UPAYA MENJAGA AKUNTABILITAS PERTUKARAN DATA DENGAN TEKNOLOGI INFORMASI *MULTIPROTOCOL LABEL SWITCHING*

Ariefah Rachmawati[1]

ABSTRACT

Data communication network, part of the information technology, becomes so important in communicating information and transferring data. Most companies in the world, including companies operating in Indonesia, have used data communication networking technology for their day-to-day operation. However, transferring data through network has some security problems. Therefore, accountants should be familiar with and have knowledge about it in order to ensure high quality work that they provide. Based on IETF – Internet Engineering Task Force a (RFC (Request for Comment)-3031), it is stailea that information technology used to communicate and transfer information as well as data should be efficient and safe. Multiprotocols Label Switching (MPLS) is a new technology used in virtual private network is one of the solutions in making data transfer efficient and safe.

Keywords: *efficiency, accountability, multiprotocol label switching*

ABSTRAK

Jaringan komunikasi data, sebagai bagian teknologi informasi, menjadi hal penting dalam komunikasi informasi dan transfer data. Kebanyakan perusahaan di dunia, termasuk perusahaan yang beroperasi di Indonesia, telah menggunakan jaringan teknologi komunikasi data dalam kegiatan perusahaan. Meskipun demikian, transfer data melalui jaringan menghadapi kendala keamanan. Oleh karena itu, para akuntan harus mengenali dan memiliki pengetahuan mengenai hal tersebut untuk menjamin kualitas kerja yang disediakan. Berdasarkan IETF – Internet Engineering Task Force (RFC (Request for Comment)-3031), dinyatakan bahwa teknologi informasi yang digunakan untuk berkomunikasi dan mentransfer informasi dan data harus efisien dan aman. Multiprotocols Label Switching (MPLS) adalah teknologi baru yang digunakan dalam jaringan pribadi maya yang dapat digunakan sebagai salah satu solusi untuk mentransfer data sehingga dapat efisien dan aman.

Kata kunci: *efisiensi, akuntabilitas, multiprotocol label switching*

[1] **Jurusan Akuntansi, Fakultas Ekonomi, Universitas Bina Nusantara, Jl. K.H. Syahdan No. 9, Palmerah, Jakarta Barat 11480, ariefahr@binus.edu**

PENDAHULUAN

Pada era informasi sekarang ini, penerapan teknologi informasi telah banyak dilakukan oleh perusahaan sebagai media pendukung kinerja kegiatan operasional maupun non-operasional perusahaan. Bagi perusahaan berskala kecil yang sangat sederhana dan tidak memiliki kantor cabang, mungkin membutuhkan teknologi informasi yang tidak memerlukan aplikasi jaringan. Akan tetapi, bagi perusahaan yang berskala besar dan memiliki satu atau lebih kantor dibutuhkan proses komunikasi data yang andal sebagai media komunikasi antara kantor yang satu dengan kantor yang lain dan juga antara klien dan partner bisnis.

Saat ini yang menjadi pertimbangan bagi perusahaan untuk melakukan pertukaran data adalah harus efisien, cepat, dan aman. Untuk itu, perusahaan harus dapat mempertimbangkan teknologi yang dapat diterapkan di dalam organisasinya. Teknologi *MPLS* menawarkan solusi terbaiknya untuk memenuhi kebutuhan perusahaan dalam hal pertukaran data.

Untuk dapat memenuhi kebutuhan komunikasi data tersebut, dapat dilakukan dengan menerapkan teknologi *networking*. Salah satu teknologi yang dapat diterapkan, antara lain dengan membangun jaringan *Virtual Private Network (VPN)*. Saat ini, terdapat teknologi pengembangan layanan *VPN,* yaitu teknologi *Multiprotocol Label Switching (MPLS)*. *MPLS* adalah arsitektur *network* yang didefinisikan oleh *Internet Engineering Task Force (IETF)* dan *MPLS* memberikan efisiensi *routing*, *forwarding,* dan *switching* dari alur trafik dalam jaringan. *MPLS* merupakan solusi untuk berbagai permasalahan yang ada pada jaringan komputer saat ini, yaitu kecepatan, skalabilitas, *quality-of-service* (QoS) *management*, dan *traffic engineering* (rekayasa trafik).

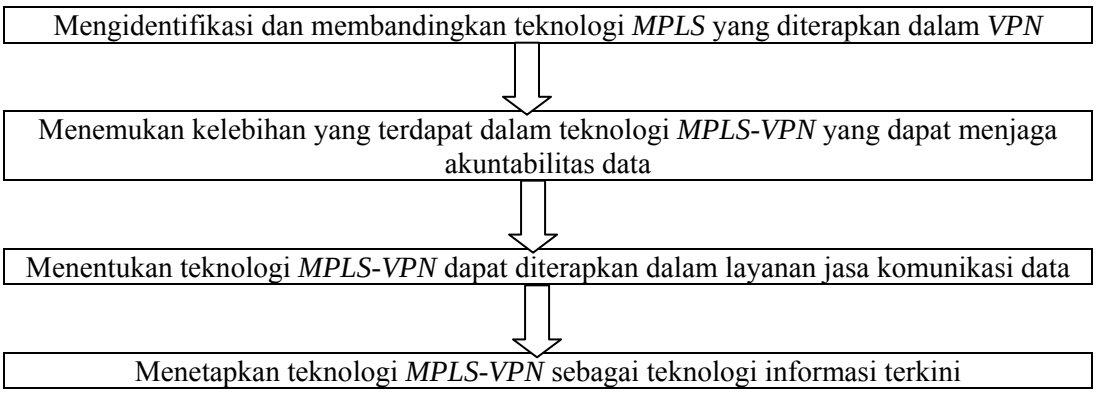
Dengan keandalan yang dimilikinya, kini layanan *VPN* berbasiskan *MPLS* mulai populer di banyak negara termasuk Eropa, Asia, dan Amerika. Di Indonesia sendiri sudah ada beberapa penyedia jasa yang berencana untuk menjual layanan dan bahkan ada pula yang telah menjual layanan *VPN* berbasis *MPLS* ini. Tujuan penelitian untuk membuktikan bahwa keandalan layanan *VPN* dengan teknologi *MPLS* ini dapat memenuhi konsep akuntabilitas dengan tipe arsitekturnya dan model implementasinya, yaitu pada *access network* dan *core network* sehingga teknologi ini benar-benar dapat diterapkan untuk layanan yang sifatnya *multiservices*.

METODE PENELITIAN

Adapun metode dalam pengumpulan data yang ditempuh adalah sebagai berikut. Pertama, penelitian kepustakaan (*Library Research*). Dalam penelitian ini, dipelajari dan dibaca berbagai buku literatur sebagai sumber naratif dan dokumen lain yang

berhubungan dengan masalah akuntabilitas dengan teknologi informasi berupa *Multiprotocol Label Switching* (MPLS). Kedua, penelitian lapangan (*Field Research*). Penelitian ini didasarkan atas penelitian langsung pada objek yang dituju guna mendapatkan data yang nyata. Adapun teknik penelitian lapangan adalah sebagai berikut: Metode observasi, yaitu melakukan penelitian dengan tindakan mengamati, melihat, dan mencatat kejadian tersebut terjadi dalam perusahaan; Metode wawancara, yaitu melakukan penelitian dengan mewawancarai pejabat yang berwenang lainnya untuk memberikan informasi.

Tahapan Penelitian yang dilakukan



Gambar 1 Tahapan Penelitian Teknologi Informasi *Multiprotocol Label Switching*

TINJAUAN PUSTAKA

Undang-Undang Bank Indonesia No. 23/1999 menuntut adanya akuntabilitas dan transparansi dalam setiap pelaksanaan tugas, wewenang, dan anggaran Bank Indonesia. Akuntabilitas dan transparansi yang dituntut dari Bank Indonesia tersebut dimaksudkan agar semua pihak yang berkepentingan dapat ikut melakukan pengawasan terhadap setiap langkah kebijakan yang ditempuh oleh Bank Indonesia. Dari segi pelaksanaan tugas dan wewenang, prinsip akuntabilitas dan transparansi diterapkan dengan cara menyampaikan informasi kepada masyarakat luas secara terbuka melalui media massa, pada setiap awal tahun, mengenai evaluasi pelaksanaan kebijakan moneter pada tahun sebelumnya, serta rencana kebijakan moneter dan penetapan sasaran moneter untuk tahun yang akan datang. Informasi tersebut juga disampaikan secara tertulis kepada Presiden dan DPR.

Virtual Private Network adalah jaringan data pribadi yang menggunakan infrastruktur telekomunikasi publik. *VPN* berbeda dengan sistem penyewaan atau *leased line* yang hanya dapat digunakan oleh satu perusahaan. Tujuan utama *VPN* adalah memberikan layanan sewa yang mempunyai kapabilitas yang sama dengan jalur sewa

pribadi dengan biaya yang lebih murah menggunakan infrastruktur publik bersama. Secara umum, layanan yang ditawarkan *VPN* dibagi dua (Anonymous, 2006). Pertama, *Overlay Model*. Pada model ini, penyedia jasa (*service provider*) menyediakan koneksi virtual antara situs. Hubungan pada jaringan penyedia jasa menggunakan koneksi *Point-to-Point*. *Routing* yang terjadi pada jaringan pelanggan terlihat jelas oleh jaringan penyedia jasa. Penyedia jasa bertanggung jawab penuh atas tranportasi data antara situs pelanggan. Kedua, *Peer Model*. Pada model ini, penyedia jasa berpartisipasi pada *layer routing* dari pelanggan. Jaringan penyedia dan pelanggan menggunakan protokol yang sama.

Menurut pendapat Wastuwibowo (2003:7), *MPLS* merupakan teknologi baru dalam arsitektur jaringan yang distandarisasikan oleh *Internet Engineering Task Force (IETF)*. *IETF* membentuk kelompok kerja *MPLS* pada tahun 1997 untuk mengembangkan metode umum yang distandarkan. Tujuan kelompok kerja *MPLS* untuk menstandarkan protokol yang menggunakan teknik pengiriman *label swapping* (pertukaran label). *MPLS* merupakan salah satu bentuk konvergensi vertikal dalam topologi jaringan. *MPLS* tidak menggantikan peran *routing IP* tetapi dapat bekerja bersamaan dengan teknologi *routing* yang sekarang dan yang akan datang untuk memberikan pengiriman data yang sangat cepat.

Jaringan *MPLS* terdiri dari jalur yang disebut *Label-Switched Path (LSP)* yang menghubungkan titik-titik yang disebut *Label-Switched Router (LSR)*. *LSR* pertama disebut *ingress* dan *LSR* yang terakhir disebut *egress*. Setiap *LSR* dikaitkan dengan sebuah *Forwarding Equivalence Class (FEC)* yang merupakan kumpulan paket yang menerima perlakukan *forwarding* yang sama di sebuah *LSR*. *FEC* diidentifikasikan dengan pemasangan label. Pertama, *MPLS Operation*. Jaringan *MPLS* terdiri dari rangkaian *node-node* yang dapata men-*switch* dan men-*route* berdasarkan *label* yang dipasang pada setiap paket. Kedua, *QoS Support* adalah kemampuan dalam menjamin pengiriman arus data penting. Ketiga, *Traffic Engineering* adalah kemampuan dalam merencanakan secara dinamis komitmen sumber daya berdasarkan permintaan yang telah diketahui, menentukan rute secara dinamis, serta mengoptimalkan penggunaan jaringan.

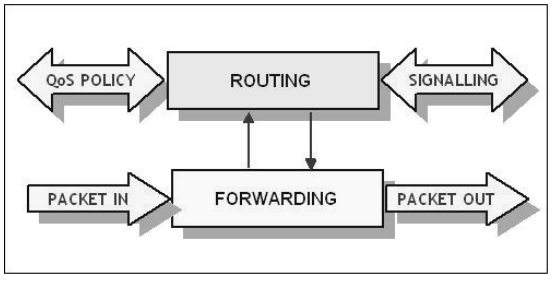
Keempat, *VPN Support*. *MPLS* memberikan mekanisme yang efektif untuk mendukung *VPN*. Teknologi *MPLS* memberikan kemampuan untuk memisah-misahkan lalu lintas dari berbagai *VPN*. Selain itu, dengan dibuatnya *tunnel* (saluran atau terowongan) akan terbentuk topologi virtual. Kelima, *Multi Protocol Support*. *MPLS* dapat digunakan pada banyak teknologi pembuatan jaringan. *MPLS* memungkinkan *router* dapat bekerja bersama dengan *router-router* biasa. *MPLS* dirancang untuk bekerja dalam jaringan ATM dan *Frame-Relay*. *MPLS* memungkinkan *switch* ATM dan *Frame-Relay* juga dapat bekerja dengan *switch* yang biasa.

PEMBAHASAN

Dengan berbagai kelebihan yang dimilikinya, teknologi *MPLS* menjadi andalan baru bagi perusahaan yang sangat membutuhkan layanan komunikasi data yang aman, cepat, andal, dan murah. Untuk sebuah organisasi yang bergerak dalam layanan jasa komunikasi data, dapat menerapkan *VPN* berbasis teknologi *MPLS* dalam mendukung kegiatan operasionalnya dan juga sebagai salah satu jasa yang ditawarkan dengan nama *VPN* Multi Service.

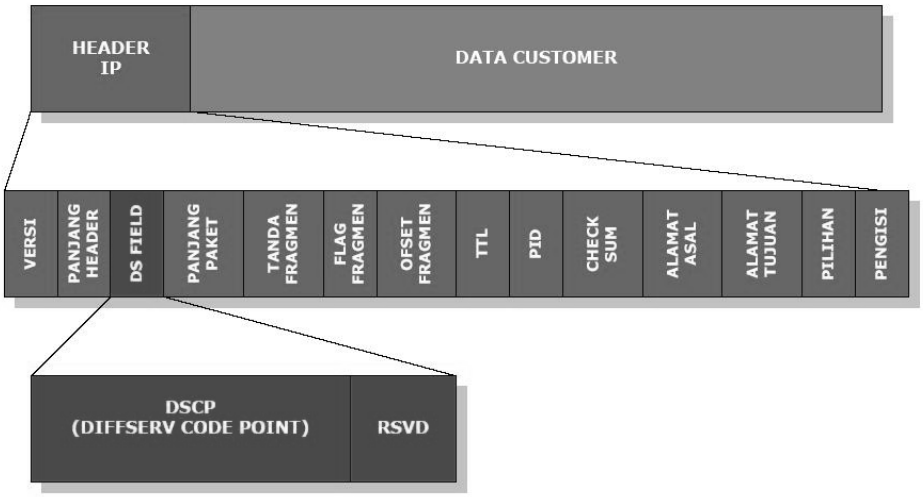
Gagasan *Virtual Private Network (VPN)* atau jaringan swasta maya cukup sederhana. Agar jaringan pribadi yang terdistribusi dapat saling berkomunikasi secara aman melalui jaringan umum seperti internet, dibutuhkan pengamanan data terhadap pencurian. Sebuah sistem *VPN* mengatasi masalah ini dengan menciptakan suatu Jaringan Pribadi Virtual (*Virtual Private Network*) sehingga *remote user* (pengguna jarak jauh) yang menjadi anggota jaringan pribadi virtual tersebut dapat berkomunikasi secara bebas dan aman melalui jaringan umum.

Dengan kata lain, *VPN* adalah suatu jaringan pribadi yang memanfaatkan infrakstruktur jaringan publik (internet). *VPN* hanya dapat digunakan oleh satu organisasi tertentu. Saat ini terdapat tiga jenis *VPN*, yaitu *VPN* akses, *VPN* intranet, dan *VPN* ekstranet. Masing-masing jenis *VPN* ini memenuhi berbagai kebutuhan bisnis. Untuk keamanan *VPN* harus ada otorisasi pengguna, otentikasi, dan enkripsi data. Otentikasi awal digunakan untuk memverifikasi pengguna/*router* dan mengijinkan dilakukan tindakan tertentu serta menolak tindakan yang lain. *Tunneling VPN* biasanya dapat memberikan perlindungan yang cukup tetapi ada beberapa lalu lintas yang memerlukan enkripsi IPSec adalah standar *IETF (Internet Engineering Task Force)* yang memberikan enkripsi 56/128/256-bit. Manejer usaha atau penyedia layanan biasanya bertanggung jawab dalam pengelolaan layanan *VPN*. Mereka menerapkan keamanan dan QoS di seluruh jaringan. Mereka juga mengelola autentikasi, otorisasi, dan akunting sistemnya.
MPLS merupakan arsitektur jaringan yang didefinisikan oleh *Internet Engineering Task Force (IETF)* untuk memadukan mekanisme *label swapping* di *layer* dua dengan *routing* di *layer* tiga untuk mempercepat pengiriman paket. Arsitektur *MPLS* didefinisikan dalam RFC-3031 (Rosen 2001).



Gambar 2 Arsitektur MPLS (RFC-3031, Rosen 2001)

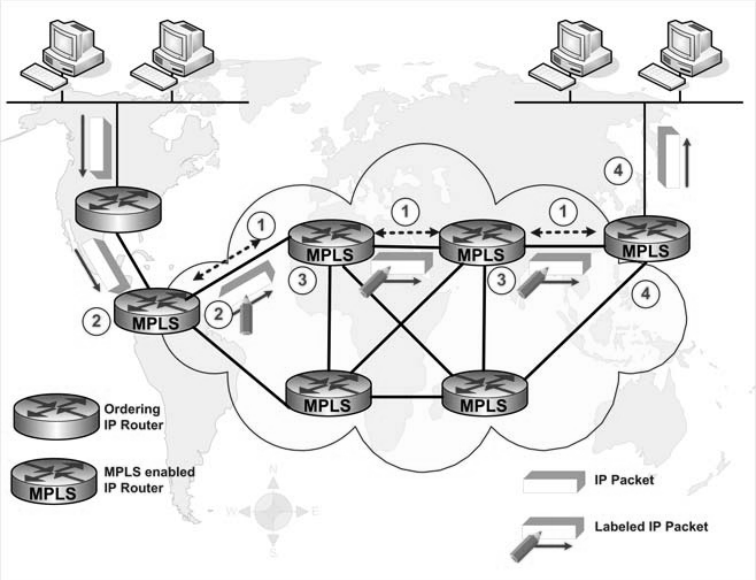
Untuk membangun jaringan lengkap dengan implementasi QoS dari ujung ke ujung, diperlukan penggabungan dua teknologi, yaitu implementasi QoS di *access network* dan QoS di *core network*. Seperti telah dipaparkan, QoS di *core network* akan tercapai secara optimal menggunakan teknologi *MPLS*. Ada beberapa alternatif untuk implementasi QoS di access network yang sangat tergantung pada jenis aplikasi yang digunakan pelanggan.



Gambar 3 *Diferensiasi Layanan DiffServ (RFC-2475)*

MPLS memberikan mekanisme yang efektif untuk mendukung *VPN*. Teknologi *MPLS* memberikan kemampuan untuk memisah-misahkan lalu lintas dari berbagai *VPN*. Selain itu, dengan dibuatnya *tunnel* (saluran atau terowongan), akan terbentuk topologi virtual. Satu lagi keuntungan dari *MPLS* sebagai teknologi *tunnel VPN* adalah *Traffic Engineering MPLS* dapat memberikan sumber daya kepada *LSR*. Keamanan *tunnel VPN* yang menggunakan *MPLS* sama seperti yang diberikan oleh ATM/*Frame-Relay* PVC.

Jaringan *MPLS* terdiri dari rangkaian node yang dapat men-switch dan men-*route* berdasarkan label yang dipasang pada setiap paket. Domain *MPLS* terdiri dari serangkaian node *MPLS* yang saling berhubungan. Node itu disebut *Label Switched Router (LSR)*. Label menentukan aliran paket diantara kedua *end point* (titik akhir). Jalur khusus melalui jaringan *LSR* untuk setiap alirannya yang disebut *Forwarding Equivalence Class (FEC)* telah ditentukan. *MPLS* adalah teknologi yang berorientasi sambungan. Setiap *FEC* memiliki karakterisasi lalu lintasnya yang menentukan persyaratan QoS untuk aliran tersebut. Karena *LSR* mengirim paket yang didasarkan pada nilai label, maka proses pengirimannya lebih sederhana daripada dengan router IP.



Gambar 4 Operasi MPLS

Pada dasarnya, *MPLS* muncul sebagai teknologi inti untuk *next-generation networks (NGN)*, pada jaringan optik tertentu. *MPLS* juga menyediakan fleksibilitas solusi *VPN* berdasarkan penggunaan tunnel *LSR* untuk enkapsulasi data *VPN*. Salah satu fitur *MPLS* adalah kemampuan membentuk *tunnel* atau *virtual circuit* yang melintasi *network*-nya. Kemampuan itu membuat *MPLS* berfungsi sebagai platform alami untuk membangun *virtual private network (VPN)*.

VPN yang dibangun dengan teknologi *MPLS* sangat berbeda dengan *VPN* yang hanya dibangun berdasarkan teknologi IP yang hanya memanfaatkan enkripsi data. *VPN* yang dibangun dengan *MPLS* lebih menyerupai *virtual circuit* dari *Frame Relay* atau ATM, yang dibangun dengan membentuk isolasi trafik. Dalam *VPN-MPLS*, suatu *VPN* umumnya terdiri dari kumpulan situs yang terkoneksi dengan jaringan inti penyedia jasa *MPLS*. *VPN* berbasis *MPLS* dibuat pada layer 3 dan didasari dari model *peer* dan dapat menjadikannya lebih *scalable* dan lebih mudah untuk dikembangkan dan dikendalikan daripada *VPN* konvensional. Terdapat nilai tambah dalam layanan *VPN-MPLS,* seperti aplikasi dan *data hosting*, *network commerce*, dan layanan telepon dapat dengan mudah dicapai dan disebarkan ke *VPN-MPLS* tertentu karena jaringan *backbone* penyedia jasa mengakui setiap *VPN-MPLS* sebagai jaringan IP yang aman dan *connectionless*.

Model *VPN-MPLS* merupakan model *VPN peer* yang dapat melaksanakan pemisahan trafik dengan memberikan *VPN* Route Forwarding Table (VRFs) yang unik kepada setiap pengguna *VPN*. Dengan itu pengguna pada *VPN* tertentu tidak dapat melihat trafik lain yang berada di luar *VPN* mereka.

Para pelanggan mengharapkan data *VPN* tetap terjaga kerahasiaannya, termasuk topologi dan skema pengalamatan untuk jaringan mereka sama baiknya ketika data dibawa melalui *VPN*. *MPLS* menyebabkan keuntungan keamanan IP serupa dengan layer 2 VCs. Maksudnya adalah peralatan pelanggan yang terkoneksi ke *VPN* tidak perlu memerlukan IPSEC atau perangkat lunak kriptografi lain. Keamanan *VPN MPLS* dapat dijelaskan sebagai berikut. Pertama, pada titik mula router penyedia jasa, seluruh data untuk *VPN* diberikan label stak yang unik ke *VPN* tujuan. Pemberian label ini untuk memastikan data dikirim hanya ke tujuan tersebut sehingga data tidak keluar dari lingkungan *VPN*. Kedua, paket yang masuk ke jaringan penyedia jasa, baik yang dikirim tanpa menggunakan *MPLS* maupun diberikan label stak yang berbeda sehingga *malicious third-party* tidak dapat memasukkan data ke dalam *VPN* dari luar jaringan penyedia jasa.

Ketiga, *router* penyedia jasa dapat menggunakan *Cryptographic Algorithm MD5* atau teknik yang serupa untuk mencegah label palsu yang masuk. Ada dua kondisi ketika pelanggan membutuhkan penggunaan kriptografi, bahkan ketika menggunakan *VPN MPLS*. Keempat, jika data pelanggan dianggap cukup peka maka harus dicegah dari pengintaian (*snooping*), bahkan dari jaringan penyedia jasa, IPSEC, atau teknik kriptografi yang serupa harus digunakan pada data *VPN* sebelum data tersebut masuk ke dalam jaringan penyedia jasa. Dalam kasus ini, pelanggan bertanggung jawab atas mendistribusi kunci kriptografi. Kelima, ketika *VPN* disediakan oleh lebih dari satu penyedia jasa, para penyedia jasa dapat memilih untuk menggunakan *tunnel* berbasis IPSEC untuk membawa trafik *VPN* antara jaringan mereka pada jaringan IP publik jika koneksi *MPLS* antara penyedia jasa tidak ada. Dalam kasus ini, para penyedia jasa bertanggung jawab atas pendistribusian kunci kriptografi.

Untuk perusahaan yang bergerak dalam layanan jasa komunikasi data terbesar, harus selalu tanggap terhadap teknologi yang berkembang (*up to date*) dengan telah menerapkan teknologi *MPLS* dalam produk layanan yang ditawarkan. Layanan *Virtual Private Network MultiService* (VPN MultiService) adalah layanan satu paket solusi komunikasi data yang memberikan layanan sampai ke *end user* berbasis IP menggunakan jaringan *MPLS (Multi Protocol Label Switch)* yang aman untuk hubungan *Wide Area Network* (WAN).

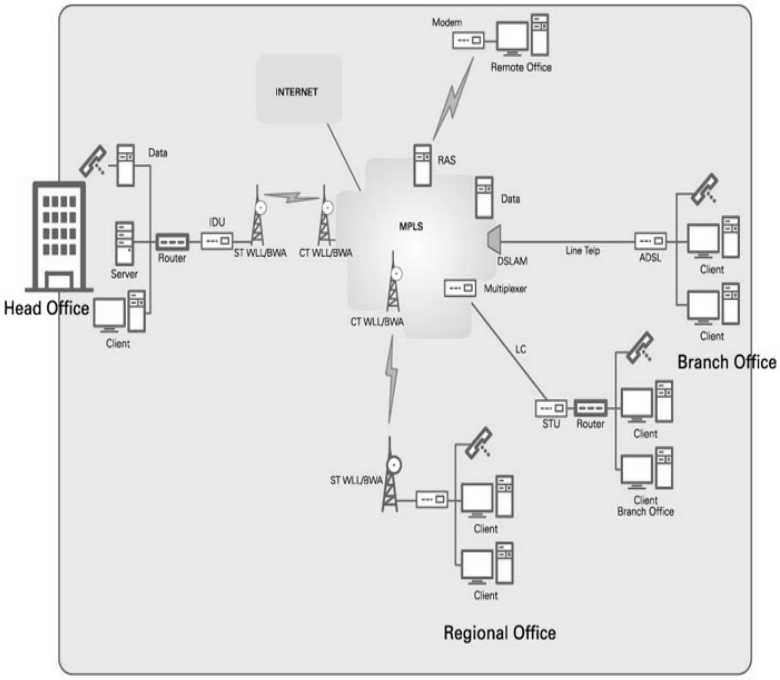
Jaringan *sharing MPLS* memadukan kemampuan *label swapping* dengan *layer network routing* untuk membentuk *private network* yang aman dan cepat dalam pengiriman paket informasi. Dengan arsitektur jaringan tersebut menjadikan biaya jaringan lebih kompetitif sebagai alternatif solusi jaringan komunikasi WAN *private*.

Sesuai dengan tujuan awalnya, *MPLS* dikembangkan untuk mempercepat proses pengiriman data. *MPLS* juga menyediakan fleksibilitas solusi *VPN* berdasarkan penggunaan tunnel *LSR* untuk enkapsulasi data *VPN*. Frame Relay merupakan koneksi *point-to-point* menggunakan *Permanent Virtual Circuit (PVC)*, yaitu saluran virtual yang dibuat secara manual menjadikan hubungan permanen antara pengirim dan penerima. Oleh karena itu, apabila dalam suatu jaringan pengirim akan mengirim data ke penerima

namun koneksi antara keduanya belum terbina maka harus terlebih dahulu dibuat *PVC*nya. Dan jelas saja pembuatan *PVC* baru ini membutuhkan waktu dan biaya yang tidak sedikit.

Seiring berkembangnya penelitian mengenai teknologi *MPLS* dan penetapan standarisasi teknologi *MPLS* oleh *IETF*, perusahaan yang bergerak dalam layanan jasa komunikasi data dapat memulai dengan menerapkan penggunaan teknologi *MPLS* dalam layanan jasa yang ditawarkan. Penggunaan teknologi *MPLS* ini sebagai teknologi pendukung jaringan *VPN* yang dibangun. Dibanding dengan teknologi *Frame Relay*, penggunaan teknologi *MPLS* pada *VPN* memiliki beberapa keuntungan, diantaranya adalah kemampuan koneksi *any-to-any*. Dengan koneksi *any-to-any*, waktu pengiriman data menjadi lebih cepat. Selain itu, biaya yang dikeluarkan, baik oleh penyedia jasa maupun pelanggan menjadi lebih sedikit.

Kemampuan *MPLS* yang mampu membuat *LSR* untuk menghubungkan node satu dengan yang lainnya juga menjadi nilai lebih penggunaan teknologi *MPLS* pada *VPN* yang memanfaatkan jaringan publik IP. Pengiriman data yang melalui *VPN* digolongkan atas prioritasnya. Oleh karena itu, dalam layanan *VPN Multiservice* diberlakukan penggunaan *Class of Service* dan juga *Quality of Service*. Tingkat keamanan yang ada pada *VPN Multiservice* juga andal, seperti *Frame Relay* atau ATM. Dengan pengggunaan IPSec dan kriptografi, pengiriman data melalui jaringan *VPN* akan dijaga kerahasiaan dan keamanannya pihak yang tidak bertanggung jawab.



Gambar 5 Konfigurasi Jaringan Layanan VPN *MultiService*

PENUTUP

Dari uraian yang telah dipaparkan, dapat diambil beberapa simpulan sebagai berikut. Teknologi *MPLS* memberikan keuntungan bagi perusahaan penyedia layanan, seperti skalabilitas *routing* dan *forwarding*, kemampuan manajemen jaringan, keamanan yang andal dan memberikan kapabilitas *traffic engineering* untuk pengadaan jaringan yang lebih baik. Teknologi *MPLS* merupakan pilihan yang sangat bagus untuk menyediakan layanan *VPN* yang andal. Jaringan VPN-IP berbasis teknologi *MPLS* memberikan konektivitas *any-to-any* dan setiap *client* dapat terkoneksi antara satu dengan yang lainnya.

Dari beberapa hal yang didapatkan di lapangan, terdapat implikasi sebagai berikut: Meskipun layanan *VPN MultiService* telah berjalan dengan baik, adakalanya jaringan *VPN MultiService* mengalami gangguan; Untuk mengatasi masalah gangguan tersebut, diperlukan *maintenance,* baik pada fisik jaringan maupun pada manajemen jaringan *VPN* MultiService; Hingga saat ini belum terbentuk dukungan *MPLS* untuk trafik non IP. Untuk kedepannya, jaringan *VPN* MultiService dapat dikembangkan menjadi Layer 2 *MPLS*; Saat ini, sedang dikaji/dikembangkan *Generalised MPLS (GMPLS)*, yaitu penggunaan konsep label untuk jaringan optik dan panjang gelombang (λ) digunakan sebagai label.

DAFTAR PUSTAKA

Hutapea, Tommy P.M. 2003. Artikel Populer Ilmukomputer.com.

Kristianto, Andi. 2003. *Jaringan Komputer*. Graha Ilmu. Jakarta.

Nazir, Mochamad. 2003. *Metode Penelitian*. Jakarta: Ghalia.

Rosen, Eric., et al. 2001. "Multiprotocol Label Switching Architecture," RFC 3031 IETF. http://www.ietf.org/rfc/3031.txt

Wijaya, Hendra. 2004. *Belajar Sendiri Cisco Router (Edisi Baru untuk Mengambil Sertifikat CCNA (640-8010)*. Jakarta: PT Elex Media Komputindo.

Wastuwibowo, Kuncoro. 2003. "Jaringan MPLS," Diakses dari http://telkom.info/artikel/mpls-overview.pdf