BAB II
TINJAUAN PUSTAKA

2.1 Profil Tempat Kerja Praktek

2.1.1. Sejarah Instansi

Kantor Pengolahan Data Elektronik *(KPDE)* Provinsi Daerah Tingkat I Jawa Barat adalah kelanjutan dari organisasi sejenis yang semula sudah ada di lingkungan Pemerintah Provinsi Daerah Tingkat I Jawa Barat dengan nama Pusat Pengolahan Data *(PUSLAHTA)* Provinsi Daerah Tingkat I Jawa Barat.

Keberadaan *PUSLAHTA* di Jawa Barat dimulai pada tahun 1977, yaitu dengan adanya Proyek Pembangunan Komputer Pemerintah Provinsi Daerah Tingkat I Jawa Barat. Proyek tersebut dimaksudkan untuk mempersiapkan sarana prasarana dalam rangka memasuki era komputer. Dalam perkembangan selanjutnya, pada tanggal 8 April 1978 dengan Surat Keputusan Gubernur Kepala Daerah Tingkat I Jawa Barat Nomor : 294/Ok.200-Oka/SK/78 diresmikan pembentukan/pendirian *Kantor Pusat Pengolahan Data (PUSLAHTA)* Provinsi Daerah Tingkat I Jawa Barat yang berkedudukan di jalan Tamansari No. 57 Bandung.

Sebagai tindak lanjut dari Surat Keputusan Gubernur Nomor : 294/Ok.200-Oka/SK/78, maka pada tanggal 29 Juni 1981 pendirian Kantor *PUSLAHTA* dikukuhkan dengan Peraturan Daerah Nomor : 2 Tahun 1981 tentang Pembentukan Pusat Pengolahan Data *(PUSLAHTA)* Provinsi Daerah Tingkat I Jawa Barat dan Peraturan Daerah Nomor : 3 Tahun 1981 tentang Susunan Organisasi dan Tata Kerja Pusat Pengolahan Data Provinsi Daerah Tingkat I Jawa Barat. Dengan kedua Peraturan Daerah tersebut keberadaan PUSLAHTA di lingkungan Pemerintah Provinsi Daerah Tingkat I Jawa Barat semakin berperan, khususnya dalam melaksanakan kebijaksanaan Gubernur Kepala Daerah di bidang komputerisasi. Akan tetapi keberadaan kedua Peraturan Daerah tersebut tidak mendapat pengesahan dari pejabat yang berwenang dalam hal ini Menteri Dalam Negeri, sehingga keberadaan PUSLAHTA di lingkungan Pemerintah Daerah Tingkat I Jawa Barat kedudukan organisasi menjadi non structural. Akan tetapi dengan keberadaan Puslahta Provinsi Daerah Tingkat I Jawa Barat pada masa itu telah banyak dirasakan manfaatnya selain

oleh lingkungan Pemerintah Provinsi Jawa Barat juga oleh instansi lain dalam bentuk kerja sama penggunaan mesin komputer IBM S-370/125 seperti :

- IPTN
- PJKA
- ITB
- Dan pihak Swasta lainnya

Dalam perjalanan waktu yang cukup panjang, yaitu lebih kurang 14 tahun sejak PUSLAHTA didirikan, pada tanggal 27 Juni 1992 dengan Surat Keputusan Gubernur Kepala Daerah Tingkat I Jawa Barat Nomor : 21 Tahun 1992 Organisasi PUSLAHTA Provinsi Daerah Tingkat I Jawa Barat dibubarkan. Di dalam salah satu pasal Surat Keputusan Gubernur No. 21 tahun 1992 dinyatakan bahwa tugas dan wewenang PUSLAHTA dialihkan ke Kantor Bappeda Provinsi Daerah Tingkat I Jawa Barat.

Pada tanggal yang sama dengan terbitnya Surat Keputusan Gubernur No. 21 tahun 1992 tentang Pembubaran PUSLAHTA Provinsi Daerah Tingkat I Jawa Barat, keluar Keputusan Gubernur Kepala Daerah Tingkat I Jawa Barat Nomor : 22 Tahun 1992 tentang Pembentukan Kantor Pengolahan Data Elektronik *(KPDE)* Provinsi Daerah Tingkat I Jawa Barat sebagai pelaksana dari Instruksi Menteri Dalam negeri Nomor : 5 tahun 1992 tentang Pembentukan Kantor Pengolahan Data Elektronik Pemerintah Daerah di seluruh Indonesia.

Sebagai tindak lanjut dari Instruksi Menteri Dalam Negeri Nomor : 5 Tahun 1992 tentang Pembentukan Kantor Pengolahan Data Elektronik, pada tanggal 30 Juni 1993 keluar persetujuan Menteri Negara Pendayagunaan Aparatur Negara *(Menpan)* dengan Nomor : B-606/I/93 perihal Persetujuan Pembentukan Kantor Pengolahan Data Elektronik untuk Provinsi Daerah Tingkat I Kalimantan Selatan, Jawa Barat, Sumatera Barat dan Daerah Istimewa Yogyakarta.

Dengan keluarnya Surat Persetujuan Menteri Pendayagunaan Aparatur Negara *(Menpan)* tersebut, maka untuk mengukuhkan Keputusan Gubernur Nomor 22 Tahun 1992 diajukan Rancangan Peraturan Daerahnya, dan akhirnya pada tanggal 21 Juni 1994 berhasil ditetapkan Peraturan Daerah Provinsi Daerah Tingkat I Jawa Barat Nomor : 4 tahun 1994 tentang Pengukuhan Dasar Hukum Pembentukan Kantor Pengolahan Data Elektronik Provinsi Daerah Tingkat I Jawa Barat dan Nomor 5 tahun

1994 tentang Organisasi dan Tata Kerja Kantor Pengolahan Data Elektronik Provinsi Daerah Tingkat I Jawa Barat.

Selanjutnya kedua Peraturan Daerah tersebut diajukan ke Menteri Dalam Negeri untuk mendapat pengesahan, dan pada tanggal 10 Juli 1995 keluar Keputusan Menteri Dalam Negeri Nomor : 59 Tahun 1995 tentang Pengesahan Peraturan Daerah Nomor : 4 dan Nomor : 5 Tahun 1994, dengan demikian KPDE Provinsi Daerah Tingkat I Jawa Barat secara resmi menjadi salah satu *Unit Pelaksana Daerah yang struktural.*

Berdasarkan Peraturan Daerah Provinsi Jawa Barat Nomor : 16 Tahun 2000 tanggal 12 Desember 2000 tentang Lembaga Teknis Daerah Provinsi Jawa Barat telah ditetapkan *Badan Pengembangan Sistem Informasi dan Telematika Daerah* disingkat *BAPESITELDA* sebagai pengembangan dari Kantor Pengolahan Data Elektronik yang dibentuk berdasarkan Keputusan Gubernur Nomor : 22 Tahun 1992 dan dikukuhkan dengan Peraturan Daerah Nomor : 5 Tahun 1994. Sedangkan Kantor Pengolahan Data Elektronik itu sendiri merupakan pengembangan dari Pusat Pengolahan Data (PUSLAHTA) Provinsi Jawa Barat yang berdiri pada tanggal 8 April 1978 melalui Surat Gubernur KDH Tingkat I Jawa Barat No. 294/OK.200-Oka/SK/78, dan keberadaannya dikukuhkan dengan Peraturan Daerah No. 2 Tahun 1981 tanggal 29 Juni 1981.

Dasar Hukum :

1. Keputusan Presiden RI Nomor 50 Tahun 2000 tentang Tim Koordinasi Telematika Indonesia
2. Peraturan Daerah Provinsi Jawa Barat No. 16 Tahun 2000 tentang Lembaga Teknis Daerah Provinsi Jawa Barat.

BAPESITELDA adalah singkatan dari Badan Pengembangan Sistem Informasi dan Telematika Daerah. *Telematika* singkatan dari Telekomunikasi, Multimedia dan Informatika .

Selanjutnya, berdasarkan *Perda Nomor 21 Tahun 2008* tentang Organisasi dan Tata Kerja Dinas Daerah Provinsi Jawa Barat, maka Bapesitelda Prov. Jabar diganti menjadi *Dinas Komunikasi dan Informatika Provinsi* Jawa Barat disingkat *DISKOMINFO,* yang berlokasi di Jalan Tamansari no. 55 Bandung.

Perubahan ini merupakan kenaikan tingkat dan memiliki ruang lingkup serta cakupan kerja lebih luas. Sasarannya tidak hanya persoalan teknis, tapi juga kebijakan, baik hubungannya kedalam maupun menyentuh kepentingan publik khususnya dibidang teknologi informasi. Dengan platform dinas, maka Diskominfo dapat mengeluarkan regulasi mengenai teknologi informasi dalam kepentingan Provinsi Jawa Barat, terutama pencapaian Jabar Cyber Province Tahun 2012.

Berdasarkan Perda tersebut, Dinas Komunikasi dan Informatika berada diperingkat 20 dengan sruktur organisasi sebagai berikut di bawah ini:

1. Kepala
2. Sekretariat, membawahkan :
    a. Sub.Bagian Perencanaan dan Program
    b. Subbagian Keuangan
    c. Subbagian Kepegawaian dan Umum
3. Bidang Pos Dan Telekomunikasi, membawahkan :
    a. Seksi Pos Dan Telekomunikasi
    b. Seksi Monitoring dan Penetiban Spektrum Frekuensi
    c. Seksi Standarisasi Pos Dan Telekomunikasi
4. Bidang sarana Komunikasi Dan Diseminasi Informasi, membawahkan :
    a. Seksi Komunikasi Sosial
    b. Seksi Komunikasi Pemerintah Dan Pemerintah daerah
    c. Seksi Penyiaran Dan Kemitraan Media
5. Bidang Telematika, membawahkan:
    a. Seksi Pengembangan Telematika
    b. Seksi Penerapan telematika
    c. Seksi Standarisasi dan Monitoring Evaluasi Telematika
6. Bidang Pengolahan Data Elektronik, membawahkan:
    a. Seksi Kompilasi Data
    b. Seksi Integrasi Data
    c. Seksi Penyajian Data dan Informasi.
7. Balai LPSE
    a. Tata Usaha LPSE

b. Layanan Informasi LPSE

c. Dukungan dan Pendayagunaan TIK LPSE[2]

2.1.2. Tugas Pokok dan Fungsi

Tugas Pokok dan fungsi dinas Komunikasi dan Informatika Propinsi Jawa Barat. Berdasarkan peraturan Gubernur no. 72 tahun 2009 tentang Tugas Pokok Rinci dan Tugas unit Dinas Komunikasi Informatika (Diskominfo) Provinsi Jawa Barat mempunyai Tugas Pokok fungsi Sebagai berikut :

A. Tugas Pokok

Melaksanakan urusan pemerintahan daerah berdasarkan asas otonomi dan tugas pembantuan bidang komunikasi dan informatika

B. Fungsi

Untuk melaksankan tugas pokok tersebut diskominfo mempunyai fungsi

1. Perumusan dan kebijakan teknis urusan bidang pos dan telekomunikasi sarana komunikasi dan diseminasi informasi, telematika, serta pengolahan data elektronik.
2. Penyelenggaraan Bidang urusan komunikasi dan informatika meliputi bidang Pos dan telekomunikasi, sarana komunikasi dan diseminasi informasi, telematika, serta pengolahan data elektronik
3. Pembinaan dan pelaksanaan tugas-tugas komunikasi dan informatika meliputi bidang pos dan telekomunikasi, sarana komunikasi dan diseminasi informasi, telematika, serta pengolahan data elektronik.
4. Pengkoordinasian dan pembinaan UPTD.
5. Pelaksanaan tugas lain dari Gubernur sesuai dengan tugas dan fungsinya.[2]

2.1.3. Tempat dan Kedudukan Instansi

Nama : Dinas Komunikasi dan Informasi Provinsi Jawa Barat

Alamat : JL. Tamansari no. 55 Bandung

Telepon : 022-2502898

Fax : 022-2512151

Email : diskominfo@jabarprov.go.id [2]

2.2 Konsep Dasar 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[1]. 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

2.3 Berdasarkan Ruang Lingkup Geografis

Berdasarkan ruang lingkup geografisnya terdapat tiga jenis jaringan komputer, antara lain [1]:

2.3.1 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.

2.3.2 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.

2.3.3 Wide Area Network

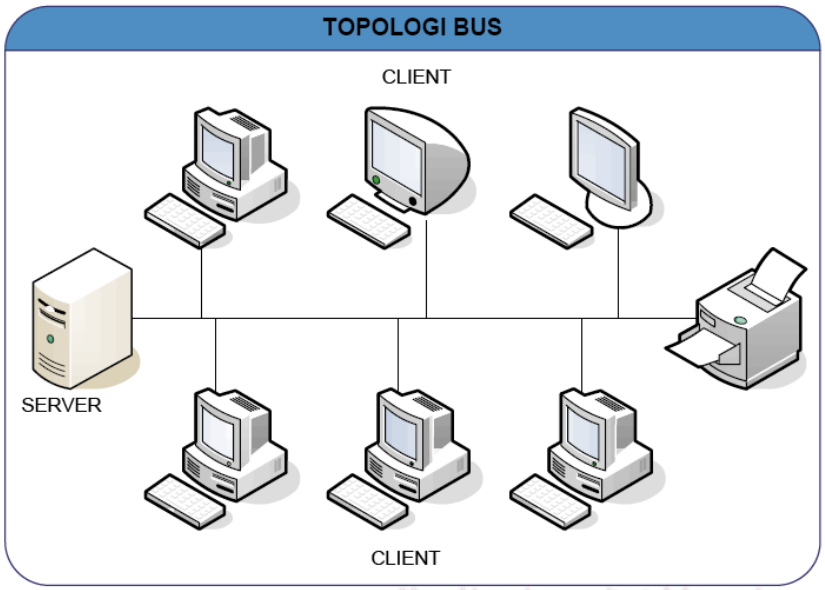
Jaringan Wide Area Network (WAN) mempunyai cakupan terluas, bahkan dapat dikatakan mencakup seluruh dunia. Jaringan ini sendiri dapat dihubungkan dengan menggunakan satelit dan media kabel fiber optic. Jaringan Wide Area Network (WAN) adalah kumpulan dari LAN dan/atau workgroup yang dihubungkan dengan 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 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*.

2.4.1 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.

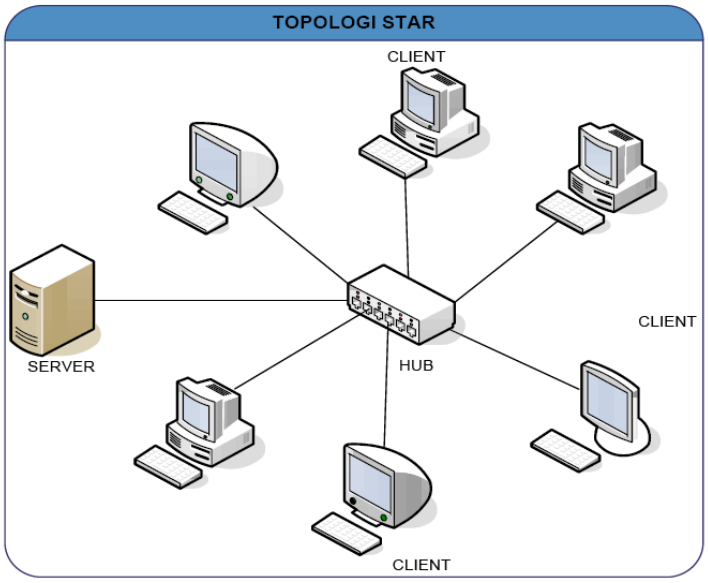


Gambar 2.1 Topologi Bus

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.

2.4.2 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.



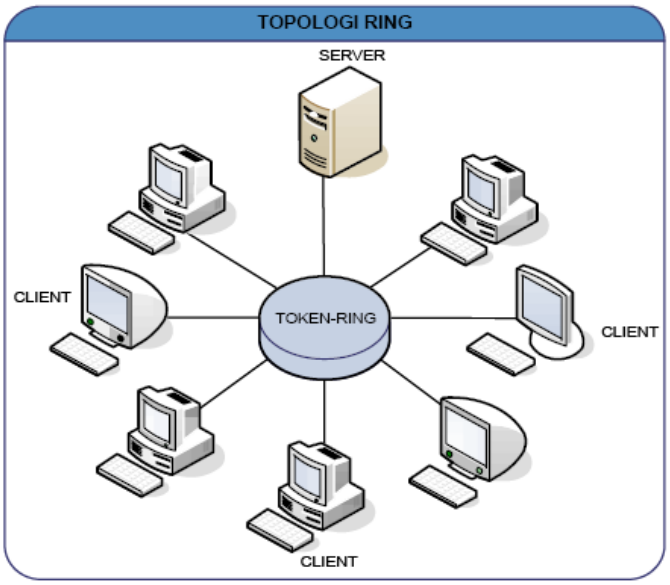
Gambar 2.2 Topologi Star

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.

2.4.3 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.



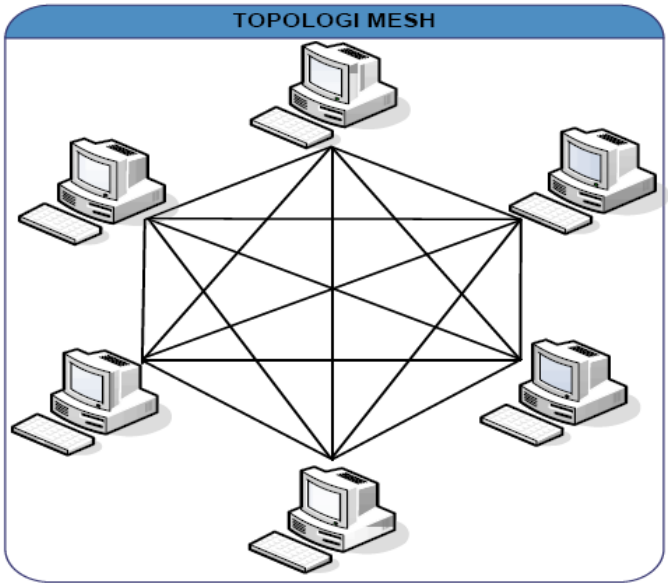
Gambar 2.3 Topologi Ring

2.4.4 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.

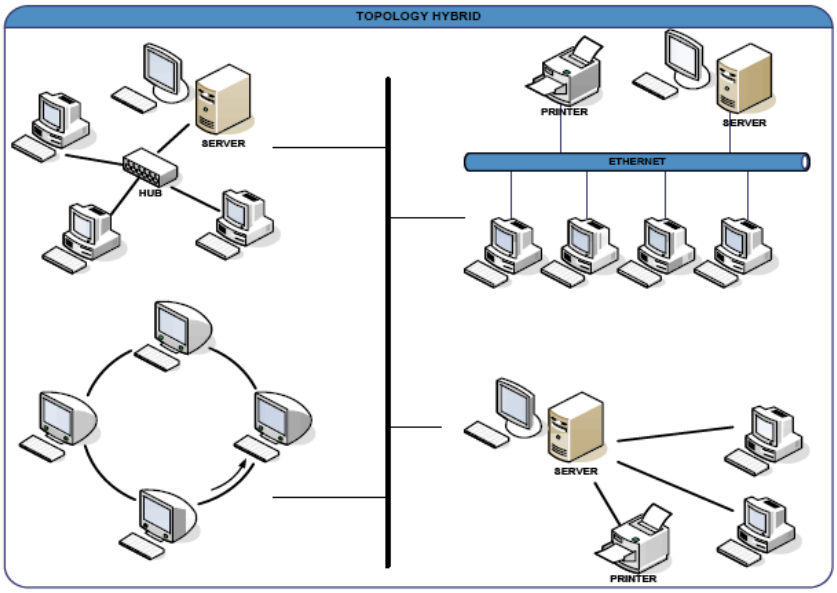
Topologi mesh memberikan keamanan data yang lebih baik, yaitu dengan menggunakan metode *multiplexing*, dimana pesan dapat dipecah-pecah menjadi beberapa paket dan dilewatkan pada jalur yang berbeda.



Gambar 2.4 Topologi Mesh

2.4.5 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.

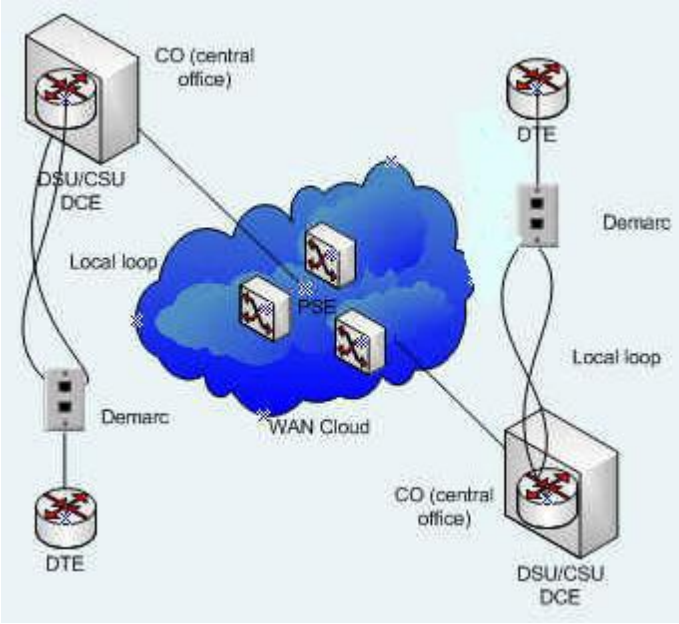


Gambar 2.5 Topologi Hybrid

2.5 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 2.6 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.

Local loop adalah kabel ekstensi ke kantor *central telephone.*

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.

2.5.1 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.

2.5.2 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

2.5.2.1 *Dedicated Connection atau Leased Line*

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.*

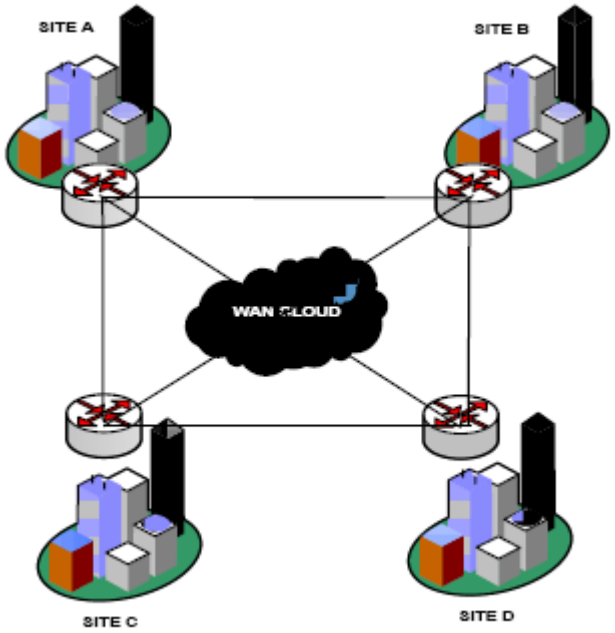
b Koneksi permanen, seperti T1, T3.

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 2.7 Dedicated Connection atau Leased Line

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.

2.5.2.2 Jaringan *Circuit-Switched*

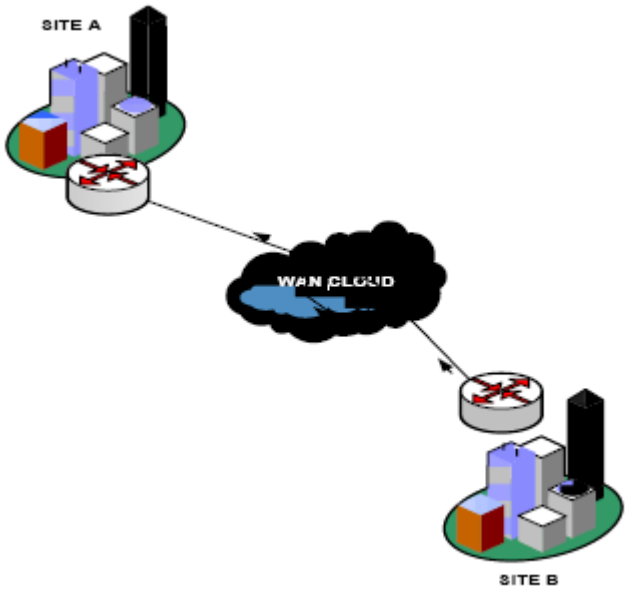
Jenis koneksi jaringan *circuit-switched* memberikan alternatif dari sambungan *leased line*, memungkinkan kita menggunakan sambungan bersama (*share line*). Koneksi WAN jenis ini bekerja dua arah, koneksi WAN *dial-in* dan *dial-out*. Saat kita memakai koneksi WAN *circuit-switched*, maka:

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 2.8 *Jaringan Circuit-Switched*

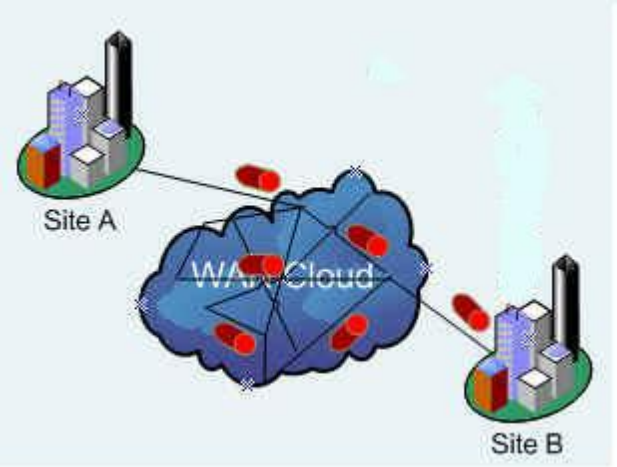
Jaringan *circuit switched* menggunakan S*witch Virtual Circuit* (SVC). Suatu jalur *dedicated* transmisi data terbentuk sebelum komunikasi dimulai dengan cara melepas *switch electric*. Jalur ini akan tetap terbentuk sampai komunikasi berakhir.

2.5.2.3 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 2.8 Jaringan *Packet-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.

2.6 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

2.6.1 *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.

2.7 *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.

2.8 *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.

2.8.1 Karakteristik 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.

2.9 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.

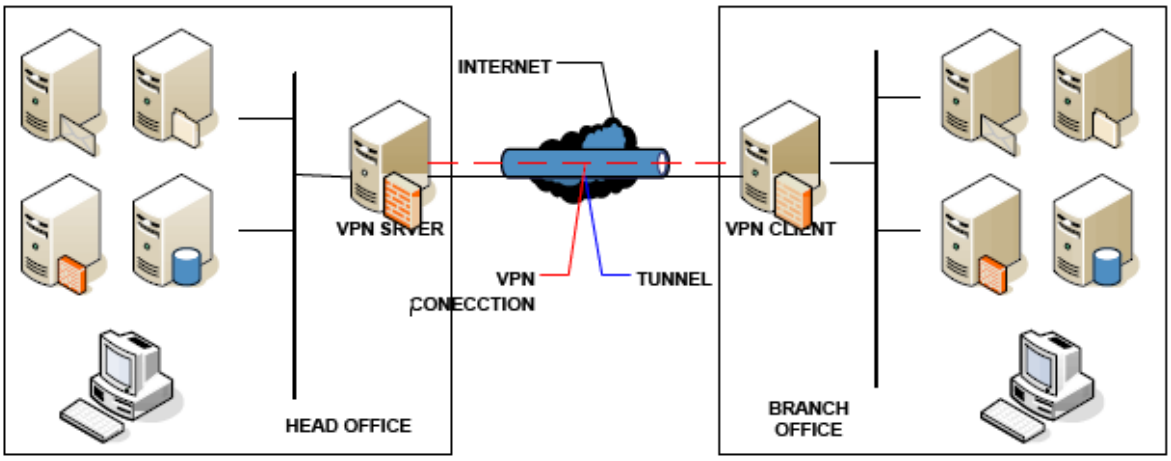
2.9.1 *Teknologi* VPN

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 :

2.9.1.1 *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 *Site to Site* VPN

2.9.1.2 *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:

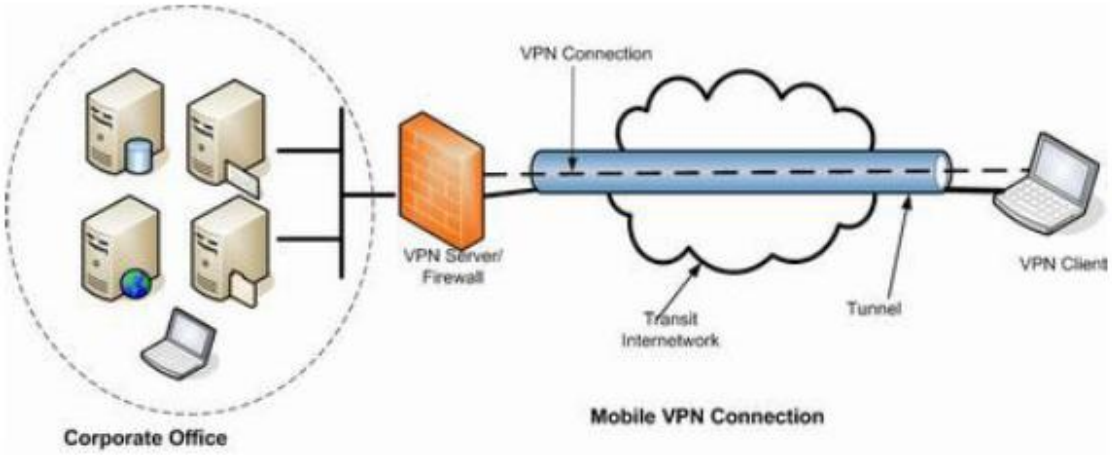
a *Client-initiated*

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 2.11 Jaringan Remote Access VPN

2.9.2 *Tunneling 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

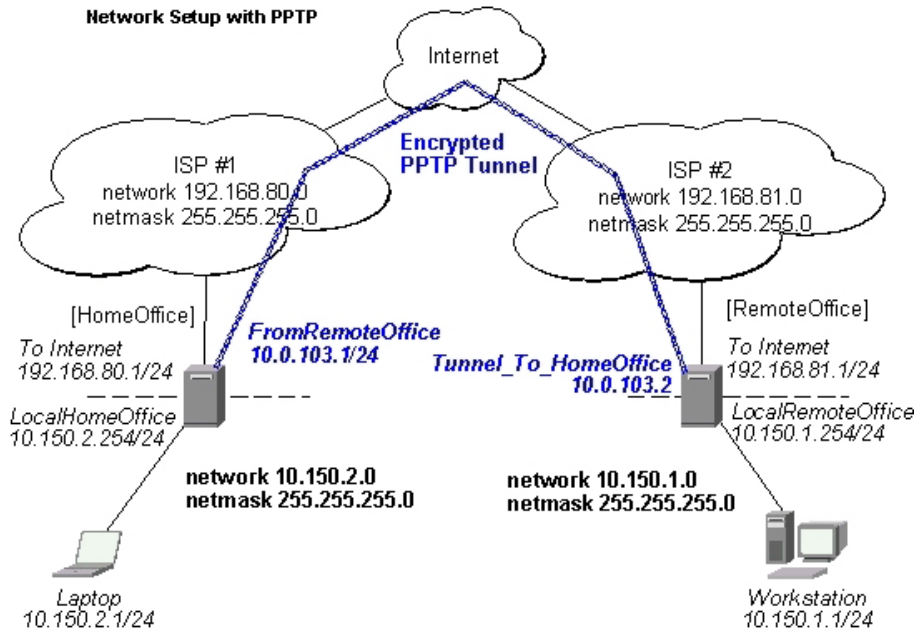
2.9.2.1 *Point-to-Point Tunneling Protocol* (PPTP)

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. 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.

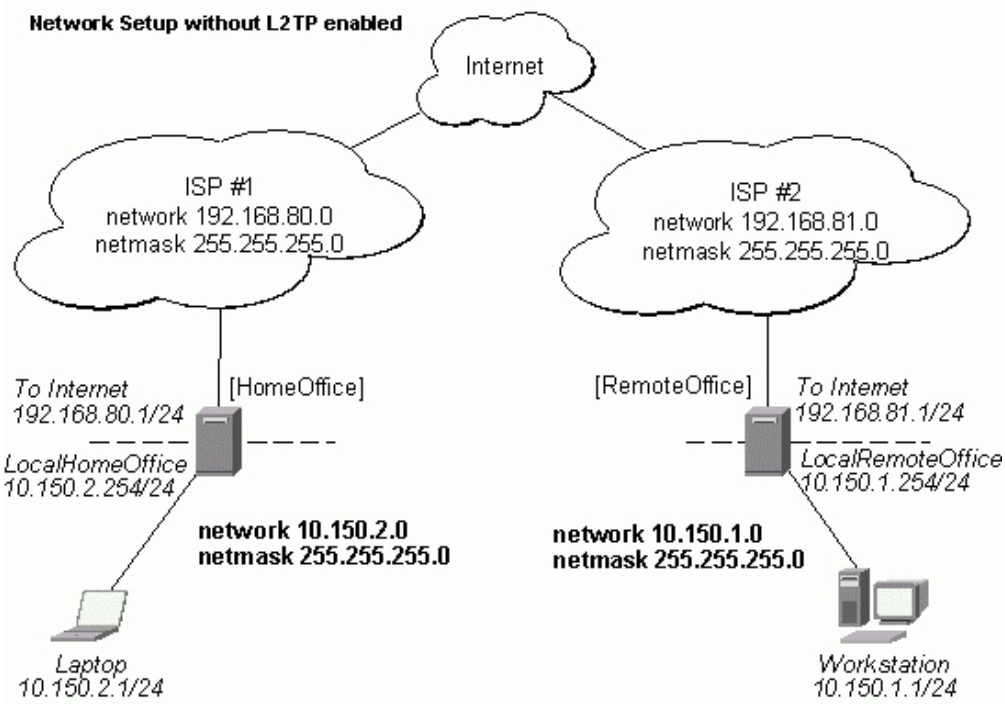


Gambar 2.12 Koneksi *Point-to-Point Tunneling Protocol* (PPTP)

2.9.2.2 *Layer 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 2.13 Koneksi 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

2.9.2.3 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*).

2.10 *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*.

Disamping *software router operating system*, *mikrotik* juga mengembangkan *hardware* dengan spesifikasi dan karakteristik unik serta mempunyai kehandalan sebagai mesin *router*. Dengan dipasarkannya *Mikrotik RouterBoard*TM 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.

*Mikrotik Router*OS 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 *router*OS yang lain, dan sangat membantu kita dalam berimprovisasi untuk mencari solusi dari kendala yang ada di lapangan.

2.11 Cisco Packet Tracer

Packet Tracer adalah simulator alat-alat jaringan Cisco yang sering digunakan sebagai media pembelajaran dan pelatihan, dan juga dalam bidang penelitian simulasi jaringan komputer. Program ini dibuat oleh Cisco Systems dan disediakan gratis untuk fakultas, siswa dan alumni yang telah berpartisipasi di Cisco Networking Academy. Tujuan utama Packet Tracer adalah untuk menyediakan alat bagi siswa dan pengajar agar dapat memahami prinsip jaringan komputer dan juga membangun skill di bidang alat-alat jaringan Cisco.[3]