BAB 2

LANDASAN TEORI

Komputer yang saling berhubungan membentuk suatu jaringan akan menjadi kaya akan sumber daya yang dibutuhkan. Jaringan komputer sendiri dapat dikelompokkan menjadi beberapa jenis, yaitu berdasarkan tipe transmisi, jarak, peranannya dalam memproses data serta media transimisi datanya. Untuk menggambarkan infrastruktur komunikasi ini bisa dibentuk dengan beberapa topologi. Beberapa topologi jaringan yang ada yaitu topologi *star*, *bus*, *ring*, *mesh* dan *tree*. Masing-masing topologi tersebut memiliki keunggulan serta kelemahannya sendiri sehingga dalam mengimplementasikannya disesuaikan dengan kebutuhan dari jaringan komputer yang akan dibangun. Oleh karena itu, deskripsi tentang topologi ini akan diberikan di awal bab landasan teori ini.

Dalam komunikasinya, jaringan mempunyai aturan sendiri atau sering disebut dengan protokol jaringan. Pada bab ini akan dijelaskan dua buah model referensi, yaitu model referensi OSI yang menjadi standar internasional dan model referensi TCP/IP. Untuk dapat menghubungkan komputer-komputer tersebut membentuk suatu jaringan, masing-masing komputer harus memiliki IP unik yang berguna untuk mengidentifikasikan dirinya sendiri. IP sendiri dibagi dalam beberapa kelas (kelas A – kelas E) dengan skala yang bervariasi dari masing-masing kelasnya. Selain itu, IP juga dapat dibagi menjadi IP publik dan privat serta dapat dikelompokkan berdasarkan jenis-jenisnya.

Teknologi jaringan komputer dalam perkembangannya memiliki berbagai teknik pengamanan data, salah satunya adalah VPN. Teknik ini akan membuat suatu jaringan khusus yang menumpang pada jaringan publik sehingga tingkat keamanan aliran data di dalamnya lebih terjamin karena melalui suatu ‘pipa’ aliran data yang bernama *tunnel* di mana data-data yang melewati *tunnel* tersebut akan dienkripsi. Terdapat beberapa teknik keamanan yang dapat diterapkan di VPN, antara lain enkripsi, autentikasi, autorisasi serta *firewall*.

2.1 Konsep Dasar Jaringan

Jaringan komputer adalah sekelompok komputer yang saling dihubungkan dengan menggunakan suatu protokol komunikasi melalui media komunikasi sehingga antara satu komputer dengan komputer yang lain dapat saling berbagi informasi, data dan sumber daya yang dapat digunakan bersama (Kristanto, Andri, 2003, p2). Tujuan dibangunnya suatu jaringan komputer adalah membawa informasi secara tepat dan tanpa adanya kesalahan dari sisi pengirim (*transmitter*) menuju sisi penerima (*receiver*) melalui media komunikasi. Adapun sasaran terbentuknya jaringan komputer adalah:

- *Sharing resources*, bertujuan agar seluruh *hardware* maupun *software* dapat dimanfaatkan bersama oleh setiap orang yang ada pada jaringan tersebut tanpa terpengaruh oleh lokasi sehingga dapat menekan biaya

pembelian *hardware* maupun *software* karena adanya peningkatan sumber daya tersebut.

- Komunikasi, baik untuk *teleconference*, *instant messaging* maupun untuk mengirim pesan (*e-mail*).
- Mendapatkan akses informasi dengan cepat, contohnya melalui internet.
- Melakukan pembagian (*sharing*) data.

2.2 Klasifikasi Jaringan Komputer

2.2.1 Berdasarkan Tipe Transmisi

Secara garis besar, terdapat dua jenis teknologi transmisi dalam sistem jaringan yaitu :

- **Jaringan *broadcast*** : Komunikasi terjadi dalam sebuah saluran komunikasi yang digunakan secara bersama-sama, di mana data berupa paket yang dikirimkan dari sebuah komputer akan diterima oleh masing-masing komputer yang ada dalam jaringan tersebut. Paket data hanya akan diproses oleh komputer tujuan dan akan diabaikan oleh komputer yang bukan merupakan tujuan dari paket tersebut.
- **Jaringan *point-to-point*** : Komunikasi data terjadi melalui beberapa koneksi antar komputer, sehingga untuk mencapai tujuannya sebuah paket mungkin harus melalui beberapa komputer

terlebih dahulu. Oleh karena itu, dalam tipe jaringan ini, pemilihan rute yang baik memegang peranan penting.

2.2.2 Berdasarkan Jarak

1. Local Area Network (LAN)

Local Area Network (LAN) merupakan suatu jaringan komunikasi lokal yang menghubungkan berbagai jenis perangkat untuk pemakaian bersama (*sharing resources*) dan menyediakan fasilitas pertukaran data dalam lingkup area geografis terbatas (dalam satu gedung dengan jarak jangkauan hingga beberapa kilometer). *Ethernet, Token Ring,* dan FDDI merupakan beberapa teknologi LAN yang umum digunakan.

2. Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN) pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya memakai teknologi yang sama dengan LAN. Area cakupan dari MAN lebih besar daripada LAN, tetapi lebih kecil dari WAN.

3. Wide Area Network (WAN)

Wide Area Network (WAN) adalah suatu jaringan komunikasi data yang mencakup area geografis yang sangat luas (radiusnya dapat mencakup suatu negara dan benua). WAN digunakan untuk menghubungkan beberapa LAN, sehingga pengguna

jaringan dari suatu lokasi dapat berkomunikasi, bertukar data maupun *sharing resources* dengan pengguna di lokasi lain tanpa mengenal jarak. Contoh yang paling tepat untuk menggambarkan WAN adalah internet.

2.2.3 Berdasarkan Peranannya Dalam Memproses Data

Jaringan komputer terbagi menjadi 2 jenis berdasarkan peranan dan hubungan tiap komputer dalam memproses data, yaitu :

- Jaringan ***Client-Server***, terdiri dari beberapa komputer *client* dan komputer server. Komputer *client* sebagai peminta layanan untuk dapat mengakses data pada komputer server sedangkan komputer server menyediakan informasi yang diperlukan oleh komputer *client*.
- Jaringan ***Peer-to-peer***, pada jaringan ini tidak terdapat komputer *client* maupun server karena semua komputer dapat melakukan pengiriman maupun penerimaan informasi dan memiliki media penyimpanan masing-masing sehingga semua komputer berfungsi sebagai *client* sekaligus server.

2.2.4 Berdasarkan Media Transmisi Data

Jaringan komputer terbagi menjadi 2 jenis berdasarkan media transmisi datanya, yaitu :

- Jaringan **Berkabel** (***Wired Network***)

  Pada jaringan ini, untuk menghubungkan satu komputer dengan komputer lain diperlukan penghubung berupa kabel jaringan. Kabel jaringan berfungsi dalam mengirimkan informasi dalam bentuk sinyal listrik antar komputer jaringan.

- Jaringan **Nirkabel** (***Wireless Network***)

  Merupakan jaringan dengan medium berupa gelombang elektromagnetik. Pada jaringan ini tidak diperlukan kabel untuk menghubungkan antar komputer karena menggunakan gelombang elektromagnetik yang akan mengirimkan sinyal informasi antar komputer jaringan.

2.3 Topologi Jaringan

Topologi jaringan adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk suatu jaringan. Topologi dasar yang bisa digunakan dalam jaringan komputer adalah sebagai berikut:

1. **Topologi *Bus***

   Seluruh komputer dalam jaringan terhubung dalam sebuah *bus* atau jalur komunikasi data utama / *backbone* (berupa kabel). Komputer dalam jaringan berkomunikasi dengan cara mengirim dan mengambil data melalui *bus*.

   Kelebihan Topologi *Bus* :

   - Pengembangan jaringan atau penambahan workstation baru dapat dilakukan dengan mudah tanpa mengganggu workstation lain.
   - Biaya murah karena hanya menggunakan sedikit kabel.
   - Mudah dalam penginstalasiannya.

   Kekurangan Topologi *Bus* :

   - Bila terdapat gangguan di sepanjang kabel pusat maka keseluruhan jaringan akan mengalami gangguan.
   - Hanya satu komputer yang dapat mengirimkan data dalam waktu yang bersamaan.

2. **Topologi *Star***

   Dalam topologi ini, masing-masing komputer dalam jaringan dihubungkan ke sebuah konsentrator dengan menggunakan jalur yang berbeda-beda, sehingga jika salah satu komputer mengalami

gangguan, jaringan tidak akan terpengaruh. Komunikasi di dalam jaringan diatur oleh konsentrator, berupa *hub*.

Kelebihan Topologi *Star* :

- Jika terjadi kerusakan pada satu link, maka hanya berakibat pada komputer yang berada pada jalur link itu saja, sedangkan komputer lainnya tetap aktif.
- Mudah dalam penambahan komputer pada jaringan star karena kita tinggal menambahkan kabel baru dari komputer tersebut ke jaringan pusat.
- Pusat dari jaringan *star* merupakan tempat yang baik untuk menentukan diagnosa kesalahan yang terjadi dalam jaringan.

Kekurangan Topologi *Star* :

- Sangat bergantung kepada hub sebagai pusat pengendali sehingga kondisi hub harus selalu dalam keadaan baik.
- Membutuhkan lebih banyak kabel karena semua kabel jaringan harus ditarik ke satu *central point*, jadi lebih banyak membutuhkan lebih banyak kabel daripada topologi jaringan yang lain.

3. Topologi *Ring*

Sesuai dengan namanya, seluruh komputer dalam jaringan terhubung pada sebuah jalur data yang menghubungkan komputer satu dengan lainnya secara berurutan sehingga menyerupai sebuah cincin. Topologi ini mirip dengan hubungan seri pada rangkaian listrik, dengan kedua ujung dihubungkan kembali, sehingga jika salah satu komputer mengalami gangguan, maka hal itu akan mempengaruhi keseluruhan jaringan. Dalam sistem jaringan ini, data dikirim secara berkeliling sepanjang jaringan (*ring*). Setiap komputer yang ingin mengirimkan data ke komputer lain harus melalui *ring* ini.

Kelebihan Topologi *Ring* :

- Identifikasi kerusakan cukup mudah karena sinyal data selalu bergerak terus dari perangkat pengirim sampai akhirnya berhenti di perangkat tujuan
- Dapat menghindari tabrakan file data yang dikirim karena data mengalir dalam satu arah sehingga untuk data yang dikirimkan selanjutnya akan dikerjakan setelah pengiriman pertama selesai.
- Mudah dalam penginstalasiannya.

Kekurangan Topologi *Ring* :

- Kerusakan pada salah satu komputer dapat memberikan pengaruh terhadap jaringan secara keseluruhan dan tentu saja akan mempersulit proses perbaikannnya.
- Penambahan dan pemindahan komputer akan mengganggu jaringan yang sedang berjalan.

4. Topologi *Mesh*

Topologi ini sering disebut "*pure peer-to-peer*", sebab merupakan implementasi suatu jaringan komputer yang menghubungkan seluruh komputer secara langsung. Saat ini sangat jarang digunakan sebab rumit dan tidak praktis.

Kelebihan Topologi *Mesh* :

- Memudahkan proses identifikasi permasalahan pada saat terjadi kerusakan koneksi antar komputer.
- Hubungan *dedicated links* menjamin data langsung dikirimkan ke komputer tujuan tanpa harus melalui komputer lainnya sehingga dapat lebih cepat karena satu link digunakan khusus untuk berkomunikasi dengan komputer yang dituju saja

- Jika terjadi kerusakan pada satu link, maka hanya berakibat pada komputer yang berada pada jalur link itu saja, sedangkan komputer lainnya tetap aktif.
- *Privacy* dan *security* pada topologi mesh lebih terjamin, karena komunikasi yang terjadi antara dua komputer tidak akan dapat diakses oleh komputer lainnya.

Kekurangan Topologi *Mesh* :

- Sulit dalam melakukan instalasi dan melakukan konfigurasi ulang saat jumlah komputer dan peralatan-peralatan yang terhubung semakin meningkat jumlahnya.
- Biaya yang besar untuk pembuatan jaringan ini.
- Banyaknya kabel yang digunakan juga mengidentifikasikan diperlukannya ruang yang lebih besar untuk melatakan kabel dan komputer.

5. Topologi *Tree*

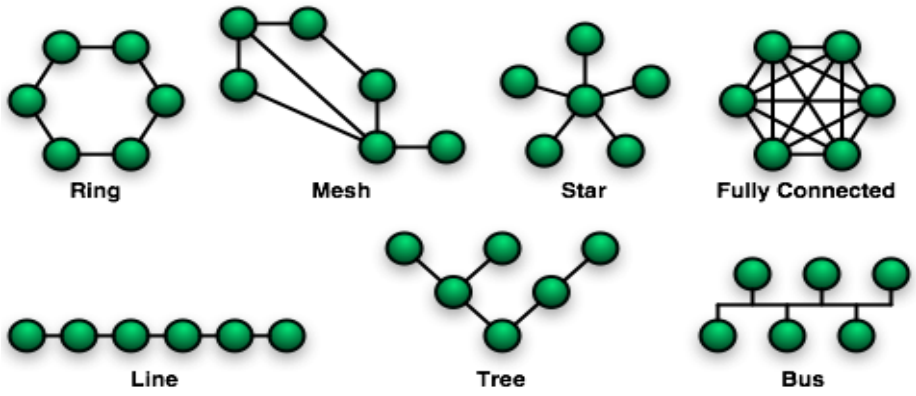
Topologi ini merupakan perpaduan antara topologi *bus* dan *star*, di mana membentuk suatu hirarkial yang menempatkan sebuah *node* sebagai pusat (*root*) dengan *node-node* lain sesuai dengan level kepentingannya.

Kelebihan Topologi *Tree* :

- Kontrol jaringan lebih mudah karena bersifat terpusat dan terbagi dalam tingkatan jenjang.
- Mudah dikembangkan.

Kekurangan Topologi *Tree* :

- Jika salah satu node atau komputer rusak, maka node yang berada di jenjang bagian bawahnya akan rusak.
- Dapat terjadi tabrakan file data (collision).



Gambar 2.1 Berbagai Macam Jenis Topologi Jaringan

(sumber: http://en.wikipedia.org/wiki/File:NetworkTopologies.png)

2.4 Protokol Jaringan

Protokol jaringan adalah aturan-aturan yang digunakan perangkat-perangkat jaringan untuk berkomunikasi satu sama lain. Kunci pokok suatu protokol adalah :

- ***Syntax***, merupakan format data dan cara pengkodean yang digunakan untuk mengkodekan sinyal.
- ***Semantic***, merupakan kontrol informasi dan mengendalikan kesalahan data yang terjadi.
- ***Timing***, merupakan penguasaan kecepatan transmisi data dan urutannya.

Model yang umum dijadikan referensi untuk mempelajari protokol jaringan adalah model referensi lapisan *Open System Interconnection* (*OSI Layers*). Sedangkan *Internet Protocol Suite* (TCP/IP) merupakan protokol jaringan yang saat ini sangat umum digunakan untuk *internetworking*.

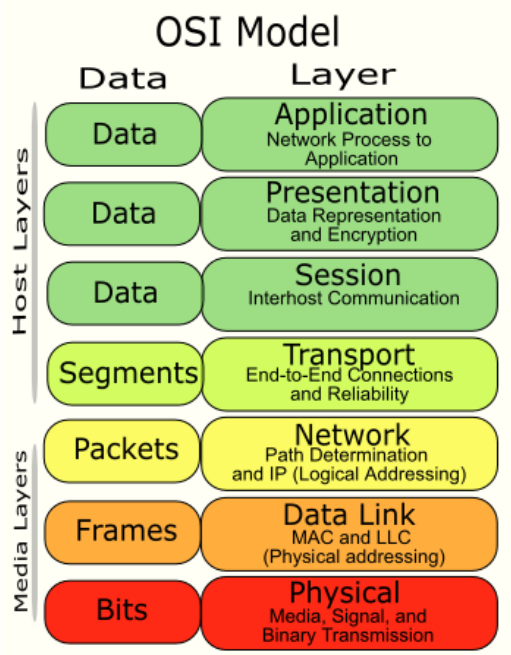
2.4.1 Model Referensi OSI

Model *Open System Interconnection* (OSI) dikembangkan oleh *International Standard Organization* (ISO) di Eropa pada tahun 1977 sebagai model untuk merancang komunikasi komputer dan sebagai kerangka dasar untuk mengembangkan protokol lainnya. Standar ini dibuat untuk mempermudah pengertian, penggunaan, perancangan, pengolahan data dan keseragaman vendor sehingga produk yang berbeda vendor dapat saling berkomunikasi. OSI terdiri dari tujuh lapisan dan masing-masing lapisan memiliki tugas dan fungsinya

masing-masing sehingga perubahan yang terjadi pada satu lapisan, tidak mempengaruhi lapisan-lapisan lainnya.

Standar OSI telah diterima di industri komunikasi dan dipakai untuk mengatur karakteristik, elektrik dan prosedur dari perlengkapan komunikasi. Tujuan dibentuknya model referensi OSI adalah:

- menjadi patokan bagi perkembangan prosedur komunikasi pada masa yang akan datang.
- mengatasi hubungan yang timbul antar pemakai dengan cara memberikan fasilitas yang sesuai.
- membagi permasalahan prosedur penyambungan menjadi sub struktur.
- memenuhi kebutuhan pemakai kini maupun masa yang akan datang.



Gambar 2.2 Model Referensi OSI

(sumber: http://id.wikipedia.org/wiki/Berkas:Osi-model-jb.png)

1. *Layer 1 – Physical Layer*

Physical layer merupakan lapisan terbawah pada model OSI. Lapisan ini berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya *Ethernet* atau *Token Ring*), topologi jaringan dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana *Network Interface Card* (NIC) dapat berinteraksi dengan media kabel atau radio. Peralatan

yang merupakan *physical layer* antara lain adalah *hub* dan *repeater*.

2. Layer 2 – Data Link Layer

Data link layer berfungsi untuk menentukan bagaimana *bit-bit* data dikelompokkan menjadi format yang disebut sebagai *frame*. Selain itu, pada level ini terjadi koreksi kesalahan (*error notification*), pengaturan pengiriman data (*flow control*), pengalamatan perangkat keras (seperti halnya *Media Access Control Address (MAC Address)*), dan menetukan bagaimana perangkat-perangkat jaringan seperti *hub, bridge, repeater,* dan *switch layer 2* beroperasi. Spesifikasi *IEEE 802*, membagi level ini menjadi dua level anak, yaitu lapisan *Logical Link Control (LLC)* dan lapisan *Media Access Control (MAC)*. *Switch* dan *bridge* merupakan peralatan yang bekerja pada layer ini.

3. Layer 3 – Network Layer

Network layer menyediakan koneksi dan pemilihan jalur antar dua sistem. *Layer* ini berfungsi mendefinisikan alamat-alamat IP (*addressing*), membuat *header* untuk paket-paket, dan kemudian melakukan *routing* melalui *internetworking* dengan menggunakan *router* dan *switch layer-3*.

4. Layer 4 – Transport Layer

Transport layer bertanggung jawab untuk menjaga komunikasi jaringan antar *node*. *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 dibuat sebuah tanda bahwa paket diterima dengan sukses *(acknowledgement)* dan mentransmisikan ulang terhadap paket-paket data yang hilang di tengah jalan. Dalam penyediaan layanan yang *reliable*, lapisan ini menyediakan *error detection* dan *recovery* serta *flow control*.

5. Layer 5 – Session Layer

Session layer bertanggung jawab untuk mengatur, membangun dan memutuskan sesi antara aplikasi serta mengatur pertukaran data antar entitas *presentation layer*. Pada lapisan ini juga disediakan *dialog control* antar perangkat atau *nodes* serta mengoordinasi komunikasi antar sistem dan mengatur komunikasi dengan cara menawarkan tiga macam mode yang berbeda yaitu *simplex, half duplex*, dan *full duplex*.

6. Layer 6 – Presentation Layer

Presentation layer merepresentasikan data ke *application layer* dan bertanggung jawab untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan agar dapat dimengerti oleh aplikasi di sistem lain. Jika diperlukan, lapisan ini juga dapat menerjemahkan beberapa data format yang berbeda, kompresi dan enkripsi. Teknik transfer data dilakukan dengan cara mengadaptasi data ke format standar sebelum dikirimkan ke tujuan. Komputer tujuan dikonfigurasi untuk menerima format data yang standar untuk kemudian diubah kembali ke bentuk aslinya agar dapat dibaca oleh aplikasi yang bersangkutan.

7. Layer 7 – Application Layer

Application layer merupakan lapisan teratas pada model OSI dan merupakan lapisan yang paling dekat dengan pengguna (*user*) di mana *user* dapat berinteraksi secara langsung dengan komputer. Lapisan ini berfungsi sebagai antarmuka antara aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan dan kemudian membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini antara lain adalah HTTP, FTP, SMTP, dan NFS.

Lapisan (Layer)	Nama	Fungsi	Pelayanan/Protokol
7	Application	Menyediakan pelayanan yang lansung mendukung aplikasi pemakai	File transfer, e-mail, dan akses ke database
6	Presentation	Menerjemahkan, kompresi, dan enkripsi data	ASCII, EBCDIC, MIDI, MPEG, TIFF, JPEG, PICT, Quick Time
5	Session	Mengkoordinasi komunikasi antara sistem	NETBEUI, RPC, SQL,XWindows
4	Transport	Memungkinkan paket data dikirim tanpa kesalahan dan tanpa duplikat	TCP, UDP, SPX
3	Network	Menentukan jalur pengiriman dan meneruskan data ke alamat peralatan lain yang berjauhan. Pada lapisan ini data dikirim dalam bentuk paket	IP, IPX, ARP, RARP, ICMP, RIP, OSFT, BGP
2	Data-Link	Mengatur binary data (0 dan 1) menjadi logical group. Pada lapisan ini data dikirim dalam bentuk frame	Ethernet, Token-Ring, FDDI, ATM, SLIP, PPP, MTU
1	Physical	Transmisi binary data lewat jaringan	10BaseT, 100BaseTX, HSSI, V.35, X.21

Tabel 2.1 Lapisan Referensi Model OSI beserta Fungsi dan Protokolnya (sumber: http://www.scribd.com/doc/7570048/Model-Model-Referensi)

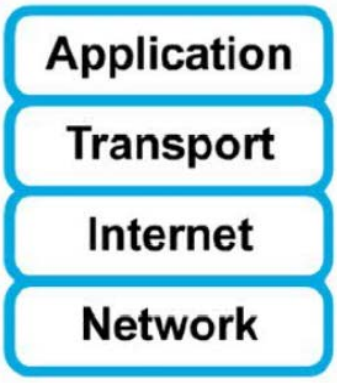
2.4.2 Model Referensi TCP/IP

TCP/IP (*Transmission Control Protocol/Internet Protocol*) merupakan standar komunikasi data yang digunakan oleh komunitas internet dalam proses pertukaran data dari satu komputer ke komputer lain di dalam jaringan internet. TCP/IP merupakan hasil penelitian yang dibuat dan dikembangkan oleh DARPA (*Defence Advanced Research Project Agency*) pada akhir dekade 1970-an hingga awal 1980-an

sebagai sebuah protokol standar untuk menghubungkan komputer-komputer dan jaringan untuk membentuk sebuah jaringan yang luas (WAN). TCP/IP merupakan sebuah standar jaringan terbuka yang bersifat independen terhadap mekanisme transport jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja.

Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut sebagai alamat IP (*IP Address*) yang mengizinkan hingga ratusan juta komputer untuk dapat saling berhubungan satu sama lainnya di Internet. Protokol ini juga bersifat ***routable*** yang berarti protokol ini cocok untuk menghubungkan sistem-sistem yang berbeda (seperti *Microsoft Windows* dan keluarga *UNIX*) untuk membentuk jaringan yang heterogen.

TCP/IP mengimplementasikan arsitektur berlapis yang terdiri atas empat lapis. Empat lapis ini dapat dipetakan (meski tidak secara langsung) terhadap model referensi OSI. Empat lapis ini antara lain yaitu *application layer, transport layer, internet layer, dan network access layer*.



Gambar 2.3 Model Referensi TCP/IP

(sumber: http://www.scribd.com/doc/7570048/Model-Model-Referensi)

1. ***Layer 1 – Network Access Layer***

   Lapisan ini bertanggung jawab dalam meletakan *frame-frame* data di atas media jaringan. Protokol yang berjalan dalam lapisan ini adalah beberapa arsitektur jaringan lokal (seperti *Ethernet* atau *Token Ring*), serta layanan teknologi WAN (seperti *Plain Old Telephone Service* (POTS), *Integrated Services Digital Network* (ISDN), *Frame Relay*, dan *Asynchronous Transfer Mode* (ATM)).

2. ***Layer 2 – Internet Layer***

   Lapisan ini bertanggung jawab dalam melakukan *routing* dan pembuatan paket IP (dengan menggunakan teknik enkapsulasi). Protokol-protokol yang berjalan pada lapisan ini adalah *Internet Protocol* (IP), *Address Resolution Protocol*

(ARP), *Internet Control Message Protocol* (ICMP), serta *Internet Group Management Protocol* (IGMP).

3. Layer 3 – Transport Layer

Lapisan ini bertanggung jawab dalam rangka membuat komunikasi antar dua *host*, dengan cara membuat sebuah sesi *connection-oriented* atau menyebarkan sebuah *connectionless broadcast*. Protokol-protokol yang berjalan pada lapisan ini adalah protokol *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP).

	TCP	**UDP**
1.	*Connection – oriented*, karena membuka sesi terlebih dahulu sebelum memulai komunikasi	*Connectionless – oriented*, karena tidak membuka sesi terlebih dahulu sebelum memulai komunikasi
2.	*Reliable*, karena melacak data yang dikirimkan, meng-*acknowledge* data yang diterima, dan mengirimkan kembali data yang tidak sampai	*Unreliable/Best Effort*, karena tidak melacak data yang dikirimkan dan tidak mengirimkan kembali data yang tidak sampai
3.	*Reassembly*, data diurutkan kembali di tujuan	Data langsung dikirimkan ke *upper layer* begitu data sampai
4.	*Flow control*, mengatur pengiriman sesuai dengan sumber daya yang ada agar penerima tidak kewalahan menerima data yang masuk	Tidak ada *flow control*
5.	*Overhead* 20 *bytes*	*Overhead* kecil, 8 *bytes*
ex	*Web access* (HTTP), *Email* (SMTP, POP3), *Download* (FTP)	DNS, DHCP, TFTP, *Video Streaming*, VoIP, *Online Gaming*

Tabel 2.2 Perbedaan TCP dan UDP

4. Layer 4 – Application Layer

Lapisan ini bertanggung jawab dalam rangka menyediakan akses kepada aplikasi terhadap jaringan TCP/IP. Protokol-protokol yang berjalan pada lapisan ini adalah protokol *Dynamic Host Configuration Protocol* (DHCP), *Domain Name System* (DNS), *Hypertext Transfer Protocol* (HTTP), *File Transfer Protocol* (FTP), *Telnet, Simple Mail Transfer Protocol* (SMTP), *Simple Network Management Protocol* (SNMP), dan lain-lain.

Nama Layer	Protokol
Application	Telnet, FTP, SMTP, Kerberos, DNS, TFTP, SNMP, NFS, XWindows
Transport	UDP,TCP
Internet	IP,ARP,RARP, ICMP, BootP
Network	Ethernet, Token Ring, FDDI

Tabel 2.3 Lapisan Referensi Model TCP/IP Beserta Protokolnya

(sumber: http://www.scribd.com/doc/7570048/Model-Model-Referensi)

MODEL OSI			TCP/IP	PROTOKOL TCP/IP	
NO.	LAPISAN			NAMA PROTOKOL	KEGUNAAN
7	Aplikasi		Aplikasi	DHCP (Dynamic Host Configuration Protocol)	Protokol untuk distribusi IP pada jaringan dengan jumlah IP yang terbatas
				DNS (Domain Name Server)	Data base nama domain mesin dan nomer IP
				FTP (File Transfer Protocol)	Protokol untuk transfer file
				HTTP (HyperText Transfer Protocol)	Protokol untuk transfer file HTML dan Web
				MIME (Multipurpose Internet Mail Extention)	Protokol untuk mengirim file binary dalam bentuk teks
				NNTP (Networ News Transfer Protocol)	Protokol untuk menerima dan mengirim newsgroup
				POP (Post Office Protocol)	Protokol untuk mengambil mail dari server
				SMB (Server Message Block)	Protokol untuk transfer berbagai server file DOS dan Windows
6	Presentasi			SMTP (Simple Mail Transfer Protocol)	Protokol untuk pertukaran mail
				SNMP (Simple Network Management Protocol)	Protokol untuk manejemen jaringan
				Telnet	Protokol untuk akses dari jarak jauh
				TFTP (Trivial FTP)	Protokol untuk transfer file
5	Sessi			NETBIOS (Network Basic Input Output System)	BIOS jaringan standar
				RPC (Remote Procedure Call)	Prosedur pemanggilan jarak jauh
				SOCKET	Input Output untuk network jenis BSD-UNIX
4	Transport		Transport	TCP (Transmission Control Protocol)	Protokol pertukaran data berorientasi (connection oriented)
				UDP (User Datagram Protocol)	Protokol pertukaran data non-orientasi (connectionless)
3	Network		Internet	IP (Internet Protocol)	Protokol untuk menetapkan routing
				RIP (Routing Information Protocol)	Protokol untuk memilih routing
				ARP (Address Resolution Protocol)	Protokol untuk mendapatkan informasi hardware dari nomer IP
				RARP (Reverse ARP)	Protokol untuk mendapatkan informasi nomer IP dari hardware
2	Datalink	LLC	Network Interface	PPP (Point to Point Protocol)	Protokol untuk point ke point
				SLIP (Serial Line Internet Protocol)	Protokol dengan menggunakan sambungan serial
		MAC		Ethernet, FDDI, ISDN, ATM	
1	Fisik				

Tabel 2.4 Hubungan Referensi Model OSI dengan Protokol Internet

2.5 Pengalamatan IP

Alamat IP (*Internet Protocol Address*) adalah deretan angka biner antara 32-bit sampai 128-bit yang dipakai sebagai alamat identifikasi untuk tiap komputer *host* dalam jaringan internet. Panjang dari angka ini adalah 32-bit (untuk IPv4 atau IP versi 4) dan 128-bit (untuk IPv6 atau IP versi 6) yang menunjukkan alamat dari komputer tersebut pada jaringan internet berbasis TCP/IP (sumber: http://id.wikipedia.org/wiki/Alamat_IP).

2.5.1 Kelas-kelas Pengalamatan IP

Pengalamatan IP terdiri dari dua bagian yakni bagian *network number* dan *host number*. Bagian yang menjadi *network number* dan *host number* diketahui dari pembagian kelas IP. Kelas IP dibedakan pada ukuran dan jumlahnya. Pengalamatan IP diatur oleh ARIN (*American Registry for Internet Numbers*). Pengalamatan IP terbagi dalam lima kelas yaitu:

- **Kelas A**

  Kelas A merupakan kelas yang memiliki jumlah *host number* terbanyak, sehingga kelas ini memiliki jumlah *network interface* terbanyak yang dapat ditampung. Kelas ini biasa digunakan oleh perusahaan yang memiliki jaringan dalam skala yang besar.

- **Kelas B**

  Kelas B memiliki 2 oktet *host number* yang mungkin untuk menampung 65534 *network interface* pada sebuah subnet. Alamat IP kelas B digunakan untuk jaringan dengan skala menengah.

- **Kelas C**

  Kelas C memiliki 1 oktet *host number* yang mungkin untuk menampung 254 *network interface* pada sebuah subnet. Kelas ini memiliki jumlah *network interface* yang paling sedikit dan juga paling banyak untuk jaringan berskala kecil.

- **Kelas D**

  Kelas D merupakan kelas khusus yang tidak dapat dipakai oleh publik karena satu blok kelas ini khusus dipakai untuk keperluan *multicast*. *Multicast* adalah jenis transmisi layaknya *broadcast*, namun dalam skala yang lebih kecil dan dapat ditentukan.

- **Kelas E**

  Kelas E adalah kelas IP yang tidak digunakan dan khusus disimpan dengan tujuan sebagai kelas cadangan untuk keperluan di masa mendatang.

	Range
Kelas A	1.x.x.x – 126.x.x.x
Kelas B	128.x.x.x – 191.x.x.x
Kelas C	192.x.x.x – 223.x.x.x
Kelas D	224.x.x.x – 239.x.x.x
Kelas E	240.x.x.x – 255.x.x.x

Tabel 2.5 *Range* Alamat IP Tiap Kelas

2.5.2 Public dan *Private* IP *Address*

Selain pembagian menurut alamat yang mampu ditampung, IP *address* juga dibagi menjadi dua macam berdasarkan pemakaiannya di internet :

- ***Private* IP *address***

  Private IP *address* adalah alamat IP yang digunakan oleh sebuah komunitas, baik itu rumah ataupun sebuah perusahaan, untuk berkomunikasi antara komputer yang satu dengan yang lainnya dalam jaringan internal. Alamat IP ini tidak bisa berkomunikasi langsung dengan komputer lain pada jaringan internet, sehingga untuk dapat berkomunikasi dibutuhkan perantara yaitu *Internet Service Provider* (ISP) yang menyediakan jasa layanan internet.

Class	RFC 1918 internal address 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

Tabel 2.6 *Range Private* IP *Address*

- ***Public* IP *address***

  Public IP *address* adalah alamat IP yang digunakan untuk berkomunikasi antar komputer yang tersambung secara langsung dalam jaringan internet. Jenis IP address banyak digunakan oleh *Internet Service Provider* (ISP) dan lembaga-lembaga dunia yang mengatur lalu-lintas di internet. *Range* alamat yang dimiliki oleh *public* IP *address* adalah semua alamat IP selain yang berada dalam *range private* IP *address* dan IP *loopback* (127.x.x.x).

2.5.3 Jenis-Jenis Alamat IP

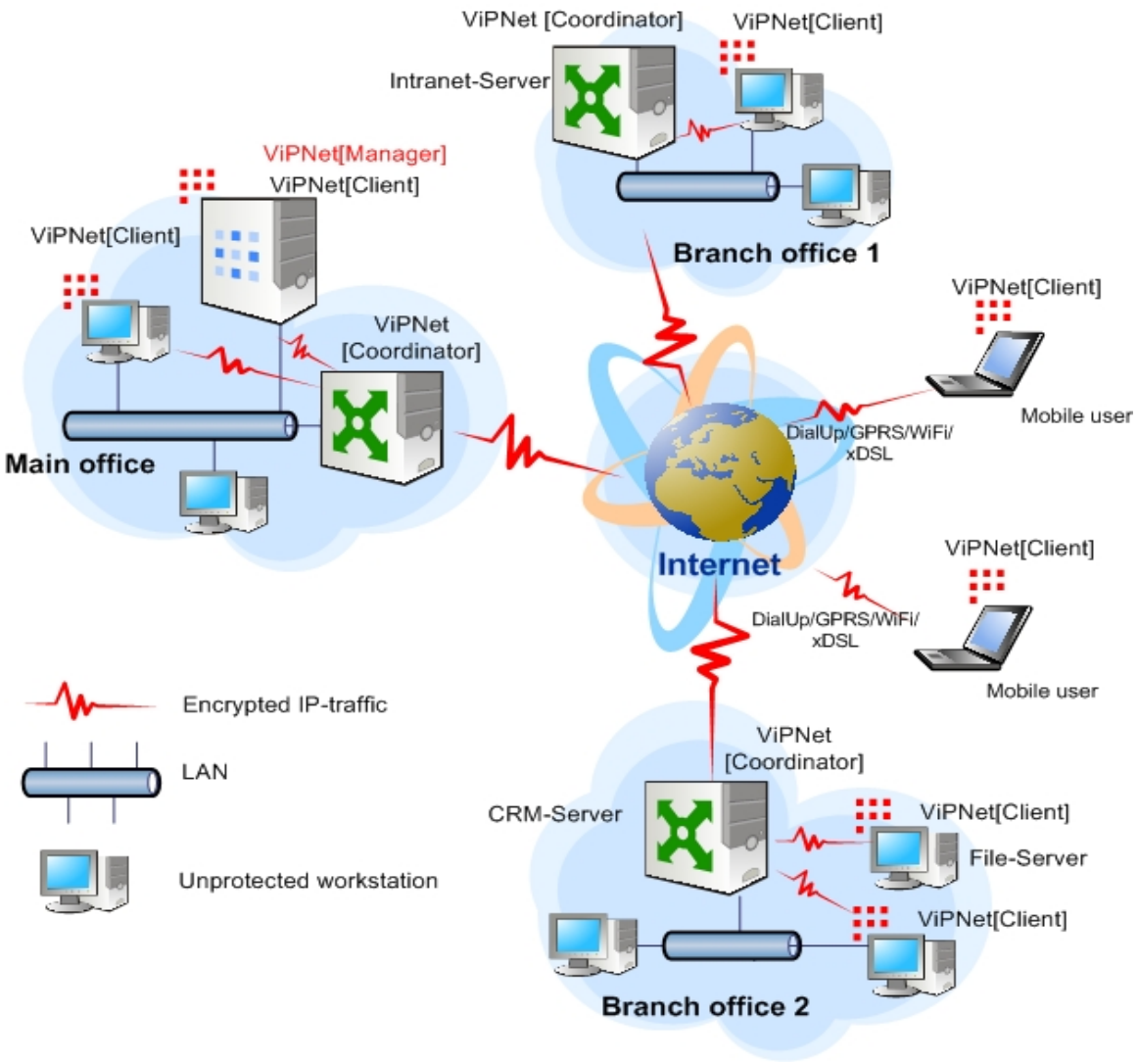
Alamat IPv4 terbagi menjadi beberapa jenis, yakni sebagai berikut:

- **Alamat Unicast**, merupakan alamat IPv4 yang ditentukan untuk sebuah antarmuka jaringan yang dihubungkan ke sebuah *internetwork* IP. Alamat *unicast* digunakan dalam komunikasi *point-to-point* atau *one-to-one*.

- **Alamat Broadcast**, merupakan alamat IPv4 yang didesain agar diproses oleh setiap *node* IP dalam segmen jaringan yang sama. Alamat broadcast digunakan dalam komunikasi *one-to-everyone*.
- **Alamat Multicast**, merupakan alamat IPv4 yang didesain agar diproses oleh satu atau beberapa node dalam segmen jaringan yang sama atau berbeda. Alamat multicast digunakan dalam komunikasi *one-to-many*.

2.6 VPN

VPN atau *Virtual Private Network* merupakan teknologi komunikasi yang memungkinkan pengguna melakukan koneksi ke jaringan privatnya melalui internet secara aman dengan sistem *tunelling,* dan menggunakan jaringan publik sebagai jalurnya.



Gambar 2.4 Gambaran VPN Secara Umum

(sumber : http://www.lisisoft.com/imglisi/4/Security/148616vpn.jpg)

2.6.1 Fungsi VPN

Teknologi VPN menyediakan tiga fungsi utama dalam penggunaanya, yaitu :

- **Kerahasiaan**

  Teknologi VPN memiliki sistem kerja mengenkripsi semua data yang melewatinya. Dengan adanya teknologi enkripsi ini, maka kerahasiaan data menjadi lebih terjaga. Dengan menerapkan sistem enkripsi ini, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data Anda dengan mudah.

- **Keutuhan Data**

  Ketika melewati jaringan internet, data 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 lain. VPN memiliki teknologi yang dapat menjaga keutuhan data yang dikirim agar sampai ke tujuannya tanpa cacat, hilang, rusak, ataupun dimanipulasi oleh orang lain.

- **Autentikasi Sumber**

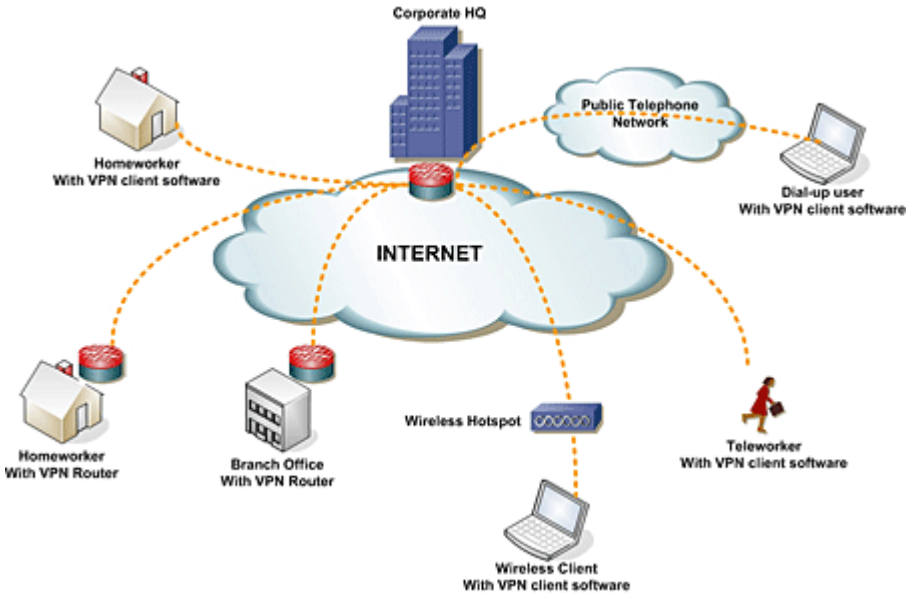
  Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan

diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil sumber informasi datanya. Kemudian alamat sumber data ini akan disetujui jika proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang semestinya. Tidak ada data yang dipalsukan atau dikirimkan oleh pihak-pihak lain.

2.6.2 Jenis-jenis VPN

- **Remote Access VPN**

  Jenis VPN ini memudahkan karyawan untuk terhubung langsung ke jaringan perusahaan dari jarak jauh (remote). Hal ini dikarenakan VPN bisa diakses di luar kantor selama karyawan tersebut memiliki akses internet. Hal ini juga berlaku bagi cabang perusahaan yang tidak memiliki koneksi secara terus-menerus ke kantor pusat. Kantor cabang tersebut dapat melakukan *dial-up* lokal ke suatu ISP dan melakukan koneksi ke kantor pusat.

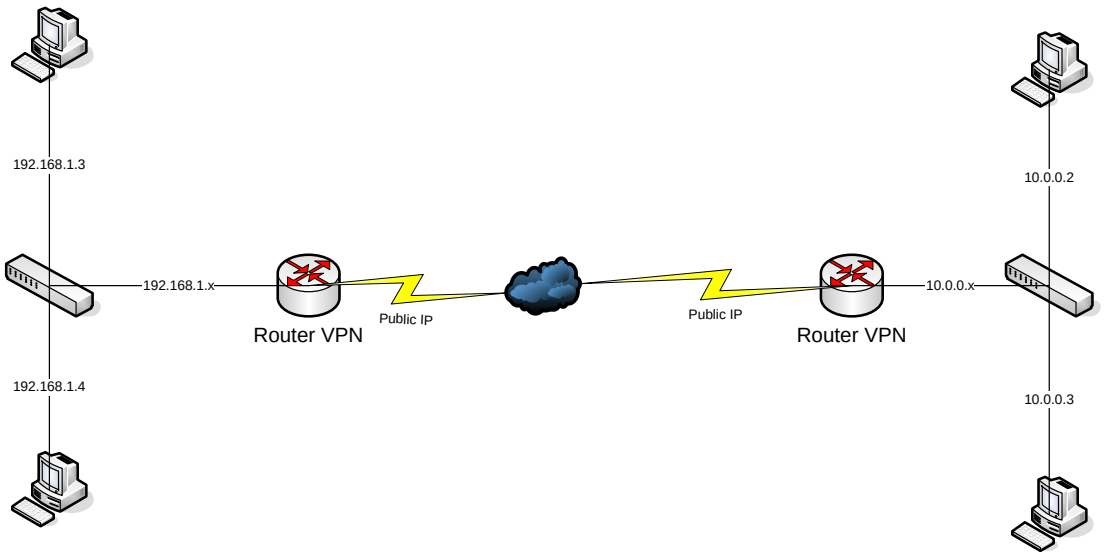


Gambar 2.5 Remote Access VPN

(sumber : http://www.networkelements.co.uk/media/vpn.gif)

- **Site-to-site VPN**

  Site-to-site VPN adalah jenis VPN yang menghubungkan dua kantor atau lebih yang letaknya berjauhan, baik kantor pusat dengan cabangnya ataupun dengan perusahaan mitra kerjanya.



Gambar 2.6 Site to Site VPN

Site-to-site VPN dibedakan menjadi dua jenis :

- Intranet VPN

  Intranet VPN digunakan untuk menghubungkan antara kantor pusat dengan kantor cabangnya.

- Extranet VPN

  Extranet VPN digunakan untuk menghubungkan antara kantor pusat dengan kantor mitra bisnisnya.

2.6.3 Keamanan VPN

Seperti yang telah dijelaskan bahwa VPN menggunakan internet sebagai media penghubungnya, maka keamanan pada jaringan VPN sangatlah diperlukan untuk mendapatkan komunikasi yang aman.

Beberapa tipe keamanan yang dapat diterapkan dala teknik VPN adalah enkripsi, autentikasi, autorisasi serta *firewall.*

2.6.3.1 Enkripsi

Enkripsi merupakan proses pengubahan data ke dalam bentuk sandi (*chipper text*) yang mana sandi-sandi tersebut hanya dapat dimengerti oleh pihak pengirim dan penerima data sehingga data tersebut tidak dapat dibaca oleh orang luar yang tidak diberikan hak akses untuk melihat data itu. Ada dua cara untuk melakukan proses enkripsi, yaitu enkripsi kunci simetrik dan enkripsi kunci asimetrik.

2.6.3.1.1 Enkripsi Kunci Simetrik

Pada enkripsi yang menggunakan kunci simetris, *user* menggunakan sebuah *private key* untuk melakukan enskripsi dan dekripsi data. Jadi sebelum mengirimkan data, perlu dipastikan bahwa pada komputer pihak penerima telah memiliki *private key* tersebut sehingga dia dapat melakukan dekripsi data. Namun kunci yang digunakan oleh pihak pengirim dan penerima sama sehingga jika

orang lain mengetahuinya maka data tersebut akan dengan mudah dibaca.

2.6.3.1.2 Enkripsi Kunci Asimetrik

Enkripsi kunci asimetrik menggunakan dua buah kunci yang berbeda, yaitu *private key* dan *public key*. *Private key* hanya diketahui oleh pihak pengirim dan *public key* diberikan kepada pihak penerima. Untuk mendekripsikan informasi yang diberikan pengirim, pihak penerima harus menggunakan *private key* miliknya dan *public key* yang diberikan oleh pengirim. Akan tetapi *private key* antara pihak penerima dan pengirim berbeda. Dikarenakan kerumitan penghitungan serta penggunaan algoritma yang kompleks, maka banyak orang yang lebih menggunakan sistem pengenkripsian data seperti ini. Sistem seperti ini biasa disebut *digital signature*.

2.6.3.2 Autentikasi

Autentikasi merupakan isu terpenting dalam pembuatan VPN. Dengan menggunakan metode autentikasi, data yang

dikirim akan menjadi jelas isi dan siapa pengirimnya. Biasanya dalam melakukan proses autentikasi, diperlukan sebuah nama (*username*) dan kata sandi (*password*) sebagai alat verifikasinya. *Username* dan *password* ini dimaksudkan agar tidak sembarang orang dapat mengakses, mengirim ataupun mengambil data yang bersifat *private*.

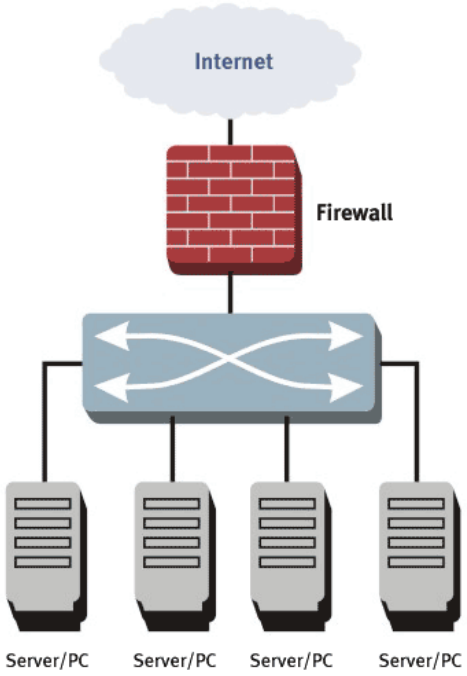
2.6.3.3 Autorisasi

Proses autorisasi merupakan tindak lanjut dari proses autentikasi. Setelah melakukan verifikasi *username* dan *password*, pengguna akan diberikan hak akses yang terbatas untuk melakukan sesuatu di jaringan VPN tersebut. Proses autorosasi inilah yang menentukan apakah pengguna tersebut dapat melakukan perintah atau tugas yang dikehendakinya pada jaringan VPN tersebut.

2.6.3.4 Firewall

Firewall merupakan suatu cara, sistem, ataupun mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu

atau semua hubungan atau kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau local area network (LAN).



Gambar 2.7 *Firewall*

(sumber : http://www.primustel.ca/en/business/images/Firewall-A2.gif)

2.6.3.4.1 Karakteristik *Firewall*

Ada beberapa karateristik yang harus dimiliki oleh suatu *firewall* sehingga *firewall* tersebut dapat dikatakan aman, antara lain:

1. Seluruh hubungan/kegiatan dari dalam ke luar harus melewati firewall. Hal ini dapat dilakukan dengan cara memblok/membatasi baik secara fisik semua akses terhadap jaringan lokal, kecuali melewati firewall.
2. Hanya kegiatan yang terdaftar/dikenal yang dapat melewati/melakukan hubungan. Hal ini dapat dilakukan dengan mengatur *policy* pada konfigurasi keamanan lokal.
3. Firewall itu sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan. Hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan sistem operasi yang relatif aman.

2.6.3.4.2 Teknik Yang Digunakan Pada *Firewall*

1. *Service control* (kendali terhadap layanan)

   Service control melakukan penyaringan berdasarkan tipe-tipe layanan yang digunakan di internet dan boleh diakses baik untuk ke dalam ataupun keluar *firewall*. Biasanya *firewall* akan mencek nomor IP *Address* dan juga nomor port yang di

gunakan baik pada protokol TCP dan UDP, bahkan bisa dilengkapi software untuk proxi yang akan menerima dan menterjemahkan setiap permintaan akan suatu layanan sebelum mengijinkannya. Bahkan bisa jadi software pada server itu sendiri, seperti layanan untuk web ataupun e-mail.

2. *User control* (kendali terhadap pengguna)

   User control melakukan penyaringan berdasarkan pengguna untuk dapat menjalankan suatu layanan, artinya ada pengguna yang bisa dan ada yang tidak dapat menjalankan suatu servis. Hal ini di karenakan pengguna tersebut tidak diijinkan untuk melewati *firewall*. Biasanya digunakan untuk membatasi pengguna dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar.

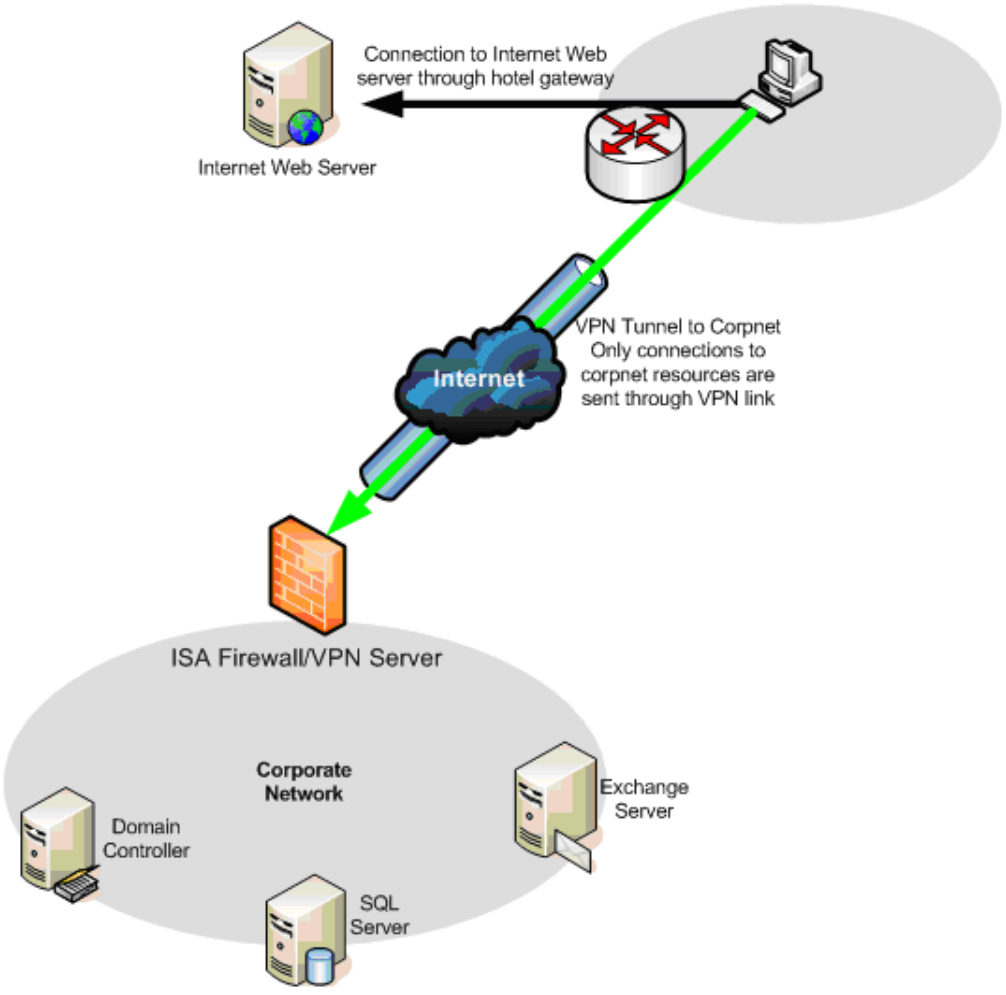
2.6.4 *Tunneling*

Teknologi *tunneling* merupakan teknologi yang bertugas untuk menangani dan menyediakan koneksi *point-to-point* dari sumber ke tujuannya. Teknologi ini disebut *tunnel* karena koneksi *point-to-point* tersebut sebenarnya terbentuk dengan melintasi jaringan umum namun tidak mempedulikan paket-paket data milik orang lain yang sama-sama melintasi jaringan umum tersebut, tetapi koneksi tersebut hanya melayani transportasi data dari pembuatnya. Koneksi *point-to-point* ini sesungguhnya tidak benar-benar ada, namun data yang dikirimkannya terlihat seperti benar-benar melewati koneksi pribadi yang bersifat *point-to-point*.

Teknologi ini dibuat dengan cara pengaturan IP *Addressing* dan IP *Routing*, sehingga antara sumber *tunnel* dengan tujuan *tunnel* dapat saling berkomunikasi melalui jaringan dengan pengalamatan IP. Apabila komunikasi antara sumber dan tujuan dari *tunnel* tidak dapat berjalan dengan baik, maka *tunnel* tersebut tidak akan terbentuk dan VPN pun tidak dapat dibangun.

Setelah *tunnel* tersebut terbentuk dengan baik, koneksi *point-to-point* tersebut dapat langsung digunakan untuk mengirim dan menerima data. Dalam implementasinya di VPN, *tunnel* tersebut tidak dibiarkan begitu saja tanpa diberikan sistem keamanan tambahan. *Tunnel* dilengkapi dengan sebuah sistem enkripsi untuk menjaga data yang

melewatinya. Proses enkripsi inilah yang menjadikan teknologi VPN bersifat pribadi dan aman.



Gambar 2.8 *Tunneling*

(sumber: http://www.isaserver.org/img/upl/2004fi11115652930967.gif)

2.6.4.1 PPTP (*Point to Point Tunneling Protocol)*

PPTP merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari *remote client* ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP. Teknologi jaringan PPTP merupakan pengembangan dari *remote access point-to-point protocol* (PPP) yang dikeluarkan oleh *Internet Engineering Task Force* (IETF). PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP datagrams agar dapat ditransmisikan melalui intenet. PPTP juga dapat digunakan pada jaringan privat LAN-to-LAN dan komputer yang terhubung dengan LAN untuk membuat VPN melalui LAN.

Fasilitas utama dari penggunaan PPTP adalah dapat digunakannya *Public-Switched Telephone Networks* (PSTNs) untuk membangun VPN. Pembangunan PPTP yang mudah dan berbiaya murah untuk digunakan secara luas, menjadi solusi untuk *remote users* dan *mobile users* karena PPTP memberikan keamanan dan enkripsi komunikasi melalui PSTN ataupun internet.

Umumnya terdapat tiga komputer yang diperlukan untuk membangun PPTP, yaitu :

- Klien PPTP
- *Network Access Server* (NAS). Tidak dibutuhkan jika ingin membuat PPTP antara klien dengan server yang terhubung dengan LAN yang sama.
- Server PPTP

Kelebihan penggunaan PPTP :

- Mendukung enkripsi melalui enkripsi *Microsoft Point-to-Point Encryption* (MPPE).
- Menggunakan *username* dan *password* untuk autentikasi.
- Pilihan yang bagus untuk kemampuan dasar VPN karena protokol PPTP ini sudah ada di dalam semua klien sistem operasi Windows modern dan tidak memerlukan suatu *public-key infrastructure* (PKI).

Kekurangan penggunaan teknologi PPTP :

- Tidak memberikan integritas data (yaitu semacam suatu bukti bahwa data tidak dimodifikasi selama dalam transit pengiriman).

- Tidak memberikan data autentikasi asli atau sumbernya (semacam bukti bahwa data dikirim oleh pengguna yang asli).

2.6.4.2 L2TP (*Layer 2 Tunneling Protocol)*

L2TP berasal dari penggabungan antara dua buah protokol *tunneling*, yaitu L2F (*Layer 2 Forwading)* milik CISCO serta PPTP milik Microsoft. Paket L2TP dikirim melalui UDP datagram. Ada dua macam tipe L2TP :

2.6.4.2.1 Voluntary Tunnel

Voluntary Tunnel merupakan *tunnel* yang dibuat berdasarkan permintaan klien. Pada awalnya klien akan melakukan koneksi kepada ISP yang menyediakan jasa VPN. Setelah menerima permintaan dari klien, ISP tersebut membuatkan jalur khusus yang menghubungkan klien tersebut dengan VPN server-nya.

2.6.4.2.2 Compulsory Tunnel

Berbeda halnya dengan *voluntary tunnel*, *compulsory tunnel* dibuat oleh perangkat

intermediate. Perangkat *intermediate* ini bisa berupa dial-up server ataupun alat lainnya. Ketika klien dan *remote client* yang terhubung dengan LAN ingin membangun koneksi, mereka harus terhubung terlebih dahulu dengan perangkat *intermediate* yang biasanya terletak di ISP. Setelah koneksi sudah terbuat maka perangkat inilah yang membuat *tunnel*.

2.6.4.3 IPSec (*IP Security)*

IPSec menggunakan dua protokol untuk menyediakan layanan keamanan lalu lintas yaitu *Authentication Header* (AH) dan *Encapsulating Security Payload* (ESP). Implementasi IPSec harus mendukung ESP dan juga AH agar sistemnya dapat berjalan dengan baik.

- **AH (*Authentication Header*)**, menyediakan layanan autentikasi (menyatakan bahwa data yang dikirim berasal dari pengirim yang benar), integritas (keaslian data), dan *replay protection* (transaksi hanya dilakukan sekali, kecuali yang berwenang telah mengizinkan), juga melakukan pengamanan terhadap IP *header*

(*header compression*). Pengamanan IP *header* dilakukan dengan menambahkan *header* baru yang mengandung nilai *hash* sehingga hanya penerimalah yang dapat mengautentifikasinya. Layanan AH ini seolah-olah membuat *tunnel* khusus pada jaringan publik sehingga hanya orang tertentu saja yang dapat mengaksesnya.

- **ESP (*Encapsulated Security Payload*)**, menyediakan layanan *authentication, intregity, replay protection, dan confidentiality* terhadap data. ESP melakukan pengamanan data terhadap segala sesuatu dalam paket data setelah header.

2.7 Mikrotik Router OS

Mikrotik Router OS merupakan sistem operasi independen berbasiskan Linux yang diperuntukkan sebagai *network router*. Router itu sendiri digunakan untuk menjalankan fungsi *routing,* yaitu mengatur jalur data agar masing-masing *network* dapat saling terhubung satu sama lain membentuk suatu jaringan.

Mikrotik dirancang untuk memberikan kemudahan bagi penggunanya dan juga dapat diinstal di PC komputer standar. Administrasinya bisa

dilakukan melalui *Windows application* (*WinBox*). PC yang akan dijadikan router mikrotik pun tidak memerlukan *resource* yang cukup besar untuk penggunaan standar, misalnya hanya sebagai *gateway*. Untuk keperluan beban yang besar (*network* yang kompleks, *routing* yang rumit dan lainnya) disarankan untuk mempertimbangkan pemilihan *resource* PC yang memadai.

Mikrotik pada standar perangkat keras berbasiskan *Personal Computer* (PC) dikenal dengan kestabilan, kualitas kontrol dan fleksibilitas untuk berbagai jenis paket data dan penanganan proses rute atau lebih dikenal dengan istilah *routing*. Mikrotik yang dibuat sebagai router berbasiskan PC banyak bermanfaat untuk sebuah ISP yang ingin menjalankan beberapa aplikasi mulai dari hal yang paling ringan hingga tingkat lanjut, contohnya aplikasi untuk *routing*, aplikasi pengatur kapasitas akses (*bandwidth management*), *firewall*, *wireless access point* (WiFi), *backhaul link*, sistem *hotspot*, *Virtual Private Network* (VPN) server dan masih banyak lainnya. Mikrotik juga mempunyai banyak servis atau *tool* sehingga bisa dijadikan DHCP server, PROXY server, RADIUS server, DNS server, VPN server selain sebagai router.

Mikrotik dapat digunakan dalam 2 tipe, yaitu dalam bentuk perangkat lunak dan perangkat keras. Mikrotik Router OS yang berbentuk *software* yang dapat di-*download* di www.mikrotik.com dan diinstal pada komputer rumahan (PC). *BUILT-IN Hardware* mikrotik dalam bentuk perangkat keras yang

khusus dikemas dalam *board router* yang di dalamnya sudah terinstal Mikrotik Router OS.