Bab 2

Landasan Teori

Pada bab ini akan disajikan teori-teori baik teori secara khusus maupun teori secara umum yang berkaitan dengan topik ini.

2.1 Teori-teori Dasar/Umum

2.1.1 Pengertian Jaringan Komputer

Jaringan Komputer adalah sebuah system yang terdiri atas sebuah komputer dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama. Komputer dapat berhubungan satu dengan yang lainnya secara tidak terbatas baik dengan menggunakan kabel tembaga, *fiber optik, infrared, gelombang microwave,* bahkan bisa juga menggunakan satellite (Odom, 2005, p5).

2.1.2 Topologi Jaringan

Terdapat bermacam-macam topologi jaringan, yaitu :

1. ***Star*** (Lukas,2006,p144)

   Didalam 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.

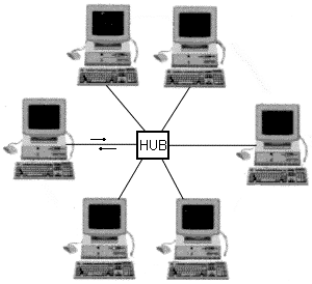
Terminal pusat akan menyediakan jalur komunikasi khusus pada dua terminal yang berkomunikasi.

Keuntungannya :

- Keterandalan terbesar di antaara topologi yang lain
- Mudah dikembangkan
- Keamanan data tinggi
- Kemudahan akses ke jaringan LAN lain

Kerugiannya :

- Lalu lintas yang padat dapat menyebabkan jaringan lambat
- Jaringan tergantung pada terminal pusat (dapat berupa komputer PC,mini atau mainframe), yang merupakan bagian paling bertanggung jawab terhadap pengaturan arah semua informasi ke terminal yang dikehendaki



Gambar 2.1 Topologi Star

2. Ring (Lukas,2006,p145)

LAN dengan topologi ini mirip dengan topologi titik ke titik tetapi semua terminal saling dihubungkan sehingga menyerupai lingkaran. Setiap informasi yang diperoleh, diperiksa

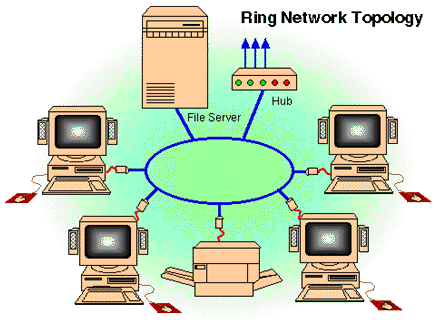
alamatnya oleh terminal yang dilewatinya. Jika bukan untuknya, informasi diputar lagi sampai menemukan alamat yang benar. Setiap terminal dalam LAN saling bergantungan, sehingga jika terjadi kerusakan pada satu terminal, seluruh LAN akan terganggu.

Keuntungannya :

- Laju data cepat
- Dapat melayani lalu lintas yang padat
- Tidak diperlukan host, relative lebih murah

Kerugiannya :

- Penambahan atau pengurangan terminal sangat sukar
- Harus ada kemampuan untuk mendeteksi kesalahan dan metode pengisolasian kesalahan
- Kerusakan pada salah satu terminal mengakibatkan kelumpuhan jaringan
- Tidak kondusif untuk pengiriman suara, video, dan data



Gambar 2.2 Topologi Ring

3. Bus (Lukas,2006,p146)

Pada Topologi bus semua terminal terhubung ke jalur komunikasi. Informasi yang hendak dikirimkan melewati semua terminal pada jalur tersebut. Jika alamat terminal sesuai dengan alamat pada informasi yang dikirim, maka informasi tersebut akan diterima dan diproses. Jika tidak, informasi tersebut akan diabaikan terminal yang dilewatinya.

Keuntungannya :

- Kemampuan pengembangan tinggi
- Jarak LAN tidak terbatas
- Keterandalan dan kecepatan jaringan tinggi
- Tidak diperlukan pengendali pusat

Kerugiannya :

- Jika tingkat lalu lintas terlalu tinggi dapat terjadi kongesti (Kemacetan)
- Diperlukan repeater untuk menguatkan sinyal pada pemasangan jarak jauh.
- Operasional jaringan LAN tergantung pada setiap terminal.

Gambar 2.3 Topologi Bus

2.1.3 Jenis-Jenis Jaringan

1. Local Area Network (LAN)

LAN adalah jaringan komputer yang jaringannya hanya mencakup wilayah kecil seperti jaringan komputer yang terdapat pada kampus, gedung, kantor, dalam rumah, sekolah atau yang lebih kecil lagi. LAN berbasiskan teknologi IEEE (*Institute of Electrical and Electronics Engineers*) 802.3 yang dikembangkan pada tahun 1983 dan mampu mentrasmisikan data dengan kecepatan 10 Megabit per detik melalui kabel koaksial. Biasanya jarak antarnode tidak lebih jauh dari sekitar 200m (http://id.wikipedia.org/wiki/Local_Area_Network).

2. Metropolitan Area Network (MAN)

MAN pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya memakai teknologi yang sama dengan LAN. MAN mencakup kantor-kantor perusahaan yang berdekatan dan dapat menunjang data, suara, dan bahkan dapat berhubungan dengan jaringan televisi kabel (Syafrizal, 2005, p16).

3. Wide Area Network (WAN)

WAN mencakup daerah geografis yang luas, seringkali mencakup sebuah Negara atau benua. Biasanya suatu WAN terdiri dari sejumlah node yang terhubung satu dengan yang lainnya (Stallings, 2001, p9).

Biasanya WAN diimplementasikan dengan menggunakan satu dari dua teknologi ini, yaitu :

1 Circuit Switching

Merupakan jaringan yang mengalokasikan sebuah sirkuit yang dedicated diantara nodes dan terminal untuk digunakan oleh pengguna untuk berkomunikasi. Sirkuit yang dedicated ini tidak dapat digunakan oleh penelepon lain sampai sirkuit itu terlepas dan koneksi baru bisa disusun, contohnya jaringan telepon.

2 Packet Switching

Merupakan jaringan yang membagi data yang akan dikirimkan (misalnya suara digital atau data komputer) menjadi kepingan-kepingan yang disebut dengan paket, dan dikirimkan melewati sebuah shared network dari satu node ke node yang lainnya sampai ke tujuannya..

2.1.4 Internet, Intranet dan Extranet

Internet ialah sistem komputer umum, yang berhubung secara global dan menggunakan TCP/IP sebagai protokol pertukaran paket (packet switching communication protocol). Rangkaian internet yang terbesar dinamakan Internet. Cara menghubungkan rangkaian dengan kaedah ini dinamakan internetworking. Rangkaian pusat yang membentuk Internet diawali pada tahun 1969 sebagai ARPANET, yang dibangun oleh ARPA (United States Department of Defense Advanced Research Projects Agency). Beberapa penyelidikan awal yang disumbang oleh ARPANET termasuk kaedah rangkaian tanpa-pusat (decentralised network), teori queueing, dan kaedah pertukaran paket (packet switching). (http://id.wikipedia.org/wiki/Internet).

Intranet adalah sebuah jaringan privat (private network) yang menggunakan protokol-protokol Internet (TCP/IP), untuk membagi informasi rahasia perusahaan atau operasi dalam perusahaan tersebut kepada karyawannya. Kadang-kadang, istilah intranet hanya menjurus kepada layanan yang terlihat, yakni situs web internal perusahaan. Untuk

membangun sebuah intranet, maka sebuah jaringan haruslah memiliki beberapa komponen yang membangun Internet, yakni protokol Internet (Protokol TCP/IP, alamat IP, dan protokol lainnya), klien dan juga server. (http://id.wikipedia.org/wiki/Intranet)

Ekstranet adalah jaringan pribadi yang menggunakan protokol internet dan sistem telekomunikasi publik untuk membagi sebagian informasi bisnis atau operasi secara aman kepada penyalur (supplier), penjual (vendor), mitra (partner), pelanggan dan lain-lain. Extranet dapat juga diartikan sebagai intranet sebuah perusahaan yang dilebarkan bagi pengguna di luar perusahaan. Perusahaan yang membangun extranet dapat bertukar data bervolume besar dengan EDI (Electronic Data Interchange), berkolaborasi dengan perusahaan lain dalam suatu jaringan kerjasama dan lain-lain. (http://id.wikipedia.org/wiki/Extranet)

2.1.5 Jenis-jenis Media Transmsi

1. Kabel

   Kabel merupakan media jaringan yang utama dalam membangun sebuah jaringan komputer termasuk juga kartu jaringan. Karena dengan dua komponen ini saja tanpa komponen media LAN expansion yaitu hub, satu jaringan komputer kecil sudah bisa dibangun dengan menggunakan topologi bus.

   Secara garis besar kabel jaringan dibagi atas 3 jenis saja, yaitu :

   - *Coaxial*

merupakan kabel yang paling banyak digunakan dalam jaringan komputer terutama pada saat masa di mana topologi bus paling populer digunakan. Kabel jenis ini menjadi pilihan karena 2 alasan utama yaitu murah dan mudah digunakan. Contoh kabel coaxial ini adalah kabel antena TV. Kabel coaxial ini terbagi lagi dalam 2 tipe yaitu *thin* (*thinnet*) dan *thick* (*thicknet*). Perbedaannya adalah kabel thin lebih fleksibel,lebih gampang digunakan dan yang penting lebih murah daripada kabel thick. Kabel thick lebih tebal dan susah dibengkokkan dan jangkauanya lebih jauh dibandingkan thin, hal ini yang membuat harganya lebih mahal. Sebagai perbandingan kabel thin jangkauannya adalah 185 meter sedangkan kabel thick jangkauannya adalah mencapai 500 meter

- *Twisted Pair*

  Merupakan jenis kabel yang paling sederhana dibandingkan dengan lainnya dan saat ini paling banyak digunakan sebagai media kabel dalam membangun sebuah jaringan komputer. Seperti halnya kabel coaxial, twisted pair ini juga dibagi atas 2 jenis yaitu *Unshielded Twisted Pair* (UTP) dan *Shielded Twisted Pair* (STP). Sesuai dengan namanya jelas bahwa perbedaan keduanya terletak pada shield atau bungkusnya. Pada kabel STP didalamnya terdapat satu lapisan pelindung kabel internalnya sehingga melindungi data yang ditransmisikan dari interferensi

atau gangguan. Kabel UTP jauh lebih populer dibandingkan dengan STP dan paling banyak digunakan sebagai kabel jaringan.

- *Fiber Optik*

  Jenis kabel yang terakhir dan paling mahal yaitu fiber optic. Pada kabel fiber, sinyal digital data ditransmisikan dengan menggunakan gelombang cahaya sehingga cukup aman untuk pengiriman data karena tidak bisa di-*tap* di tengah jalan sehingga data tidak bisa dicuri orang ditengah transmisi. Kabel fiber terdiri atas 3 lapisan. Lapisan luarnya atau disebut jacket dan lapisan kedua yaitu glass cladding dan lapisan intinya merupakan fiber optic itu sendiri.

Tabel 2.1 Perbandingan Media Transmisi

Medium Transmisi	***Total Data Rate***	***Bandwidth***	***Jarak Repeater***
Twisted Pair	3 Mhz	3 Mhz	2-10 km
Coaxial cable	500 Mhz	500 Mhz	1-10 km
Optikal fiber	2-10 Gbps	2-10 Gbps	10-100 km

2. Wireless

Jaringan nirkabel yang sering disebut dengan wireless network cukup mudah untuk di set up, dan juga terasa sangat nyaman, terutama jika menginginkan agar bisa berjalan jalan keliling rumah

atau kantor dengan komputer portable tetapi tetap bisa mengakses jaringan internet. (Lukas,2006,p69)

- Gelombang *Radio*

  Wireless LAN bekerja dengan menggunakan gelombang radio. Sinyal radio menjalar dari pengirim ke penerima melalui free space, pantulan, difraksi, dan Line of Sight. Ini berarti sinyal radio tiba di penerima melalui banyak jalur (*Multipath*), dimana tiap sinyal (pada jalur yang berbeda-beda) memiliki level kekuatan, *delay* dan fasa yang berbeda-beda.

- Gelombang *Mikro*

  Penggunaan gelombang mikro yang paling umun adalah untuk komunikasi jarak jauh (long-houl) dan umumnya digunakan untuk transmisi gelombang suara (radio) dan televisi. Aplikasi lainnya untuk gelombang mikro adalah untuk transmisi point to point jarak pendek, terutama untuk komunikasi antar gedung perkantoran.

- *Infrared*

  Komunikasi infrared dapat dilakukan dengan menggunakan transmitter (pengirim) dan receiver (penerima) yang dapat mengatur / modulasi sinar infra merah yang tidak kohern atau tidak menyatu (terpisah). Transceiver (alat penerima signal yang mendistribusikan signak kebeberapa receiver yang lebih kecil) masing-masing harus terletak pada satu garis lurus untuk menerima pemancaran secara langsung maupun cahaya

pantulan dari suatu permukaan yang berwarna terang misalnya langit – langit didalam.

2.1.6 Model referensi jaringan

1. Model referensi OSI layer

Model referensi jaringan terbuka OSI (*Open System Interconnection*)adalah sebuah model arsitektural jaringan yang dikembangkan oleh badan Internasional Organization for Standardzation (ISO) di Eropa pada tahun 1977.

OSI Reference Model memiliki tujuh lapisan , yakni sebagai berikut :

(http://id.wikipedia.org/wiki/OSI_Reference_Model)

1. *Layer 1 - Physical Layer*

   Layer ini berfungsi untuk mendefinisikan media trasmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya Ethernet atau Token Ring), topologi jaringan dan pengabelan. Physical layer juga mendefinisikan *Network Interface Card* (NIC) dapat berinteraksi dengan media kabel atau radio.

2. *Layer 2 - Data-Link Layer*

   Layer ini berfungsi untuk menentukan bagaimana bit - bit data dikelompokkan menjadi format yang disebut *frame. Data link layer* bertugas menjamin pesan yang dikirimkan ke media yang tepat dan mentrejemahkan pesan dari *network layer* ke dalam bentuk bit di physical layer untuk dikirimkan ke *host* lain.

3. *Layer 3 - Network Layer*

Layer ini berfungsi untuk mendefinisikan alamat- alamat IP, membuat header untuk paket-paket, dan kemudian melakukan routing melalui *internetnetworking* dengan menggunakan router dan *switch layer-3.*

4. *Layer 4 - Transport Layer*

Layer ini berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (acknowledgement), dan mentransmisikan ulang terhadap paket-paket yang hilang di tengah jalan.

Pada *transport layer*, proses pengiriman dapat dilakukan dengan 2 mekanisme :

1. TCP (*Transmission Control Protocol*)
    - Berorientasi sambungan (connection-oriented), sebelum data dapat ditransmisikan antara dua host, dua proses yang berjalan pada lapisan aplikasi harus melakukan negosiasi untuk membuat sesi koneksi terlebih dahulu. Koneksi TCP ditutup dengan menggunakan proses terminasi koneksi TCP (TCP connection termination).
    - Full-duplex, koneksi yang terjadi antara dua host terdiri atas dua buah jalur, yakni jalur keluar dan jalur masuk.

Koneksi yang terjadi ini dapat secara simultan diterima dan dikirim.

- Reliable, data yang dikirimkan ke sebuah koneksi TCP akan diurutkan dengan sebuah nomor urut paket dan akan mengharapkan paket *positive acknowledgment* dari penerima.
- *Flow Contol*, berfungsi untuk mencegah data terlalu banyak dikirimkan pada satu waktu yang akan membuat macet jaringan *internetwork IP*.

2. UDP (*User Datagram Protocol*)

- *Connectionless*, pesan-pesan UDP yang dikirimkan tanpa harus melakukan proses negosiasi koneksi antara dua host yang hendak bertukar informasi.
- *Unreliable*, pesan-pesan UDP akan dikirimkan sebagai datagram tanpa adanya nomor urut.
- UDP menyediakan mekanisme untuk mengirim pesan-pesan ke sebuah protokol lapisan aplikasi di dalam sebuah host dalam jaringan yang menggunakan TCP/IP.

5. Layer 5 - Session Layer

Layer ini berfungsi untuk mengkoordinasi komunikasi yang berjalan, melakukan proses pembentukan, pengelolaan dan

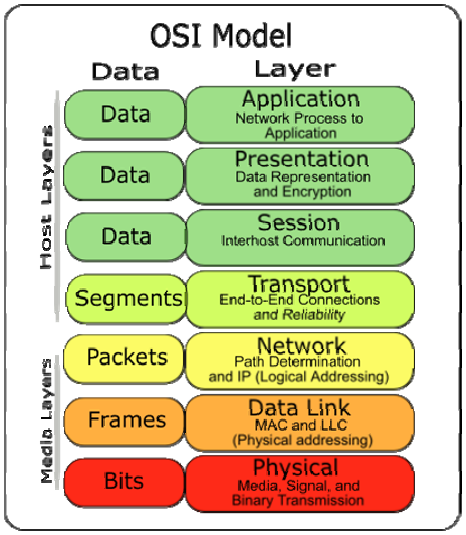
pemutusan session antar sistem aplikasi, mengendalikan dialog antar *device* atau *nodes.*

6. *Layer 6 - Presentation Layer*

   Layer ini berfungsi menyediakan sistem penyajian data ke *application layer,* menyediakan layanan *translation* (menjamin data dapat dibaca diantara system yang berbeda pada *application layer*), dan di layer ini dapat melakukan *compression, decompression, encryption,* dan *decryption.*

7. *Layer 7 - Application Layer*

   Layer ini berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan (seperti *e-mail, transfer file*). *Application layer* mengidentifikasi dan membangun komunikasi yang diinginkan, Layer ini merupakan tempat dimana user berinteraksi dengan komputer. Layer ini hanya berperan ketika dibutuhkan akses ke *network.*



Gambar 2.4 OSI Model

2. Model Referensi TCP/IP

Merupakan model yang dikembangkan sebagai sebuah riset militer Amerika Serikat yang didanai oleh Department Pertahanan (DOD) (Stalling,2001,p54). TCP/IP dikembangkan sebagai sebuah *open standard* yang artinya bahwa setiap orang dapat menggunakan TCP/IP secara bebas dan dapat membantu pengembangan TCP/IP sebagai sebuah standarisasi.TCP/IP mengimplemenasikan arsitektur berlapis yang terdiri atas empat lapis.Empat lapis ini, kadang-kadang disebut sebagau *DARPA Model*, *Internet Model*, atau *DoD Model.*

Ciri – ciri *TCP/IP* adalah :

- Setiap paket yang dikirim akan mendapatkan tanda terima.
- Apabila terjadi error pada saat pengiriman paket, maka paket akan dikirimkan kembali.
- Paket tersebut akan diurutkan kembali setelah sampai di tujuan.

Model ini memiliki empat layer, yaitu :

1. *Layer 1 - Network Access Layer*

   Network access layer berkaitan dengan pertukaran data antara dua *end system*, dan jaringan yang menghubungkannya.

2. *Layer 2 - Internet Layer*

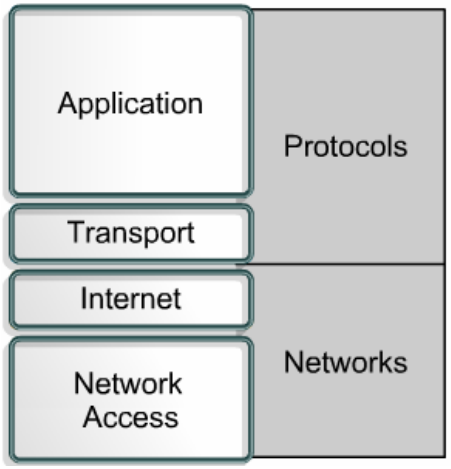
Internet layer bertugas untuk memilih jalur yang terbaik pada jaringan yang akan dilewati oleh paket. Protokol utama yang berfungsi pada layer ini adalah *Internet Protocol (IP)*.

3. *Layer 3 - Transport Layer*

Transport Layer berfungsi untuk menyediakan layanan transfer data. *Layer* ini sejalan dengan fungsi *transport layer* pada OSI. *Layer* ini menangani masalah seperti menciptakan komunikasi *end-to-end* (ujung ke ujung) yang handal dan memastikan data tersebut bebas dari kesalahan pada saat pengiriman. *Layer* ini juga menangani paket yang berurutan (*packet sequencing*) dan menjaga integritas data.

4. *Layer 4 - Application Layer*

Layer ini bertanggung jawab untuk menyediakan akses kepada aplikasi terhadap layanan jaringan TCP/IP.



Gambar 2.5 TCP/IP Model

2.1.7 Perbedaan antara OSI *layer* dan TCP *layer*

Perbedaan antara TCP/IP model dengan OSI model adalah sebagai berikut :

- TCP/IP menggabungkan *layer application, presentation* dan *session* dari OSI Model ke dalam *layer application.*
- TCP/IP menggabungkan *layer data link* dan *physical* dari OSI Model ke dalam *layer network access*.

2.1.8 IP Address

IP *address* terdiri dari bilangan biner sepanjang 32 bit yang dibagi atas 4 segmen.Tiap segmen terdiri atas 8 bit yang berarti memiliki nilai desimal dari 0-255. Range address yang bisa digunakan adalah dari 00000000. 00000000. 00000000. 00000000 sampai dengan 11111111. 11111111. 11111111. 11111111. Jadi ada sebanyak 232 kombinasi address yang bisa dipakai di seluruh dunia (walaupun pada kenyataanya ada sejumlah ip *address* yang digunakan untuk keperluan khusus). Jadi jaringan TCP/IP dengan 32 bit address ini mampu menampung sebanyak 232 atau lebih dari 4 milyar host.

Untuk memudahkan pembacaan dan penulisan, IP address biasanya direpresentasikan dalam bilangan desimal. Jadi range address diatas dapat diubah menjadi address 0.0.0.0 sampai dengan 255.255.255.255. Nilai desimal dari IP *Address* inilah yang dikenal dalam pemakaian sehari-hari. Contohnya 192.168.10.10 dalam bilangan binary adalah 11000000.10101000.00001010.00001010

Ip *address* dapat dipisahkan menjadi 2 bagian, yakni bagian network (bit-bit network/network bit) dan bagian host (bit-bit host/host bit). Bit network berperan dalam identifikasi suatu network dari network lainnya, sedangkan bit host berperan dalam identifikasi host dalam suatu network. Jadi seluruh host yang tersambung dalam jaringan yang sama memiliki bit network yang sama. Sebagian dari bit-bit bagian awal dari IP Address merupakan network bit/network number, sedangkan sisanya untuk host. Garis pemisah antara bagian network dan host tidak tetap, bergantung kepada kelas network.

Network address adalah address yang digunakan untuk mengenali suatu network pada jaringan internet. Tujuannya adalah untuk menyederhanakan informasi routing pada internet. Router cukup melihat network address untuk menentukan kemana paket tersebut harus dikirimkan. Contoh suatu network address untuk IP *address* 202.152.1.25 adalah 202.152.1.0. Contoh analoginya adalah pengolahan surat pada kantor pos. Petugas penyortir surat pada kantor pos cukup melihat kota tujuan pada alamat surat untuk menentukan jalur mana yang harus ditempuh surat tersebut.

Broadcast Address adalah *address* yang digunakan untuk mengirim/menerima informasi yang harus diketahui oleh seluruh *host* yang ada pada suatu network. Apabila host ingin mengirimkan paket kepada seluruh host yang ada pada network maka *host* cukup mengirim paket tersebut ke alamat *broadcast* yang ada maka seluruh *host* yang ada pada network akan menerima paket tersebut. Konsekuensinya seluruh

host pada network yang sama harus memiliki address broadcast yang sama dan *address* tersebut tidak boleh digunakan sebagai *IP address* untuk *host* tertentu.

1. Pembagian Class IP *address*

a *Class A address*

Class A address didesain untuk digunakan didalam *network* yang besar, dengan jumlah lebih dari 16 juta *host address* yang tersedia IP *address*.*Class A address* hanya menggunakan oktet yang pertama menunjukkan *network addre*ss dari tiga oktet sisanya yang tersedia untuk host address.Bit pertama pada *Class A* address adalah 0. Dengan bit pertama adalah 0 dan angka tertinggi adalah 127. Angka 0 dan 127 tidak dapat digunakan, serta IP address 127.0.0.0 tidak dapat digunakan karena dipakai untuk *loopback testing* yang berfungsi untuk mem-verifikasi fungsi TCP/IP stack dan fungsi transmit/receive NIC.Jadi range IP pada Class A adalah 1-126.

b *Class B address*

Class B address didesain untuk kebutuhan jaringan dengan ukuran menengah sampai dengan ukuran besar. *Class B address* menggunakan dua oktet pertama dari empat oktet untuk menunjukkan *network address* dan sisanya menunjukkan *host address*. Range IP pada class B adalah 128-191.

c *Class C address*

Classs C address didesain untuk mensupport jaringan kecil dengan jumlah maksimum 254 *host. Address IP* yang oktet pertamanya dimulai dengan angka 192 – 223.

d *Class D address*

Class D address didesain untuk *multicasting* di dalam suatu IP address. *Multicasst address* merupakan suatu *network address* unik yang menunjukkan paket dengan address tujuan ke group yang telah ditentukan dari sebuah *IP address. Multicast Address* tidak digunakan untuk alamat suatu host tetapi ditujukan untuk mengalamatkan sejumlah host yang bergabung dalam satu grup yang menjalankan aplikasi yang sama. *Range IP Class D* adalah 224 – 239.

e *Class E address*

Class E address digunakan untuk keperluan riset, oleh karena tu tidak ada IP di *class E address* yang dikeluarkan di internet.*Range IP Class E* adalah 240 - 255.

Tabel 2.2 Kelas-kelas IP Address

Ip Address Class	*Ip Address Range*
Class A	1-126 (00000001 – 01111110)
Class B	128-191 (10000000 - 10111111)
Class C	192-223 (11000000 - 11011111)

Class D	224-239 (11100000 – 11101111)
Class E	240-255 (11110000 - 11111111)

2. *IP Public* dan *IP Private*

IP Public adalah alamat-alamat yang telah ditetapkan oleh Information Center (InterNIC) dan berisi beberapa buah *network identifier* yang telah dijamin unik (artinya tidak ada dua host yang menggunakan alamat yang sama) jika intranet tersebut telah terhubung ke Internet. Dengan perkembangan internet yang begitu pesat, *IP Public* makin lama makin menipis sehingga skema addressing yang baru seperti IPv6 dikembangkan untuk memecahkan masalah tersebut

IP Private adalah alamat IP yang digunakan di jaringan Private tidak digunakan di jaringan public. Pada kasus internet, setiap node di dalam sebuah jaringan yang terhubung ke internet akan membutuhkan sebuah alamat yang unik secara global terhadapat internet. Karena perkembangan internet yang amat pesat, organisasi-organisasi yang menghubungkan *intranet* miliknya ke internet membutuhkan sebuah alamat *IP public* untuk setiap node di dalam intranet miliknya tersebut. Oleh karena itu akan membutuhkan sebuah alamat public yang unik secara global.

Kelas-kelas pada IP private dapat dilihat pada table dibawah ini :

Tabel 2.3 Kelas-kelas IP Private.

Class	*Start of Range*	*End of Range*
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

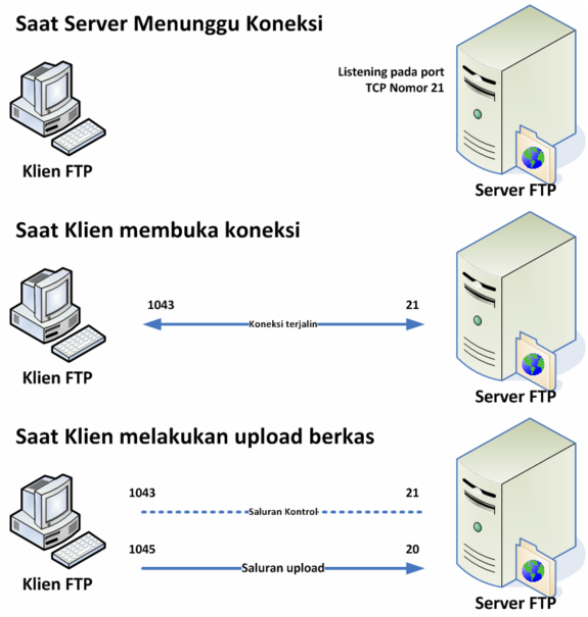
2.2 Teori-teori Khusus

2.2.1 File Transfer Protocol (*FTP*)

FTP adalah sebuah protocol internet yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pentransferan berkas (file) komputer antar mesin-mesin dalam sebuah internetwork. *FTP* merupakan salah satu protocol internet yang paling awal dikembangkan dan masih digunakan saat ini untuk melakukan *download* dan *upload* untuk berkas-berkas komputer antara *client FTP* dan *server FTP*. Sebuah client FTP merupakan aplikasi yang dapat mengeluarkan perintah- perintah FTP ke sebuah server FTP sementara server FTP adalah sebuah windows service atau *daemon* yang berjalan diatas sebuah komputer yang merespons perintah- perintah dari sebuah klient FTP. Perintah-perintah FTP dapat digunakan untuk mengubah direktori, mengubah modus transfer antara *biner* dan *ASCII*, upload berkas komputer ke server FTP, serta *download* berkas dari server FTP.

Sebuah server FTP diakses dengan menggunakan *Universal Resource Identifier* (URI) dengan menggunakan format ftp://namaserver/.

Klien FTP dapat menghubungi server FTP dengan membuka URI tersebut.



Gambar 2.6 Koneksi FTP

FTP menggunakan protocol *TCP* untuk komunikasi data antara klien dan server sehingga diantara kedua komponen tersebut akan dibuat sebuah sesi komunikasi sebelum transfer data di mulai. Sebelum membuat koneksi, port TCP nomor 21 di sisi *server* akan ”mendengarkan” percobaan koneksi dari sebuah client FTP dan kemudian akan digunakan sebagai port pengatur untuk :

1. Membuat sebuah koneksi antara client dan *server*.
2. Mengijinkan *client* untuk mengirim sebuah perintah FTP kepada server.
3. Mengembalikan respons *server* ke perintah tersebut.

Setelah koneksi kontrol telah dibuat, maka *server* akan mulai membuka port *TCP* nomor 20 untuk membentuk sebuah koneksi baru dengan client untuk mentransfer data aktual yang sedang di pertukarkan saat melakukan *download* dan *upload.* FTP hanya menggunakan metode *autentikasi* standar, yakni menggunakan *username* dan *password* yang dikirim dalam bentuk tidak terenkripsi. Pengguna terdaftar dapat menggunakan *username* dan *password*-nya untuk mengakses, men-*download*, dan meng-*upload* berkas-berkas yang ia kehendaki. Umumnya, para pengguna terdaftar memiliki akses penuh terhadap beberapa direktori, sehingga mereka dapat membuat berkas, membuat direktori, dan bahkan menghapus berkas.

2.2.2 Winzip

Winzip adalah sebuah program computer yang digunakan untuk mengkompres/ menciutkan/ mengecilkan sebuah file dan untuk membukanya kembali. Contohnya sebuah file dengan ukuran 110 KB bisa dikecilkan menjadi 86 KB dengan *Winzip*. File dengan ukuran yang kecil lebih mudah untuk dikirim daripada file dengan ukuran yang besar. Kompresi atau Zip adalah istilah yang umum digunakan untuk merujuk pada penyusutan ukuran file dari ukuran sebenarnya. Setelah suatu file dikompresi dengan menggunakan program Winzip, tipe filenya (ditandakan pada 3 huruf setelah titik pada nama file, misal dataku.doc, maka tipe file/ekstensinya adalah .doc) akan berubah menjadi .zip. Dekompresi atau Ekstrak adalah proses kebalikan dari kompresi, yakni

mengembalikan file .zip yang telah dikompresi ke bentuk asalnya. Winzip adalah salah satu dari sekian banyak program yang dipergunakan untuk memanipulasi ukuran file untuk tujuan yang bervariasi mulai dari penghematan ruang penyimpanan hingga untuk keperluan keamanan transfer tersebut. Untuk keamanannya maka bisa menambahkan *password* pada file yang di winzip tersebut sebelum data akan di kirimkan.

2.2.3 Secure Shell (SSH)

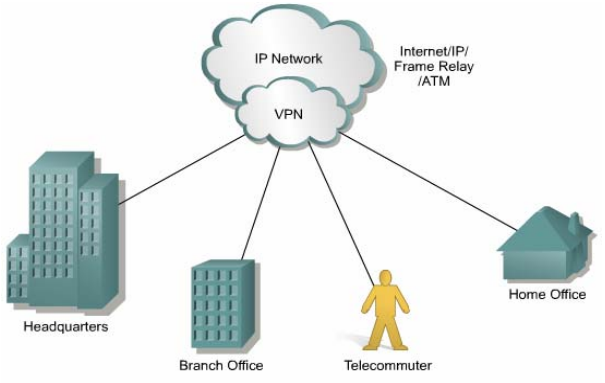
Secure Shell (SSH) adalah program yang memungkinkan user login ke mesin melewati jaringan, mampu mengeksekusi mesin secara remote, dan memindahkan file dari satu mesin ke mesin lain. SSH memberikan *autentikasi* dan komunikasi yang aman melewati jalur yang tidak aman. Ketika user menggunakan ssh, semua sesi login, termasuk transmisi *password* dienkripsi maka menjadi lebih aman. SSH menggunakan port 22 dan mendukung authentikasi dengan *username* dan *password*. Protocol SSH memiliki fitur sebagai berikut :

1. Enkripsi, melindungi data saat melewati jaringan dengan cara mengenkripsinya,
2. Integritas, menjamin data yang dikirim melalui jaringan sampai ke penerima dalam keadaan utuh.
3. Autentikasi, menjamin bahwa data yang dikirim berasal dari sumber yang semestinya.

Algoritma enkripsi yang di dukung oleh *SSH* diantaranya *BlowFish* (BRUCE SCHNEIER), *Triple DES* (Pengembangan dari DES oleh IBM), *IDEA* (*The International Data Encryption Algorithm*) dan *RSA*(*The Riverst-Shamir-Adelman*).

2.2.4 Virtual Private Network

Virtual Private Network (VPN) adalah sebuah jaringan *private* yang dibuat di atas jaringan *public* dengan menggunakan internet sebagai media komunikasinya.(Stalling 2003). VPN menggunakan layer *datalink* dalam melakukan proses tunnelingnya, proses encapsulasi dan pada saat pengirimannya menggunakan layer *networking*.VPN biasanya hanya dimiliki oleh suatu perusahaan yang memiliki beberapa cabang dimana cabang-cabang tersebut dihubungkan melalui infrastruktur jaringan yang dimiliki oleh suatu *service provider*.



Gambar 2.7 *Virtual Private Network*

Teknologi VPN menyediakan tiga fungsi utama untuk penggunanya. Fungsi utama tersebut adalah sebagai berikut:

1. Confidentiality (Kerahasiaan)

Teknologi VPN memiliki sistem kerja mengenkripsi semua data yang lewat melaluinya. Dengan adanya teknologi enkripsi ini, maka kerahasiaan Anda menjadi lebih terjaga. Biarpun ada pihak yang dapat menyadap data Anda yang lalu-lalang, namun belum tentu mereka bisa membacanya dengan mudah karena memang sudah diacak. Dengan menerapkan sistem enkripsi ini, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data Anda dengan mudah.

2. Data Integrity (Keutuhan Data)

Ketika melewati jaringan Internet, data Anda sebenarnya sudah berjalan sangat jauh melintasi berbagai negara. Di tengah perjalanannya, apapun bisa terjadi terhadap isinya. Baik itu hilang, rusak, bahkan dimanipulasi isinya oleh orang-orang iseng. VPN memiliki teknologi yang dapat menjaga keutuhan data yang Anda kirim agar sampai ke tujuannya tanpa cacat, hilang, rusak, ataupun dimanipulasi oleh orang lain.

3. Origin Authentication (Autentikasi Sumber)

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi source datanya. Kemudian alamat source data ini akan disetujui jika proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan

diterima oleh Anda berasal dari sumber yang semestinya. Tidak ada data yang dipalsukan atau dikirimkan oleh pihak-pihak lain.

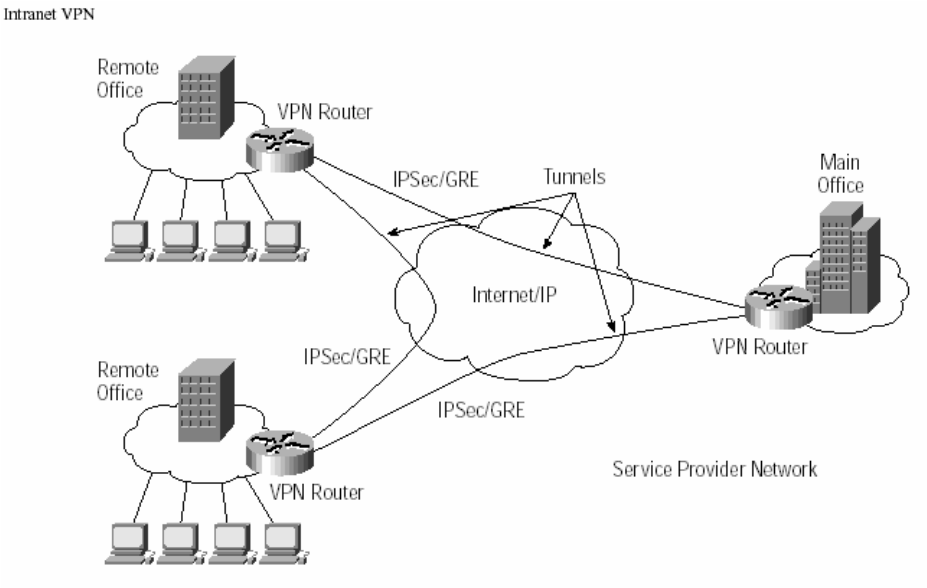
Beberapa keuntungan yang diperoleh dengan menggunakan layanan VPN ini adalah :

1. Meningkatkan security.
2. Memberikan konektivitas geografis yang luas.
3. Mereduksi biaya operational.
4. Mereduksi waktu transit dan biaya transportasi untuk user-user remote.
5. Meningkatkan produktifitas.
6. Menyederhanakan topologi jaringan.
7. Memberikan peluang-peluang networking global.

2.2.5 Jenis Implementasi VPN

1 Site to Site VPN

Merupakan jenis VPN yang digunakan untuk mengembangkan LAN yang ada di suatu perusahaan ke gedung/perusahaan lainnya dengan menggunakan perangkat yang ada sehingga para pegawai perusahaan tersebut dapat memanfaatkan layanan jaringan yang sama. (Thomas, 2005, p273).



Gambar 2.8 *Site to Site VPN*

- **Intranet VPN**

  Digunakan untuk menghubungkan kantor pusat dengan kantor cabang.

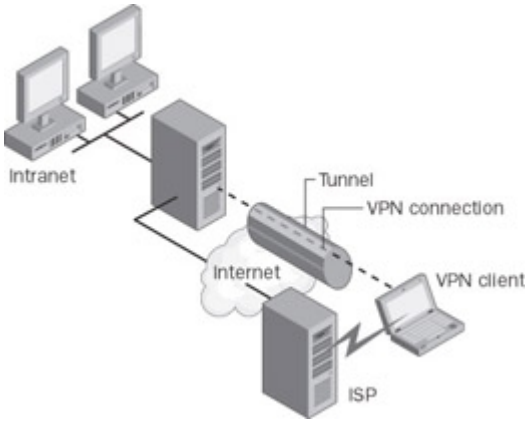
- **Extranet VPN**

  Digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lainnya**,** contohnya mitra kerja, supplier atau pelanggan.

2 Remote Access VPN

Merupakan jenis VPN yang menghubungkan antara pengguna yang *mobile* dengan *Local Area Network* (LAN). Jenis VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan

khusus perusahaannya dari berbagai lokasi yang jauh (*remote*) dari perusahaannya (Thomas, 2005, p272).



Gambar 2.9 *Remote Access VPN*

2.2.6 Tunneling

Tunneling adalah suatu proses mengenkapsulasi (membungkus) paket-paket atau frame-frame dengan header yang berisi informasi routing untuk mendapatkan koneksi point to point sehingga data dapat melewati jaringan public dan dapat mencapai akhir tujuan.

Tunneling protocol yang digunakan adalah sebagai berikut :

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

PPTP merupakan teknologi jaringan baru yang mendukung multiprotocol VPN dan merupakan protocol yang dikembangkan oleh sebuah konsorsium dari Microsoft . Dengan menggunakan PPTP, user dapat menggunakan Microsoft Windows 95 atau Windows NT Workstation atau system client lainnya yang mendukung point-to-point protocol (PPP) untuk mendial in ke Internet Service Provider (ISP) local dan kemudian membuat

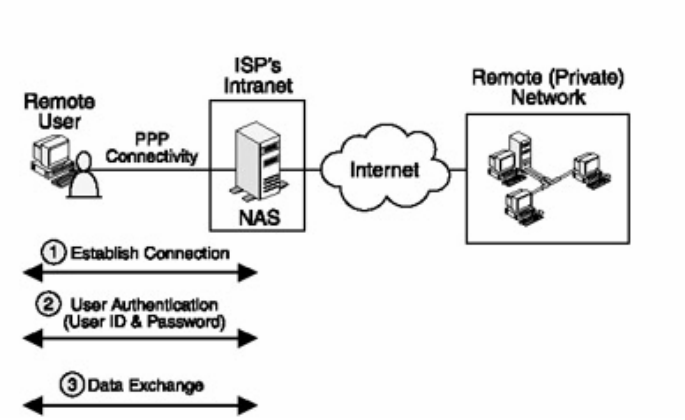
hubungan secara aman kepada jaringan perusahaan melalui internet. Setiap sesi koneksi PPTP dapat membuat koneksi yang aman dari Internet ke pemakai dan kembali menuju ke jaringan perusahaan. Hal yang terpenting dalam menggunakan PPTP adalah konfigurasi jaringan perusahaan tidak perlu berubah, termasuk pengalamatan komputer-komputer di dalam jaringan intranet.

Keunggulan-keunggulan PPTP adalah :

- Lebih aman
- Tidak perlu melakukan perubahan pengalamatan jaringan internal
- Murah

PPP mempunyai peranan penting pada transaksi PPTP karena PPTP merupakan ekstensi logika dari PPP dan tidak mengubah teknologi PPP. PPTP juga mendukung multi koneksi. Semua koneksi yang terjadi pada PPTP harus titik ke titik. Dalam transaksi PPTP, PPP mempunyai fungsi sebagai berikut :

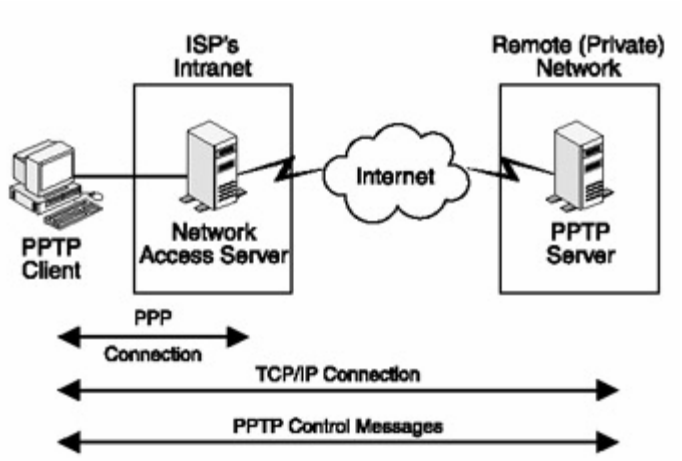
- Membangun dan memutuskan koneksi antara server dan client.
- Melakukan *authentikasi* pada client PPTP.
- Melakukan e*nkripsi* untuk mengamankan pertukaran data tersebut.



Gambar 2.10 Tiga Peran PPP pada Transaksi PPTP

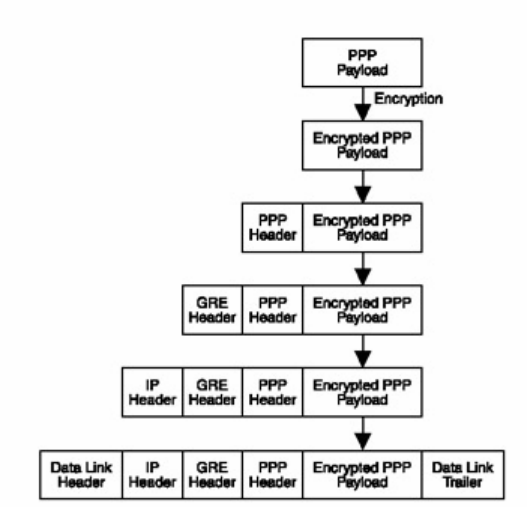
PPTP mempunyai tiga proses untuk mengamankan komunikasi berbasisi PPTP,yaitu :

- Membangun koneksi berbasis PPP antara server dan client.
- Mengendalikan koneksi PPTP, kendali koneksi PPTP dibuat berdasarkan alamat IP client dan IP server dengan menggunakan port TCP yang dialokasikan secara dinamis. Setelah kendali koneksi dibuat, pihak yang berkomunikasi saling bertukar kendali dan manajemen. Pesan – pesan ini bertanggung jawab untuk memelihara, mengatur dan memutuskan tunnel PPTP.



Gambar 2.11 Pertukaran Pesan Kendali Melalui Koneksi PPP
(sumber : Gupta, Meeta (2003))

- PPTP *tunneling* dan data transfer



Gambar 2.12 Proses Tunneling PPTP
(sumber : Gupta, Meeta (2003))

2. L2F (Layer 2 Forwarding)

L2F dibuat oleh Cisco pada tahun 1996. L2F merupakan suatu protocol transmisi yang memungkinkan server akses dial-up membingkai lalu lintas dial-up di dalam Point-to-Point Protocol

(PPP) dan mentransmisikannya pada hubungan WAN ke server L2F (router), L2F bisa menggunakan ATM dan Frame Relay dan tidak membutuhkan IP. L2F juga menyediakan otentikasi untuk tunnel endpoints.

3. L2TP (Layer 2 Tunneling Protocol)

L2TP adalah sebuah tunneling protocol yang memadukan dan mengombinasikan dua buah tunneling protocol yang bersifat proprietary, yaitu L2F (Layer 2 Forwarding) milik Cisco Systems dengan PPTP (Point-to-Point Tunneling Protocol) milik Microsoft. Namun, teknologi tunneling ini tidak memiliki mekanisme untuk menyediakan fasilitas enkripsi karena memang benar-benar murni hanya membentuk jaringan tunnel. Selain itu, apa yang lalu-lalang di dalam tunnel ini dapat ditangkap dan dimonitor dengan menggunakan protocol analizer. L2TP dikembangkan oleh Microsoft dan Cisco. Bisa mengenkapsulasi data dalam IP, ATM, Frame Relay dan X.25.

Keuntungan L2TP dibandingkan PPTP adalah :

- *multiple tunnels* antara *endpoints*, sehingga ada beberapa jalur yang memiliki perbedaan *Quality of Service* (QoS).
- mendukung kompresi.
- bisa melakukan *tunnel authentication.*
- bisa bekerja pada jaringan *non*-IP seperti ATM dan *Frame Relay*.

4. IPSec

IpSec adalah sekumpulan ekstensi dari keluarga protocol IP. *IPSec* menyediakan layanan *authenticity, integrity, access control, confidentiality,* dan *anti reply*. Layanan *IPSec* mirip dengan *SSL* namun, *IPSec* melayani lapisan network dan dilakukan secara transparan. Layanan tersebut adalah sebagai berikut :

- *Confidentiality,*

Layanan yang digunakan untuk menjaga isi informasi dari siapapun kecuali yang memiliki otoritas kerahasiaan.

- *Integrity*

  Untuk menjamin bahwa data tidak berubah dalam perjalanan menuju tujuan.

- *Authenticity*

  Untuk menandai bahwa data yang dikirimkan memang berasal dari pengirim yang benar.

- *Anti Replay*

  Untuk meyakinkan bahwa transaksi hanya dilakukan sekali, kecuali yang berwenang telah mengizinkan untuk mengulang.

Protocol yang berjalan di belakang *IPSec* adalah :

a. AH (*Authentication header*), AH menyediakan layanan *authentication, integrity* dan *replay protection,* namun tidak dengan *confidentiality*. AH juga melakukan pengamanan terhadapat header IP.

b. ESP (*Encasulapted security payload*), ESP menyediakan layanan *authentication, integrity, replay protection,* dan *confidentiality* terhadapat data .

2.2.7 VPN *Security*

1. Authentication

Proses mengidentifikasi komputer dan manusia / *user* yang memulai VPN connection.

a Extensible Authentication Protocol (EAP)

EAP adalah protocol authentication PPP baru yg melakukan metode authentication secara acak. EAP mendukung dua tipe authentication, dimana metode tersebut disarankan untuk keamanan authentication yang ketat.

b Challenge Handshake Authentication (CHAP)

Jenis protocol yang menggunakan proses encripsi dengan menggunakan password dalam membuat koneksinya, jadi lebih aman dari pada *PAP* (*CHAP* merupakan pengembangan dari *PAP*). *CHAP* dianjurkan untuk proses VPN, karena lebih aman (karena mengalami proses encrip). Proses encryption pada *CHAP* menggunakan algoritma *MD5*. Proses kerja *CHAP* menggunakan system 3-way handshake dimana *CHAP* digunakan pada saat koneksi VPN berlangsung.

c MS – CHAP

MS-CHAP adalah mekanisme authentication enkrip yang mirip dengan *CHAP*. Perbedaanya antara *MS-CHAP* dengan *CHAP* adalah bahwa client mengecek authenticationnya terlebih dahulu sebelum melewati gateway sistem. *MS-CHAP* menggunakan 1-way handshake.

d MS – CHAP v2

MS-CHAPv2 memiliki system keamanan yang lebih baik dibandingkan dengan *MS-CHAP*. Pada *authentication* akan terjadi pengecekan antara *client* dan *gateway***.** *Gateway* mempercayakan kepada *server* untuk mengeset *encryption* dari *client* dan begitu juga dengan *client*. MS-CHAPv2 merupakan protocol yang disarankan dalam *Microsoft* VPN.

Perbedaan antara *MS – CHAP* dengan *MS – CHAP v2* adalah :

- MS – CHAP
  - Server mengirim nilai challenge 8 byte.
  - Client mengirim 24 byte LANMAN dan respon 24 byte.
  - Server mengirimkan respon keadaan sukses atau gagal.
  - Client memutuskan meneruskan atau mengakhiri berdasarkan sukses atau gagal dari respon diatas.

- MS – CHAP v2
  - Server mengirim nilai challenge 16 byte yang digunakan client untuk membuat 8 byte nilai challenge.
  - Client mengirimkan 16 byte ‘Peer Challenge’ yang digunakan untuk menghasilkan 8 byte challenge yang tersebunyi dan respon 24 byte.
  - Server mengirimkan respon keadaan sukses atau gagal dan dukungan dari authenticator response menjadi 16 byte peer challenge .
  - Client memutuskan meneruskan atau mengakhiri berdasarkan sukses atau gagal dari respon diatas dengan tambahan, client akan mengecek validasi dari authenticator response dan memutuskan hubungan jika tidak mencapai nilai yang diinginkan.

e Password Authentication Protocol (PAP)

PAP merupakan jenis *authentication* PAP yang sederhana menggunakan skema clear-text *authentication*. PAP menggunakan system 2-way handshake dimana PAP digunakan untuk *troubleshooting* dan setting dari VPN, PAP tidak aman digunakan pada VPN, karena tidak melakukan enkripsi data dan tidak direkomendasikan untuk menggunakan PAP pada saat koneksi VPN sedang berlangsung

f Shiva – PAP

Adalah versi spesifik-shiva dari PAP, penambahan pada versi PAP. Protocol ini mengenkripsi password sebelum dikirim ke remote system.

2. Authorization

Authorization digunakan untuk menetukan apa yang boleh dan yang tidak boleh di akses oleh user.

3. Encryption

Encryption merupakan sebuah proses yang merubah sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti. *Encryption* ini diartikan sebagai kode atau *cipher*. *Cipher* merupakan sebuah algoritma untuk menampilkan enkripsi dan kebalikannya dekripsi, Informasi yang asli disebut *plaintext*, dan bentuk yang sudah dienkripsi disebut sebagai *chipertext*. Pesan *chipertext* berisi seluruh informasi dari pesan plaintext, tetapi tidak dalam format yang dapat dibaca manusia ataupun komputer tanpa menggunakan mekanisme yang tepat untuk melakukan dekripsi. Enkripsi dibagi menjadi 2 jenis :

1. *Symmetric Encryption*

   Algoritma simetrik ini merupakan jenis algoritma enkripsi yang paling umun digunakan. Algoritma ini disebut simetrik sebab memiliki kunci yang sama untuk

proses *enkripsi* dan *dekripsi*. Berbeda halnya dengan kunci yang digunakan pada algoritma kunci publik, kunci yang digunakan pada *simetrik key* biasanya sering diubah-ubah. Oleh karena itu biasanya kunci pada *simetrik key* disebut sebagai *session key*, artinya kunci yang dipakai hanya pada satu sesi proses enkripsi. Jika dibandingkan dengan algoritma kunci publik, algoritma simetrik key sangat cepat dan oleh karena itu lebih cocok jika digunakan untuk melakukan enkripsi data yang sangat besar. Salah satu algoritma simetrik yang dikenal adalah *RC4* dan *DES (Data Encryption Standar).* Protokol kriptografi modern pada saat ini banyak yang menggabungkan algoritma kunci publik dengan algoritma simetrik untuk memperoleh keunggulan-keunggulan pada masing-masing algoritma. Algoritma kunci publik digunakan untuk proses pertukaran *session key* yang berukuran kecil sekitar 16 bytes , sedangkan algoritma simetrik digunakan untuk melakukan enkripsi data yang sesungguhnya.

2. *Asymetric Encryption*

Asimetrik key juga di kenal dengan pulic key. *Public key cryptography* (lawan dari *symmetric key cryptography*) bekerja berdasarkan fungsi satu arah. *Public key cryptography* dilakukan dengan menggabungkan secara kriptografi dua buah kunci yang

berhubungan yang disebut sebagai pasangan kunci publik dan kunci privat. Sebagai contohnya, A dan B ingin berkomunikasi aman dengan menggunakan sistem enkripsi ini. Untuk itu, keduanya harus memiliki *public key* dan *private key* terlebih dahulu. A harus memiliki public dan *private key*, begitu juga dengan B. Ketika proses komunikasi dimulai, mereka akan menggunakan kunci-kunci yang berbeda untuk mengenkrip dan mendekrip data. Kunci boleh berbeda, namun data dapat dihantarkan dengan mulus berkat algoritma yang sama. Kedua kunci tersebut dibuat pada waktu yang bersamaan dan berhubungan secara matematis. Secara matematis, kunci privat dibutuhkan untuk melakukan operasi invers terhadap kunci public dan juga sebaliknya. Jika kunci publik didistribusikan secara luas, dan kunci privat disimpan di tempat yang tersembunyi maka akan diperoleh fungsi dari banyak ke satu, yaitu pada saat orang yang memegang kunci privat melakukan operasi enkripsi maka semua orang yang memiliki kunci publik dapat melakukan invers terhadap data hasil enkripsi tersebut.

Metode yang digunakan dalam Encryption adalah :

1 MPPE (Microsoft Point To Point Encryption)

MPPE berbasis pada medote enkripsi *shared-secret* dan menyediakan keamanan data untuk koneksi PPTP yang

berada diantara VPN *client* dan VPN *server*. 40-bit session digunakan untuk mengenkripsi *user ID* dan *password* yang didapat dari *hashed algorithm* yang disimpan pada klien dan *server*. *Hashed algorithm* yang digunakan untuk menghasilkan *key* itu adalah RC4. *Key* ini digunakan untuk mengenkripsikan semua data yang dikirim melalui *tunnel*. Sekarang ini versi 128-bit *key* telah tersedia dengan tujuan untuk meningkatkan tingkat keamanan. Jika menggunakan enkripsi data yang berbasis MPPE, maka harus memilih metode authentikasi MS-CHAP, MS-CHAP v2, atau EAP-TLS.

RC4 merupakan salah satu jenis *stream cipher*, yaitu memproses unit atau input data, pesan atau informasi pada satu saat. Unit atau data pada umumnya sebuah *byte* atau bahkan kadang kadang bit (*byte* dalam hal RC4). Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang yang variabel. Algoritma ini tidak harus menunggu sejumlah input data, pesan atau informasi tertentu sebelum diproses, atau menambahkan byte tambahan untuk mengenkrip. Contoh *stream cipher* adalah RC4, Seal, A5, Oryx, dan lain-lain.

RC4 merupakan salah satu jenis *stream cipher* yang didesain oleh Ron Rivest di laboratorium RSA (RSA *Data Security inc*) pada tahun 1987. RC4 sendiri merupakan kepanjangan dari Ron Code atau Rivest's *Cipher*. RC4

menggunakan panjang kunci dari 1 sampai 256 *bit* yang digunakan untuk menginisialisasikan tabel sepanjang 256 *bit*. Tabel ini digunakan untuk generasi yang berikut dari *peudo random* yang menggunakan XOR dengan *plain-text* untuk menghasilkan *cipher-text.*

Algoritma RC4 cukup mudah untuk dijelaskan. RC4 mempunyai sebuah *S-Box*, $S_0,S_1,...,S_{255}$, yang berisi permutasi dari bilangan 0 sampai 255, dan permutasi merupakan fungsi dari kunci dengan panjang yang variabel. Terdapat dua indeks yaitu i dan j, yang diinisialisasi dengan bilangan nol. Untuk menghasilkan random byte langkahnya adalah sebagai berikut:

$i = (i + 1) \bmod 256$

$j = (j + S_i) \bmod 256$

swap S_i dan S_j

$t = (S_i + S_j) \bmod 256$

$K = S_t$

Byte K di XOR dengan *plaintexs* untuk menghasilkan *cipherteks* atau di XOR dengan cipherteks untuk menghasilkan *plainteks*. Enkripsi sangat cepat kurang lebih 10 kali lebih cepat dari DES.

2 DES dan 3DES

Algoritma *DES* didesain oleh IBM dan pertama kali di publish pada tahun 1975. DES dipilih oleh FIPS (Federal Information Processing Standard) untuk menjadi standard di Amerika pada tahun 1976 dan mulai banyak digunakan di seluruh dunia. *DES* merupakan salah satu algoritma enkripsi golongan *block chiper*. *Block chiper* adalah suatu *chiper* yang bertipe *symetric key* dan bekerja pada suatu kelompok bit yang panjangnya sudah pasti. Ini sangat berbeda dengan golongan *stream chiper* dimana akan mengenkripsi setiap bit pada suatu teks. *DES* memiliki ukuran block chiper sebesar 64 bit dan panjang key-nya adalah 56 bit. Maksudnya, algoritma ini akan menjalankan serangkaian proses pengacakan 64-bit data yang masuk untuk kemudian dikeluarkan menjadi 64-bit data acak. Proses tersebut menggunakan 64-bit kunci di mana 56-bit-nya dipilih secara acak, 8 bit nya berasal dari parity bit dari data Anda. Kedelapan bit tersebut diselipkan di antara ke 56-bit tadi. Kunci yang dihasilkan kemudian dikirimkan ke si penerima data. Panjang key 56 bit ini dipandang sangat pendek dan mudah sekali untuk dipecahkan. Pada tahun 1998 *DES* bisa dipecahkan melalui sebuah mesin yang diciptakan khusus untuk itu. Pihak yang mendemonstrasikan pemecahan *DES* ini adalah Eletronic Frontier Foundation. Melihat kelemahan

tersebut maka *DES* kemudian dikembangkan dan lahirlah *3DES (triple DES*) yang dikembangkan oleh Walter Tuchman. *3DES* ini menggunakan triple-encrypts blocks yang biasanya menggunakan dua key (kunci). Ini menghasilkan panjang key 112 bit. Jadi kunci yang dihasilkan dan dibutuhkan untuk membuka enkripsi adalah sebanyak tiga buah.

3 Blowfish

Blowfish merupakan metoda enkripsi yang mirip dengan *DES (DES-like cipher)* dan diciptakan oleh Bruce Schneier yang ditujukan untuk mikroposesor besar (32 bit ke atas dengan cache data yang besar). *Blowfish* dikembangkan untuk memenuhi kriteria disain sebagai berikut:

- Cepat, pada implementasi yang optimal *Blowfish* dapat mencapai kecepatan 26 clock cycle per byte.
- Kompak, *Blowfish* dapat berjalan pada memori kurang dari 5 KB.
- Sederhana, *Blowfish* hanya menggunakan operasi yang simpel: penambahan (addition), XOR, dan penelusuran tabel (table lookup) pada operand 32 bit. Desainnya mudah untuk dianalisa yang membuatnya resisten terhadap kesalahan implementasi.

- Keamanan yang variabel, panjang kunci *Blowfish* dapat bervariasi dan dapat mencapai 448 bit (56 byte).

Blowfish dioptimasikan untuk aplikasi dimana kunci tidak sering berubah, seperti jalur komunikasi atau enkripsi file otomatis. *Blowfish* jauh lebih cepat dari DES bila diimplementasikan pada 32 bit mikroprosesor dengan cache data yang besar, seperti Pentium dan Power PC, Blowfish tidak cocok untuk aplikasi seperti packet switching, dengan perubahan kunci yang sering, atau sebagai fungsi hash satu arah.

4 SSL (Secure Socket Layer)

Secure Sockets Layer atau yang disingkat SSL adalah sebuah protokol keamanan data yang digunakan untuk menjaga pengiriman data antara web server dan pengguna situs web tersebut. 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 dikirimkan, dipecahkan kedalam blok-blok yang teratur, kemudian dikompres jika perlu, menerapkan MAC, dienkripsi, dan hasilnya dikirimkan. Di tempat tujuan, data didekripsi, verifikasi, dekompres, dan disusun kembali. Hasilnya

dikirimkan ke klien di atasnya. SSL umumnya sudah terinstall didalam mayoritas browser web yang ada (IE, Netscape, Firefox, dll), sehingga pengguna situs web dapat mengidentifikasi tingkat keamanan situs web tersebut yang menggunakan protokol keamanan SSL ini. Browser web secara otomatis akan mencek apakah sertifikat SSL dan identitas situs web valid dan situs tersebut terdaftar pada otoritas sertifikasi (CA) SSL (cth. Verisign). Dengan demikian, SSL ini menjadi sangat penting terutama untuk situs web yang menjalankan transaksi online. Koneksi SSL akan memproteksi informasi vital dengan meng-enkripsi informasi yang dikirim dan diterima antara pc pengguna situs dan web server, sehingga informasi yang berjalan tidak mungkin dapat diambil ditengah jalan dan dibaca isinya. Hal ini berarti pengguna tidak perlu ragu untuk mengirim informasi vital seperti nomor kartu kredit kepada situs web yang telah memasang SSL tersertifikat ini.

Cara kerja SSL

Seorang pelanggan masuk kedalam situs anda dan melakukan akses ke URL yang terproteksi (ditandai dengan awalan https atau dengan munculnya pesan dari browser). Server anda akan memberitahukan secara otomatis kepada pelanggan tersebut mengenai sertifikat digital situs anda yang menyatakan bahwa situs anda telah tervalidasi sebagai

situs yang menggunakan SSL. Browser pelanggan akan mengacak "session key" dengan "public key" situs anda sehingga hanya situs anda yang akan dapat membaca semua transaksi yang terjadi antara browser pelanggan dengan situs anda. Hal itu semua terjadi dalam hitungan detik dan tidak memerlukan aktifitas apapun dari pelanggan.

SSL hanya mengenkripsikan data yang dikirim lewat http. Cara kerja SSL dapat digambarkan sebagai berikut :

- Pada saat koneksi mulai berjalan, klien dan server membuat dan mempertukarkan kunci rahasia, yang dipergunakan untuk mengenkripsi data yang akan dikomunikasikan. Meskipun sesi antara klien 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.