IMPLEMENTASI VIRTUAL PRIVATE NETWORK - WAN DALAM DUNIA BISNIS

Erma Suryani, Syamsu Nur Row Honey
Program Studi Sistem Infomasi,
Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember
Kampus ITS, Jl. Raya ITS, Sukolilo – Surabaya 60111, Telp. + 62 31 5939214, Fax. + 62 31 5913804
E-mail: erma@its-sby.edu

ABSTRAK

Dalam dunia bisnis, biasanya sebuah organisasi ingin membangun Wide Area Network (WAN) untuk menghubungkan beberapa kantor cabangnya. Sebelum munculnya Virtual Private Network (VPN), mereka umumnya menggunakan " leased line" yang mahal sehingga hanya perusahaan besar yang dapat memilikinya.

VPN - WAN memberi solusi alternatif karena dapat mengurangi biaya pembuatan infrastruktur jaringan dan memotong biaya operasional dengan memanfaatkan failitas internet sebagai media komunikasinya. Perusahaan cukup menghubungi Internet Service Provider (ISP) terdekat untuk mendapatkan layanan ini.Setiap paket informasi yang dikirim dapat diakses, diawasi atau bahkan dimanipulasi oleh pengguna. Supaya komunikasi berjalan aman maka diperlukan protokol tambahan khusus yang dirancang untuk mengamankan data yang dikirim. Dewasa ini sudah banyak perusahaan seperti : perusahaan manufaktur, distribusi dan retail; pertambangan minyak dan gas, telekomunikasi, finansial, pemerintahan serta industri transportasi yang menggunakan VPN karena fasilitas –fasilitas yang ditawarkan berupa remote access client, internetworking LAN to LAN serta akses yang terkontrol dengan biaya yang murah. Uji coba yang dilakukan Miercom(LAB penyedia testing kinerja perangkat keras) terhadap Cisco 1841 membuktikan bahwa Cisco 1841 dapat menopang suatu komunikasi dua arah, interkoneksi IP WAN kapasitas E1 dengan enkripsi 3DES yang dapat menunjang throughput sampai dengan 2 Mbps dalam koneksi E1 IP-WAN.

Penggunaan VPN akan meningkatkan efektivitas, efisiensi kerja serta skalabilitas perusahaan. Keuntungan lain yang didapat dari VPN adalah pada biaya pulsa yang jauh lebih murah dibandingkan dengan menggunakan" leased line".

Kata Kunci: *VPN, WAN, paket informasi, ISP, remote access client, skalabilitas.*

1. PENDAHULUAN

Dewasa ini dalam kehidupan dunia yang semakin maju di segala bidang termasuk pula perkembangan teknologi yang sangat pesat dan berdampak pada kehidupan peradaban dunia saat ini. Semua saling berlomba untuk mengembangkan diri untuk mencapai perkembangan hasil yang semakin baik dari hari ke hari.

Perkembangan yang pesat dalam bidang Teknologi Informasi baik dalam bidang sistem manajemen, sistem ketenagakerjaan maupun dalam bidang komputerisasi, menyebabkan munculnya banyak peralatan dengan menggunakan prinsip dasar pengiriman data dengan piranti yang tentu saja semakin kreatif dan inovatif disesuaikan dengan kebutuhan zaman. Hal inilah yang menyebabkan pemerintah maupun swasta mulai mengembangkan pengetahuan tentang komunikasi data dengan menggunakan jaringan baik menggunakan kabel maupun tanpa kebel.

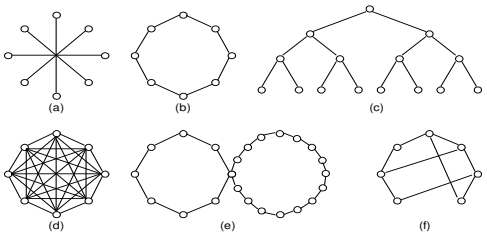
WAN merupakan salah satu jenis jaringan yang mempunyai jangkauan jaringan yang luas dan sangat cepat karena menggunakan media transmisi salelit, maupun telepon. Karena teknologi WAN yang sudah modern, maka banyak hal-hal yang harus dipelajari dan dimengerti, sehingga permasalahan yang dihadapi diantaranya adalah:

1. Bagaimana mengimplementasikan WAN di dunia bisnis
2. Bagaimana melakukan setting terhadap WAN

2. WIDE AREA NETWORK

Wide Area Network (WAN) merupakan jaringan komputer yang saling berjauhan dan mencakup daerah geografis yang luas, seringkali mencakup sebuah negara atau benua. Dalam melaksanakan koneksinya WAN seringkali menggunakan satelit sebagai media perantara, akan tetapi WAN juga bisa menggunakan koneksi antar router yang biasa disebut dengan *point-to-poin.*

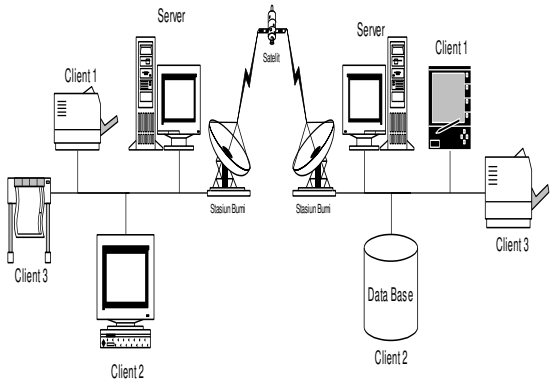
Pada subnet *point-to-point*, masalah rancangan yang penting adalah pemilihan jenis topologi interkoneksi router (Cisco, 2004). Gambar 1 menunjukkan beberapa jenis topologi WAN.



(a)Bintang (b)Cincin (c)Pohon (d)Lengkap (e)Cincin berinteraksi (f)Sembarang.

Gambar 1 Jenis – Jenis Topologi Subnet Point-to-Point

Sedangkan skema WAN dapat dilihat pada gambar 2.



Gambar 2 Skema WAN

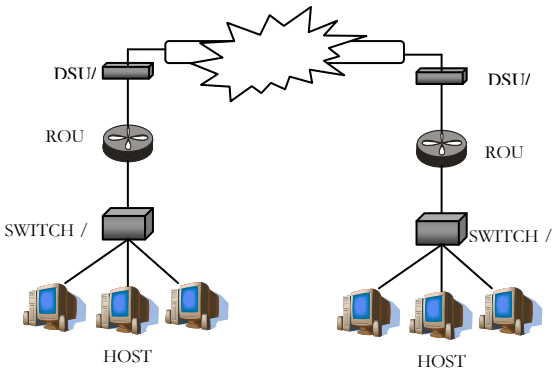
Ditinjau dari segi koneksitasnya WAN memiliki beberapa jenis koneksi dengan karakteristik tertentu. Jenis dan karakteristik WAN dapat dilihat pada tabel 1.

Tabel 1 Jenis Koneksi WAN dan Karakteristiknya

Jenis	Karakteristik
Protokol X.25	menggunakan packed swiching yaitu memecah-mecah pesan yang panjang menjadi kecil-kecil sebelum data dikirim
Frame Relay	lalu lintas data tidak membebani prosesor
Integrated Service Digital Network (ISDN)	1. Menggunakan jaringan digital. 2. menggunakan bandwidth dua buah jalur 64 Kbps untuk komunikasi keluar dan masuk
Broadband ISDN	Sama dengan ISDN
Asynchronous Transfer Mode (ATM)	seperti halnya X.25 dan Frame Relay, yaitu memecah-mecah pesan yang panjang menjadi kecil-kecil sebelum data dikirim, tapi tidak membebani prosesor

3. IMPLEMENTASI WAN

Sering kali kita menyebut komputer client sebagai host. Host dihubungkan dengan sebuah subnet komunikasi, atau cukup disebut subnet. Tugas subnet adalah membawa pesan dari host ke host lainnya, seperti halnya sistem telepon yang membawa isi pembicaraan dari pembicara ke pendengar. Dengan memisahkan aspek komunikasi murni sebuah jaringan (subnet) dari aspek-aspek aplikasi (host), rancangan jaringan lengkap menjadi jauh lebih sederhana. Untuk lebih jelasnya bagaimana cara kerja WAN dapat dilihat pada gambar 3 (Cisco, 2004).

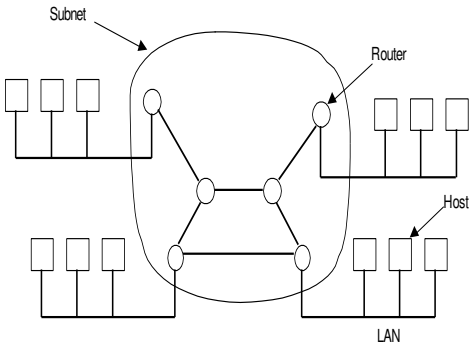


Gambar 3 Cara Kerja WAN

Pada sebagian besar WAN, subnet terdiri dari dua komponen, yaitu kabel transmisi dan elemen switching. Kabel transmisi (disebut juga sirkuit, channel, atau trunk) memindahkan bit-bit dari satu mesin ke mesin lainnya.

Element *switching* adalah komputer khusus yang dipakai untuk menghubungkan dua kabel transmisi atau lebih. Saat data sampai ke kabel penerima, element switching harus memilih kabel pengirim untuk meneruskan pesan-pesan tersebut. Jenis - jenisnya sangat bervariasi diantaranya yaitu *packet switching node*, *intermidiate system*, serta *data switching exchange*.

Setiap host dihubungkan ke LAN tempat dimana terdapat sebuah *router* (komputer *switching*) seperti ditunjukkan dalam gambar 4. Dalam beberapa keadaan tertentu sebuah host dapat dihubungkan langsung ke sebuah router. Kumpulan saluran komunikasi dan router akan membentuk subnet.



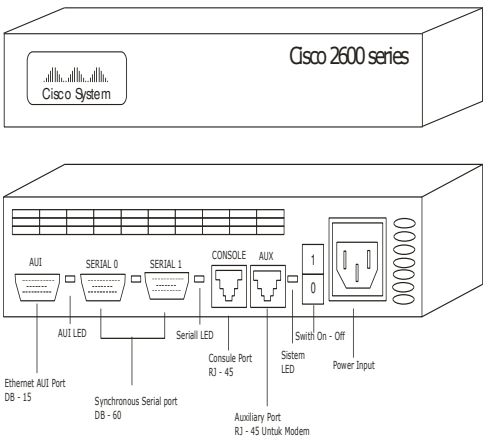
Gambar 4 Hubungan antara Host-Host dengan Subnet

Pada sebagian besar WAN, jaringan terdiri dari sejumlah banyak kabel atau saluran telepon yang menghubungkan sepasang router. Bila dua router yang tidak mengandung kabel yang sama akan melakukan komunikasi, keduanya harus berkomunikasi secara tak langsung melalui router lainnya. Ketika sebuah paket dikirimkan dari sebuah router ke router lainnya melalui router perantara atau lebih, maka paket akan diterima router dalam keadaan lengkap, disimpan sampai saluran output menjadi bebas, dan kemudian baru diteruskan.

Subnet yang mengandung prinsip seperti ini disebut subnet *point-to-point, store-and-forward*, atau *packet-switched*. Hampir semua WAN (kecuali yang menggunakan satelit) memiliki subnet *store-and-forward*.

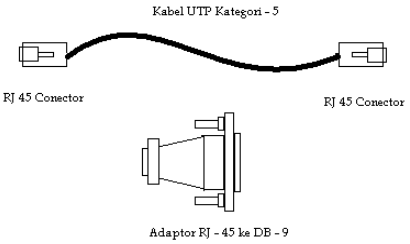
4. SETTING WAN DENGAN VPN

VPN (Virtual Private Network) merupakan salah satu jaringan WAN yang memiliki jalur khusus (diberikan langsung oleh Telkom), sehingga proses komunikasinya lebih cepat. Untuk dapat mengakses router Cisco diperlukan *console port* dengan perantaraan suatu terminal atau komputer (Cisco, 2004). Dari gambar 5 dapat dilihat tampak depan dan belakang router.



Gambar 5 Router dari depan dan belakang

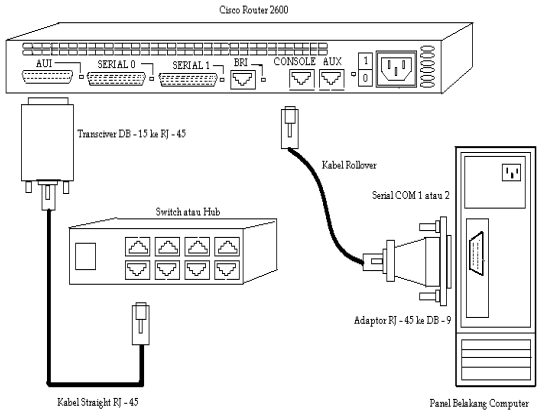
Untuk menghubungkan Cisco router kesuatu terminal atau komputer, diperlukan kabel rollover seperti tampak pada gambar 6 dan adaptor RJ-45 ke DB-9 yang biasanya disertakan dengan peralatan router tersebut.



Gambar 6 Kabel rollover & adaptor RJ-45 ke DB-9

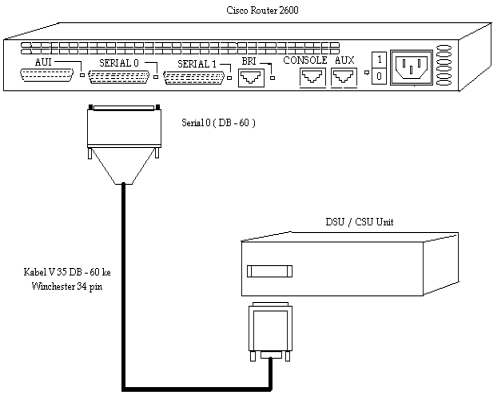
Kabel rollover ini dihubungkan dari console port router ke serial port COM 1 atau COM 2 komputer seperti pada gambar 7. Jika serial port computer menggunakan konektor DB-9 atau DB-25, maka diperlukan adaptor RJ-45 ke DB-9 atau DB-25 yang sesuai.

Untuk menghubungkan router ke switch atau hub pada suatu jaringan, diperlukan kabel UTP kategori 5, dimana koneksi TJ-45 pada switch atau hub sedangkan ke routernya dikoneksikan ke AUI port menggukan adaptor transceiver AUI DB-15 ke 10BaseT RJ-45. Perlu diperhatikan bahwa kabel UTP yang digunakan adalah jenis Straight.



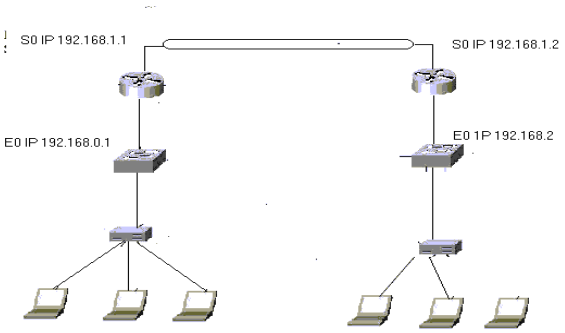
Gambar 7 Koneksi Router ke Komputer dan Router ke Switch/Hub

Sedangkan untuk koneksi dari modem (DSU/CSU) ke router menggunakan kabel V 35 DB-60 ke Winchester 34 Pin, yang dihubungkan ke SERIAL 0 (DB-60).



Gambar 8 Koneksi Modem (DSU / CSU) ke Router

Disain WAN dengan VPN – IP dapat dilihat pada gambar 9



Gambar 9 Disain WAN dengan VPN IP

5. SEKURITAS DAN PROTOKOL VPN

Teknologi VPN didasarkan pada strategi *tunneling*. *Tunneling* menyertakan paket enkapsulasi yang dikonstruksi dalam sebuah format protokol dasar dalam beberapa protokol lainnya (Cisco, 2004). Dalam kasus dimana VPN berjalan melewati Internet, paket dalam satu dari beberapa format protokol VPN dienkapsulasi dalam paket IP.

Sekuritas VPN

Kebanyakan teknologi VPN mengimplementasikan enkripsi yang baik, sehingga data tidak dapat dilihat langsung melalui network sniffer (Cisco, 2004). VPN kemungkinan lebih rentan pada serangan '*man in the middle*', yang mencegat sesi dan berkedok dari client atau server. Sebagai tambahan, beberapa data pribadi tidak dapat dienkripsi VPN sebelum ditransmisikan pada public wire.

Protokol-Protokol VPN

Beberapa protokol network yang menarik telah diimplementasikan untuk penggunaan VPN. Protokol-protokol ini mencoba untuk menutup beberapa hole sekuritas bawaan dalam VPN. Protokol-protokol ini pun melanjutkan untuk bersaing dengan lainnya dalam hal penerimaan dunia industri. Beberapa protokol network mulai populer sebagai efek pengembangan VPN diantaranya adalah:

1. PPTP (Point-to-point Tunneling Protocol)
2. L2TP (Layer Two Tunneling Protocol)
3. IPsec (Internet Protocol Security)
4. SOCKS Network Security Protocol

- **Point-to-point Tunneling Protocol (PPTP)**
  PPTP adalah spesifikasi protokol yang dikembangkan oleh beberapa perusahaan. Orang-orang pada umumnya mengasosiasikan PPTP dengan Microsoft karena hampir semua selera Windows memasukkan built-in support untuk protokol ini. Keluaran awal dari PPTP for Windows oleh Microsoft memiliki fitur sekuritas dimana beberapa expert mengklaim terlalu lemah untuk penggunaan yang serius. Microsoft pun terus meningkatkan dukungan PPTP-nya. Kekuatan utama PPTP adalah kemampuannya dalam mendukung protokol non-IP. Kekurangan utama dari PPTP adalah kesalahannya memilih sebuah standar tunggal untuk enkripsi dan autentikasi. Dua produk yang keduanya benar-benar sesuai dengan spesifikasi PPTP dapat secara total incompatible dengan lainnya jika mereka mengenkrip data yang berbeda.

- **Layer Two Tunneling Protocol (L2TP)**
  L2TP muncul pada layer data link (layer 2), dalam model OSI. Seperti PPTP, L2TP juga mendukung client non-IP. L2TP mendukung VPN yang tidak berbasiskan Internet termasuk frame relay, ATM, dan SONET.

- **Internet Protocol Security (IPsec)**
  IPsec merupakan protokol VPN yang lengkap, atau dapat digunakan secara sederhana sebagai skema enkripsi dalam L2TP atau PPTP. IPsec muncul pada layer network (layer 3) dari OSI. IPsec memperluas standar IP untuk tujuan mendukung layanan berbasis internet yang lebih aman (termasuk, tidak dibatasi hanya untuk VPN). IPsec secara spesifikasi memproteksi serangan 'man in the middle' dengan menyembunyikan alamat IP yang kemungkinan akan muncul di kabel.

- **SOCKS Network Security Protocol**
  Sistem SOCK menyediakan sebuah alternatif unik ke protokol VPN lainnya. Fungsi SOCKS pada layer session (layer 5) dalam OSI, membandingkan semua protokol VPN lainnya

yang bekerja pada layer 2 atau 3. Implementasi ini menawarkan keuntungan sekaligus kerugian melalui pilihan-pilihan protokol lainnya tersebut. Fungsi pada level yang lebih tinggi, SOCKS mengizinkan administrator untuk membatasi trafik VPN untuk aplikasi tertentu saja. Untuk menggunakan SOCKS, administrator harus mengkonfigurasikan SOCKS proxy server dalam lingkungan client seperti software SOCKS pada client itu sendiri.

Protokol-protokol di atas menekankan autentikasi dan enkripsi dalam VPN. Autentikasi mengizinkan client VPN dan server untuk membangun identitas orang-orang dalam jaringan dengan benar. Enkripsi mengizinkan data yang bersifat sensitif untuk disembunyikan dari publik. Banyak vendor telah mengembangkan hardware VPN dan softwarenya. Namun sayangnya, standar VPN yang belum matang membuat beberapa produk tersebut saling tidak kompatibel.

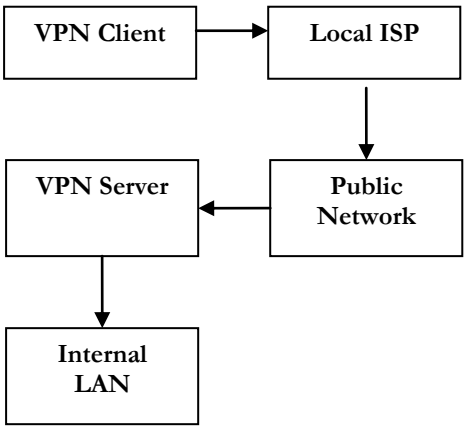
6. FASILITAS – FASILITAS VPN

VPN menyediakan konektivitas network melewati jarak fisik yang jauh. Kunci utama dari VPN, adalah pada kemampuannya menggunakan jaringan publik seperti Internet seperti layaknya kita mempercayai *leased line private* kita. Teknologi VPN mengimplementasikan akses terbatas ke dalam jaringan yang menggunakan *cabling* dan *router* yang sama seperti yang dimiliki sebuah jaringan publik, tanpa mengurangi fitur atau sekuritas dasarnya. VPN mendukung sekurangnya tiga mode penggunaan yang berbeda, yakni :

1. Koneksi *remote access client*
2. Internetworking LAN-to-LAN
3. Akses yang terkontrol dalam sebuah intranet

VPN untuk Remote Access

VPN dapat mensupport layanan *remote access*. Dalam beberapa tahun terakhir, banyak perusahaan telah meningkatkan mobilitas karyawan mereka dengan mengizinkan para karyawan untuk melakukan *telecommuting*.
Karyawan dapat menghubungi ke server akses remote kantor mereka menggunakan nomor khusus (*local number*). *Overhead* pemeliharaan sistem ini secara internal, bergandengan dengan kemungkinan biaya jarak jauh dari si karyawan, sehingga mau tidak mau VPN menjadi sebuah alternatif. Ilustrasi layanan VPN dapat dilihat pada gambar 10 (www.Vel.net, 2004) .



Gambar 10 Ilustrasi Layanan VPN

Diagram ini mengilustrasikan solusi VPN remote access. Sebuah *remote node* (client) yang hendak *log-in* ke dalam kantor VPN akan memanggil local server yang terkoneksi ke *public network*. VPN client akan membangun sebuah koneksi ke server VPN di kantor. Sekali koneksi telah terbangun, remote client dapat berkomunikasi dengan jaringan kantor dengan aman sebagaimana layaknya jaringan publik seakan-akan dia berada dalam internal LAN.

VPN untuk Internetworking

Sebuah ekstensi sederhana dari arsitektur VPN *remote-access* yang disebutkan diatas mengizinkan keseluruhan *remote network* (tidak hanya satu *remote client*) untuk bergabung ke dalam *local network*. Lebih dari sebuah koneksi client-server, sebuah koneksi VPN server-to-server menggabungkan dua jaringan ke dalam intranet.

VPN dibalik Firewall

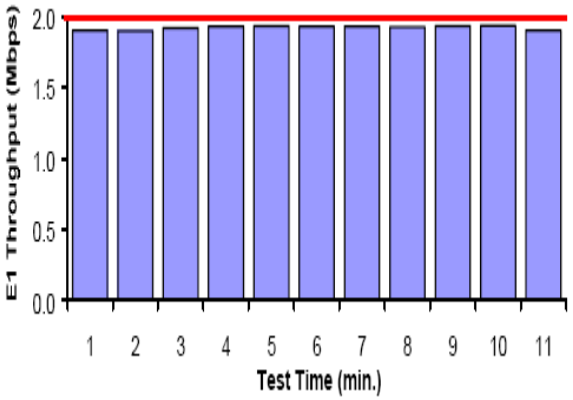
Intranet juga dapat memanfaatkan teknologi VPN untuk mengimplementasikan akses kontrol ke subnet individual pada jaringan private. Pada mode ini, VPN client akan terhubung ke VPN server yang bertindak sebagai sebuah gateway untuk komputer-komputer yang berada di belakangnya pada subnet (www.networkworld.com, 2005). Perlu dicatat bahwa tipe penggunaan VPN ini tidak melibatkan ISP ataupun kabel public network. Namun bagaimanapun, fitur sekuritas dan kenyamanan dari teknologi VPN merupakan sebuah keuntungan.

7. UJICOBA KINERJA VPN-WAN

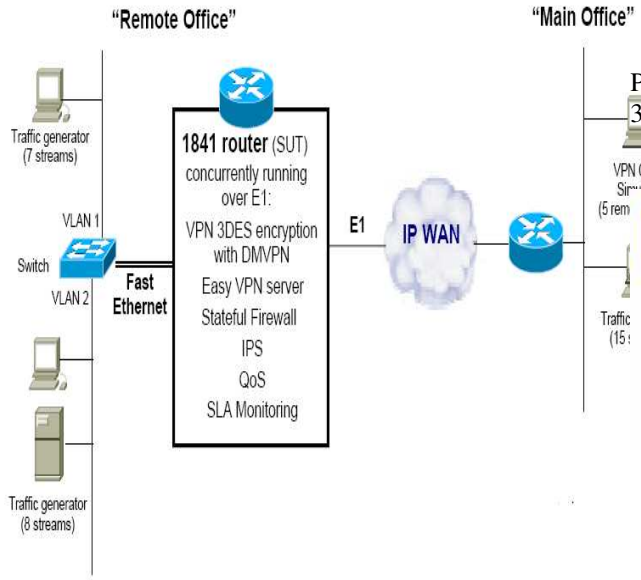
Sistem CISCO menggunakan ISR (Integrated Service Router) 1841 untuk melakukan proses verifikasi konfigurasi secara independent dan proses operasionalnya unjuk mencapai kinerja yang diinginkan. Cisco 1841 merupakan suatu evolusi dari Cisco 1721 router . Cisco 1841 dirancang

untuk berbagai jasa yang meliputi *stateful firewall*, saluran VPN dan enkripsi, serta pencegahan gangguan pada system (Intrusion Prevention System) (Cisco, 2004).

Sebagai bukti verifikasi, saat Cisco 1841 ini berkolaborasi dengan prosesor crypto yang dapat mempercepat akselarasi VPN dengan menggunakan image security IOS, performance enkripsi dapat ditingkatkan menjadi Modul Integrasi Tingkat Tinggi (Advanced Integration Module), sebagaimana diuraikan dalam uji coba berikut.



Gambar 11 E1 Throuput VPN-WAN



Gambar 12 Setup Uji Coba Router Cisco 1841

Setup uji coba dilakukan dengan menghubungkan Cisco 1841 dengan suatu Ethernet 10/100, IEEE 802 yang dapat menopang dua subnet LAN. Router 1841 ini kemudian dihubungkan dengan IPsec VPNtunnel melalui sebuah IP-WAN yang terhubung dengan kantor pusat atau "main office."

Pada uji coba ini, Cisco 1841 menjalankan suatu late-beta versi IOS 12.3(11)T. ***Miercom*** sebagai LAB penyedia testing kinerja perangkat keras membuktikan bahwa, Cisco 1841 dapat menopang suatu komunikasi dua arah, interkoneksi IP WAN kapasitas E1 dengan enkripsi 3DES dengan beban jalur seperti terlihat pada gambar 11. Router ini dirancang untuk menyampaikan layanan data yang aman dengan kecepatan T1/E1. E1 merupakan througput (Mbps) dan T1 merupakan waktu. Dalam pengukuran ini ditemukan bahwa route 1841 dapat menunjang throughput sampai dengan 2 Mbps dalam koneksi E1 IP-WAN. Semua data diklasifikasikan dalam Oos, enskripsi 3DES dan terjamin aman dalam Cisco's Dynamic Multi-point VPN (DMVPN). Dari tabel 2 dapat dilihat konfigurasi modul Cisco 1841.

Proses verifikasi Cisco 1841 dalam proses Enkripsi 3DES dapat dilihat pada tabel 3

Tabel 2 Konfogurasi Modul Cisco 1841

Modules Installed in the 1841 (System Under Test)	
Module	**Description**
HWIC slot 0: WIC-1B-U-V2	ISDN BRI-U-WAN card
HWIC slot 1: VWIC-2MFT-E1-DI (drop and insert)	E1 (2 port) Multi-flex trunk WAN Card
AIM slot 0: AIM-VPN/BPII-PLUS	Advanced Integration Module – VPN hardware encryption module

Tabel 3 Proses Verifikasi Cisco 1841 Dalam Proses Enkripsi 3DES

Concurrent Services Running and Verified on the Cisco 1841 Integrated Services Router While Processing E1 (2 Mbps) load of 3DES-encrypted, IP-WAN Throughput		
Services / Features	**How 1841 supports**	**How Tested/Verified**
QoS processing, DMVPN with 3DES encryption at sustained 2- Mbps rate	Integrated in IOS, optional AIM	Via multiple test systems, link monitors, CLI
Easy VPN server (dynamic, auto-negotiated, remote-client tunnels)	Integrated in IOS; optional AIM VPN hardware encryption module	Remote simulator set-up five dynamic client VPN tunnels
Stateful Firewall	Integrated in IOS	On E1 IP WAN; viewed sessions via CLI
Traffic Statistics, Load Monitoring	Integrated in IOS	Output viewed via CLI during testing
SLA Monitoring	Integrated in IOS	Receiver mode; output viewed via CLI
Routing and QoS	Integrated in IOS	EIGRP traffic routing; CBWFQ, WRED
Inline IPS (Intrusion Prevention)	Integrated in IOS	Over IP WAN; launched ping assault; monitored alarms via CLI

8. INVESTASI VPN

Peluang kembalinya investasi VPN (ROI = *Return On Investment*) lebih cepat dari pada investasi pada *leased line*. Berdasarkan artikel "Delivering Profitable Virtual Private LAN Services - Business Case White Paper" bulan November 2003, telah dilakukan studi kasus pada kota berukuran medium di Amerika Utara. Artikel tersebut menunjukkan bahwa dengan beberapa asumsi parameter yang dilihat pada tabel 2. Dari tabel 4 dapat dilihat VPN dapat mengembalikan nilai investasi dalam 2.1 tahun. Bahkan dengan peningkatan penetrasi pasar dan perubahan kecenderungan pelanggan untuk menyewa *bandwidth* yang besar akan mempercepat jangka waktu ROI, yaitu dalam 1 tahun.

Tabel 4 Perbandingan Parameter ROI

Assumptions Parameter		2.1 Year Payback	1 Year Payback
Market Penetration		12.50%	15%
Year 1 Adoption Rate		4%	8%
# of Sites per Medium Enterprise		5	8
Subscriber BW % of Total Subs by BW	1.5Mbps	5.0 %	5.0 %
	6Mbps	45.0 %	20.0 %
	10Mbps	35.0 %	45.0 %
	45Mbps	10.0 %	10.0 %
	100Mbps	5.0 %	20.0 %

9. PERBANDINGAN BIAYA *LEASED LINE* DAN VPN

Biaya *leased line*

Dengan leased line tarif telepon lokal pukul 00.00-24.00 adalah Rp325 per dua menit. Sedangkan dengan tarif SLJJ, per menit sekitar Rp1.400 per menit pada zona di atas 200 km (Telkom.co.id).

Biaya dengan VPN

Perhitungan VPN Dial dilakukan dengan memperhitungkan jumlah port VPN Dial dan link ke Perusahaan. Untuk perhitungan akses dedicated ke TELKOM dapat digunakan VPN FR atau DINAccess. Untuk hubungan ke luar negeri, hanya dikenakan biaya Rp. 99/6 detik (Rp. 990 / menit) (Telkom.co.id)

10. KEUNTUNGAN DAN KERUGIAN VPN

Beberapa keuntungan yang dapat diperoleh dengan menggunakan VPN diantaranya adalah:

1. Jangkauan jaringan lokal yang dimiliki suatu perusahaan akan menjadi luas, sehingga perusahaan dapat mengembangkan bisnisnya di daerah lain.
2. Waktu yang dibutuhkan untuk menghubungkan jaringan lokal ke tempat lain juga semakin cepat, karena proses instalasi infrastruktur jaringan dilakukan dari perusahaan / kantor cabang yang baru dengan ISP terdekat di daerahnya. Dengan demikian penggunaan VPN secara tidak langsung akan meningkatkan efektivitas dan efisiensi kerja.
3. Penggunaaan VPN dapat memotong biaya operasional bila dibandingkan dengan penggunaan *leased line,* karena VPN menggunakan internet sebagai media komunikasinya (www.Vel.net, 2004). Perusahaan hanya membutuhkan kabel dalam jumlah yang relatif kecil untuk menghubungkan perusahaan tersebut dengan pihak ISP (*internet service provider*) terdekat.
4. Penggunaan VPN akan meningkatkan skalabilitas. Perusahaan yang tumbuh pesat akan membutuhkan kantor cabang baru di beberapa tempat yang terhubung dengan jaringan lokal kantor pusat. Penambahan satu kantor cabang hanya membutuhkan satu jalur, yaitu jalur yang menhubungkan kantor cabang yang baru dengan ISP terdekat. Selanjutnya jalur dari ISP akan terhubung ke internet yang merupakan jaringan global. Dengan demikian penggunaan VPN untuk implementasi WAN akan menyederhanakan topologi jaringannya.
5. VPN memberi kemudahan untuk diakses dari mana saja, karena VPN terhubung ke internet (www.Vel.net, 2004). Sehingga karyawan yang menggunakan *mobile* dapat mengakses jaringan khusus perusahaan di manapun dia berada. Selama dia bisa mendapatkan akses ke internet ke ISP terdekat, karyawan dapat melakukan koneksi dengan jaringan khusus perusahaan. Hal ini tidak dapat dilakukan jika menggunakan *leased line* yang hanya dapat diakses pada terminal tertentu saja.

VPN juga memiliki beberapa kelemahan diantaranya yaitu :

1. VPN membutuhkan perhatian yang serius pada keamanan jaringan publik (internet). Diperlukan tindakan yang tepat untuk mencegah terjadinya hal-hal yang tidak diinginkan seperti penyadapan, *hacking* dan tindakan *cyber crime* pada jaringan VPN.
2. Ketersediaan dan performansi jaringan khusus perusahaan melalui media internet sangat tergantung pada faktor-faktor yang berada di luar kendali pihak perusahaan. Kecepatan dan keandalan transmisi data melalui internet yang digunakan sebagai media komunikasi jaringan VPN tidak dapat diatur oleh pihak pengguna jaringan VPN, karena *traffic* yang terjadi di internet melibatkan semua pihak pengguna internet di seluruh dunia.

3. Perangkat pembangun teknologi jaringan VPN dari beberapa *vendor* yang berbeda ada kemungkinan tidak dapat digunakan secara bersama-sama karena standar yang ada untuk teknologi VPN belum memadai. Oleh karena itu fleksibilitas dalam memilih perangkat yang sesuai dengan kebutuhan dan keuangan perusahaan sangat kurang.
4. VPN harus mampu menampung protokol lain selain IP dan teknologi jaringan internal yang sudah ada.

9. KESIMPULAN

Kesimpulan yang dapat diambil dari implementasi Virtual Private Network – WAN diantaranya adalah:

1. Secara umum hardware yang digunakan dalam mengaplikasikan WAN adalah *workstation, servers, bridge, router, switch, hub.*
2. Router yang saling berkoneksi dan saling mengirim dan menerima dalam satu jaringan atau lebih disebut sistem *point-to-point, store-and-forward*, atau *packet-switched.*
3. Jenis jaringan WAN yang mempunyai kecepatan tinggi adalah VPN, karena menggunakan jalur khusus yang diberikan langsung oleh PT. Telkom berupa IP dengan bandwidth kelipatan 64 mb.
4. Hardware yang digunakan WAN dengan jaringan VPN antara lain Router, Kabel rollove, adaptor RJ-45 ke DB-9, switch / hub, Modem (DSU / CSU)
5. VPN mempunyai fasilitas antara lain
   a. Remote Access
      Melakukan koneksi antara keryawan dengan server kantor yang bertujuan untuk mengetahui data-data yang terjadi dikantor walaupun wilayahnya sangat jauh dan tidak dicapai oleh jatingan *leased line*
   b. Firewall
      Salah satu keamanan yang sangat penting dalam mengamankan data yang ada di perusahaan, karena sistem koneksinya menggunakan satelit maka VPN sangat aman dari jaringan Public
   c. Link Internet.
      Walaupun jaringannya menggunakna jaringan satelit, VPN juga bisa link ke jaringan *leased line* dan bergabung dengan dunia luar.

11. DAFTAR PUSTAKA

1. "Virtual Private Network – Wide Area Network – Managed VPN Solution", www.Vel.net./WAN - Managed-Vpn.solution
2. "Cisco System Inc", 2004 www.Cisco.com/en/US humpgs
3. "Firewall , VPNs, Intrusion Prevention, SSL and IPSec", www.Network World.com/topics/firewall.html
4. "Delivering Profitable Virtual Private LAN Services - Business Case White Paper" , November 2003
5. http:// www.telkom.co.id / produk-layanan layanan/korporat/data-internet/telkomnet-hole-sale-vpn-dial.html