BAB 2

LANDASAN TEORI

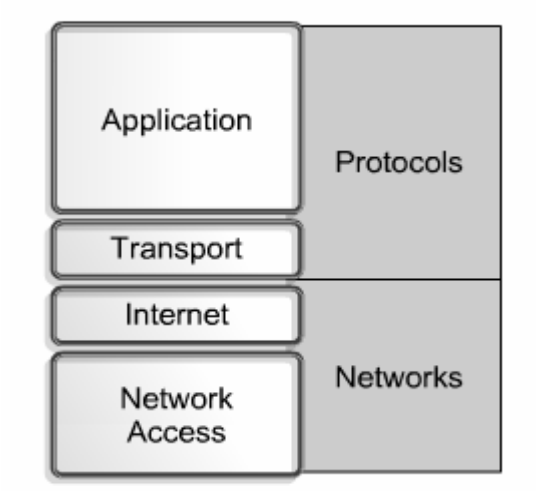
2.1 Jaringan Komunikasi

Jaringan adalah suatu mekanisme yang memungkinkan berbagai komputer terhubung dan para penggunanya dapat berkomunikasi dan *share resources* satu sama lain (Norton, 1999, p5). Informasi dan data bergerak melalui media transmisi jaringan sehingga memungkinkan pengguna jaringan komputer untuk saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama-sama menggunakan *hardware*/*software* yang terhubung dengan jaringan. Tiap komputer, *printer* atau peralatan lainnya yang terhubung dengan jaringan disebut *node*. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan bahkan jutaan *node*.

2.1.1 Model TCP/IP layer

Model TCP/IP dikembangkan Departemen Pertahanan USA (DoD) dengan tujuan ingin menciptakan suatu jaringan yang dapat bertahan dalam segala kondisi. TCP/IP adalah jenis protokol pertama yang digunakan dalam hubungan internet, sehingga banyak istilah dan konsep yang dipakai dalam hubungan internet berasal dari istilah dan konsep yang dipakai oleh protokol TCP/IP. Perkembangan TCP/IP menciptakan suatu *standar de facto*, yaitu suatu standar yang diterima oleh kalangan pemakai dengan sendirinya karena pemakaian yang luas. Model TCP/IP ini mempunyai 4 layer, yaitu : *application layer*, *transport layer*, *internet layer*, dan *network access layer*. Beberapa layer pada model TCP/IP mempunyai nama yang sama dengan model

OSI. Gambar 2.1 dibawah ini merupakan gambaran dari model TCP/IP dimana dapat dilihat bahwa model TCP/IP juga dibagi menjadi 2 bagian, yaitu bagian *networks* dan *protocols*.



Gambar 2.1 TPC/IP Layer

2.1.1.1 *Application Layer*

Application layer pada model TCP/IP menangani protokol tingkat tinggi yang berhubungan dengan representasi, *encoding* dan *dialog control*. Protokol TCP/IP menggabungkan seluruh hal yang berhubungan dengan aplikasi ke dalam satu layer dan menjamin data dipaketkan dengan benar sebelum masuk ke layer berikutnya. Beberapa program berjalan pada layer ini, menyediakan layanan langsung kepada user. Program-program ini dan protokol yang berhubungannya meliputi HTTP (*The World Wide Web*), FTP, TFTP (*File Transport*), SMTP (*Email*), Telnet, SSH (*Secure remote login*), DNS (*Name management*).

2.1.1.2 *Transport Layer*

Layer transport menyediakan layanan transportasi dari *host* sumber ke *host* tujuan. Layer transport merupakan suatu koneksi logical diantara *endpoints* dari suatu jaringan, yaitu *sending host* dan *receiving host*. Transport protokol membuat segment dan mengumpulkan kembali aplikasi layer diatasnya menjadi *data stream* yang sama diantara *endpoints*. *Data stream* layer transport menyediakan layanan transportasi *end-to-end*. Protokol-protocol yang berfungsi pada layer ini adalah :

- ***Transmission Control Protocol* (TCP)**

  TCP berfungsi untuk mengubah suatu blok data yang besar menjadi segmen-segmen yang dinomori dan disusun secara berurutan agar si penerima dapat menyusun kembali segmen-segmen tersebut seperti waktu pengiriman. TCP ini adalah jenis protocol *connection oriented* yang memberikan layanan bergaransi. Sifat dari protokol ini diantara yaitu :

  - *connection oriented*

    Dua aplikasi pengguna TCP harus melakukan pembentukan hubungan untuk dapat melakukan pertukaran data.

  - *reliable*

    TCP menerapkan proses deteksi kesalahan paket dan retransmisi.

  - *byte stream service*

    Paket yang dikirim akan sampai pada tujuan secara berurutan.

- ***User Datagram Protokol* (UDP)**

  UDP adalah jenis protocol *connectionless oriented*. UDP bergantung pada lapisan atas untuk mengontrol kebutuhan data. Oleh karena penggunaan *bandwidth* yang efektif, UDP banyak dipergunakan untuk aplikasi-aplikasi yang

tidak peka terhadap gangguan jaringan seperti SNMP dan TFTP. Sifat dari protokol ini yaitu

- *connectionless*

  Dalam mengirim paket dari tempat asal ke tempat tujuan, masing-masing tidak mengadakan *handshake* terlebih dahulu.

- *unreliable*

  Protokol tidak menjamin datagram yang dikirim sampai ke tempat tujuan tetapi berusaha sebaik-baiknya agar paket yang dikirim sampai pada tempat tujuan.

2.1.1.3 *Internet Layer*

Tujuan dari layer internet adalah untuk memilih jalur/path terbaik bagi paket-paket data di dalam jaringan. Protokol utama yang berfungsi pada layer ini adalah *Internet Protocol* (IP). Penentuan jalur terbaik dan *packet switching* terjadi pada layer ini. Protokol-protokol yang berfungsi pada layer ini antara lain adalah IP, ARP, RARP, BOOTP, DHCP, ICMP.

- IP merupakan protokol yang memberikan alamat atau identitas logika untuk peralatan di jaringan komputer. IP mempunyai tiga fungsi utama, yaitu servis yang tidak bergaransi (*connectionless oriented*), pemecahan (*fragmentation*) dan penyatuan paket-paket, fungsi meneruskan paket (*routing*).
- *Address Resolution Protocol* (ARP) adalah protokol yang mengadakan translasi dari IP address yang diketahui menjadi alamat *hardware* atau *MAC address*. ARP ini termasuk jenis protokol *broadcast*.

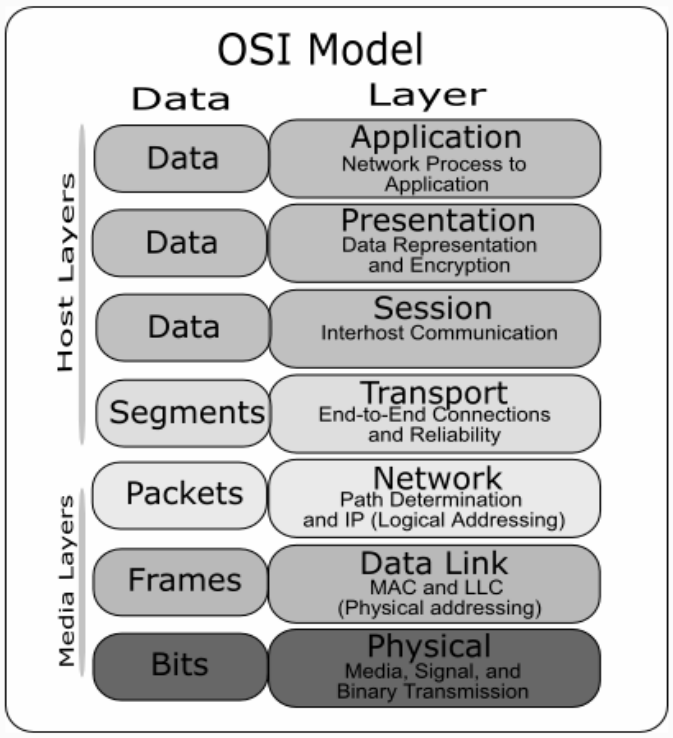
- *Reverse Address Resolution Protocol* (RARP) adalah protokol yang berguna mengadakan translasi *MAC address* yang diketahui menjadi *IP address*. Router menggunakan protokol RARP ini untuk mendapatkan *IP address* dari suatu *MAC address* yang diketahuinya.
- *Bootstrap Protocol* (BOOTP) adalah protokol yang digunakan untuk proses *boot diskless workstation*. Dengan protocol ini, suatu IP address dapat diberikan ke suatu peralatan di jaringan berdasarkan *MAC address*-nya.
- *Dynamic Host Configuration Protocol* (DHCP) merupakan kelanjutan protokol *bootstrap* yang dapat memberikan *IP address* secara otomatis ke suatu *workstation* yang menggunakan protocol TCP/IP. DHCP bekerja dengan relasi *client-server*.
- *Internet Control Message Protocol* (ICMP) adalah protokol yang berguna untuk melaporkan jika terjadi suatu masalah dalam pengiriman data.

2.1.1.4 *Network Access Layer*

Network access layer disebut juga *host-to-network layer*. Layer ini berkaitan dengan hal-hal yang paket IP perlukan untuk membuat hubungan fisik dengan media jaringan. *Driver* untuk *software* aplikasi, modem, dan alat lainya beroperasi pada layer ini. *Network access layer* berfungsi memetakan *IP address* ke alamat fisik *hardware* dan enkapsulasi dari paket-paket IP menjadi *frame-frame*. Protokol-protokol yang berfungsi pada layer ini adalah Ethernet, Token Ring, FDDI.

2.1.2 Model OSI Layer

Open Systems Interconnection Reference Model (Model OSI) merupakan suatu deskripsi abstrak *layering* untuk rancangan jaringan komputer dan komunikasi, yang dikembangkan sebagai bagian dari *Open Systems Interconnect (wikipedia.com)*. Biasanya juga disebut sebagai *seven OSI layers model*. Model OSI membagi fungsi-fungsi dari suatu protokol menjadi beberapa layer. Setiap layer mempunyai properti yang menggunakan fungsi layer dibawahnya, memproses data pada layer tersebut, lalu mengirim ke layer yang selanjutnya. Berikut pada Gambar 2.2 dibawah ini merupakan tujuh layer dari model OSI beserta dengan fungsinya masing-masing pada setiap layer. Layer pada model OSI dibagi menjadi 2 bagian besar, yaitu layer media dan layer host.



Gambar 2.2 OSI Layer

2.1.2.1 *Physical Layer*

Layer ini berhubungan langsung dengan *hardware*. *Physical layer* mendefinisikan semua spesifikasi fisik dan elektris untuk semua peralatan meliputi level tegangan, spesifikasi kabel, tipe konektor dan *timing*. Fungsi utama dari layer ini adalah bertanggung jawab untuk mengaktifkan dan mengatur *physical interface* dari jaringan komputer, memodulasi data digital antara peralatan yang digunakan user dengan signal yang berhubungan. Peralatan yang merupakan *physical layer* antara lain hub dan repeater.

2.1.2.2 *Data link Layer*

Layer *Data Link* berfungsi menghasilkan alamat fisik (*physical addressing*), pesan-pesan kesalahan (*error notifications*), pemesanan pengiriman data (*flow control*). Switch dan bridge merupakan peralatan yang bekerja pada layer ini.

2.1.2.3 *Network Layer*

Network layer menyediakan prosedur dalam mentransfer data dari suatu sumber ke suatu tujuan melalui satu atau lebih jaringan (*path selection*) dengan memperhatikan *quality of service* yang diperlukan oleh layer transport. *Network layer* bertanggung jawab dalam *network routing*, *addressing* dan *logical protocol*. Peralatan yang bekerja pada layer ini adalah router.

2.1.2.4 *Transport Layer*

Layer transport mensegmentasi data dari pengirim dan merakit kembali data ke dalam sebuah *data stream* pada komputer penerima. Pada layer ini juga menyediakan servis komunikasi. Dalam menyediakan sebuah servis yang reliabel pada layer ini menyediakan *error detection* dan *recovery* serta *flow control*.

2.1.2.5 *Session Layer*

Sesuai dengan namanya, layer ini berfungsi untuk menyelenggarakan, mengatur dan memutuskan sesi komunikasi. *Session layer* menyediakan servis kepada layer presentation. Layer ini juga mensinkronisasi dialog diantara dua host layer presentation dan mengatur pertukaran data.

2.1.2.6 *Presentasion Layer*

Layer ini mengelola informasi yang disediakan oleh layer aplikasi (*application layer*) supaya informasi yang dikirimkan dapat dibaca oleh layer aplikasi pada sistem lain. Jika diperlukan, pada layer ini dapat menterjemahkan beberapa data format yang berbeda, kompresi, dan enkripsi.

2.1.2.7 *Application Layer*

Layer ini adalah layer yang paling dekat dengan *user*/pengguna, layer ini menyediakan sebuah layanan jaringan kepada pengguna aplikasi. Layer ini berbeda dengan layer lainnya yang dapat menyediakan layanan kepada layer lain. Sebagai contoh : program pengolah kata, email, ftp, dll.

2.2 Klasifikasi Jaringan

Jaringan dibagi menjadi tiga klasifikasi utama, yaitu *Local Area Network* (LAN), *Metropolitan Area Network* (MAN) dan *Wide Area Network* (WAN).

2.2.1 *Local Area Network* (LAN)

LAN merupakan suatu jaringan komunikasi yang saling menghubungkan berbagai jenis perangkat dan menyediakan pertukaran data diantara perangkat-perangkat tersebut (Stallings, 2004, p16). Jaringan datanya bersifat *high-speed, fault-tolerant* dan memiliki cakupan area geografis yang sempit. Sebuah LAN adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan seperti sebuah perkantoran di sebuah gedung, atau sebuah sekolah, dan biasanya tidak jauh dari sekitar 1 km persegi (cisco.netacad.net). LAN biasanya didesain untuk beroperasi pada area geografis yang terbatas, memungkinkan *multi-access* terhadap high-bandwidth media, mengontrol jaringan secara privat dalam administrasi lokal, menyediakan *full-time connectivity* terhadap layanan lokal, dan menghubungkan peralatan yang bersebelahan secara fisik.

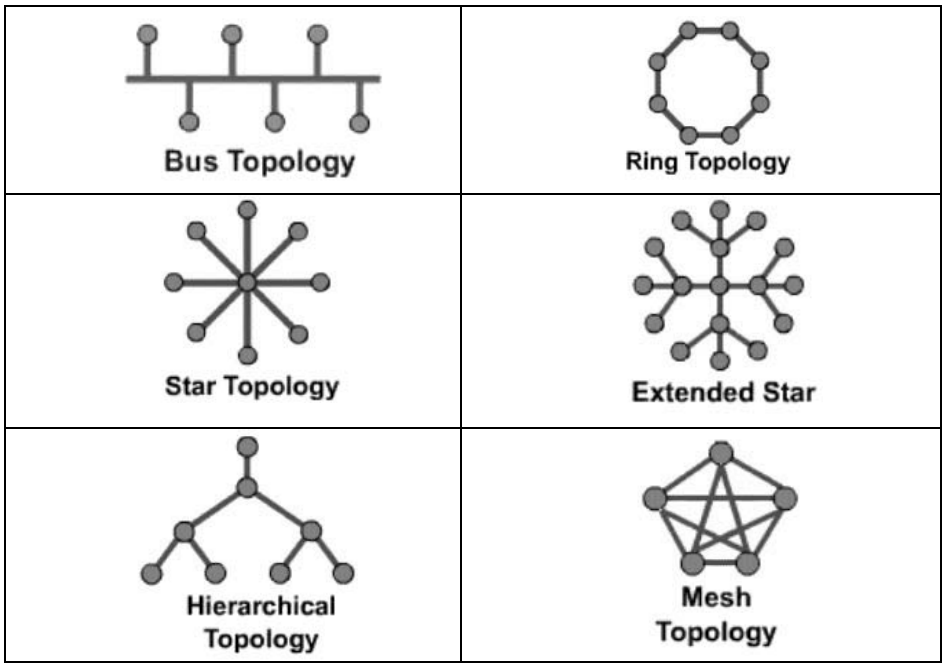
Ciri-ciri LAN :

- Ruang lingkup kecil (Gedung atau kampus kecil).
- *Rate* data harus tinggi.
- Biasanya menggunakan sistem *broadcast.*
- Dikendalikan secara *private* oleh administrator lokal.
- Menghubungkan secara fisik alat-alat yang berdekatan.

- Menyediakan koneksi ke layanan lokal setiap saat (seperti *printer* dan file di *server*).

2.2.2.1 Topologi Jaringan

Denah bagaimana cara menghubungkan komputer satu dengan yang lainnya disebut topologi jaringan. Topologi LAN dapat digambarkan baik secara fisikal maupun logikal. *Physical topology* menggambarkan penempatan komponen-komponen yang membuat suatu LAN. Topologinya bukan suatu peta jaringan. Sedangkan *logical topology* menggambarkan koneksi yang mungkin antara pasangan-pasangan *endpoint devices* yang dapat berkomunikasi serta bagaimana koneksi fisiknya (Norton, 1999, p139). *Physical topology* suatu jaringan yang sering digunakan adalah topologi *bus*, *ring*, *star*, *extended star*, *hierarchical*, dan *mesh*. Gambar 2.3 dibawah ini adalah gambaran mengenai berbagai topologi fisik yang sering digunakan.



Gambar 2.3 Topologi jaringan

- **Topologi Bus**

  Menggunakan "*single backbone segment*" yang biasanya berupa kabel coaxial sebagai penghubung semua komputer yang ada pada jaringan. Semua komputer tersebut terhubung secara langsung ke kabel tersebut.

- **Topologi Ring**

  Topologi ring menghubungkan satu komputer dengan komputer berikut, dan seterusnya sehingga komputer paling akhir akan kembali terhubung ke komputer yang pertama (akan membentuk seolah-olah menjadi sebuah bentuk lingkaran/cincin). Kelemahan dari topologi ini adalah jika ada salah satu hubungan yang terputus maka seluruh jaringan akan terpengaruh.

- **Topologi Star**

  Topologi star menghubungkan semua kabel ke satu buah titik pusat. Titik pusat ini biasanya berupa *hub* atau *switch* yang berfungsi sebagai konsenrator sehingga seolah-olah komputer yang terhubung berbentuk seperti bintang. Kerugian dari topologi ini adalah banyaknya biaya yang dikeluarkan untuk kabel-kabel dan sebuah device khusus. Tetapi topologi ini lebih cepat karena masing-masing terminal komputer dihubungkan dengan komputer pusat.

- **Topologi Extended Star**

  Topologi extended star menggabungkan beberapa topologi star menjadi satu. *Hub*/*switch* yang dipakai untuk menghubungkan beberapa komputer pada satu jaringan dengan menggunakan topologi star, akan dihubungkan lagi ke *hub*/*switch* utama.

- **Topologi Hiearchical**

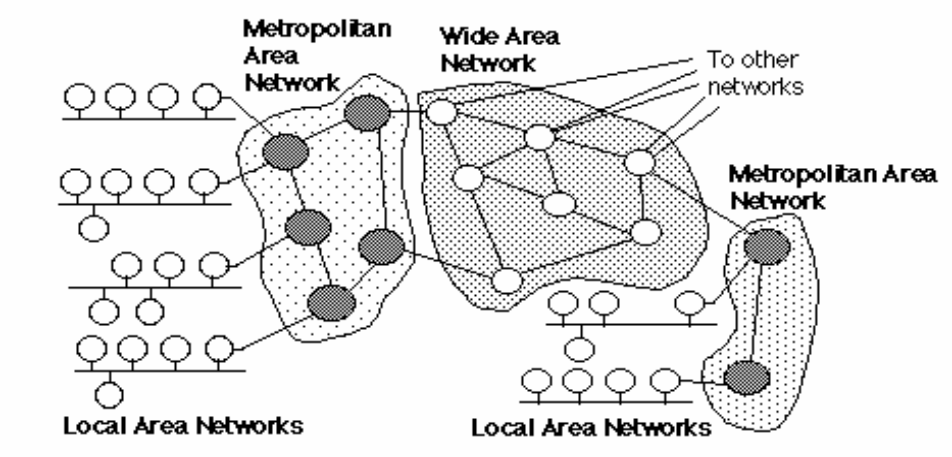
  Topologi hierarchical dibuat mirip dengan topologi extended star tetapi pada system jaringan yang dihubungkan dapat mengontrol arus data pada topologi.

- **Topologi Mesh**

  Topologi Mesh digunakan ketika dalam suatu jaringan yang dibuat tidak boleh terjadi adanya kesalahan, contohnya sistem kontrol pembangkit tenaga nuklir. Jadi seperti yang bisa anda liat pada gambar. Setiap *host* memiliki hubungan lansung dengan semua *host* lainnya dalam jaringan. Hal ini juga merefleksikan Internet, yang memiliki banyak jalur ke satu titik.

2.2.2 *Metropolitan Area Network* (MAN)

Sebuah MAN, biasanya meliputi area yang lebih besar dari LAN, misalnya antar wilayah dalam satu propinsi. Dalam hal ini jaringan menghubungkan beberapa buah jaringan-jaringan kecil ke dalam lingkungan area yang lebih besar, misalnya jaringan Bank dimana beberapa kantor cabang sebuah Bank di dalam sebuah kota besar dihubungkan antara satu dengan lainnya.



Gambar 2.4 LAN, MAN, WAN

2.2.3 *Wide Area Network* (WAN)

Wide Area Network adalah jaringan yang lingkupnya biasanya sudah menggunakan sarana satelit ataupun kabel bawah laut yang menghubungkan pengguna jaringan-jaringan dalam area geografis yang sangat luas. WAN biasanya didesain untuk beroperasi pada area geografis yang luas, memungkinkan akses melalui *serial interface* yang beroperasi pada kecepatan yang lebih rendah, menyediakan koneksi *full-time* dan *part-time* dan menghubungkan berbagai peralatan yang terpisah jauh, bahkan pada area global.

Ciri-ciri WAN :

- Daerah geografisnya luas.
- Memiliki kecepatan transfer yang lebih rendah daripada LAN.
- Menghubungkan alat-alat yang terpisah dalam jarak jauh, bahkan global.
- Memungkingkan akses melalui *interface* serial yang beroperasi pada kecepatan yang rendah.
- Menyediakan konektifitas *fulltime* dan *parttime.*

2.2.3.1 Teknologi WAN

Ada dua teknologi yang benar-benar berbeda yang digunakan dalam *Wide Area Network* (WAN), yaitu *circuit switching* dan *paket switching*. Kedua teknologi ini berlainan dalam hal simpul yang melakukan *switching* informasi dari satu jalur ke jalur yang lain, yakni dengan jalan dari sumber ke tujuan. (Stallings, 2004, pp299 – 328).

1. *Circuit switching*

   Untuk komunikasi melalui *circuit switching* disediakan jalur komunikasi yang ditempatkan di antara dua *station*. Jalur tersebut berupa rangkaian jalur

yang saling dihubungkan satu sama lain diantara simpul jaringan. Pada jalur-jalur fisik, terdapat *channel* logik yang diperuntukkan untuk koneksi. Komunikasi melalui *circuit switching* meliputi tiga tahap, yaitu pembangunan sirkuit, transfer data, dan pemutusan sirkuit.

2. *Paket switching*

   Jaringan *paket switching* merupakan sekumpulan simpul-simpul *packet switching* yang tersebar. Data yang dikirimkan dalam paket kecil dan tidak harus sesuai dengan urutan yang ada. Paket-paket ini dikirimkan dari node ke node antara *source* dan *destination*. Biasanya digunakan untuk komunikasi dari terminal ke komputer dan dari komputer ke komputer.

2.2.3.2 Topologi WAN

Topologi WAN menggambarkan cara fasilitas transmisi digunakan berdasarkan lokasi-lokasi yang terhubung. Banyak topologi yang memungkinkan, masing-masing mempunyai perbedaan cost, performance dan scalability sendiri-sendiri. Topologi-topologi yang sering digunakan antara lain *peer-to-peer*, *ring*, *star*, *full-mesh*, *partial-mesh* yang memiliki bentuk topologi yang sama dengan LAN, dan *multi-tiered* meliputi *two-tiered* dan *three-tiered* yang tidak terdapat pada LAN.

2.2.3.3 Protokol WAN

Pada jaringan WAN terdapat protokol-protokol seperti : *High-Level Data-Link Control* (HDLC) yang dipergunakan oleh Cisco router sebagai protokol *default* untuk berhubungan lewat interface *synchronous* serialnya, PPP yang merupakan standar protokol untuk hubungan *point-to-point interface* serial yang menggunakan protokol

TCP/IP, X.25 yang merupakan protokol WAN yang paling tua menggunakan teknologi *packet switching* antara DTE dan DCE dan ATM yang cara kerjanya menggunakan jalur virtual seperti *Permanent Virtual Cicuit* (PVC) dan *Switched Virtual Circuit* (SVC).

2.3 IP *address*

IP *address* adalah alamat logika yang diberikan ke peralatan jaringan yang menggunakan protokol TCP/IP (Wijaya, 2004, p27). IP *address* terdiri dari 32 bit angka binari, yang ditulis dalam empat kelompok terdiri atas 8 bit (oktat) yang dipisah oleh tanda titik. Contohnya : 11000000.00010000.00001010.00000001 atau dapat juga ditulis dalam bentuk empat kelompok angka desimal (0-255) misalnya 192.16.10.1. IP *address* yang terdiri atas 32 bit angka dikenal sebagai IP versi 4 (IPv4).

TCP/IP melihat semua IP *address* sebagai dua bagian jaringan, yaitu *network* ID dan *host* ID. *Network* ID menentukan alamat jaringan sedangkan *host* ID menentukan alamat *host* atau *komputer*. Oleh sebab itu, IP *address* memberikan alamat lengkap suatu komputer berupa gabungan alamat jaringan dan alamat *host*. Berapa jumlah kelompok angka yang termasuk *network* ID dan berapa yang termasuk *host* ID adalah bergantung pada kelas IP *address* yang dipakai.

2.3.1 Kelas-kelas dalam IP *address*

IP *address* dapat dibedakan menjadi lima kelas, yaitu A, B, C, D, dan E (Mansfield, 2002, p134). Dalam hal ini kelas A, B, dan C digunakan untuk address biasa. Sedangkan kelas D digunakan untuk *multicasting* (224.0.0.0 – 239.255.255.255) dan kelas E (240.0.0.0 – 247.255.255.255) dicadangkan dan belum digunakan. Agar peralatan dapat mengetahui kelas suatu IP *address*, maka setiap IP harus memiliki *subnet mask*. Dengan memperhatikan default *subnet mask* yang diberikan, kelas suatu IP *address* dapat diketahui. Berikut pada Tabel 2.1 dijelaskan mengenai pengelompokan kelas-kelas IP address beserta dengan jumlah jaringan dan jumlah host per jaringan yang dapat digunakan beserta default subnet mask-nya.

Kelas IP *Address*	**Kelompok oktat pertama**	***Network* ID**	***Host* ID**	**Jumlah jaringan**	**Jumlah host per jaringan**	***Default subnet mask***
A	1 – 126	w.	x.y.z	127	16.777.216	255.0.0.0
B	128 – 191	w.x	y.z	16.384	65.536	255.255.0.0
C	192 - 223	w.x.y	z	2.097.152	256	255.255.255.0

Tabel 2.1 Kelas-kelas IP *address*

Dalam penggunaan IP address ada peraturan tambahan yang harus diketahui, yaitu :

- Angka 127 pada oktat pertama digunakan untuk *loopback.*
- *Network* ID tidak boleh semuanya terdiri atas angka 0 atau 1.
- *Host* ID tidak boleh semuanya terdiri atas angka 0 atau 1.

Jika *host* ID berupa angka binari 0, IP *address* ini merupakan *network* ID jaringannya. Jika *host* ID semuanya berupa angka binari 1, IP *address* ini biasanya digunakan untuk *broadcast* ke semua host dalam jaringan lokal.

2.3.2 *Private* dan *Public IP address*

Internet Assigned Number Authority (IANA) yang merupakan badan internasional, yang mengatur masalah pemberian IP *address* untuk digunakan dalam internet, menyediakan kelompok-kelompok IP *address* yang dapat dipakai tanpa pendaftaran yang disebut *private* IP *address*. *Private address* atau *non-routable* ini dialokasikan untuk digunakan pada jaringan yang tidak terkoneksi ke internet. Berikut ini pada Tabel 2.2 merupakan kelompok IP *address* yang termasuk ke dalam kelompok *private address*.

Kelas ***private IP address***	**Kelompok** ***private IP addess***
A	10.0.0.1 – 10.255.255.254
B	172.16.0.1 – 172.31.255.254
C	192.168.0.1 – 192.168.255.254

Tabel 2.2 Kelompok *private IP address*

Sedangkan untuk *public IP address*, alamat yang digunakan diluar dari *private IP address* tersebut. Setiap komputer yang terhubung dengan internet menggunakan *public IP address* sebagai alamatnya, oleh karena itu tidak boleh ada *public IP address* yang sama dalam internet. Pembagian *public IP address* juga dilakukan oleh IANA. Public IP address bisa didapatkan dengan membeli pada *Internet Service Provider (ISP)* terdekat.

2.4 Virtual Private Network (VPN)

Virtual Private Network (VPN), menurut Bruce Perlmutter (2000, p10), merupakan suatu jaringan komunikasi, yang dibangun untuk *private use* dari suatu perusahaan, melalui infrastruktur umum yang digunakan bersama-sama (*shared public infrastructure*). Dengan kata lain VPN merupakan suatu jaringan data private yang menggunakan jaringan publik (biasanya internet) atau layanan jaringan lainnya untuk menghubungkan *remote sites* atau *mobile user* dengan menjaga privacy melalui penggunaan *tunneling protocol* dan prosedur keamanan (VPN Consortium, 2004).

Di dalam suatu VPN, koneksi *dial-up* ke *remote users* dan koneksi *leased line* atau *frame relay* ke *remote sites* digantikan dengan koneksi lokal ke suatu *Internet Service Provider* (ISP) atau *point of presence* (POP) *service provider* lainnya. VPN membuat private intranet menjadi secure ketika melewati internet atau layanan jaringan lainnya, memfasilitasi koneksi *e-commerce* dan *extranet* yang aman dengan partner bisnis, *suppliers* dan *customers*. Berikut pada Gambar 2.5 merupakan contoh dari suatu VPN yang menghubungkan main office dengan remote office, business partner, mobile workers dan home office.

Gambar 2.5 *Virtual Private Networking* (VPN)

2.4.1 Tipe-tipe VPN

Tujuan utama dari membangun VPN adalah untuk memenuhi kebutuhan seperti kemampuan mengakses sumberdaya yang ada di perusahaan kapan saja dan dimana saja, dan juga kemampuan untuk saling berhubungan antara kantor cabang dan kantor pusat. Dengan melihat dan untuk memenuhi kebutuhan diatas, VPN dibagi menjadi 3 kategori :

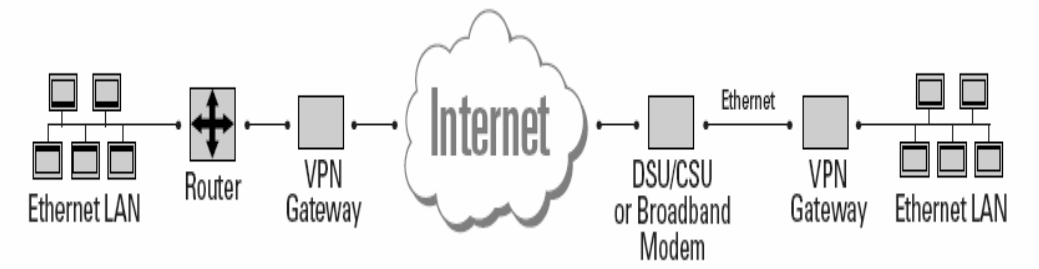
- *Site-to-site* VPN
- *Extranet* VPN
- *Remote Access* VPN

Masing-masing dari kategori ini akan dijelaskan dibawah ini.

2.4.1.1 *Site-to-site* VPN

Site-to-site VPN atau biasa disebut *intranet* VPN memungkinkan suatu *private network* diperluas melintasi internet atau layanan *public network* lainnya dengan cara yang aman. *Site-to-site* VPN merupakan suatu alternatif infrastruktur WAN yang biasa

menghubungkan kantor-kantor cabang, kantor pusat, atau partner bisnis ke seluruh jaringan perusahaan. Gambar 2.6 dibawah ini menunjukan bagaimana Gambaran mengenai suatu site-to-site VPN yang menghubungkan kedua ethernet LAN dengan melewati internet melalui VPN *gateway*.



Gambar 2.6 *Site-to-Site* VPN

Keuntungan dari penggunaan *site-to-site* VPN adalah sebagai berikut :

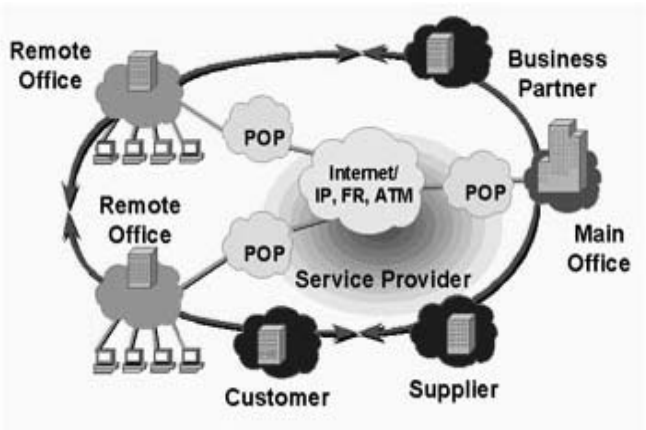
- Kemudahan untuk menambah peer-to-peer link jika ada pembangunan cabang baru, hal ini dikarenakan penggunaan internet sebagai media pengiriman data.
- Dapat dengan mudah membangung sebuah *backup facility* dengan mengasosiasikan teknologi VPN dengan teknologi *fast switching* seperti *frame relay*

Kerugian dari penggunaan *site-to-site* VPN adalah sebagai berikut :

- Karena *data* dikirim melalui internet maka kemungkinan untuk terjadinya serangan terhadap server-server VPN sangat besar.
- Kemungkinan terjadinya tabrakan data pada saat pengiriman sangat tinggi.
- Kualitas dari *bandwidth* dan *throughput* tidak dapat dijamin.

2.4.1.2 *Extranet* VPN

Extranet VPN menyediakan koneksi yang aman dengan partner bisnis, *supplier* dan *customer* untuk tujuan dari *e-commerce*. *Extranet* VPN adalah perluasan dari intranet VPN dengan penambahan firewall untuk proteksi *internal network*. Bisnis-bisnis menikmati kebijakan yang sama seperti suatu *private network*, yang meliputi security, QoS, *manageability* dan *reability*. Perbedaan extranet VPN dengan *site-to-site* VPN adalah pada *site-to-site* VPN hanya menghubungkan dua point, misal kantor pusat dengan satu kantor cabang. Sedangkan pada extranet menghubungkan multipoint. Gambar 2.7 merupakan contoh dari extranet VPN yang saling terhubung antara main office, business partner, remote office, suplier dan customer melalui *Service Provider*.



Gambar 2.7 *Extranet* VPN

Keuntungan dari penggunaan *extranet* VPN adalah sebagai berikut :

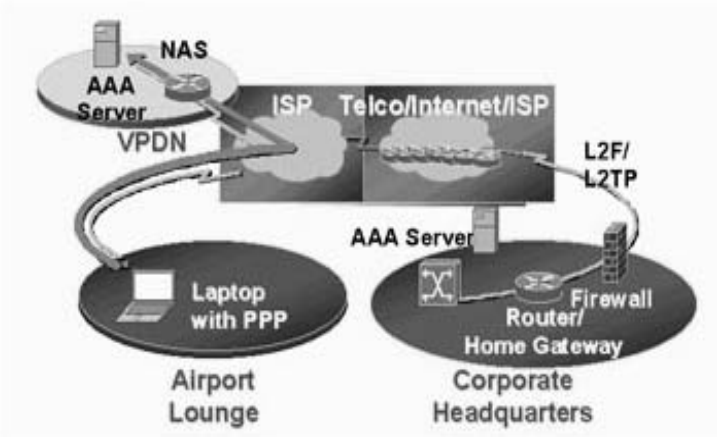
- Karena konektivitas internet dilakukan oleh ISP maka kebutuhan tenaga kerja pada bagian ISP akan berkurang.

Kerugian dari penggunaan extranet VPN adalah sebagai berikut :

- Ancaman dari sisi keamanan tetap ada.

2.4.1.3 *Remote Access* VPN

Remote Access VPN memberikan kemampuan pada *individual user* yang menggunakan *dial-up* untuk terhubung ke *central site* melalui internet atau layanan *public network* lainnya dengan cara yang terjamin aman, kapan saja, dimana saja dan ketika diperlukan. *Remote Access* VPN meliputi *analog*, *dial*, ISDN, *digital subscriber line* (DSL), *mobile* IP dan teknologi *cable* untuk menghubungkan dengan aman *mobile users*, *telecommuters* atau kantor-kantor cabang. *Remote access* VPN kadang disebut juga sebagai *dial* VPN. Gambar 2.8 merupakan suatu gambaran tentang *remote access* VPN, dimana *mobile user* pada *airport* dapat mengakses jaringan kantor pusatnya melalui laptop yang terhubung ke suatu ISP.



Gambar 2.8 *Remote Access* VPN

Keuntungan dari *remote access* VPN adalah sebagai berikut :

- Meningkatkan mobilitas user dalam bekerja.
- Biaya koneksi yang murah karena hanya menggunakan *dial-up* yang digunakan pada saat dibutuhkan.
- Menghemat bandwidth.

Kerugian dari *remote access* VPN adalah sebagai berikut :

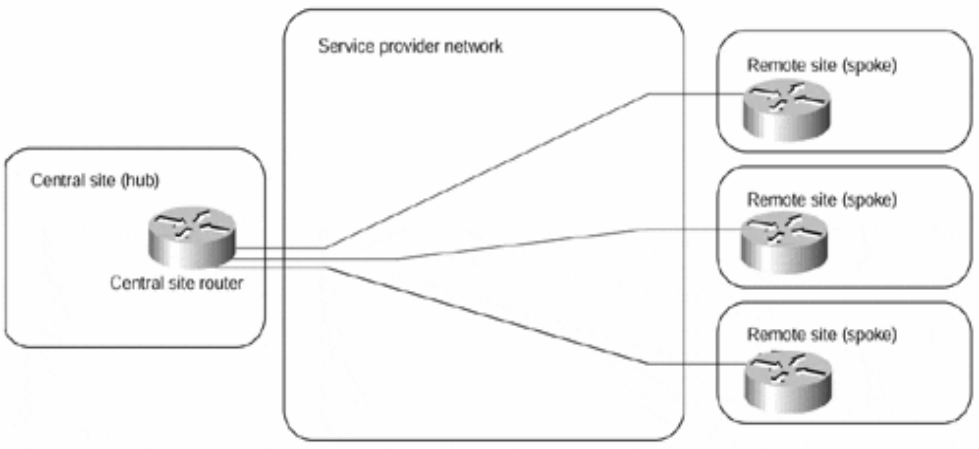
- Pengiriman data berupa animasi, suara, dan video mengakibatkan koneksi pada dial-up user menjadi lambat.
- Kemungkinan untuk kehilangan data sangat tinggi, dikarenakan kesalahan dalam punyusunan fragmentasi sehingga data yang diterima tidak sesuai urutan.

2.4.2 Topologi VPN

Topologi VPN yang dibuat suatu perusahaan seharusnya dibuat berdasarkan bisnis yang ingin diatasi oleh perusahaan. Akan tetapi, ada beberapa topologi yang cukup terkenal. Topologi yang sama dapat memecahkan berbagai macam masalah bisnis di pasar industri yang berbeda. Menurut Guichard dan Pepelnjak (2000) topologi VPN dapat kelompokkan menjadi tiga kategori, yaitu topologi *hub-and-spoke*, topologi *partial atau full-mesh*, dan topologi *hybrid.*

2.4.2.1 Topologi *Hub-and-spoke*

Topologi yang biasa ditemui adalah topologi *hub-and-spoke*, dimana beberapa *remote office* (*spokes*) terhubung dengan *central site* (*hub*), seperti ditunjukkan pada Gambar 2.9. *Remote offices* biasanya dapat bertukar data (tanpa adanya batas-batas keamanan secara explisit di *inter-office traffic*), tetapi jumlah data yang ditukarkan bisa diabaikan. Topologi ini biasa dipakai di organisasi dengan struktur hierarki yang ketat contohnya antara bank, organisasi pemerintahan atau toko retail dengan kantor cabang yang kecil.



Gambar 2.9 Topologi *hub-and-spoke*

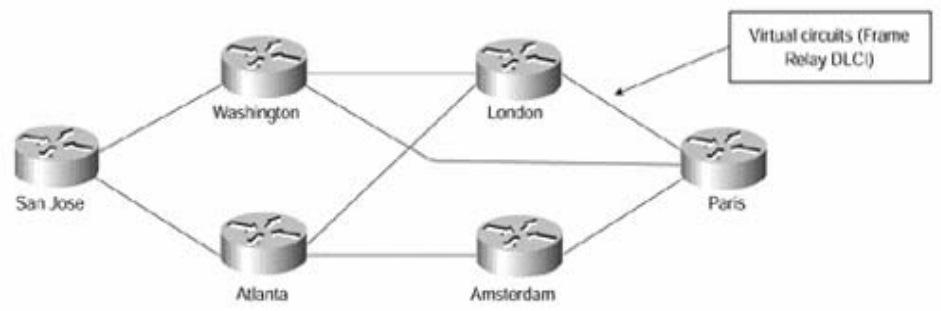
Topologi *hub-and-spoke* cocok untuk lingkungan dimana *remote offices* banyak bertukar data dengan *central site* tetapi tidak antar *remote offices*. Pertukaran data antara *remote offices* selalu dikirim melalui *central site*. Jika jumlah pertukaran data antara *remote offices* menunjukkan proporsi trafik network yang cukup besar, topologi *partial-mesh* atau *full-mesh* mungkin lebih tepat untuk diterapkan.

2.4.2.2 Topologi *Partial* atau *Full Mesh*

Tidak semua konsumen dapat mengimplementasikan topologi *hub-and-spoke* di jaringan mereka karena berbagai alasan seperti :

- Perusahaan mungkin kurang terorganisir strukturnya, pertukaran data terjadi di berbagai tempat di perusahaan.
- Aplikasi yang digunakan di perusahaan membutuhkan komunikasi *peer-to-peer* seperti *messaging* atau sistem kolaborasi.
- Untuk perusahaan multinational, biaya topologi *hub-and-spoke* dapat sangat tinggi karena biaya jaringan international.

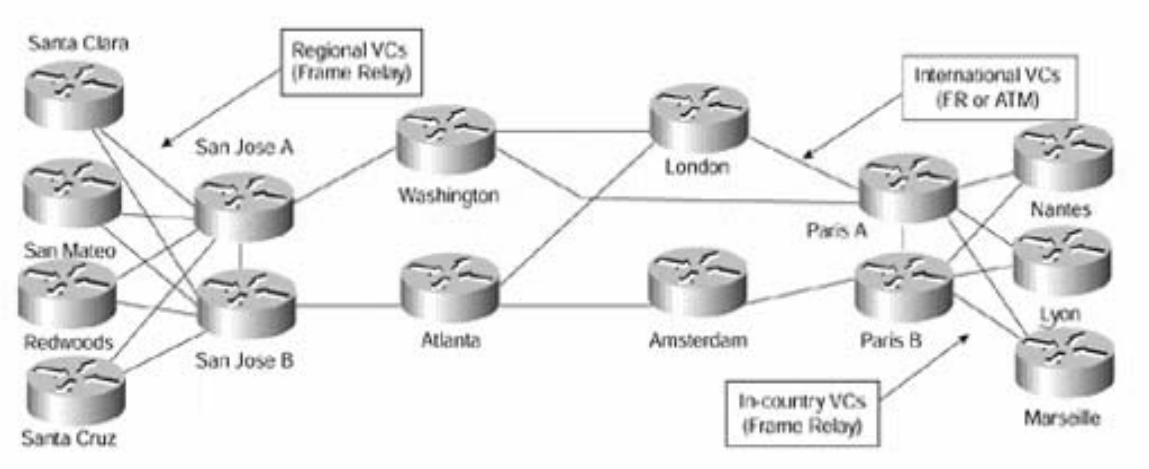
Untuk itu, topologi VPN yang cocok untuk perusahaan adalah topologi *partial-mesh*, dimana *site* di VPN terhubung dengan VC diatur oleh kebutuhan trafik. Jika tidak semua tempat mempunyai hubungan langsung dengan semua tempat (seperti Gambar 2.10), topologi ini disebut *partial mesh*, tetapi jika semua tempat terhubung ke semua tempat maka topologi ini disebut *full mesh*.



Gambar 2.10 Topologi *partial mesh*

2.4.2.3 Topologi *Hybrid*

Jaringan VPN yang besar biasanya menggabungkan topologi *hub-and-spoke* dengan *partial-mesh*. Sebagai contoh, perusahan multinasional yang besar mungkin mengakses jaringan di setiap negara yang terhubung dengan topologi *hub-and-spoke*, dan jaringan pusat internasional dihubungkan dengan topologi *partial-mesh* seperti pada Gambar 2.11 Topologi seperti ini dinamakan topologi *hybrid*.



Gambar 2.11 Topologi *hybrid*

2.4.3 Arsitektur untuk VPN

Dalam membangun sebuah jaringan VPN, terdapat beberapa pilihan arsitektur, yang dapat dilihat pada Tabel 2.3 .

Layanan	Arsitektur	Teknologi
Access VPN	Client-Initiated	L2F/L2TP, IPSec, Dial, ISDN, DSL, Mobile IP, Cable
	NAS-Initiated	
Intranet dan Extranet VPN	IP Tunnel	GRE, IPSec, Mobile IP
	Virtual Circuit	Frame Relay, ATM
	MPLS	IP, IP+ATM

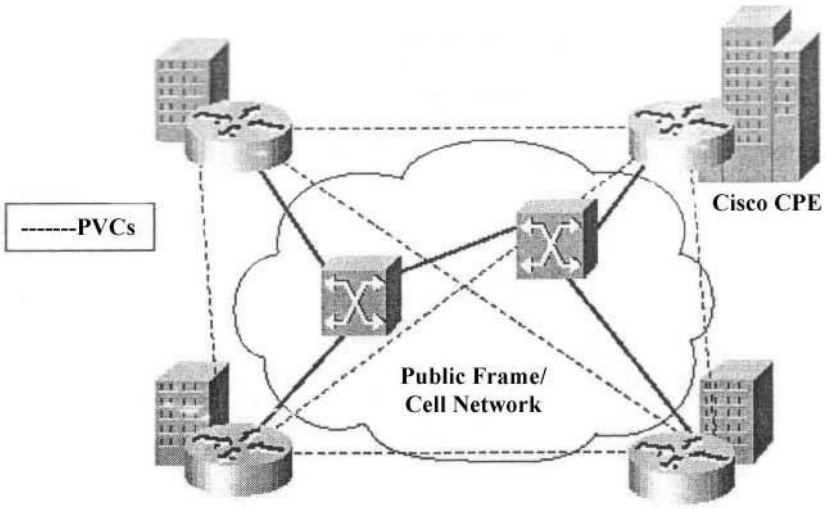
Tabel 2.3 Klasifikasi Layanan VPN

Pada dasarnya semua alternatif arsitektur VPN merupakan teknologi yang stabil dan dapat diandalkan, namun pada setiap arsitektur tersebut terdapat kelebihan dan kekurangan, untuk itu perlu dilakukan pemilihan arsitektur dan teknologi yang tepat sesuai kebutuhan masing-masing organisasi.

2.4.3.1 Arsitektur Frame Relay atau ATM Virtual Circuit

Teknologi VPN yang berbasis Virtual Circuit (VC) menyediakan fasilitas IP melalui jaringan *Frame Relay* umum atau jaringan ATM. Pada jaringan ini, enkripsi pada lapisan "link" bukan merupakan sesuatu yang mutlak, karena *Permanent Virtual Circuits* (PVCs) dan *Switched Virtual Circuits* (SVCs) telah merupakan jaringan yang bersifat pribadi. Penerapan enkripsi dapat dilakukan pada aplikasi tertentu saja yang bersifat kritikal sehingga tidak akan menimbulkan kelebihan beban kerja pada CPU.

Umumnya, penyedia jasa layanan akan memberikan layanan solusi total, yaitu dengan memberikan fasilitas *router* yang diatur oleh penyedia jasa layanan disisi pelanggan. Dengan demikian para penyedia jasa layanan tersebut dapat membuat jasa layanan seperti IP VPN dengan menggunakan PVCs dan SVCs untuk membangun hubungan point to point melalui *Frame Relay* atau jaringan ATM. Hal ini dapat dilakukan dengan menggunkan *router* untuk mengatur informasi yang ada pada lapisan ke 3. Sistem hubungan (*connectivity*) seperti ini, biasa disebut dengan arsitektur PVC "*spoke*" atau "*mesh*". Seperti terlihat pada Gambar 2.12.



Gambar 2.12 Arsitektur PVC pada jaringan *Frame Relay*

Kelebihan :

- Dengan memberikan *router* sebagai fasilitas tambahan, merupakan cara atau metode yang paling efisien, efektif dan cepat untuk menyediakan layanan VPN, khususnya bagi para service provider yang telah memiliki infrastruktur ATM atau *Frame Relay*
- Pembagian Bandwidth berbasiskan CIR pada *Frame Relay*, SCR atau MCR pada ATM.
- Dengan topologi VC, jaringan dapat dikembangkan.
- Penggunaan PVCs telah memberikan pemisahan VPN secara logical, sehingga penerapan enkripsi bukan merupakan keharusan.

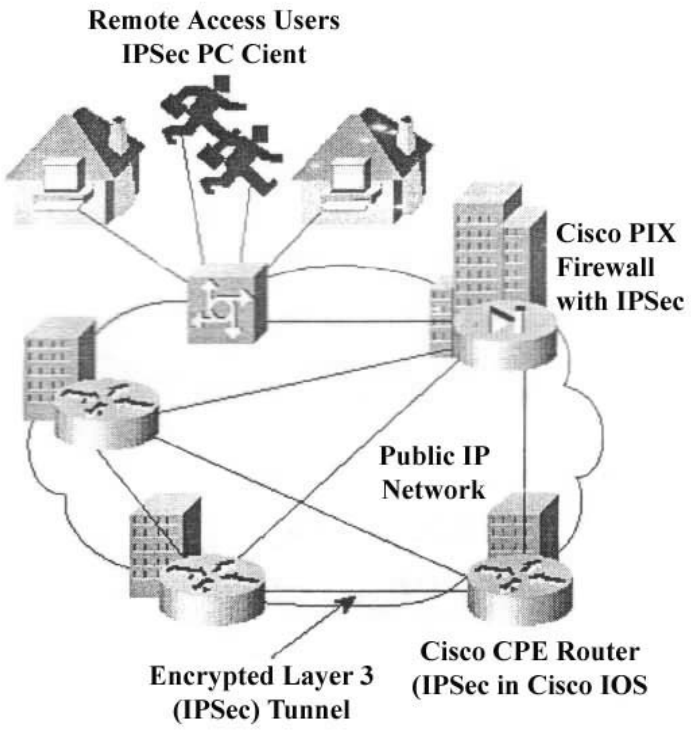
Kekurangan :

- Kemampuan *network* untuk mengembangkan "*any-to-any*" trafik menjadi terbatas dengan penerapan topologi *full mesh point-to-point*. Hal ini mengingat bahwa jumlah VC akan bertambah seiring dengan penambahan jumlah lokasi.
- Pada semua perangkat VPN di sisi pelanggan harus disimpan topologi VPN secara keseluruhan.
- Perubahan, penambahan, dan perpindahan harus disebarkan secara manual pada setiap pelanggan.
- QoS tidak dapat dijamin dengan melakukan mapping atau pemetaan aliran trafik IP, kecuali setiap perangkat pada sisi pelanggan dapat mengenali setiap aplikasi.

2.4.3.2 Arsitektur IP Tunneling

VPN dengan berbasiskan *tunnel* IP dapat dilakukan pada jaringan layer 3 dengan menggunakan protokol IPSec atau protokol GRE. *Tunnel* akan berfungsi layaknya sebuah amplop untuk mengetahui aliran paket dan menyembunyikan sebagian level dari informasi. Seperti terlihat pada Gambar 2.13, untuk dapat membangun sebuah tunnel, maka diperlukan perangkat security yang dapat melakukan enkripsi pada setiap paket.

Agar lebih terfokus, pada skripsi ini hanya akan dibahas *tunneling* dengan menggunakan protokol IPSec saja .



Gambar 2.13 Skenario VPN dengan menggunakan *tunnel* IPSec antara *router-router*.

Keuntungan :

- *Fast time-to-market*. Layanan VPN ini dapat diterapkan tanpa adanya perubahan pada infrastruktur pada sisi service provider.
- QoS. Service provider dapat memberikan penawaran fasilitas QoS dengan menggunakan atau melihat dari packet header.
- Penambahan fasilitas hubungan melalui dial-up dapat dilakukan dengan memberikan program IPSec client pada setiap notebook atau komputer, tanpa harus melakukan perubahan pada infrastruktur.

Kekurangan :

- Pemilihan fasilitas QoS terbatas, hal ini karena adanya proses tunnel sehingga ada beberapa packet header yang “tersembunyi” dengan adanya proses enkapsulasi IPSec. Dengan demikian jaringan tidak dapat membedakan paketnya.
- QoS melalui jaringan internet sangat terbatas dan tidak memungkinkan untuk mengirimkan aplikasi yang mission critical.
- Dapat merupakan solusi yang cukup mahal untuk dibangun dan diatur.

2.4.3.3 Arsitektur MPLS

MPLS merupakan teknologi yang memberikan terobosan baru terhadap dunia layanan IP VPN. Dengan menggunakan teknologi MPLS, para service provider mampu menyediakan layanan dengan skala besar, dan mampu untuk memberikan perbedaan pada layanan business VPN. Kesemuanya ini tidak memerlukan konfigurasi yang sulit baik di sisi service provider dan pada sisi pelanggan.

MPLS beroperasi dalam dua mode, yaitu : *extended mode* dan *full-compliance* mode. MPLS adalah suatu inovasi yang menggunakan pendekatan paradigma "*label-based forwarding*". Label tersebut akan menentukan jalur dan attribute layanan. Pada *ingress edge*, paket yang datang akan diperoses dan akan dipilihkan dan diterapkan label tersebut. Kemudian network equipment pada sisi CORE akan membaca label tersebut, dan menerapkan layanan yang sesuai dan meneruskan paket sesuai dengan tujuan yang ada pada label. Proses-proses analisa yang intesif, pembagian, dan penyaringan hanya terjadi sekali, yaitu pada saat paket pertama kali masuk (di *ingress edge*). Pada titik akhir (*egress edge*), label-label tersebut akan dihilangkan dan paket akan dilanjutkan pada tujuan terakhir.

Beberapa terminology MPLS :

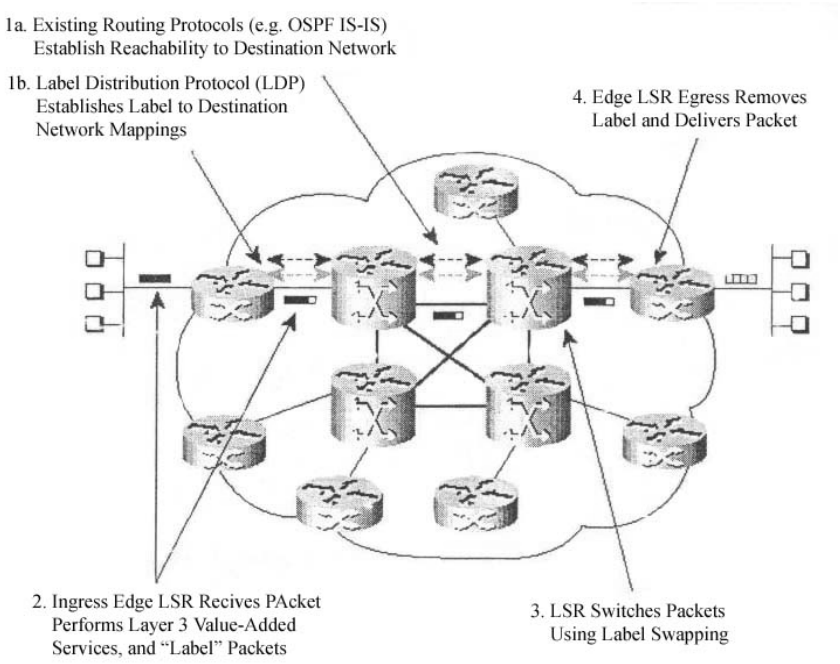
- *Edge label switch router* (Edge LSR) adalah perangkat VPN yang melakukan proses awal dan klasifikasi pada setiap paket serta menerapkan label yang pertama.
- *Label switch router* (LSR) adalah perangkat utama jaringan VPN yang melakukan pertukaran paket-paket yang telah diberi label. Pertukaran tersebut berdasarkan pada switching table yang telah di hitung sebelumnya. Perangkat ini bisa berupa switch ataupun router.
- *Label distribution protocol* (LDP) adalah protokol yang menyediakan jalur komunikasi antara perangkat *edge* dan *core*. Perangkat ini akan memberikan label pada perangkat di sisi *edge* dan *core* untuk membangun jalur label *switched paths* (LSPs), yang berhubungan dengan beberapa routing protocols, seperti OSPF,

Intermediate System-to-Intermediate System (IS-IS), *enhanced interior gateway routing protocol* (EIGRP), atau *border gateway protocol* (BGP)

- *Label switched path* (LSP) merupakan jalur yang ditetapkan oleh semua label diantara kedua titik akhir jalur MPLS. LSP dapat bersifat dinamis ataupun statik.
- Label adalah penanda yang dimiliki oleh setiap paket dan digunakan oleh LSR untuk meneruskan paket. Letak dari label pada tiap paket berbeda-beda, bergantung pada karakteristik jaringan. Pada jaringan berbasis *router*, label terletak pada "shim" header yang terpisah, yang terletak di depan IP header. Pada "shim" ini juga terdapat informasi untuk QoS (*Quality of Service*). Pada jaringan ATM, label diletakkan pada *virtual channel identifier/virtual path identifier* (VCI/VPI) dari sel ATM header.

Sistem Operasi MPLS

Secara umum, Gambaran proses VPN MPLS ini terlihat pada Gambar 2.14 .



Gambar 2.14 Sistem Kerja MPLS

- Tahap 1 → Jaringan secara otomatis membangun *routing tables*, sementara itu, semua perangkat (*router* dan *switch*) pada jaringan MPLS akan berpartisipasi dengan menggunakan *interior gateway protocols*, seperti OSPF, IS-IS, atau EIGRP. Dengan menggunakan topologi jalur (jaringan) yang terdapat pada *routing tables*, nilai label antara perangkat yang bersebelahan akan dibuat. Proses ini akan menghasilkan LSPs atau pre-configured map antara tujuan dan titik akhir. Label ini akan diberikan secara otomatis, tidak seperti PVC pada jaringan ATM.
- Tahap 2 → Paket akan mulai diproses pada LSR awal, dimana akan ditentukan jenis layanan lapisan 3 yang dibutuhkan, seperti QoS dan pengaturan *bandwidth*. Berdasarkan *routing* dan *policy requirements*, *edge* LSR akan memilih dan menerapkan label pada *header* dari paket.
- Tahap 3 → LSR pada pusat akan membaca label pada setiap paket, dan menggantikannya dengan label yang baru, sesuai dengan yang ada pada *forwarding table*, dan meneruskan paket. Proses ini akan berulang di setiap hops.
- Tahap 4 → LSR pada titik *egress* akan menghilangkan label pada paket header dan meneruskan paket ke tujuan akhir.

Label MPLS ini sebanding dengan *table switching* pada LSR core yang berisikan informasi layer 3 yang kemudian setiap LSR dapat secara langsung menerapkan layanan IP pada setiap paket. Tabel-tabel tersebut telah dilakukan perhitungan sebelumnya, sehingga tidak diperlukan untuk melakukan proses ulang paket pada setiap hop.

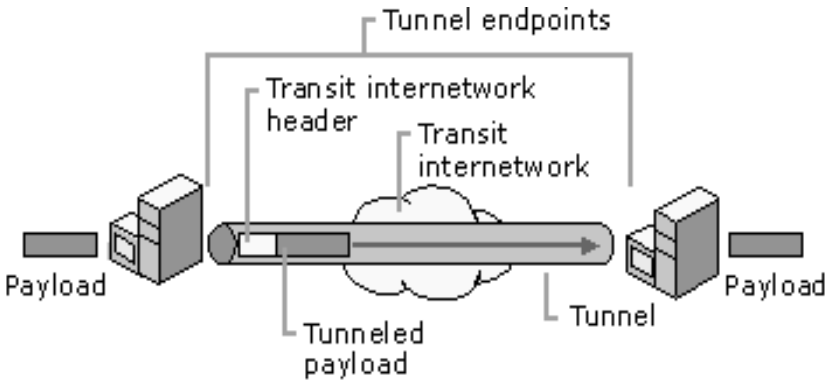
Pada *framework* ini, tidak hanya dapat memisahkan paket berdasarkan jenis trafiknya (seperti *best-effort*, atau *mission critical*), tetapi juga memberikan tingkat

skalabilitas yang tinggi. Karena MPLS menggunakan sistem policy yang berbeda untuk menentukan satu label pada setiap paket, yaitu dengan memisahkan *packet forwarding* dari isi IP headers. Setiap label mempunyai arti secara local, dan tetap digunakan beberapa kali pada network berskala besar, oleh karena itu, sangat kecil kemungkinannya untuk kehabisan label.

2.5 *Tunneling*

Tunneling merupakan enkapsulasi peket-paket atau *frame-frame* didalam paket-paket atau *frame-frame* lainnya, seperti halnya meletakan suatu amplop ke dalam amplop lainnya (Perlmutter, 2000, p104). *Tunneling* merupakan metode untuk transfer data dari satu jaringan ke jaringan lain dengan memanfaatkan jaringan *internet* secara terselubung. Disebut *tunnel* atau saluran karena aplikasi yang memanfaatkannya hanya melihat dua *end point* atau ujung, sehingga paket data yang lewat pada tunnel hanya akan melakukan satu kali lompatan atau hop. Ketika akan mengirim *frame* data, *protocol tunneling* akan mengenkapsulasi *frame* tersebut dengan *header* tambahan. *Header* tambahan tersebut berisi informasi *routing* sehingga data dan *frame* yang dikirim dapat melewati jaringan internet. Jalur yang dilewati data dalam internet disebut tunnel. Saat data tiba pada jaringan tujuan, proses yang terjadi selanjutnya adalah dekapsulasi, kemudian data original akan dikirim ke penerima terakhir. Tunneling mencakup keseluruhan proses mulai dari enkapsulasi, transmisi dan dekapsulasi.

Secara keseluruhan dapat dikatakan proses *tunneling,* seperti yang ditunjukan pada Gambar 2.15, merupakan proses enkapsulasi, transmisi, dan dekapsulasi paket data.



Gambar 2.15 *Tunneling*

2.5.1 Fungsi-fungsi *Tunneling*

Tunneling memiliki sejumlah fungsi dan peranan yang sangat penting dalam pengembangan dan penggunaan VPN, dan VPN itu sendiri juga bukanlah *tunnel*. Menurut Perlmutter ada 4 peranan penting suatu *tunnel* yaitu :

1. **Menyembunyikan Alamat *Private***

   Tunneling menyembunyikan paket privat dan alamat paket di dalam paket yang dialamatkan secara publik sehingga paket privat dapat menyeberangi jaringan publik. Sebagai contoh, sebuah organisasi yang menggunakan alamat IP yang tidak terregistrasi di dalam jaringan privat dapat menggunakan tunneling untuk memfasilitasi komunikasi melalui jaringan publik tanpa merubah rancangan pengalamatan IP-nya.

2. **Mentransportasikan *Non-IP Payload***

   VPN *Tunneling* juga mengizinkan transpor dari *non-IP Payload*, seperti IPX atau paket AppleTalk, dengan membangun *header* IP, diiikuti sebuah *header protokol tunneling*, sekitar payload. Bergantung pada protokol *tunneling* sendiri, *payload* sama juga dengan paket layer 3 atau frame layer 2. Demikian, paket non-IP

menjadi *payload* yang dapat ditransportasikan melalui network IP seperti internet.

3. **Memfasilitasi Aliran Data**

   Tunneling menyediakan jalan mudah untuk mem-*forward* keseluruhan paket atau *frame* secara langsung ke lokasi yang khusus. Di sana paket itu dapat dibahas mengenai keamanannya, QOS-nya, kebijaksanaan administrasi suatu network organisasi tertentu dari tujuan network tersebut.

4. **Menyediakan *built-in security***

   Beberapa *protocol tunneling*, khususnya IPSec, menambahkan *security layer* tambahan (*encryption, authentication*, dll) sebagai komponen *built-in* dari protokol. Protokol lainnya seperti L2TP, membuat rekomendasi tentang bagaimana mengimplementasikan *security*. PPTP juga memberikan enkripsi sebagai suatu pilihan dalam protokol.

2.5.2 Protokol *Tunneling* pada Layer 2

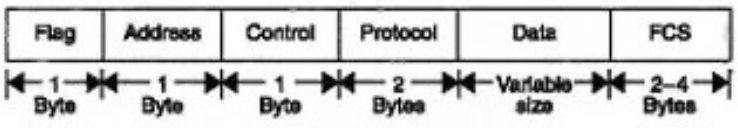
Protokol tunneling layer 2 pada OSI layer ini merupakan faktor penting dalam keamanan data pada pengiriman data melalui internet

2.5.2.1 *Point-to-Point Protocol* (PPP)

PPP adalah protokol enkapsulasi yang memfasilitasi transportasi antara jaringan dengan menggunakan koneksi *serial*. Keuntungan terbesar dari penggunaan PPP adalah PPP dapat bekerja dengan menggunakan di semua *Data Terminal Equipment* (DTE) atau *Data Connection Equipment* (DCE) yang termasuk dalam EIA/TIA-232-C dan ITU-T V.35.

Fungsi lain dari PPP selain protokol enkapsulasi IP adalah sebagai berikut :

- Memberikan dan mengontorol IP address.
- Konfigurasi dan test untuk mengetahui jalur stabil atau tidak.
- *Error detection* pada saat transmisi data.
- Memiliki standart dalam enkapsulasi untuk pengiriman data melalui *PPP-links*.
- Memiliki standart dalam membangun, mengkonfigurasi, dan melakukan testing pada koneksi dengan menggunakan *Link Control Protocol* (LCP).
- Standart untuk menstabilkan dan mengkonfigurasi protokol-protokol pada *Network-layer* dan mendeteksi kesalahan pada saat pengiriman data dengan menggunakan *Network Control Protocol* (NCP).

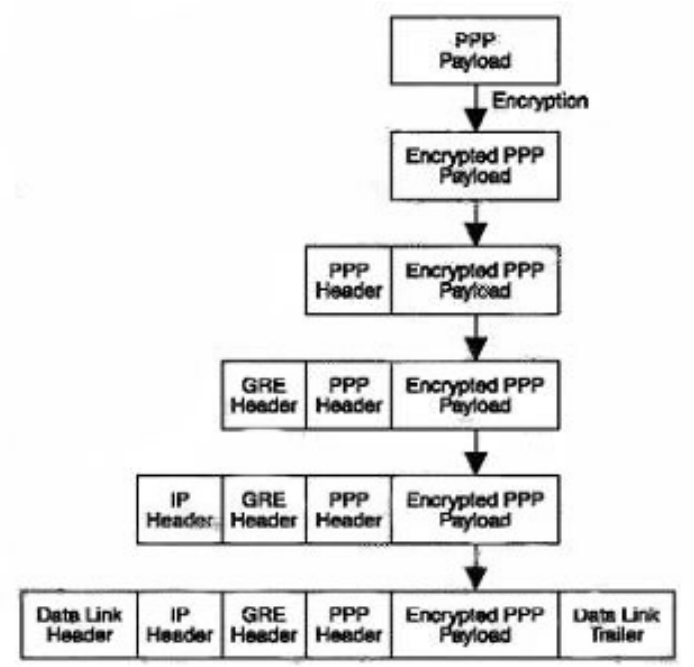


Gambar 2.16 Format pada PPP frame

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

PPTP adalah protokol yang memungkinkan terjadinya transfer data antara *remote client* dan *enterprise server* secara aman dengan menggunakan VPN yang berbasis IP *address.* PPTP dibangun oleh konsorsium PPTP yang terdiri dari Microsoft Corp. Ascend Communication, 3COM, US Robotics, ECI Telematics.

PPTP secara logika adalah protokol hasil dari modifikasi PPP, yang mendefinisikan cara pengiriman data PPP melalui internet. PPTP memungkinkan untuk mengenkipsi paket IP, IPX dan NetBEUI lalu mengenkapsulasikan dalam IP header untuk kemudian ditransfer melalui jaringan internet.



Gambar 2.17 Proses PPTP *Tunneling*

Keuntungan dari penggunaan PPTP :

- PPTP merupakan built-in soluion yang tersedia dalam produk microsoft yang sudah digunakan secara luas.
- PPTP mendukung protokol non-IP.
- PPTP didukung oleh berbagai macam platform seperti Unix. Linux, Apple, dan platform lain yang didukung bisa menggunakan router yang memiliki service PPTP.

Kerugian dari penggunaan PPTP :

- Security yang dimiliki lebih lemah dibanding L2PT dan Ipsec.
- Protokol PPTP tergantung pada platform.
- PPTP sulit untuk dikonfigurasi.

2.5.2.3 *Layer 2 Forwarding* (L2F)

L2F merupakan protokol yang diciptakan oleh Cisco dan Nortel untuk mengatasi kekurangan yang ada pada PPTP, dalam hal ini adalah keamanan pada saat pengiriman data. Kelebihan lain dari penggunaan L2F yaitu ada dukungan teknologi jaringan yang luas seperti *ATM, FDDI, IPX, Net-BEUI* dan *Frame Relay*. Selain itu L2F juga menawarkan fungsi yang sangat bagus dalam perkembangan teknologi jaringan yaitu tunnel pada L2F dapat mendukung satu atau lebih *sessions* yang dijalankan secara bersamaan, dengan kata lain beberapa user dapat mengakses VPN di tempat lain dengan satu koneksi dial-up yang digunakan secara bersama-sama.

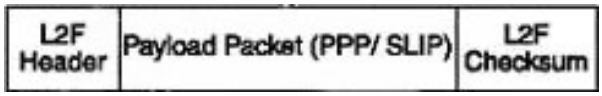
Keuntungan dari penggunaan L2F :

- Memperkuat keamanan data pada saat pengiriman data.
- Tidak tergantung pada platform tertentu.
- Mendukung banyak teknologi jaringan lain seperti *ATM, FDDI, IPX, NetBEUI,* dan *Frame Relay.*

Kekurangan dari penggunaan L2F adalah :

- Banyaknya konfigurasi yang harus dilakukan.
- L2F tidak mendukung flow control, jadi jika pada saat pengiriman kondisi tunnel sedang padat maka data yang terkirim akan di *drop,* hal ini akan menyebabkan proses pengiriman data dilakukan kembali yang akan menyebabkan penurunan pada kecepatan transaksi data.

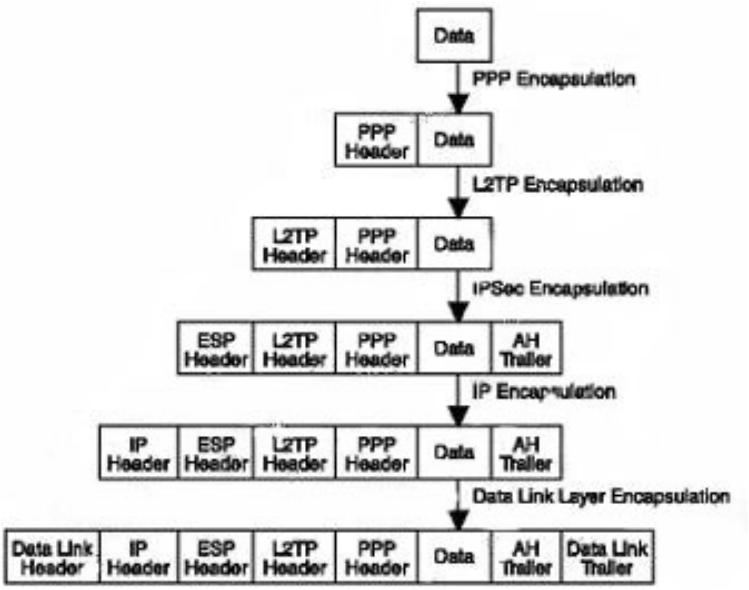
- Kecepatan pengiriman data pada L2F jika dibandingkan denga PPTP lebih lambat, karena proses authentikasi dan enkripsi pada L2F memakan sumber daya yang sangat besar.



Gambar 2.18 Format paket L2F

2.5.2.4 *Layer 2 Tunneling Protocol* (L2TP)

L2TP dibangun oleh Internet Engineering Task Force (IETF) dan didukung oleh Cisco System, Microsoft, 3COM, dan Ascend. L2TP adalah kombinasi dari protokol-protokol tunneling yang sebelumnya yaitu PPTP dan L2F, dengan kata lain L2TP merupakan penggabungan dari fitur-fitur terbaik yang ada pada PPTP dan L2F. L2TP memiliki beberapa fitur yaitu dukungan terhadap berbagai macam protokol, tidak membutuhkan tambahan software seperti driver atau *operating system* tertentu, L2PT juga mengijinkan *remote user* dengan alamat IP yang tidak terdaftar seperti IP *private* untuk bisa mengakses VPN.



Gambar 2.19 Proses enkapsulasi data pada L2TP

Keuntungan dari penggunaan L2TP adalah :

- Protokol ini tidak tergantung pada *platform* tertentu.
- Tidak membutuhkan konfigurasi pada user maupun pada ISP.
- Authentikasi user diatur oleh organisasi.
- Mendukung *flow control* sehingga membuat proses pengiriman data lebih cepat.
- Meningkatkan keamanan data, karena L2TP menggunakan enkripsi *payload* yang berbasis IPsec.

Kekurangan dari penggunaan L2TP adalah :

- L2TP lebih lambat dari PPTP maupun L2F.
- Perlu konfigurasi lebih lanjut pada *Routing and Remote Access Server* (RRAS).

Feature	PPTP	L2F	L2TP
Support to multiple protocols	Yes	Yes	Yes
Support to multiple PPP links	No	Yes	Yes
Support to multiple connections per tunnel	No	Yes	Yes
Operation modes supported	Incoming & Outgoing	Incoming	Incoming
Tunnel modes supported	Voluntary	Voluntary & Compulsory	Voluntary & Compulsory
Carrier protocol	IP/GRE	IP/UDP, IP/FR, IP/ATM	IP/UDP, IP/FR, IP/ATM
Control Protocol	TCP, Port: 1723	UDP, Port: 1701	UDP, Port: 1701
Authentication mechanisms	MS-CHAP, PAP	CHAP, PAP, SPAP, EAP, IPSec, RADIUS RADIUS & & TACACS	CHAP, PAP, SPAP, EAP, IPSec, TACACS
Encryption mechanisms	MPPE	MPPE, IPSec	MPPE, IPSec, ECP

Tabel 2.4 Perbandingan antara PPTP, L2F dan L2PT

2.6 *Internet Protocol Security* (IPSec)

IPSec merupakan suatu standar untuk mengamankan komunikasi-komunikasi *Internet Protocol* (IP) dengan mengenkripsi dan/atau mengautentikasi semua paket-paket IP (wikipedia.com). IPSec menyediakan *security* pada *network layer*. Berdasarkan pada standar yang dikembangkan oleh *Internet Engineering Task Force* (IETF), IPSec memastikan *confidentiality*, *integrity* dan *authenticity* dari suatu komunikasi yang melewati jaringan IP. IPSec menyediakan komponen standar yang diperlukan dan solusi fleksibel untuk membuat suatu kebijakan keamanan jaringan. IPSec juga mendukung baik itu IP Versi 4 (IPV4) maupun IP Versi 6 (IPV6). Dalam IPV6, IPSec merupakan komponen standar dari protokol. IPSec menyediakan *integrity* dan *confidentiality* untuk paket-paket IP. Untuk menyediakan layanan tersebut, IPSec terdiri dari 3 elemen dasar yaitu *authentication, encryption*, dan *key management*. Ketiganya itu berguna dalam suatu protokol VPN.

2.6.1 *Authentication*

IPSec memiliki suatu mekanisme yang sangat kuat untuk memverifikasi pengirim data dan mengetahui terjadinya modifikasi pada isi paket data. Hal ini dilakukan dengan cara menambahkan *Authentication Header* pada paket IP datagram, *header* ini akan membantu mendeteksi adanya perubahan pada isi dari IP datagram oleh pihak lain pada saat perjalanan.

2.6.1.1 *User Authentication.*

Dengan *user authentication*, orang yang tidak berhak masuk ke *network* dapat dikenali. Ada beberapa metode *user authentication* antara lain :

- *Pre-Shared Key*.

  Pre-shared key adalah *password* yang diberikan kepada *user* yang tidak memiliki hubungan dengan infrastruktur VPN. *Password* ini memberikan cara mudah bagi *remote user* tertentu untuk masuk ke dalam VPN.

- *Digital Signature*

  Digital Signatures adalah bukti elektronik untuk membuktikan identitas *user*. Sertifikat/*Signature* ini disimpan di *remote computer* atau token yang dibawa user. Sekarang ini algoritma *public key* RSA dan *Digital Signature Standard* (DSS) telah didukung oleh *digital signature*.

- *Hybrid mode Authentication*

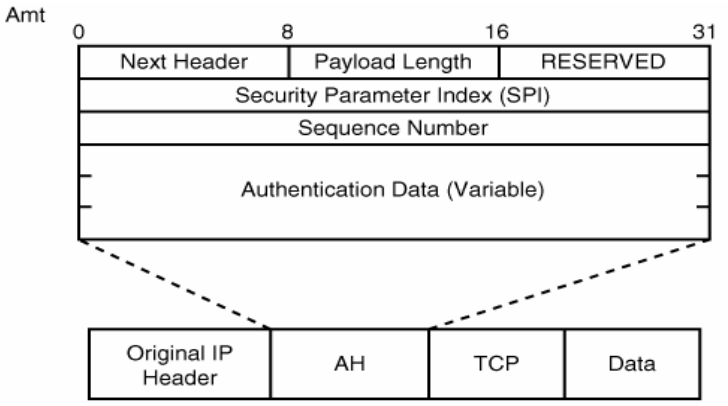
  Hybrid mode authentication memperbolehkan organisasi untuk menginterasikan sistem *authentication* seperti SecureID, TACACS+, dan RADIUS dengan VPN.

2.6.1.2 *Data Authentication*.

Untuk memastikan apakah data tidak berubah dalam perjalanan, sistem VPN menggunakan *data authentication*. Salah satu tehnik *data authentication* adalah *hash function*. Tehnik ini membuat suatu angka, yang disebut *hash*, berdasarkan dari panjang bit tertentu. Pengirim menambahkan angka *hash* tersebut ke dalam paket data sebelum *encryption*. Ketika penerima mendapatkan data dan melakukan *decription*, penerima akan melakukan perhitungan *hash* kembali. Apabila kedua angka *hash* tersebut cocok, maka dipastikan data tidak mengalami perubahan dalam perjalanan.

2.6.1.3 *Authentication Header* (AH)

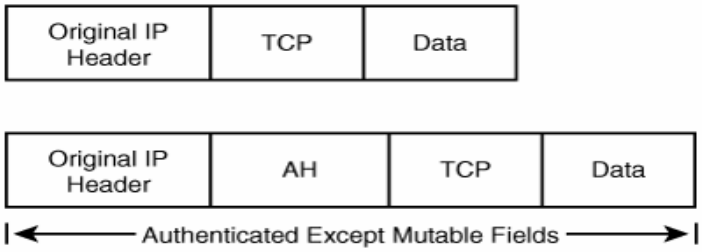
Header ini ditambahkan pada IP datagram untuk mendeteksi adanya perubahan pada isi dari datagram, header ini juga akan memastikan *integrity, authenticity* suatu data, dan *optional replay protection* termasuk *invariant field* diluar IP *header*.



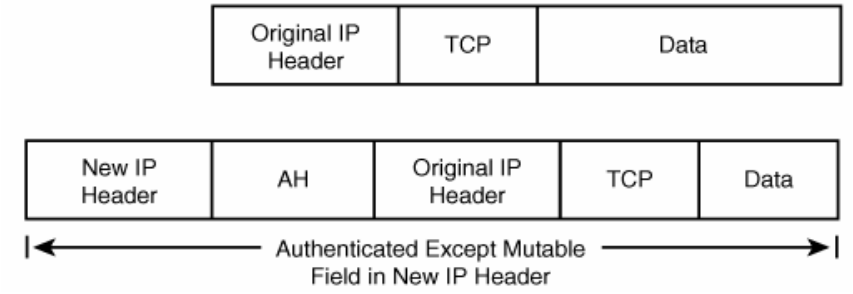
Gambar 2.20 Paket yang diproteksi AH

AH merupakan suatu protokol IP yang diidentifikasikan dengan nomor 51 dalam IP *header*. Dalam *transport mode, header* selanjutnya sesudah AH akan menjadi nilai

dari *upper layer protocol* yang diproteksi (UDP atau TCP). Dalam *tunnel mode*, nilainya 4. Posisi AH dalam *transport* dan *tunnel mode* ditunjukan pada Gambar 2.21 dan Gambar 2.22. Pada AH digunakan suatu *key-hash function* bukannya *digital signature* karena teknologi *digital signature* terlalu lama dan akan mengurangi *network throughput.*



Gambar 2.21 Paket IP yang diproteksi dengan AH dalam *transport mode*



Gambar 2.22 Paket IP yang diproteksi dengan AH dalam *tunnel mode*

2.6.2 *Encryption*

Encryption merupakan suatu teknik untuk mengacak dan menyusun kembali suatu informasi. Dengan *encryption*, kita mengubah isi dari data yang kita kirim sehingga data tersebut tidak dapat dibaca oleh orang yang tidak berhak mendapatkannya. Informasi yang tidak acak disebut *clear-text* sedangkan yang sudah diacak disebut *cipher-text*. Disetiap tunnel VPN terdapat VPN gateway. Gateway tempat pengiriman data meng-*encrypt* atau mengubah informasi *clear-text* menjadi *cipher-text* sebelum

dikirim melalui *tunnel* ke internet. VPN gateway di tempat penerima men-decrypt atau mengubah *cipher-text* tersebut kembali menjadi *clear-text*.

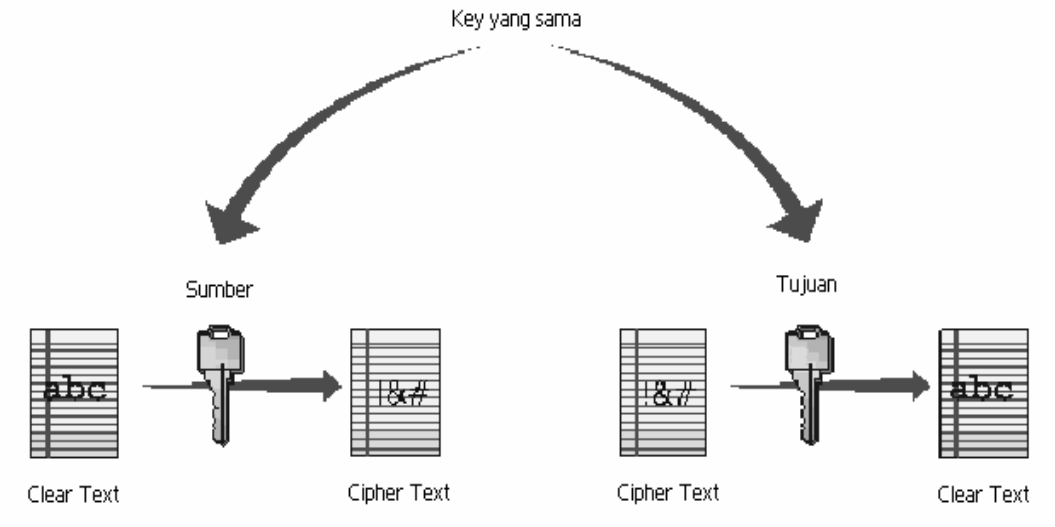
Untuk meng-*encrypt* dan men-*decrypt* informasi diperlukan sebuah *key*, yaitu kode rahasia yang berisi mengenai algoritma enkripsi tersebut. Dengan menggunakan sebuah 16-bit *key*, seorang hacker perlu mencoba 65.536 kombinasi untuk men-*decrypt cipher-text* tetapi ini dapat dilakukan dengan mudah oleh komputer di masa sekarang. Oleh karena itu, VPN sekarang lebih banyak menggunakan 168-bit key yang menciptakan 374.144.419.156.711 x 10^{36} kombinasi bahkan ada yang menggunakan lebih dari 168-bit *key*. Untuk meningkatkan keamanan, kita dapat mengganti key secara berkala. Lama waktu pemakaian suatu key tertentu disebut *cryptho-period*. Bahayanya penggantian *key* secara berkala, yaitu ada kemungkinan *key* yang baru memiliki persamaan dengan *key* yang lama dan kemiripan ini akan makin terlihat setiap kali *key* yang baru terbentuk. Di masa sekarang, terdapat dua metode *key* yang sekarang banyak dipakai, yaitu *symmetrical* dan *asymmetrical key encryption*.

2.6.2.1 *Symmetrical Key Encryption*

Symmetrical key encryption menggunakan *private key* berarti komputer pengirim dan penerima sama-sama menggunakan kunci yang sama untuk meng-encrypt dan men-decrypt informasi. Karena satu *key* digunakan bersama-sama untuk *encryption* dan *decryption*, maka harus ada pengertian antara kedua pihak untuk menjaga kerahasiaan *key* tersebut. Apabila ada orang yang berhasil mencuri key tersebut, maka dia bisa mendapatkan semua informasi yang ada.

Beberapa algoritma *private key* antara lain *Data Encryptian Standard* (DES) yang menggunakan 56-bit key untuk mengkompresi 64-bit data, RC4 yang

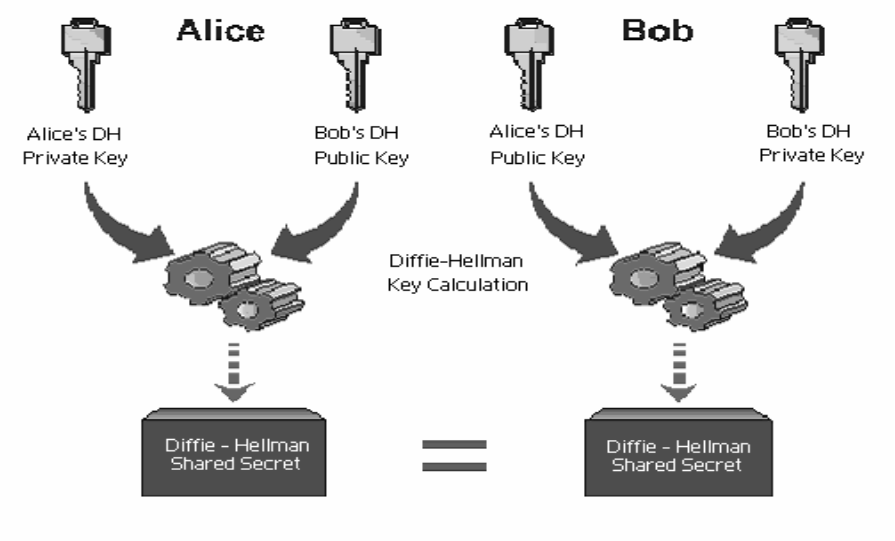
menggunakan 40-bit sampai128-bit key, dan Triple-DES (3-DES) yang menggunakan tiga kunci sekaligus sehingga menciptakan *encryption* yang lebih kompleks. Gambar 2.23 menunjukan gambaran mengenai *symmetrical key ecnryption* dengan menggunakan *key* yang sama.



Gambar 2.23 Symmetrical Key Encryption

2.6.2.2 *Asymmetrical Key Encryption*

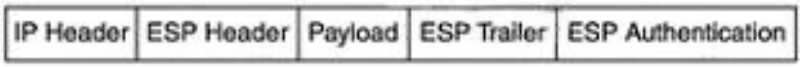
Asymmetrical Key Encryption meng-*encrypt* informasi dengan suatu *key* dan men-*decrypt* dengan *key* yang lain. Sistem ini menggunakan kombinasi dari dua buah *key*, yaitu *private key* yang disimpan untuk diri sendiri, dan *public key* yang diberikan untuk *remote user*. *Public-key* yang terkenal diantaranya Diffie-Hellman (DH) dan Rivest Shamir Adlemen (RSA). Gambar 2.24 menunjukan bagaimana *asymmetrical key encryption* dilakukan.



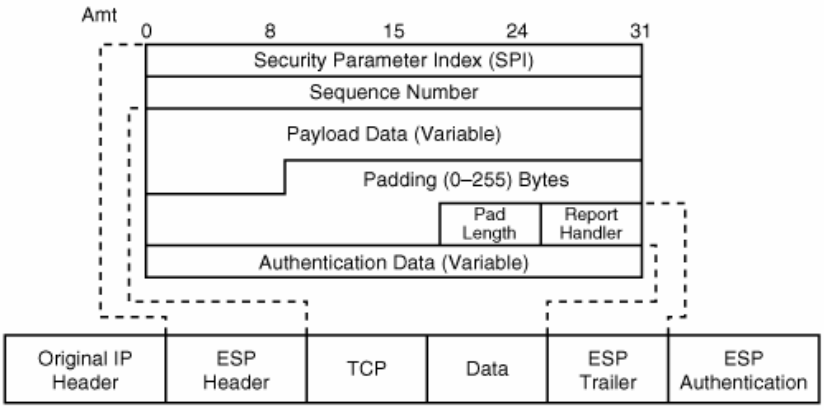
Gambar 2.24 Asymmetrical Key Encryption

2.6.2.3 *Encapsulation Security Payload* (ESP)

Header ESP ini, ketika ditambahkan ke IP *datagram*, akan melindungi *confidentiality*, *integrity*, *authenticity* dari suatu data dan *optional anti-replay services*. ESP menyediakan layanan ini dengan mengenkripsi muatan awal dan mengenkapsulasi paket diantara header dan trailer, seperti yang ditunjukkan pada Gambar 2.25.

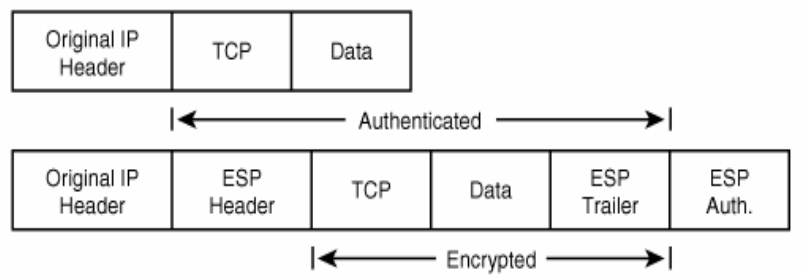


Gambar 2.25 Paket IP setelah ditambahkan ESP *header*

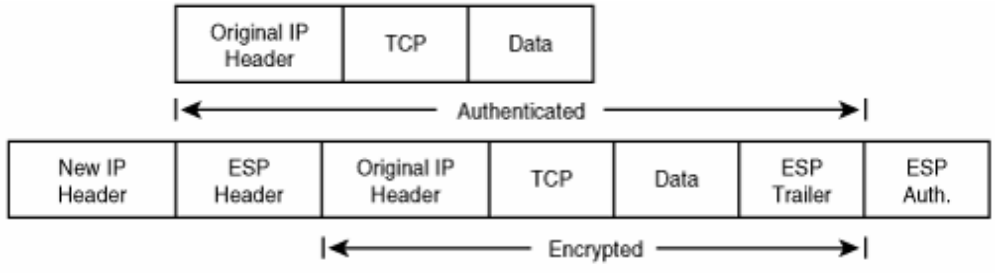


Gambar 2.26 Paket IP yang diproteksi dengan ESP

Bila dibandingkan dengan AH, yang menawarkan *confidentiality* dan *integrity* pada datagram IP, ESP tidak melindungi seluruh datagram. Hanya *payload*nya saja yang proteksi. Juga ESP tidak membebankan CPU jadi sebagai hasilnya ESP lebih cepat dari AH , tetapi 24 byte yang ditambahkan ESP ke dalam datagaram dapat menurunkan *throughput* dari jaringan itu sendiri.



Gambar 2.27 Paket IP yang diproteksi dengan ESP dalam *transport mode*



Gambar 2.28 Paket IP yang diproteksi dengan ESP dalam *tunnel mode*

2.6.3 *Key Management*

IPSec menyediakan banyak pilihan untuk menunjukan enkripsi dan authentikasi jaringan. Setiap koneksi IPSec dapat menyediakan baik enkripsi dan juga integritas dan authentikasi atau kedua-duanya. Ketika layanan keamanan ditetapkan, 2 node komunikasi harus menentukan algoritma mana yang akan digunakan (contohnya, DES atau 3DES untuk enkripsi; MD5 atau SHA untuk integritas). Setelah menentukan

algoritma, dua *device* tersebut harus men-*share session key* yang juga harus ada pengaturannya. *Security Association* (SA) merupakan metode yang IPSec gunakan untuk mencari semua yang berhubungan dengan sesi komunikasi IPSec. *Security association* merupakan hubungan antara dua kesatuan atau lebih yang menjelaskan bagaimana kesatuan tersebut akan menggunakan layanan security untuk berkomunikasi secara aman. *Security Association* menentukan algoritma authentikasi dan enkripsi yang digunakan, *encryption key* yang digunakan selama *session*, dan berapa lama *key* dan *security association* itu sendiri dipertahankan. SA pada umumnya digabungkan dengan Internet Key Exchange (IKE). IKE berfungsi untuk membantu kedua pihak yang saling berkomunikasi untuk bernegosiasi mengenai *security parameter* dan *authentication key* sebelum dijalankannya sesi IPSec. *Security parameters* yang dinegosiasikan merupakan parameter-parameter yang didefinisikan pada SA. Selain itu IKE juga memodifikasi *security parameters* dan *keys* pada saat session berlangsung jika dibutuhkan. IKE juga bertanggung jawab untuk menghapus semua *security parameters* dan *keys* ketika komunikasi yang menggunakan IPSec selesai. IKE bekerja dengan menggunakan 2 fase, yaitu :

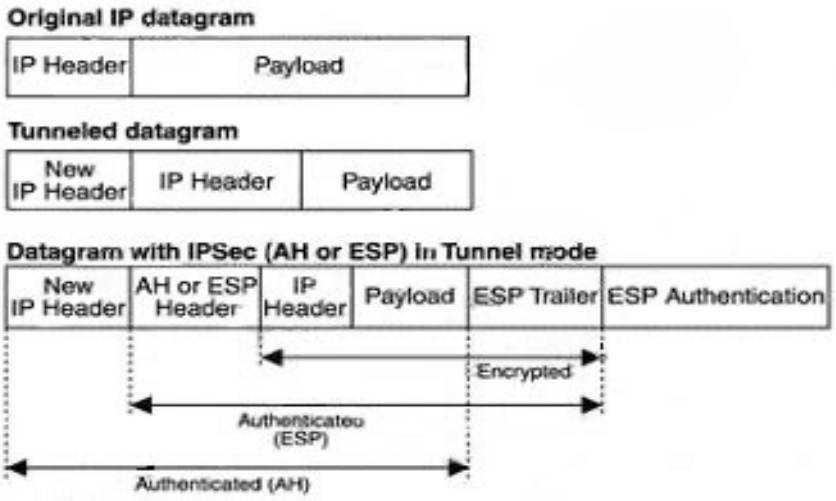
1. Tahap pertama membolehkan 2 *gateway security* untuk mengauthentifikasi satu sama lain dan membuat parameter komunikasi untuk tahap kedua. Diakhir tahap pertama, *security association* (IKE SA) dijalankan.
2. Tahap kedua memperbolehkan 2 *gateway security* untuk menyetujui parameter komunikasi IPSec berdasarkan pada masing-masing *host.* Diakhir tahap kedua, IPSec SA dijalankan

2.6.4 Mode pada IPSec

IPSec dapat digunakan dalam dua mode, mode transport yang mana mengamankan paket IP yang ada dari sumber ke tujuan, dan mode tunnel yang mana meletakkan paket IP dalam paket IP yang baru lalu dikirim ke sebuah *tunnel end point* dalam bentuk IPSec. Kedua mode, transpor dan tunnel dapat dienkapsulasikan dalam ESP atau header AH.

2.6.4.1 *IPSec Transport Mode*

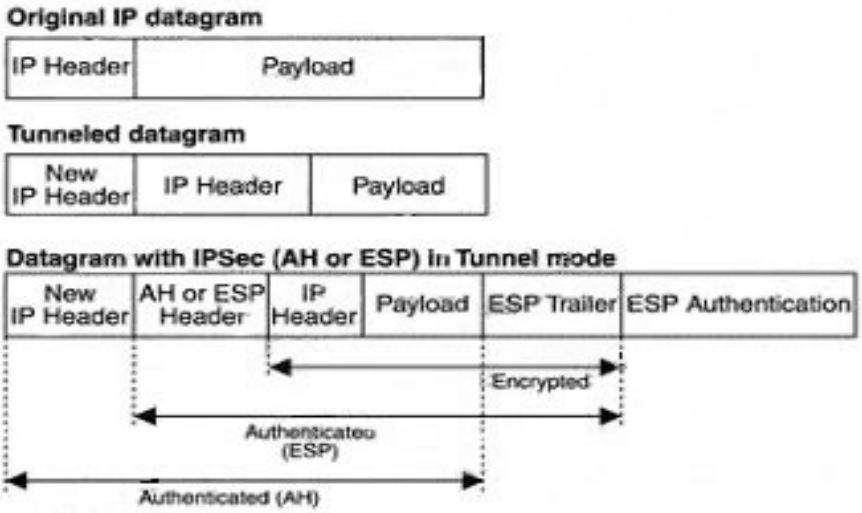
Dalam *transport mode*, IPSec *header* (AH atau ESP) disisipkan diantara IP *header* dan *upper layer* protokol *heade*r. Gambar 2.29 menunjukan IP packet yang diproteksi oleh IPSec dalam *transport mode*. Di mode ini, IP header sama dengan IP packet aslinya kecuali pada *field IP protocol*-nya , yang berubah menjadi ESP (50) atau AH (51) dan IP *header checksum*, yang dihitung kembali. Keuntungan mode ini adalah karena hanya menambah sedikit byte pada setiap paketnya dan mempunyai kemampuan untuk memungkinkan special processing (seperti *quality of service*) pada intermediate network berdasarkan informasi dalam IP *header*. Mode ini sangat berguna ketika *traffic* antara 2 *host* harus diproteksi, daripada ketika *traffic* berpindah dari *site* ke *site* lainnya, dan setiap *site* mempunyai banyak *host.*



Gambar 2.29 Paket IP dalam *IPSec Tranport Mode*

2.6.4.2 *IPSec Tunnel Mode*

Dalam *tunnel mode*, paket IP yang asli dienkapsulasi ke IP *datagram* yang lainnya, dan IPSec header (AH atau ESP) disisipkan diantara *inner* dan *outer* header. Karena enkapsulasi ini dengan suatu *outer IP packet*, *tunnel mode* dapat digunakan untuk menyediakan *security* antara *site* untuk kepentingan node IP yang berada dibelakang gateway router pada setiap *site*.



Gambar 2.30 Paket IP dalam *IPSec Tunnel Mode.*

2.7 *Secure Socket Layer* (SSL)

SSL protokol adalah satu set aturan komunikasi yang sepenuhnya disandikan dan hanya dapat dipahami oleh pengguna dan server yang sedang berkomunikasi. Protokol ini dikembangkan untuk mengamankan transmisi data penting pada jaringan internet.

SSL merupakan salah satu metode enkripsi dalam komunikasi data yang dibuat oleh Netscape Communication Corporation. SSL adalah protokol berlapis. Dalam tiap lapisannya, sebuah data terdiri dari panjang, deskripsi dan isi. SSL mengambil data untuk dikirim, dipecahkan ke dalam blok-blok yang teratur, kemudian dikompres jika perlu, menerapkan MAC, dienkripsi, dan hasilnya dikirim. Ditempat tujuan, data didekripsi, verifikasi, dekompres, dan disusun kembali.

SSL hanya mengenkripsikan data yang dikirim lewat HTTP. Bagaimana SSL berjalan dapat digambarkan sebagai berikut :

- Pada saat koneksi mulai berjalan, client dan server membuat dan mempertukarkan kunci rahasia, yang dipergunakan untuk mengenkripsi data yang akan dikomunikasikan. Meskipun sesi antara client dan server “diintip” pihak lain, namun data yang terlihat sulit untuk dibaca karena sudah dienkripsi.
- SSL mendukung kriptografi public key, sehingga server dapat melakukan autentikasi dengan metode yang sudah dikenal umum seperti RSA dan *Digital Signature Standard* (DSS).
- SSL dapat melakukan verifikasi integritas sesi yang sedang berjalan dengan menggunakan algoritma digest seperti MD5 dan SHA. Hal ini menghindarkan pembajakan suatu sesi.