BAB II

LANDASAN TEORI

Pada bab ini akan dibahas berbagai teori yang mendasari penyusunan tugas akhir ini.

2.1 Perkembangan WLAN (Wireless LAN)

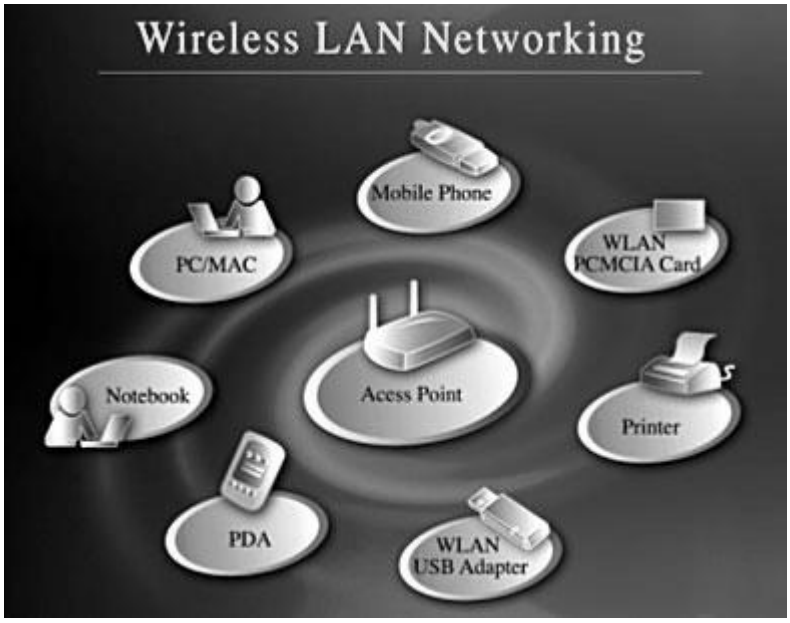
Sekitar akhir 1970-an IBM mengeluarkan hasil percobaan mereka dalam merancang WLAN dengan teknologi IR, perusahaan lain seperti *Hewlett-Packard* (HP) menguji WLAN dengan RF. Kedua perusahaan tersebut hanya mencapai data rate 100 Kbps. Karena tidak memenuhi standar IEEE 802 untuk LAN yaitu 1 Mbps maka produknya tidak dipasarkan. Baru pada tahun 1985, *Federal Communication Commission* (FCC) menetapkan pita *Industrial,Scientific and Medical* (ISM band) yaitu 902-928 MHz, 2400-2483.5 MHz dan 5725-5850 Mhz yang bersifat tidak terlisensi, sehingga pengembangan WLAN secara komersial memasuki tahapan serius. Barulah pada tahun 1990 WLAN dapat dipasarkan dengan produk yang menggunakan teknik *spread spectrum* (SS) pada pita ISM, frekuensi terlisensi 18-19 GHz dan teknologi IR dengan data rate lebih dari 1 Mbps.

Pasar yang menjadi targetnya adalah pabrik, kantor-kantor yang mengalami kesulitan dalam pengkabelan (seperti kantor dengan interior marmer dan lain-lain), perkulakan, laboratorium, tempat-tempat yang bersifat sementara (seperti ruang kuliah, rapat, konfrensi, dan lain-lain) dan kampus).

Dengan adanya berbagai merek perangkat keras dan lunak, maka diperlukan suatu standar, di mana perangkat-perangkat yang berbeda merek dan difungsikan pada perangkat merek lain. Standar-standar WLAN adalah IEEE 802.11, WINForum dan HIPERLAN.

Wireless Information Network Forum (WINForum) dilahirkan oleh Apple Computer dan bertujuan untuk mencapai pita Personal Communication Service (PCS) yang tidak terlisensi untuk aplikasi data menawarkan peraturan-peraturan

yang sangat minim dan akses yang adil. High Performance Radio Local Area Network (HIPERLAN) dilahirkan oleh European Telekommunications Standards Insitute (ETSI) yang memfokuskan diri pada pita 5.12-5.30 GHz dan 17.1-17.3 GHz, IEEE 802.11 dilahirkan oleh Institute Electrical and Electronics Engineer (IEEE) dan berfokus pada pita ISM dan memanfaatkan teknik spread spectrum (SS) yaitu Direct Sequence (DS) dan Frequency Hipping (FH), standar ini adalah yang paling banyak dipakai.



Gambar 2.1 Koneksi Jaringan wireless

2.1.1 Mengenal Jaringan Wireless

Teknologi wireless sangat cocok dan banyak digunakan sebagai pengganti kabel-kabel seperti kabel mouse, kabel jaringan LAN dan bahkan kabel WAN (*Wide Area Network*). Semakin jauh daya jangkauan wireless semakin tinggi juga kebutuhan hardware yang diperlukan. Teknologi wireless yang popular untuk kelompok LAN adalah Wi-Fi. Kecepatan transfer data Wi-Fi yang saat ini sudah mencapai 54 Mps. Memang masih tidak sebanding dengan kecepatan dengan kabel UTP yang sudahmencapai 1 Gbps. Walau demikian sebagian besar pengguna merasa kecepatan ini sudah memadai.

2.1.2 Konsep Jaringan Komputer

Jaringan komputer adalah sekelompok komputer otonom yang saling berhubungan antara satu dengan lainnya dengan menggunakan protokol komunikasi untuk komputer, sehingga dapat saling berbagi informasi, program-program, penggunaan bersama perangkat keras seperti *printer*, *hardisk*, dan lain sebagainya. Selain itu jaringan komputer bisa diartikan sebagai kumpulan sejumlah terminal komputer yang berada diberbagai lokasi yang terdiri dari lebih dari satu komputer yang saling berhubungan.

Pembangunan jaringan komputer dapat mencegah ketergantungan pada komputer pusat. Setiap proses data tidak harus dilakukan pada satu komputer saja, melainkan dapat didistribusikan ke tempat lainnya. Sehingga dapat terbentuk data yang terintegrasi dengan demikian memudahkan pemakai untuk memperoleh dan mengolah informasi setiap saat.

Dengan adanya jaringan komputer ini, maka pengembangan peralatan dapat dilakukan dengan mudah dan menghemat biaya. Jaringan komputer dapat memudahkan pemakai dalam merawat *Central Processing Unit* (CPU), misalnya untuk memberikan perlindungan terhadap serangan virus, maka pemakai cukup memusatkan perhatian pada CPU yang ada di komputer pusat.

Sistem jaringan komputer memberikan perlindungan terhadap data. Jaminan keamanan data tersebut diberikan melalui pengaturan hak akses para pemakai dan *password*, serta teknik perlindungan terhadap hardisk sehingga data mendapatkan perlindungan yang efektif.

Dengan adanya pemakaian sumber daya secara bersama-sama, maka pemakai bisa mendapatkan hasil dengan maksimal dan kualitas yang tinggi. Selain itu data atau informasi yang diakses selalu terbaru, karena setiap ada perubahan yang terjadi dapat segera lengsung diketahui oleh setiap pemakai.

2.2 Berdasarkan Ruang Lingkup Geografis

Berdasarkan ruang lingkup geografisnya terdapat tiga jenis jaringan komputer, antara lain :

2.2.1 Local Area Network

Jarak jangkauan *Local Area Network* (LAN) tidak terlalu jauh. Biasanya diterapkan pada suatu gedung atau antar gedung dalam suatu kompleks perkantoran atau sekolah. LAN merupakan suatu sistem komunikasi data yang mengijinkan sejumlah peralatan yang berdiri sendiri (*independent*) untuk dapat berkomunikasi secara langung satu dengan yang lain dengan kecepatan transfer 1 Gbps atau 1000 Mbps yang terdapat pada satu otoritas.

2.2.2 Metropolitan Area Network

Jarak jangkaunya lebih luas dari LAN. Jangkauan *Metropolotan Area Network* (MAN) dapat mencapai antar kota. Contoh penerapan dari MAN ialah peyediaan layanan internet oleh *Internet Service Provider* (ISP). Pengguna jasa ISP ini akan tercakup dalam jaringan MAN yang disediakan oleh ISP tersebut.

2.2.3 Wide Area Network

Jaringan *Wide Area Network* (WAN) mempunyai cakupan terluas, bahkan dapat dikatakan mencakup seluruh dunia. Jaringan ini sendiri dapat dihubungkan dengan menggunakan satelit dan media kabel fiber optic. Jaringan *Wide Area Network* (*WAN*) adalah kumpulan dari LAN dan/atau *workgroup* yang dihubungkan dengan menggunakan alat komunikasi modem dan jaringan Internet, dari/ke kantor pusat dan kantor cabang, maupun antar kantor cabang. Dengan sistem jaringan ini, pertukaran data antar kantor dapat dilakukan dengan cepat serta dengan biaya yang relatif murah. Sistem jaringan ini dapat menggunakan jaringan Internet yang sudah ada, untuk menghubungkan antara kantor pusat dan kantor cabang atau dengan PC *Stand Alone/Notebook* yang berada di lain kota ataupun negara.

2.4 Berdasarkan Service

2.4.1 Intranet

Service yang diberikan hanya diberikan kepada pihak-pihak dalam yang mendapat ijin dari otoritas jaringan, dan bukan untuk pihak luar. Terdapat kerahasiaan di dalamnya.

2.4.2 Extranet

Terdapat suatu layanan yang juga dapat digunakan oleh pihak luar yang telah memiliki *account* yang diijinkan. Layanan yang diberikan kepada pihak luar ini bersifat terbatas.

2.4.3 Internet

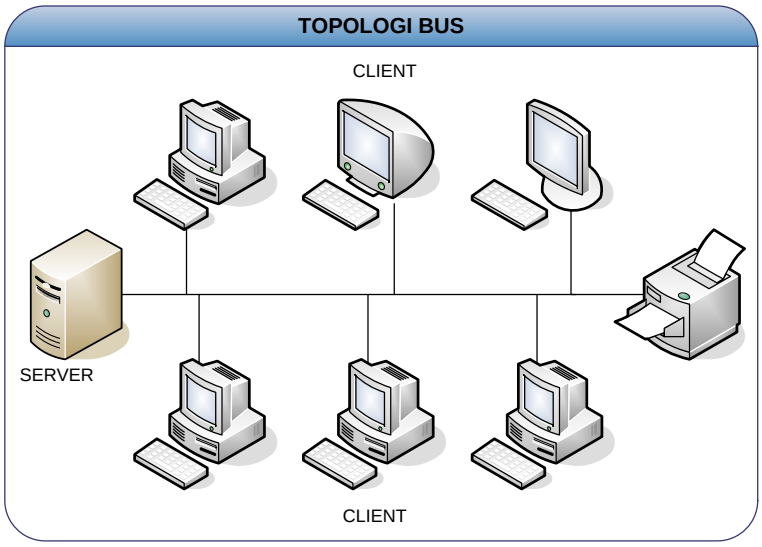
Layanan yang disediakan diberikan secara luas kepada pihak manapun, tanpa harus mendapatkan *account* terlebih dahulu.

2.5 Topologi Jaringan Komputer

Topologi jaringan komputer adalah pola hubungan antar terminal dalam suatu jaringan komputer. Ada beberapa macam topologi yang dapat digunakan, tetapi bentuk topologi yang utama adalah *Bus, Star*, dan *Ring.*

2.5.1 Topologi *Bus*

Pada topologi *Bus* semua terminal terhubung ke jalur komunikasi. Informasi yang dikirim akan melewati semua terminal pada jalur tersebut. Jika alamat yang tercantum dalam data atau informasi yang dikirim sesuai dengan alamat terminal yang dilewati, maka data atau informasi tersebut akan diterima dan diproses. Jika alamat tersebut tidak sesuai, maka informasi tersebut akan diabaikan oleh terminal yang dilewati.

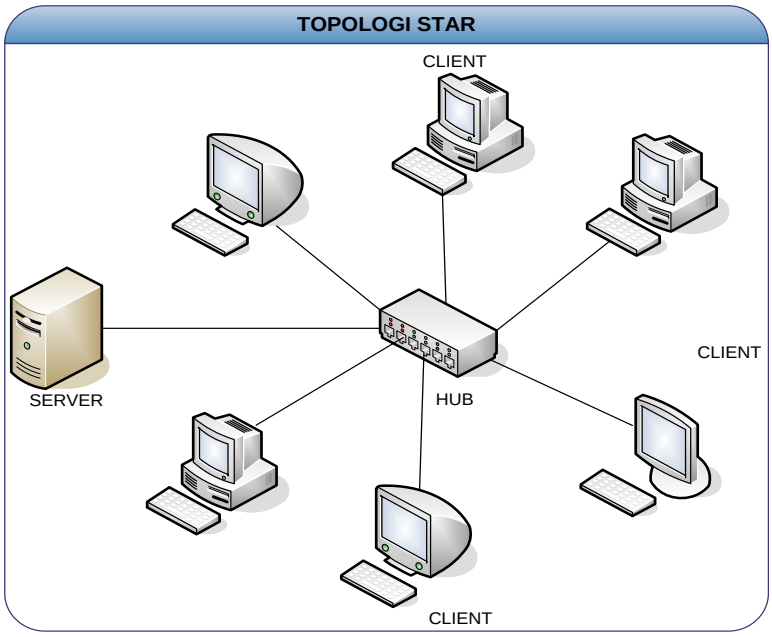


Gambar 2.2 *Topologi Bus*

Jumlah terminal dapat ditambahkan dan dikurangi secara fleksibel. Namun demikian, jumlah terminal hendaknya perlu dibatasi, karena pada topologi model ini, jika terminal yang terhubung sangat banyak, maka kinerja jaringan akan turun drastis. Kekurangan yang lain dari topologi ini, bila ada terminal yang mati, maka operasional jaringan akan terganggu.

2.5.2 Topologi *Star*

Dalam topologi *star*, sebuah terminal pusat bertindak sebagai pengatur dan pengendali semua komunikasi data yang terjadi. Terminal-terminal lain terhubung padanya dan pengiriman data dari satu terminal ke terminal lainnya melalui terminal pusat. Terminal pusat akan menyediakan jalur komunikasi khusus untuk dua terminal yang akan berkomunikasi. Sebagai salah satu contoh penggunaan topologi *Star* adalah jaringan telepon.

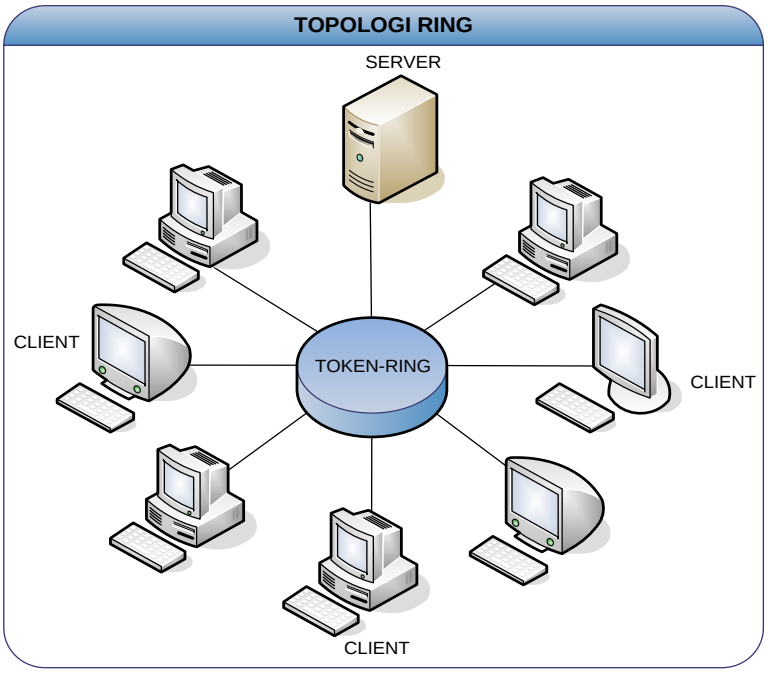


Gambar 2.3 *Topologi Star*

Topologi ini mudah untuk dikembangkan, baik untuk penambahan maupun pengurangan terminal. Banyak terminal yang dapat terhubung tergantung pada jumlah port yang tersedia pada hub yang digunakan. Pada topologi *Star* ini, hub yang digunakan akan menjadi titik kritis, sehingga perlu adanya perhatian dan pemeliharaan terhadap hub tersebut.

2.5.3 Topologi *Ring*

Jaringan komputer lokal dengan topologi ini mirip dengan topologi Bus, tetapi kedua terminal yang berada diujung saling dihubungkan sehingga menyerupai lingkaran. Setiap informasi yang diperoleh diperiksa alamatnya oleh terminal yang dilewatinya. Jika bukan untuknya, informasi dilewatkan sampai menemukan alamat yang benar. Setiap terminal dalam jaringan komputer lokal saling tergantung sehingga jika terjadi kerusakan pada satu terminal maka seluruh jaringan akan terganggu.



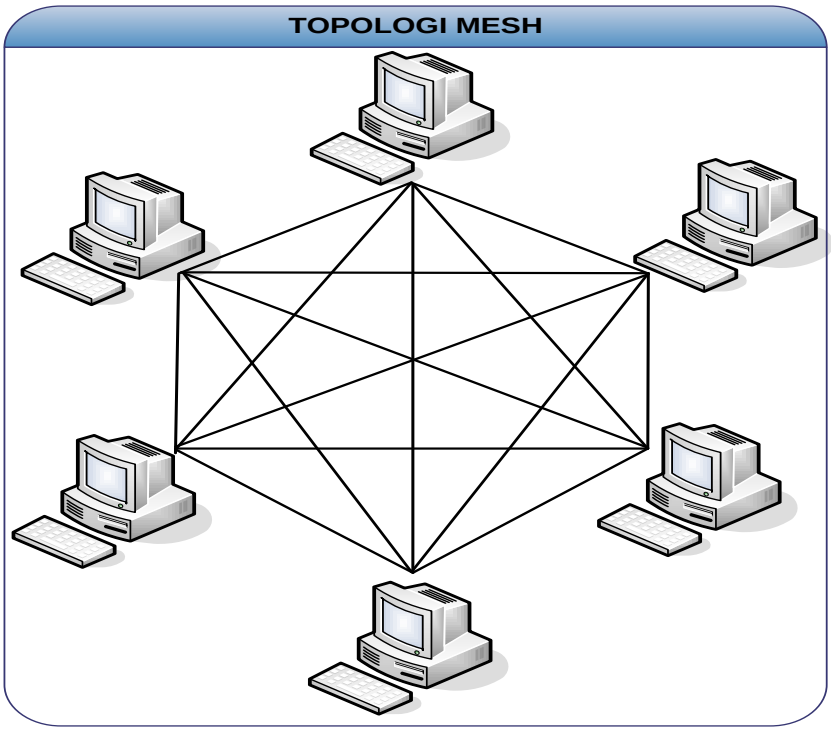
Gambar 2.4 ***Topologi Ring***

2.5.4 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 ini dikembangkan dengan ruang lingkup yang luas dengan jarak antar komputer berjauhan.

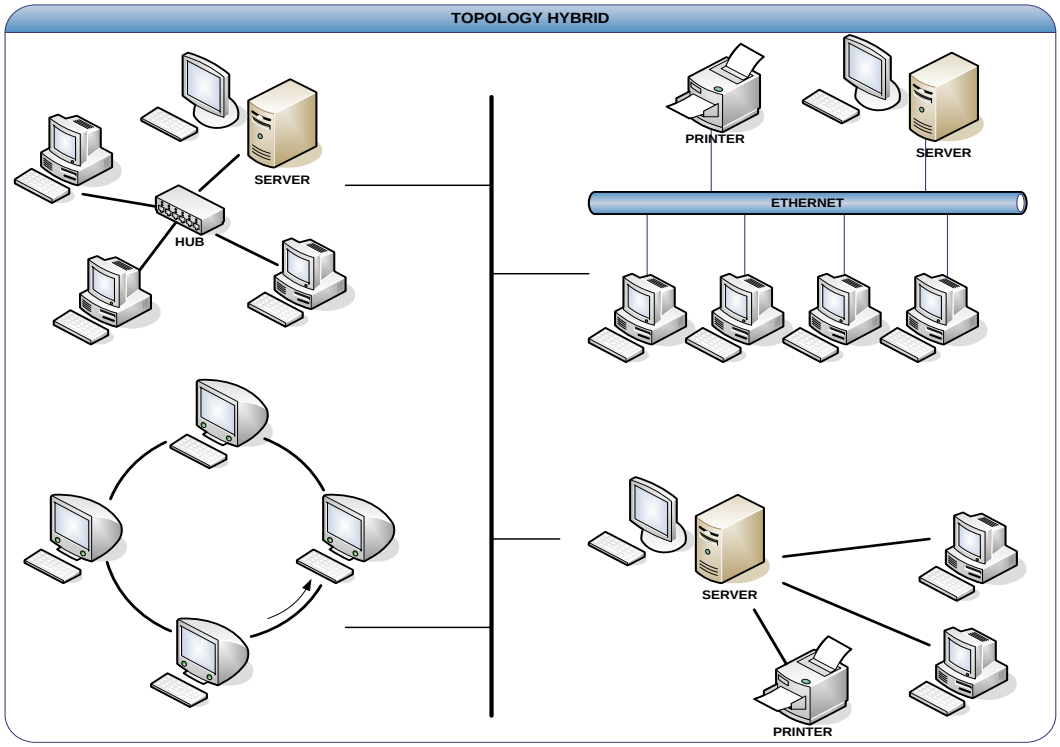
Topologi mesh memberikan keamanan data yang lebih baik, yaitu dengan menggunakan metode *multiplexing*, dimana pesan dapat dipecah-pecah menjadi beberapa paket dan dilewatkan pada jalur yang berbeda.



Gambar 2.5 Topologi Mesh

2.5.3 Topologi Hybrid

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

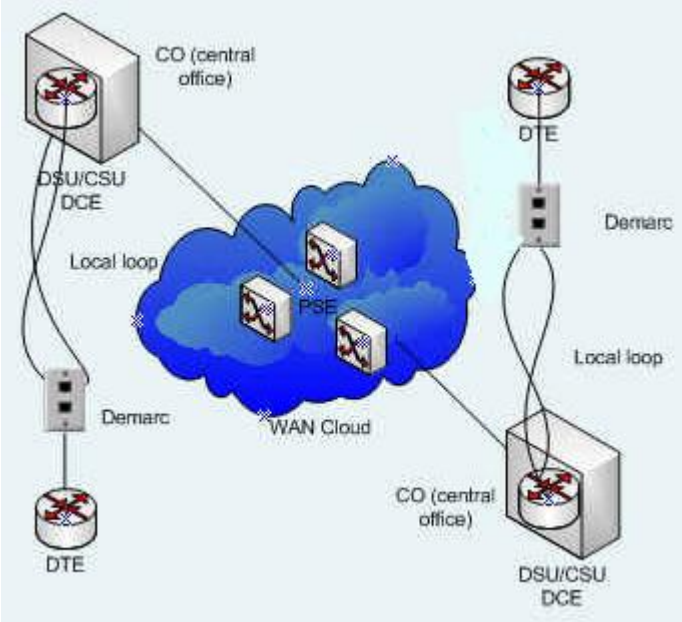


Gambar 2.6 Topologi Hybrid

2.6 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 2.7 Struktur 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.

Demarc adalah titik demarkasi dimana perkabelan dari perusahaan telpon terhubung ke perkabelan disisi rumah pelanggan. Umumnya pelanggan 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.

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.

2.6.1 Standar Koneksi WAN

Koneksi standard WAN yang direkomendasikan adalah sebagai berikut.

a Untuk layanan WAN menggunakan koneksi serial, gunakanlah kabel serial V.35

b Untuk koneksi WAN berkecepatan rendah (dibawah 64Kbps) yang biasa diasosiasikan dengan PSTN analog, gunakanlah kebel serial RS-232.

c Untuk koneksi ISDN BRI, kabel UTP (Cat5) yang digunakan seharusnya memakai kabel dengan warna yang berbeda (putih atau kuning) dari kabel UTP yang umum dipakai untuk menunjukkan bahwa kabel tersebut adalah koneksi WAN. Perlu diperhatikan bahwa peralatan ISDN yang disambungkan pada piranti yang bukan ISDN bisa menyebabkan kerusakan.

d Untuk koneksi WAN ISDN, Terminal Adapter (TA) haruslah dihindari; sebaiknya gunakan router ISDN native.

e Semua perkabelan haruslah di dokumentasikan dan diberi label dengan jelas.

2.6.2 Kategori Koneksi WAN

a *Dedicated Point-to-Point* atau *leased line* (*serial synchronous*) seperti T1, T3

b Jaringan *circuit-switched* (*asynchronous serial*) seperti ISDN

c Jaringan *Packet-switched* (*synchronous serial*) seperti frame relay, x.25

2.6.3 Dedicated connection atau leased line

adalah koneksi sambungan permanen *point-to-point* antara dua piranti yang mempunyai karakteristik berikut ini:

a *Dedicated point-to-point – serial synchronous.*

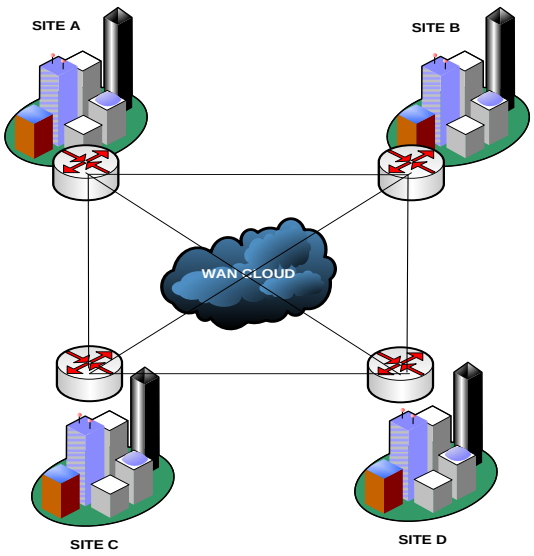
b Koneksi permanen, seperti T1, T3.

c Ketersediannya tinggi.

d Sambungan biasanya disewa dari penyedia layanan WAN.

e *Leased line* lebih mahal dibanding solusi WAN lainnya.

f Menggunakan koneksi terpisah di masing-masing titik.



Gambar 2.8 **Koneksi WAN *Point to Point***

Penggunaan Sambungan WAN jenis *Leased Line*

a Jika jaringan kita mempunyai trafik yang sangat tinggi melalui jaringan WAN.

b Jika memerlukan sambungan konstan antar site.

c Hanya mempunyai beberapa interkoneksi site saja.

2.6.4 Jaringan Circuit-Switched

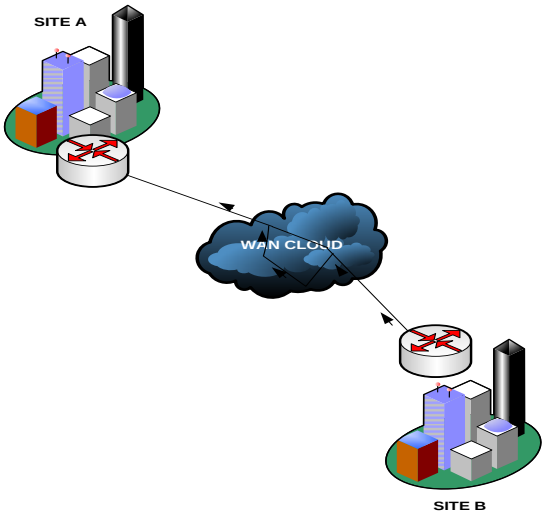
Jenis koneksi jaringan *circuit-switched* memberikan alternatif dari sambungan *leased line*, memungkinkan kita menggunakan sambungan bersama (*share line*). Koneksi WAN jenis ini bekerja dua arah, koneksi WAN *dial-in* dan *dial-out*. Saat kita memakai koneksi WAN *circuit-switched*, maka:

a Komputer pengirim *dials-in* ke sambungan dan terbentuklah koneksi WAN

b Komputer penerima mengirim pemberitahuan dan mengunci sambungan

c Komputer pengirim mentransmisikan data melalui koneksi WAN ini

d Setelah transmisi selesai, koneksi dilepas agar *user* yang lain bisa memakai



Gambar 2.9 Koneksi WAN *Circuit Switched*

Jaringan *circuit switched* menggunakan S*witch Virtual Circuit* (SVC). Suatu jalur *dedicated* transmisi data terbentuk sebelum komunikasi dimulai dengan cara melepas *switch electric*. Jalur ini akan tetap terbentuk sampai komunikasi berakhir.

2.6.5 Jaringan Packet-Switched

Jaringan *packet-switched* tidak memerlukan sambungan tersendiri atau sambungan cadangan sementara. Sebaliknya jenis jaringan *packet-switched* ini memungkinkan jalur paket data di set secara dinamis ketika data mengalir melalui jaringan. Jenis koneksi jaringan ini mempunyai karakteristik sebagai berikut:

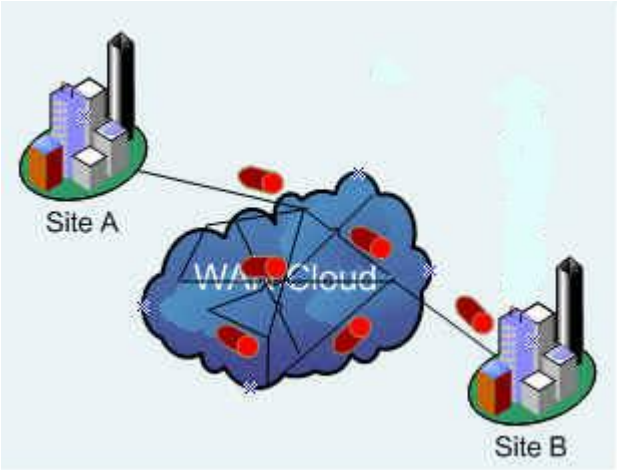
a. *Message* dipecah kedalam paket-paket

b. Paket-paket menjelajah secara *independen* melalui interjaringan (yaitu mengambil jalur yang berbeda)

c. Pada sisi penerima paket di *assembling* ulang pada urutan yang tepat

d. Piranti pengirim dan penerima mengasumsikan suatu koneksi yang ’selalu *on*’ (tidak memerlukan dial-up)

Jenis koneksi jaringan WAN ini menggunakan *Permanent Virtual Circuit* (PVC). Walaupun suatu PVC terlihat terhubung langsung – jalur WAN tersendiri, jalur yang diambil setiap paket melalui inter-jaringan dapat berbeda



Gambar 2.10 Koneksi WAN paket switched

Jaringan *dedicated* dan *packet-switched* mempunyai sambungan koneksi WAN yang selalu tersedia ke dalam jaringan, sementara jaringan *circuit-switched* pertama harus membuat jalur koeksi WAN terbentuk terlebih dahulu antar piranti (melalui *dial-up*). *Dial-on-Demand Routing* (DDR) dapat mensimulasikan koneksi WAN yang selalu on. Dengan DDR router secara automatis membuka koneksi WAN baru jika data perlu dikirim, dan kemudian menutup sendiri saat sambungan jadi *idle.* Teknologi WAN terbaru memperbaiki proses koneksi WAN menjadi lebih pendek.

2.7 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 E didefinisikan, tetapi tidak digunakan dalam penggunaan normal, dan kelas E untuk keperluan eksperimental

2.7.1 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 IP address 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.

2.8 Elemen Dasar Jaringan

Jaringan komputer tersusun dari beberapa elemen dasar yang meliputi komponen *hardware* dan *software*, yaitu :

2.8.1 Komponen *Hardware*

a. *Personal computer* (PC) :



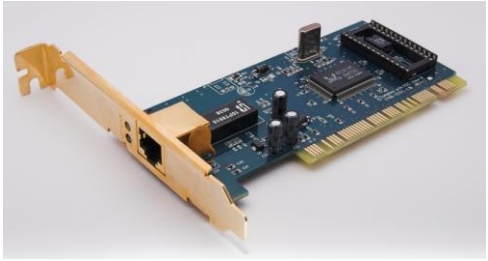
Gambar 2.11 PC Desktop

Tipe personal komputer yang digunakan di dalam jaringan akan sangat menentukan untuk kerja dari jaringan tersebut. Komputer dengan untuk kerja tinggi akan mampu mengirim dan mengakses data dalam jaringan

dengan cepat. Di dalam jaringan tipe *Client-Server*, komputer yang difungsikan sebagai *server* mutlak harus memiliki unjuk kerja yang lebih tinggi dibandingkan komputer-komputer lain sebagai workstation-nya, karena *server* akan bertugas menyediakan fasilitas dan mengelola operasional jaringan tersebut.

b. *Network Interface Card* (NIC) :

Berdasarkan tipe bus, ada beberapa tipe *Network Interface Card* (NIC) atau *Network Card*, yaitu ISA dan PCI. Saat ini terdapat jenis *network card* yang banyak digunakan, yaitu PCI.



Gambar 2.12 *Network interface card*

c. *Ethernet* :

Dalam jaringan dengan *protocol* akses CSMA/CD atau *Carrier Sense Multiple Access with Collision Detection*, suatu node (A) yang akan mengirimkan data akan memeriksa dahulu kondisi jalur data. Bila tidak terdapat aliran data/kosong maka node tersebut akan mengirimkan datanya dan bila node lain (B) yang sedang menggunakan jalur data maka node (A) akan menunggu dan akan mencoba memeriksa kembali. Dalam protokol akses ini dimungkinkan pada suatu saat terjadi beberapa node mengirimkan datanya secara bersamaan sehingga mengakibatkan collision atau tabrakan. Dalam kondisi demikian node-node tersebut akan batal mengirimkan data dan akan mencobanya kembali bila jalur tidak sibuk.

d. *Network Adapter Card* :

Setiap *network card* akan memiliki driver atau program yang berfungsi untuk mengaktifkan dan mengkonfigurasi *network adapter* tersebut disesuaikan dengan lingkungan dimana *network card* tersebut dipasang agar dapat digunakan untuk melakukan komunikasi data.

2.8.2 Komponen *Software*

a. Sistem Operasi Jaringan

Untuk mengelola suatu jaringan diperlukan adanya sistem operasi jaringan. Sistem operasi jaringan dibedakan menjadi dua berdasarkan tipe jaringannya, yaitu sistem operasi *client-server* dan operasi jaringan peer to peer.

b. *Network Adapter* Driver

Agar perangkat keras *network interface card* (NIC) dapat berkomunikasi dengan sistem operasi, dibutuhkan *network adapter driver* sebagai jembatan komunikasi antara kedua poin berikut.

c. Protokol Jaringan

Suatu standarisasi yang mengatur bagaimana caranya agar antar komponen diatas dapat berkomunikasi.

2.8.3 Sharing Resource

Sharing resource bertujuan agar seluruh program, peralatan atau *peripheral* lainnya dapat dimanfaatkan oleh setiap orang yang ada pada jaringan komputer tanpa terpengaruh oleh lokasi maupun pengaruh dari pemakai. Dengan kata lain, seorang pemakai yang letaknya yang sangat jauh sekalipun dapat memanfaatkan data maupun informasi yang lainnya tanpa mengalami kesulitan. Jadi dengan adanya *sharing resources* ini dapat menekan biaya pembelian *peripheral* atau *software* karena adanya peningkatan sumber daya tersebu

2.8.4 Integrasi Data

Pembangunan jaringan komputer dapat mencegah ketergantungan pada komputer pusat. Setiap proses data tidak harus dilakukan pada satu komputer saja, melainkan dapat didistribusikan ketempat lainnya. Oleh sebab inilah maka dapat terbentuk data yang terintegrasi sehingga dengan demikian memudahkan pemakai untuk memperoleh dan mengolah informasi setiap saat.

2.8.5 Pengembangan dan Pemeliharaan

Dengan adanya jaringan komputer ini, maka pengembangan peralatan dapat dilakukan dengan mudah dan menghemat biaya. Jaringan komputer dapat memudahkan pemakai dalam merawat *hardisk* dan peralatan lainnya, misalnya untuk memberikan perlindungan terhadap serangan virus maka pemakai cukup memusatkan perhatian pada hardisk yang ada di komputer *server*.

2.8.6 Keamanan Data

Sistem jaringan komputer memberikan perlindungan terhadap data. Jaminan keamanan data tersebut diberikan melelui pengaturan hak akses para pemakai dan *password*, serta teknik perlindungan terhadap *hardisk* sehingga data mendapatkan perlindungan yang efektif.

a. Sumber Daya Lebih Efisien dan Informasi Terkini

Dengan adanya pemakaian sumber daya secara bersama-sama, maka pemakai bisa mendapatkan hasil dengan maksimal dan kualitas yang tinggi. Selain itu data atau informasi yang diakses selalu terbaru, karena setiap ada perubahan yang terjadi dapat segera lengsung diketahui oleh setiap pemakai.

2.9 Konsep Dasar *Internet Protocol*

Pada dasarnya, komunikasi data merupakan proses mengirimkan data dari satu komputer ke komputer yang lain. Untuk dapat mengirimkan data, pada komputer harus ditambahkan alat khusus, yang dikenal dengan *network interface* (*interface* jaringan). Jenis *interface* jaringan ini bermacam-macam, tergantung pada media fisik yang digunakan untuk men-*transfer* data tersebut.

Dalam proses pengiriman data ini terdapat beberapa masalah yang harus dipecahkan. Pertama, data harus dikirim ke komputer yang tepat, sesuai tujuannya. Hal ini akan menjadi rumit jika komputer tujuan *transfer* data ini tidak berada pada jaringan lokal, melainkan ditempat yang jauh. Jika lokasi komputer yang saling berkomunikasi ”jauh” (secara jaringan) maka terdapat kemungkinan data rusak atau hilang karenanya perlu ada mekanisme yang mencegah rusaknya data ini. Hal ini yang perlu diperhatikan ialah pada komputer tujuan *transfer* data mungkin terdapat lebih dari satu aplikasi yang menunggu datangnya data. Data yang dikirim harus sampai ke aplikasi yang tepat, pada komputer yang tepat, tanpa kesalahan.

Cara alamiah untuk menghadapi setiap masalah yang rumit ialah memecahkan masalah tersebut menjadi bagian yang lebih kecil. Dalam memecahkan masalah *transfer* data di atas, para ahli jaringan komputerpun melakukan hal yang sama. Untuk setiap problem komunikasi data, diciptakan solusi khusus berupa aturan-aturan yang menangani problem tersebut. Untuk menangani suatu masalah komunikasi data, keseluruhan aturan ini harus kerja sama satu dengan lainnya. Sekumpulan aturan untuk mengatur proses pengiriman data ini disebut sebagai *protokol komunikasi data*. Protokol ini di implementasikan dalam bentuk program komputer (*software*) yang terdapat pada komputer dan peralatan komunikasi data lainnya.

Dalam dunia komunikasi data komputer, protokol mengatur bagaimana sebuah komputer berkomunikasi dengan komputer lain. Dalam jaringan komputer kita dapat menggunkan banyak macam protokol tapi agar sebuah komputer dapat berkomunikasi, keduanya harus mengunakan protokol yang sama. Protokol berfungsi mirip dengan bahasa. Agar dapat berkomunikasi seseorang perlu berbicara dan mengerti bahasa yang mereka gunakan.

2.9.1 Model Referensi OSI dan Standarisasi

Untuk menyelenggarakan komunikasi berbagai macam vendor komputer diperlukan sebuah aturan baku yang standar dan disetejui berbagai pihak. Seperti halnya dua orang yang berlainan bangsa, maka untuk berkomunikasi memerlukan penerjemah/*interpreter* atau satu bahasa yang dimengerti kedua belah pihak.

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 mengembangkan protokolnya.

Model referensi OSI terdiri dari tujuh 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**
7	Aplikasi	Aplikasi	DHCP (Dynamic Host Configuration Protocol)	Protokol untuk distribusi IP pada jaringan dengan jumlah IP yang terbatas
			DNS (Domain Name Server)	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
6	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
5	Sessi		NETBIOS (Network Basic Input Output System)	BIOS jaringan standar
			RPC (Remote Procedure Call)	Prosedur pemanggilan jarak jauh
			SOCKET	Input Output untuk network jenis BSD-UNIX
4	Transport	Transport	TCP (Transmission Control Protocol)	Protokol pertukaran data berorientasi (connection oriented)
			UDP (User Datagram Protocol)	Protokol pertukaran data non-orientasi (connectionless)
3	Network	Internet	IP (Internet Protocol)	Protokol untuk menetapkan routing
			RIP (Routing Information Protocol)	Protokol untuk memilih routing
			ARP (Address	Protokol untuk mendapatkan

				Resolution Protocol)	informasi hardware dari nomer IP
				RARP (Reverse ARP)	Protokol untuk mendapatkan informasi nomer IP dari hardware
2	Datalink	LLC	Network Interface	PPP (Point to Point Protocol)	Protokol untuk point ke point
				SLIP (Serial Line Internet Protocol)	Protokol dengan menggunakan sambungan serial
		MAC		Ethernet, FDDI, ISDN, ATM	
1	Fisik				

2.9.2 Transmision Control Protocol (TCP)

TCP/IP (*Transmission Control Protocol / Internet Protocol*) adalah sekumpulan protokol yang mengatur komuniksai data komputer dengan komputer yang lain maupun komputer dengan jaringan *Internet*. Karena menggunakan bahasa yang sama, yaitu protokol TCP/IP, perbedaan jenis komputer dan sistem operasi tidak menjadi masalah.

Komputer PC dengan menggunakan sistem operasi *Windows* dapat berkomunikasi dengan komputer *Macintos* atau dengan *Sun SPARC* yang menjalankan Solaris. Jadi, jika sebuah komputer menggunakan protokol TCP/IP dan terhubung langsung ke *Internet*, maka komputer tersebut dapat berhubungan dengan komputer di belahan dunia manapun yang juga terhubung ke *Internet*.

Perkembangan TCP/IP yang diterima luas dan praktis menjadi standar defacto jaringan komputer berkaitan dengan ciri-ciri yang terdapat pada protokol itu sendiri :

a. Protokol TCP/IP dikembangkan menggunakan standart protokol yang terbuka.

b. Standart protokol TCP/IP dalam bentuk *Request For Comment* (RFC) dapat diambil oleh siapun tanpa biaya.

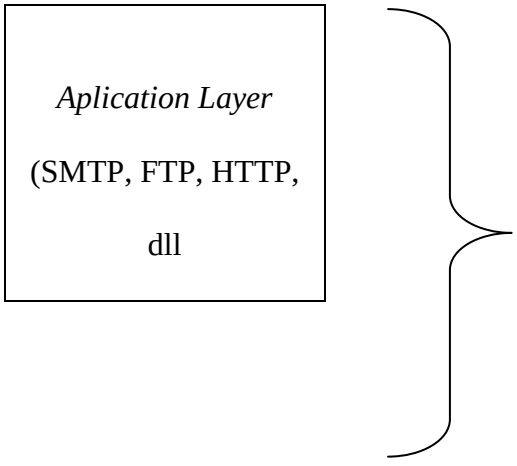
c. TCP/IP dikembangkan dengan tidak tergantung pada sistem operasi atau perangkat keras tertentu.

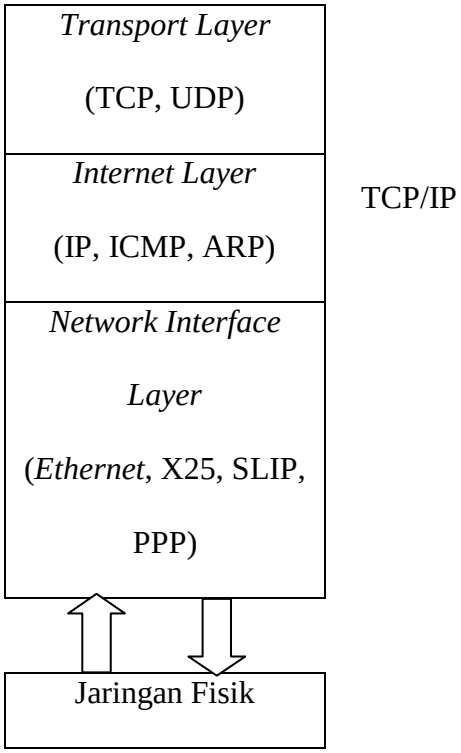
d. Pengembangan TCP/IP dilakukan dengan konsensus dan tidak tergantung pada vendor tertentu.

e. TCP/IP independen terhadap perangkat keras jaringan dan dapat dijalankan pada jaringan *Ethernet*, *Token Ring*, Jalur telepon dial-up, jaringan X25, dan praktis jenis media transmisi apa pun..

f. Pengalamatan TCP/IP bersifat untuk dalam skala global. Dengan cara ini, komputer dapat saling terhubung walaupun jaringannya seluas *internet* sekarang ini.

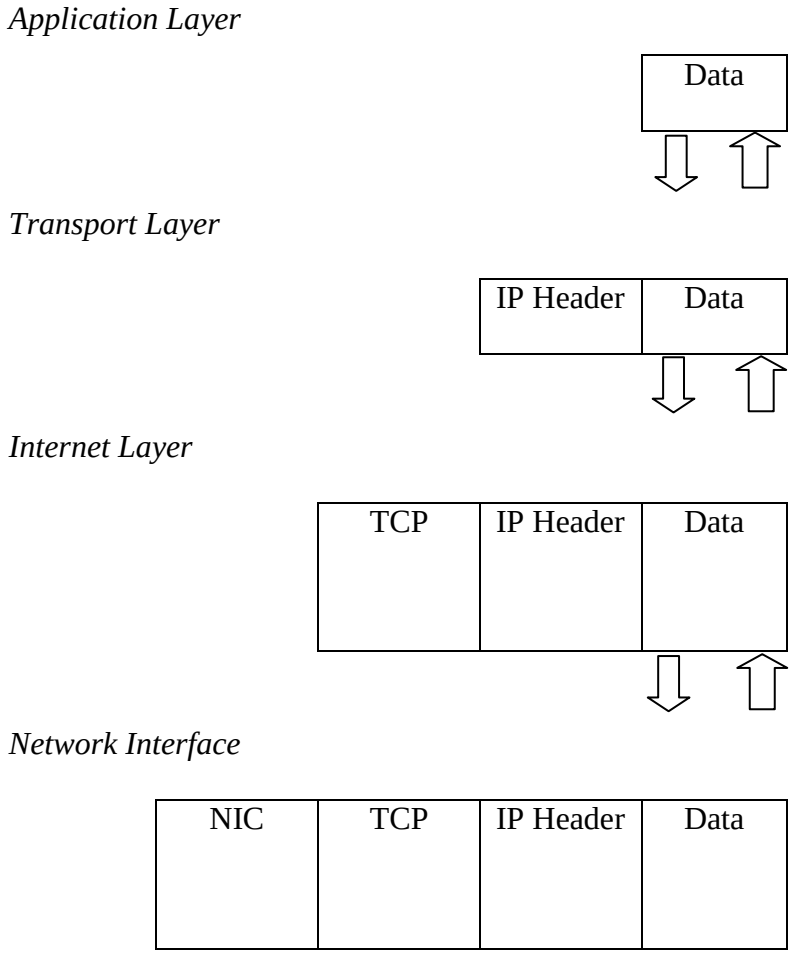
TCP/IP bukanlah sebuah protokol tunggal, tetapi satu kesatuan protokol. TCP/IP merupakan sekumpulan protokol yang didesain untuk melakukan fungsi-fungsi komunikasi data pada *Wide Area Network* (WAN). TCP/IP terdiri dari protokol-protokol yang bertanggung jawab atas bagian-bagian tertentu dari komunikasi data. Berkat prinsip ini, tugas masing-masing protokol menjadi jelas dan sederhana. Protokol yang satu tidak perlu mengetahui cara kerja protokol yang lain, sepanjang ia masih bisa mengirim dan menerima data. Berkat penggunaan prinsip ini, TCP/IP menjadi protokol komunikasi data yang fleksibel. Protokol TCP/IP dapat diterapkan dengan mudah di setiap jenis komputer dan *interface* jaringan, karena sebagian besar isi kumpulan protokol ini tidak spesifik terhadap satu komputer atau peralatan jaringan tertentu. Sekumpulan protokol TCP/IP ini dimodelkan dengan empat *layer* TCP/IP, sebagai mana terlihat pada gambar di bawah ini.





Gambar 2.13 Model protokol TCP/IP

Jika suatu protokol menerima data dari protokol lain di *layer* atasnya, ia akan menambahkan informasi tambahan miliknya ke data tersebut, informasi ini memiliki fungsi yang sesuai dengan fungsi protokol tersebut. Setelah itu, data ini diteruskan lagi ke protokol pada *layer* dibawahnya. Hal ini yang sebaliknya terjadi jika suatu protokol menerima data dari protokol lain yang berada pada *layer* dibawahnya. Jika data ini dianggap *valid*, protokol akan melepas informasi tambahan tersebut, untuk kemudian meneruskan data itu ke protokol lain yang berada pada *layer* di atasnya. Pergerakan data dalam *layer* TCP/IP seperti gambar dibawah ini:



Gambar 2.14 **Pergerakan data dalam *layer* TCP/IP**

TCP/IP terdiri atas empat lapis kumpulan protokol yang bertingkat. Keempat lapisan/*layer* tersebut adalah :

2.9.2.1 Network Interface Layer

Bertanggung jawab mengirim dan menerima data ke dan dari media fisik (berupa kabel, serat optik atau gelombang radio), maka dari itu harus mampu menerjemahkan sinyal listrik menjadi digital yang dimengerti komputer.

2.9.2.2 Internet Layer

Bertanggung jawab dalam proses pengiriman paket ke alamat yang tepat. Pada *layer* ini terdapat tiga macam protokol yaitu:

a. IP (*Internet Protocol*) berfungsi untuk menyampaikan paket data ke alamat yang tepat, IP memiliki sifat sebagai *unrealieble* (ketidakandalan: tidak menjamin *datagram* yang terkirim sampai tujuan), *connectionless*, *datagram delivery service*.

b. ARP (*Address Resolution Protocol*) Protokol yang digunakan untuk nenemukan alamat *Hardware* dari *host*/komputer yang terletak pada *network* yang sama.

c. ICMP (*Internet Control message protokol*) Protokol yang digunakan untuk mengirimkan pesan dan melapor kegagalan pengiriman data.

2.9.2.3 Transport Layer

Bertanggung jawab untuk mengadakan komunikasi antara dua host/komputer, yang terdiri dari protokol *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP). TCP merupakan protokol yang menyediakan service *connection oriented*, sebelum melakukan pertukaran data, dua aplikasi pengguna TCP harus melakukan pembentukann hubungan terlebih dahulu.

2.9.2.4 Aplication Layer

Terletak semua aplikasi yang menggunakan protokol TCP/IP.Fungsi masing-masing *layer* / lapisan protokol serta aliran data pada *layer* TCP / IP diatas, dapat dicontohkan dengan mengggunakan analogi yang sangat sederhana. Seperti analogi pengiriman surat, seperti berikut ini:

a. Pertama, kita harus menulis dahulu isi surat tersebut. Maka kita harus mengambil selembar kertas dengan ballpoint untuk menulis berita tersebut.

b. Setelah langkah ini terselesaikan, maka kita harus mengambil amplop surat agar terlindung dari kerusakan.

c. Maka kita harus memilih amplop yang tertutup (TCP) atau amplop yang terbuka (UDP).

d. Barulah kita menulis alamat yang dituju dengan jelas, serta nama pengirim dan alamat pengirim.

e. Maka selesailah sudah pengiriman surat tersebut dengan menitipkan surat itu pada kantor pos.

Cara kerja TCP/IP dalam satu komputer adalah sangat mirip dengan cerita diatas. Mengirimkan e-mail dll, terlebih dahulu diolah di TCP. Saat diolah TCP memberi amplop untuk melindungi data-data yang hendak dikirim, yang berupa data tambahan (no.urut), 16 bit *source port* number (nama pengirim dan penerima).

Komputer dengan protokol TCP/IP dapat berhubungan dengan komputer lain dan jaringan lain karena bantuan peralatan jaringan komputer. Peralatan ini biasanya disebut *network interface*. Selain peralatan tersebut masih diperlukan peralatan lain yang disebut dengan *device* penghubung jaringan, yang secara umum dibagi menjadi beberapa kategori :

a. ***Repeater***

Fungsinya adalah menerima sinyal dari satu segment kabel LAN dan memancarkan kembali dengan kekuatan yang sama dengan sinyal aslinya. Pada *segment* (satu atau lebih) kabel LAN lain, dengan adanya *repeater* ini jarak antara dua jaringan komputer bisa diperjauh.

b. ***Bridge***

Bridge lebih cerdas dan fleksibel dibandingkan dengan *repeater*. *Bridge* bekerja dengan meneruskan paket *ethernet* dari satu jaringan ke jaringan yang lain. Beberapa *bridge* mempelajari alamat *ethernet* setiap device yang terhubung dengannya dan mengatur alur *frame* berdasarkan alamat tersebut. Dapat dihubungkan dalam jaringan dengan metode transmisi yang berbeda. LAN *ethernet* dengan LAN token ring dan mampu memisahkan sebagian trafik karena adanya pemfilteran *frame*.

c. ***Router***

Melewatkan paket IP dari satu jaringan ke jaringan lain yang mungkin memiliki banyak jalur diantara keduanya.

2.9.3 User Datagram Protocol (UDP)

UDP yang merupakan salah satu *protocol* utama diatas IP merupakan *transport protocol* yang lebih sederhana dibandingkan dengan TCP. UDP digunakan untuk situasi yang tidak mementingkan mekanisme reliabilitas. *Header* UDP hanya berisi empat *field* yaitu *source port, destination port, length* dan UDP *checksum* dimana fungsinya hampir sama dengan TCP, namun fasilitas *checksum* pada UDP bersifat opsional.

2.9.3.1Karakteristik UDP

a *Connectionless* (tanpa koneksi): Pesan-pesan UDP akan dikirimkan tanpa harus dilakukan proses negosiasi koneksi antara dua host yang hendak bertukar informasi.

b *Unreliable* (tidak nyata): Pesan-pesan UDP akan dikirimkan sebagai datagram tanpa adanya nomor urut atau pesan. Protokol lapisan aplikasi yang berjalan di atas UDP harus melakukan pemulihan terhadap pesan-pesan yang hilang selama transmisi. Umumnya, protokol lapisan aplikasi yang berjalan di atas UDP mengimplementasikan layanan keandalan mereka masing-masing, atau mengirim pesan secara periodik atau dengan menggunakan waktu yang telah didefinisikan.

c UDP menyediakan mekanisme untuk mengirim pesan-pesan ke sebuah protokol lapisan aplikasi atau proses tertentu di dalam sebuah host dalam jaringan yang menggunakan TCP/IP. *Header* UDP berisi *field Source Process Identification* dan *Destination Process Identification*.

d UDP menyediakan penghitungan checksum berukuran 16-bit terhadap keseluruhan pesan UDP.

2.10 Konsep Dasar Jaringan *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. Dengan memakai 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 :

a Koneksi *client* untuk akses jarak jauh

b LAN-to-LAN *internetworking*

c 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 Keamanan, antara lain dengan *tunneling* (pembungkusan paket data), enkripsi, autentikasi paket, autentikasi pemakai dan kontrol akses

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* VPN harus 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.*

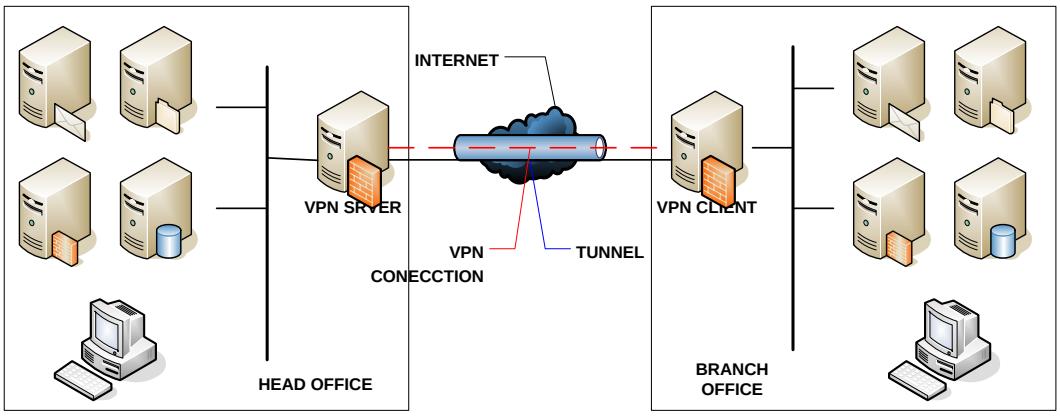
Protokol-protokol di atas menekankan pada *authentikasi* dan enkripsi dalam VPN. Adanya sistem otentifikasi akan mengijinkan *clien* dan server untuk menempatkan identitas orang yang berbeda di dalam jaringan secara benar. Enkripsi mengijinkan data yang dikirim dan diterima tersembunyi dari publik saat 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 pula dibuat koneksi pribadi, dan juga dari kantor juga memungkinkan untuk dibuat jalur komunikasi pribadi yang ekonomis.

2.10.1 *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 :

2.10.1.1Site 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 2.15 Jaringan *site to site* VPN

2.10.2.2 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:

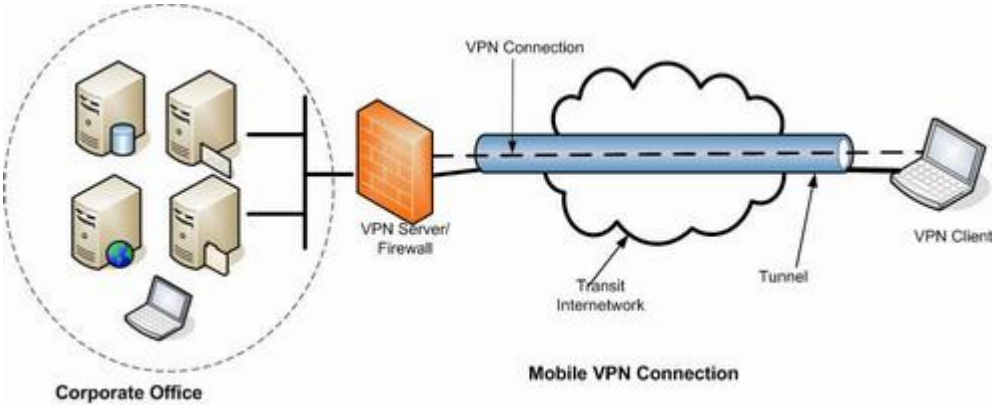
a ***Client-initiated***

Client-initiated arti harafiahnya adalah pihak klien yang berinisiatif untuk melakukan sesuatu. VPN jenis ini juga demikian dan ini merupakan jenis VPN yang paling umum digunakan. Jadi ketika PC Anda ingin membangun koneksi VPN, maka PC tersebutlah yang berusaha

membangun tunnel dan melakukan enkripsi hingga mencapai tujuannya dengan aman. Namun, proses ini tetap mengandalkan jaringan ISP yang digunakan secara umum. *Clientinitiated* VPN sering digunakan oleh PC-PC 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 2.16 **Jaringan *Remote Access* VPN**

2.10.2Tunneling Protocol

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

a *Point-to-Point Tunneling Protocol* (PPTP)

b *Layer 2 Tunneling Protocol* (L2TP)

c Ipsec

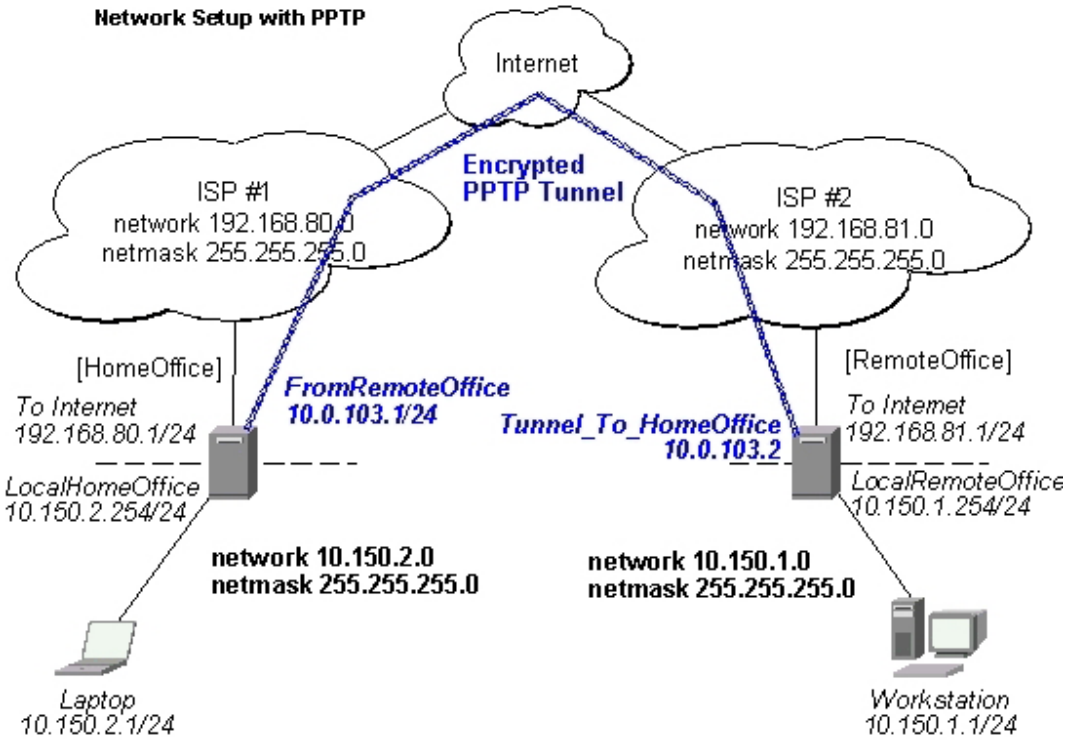
2.10.2.1Point-to-Point Tunneling Protocol (PPTP)

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. Pembangunan PPTP yang mudah dan berbiaya murah untuk digunakan secara luas, menjadi solusi untuk *remote users* dan mobile *users* karena PPTP memberikan keamanan dan enkripsi komunikasi melalui PSTN ataupun internet.

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

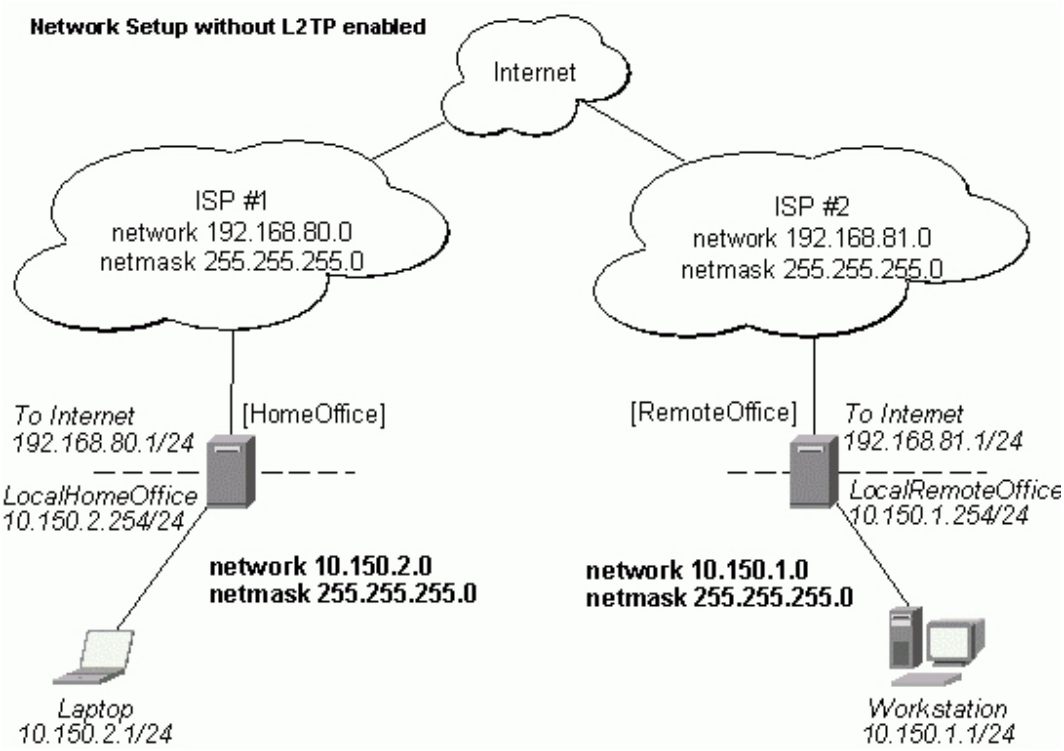


Gambar 2.17 Koneksi *Point-to-Point Tunneling Protocol* (PPTP)

2.10.2.1Layer 2 Tunneling Protocol (L2TP)

L2TP adalah *tunneling protocol* yang memadukan dua buah *tunneling protocol* yaitu L2F (Layer 2 *Forwarding*) milik cisco dan PPTP milik Microsoft (Gupta, 2003). L2TP biasa digunakan dalam membuat *Virtual Private Dial Network* (VPDN) yang dapat bekerja membawa semua jenis protokol komunikasi didalamnya. Umunnya L2TP menggunakan port 1702 dengan protocol UDP untuk mengirimkan L2TP *encapsulated* PPP frames sebagai data yang di tunnel.Terdapat dua model tunnel yang dikenal (Lewis, 2006), yaitu *compulsory*dan *voluntary*. Perbedaan utama keduanya terletak pada *endpoint tunnel*-nya. Pada *compulsory tunnel*, ujung tunnel berada pada ISP, sedangkan pada *voluntary* ujung tunnel berada pada client remote.

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



Gambar 2.18 Koneksi L2TP

2.10.2.1IPsec

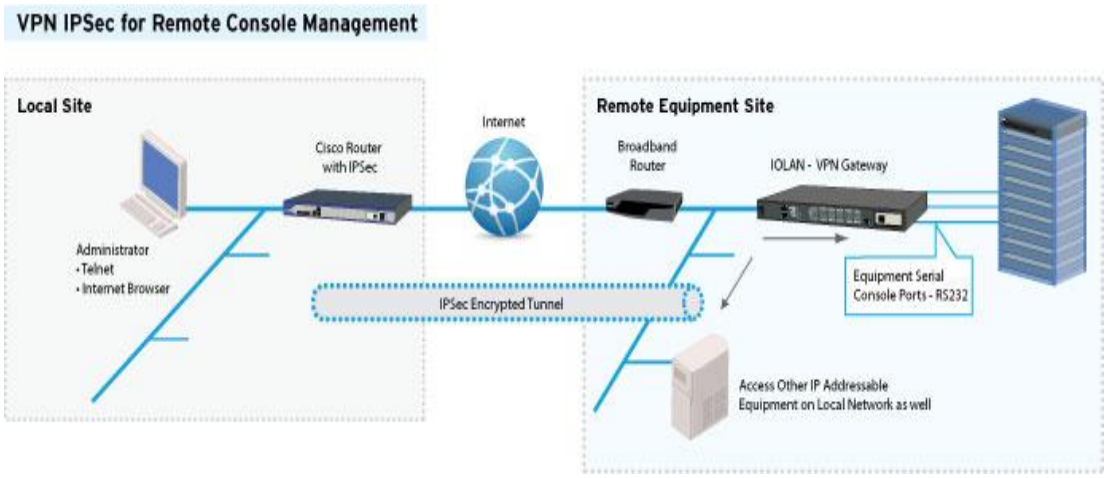
IPSec merupakan suatu pengembangan dari protokol IP yang bertujuan untuk menyediakan keamanan pada suatu IP dan layer yang berada diatasnya (Carmouche, 2006). IPSec (*Internet Protocol Security*) merupakan salah satu mekanisme yang diimplementasikan pada *Virtual Private Network*. Paket IP tidak memiliki 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*).



Gambar 2.19 Tampilan koneksi IPsecurity

2.11 Virtual Private server

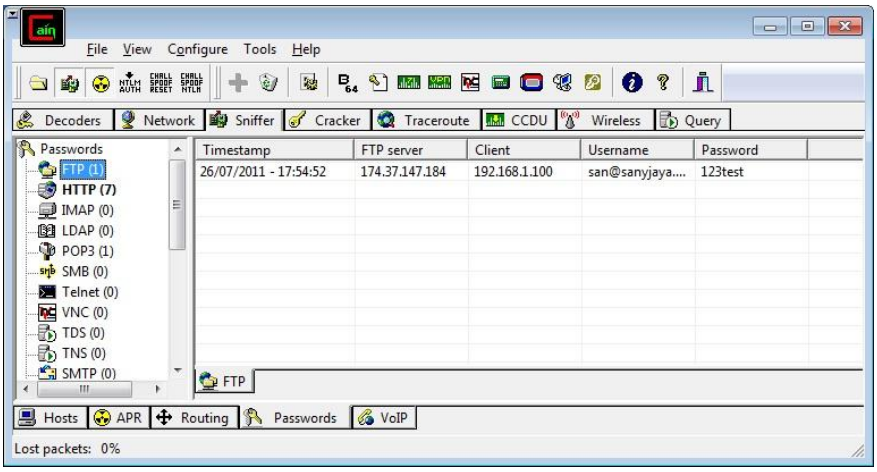
Virtual Private Server (VPS), juga dikenal dengan *Virtual Dedicated Server* (VDS) adalah teknologi *server side* tentang *sistem operasi* dan perangkat lunak yang memungkinkan sebuah mesin dengan kapasitas besar dibagi ke

beberapa virtual mesin. Tiap virtual mesin ini melayani sistem operasi dan perangkat lunak secara mandiri dan dengan konfigurasi yang cepat.

Dengan *VPS* bisa Berbagi-pakai *hosting* yang biasa kita kenal memiliki sangat banyak keterbatasan terhadap aplikasi yang berjalan karena user hanya mempunyai hak akses sebagai level user biasa. Apabila user ingin mendapatkan akses terhadap aplikasi dan resource yang lebih dari sekedar level user biasa maka user harus menggunakan ke *Dedicated Server*, hal ini membuat dana melonjak sangat tinggi seiring dengan mahalnya harga *dedicated* perangkat keras dan sewa lokasi data center. Dengan menggunakan teknologi *Virtual Private Server* memberikan solusi jembatan penghubung antara budget financial, resource system dan *level user.*

2.11.1 Cain & Abel

Cain & Abel adalah *program* yang berguna untuk memonitor (baca,menyadap) paket-paket data yang lewat di jaringan, termasuk paket yang berisi *user,pasword* dengan cain abel bisa digunakan untuk berbagai macam kegunaan



Gambar 2.20 Tampilan Aplikasi Cain abel