BAB II
TINJAUAN PUSTAKA

1.1. Unit Usaha

1.1.1. Padmanet

Merupakan suatu unit usaha yang bergerak di bidang Informasi dan Teknologi, fungsi utama dari padmanet yaitu memberikan palayanan jasa koneksi internet, intergrasi antar unit dalam bentuk WAN (Wide Area Network), pusat data dan informasi internal, serta pelayanan service kepada masyarakat luas dalam penyediaan teknologi informasi

1.1.2. Dokumen Imigrasi

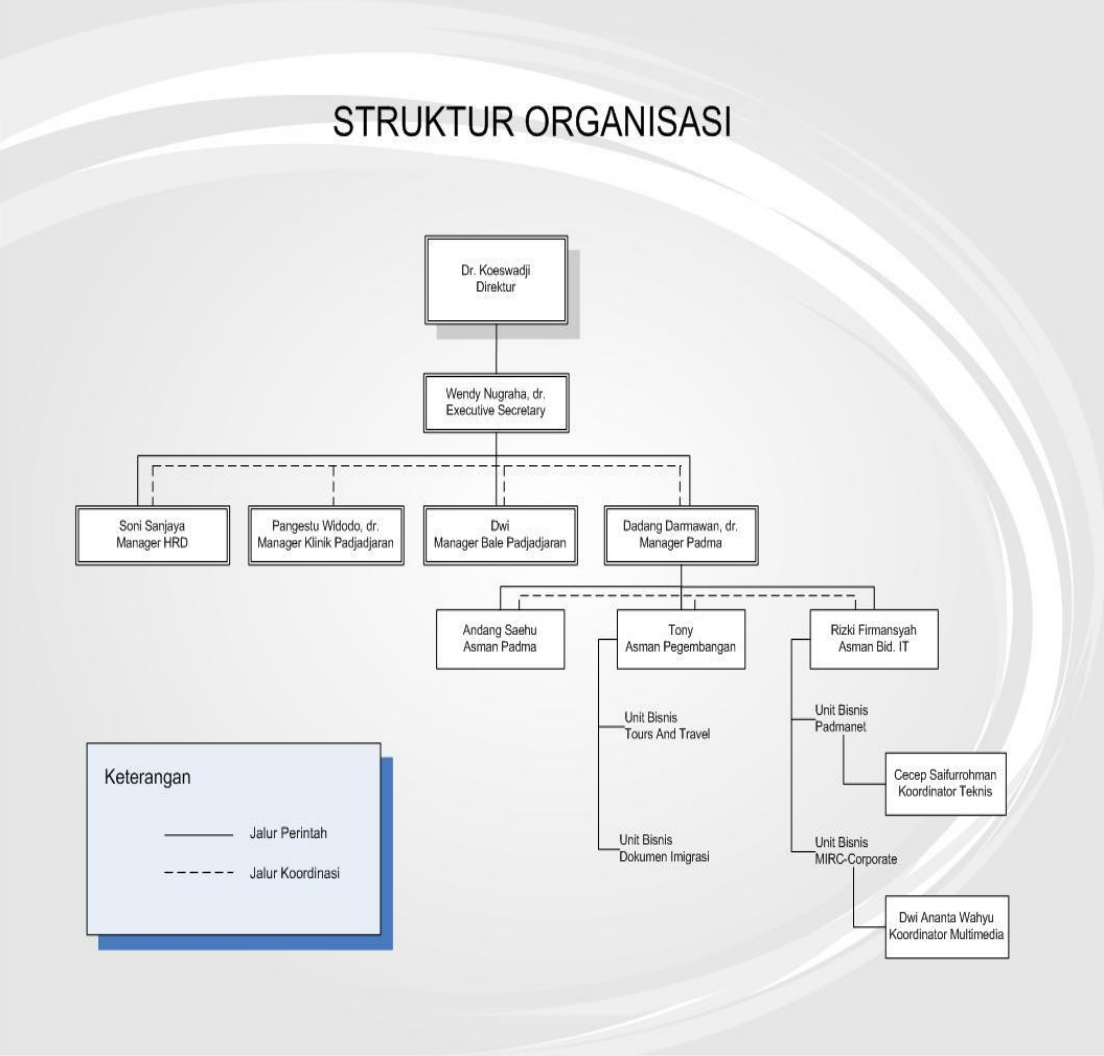
Merupakan unit pelayanan dokumen keimigrasian untuk mahasiswa asing yang belajar di Indonesia dan pelayanan dokumen imigrasi untuk masyarakat luas pada umumnya.

1.1.3. Tours and Travel

Merupakan unit usaha dalam penyediaan keperluan hiburan dan perjalanan wisata lainnya, termasuk juga dalam penyediaan tiket transportasi (darat dan udara) serta pelananan dalam penyediaan hotel.

1.1.4. MIR-C Corporate

Memiliki sumberdaya manusia dengan latar belakang pengalaman bekerja di lingkungan pendidikan kedokteran dan kesehatan, serta tenaga pelaksana yang profesional mulai dari desain, produksi sampai pasca produksi maka dihasilkan produk-produk bernuansa kedokteran yang berkualitas.



Gambar 2.1 Struktur Organisasi

1.1.5. Padjadjaran Mitra Net

PadmaNet adalah bidang usaha yang di bangun sebagai penyedia jasa solusi di bidang Teknologi Informasi bagi anda. Melalui keberadaan kami, kami berusaha memajukan pengetahuan masyarakat akan teknologi informasi dan juga memenuhi kebutuhan yang diiringi oleh permintaan akan hal ini. Sebagai bidang usaha yang memposisikan diri sebagai konsultan, kami menawarkan jasa kami untuk berbagai aspek kebutuhan yang anda butuhkan.

1. Pembangunan Perangkat Lunak

   Sistem terkomputerisasi tidak dapat dipungkiri menawarkan kecepatan dan akurasi data. Bagi anda atau instansi yang membutuhkan aplikasi untuk proses

bisnis, kami menawarkan jasa analisis proses dan pembuatan program yang sesuai dengan kebutuhan anda.

2. Instalasi Jaringan Komputer

   Konsep networking telah terbukti mampu menekan angka investasi suatu proses bisnis. PadmaNet hadir bagi anda yang membutuhkan tenaga ahli untuk menciptakan suatu sistem komputer yang terhubung dalam jaringan (intranet / internet).

Selain menawarkan jasa, melalui sistem support, kami juga berusaha menyediakan media komunikasi dua-arah, yang memfasilitasi antara anda dan kami. Tulisan-tulisan yang ada disini adalah disajikan sebagai informasi bagi anda yang membutuhkan. Karena kami berpikir bahwa peluang yang kami peroleh, sudah sepatutnya dibagikan kepada siapa saja. Dan bukanlah sesuatu yang ekslusif untuk dikonsumsi oleh kalangan tertentu saja.

2.2. Visi Dan Misi Padjadjaran Mitra Net

2.2.1. Visi

Menjadi unit bisnis jasa teknologi informasi terdepan yang terpercaya.

2.2.2. Misi

Menyebarkan dan memberdayakan kemajuan teknologi informasi khususnya dalam kalangan pendidikan dan umumnya kepada masyarakat luas, dengan menciptakan infrastruktur yang kuat dan handal, menyediaan layanan teknologi informasi, dengan pengembangan usaha yang tinggi dan memberikan manfaat dan profitabilitas yang optimal.

Goals Dengan Tujuan membangun Teknologi Informasi Indonesia, PadmaNet memberikan banyak fasilitas dan inovasi untuk memecahkan permasalahan dalam Teknologi Informasi. Fasilitas yang diberikan secara keseluruhan menjadikan PadmaNet sebagai software house dan local provider yang dapat menjadi portal kelancaran usaha anda dengan cara membangun relasi yang baik antara komunitas, client dan PadmaNet.

Produk PadmaNet diantaranya

1. Internet Access

   Akses internet global memungkinkan anda untuk mengaskes internet 24 jam browsing web, email, chat, e-commerce, hotnews dll.

2. IIX Acess

   Akses internet khusus koneksi lokal (Indonesia) solusi paling efisien untuk sharing data dan komunikasi data secara local.

3. Infrastruktur Networking / Jaringan

   Pembangunan infrastruktur network / jaringan bagi perusahaan untuk komunikasi data dengan menggunakan teknologi wireless maupun kabel, dengan installasi server berbasis linux, unix dan freeBSD. Anda juga akan mendapat service berupa maintenace jaringan bila diperlukan. Kami siap untuk membangun jaringan komputer anda dengan teknologi wireless 2.4 Ghz dengan daya jangkau luas yang sangat bermanfaat bagi anda yang ingin menghubungkan kantor - kantor anda dalam satu jaringan komputer terpadu.

4. Hot spot

   Akses internet tanpa terhubung dengan kabel atau tanpa menggunakan perangkat radio wireless, anda cukup menggunakan PCMCIA card dan laptop anda akan terhubung ke internet tanpa perlu setting apapun di laptop anda,anda cukup mengisi username dan password untuk Authentication dan anda terhubung ke internet.

5. Application software

   Kebutuhan akan aplikasi komputer penunjang pekerjaan semakin meningkat, untuk itu kami berusaha memenuhi kebutuhan anda dengan memberikan layanan dibidang software programing. Software yang kami desain bukanlah sekedar software yang bisa berfungsi saja, tetapi kami memberikan solusi melebihi yang anda minta. Setiap software yang kami hasilkan akan terlebih dahulu kami uji stabilitas, keamanan dan perfomancenya.

2.3. Pengguna Jasa Padjadjaran Mitra Net

Adapun yang menjadi pengguna jasa adalah seluruh perusahaan ataupun individu dari seluruh layanan produk. Beberapa perusahaan yang telah menggunakan jasa PadmaNet, antara lain:

2.3.1. Klinik Padjadjaran (Divisi Kesehatan PT RSP)

1. Sistim Informasi Klinik (SIKI)
    1. SIKI V.1, V.2, V.3
    2. SIKI CNP (Clinik Network Program)
    3. SIKI Versi Single Dokter

2. Pembangunan Infrastruktur Networking
    1. Fix Line
    2. Hotspot system
3. Pembangunan Server aplikasi (Linux based)
4. Pembuatan Office Online

2.3.2. Fakultas Kedokteran Unpad

1. Pembuatan Website Asian Education Conference (Amea 2009)
   Homepage: http://amea2009.fk.unpad.ac.id
2. Penyediaan Layanan Internet

2.3.3. Fakultas Kedokteran Unisba

Pemeliharaan Infrastruktur IT dan konsultan IT Unisba

2.3.4. Bale Market

Pembuatan Sistim Informasi Mini Market

2.3.5. Organisasi Penanggulangan dan penyuluhan HIV/AIDS IMPACT

Pembuatan website impactHomepage :http://www.impactbandung.org

2.4. Landasan Teori

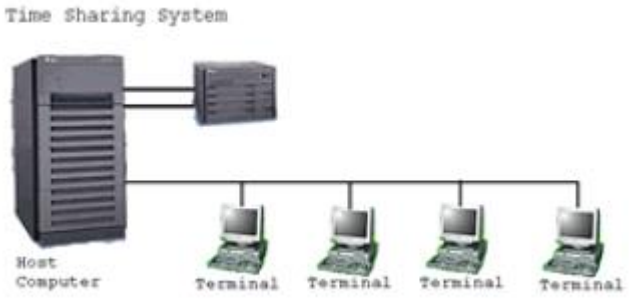
2.4.1. Jaringan Komputer

Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam suatu kesatuan. Informasi dan data bergerak melalui kabel-kabel atau tanpa kabelsehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama-sama menggunakan hardware/software yang terhubung dengan jaringan. Setiap komputer, printer atau periferal yang terhubung dengan jaringan disebut node. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan atau bahkan jutaan node

2.4.2. Sejarah Jaringan Komputer

Konsep jaringan komputer lahir pada tahun 1940-an di Amerika dari sebuah proyek pengembangan komputer MODEL I di laboratorium Bell dan group riset Harvard University yang dipimpin profesor H. Aiken. Pada mulanya proyek tersebut hanyalah ingin memanfaatkan sebuah perangkat komputer yang harus dipakai bersama. Untuk mengerjakan beberapa proses tanpa banyak membuang waktu kosong dibuatlah proses beruntun (Batch Processing), sehingga beberapa program bisa dijalankan dalam sebuah komputer dengan dengan kaidah antrian.

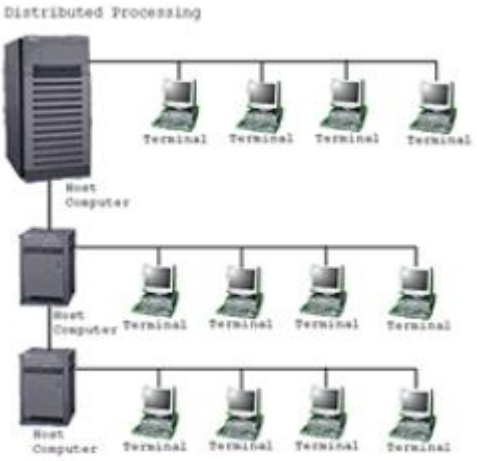
Ditahun 1950-an ketika jenis komputer mulai membesar sampai terciptanya super komputer, maka sebuah komputer mesti melayani beberapa terminal (lihat Gambar 2) Untuk itu ditemukan konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (Time Sharing System), maka untuk pertama kali bentuk jaringan (network) komputer diaplikasikan. Pada sistem TSS beberapa terminal terhubung secara seri ke sebuah host komputer. Dalam proses TSS mulai nampak perpaduan 16 teknologi komputer dan teknologi telekomunikasi yang pada awalnya berkembang sendiri-sendiri.



Gambar 2.2 Jaringan Komputer Model TSS

Memasuki tahun 1970-an, setelah beban pekerjaan bertambah banyak dan harga perangkat komputer besar mulai terasa sangat mahal, maka mulailah digunakan konsep proses distribusi (Distributed Processing). Seperti pada Gambar 2, dalam proses ini beberapa host komputer mengerjakan sebuah pekerjaan besar secara paralel untuk melayani beberapa terminal yang tersambung secara seri disetiap host komputer. Dala proses distribusi sudah mutlak diperlukan perpaduan yang mendalam antara teknologi komputer dan telekomunikasi, karena selain proses yang harus

didistribusikan, semua host komputer wajib melayani terminalterminalnya dalam satu perintah dari komputer pusat.



Gambar 2.3Jaringan komputer model distributed processing

Selanjutnya ketika harga-harga komputer kecil sudah mulai menurun dan konsep proses distribusi sudah matang, maka penggunaan komputer dan jaringannya sudah mulai beragam dari mulai menangani proses bersama maupun komunikasi antar komputer (Peer to Peer System) saja tanpa melalui komputer pusat. Untuk itu mulailah berkembang teknologijaringan lokal yang dikenal dengan sebutan LAN. Demikian pula ketika Internet mulai dikenalkan, maka sebagian besar LAN yang berdiri sendiri mulai berhubungan dan terbentuklah jaringan raksasa WAN.

2.4.3. Jenis Jaringan Komputer

Secara umum jaringan komputer dibagi atas lima jenis, yaitu;

1. Local Area Network (LAN)

   Local Area Network (LAN), merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor suatu perusahaan atau pabrik-pabrik untuk memakai bersama sumberdaya (misalnya printer) dan saling bertukar informasi.

2. Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN), pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel.

3. Wide Area Network (WAN)

Wide Area Network (WAN), jangkauannya mencakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan programprogram (aplikasi) pemakai.

4. Internet

Sebenarnya terdapat banyak jaringan didunia ini, seringkali menggunakan perangkat keras dan perangkat lunak yang berbeda-beda. Orang yang terhubung ke jaringan sering berharap untuk bisa berkomunikasi dengan orang lain yang terhubung ke jaringan lainnya. Keinginan seperti ini memerlukan hubungan antar jaringan yang seringkali tidak kampatibel dan berbeda. Biasanya untuk melakukan hal ini diperlukan sebuah mesin yang disebut gateway guna melakukan hubungan dan melaksanakan terjemahan yang diperlukan, baik perangkat keras maupun perangkat lunaknya. Kumpulan jaringan yang terinterkoneksi inilah yang disebut dengan internet.

5. Jaringan

Tanpa Kabel Jaringan tanpa kabel merupakan suatu solusi terhadap komunikasi yang tidak bisa dilakukan dengan jaringan yang menggunakan kabel. Misalnya orang yang ingin mendapat informasi atau melakukan komunikasi walaupun sedang berada diatas mobil atau pesawat terbang, maka mutlak jaringan tanpa kabel diperlukan karena koneksi kabel tidaklah mungkin dibuat di dalam mobil atau pesawat. Saat ini jaringan tanpa kabel sudah marak digunakan dengan memanfaatkan jasa satelit dan mampu memberikan kecepatan akses yang lebih cepat dibandingkan dengan jaringan yang menggunakan kabel.

2.4.4. Model Referensi Osi Dan Standarisasi

Untuk menyelenggarakan komunikasi berbagai macam vendor komputer diperlukan sebuah aturan baku yang standar dan disetejui berbagai fihak. Seperti halnya dua orang yang berlainan bangsa, maka untuk berkomunikasi memerlukan penerjemah/interpreter atau satu bahasa yang dimengerti kedua belah fihak. Dalam dunia komputer dan telekomunikasi interpreter identik dengan protokol. Untuk itu maka badan dunia yang menangani masalah standarisasi ISO (International Standardization Organization) membuat aturan baku yang dikenal dengan nama model referensi OSI (Open System Interconnection). Dengan demikian diharapkan semua vendor perangkat telekomunikasi haruslah berpedoman dengan model referensi ini dalam mengembangkanprotokolnya. Model referensi OSI terdiri dari 7 lapisan, mulai dari lapisan fisik sampai dengan aplikasi. Model referensi ini tidak hanya berguna untuk produk-produk LAN saja, tetapi dalam membangung jaringan Internet sekalipun sangat diperlukan. Hubungan antara model referensi OSI dengan protokol Internet bisa dilihat dalam Tabel 2.1.

Tabel 2.1 Hubungan referensi model OSI dengan protokol Internet

MODEL OSI		TCP/IP	PROTOKOL TCP/IP	
NO	LAPISAN		NAMA PROTOKOL	KEGUNAAN
1	APLIKASI	APLIKASI	DHCP (Dynamic Host Configuration Protocol)	Protokol untuk distribusi IP pada jaringan dengan jumlah IP yang terbatas
			FTP (File Transfer Protocol)	Data base nama domain mesin dan nomer IP
			FTP (File Transfer Protocol)	Protokol untuk transfer file
			HTTP (HyperText Transfer Protocol)	Protokol untuk transfer file HTML dan Web
			MIME (Multipurpose Internet Mail Extention)	Protokol untuk mengirim file binary dalam bentuk teks

			NNTP (Networ News Transfer Protocol)	Protokol untuk menerima dan mengirim newsgroup
			POP (Post Office Protocol)	Protokol untuk mengambil mail dari server
			SMB (Server Message Block)	Protokol untuk transfer berbagai server file DOS dan Windows
2	Presentasi		SMTP (Simple Mail Transfer Protocol)	Protokol untuk pertukaran mail
			SNMP (Simple Network Management Protocol)	Protokol untuk manejemen jaringan
			Telnet	Protokol untuk akses dari jarak jauh
			TFTP (Trivial FTP)	Protokol untuk transfer file
3	Sessi		NETBIOS (Network Basic Input Output System)	BIOS jaringan Standar
			RPC (Remote Procedure Call)	Prosedur pemanggilan jarak jauh
			SOCKET	Input Output untuk network jenis BSDUNIX
4	Transport	Transport	TCP (Transmission Control Protocol)	Protokol pertukaran data berorientasi (connection oriented)

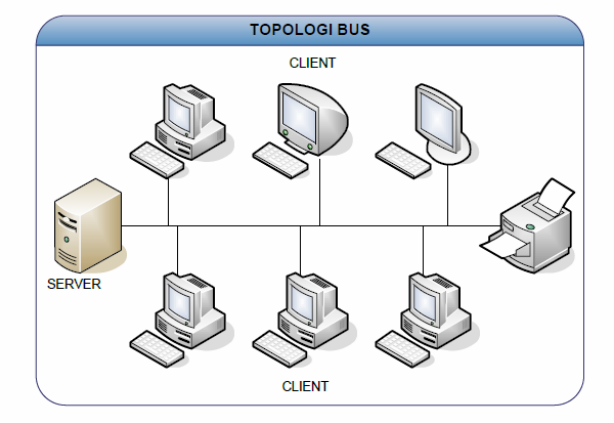
			UDP (User Datagram Protocol)	Protokol pertukaran data non-orientasi (connectionless)
5	Network	Internet	IP (Internet Protocol)	Protokol untuk menetapkan routing
			RIP (Routing Information Protocol)	Protokol untuk memilih routing
			ARP (Address Resolution Protocol)	Protokol untuk mendapatkan informasi hardware dari nomer IP
			RARP (Reverse ARP)	Protokol untuk mendapatkan informasi nomer IP dari hardware
		Network Interface	PPP (Point to Point Protocol)	Protokol untuk point ke point
6	Datalink LLC MAC		SLIP (Serial Line Internet Protocol)	Protokol dengan menggunakan sambungan serial
7	Fisik		Ethernet, FDDI, ISDN, ATM	

Standarisasi masalah jaringan tidak hanya dilakukan oleh ISO saja, tetapi juga diselenggarakan oleh badan dunia lainnya seperti ITU (*International Telecommunication Union*), ANSI (*American National Standard Institute*), NCITS (*National Committee for Information Technology Standardization*), bahkan juga oleh lembaga asosiasi profesi IEEE (*Institute of Electrical and Electronics Engineers*) dan ATM-Forum di Amerika. Pada Topologi Jaringan Komputer.

Topologi adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Cara yang saat ini banyak digunakan adalah bus, token-ring, star dan peer-to-peer network. Masing-masing topologi ini mempunyai ciri khas, dengan kelebihan dan kekurangannya sendiri.

2.4.5.1. Topologi BUS

Topologi bus terlihat pada skema dibawah ini.



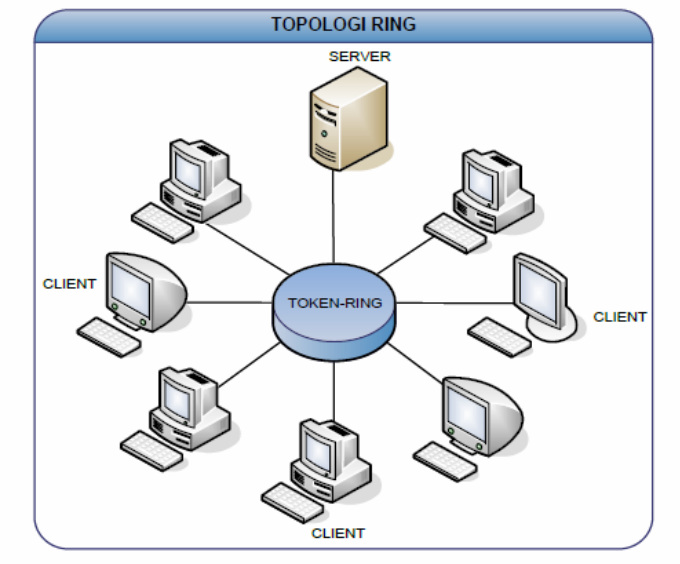
Gambar 2.4 Topologi BUS

Terdapat keuntungan dan kerugian dari tipe ini yaitu:

1. Keuntungan
    a. Hemat Kabel
    b. Layout kabel sederhana
    c. Mudah di kembangkan
2. Kerugian
    a. Deteksi dan kesalahan isolasi sangat kecil
    b. Kepadatan lalulintas
    c. Bila salah satu clint rusak, maka jaringan tidak bisa berfungsi
    d. Diperlukan repeter untuk jarak jauh

2.4.5.2. Topologi TokenRING

Topologi bus terlihat pada skema dibawah ini. Terdapat keuntungan dan kerugian dari tipe ini yaitu:



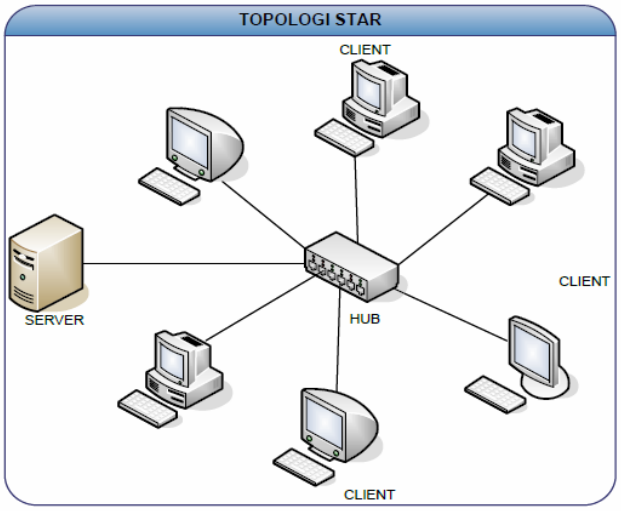
Gambar 2.5 Topologi TokenRING

Metode token-ring (seringdisebut ring saja) adalah cara menghubungkan komputer sehingga berbentuk ring(lingkaran). Setiap simpul mempunyai tingkatan yang sama. Jaringan akan disebutsebagai loop, data dikirimkan kesetiap simpul dan setiap informasi yang diterimasimpul diperiksa alamatnya apakah data itu untuknya atau bukan. Terdapatkeuntungan dan kerugian dari tipe ini yaitu:

1. Keuntungan
    a. Hemat Kabel
2. Kerugian
    a. Peka kesalahan
    b. Pengembangan jaringan lebih kaku

2.4.5.3. Topologi Star

Topologi Star terlihat pada skema dibawah ini. Terdapat keuntungan dan kerugian dari tipe ini yaitu:



Gambar 2.6 Topologi Star

Merupakan kontrol terpusat, semua link harus melewati pusat yang menyalurkan data tersebut kesemua simpul atau client yang dipilihnya. Simpul pusat dinamakanstasium primer atau server dan lainnya dinamakan stasiun sekunder atau clientserver. Setelah hubungan jaringan dimulai oleh server maka setiap client serversewaktu-waktu dapat menggunakan hubungan jaringan tersebut tanpa menungguperintah dari server. Terdapat keuntungan dan kerugian dari tipe ini yaitu:

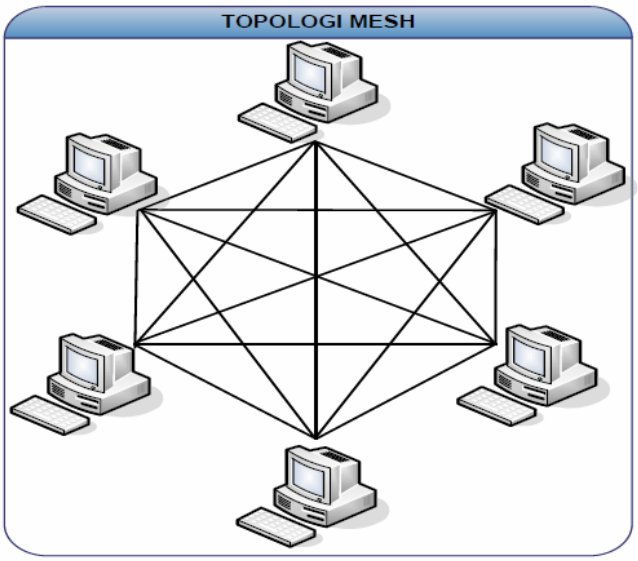
1. Keuntungan
    a. Paling fleksibel
    b. Pemasangan/perubahan stasiun sangat mudah dan tidak mengganggu bagian
    c. Kontrol terpusat
    d. Kemudahan deteksi dan isolasi kesalahan/kerusakan
    e. Kemudahaan pengelolaan jaringan
2. Kerugian
    a. Boros kabel
    b. Perlu penanganan khusus
    c. Kontrol terpusat (HUB) jadi elemen kritis

2.4.5.4. Topologi Mesh

Topologi ini menerapkan hubungan secara penuh dengan komputer yang lain. Setiap komputer akan mempunyai jalur secara langsung ke komputer-komputer yang lain. Sehingga setiap komputer akan memiliki beberapa jalur untuk komunikasi data.

Pada prinsipnya, topologi mesh mirip dengan topologi star, tetapi topologi mesh memiliki jalur ganda pada setiap komputer. Umumnya topologi inidikembangkan dengan ruang lingkup yang luas dengan jarak antar komputerberjauhan.

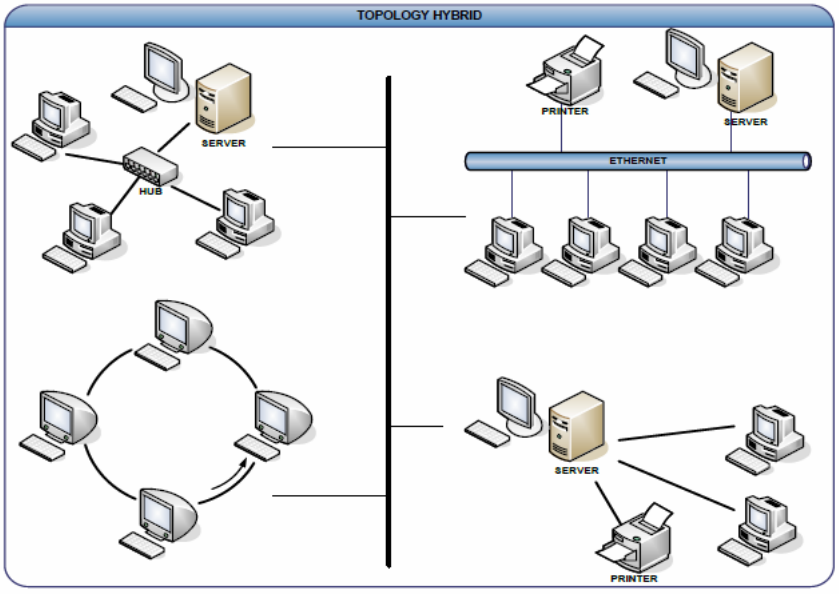
Topologi mesh memberikan keamanan data yang lebih baik, yaitu denganmenggunakan metode multiplexing, dimana pesan dapat dipecah-pecah menjadibeberapa paket dan dilewatkan pada jalur yang berbeda.



Gambar 2.7 Topologi Mesh

2.4.5.5. Topologi Hybrid

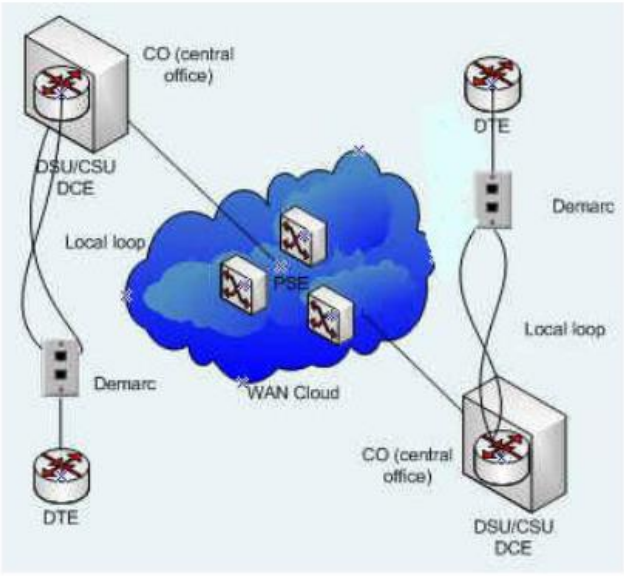
Topologi hybrid merupakan gabungan dari beberapa topologi (bus, ring,star, atau mesh). Topologi hybrid dibangun untuk dapat mengkombinasikankeunggulan-keunggulan yang dimiliki setiap topologi. Contoh topologi ini ialahtopologi pohon (tree topology)Topologi pohon merupakan perpaduan antaratopologi bus dengan topologi star.



Gambar 2.8 Topologi Hybrid

2.4.5. Koneksi WAN

Jenis koneksi WAN normalnya tergantung pada layanan yang bisa diberikan oleh penyedia WAN, dan juga berhubungan dengan jenis *interface* fisik yang dipakai untuk menghubungkan router. Ada banyak sekali jenis koneksi, akan tetapi jika memungkinkan pilihlah jenis koneksi yang teknologinya bisa mendukung data rate yang lebih tinggi dan mendukung konfigurasi yang fleksibel. Diagram dibawah ini adalah struktur koneksi WAN yang umum dipakai.



Gambar 2.9Struktur Koneksi WAN

DTE adalah Data Terminal Equipment yang berada pada sisi koneksi link WAN yang mengirim dan menerima data. DTE ini berada pada sisi bangunan pelanggan dan sebagai titik tanda masuk antara jaringan WAN dan LAN. DTE ini biasanya berupa router, akan tetapi komputer dan multiplexer juga bisa bertindak sebagai DTE. Secara luas, DTE adalah semua equipment yang berada pada sisi tempat pelanggan yang berkomunikasi dengan DCE pada sisi yang lain.bertanggung jawab terhadap semua equipment disisi demark dan pihak Telkom bertanggung jawab semua equipment disisi lain dari demark.

Central office adalah fasilitas switching dan juga memberikan entry WAN cloud dan juga exit points untuk panggilan masuk dan keluar, dan juga bertindak sebagai switching point untuk meneruskan data ke central office lainnya. Central office juga memberikan layanan seperti switching sinyal telpon masuk menuju trunk line. CO juga berfungsi memberikan catu daya DC ke local loop untuk membentuk circuit electric.

DCE adalah peralatan data circuit terminating yang berkomunikasi dengan DTE dan juga WAN cloud. DCE pada umumnya berupa router disisi penyedia jasa yang merelay data pesan antara customer dan WAN cloud. DCE adalah piranti yang mensuplay signal clocking ke DTE. Suatu modem atau CSU/DSU disisi pelanggan sering diklasifikasikan sebagai DCE. DCE bisa serupa DTE seperti router akan tetapi masing-masing mempunyai perannya sendiri.

PSE adalah Packet Switching Exchange, suatu switch pada jaringan pembawa packet-switched. PSE merupakana titik perantara di WAN cloud.

WAN cloud adalah hirarkhi dari trunk, switch, dan central office yang membentuk jaringan sambungan telpon. Kenapa di presentasikan dengan Cloud karena struktur fisik bermacam-macam dan jaringan-jaringan dengan titik koneksi bersama bisa saling timpang tindih.

2.4.7. Kelas IP Address

Untuk mempermudah proses pembagiannya, IP address dikelompokan dalam kelas-kelas. Dasar pertimbangan pembagian IP address ke dalam kelas-kelas adalah untuk memudahkan pendistribusian pendaftaran IP address. Dengan memberikan sebuah ruang nomor jaringan (beberapa blok IP address) kepada Internet Service

Provider (ISP) di suatu area diasumsikan penanganan komunitas lokal tersebut akan lebih baik, dibandngkan dengan jika setiap pemakaian individual harus meminta IP address ke otoritas pusat, yaitu internet Assigned Numbers Authority (IANA) IP address ini dikelompokan dalam lima kelas : kelas A, Kelas B, Kelas C, Kelas D, dan kelas E. Perbedaan pada tiap kelas tersebut adalah pada ukuran dan jumlahnya. IP kelas A di pakai oleh sedikit jaringan namun jaringan ini memiliki anggota yang besar. Kelas C dipakai oleh banyak jaringan, namun anggota masing-masing jaringan sedikit. Kelas D dan Edidefinisikan, tetapi tidak digunakan dalam penggunaan normal, dan kelas E untuk keperluan eksperimental

2.4.7.1. Network ID dan host ID

Pembagian kelas-kelas IP address didasarkan pada dua hal : network ID dan host ID dari suatu IP address. Setiap IP address selalu merupakan sebuah pasangan dari network ID (Identitas Jaringan) dan host ID (identitas host dalam jaringan tersebut). Network ID adalah bagian dari IP address yang digunakan untuk menujukan jaringan tempat komputer ini berada. Sedangkan host ID adalah bagian dari IP address yang digunakan untuk menunjukan workstation, server,router, dan semua host TCP/IP lainnya dalam jaringan tersebut. Dalam suatu jaringan, host ID ini harus unik (tidak boleh ada yang sama).

Kelas A

Karakteristik :

Format : 0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

Bit Pertama : 0

Panjang Net ID : 8 bit

Panjang Host ID : 24 bit

Byte Pertama : 0 – 127

Jumlah : 126 Kelas A (0 dan 127 dicadangkan)

Range IP : 1.xxx.xxx.xxx sampai 126.xxx.xxx.xxx

Jumlah IP : 16.777.214. IP address pada tiap kelas A

IP address kelas A diberikan untuk jaringan dengan jumlah host yang sangat besar. Bit pertama dari IP address kelas A selalu di set 0 (nol) sehingga byte terdepan dari IP address A selalu bernilai antara angka 0 dan 127. Pada IP address kelas A, Network ID adalah delapan bit pertama, sedangkan host ID ialah 24 bit berikutnya. Dengan demikain, cara membaca IP address kelas A, misalnya 113.46.5.6 ialah:

Network ID = 113

Host ID = 46.5.6

Sehingga IP address diatas berarti host nomor 46.5.6 pada network nomor 113. Dengan panjang host ID yang 24 bit, network dengan IP address A ini dapat menampung sekitar 16 juta host.

Kelas B

Karakteristik :

Format : 10.nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh

Bit Pertama : 10

Panjang Net ID : 16 bit

Panjang host ID : 16 bit

Byte Pertama : 128-191

Jumlah : 16.184 Kelas B

Range IP : 128.0.xxx.xxx sampai 191.225.xxx.xxx

Jumlah IP : 65.532 IP address pada tiap kelas B

IP address kelas B biasanya dialokasikan untuk jaringan ukuran sedang dan besar. Dua bit pertama dari IP address kelas B selalu di set 10 (satu nol) sehingga byte terdepan dari IP address kelas B selalu bernilai antara 128 hingga 191. Pada IP address kelas B, network ID adalah enambelas bit

pertama, sedangkan host ID adalah 16 bit berikutnya. Dengan demikian, cara membaca IPaddress kelas B, misalnya 132.92.121.1 ialah :

Network ID = 132.92

Host ID = 121.1

Sehingga IP address di atas berarti host nomor 121.1 pada netowrk nomor 132.92 dengan panjang host ID yang 16 bit, network dengan IP address kelas B ini dapat menampung sekitar 65000 host.

Kelas C

Karakteristik :

Format : 110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh

Bit Pertama : 110

Panjang Net ID : 24 bit

Panjang Host ID : 8 bit

Byte pertama : 192-223

Jumlah : 2.097.152 kelas C

Range IP : 192.0.0.xxx sampai 191.255.255.xxx

Jumlah IP : 254 IP address pada tiap kelas C

IP address kelas C awalnya digunakan untuk jaringan ukuran kecil (misalnya LAN). Tiga bit pertama dari IP address kelas C selalu berisi 111. Bersama 21 bit berikutnya, angka ini membentuk network ID 24 bit. Host-ID ialah 8 bit terakhir. Dengan konfigurasi ini, bisa dibentuk sekitar dua juta network dengan masing-masing network memiliki 256 IP address.

Kelas D

Karakteristik :

Format : 1110.mmmm.mmmmmmmm.mmmmmmmm.

Mmmmmmmm

4 Bit Pertama : 1110

Bit Multicast : 28 bit

Byte Inisial : 224-247

Deskripsi : Kelas D adalah ruang alamat multicast (RFC 1112)

IP address kelas D digunakan untuk keperluan IP multicasting. 4 bit pertama IP address kelas D di set 1110. Bit-bit berikutnya diatur sesuai keperluan multicast group yang menggunakan IP address ini. Dalam multicasting tidak dikenal *network* bit dan host bit.

Kelas E

Karakteristik :

Format : 1111.rrrr.rrrrrrrr.rrrrrrrr.rrrrrrrr

4 Bit Pertama : 1111

Bit Multicast : 28 bit

Byte Inisial : 248-255

Deskripsi kelas E adalah ruang alamat yang dicadangkan untuk keperluan eksperimantal. IP address kelas E tidak digunakan untuk umum. 4 bit pertama IP address ini di set 1111.

2.4.8. Virtual Private Network (VPN)

Yang dimaksud dengan Virtual Private Network adalah suatu jaringan private yang mempergunakan sarana jaringan komunikasi publik (dalam hal ini internet) dengan memakai tunnelling protocol dan prosedur pengamanan. Denganmemakai jaringan publik yang ada, dalam hal ini internet, maka biaya pengembangan yang dikeluarkan akan jauh relatif lebih murah daripada harus membangun sebuah jaringan internasional tertutup sendiri.

Namun pemakaian Internet sebagai sarana jaringan publik juga mengandung resiko, karena Internet terbuka untuk umum, maka masalah kerahasiaan dan

authentifikasi atas data yang dikirim pun juga terbuka. Oleh karenanya VPN menjaminnya dengan penerapan enkripsi data. Sebelum dikirimkan, terlebih dahulu data akan dienkripsikan untuk mengurangi resiko pembacaan dan pembajakan data di jalan oleh pihak yang tidak terkait. Setelah sampai ke alamat tujuan, maka data tersebut akan di-deskripsikan ulang sehingga bentuk informasi dapat kembali menjadi seperti sedia kala. Selain memakai metode pengamanan enkripsi-deskripsi, VPN masih memakai kriptografi lainnya untuk mendukung pengamanan data.

VPN saat ini banyak digunakan untuk diterapkan pada jaringan extranet ataupun intranet perusahaan-perusahaan besar. VPN harus dapat mendukung paling tidak 3 mode pemakaian :

1. Koneksi client untuk akses jarak jauh
2. LAN-to-LAN internetworking
3. Pengontrolan akses dalam suatu intranet

Oleh karena infrastruktur VPN menggunakan infrastruktur telekomunikasi umum, maka dalam VPN harus menyediakan beberapa komponen, antara lain :

a. Konfigurasi, harus mendukung skalabilitas platform yang digunakan, mulai dari konfigurasi untuk kantor kecil sampai tingkat enterprise (perusahaan besar).
b. Konfigurasi, harus mendukung skalabilitas platform yang digunakan, mulai dari konfigurasi untuk kantor kecil sampai tingkat enterprise (perusahaan besar).
c. Layanan-layanan VPN, antara lain fungsi Quality of Services (QoS), layanan routing VPN yang menggunakan BGP, OSPF dan EIGRP
d. Peralatan, antara lain Firewall, pendeteksi pengganggu, dan auditing keamanan
e. Manajemen, untuk memonitor jaringan VPN

Sedangkan untuk mendapatkan koneksi bersifat private, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi. Proses enkapsulasi data sering disebut “tunneling”. Berikut adalah beberapa kriteria yang harus dipenuhi oleh VPN:

a. User Authentication VPN harus mampu mengklarifikasi identitas klien serta membatasi hak akses user sesuai dengan otoritasnya. VPN juga dituntut mampu memantau aktifitas klien tentang masalah waktu, kapan, di mana dan berapa lama seorang klien mengakses jaringan serta jenis resource yang diakses oleh klien tersebut. Address Management VPNharus dapat mencantumkan alamat klien pada intranet dan memastikan alamat tersebut tetap rahasia.
b. Data Encryption Data yang melewati jaringan harus dibuat agar tidak dapat dibaca oleh pihak-pihak atau klien yang tidak berwenang.
c. Key Management VPN harus mampu membuat dan memperbarui encryption key untuk server dan clien.
d. Multiprotocol Support VPN harus mampu menangani berbagai macam protocol dalam jaringan publik seperti IP, IPX , dan sebagainya. Terdapat tiga protokol yang hingga saat ini paling banyak digunakan untuk VPN. Ketiga protokol tersebut antara lain adalah Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), IPSec SOCKS CIPE.

Protokol-protokol di atas menekankan pada *authentikasi* dan enkripsi dalam VPN. Adanya sistem otentifikasi akan mengijinkan *clien* dan server untuk menempatkan identitas orang yang berbeda di dalam jaringan secara benar. Enkripsi mengijinkan data yang dikirim dan diterima tersembunyi dari publik saat melewati jaringan publik. *Intranet* merupakan koneksi VPN yang membuka jalur komunikasi pribadi menuju ke jaringan lokal yang bersifat pribadi melalui jaringan publik seperti internet. Dengan melalui VPN jenis ini, *user* dapat langsung mengakses *file-file* kerja dengan leluasa tanpa terikat tempat dan waktu. Apabila dianalogikan pada sebuah perusahaan, koneksi ke kantor pusat dapat dilakukan dari mana saja, dari kantor pusat menuju ke kantor cabang dapat puladibuat koneksi pribadi, dan juga dari kantor juga memungkinkan untuk dibuat jalur komunikasi pribadi yang ekonomis.

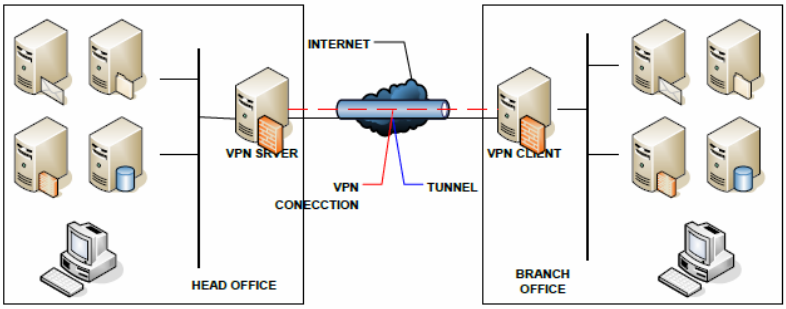
2.4.8.1. Teknologi VPN

Teknologi VPN sangat populer saat ini, dikarenakan VPN memberikan keamanan serta reliabilitas yang sama seperti jaringan private. Pengguna VPN dapat mengakses Local Area Network (LAN) suatu perusahaan atau organisasi dengan mengunakan jaringan internet. VPN menjamin keamanan karena koneksi yang dilakukan oleh VPN menggunakan

piranti yang menerapkan metode autentikasi, serta data yang dikirimkan dienkripsi. Melihat dari jenis jaringan yang ada dalam jaringan VPN dapat di bagi menjadi dua tipe jaringan VPN, yaitu :

1. Site to Site VPN

Jenis implementasi site-to-site VPN, implementasi jenis ini menghubungkan antara dua kantor atau lebih yang letaknya berjauhan, baik kantor yang dimiliki perusahaan itu sendiri maupun kantor perusahaan mitra kerjanya. VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, supplier atau pelanggan) disebut ekstranet. Sedangkan bila VPN digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis intranet site-to-site VPN.



Gambar 2.10 Jaringan site to site VPN

2. Remote Access VPN

Pada dasarnya, VPN merupakan sebuah proses *remote access* yang bertujuan mendapatkan koneksi ke jaringan *private* tujuannya. Proses *remote access* VPN ini dipisahkan menjadi dua jenis lagi berdasarkan oleh siapa proses *remote access* VPN tersebut dilakukan. Berikut ini adalah jenis-jenisnya:

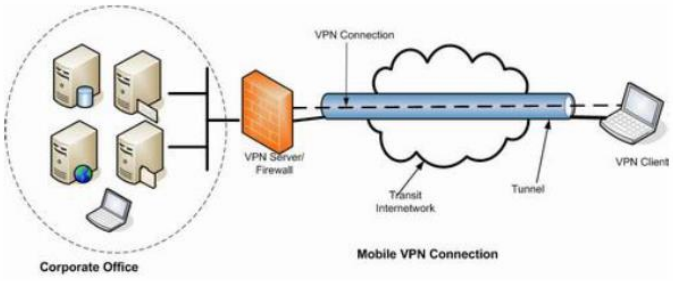
a. Client-initiated

Client-initiated arti harafiahnya adalah pihak klien yang berinisiatif untukmelakukan sesuatu. VPN jenis ini juga demikian dan ini merupakan jenisVPN yang paling umum digunakan. Jadi ketika PC Anda inginmembangun koneksi VPN, maka PC tersebutlah yang berusahamembangun tunnel dan melakukan enkripsi hingga mencapai

tujuannyadengan aman. Namun, proses ini tetap mengandalkan jaringan ISP yangdigunakan secara umum. Clientinitiated VPN sering digunakan oleh PCPC umum dengan mengandalkan VPN server atau VPN concentrator pada jaringan tujuannya.

b. Network Access Server – initiated

Lain dengan client-initiated, VPN jenis ini tidak mengharuskan client-nya membuat tunnel dan melakukan enkripsi dan dekripsi sendiri. VPN jenis ini hanya mengharuskan penggunanya melakukan dial-in ke Network Access Server (NAS) ISP. Kemudian NAS inilah yang membangun tunnel menuju ke jaringan private yang dituju oleh clien tersebut. Dengan demikian, koneksi VPN dapat dibangun oleh banyak clien dari manapun karena biasanya NAS milik ISP tersebut memang sering kali dibuka untuk umum.



Gambar 2.11 Jaringan Remote Access VPN

2.4.9. Tunneling Protocol

Dalam jaringan VPN ada Tiga protokol tunneling utama digunakan dalam Jaringan VPN untuk menjamin aspek keamanan transaksi berbasis VPN, yaitu :

1. Point-to-Point Tunneling Protocol (PPTP)
2. Layer 2 Tunneling Protocol (L2TP)
3. Ipsec

2.4.9.1. Point-to-Point Tunneling Protocol (PPTP)

PPTP dikembangkan oleh Microsoft dan Cisco merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari remote client ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP. Teknologi jaringan PPTP merupakan pengembangan dari remote access Point-to-Point protocol yang dikeluarkan oleh Internet Engineering Task Force (IETF). PPTP merupakan protokol jaringan yang merubah paket PPP menjadi

IP datagrams agar dapat ditransmisikan melalui intenet. PPTP juga dapat digunakan pada jaringan private LAN-to-LAN.

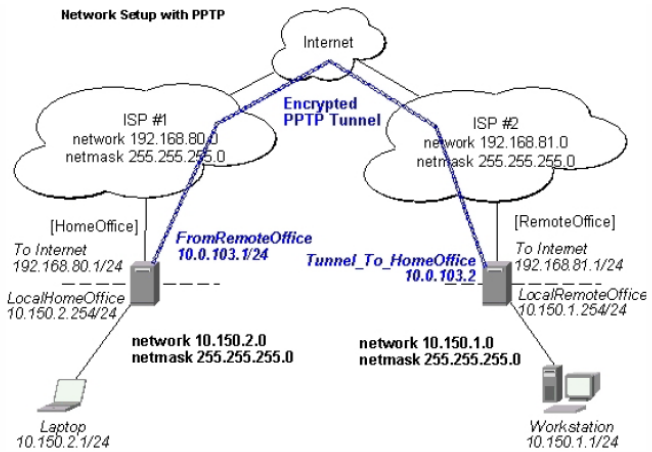
PPTP terdapat sejak dalam sistem operasi Windows NT server dan Windows NT Workstation versi 4.0. Komputer yang berjalan dengan sistem operasi tersebut dapat menggunakan protokol PPTP dengan aman untuk terhubung dengan private network sebagai klien dengan remote access melalui internet. PPTP juga dapat digunakan oleh komputer yang terhubung dengan LAN untuk membuat VPN melalui LAN.

Fasilitas utama dari penggunaan PPTP adalah dapat digunakannya Public-Switched Telephone Network (PSTN) untuk membangun VPN. PembangunanPPTP yang mudah dan berbiaya murah untuk digunakan secara luas, menjadisolusi untuk remote users dan mobile users karena PPTP memberikan keamanandan enkripsi komunikasi melalui PSTN ataupun internet.

PPTP sangat cocok digunakan untuk membangun jaringan akses kepada LAN melalui intenet . Keunggulan-keunggulan utama pemakaian PPTP adalah:

1. Lebih aman
2. Tidak perlu melakukan perubahan pengalamatan jaringan internal
3. Murah

Berikut ini adalah contoh koneksi dua intranet menggunakan sebuahterowongan dienkripsi PPTP melalui jaringan internet.

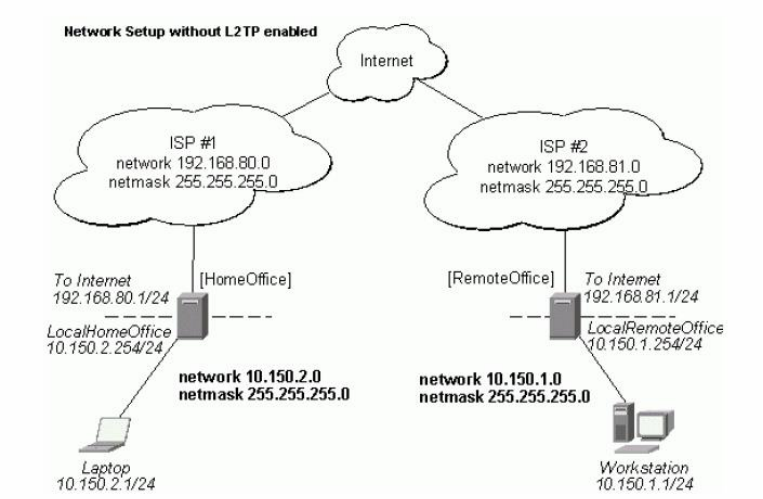


Gambar 2.12Koneksi Point-to-Point Tunneling Protocol (PPTP)

2.4.9.2. Layer 2 Tunneling Protocol (L2TP)

L2TP adalah tunneling protocol yang memadukan dua buah tunnelingprotocol yaitu L2F (Layer 2 Forwarding) milik cisco dan PPTP milik Microsoft(Gupta, 2003). L2TP biasa digunakan dalam membuat Virtual Private DialNetwork (VPDN) yang dapat bekerja membawa semua jenis protokol komunikasididalamnya. Umunnya L2TP menggunakan port 1702 dengan protocol UDPuntuk mengirimkan L2TP encapsulated PPP frames sebagai data yang ditunnel.Terdapat dua model tunnel yang dikenal (Lewis, 2006), yaitucompulsorydan voluntary. Perbedaan utama keduanya terletak pada endpointtunnel-nya. Pada compulsory tunnel, ujung tunnel berada pada ISP, sedangkanpada voluntary ujung tunnel berada pada client remote.

Berikut ini adalah contoh koneksi dua intranet menggunakan sebuah terowongan dienkripsi L2TP melalui jaringan internet.



Gambar 2.13Koneksi L2TP

Ada dua router dalam contoh di atas :

1. [Home office]
   Interface local home office 10.150.254/24
   Interface To internet 192.168.80.1/24
2. [Remote Office]
   Interface To Internet 192.168.81.1/24
   Iterface local home office 10.150.1.254/24

2.4.9.3. Ipsec

IPSec merupakan suatu pengembangan dari protokol IP yang bertujuan untuk menyediakan keamanan pada suatu IP dan layer yang berada diatasnya (Carmouche, 2006). IPSec (Internet Protocol Security) merupakan salah satu mekanisme yang diimplementasikan pada Virtual Private Network. Paket IP tidak memiliki aspek security, maka hal ini akan memudahkan untuk mengetahui isi dari paket dan alamat IP itu sendiri. Sehingga tidak ada garansi bahwa menerima paket IP merupakan dari pengirim yang benar, kebenaran data ketika ditransmisikan. IPSecmerupakan metode yang memproteksi IP datagram ketika paket ditransmisikan pada traffic. IPSec berkerja pada layer tiga OSI yaitu network layer sehingga dapat mengamankan data dari layer yang berada atasnya. IPSec terdiri dari dua buah security protokol (Carmouche, 2006)

a. AH (Authentication Header). Melakukan autentikasi datagram untuk mengidentifikasi pengirim data tersebut.
b. ESP (Encapsulating Security Header). Melakukan enkripsi dan layanan autentifikasi.

IPSec menggunakan dua buah protokol berbeda untuk menyediakan pengamanan data yaitu AH dan ESP. keduanya dapat dikombinasikan ataupun berdiri sendiri.

IPSec memberikan layanan security pada level IP dengan memungkinkan suatu system memilih protokol security yang dibutuhkan, algoritma yang digunakan untuk layanan, dan menempatkan kunci kirptografi yang dibutuhkan unutk menyediakan layanan. Dua buah protokol yang digunakan untuk memberikan layanan kemanan yaitu autentikasi protokol yang ditunjuk pada header protokol yaitu AH (Authentication Header) dan sebuah protokol yang mengkombinasikan enkripsi dan autentikasi yang ditunjuk oleh header paket untuk format tersebut yaitu ESP (Encapsulating Security Payload).

2.4.10. Pilihan Menggunakan VPN

Setelah Anda mengetahui VPN adalah salah satu alternatif untuk berkomunikasi data, Mungkin Anda perlu mengetahui bahwa VPN memiliki banyak

keuntungan yang khas dibandingkan dengan teknologi komunikasi tradisional seperti misalnya jaringan leased line. Keuntungan tersebut adalah sebagai berikut:

1. VPN Menawarkan Solusi dengan Biaya Murah

   Kebutuhan Anda untuk berkomunikasi dengan banyak kantor cabang mungkin tidak bisa ditawar-tawar lagi, namun biasanya yang menjadi kendala adalah mahalnya biaya kepemilikan untuk membangun jaringan komunikasinya. Menggunakan jaringan leased line khusus atau jaringan packet switching tentu juga memerlukan biaya ekstra yang tidak kecil. Salah satu mengakalinya adalah dengan menggunakan solusi VPN. Dengan menggunakan VPN, Anda dapat membangun jaringan pribadi ini melalui koneksi Internet yang telah Anda miliki. Perangkat-perangkat yang dibutuhkan juga tidak banyak, dan maintenance-nya pun tidak terlalu sulit.
2. VPN Menawarkan Feksibilitas Seiring dengan Perkembangan Internet.

   Roda perekonomian dunia tidak luput juga dari pengaruh perkembangan Internet dan komunikasi data. Jika dulunya kantor-kantor cabang sebuah perusahaan harus menggunakan WAN antarkota bahkan antarnegara untuk dapat saling bertukar informasi, kini seiring dengan perkembangan Internet, hal itu tidak diperlukan lagi. VPN dapat membawa data Anda tepat ke lokasi kantor cabang yang Anda tuju melalui jaringan umum Internet, namun dengan perlakuan seperti layaknya melewati jalur pribadi. Dengan adanya kemudahan seperti ini, maka fleksibilitas tentu akan Anda rasakan. Anda dapat membuat kantor cabang di mana saja, kemudian berlangganan koneksi Internet dan percayakan jalur komunikasi datanya ke pusat dengan menggunakan VPN. Ketika Anda berada di luar negeri, hubungan data Anda tidak akan terputus selama masih ada koneksiInternet. Selain itu, masih banyak lagi fleksibilitas yang akan Anda dapatkan dari VPN.
3. VPN Menawarkan Kemudahan dan Administrasi dibandingkan dengan Jaringan Leased Line.

   Anda tidak perlu memonitor modem-modem leased line Anda untuk menjaga agar koneksinya tidak putus. Anda tidak perlu menyediakan perangkat dan ruangan khusus untuk me-maintenance jaringan Anda ke kantor-kantor cabang ini. Dengan VPN, Anda tidak perlu lakukan semua itu. Cukup menginstal

server VPN, install klien-kliennya di PC kerja Anda, jadilah koneksi pribadi Anda.

4. VPN menggunakan teknologi tunnel yang mengurangi kerumitan pengaturannya

   Dalam mewujudkan sebuah koneksi pribadi, VPN menggunakan sebuah teknologi bernama tunneling atau arti harafiahnya adalah terowongan. Tunnel inilah kunci dari VPN, di mana koneksi pribadi bisa Anda dapatkan dari mana salah lokasi Anda berada, selama terbentuk sebuah tunnel yang menghubungkannya. Dengan adanya teknologi tunnel ini, Anda tidak perlu pusing dengan pengaturan-pengaturan yang ada di luar tunnel tersebut. Asalkan sumber dari tunnel tersebut dapat menjangkau tujuannya, maka tunnel akan terbentuk.

2.4.11. Penggunaan Teknologi VPN

VPN memang telah menjadi sebuah teknologi alternatif sejak lama. Dunia bisnis juga sudah tidak sungkan untuk menggunakan VPN sebagai kunci dari proses bisnisnya. Seperti misalnya pemesanan tiket perjalanan, transaksi perbankan, transaksi informasi keuangan, dan banyak lagi sektor penting juga sudah mempercayakan VPN sejak lama. Dilihat dari segi siapa saja yang dapat terkoneksi dengan VPN dan apa saja yang dapat dijangkau oleh pihak yang terkoneksi tersebut, VPN dapat dibagi menjadi dua jenis. Jenis-jenis tersebut adalah sebagai berikut:

2.4.11.1. Intranet VPN

Intranet VPN merupakan koneksi VPN yang membuka jalur komunikasi pribadi menuju ke jaringan lokal yang bersifat pribadi melalui jaringan publik seperti Internet. Melalui VPN jenis ini, biasanya para pengguna VPN dapat langsung mengakses file-file kerja mereka dengan leluasa tanpa terikat dengan tempat dan waktu. Koneksi ke kantor pusat dapat dilakukan dari mana saja, dari kantor pusat menuju ke kantor cabang Anda dapat membuat koneksi pribadi, dan dari kantor cabang juga memungkinkan untuk dibuat jalur komunikasi pribadi nan ekonomis asalkan menggunakan VPN.

2.4.11.2. Extranet VPN

Extranet VPN biasanya adalah fasilitas VPN yang diperuntukkan bagi pihak-pihak di luar anggota organisasi atau perusahaan Anda, namun mempunyai hak dan kepentingan untuk mengakses data di dalam kantor Anda.

Biasanya 64 penggunaan VPN jenis ini diperuntukkan bagi para customer, vendor, supplier, partner, dan banyak lagi pihak luar yang juga memiliki kepentingan di dalam jaringan Anda.

2.4.12. Mikrotik

Mikrotik RouterOS™ adalah sistem operasi dan yang dapat digunakan untuk menjadikan komputer manjadi router network yang handal, mencakup berbagai fitur lengkap untuk network dan wireless.



Gambar 2.14Negara asal mikrotik

Disamping software router operating system, mikrotik juga mengembangkan hardware dengan spesifikasi dan karakteristik unik serta mempunyai kehandalan sebagai mesin router. Dengan dipasarkannya Mikrotik RouterBoardTM dalam berbagai seri memudahkan kita untuk memilih produk sesuai dengan kebutuhan. Fleksibilitas ini salah satu faktor yang menjadikan mikrotik RouterBoard booming dan menjadi pilihan ekonomis dengna kualitas prima disamping banyak keunggulan-keunggulan lainnya.



Gambar 2.15 Routerboard

Mikrotik RouterOS adalah sistem operasi untuk Router dari Mikrotik berbasis pada Linux Software Programme. Pada saat sekarang, mikrotik dapat dijalankan

melalui program berbasis windows yang dinamakan winbox, sehingga user dapat dengan mudah mengakses dan mengkonfigurasi router sesuai dengan kebutuhan dengan mudah dan efektif dan efisien. Memperkecil kesalahan pada waktu konfigurasi, mudak dipahami dan customize sesuai yang kita inginkan. Fitur-fitur mikrotik router OS cukup banyak, bahkan lebih lengkap dibanding routerOS yang lain, dan sangat membantu kita dalam berimprovisasi untuk mencari solusi dari kendala yang ada di lapangan. Berikut overview tentang karakter dan kemampuan mikrotik routerOS, diantaranya adalah sebagai berikut :

2.4.12.1. Penanganan Protokol TCP/IP

Mikrotik dapat melakukan pengaturan – pengaturan pada protokol tcp/ip yang meliputi :

a. Firewall dan NAT

   Paket filtering yang stabil, filtering peer to peer, source and destination. NAT diklasifikasikan oleh source MAC, ip address, ports, protocols, pilihan protocols, interfaces, internal marks, content, matching.

b. Routing – static

   Static routing, multi path routing yang efisien, policy based routing, RIP v1, V2, OSPF v2, BGP v4.

c. Data rate management

   Per ip / protocol / subnet / port / firewall mark , HTB, PCQ , RED, SFQ, byte limited queue, paket limited queue, pembatasan hirarkis berjenjang, CIR, MIR

d. Hotspot

   Hotspot gateway dengan RADIUS autentikasi dan akunting, pembatasan data rate, quota traffic, inmformasi status real time, walled garden, HTML login page customize, mendukung iPass, SSL secure authentication.

e. Point to point tunneling protocol

   PPTP, PPPoE and L2TP access concentrator and clients, PAP, CHAP, MSCHAPv1, RADIUS authentication and accounting, MPPE encryption, PPPoE dial on demand.

f. Simple tunnels

IPIP tunnels, EoIP (ethernet over IP), IP sec – IP security AH and ESP protocols.

g. Web proxy

FTP, HTTP and HTTPS caching proxy server, transparent HTTP caching proxy, mendukung SOCKS protocol, mendukung caching drive terpisah,access control list, caching list, parent proxy support dengan nama disesuaikan untuk pemakain alokal, dynamic DNS client, local DNS cache with static entries

h. DHCP

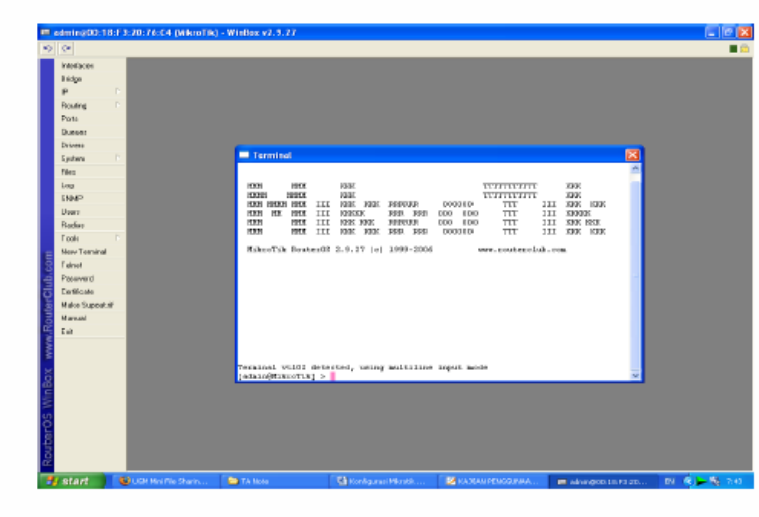
DHCP server per interface, DHCP relay, DHCP client, multiple DHCP Network, static and dynamic DHCP leases

i. Universal client
j. VRRP protocol untuk penggunaan tinggi
k. UPnP
l. NTP
m. Monitoring dan accounting
n. SNMP
o. M3p (mikrotik packet packer protocol for wireless link and ethernet)
p. MNDP (mikotik neighbor discovery protocol)
q. Tools

ping, traceroute, bandwith test, ping flood, telnet, SSH, packet sniffer

2.4.12.2. Pilihan Konfigurasi

RouterOS menyediakan interface konfigurasi command line interface yang kuat. Anda juga bisa mengelola router melalui winbox. Winbox lebih mudahdigunakan dan mendukung remote programming yang mudah digunakan dan dapat dijalankan pada komputer berbabasis windows. Sedangkan kalau kita menggunakan Command line, kita harus hafal perintah-perintah yang akan digunakan beserta opsi-opsi yang menyertainya.



Gambar 2.12 Routerboard

Feature utama:

1. User interface yang bersih dan konsisten
2. Konfigurasi dan monitoring yang sesuai waktu
3. Multiple connections
4. Mengikuti aturan pengguna
5. Action history, undo/redo actions
6. Safe mode operation
7. Script bisa dijadwalkan untuk eksekusi waktu tertentu, periodik atau insidentil. Semua perintah command line mendukung scripts.

Jika router tidak dikenal, hanya ada dua cara untuk mengkonfigurasikannya

1. local terminal console

   AT, PS/2 or USB keyboard and VGA compatible video card dengan monitor.

2. Serial console

   Menggunakan port serial yang pertama (COM1) yang diset deafault ke 9600bit/s, 8 data bits, 1 stop bits, no parity.

Setelah router dikonfigurasikan, harus dikelola dengan menggunakan interface berikut :

1. local terminal console

AT, PS/2 or USB keyboard and VGA compatible video card dengan monitor.

2. Serial console

   Menggunakn port serial yang pertama (COM1) yang diset deafault ke 9600bit/s, 8 data bits, 1 stop bits, no parity.

3. Telnet

   telnet server diposisikan pada port TCP 23 secara default.

4. SSH

   Cara ini tersedia jika paket security d2nstalasi, menggunakan port TCP 22.

5. MAC telnet

   Server mikrotik MAC Telnet protocol secara default berjalan di semua interface ethernet yang ada.

6. Winbox

   Winbox adalah administrasi routerOS remote GUI for windows, menggunakan port TCP 3986.Karakteristik mikrotik routerOS diatas cukup membuktikan bahwa dengan system hardware, software, brainware yang terintegrasi dengan seimbang, mampu mempersembahkan kinerja optimal dan mendobrak berbagai kendala penghalang.