah jalur *tunnel*, sehingga pada DMVPN ini lebih *scalable* dibandingkan dengan VPN dengan komunikasi *point to point*. Penelitian ini bertujuan untuk mencari tahu bagaimana unjuk kerja dari jaringan bertipe *full mesh* DMVPN jika berjalan dengan alternatif *routing* yang menggunakan *routing Internal Border Gateway Protocol* (IBGP) dan *External* BGP (EBGP), serta dijalankan dengan *device* alternatif *routing*-nya berupa *Free Range Routing* (*FRRouting*). Simulasi jaringan DMVPN akan diukur performansi yang terjadi pada saat proses pengiriman paket *Transmission Control Protocol* (TCP) antar *client* di masing-masing *site*. Hasil performansi akan didapatkan dari nilai *Quality of Service* (QoS) dengan parameter *throughput, delay, jitter*, dan *packet loss*. Tolok ukur QoS yang digunakan berstandar *tiphon*. Hasil pengukuran menunjukkan hampir semua parameter tergolong dalam kategori yang sangat bagus. Nilai *throughput* tertinggi ada pada 3551 Kbps, *delay* terkecilnya adalah 0,43 detik, nilai *jitter* terkecil adalah 0,324 ms, dan *packet loss* yang dihasilkan adalah 0%. Berdasarkan hasil yang didapatkan ini, DMVPN mampu berjalan dengan sangat baik dan perangkat altenatif *routing*-nya mampu mengganti peran perangkat *router* konvensional seperti Cisco ataupun Juniper.

Kata kunci: VPN, *tunneling*, DMVPN, QoS

Abstract

Dynamic Multipoint Virtual Private Network (DMVPN) is a type of VPN technology. In contrast to other VPN models that require a point to point connection to be established on the tunnel path, in DMVPN the tunnel communication path can be formed point to multipoint, meaning that to connect several sites that are large in number on the DMVPN network only requires one tunnel path, so that at This DMVPN is more scalable than a VPN with point to point communication. This study aims to find out how the performance of the DMVPN full mesh type network if it runs with alternative routing that uses Internal Border Gateway Protocol (IBGP) and External BGP (EBGP) routing, and is run with alternative routing devices in the form of Free Range Routing (FRRouting). The DMVPN network simulation will measure the performance that occurs during the process of sending Transmission Control Protocol (TCP) packets between clients at each site. Performance results will be obtained from the value of Quality of Service (QoS) with parameters throughput, delay, jitter, and packet loss. The QoS benchmark used is the typhoon standard. The measurement results show that almost all parameters belong to the very good category. The highest throughput value is at 3551 Kbps, the smallest delay is 0.43 seconds, the smallest jitter value is 0.324 ms, and the resulting packet loss is 0%. Based on these results, DMVPN is able to run very well and its alternative routing device is able to replace the role of conventional router devices such as Cisco or Juniper.

Keywords: *VPN, tunneling, DMVPN, QoS*

I. PENDAHULUAN

Virtual Private Network (VPN) adalah suatu bentuk penerapan dalam teknologi jaringan yang membuat dapat terhubung dengan jaringan publik dengan sebuah koneksi yang bersifat *private* dan hanya bisa diakses oleh pihak tertentu saja. Cara kerja dari jaringan VPN adalah dengan membuat suatu jaringan *private* (*tunnel)* yang dapat

Diterima: 1 Januari 2021; Direvisi: 6 Februari 2021; Disetujui: 8 Maret 2021
JTERA, Vol. 6, No. 1, Juni 2021

© 2021 JTERA (Jurnal Teknologi Rekayasa), Politeknik Sukabumi

menghubungkan satu tempat ke tempat yang lain. Tetapi yang perlu digarisbawahi dalam VPN ini, untuk komunikasi yang digunakan masih bersifat *point to point* [1]. Sifat jaringan yang *point to point* inilah yang menyebabkan jaringan VPN kurang cocok jika diterapkan pada geografis yang memiliki kebutuhan *device* yang terbilang banyak. Dalam mengatasi hal tersebut, terdapat suatu teknologi VPN yang bisa membuat sifat koneksinya bukan secara *point to point* dan dapat membuat jaringan VPN lebih *scalable*. Teknologi ini disebut *Dynamic Multipoint Virtual Private Network* (DMVPN). Jaringan DMVPN ini terdiri dari *router-router* yang dikonfigurasikan dengan menggunakan *interface multipoint Generic Routing Encapsulation* (GRE). Oleh sebab itu, teknologi *tunneling* yang terbentuk di DMVPN bukan *point to point* lagi melainkan *point to multipoint* [2]. Dengan DMVPN ini, maka akan menghubungkan tempat-tempat yang sangat banyak secara dinamis, otomatis, dan sesuai dengan permintaan [3].

Beberapa penelitian terkait DMVPN sudah dilakukan. Penelitian [4] mengkaji mengenai evaluasi kinerja jaringan DMVPN dari mulai *phase 1* sampai *phase 3* dengan menggunakan berbagai macam *routing protocol*. *Device* yang dipakai dalam penelitian tersebut adalah menggunakan *router* Cisco. Hasil yang didapatkan adalah untuk nilai *throughput* terbesar didapatkan ketika menggunakan DMVPN *phase 2* RIPv2-BGP. Nilai *jitter* terbaik ada pada DMVPN *phase 2* EIGRP-BGP. *Packet loss* ada pada DMVPN *phase 3* RIPV2-BGP. Untuk *network convergence* didapatkan oleh DMVPN *phase 1* EIGRP-BGP. Pada penelitian [5], didapatkan bahwa nilai *throughput* terbaik ada pada DMVPN *phase 2* RIP, sedangkan untuk *jitter* dan *packet loss* berturut-turut mengalami nilai terbaik ketika menggunakan DMVPN *phase 2* EIGRP. Pada penelitian lain yang hanya berfokus pada implementasi DMVPN dikemukakan jika penerapannya dapat membuat jumlah *hop count* yang digunakan pada suatu topologi jaringan berkurang [6]. Peneliti [7], mencoba mengimplementasi jaringan DMVPN dengan protokol lain yaitu HSRP, dimana pada penelitian tersebut hanya diuji dengan *routing* EIGRP. Hasil yang diperoleh pada penelitian tersebut menjelaskan jika jaringan DMVPN akan menghasilkan nilai parameter-parameter yang baik. Penelitian tersebut mengatakan bahwa kedepannya DMVPN yang diterapkan dengan protokol lain (HSRP) ke depannya akan lebih sering diimplementasikan.

DMVPN bisa dengan sangat baik digabungkan dengan beberapa elemen untuk kemanan jaringan. Seperti pada penelitian [8] dan penelitian [9] yang mengkaji DMVPN dari segi keamanan jaringan dan enkripsi yang ada. Secara spesifik peneliti [8] mengemukakan bahwa DMVPN mampu mengenkripsi setiap paket yang dikirimkan pada jaringan. Terkait dari peforma jaringan DMVPN yang menerapkan skema keamanan sendiri disinggung pada penelitian [9]. Penelitian tersebut menguji dengan menggunakan TFTP dan video *streaming* dengan menggunakan berbagai metode enkripsi yang berbeda. Hasil yang didapatkan adalah ketika tanpa menggunakan enkripsi memiliki waktu transfer tercepat pada TFTP, sedangkan pada uji coba streaming AES memiliki kinerja yang lebih baik.

Penelitian ini akan mencoba mengkaji dengan hanya menfokuskan pada kinerja dari performa DMVPN dengan menggunakan pendekatan *routing* yang berbeda dengan penelitian yang kebanyakan menggunakan IGP (OSPF dan EIGRP). Penelitian ini akan mencoba menggunakan *routing* IBGP dan EBGP. Sifat topologi jaringannya nanti jika sudah menerapkan DMVPN berupa *full mesh*. Perbedaannya di sini dengan penelitian sebelumnya untuk menjalankan *service* DMVPN ini akan menggunakan *open source networking* yaitu *Free Range Routing* (FRR), berbeda seperti pada penelitian sebelumnya yang menggunakan *device vendor* Cisco.

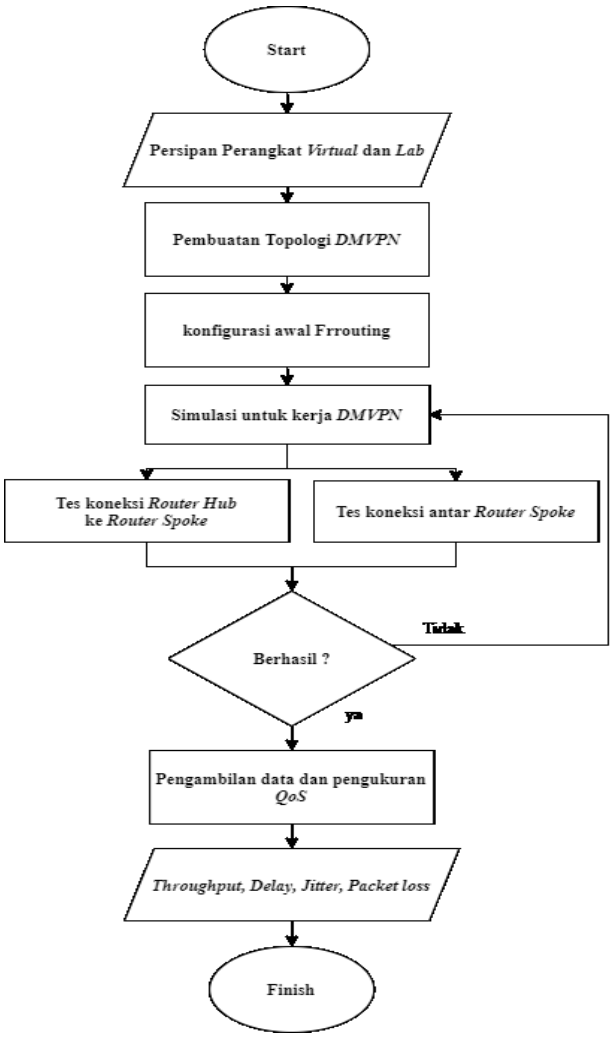
II. METODE PENELITIAN

Penelitian ini menggunakan suatu simulasi jaringan dalam menganalisis unjuk kerja DMVPN pada FRR dengan *routing* BGP. *Routing* BGP akan menerapkan dua skema yaitu *IBGP* dan *EBGP*. Skema kerja dari DMVPN nantinya akan menguji komuikasi yang terjadi pada saat antar *client* pada jaringan yang saling bertukar paket TCP. Model simulasi yang diterapkan dalam penelitian ini menggunakan program *network simulator* GNS3 dan bantuan *software* pendukung lain seperti Wireshark untuk menangkap *packet loss* dan menggunakan D-ITG *Traffic Generator* untuk mendapatkan nilai-nilai dari parameter *Quality of Service* (QoS).

A. Alur Penelitian

Gambar 1 merupakan alur kerja dari penelitian yang menggambarkan langkah-langkah implementasi DMVPN pada FRR dengan *routing* BGP.

Alur kerja dimulai dengan mempersiapkan *device virtual* dan lab yang diperlukan yaitu sebuah *router* FRR. Langkah selanjutnya yang dilakukan adalah menyusun topologi yang akan disimulasikan pada *software network* simulator GNS3.



Gambar 1. *Flowchart* pengerjaan DMVPN

Selanjutnya melakukan konfigurasi awal pada FRR yang mencakup pengaktifan *service* yang nanti akan dijalankan, pembuatan IP *address*, *tunnel*, dan IP *tables* yang akan mengizinkan komunikasi langsung antar *spoke* terjalin tanpa melalui *hub*. Setelah topologi dan konfigurasi awal terbentuk baru bisa dilakukan simulasi unjuk kerja untuk jaringan DMVPN tersebut dengan melakukan tes koneksi dari *router hub* ke *router spoke* dan antar *router spoke*. Jika berhasil maka hal terakhir yang perlu dilakukan adalah pengambilan data beserta pengukuran QoS-nya yang mencakup *throughput*, *delay*, *jitter*, dan *packet loss*.

B. Free Range Routing

FRRouting (FRR) adalah IP *routing suite* yang memiliki performa tinggi, fitur yang lengkap, dan bersifat *open source*. FRR mengimplementasikan semua protokol *routing dynamic* seperti BGP, RIP, OSPF, IS-IS, dan lainnya. FRR adalah perangkat yang berkinerja tinggi dan dapat mudah menangani tabel perutean internet secara lengkap dan cocok digunakan pada perangkat keras mulai dari SBC murah hingga *router* kelas komersial. FRR secara aktif digunakan dalam produksi oleh ratusan perusahaan, universitas, laboratorium penelitian, dan pemerintah [10].

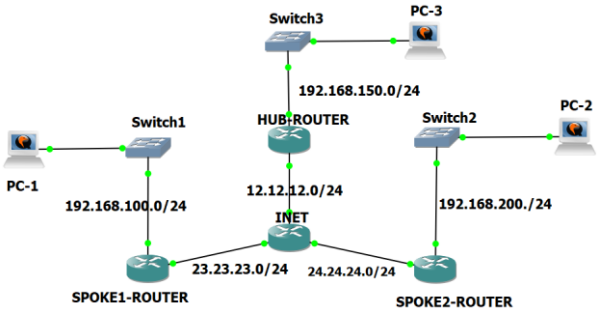
C. DMVPN

DMVPN merupakan suatu teknologi dari Cisco yang digunakan untuk memastikan koneksi jaringan antara beberapa *site* dengan cara yang dinamis, cepat dan otomatis. DMVPN menawarkan skalabilitas dan tidak melibatkan konfigurasi tambahan pada perangkat yang sudah dikonfigurasi [11]. DMVPN menggabungkan beberapa *protocol* yaitu ada *multipoint* GRE (mGRE), *Next Hop Resolution Protocol* (NHRP), protokol IP *security* sebagai opsional tambahan dari segi keamanan, dan sebuah *dynamic routing protocols*. Protokol utama yang sangat dibutuhkan dari DMVPN terdiri dari mGRE dan NHRP. mGRE ini nantinya digunakan untuk membuat koneksi *multipoint* VPN hanya dengan satu buah *interface tunnel* [12], sedangkan NHRP berfungsi untuk meningkatkan efisiensi perutean lalu lintas jaringan komputer melalui jaringan NBMA (*Non-Broadcast, Multiple Access*) yaitu alamat fisik suatu *router*. NHRP menyediakan solusi mirip ARP yang memungkinkan sistem secara dinamis mempelajari alamat NBMA dari perangkat yang merupakan bagian dari jaringan itu dan memungkinkan sistem ini untuk berkomunikasi secara langsung tanpa memerlukan lalu lintas untuk menggunakan *hop* perantara [10]. Pada jaringan DMVPN terdapat istilah *router hub* yang merupakan *router* pusat informasi dari jaringan DMVPN, dan satu lagi adalah *router spoke* yang merupakan *router* cabang atau *client*.

D. Topologi Jaringan

Topologi yang dikerjakan akan menggunakan 4 FRR, 3 *switch*, dan 3 PC yang berperan sebagai *client*, seluruh bagiannya akan ditampilkan pada Gambar 2. *Router* bagian atas akan menjadi *hub*-nya, tengah akan menjadi *router* dua bagian bawah akan menjadi *spoke* dimana dihubungkan dengan *router* bagian tengah. Cara kerja nantinya dari *client* PC dari *router spoke* akan berkomunikasi dengan *client* PC dari *router hub* melalui jalur koneksi *tunneling* dan bukan melewati jalur kabel biasa.

Komunikasi antar *client* yang ada pada *router spoke* sendiri juga akan melalui jalur *interface tunnel* yang terbentuk antar masing masing *spoke* jadi disini komunikasinya bisa langsung menuju *spoke* yang lain tanpa melewati *router hub* terlebih dahulu. Di sini untuk jalur *interface tunnel*-nya hanya diperlukan satu buah yang sifatnya *point to multipoint*. Jenis topologi di atas jika menerapkan DMVPN tergolong dalam *full mesh topology.*



Gambar 2. Topologi jaringan

Tabel 1. Kategori *throughput* berdasarkan standar Tiphon [13]

Kategori	Nilai (%)
Sangat Bagus	100
Bagus	75
Sedang	50
Buruk	< 25

E. Quality of Service (QoS)

QoS merupakan suatu nilai yang menunjukan kehandalan suatu jaringan apakah bisa menyediakan layanan yang baik dengan menyediakan *bandwidth* yang sesuai dan kemampuan dalam mengatasi *jitter* dan *delay* yang ada. Parameter yang tercakup secara umum dalam QoS antara lain *throughput*, *delay*, *jitter*, dan *packet loss* [13].

F. Throughput

Throughput adalah jumlah total kedatangan paket IP sukses yang diamati di tempat pengukuran pada *destination* selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut (sama dengan jumlah pengiriman paket IP sukses per *service-second*). *Throughput* lebih pada menggambarkan *bandwidth* yang sebenarnya pada waktu tertentu dan pada kondisi dan jaringan internet tertentu yang digunakan untuk mengunduh suatu *file* dengan ukuran tertentu [14]. Adapun kategori *throughput* berdasarkan standar Tiphon dapat dilihat pada Tabel 1. Nilai pada *throughput* diperoleh dengan rumus sebagai berikut [15]:

$$Throughput = \frac{jumlah\ packet\ yan\ dikirim\ (bit)}{lamanya\ waktu\ pengiriman} bps \quad (1)$$

G. Delay

Delay merupakan lama yang dibutuhkan suatu paket atau data untuk dikirimkan ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama. Besarnya *delay* dikategorikan berdasarkan standar Tiphon seperti pada Tabel 2. Nilai *delay* bisa didapatkan dengan rumus [15]:

Tabel 2. Kategori *delay* mengacu pada standar Tiphon [13]

Kategori	Nilai (ms)
Sangat Bagus	< 150
Bagus	150 – 300
Sedang	300 – 450
Buruk	> 450

Tabel 3. Kategori *jitter* mengacu pada standar Tiphon [13]

Kategori	Nilai (ms)
Sangat Bagus	0
Bagus	0 – 75
Sedang	75 – 125
Buruk	125 – 225

Tabel 4. Kategori *packet loss* mengacu pada standar Tiphon [13]

Kategori	Nilai (%)
Sangat Bagus	0
Bagus	3
Sedang	15
Buruk	25

$$Delay = \frac{\text{panjang paket } (bit)}{link\ bandwith\ (bps)} second \quad (2)$$

H. Jitter

Jitter sebenarnya adalah *delay* juga. Tetapi *delay* yang sifatnya divariasikan dan juga berhubungan erat dengan *latency*, *jitter* ini merepresentasikan banyaknya variasi *delay* pada transmisi data di jaringan. *Delay* antrian pada perangkat jaringan seperti *router* dan *switch* dapat menyebabkan *jitter*. Besarnya *jitter* dikategorikan berdasarkan standar Tiphon seperti pada Tabel 3. *Jitter* diperoleh dengan rumus [15]:

$$Jitter = \frac{\text{total variasi } delay}{\text{total paket yang diterima}} second \quad (3)$$

I. Packet Loss

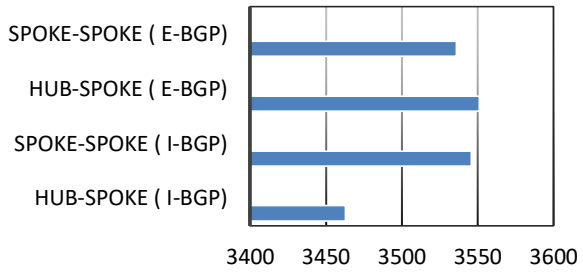
Packet loss (PL) adalah parameter yang menunjukkan jumlah total paket yang hilang selama data kirim yang biasanya dapat terjadi karena *collision* dan *congestion* pada jaringan. Besarnya *packet loss* dikategorikan berdasarkan standar Tiphon seperti pada Tabel 4. *Packet loss* diperoleh dengan rumus [15]:

$$PL = \frac{packets\ send - packets\ recieved}{packets\ send} \text{x}100\% \quad (4)$$

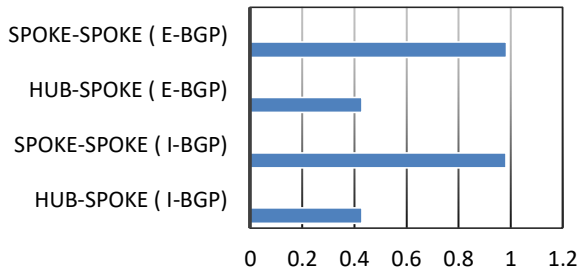
III. HASIL DAN PEMBAHASAN

A. Pengujian Throughput

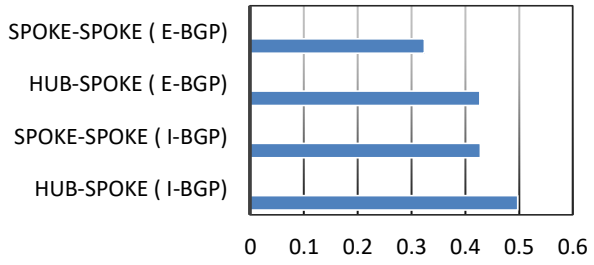
Gambar 3 merupakan hasil *throughput* yang diukur. Pada nilai *throughput* ini semakin besar nilai *throughput* yang ada menunjukan semakin bagus kualitas jaringan yang berjalan. Dari hasil pengukuran nilai *throughput* yang dilakukan didapatkan hasil yang nilainya hampir saling mendekati satu sama lain dengan rentang nilai 3400-3500 kbps. Nilai pengukuran yang didapat tersebut jika merujuk ke standar Tiphon bisa dikatakan sangat bagus. *Throughput* terbesar diperoleh saat proses komunikasi *hub-spoke* menggunakan *routing* E-BGP nilainya mencapai 3551. Kedua ada pada komunikasi antar *spoke* menggunakan *routing* IBGP, nilainya adalah 3546 kbps. Terbesar ketiga dimiliki oleh komunikasi antar *spoke* mengunakan *routing* EBGP nilainya 3536 kpbs. *Throughput* terkecil didapatkan saat terjadi proses komunikasi antar *hub-spoke* menggunakan IBGP dengan nilai yang sebenarnya tidak terlalu jauh yaitu 3463 kbps.



Gambar 3. Hasil pengujian *throughput*



Gambar 4. Hasil pengukuran *delay*



Gambar 5. Hasil pengukuran *jitter*

B. Pengujian Delay

Delay berpengaruh pada proses pengiriman paket. Semakin kecil nilai suatu *delay* maka kualitas jaringan pun semakin bagus. Dari hasil pengukuran *delay* yang ditampilkan Gambar 4 menunjukkan *delay* ada pada *range* nilai 0,4 s sampai hampir mendekati 1 s. Merujuk pada standar Tiphon yang ada, *delay* yang dihasilkan dari semua jenis komunikasi dapat dikatakan buruk. Dari hasil yang didapatkan nilai *delay* terbaik berada pada saat komunikasi dari *hub* menuju *spoke* baik menggunakan *routing* IBGP maupun EBGP, keduanya sama-sama menghasilkan nilai 0,429 s. Sedangkan untuk komunikasi antar *spoke*-nya berurutan di posisi ketiga dan keempat untuk kualitas *delay*-nya yaitu pada IBGP sendiri didapatkan nilai 0,983 s disusul dengan EBGP dengan *delay* 0,984 s.

C. Pengujian Jitter

Nilai *jitter* akan semakin bagus jika nilai yang dihasilkan juga semakin kecil. Berdasarkan hasil pengukuran pada Gambar 5, *jitter* yang didapatkan dari pengukuran sendiri berada pada angka 0,3 ms sampai 0,4 ms. Merujuk ke standarisasi Tiphon maka kualitas *jitter* pada DMVPN yang dihasilkan terbilang sangat baik. *Jitter* terbagus didapatkan saat proses komunikasi antar *spoke* dengan *routing* EBGP, nilai yang dihasilkannya adalah 0,324 ms. Berlanjut ke *hub spoke* dengan nilainya adalah 0,428 ms. Nilai tersebut sangat berdekatan dengan komunikasi antar *spoke* dengan *routing* IBGP yaitu 0,429 ms. Pada komunikasi *hub spoke* dengan IBGP merupakan nilai yang terbesar yakni 0,498 ms.

D. Pengujian Packet Loss

Pengukuran *packet loss* di jaringan DMVPN semua model komunikasi yang berjalan menghasilkan nilai yang sama yaitu sebesar 0%. Nilai *packet loss* merujuk kepada berapa besar paket yang hilang selama proses pengiriman paket ataupun komunikasi dari satu *client* menuju *client* yang lain, atau dari pengirim menuju penerima artinya selama proses pengiriman *packet* berlangsung tidak ada *packet* yang di-*drop* sama sekali. Berdasarkan proses pengukuran yang telah dilakukan menunjukan jika jaringan DMVPN sama sekali tidak memiliki *packet loss* yang berarti data yang dikirim menuju penerima utuh sempurna.

E. Diskusi

Merujuk dari beberapa penelitian yang ada, hasil QoS dalam penelitian ini tergolong sangat baik. Nilai *throughput* terbaik yang didapatkan pada peneliti [5] adalah 1262,2 kbps, peneliti [9] berada pada rentang 1000 kbps, sedangkan pada penelitian

ini mencapai 3551 kbps. *Throughput* yang dihasilkan hanya lebih kecil dari peneliti [7] dengan nilai terbesarnya 3829 kbps, dengan catatan pada penelitian [7] tersebut menggunakan skema *dual hub.* Nilai *jitter* terbaik yang ada di penelitian ini yaitu 0,324 ms menjadi yang terbaik dari semua penelitian sebelumnya, salah satu contohnya yaitu *jitter* yang dihasilkan peneliti [5] yaitu sebesar 11,2148 ms. Sebanding juga dengan *packet loss* pada penelitian ini selama pengujian dilakukan tidak ditemukan *packet loss*, sama seperti pada penelitian [4] dan [5] dengan *packet loss* 0%. Pada nilai *delay* sendiri, hanya penelitian inilah yang memaparkan hasilnya. Pada berbagai penelitian yang ada, waktu *delay* langsung diwakili oleh *jitter*.

IV. KESIMPULAN

Berdasarkan pengujian simulasi jaringan DMVPN dan pengukuran yang dilakukan dengan menggunakan alternatif *routing* berupa FRR, diperoleh performa QoS yang mencakup *throughput*, *jitter*, dan *packet loss* semua nilainya tergolong ke dalam kualitas jaringan yang sangat baik. Akan tetapi pada parameter *delay*-nya sendiri didapatkan nilai yang buruk. Secara keseluruhan, walaupun FRR ini bukan merupakan perangkat *routing* asli melainkan sebenarnya hanya sebuah *computer* yang dialihkan menjadi sebuah *router*, dari segi performansi tidak kalah dengan perangkat *vendor* lainnya seperti Cisco, Mikrotik, dan Juniper. Selain itu pada FRR ini bisa menjalankan *service* DMVPN dengan sempurna tanpa ada kendala. Secara keseluruhan performa paling maksimal terjadi saat menggunakan *routing* EBGP. Performansi *routing* EBGP pada DMVPN ini ke depannya mungkin bisa diuji dengan beberapa *routing protocol* lain yang ada seperti RIPV2, OSPF, dan EIGRP untuk mencari performansi yang lebih baik pada penelitian ini dan tentunya semua menggunakan alternatif *routing* (FRR) untuk perangkat yang digunakan.

REFERENSI

[1] P. Oktivasari and A. B. Utomo, "ANALISA VIRTUAL PRIVATE NETWORK MENGGUNAKAN OPENVPN DAN POINT TO POINT TUNNELING PROTOCOL ANALYSIS OF VIRTUAL PRIVATE NETWORK USING OPENVPN AND POINT TO POINT," *Jurnal Penelitian Komunikasi dan Opini Publik*, vol. 20, no. 2, pp. 185–202, 2016.

[2] G. A. Tizazu, K. H. Kim, and A. B. Berhe, "Dynamic routing influence on secure enterprise network based on DMVPN," *Int. Conf. Ubiquitous Futur. Networks, ICUFN*, pp. 756–759, 2017.

[3] A. Bahnasse, F. E. Louhab, A. Khiat, A. Badri, M. Talea, and A. Sahel, "Dynamic Multipoint Virtual Private Network influence on Video Conferencing Quality of Service," *2nd Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2019*, pp. 1–6, 2019.

[4] M. Rizal and S. U. Masruroh, "EVALUASI KINERJA JARINGAN DMVPN MENGGUNAKAN ROUTING PROTOCOL RIPv2, OSPF, EIGRP DENGAN BGP," *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 2, no. 3, pp. 143–150, 2018.

[5] P. Rip, S. U. Masruroh, and A. Fiade, "Performance Evaluation DMVPN Using Routing Protocol RIP, OSPF, And EIGRP," *2018 6th Int. Conf. Cyber IT Serv. Manag.*, pp. 1–6, 2018.

[6] N. Angelescu, D. C. Puchianu, G. Predusca, L. D. Circiumarescu, and G. Movila, "DMVPN simulation in GNS3 network simulation software," *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pp. 1–4, 2017.

[7] T. Alam, "Design and Implementation of a Secured Enterprise Network using Dynamic Multipoint VPN with HSRP Protocol," *2018 Int. Conf. Innov. Sci. Eng. Technol. ICISET 2018*, no. October, pp. 367–371, 2018.

[8] H. Li, P. W. C. Prasad, A. Alsadoon, L. Pham, and A. Elchouemi, "An improvement of backbone network security using DMVPN over an EZVPN structure," *2016 Int. Conf. Adv. Electr. Electron. Syst. Eng. ICAEES 2016*, pp. 203–207, 2017.

[9] F. A. Daud, R. Ab Rahman, M. Kassim, and A. Idris, "Performance of encryption techniques using dynamic virtual protocol network technology," *ICSET 2018 - 2018 IEEE 8th Int. Conf. Syst. Eng. Technol. Proc.*, no. October, pp. 29–34, 2019.

[10] FRR User Manual Release latest. 2020.

[11] Dynamic Multipoint VPN (DMVPN), "Design Guide,Corporate Headquarters Cisco Systems", 2006.

[12] S. H. Kurniadi, E. Utami, and F. W. Wibowo, "Building Dynamic Mesh VPN Network using MikroTik Router," *J. Phys. Conf. Ser.*, vol. 1140, no. 1, 2018.

[13] Y. Yanto, "Analisis Qos (Quality of Service) Pada Jaringan Internet (Studi Kasus : Fakultas Teknik Universitas Tanjungpura)," *JUSTIN (Jurnal Sistem dan Teknologi Informasi)*, vol. 1, no. 1 pp. 11–16, 2013.

[14] B. Sugiantoro and Y. B. Mahardhika, "ANALISIS QUALITY OF SERVICE JARINGAN WIRELESS SUKANET WiFi DI FAKULTAS SAINS DAN TEKNOLOGI UIN SUNAN KALIJAGA," *J. Tek. Inform.*, vol. 10, no. 2, pp. 191–201, 2018.

[15] W. Sugeng, J. E. Istiyanto, K. Mustofa, and A. Ashari, "The Impact of QoS Changes towards Network Performance," *Int. J. Comput. Networks Commun. Secur.*, vol. 3, no. 2, pp. 48–53, 2015.