Simulasi Perancangan Jaringan DMVPN dengan GNS3

Satria Adidaya[1], Ade Nurhayati[2]
[1,2]Akademi Teknik Telekomunikasi Sandhy Putra Jakarta
[1,2]Jalan Daan Mogot KM 11, RT. 1/RW.4,Cengkareng, Daerah Khusus Ibukota Jakarta 11710, Indonesia
satriaadidaya123@gmail.com

Abstrak – DMVPN (*Dynamic Multipoint Virtual Private Network*) adalah teknologi VPN yang diciptakan oleh Cisco. DMVPN menggabungkan beberapa protokol seperti NHRP (*Next Hop Resolution Protocol*) untuk pemetaan alamat IP, *multipoint* GRE (*Generic Routing Encapsulation*) untuk protokol *tunnel*, IPSec untuk keamanan dan protokol routing statis atau dinamis. Kelebihan teknologi ini dibandingkan VPN tradisional adalah jaringan VPN nya yang dinamis sehingga mudah digunakan dalam jaringan berskala besar dan apabila terjadi penambahan *router* baru konfigurasi cukup dilakukan pada *router* yang baru ditambahkan tanpa menambah atau mengubah konfigurasi *router* yang lain. Jaringan DMVPN bekerja seperti model *client-server*,memiliki NHS (*Next Hop Server*) dan NHC (*Next Hop Client*),NHS berperan untuk menyimpan *database* alamat IP dan melayani *query* dari *router-router* lain yang berperan sebagai NHC. Penelitian ini mensimulasikan jaringan DMVPN dengan GNS3 dan melakukan pengujian QoS dengan membandingkan kinerja VPN *site-to-site*, jaringan tanpa VPN dan DMVPN dengan menggunakan beban *video streaming*. Hasil pengujian *throughput* sekitar 99%,hasil ini dikategorikan sangat baik menurut standar TIPHON karena nilai throughput 76%-100% dari data yang dikirimkan. Hasil pengujian *delay* dikategorikan sangat baik menurut standar TIPHON karena nilai *delay* <150 ms sehingga dapat digunakan untuk *video streaming*.Hasil pengujian *packet loss* sebesar 0% dikategorikan sangat bagus menurut standar TIPHON karena menunjukkan tidak ada paket yang hilang selama proses transmisi.

Kata kunci – *DMVPN, NHRP, multipoint GRE, IPSec, NHS, NHC*

Abstract*— DMVPN (Dynamic Multipoint Virtual Private Network) is a VPN technology created by Cisco. DMVPN combines several protocols, such as NHRP (Next Hop Resolution Protocol) for IP address mapping, multipoint GRE (Generic Routing Encapsulation) for tunnel protocols and IPSec for security and static or dynamic routing protocols. The advantages of this technology compared to traditional VPNs are its dynamic aspect of VPN network so that it is easy to use on a larger scale network. Moreover, when there is an additional new router, the configuration is sufficient to be done on newly added routers without adding or changing the configuration of other routers. DMVPN network works like a client-server model. It has NHS (Next Hop Server) and NHC (Next Hop Client). NHS has a role to store IP address database and serves queries from other routers that act as NHC. This research simulates DMVPN network with GNS3 and performs QoS testing by comparing the performance of VPN site-to-site, network without VPN and DMVPN by using video streaming load. The throughput test results are around 99%, which are categorized as excellent according to TIPHON standards because the throughput value is 76% -100% of the total data sent. The delay test results are categorized as excellent according to the TIPHON standard. The delay value is <150 ms so that the DMVPN network with such delay value can be used for video streaming. The result of packet loss testing is 0% which is considered excellent according to TIPHON standard because it shows that no packet was lost during the transmission process*

Keywords *– DMVPN, NHRP, multipoint GRE, IPSec, NHS, NHC*

I. PENDAHULUAN

A. Latar Belakang

Seiring perkembangan ekonomi dan kemajuan telekomunikasi di Indonesia,banyak perusahaan yang mulai membuka cabangnya di daerah.Setiap kantor cabang tersebut harus terhubung dengan kantor pusat, hubungan yang dibangun tentunya harus memiliki privasi,keamanan,fleksibilitas dan cepat.Metode yang dapat dibangun untuk model jaringan seperti itu adalah *Dynamic Multipoint Virtual Private Network* (DMVPN).

DMVPN adalah metode yang dikenal secara luas dan mudah untuk diterapkan sehingga dapat menjadi pilihan untuk membangun jaringan virtual yang aman dan berskala besar. Metode DMVPN diciptakan oleh Cisco sebagai pengganti dari teknologi VPN tradisional yang masih bersifat *point-to-point.* Teknologi ini menggabungkan IPSec, NHRP dan *multipoint* GRE, sehingga akan didapat jaringan VPN yang aman dan dinamis. DMVPN memudahkan pekerjaan administrator karena jaringan VPN dapat dibentuk otomatis secara *point-to-multipoint* sehingga tidak perlu membuat *tunnel* satu per satu ke masing-masing cabang.

Beberapa penelitian mengenai jaringan DMVPN sudah banyak dilakukan, diantaranya adalah *DMVPN simulation in GNS3 network simulation* software yang ditulis oleh N. Angelescu dkk (2017). Penelitian tersebut membahas mengenai simulasi jaringan DMVPN dengan software GNS3. Penelitian lainnya adalah *Established Secured Enterprise Network Routing Protocols by using DMVPN* yang ditulis oleh K.Sandhya dan V.Kakulapati (2018). Penelitian tersebut membahas mengenai simulasi jaringan DMVPN dengan membandingkan kinerja protokol routing OSPF dan EIGRP.

B. Tujuan Penelitian

1. Merancang jaringan DMVPN dengan software simulator GNS3
2. Menguji konektivitas dan mengukur QoS pada jaringan DMVPN dengan menggunakan *software* Wireshark

C. Rumusan Masalah

1. Apa yang dimaksud dengan jaringan DMPVN?
2. Bagaimana cara merancang jaringan DMVPN dalam simulator?
3. Bagaimana cara menguji konektivitas dan mengukur QoS pada jaringan DMVPN?

D. Batasan Masalah

1. Simulator yang digunakan penulis adalah GNS3 versi 1.2.3
2. Simulasi ini dilakukan dengan perangkat yang terbatas
3. Pengujian QoS hanya menggunakan video streaming
4. Pengujian QoS juga membandingkan antara jaringan VPN site-to-site dan tanpa VPN

II. DASAR TEORI

A. Jaringan Komputer

Jaringan komputer adalah dua atau lebih komputer yang saling terhubung satu sama lain melalui media transmisi sehingga dapat saling berkomunikasi dan berbagi sumber daya seperti data,*hardisk*,*printer* dan *scanner*.Adanya jaringan komputer,memungkinkan pengguna untuk berkomunikasi dan mendapatkan informasi dengan mudah.Jaringan komputer juga dapat menghemat sumber daya,berbagai perangkat seperti *hardisk*,*printer* dan *scanner* dapat digunakan secara bersama-sama,sehingga masing-masing pengguna tidak harus memiliki perangkat tersebut. [12]

Berikut ini adalah komponen-komponen jaringan komputer :

1. ***Protocol***

   Protokol adalah aturan-aturan atau prosedur yang digunakan oleh komputer untuk saling berkomunikasi.Protokol jaringan dibuat agar setiap komputer dapat saling berkomunikasi walaupun berbeda spesifikasi dan dari vendor yang berbeda.Contoh dari protokol jaringan yang dikenal adalah OSI dan TCP/IP. [13]

2. ***Medium***

   Medium adalah media yang menghantarkan data antara pengirim dan penerima.Media transmisi dapat berupa kabel seperti kabel Coaxial,kabel UTP,kabel Fiber Optik atau berupa nirkabel seperti gelombang radio. [13]

3. ***Messages***

   Messages adalah data yang dikirim atau diterima dalam jaringan komputer.Contohnya adalah *e-mail*,*voip*,*web page* dan lain-lain. [13]

4. ***Device***

   Device adalah perangkat yang digunakan untuk berkomunikasi dalam jaringan komputer.Ada dua jenis device yaitu *End Device* dan *Intermediary Device*.*End Device* adalah perangkat yang berada disisi pengguna (*end*) seperti PC,IP *Phone*,*server*,*printer*.Sedangkan *Intermediary Device* adalah perangkat yang berfungsi sebagai penghubung antar *end device* seperti *switch*,*router*,*wireless access point.* [13]

B. VPN

VPN adalah jaringan *private* yang menghubungkan beberapa jaringan lokal menggunakan jaringan publik (internet).VPN menggunakan jaringan publik sebagai perantaranya,tetapi karena jaringan ini disebut *private*,jaringan ini hanya dapat diakses oleh penggunanya saja [10].Walaupun VPN menggunakan jaringan publik sebagai perantaranya,pengguna VPN dapat tetap menggunakan jaringan dengan aman.Hal ini karena VPN menyediakan berbagai keamanan bagi penggunanya dengan cara melakukan berbagai metode seperti enkripsi,*hashing*,autentikasi dan *anti-replay*.

Berikut ini adalah keuntungan dari penggunaaan jaringan VPN :

1. Perusahaan dapat mengembangkan jaringannya dengan mudah tanpa harus menyewa *leased line* [15].
2. Biaya implementasi yang murah dibandingkan *private leased line*.Hal ini karena VPN menggunakan jaringan publik (internet) sebagai perantaranya [15].
3. Meningkatkan skalabilitas karena perusahaan yang membuka cabang baru tidak perlu menggunakan *leased line*.Perusahaan pusat dan cabang cukup terhubung dengan internet dan VPN dapat langsung digunakan [15].
4. *Availability* yang tinggi karena pengguna VPN dapat terhubung dimana saja selama memiliki koneksi internet [15].

C. Multipoint GRE

Generic Routing Encapsulation (GRE) adalah protokol *tunneling* yang diciptakan oleh Cisco.GRE *tunnel* adalah jaringan *overlay* karena GRE dibangun diatas jaringan *transport*.GRE dapat mengenkapsulasi berbagai protokol layer 3 dan mendukung protokol *routing dynamic* sehingga menjadikan protokol ini sangat fleksibel [6].

Jenis lain yang akan penulis gunakan dalam DMVPN ini adalah *multipoint* GRE.*Multipoint* GRE adalah *tunnel* GRE yang mempunyai kemampuan untuk membentuk *tunnel* yang bersifat *point-to-multipoint*

D. Next Hop Resolution Protocol

Next Hop Resolution Protocol (NHRP) adalah protokol yang digunakan untuk menyediakan resolusi pengalamatan untuk *host* ataupun untuk jaringan *non-broadcast multi-access* (NBMA) seperti ATM dan *Frame Relay* [7].

NHRP bekerja dengan metode *client-server*.Ada dua bagian dalam NHRP yaitu *Next Hop Server* (NHS) dan *Next Hop Client* (NHC) atau disebut juga *hub-and-spoke*.Sebuah *router* akan digunakan sebagai *hub* dan *router* yang lain akan menjadi *spoke*.Router *hub* berfungsi untuk menyimpan *database* NHRP dan menjawab NHRP *query* yang dikirim oleh *spoke*.*Router spoke* akan dikonfigurasi alamat *hub* secara statis dan ketika *spoke* aktif,secara otomatis akan mendaftarkan alamat *tunnel* dan fisik nya ke *hub* yang sudah dikonfigurasi [6].

E. IP Security

IP *Security* atau *IPSec* adalah sekumpulan protokol yang menyediakan keamanan untuk jaringan VPN. *IPSec* bekerja pada *layer* ketiga OSI (*network layer*) dan menyediakan beberapa layanan keamanan sebagai berikut [16]:

1. ***Confidentiality* (Kerahasiaan)**
   Kerahasiaan pengguna didapat dengan melakukan enkripsi data sehingga data tidak dapat dibaca oleh pihak-pihak lain diluar jaringan VPN. Enkripsi data dapat menggunakan algoritma tertentu seperti *Digital Encryption Standar* (DES),*Triple* DES (3DES),*Advanced Encryption Standard* (AES) atau *Software-optimized Encryption Algorithm* (SEAL).
2. ***Data Integrity* (Integritas Data)**
   Integritas data berarti data tidak berubah atau dimanipulasi selama perjalanan dari pengirim ke tujuan. Hal ini dapat dilakukan dengan metode *hashing*,ada beberapa algoritma yang digunakan untuk *hashing* seperti *Message Digest Algorithm 5* (MD5) atau *Secure Hash Algorithm* (SHA).
3. ***Authentication* (Autentikasi)**
   IPSec menjamin bahwa data yang diterima adalah berasal dari sumber yang seharusnya. Autentikasi dalam jaringan VPN menggunakan protokol *Internet Key Exchange* (IKE).
4. ***Anti-replay Protection***
   Anti-replay menjamin bahwa data bersifat unik dan tidak diduplikasi selama perjalanan dari pengirim ke tujuan.

F. Dynamic Multipoint VPN (DMVPN)

DMVPN adalah teknologi VPN yang diciptakan oleh Cisco.VPN ini menggunakan multipoint *Generic Routing Encapsulation* (GRE) sebagai *tunnelnya*,*Next Hop Resolution Protocol* (NHRP) untuk memetakan alamat IP dan IP *Security* yang berfungsi untuk mengamankan koneksi sehingga dapat menciptakan koneksi VPN yang aman dan bersifat *full-mesh* [4].Hal ini dapat meringankan tugas administrator karena pembentukan jaringan VPN akan lebih mudah dibandingkan dengan VPN tradisional yang masih bersifat *point-to-point*.

Dalam jaringan DMVPN,masing-masing *spoke* membentuk *tunnel* menuju *hub*,tunnel ini bersifat tetap,yang berfungsi untuk mendaftarkan alamat IP fisik dan tunnel *spoke* ke *hub*.Sementara *tunnel spoke-to-spoke* hanya akan dibentuk ketika *spoke* ingin berkomunikasi dengan *spoke* lain, ketika tidak ada komunikasi melalui *tunnel*,*tunnel* ini akan dinonaktifkan. [4]

Secara default,jaringan DMVPN tidak mengenkripsi data-data yang ada didalamnya. Hal ini tentu saja tidak aman karena data-data yang melewati jaringan VPN bersifat pribadi. Untuk mengatasi masalah tersebut,*framework* IPSec dapat diimplementasikan pada *tunnel* untuk memberikan layanan keamanan seperti autentikasi,enkripsi,*hashing* dan *anti-replay*.

DMVPN bekerja menggunakan dua teknologi utama yaitu NHRP dan *multipoint* GRE. NHRP berfungsi untuk memetakan alamat IP dan *multipoint GRE* berfungsi untuk pembentukan *tunnel* secara *point-to-multipoint*. Saat jaringan DMVPN dibentuk,satu *router* akan ditunjuk sebagai *hub* atau *Next Hop Server* (NHS) dan yang lain sebagai *spoke* atau *Next Hop Client* (NHC).

Masing-masing *spoke* akan dikonfigurasi alamat *hub* secara statis,sehingga ketika *spoke* aktif,secara otomatis akan mendaftarkan alamat IP fisik dan *tunnel*nya ke *hub*,lalu *hub* akan menyimpan alamat-alamat tersebut ke dalam *database*nya.Saat ada *spoke* yang ingin berkomunikasi dengan *spoke* yang lain,dia akan membentuk *tunnel* ke arah *hub* dan mengirimkan NHRP *query* untuk meminta informasi mengenai alamat fisik dari *tunnel* tujuannya,lalu *hub* akan mengirimkan NHRP *reply* yang berisi alamat yang dituju *spoke* tersebut.Setelah *spoke* mengetahui alamat tersebut,maka *spoke* akan membentuk *tunnel multipoint* GRE ke tujuan.[6]

DMVPN dalam implementasinya memiliki tiga metode atau biasa disebut sebagai p*hase*,sebagai berikut [9] :

1. **DMVPN *Phase* 1**

   Koneksi yang ada dalam *phase* ini adalah *spoke*-to-*hub*.Sehingga apabila antar *spoke* ingin berkomunikasi maka data akan melewati *hub* terlebih dahulu.*Tunnel* yang dibangun pada *hub* adalah multipoint GRE sedangkan *spoke* menggunakan tunnel point-to-point GRE ke *hub*.*Phase* ini tidak membangun *tunnel* yang dinamis antar *spoke*.

2 **DMVPN *Phase* 2**

   DMVPN p*hase* 2 memungkinkan antar *spoke* untuk saling berkomunikasi secara dinamis tanpa melalui *hub*.*Phase* ini,baik *hub* ataupun *spoke* menggunakan tunnel multipoint GRE.

3. **DMVPN *Phase* 3**

   DMVPN *phase* 3 mendukung adanya summarization dalam jaringan DMVPN.*Phase* ini juga menambahkan NHRP *redirect* dan NHRP *shortcut*.NHRP *redirect* dikonfigurasi pada *hub*,berfungsi untuk memberitahukan *spoke* bahwa ada jalur yang lebih baik selain melalui *hub*.NHRP *shortcut* berfungsi untuk mengubah informasi CEF pada *spoke*.

G. Enhanced Interior Gateway Routing Protocol (EIGRP)

Enhanced Interior Gateway Routing Protocol (EIGRP) adalah protokol *routing* yang bersifat *Distance Vector*,protokol ini diciptakan oleh Cisco (Cisco Proprietary).EIGRP termasuk ke dalam kategori IGP *(Interior Gateway Protocol*) yang digunakan untuk menghubungkan jaringan-jaringan dalam satu *autonomous system* (AS) [2].

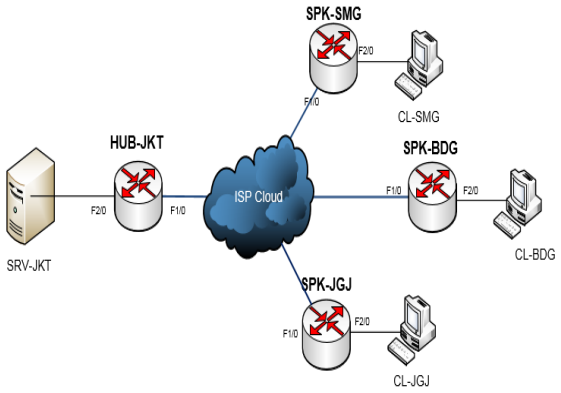
Kelebihan EIGRP dibandingkan protokol *routing distance vector* yang lain adalah EIGRP menggabungkan karakteristik dari *distance vector* dan *link state*.Protokol *routing* ini memiliki waktu konvergensi yang cepat, menggunakan algoritma *Diffusing Update Algorithm* (DUAL) untuk menentukan jalur terbaik ke tujuan dengan mempertimbangkan *bandwidth,Delay,reliability,load dan mtu* untuk *metric* nya.EIGRP memiliki nilai *administrative distance* (AD) 90 untuk internal, 170 untuk eksternal dan 5 untuk *route summary*.EIGRP mendukung protokol IP, IPX dan *AppleTalk* [2].

H. Border Gateway Protocol

Border Gateway Protocol (BGP) adalah protokol *routing* yang digunakan untuk meng*hub*ungkan antar *autonomous system* (AS). BGP menggunakan algoritma *path-vector* yang memilih rute berdasarkan aturan-aturan tertentu atau biasa disebut *attribute*. BGP terbagi menjadi 2 yaitu BGP internal dan BGP eksternal. BGP internal digunakan untuk menghubungkan jaringan di dalam suatu AS dan eksternal untuk menghubungkan antar AS. BGP memiliki waktu konvergensi yang lambat,memiliki nilai *administrative distance* 20 untuk internal dan 200 untuk eksternal [2].

III. PERANCANGAN

A. Rancangan Topologi



Gambar 1.1 Topologi Jaringan

Skenario dari simulasi ini diasumsikan ada sebuah perusahaan yang memiliki kantor pusat di Jakarta (HUB-JKT).Perusahaan tersebut kemudian membuka cabangnya masing-masing di kota Semarang (SPK-SMG), Bandung (SPK-BDG) yang masing-masing terhubung dengan VPN *site-to-site*.Suatu ketika perusahaan tersebut membuka cabang di Yogyakarta (SPK-JGJ), perusahaan ini memutuskan untuk mengimplementasikan DMVPN dikarenakan kemudahannya apabila ada penambahan cabang suatu saat nanti.

Jaringan DMVPN ini dirancang untuk dapat mentransmisikan semua jenis paket data,terutama yang sifatnya *real-time* seperti *voice* dan *video*.Penulis hanya akan menguji menggunakan *video streaming* karena dianggap dapat mewakili paket data yang lain.

Perancangan jaringan DMVPN dimulai dari pengalamatan IP *address* pada masing-masing perangkat dan mengaktifkan protokol *routing* BGP agar setiap perangkat terhubung satu sama lain,dilanjutkan dengan membentuk *tunnel* pada setiap router.Setelah *tunnel* terbentuk,router kantor pusat akan diaktifkan sebagai NHRP *server* (hub) dan kantor cabang akan menjadi NHRP *client* (spoke),lalu untuk menyediakan keamanan *framework* IP *Security* akan diaktifkan dan untuk proses *forwarding* data pada *tunnel*,di router kantor pusat dan cabang akan diaktifkan protokol *routing* EIGRP.

Penulis menggunakan beberapa *software* dan *hardware* untuk merancang jaringan DMVPN.Tabel 1.1 menunjukkan *software-software* yang penulis gunakan.

Tabel 1.1 *Software* yang digunakan

No	Daftar Software

	Aplikasi	Jenis / Versi
1.	Oracle VM VirtualBox	4.3.8
2.	GNS3	*Version* 1.2.3
3.	*Image* GNS3	*c3745-adventerprisek9-mz.124-15.T14*
4.	*Wireshark*	*Version 2.4.5*
5.	*Windows 7*	*Ultimate*

Untuk menjalankan *software-software* diatas, dibutuhkan spesifikasi laptop seperti dalam tabel berikut :

Tabel 1.2 *Hardware* yang digunakan

NO.	Daftar Spesifikasi Laptop	
	Jenis	**Spesifikasi**
1	*Processor*	*Intel Pentium CPU 2117U @ 1.80 (2 CPUs)*
2	RAM	DDR3L 4GB PC-12800

B.Flowchart

Gambar 1.2 Diagram Proses Simulasi

Langkah-langkah yang dilakukan untuk merancang jaringan DMVPN dalam penelitian ini adalah :

1. Instalasi *software* yang dibutuhkan untuk perancangan jaringan DMVPN.
2. Pembuatan topologi dan IP *address*nya
3. Konfigurasi untuk jaringan DMVPN
4. Pengujian jaringan dan QoS

IV. PENGUJIAN DAN ANALISA

A. Pengujian

Skenario pengujian yang penulis lakukan adalah menguji QoS jaringan dengan menggunakan VPN *site-to-site*, tanpa VPN dan dengan DMVPN. Parameter-parameter yang diuji dalam penelitian ini adalah *throughput*, *delay* dan *packet loss*. Untuk pengujian, penulis menggunakan *bandwidth* sebesar 100 Mbps dan *video streaming* karena dianggap dapat mewakili jenis *file* yang lain.Video yang digunakan untuk melakukan pengujian berukuran 7,58 MB dengan resolusi 640 x 360 dan durasi 2 menit 1 detik.

B. Analisa Throughput

1. Pengujian *throughput* sebanyak 5 kali yang telah dilakukan pada jaringan *site-to-site* VPN dengan hasil 99,72% pada CL-SMG,dan 99,69% pada CL-BDG dan CL-JGJ.Hasil ini termasuk dalam kategori sangat baik menurut standar TIPHON karena nilai *throughput* 76%-100% dari data yang dikirim
2. Pengujian *throughput* sebanyak 5 kali yang telah dilakukan pada jaringan tanpa VPN dengan hasil 99,96% pada CL-SMG dan CL-BDG dan 99,95% pada CL-JGJ.Hasil ini termasuk dalam kategori sangat baik menurut standar TIPHON karena nilai *throughput* 76%-100% dari data yang dikirim.
3. Pengujian *throughput* sebanyak 5 kali yang telah dilakukan pada jaringan DMVPN dengan hasil 99,86% pada CL-SMG, dan 99,89% pada CL-BDG dan CL-JGJ.Hasil ini termasuk dalam kategori sangat baik menurut standar TIPHON karena nilai *throughput* 76%-100% dari data yang dikirim.

C. Analisa Delay

1. Pengujian *delay* yang telah dilakukan pada jaringan *site-to-site* VPN dengan hasil 46,71 ms pada CL-SMG, 38,30 ms pada CL-BDG dan 51,81 ms pada CL-JGJ.Hasil *delay* ini dapat dikategorikan sangat bagus menurut standar TIPHON karena *delay* <150 ms.
2. Pengujian *delay* yang telah dilakukan pada jaringan tanpa VPN dengan hasil 40,00 ms pada CL-SMG, 35,30 ms pada CL-BDG dan 32,00 ms pada CL-JGJ. Hasil *delay* ini dapat dikategorikan sangat bagus menurut standar TIPHON karena *delay* <150 ms.
3. Pengujian *delay* sebanyak 5 kali yang telah dilakukan pada jaringan DMVPN dengan hasil 12,50 ms pada CL-SMG, 51,11 ms pada CL-BDG dan 37,80 ms pada CL-JGJ. Hasil *delay* ini dapat dikategorikan sangat bagus menurut standar TIPHON karena *delay* <150 ms.

D. Analisa Packet Loss

1. Pengujian *packet loss* sebanyak 5 kali yang telah dilakukan pada jaringan *site-to-site* VPN dengan hasil *packet loss* 0%.Hasil ini dikategorikan sangat bagus menurut standar TIPHON.
2. Pengujian *packet loss* sebanyak 5 kali yang telah dilakukan pada jaringan tanpa VPN dengan hasil *packet loss* 0%.Hasil ini dikategorikan sangat bagus menurut standar TIPHON.
3. Pengujian *packet loss* sebanyak 5 kali yang telah dilakukan pada jaringan DMVPN dengan hasil *packet loss* 0%.Hasil ini dikategorikan sangat bagus menurut standar TIPHON.

V. PENUTUP

A. Kesimpulan

1. Perancangan jaringan DMVPN ini dapat dikatakan berhasil, karena setiap perangkat berhasil berkomunikasi dengan baik.
2. Parameter-parameter yang diujikan adalah *throughput*, *delay* dan *packet loss* dengan menggunakan beban *video streaming*. Pengujian menggunakan tiga model jaringan yang berbeda yaitu VPN *site-to-site*,tanpa VPN dan DMVPN.
3. Hasil *throughput* pada keseluruhan model jaringan didapatkan hasil yang relatif sama,sekitar 99% dari data yang dikirimkan. Nilai *throughput* dikategorikan sangat baik menurut standar TIPHON.
4. Hasil *delay* yang didapat dari seluruh pengujian dapat diterima sekitar <150 ms.Nilai *delay* dikategorikan sangat baik sehingga dapat digunakan untuk layanan *video streaming.*
5. Hasil *packet loss* dari pengujian yang telah dilakukan menunjukkan hasil yang sangat bagus menurut standar TIPHON dikarenakan tidak ada *packet loss* selama pengiriman data berlangsung.

B. Saran

Saran yang dapat diberikan untuk penelitian selanjutnya adalah :

1. Menambah jumlah *router* yang digunakan, sebanyak 5-10 *router* sehingga keunggulan dari DMVPN dapat lebih terlihat.
2. Menggunakan perangkat *router* dan PC yang *real* atau dengan menggunakan simulator dengan spesifikasi yang lebih tinggi.
3. Melakukan pengujian QoS dengan beban yang berbeda-beda seperti FTP, *Voice over* IP dan lain-lain serta melakukan pengujian dengan cara *broadcast* dan *multicast*.

DAFTAR PUSTAKA

[1] Angraeni, C. S., Nugroho, H., & Pramesta, E. D. (2017). Implementasi Virtual Private Network Openstack Terkoneksi Dengan Virtual Private Network Mikrotik Untuk Komunikasi Data Lebih Aman. Jurnal ICT Akademi Telkom Jakarta, 8, 42-50.

[2] Balchunas, A.(2012). Cisco CCNP Routing Study Guide v1.22

[3] Dwijaya, M. R. (2018). Simulasi dan Analisis Performansi Load Sharing Menggunakan Protokol Glbp dengan Simulator GNS3 Ver.2. (Proyek Akhir). Program Studi Teknik Telekomunikasi, Akademi Teknik Telekomunikasi Sandhy Putra, Jakarta

[4] Edgeworth, B., Barozet, J.-M., Prall, D., Lockhart, A., & Ben-Dvora, N. (2017). Cisco Intelligent WAN (IWAN). Indianapolis: Cisco Press.

[5] Ghein, L. D. (2007). MPLS Fundamentals. Indianapolis: Cisco Press.

[6] Hucaby, D. (2015). Cisco CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. Indianapolis: Cisco Press.

[7] K.Shandya, & V.Kakulapati. (2018). Established Secured Enterprise Network Routing Protocols by using DMVPN. International Journal of Computer Science & Information Security,16,144-152.

[8] N.Angelescu dkk. (2017). DMVPN simulation in GNS3 network simulation software. ECAI 2017 – International Conference – 9th Edition.

[9] Occhiogrosso, S. J. (2012). Different DMVPN phases. Tersedia di https://ccie-or-null.net/2012/08/22/different-dmvpn-phases/ diakses 29/03/2019

[10] Octavian, R. (2017). Simulasi Perancangan Protocol Jaringan MPLS-L3 VPN Cisco Menggunakan Aplikasi GNS3. (Proyek Akhir). Program Studi Teknik Telekomunikasi, Akademi Teknik Telekomunikasi Sandhy Putra, Jakarta

[11] Pranata, A.Y., Fibriani, I.,& Utomo, S.B. (2016). Analisis Optimasi Kinerja Quality Of Service Pada Layanan Komunikasi Data Menggunakan NS-2 Di PT. PLN (Persero) Jember. Sinergi, 20, 149-156.

[12] Prasetya, A. (2011). Perancangan dan Penerapan Teknologi VPN (Virtual Private Network) Untuk Komunikasi Data (Studi Kasus:Gardanet Corporation). (Skripsi). Program Studi Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Syarif Hidayatullah, Jakarta

[13] Rahman, M. (2011, 11 13). Networking Basic Theory 1. Tersedia di https://belajarcomputernetwork.com/2011/11/13/networking-basic-theory-1/ diakses tanggal 28/03/2019

[14] Rahman, M. (2013). QoS (Quality of Services). Tersedia di https://belajarcomputernetwork.com/2013/04/14/qos-quality-of-service/ diakses tanggal 28/03/2019

[15] Suryani, E., & Honey, S. N. (2007). Implementasi Virtual Private Network - WAN Dalam Dunia Bisnis. 31-38.

[16] Vachon, B. (2016). CCNA Security Portable Command Guide. Indianapolis: Cisco Press.