

SIMULASI DAN ANALISIS PENGGUNAAN JARINGAN VIRTUAL PRIVATE NETWORK (VPN) BERBASIS MIKROTIK OS

SIMULATION AND ANALYSIS OF VIRTUAL PRIVATE NETWORK (VPN) USING MIKROTIK OS

Wiwaha, Ilman Ramdan Raksa ¹

Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Ilmanramdanrwa@telkomuniversity.ac.id

Abstrak - Jaringan komputer tentu mengandung sebuah informasi dan data yang sangatlah penting, informasi harus dapat di akses melalui jaringan komputer yang dapat menjamin keamanan, kecepatan, kemudahan, dan akurat. Terdapat tiga aspek utama ketika berbicara tentang keamanan data : 1. Privacy atau Confidentiality, 2. Message Integrity, 3. Authentication, Dengan masalah ini dibutuhkan suatu sistem yang dapat menjaga keamanan dari data-data agar informasi dapat tersebar dengan aman. VPN (*Virtual Private Network*) merupakan teknologi komunikasi yang memungkinkan terkoneksi ke jaringan publik dan bergabung dengan jaringan lokal, VPN menyediakan keamanan jaringan pada komunikasi antara *server* dengan *client* dan juga sebaliknya.

Penelitian ini bertujuan membuat simulasi dan analisa terhadap VPN (*Virtual Private Network*) PPTP (*Point-to-Point Tunneling Protocol*) yang berbasis Mikrotik OS menggunakan aplikasi GNS3 dengan mengasumsikan sebuah server dan empat client yang bekerja pada kanal. Tujuan utama penelitian ini adalah membuat desain dan implementasi sistem VPN dengan membandingkan Normal dan PPTP VPN, serta menguji QoS dari sistem VPN yang dibuat dengan membandingkan sistem Normal dan PPTP VPN. Kanal yang disimulasikan akan diuji kualitas dan performansi dengan menggunakan QoS yang ditinjau dengan aplikasi Wireshark untuk melihat paket yang melewati kanal dan di analisa hasil dari protokol PPTP yang ada pada kanal, pengujian kualitas diuji menggunakan standar TIPHON.

Simpulan penelitian, pembuatan desain dan simulasi dari kanal VPN yang dibuat dapat berjalan dengan normal dengan kualitas secara keseluruhan berstandar 2.6875 Dengan pengujian QoS standar TIPHON, fungsi sistem yang dibuat dapat berjalan dengan baik dengan menampilkan QoS (*Quality of Service*) dengan nilai rata-rata throughput pada pengiriman dari client menuju server adalah 50.81434 bytes/s yang menunjukkan indeks bagus, Delay rata-rata yang terjadi pada pengiriman dari client menuju kepada server adalah 28011.6625 ms yang menunjukkan indeks jelek, dengan rata-rata jitter 0.019410733 ms yang menunjukkan indeks Bagus, dan rata-rata packet loss pada saat pengiriman paket berlangsung adalah 0% yang menunjukkan indeks bagus. Perbandingan kanal VPN dan kanal normal hasilnya cukup memuaskan, Hasil dari kanal yang dibuat dapat digunakan dengan semestinya dan diharapkan dapat diaplikasikan di kemudian hari.

Kata kunci : *Virtual Private Network, Virtual Private Network Server, Point-to-point Tunneling Protocol, Kanal Komunikasi, Quality of Service.*

Abstract - Computer network is certainly included an important information and data, information must be accessible through a computer network that can guarantee security, speed, convenience, and accuracy. There are three main aspects when talking about data security: 1. Privacy or Confidentiality, 2. Message Integrity, 3. Authentication, With this problem we need a system that can maintain the security of data so that information can be spread safely. VPN (*Virtual Private Network*) is a communication technology that allows user connected to public networks and joining local networks, VPN provides network security on communication between server and client or client to server.

This study aims to make a simulation and analysis of PPTP (*Point-to-Point Tunneling Protocol*) VPN-based Virtual Private Network based on the OS OS using GNS3 application by assuming a server and four clients working on the channel. The main objective of this study is to design and implement a VPN system by comparing Normal and PPTP VPN, and testing the QOS of a VPN system created by comparing the Normal and PPTP VPN systems. The simulated channel will be tested for quality and performance by using QoS which is reviewed with the Wireshark

application to see packets that pass through the channel and analyzed the results of the PPTP protocol on the channel, quality testing is tested using the

Conclusions of research, design and simulation of VPN channels that are made can run normally with overall quality standard 2.6875 With TIPHON standard QoS testing, system functions are made to run well by displaying QoS (Quality of Service) with an average value of throughput the delivery from the client to the server is 50.81434 bytes / s which shows a good index, the average delay that occurs in sending from the client to the server is 28011.6625 ms which shows a bad index, with an average jitter 0.019410733 ms which shows a good index, and the average packet loss at the time of packet delivery is 0%, which indicates a good index. Comparison of VPN channels and normal channels results are quite satisfactory, The results of the channels created can be used properly and are expected to be implemented later on.

Keywords: *Virtual Private Network, Virtual Private Network Server, Point-to-point Tunneling Protocol, communication Tunnel, Quality of Service.*

I. PENDAHULUAN

Dalam sebuah institusi sebuah informasi yang sangatlah penting, informasi ini sangat berguna karena dapat mengandung hal-hal yang dapat bersifat sensitive dan sangat penting. Informasi pada institusi harus dapat di akses melalui jaringan komputer yang dapat menjamin keamanan, kecepatan, kemudahan, dan akurat. Jaringan komputer yang ada pada institusi harus terjamin keamanan dan juga kredibilitasnya, agar data yang ada pada institusi tidak tersebar ke khalayak luas. Adapun beberapa aspek utama ketika berbicara tentang keamanan data yaitu *Privacy* atau *Confidentiality*, mencakup kerahasiaan informasi. Inti aspek *privacy* adalah bagaimana menjaga informasi agar tidak dilihat atau diakses oleh orang yang tidak berhak, Lalu, *Message Integrity*, atau integritas mencakup keutuhan informasi. Inti aspek *integrity* adalah bagaimana menjaga informasi agar tetap utuh atau dapat dikatakan apa yang diterima harus sama dengan apa yang dikirim, dan *Authentication*, atau otentikasi berkaitan dengan keabsahan pemilik informasi. Harus ada cara untuk mengetahui informasi benar-benar asli, kemudian hanya yang berhak saja yang boleh memberikan informasi dapat dikatakan komunikasi harus dengan rekan yang tepat [1]. Untuk memenuhi aspek-aspek tersebut diperlukan sebuah sistem yang bisa mengakomodasi kebutuhan keamanan jaringan.

Dengan masalah ini dibutuhkan suatu sistem yang dapat menjaga keamanan dari data-data agar informasi dapat tersebar dengan aman. dengan mempertimbangkan kerahasiaan data, salah satu solusi yang dapat digunakan adalah dengan penggunaan VPN (Virtual Private Network), VPN akan membuat jaringan yang digunakan di institusi bersifat privasi tetapi bisa digunakan pada jaringan publik atau internet. VPN adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal [2]. Dengan mengaplikasikan VPN pada jaringan yang ada institusi tidak perlu mengkhawatir pengiriman data melalui publik atau internet karena akan aman meski di tempat umum sekalipun. VPN adalah sebuah cara aman untuk mengakses *local area network* yang berada pada jangkauan, dengan menggunakan internet atau jaringan umum lainnya untuk melakukan transmisi data paket secara pribadi, dengan enkripsi perlu penerapan teknologi tertentu sehingga walaupun menggunakan medium yang umum, tetapi traffic (lalu lintas) antar remote-site tidak dapat disadap dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan traffic yang tidak semestinya ke dalam remote-site [3].

II. DASAR TEORI

2.1 Virtual Private Network (VPN)

VPN adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal[2]. Teknologi ini akan menjadi dasar dari pembuatan Tugas Akhir, karena pada jaringan konvensional tidak serta merta memberikan keamanan seperti yang dilakukan oleh VPN. VPN bisa juga didefinisikan sebagai sebuah terowongan Virtual (Virtual Tunnel) dari jaringan ke jaringan lain yang terenkripsi. VPN *server* dan VPN *Client* harus saling ter-autentikasi. VPN mengkoneksikan dua jaringan seperti Remote User tunggal ke kantor[5].

2.2 Point-to-Point Tunneling Protocol (PPTP)

PPTP adalah salah satu teknik *tunneling* dengan akses jarak jauh. Protokol ini memungkinkan perluasan jaringan dengan menggunakan metode *tunneling* pribadi. PPTP merupakan protokol *tunneling* pada layer dua yang memperluas standar Point to Point Protocol (PPP) untuk jaringan dial-up. Pertama-tama PPTP merangkum paket-paket di dalam paket-paket PPP, kemudian dienkapsulasi dengan Generic Routing Encapsulation (GRE) dan terakhir dibungkus dengan header IP. Teknik *tunneling* ini bekerja dalam arsitektur *client-server*. PPTP memastikan autentikasi dan enkripsi[4].

2.3 Quality of Service (QoS)

Quality of Service (QoS) merupakan suatu terminologi yang digunakan guna mengetahui seberapa baik kualitas dari layanan yang digunakan dengan mendefinisikan karakteristik suatu layanan (service) jaringan. Dalam penelitian ini parameter QoS yang akan dianalisa adalah *delay*, *jitter*, *packet loss*[6].

1. Throughput

Throughput yaitu kecepatan (rate) transfer data efektif, yang diukur dalam bps (bit per second). *Throughput* adalah jumlah total kedatangan paket yang sukses yang diamati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut.[7]

Persamaan Throughput :

$$\text{Throughput} = \frac{\text{Paket Data Terima}}{\text{Lama Pengamatan}} \quad (1)$$

Tabel 1

Standar *Throughput*

Kategori <i>Throughput</i>	<i>Throughput</i> (bps)	Indeks
Sangat Bagus	75 s/d 100	4
Bagus	50 s/d 75	3
Sedang	25 s/d 50	2
Jelek	<25	1

(Sumber : TIPHON) [7]

2. Delay

Delay merupakan waktu tunda dalam suatu pemrosesan data, dimana untuk kualitas *delay* dikatakan baik apabila waktu tundanya hanya sekitar 0 – 150 ms[6].

1. Propagation *delay* (terjadi akibat transmisi melalui jarak antara pengirim dan penerima).
2. Serialization *delay* (terjadi pada saat proses peletan bit kedalam circuit).
3. Processiong *delay* (terjadi pada saat proses coding, compression, decompression serta decoding).
4. Packetization *delay* (terjadi pada saat proses paketisasi digital voice sample)
5. Queuing *delay* (terjadi akibat waktu tunggu paket sampai dilayani)
6. *Jitter Buffer delay* (delay akibat adanya buffer untuk mengatasi *jitter*)

Persamaan *Delay* :

$$\text{Delay} = \frac{\text{Panjang Paket}}{\text{Link Bandwith}} \quad (2)$$

Tabel 2

Standar *Delay*

Kategori Latensi	<i>Delay</i> (ms)	Indeks
Sangat Bagus	<150	4
Bagus	150 s/d 300	3
Sedang	300 s/d 450	2
Jelek	>450	1

(Sumber : TIPHON) [7]

3. Jitter

Jitter adalah perbedaan selang waktu kedatangan antar paket di terminal tujuan, atau dengan kata lain *jitter* merupakan variasi dari *delay*. Besarnya nilai *jitter* mengakibatkan rusaknya data yang diterima, baik itu berupa penerimaan yang terputus-putus atau hilangnya data akibat overlap dengan paket data yang lain. Banyak hal yang dapat menyebabkan *jitter*, diantaranya adalah peningkatan traffic secara tiba-tiba sehingga menyebabkan penyempitan bandwidth dan menimbulkan antrian. Untuk kualitas *Jitter* dikatakan baik apabila waktunya hanya sekitar 0 – 20 ms[6].

Persamaan *Jitter* :

$$Jitter = \frac{\text{Total Variasi Delay}}{\text{Total Paket yang diterima}} \quad (3)$$

Tabel 3
Standar *Jitter*

Kategori <i>Jiter</i>	<i>Jiter</i> (bps)	Indeks
Sangat Bagus	0	4
Bagus	0 s/d 75	3
Sedang	75 s/d 125	2
Jelek	125 s/d 225	1

(Sumber : TIPHON) [7]

4. Packet loss

Packet loss yaitu jumlah paket yang hilang dalam suatu pengiriman paket data pada suatu jaringan. Beberapa penyebab terjadinya *packet loss* adalah adanya noise, collision dan congestion yang disebabkan oleh terjadinya antrian yang berlebihan dalam jaringan. *Packet loss* pada VoIP dikatakan baik apabila jumlah tingkatan paket yang hilang berkisar antara 0 s/d 0.5 % dari pengiriman data[6].

Persamaan *Packet loss* :

$$Packet\ loss = \frac{(\text{Paket data dikirim} - \text{Paket data diterima}) \times 100 \%}{\text{Paket data yang dikirim}} \quad (4)$$

Tabel 4
Standar *Packet loss*

Kategori <i>Packet loss</i>	<i>Packet loss</i> (bps)	Indeks
Sangat Bagus	0	4
Bagus	3	3
Sedang	15	2
Jelek	25	1

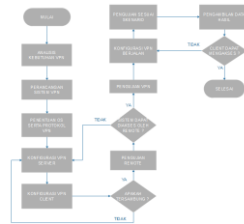
(Sumber : TIPHON) [7]

III. PERANCANGAN VPN

3.1. Diagram Alur

Dari diagram alur proses dimulainya tugas akhir ini akan diawali dengan analisis kebutuhan apa saja yang akan digunakan pada tugas akhir ini lalu dilanjutkan dengan perancangan sistem yang akan digunakan pada tugas akhir ini dengan itu penyusun dapat menentukan OS dan Protokol yang akan digunakan pada sistem VPN ini setelah menentukan kita harus mengkonfigurasi VPN *server* yang selanjutnya mengkonfigurasi VPN *Client* lalu di cek apakah uji koneksi *server* dengan *client* berhasil jika tidak, ulangi di langkah konfigurasi VPN *server* jika berhasil dilanjutkan ke tahap pengujian remote *server*, Jika remote tidak dapat digunakan maka harus di konfigurasi kembali pada VPN *server*, dan jika remote dapat digunakan maka dilanjutkan dengan pengujian VPN pada *server* dan juga dilanjutkan pada *client* jika sudah berjalan dengan baik maka uji sistem bisa langsung dilakukan sesuai dengan skenario yang sudah dibuat lalu data bisa diambil setelah itu dipastikan

bahwa bisa diakses oleh pekerja, jika tidak berkerja maka harus dipastikan kembali bahwa VPN *server* berjalan dengan baik.



Gambar 1 Diagram alur dari simulasi

3.2 Pembuatan Kanal VPN PPTP

Pada pembuatan kanal VPN PPTP ini prosesnya mendekati normal hanya saja kita membuat kanal terlebih dahulu melalui aplikasi winbox. Koneksikan winbox kepada GNS3. Koneksikan winbox terhadap IP address yang digunakan untuk menyambungkan router internet dan router yang ada di kantor-kantor, untuk mensetting masuk ke menu PPP lalu pilih interface dan buat PPTP *server* untuk membuat kanal PPTP *server*, lalu, langkah selanjutnya adalah masuk menu secret untuk membuat id PPP *server* dan masukan data untuk keamanan kanal. Masukan IP yang akan digunakan sebagai kanal PPTP, lalu masuk ke menu dial-out untuk mengonfirmasi data yang digunakan dalam kanal, dengan langkah yang sama buat data di PC *Server* untuk konfirmasi kanal yang dibuat, langkah selanjutnya yang harus dilakukan adalah konfigurasi routing *active static* dari PPTP dengan IP address seperti pada tabel 5 Untuk konfigurasi ini masuk pada menu IP lalu pilih menu routes lalu tambahkan *active static* route .hal ini dilakukan agar PC *client* dapat terhubung ke PC *server*.

Tabel 5 Konfigurasi Routing *active static* pada kanal pptp

Router	Konfigurasi
Router 1	Dest. Address 192.168.5.0/24 dan Gateway 172.16.1.5
Router 2	Dest. Address 192.168.5.0/24 dan Gateway 172.16.1.5
Router 3	Dest. Address 192.168.5.0/24 dan Gateway 172.16.1.5
Router 4	Dest. Address 192.168.5.0/24 dan Gateway 172.16.1.5
Router 5	Dest. Address 192.168.1.0/24 dan Gateway 172.16.1.1 Dest. Address 192.168.2.0/24 dan Gateway 172.16.1.2 Dest. Address 192.168.3.0/24 dan Gateway 172.16.1.3 Dest. Address 192.168.4.0/24 dan Gateway 172.16.1.4

Maka hasil dari konfigurasi ini dapat dilihat pada menu IP lalu address, akan terlihat bahwa konfigurasi telah diterapkan pada *topology*. Kanal telah berhasil dibuat dan sudah bisa digunakan pada GNS3, langkah selanjutnya adalah mencoba untuk ping dari PC cabang ke PC pusat. Jika ping berhasil dilakukan maka tunnel yang dibuat berhasil, jika gagal maka ulang kembali langkah-langkah yang ada.

3.3 Pengujian QoS

Pengujian dari *QoS* bertujuan untuk mengukur transfer data efektif dari kanal VPN yang dibuat (*Throughput*), mengetahui waktu yang dibutuhkan data untuk menempuh jarak dari asal sampai ke tujuan (*Delay*), mengetahui variasi dari *delay* dalam pengiriman paket (*Jitter*), untuk total paket yang hilang pada saat paket dikirimkan dari asal ke tujuan (*Packet Loss*). Hasil pengujian dari *QoS* pada *topology* yang digunakan dapat menjadi tolak ukur dari kualitas kanal *topology* yang telah dibuat menggunakan aplikasi GNS3.

1. Throughput

Cara mendapatkan nilai *throughput* pada wireshark dilakukan dengan cara menuliskan terlebih dahulu protocol yang akan di nilai lalu masuk kedalam menu *statistics* dan tekan capture data. Maka akan muncul data dari kanal yang diuji seperti jumlah bytes, jumlah paket, jumlah waktu, dan *throughput*. Data *throughput* didapatkan dengan cara membagi total bytes dengan jumlah waktu maka akan didapatkan hasil *throughput* dalam satuan bytes / second.

2. Delay

Cara mendapatkan nilai *delay* pada wireshark dilakukan dengan cara menuliskan terlebih dahulu protocol yang akan di nilai lalu masuk kedalam menu *Export packet dissections* dan simpan data dalam bentuk file .csv. Pengujian dilakukan dengan cara mengurangi waktu tempuh pertama dengan waktu tempuh selanjutnya sehingga mendapatkan nilai selisih dari waktu yang ditempuh oleh packet. Lalu cari dengan total selisih waktu dibagi dengan jumlah paket. Pengujian dilakukan dengan manual pada Microsoft excel. Pengujian yang dilakukan berlaku pada setiap pengujian.

3. Jitter

Cara mendapatkan nilai *jitter* pada wireshark dilakukan dengan cara menuliskan terlebih dahulu protocol yang akan di nilai lalu masuk kedalam menu *Export packet dissections* dan simpan data dalam bentuk file .csv. Pengujian dilakukan dengan cara mengurangi *delay* pertama dengan *delay* selanjutnya sehingga mendapatkan nilai selisih dari waktu yang ditempuh oleh packet. Lalu cari dengan total selisih *delay* dibagi dengan jumlah paket. Pengujian dilakukan dengan manual pada Microsoft excel. Pengujian berlaku pada setiap pengujian data wireshark. Tabel 10 Hasil

4. Packet Loss

Cara mendapatkan nilai *packet loss* dapat dilihat pada *vpcs* yang digunakan pada saat mengirimkan ping dari PC cabang ke PC pusat.

3.4 Analisis

Hasil keseluruhan dari kanal komunikasi yang dibuat pada kantor cabang menuju ke kantor pusat dapat terbilang cukup baik, karena pada tabel 4.9 dapat dilihat total kualitas yang didapatkan oleh kanal komunikasi kantor cabang menuju kantor pusat memiliki angka yang bervariasi dan tidak ada yang mempunyai nilai kurang dari 2.5 dimana hasil tersebut menunjukkan hasil “Sedang-Bagus” pada standar TIPHON. Data ini juga menunjukkan bahwa pada pengujian ini kanal komunikasi VPN PPTP dapat digunakan dan diaplikasikan pada kantor PT. Karsa Abdi Husada untuk kedepannya.

1. Throughput

Pada pengujian ini hasil dari *throughput* menunjukkan hasil sedang dan bagus hal ini menunjukkan bahwa kanal komunikasi yang dibuat memiliki tipe data yang ditransfer kurang baik, topology jaringan yang kurang baik maupun spesifikasi PC dari client maupun server. Rata-rata hasil dari kanal komunikasi normal adalah 32.86662 dengan indeks “sedang” sedangkan rata-rata hasil dari kanal komunikasi VPN PPTP adalah 50.81434, hasil tersebut memiliki indeks “bagus”. Meskipun begitu hasil dari perhitungan dapat dikatakan baik secara keseluruhan sesuai dengan gambar 4.4.

2. Delay

Pada pengujian *delay* hasil yang ditunjukkan oleh pengujian menunjukkan hasil yang jelek ataupun buruk seperti pada gambar 4.6, Rata-rata hasil dari kanal komunikasi normal adalah 4444.02575 dengan indeks “Jelek” sedangkan rata-rata hasil dari kanal komunikasi VPN PPTP adalah 28011.6625, hasil tersebut memiliki indeks “Jelek”. kualitas ini memperlihatkan bahwa kualitas kanal komunikasi yang dibuat memiliki jarak yang jauh

ataupun konfigurasi dari router yang dibuat memiliki konfigurasi yang kurang baik, ataupun tipe data yang di analisa kurang baik.

3. Jitter

Pada pengujian jitter menunjukkan bahwa hasil dari pengujian memperlihatkan hasil yang bagus dan sangat bagus seperti pada gambar 4.8 yang berarti pada pengujian jitter pada kanal komunikasi ini memiliki jitter yang bagus dan layak. Rata-rata hasil dari kanal komunikasi normal adalah 0.02295 dengan indeks “Bagus” sedangkan rata-rata hasil dari kanal komunikasi VPN PPTP adalah 0.01941, hasil tersebut memiliki indeks “bagus”. Yang artinya kanal komunikasi ini tidak ada antrian yang banyak dan juga tidak ada peningkatan trafik yang banyak dan mengganggu

4. Packet Loss

Pada pengujian packet loss menunjukkan bahwa hasil dari pengujian memperlihatkan hasil yang sangat bagus seperti pada gambar 4.10 yang berarti pada pengujian packet loss pada kanal komunikasi ini memiliki jitter yang bagus dan layak. Rata-rata hasil dari kanal komunikasi normal adalah 0% dengan indeks “Sangat Bagus” sedangkan rata-rata hasil dari kanal komunikasi VPN PPTP adalah 0% dengan indeks “Sangat Bagus”. Yang berarti tidak ada paket yang hilang pada transmisi paket, baik hilang karena collision ataupun congestion.

5. Analisis kanal keseluruhan

Dari hasil pengujian didapatkan data seperti pada tabel 14 dan gambar 7, yang menunjukkan hasil dari kanal komunikasi normal dan kanal komunikasi VPN PPTP yang ada pada topology memiliki nilai “Sedang-Bagus” yang berarti kanal yang dibuat dapat digunakan untuk komunikasi FTP pada kantor cabang menuju kantor pusat untuk topologi yang dibuat, dan diharapkan akan bisa diaplikasikan kepada PT.Karsa Abdi Husada.

Hasil dari tabel 14 dapat dirata-ratakan menjadi 2.685 yang memiliki indeks diantara sedang dan bagus. Hasil ini berlaku sama pada kanal komunikasi normal maupun kanal komunikasi VPN PPTP yang telah dibuat.

Tabel 14 Hasil Pengujian Total kanal kantor cabang

No	Lokasi	Total Nilai Kanal	
		Normal	PPTP
1	Kantor Cab. Bandung	2.75	2.5
2	Kantor Cab. Tasikmalaya	2.75	2.75
3	Kantor Cab. Ciamis	2.5	2.75
4	Kantor Cab. Subang	2.75	2.75



Gambar 7 Perbandingan Total

Dari hasil analisis kanal yang dibuat didapatkan hasil yang cukup dari kedua kanal yang disimulasikan, dan kanal VPN yang dibuat dapat berjalan dengan cukup baik serta lancar. Dimana hasil dari kanal yang dibuat dari beberapa kantor cabang bisa digunakan meskipun masih belum mendekati kata sangat baik tetapi kanal yang dibuat masih layak untuk digunakan.

IV. KESIMPULAN

Berdasarkan pada hasil analisis dari pengujian kanal yang dibuat dapat diambil beberapa kesimpulan :

1. Berdasarkan hasil simulasi, maka dapat disimpulkan bahwa pembuatan desain dan simulasi dari kanal VPN yang dibuat dapat berjalan dengan normal dengan kualitas secara keseluruhan berstandar 2.6875 Dengan pengujian QoS standar TIPHON.
2. Menurut hasil Analisa performansi dari kanal VPN yang telah dibuat, menghasilkan performansi dari kanal VPN dengan rata-rata kualitas *throughput* 50.81434 bytes/s, *Delay* 28011.6625 ms , *jitter* 0.019410733 ms , dan *packet loss* 0%. Pengujian dilakukan dalam rentang waktu sekitar 7-8 menit pada kanal normal maupun kanal VPN.
3. Berdasarkan hasil perbandingan kanal VPN dan juga kanal Normal, dihasilkan hasil yang Cukup memuaskan pada kedua kanal yang dibuat. Kedua kanal dibandingkan melalui standar TIPHON dan menghasilkan hasil yang cukup memuaskan.
4. Hasil dari kanal yang dibuat dapat digunakan dengan semestinya dan diharapkan dapat diaplikasikan di kemudian hari.

Daftar Pustaka:

- [1] H. Pranata, L. Abdillah, U. E. preprint arXiv:1508.05457, and undefined 2015, "Analisis Keamanan Protokol Secure Socket Layer (SSL) Terhadap Proses Sniffing di Jaringan," *arxiv.org*.
- [2] E. B. S. IRAWAN AFRIANTO, "KAJIAN VIRTUAL PRIVATE NETWORK (VPN) SEBAGAI SISTEM PENGAMANAN (Studi Kasus Jaringan Komputer Unikom)," *Maj. Ilm. UNIKOM*, vol. 12, no. 1, pp. 43-52, 2014.
- [3] Y. Yuniati, ... H. F.-J. S. dan, and undefined 2014, "Analisa Perancangan Server VoIP (Voice Internet Protocol) dengan Opensource Asterisk dan VPN (Virtual Private Network) Sebagai Pengaman Jaringan Antar Client," *ejournal.uin-suska.ac.id*.
- [4] S. Jahan, M. Rahman, S. S.-2017 I. Conference, and undefined 2017, "Application specific tunneling protocol selection for Virtual Private Networks," *ieeexplore.ieee.org*.
- [5] K. A. Farly, X. B. N. Najoran, and A. S. M. Lumenta, "Perancangan dan Implementasi VPN Server dengan menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Studi Kasus Kampus Universitas Sam Ratulangi," *J. Jarkom*, vol. Vol 11, No, no. 1, 2017.
- [6] E. S.-K. J. I. K. dan and undefined 2012, "Analisa Quality Of Services (Qos) Voice Over Internet Protocol (Voip) Dengan Protokol H. 323 Dan Session Initial Protocol (Sip)," *search.unikom.ac.id*.
- [7] R. Wulandari, "ANALISIS QoS (QUALITY OF SERVICE) PADA JARINGAN INTERNET (STUDI KASUS : UPT LOKA UJI TEKNIK PENAMBANGAN JAMPANG KULON-LIPI)," 2016.