Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.1, Februari 2022

ANALISA *VIRTUAL PRIVATE NETWORK* (VPN) *IP MULTI PROTOCOL LABEL SWITCHING* (MPLS) UNTUK JARINGAN WIDE AREA NETWORK (WAN)

Sari Dewi [1], Sulistiyah[2]
Sistem Informasi PSDKU Kota Pontianak
Fakultas Teknik dan Informatika
Universitas Bina Sarana Informatika
Sari.sre@bsi.ac.id , Sulistiyah.slt@bsi.ac.id

Received: November 22, 2022**. Revised:** December 15, 2021**. Accepted:** December 21, 2021**. Issue Period:** Vol.6 No.1 (2022), Page 16-25

Abstrak: Teknologi jaringan saat ini berkembang pesat salah satunya teknologi VPN hal ini sangat berguna pada pertukaran data yang terjadi agar dapat berjalan dengan aman dan lancar, dengan harapan jaringan tersebut dapat meningkatkan kinerja dan performa perusahaan dalam mendukung proses bisnis yang dijalankan dimana harus tetap terhubung walaupun dengan jarak yang jauh antar pulau dan antar provinsi di seluruh indonesia. MPLS VPN menawarkan berbagai kehandalan dan kecepatan pengiriman paket data, hal ini lah yang mendorong banyak perusahaan yang memiliki kantor cabang untuk menggunakan teknologi tersebut, Jaringan MPLS akan mengirimkan paket sesuai dengan label yang ada pada header paket ke tujuan yang diinginkan dan VPN akan membatasi siapa pengguna yang berhak mengakses jaringan menggunakan konfigurasi VRF. Hasil yang dapat dicapai ialah rancangan simulasi jaringan berbasis VPN IP MPLS yang dapat meningkatkan dan menjamin faktor keamanan antara kantor pusat dengan kantor-kantor cabangnya. Tentunya keamanan dalam jaringan tersebut sangat dibutuhkan, karena data yang mengalir dalam jaringan merupakan data yang sangat penting. dengan menggunakan jaringan VPN IP MPLS maka kinerja perusahan dan pertukaran data antara kantor pusat dan kantor-kantor cabang lebih aman, lancar, dan terjamin

Kata Kunci: **Jaringan, VPN, IP MPLS.**

Abstract: *Network technology is currently developing rapidly, one of which is VPN technology, it is very useful in data exchanges that occur so that they can run safely and smoothly, with the hope that the network can improve the performance and performance of the company in supporting business processes that are run which must remain connected even at a distance. which is far between islands and between provinces throughout Indonesia. MPLS VPN offers a variety of reliability and speed of sending data packets, this is what encourages many companies that have branch offices to use this technology, the MPLS network will send packets according to the label on the packet header to the desired destination and VPN will limit who the user is who has the right to access the network using the VRF configuration. The result that can be achieved is the design of a VPN IP MPLS-based network simulation that can improve and guarantee the security factor between the head office and its branch offices. Of course, security in the network is needed, because the data flowing in the network is very important data. By using the MPLS IP VPN network, the company's performance and data exchange between the head office and branch offices are safer, smoother, and more secure*

DOI: 10.52362/jisamar.v6i1.662
Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.1, Februari 2022

Keyword: Network, VPN, IP MPLS

I. PENDAHULUAN

Pekembangan teknologi informasi dan komunikasi berkembang sangat cepat terbukti sebagai sumber informasi yang sangat diandalkan. Hal ini dikarenakan semua bidang kegiatan memanfaatkan ilmu pengetahuan pada teknologi. Semua pihak menuntut semua sistem informasi yang cepat, tepat, dan akurat. Kini hampir disetiap instansi baik swasta maupun instasi pendidikan membutuhkan adanya komputer, salah satu kegunaan dari komputer didalam dunia kerja adalah untuk pendataan, pengolahan, serta pembuatan laporan data secara cepat dan akurat, yang hasilnya berupa informasi, apalagi ditambah dengan situasi global saat ini diera new normal covid 19 yang terjadi hampil 2 tahun lamanya.

Salah satu teknologi jaringan yang dapat mendukung hal ini adalah teknolagi *Virtual Private Network* (VPN), yang dapat mengemulasikan dua jaringan yang lokasinya berjauhan untuk saling berkomunikasi seakan-akan kedua jaringan tersebut di dalam suatu area yang sama, Jaringan VPN merupakan jaringan komunikasi private yang menggunakan jaringan publik untuk membentuk jaringan Wide Area Network. VPN umumnya didasarkan pada jaringan IP yang prinsip dasarnya menggunakan teknologi tunnel (Euginia & Ghozali, 2018). Encapsulating data dengan protokol tunnel, dan membangun tunnel berdasarkan jaringan public seperti internet untuk menghubungkan titik ke titik. Teknologi VPN yang terus menerus berkembang memberikan keuntungan ISP dan pelanggan (Mardiyanto, 2019) sedangkan MPLS merupakan solusi untuk berbagai permasalahan pada jaringan komputer saat ini yaitu kecepatan, skalabilitas, *qualiy of service* (QoS) management dan *trafic engineering*." dengan berbagai kelebihan yang dimilikinya, MPLS menjadi andalan baru bagi perusahan yang sangat membutuhkan layanan komunikasi data yang aman, cepat, handal dan murah. Multi Protocol Label Switching merupakan salah satu bentuk konvergensi vertikal dengan topologi jaringan, Multi protocol label switching menjanjikan banyak harapan untuk peningkatan performasi jaringan paket tanpa harus menjadi rumit, Multi protocol label switching adalah teknologi penyampaian paket pada jaringan backbone berkecepatan tinggi (Arnita & Farid, 2020) sebuah jaringan telekomunikasi terdapat mekanisme MPLS yang mana mekanisme tersebut digunakan untuk mengaktifkan rangkian data switching yang dibangun berbasis paket IP (Rahmawati, Ikhwan, & Hadi, 2018) Untuk itu sebuah perusahan dapat menerapkan VPN berbasis MPLS dalam menyangkup operasionalnya.

II. METODE DAN MATERI

Desain sistem untuk mengetahui masalah yang dihadapi perusahaan dapat dilihat dari pemilihan alternatif system jaringan yang terbaik. Kegiatan yang dilakukan dalam tahap desain antara lain, mengambar skema jaringan, topologi jaringan yang di gunakan ,koneksi VPN, Tipe VPN untuk menghubungkan kantor pusat dan cabang-cabang menggunakan model *Site-to-Site VPN*(Wahyudi & Purnama, 2019), dalam hal ini untuk Membangun rancangan VPN IP MPLS yang telah telah dibuat dengan menggunakan simulasi Opnet dan Packet Tracer.

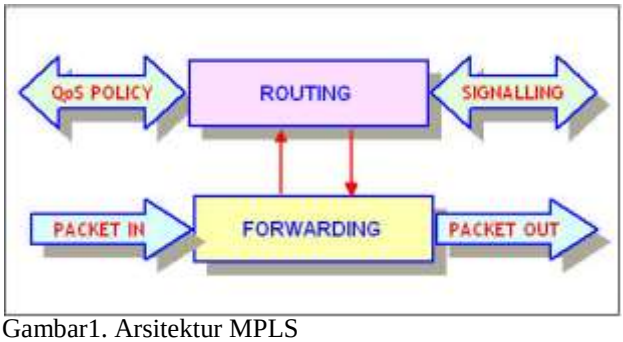
Jaringan *sharing* MPLS memadukan kemampuan *label swapping* dengan *layer network routing* untuk membentuk private network yang aman dan cepat dalam pengiriman paket informasi. Dengan arsitektur jaringan tersebut menjadikan biaya jaringan lebih kompetitif sebagai alternatif solusi jaringan komunikasi WAN *private*. Teknologi *Multiprotocol Label Switching* (MPLS) (Setiawan et al., 2016).

DOI: 10.52362/jisamar.v6i1.662
Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.1, Februari 2022

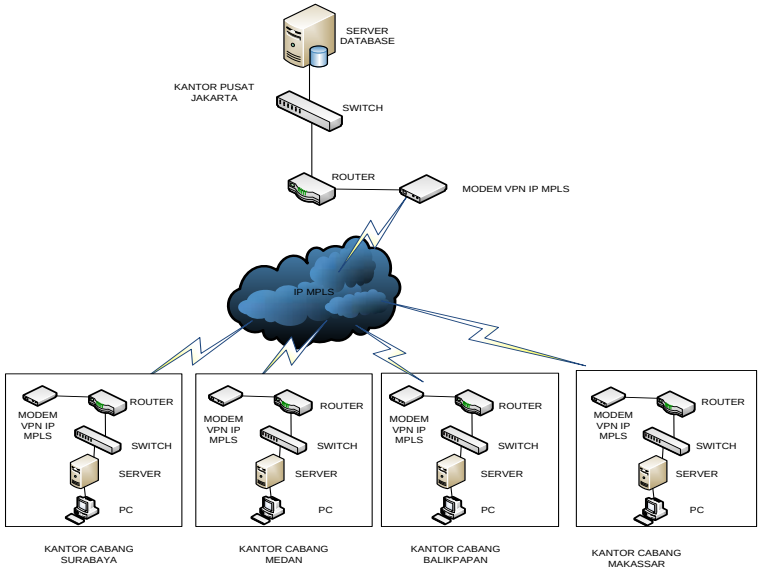
Dengan MPLS maka dapat diperoleh keuntungan diantaranya:

1. Mengurangi banyaknya proses pengolahan di IP *routers*, serta memperbaiki proses pengiriman suatu paket data.
2. Menyediakan *Quality of Service* (QoS) dalam jaringan *backbone*, sehingga setiap layanan paket yang dikirimkan akan mendapat perlakuan sesuai dengan skala prioritas (Septarindra, Munadi, & Negara, 2016).



Gambar1. Arsitektur MPLS

Pada management jaringan yang digunakan mengunakan topology star karena seluruh PC disana terkoneksi pada switch dan hub, protocol jaringan yang digunakan adalah TCP/IP, seluruh NIC yang di gunakan mendukung kecepatan 10/100 Mbps. Pada kantor cabang topologi yang di pakai juga menggunakan topologi star hal ini karna lebih memudahkan pada saat proses instalasi perangkat yang di butuhkan pada jaringan tersebut, Sistem keamanan yang diterapkan baik pada kantor pusat maupun kantor cabang, bertumpu pada PC *Router* yang dilengkapi dengan *firewall*. Sedangkan pada sisi *client* terpasang *software antivirus* dan *internet security*



Gambar 2. Topologi Jaringan Pusat dan Cabang

DOI: 10.52362/jisamar.v6i1.662
Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.1, Februari 2022

Untuk membantu kinerja jaringan sebuah perusahaan, untuk mendukung berjalannya proses bisnis pada dibutuhkan jaringan yang mampu menghubungkan antara kantor pusat dan

kantor-kantor cabang yang letaknya berjauhan, sehingga proses bisnis dan pertukaran data antara kantor pusat dan kantor cabang menjadi lebih efisien. Data yang ada pada Database Server akan selalu up-to-date dibandingkan dengan proses yang sebelumnya dimana update dilakukan pada sore hari, setelah kantor tutup. Dan tentu saja keamanan dalam jaringan tersebut sangat dibutuhkan, karena data yang mengalir dalam jaringan merupakan data yang penting. Teknologi jaringan yang dapat mendukung hal ini adalah teknologi Virtual Private Network (VPN) (Sari & Kemala, 2020). Dengan VPN jaringan pada kantor cabang dan jaringan kantor pusat dapat dihubungkan menjadi satu jaringan internal yang besar dengan memanfaatkan jaringan publik sebagai media penghubungnya. VPN menyediakan fasilitas keamanan pertukaran data melalui jaringan publik yang tidak aman. Semua data yang dipertukarkan atau yang melalui VPN akan dilewatkan ke dalam tunnel, dimana proses ini disebut tunneling. Dengan demikian data perusahaan yang penting dapat dengan aman dipertukarkan, pada permasalahan ini penulis menggunakan VPN-IP MPLS. Karena VPN-IP MPLS mempunyai keuntungan-keuntungan, yaitu :

a. *Multiservices Offering*

VPN-MPLS menawarkan berbagai macam aplikasi bisnis antara lain berupa voice, data, dan video (Suryanto & Dewi, 2013).

b. *Provisioning Scalability*

VPN-MPLS bersifat fleksibel sehingga apabila ingin merubah jaringan tidak perlu merubah jaringan yang sudah ada. Pengembangan jaringan VPN-MPLS dapat dilakukan secara bertahap, mudah dan cepat. Rekonfigurasi dapat dilakukan dengan cepat tanpa diperlukan konfigurasi any to any. Sehingga penambahan jaringan perusahaan dapat dilakukan secara mudah (Suryanto & Dewi, 2013).

c. *Cost Saving Opportunity*

Penggunaaan VPN-MPLS dapat mereduksi biaya operasional bila dibandingkan dengan penggunaan leased line sebagai cara tradisional untuk mengimplementasikan WAN.

d. *Security*

Dengan menggunakan VPN-MPLS akses data kedua data center berjalan aman karena lalu lintas data dapat dipisahkan dengan VPN-MPLS tersebut.

III. PEMBAHASA DAN HASIL

Teknologi VPN yang akan digunakan untuk menghubungkan jaringan kantor pusat dan kantor cabang pada Perusahaan yaitu VPN IP MPLS. VPN yang dibangun dengan MPLS sangat berbeda dengan VPN yang hanya dibangun berdasarkan teknologi IP, yang memanfaatkan enkripsi data. VPN pada MPLS lebih mirip dengan *virtual circuit* dari *frame relay* atau ATM (Fathurrahmad, Yusuf, 2019) , yang dibangun dengan membentuk isolasi trafik. Trafik benar-benar dipisah dan tidak dapat dibocorkan ke luar lingkup VPN yang didefinisikan. VPN IP MPLS ini memiliki kelebihan dibandingkan dengan VPN berbasis *frame relay* atau ATM . VPN IP digunakan untuk merealisasikan CoS dimana pelanggan dapat mengimplementasikan aplikasinya baik berupa aplikasi yang *delay sensitive*, *mission critical* maupun *non mission critical* pada satu platform jaringan privat IP MPLS (Suryanto & Dewi, 2013). VPN IP MPLS juga memiliki keunggulan-

DOI: 10.52362/jisamar.v6i1.662
Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.1, Februari 2022

keunggulan lainnya, seperti yang telah dipaparkan pada sub Layanan VPN IP MPLS yang digunakan adalah fasilitas dari PT. Telkom, yaitu TelkomLink VPN IP MPLS. PT. Telkom mampu menyediakan layanan VPN IP MPLS dalam skala yang besar dan mampu menjangkau ke sebagian besar wilayah di Indonesia. PT. Telkom juga memberikan kemudahan dalam hal konfigurasi dan dalam penyediaan perangkat (modem dan router). Bandwidth yang digunakan untuk kantor pusat adalah 300 Mbps, sedangkan untuk tiap-tiap kantor cabang cukup 100 Mbps saja.

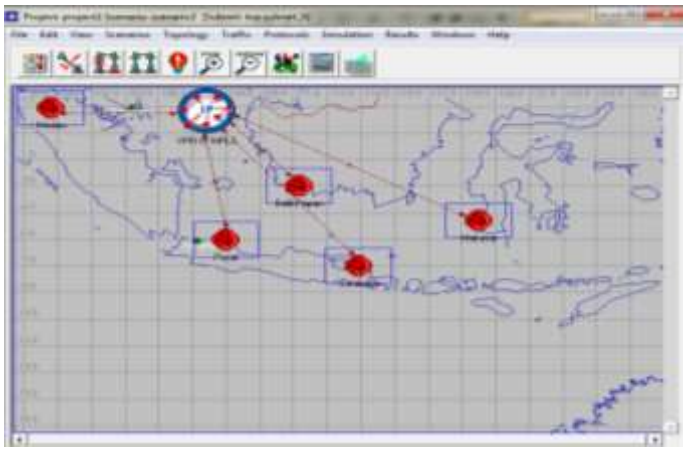
A. Menyusun Model-Model Jaringan

Pada langkah ini disusun model-model jaringan yang sesuai dengan rancangan VPN yang telah dibuat. OPNET menyediakan objek-objek atau node-node beserta media penghubungnya dari berbagai macam jenis, tipe, dan merek yang ada.

Pertama-tama menyusun gambaran besar dari rancangan jaringan VPN terlebih dulu, yang terdiri dari :

1. 5 subnet yang mewakili : Kantor Pusat, Kantor Cabang Jakarta,Kantor Cabang Makasar, Kantor Cabang Makasar Kantor Cabang Surabaya.
2. 1 buah cloud yang mewakili jaringan IP MPLS PT.TELKOM.
3. 1 buah database server yang berada di jaringan Kantor Pusat.
4. Link yang menghubungkan Kantor_Pusat_JKT dengan cloud (datarate : 1M bps)
5. Link yang menghubungkan Kantor-kantor Cabang dengan cloud (datarate : 128Kbps)

Setelah itu menyusun model-model jaringan untuk masing- masing subnet yang ada. Untuk subnet Kantor Pusat Jakarta penyusunannya dapat dilihat digambar berikut mengunakan simulator opnet.

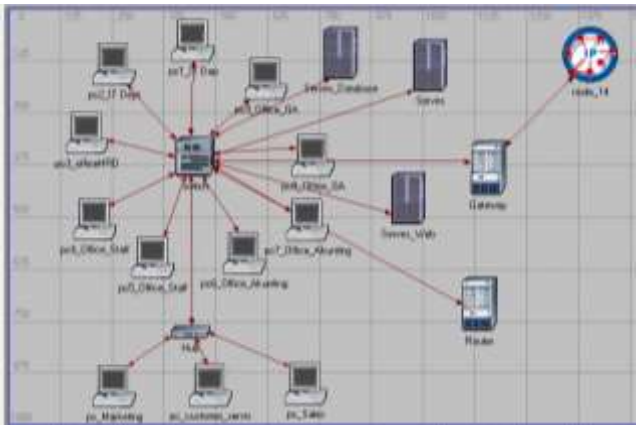


Gambar 3. Rancangan Koneksi VPN IP MPLS.

Setelah itu kita rancang jaringan untuk kantor pusat dengan simulator OPNET

DOI: 10.52362/jisamar.v6i1.662
Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.1, Februari 2022

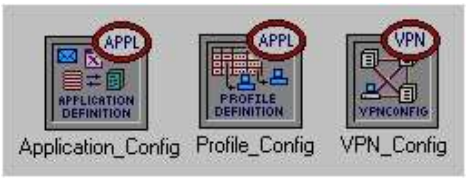


Gambar 4. Skema Jaringan Pusat.

B. Mengkonfigurasi Node-Node Jaringan

Pada langkah konfigurasi ini, pertama-tama diperlukan 3 node konfigurasi baru. Node-node ini tidak terhubung dengan node-node lain yang ada. Node-node ini hanya digunakan untuk melakukan konfigurasi saja. Node-node tersebut adalah :

1. Application Definition
2. Profile Definition
3. VPN Config



Gambar 5. Skema Jaringan Pusat.

C. Konfigurasi Aplikasi-Aplikasi yang Digunakan

1. Konfigunasi Aplication Config

Untuk mengkonfigurasi aplikasi-aplikasi apa saja yang akan digunakan dalam simulasi klik kanan pada node ”*ApplicationDefinition”* kemudian pilih ”Edit Attributes”. Lalu akan keluar kotak dialog ”Attributes”, klik pada baris ”*Application Definitions*” kolom ”Value” kemudian pilih ”edit”,lalu akan muncul kotak dialog ”Application Definitions Table”.

2. Konfigurasi Profile.

Klik kanan pada node “Profile Definition” kemudian pilih “Edit Attributes”. Lalu akan keluar kotak dialog ”Attributes”, klik pada baris ”Profile Configuration” kolom ”Value” kemudian pilih ”edit”, lalu akan muncul kotak dialog ”Profile Configuration Table”.

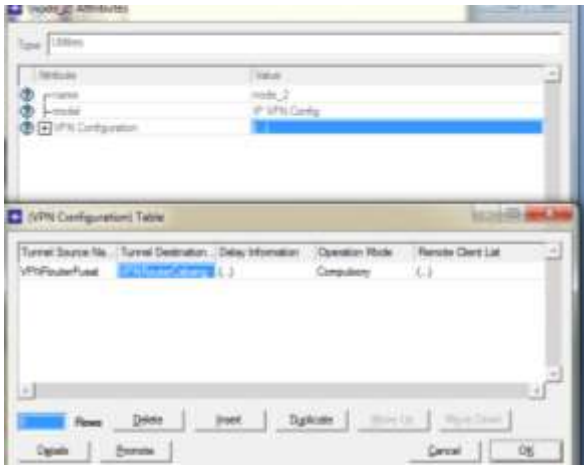
DOI: 10.52362/jisamar.v6i1.662
Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.1, Februari 2022

Konfigurasi berikutnya adalah mengaktifkan layanan aplikasi Database pada node Database_Server. Klik kanan pada node ”Database Server” kemudian pilih ”Edit Attributes”, edit ”Application: Supported Services” dan pilih aplikasi ”Database”. Node node yang memiliki profile database access adalah node bagian marketing, bagian costing, bagian finance dan accounting ,dan bagian material. Klik kanan pada salah satu node di atas, kemudian pilih ”Edit Attributes”, edit ”Application: Supported Profiles” dan pilih profile ”Database Access”. Lakukan yang sama untuk tiap node di atas.

3. Konfigurasi VPN

Konfigurasi ini bertujuan untuk mengkonfigurasi tunnel.M enentukan tunnel source dan tunnel destination, serta menentukan mode tunnel yang digunakan.Untuk mengkonfigurasi VPN pada node ”VPN_Config” kemudian pilih ”Edit Attributes”. Lalu akan keluar kotak dialog ”Attributes”, klik pada baris ”VPN Configuration” kolom ”Value” kemudian pilih ”edit”, lalu akan muncul kotak dialog ”VPN Configuration Table”. Lalu isi tabel konfigurasi VPN seperti pada gambar dibawah ini.



Gambar 6. Konfigurasi VPN pada OPNET.

Set ”Tunnel Source Name” menjadi VPNRouterPusat yang ada pada dan set ”Tunnel Destination Name” menjadi VPNRouterCabang. Edit ”Remote Client List” dan set ”Client Node Name” ke MainSwitch yang ada pada subnet kantor cabang.

4. Memilih Statistik

Statistik yang akan diambil dari simulasi ini meliputi IP VPN Tunnel delay,response time DB query ,. Untuk memilih statistik diatas klik kanan pada lembar kerja OPNET, pilih individual statistic. Untuk ”IP VPN Tunnel Delay” terdapat pada”Node Statistics>IP VPN Tunnel>Tunnel Delay (secs)” Untuk Response time DB Query terdapat pada “Global Statistic>DB Query>response time(secs)”. Simulasi akan dijalan kan 1 jam, artinya durasi simulasi seolah olah berjalan selama 1 jam.

5. Konfigurasi Cloud IP MPLS

Nilai packet latency/delay pada cloud IP MPLS diatur, yaitu dari 0,125 – 0,150 detik. Nilai ini berdasarkan Service Level Guarantee (SLG) dari PT.TELKOM .Untuk mengeset nilai packet latency/delay pada cloud IP

DOI: 10.52362/jisamar.v6i1.662
Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional

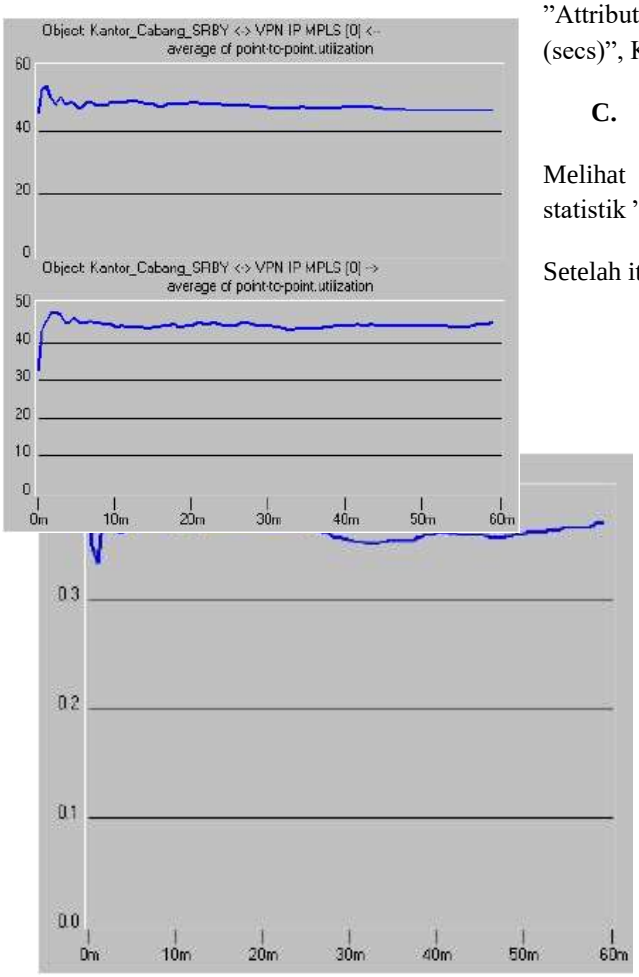
Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.1, Februari 2022

MPLS, klik kanan pada node ”VPN IP MPLS”pilih ”Edit Attributes”. Lalu akan keluar kotak dialog ”Attributes”, klik kolom ”Value” pada baris”Packet Latency (secs)”, Kemudian isi spesifikasinya.

C. Pengujian Jaringan Akhir

Melihat dan Menganalisa Hasil Simulasi Berikut ini adalah statistik ”IP VPN Tunnel Delay” yang didapat dari simulasi.

Setelah itu pengujan untuk kantor pusat dengan VPN IP MPLS



Gambar 7. Tunel Delay Kantor Pusat dengan VPN

Setelah itu pengujan untuk kantor pusat dengan VPN IP MPLS

DOI: 10.52362/jisamar.v6i1.662
Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 6 No.1, Februari 2022

Gambar 8. Tunel Delay Kantor cabang dengan VPN IP MPLS

Evaluasi Hasil

Incoming utilization/ outcoming utilization =

$$\frac{\text{Data Throughput terukur}}{\text{Kapasitas Bandwidth yang tersedia}} * 100\%$$

Berdasarkan hasil simulasi menggunakan software OPNET di atas, didapatkan bahwa besarnya delay pada masing-masing tunnel berkisar dari 0,38 detik sampai 0.39 detik, dimana delay sebesar ini masih dapat diterima dalam melakukan pertukaran data. Utilisasi penggunaan bandwidth pada kantor pusat sekitar 30% dari 300 Mbps bandwidth yang digunakan, sedangkan pada kantor- kantor cabang berkisar antara 50 % sampai 52 % dari 100 Mbps bandwidth yang digunakan. Utilisasi penggunaan bandwidth pada kantor pusat yang berkisar antara 30% cukup bagus, karena masih ada sisa bandwidth yang dapat digunakan apabila terdapat kantor-kantor cabang yang baru. Sedangkan utilisasi penggunaan bandwidth pada kantor cabang sekitar 52% sudah cukup efektif, karena masih ada sisa bandwidth sekitar 55%, maka utilisasi kegunaan bandwidthnya bisa mencapai lebih dari 90%.

IV. KESIMPULAN

Proses pengiriman data dari cabang ke pusat yang sebelumnya digunakan secara keamanan belum maksimal di karnakan tidak ada nya metode enscaptulation data sehingga untuk adanya kemungkinan serangan dari malware, adware atau bahkan creaker.untuk itu sebaiknya menggunakan Virtual Private Network (VPN) agar keamanannya lebih baik dari sebelumnya, serta memiliki kelebihan seperti fasilitas koneksi jarak jauh (access remote). Penggunaan VPN akan menjadi sangat populer saat ini karena VPN memberikan jaminan keamanan dan reliabilitas yang hampir sama dengan jaringan pribadi. VPN sangat mudah digunakan, dengan menginstalasikan VPN client pada komputer atau laptop pemakai, maka pemakai dapat akses ke Lokal Area Network dengan fasilitas VPN lewat jaringan internet. Pertukaran data melalui VPN IP MPLS jauh lebih mudah, cepat dan lebih aman dan koneksi jaringan lebih stabil.

REFERENASI

DOI: 10.52362/jisamar.v6i1.662
Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional

[1]Arnita, A., & Farid, M. (2020). Implementasi jaringan virtual private network dengan teknologi Multi Protocol Label Switching (MPLS). *Jurnal Riset Tindakan Indonesiaurnal Riset Tindakan Indonesia*, *5*(2), 28–39.
[2]Euginia, B., & Ghozali, T. (2018). Simulasi Multi Protocol Label Switching Virtual Private Network (MPLS VPN) Dengan Virtual Local Area Network (VLAN) Menggunakan Router MIKROTIK. *Tesla*, *20*(2), 109–117.
[3]Fathurrahmad, Yusuf, S. (2019). Implementasi Jaringan VPN dengan Routing Protocol terhadap Jaringan Multiprotocol Label Switching (MPLS). *Jurnal JTIK*, *3*(1).
[4]Mardiyanto. (2019). Analisis Quality of Service (QoS) pada Jaringan VPN dan MPLS VPN Menggunakan GNS3. *Jurnal Sains Dan Informatika*, *5*(November), 98–107. https://doi.org/10.34128/jsi.v5i2.191
[5]Rahmawati, Y., Ikhwan, S., & Hadi, I. P. (2018). (MPLS VPN) DENGAN MENGGUNAKAN SIMULATOR. *CENTIVE*, 367–371.
[6]Sari, A. P., & Kemala, N. (2020). PERANCANGAN JARINGAN VIRTUAL PRIVATE NETWORK BERBASIS IP SECURITY MENGGUNAKAN ROUTER MIKROTIK. *Jurnal PROSISKO Vol.*, *7*(2), 150–164.
[7]Septarindra, A., Munadi, R., & Negara, R. M. (2016). IMPLEMENTASI DAN ANALISIS PERFORMA MULTI PROTOCOL LABEL SWITCHING - VIRTUAL PRIVATE NETWORK (MPLS-VPN) DENGAN METODE GENERIC ROUTING ENCAPSULATION PADA LAYANAN BERBASIS FILE TRANSFER PROTOCOL (FTP) IMPLEMENTATION AND ANALYSIS MULTI PROTOCOL LABEL SWIT. *E-Proceeding of Engineering*, *3*(3), 4504–4511.
[8]Setiawan, A., Priyanto, H., Irwansyah, M. A., Eng, M., Studi, P., Informatika, T., … Tanjungpura, U. (2016). PERANCANGAN DAN IMPLEMENTASI VIRTUAL PRIVATE NETWORK DENGAN PROTOKOL PPTP PADA CISCO. *Jurnal Sistem Dan Teknologi Informasi (JUSTIN)*, *1*(1), 1.
[9]Suryanto, & Dewi, S. (2013). IMPLEMENTASI JARINGAN VPN BERBASIS IP-MPLS. *Paradigma*, *XV*(1), 98–105.
[10]Wahyudi, M., & Purnama, R. A. (2019). Analisis Performa Site to Site IP Security Virtual Private Network (VPN) Menggunakan Algoritma Enkripsi ISAKMP (Performance Analysis Site to Site IP Security Virtual Private Network (VPN) with Algorithm Encryption ISAKMP). *JUITA*, *7*(November), 129–135.

DOI: 10.52362/jisamar.v6i1.662
Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional