BAB 2

LANDASAN TEORI

Kumpulan komputer yang saling terhubung membentuk sebuah jaringan akan menjadi kaya akan sumber daya yang dibutuhkan. Jaringan komputer sendiri memiliki berbagai macam tipe dan kelompok yang dibedakan berdasarkan area jangkauan,media transmisi dan fungsi. Selain itu untuk menggambarkan infrastruktur suatu jaringan yang berbeda-beda dapat dibentuk dengan beberapa topologi, seperti topologi *bus,star,ring,mesh,*dan *tree.* Yang masing-masing topologi tersebut memiliki kelebihan dan kekurangannya masing-masing sehingga dapat disesuaikan dengan kebutuhan dalam membangun suatu jaringan komputer. Selain itu jaringan juga memiliki aturan sendiri atau yang biasa disebut protokol jaringan yang berbeda. Dalam pengembangan teknologi jaringan komputer terdapat beberapa teknik pengamanan data, salah satunya adalah VPN. Teknik ini dapat membuat suatu jaringan *private/*khusus yang menumpang kepada jaringan *public* sehingga tingkat keamanan suatu data dapat terjamin.

Dalam bab ini akan dijelaskan beberapa teori-teori mengenai suatu jaringan komputer, mulai dari pengertian dasar dari suatu jaringan komputer, lalu klasifikasi jaringan komputer yang berbeda-beda menurut area jangkauan,media transmisi dan fungsinya, selain itu juga ada penjelasan mengenai beberapa topologi yang digunakan dalam suatu jaringan komputer, penjelasan beberapa perangkat yang sering digunakan dalam suatu jaringan komputer, lalu ada penjelasan tentang protokol jaringan dan juga IP addressing atau pengalamatan IP. Selain itu juga akan dijelaskan mengenai

teknologi VPN, mulai dari pengertian dasar teknologi tersebut, kemudian ada fungsi-fungsi dari VPN, dan juga ada penjelasan mengenai cara kerja VPN , serta jenis-jenis VPN yang ada sekarang ini dan metode keamanan yang digunakan dalam VPN.

2.1 Teori Umum

2.1.1 Definisi Jaringan Komputer

Jaringan adalah kumpulan dua atau lebih komputer yang masing-masing berdiri sendiri dan terhubung melalui sebuah teknologi. Hubungan antar komputer tersebut tidak terbatas berupa kabel tembaga saja, namun juga bisa melalui *fiber optic*, gelombang *microwave*, *infrared*, bahkan melalui satelit (Tanenbaum, 2003, p10). Tujuan dibangunnya suatu jaringan komputer adalah membawa informasi secara tepat dan tanpa adanya kesalahan dari sisi pengirim menuju ke sisi penerima melalui media komunikasi. Beberapa sasaran dibentuknya suatu jaringan komputer diantaranya:

- *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.

- Mendapatkan akses informasi dengan cepat, contohnya melalui *internet*

- Melakukan pembagian (*sharing*) data.

2.1.2 Klasifikasi Jaringan Komputer

Untuk membedakan setiap jaringan komputer para ahli membedakannya dengan mengklasifikasikan jaringan komputer agar lebih mudah di ketahui, di antaranya:

-berdasarkan area jangkauan

-berdasarkan media transmisi

-berdasarkan fungsi

Mungkin saja ada yang mengklasifikasikannya secara berbeda, namun biasanya ini hanyalah masalah perbedaan sudut pandang dan kata-kata saja.

2.1.2.1 Berdasarkan area jangkauan

1. *Local Area Network* (LAN)

   LAN merupakan jaringan komputer lokal yang biasa digunakan dalam cakupan area yang tidak terlalu besar (dengan jarak beberapa kilometer) seperti gedung perkantoran ataupun kampus. LAN juga seringkali digunakan untuk menghubungkan komputer pribadi atau *workstation* lainnya agar dapat menggunakan suatu *resource* (misalnya *printer,scanner*) secara bersamaan dan juga dapat digunakan sebagai sarana bertukar data dan informasi antar user dalam jaringan tersebut.

Karena LAN memiliki skala cakupan yang kecil dan terbatas, maka memudahkan seseorang untuk membuat,mengontrol dan memanajemen kinerja jaringan tersebut, serta faktor terjadinya suatu kesalahan cenderung lebih kecil dan lebih mudah di lacak.

2. *Metropolitan Area Network* (MAN)

   MAN pada dasarnya sama seperti jaringan LAN namun memiliki cakupan area yang jauh lebih luas seperti dalam kota, antar kota atau bahkan dalam satu provinsi dan juga biasanya memiliki teknologi yang tidak jauh berbeda dari LAN. MAN dapat mencakup kantor-kantor perusahaan yang berdekatan dan dapat dimanfaatkan untuk keperluan pribadi atau umum, MAN juga mampu menunjang data dan suara, bahkan beberapa dapat berhubungan dengan jaringan televisi kabel.

3. *Wide Area Network* (WAN)

   WAN merupakan suatu jaringan komputer yang menghubungkan antar jaringan LAN dalam cakupan area yang sangat jauh dalam hal ini antar negara dan antar benua. Biasanya WAN menghubungkan jaringan LAN menggunakan fasilitas transmisi yang disediakan oleh penyedia jaringan,seperti perusahan telepon. WAN digunakan untuk menghubungkan LAN-LAN, sehingga *user* dan komputer dari satu lokasi dapat berkomunikasi dengan *user* di lokasi lainnya secara *real-time* dan

saling bertukar data dan informasi, dan juga mendukung penggunaan *email,internet,file transfer,* dan *e-commerce.*

2.1.2.2 Berdasarkan Media Transmisi

1. *Wire Network*

   Wire Network adalah jaringan komputer yang menggunakan kabel sebagai media transmisi nya. Jadi data mengalir dalam suatu jaringan tersebut melalui kabel tersebut. Biasanya bahan kabel yang di gunakan terbuat dari tembaga bila memerlukan yang lebih cepat dapat menggunakan serat optik sebagai pilihannya. Beberapa jenis kabel tersebut diantaranya adalah:

   - *Twisted pair* , adalah suatu media transmisi dua kabel yang disekat dan disusun dalam pola spiral beraturan. Dengan semakin berkembangnya teknologi jenis kabel ini menjadi yang paling banyak dipakai karena kecepatannya semakin meningkat dan harganya yang relatif murah.
   - *Coaxial Cable,* adalah kabel yang terdiri dari lapisan sekat konduktor silindris luar yang mengelilingi suatu inti konduktor.
   - Serat Optik / *Fibre Optic* , adalah suatu media fisik yang mampu melakukan transmisi cahaya termodulasi. Serat optik memiliki tingkatan gangguan yang sangat minim, salah satu alasannya adalah karena tidak terpengaruh oleh gelombang elektromagnetik. Dan jenis ini menjadi pilihan yang baik bagi yang membutuhkan jaringan berkecepatan tinggi dan *traffic* yang ramai.

2. *Wireless Network*

Wireless network merupakan jaringan komputer yang menggunakan gelombang radio atau cahaya *infrared* sebagai pengahantarnya yang di pancarkan melalui udara dengan menggunakan antena, dan di terima oleh *user* juga melalui antena penerima. Frekuensi yang digunakan pada radio untuk jaringan komputer biasanya menggunakan ferkuensi tinggi, yaitu 2.4 GHz dan 5.8 GHz. Sedangkan *infrared* umumnya terbatas pada jaringan yang menghubungkan dua buah komputer atau yang disebut *point to point*, hal ini menyebabkan *infrared* tidak banyak dipakai dibandingkan gelombang radio.

Beberapa jenis transmisi yang bisa digunakan sebagai sarana *wireless* adalah:

- Gelombang mikro terresterial
- Gelombang mikro satelit
- Radio *broadcast* / gelombang radio
- *Infrared* / infra merah

2.1.2.3 Berdasarkan fungsi

1. *Client Server*

Client Server adalah jaringan komputer yang salah satu (atau lebih) komputer dijadikan sebagai *server* atau induk dari komputer lain. *Server*

melayani komputer lain yang disebut sebagai *client*. Layanan yang diberikan bisa berupa akses *web,e-mail,file* atau yang lainnya. *Client server* banyak dipakai pada *internet*, namun jaringan lainnya pun bisa juga mengimplementasikan *client server*, tergantung pada kebutuhannya masing-masing.

2. *Peer to Peer*

   Pada jaringan ini setiap komputer bisa memiliki akses sebagai *server* maupun *client*, karena setiap komputer dapat memberi dan menerima *access* dari atau ke komputer lain dan mempunyai media penyimpanannya masing-masing. *Peer to Peer* banyak di implementasikan pada jaringan LAN, namun dapat juga di implementasikan pada jaringan MAN dan WAN. Tetapi hal itu jarang ditemukan, karena dari segi keamanan dan manajemen sangat sulit menjaganya dan mengontrolnya apalagi berhubungan dengan pengguna komputer yang bisa dibilang sangat banyak.

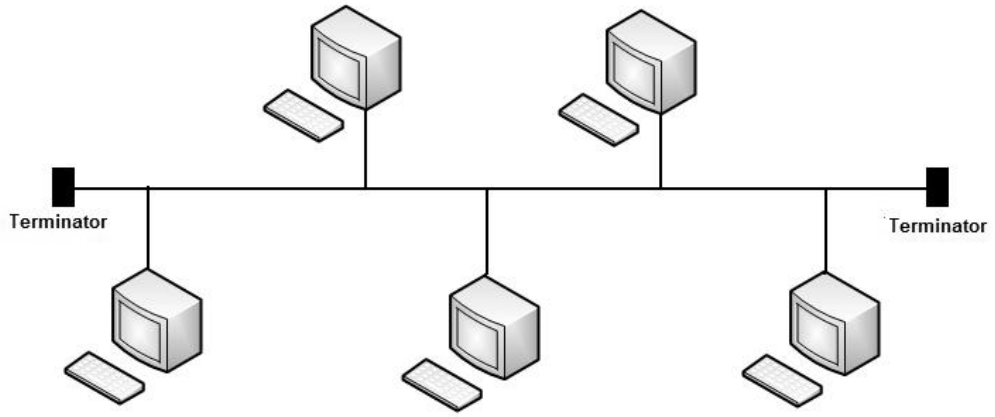
2.1.3 Topologi Jaringan

Topologi jaringan adalah suatu cara atau aturan tentang bagaimana konfigurasi atau pengaturan hubungan antar komputer secara fisik dan juga hubungannya dengan komponen lain yang saling berkomunikasi seperti *server,workstation,hub/switch,*dan media transmisinya di dalam jaringan komputer. Ketika memakai suatu topologi jaringan maka kita perlu mengikuti beberapa

spesifikasi tertentu. Tetapi dalam memikirkan suatu topologi jaringan kita perlu memikirkan berdasarkan kegunaan, keterbatasan *resource* dan keterbatasan biaya, sehingga topologi-topologi jaringan yang ada bisa disesuaikan dengan keadaan di lapangan.

Berikut beberapa jenis topologi yang ada:

1. Topologi *Bus*



Gambar 2.1 Topologi *Bus*

Topologi ini adalah topologi yang pertama di gunakan untuk menghubungkan komputer. Dalam topologi ini masing-masing komputer akan terhubung ke satu kabel panjang (*bus*) dengan beberapa terminal, dan pada akhir dari kabel harus di akhiri dengan satu *terminator*. Komputer berkomunikasi dengan cara mengirim dan mengambil data melalui bus tersebut.

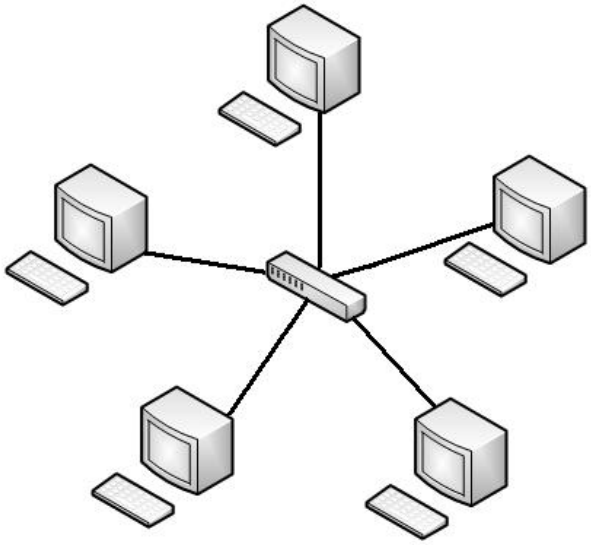
Kelebihan Topologi *Bus*:

- Pengembangan jaringan dan penambahan *workstation* baru dapat dilakukan lebih mudah tanpa mengganggu *workstation* lainnya.
- Biaya yang lebih murah
- Mudah dalam pemasangannya

Kekurangan Topologi *Bus*:

- Jika terjadi gangguan di sepanjang kabel maka seluruh jaringan juga akan ikut mengalami gangguan.
- Hanya satu komputer yang dapat mengirimkan data dalam waktu yang bersamaan.

2. Topologi *Star*



Gambar 2.2 Topologi *Star*

Topologi ini telah menggunakan bantuan alat untuk menghubungkan jaringan, biasanya berupa *hub* atau *switch*. Masing-masing komputer dihubungkan ke alat tersebut menggunakan jalur yang berbeda-beda, jadi jika salah satu mengalami gangguan tidak akan mempengaruhi yang lainnya.

Kelebihan Topologi *Star*:

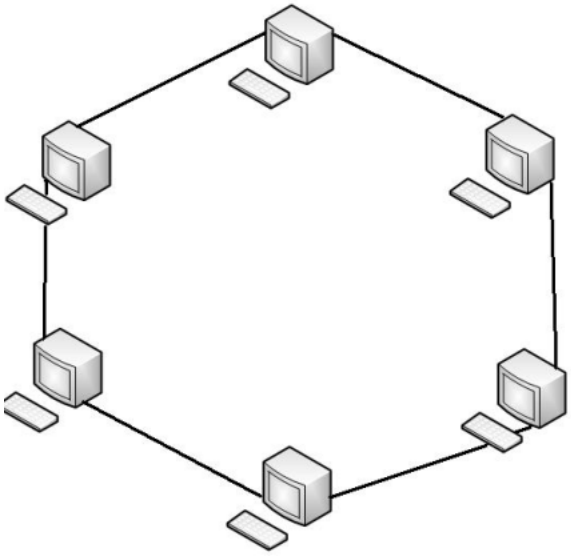
- Jika terjadi gangguan pada satu komputer atau *link*, maka hanya berakibat pada komputer yang berada di jalur tersebut saja. Sedangkan komputer lainnya tetap berjalan seperti biasa.

- Mudah dalam penambahan komputer baru pada jaringan tersebut, hanya tinggal menyambungkan kabel baru ke jaringan pusatnya dengan komputer baru tersebut.
- Pusat jaringan ini merupakan tempat yang baik untuk mencari kesalahan yang terjadi dalam jaringan.

Kekurangan Topologi *Star*:

- Sangat bergantung pada *hub/switch* sebagai pusat kendali, sehingga kondisinya harus selalu baik. Jika rusak berdampak pada keseluruhan jaringan tersebut.
- Membutuhkan lebih banyak kabel, karena tiap komputer membutuhkan link tersendiri untuk menghubungkannya dengan *central point(hub/switch)* tersebut.
- Otomatis biaya bertambah

3. Topologi *Ring*



Gambar 2.3 Topologi *Ring*

Dalam topologi ini seluruh komputer pada jaringan terhubung ada sebuah jalur data yang menghubungkan komputer yang satu dengan yang lain secara berurutan sehingga menyerupai sebuah lintasan atau cincin. Topologi ini tidak berbeda jauh dari topologi bus, hanya saja kedua ujungnya saling berhubungan, sehingga jika salah satu komputer mengalami gangguan maka akan mempengaruhi keseluruhan jaringan pula.

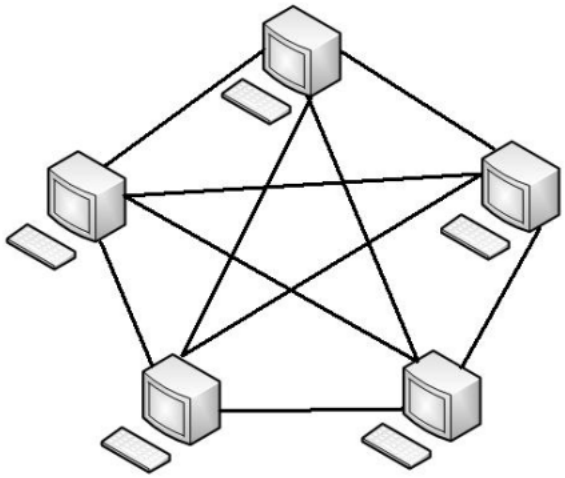
Kelebihan Topologi *Ring*:

- Identifikasi kerusakan cukup mudah karena sinyal data terus bergerak dari si pengirim ke penerima.
- Dapat menghindari tabrakan dalam pengiriman data karena mengalir dalam satu arah, sehingga data yg dikirim selanjutnya akan dikerjakan setelah pengiriman yang pertama selesai.

Kekurangan Topologi *Ring*:

- Kerusakan pada satu komputer memberikan dampak terhadap keseluruhan jaringan dan tentu saja akan mempersulit proses perbaikannya.
- Penambahan dan pemindahan komputer akan mengganggu jaringan sementara karena harus memutus jaringan untuk beberapa saat.

4. Topologi *Mesh*



Gambar 2.4 Topologi *Mesh*

Topologi ini biasa di kenal dengan hubungan point to point atau juga *pure peer to peer* karena setiap komputer saling terhubung ke komputer lain menggunakan kabel. Topologi ini paling jarang dipakai karena selain rumit dan tidak praktis topologi ini juga memerlukan banyak kabel sehingga akan lebih boros.

Kelebihan Topologi *Mesh*:

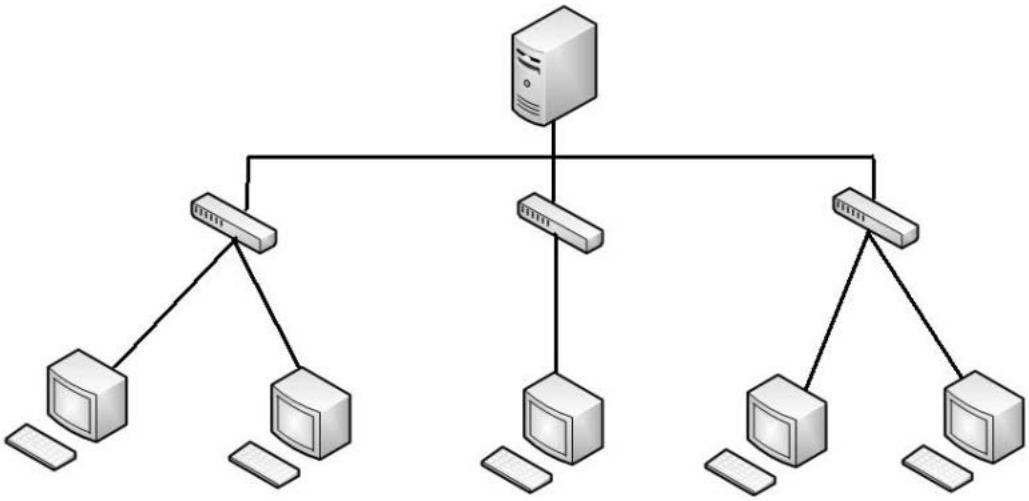
- Lebih mudah dalam mengidentifikasi permasalahan yang terjadi pada koneksi antar komputer.
- Hubungan langsung antar komputer menjamin data langsung dikirim ke tujuan tanpa harus melalui komputer lain, sehingga penyampaian data lebih cepat.
- Jika terjadi kerusakan pada satu link hanya akan berpengaruh pada komputer yang berada di link tersebut saja, sedangkan komputer lain tetap aktif seperti biasa.

- *Privacy* dan *security* lebih terjamin karena komunikasi antara dua komputer tidak bisa diakses oleh komputer lain.

Kekurangan Topologi *Mesh*:

- Sulit dalam melakukan penginstalan dan konfigurasi ulang apalagi jika jumlah komputer dan peralatan lain yang terhubung semakin banyak.
- Biaya yang cukup besar untuk pembuatan jaringan ini.
- Banyaknya kabel yang digunakan juga menunjukan perlunya ruang yang lebih besar untuk pengaturan dan peletakan kabel serta komputer itu sendiri.

5. Topologi *Tree*



Gambar 2.5 Topologi *Tree*

Topologi *Tree* atau biasa juga disebut Topologi Hierarki ini merupakan penggabungan dari topologi *bus* dengan topolgi *star*, dimana membentuk

sebuah tingkatan yang menempatkan sebuah node sebagai pusat dengan node-node lainnya sesuai dengan level kepentingannya.

Kelebihan Topologi *Tree*:

- Kontrol jaringan lebih mudah karena bersifat terpusat dan terbagi dalam tiap *level* atau tingkatan yang berbeda.
- Mudah untuk dikembangkan.

Kekurangan Topologi *Tree*:

- Jika salah satu *node* atau komputer rusak, maka komputer yang berada di level atau tingkatan bawahnya juga akan ikut mengalami kerusakan.
- Dapat terjadi tabrakan *file* atau data saat pengiriman yang bersamaan.

2.1.4 Perangkat Jaringan

Beberapa perangkat jaringan yang sering digunakan untuk membangun sebuah jaringan adalah:

- *NIC*
- *Hub*
- *Repeater*
- *Bridge*
- *Switch*
- *Router*

Berikut beberapa penjelasan dari beberapa perangkat jaringan tersebut:

1. *Network Interface Card* (NIC)

   NIC merupakan peralatan fisik yang menghubungkan komputer dengan suatu jaringan agar dapat saling berkomunikasi. NIC juga menentukan kecepatan dalam suatu jaringan. NIC biasa berbentuk kartu yang dipasang di dalam komputer, bisa berupa *card* ISA,PCI, atau PCMCIA.

2. *Hub*

   Hub merupakan alat yang dapat menggandakan *frame* data yang bearasal dari salah satu komputer ke semua port yang ada pada hub tersebut. Sehingga semua komputer yang terhubung dengan *port hub* juga akan menerima data yang sama. Ada beberapa kategori *hub* diantaranya :

   - *Passive hub*

     Merupakan *hub* biasa yang hanya meneruskan sinyal ke seluruh *node*, tetapi tidak memperkuat sinyalnya.

   - *Active hub*

     Memiliki fungsi yang sama dengan *passive hub*, hanya saja *hub* ini dapat sekaligus memperkuat sinyal sehingga jangkauannya menjadi lebih luas.

   - *Intelligent hub*

     Hub jenis ini dapat melakukan seleksi alamat paket dan tujuan, sehingga hanya node yang diinginkan saja yang dapat menerimanya.

3. *Repeater*

   Repeater merupakan salah satu contoh *active hub*. *Repeater* merupakan alat yang dapat menerima sinyal untuk kemudian memperkuat dan mengirimkan kembali sinyal tersebut ke tempat lain, sehingga jangkauan sinyal tersebut menjadi lebih jauh.

4. *Bridge*

   Bridge merupakan alat yang dapat menghubungkan beberapa segmen kecil dalam sebuah jaringan. Berbeda dengan *hub*, *bridge* dapat mempelajari MAC *address* tujuan. Sehingga saat sebuah komputer mengirimkan data untuk komputer tertentu, ia akan coba mencari port dari MAC *address* yang ia tuju dan mengirimkan hanya kepada komputer tersebut saja.

5. *Switch*

   Switch adalah sejenis *bridge* yang juga bekerja pada lapisan *data link*, tetapi memiliki keunggulan karena memiliki *port* yang masing-masing mempunyai *domain collision* sendiri. *Switch* menciptakan *virtual private network* (VPN) dari *port* pengirim dan penerima, jadi jika dua komputer berkomunikasi melalui VPN tersebut maka segmen lainnya tidak terganggu. Jika satu *port* sedang sibuk maka *port* lainnya tetap berfungsi seperti biasa. Dengan *switch* memungkinkan transmisi *full-duplex* untuk hubungan antar *port*,dengan syarat hanya ada satu komputer yang dapat dihubungkan ke satu *port* dari *switch*, serta NIC komputer tersebut harus yang mendukung transmisi *full-duplex*, dan *collision detection* dan *loopback* harus dimatikan.

6. *Router*

Router adalah peralatan jaringan yang dapat menghubungkan satu jaringan dengan jaringan yang lain. Sepintas *router* memang mirip dengan *bridge*, namun *router* sebenarnya lebih ‘cerdas’ dibandingkan dengan *bridge*. *Router* bekerja menggunakan *routing table* yang disimpan di *memory*-nya untuk membuat keputusan tentang ke mana dan bagaimana paket dikirimkan. *Router* dapat memutuskan rute terbaik yang akan ditempuh oleh paket data. *Router* akan memutuskan media fisik yang ‘disukai’ dan yang ‘tidak disukai’. *Protocol routing* dapat mengantisipasi berbagai kondisi yang tidak dimiliki oleh *bridge*.

2.1.5 Protokol Jaringan

Protokol jaringan adalah suatu aturan yang mengatur cara-cara dalam suatu jaringan untuk bertukar informasi. Model yang umum dijadikan referensi untuk mempelajari *protocol* jaringan adalah model referensi OSI *layer* atau *Open system interconnection layer*. Sedangkan *Internet protocol suiter* (TCP/IP) merupakan protokol jaringan yang saat ini paling umum digunakan untuk *internetworking*.

2.1.5.1 Model Referensi OSI

Gambar 2.6 OSI *Layer Model*

Model referensi jaringan terbuka OSI atau OSI *Reference Model for open networking* adalah sebuah model arsitektural jaringan yang dikembangkan oleh badan *International Organization for Standarization* (ISO) di Eropa pada tahun 1977. OSI sendiri merupakan singkatan dari *Open System*

Interconnection. Model ini juga disebut dengan "Model tujuh lapis OSI" (OSI *seven layer model*). OSI *layer* adalah sebuah kerangka yang digunakan untuk dapat mengetahui bagaimana informasi dapat dipindahkan melalui *network*. OSI *layer* menjelaskan bagaimana paket-paket dapat berpindah melalui berbagai *layers* menuju ke *device* yang lain di dalam *network*, walaupun jika pengirim dan tujuan mempunyai tipe media jaringan yang berbeda.

Di dalam OSI *reference model* terdapat tujuh buah *layers* dan masing-masing mempunyai tugas yang berbeda. Pembagian jaringan menjadi tujuh *layers* memberikan kentungan sebagai berikut:

- Dapat memecah komunikasi jaringan menjadi lebih kecil.
- Standarisasi komponen jaringan untuk pengembangan *vendor* yang berbeda.
- Mendukung berbagai macam tipe *network hardware* dan *software* yang berbeda untuk saling berkomunikasi.
- Dapat mencegah perubahan di satu *layer* yang dapat mempengaruhi *layer* yang lain.
- Membagi komunikasi *network* menjadi bagian yang lebih kecil sehingga lebih mudah dimengerti.

Berikut penjelasan mengenai 7 *layer* pada OSI *layer*:

1. Layer 1 – *Physical Layer*

   Physical layer merupakan lapisan terbawah pada model OSI. *Physical layer* berkomunikasi secara langsung dengan berbagai tipe media

komunikasi ataupun *hardware*. *Physical layer* menjelaskan spesifikasi kelistrikan, mekanisme, prosedur, dan fungsi untuk mengaktifkan, pemeliharaan, dan menonaktifkan hubungan fisik antar sistem. *Physical layer* melakukan dua hal yaitu mengirim dan menerima *bit*. *Bit* hanya mempunyai dua nilai 1 dan 0, berbagai jenis media mempresentasikan nilai *bit* ini dengan cara yang berbeda. Beberapa menggunakan nada audio, sementara yang lain menggunakan *state transition*- yaitu perubahan tegangan listrik dari tinggi ke rendah dan sebaliknya. Peralatan yang merupakan *physical layer* antara lain *hub* dan *repeater*.

2. Layer 2 – *Data Link Layer*

   Berfungsi untuk menentukan bagaimana *bit-bit* data dikelompokkan menjadi format yang disebut sebagai *frame*. *Frame-frame* tersebut di transmisikan secara berurutan dan memproses *acknowledgement frame* yang dikirim. Selain itu, pada *level* ini terjadi koreksi kesalahan (*error notification*), pemesanan pengiriman data (*flow control*), pengalamatan perangkat keras (seperti halnya MAC *address*), dan menentukan bagaimana perangkat-perangkat jaringan seperti *hub*, *bridge*, *repeater*, dan *switch* beroperasi.

3. Layer 3 – *Network Layer*

   Layer ini menyediakan koneksi dan pemilihan jalur antar dua sistem. *Network layer* adalah *layer* dimana *routing* terjadi, ketika sebuah paket diterima sebuah *interface router*, alamat IP tujuan akan diperiksa. Jika paket ditujukan untuk *router* tersebut, *router* akan melakukan pengecekan alamat *network* tujuan pada *routing table* yang dimilikinya. Pada saat *router* memilih *interface* keluar untuk paket tersebut, paket akan dikirimkan ke *interface* tersebut untuk dibungkus menjadi *frame* data dan dikirimkan keluar ke jaringan lokal. Jika *router* tidak menemukan *entry* untuk jaringan tujuan di *routing table*, *router* akan membuang paket tersebut.

4. Layer 4 – *Transport Layer*

   Layer ini bertanggung jawab untuk menjaga komunikasi jaringan antara *node*. Transport layer menyediakan mekanisme untuk membangun, memelihara, dan memutuskan *virtual circuit*, deteksi dan pemulihan kesalahan pengiriman dan pengendali aliran informasi. *Transport layer* melakukan segmentasi dan menyatukan kembali data yang tersegmentasi tadi menjadi sebuah arus data. Layanan-layanan yang terdapat di transport layer melakukan baik segmentasi maupun penyatu kembali daya yang tersegmentasi tersebut (*reassembling*), dari aplikasi-aplikasi *upper-layer* dan menggabungkannya kedalam arus data yang sama. Layanan-layanan ini menyediakan layanan

transportasi data dari ujung ke ujung, dan dapat membuat sebuah koneksi logikal antara *host* pengirim dan *host* tujuan pada sebuah *internetwork*. Pada transport *layer*, proses pengiriman data berupa segment dengan menggunakan *protocol* TCP dan UDP.

5. Layer 5 – *Session Layer*

   Layer ini membangun, mengatur dan memutuskan sesi antara aplikasi dan mengatur pertukaran data antara entitas *presentation layer*. *Session layer* juga menyediakan kontrol dialog antar peralatan atau titik jaringan (*node*). Ia melakukan koordinasi antar sistem-sistem dan mengorganisasi komunikasinya dengan menawarkan tiga mode berikut: *simplex, half-duplex, full-duplex*. Kesimpulannya, *session layer* pada dasarnya menjaga terpisahnya data dari aplikasi yang satu dengan data dari aplikasi yang lain.

6. Layer 6 – *Presentation Layer*

   Layer ini memastikan informasi yang dikirim oleh *application layer* dari suatu sistem dapat dimengerti oleh *application layer* di sistem lain. *Application layer* juga berhubungan dengan struktur data yang digunakan oleh program-program dan menegosiasikan sintaks pengiriman data untuk *application layer*. *Layer* ini pada dasarnya adalah penerjemah dan melakukan fungsi pengkodean dan konversi. Teknik *transfer* data yang berhasil adalah dengan mengadaptasi data

tersebut ke dalam format yang standar sebelum dikirimkan. Komputer dikonfigurasi untuk menerima format yang standar atau generik ini untuk kemudian diubah kembali ke bentuk aslinya untuk dibaca oleh aplikasi bersangkutan.

7. Layer 7 – *Application Layer*

   Application layer merupakan layer teratas dari model OSI. Layer ini menyediakan layanan untuk proses aplikasi (seperti e-*mail*, *file transfer*, dan *terminal emulation*) yang berada di luar model OSI. *Application layer* mengidentifikasi dan membangun ketersediaan pasangan komunikasi yang diinginkan (dan sumber daya yang dibutuhkan untuk terhubung bersamanya), menyesuaikan aplikasi yang berhubungan dan membangun kesepakatan pada prosedur pemulihan kesalahan dan pengendali integritas data. *Layer* ini merupakan tempat dimana *user* atau pengguna berinteraksi dengan komputer. Layer ini sebenarnya hanya berperan ketika dibutuhkan akses ke *network*.

2.1.5.2 Model Referensi TCP/IP

Gambar 2.7 TCP/IP *Layer Model*

TCP/IP diciptakan oleh Departemen Pertahanan Amerika Serikat, dan dibuat karena Departemen Pertahanan Amerika Serikat ingin mendesain sebuah jaringan yang dapat bertahan dalam berbagai kondisi termasuk dalam perang nuklir, dan juga transmisi dari paket setiap waktu dan di dalam kondisi apapun. Protokol ini adalah standar komunikasi data yang digunakan oleh komunitas *internet* dalam proses tukar-menukar data antar komputer dalam jaringan internet. Protokol ini tidak dapat berdiri sendiri, karena protokol ini berupa kumpulan protokol (*protocol suite*). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut diimplementasikan dalam bentuk perangkat lunak (*software*) di

sistem operasi. Istilah yang diberikan kepada perangkat lunak ini adalah TCP/IP *stack*.

Protokol TCP/IP dikembangkan pada akhir decade 1970-an hingga awal 1980-an sebagai sebuah protokol standar untuk menghubungkan komputer-komputer dan jaringan 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 dimana saja. Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut sebagai alamat IP (IP *Address*) yang mengizinkan hingga beberapa ratus 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 berbeda (seperti *Microsoft Windows* dan keluarga *UNIX* atau *Linux*) untuk membentuk jaringan yang heterogen.

Model TCP/IP mempunyai 4 *layer*, yaitu : *application layer*, *transport layer, internet layer,* dan *network access layer*. Beberapa *layer* pada model TCP/IP mempunyai nama yang sama dengan model OSI. Berikut penjelasan mengenai *layer* pada protokol TCP/IP :

1. Layer 1 – *Network Access layer*

   Network Access Layer mengizinkan sebuah paket *internet protocol* (IP) untuk membuat *physical link* ke dalam *network media*. *Drivers* untuk aplikasi *software*, *modem cards*, dan *device* yang lain beroperasi pada *layer network access*. *Network access layer*

menjelaskan langkah-langkah yang digunakan dengan perangkat keras jaringan dan pengaksesan medium transmisi.

Network access layer protocol juga memetakan IP *address* ke alamat *physical address* dan mengenkapsulasi paket IP kedalam *frame-frame*. *Network access layer* juga mendefinisikan koneksi media *physical* berdasarkan tipe perangkat keras dan alat jaringan.

2. Layer 2 – *Internet Layer*

Tujuan utama dari *internet layer* adalah untuk memilih jalur terbaik pada *network* untuk pengiriman paket. Protokol utama yang bekerja pada *layer* ini adalah *internet protocol* (IP). Pemilihan jalur terbaik dan paket-*switching* terjadi pada *layer* ini.

Jenis-jenis protokol yang bekerja pada TCP/IP *internet layer* :

- *Internet Control Message Protocol* (ICMP) menyediakan kemampuan kontrol dan pesan.
- *Address Resolution Protocol* (ARP) menentukan alamat dari data *link layer* atau MAC *address* untuk IP *address* yang diketahui.
- *Reverse Address Resolution Protocol* (RARP) menentukan IP *address* untuk MAC *address* yang diketahui.

3. Layer 3 – *Transport Layer*

Transport Layer menyediakan sebuah *logical connection* antara alamat sumber dan alamat tujuan. *Protocol transport* membagi

dan mengumpulkan data yang dikirimkan oleh *application layer* atas ke dalam aliran data yang sama atau *logical connection*.

Tugas utama dari *transport layer* adalah untuk menyediakan *end-to-end control* dan dapat diandalkan sebagai data travel melalui media komunikasi. *Transport layer* juga menjelaskan *end-to-end connectivity* antara aplikasi *host*. *Protocol transport layer* adalah TCP dan UDP.

- *Transmission Control Protocol* (TCP)

  TCP berfungsi untuk mengubah suatu blok data yang besar menjadi segmen-segmen yang diberi nomor dan disusun secara berurutan agar si penerima dapat menyusun kembali segmen-segmen tersebut seperti pada waktu pengiriman. TCP ini adalah jenis protokol *connection oriented* yang memberikan layanan bergaransi.

- *User Datagram Protocol* (UDP)

  UDP adalah jenis protokol *connectionless oriented*. UDP bergantung pada lapisan atas untuk mengontrol kebutuhan data. Oleh karena penggunaan *bandwidth* yang efektif, UDP banyak dipergunakan untuk aplikasi-aplikasi yang tidak peka terhadap gangguan jaringan seperti SNMP dan TFTP.

4. Layer 4 – *Application Layer*

Application Layer menangani *high-level protocol*, representasi, *encoding* dan *dialog control*. TCP/IP mengkombinasikan semua aplikasi yang berhubungan dengan *issue* menjadi satu *layer*. Ini menjamin bahwa data yang di paket secara baik sebelum dikirim ke *layer* berikutnya. Jenis-jenis protokol pada *application layer:*

- *File Transfer Protocol* (FTP)

  FTP dapat diandalkan, servis *connection oriented* menggunakan TCP untuk mengirimkan *file* melalui sistem yang mendukung FTP.

- *Trivial File Transfer Protocol* (TFTP)

  TFTP adalah servis *connectionless* yang menggunakan UDP. TFTP digunakan pada *router* untuk mengirimkan *file* konfigurasi dan *Cisco images* dan juga untuk mengirimkan *file* antar sistem yang mendukung TFTP.

- *Network File System* (NFS)

  NFS adalah *protocol file system* yang terdistribusi yang dikembangkan oleh *Sun Microsystems* yang mengizinkan *file* untuk mengakses ke sebuah *remote storage device* seperti *hard disk*.

- *Simple Mail Transfer Protocol* (SMTP)

  SMTP mengadministrasikan transmisi dari *email* melalui jaringan komputer dan tidak menyediakan support untuk transmisi data lain selain *plain-text*.

- *Telnet*

  Telnet menyediakan kemampuan untuk mengendalikan akses komputer lain. Ini memungkinkan sebuah *user* untuk *login* ke dalam sebuah *internet host* dan mengeksekusi perintah. *Telnet client* ditunjuk sebagai sebuah *local host* dan *telnet server* ditunjuk sebagai sebuah *remote host.*

- *Domain Name System* (DNS)

  DNS adalah sebuah sistem yang digunakan dalam *internet* untuk menterjemahkan *domain name* dan *network node* ke dalam IP *address*.

2.1.5.3 Perbedaan dan Persamaan antara OSI *Layer* dan TCP *Layer*

Osi *layer* dan TCP *layer* mempunyai beberapa perbedaan yaitu:

- *Layer session, presentation,* dan a*pplication* yang terdapat pada OSI *layer* digabungkan menjadi satu *layer* pada TCP *layer* yang dinamakan *application layer*.
- *Layer data link* dan *physical* yang terdapat pada OSI *layer* digabungkan menjadi satu *layer* pada TCP *layer* yang dinamakan *network access layer*.
- Model TCP/IP lebih sederhana dalam pembaguan *layernya.*

Selain itu juga terdapat persamaan antara OSI *layer* dan TCP *layer*, yaitu :

- Keduanya mempunyai *layer*

- Keduanya mempunyai *application layer* walaupun mempunyai *service* yang berbeda.
- Keduanya mempunyai *paket-switched* dalam proses pengiriman data.

2.1.6 IPv4 *Addressing*

IP *address* adalah sebuah rangkaian 32-bit yang terdiri dari angka 1 dan 0. Untuk membuat IP *addres* lebih mudah diingat biasanya ditulis dengan 4 angka desimal yang dipisahkan dengan sebuah tanda titik. Sebagai contoh, IP *address* dari sebuah komputer adalah 192.168.1.2 dan disebut dengan format desimal. Setiap bagian dari alamat ini disebut dengan *octet* karena dibuat dari delapan digit *binary*. Seperti contoh 192.168.1.6 dalam bilangan *binary* adalah 11000000.10101000.00000001.00000110 .

Baik bilangan *binary* dan desimal mempresentasikan nilai yang sama. Namun IP *address* lebih mudah dimengerti dalam notasi bilangan desimal. Salah satu masalah dengan penggunaan bilangan *binary* adalah pengulangan bilangan 0 dan 1 yang panjang akan membuat faktor terjadinya suatu kesalahan semakin besar.

Setiap IP *address* mempunyai dua bagian. Bagian pertaman menandakan jaringan dimana *host* terkoneksi dan bagian kedua menandakan *host*, masing-masing *octet* tersusun dari angka 0-255.

IP *address* dibagi menjadi kelas-kelas untuk menetapkan besar kecilnya suatu jaringan. *Class* A ditetapkan untuk ukuran jaringan yang besar. *Class* B ditetapkan

untuk ukuran jaringan yang medium atau menengah dan *Class* C digunakan untuk ukuran jaringan yang lebih kecil. Langkah pertama yang digunakan untuk menentukan bagian dari *address* yang menandakan jaringan dan bagian mana yang menandakan *host* adalah dengan mengetahui jenis kelas dari IP tersebut.

2.1.6.1 Pembagian *Class* IP *Address*

1. *Class* A *address*

   Class A didesain untuk mendukung jaringan yang besar, dengan jumlah lebih dari 16 juta *host address* yang tersedia. IP *address class* A hanya menggunakan oktet yang pertama untuk menunjukan *network address*, dan tiga oktet sisanya tersedia untuk *host address*.

   Bit pertama dari *class* A *address* adalah 0. Dengan bit pertama adalah 0 maka angka terendah yang dapat direpresentasikan adalah 00000000 dalam biner sedangkan dalam bilangan desimal adalah 0. Dan angka tertinggi yang dapat direpresentasikan adalah 01111111 dalam bilangan biner dan dalam bilangan desimal adalah 127. Angka 0 dan 127 tidak dapat digunakan, serta IP *address* 127.0.0.0 tidak dapat digunakan karena dipakai untuk *loopback* testing, maka alamat IP *address* yang oktet pertamanya dimulai dengan angka 1 sampai 126 di dalam oktet pertama adalah alamat *class* A.

2. *Class* B *Address*

Class B *address* didesain untuk mendukung kebutuhan jaringan dengan ukuran menengah sampai dengan ukuran yang besar. Sebuah IP *address class* B menggunakan dua oktet pertama dari empat oktet untuk menunjukan *network address*, dan sisanya menunjukan *host address*.

Dua *bit* pertama dari oktet pertama *class* B selalu 10. Sisa dari itu enam *bit* berikutnya diisi baik oleh 0 maupun 1, oleh karena itu angka terendah yang dapat direpresentasikan dalam bilangan biner adalah 10000000 dan dalam bilangan desimal adalah 128, sedangkan angka tertinggi yang dapat direpresentasikan dalam bilangan biner adalah 10111111 dan dalam bilangan desimal adalah 191. *Address* IP yang oktet pertamanya dimulai dengan angka 128-191 adalah alamat *class* B.

3. *Class* C *Address*

Class C *address* adalah kebanyakan yang dipakai untuk alamat *address* yang sebenarnya. Alamat ini dimaksudkan untuk mendukung jaringan kecil dengan jumlah maksimum 254 host.

Class C dimulai dengan bilangan biner 110. Oleh karena itu, angka terendah yang dapat direpresentasikan adalah 11000000 dalam bilangan biner dan dalam bilangan desimal adalah 192, sedangkan angka tertinggi yang dapat direpresentasikan adalah 11011111 dalam

bilangan biner dan dalam bilangan desimal adalah 223. *Address* IP yang oktet pertamanya dimulai dengan angka 192-223 adalah alamat *class* C.

4. *Class* D *Address*

Class D *address* diciptakan untuk memungkinkan *multicasting* di dalam suatu OP *address*. *Multicast address* adalah *network address* unik yang menunjukan paket dengan *address* tujuan ke group *predefined* dari sebuah IP *address*, oleh karena itu *single unit* dapat mentransmisi aliran tunggal dari data secara simultan ke penerima lebih dari satu.

Class D *address* dimulai dengan bilangan biner 1110. Oleh karena itu, angka terendah yang dapat direpresentasikan adalah 11100000 dalam bilangan biner dan dalam bilangan desimal adalah 224, sedangkan angka tertinggi yang dapat direpresentasikan adalah 11101111 dalam bilangan biner dan dalam bilangan desimal adalah 239. *Address* IP yang oktet pertamanya dimulai dengan angka 224-239 adalah alamat *class* D.

5. *Class* E *Address*

Class E *address* telah ditetapkan, namun *Internet Engineering Task Force* (IETF) menetapkan *address* ini untuk keperluan riset, oleh karena itu tidak ada IP di *class* E *address* yang dikeluarkan untuk

digunakan dalam *internet*. Empat *bit* pertama dari *class* E *address* selalu di set menjadi 1111. Oleh karena itu, *range* oktet pertama untuk *class* E *address* adalah 11110000 sampai 11111111 dalam bilangan biner atau 240 sampai 255 dalam bilangan desimal.

2.1.6.2 *Public* dan *Private* IP *Address*

Public IP *address* sangat unik, tidak ada dua *device* yang dapat terhubung ke sebuah *public network* dengan IP *address* yang sama karena *public* IP *address* adalah global dan distandarisasi.

Dengan perkembangan *internet* yang begitu pesat, *public* IP *address* makin lama makin menipis. Skema *addressing* yang baru seperti *Classless Interdomain Routing* (CIDR) dan IPv6 dikembangkan untuk memecahkan masalah tersebut.

Private IP *address* adalah salah satu solusi untuk masalah kesulitan di masa yang akan datang dari *public* IP *address*. Seperti yang kita ketahui, *public network* mengharuskan *host* untuk memiliki IP *address* yang unik, namun *private networks* yang tidak terhubung ke *internet* boleh menggunakan *host address* yang mana saja, selama tiap *host* pada *private network* berbeda satu sama lain.

Banyak *private network* berada di antara jalur *public network*, namun *private network* dengan menggunakan *address* yang mana saja tidak disarankan karena mungkin saja *network* tersebut terhubung dengan *internet*.

RFC 1918 menetapkan tiga blok dari IP *address* untuk *private*, tiga blok terdiri dari *class* A, *class* B dan *class* C.

1. *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*.

2. *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* ini 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 di dalam *range* private IP *address* dan IP *looback* (127.*.*.*).

2.1.6.3 Jenis IP *Addresing*

Alamat IP terbagi lagi menjadi beberapa jenis, yaitu:

1. Alamat *Unicast*

   Merupakan alamat IPv4 yang ditentukan sebuah *interface* jaringan yang dihubungkan ke sebuah *internetwork* IP. Alamat *unicast* digunakan dalam komunikasi *point-to-point* atau *one-to-one.*

2. 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.*

3. 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.*

2.2 Teori Khusus

2.2.1 *Virtual Private Network* (VPN)

Menurut Stallings (2003) *Virtual Private Network* (VPN) adalah sebuah jaringan *private* yang dibuat di jaringan *public* dengan menggunakan *internet* sebagai

media komunikasinya. VPN dapat mengirim data antara dua komputer yang melewati jaringan *public* sehingga seolah-olah terhubung secara *poin-to-point*. Data di enkapsulasi dengan *header* yang berisi informasi *routing* untuk mendapatkan koneksi *point-to-point* sehingga data dapat melewati jaringan publik dan dapat mencapai tujuan akhir.

Sedangkan untuk mendapatkan koneksi bersifat *private*, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi. Proses enkapsulasi data sering disebut *tunneling*.

Anda dapat mengakses *server* kantor melalui VPN dimana saja, entah itu dirumah ataupun dijalan secara aman meskipun anda menggunakan infrastruktur jaringan *internet* dalam penggunaannya. Menurut pandangan *user*, koneksi VPN merupakan koneksi *point-to-point* antara *user* komputer dengan *server* korporasi dan data terkirim di atas jaringan *dedicated*, padahal kenyataannya tidak demikian.

2.2.2 Fungsi VPN

Teknologi VPN menyediakan tiga fungsi utama dalam penggunaanya, yaitu

1. 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 tidak berhak dapat mengakses dan membaca data dalam jaringan anda dengan mudah.

2. Keutuhan Data

   Ketika melewati jaringan *internet*, data sebenarnya sudah berjalan sangan jauh melintasi berbagai Negara. Di tengah perjalanannya, apapun bisa terjadi terhadap isinya baik itu hilang, rusak, bahkan dimanipulasi isinya oleh orang yang tidak bertanggung jawab. VPN memiliki teknologi yang dapat menjaga keutuhan data yang dikirim agar sampai ke tujuannya tanpa cacat, hilang, rusak, ataupun dimanipulasi oleh orang lain.

3. 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 autentikasunya 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.

2.2.3 Cara Kerja VPN

Hal utama yang dibutuhkan oleh sebuah VPN untuk bekerja adalah adanya koneksi *internet* yang baik. Kemudian juga diperlukan *internet gateway router* untuk

melakukan *setting* akses *internet* bagi para *staff*. Router ini dikonfigurasikan untuk melindungi jaringan lokal perusahaan atau organisasi dari orang yang tidak berhak mengaksesnya melalui *internet*. Dapat juga dikatakan *router* ini berfungsi sebagai *firewall*.

Kemudian *software* VPN di *install* pada *router* yang berfungsi sebagai *firewall* ini. Kemudian dikonfigurasikan agar dapat tersambung dan tercipta sebuah koneksi *virtual*. Jika tahap ini sukses maka dua atau lebih jaringan perusahaan atau kantor sudah dapat terhubung melalui jaringan *virtual* (*internet*) layaknya jaringan nyata. Sudah dapat saling mengirim data dan saling mengakses jaringan, namun belum menjadi jaringan *private* karena belum terlindungi, sehingga orang lain yang memakai *internet* juga dapat mengambil data yang dikirim melalui jaringan ini.

Untuk menjadikan jaringan ini menjadi sebuah jaringan yang *private*, maka solusinya adalah dengan menggunakan enkripsi. *Traffic* VPN antara dua atau lebih perusahaan/kantor yang menggunakan VPN di kunci dengan enkripsi, dan hanya komputer atau orang yang berhak saja yang dapat membuka kunci dan melihat data yang dikirim dengan enkripsi tersebut. Data yang dikirim akan dienkripsi terlebih dahulu, lalu setelah sampai pada tujuan akan di dekripsi. Enkripsi menjaga data tetap aman dalam jaringan internet yang begitu luas. Seperti terowongan kereta yang melewati gunung atau bawah tanah. Enkripsi menjaga transfer data tetap aman melalui media *internet* yang luas. Menciptakan terowongan *virtual*, jalur *private*, atau yang lebih dikenal dengan teknologi *tunneling*.

Jadi VPN adalah jaringan virtual yang menggunakan *internet* sebagai media perantara yang dibangun di antara dua *internet access router* yang dilengkapi dengan

firewall dan *software* VPN. *Software* harus di *install* di masing-masing *router* yang berfungsi sebagai penghubung, *firewall* harus di *setting* untuk pemberian akses, dan pertukaran data melalui VPN harus di enkripsi. Enkripsi harus diberikan pada semua *partner* yang menggunakan VPN, sehingga pertukaran data hanya dapat dilakukan dan diterima oleh *partner* yang berhak saja.

2.2.4 Jenis-Jenis VPN

1. *Remote Access* VPN

   Remote Access VPN memungkinkan akses kapan saja dimana saja ke jaringan perusahaan/kantor. Jaringan ini biasa digunakan atau diminta oleh pegawai perusahaan yang berpergian jauh tetapi ingin selalu terhubung dengan jaringan perusahaannya. Biasanya perusahaan yang ingin membuat jaringan VPN tipe ini akan bekerja sama dengan *Enterprise Service Provider* (ESP). ESP akan memberikan suatu *Network Access Server* (NAS) bagi perusahaan tersebut. ESP juga akan menyediakan *software* klien untuk komputer-komputer yang digunakan pegawai perusahaan tersebut.

   Untuk mengakses jaringan lokal perusahaan, pegawai tersebut harus terhubung ke NAS dengan men-dial nomor telepon yang sudah ditentukan. Kemudian dengan menggunakan *software* klien, pegawai tersebut dapat terhubung ke jaringan lokal perusahaan.

   Perusahaan yang memiliki pegawai yang ada di lapangan dalam jumlah besar dapat menggunakan *remote access* VPN untuk membangun

WAN. VPN tipe ini akan memberi keamanan, dengan mengenkripsi koneksi antara jaringan lokal perusahaan dengan pegawainya yang ada di lapangan. Pihak ketiga yang melakukan enkripsi ini adalah ISP.

2. *Site-to-Site* VPN

Site-to-Site VPN disebut juga *router-to-router* VPN merupakan salah satu alternatif infrastruktur WAN yang biasa digunakan. VPN jenis ini mengubungkan dua atau lebih kantor cabang, kantor pusat, ataupun *partner* bisnis ke seluruh jaringan perusahaan. *Site-to-site* terbagi menjadi dua, yaitu:

a. *Intranet* VPN

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

b. *Extranet* VPN

Extranet VPN digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lainnya (contohnya mitra kerja, pelanggan, atau *supplier*)

2.2.5 Topologi VPN

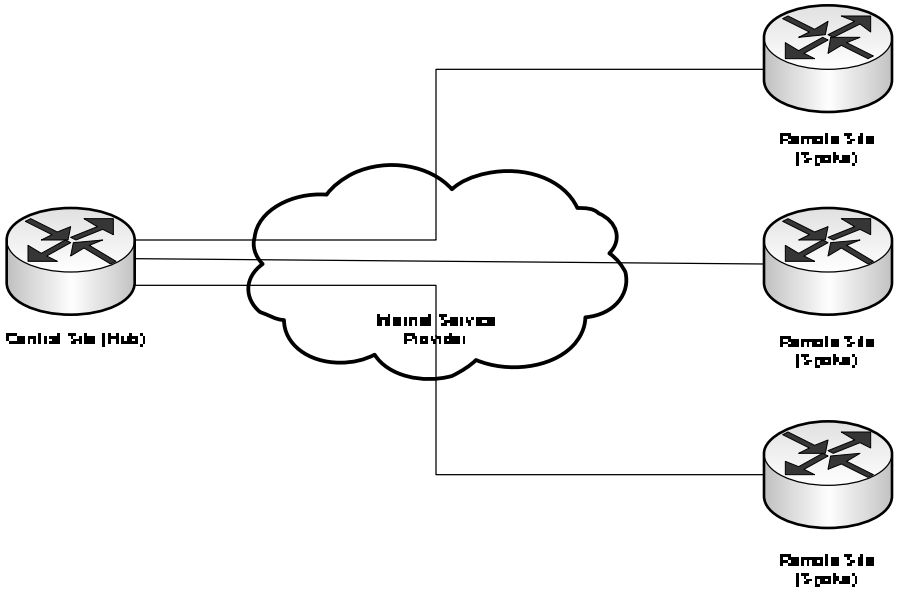
Topologi VPN biasa dibuat berdasarkan dengan proses bisnis yang ada dan sedang berjalan di suatu perusahaan. Tetapi ada beberapa topologi VPN yang sudah cukup terkenal dan biasa di pakai di berbagai perusahaan. Topologi yang sejenis dapat memecahkan berbagai macam masalah bisnis di

industri yang berbeda-beda. Topologi VPN dapat dikelompokan menjadi tiga kategori, yaitu *hub-and-spoke, partial atau full-mesh,* dan *hybrid*

1. Topologi *Hub-and-spoke*

   Topologi yang biasa ditemui adalah topologi ini, dimana beberapa *remote office (spokes)* terhubung dengan sebuah *central site* (*hub*). *Remote offices* biasanya dapat bertukar data tanpa ada batas keamanan secara explisit di dalam satu kantor, tetapi jumlah data yang ditukarkan bisa diabaikan. Topologi ini biasa dipakai di organisasi dengan struktur hierarki yang ketat seperti antara bank dengan kantor cabang yang lebih kecil.

   Topologi *hub-and-spoke* cocok untuk lingkungan dimana *remote offices* banyak bertukar data dengan *central site*, tetapi tidak antar *remote offices*. Pertukaran data antar *remote offices* selalu dikirim melalui *central site*.



Gambar 2.8 Topologi *Hub-and-Spoke*

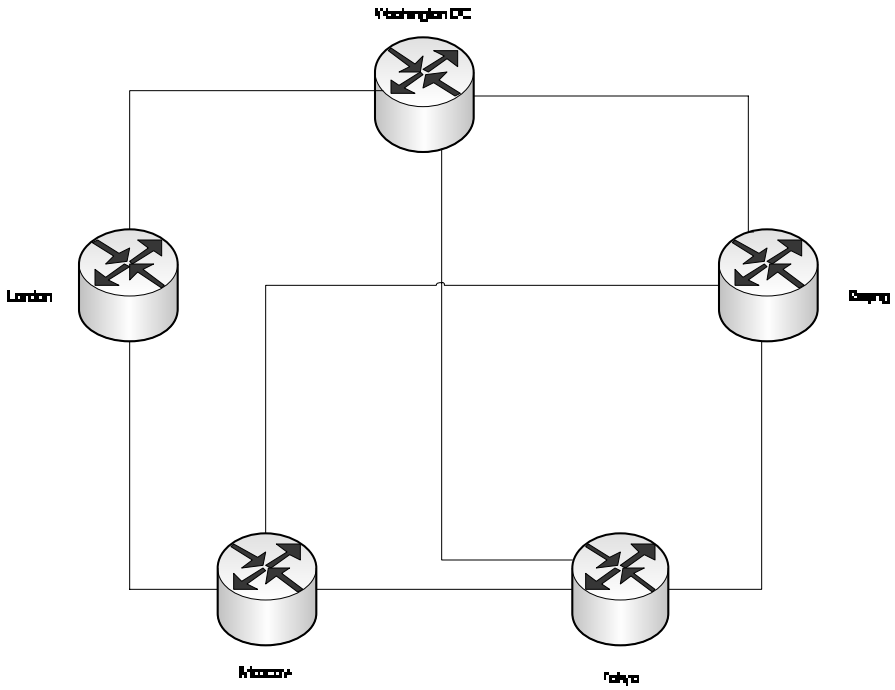
2. Topologi *Partial* atau *Full Mesh*

Topologi *hub-and-spoke* di atas tidak semua konsumen dapat mengimplementasikannya di jaringan mereka karena berbagai alasan seperti:

- Perusahaan yang mungkin kurang terorganisir strukturnya
- Pertukaran data terjadi diberbagai tempat di perusahaan
- Aplikasi yang digunakan dalam perusahaan membutuhkan komunikasi *peer-to-peer* seperti *messaging*.
- Untuk perusahaan multinasional, biaya topologi *hub-and-spoke* sangat tinggi karena lintas negara.

Untuk itu, topologi VPN lain yang bisa digunakan adalah topologi *partial* atau *full-mesh*, dimana site VPN terhubung dengan VC diatur oleh kebutuhan trafik. Jika semua tempat tidak saling terhubung secara

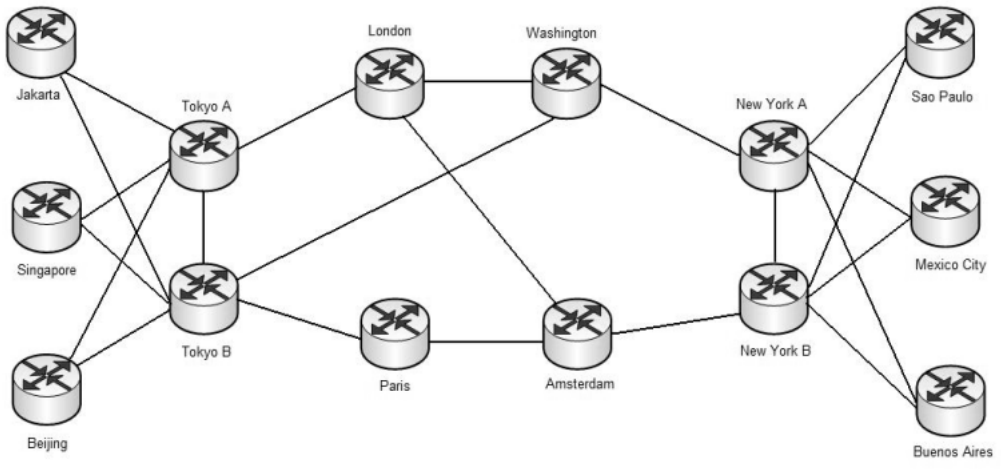
langsung ke berbagai tempat lain, topologi ini disebut *partial mesh*, tetapi jika semua tempat saling terhubung ke semua tempat lain maka topologi ini disebut *full mesh*.



Gambar 2.9 Topologi *Partial Mesh*

3. Topologi *Hybrid*

Jaringan VPN yang besar biasanya menggunakan gabungan antara topologi *hub-and-spoke* dengan *partial-mesh*. Sebagai contoh perusahaan multinasional yang besar mungkin mengakses jaringan di tiap negara yang terhubung dengan topologi *hub-and-spoke*, dan jaringan pusat internasional dihubungkan dengan topologi *partial-mesh*.



Gambar 2.10 Topologi *Hybrid*

2.2.6 VPN *Security*

Ada tiga hal dalam pengamanan IT dan juga berlaku dalam VPN yang harus selalu dimiliki:

1. *Privacy (Confidentiality)*

   Data yang dikirimkan hanya dapat dibuka/diakses oleh yang berhak

2. *Reliability (Integrity)*

   Data yang dikirimkan tidak boleh mengalami perubahan dari pengirim data ke penerima data.

3. *Availability*

   Data yang dikirimkan harus tersedia ketika dibutuhkan.

Semua tujuan ini harus dicapai dengan menggunakan *software*, *hardware*, ISP, dan kebijakan keamanan yang tepat. Keamanan VPN itu sendiri dapat dicapai dengan

menjaga lalu lintas (*traffic*), metode enkripsi yang kuat, teknik otentikasi yang aman, dan *firewall* yang mengatur *traffic* ke dan dari *tunnel*.

a. Enkripsi

Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti. Dengan enkripsi, kita mengubah isi dari data yang kita kirim sehingga data tersebut tidak dapat dibaca oleh orang yang tidak berhak mendapatkannya. Informasi yang tidak diacak disebut *clear-text* sedangkan yang sudah diacak disebut *cipher-text*. Di setiap tunnel VPN terdapat VPN *gateway*. *Gateway* tempat pegiriman data mengenkripsi atau mengubah informasi *clear-text* menjadi *cipher-text* sebelum dikirim melalui *tunnel* ke *internet*. VPN *gateway* di tempat penerima mendeskripsi atau mengubah *cipher-text* tersebut kembali menjadi *clear-text*.

Enkripsi terdiri dari dua jenis, yaitu *symmetric encryption* dan *asymmetric encryption*. *Asymmetric encryption* menggunakan *public* dan *private key* dalam proses enkripsi dan dekripsi, sedangkan *symmetric encryption* menggunakan *key* yang sama dalam proses enkripsi dan dekripsi. Berikut merupakan metode-metode *encryption* :

1. *Symmetric Encryption*

Symmetric key encryption menggunakan *private key* berarti komputer pengirim dan penerima sama-sama menggunakan kunci yang sama untuk mengenkripsi dan

mendekripsi informasi. Karena satu *key* digunakan bersama-sama untuk enkripsi dan dekripsi, maka harus ada pengertian antara kedua pihak untuk menjaga kerahasiaan *key* tersebut.

Semua yang mempunyai kunci enkripsi dapat mendekripsi data apa saja yang ada dalam lalu lintas VPN. Jika orang yang tak berwenang memiliki kunci enkripsi, ia dapat mendekripsi data yang ada dan masuk ke setiap jaringan yang terhubung melalui VPN. Selain itu kunci enkripsi juga dapat dibuka dengan melakukan *brute force attack*. Hanya masalah waktu sampai sang *attacker* dapat membuka kunci enkripsi.

Oleh karena itu, *software* VPN seperti *IPsec* mengganti kunci enkripsi secara berkala dalam suatu interval waktu. Setiap kunci enkripsi hanya berlaku dalam jangka waktu tertentu.

IPsec, teknologi VPN yang paling sering digunakan mempunyai protokol penggantian kunci enkripsi sendiri. Protokol ini diberi nama *Internet Key Exchange* (IKE). Dalam klasik VPN yang menggunakan *symmetric key*, ada beberapa lapis otentikasi, pergantian kunci, dan enkripsi atau dekripsi. Dibawah ini adalah tiga langkah dari VPN yang menggunakan *symmetric encryption*

- Pengirim dan penerima harus saling melakukan otentikasi satu sama lain

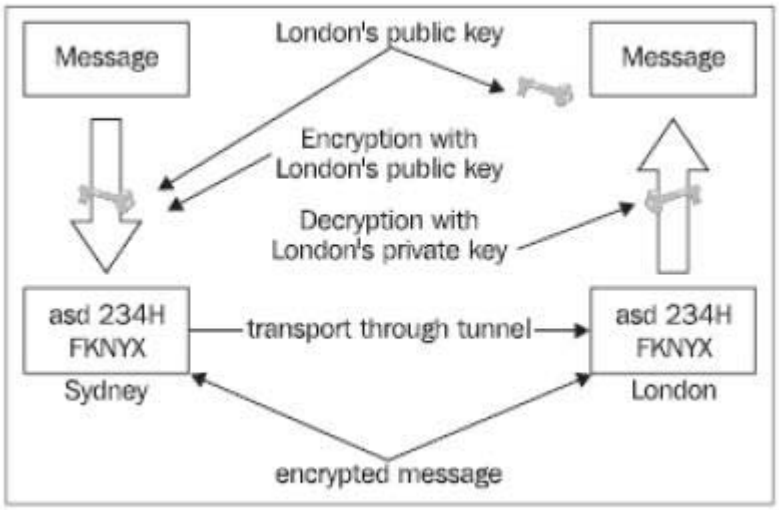
- Mereka harus saling setuju dalam metode pengenkripsian
- Mereka harus saling setuju dalam metode penggantian kunci

Hal inilah yang menjadikan VPN sedikit lebih kompleks dan sulit.

2. *Asymmetric Encryption*

Asymmetric key encryption mengenkripsi informasi dengan suatu *key* dan mendekripsi dengan *key* lainnya. Sistem ini menggunakan kombinasi dari dua buah *key*, yaitu *private key* yang disimpan untuk diri sendiri, dan *public key* yang diberikan untuk *remote user*.

SSL/TLS menggunakan salah satu metode pengenkripsian *asymmetric encryption* ini untuk memastikan identifikasi dari masing-masing pengguna VPN.



Gambar 2.11 *Assymetric Encryption*

Pada contoh diatas sebuah pesan di enkripsi di Sidney mengunakan *public key* dari London. Hasil dari enkripsi tersebut berupa kode dikirim ke London yang hanya dapat dibuka menggunakan London *private key*.

Prosedur yang sama dapat juga dilakukan untuk melakukan otentikasi. London mengirim sejumlah angka *random* ke Sidney, dimana akan di *encode* si Sidney menggunakan *private key* dan dikirim kembali. Di London, menggunakan Sidney *public key* angka tersebut dapat di *decode*. Jika angka yang dikirimkan kembali benar, maka pasti yang mengirim kembali adalah pemegang *private key* Sidney. Sistem ini disebut *digital signature*.

b. Autentikasi

Selain enkripsi, salah satu aspek penting dalam VPN, yaitu memastikan identitas suatu *user* (*user authentication*) dan data sampai tanpa adanya kerusakan atau modifikasi (*Data Authentication*).

1. *User Authentication*

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

a. *Pre-Shared Key*

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

b. *Digital Signatures*

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

c. *Hybrid Mode Authentication*

Hybrid Mode Authentication memperbolehkan organisasi untuk mengintegrasikan sistem *authentication* seperti *SecureID*, TACACA+, dan RADIUS dengan VPN.

2. Data *Authentication*

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

c. 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 autorisasi inilah yang menentukan apakah pengguna

tersebut dapat melanjutkan perintah atau tugas yang dikehendakinya pada jaringan VPN tersebut.

d. Firewall

Firewall merupakan suatu cara, sistem, ataupun mekanisme yang diterapkan baik terhadap *software*, *hardware*, 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 LAN.

1. Karakteristik *Firewall*

   Ada beberapa karakteristik yang harus dimiliki oleh suatu *firewall* sehingga *firewall* tersebut dapat dikatakan aman, diantaranya:

   - 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*.
   - Hanya kegiatan yang terdaftar/dikenal yang dapat melewati hubungan. Hal ini dapat dilakukan dengan mengatur *policy* pada konfigurasi keamanan lokal

- *Firewall* itu sendiri haruslah kebal atau relatif kuat terhadap serangan. Hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan sistem operasi yang relatif aman.

2. Teknik yang Digunakan pada *Firewall*

   a. *Service Control* (kendali terhadap layanan)

      Service control melakukan penyaringan berdasarkan tipe-tipe layanan yang digunakan di *internet* dan boleh di akses baik untuk ke dalam maupun ke luar *firewall*. Biasanya *firewall* akan mengecek nomor IP *address* dan juga nomor *port* yang digunakan baik pada protokol TCP dan UDP, bahkan bisa dilengkapi *software* untuk *proxy* 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*.

   b. *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 dikarenakan 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.

e. 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 memperdulikan 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.

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 *Internet Engineering Task Force* (IETF). PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP *datagrams* agar dapat ditransmisikan melalui internet. PPTP juga dapat digunakan pada jaringan *private* 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 menggunakan 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. L2TP (*Layer 2 Tunneling Protocol*)

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

a. 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 perminataan dari klien, ISP tersebut membuatkan jalur khusus yang menghubungkan klien tersebut dengan VPN *server*-nya.

b. *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*.

Kelebihan L2TP dibandingkan PPTP

- *Multiple tunnels* antara *endpoints*, sehingga bisa ada beberapa jalur yang memiliki perbedaan *Quality of Service* (QoS).
- Mendukung kompresi
- Bisa melakukan *tunnel authentication*
- Bisa bekerja di jaringan *non*-IP seperti ATM dan *frame relay*
- *Vendor interopability*

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, integrity, replay protection,* dan *confidentiality* terhadap data. ESP melakukan pengamanan data terhadap segala sesuatu dalam paket data setelah header.