InComTech: Jurnal Telekomunikasi dan Komputer
vol.10, no.2, Agustus 2020, 49-56
http://publikasi.mercubuana.ac.id/index.php/Incomtech
P-ISSN: 2085-4811 E-ISSN: 2579-6089

Simulasi dan Analisa QoS dalam Jaringan VPN *Site To Site* Berbasis IPSec dengan *Routing Dynamic*

Ahmad Firdausi[1], Hamam Wira Wardani[2*]

[1]*Teknik Elektro, Universitas Mercu Buana,*
Jl. Meruya Selatan, Jakarta 11650, Indonesia
[2*]*PT. Packet System Indonesia, Jakarta,*
Jl. TB Simatupang Kav. 1s, Jakarta 12560, Indonesia
*Email Penulis Koresponden: hamamwardani@gmail.com

***Abstrak*:**
Kebeberadaan jaringan komputer merupakan hal mutlak dalam suatu perusahaan. Anak cabang perusahaan di berbagai daerah seharusnya dapat menjalin komunikasi dan menjaga keamanan data. Salah satu teknologi yang sedang berkembang adalah VPN berbasis IPSec. Sistem yang dibuat mensimulasikan bagaimana VPN tunnel berbasis IPSec dapat terkoneksi. Setelah itu dilakukan penghitungan dan analisa QoS terhadap routing OSPF, RIPv2 dan EIGRP. Simulasi dilakukan di EVE-NG dengan mengibaratkan sebuah perusahaan yang memiliki 1 kantor pusat dan 2 kantor cabang dengan server yang berada di data center. Simulasi dilakukan pada layanan VoIP dengan server asterisk. Dari hasil pengujian fungsional, sistem dapat berfungsi sesuai yang direncanakan. Uji performansi menunjukan packet loss untuk OSPF, RIPv2 dan EIGRP adalah 0.0 %. Dari hasil pengujian yang telah dilakukan semua parameter dalam batas kualitas standar ITU-T.

***Katakunci*:**
IPSec;
QoS;
Routing;
VPN;

Riwayat Artikel:
Diserahkan 11 Juli 2020
Direvisi 4 Agustus 2020
Diterima 9 Agustus 2020
Dipublikasi 25 Agustus 2020

DOI:
10.22441/incomtech.v10i2.8131

1. PENDAHULUAN

Di era digital seperti saat ini penggunaan jaringan komputer adalah sebuah hal mutlak yang harus ada dalam suatu perusahaan baik skala kecil maupun skala besar. Seiring perkembangan teknologi digital yang sudah terasa manfaatnya dalam berbagai sektor, seperti ekonomi dan bisnis. Teknologi digital sangat membantu proses pekerjaan sehari hari, seperti transaksi data antar cabang, sentralisasi data, manajemen data, dan keamanan data. Banyak perusahaan besar yang sudah mempunyai anak cabang diberbagai daerah atau perusahaan perusahaan yang mempunyai banyak rekanan di daerah daerah. Untuk menjalin koneksi dan menjaga keamanan data ketika melakukan suatu pengiriman data yang aman maka dibuatlah sebuah jaringan *Virtual Private Network* (VPN) sebagai solusi dalam pengiriman

serta melindungi data penting perusahaan saat melakukan transmisi data. VPN adalah sebuah metode yang menggunakan *tunneling* untuk membuat jaringan pribadi pada jaringan publik dimana keamanan jaringan tersebut setara dengan keamanan yang di sediakan oleh *leased line.* VPN memiliki dua jenis klasifikasi berdasarkan topologi jaringan yaitu *Remote Access* VPN *dan Site-to-site* VPN [2][3][4].

Routing adalah suatu teknik pemilihan jalur dalam sebuah jaringan. *Routing protocol* merupakan sekumpulan aturan dalam menentukan jalur di sebuah jaringan. Ada banyak jenis dari *routing protocol. Routing* terbagi menjadi dua jenis yaitu *static routing* dan *dynamic routing*. Dalam *static routing* dibutuhkan seorang admin yang akan mengatur dan juga memilih jalur terbaik dalam pertukaran data. Berbeda dengan *static*, *dynamic routing* menggunakan *table routing* yang dapat memudahkan dalam pemilihan jalur. Pada jenis ini, tidak diperlukan seorang admin untuk mengatur jalannya komunikasi [5][6].

Salah satu parameter yang perlu diperhatikan dalam suatu sistem komunikasi adalah *Quality of Service* (QoS). Saat ini QoS merupakan hal yang sangat penting untuk memberikan jaminan kepada pengguna jaringan untuk memperbaiki layanannya [6][7].

Penelitian ini bertujuan untuk mesimulasikan sebuah kantor pusat dapat terhubung dengan kantor cabang dengan memanfaatkan internet dan IPSec. Dalam penelitian ini akan dianalisa juga mengenai QOS dalam routing OSPF dan RIP dan EIGRP untuk layanan VoIP. untuk menghasilkan suatu informasi berupa:

- Waktu yang dibutuhkan oleh sebuah paket data terhitung dari saat pengiriman oleh *transmitter* sampai saat diterima oleh *receiver* (*throughput*).
- Perbedaan selang waktu kedatangan antar paket di terminal tujuan (*delay/latency*).
- Banyaknya paket yang hilang selama proses transmisi ke tujuan (*packet loss*).
- Jumlah bit yang diterima dengan sukses perdetik melalui sebuah sistem atau media komunikasi (kemampuan sebenarnya suatu jaringan dalam melakukan pengiriman data) (*jitter*)

2. METODE

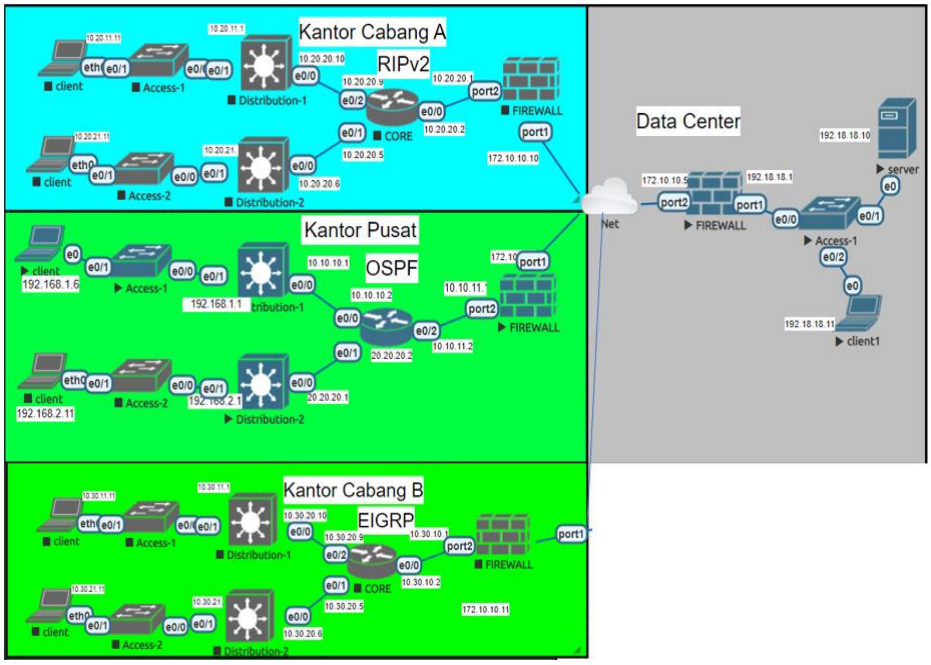
2.1. Topologi Jaringan dan Metode Penelitian

Gambar 1 merupakan model topologi yang akan di konfigurasi pada aplikasi simulator *Eve-NG*. *Eve-NG* adalah *emulator* berbasis web. Pada sisi server *Data Center* (DC) terdiri dari server asterisk yang akan digunakan sebagai server *VoIP*. Pada kantor pusat, kantor dan kantor cabang A, menggunakan *routing* yang berbeda sebagai perbandingan dan analisa. perangkat terdiri terdiri dari firewall, core switch, distribution switch, access switch dan klien linux. Topologi yang digunakan adalah star sehingga semua site dapat saling berkomunikasi satu sama lain dan menggunakan jaringan *broadband* dengan transmisi *fiber optic*.

Pada penelitian ini menggunakan metode *tunnel* VPN untuk menghubungkan jaringan antar site dengan routing protocol OSPF, RIPv2 dan EIGRP. Pada penelitian ini menggunakan metode *tunnel* VPN untuk menghubungkan jaringan antar site dengan *routing* protocol OSPF, RIPv2 dan EIGRP. Terdapat *asterik* sebagai server VoIP, 4 Firewall sebagai pembentuk tunnel VPN dengan IPSec 2 core switch, 4 distribution switch sebagai backbone dan 4 akses switch sebagai

penghubung ke client VoIP. Adapun mekanisme pengiriman packet VoIP dari server ke klien sebagai berikut:

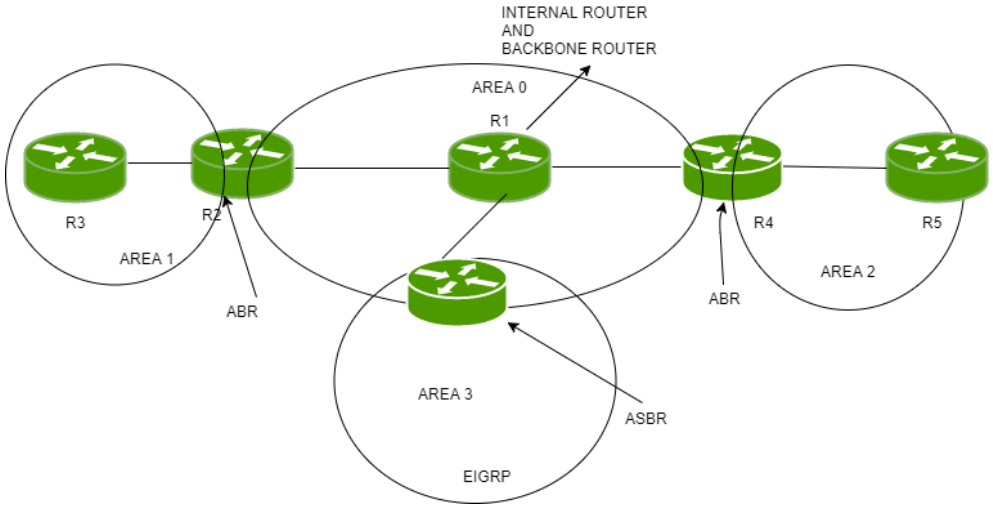
1. *Packet* VoIP akan di kirimkan dari server *asterisk* menuju client *twinkle.*
2. *Firewall data center* akan meneruskan *packet* ke *firewall* dikantor pusat dan cabang melalui *tunnel* VPN yang sudah terkoneksi atau *terestablish* sebelumnya.
3. *Firewall dan core switch* akan menerima paket yang sudah masuk melalui firewall kemudian akan menuruskan ke *distribution switch* dengan *routing OSPF* pada kantor pusat, *routing* RIPv2 pada kantor cabang A dan EIGRP pada kantor cabang B
4. Setelah proses *routing packet* akan langsung diteruskan dengan akses *switch* dengan *layer* 2 tanpa ada *routing* kembali.
5. Di dalam akses *switch* paket akan disampaikan ke *client twinkle.*
6. Untuk mendapatkan hasil yang akurat maka pengujian dilakukan dengan memutar video di sisi *server,* sehingga inputan yang dimasukkan memiliki nilai yang sama.



Gambar 1. Topologi Jaringan

2.2. Konfigurasi OSPF

Open Shortest Path First (OSPF) adalah suatu protocol routing yang handal dengan fasilitas *least-cost routing*, *multipath routing* dan *load balancing*. Penentuan jalur tercepat dan terbaik pada jaringan dihitung dengan metode algoritma *Dijkstra*. Pertama router menggunakan paket "*hello*" untuk mengindentifikasi informasi interface sekitarnya dan membangun *adjacencies* (hubungan untuk pertukaran update routing) dengan yang lain. Selanjutnya router memulai dengan fase ExStart [8]. Konfigurasi dengan *routing OSPF* akan digunakan pada *Firewall*, *core switch* dan *distribution switch* di kantor Pusat. Koneksi ke arah *server* akan menggunakan *VPN tunnel* dengan *IPSec* 172.10.10.1. sedangkan IP yang digunakan pada klien adalah *segment* 192.168.1.0/24 dan 192.168.2.0/24. Contoh sebuah OPSF diperlihatkan pada Gambar 2.



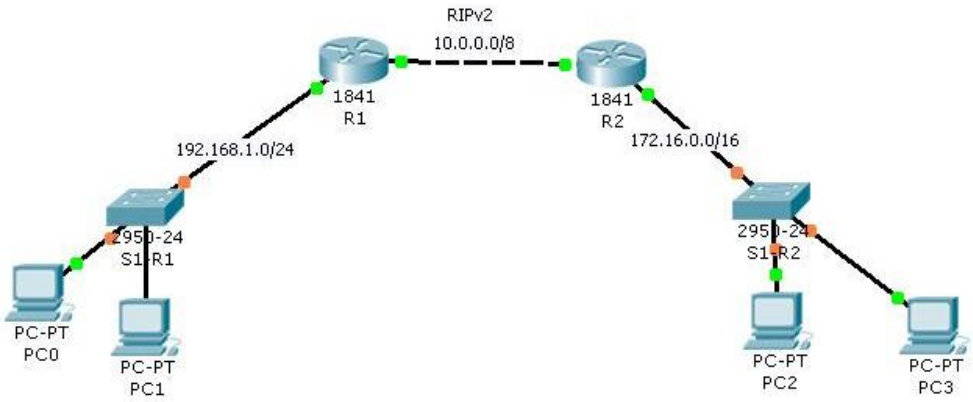
Gambar 2. *Open Shortest Path First* (OSPF)

2.3. Konfigurasi VPN IPSec

Internet Protocol Security (IPsec) adalah protokol untuk mengamankan Internet Protocol (IP) komunikasi dengan otentikasi dan mengenkripsi setiap paket IP dari suatu sesi komunikasi. IPsec juga mencakup protokol untuk mendirikan otentikasi bersama antara agen pada awal sesi dan negosiasi kunci kriptografi yang akan digunakan selama sesi [9]. *IPSec* VPN akan dikonfigurasi pada *firewall fortigate* di semua *site*. Tujuannya agar dari kantor pusat, kantor cabang A dan kantor cabang B dapat terhubung ke *Server* atau *data center*.

2.4. Konfigurasi RIPv2

Routing Information Protokol (RIP) adalah standard dasar dari *protocol routing distance vector, Interior gateway*. RIP menggunakan hop *count* untuk menentukan jalur terbaik diantara dua lokasi. Setiap paket melewati router maka dihitung satu hop [10]. konfigurasi dengan *routing* RIPv2 akan digunakan pada *Firewall, core switch dan distribution switch* di kantor Cabang A. Koneksi ke arah server akan menggunakan VPN *tunnel* dengan IPSec 172.10.10.10. sedangkan IP yang digunakan pada client adalah segment 10.20.10.0/24 dan 10.20.11.0/24. Gambar 3 memperlihatkan sebuah konfigurasi RIPv2.

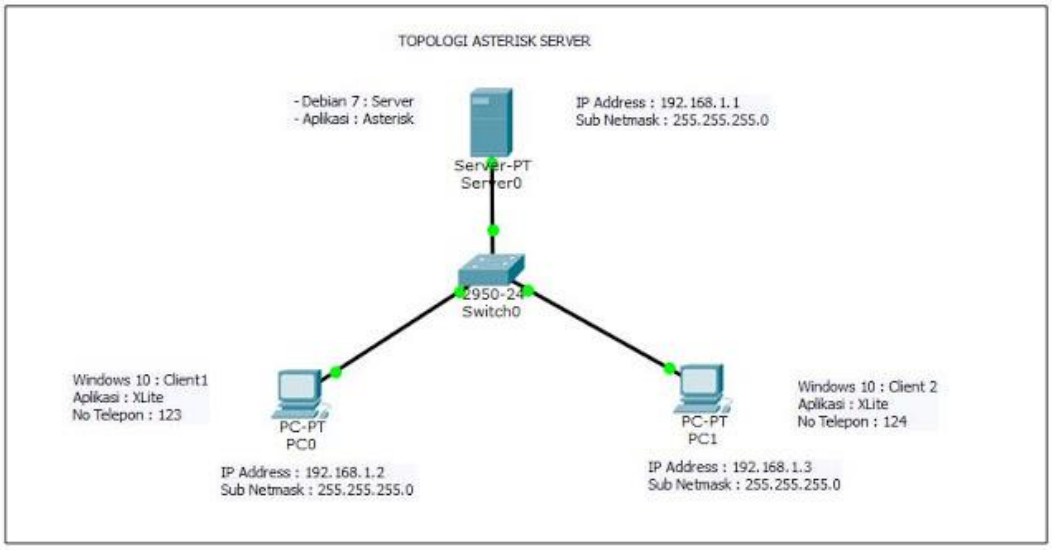


Gambar 3. Konfigurasi RIPv2

EIGRP ini hanya bisa digunakan sesama router cisco saja. EIGRP akan mengirimkan hello packet utk mengetahui apakah router-router tetangganya masih hidup ataukah mati [11]. Konfigurasi dengan *routing* EIGRP akan digunakan pada, *core switch* dan *distribution switch* di kantor Cabang B. Pada *firewall* akan dikonfigurasi static route ke arah core. Karena pada EIGRP hanya bisa dikonfigurasi pada perangkat Cisco, koneksi ke arah server akan menggunakan VPN *tunnel* dengan IPSec 172.10.10.11. Sedangkan IP yang digunakan pada *client* adalah segment 10.30.10.0/24 dan 10.30.11.0/24.

2.6. Konfigurasi *Asterisk* dan *Twinkle*

Asterisk digunakan untuk membangun suatu sistem layanan komunikasi serta memberikan kemudahan kepada penggunanya untuk mengembangkan suatu sistem layanan komunikasi serta telepon sendiri dengan kustomisasi yang seluas-luasnya diberikan kepada pihak pengguna [12]. Asterisk akan digunakan sebagai *server* VoIP untuk pengujian terhadap QoS pada *routing* OSPF, RIPv2 dan EIGRP yang sudah dilakukan. Sedangkan twinkle akan digunakan untuk klien VoIP. Sehingga antara klien dapat melakukan panggilan. konfigurasi *server Asterisk* pada linux di data center menggunkan ip 192.18.18.10 kemudian klien di kantor pusat dengan nomor 7001, klien 7002 di klien data center dan klien di kantor cabang A dengan nomor 7003. *Twinkle* merupakan aplikasi yang digunakan disisi klien untuk dapat melakukan panggilan ke nomor yang dituju.



Gambar 4. Konfigurasi Asterisk

2.7. Metode Simulasi

Pada simulasi penelitian ini menggunakan metode *tunnel* VPN untuk menghubungkan jaringan antar site dengan *routing protocol* OSPF, RIPv2 dan EIGRP. Terdapat *asterik* sebagai server VoIP. Packet VoIP akan di kirimkan dari server *asterisk* menuju client *twinkle. Firewall data center* akan meneruskan *packet* ke firewall dikantor pusat dan cabang melalui *tunnel* VPN yang sudah terkoneksi atau *terestablish* sebelumnya. *firewall dan core switch* akan menerima paket yang sudah masuk melalui firewall kemudian akan menuruskan ke distribution switch dengan *routing* OSPF pada kantor pusat, routing RIPv2 pada kantor cabang A dan EIGRP pada kantor cabang B di dalam akses switch paket akan disampaikan ke

client twinkle. Untuk mendapatkan hasil yang akurat maka pengujian dilakukan dengan memutar video dan suara, sehingga inputan yang dimasukkan memiliki nilai yang sama. Saat semua konfigurasi sudah berjalan maka dilakukan pengambilan data dengan melakukan panggilan dari *client* ke server dan memutar sebuah video dan suara. Semua paket yang keluar masuk disisi *client* di-*capture* menggunakan *Network Analyzer* yaitu Wireshark [13]. Pengukuran dilakukan dengan durasi 5 menit panggilan. Kemudian dapat melihat hasilnya di *statistic* dan summary pada Wireshark.

3. HASIL DAN PEMBAHASAN

Dari hasil pengujian yang sudah dilakukan, semua konfigurasi semua perangkat sudah terkoneksi dan dapat saling berkomunikasi. Setelah tahap pengujian konfigurasi selesai maka selanjutnya adalah melakukan pengukuran QoS. Pengukuran pada layanan VoIP digunakan untuk menilai kehandalan dari layanan Voip pada jaringan VPN *Tunnel*. pengukuran dilakukan dengan melakukan interkoneksi antara server *asterisk di Data Center* dengan *routing* yang berbeda pada masing-masing kantor. Setelah berhasil melakukan panggilan dan selama panggilan berlangsung semua komunikasi di *capture* menggunakan *network analyzer* yaitu Wireshark. Pengukuran dilakukan dengan durasi 5 menit panggilan dari klien di masing-masing kantor dengan data center. Tabel 1 menunjukkan hasil dari pengukuran yang telah dilakukan.

Tabel 1. Hasil pengukuran QoS

Bandwidth	***Throughput*** **(Kbps)**	***Packet loss*** **(%)**	***Delay*** **(ms)**	**Keterangan**
64	383	0	7,28	OSPF (Kantor Pusat)
128	632	0	2,4	
256	714	0	1,1	
64	119	0	10,34	RIPv2 (Kantor Cabang A)
128	397	0	4,88	
256	166	0	3,86	
64	380	0	8,08	EIGRP (kantor cabang B)
128	538	0	3,38	
256	397	0	2,32	

Pengukuran pada masing-masing *routing* sudah sesuai dengan standar ITU-T, yaitu paket loss kurang dari 1%. Berikut ini merupakan standar QoS untuk parameter paket loss pada layanan VoIP menurut *International Telecommunication Union Telecommunication Standardization Sector* (ITU-T) [14].

Tabel 2. Standar *packet loss*

No	***Packet Loss*** **(%)**	**Kualitas**
1.	0 %	Baik
2.	1 – 5 %	Dapat diterima
3.	> 10 %	Tidak dapat diterima

Pada pengukuran parameter delay hasil pengukuran sudah sesuai dengan standar ITU-T yaitu delay kurang dari 50 ms. Tabel 3 memperlihatkan tabel standar delay yang ditetapkan oleh ITU-T [15].

Tabel 3. Standar *packet loss*

Kategori *Delay*	Besar *Delay*
0 %	Baik
1 – 5 %	Dapat diterima
> 10 %	Tidak dapat diterima

Dari Tabel 3 terlihat bahwa *bandwidth* berpengaruh terhadap QoS, pada pengujian dengan routing OSPF, RIPv2 maupun EIGRP terlihat bahwa semakin besar *bandwidth* yang diberikan maka akan semakin baik kualitas dari sebuah jaringan tersebut, ini dapat dilihat pada *delay* yang semakin kecil dan *troughput* yang semakin besar pada *bandwidth* yang lebih besar. Pada pengujian yang sudah dilakukan terlihat bahwa routing dengan kualitas yang paling baik adalah dengan *routing* OSPF.

4. KESIMPULAN

Dari simulasi dan analisa QoS dalam jaringan *Virtual Private Network* (VPN) *Site toSite* berbasis IPSec dengan Routing *Dynamic* dapat disimpulkan sebagai berikut. Pertama, sistem dapat terealisasi dan berfungsi sesuai yang direncanakan dari gambaran topologi diatas sudah mempresentasikan keadaan yang real saat kantor-kantor meimplementasikan sebuah jaringan perusahaan. Kemudian, hasil pengukuran *throughput* pada *bandwidth* 64 kbps, 128 kbps dan 256 Kbps yang didapat pada klien kantor pusat dengan *routing* OSPF adalah sebesar 382 kbps, 632 kbps, 714 kbps, hasil yang didapat untuk klien kantor cabang A dengan *routing RIPv2* adalah 119 kbps, 397 kbps, 166 kbps dan di kantor cabang B dengan *routing EIGRP* adalah 380 kbps, 538 kbps, 397 kbps. Sedangkan hasil pengukuran *Delay* pada *bandwidth* 64 kbps, 128 kbps dan 256 Kbps yang didapat pada klien kantor pusat dengan *routing* OSPF adalah sebesar 7.28 ms, 2.4 ms, 1.1 ms, hasil yang didapat untuk klien kantor cabang A dengan *routing* RIPv2 adalah 10.34 ms, 4.88 ms, 3.86 ms dan di kantor cabang B dengan *routing* EIGRP adalah 8.08 ms, 3.38 ms, 2.32 ms. Hasil uji performansi menunjukan *packet loss* untuk OSPF, RIPv2 dan EIGRP adalah 0.0 %. Ketiga parameter kinerja tersebut berada dalam batas-batas kualitas standar ITU-T.

REFERENSI

[1] Y. Zhu, V. L. Wang, Y. J. Wang and J. Nastos, "Business-to-business referral as digital cooperation strategy. Insight from industry-wise digital business network', *European Journal of Marketing,* vol. 54, no. 6, pp. pp. 1181-1203, 2019. DOI: 10.1108/EJM-2019-0011

[2] F. Hauser, M. Häberle and M. Menth, "P4-IPsec: Site-to-Site and Host-to-Site VPN with IPsec in P4-Based SDN," *IEEE Access,* vol. 8, pp. 139567-139576, 2020. DOI: 10.1109/ACCESS.2020.3012738

[3] M. Juma, A. A. Monem and K. Shaalan, "Hybrid End-to-End VPN Security Approach for Smart IoT Objects'", *Journal of Network and Computer Applications,* vol. 158, May 2020. DOI: 10.1016/j.jnca.2020.102598

[4] A. Munggaran, R. Munadi and D. Perdana, "Analisis Dan Simulasi Perbandingan QoS Di Routing Protokol Mpls OSPF dan MPLS IS-IS Di Jaringan Ipv6 Menggunakan Gns3 Untuk Layanan Video Streaming", *e-Proceeding of Engineering,* vol. 5, no. 3, pp. 4374-4384, Desember 2018

[5] S. Chairunnisa, R. Munadi and D. D. Sanjoyo, "Analisis Performansi Quality of Service Inter

As MPLS-VPN Backto-Back VRF Pada Layanan IMS", *e-Proceeding of Engineering*, vol. 5, no. 3, pp. 4650-4567, Desember 2018

[6] N. Djedjig, D. Tandjaoui, F. Medjek and I. Romdhani, "Trust-aware and cooperative routing protocol for IoT Security," *Journal of Information Security and Applications,* vol. 52, June 2020. DOI: 10.1016/j.jisa.2020.102467

[7] E. Ramadhan, A. Firdausi and S. Budiyanto, "Design and analysis QoS VoIP using routing Border Gateway Protocol (BGP)", *2017 International Conference on Broadband Communication, Wireless Sensors and Powering (BCWSP),* Jakarta, Indonesia, 2017, pp. 1-4. DOI: 10.1109/BCWSP.2017.8272556

[8] S. H. Ghafouri, S. M. Hashemi and P. C. K. Hung, "A Survey on Web Service QoS Prediction Methods," *IEEE Transcations on Service Computing*, 2020. DOI: 1109/TSC.2020.2980793

[9] A. Roussinos, *Performance Comparison of OSPF and IS-IS Routing Protocols in Dual-Stack Enterprise Networks,* Edinburgh Napier University. 40134490, July 2014

[10] F. M. Ridwan, D. Perdana and L. V. Yovita, "*Analisa dan Simulasi IPSec Vpn Tunnel* sebagai Alternatif Keamanan Konektivitas Antar *Network*", *Skripsi,* OpenLibrary Telkom University, 18.04.552, 2018

[11] D. W. P. Pratama and I. Nurhaida, "Perbandingan Kinerja Routing IGP Pada Jaringan VPN Berbasis MPLS Dan Direct-Link Backup", *Skripsi,* Repository Mercu Buana, 29 September 2018.

[12] H. A. Musril, "Analisis Unjuk Kerja RIPv2 dan EIGRP Dalam Dynamic Routing Protocol", *JETT: Jurnal Elektro dan Telekomunikasi Terapan*, vol. 2, no 2, pp. 116-124, Desember 2015

[13] R. G. Nindya, D. Wisaksono and E. M. Jadied, "Pembangunan Softphone untuk Penanganan Serangan Denial of Service pada Cloud VoIP Gateway yang Secara Otomatis Berpindah", *Skripsi,* Repository Telkom University, 2019

[14] F. S. YEG, D. W. Sudiharto and S. Setyorini "Analisis peformansi QoS pada EasyRTC menggunakan Algoritma Distribution Hash Table," *e-Proceeding of Engineering*, vol. 5, no. 3, pp. 7457-7463, Desember 2018.

[15] ITU-T Publications, "*G.1010: End-user multimedia QoS categories*", 2011 11 29. [Online]. Available: https://www.itu.int/rec/T-REC-G.1010-200111-I/en [Accessed: 02-Nov-2019]