BAB 2

LANDASAN TEORI

2.1 Teori - Teori Umum

2.1.1 Definisi Jaringan Komputer

Menurut Tanenbaum, jaringan komputer merupakan penggabungan teknologi komputer dan berkomunikasi yang merupakan sekumpulan komputer berjumlah banyak yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya. (Tanenbaum,2003)

Jaringan komputer / *network* adalah sebuah sistem yang terdiri atas komputer dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama. Tujuan dari jaringan komputer adalah :

- Membagi sumber daya, misalnya membagi printer, CPU, memori ataupun harddisk.
- Komunikasi, misalnya *e-mail, instant messaging*, dan *chatting*.
- Akses informasi, misalnya *web browsing.*

2.1.2 Klasifikasi Jaringan Komputer

Berdasarkan daerah jangkauannya, jaringan dapat dibagi menjadi tiga macam, yaitu :

1. ***Local Area Network*** **(LAN)**

   Local Area Network adalah sejumlah komputer yang saling dihubungkan bersama di dalam satu areal tertentu yang

tidak begitu luas, seperti di dalam kantor atau gedung. *Local Area Network* memungkinkan pengguna untuk berbagi akses ke file-file yang sama dan menggunakan *printer* secara lebih efisien, serta membentuk komunikasi internal. Secara garis besar terdapat dua tipe jaringan atau LAN, yaitu jaringan *Peer-to-Peer* dan jaringan *Client-Server*. Pada jaringan *peer-to-peer*, setiap komputer yang terhubung ke jaringan dapat bertindak baik sebagai *workstation* maupun *server*. Sedangkan pada jaringan *Client-Server*, hanya satu komputer yang bertugas sebagai *server* dan komputer lain berperan sebagai *workstation*.

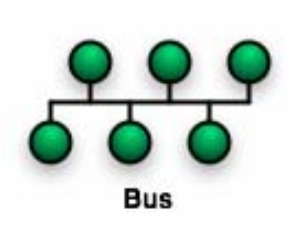
Topologi LAN

Topologi jaringan adalah bagian yang menjelaskan hubungan antar komputer yang dibangun berdasarkan kegunaan, keterbatasan *resource* dan keterbatasan biaya. Berarti topologi-topologi jaringan yang ada bisa disesuaikan dengan keadaan di lapangan.

- **Topologi *Bus***

  Merupakan sebuah arsitektur jaringan dimana satu set *client* terhubung pada satu kabel utama (*backbone*) yang dinamakan *bus*. Jaringan *bus* adalah cara yang paling sederhana untuk menghubungkan banyak *client*, namun masalah yang paling sering dihadapi adalah pada saat dua *client* akan mengirimkan data pada saat yang

bersamaan pada *bus* yang sama, dan juga apabila terdapat gangguan di sepanjang kabel pusat.



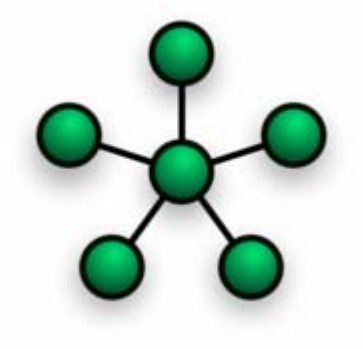
Gambar 2.1 Topologi *Bus*

- **Topologi *Star***

  Merupakan salah satu topologi yang paling umum digunakan. Jaringan *star* terdiri atas sebuah *switch* utama yang bertugas seperti *router* yang mentransmisikan data. Topologi star menyambungkan setiap *node* (komputer dan peralatan jaringan lainnya) ke *hub* atau *switch*. Data yang ditransmisikan harus melalui *hub* atau *switch* sebelum sampai ke *node* tujuannya. Kabel yang digunakan adalah *unshielded twisted pair* atau *fiber optic*.

  Keunggulan dari topologi tipe *Star* ini adalah bahwa dengan adanya kabel tersendiri untuk setiap *workstation* ke *server*, maka *bandwidth* atau lebar jalur komunikasi dalam kabel akan semakin lebar, sehingga akan meningkatkan kinerja jaringan secara keseluruhan. Dan juga bila terdapat gangguan di suatu jalur kabel, maka gangguan hanya akan terjadi dalam komunikasi

antara *workstation* yang bersangkutan dengan *server*, dan jaringan sercara keseluruhan tidak mengalami gangguan. Kelemahan dari topologi *Star* adalah kebutuhan kabel yang lebih besar dibandingkan dengan topologi lainnya.



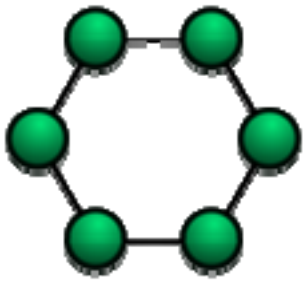
Gambar 2.2 Topologi *Star*

- **Topologi *Ring***

  Tipe dari topologi jaringan *ring* adalah masing-masing *node* dalam jaringan terhubung dengan dua *node* lainnya dalam jaringan yang sama, dan *node* pertama dan *node* terakhir juga terhubung satu sama lain, sehingga membentuk sebuah cincin (*ring*). Tiap *workstation* ataupun *server* akan menerima dan melewatkan informasi dari satu komputer ke komputer lain. Bila alamat-alamat yang dimaksud sesuai, maka informasi diterima, dan bila tidak, informasi akan dilewatkan. Semua data yang ditransmisikan diantara *node-node* di dalam jaringan

berjalan dari satu *node* ke *node* yang lain di dalam *circular manner* dan data mengalir dalam satu arah saja.

Kelemahan dari topologi ini adalah setiap *node* dalam jaringan akan selalu ikut serta mengelola informasi yang dilewatkan dalam jaringan, sehingga bila terdapat gangguan di suatu *node* maka seluruh jaringan akan terganggu. Keunggulan topologi *Ring* adalah tidak terjadinya *collision* atau tabrakan pengiriman data seperti pada topologi *Bus*, karena hanya satu *node* dapat mengirimkan data pada suatu saat.



Gambar 2.3 Topologi *Ring*

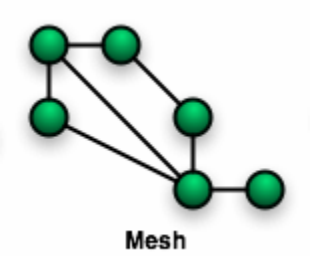
- **Topologi *Mesh***

Topologi *mesh* (berantakan) diimplementasikan untuk menyedia-kan sebanyak mungkin perlindungan dari interupsi pengiriman data. Sebagai contoh, pembangkit tenaga nuklir mungkin menggunakan topologi *mesh* ini. Topologi yang benar-benar dalam suatu sistem kendali

(*controlling*). Sebagaimana dapat dilihat dari gambar dibawah ini, setiap *host* mempunyai koneksi sendiri ke semua *host*. Meskipun *internet* mempunyai beberapa jalur ke semua lokasi, tetapi tidak mengadopsi topologi ini secara penuh.

Kerugian dari penggunaan topologi ini adalah penggunaan *ethernet* dan kabel yang banyak sehingga dibutuhkan dana yang besar.

Keuntungan dari penggunaan topologi ini adalah apabila ada salah satu jalur pada komputer putus, komputer masih dapat berhubungan dengan jalur yang lain.



Gambar 2.4 Topologi *Mesh*

Protokol LAN

Protokol adalah peraturan-peraturan yang dibuat agar peralatan jaringan komputer satu dengan yang lain dapat saling berkomunikasi dengan baik. Protokol -protokol yang dapat dipakai untuk jaringan LAN adalah protokol *Ethernet, Token*

Ring, FDDI, dan ATM.

Protokol *ethernet* merupakan protokol LAN yang paling banyak dipakai karena berkemampuan tinggi dengan biaya yang relatif murah. *Ethernet* pada mulanya mendukung jaringan berkecepatan 10 Mbps, tetapi dengan makin meningkatnya arus lalu lintas data jaringan LAN, maka diciptakan *protocol FastEthernet* yang berkecepatan 100 Mbps dan *Gigabit Ethernet* yang berkecepatan 1000 Mbps.

2. *Metropolitan Area Network* (MAN)

Jaringan ini lebih luas dari jaringan LAN dan menjangkau antar wilayah dalam suatu kota. Jaringan MAN menghubungkan jaringan-jaringan kecil yang ada, seperti LAN yang menuju pada linkungan area yang lebih besar. MAN biasanya menghubungkan jaringan kantor-kantor dalam suatu kota dengan pabrik/instansi atau dengan kantor pusat.

Menurut Tanenbaum, MAN mencakup area geografis sebuah kota seperti jasa televisi kabel dalam sebuah kota atau sebuah bank dengan banyak kantor cabang di satu kota. (Tanenbaum,2003)

3. *Wide Area Network* (WAN)

WAN adalah sebuah jaringan komputer yang jangkauannya mencakup daerah geografis yang luas, dan mampu menjangkau batas propinsi, sampai negara yang ada di belahan

bumi lain. WAN memungkinkan terjadinya komunikasi diantara dua perangkat yang terpisah jarak yang sangat jauh. WAN menginterkoneksikan beberapa LAN yang kemudian menyediakan akses ke komputer - komputer atau file *server* pada lokasi lain.

Menurut Tanenbaum, *Wide Area Network* merupakan jaringan yang memiliki luas jangkauan yang sangat besar, biasanya meliputi sebuah negara atau benua. (Tanenbaum,2003)

Jaringan WAN dapat menghubungkan satu komputer dengan komputer lain dengan menggunakan satelit atau kabel bawah laut.

Beberapa teknologi WAN yang banyak dijumpai : modem, *Integrated Services Digital Network* (ISDN), *Digital Subscriber Line* (DSL), *frame relay.*

2.1.3 Perangkat Jaringan

Terdapat sejumlah perangkat yang melewatkan aliran informasi data dalam sebuah jaringan LAN. Penggabungan perangkat tersebut akan menciptakan infrastruktur LAN. Perangkat-perangkat tersebut adalah :

1. ***Modem***

   Modem (*modulators-demodulators*) adalah perangkat *end user* yang digunakan untuk mengubah sinyal *digital* menjadi sinyal analog yang dikirimkan melalui line telepon. Dan

sebaliknya *modem* dapat menerima sinyal *analog* kemudian mengubahnya menjadi sinyal *digital* sebagai masukan ke perangkat yang terhubung, biasanya komputer.

2. Hub

Hub menghubungkan semua komputer yang terhubung ke LAN. *Hub* adalah repeater dengan jumlah *port* banyak (*multiport repeater*). *Hub* tidak mampu menentukan tujuan, hanya mentransmisikan sinyal ke setiap *line* yang terkoneksi dengannya dengan menggunakan mode *half-duplex*.

3. Switch

*Switc*h menghubungkan semua komputer yang terhubung ke LAN, sama seperti *hub*. Perbedaannya adalah *switch* dapat beroperasi dengan mode *full-duplex* dan mampu mengalihkan jalur dan memfilter informasi ke dan dari tujuan yang spesifik.

4. Router

Router adalah peningkatan kemampuan dari *bridge*. *Router* mampu menunjukkan rute/jalur (*route*) dan memfilter informasi pada jaringan yang berbeda. Beberapa *router* mampu secara otomatis mendeteksi masalah dan mengalihkan jalur informasi dari area yang bermasalah.

2.1.4 Media Transmisi Data

Dalam suatu sistem transmisi data, media transmisi merupakan

jalur fisik diantara pengirim dan penerima. Media transmisi untuk gelombang elektromagnetik dibedakan menjadi dua yaitu *Guided* dan *Unguided*. Karakteristik dan mutu suatu transmisi data ditentukan oleh dua hal yaitu karakteristik media dan karakteristik sinyal. Untuk media *guided*, media itu sendiri menjadi lebih penting dalam penentuan batasan-batasan transmisi. Untuk media *unguided*, karakteristik transmisi lebih ditentukan oleh kualitas sinyal yang dihasilkan melalui antena transmisi dibandingkan oleh medianya sendiri.

Dengan mempertimbangkan desain sistem transmisi data, perhatian ditekankan pada *rate* data dan jarak. Semakin besar *rate* data dan semakin kecil jarak, maka akan semakin baik. Sejumlah faktor-faktor perancangan yang berkaitan dengan media transmisi dan sinyal yang menentukan *rate* data dan jarak adalah:

- ***Bandwidth***: Selama faktor lain tetap konstan, maka semakin besar *bandwidth* suatu sinyal, akan semakin tinggi *rate* data yang diperoleh
- **Gangguan sinyal**: Gangguan, seperti misalnya, atenuasi, membatasi jarak.
- **Interferensi**: Interferensi dari sinyal-sinyal yang berkompetisi dalam *band* frekuensi yang saling tumpang tindih dapat mengubah atau menghapuskan sinyal.
- **Jumlah *reciever***: suatu media *guided* bisa dipergunakan untuk membangun suatu hubungan titik ke titik atau hubungan

terbagi pada alat-alat tambahan. Masing-masing alat tambahan akan memunculkan beberapa atenuasi dan distorsi dengan segera, serta membatasi jarak dan/atau *rate* data.

2.1.4.1 *Guided* / *Wired*

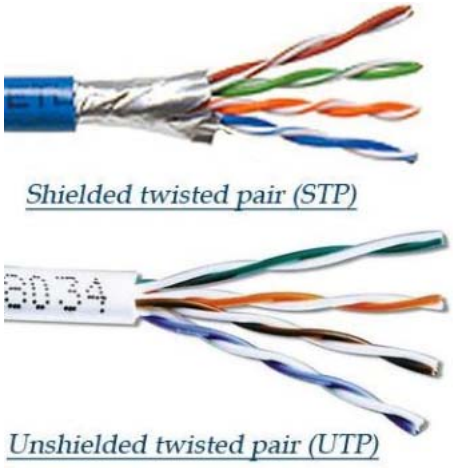
Untuk media *guided*, kapasitas transmisi, baik dalam hal *rate* data maupun *bandwidth*, sangat tergantung pada jarak dan sistem transmisi medianya dari titik ke titik ataukah multititik, seperti misalnya dalam suatu LAN.

1. Twisted Pair

Kabel *twisted-pair* ini memiliki 2 jenis utama yaitu *unshielded* (tidak memiliki selimut) yang biasa disebut UTP, merupakan kawat telepon biasa, atau lebih banyak lagi digunakan sebagai medium untuk *Local Area Network* (LAN) karena jauh lebih murah dan lebih mudah digunakan dan dipasang. UTP dapat menyebabkan tranmisi lebih mudah terpengaruh oleh gangguan *noise* yang berasal dari lingkungan sekitar. Dan *shielded* (berselimut) yang biasa disebut STP, memiliki kinerja lebih baik pada laju data yang tinggi sehingga harganya lebih mahal dan lebih sulit dalam penggunaanya dibandingkan dengan UTP.

UTP yang digunakan sebagai medium untuk LAN terdiri dari 4 pasang kabel yang dipilin untuk mengurangi

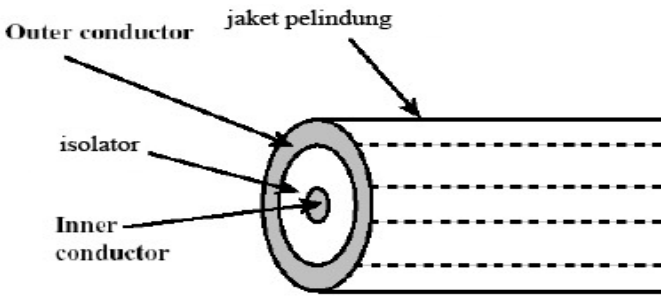
interferensi.



Gambar 2.5 STP dan UTP

2. Coaxial Cable

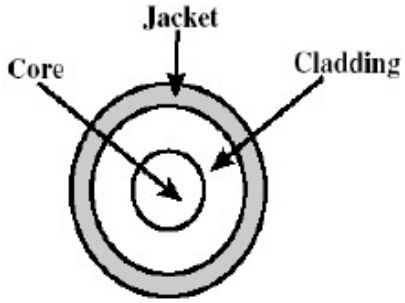
Coaxial cable adalah kabel yang terdiri dari konduktor berbentuk silinder untuk lapisan luar, yang mengelilingi konduktor bagian dalam. Konduktor bagian dalam dilapisi oleh bahan isolator, sedangkan konduktor bagian luar dilapisi oleh jaket pelindung. Karena konstruksi dan pelapisan kabel yang baik, maka kabel *coaxial cable* lebih sedikit mengalami interferensi bila dibandingkan dengan *twisted pair*. *Coaxial Cable* dapat digunakan untuk jarak yang lebih jauh dan dalam jaringan komunikasi yang lebih luas dengan stasiun dan jalur komunikasi yang lebih banyak.



Gambar 2.6 *Coaxial Cable.*

3. Fiber Optic

Suatu media fisik yang mampu melakukan transmisi cahaya, memiliki kecepatan yang tinggi dan dapat mencapai jarak yang jauh tanpa kehilangan data. Kabel *fiber optic* memiliki tingkat gangguan yang sangat minim, salah satu alasannya adalah karena media ini tidak terpengaruhi oleh gelombang elektromagnetik. Kabel *fiber optic* jauh lebih mahal jika dibandingkan dengan *twisted pair* dan *coaxial cable*, dan pemasangannya sulit.



Gambar 2.7 *Fiber Optic.*

2.1.4.2 *Unguided/Wireless*

Untuk *unguided* media, transmisi dan penangkapan diperoleh melalui suatu alat yang disebut dengan antena. Untuk transmisi, antena menyebarkan energi elektromagnetik ke dalam media (biasanya udara), sedangkan untuk penerimaan sinyal, antena menangkap gelombang elektromagnetik dari media. Pada dasarnya terdapat dua jenis konfigurasi untuk transmisi *wireless*, yaitu searah dan segala arah.

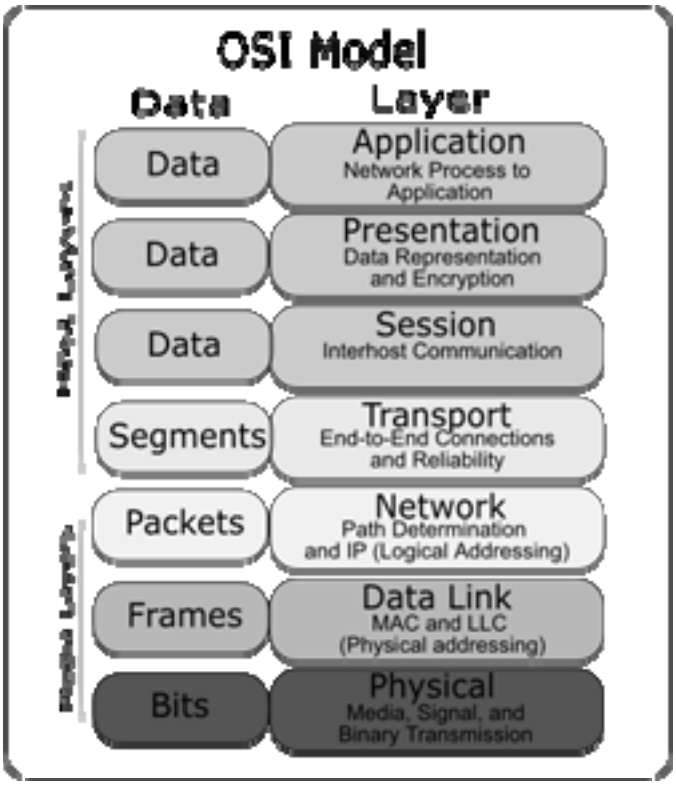
Jenis-jenis transmisi *wireless* adalah sebagai berikut:

- Gelombang mikro *terrestrial*
- Gelombang mikro satelit
- *Radio broadcast*
- Infra merah

2.1.5 Protokol Jaringan

Protokol jaringan adalah suatu set aturan yang mengatur cara perangkat-perangkat dalam suatu jaringan bertukar informasi. Model yang umum dijadikan referensi untuk mempelajari protokol jaringan adalah model referensi lapisan *Open System Interconnection* (OSI *Layers*) dan TCP/IP merupakan protokol jaringan yang saat ini sangat umum digunakan untuk *internetworking*.

2.1.5.1 Model OSI *Layer*



Gambar 2.8 Model OSI *Layer* (sumber: http://en.wikipedia.org/wiki/OSI_Model)

Model referensi OSI (*Open System Interconnection*) menggambarkan bagaimana informasi dari suatu *software* aplikasi di sebuah komputer berpindah melewati sebuah media jaringan ke suatu *software* aplikasi di komputer lain. Model referensi OSI secara konseptual terbagi ke dalam 7 lapisan dimana masing-masing lapisan memiliki fungsi jaringan yang spesifik. Model ini diciptakan berdasarkan sebuah proposal yang dibuat oleh the *International Standards Organization* (ISO) sebagai langkah awal menuju standarisasi protokol internasional

yang digunakan pada berbagai *layer* . Model ini disebut ISO OSI (*Open System Interconnection*) Reference Model karena model ini ditujukan bagi pengkoneksian open system. *Open System* dapat diartikan sebagai suatu sistem yang terbuka untuk berkomunikasi dengan sistem-sistem lainnya.

Model referensi OSI terdiri dari tujuh *layer*, yaitu:

1. ***Physical Layer***

   Layer ini berhubungan langsung dengan *hardware*. Fungsi utama dari *layer* ini adalah bertanggung jawab untuk mengaktifkan dan mengatur *physical interface* dari jaringan komputer, memodulasi data *digital* antara peralatan yang digunakan user dengan signal yang berhubungan. Peralatan yang merupakan *physical layer* antara lain *hub* dan *repeater*.

2. ***Data Link Layer***

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

3. ***Network Layer***

   Network layer menyediakan prosedur dalam mentransfer data dari suatu sumber ke suatu tujuan

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

4. *Transport Layer*

Fungsi dasar *transport layer* adalah menyediakan kepercayaan, kejernihan transfer data di akhir *point* serta menyediakan *end-to-end error recovery,*dan *flow control.*

5. *Session Layer*

Sesuai dengan namanya, *layer* ini berfungsi untuk menyelenggarakan, mengatur dan memutuskan sesi komunikasi. *Session layer* menyediakan servis kepada *layer presentation.*

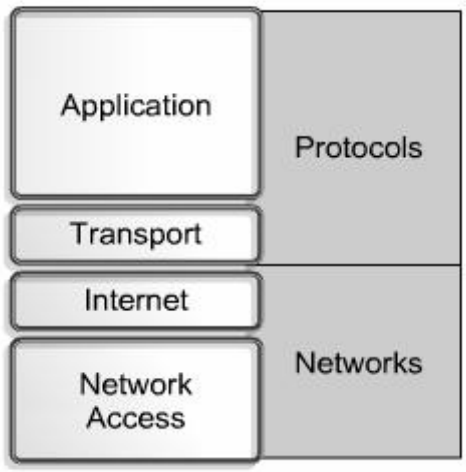
6. *Presentation Layer*

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

7. ***Application Layer***

Layer ini adalah *layer* yang paling dekat dengan *user*/pengguna, *layer* ini menyediakan sebuah layanan jaringan kepada pengguna aplikasi.

2.1.5.2 Model TCP/IP *Layer*



Gambar 2.9 Model TCP/IP *Layer* (sumber: *http://en.wikipedia.org/wiki/*TCP/IP)

TCP/IP (singkatan dari *Transmission Control Protocol*/*Internet Protocol*) adalah standar komunikasi data yang digunakan oleh komunitas *internet* dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang 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

Layer – layer pada model referensi TCP/IP :

1. ***Application Layer***

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

2. ***Transport Layer***

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

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

  TCP berfungsi untuk mengubah suatu blok data yang besar menjadi segmen-segmen yang dinomori dan disusun secara berurutan agar si penerima dapat menyusun kembali segmen-segmen tersebut seperti waktu pengiriman. TCP ini adalah jenis *protocol connection oriented* yang memberikan layanan bergaransi (Dua aplikasi pengguna TCP harus melakukan pembentukan hubungan untuk dapat melakukan pertukaran data), *reliable* (TCP menerapkan proses deteksi kesalahan paket dan retransmisi), *byte stream service* (Paket yang dikirim akan sampai pada tujuan secara berurutan)

- **UDP (*User Datagram Protocol*)**

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

tempat asal ke tempat tujuan, masing-masing tidak perlu melakukan pembentukan hubungan terlebih dahulu).

3. Internet Layer

Satu tingkat di atas *Network Access Layer* terdapat *Internet Layer*. *Internet Protokol* (IP) merupakan jantung dari TCP/IP dan protokol paling penting pada Internet. *Internet Layer* menyediakan layanan pengiriman paket dasar pada jaringan tempat TCP/IP *network* dibangun. Seluruh protokol di atas dan di bawah *Internet Layer*, menggunakan *internet* Protokol untuk mengirimkan data. Semua data TCP/IP mengalir melalui IP, baik data yang akan masuk maupun yang akan keluar. *Internet Layer* bertanggung-jawab dalam proses pengiriman paket ke alamat yang tepat.

4. Network Access Layer

Protokol pada *layer* ini menyediakan media bagi sistem untuk mengirimkan data pada *device* lain yang terhubung secara langsung dengan jaringan. *Network Access Layer* merupakan gabungan antara *Physical Layer* dan *Data Link Layer*. Fungsi *Network Access Layer* dalam *layer* ini adalah mengubah IP datagram ke dalam *frame* yang ditransmisikan oleh *network*, dan memetakan

IP *Address* ke *physical address* yang digunakan dalam jaringan.

2.1.6 Pengalamatan IP

Alamat *network* memberikan identifikasi unik untuk setiap jaringan. Setiap mesin pada jaringan yang sama menggunakan atau berbagi alamat *network* yang sama sebagai bagian dari pengalamatan IP.

Alamat *node* memberikan identifikasi secara unik pada setiap mesin di dalam *network*. Bagian dari alamat ini haruslah unik karena alamat *node* mengidentifikasikan sebuah mesin tertentu yang merupakan *group*. Dapat juga disebut dengan alamat *host.*

2.1.6.1 Kelas-kelas IP

Terdapat tiga jenis *class* yang digunakan dalam pengalamatan jaringan, yaitu *class* A, *class* B, dan *class* C.

	8 *bits*	8 *bits*	8 *bits*	8 *bits*
Class A :	*Network*	*Host*	*Host*	*Host*
Class B :	*Network*	*Network*	*Host*	*Host*
Class C :	*Network*	*Network*	*Network*	*Host*

Tabel 2.1 Tabel Tiga *Class* IP

- ***Class* A**

  Di dalam jaringan *class* A, *byte* pertama digunakan untuk menunjukkan alamat *network*, dan tiga *byte* sisanya digunakan untuk alamat *host.*

  Pada *class* ini, *bit* pertama dari *byte* pertama harus selalu *off* atau bernilai 0. Ini berarti alamat *class* A adalah semua nilai antara 0 dan 127.

  Formatnya adalah *network.host.host.host,* atau jika digantikan dengan binari akan menjadi :

  0XXXXXXX.host.host.host

  Jika pada *byte* pertama tanda 'X' diganti dengan 0 maka akan menjadi 00000000 = 0

  Dan jika tanda 'X' diganti dengan 1 maka akan menjadi 01111111 = 127

- ***Class* B**

  Pada jaringan *class* B, dua *byte* pertama menunjukkan alamat *network* dan dua *byte* selebihnya digunakan untuk alamat *host.*

  Pada *class* ini, *bit* pertama dari *byte* pertama harus selalu dalam kondisi *on*, tapi *bit* kedua harus selalu dalam kondisi *off.* Ini berarti alamat *class* B adalah semua nilai antara 128 dan 191.

Formatnya adalah *network.network.host.host,* atau jika digantikan dengan binari akan menjadi :

10XXXXXX.XXXXXXXX.*host.host*

Jika pada *byte* pertama tanda ‘X’ diganti dengan 0 maka akan menjadi : 10000000 = 128

Dan jika tanda ‘X’ diganti dengan 1 maka akan menjadi : 10111111 = 191

- ***Class* C**

Tiga *byte* pertama dari pengalamatan jaringan *class* C digunakan untuk alamat *network,* dengan hanya menyisakan satu *byte* kecil untuk alamat *host.*

Pada *class* ini, 2 *bit* pertama dari *byte* pertama harus selalu dalam kondisi *on,* tapi *bit* ketiga harus selalu dalam kondisi *off.* Ini berarti alamat *class* C adalah semua nilai antara 192 dan 223.

Formatnya adalah *network.network.network.host,* atau jika digantikan dengan binari akan menjadi :

110XXXXX.XXXXXXXX.XXXXXXXX.*host*

Jika pada *byte* pertama tanda ‘X’ diganti dengan 0 maka akan menjadi : 11000000 = 192

Dan jika tanda ‘X’ diganti dengan 1 maka akan menjadi : 11011111 = 223

2.1.6.2 Pengalamatan IP *Private*

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

Kelas IP *Private*	Kelompok IP *Private*
A	**10.0.0.1 – 10.255.255.254**
B	**172.16.0.1 – 172.31.255.254**
C	**192.168.0.1 – 192.168.255.254**

Tabel 2.2 Tabel Pengalamatan IP *Private*

2.2 Teori - Teori Khusus

2.2.1 VPN (*Virtual Private Network*)

2.2.1.1 Definisi VPN (*Virtual Private Network*)

VPN adalah singkatan dari *virtual private network*, yaitu jaringan pribadi (bukan untuk akses umum) yang menggunakan medium nonpribadi (misalnya *internet*) untuk menghubungkan antar *remote-site* secara aman. Perlu penerapan teknologi tertentu agar walaupun menggunakan medium yang umum, tetapi *traffic* (lalu lintas) antar *remote-site* tidak dapat disadap dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan *traffic*

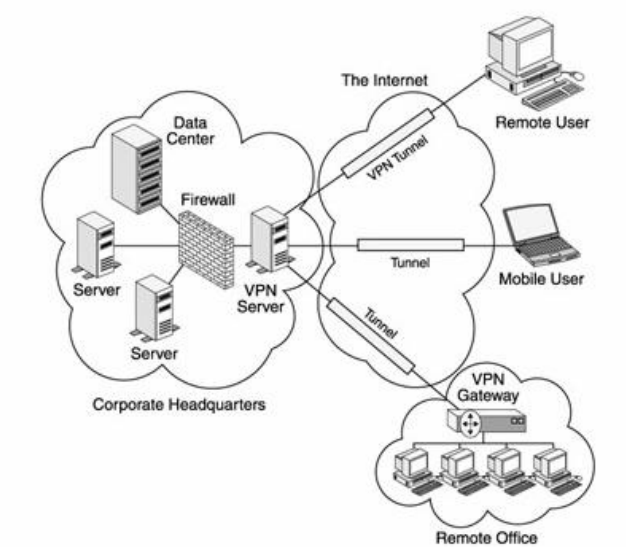
yang tidak semestinya ke dalam *remote-site*.

Gambar 2.10 VPN (*Virtual Private Network*)

2.2.1.2 Tipe–Tipe VPN

1. ***Remote Access* VPN**

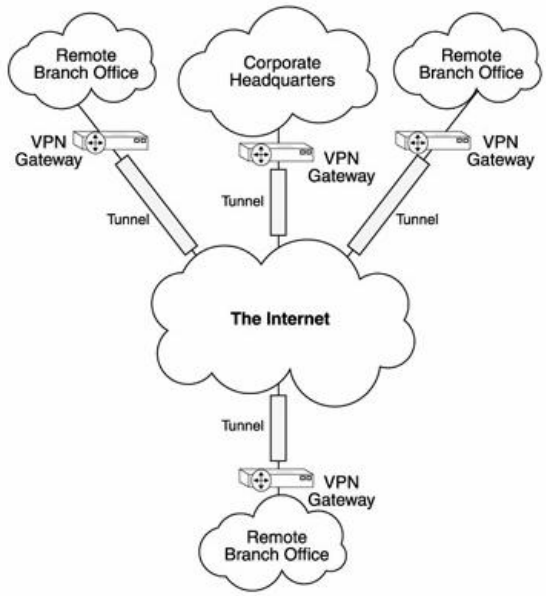
   Remote Access VPN menyediakan akses kapan saja dengan akses jarak jauh, mobilitas, dan telekomunikasi karyawan dari mana saja ke jaringan pusat perusahaan. Biasanya *remote access* ini diperuntukkan untuk pemakai yang *mobile* (sering bepergian) atau oleh kantor cabang kecil dan kantor cabang yang berjauhan (*remote*) yang tidak memiliki koneksi yang tetap ke jaringan pusat perusahaan. Dalam *Remote Access* VPN, para pemakai dan kantor cabang *remote* hanya membutuhkan *dial-up* koneksi lokal ke ISP dan mengakses jaringan pusat perusahaan melalui *Internet*.



Gambar 2.11 *Remote Access* VPN

2. *Site-to-Site Intranet* VPN

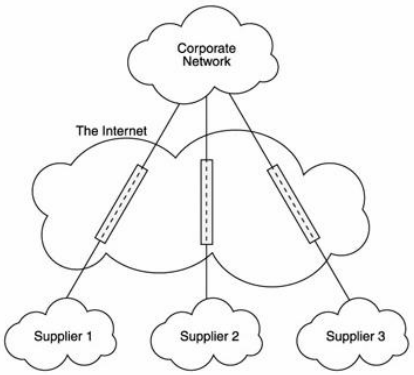
Site-to-site Intranet VPN memungkinkan suatu *private network* diperluas dengan menghubungkan 2 atau lebih jaringan tetap yang tidak berpindah-pindah melalui *internet* atau layanan *public network* lainnya dengan cara yang aman. *Site-to-site Intranet* VPN merupakan suatu alternatif infrastruktur WAN yang biasa menghubungkan kantor-kantor cabang, kantor pusat, atau partner bisnis ke seluruh jaringan perusahaan.



Gambar 2.12 *Site-to-Site Intranet* VPN

3. *Site-to-Site Extranet* VPN

Site-to-site Extranet merupakan *intranet* dari suatu perusahaan yang diperluas untuk menggabungkan para pemakai dari luar perusahaan, yaitu : pemasok, penjual, pelanggan, atau relasi bisnis. Sehingga seluruh bagian atau perusahaan dapat saling berbagi informasi dengan cepat dan mudah dengan penambahan *firewall* untuk keamanan *internal network*.



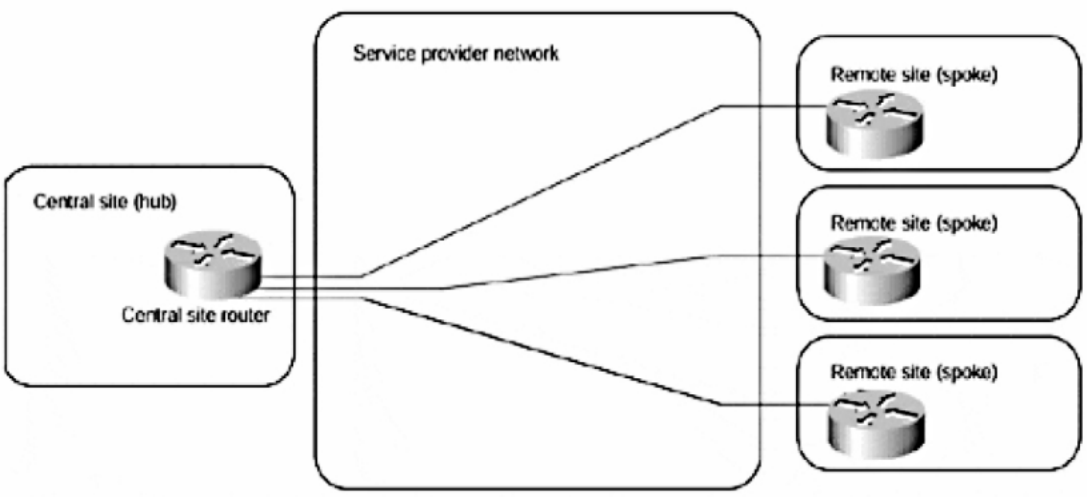
Gambar 2.13 *Site-to-Site Extranet* VPN

2.2.1.3 Topologi VPN

Topologi VPN yang dibuat suatu perusahaan seharusnya dibuat berdasarkan bisnis yang ingin diatasi oleh perusahaan. Akan tetapi, ada beberapa topologi yang cukup terkenal. Topologi yang sama dapat memecahkan berbagai macam masalah bisnis di pasar industri yang berbeda. Menurut Guichard dan Pepelnjak (2001) topologi VPN dapat dikelompokkan menjadi tiga kategori, yaitu topologi *hub-and-spoke*, topologi *partial atau full-mesh*, dan topologi *hybrid*.

1. **Topologi *Hub-and-spoke***

   Topologi yang biasa ditemui adalah topologi *hub-and-spoke*, dimana beberapa *remote office* (*spokes*) terhubung dengan *central site* (*hub*), seperti ditunjukkan pada Gambar 2.14. *Remote offices* biasanya dapat bertukar data (tanpa adanya batas-batas keamanan secara explisit di *inter-office traffic*), tetapi jumlah data yang ditukarkan bisa diabaikan. Topologi ini biasa dipakai di organisasi dengan struktur hierarki yang ketat contohnya antara bank, organisasi pemerintahan atau toko retail dengan kantor cabang yang kecil.



Gambar 2.14 Topologi *hub-and-spoke*

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

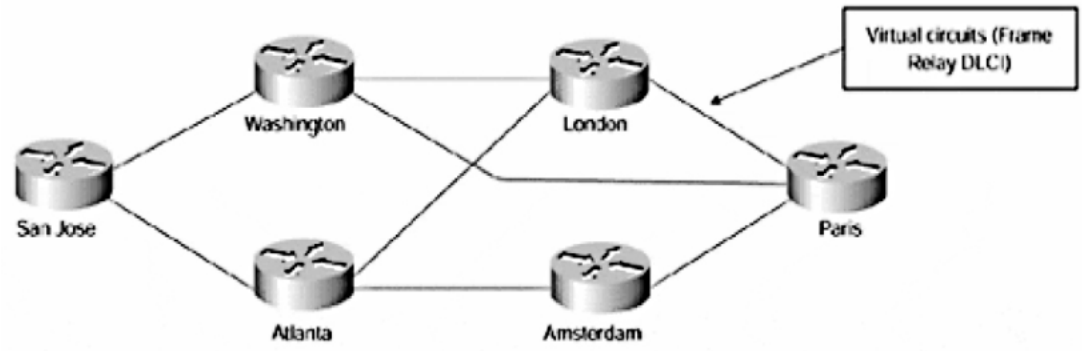
2. Topologi *Partial* atau *Full Mesh*

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

- Perusahaan mungkin kurang terorganisir strukturnya, pertukaran data terjadi di berbagai tempat di perusahaan.

- Aplikasi yang digunakan di perusahaan membutuhkan komunikasi *peer-to-peer* seperti *messaging* atau sistem kolaborasi.
- Untuk perusahaan multinasional, biaya topologi *hub-and-spoke* dapat sangat tinggi karena biaya jaringan internasional.

Untuk itu, topologi VPN yang cocok untuk perusahaan adalah topologi *partial-mesh*, dimana *site* di VPN terhubung dengan VC diatur oleh kebutuhan trafik. Jika tidak semua tempat mempunyai hubungan langsung dengan semua tempat (seperti Gambar 2.15), topologi ini disebut *partial mesh*, tetapi jika semua tempat terhubung ke semua tempat maka topologi ini disebut *full mesh*.

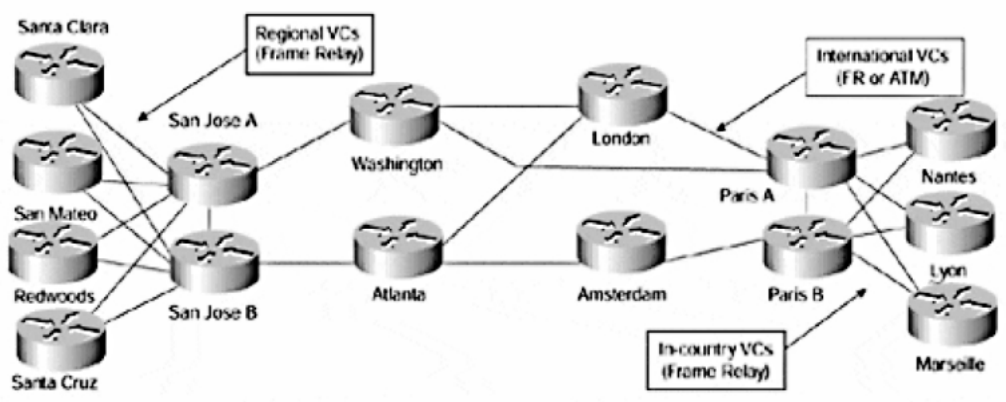


Gambar 2.15 Topologi *Partial Mesh*

3. Topologi *Hybrid*

Jaringan VPN yang besar biasanya menggabungkan topologi *hub-and-spoke* dengan *partial-mesh*. Sebagai contoh, perusahaan multinasional yang

besar mungkin mengakses jaringan di setiap negara yang terhubung dengan topologi *hub-and-spoke*, dan jaringan pusat internasional dihubungkan dengan topologi *partial-mesh* seperti pada Gambar 2.16 Topologi seperti ini dinamakan topologi *hybrid*.



Gambar 2.16 Topologi *hybrid*

2.2.1.4 Teknologi VPN

1. ***Frame Relay* atau ATM *Virtual Circuit***

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

Umumnya, penyedia jasa layanan akan memberikan layanan solusi total, yaitu dengan memberikan fasilitas *router* yang diatur oleh penyedia jasa layanan disisi pelanggan. Dengan demikian para penyedia jasa layanan tersebut dapat membuat jasa layanan seperti IP VPN dengan menggunakan PVCs dan SVCs untuk membangun hubungan *point-to-point* melalui *Frame Relay* atau jaringan ATM. Hal ini dapat dilakukan dengan menggunakan *router* untuk mengatur informasi yang ada pada lapisan ke 3.

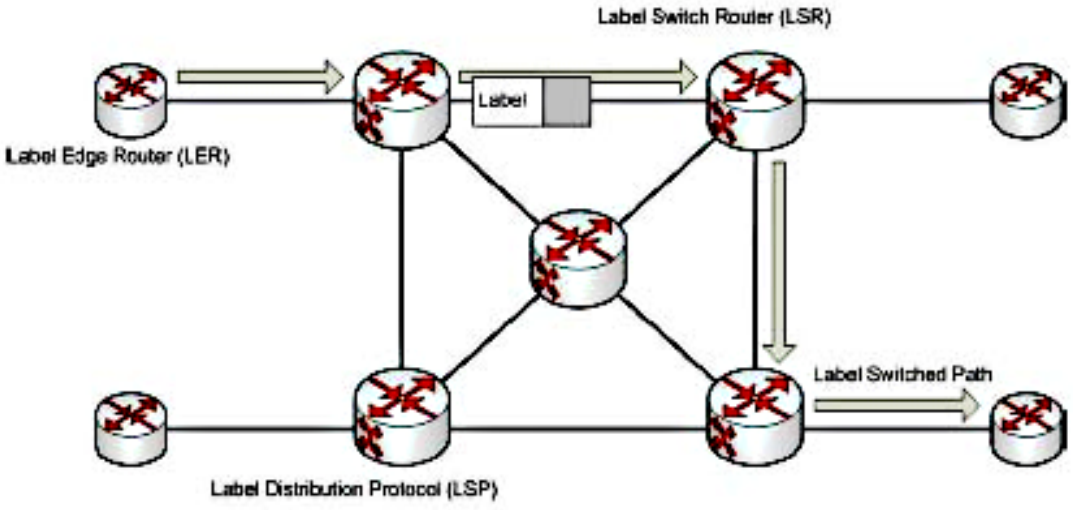
2. VPN IP-MPLS

Konsep dasar MPLS (*Multi-Protocol Label Switching)* adalah teknik peletakan *label* dalam setiap paket yang dikirim dalam jaringan ini. MPLS bekerja dengan cara memberi *label* paket-paket data yang memuat rute dan prioritas pengiriman (*treatment*) paket tersebut. Label tersebut akan memuat informasi penting yang berhubungan dengan informasi *routing* suatu paket. Teknik pelabelan ini biasa disebut dengan *label switching.*

Network MPLS terdiri atas sirkuit yang disebut *Label-Switched Path* (LSP), yang menghubungkan titik-titik yang disebut *Label-Switched Router* (LSR). LSR pertama dan terakhir disebut *ingress* dan *egress*. Setiap LSP dikaitkan dengan sebuah *Forwarding Equivalence*

Class (FEC). FEC merupakan kumpulan paket yang menerima perlakuan *forwarding* yang sama di sebuah LSR dan diidentifikasikan dengan pemasangan label.

Secara umum, jaringan MPLS dapat dilihat pada gambar 2.17. LSR berfungsi untuk mengaplikasikan label ke dalam paket-paket yang masuk ke dalam jaringan MPLS. Paket yang telah dilabeli kemudian dihubungkan ke LSR yang juga berfungsi sebagai router.



Gambar 2.17 IP MPLS

Berikut detail komponen yang ada dalam MPLS.

a. *Label Switched Path* (LSP)

Merupakan jalur yang melalui satu atau serangkaian LSR dimana paket diteruskan oleh *label swapping* dari satu MPLS *node* ke MPLS *node* yang lain.

b. *Label Switching Router* (LSR)

Merupakan *router* dalam MPLS yang berperan dalam menetapkan LSP dengan menggunakan teknik *label swapping* dengan kecepatan yang telah ditetapkan.

c. MPLS *Edge Node* atau *Label Edge Router* (LER)

Merupakan *router* MPLS yang menghubungkan sebuah MPLS *domain* dengan *node* yang berada di luar MPLS *domain*.

d. MPLS Label

Merupakan deretan *bit* informasi yang ditambahkan pada *header* suatu paket data dalam MPLS. Label MPLS atau yang disebut juga MPLS *header* ini terletak di antara *header layer* 2 dan *header layer* 3.

e. MPLS *Node*

Node yang menjalankan MPLS. MPLS *node* ini sebagai *control protocol* yang akan meneruskan paket berdasarkan label. Dalam hal ini MPLS *node* merupakan sebuah *router*.

f. *Forward Equivalance Class* (FEC)

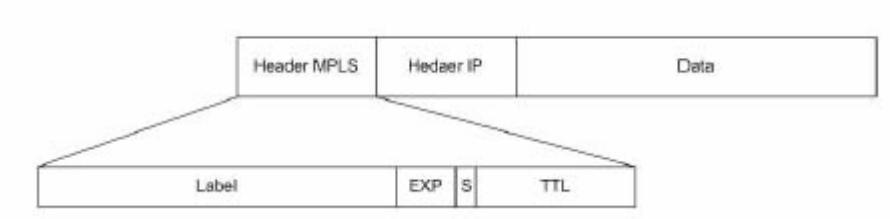
Merupakan representasi dari beberapa paket data yang diklasifikasikan berdasarkan kebutuhan *resource* yang sama di dalam proses pertukaran data.

g. *Label Distribution Path* (LDP)

Merupakan protokol yang berfungsi untuk mendistribusikan informasi yang ada pada label ke setiap LSR pada MPLS. Protokol ini digunakan untuk memetakan FEC ke dalam label untuk selanjutnya akan dipakai untuk menentukan LSP.

MPLS berbeda dengan ATM yang memecah paket-paket IP. MPLS hanya melakukan enkapsulasi paket IP dengan menempelkan *header* MPLS pada suatu paket. *Header* MPLS terdiri atas 32 *bit* data, termasuk 20 *bit* label, 3 *bit* eksperimen, 1 *bit* identifikasi *stack*, serta 8 *bit* TTL. Label adalah bagian dari *header*, memiliki panjang yang bersifat tetap, dan merupakan satu-satunya tanda identifikasi paket.

Berikut pemetaan *header packet* MPLS.



Gambar 2.18 Pemetaan *Header Packet* MPLS

VPN IP MPLS adalah layanan komunikasi data *any to any connection* berbasis IP *Multi Protocol Label Switching* (MPLS). Dalam hal keamanan, VPN IP MPLS ini setingkat dengan *frame relay*/ATM, dimana trafik atau lalu lintas data dialirkan dalam suatu jaringan yang

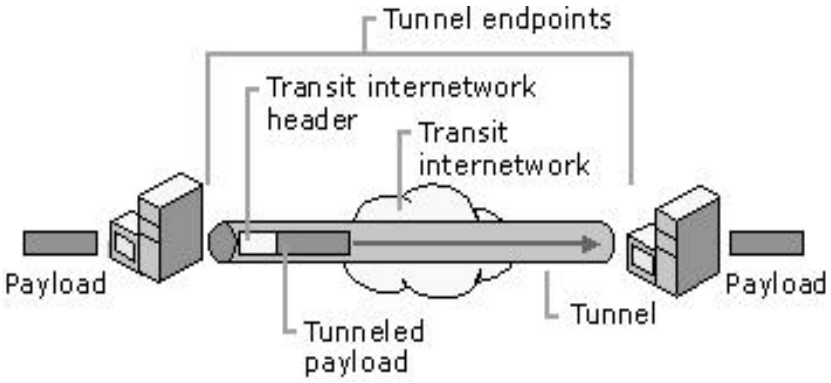
terpisah dengan jaringan publik lainnya atau jaringan *internet.* Beberapa kelebihan yang dapat disediakan oleh VPN IP MPLS adalah sebagai berikut:

- ***Multiservices Offering***, mampu menyalurkan semua jenis trafik *voice,* video, grafis dan data.
- ***Quality of Service* (QoS),** VPN IP MPLS digunakan untuk merealisasikan *Class Of Service* (CoS) dimana pelanggan dapat mengimplementasikan aplikasinya baik berupa aplikasi yang *delay sensitive, mission critical* maupun *non mission critical* pada satu *platform* jaringan privat IP MPLS.
- ***Scalability and Flexible***, dapat dimulai dari skala jaringan yang kecil dan terbatas dapat dikembangkan secara mudah dan praktis, meliputi perubahan *bandwidth* dan konfigurasi.
- ***End to End Manageability,*** *user friendly* dan pengendalian yang mudah.
- ***Cost Saving Opportunity,*** harga IP MPLS dapat ditekan lebih rendah karena disesuaikan dengan fasilitas layanan yang dipilih dan kebutuhan penggunaan *bandwidth,* serta harga tidak tergantung jarak.

2.2.1.5 *Tunneling*

Tunneling merupakan pengenkapsulasian paket-paket atau *frame-frame* yang terdapat di dalam paket-paket atau *frame-frame* lainnya, seperti halnya meletakan suatu amplop ke dalam amplop lainnya (Perlmutter, 2000, p104). Aspek terpenting dari *tunneling* ialah paket data asli, bisa merupakan protokol yang berbeda. Daripada mentransfer paket asli, yang bisa saja tidak dapat berjalan pada infrastruktur yang ada, pada header paket ditambahkan protokol yang kompatibel. Header ini berfungsi agar paket bisa dikirimkan dengan baik melalui infrastruktur yang ada (Gupta, 2003).

Dengan *tunneling*, proses transfer data dari satu jaringan ke jaringan lain memanfaatkan jaringan publik atau *internet* secara terselubung. Disebut *tunnel* atau saluran karena aplikasi yang memanfaatkannya hanya melihat dua *end point* yang telah ditentukan sebelumnya.



Gambar 2.19 *Tunneling*

Tipe-Tipe *Tunneling*

1. *Voluntary Tunnel*

Dimana *client* atau *user* yang mengajukan VPN *request* untuk membuat *voluntary tunnel*. Untuk melakukan ini, *protocol tunneling* yang sesuai harus di*install* pada computer *client*. Pada *voluntary tunnel* ini komputer *user* merupakan *end point*nya dan berlaku sebagai VPN *client*. *Voluntary tunnels* membutuhkan koneksi IP baik dari koneksi LAN atau koneksi *dial-up*. Sebuah *tunnel* dibuat terpisah untuk tiap pasangan komunikasi. Setelah komunikasi antara dua titik berakhir, *tunnel* tersebut ditutup.

2. *Compulsory Tunne*l

Pada *Compulsory tunnel* ini (NAS-*Network Access Server*) atau ISP yang digunakan oleh *client* yang merupakan *end point*nya. Dan NAS inilah yang membuat dan menyediakan *tunnel* beserta *protocol tunneling* untuk *client*. Tidak seperti *voluntary tunnel* yang membuat *tunnel* terpisah untuk setiap pasangan komunikasi, setiap c*ompulsory tunnel* yang dibuat dapat digunakan untuk banyak *client*. *Tunnel* akan terus terbuka selama ada *client* yang menggunakan *tunnel* tersebut.

2.2.2 OPNET

OPNET merupakan suatu alat atau *software* untuk melakukan pemodelan dan simulasi komunikasi, peralatan-peralatan, dan protokol-protokol jaringan. OPNET merupakan pemodelan *object-oriented* dengan editor grafis atau visual yang mencerminkan struktur dari jaringan dan komponen jaringan yang sesungguhnya. OPNET menyediakan hasil simulasi dalam bentuk grafik, *log*, dan *web report* (dalam bentuk html).

Dalam skripsi ini penulis menggunakan langkah-langkah berikut ini dalam melakukan simulasi dengan menggunakan OPNET :

1. **Menentukan Skenario Simulasi**

   Langkah pertama yang perlu dilakukan untuk melakukan simulasi adalah menentukan terlebih dahulu seperti apa skenario yang akan diuji. Jaringan seperti apa yang akan disimulasi, teknologi apa yang akan digunakan dalam simulasi.

2. **Menyusun Model-Model Jaringan**

   Menyusun model-model jaringan yang akan disimulasikan dengan objek-objek yang telah disediakan dari OPNET. OPNET menyediakan perangkat-perangkat jaringan dari berbagai macam jenis dan penjual berikut dengan macam-macam media komunikasi yang ada.

3. Mengkonfigurasi *Node-Node* Jaringan

Konfigurasi dilakukan sesuai dengan keadaan jaringan yang akan disimulasikan. Konfigurasi-konfigurasi yang dilakukan juga termasuk konfigurasi *traffic generator* dan memilih aplikasi-aplikasi apa saja yang akan digunakan dalam simulasi.

4. Memilih Statistik

Memilih statistik-statistik apa saja yang akan diambil dari simulasi. Statistik yang dapat diambil dibagi menjadi tiga yaitu, *global statistics*, *node statistics*, dan *link statistics*.

5. Menjalankan Simulasi

Setelah semua telah dikonfigurasi dan statistik yang akan diambil dari simulasi sudah dipilih, maka simulasi siap dijalankan. Simulasi dijalankan selama waktu yang diinginkan. Waktu disini merupakan waktu dari sebuah model jaringan yang berjalan secara nyata yang disimulasikan.

6. Melihat dan Menganalisa Hasil Simulasi

Hasil yang dapat dilihat dari simulasi ini berdasarkan statistik-statistik apa saja yang tadi telah dipilih. *Simulation Log* berisi informasi-informasi tambahan dari simulasi seperti *ping report* atau *error log*. *Simulation Log* membantu untuk mengindikasi apa penyebab *error* dan membantu bagaimana untuk memperbaikinya.