IMPLEMENTASI JARINGAN VPN BERBASIS IP-MPLS PADA PT. MHE DEMAG INDONESIA

[1]Suryanto, [2]Sari Dewi

[1]Manajemen Informatika, AMIK BSI Jakarta
Jl. Rs. Fatmawati No. 105 Pondok Labu Jakarta Selatan
E-Mail: suryanto.syt@bsi.ac.id
[2]Teknik Informatika, STMIK Nusa Mandiri
Jl. Kramat Raya 25, Jakarta Pusat
E-Mail: sari_tk07@yahoo.co.id

ABSTRACT

The research objective is to design and build a network linking the headquarters with a branch office in PT. MHE DEMAG Indonesia, so change data going to run safely and smoothly with the hope it can improve network performance and company performance in support of business processes. To meet these needs may use a technology called Virtual Private Network (VPN). IP-VPN MPLS has a better degree of flexibility compared to leased lines, frame relay, and ATM, and also offer a cheaper solution. VPN technology can be formed with a facility that can tunnel across the MPLS network. The tunnel facility can build a site to site connection lines are virtual and have a pretty good level of security because it can only be accessed by users who are on the wrong site (private connection). IP MPLS is a data communication services in the form of dedicated leased IP-based channel with its main advantage is able to provide any services to any connection. MPLS-based IP VPN technology can provide services include: Intranet, Extranet, and Remote Dial. In addition, this technology also has some clappers like: Multiservices Platform, Provisioning Scalability, Cost Saving Opportunity and Security. This study discusses the implementation of IP-based MPLS VPN used on PT. MHE DEMAG Indonesia and the authors conducted experiments with simulations. Simulation program used is GNS3 and Cisco IOS. Simulation test results showed IP-MPLS VPN works. VPN-MPLS IP VPN is able to separate the one with the other so as to improve and guarantee the safety factor between head office and branch offices.

Keywords*: Internet Protocol, Komunikasi data, MPLS, VPN*

1. Pendahuluan

Suatu jaringan idealnya dapat menghubungkan antartitik secara any to any. Di masa lalu, perusahaan yang hendak menghubungkan cabang-cabang kantornya dalam suatu jaringan akan mengunakan saluran sewa secara titik ke titik (point to point) yang tentu saja biayanya sangat besar. Seiring dengan maraknya penggunaan jaringan publik (Internet), banyak perusahaan yang kemudian beralih menggunakan jaringan publik sebagai bagian dari jaringan mereka untuk menghemat biaya. Begitu juga dengan PT. MHE DEMAG yang memanfaatkan jaringan untuk mendukung proses bisnisnya namun belum dimanfaatkan secara maksimal dan melalui jaringan yang aman, sebagai contoh untuk pertukaran data antara kantor cabang dan kantor pusat dilalukan via e-mail yang diberikan oleh operator penyedia internet (*Internet Service Provider*) atau e-mail yang disediakan secara gratis seperti dari yahoo, gmail dan lainnya sehingga aliran data penting perusahaan seperti data keuangan, data custumer sepenuhnya tergantung pada fasilitas atau layanan yang diberikan pada email tersebut, dimana layanan e-mail ini tidak dapat menjamin keamanan datanya dan apabila penyedia layanan email mengalami ganguan atau masalah maka aliran data penting dari perusahaan akan ikut terganggu atau terhambat. Begitu juga dengan data yang ada di database tidak bisa langsung *diupdate* sesuai dengan transaksi yang sedang berjalan karna tidak adanya jaringan yang langsung di hubungkan antara kantor pusat dengan kantor cabang, sehingga ketika sales cabang ingin mengetahui stok barang yang tersedia secara keseluruhan maka sales tersebut harus mengecek barang pada cabang-cabang yang lain via telephon, dimana komunikasi via

telephon ini tidak efektif dan tidak aman. Permasalahan-permasalahan tersebut menjadi kendala yang membutuhkan penyelesaian.

Teknologi jaringan yang dapat menjadi solusi permasalaahan tersebut 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 jaringan internet yang besar dan aman.

Teknologi VPN terus berkembang untuk memberikan keuntungan bagi penggunannya dan teknolgi yang sekarang mulai banyak diterapkan oleh perusahaan adalah VPN IP-MPLS yaitu layanan VPN yang melintasi jaringan MPLS (*Multi Protocol Label Switching*). Dipilihnya teknologi ini karena memiliki kemampuan untuk membuat sambungan any to any yang dapat dihubungkan ke jaringan publik seperti Internet. VPN IP mengkombinasikan berbagai unsur dalam teknologi IP untuk memberi layanan yang memenuhi berbagai komponen layanan komunikasi baku yang ditawarkan oleh teknologi sebelumnya. Semisal yang ditawarkan oleh saluran sewa (leased line), frame relay dan ATM (Asynchronous Transport Mode). 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.

2. Tinjauan Pustaka

Virtual Private Network (VPN) merupakan teknologi untuk membentuk jalur khusus yang menghubungkan antara komputer satu dengan yang lainya. Jalur khusus tersebut dapat melewati internet maupun jaringan jaringan tertentu namun tidak tercampur dengan aktifitas jalur yang ditumpangi. Pada gambar 1 menggambarkan tentang struktur jaringan VPN.

Adapun alasan VPN banyak digunakan saat ini adalah

1. Menekan biaya interkoneksi.
2. Memperluas interkoneksi user yang selama ini susah di jangkau
3. Dapat mengirimkan Aplikasi baru berbasis Internet Protocol
4. Fleksibelitas dalam memilih Topology
5. Skalabilitas Networking terjaga
6. Meningkatkan tinggkat security

MPLS merupakan protokol jaringan telekomunikasi untuk lalu lintas berkecepatan tinggi terutama untuk lapisan *backbone* (*core*) internet. Istilah Multi Protocol berarti menjembatani perbedaan protokol pada perangkat terutama layer 2 OSI dan layer 3 OSI, misalnya pada ATM dan Router. Teknologi MPLS mempersingkat proses-proses yang ada di IP *Routing* Tradisional dengan mengandalkan sistem label *switching*. Dengan label *switching* paket-paket data akan keluar masuk dengan kecepatan yang tinggi karena banyak sekali proses yang dapat diringkas.

Layanan *Virtual Private Network Multi Service* (VPN Multi Service) adalah layanan satu paket solusi komunikasi data yang memberikan layanan sampai ke *end user* berbasis IP dengan menggunakan jaringan MPLS (*Multi Protocol Label Switch*) yang aman untuk hubungan *Wide Area Network* (WAN). Jaringan *sharing* MPLS memadukan kemampuan *label swapping* dengan *layer network routing* untuk membentuk private network yang aman dan cepat dalam pengiriman paket informasi.

IP MPLS adalah teknik untuk mengintegrasikan *Internet Protocol* (IP) dengan *Asynchronous Transfer Mode* (ATM) dalam jaringan *backbone* yang sama. Dengan MPLS maka dapat diperoleh keuntungan diantaranya:

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

VPN IP-MPLS mampu memberikan layanan komunikasi data any to any connection berbasis IP *Multi Protocol Label Switching* (MPLS). Dalam hal keamanan, VPN IP-MPLS ini setingkat dengan frame relay/ATM, dimana trafik atau lalu lintas data dialirkan dalam suatu jaringan yang terpisah dengan jaringan publik lainnya atau jaringan internet. Beberapa kelebihan yang dapat disediakan oleh VPN IP-MPLS adalah sebagai berikut:

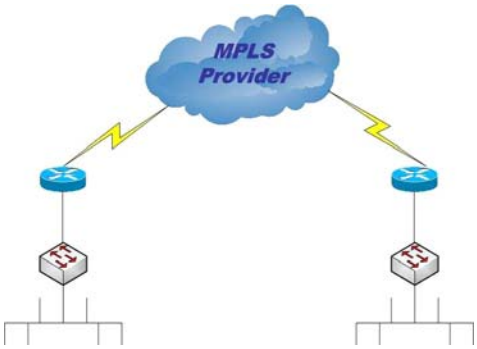
a. Multiservices Offering

VPN-MPLS menawarkan berbagai macam aplikasi bisnis antara lain berupa voice, data, dan video.

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.

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



Gambar 1. Konfigurasi Umum VPN IP-MPLS

Dengan menggunakan VPN IP MPLS diharapakan akses data dari kedua *site* tesebut dapat berjalan aman karena lalu lintas data dapat dipisahkan dengan VPN IP-MPLS tersebut. VPN IP-MPLS dapat menyembunyikan struktur alamat *Core Network* dan VPN di dalamnya. Pultz, Richard (2004) dari *Gartner Research* menyatakan bahwa "sangatlah tidak mungkin jaringan di luar *Core Network* melakukan penyusupan ke dalam *Core Network* dan VPN di dalamnya dengan cara merusak mekanisme MPLS"

Dengan fleksibilitas jaringan IP yang sangat tinggi maka berbagai macam layanan dan aplikasi dapat dijalankan di atas jaringan sistem IP MPLS. Layanan dari tingkat integritas dan interaktivitas tinggi seperti video, voice dan data tertentu sampai dengan layanan non-critical dan non-delay sensitive seperti layanan internet dan E-mail dapat secara optimal dilayani dalam satu jaringan fleksibel IP MPLS. Beberapa fitur IP MPLS antara lain:

a. Intranet
Jaringan Intranet umumnya terdiri atas berbagai aplikasi yang kemudian dibawa dalam bentuk bermacammacam jenis trafik pula. IP MPLS dengan kemampuan CoS-nya sangat sesuai untuk digunakan sebagai jaringan aplikasi semacam ini.

b. Extranet
Faktor terpenting dalam jaringan extranet adalah security dan accessabilitiy. IP MPLS mendukung kedua requirement ini. Sistem keamanan selain telah dijamin di dalam core network IP MPLS dalam bentuk VPN untuk setiap group pemakai, di sisi pemakai masih dapat ditambah firewall atau sistem keamanan lain seperti enkripsi, dan lain-lain. Dalam hal accessabilitiy jaringan IP memiliki kemampuan penuh untuk dapat dipergunakan oleh berbagai aplikasi.

c. Remote Dial
Faktor accessability dapat dijawab pula dengan remote dial system dalam jaringan IP MPLS. System remote dial ini dapat pula diaplikasikan dalam bentuk VPN Dial yang dapat mengintegrasikan berbagai jaringan termasuk IP MPLS, Frame Relay dan jenis LC (Leased Channel) lainnya.

3. Metodologi Penelitian

Metodologi yang digunakan meliputi:

a. Analisis
1. Melakukan survei terhadap sistem yang sedang berjalan dengan carawawancara dengan staf dan manajer IT, kemudian menganalisis hasil survei tersebut untuk mendapatkan rumusan masalah yang sedang dihadapi oleh perusahaan dan mendapatkan alternatif pemecahan masalah.
2. Studi Literatur yang merupakan teknik pengumpulan data atau informasi dengan mempelajari buku-buku yang berisi konsep dan implementasi VPN menggunakan koneksi *virtual* yang dikirimkan melalui jaringan MPLS yang digunakan sebagi dasar dari pengembangan penulisan artikel ini.

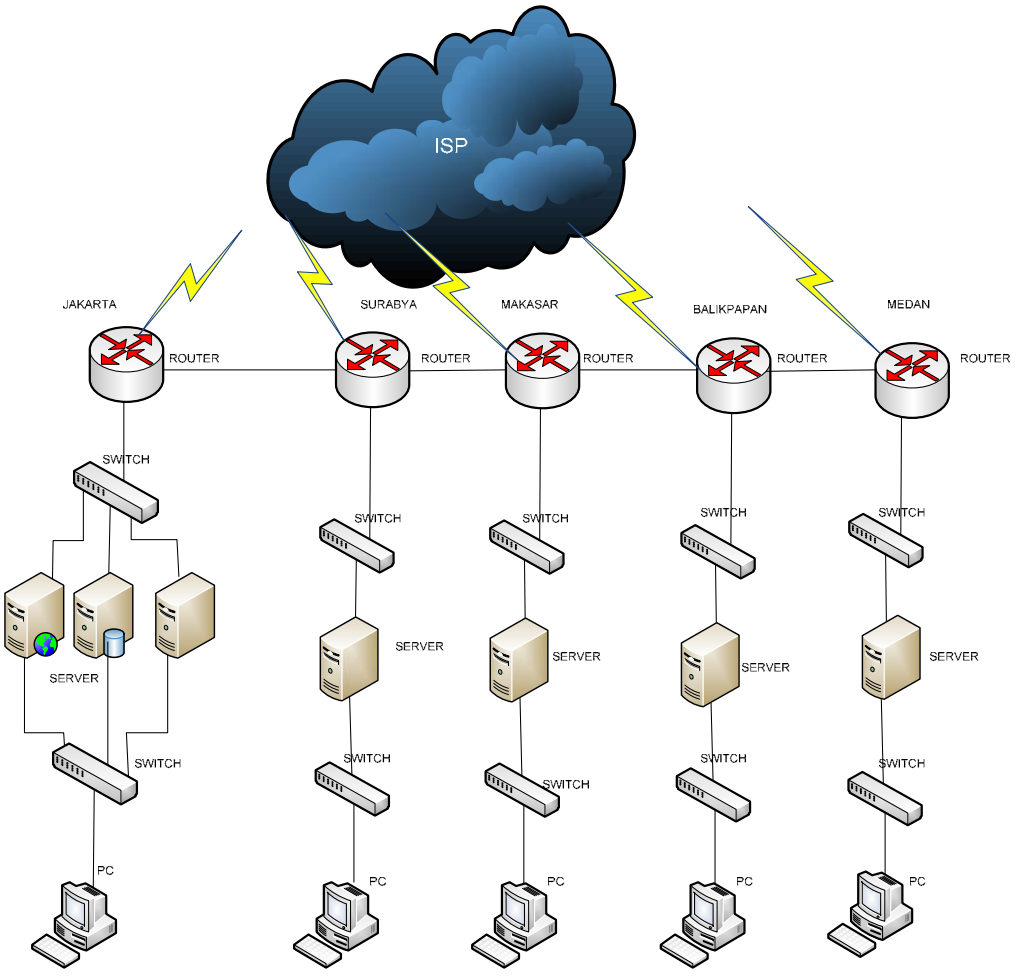
b. Perancangan
Perancangan VPN (*Virtual Private Network*) mulai dari topologi koneksi VPN, tipe VPN, beserta alat-alat jaringan

yang akan digunakan.

c. Membangun Simulasi Jaringan VPN IP MPLS
   Membangun rancangan VPN IP MPLS yang telah dibuat dengan menggunakan *Software* simulasi OPNET.
d. Pengujian Simulasi Jaringan
   Jaringan yang telah disimulasi akan diuji untuk melihat bagaimana kinerjanya dan kemudian mengevaluasinya.

Pada analisis yang sudah dilakukan pada PT.MHE DEMAG, pertukaran data hanya diperlukan antara kantor pusat dan kantor-kantor cabang. Walaupun kadang-kadang bisa terjadi pertukaran data antara kantor-kantor cabang, itu dikarenakan kantor cabang tidak mempunyai data yang selalu ter-update dari kantor pusat. Arsitektur jaringan pada PT.MHE DEMAG sebelum diterapkannya VPN dapat dilihat pada gambar 2 dibawah ini:

4. Pembahasan



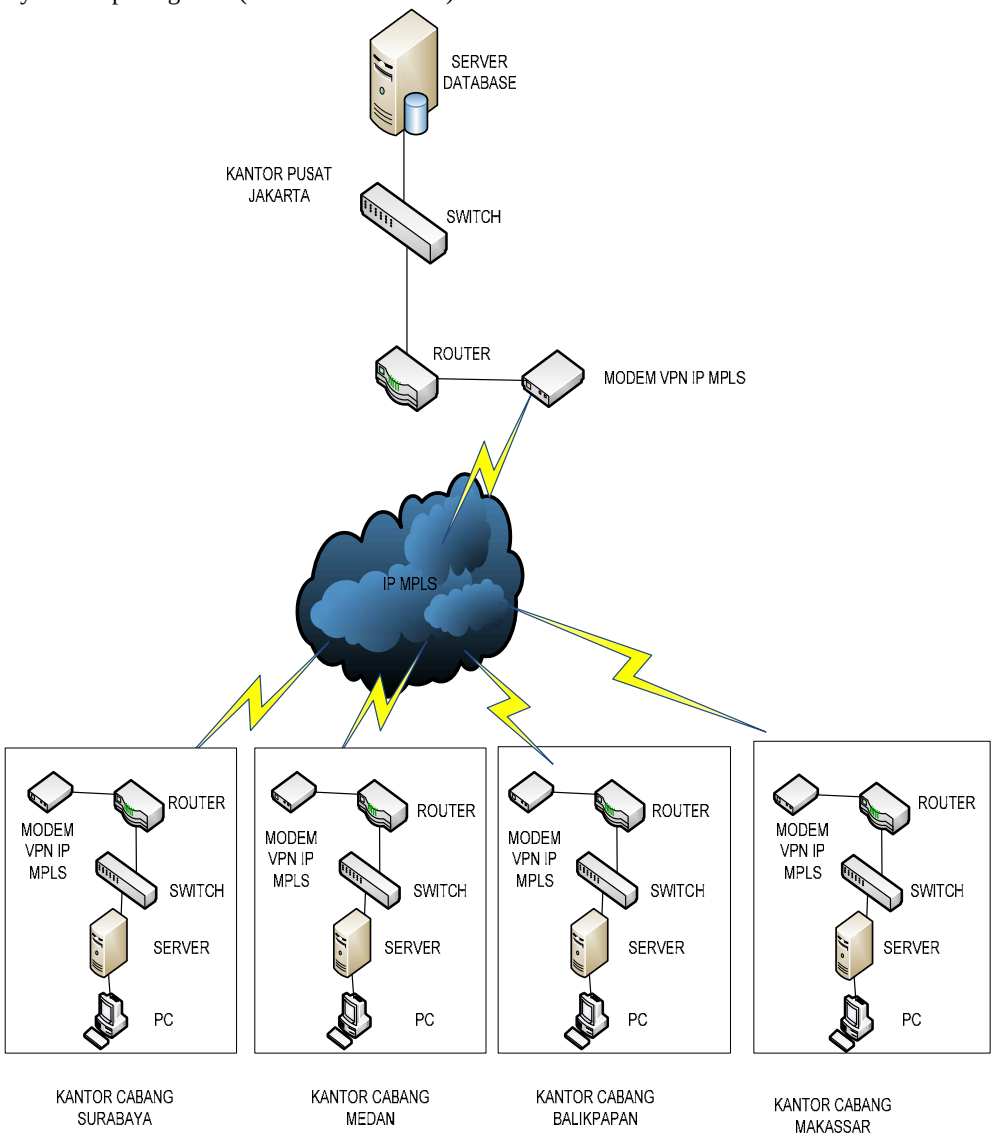
Gambar 2. Arsitektur jaringan pada PT.MHE DEMAG sebelum ada VPN

Teknologi VPN yang akan digunakan untuk menghubungkan jaringan kantor pusat dan kantor cabang pada Perusahaan MHE DEMAG adalah 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, 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.

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 1 Mbps, sedangkan untuk tiap-tiap kantor cabang cukup 128 Kbps saja.

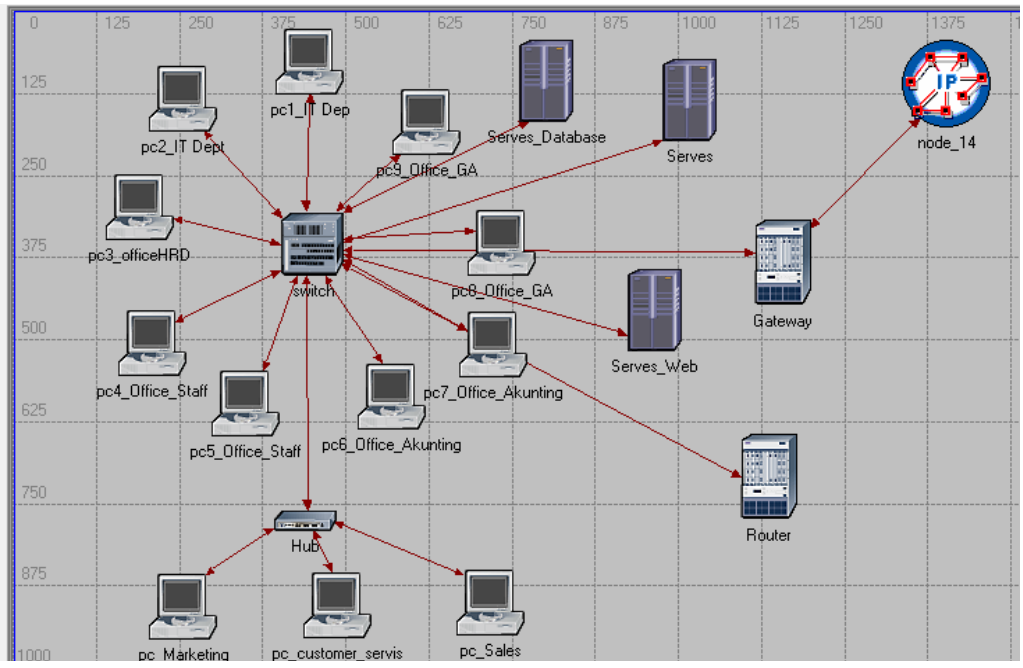
Setelah kantor pusat dan kantor-kantor cabang terhubung menggunakan VPN, masing-masing kantor cabang dapat mendapatkan data yang selalu ter-*update* dan tidak diperlukan lagi adanya pertukaran data antara kantor-kantor cabang. Ini menjadikan kantor pusat sebagi *central site (star)* dan kantor-kantor cabang sebagai *remote office (spokes)*. Topologi *star* and *spokes* juga mudah untuk dikembangkan jika terdapat kantor-kantor cabang yang baru dari berbagai kota yang ingin dihubungkan dengan kantor pusat. Arsitektur jaringan setelah adanya VPN IP-MPLS dapat dilihat pada gambar 3.



Gambar 3.Arsitektur jaringan setelah adanya VPN

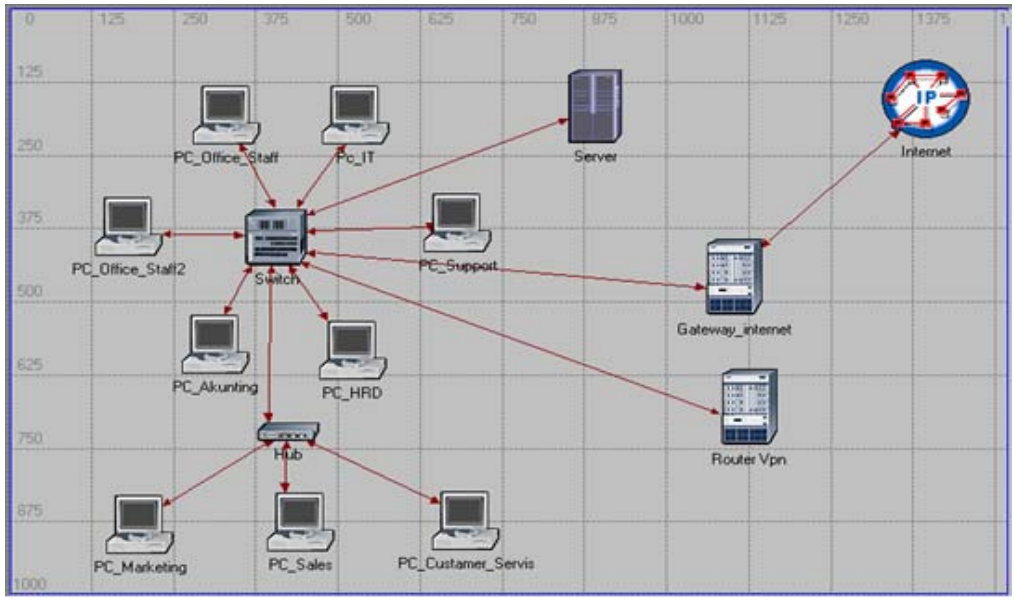
Dengan adanya rancangan VPN seperti pada gambar 3, maka perlu dilakukan beberapa perubahan pada jaringan Kantor Pusat PT.MHE DEMAG. adanya penambahan alat jaringan, yaitu modem dan router untuk VPN IP MPLS yang disediakan dari PT. TELKOM dan mitra kerja PT. TELKOM. Lalu jaringan pada kantor pusat akan dibagi menjadi dua bagian, yaitu jaringan yang dapat mengakses database dan jaringan yang tidak dapat mengakses database (hanya dapat mengakses internet). Tetapi supaya jaringan yang dapat mengakses database juga dapat mengakses internet, maka modem ADSL dihubungkan dengan *router* VPN. Pembagian jaringan dilakukan agar database yang ada hanya dapat diakses oleh bagian-bagian tertentu seperti bagian marketing, manajer, *Office*, direktur, dan accounting sedangkan bagian yang lainnya hanya bisa mengakses internet dan LAN saja.

Untuk pengujian jaringan Skenario yang akan diujikan adalah sesuai dengan rancangan VPN , yaitu 1 kantor pusat dan 4 kantor cabang yang terhubung dengan teknologi VPN IP MPLS, dengan Database Server yang terletak di kantor pusat yang diakses dari kantor-kantor cabang dan kantor pusat. Kemudian yang akan diuji dalam simulasi ini meliputi : besar Tunnel Delay pada masing-masing tunnel dan utilisasi penggunaan bandwidth pada kantor pusat daripada masing-masing kantor cabang. Penting untuk mengetahui seberapa besar delay yang mungkin terjadi pada tunnel, karena delay memberikan pengaruh yang besar dalam proses komunikasi dan kelancaran aliran data, dan tujuan utama dibangun VPN IP MPLS ini adalah supaya kantor cabang dapat mendapatkan data yang terupdate dengan cepat. Pengujian utilisasi penggunaan bandwidth adalah untuk memperkirakan apakah bandwidth yang akan digunakan pada kantor pusat dan kantor-kantor cabang dapat mencukupi kebutuhan penggunaannya masing-masing.



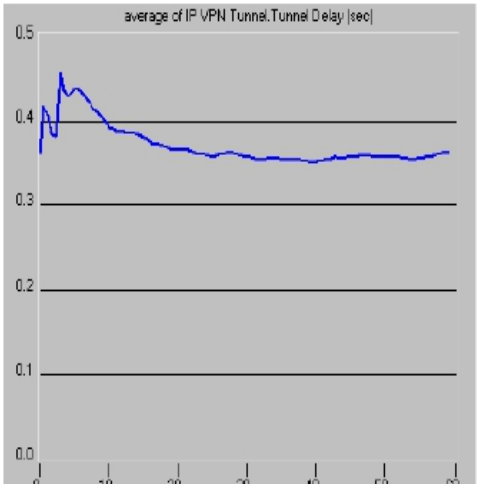
Gambar 3. Rancangan Jaringan Simulasi VPN IP MPLS Kantor Pusat

Untuk subnet Kantor Cabang Surabaya, Makasar, Medan, Balikpapan penyusunannya sama dan dapat dilihat pada gambar 4.



Gambar 4. Rancangan Jaringan Simulasi VPN IP MPLS Kantor Cabang

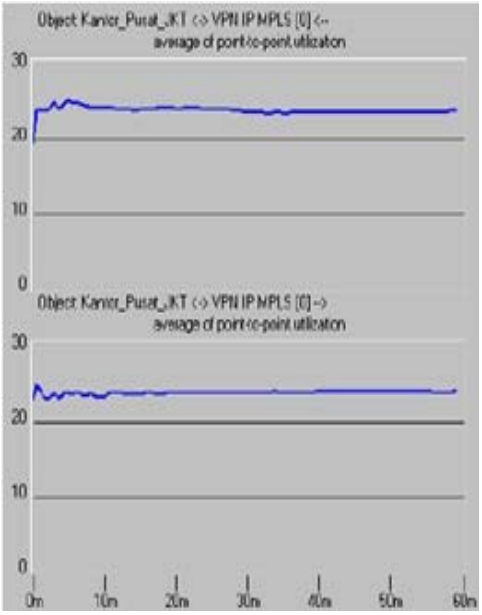
Berikut ini adalah statistik ”IP VPN Tunnel Delay” yang didapat dari simulasi.



Gambar 5. Tunnel Delay antara Kantor Pusat dan Kantor Cabang

Berdasarkan hasil pengujian delay pada jaringan simulasi pada gambar 3, didapatkan bahwa besarnya delay pada masing-masing tunnel berkisar dari 0,34 detik sampai 0.375 detik, dimana delay sebesar ini masih dapat diterima dalam melakukan pertukaran data.

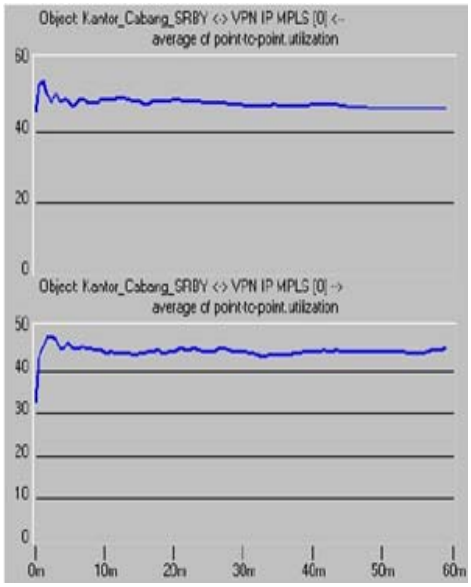
Berikut ini adalah hasil pengujian pengunaan bandwith sebelum dan sesudah implementasi VPN IP MPLS.



Gambar 6. Hasil Pengujian Penggunaan Bandwith pada Kantor Pusat

Dari hasil pengujian seperti yang terlihat pada gambar 6, penggunaan bandwidth pada kantor pusat sekitar 24% dari 1 Mbps bandwidth yang digunakan, hasil ini cukup bagus karena masih ada sisa bandwidth yang dapat digunakan apabila terdapat kantor-kantor

cabang yang baru dan komunikasi data dapat dilakukan dengan baik.



Gambar 7. Hasil Pengujian Penggunaan Bandwith pada Kantor Cabang

Sedangkan pada pada pengujian kantor-kantor cabang seperti yang terlihat pada gambar 7 menunjukan penggunaan bandwidth berkisar antara 45% sampai 47% dari 128Kbps bandwidth yang digunakan. Dari hasil yang didapat menunjukan bahwa penggunaan bandwidth pada kantor cabang sudah cukup efektif, karena masih ada sisa bandwidth sekitar 55%, selain itu, jika hanya diberi bandwidth 64Kbps, maka utilisasi kegunaan bandwidthnya bisa mencapai lebih dari 90%. Dari hasil pengujian dikantor cabang ini memberikan gambaran bahwa kesedian bandwidth pada kantor cabang tidak boleh kurang dari 64 Kbps agar komunikasi data bias berjalan dengan baik.

5. Kesimpulan

Setelah menganalisis, merancangan dan mensimulasikan jaringan VPN IP-MPLS di PT. MHE DEMAG INDONESIA maka penulis dapat mengambil kesimpulan bahwa:

1. Dari analisis kondisi jaringan saat penulis melakukan penelitian di PT. MHE DEMAG INDONESIA didapatkan bahwa proses pengiriman data dari cabang ke pusat secara keaman belum maksimal di karnakan tidak ada nya metode keamanan data enscaptulation data sehingga untuk adanya kemungkinan serangan dari *malware, adware* atau bahkan *creaker*.
2. Untuk itu sebaiknya perusahaan PT. MHE DEMAG Indonesia 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.
3. Pertukaran data melalui VPN IP MPLS jauh lebih mudah, cepat dan lebih aman apabila dibandingkan dengan cara yang sebelumnya digunakan, yaitu melalui e-mail dan telepon. Dengan demikian akan meningkatkan kinerja perusahaan terutama dalam hal komunikasi dan pertukaran data.

Daftar Pustaka

Basalamah, Abdullah. 2008. Kajian Metode load Balancing Routing Dengan Bandwidth Delay Guarrantee untuk layanan VPN Pada Jaringan MPLS.ISSN:1411-7797.Makasar:Al-Jibra, Vol IX No 2, Agustus 2008:95-99

Fadillah, Rizal dan Djumhadi. 2009. Penggunaan Telekomunikasi Komunikasi Data Berbasis VPN-IP MPLS untuk pemilihan Umum. ISSN:1979-2328. Yogyakarta:Seminar Nasional Informatika 2009 UPN"Veteran" 23 Mei 2009.

Pultz, Richard. 2004. *Analysis of MPLS-Based IP VPN Security: Comparison to Traditional L2VPNs such as ATM and Frame Relay, and Deployment Guidelines.*

Rachmawati, Ariefah. 2007. Upaya Menjaga Akuntabilitas Pertukaran Data Dengan Teknologi Informasi Multi Protocol Labeling Switching. ISSN:1412-1212.Jakarta:Journal The Winners Vol.8 No.2, September 2007:155-164.