BAB II

LANDASAN TEORI DAN

Dalam melaksanakan kerja praktek Kami menggunakan dasar-dasar teori sistem informasi sebagai bahan acuan. Berikut adalah dasar-dasar pengamatan alat alat penunjang dalam pengkoneksian jaringan baik hardware maupun software yang digunakan dalam laporan ini. Dengan adanya perangkat keras dan perangkat lunak yang ada sehingga memberikan kemudahan dalam pengkoneksian jaringan internet .

2.1 Definisi perangkat lunak dan perangkat keras yang menunjang

Pengertian sederhana dari perangkat lunak dan perangkat keras yang menunjang adalah sekumpulan perangkat yang dapat digunakan untuk menyimpan dan manipulasi data elektronis dan pesan-pesan, saling terkait satu dengan lainnya di mana dengan cara tersebut pengguna dapat merasakankemudahan dalam berkoneksi dalam pemakaian jaringan internet, saling berbagi-pakai terhadap informasi yang tersedia. Pada umumnya yang dihubungkan oleh jaringan terdiri dari komputer mikro, terminal, printer dan media penyimpan data, serta perangkat jaringan lainnya.

2.2 Topologi Jaringan Internet

Arsitektur adalah struktur dari suatu jaringan komunikasi. Arsitektur menentukan bagaimana berbagai bagian dari suatu jaringan dihubungkan satu sama lainnya, bagaimana pengaturan cara bekerjanya, dan bagaimana menentukan bahwa satu atau dua bagian atau lebih harus saling menunjang proses yang dilakukan dalam jaringan tersebut. Hubungan antar bagian dalam struktur tersebut dapat dilihat dari medium yang dipakai untuk menghubungkan bagian-bagian tersebut secara fisik (melalui kabel misalnya) atau dilihat dari bagaimana bentuk

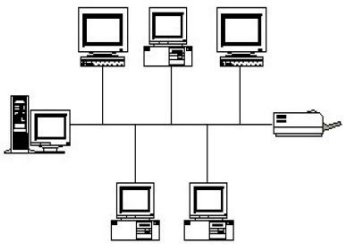
dari jaringan tersebut. Topologi jaringan komputer adalah pola hubungan antar terminal dalam suatu jaringan komputer. Dapat juga diartikan suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Pada PT.Telekomunikasi Indonesia ,tbk Bandung menggunakan topologi jaringan star. Berikut ini adalah beberapa tipe topologi jaringan komputer lainnya yang banyak digunakan.

- Bus
- Star
- Ring
- Tree

Masing-masing topologi diatas mempunyai ciri-ciri dan karakteristik tersendiri serta kelebihan dan kekurangannya masing-masing. Berikut akan kami jelaskan beberapa tipe jaringan diatas

2.2.1 Topologi Bus

Pada topologi bus semua terminal terhubung kejalur komunikasi. Informasi yang dikirim akan melewati semua terminal pada jalur tersebut. Jika alamat yang tercantum dalam data atau informasi yang dikirim sesuai dengan alamat terminal yang dilewati, maka data atau informasi tersebut akan diterima dan diproses, jika alamat tersebut tidak sesuai, maka informasi tersebut akan diabaikan oleh terminal yang dilewati.

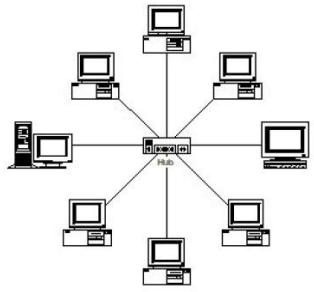


Gambar 2.6 Topologi Bus

- **Kelebihan :**
    1. Mudah dalam mengkonfigurasi computer atau perangkat lainya kedalam sebuah sebuah kabel utama
    2. Tidak terlalu banyak menggunakan kabel dibandingkan dengan topologi star atau bintang
- **Kelemahan :**
    1. Seluruh jaringan mati jika kabel utama rusak
    2. Membutuhkan terminator pada kedua sisi kabel utamanya
    3. Sulit mengidentifikasi masalah jika jaringan sedang jatuh atau rusak
    4. Sangat tidak disarankan di pakai pada penggunaan jaringan di gedung besar.

2.2.2 Topologi Star

Topologi star dirancang sedemikian, sehingga seluruh komputer dan peralatan lain terhubung secara langsung pada suatu pusat jaringan yang berupa hub atau konsentrator. Hub atau konsentrator bertindak sebagai pengelola dan pengendali semua fungsi dalam jaringan. Hub juga berfungsi sebagai repeater aliran data. Data pada jaringan bertopologi star selalu melintasi hub atau konsentrator sebelum melanjutkan ketujuan akhirnya.

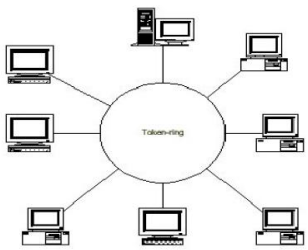


Gambar 2.7 Topologi Star

- **Keunggulan :**
    1. Proses data langsung ke tujuan
    2. Mudah dalam pemasangan kabel
    3. Mempunyai kecepatan 100 Mbps
    4. Jika salah satu koneksi terputus tidak akan mempengaruhi koneksi yang lain
    5. Mudah untuk mendeteksi kesalahan dan memindahkan perangkat-perangkat lainya
    6. Mempunyai concentrator sebagai pusat penghubung jaringan
- **Kekurangan :**
    1. Membutuhkan banyak kabel dari pada topologi linear bus
    2. Lebih mahal dibandingkan topologi linear Bus
    3. Membutuhkan concentrator, dan bilamana concentrator itu rusak node yang terkoneksi tidak dapat terdeteksi

2.2.3 RING

Metode token-ring (sering disebut ring saja) adalah cara menghubungkan computer sehingga berbentuk ring (lingkaran). Setiap simpul mempunyai tingkatan yang sama. Jaringan akan disebut sebagai loop, data dikirimkan kesetiap simpul dan setiap informasi yang diterima simpul diperiksa alamatnya apakah data itu untuknya atau bukan.

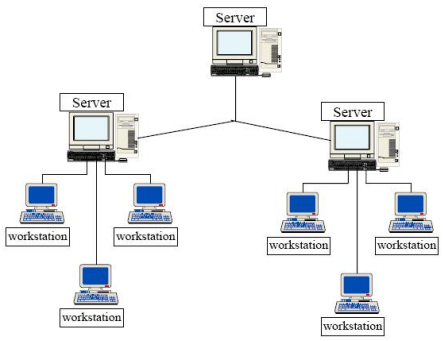


Gambar 2.8 Topologi Ring

- **Kelebihan :**
  1. Keamanan data lebih terjamin
  2. Bila ada error mudah di deteksi
- **Kekurangan :**
  1. Biaya pengembangan sangat mahal
  2. Butuh keahlian khusus
  3. Perangkat keras yang terlibat sedikit di produksi

2.2.4 TREE

Topologi ring menggabungkan dua topologi sekaligus yaitu topologi bus dan topologi star. Topologi jaringan ini meliputi beberapa kelompok konfigurasi workstation bertopologi star yang kemudian dihubungkan dalam kabel utama sebagai bus. Dalam topologi tree dimungkinkan melakukan perluasan jaringan secara mudah.



Gambar 2.9 Topologi Tree

- **Kelebihan**
  1. Proses konfigurasi jaringan dilakukan dari titik ke titik pada masing-masing segmen;
  3. Di dukung oleh berbagai macam perangkat keras dan lunak;

- **Kekurangan**
  1. Keseluruhan panjang kabel pada tiap-tiap segmen dibatasi oleh tiap kabel yang digunakan;
  2. Jika jaringan utama (backbone) rusak, maka keseluruhan segmen ikut rusak juga;
  3. Sangat relatif sulit untuk konfigurasi dan proses pengkabelannya dibandingkan topologi jaringan lain

2.3 Model Hubungan Pada LAN

Secara garis besar terdapat dua model hubungan pada LAN, yaitu jaringan *peer to peer* dan *client server*

2.3.1 Peer to Peer

Pada jaringan *peer to peer*, setiap komputer yang terhubung ke jaringan dapat bertindak sebagai *workstation* ataupun *server*. *Server* adalah komputer yang menyediakan fasilitas bagi komputer-komputer lain didalam jaringan dan *client* adalah komputer-komputer yang menerima atau menggunakan fasilitas yang disediakan oleh *server*. *Server* dijaringan tipe *client-server* disebut dengan *Dedicated Server* karena murni berperan sebagai *server* yang menyediakan fasilitas kepada *workstation* dan *server* tersebut tidak dapat berperan sebagai *workstation*.

- **Keunggulan**
  1. Kecepatan akses lebih tinggi karena penyediaan fasilitas jaringan dan pengelolaannya dilakukan secara khusus oleh satu komputer (*server*) yang tidak dibebani dengan tugas lain sebagai *workstation*.
  2. Sistem keamanan dan administrasi jaringan lebih baik, karena terdapat seorang pemakai yang bertugas sebagai administrator jaringan, yang mengelola administrasi dan sistem keamanan jaringan.

3. Sistem backup data lebih baik, karena pada jaringan *client-server* backup dilakukan terpusat di *server*, yang akan membackup seluruh data yang digunakan di dalam jaringan.

- **Kelemahan**

1. Biaya operasional relatif lebih mahal.
2. Diperlukan adanya satu komputer khusus yang berkemampuan lebih untuk ditugaskan sebagai *server*.
3. Kelangsungan jaringan sangat tergantung pada *server*. Bila *server* mengalami gangguan maka secara keseluruhan jaringan akan terganggu

2.3.2 Client-Server

Pada jaringan *client server*, hanya ada satu komputer yang bertugas sebagai *server* dan komputer lain berperan sebagai *workstation*. peer diistilahkan non-dedicated server, karena server tidak berperan sebagai server murni melainkan sekaligus dapat berperan sebagai *workstation*

- **Keunggulan**

1. Antar komputer dalam jaringan dapat saling berbagi-pakai fasilitas yang dimilikinya seperti: harddisk, drive, fax/modem, printer.
2. Biaya operasional relatif lebih murah dibandingkan dengan tipe jaringan client-server, salah satunya karena tidak memerlukan adanya server yang memiliki kemampuan khusus untuk mengorganisasikan dan menyediakan fasilitas jaringan.
3. Kelangsungan kerja jaringan tidak tergantung pada satu server. Sehingga bila salah satu komputer/peer mati atau rusak, jaringan secara keseluruhan tidak akan mengalami gangguan.

- **Kelemahan**

1. Troubleshooting jaringan relatif lebih sulit, karena pada jaringan tipe peer to peer setiap komputer dimungkinkan untuk terlibat dalam komunikasi yang ada. Di jaringan client-server, komunikasi adalah antara server dengan *workstation*.
2. Unjuk kerja lebih rendah dibandingkan dengan jaringan client-server,

karena setiap komputer/peer disamping harus mengelola pemakaian fasilitas jaringan juga harus mengelola pekerjaan atau aplikasi sendiri.

3. Sistem keamanan jaringan ditentukan oleh masing-masing user dengan mengatur keamanan masing-masing fasilitas yang dimiliki.
4. Karena data jaringan tersebar di masing-masing komputer dalam jaringan,maka backup harus dilakukan oleh masing-masing komputer tersebut

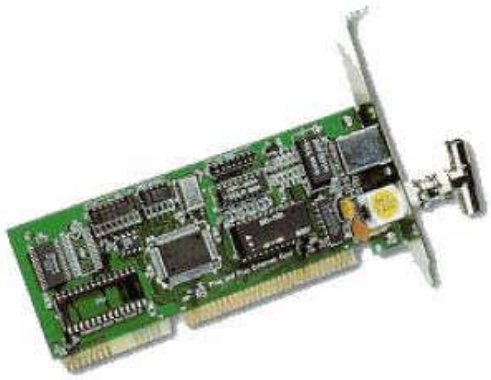
2.4 Komponen jaringan

Secara umum suatu jaringan terdiri dari beberapa perangkat keras berikut ini :

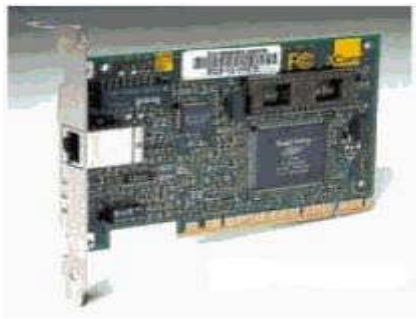
- NIC (Network Interface Card)
- Router
- Modem
- Hub
- Switch
- Bridge
- Repeater

2.4.1 NIC (Network Interface Card)

NIC atau kartu antarmuka jaringan atau kartu jaringan merupakan peralatan yang memungkinkan terjadinya hubungan antara jaringan dengan komputer workstation atau jaringan dengan komputer server. NIC berfungsi untuk menghubungkan antara computer dengan kabel jaringan yang terpasang secara fisik. Pemasangan card ini dihubungkan pada slot ekspansi dalam komputer baik slot ekspansi ISA maupun slot ekspansi PCI bahkan pada beberapa motherboard komputer NIC sudah terpasang secara onboard. Dalam computer notebook NIC kadang-kadang dipasang pada slot PCMCIA. Secara umum NIC tersedia untuk kabel Coaxial dan kabel Twisted-pair



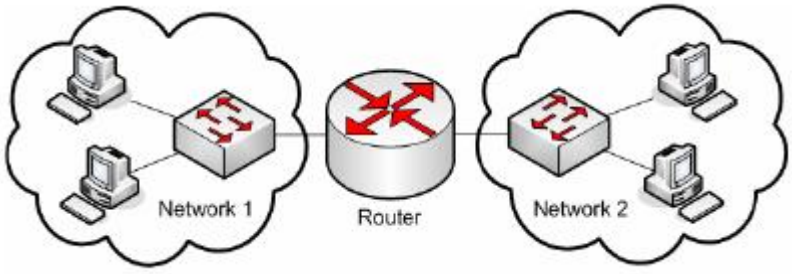
Gambar 2.10 NIC base 2



Gambar 2.11 NIC base T

2.4.2 Router

Router adalah perangkat yang dapat digunakan untuk menghubungkan dua jaringan local yang mempunyai protocol sama pada lapisan jaringan OSI sedangkan protocol pada lapisan fisik dan link berbeda. Jadi fungsi utama Router digunakan untuk pengiriman data jika terdapat perbedaan dalam beberapa bagian protokol. Perbedaan dari beberapa bagian protokol ini terjadi pada hubungan antar jaringan LAN dengan LAN dalam suatu WAN (Wide Area Network). Router ini menghubungkan antar LAN tersebut



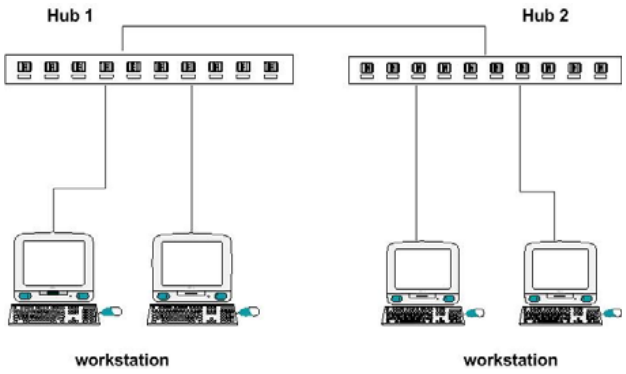
Gambar 2.12 Dua jaringan yang terhubung melalui router

2.4.3 Modem

Modem (Modulator Demodulator) berfungsi sebagai media untuk pengiriman data pada jarak jauh atau data pada jaringan global. Proses pengiriman data dilakukan secara serial dalam bentuk pulsa analog frekuensi tinggi dengan prinsip dasar modulasi. Untuk pengiriman jarak jauh digunakan sinyal analog mengingat sinyal digital mempunyai jarak jangkau yang pendek sebagai akibat pengaruh redaman maupun derau pada media pengirimannya, sedangkan pada sinyal analog meskipun mempunyai kelemahan yakni terpengaruh oleh derau selama pengiriman tetapi hal ini dapat diatasi dengan pengiriman pada frekuensi tinggi.

2.4.4 Hub

Koneksi yang sering digunakan dalam perangkat jaringan. Digunakan untuk menghubungkan segmen dari LAN. Sebuah hub memiliki beberapa ports. Ketika data datang pada sebuah port, data tersebut akan diduplikasi ke port yang lain jadi semua segmen pada LAN akan mengetahui data tersebut. Perbedaan utama antara Hub dan Switch adalah Hub tidak memiliki fasilitas routing, sehingga semua informasi yang datang akan dikirimkan ke semua komputer (broadcast). Sementara Switch memiliki fasilitas routing sehingga informasi yang diterima hanya dikirimkan ke komputer tujuan.



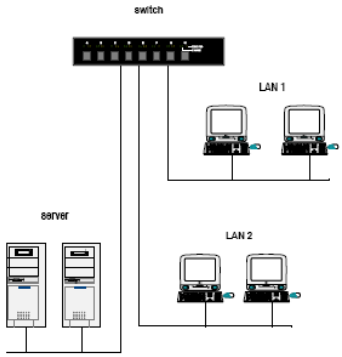
Gambar 2.13 Jaringan yang terhubung oleh Hub

- **Ciri-ciri yang dimiliki Konsentrator adalah** :

1. Biasanya terdiri dari 8, 12, atau 24 port RJ-45
2. Digunakan pada topologi Bintang/Star
3. Biasanya di jual dengan aplikasi khusus yaitu aplikasi yang mengatur manjemen port tersebut.
4. Biasanya disebut hub
5. Biasanya di pasang pada rak khusus, yang didalamnya ada Bridges, router

2.4.5 Switch

Switch adalah alat yang digunakan untuk menghubungkan beberapa LAN yang terpisah dan untuk meningkatkan kinerja jaringan suatu organisasi dengan cara pembagian jaringan yang besar dalam beberapa jaringan yang lebih kecil. Meskipun terhubung dengan jaringan yang bebeda pada masing-masing port, switch dapat memindahkan paket data antar jaringan apabila diperlukan.



Gambar 2.14 Jaringan yang terhubung dengan switch

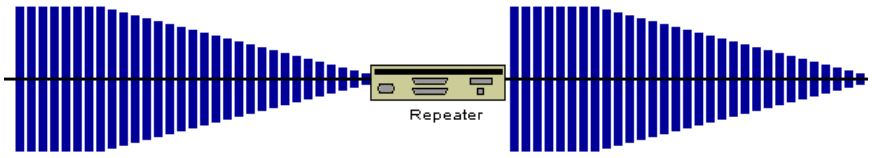
2.4.6 Bridge

Adalah sebuah perangkat yang membagi satu buah jaringan kedalam dua buah jaringan, ini digunakan untuk mendapatkan jaringan yang efisien, dimana kadang pertumbuhan network sangat cepat makanya di perlukan jembatan untuk itu. Kebanyakan Bridges dapat mengetahui masing-masing alamat dari tiap-tiap segmen komputer pada jaringan sebelahnya dan juga pada jaringan yang lain di sebelahnya pula. Diibaratkan bahwa Bridges ini seperti polisi lalu lintas yang

mengatur di persimpangan jalan pada saat jam jam sibuk. Dia mengatur agar informasi di antara kedua sisi network tetap jalan dengan baik dan teratur. Bridges juga dapat di gunakan untuk mengkoneksi diantara network yang menggunakan tipe kabel yang berbeda ataupun topologi yang berbeda pula

2.4.7 Repeater

Repeater merupakan suatu alat untuk menguatkan aliran sinyal yang masuk, repeater akan menggandakan sinyal tersebut lalu mengirimkannya ke tujuan. Contoh yang paling mudah adalah pada sebuah LAN menggunakan topologi Bintang dengan menggunakan kabel unshielded twisted pair. Dimana diketahui panjang maksimal untuk sebuah kabel unshileded twisted pair adalah 100 meter,maka untuk menguatkan sinyal dari kabel tersebut dipasanglah sebuah repeater pada jaringan tersebut



Gambar 2.15 Repeater

2.5 Protocol Jaringan

Protokol adalah aturan-aturan main yang mengatur komunikasi diantara beberapa komputer di dalam sebuah jaringan, aturan itu termasuk di dalamnya petunjuk yang berlaku bagi cara-cara atau metode mengakses sebuah jaringan, topologi fisik, tipe-tipe kabel dan kecepatan transfer data. Protokol-Protokol yang dikenal adalah sebagai berikut :

1. Ethernet
2. Local Talk
3. Token Ring
4. FDDI
5. ATM

2.5.1 Ethernet

Ethernet mula-mula dikembangkan oleh Digital Equipment Cooporation (DEC), Intel dan Xerox mulai tahun 1980. Usaha pembakuan telah dilakukan oleh *Intitute Of Electronic and Electrical Engineers* (IEEE). Pembakuan atau standar ini dikenal sebagai standar IEEE 802.3 yang menjadi dasar perkembangan Ethernet selanjutnya. Protocol Ethernet sejauh ini adalah protocol yang paling banyak digunakan, Ethernet menggunakan metode akses yang disebut CSMA/CD *(Carrier Sense Multiple Access/Collision Detection)*. Sistem ini menjelaskan bahwa setiap komputer memperhatikan ke dalam kabel dari network sebelum mengirimkan sesuatu ke dalamnya. Jika dalam jaringan tidak ada aktifitas atau bersih komputer akan mentransmisikan data, jika ada transmisi lain di dalam kabel, komputer akan menunggu dan akan mencoba kembali transmisi jika jaringan telah bersih. Kadangkala dua buah komputer melakukan transmisi pada saat yang sama, ketika hal ini terjadi, masingmasing komputer akan mundur dan akan menunggu kesempatan secara acak untuk mentransmisikan data kembali. Metode ini dikenal dengan koalisi, dan tidak akan berpengaruh pada kecepatan transmisi dari network. Ada beberapa macam tipe jaringan Ethernet antara lain sebagai berikut :

- 10 Base-5 menggunakan kabel coaxcial tebal (RJ-8)
- 10 Base-2 menggunakan kabel coaxcial tipis (RJ-58)
- 10 Base-36 menggunakan kabel broadband
- 10 Base-T menggunakan kabel UTP kategori 3 (UTP Cat-3)
- 10 Base-F menggunakan kabel serat optik (fiber optic)

Sebagai perkembangan dari standar ethernet 802.3 ditetapkan standar jaringan Fast Ethernet IEEE 802.3u untuk jaringan ethernet yang memerlukan kecepatan transmisi yang lebih tinggi. Standar ini meningkatkan kecepatan jaringan Ethernet dari 10 Mbps menjadi 100 Mbps dengan perubahan pada struktur kabel. Ada tiga tipe jaringan fast Ethernet yaitu :

- 100 Base-TX menggunakan kabel UTP cat-5
- 100 Base-FX menggunakan kabel serat optik

- 100 Base-T4 menggunakan kabel UTP cat-3

Standar 100 Base-TX menjadi popular karena sangat kompatibel dengan standar 10 Base-T. Perkembangan berikutnya dari jaringan Ethernet adalah Gigabit Ethernet yang menggunakan standar IEEE 802.3z. sistem jaringan ini mampu melakukan transmisi data maksimum sampai 1000 Mbps. Ada dua tipe jaringan ini yaitu :

- 1000 Base-X menggunakan kabel serat optik dan twinax
- 1000 Base-T menggunakan kabel UTP cat-5e

2.5.2 Local Talk

LocalTalk adalah sebuh protokol network yang dikembangkan oleh Apple Komputer, Inc ntuk mesin-mesin komputer Macintosh . Metode yang digunakan oleh LocalTalk adalah CSMA/CA *(Carrier Sense Multiple Access with Collision Avoidance).* Hampir sama dengan CSMA/CD. Adapter LocalTalk dan cable twisted pair khusus dapat digunakan untuk menghubungkan beberapa komputer melewati port serial. Sistem operasi Macintosh memungkinkan koneksi secara jaringan peer-to-peer tanpa membutuhkan tambahan aplikasi khusus Protokol LocalTalk dapat digunakan untuk model jaringan garis lurus, bintang, ataupun model pohon dengan menggunakan kabel twisted pair . Kekurangan yang paling mencolok yaitu kecepatan transmisinya. Kecepatan transmisinya hanya 230 Kbps.

2.5.3 Token Ring

Protokol Token Ring di kembangkan oleh IBM pada pertengahan tahun 1980. Metode Aksesnya melalui lewatnya sebuah token dalam sebuah lingkaran seperti Cincin. Dalam lingkaran token, komputer-komputer dihubungkan satu dengan yang lainnya seperti sebuah cincin. Sebuah sinyal token bergerak berputar dalam sebuah lingkaran (cincin) dalam sebuah jaringan dan bergerak dari sebuah komputer menuju ke komputer berikutnya, jika pada persinggahan di salah satu

komputer ternyata ada data yang ingin ditransmisikan, token akan mengangkutnya ke tempat dimana data itu ingin ditujukan, token bergerak terus untuk saling mengkoneksikan diantara masing-masing komputer. Protokol Token Ring membutuhkan model jaringan bintang atau star dengan menggunakan kabel twisted pair atau kabel fiber optic . Dan dapat melakukan kecepatan transmisi 4 Mbps atau 16 Mbps. Sejalan dengan perkembangan Ethernet, penggunaan Token Ring makin berkurang sampai sekarang.

2.5.4 FDDI

Fiber Distributed Data Interface (FDDI) adalah sebuah Protokol jaringan yang menghubungkan antara dua atau lebih jaringan bahkan pada jarak yang jauh . Metode aksesnya yang digunakan oleh FDDI adalah model token. FDDI menggunakan dua buah topologi ring secara fisik. Proses transmisi baiasanya menggunakan satu buah ring, namun jika ada masalah ditemukan akan secara otomatis menggunakan ring yang kedua. Sebuah keuntungan dari FDDI adalah kecepatan dengan menggunakan fiber optic kabel pada kecepatan 100 Mbps

2.5.5 ATM

ATM adalah singkatan dari Asynchronous Transfer Mode (ATM) yaitu sebuah protokol jaringan yang mentransmisikan pada kecepatan 155 Mbps atau lebih. ATM mentarnsmisikan data kedalam satu paket dimana pada protokol yang lain mentransfer pada besar-kecilnya paket. ATM mendukung variasi media seperti video, CD-audio, dan gambar. ATM bekerja pada model topologi bintang , dengan menggunakan kabel fiber optic ataupun kabel twisted pair. ATM pada umumnya digunakan untuk menghubungkan dua atau lebih LAN . dia juga banyak dipakai oleh Internet Service Providers (ISP) untuk meningkatkan kecepatan akses Internet untuk klien mereka.

2.6 Media Transmisi

Sesuai dengan fungsinya yaitu untuk membawa aliran bit data dari satu komputer ke komputer lainnya, maka dalam pengiriman data memerlukan media

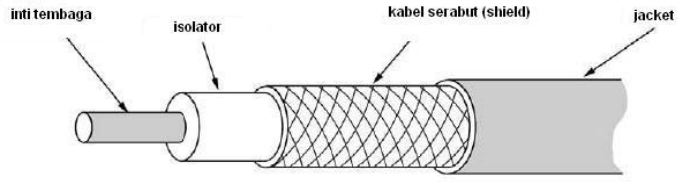
transmisi yang nantinya digunakan untuk keperluan transmisi. Media transmisi memerlukan suatu jalur fisik antara transmitter dan receiver dalam sistem transmisi data. Media transmisi dibagi menjadi dua yaitu :

2.6.1 Media Terarah (Guided Trasmision Data)

Suatu media yang digunakan untuk mengirimkan data, dimana arah ujung yang satu dengan ujung yang lainnya sudah jelas, contoh : kabel. Bila sumber data dan penerima jaraknya tidak terlalu jauh dan dalam area local, maka dapat digunakan kabel sebagai media transmisinya. Kabel merupakan komponen fisik jaringan yang paling rentan dan harus diinstalasi secra cermat dan teliti. Kabel sebagai media transmisi yang terpadu yang secara umum digunakan untuk transmisi data adalah coaxcial, twisted pair, dan fiber optic.

1. **Coaxcial**

   Coaxcial secara umum digunakan sebagai antenna televisi, transmisi telephone jarak jauh, link komputer dan LAN. Coaxcial dapat digunakan untuk sinyal analog maupun digital. Coaxcial terdiri dari dua konduktor, dibentuk untuk beroperasi pada pita frekuensi. Kabel coaxcial terdiri dari dua penghantar yaitu penghantar dalam yang berupa inti tembaga dan penghantar luar yang berbentuk serabut (shield).

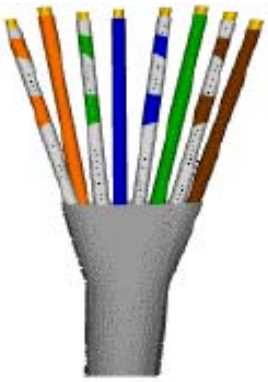


Gambar 2.16 Kabel Coaxial

2. **Twisted Pair**

   Twisted pair merupakan jenis kabel paling sederhana yang paling banyak digunakan dalam membangun jaringan komputer. Kabel berpilin (*Twisted Pair*), menggunakan kabel berpasangan dimana tujuannya untuk

menghilangkan efek *crosstalk*. Banyak digunakan untuk jaringan LAN, dikarenakan mampu mengirimkan bandwidth dengan jumlah yang besar. Kabel ini menggunakan konektor seri *Registered Jack* (RJ), dan tergantung dari jenis kategorinya. Untuk kategori 2 menggunakan RJ11 sedangkan untuk kategori 5 keatas menggunakan RJ-45.



Gambar 2.17 Kabel Twisted Pair

Catagory	**Transfer data maximum**	**Penggunaan**
CAT 1	1 Mbps	Analog Voice, ISDN
CAT 2	4 Mbps	Token ring
CAT 3	16 Mbps	Voice dan data 10 Base T
CAT 4	20 Mbps	16 Mbps Token Ring
CAT 5	100 Mbps	ATM
CAT 5 E	1000 Mbps	Ethernet
CAT 6	400 Mhz	Super Fast broadband
CAT 6 E	500 Mhz	10G Base T
CAT 7	1.2 Ghz	Full Motion Video Teleradiology

Tabel 2.1 Katagory kabel twisted pair

Jenis kabel twisted pair menurut pelindungnya dapat di bagi menjadi :

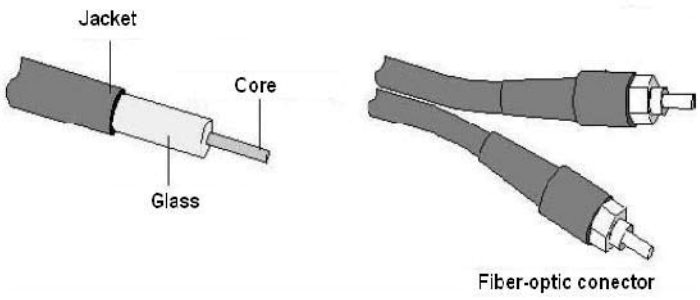
- Unshiled Twisted Pair (UTP)

- Shielded Twisted pair (STP)
- Screened Shielded Twisted Pair (S/STP)
- Screened Unshielded Twisted Pair(S/UTP)

3. Fiber Optik

Fiber optik adalah teknologi perkabelan terkini yang memiliki kecepatan sangat tinggi. Kabel fiber optic bentuknya sama dengan kabel coaxcial. Jenis kabel ini tidak menggunakan tembaga (*cooper*), melainkan serat optik. Dimana sinyal yang dialirkan berupa berkas cahaya. Mampu mengirimkan bandwidth lebih banyak. Banyak digunakan untuk komunikasi antar Backbone, LAN dengan kecepatan tinggi. Pada pusat kebel terdapat inti kaca yang merupakan tempat cahaya akan berpropagasi. Pada fiber bermode banyak, diameter inti sebesar 50 mikron (setebal diameter rambut manusia). Sedangkan fiber bermode tunggal memiliki diameter setebal 8-10 mikron. Berdasarkan jumlah sumber cahaya yang masuk pada core FO, kabel FO dibagi menjadi 2 yaitu:

- Multimode, jumlah sumber lebih dari 1. Menggunakan diameter core dengan ukuran 50 micron – 100 micron
- Singlemode, jumlah sumber 1. Menggunakan diameter core dengan ukuran 2 – 8 micron



Gambar 2.18 Fiber Optik

Sistem komunimasi Fiber optic terdiri dari tiga komponen utama yaitu :

a. Transmitter berupa Laser Diode (LD) dan Light Emmiting Diode (LED)
b. Media transmisi berupa fiber optik
c. Receiver yang merupakan detektor penerima digunakan PIN dan APD.

- **Transmitter**

  Transmitter terdiri dari 2 bagian yaitu :

  a. Rangkaian elektrik berfungsi untuk mengkonversi sinyal digital menjadi sinyal analog, selanjutnya data tersebut ditumpangkan kedalam sinyal gelombang optik yang telah termodulasi
  b. Sumber gelombang optik berupa sinar Laser Diode (LD) dan LED (light emmiting diode) yang pemakaiannya disesuaikan dengan sistem komunikasi yang diperlukan.

Laser Diode dapat digunakan untuk sistem komunikasi optik yang sangat jauh seperti Sistem Komunikasi Kabel Laut (SKKL) dan Sistem Komunikasi Serat Optik (SKSO), karena laser LD mempunyai karakteristik yang handal yaitu dapat memancarkan daya dengan intensitas yang tinggi, stabil, hampir monokromatis, terfokus, dan merambat dengan kecepatan sangat tinggi, sehingga dapat menempuh jarak sangat jauh. Pembuatannya sangat sukar karena memerlukan spesifikasi tertentu sehingga harganya pun mahal. Jadi LD tidak ekonomis dan tidak efisien jika digunakan untuk sistem komunikasi jarak dekat dan pada trafik kurang padat.

- LED digunakan untuk sistem komunikasi jarak sedang dan dekat agar sistem dapat ekonomis dan efektif karena LED lebih mudah pembuatanya, sehingga harganya pun lebih murah.
- *Receiver*

  Receiver atau bagian penerima terdiri dari 2 bagian yaitu detektor penerima dan rangakaian elektrik.

  a. Detektor penerima berfungsi untuk mengkap cahaya yang berupa gelombang optic pembawa informasi, dapat berupa PIN diode atau APD

(Avalance Photo Diode) pemilihannya tergantung keperluan sistem komunikasinya.

- Untuk komunikasi jarak jauh digunakan detektor APD yang dapat bekerja pada panjang gelombang 1300 nm, 1500 nm serta 1550 nm dengan kualitas yang baik. Artinya detektor APD mempunyai sensitivitas dan response yang tinggi terhadap sinar laser LD sebagai pembawa gelombang optik informasi.
- Untuk komunikasi jarak pendek lebih efisien jika menggunakan ditektor PIN diode, karena PIN baik digunakan untuk bit rate rendah dan sensitivitasnya tinggi untuk LED.
- Sumber cahaya LD terlihat memiliki daya lebih besar, stabil, konstan pada bit rate berapapun, sedangkan sumber cahaya LED mempunyai daya pancar yang lebih kecil dan pada bit rate 100 Mbps dayanya mulai menurun.
- Detektor penerima PIN bereaksi baik pada bit rate rendah tetapi kurang sensitif bila bit rate dinaikan.
- Detektor penerima APD lebih sensitif pada bit rate tinggi. Untuk transmisi jarak jauh diperlukan daya pancar yang lebih besar dan sensitifitas yang tinggi, sistem fiber optik akan menggunakan laser LD sebagai sumber cahaya dan APD sebagai detector penerima. Sedangkan untuk transmisi jarak dekat cukup digunakan LED sebagai sumber optik dan PIN sebagai ditektor penerima.

b. Rangkaian elektrik berfungsi untuk mengkonversi cahaya pembawa informasi terhadap data informasi terhadap data informasi yang dibawa dengan melakukan regenerasi timing, regenerasi pulse serta konversi sinyal elektrik ke dalam interface V.28 yang berupa sinyal digital dan sebaliknya.

- *Atenuasi*

Atenuasi adalah besaran pelemahan energi sinyal informasi dari fiber optik yang dinyatakan dalam dB dan disebabkan oleh 3 faktor utama yaitu absorpsi, hamburan (scattering) dan mikro-bending. Gelas yang merupakan bahan

pembuat fiber optik biasanya terbentuk dari silicon-dioksida (SiO2). Variasi indeks bisa diperoleh dengan menambahkan bahan lain seperti titanium, thallium, germanium atau boron. Dengan susunan bahan yang tepat maka akan didapatkan atenuasi yang sekecil mungkin. Atenuasi menyebabkan pelemahan energi sehingga amplitudo gelombang yang sampai pada penerima menjadi lebih kecil dari pada amplitudo yang dikirimkan oleh pemancar.

a. Absorpsi.

Absorpsi merupakan sifat alami suatu gelas. Pada daerah-daerah tertentu gelas dapatmengabsorpsi sebagian besar cahaya seperti pada daerah ultraviolet. Hal ini disebabkan oleh adanya gerakan elektron yang kuat. Demikian pula untuk daerah inframerah, terjadi absorpsi yang besar. Ini disebabkan adanya getaran ikatan kimia.Oleh karena itu sebaiknya penggunaan fiber optik harus menjauhi daerah ultraviolet dan inframerah. Penyebab absorpsi lain adanya transmisi ion-ion logam dan ion OH. Ion OH ini ternyata memberikan sumbangan absorpsi yang cukup besar. Semakin lama usia suatu fiber maka bisa diduga akan semakin banyak ion OH di dalamnya yang menyebabkan kualitas fiber menurun.

b. Hamburan

Seberkas cahaya yang melalui suatu gelas dengan variasi indeks bias disepanjang gelas tadi, sebagian energinya akan hilang dihamburkan oleh benda benda kecil yang

ada di dalam gelas. Hamburan yang disebabkan oleh tumbukan cahaya dengan partikel tersebut dinamakan hamburan Rayleigh. Besarnya hamburan Rayleigh ini berbanding terbalik dengan pangkat empat dari pangjang gelombang cahaya yaitu : $1/\lambda$. Sehingga dapat disimpulkan untuk lamda kecil, hamburan Rayleigh besar dan sebaliknya. Hamburan Rayleigh memberikan loss akibat hamburan sangat kecil dibandingkan dengan loss fiber optik multimode. Karena itu fiber optik singlemode lebih baik mutunya sebagai media transmisi dibandingkan dengan fiber optic multimode.

c. Mikro-bending

Atenuasi lainya adalah atenuasi yang disebabkan mikro-bending yaitu pembengkokan fiber optik untuk memenuhi persyaratan ruangan. Namun pembengkokan dapat pula terjadi secara tidak sengaja seperti misalnya fiber optik yang mendapat tekanan cukup keras sehingga cahaya yang merambat di dalamnya akan berbelok dari arah transmisi dan hilang. Hal ini tentu saja menyebabkan atenuasi.

2.6.2 Media Tak Terarah (Un-Guided Transmision Data)

Suatu media yang digunakan untuk mengirimkan data, dimana arah ujung yang satu dengan ujung yang lainnya tersebar, contoh : nirkabel (*wireless*). Komunikasi ini mengirimkan sinyal ke udara berdasarkan spektrum elektromagnetik.

1. Transmisi Radio

Perkembangan teknologi komunikasi radio sangat pesat, penggunaan wireless LAN sudah semakin populer. Untuk mengirimkan data menggunakan komunikasi radio ada beberapa cara yaitu :

• Memancarkan langsung, sesuai dengan permukaan bumi

• Dipantulkan melalui lapisan atmosfir

Komunikasi radio ini menggunakan frekuensi khusus supaya tidak mengakibatkan *interference* dengan penggunaan frekuensi lainnya, frekuensi yang boleh digunakan disebut ISM band. ISM singkatan dari *Industrial, Scientific and Medical*.

2. Komunikasi Satelit

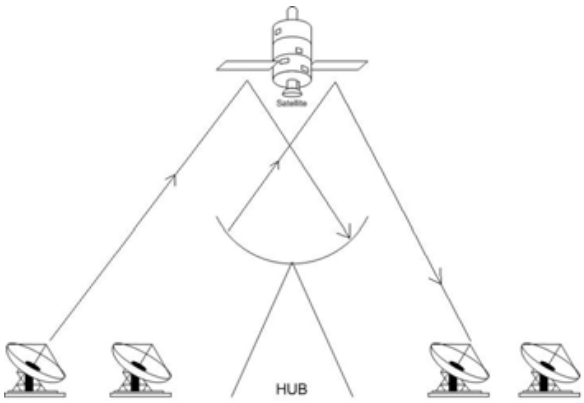
Komunikasi ini digunakan untuk komunikasi jarak jauh atau antar benua. Dimana untuk menghubungkannya diperlukan teknologi satelit. Menurut jaraknya satelit bias dikategorikan menjadi :

• Geostationary

• Medium-Earth Orbit

• Low-Earth Orbit

Untuk menghubungi *site* yang lain, bisa dilakukan dengan *Very Small Aperture Terminal* (VSAT). VSAT adalah sebuah stasiun bumi kecil yang bekerja pada satelit geostasioner, dan digunakan untuk berbagai aplkasi di dunia telekomunikasi, termasuk data interaktif pelayanan komunikasi suara, data, video digital serta dapat diaplikasikan untuk jaringan WAN (Wide Area Network). Jaringan VSAT sendiri dapat diintgrasikan dengan jaringan lain yang sudah ada misalnya PSTN dan jaringan internet.VSAT merupakan suatu mikristation yang dapat menghubungkan dua tempat yang secara geografis sangat berjauhan. Hubungan antara dua buah VSAT menggunakan perantara satelit. Terminal ini memiliki antena setinggi 1 meter dan membutuhkan daya sekitar 1 watt. VSAT memiliki kecepatan uplik sebesar 19.2 Bps, sedangkan kecepatan downlinknya bias mencapai 512 Kbps. Untuk merelay komunikasi antara dua buah VSAT yang berjauhan, diperlukan stasiun bumi khusus yang dinamakan hub (hub disini berbeda dengan hub pada LAN). VSAT memiliki dua unit bagian, yaitu Indoor Unit dan Outdoor Unit. Indoor unit terdiri dari moden dan interface yang menghubungaka ke peralatan pelanggan sepertan komputer, LAN, Telephones, atau PABX. Sedangkan Outdoor unit terdiri dari antena, Up- Down Converter, penguat SSPA, dan LNA. Diameter antena biasanya antara 1,8 meter sampai 3,8 meter. Antara indoor dan outdoor dihubungkan oleh IFL (Inter Facility Link) berupa kebel coaxcial dengan redaman yang kecil. Keuntungan menggunakan VSAT adalah baik pengirim atau penerima tidak tergantung pada letak geografisnya. Disamping keuntungan adapula kerugiannya VSAT adalah Delay time yang lama.



Gambar 2.19 Komunikasi satelit dengan VSAT

2.7 IP Address

Pembagian kelas-kelas IP address didasarkan pada dua hal : *network ID* dan *host ID* dari suatu IP address. Setiap IP address selalu merupakan sebuah pasangan dari *network-ID* (identitas jaringan) dan host-ID (identitas host dalam jarinangan tersebut). *Network-ID* ialah bagian dari IP address yang digunakan untuk menunjukkan jaringan tempat komputer ini berada. Sedangkah *host-ID* ialah bagian dari IP address yang digunakan untuk menunjukkan workstation, server, router, dan semua host TCP/IP lainnya dalam jaringan terserbut. Dalam satu jaringan, *host-ID* ini harus unik (tidak boleh ada yang sama)

Kelas-kelas IP Address :

- **Kelas A**

  Format : 0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

  Bit Pertama : 0

  Panjang Net ID : 8 bit

  Pangjang Host ID : 24 bit

  Byte Pertama : 0-127

  Jumlah : 126 Kelas A (0 dan 127 dicadangkan)

Range IP : 1.xxx.xxx.xxx sampai 126.xxx.xxx.xxx

Jumlah IP : 16.777.214 IP address pada tiap kelas A

❖ **Kelas B**

Format : 10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh

Bit Pertam : 10

Panjang Net ID : 16 bit

Pangjang Host ID : 16 bit

Byte Pertama : 128-191

Jumlah : 16.184 Kelas B

Range IP : 128.0.xxx.xxx sampai 191.255.xxx.xxx

Jumlah IP : 65.532 IP address pada tiap kelas B

❖ **Kelas C**

Format : 110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh

Bit Pertama : 110

Panjang Net ID : 24 bit

Pangjang Host ID : 8 bit

Byte Pertama : 192-223

Jumlah : 2.097.152 Kelas C

Range IP : 192.0.0.xxx sampai 191.255.255.xxx

Jumlah IP : 254 IP address pada tiap kelas C

❖ **Kelas D**

Format :

1110mmmm.mmmmmmmm.mmmmmmmm.mmmmmmmm

4 Bit Pertama : 1110

Bit Multicast : 28 Bit

Byte Inisial : 224-247

Deskripsi : Kelas D adalah ruang alamat multicast (RFC 1112)

- **Kelas E**

Format : 1111rrrr. rrrrrrrr. rrrrrrrr.rrrrrrrr

4 Bit Pertama : 1111

Bit Multicast : 28 Bit

Byte Inisial : 248-255

Deskripsi : Kelas E adalah ruang alamat yang dicadangkan untuk kepeluan eksperimental.

2.8 Subnetting IP Address

Subnetting IP Address adalah Efisiensi dalam penggunaan IP Address supaya dapat mengalamati semaksimal mungkin host yang ada dalam satu jaringan. Tujuan lain dari subnetting adalah untuk mengurangi tingkat congesti dalam suatu network. Untuk menghindari terjadinya congesti(tabrakan) akibat terlalu banyak host dalam suatu physical network, dilakukan segmentasi jaringan.

2.9 Subnet Mask

Suatu subnet didefinisikan dengan mengimplementasikan masking bit (Subnet Mask) kepada IP address. Strukturnya terdiri dari 32 bit yang dibagi atas empat segmen. Bentuk subnet mask adalah urutan bit 1, diikuti bit 0. jumlah bit 1 menentukan tingkat subnet mask. Contoh subnet mask :

NO	Subnet Mask (biner)	Desimal	Hexa	Tingkat
1	11111111.11111111.00000000.000.0000	255.255.0.0	FF.FF.00.00	16 bit

2	11111111.11111111.11111111.0000.0000	55.2255.255.0	FF.FF.FF.00	24 bit
3	11111111.11111111.11111111.1000.0000	255.255.255.128	FF.FF.FF.80	25 bit
4	11111111.11111111.11111111.1100.0000	255.255.255.192	FF.FF.FF.C0	26 bit
5	11111111.11111111.11111111.1110.0000	255.255.255.224	FF.FF.FF.E0	27 bit

Tabel 2.2 klasifikasi kelas IP address

- **Implementasi Subnetting pada LAN**

Komposisi	Tinjauan 8 bit (segmen ke 4)		Jumlah Network	Jumlah Host	Subnet Mask (32 bit/4sgmn)
	Bit network	Bit Host			
hhhhhhhh	**0**	**8**	**2^0 = 1**	**2^8 = 256**	**24**
nhhhhhhh	**1**	**7**	**2^1 = 2**	**2^7 = 128**	**25**
nnhhhhhh	**2**	**6**	**2^2 = 4**	**2^6 = 64**	**26**
nnnhhhhh	**3**	**5**	**2^3 = 8**	**2^5 = 32**	**27**
nnnnhhhh	**4**	**4**	**2^4 = 16**	**2^4 = 16**	**28**
nnnnnhhh	**5**	**3**	**2^5 = 32**	**2^3 = 8**	**29**
nnnnnnh	***6***	***2***	***2^6 = 64***	***2^2 = 4***	***30***

Tabel 2.3 kalsifikasi subnetting LAN

2.10 Internet Working

Internet adalah suatu jaringan global yang terbentuk dari jaringan-jaringan local dan regional yang memungkinkan komunikasi data antar computer yang terhubung ke jaringan tersebut.

1. **Protokol**

   Agar computer-komputer dalam satu jaringan dapat berkomunikasi, maka dibutuhkan suatu protokol atau suatu aturan standar komunikasi baik antar computer ataupun antar jaringan komputer. Contohnya : IPX/SPX dan AppleTalk.

2. **Standar TCP/IP**

   Protokol TCP/IP dibuat lima lapisan yaitu : physical, data link, network, transport dan application. Protokol TCP/IP mendefinisikan 2 buah protocol yakni Transmision Control Protocol (TCP) dan User Datagram Protocol (UDP). Pada lapisan ketiga, TCP/IP mendefinisikan sebagai Internetworking Protocol (IP), namun ada beberapa protocol lain yang mendukung pergerakan data pada lapisan ini. Badan-Badan Pengatur Internet. Ada bebrapa Badan yang bertanggung jawab dalam mengatur, mengontrol serta melakukan standarisasi protocol yang digunakan, di antaranya :

a. *Internet Society* (ISOC), merupakan badan profesional yang memfasilitasi, mendukung, serta mempromosikan pertumbuhan internet, sebagai infrastruktur komunikasi global untuk riset. Badan ini berurusan tidak hanya dengan aspek-aspek teknis, namun juga aspek politik dan sosial dari jaringan internet.

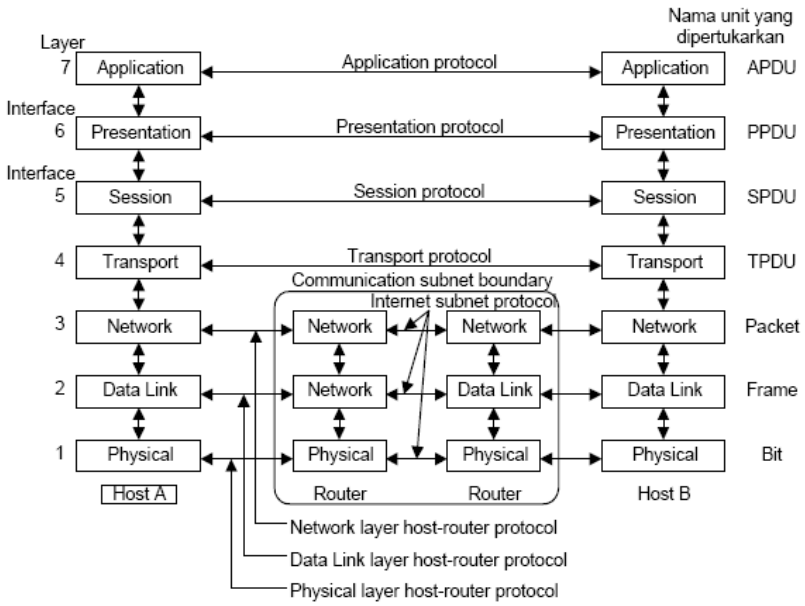
b. *Internet Architecture Board* (IAB), merupakan badan koordinasi dan penasehat teknis bagi *Internet Society*. Badan ini bertindak sebagai *review* teknis dan editorial akhir semua standar internet. IAB memiliki otoritas

untuk menerbitkan dokumen standar internet yang dikenal sebagai RFC (*Request For Comment*). Tugas lain IAB ialah mengatur angka-angka dan konstanta yang digunakan dalam protokol internet (nomor port TCP, kode protokol IP,dll).

c. *Internet Engineering Task Force* (IETF), badan yang berorientasi untuk membentuk standar internet. IETF dibagi dalam sembilan kelompok kerja (misalnya aplikasi, *routing* dan *addressing*, keamanan komputer) dan bertugas menghasilkan standar-standar internet.Internet Research Task Force (IRTF) ialah badan yang memiliki orientasi pada riset-riset jangka panjang.

2.11 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.



Gambar 2.20 Model OSI

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 protocol 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 OSI memiliki tujuh layer. Prinsip-prinsip yang digunakan bagi ketujuh layer tersebut adalah :

1. Sebuah layer harus dibuat bila diperlukan tingkat abstraksi yang berbeda.
2. Setiap layer harus memiliki fungsi-fungsi tertentu.
3. Fungsi setiap layer harus dipilih dengan teliti sesuai dengan ketentuan standar protocol internasional.
4. Batas-batas layer diusahakan agar meminimalkan aliran informasi yang melewati interface.
5. Jumlah layer harus cukup banyak, sehingga fungsi-fungsi yang berbeda tidak perlu disatukan dalam satu layer diluar keperluannya. Akan tetapi jumlah layer juga harus diusahakan sesedikit mungkin sehingga arsitektur jaringan tidak menjadi sulit dipakai.

2.11.1 Karakteristik Lapisan OSI

Ke tujuh lapisan dari model referensi OSI dapat dibagi ke dalam dua kategori, yaitu lapisan atas dan lapisan bawah. Lapisan atas dari model OSI berurusan dengan persoalan aplikasi dan pada umumnya diimplementasi hanya pada software. Lapisan tertinggi (lapisan applikasi) adalah lapisan penutup sebelum ke pengguna (user), keduanya, pengguna dan lapisan aplikasi saling berinteraksi proses dengan software aplikasi yang berisi sebuah komponen komunikasi. Istilah lapisan atas kadang-kadang digunakan untuk menunjuk ke beberapa lapisan atas dari lapisan lapisan yang lain di model OSI. Lapisan bawah dari model OSI mengendalikan persoalan transport data. Lapisan fisik dan lapisan data link diimplementasikan ke dalam hardware dan software. Lapisan-lapisan bawah yang lain pada umumnya hanya diimplementasikan dalam software.

Lapisan terbawah, yaitu lapisan fisik adalah lapisan penutup bagi media jaringan fisik (misalnya jaringan kabel), dan sebagai penanggung jawab bagi penempatan informasi pada media jaringan.

1. Physical Layer

Physical Layer berfungsi dalam pengiriman raw bit ke channel komunikasi. Masalah desain yang harus diperhatikan disini adalah memastikan bahwa bila satu sisi mengirim data 1 bit, data tersebut harus diterima oleh sisi lainnya sebagai 1 bit pula, dan bukan 0 bit. Pertanyaan yang timbul dalam hal ini adalah : berapa volt yang perlu digunakan untuk menyatakan nilai 1? dan berapa volt pula yang diperlukan untuk angka 0?. Diperlukan berapa mikrosekon suatu bit akan habis? Apakah transmisi dapat diproses secara simultan pada kedua arahnya? Berapa jumlah pin yang dimiliki jaringan dan apa kegunaan masing-masing pin? Secara umum masalah-masalah desain yang ditemukan di sini berhubungan secara mekanik, elektrik dan interface prosedural, dan media fisik yang berada di bawah physical layer.

2. Data Link Layer

Tugas utama data link layer adalah sebagai fasilitas transmisi raw data dan mentransformasi data tersebut ke saluran yang bebas dari kesalahan transmisi. Sebelum diteruskan kenetwork layer, data link layer melaksanakan tugas ini dengan memungkinkan pengirim memecag-mecah data input menjadi sejumlah data frame (biasanya berjumlah ratusan atau ribuan byte). Kemudian data link layer mentransmisikan frame tersebut secara berurutan, dan memproses acknowledgement frame yang dikirim kembali oleh penerima. Karena physical layer menerima dan mengirim aliran bit tanpa mengindahkan arti atau arsitektur frame, maka tergantung pada data link layer-lah untuk membuat dan mengenali batas-batas frame itu. Hal ini bisa dilakukan dengan cara membubuhkan bit khusus ke awal dan akhir frame. Bila secara insidental pola-pola bit ini bisa

ditemui pada data, maka diperlukan perhatian khusus untuk menyakinkan bahwa pola tersebut tidak secara salah dianggap sebagai batas-batas frame.

Terjadinya noise pada saluran dapat merusak frame. Dalam hal ini, perangkat lunak data link layer pada mesin sumber dapat mengirim kembali frame yang rusak tersebut. Akan tetapi transmisi frame sama secara berulang-ulang bisa menimbulkan duplikasi frame. Frame duplikat perlu dikirim apabila acknowledgement frame dari penerima yang dikembalikan ke pengirim telah hilang. Tergantung pada layer inilah untuk mengatasi masalah-masalah yang disebabkan rusaknya, hilangnya dan duplikasi frame. Data link layer menyediakan beberapa kelas layanan bagi network layer. Kelas layanan ini dapat dibedakan dalam hal kualitas dan harganya. Masalah-masalah lainnya yang timbul pada data link layer (dan juga sebagian besar layer-layer di atasnya) adalah mengusahakan kelancaran proses pengiriman data dari pengirim yang cepat ke penerima yang lambat. Mekanisme pengaturan lalu-lintas data harus memungkinkan pengirim mengetahui jumlah ruang buffer yang dimiliki penerima pada suatu saat tertentu. Seringkali pengaturan aliran dan penanganan error ini dilakukan secara terintegrasi. Saluran yang dapat mengirim data pada kedua arahnya juga bisa menimbulkan masalah. Sehingga dengan demikian perlu dijadikan bahan pertimbangan bagi software data link layer. Masalah yang dapat timbul di sini adalah bahwa frame-frame acknoeledgement yang mengalir dari A ke B bersaing saling mendahului dengan aliran dari B ke A. Penyelesaian yang terbaik (piggy backing) telah bisa digunakan; nanti kita akan membahasnya secara mendalam. Jaringan broadcast memiliki masalah tambahan pada data link layer. Masalah tersebut adalah dalam hal mengontrol akses ke saluran yang dipakai bersama. Untuk mengatasinya dapat digunakan sublayer khusus data link layer, yang disebut medium access sublayer.

3. Network Layer

Network layer berfungsi untuk pengendalian operasi subnet. Masalah desain yang penting adalah bagaimana caranya menentukan route pengiriman paket dari sumber ke tujuannya. Route dapat didasarkan pada table statik yang

“dihubungkan ke” network. Route juga dapat ditentukan pada saat awal percakapan misalnya session terminal. Terakhir, route dapat juga sangat dinamik, dapat berbeda bagi setiap paketnya. Oleh karena itu, route pengiriman sebuah paket tergantung beban jaringan saat itu. Bila pada saat yang sama dalam sebuah subnet terdapat terlalu banyak paket, maka ada kemungkinan paket-paket tersebut tiba pada saat yang bersamaan. Hal ini dapat menyebabkan terjadinya bottleneck. Pengendalian kemacetan seperti itu juga merupakan tugas network layer.

Karena operator subnet mengharap bayaran yang baik atas tugas pekerjaannya. seringkali terdapat beberapa fungsi accounting yang dibuat pada network layer. Untuk membuat informasi tagihan, setidaknya software mesti menghitung jumlah paket atau karakter atau bit yang dikirimkan oleh setiap pelanggannya. Accounting menjadi lebih rumit, bilamana sebuah paket melintasi batas negara yang memiliki tarip yang berbeda. Perpindahan paket dari satu jaringan ke jaringan lainnya juga dapat menimbulkan masalah yang tidak sedikit. Cara pengalamatan yang digunakan oleh sebuah jaringan dapat berbeda dengan cara yang dipakai oleh jaringan lainnya. Suatu jaringan mungkin tidak dapat menerima paket sama sekali karena ukuran paket yang terlalu besar. Protokolnyapun bias berbeda pula, demikian juga dengan yang lainnya. Network layer telah mendapat tugas untuk mengatasi semua masalah seperti ini, sehingga memungkinkan jaringan-jaringan yang berbeda untuk saling terinterkoneksi.

4. Transport Layer

Fungsi dasar transport layer adalah menerima data dari session layer, memecah data menjadi bagian-bagian yang lebih kecil bila perlu, meneruskan data ke network layer, dan menjamin bahwa semua potongan data tersebut bisa tiba di sisi lainnya dengan benar. Selain itu, semua hal tersebut harus dilaksanakan secara efisien, dan bertujuan dapat melindungi layer-layer bagian atas dari perubahan teknologi hardware yang tidak dapat dihindari. Dalam keadaan normal, transport layer membuat koneksi jaringan yang berbeda bagi setiap koneksi transport yang diperlukan oleh session layer. Bila koneksi transport memerlukan throughput yang tinggi, maka transport layer dapat membuat koneksi jaringan yang banyak.

Transport layer membagi-bagi pengiriman data ke sejumlah jaringan untuk meningkatkan throughput. Di lain pihak, bila pembuatan atau pemeliharaan koneksi jaringan cukup mahal, transport layer dapat menggabungkan beberapa koneksi transport ke koneksi jaringan yang sama. Hal tersebut dilakukan untuk membuat penggabungan ini tidak terlihat oleh session layer. Transport layer juga menentukan jenis layanan untuk session layer, dan pada gilirannya jenis layanan bagi para pengguna jaringan. Jenis transport layer yang paling populer adalah saluran error-free point to point yang meneruskan pesan atau byte sesuai dengan urutan pengirimannya. Akan tetapi, terdapat pula jenis layanan transport lainnya. Layanan tersebut adalah transport pesan terisolasi yang tidak menjamin urutan pengiriman, dan membroadcast pesan-pesan ke sejumlah tujuan. Jenis layanan ditentukan pada saat koneksi dimulai. Transport layer merupakan layer end to end sebenarnya, dari sumber ke tujuan. Dengan kata lain, sebuah program pada mesin sumber membawa percakapan dengan program yang sama dengan pada mesin yang dituju. Pada layer-layer bawah, protokol terdapat di antara kedua mesin dan mesin-mesin lain yang berada didekatnya. Protokol tidak terdapat pada mesin sumber terluar atau mesin tujuan terluar, yang mungkin dipisahkan oleh sejumlah router. Perbedaan antara layer 1 sampai 3 yang terjalin, dan layer 4 sampai 7 yang end to end. Sebagai tambahan bagi penggabungan beberapa aliran pesan ke satu channel, transport layer harus hati-hati dalam menetapkan dan memutuskan koneksi pada jaringan. Proses ini memerlukan mekanisma penamaan, sehingga suatu proses pada sebuah mesin mempunyai cara untuk menerangkan dengan siapa mesin itu ingin bercakap-cakap. Juga harus ada mekanisme untuk mengatur arus informasi, sehingga arus informasi dari host yang cepat tidak membanjiri host yang lambat. Mekanisme seperti itu disebut pengendalian aliran dan memainkan peranan penting pada transport layer (juga pada layer-layer lainnya). Pengendalian aliran antara host dengan host berbeda dengan pengendalian aliran router dengan router. Kita akan mengetahui nanti bahwa prinsip-prinsip yang sama digunakan untuk kedua jenis pengendalian tersebut.

5. Session Layer

Session layer mengijinkan para pengguna untuk menetapkan session dengan pengguna lainnya. Sebuah session selain memungkinkan transport data biasa, seperti yang dilakukan oleh transport layer, juga menyediakan layanan yang istimewa untuk aplikasi-aplikasi tertentu. Sebuah session digunakan untuk memungkinkan seseorang pengguna log ke remote timesharing system atau untuk memindahkan file dari satu mesin kemesin lainnya. Sebuah layanan session layer adalah untuk melaksanakan pengendalian dialog. Session dapat memungkinkan lalu lintas bergerak dalam bentuk dua arah pada suatu saat, atau hanya satu arah saja. Jika pada satu saat lalu lintas hanya satu arah saja (analog dengan rel kereta api tunggal), session layer membantu untuk menentukan giliran yang berhak menggunakan saluran pada suatu saat. Layanan session di atas disebut manajemen token. Untuk sebagian protokol, adalah penting untuk memastikan bahwa kedua pihak yang bersangkutan tidak melakukan operasi pada saat yang sama. Untuk mengatur aktivitas ini, session layer menyediakan token-token yang dapat digilirkan. Hanya pihak yang memegang token yang diijinkan melakukan operasi kritis. Layanan session lainnya adalah sinkronisasi. Ambil contoh yang dapat terjadi ketika mencoba transfer file yang berdurasi 2 jam dari mesin yang satu ke mesin lainnya dengan kemungkinan mempunyai selang waktu 1 jam antara dua crash yang dapat terjadi. Setelah masing-masing transfer dibatalkan, seluruh transfer mungkin perlu diulangi lagi dari awal, dan mungkin saja mengalami kegagalan lain. Untuk mengurangi kemungkinan terjadinya masalah ini, session layer dapat menyisipkan tanda tertentu ke aliran data. Karena itu bila terjadi crash, hanya data yang berada sesudah tanda tersebut yang akan ditransfer ulang.

6. Pressentation Layer

Pressentation layer melakukan fungsi-fungsi tertentu yang diminta untuk menjamin penemuan sebuah penyelesaian umum bagi masalah tertentu. Pressentation Layer tidak mengijinkan pengguna untuk menyelesaikan sendiri suatu masalah. Tidak seperti layer-layer di bawahnya yang hanya melakukan pemindahan bit dari satu tempat ke tempat lainnya, presentation layer memperhatikan syntax dan semantik informasi yang dikirimkan. Satu contoh

layanan pressentation adalah encoding data. Kebanyakan pengguna tidak memindahkan string bit biner yang random. Para pengguna saling bertukar data sperti nama orang, tanggal, jumlah uang, dan tagihan. Item-item tersebut dinyatakan dalam bentuk string karakter, bilangan interger, bilangan floating point, struktur data yang dibentuk dari beberapa item yang lebih sederhana. Terdapat perbedaan antara satu komputer dengan computer lainnya dalam memberi kode untuk menyatakan string karakter (misalnya, ASCII dan Unicode), integer (misalnya komplemen satu dan komplemen dua), dan sebagainya. Untuk memungkinkan dua buah komputer yang memiliki presentation yang berbeda untuk dapat berkomunikasi, struktur data yang akan dipertukarkan dapat dinyatakan dengan cara abstrak, sesuai dengan encoding standard yang akan digunakan “pada saluran”. Presentation layer mengatur data-struktur abstrak ini dan mengkonversi dari representation yang digunakan pada sebuah komputer menjadi representation standard jaringan, dan sebaliknya.

7. Application Layer

Application layer terdiri dari bermacam-macam protokol. Misalnya terdapat ratusan jenis terminal yang tidak kompatibel di seluruh dunia. Ambil keadaan dimana editor layar penuh yang diharapkan bekerja pada jaringan dengan bermacam-macam terminal, yang masing-masing memiliki layout layar yang berlainan, mempunyai cara urutan penekanan tombol yang berbeda untuk penyisipan dan penghapusan teks, memindahkan sensor dan sebagainya. Suatu cara untuk mengatasi masalah seperti di ata, adalah dengan menentukan terminal virtual jaringan abstrak, serhingga editor dan program-program lainnya dapat ditulis agar saling bersesuaian. Untuk menangani setiap jenis terminal, satu bagian software harus ditulis untuk memetakan fungsi terminal virtual jaringan ke terminal sebenarnya. Misalnya, saat editor menggerakkan cursor terminal virtual ke sudut layar kiri, software tersebut harus mengeluarkan urutan perintah yang sesuai untuk mencapai cursor tersebut. Seluruh software terminal virtual berada pada application layer. Fungsi application layer lainnya adalah pemindahan file. Sistem file yang satu dengan yang lainnya memiliki konvensi penamaan yang

berbeda, cara menyatakan barisbaris teks yang berbeda, dan sebagainya. Perpindahan file dari sebuah sistem ke system lainnya yang berbeda memerlukan penanganan untuk mengatasi adanya ketidakkompatibelan ini. Tugas tersebut juga merupakan pekerjaan appication layer, seperti pada surat elektronik, remote job entry, directory lookup, dan berbagai fasilitas bertujuan umum dan fasilitas bertujuan khusus lainnya.

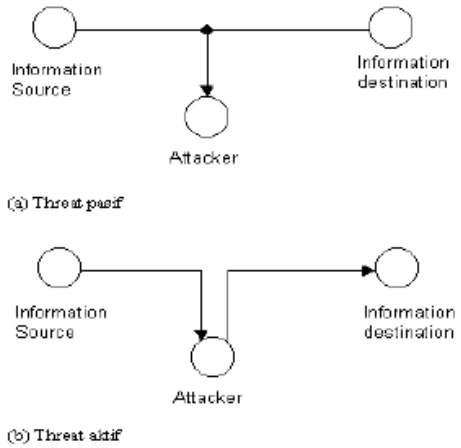
2.12 Keamanan Jaringan

Keamanan jaringan saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan sistem saat ini menjadi suatu garapan yang membutuhkan biaya penanganan dan proteksi yang sedemikian besar. Sistem-sistem vital seperti sistem pertahanan, sistem perbankan dan sistem-sistem setingkat itu, membutuhkan tingkat keamanan yang sedemikian tinggi. Hal ini lebih disebabkan karena kemajuan bidang jaringan komputer dengan konsep open sistemnya sehingga siapapun, di manapun dan kapanpun, mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut. Keamanan jaringan didefinisikan sebagai sebuah perlindungan dari sumber daya daya terhadap upaya penyingkapan, modifikasi, utilisasi, pelarangan dan perusakan oleh person yang tidak diijinkan. Beberapa insinyur jaringan mengatakan bahwa hanya ada satu cara mudah dan ampuh untuk mewujudkan sistem jaringan komputer yang aman yaitu dengan menggunakan pemisah antara komputer dengan jaringan selebar satu inci, dengan kata lain, hanya komputer yang tidak terhubung ke jaringanlah yang mempunyai keamanan yang sempurna. Meskipun ini adalah solusi yang buruk, tetapi ini menjadi trade-off antara pertimbangan fungsionalitas dan memasukan kekebalan terhadap gangguan. Protokol suatu jaringan sendiri dapat dibuat aman. Server-server baru yang menerapkan protokol-protokol yang sudah dimodifikasi harus diterapkan. Sebuah protokol atau layanan (service) dianggap cukup aman apabila mempunyai kekebalan ITL klas 0 (tentang ITL akan dibahas nanti). Sebagai contoh, protokol seperti FTP atau Telnet, yang sering mengirimkan password secara terbuka melintasi jaringan, dapat dimodifikasi dengan menggunakan teknik enkripsi. Jaringan daemon, seperti

sendmail atau fingerd, dapat dibuat lebih aman oleh pihak vendor dengan pemeriksaan kode dan patching. Bagaimanapun, permasalahan miskonfigurasi, seperti misalnya spesifikasi yang tidak benar dari netgroup, dapat menimbulkan permasalahan kekebalan (menjadi rentan). Demikian juga kebijakan dari departemen teknologi informasi seringkali memunculkan kerumitan pemecahan masalah untuk membuat sistem menjadi kebal.

1. Tipe *Threat*

Terdapat dua kategori threat yaitu ***threat* pasif** dan ***threat* aktif**. ***Threat* pasif** melakukan pemantauan dan atau perekaman data selama data ditranmisikan lewat fasilitas komunikasi. Tujuan penyerang adalah untuk mendapatkan informasi yang sedang dikirimkan. Kategori ini memiliki dua tipe *yaitu release of message contain* dan *traffic analysis*. Tipe *Release of message contain* memungkinan penyusup utnuk mendengar pesan, sedangkan tipe *traffic analysis* memungkinan penyusup untuk membaca *header* dari suatu paket sehingga bisa menentukan arah atau alamat tujuan paket dikirimkan. Penyusup dapat pula menentukan panjang dan frekuensi pesan.



Gambar 2.21 Kategori threat

***Threat* aktif** merupakan pengguna gelap suatu peralatan terhubung fasilitas komunikasi untuk mengubah transmisi data atau mengubah isyarat kendali atau memunculkandata atau isyarat kendali palsu. Untuk kategori ini terdapat tida tipe

yaitu : *message-stream modification, denial of message service* dan *masquerade*. Tipe *message-stream modification* memungkinan pelaku untuk memilih untuk menghapus, memodifikasi, menunda, melakukan reorder dan menduplikasi pesan asli. Pelaku juga mungkin untuk menambahkan pesan-pesan palsu. Tipe *denial of message service* memungkinkan pelaku untuk merusak atau menunda sebagian besar atau seluruh pesan. Tipe *masquerade* memungkinkan pelaku untuk menyamar sebagi host atau switch asli dan berkomunikasi dengan yang host yang lain atau switch untuk mendapatkan data atau pelayanan.

2. Internet Threat Level

Celah-celah keamanan sistem internet, dapat disusun dalam skala klasifikasi. Skala klasifikasi ini disebut dengan istilah skala Internet Threat Level atau skala ITL. Ancaman terendah digolongkan dalam ITL kelas 0, sedangkan ancaman tertinggi digolongkan dalam ITL kelas 9. Kebanyakan permasalahan keamanan dapat diklasifikasikan ke dalam 3 kategori utama, tergantung pada kerumitan perilaku ancaman kepada sistem sasaran, yaitu:

• Ancaman-ancaman lokal.
• Ancaman-ancaman remote.
• Ancaman-ancaman dari lintas firewall.

Selanjutnya klasifikasi ini dapat dipisah dalam derajat yang lebih rinci, yaitu :

• *Read access*
• *Non-root write and execution access*
• *Root write and execution access*

Table Skala Internet Threat Level (ITL)

Kelas	**Penjelasan**
0	Denial of service attack—user tidak dapat mengakses file atau program

1	Local users can gain read access to files on the local system.
2	Local users can gain write and/or execution access to non–root-owned files on the system
3	Local users can gain write and/or execution access to root-owned files on the system.
4	Remote users on the same network can gain read access to files on the system or transmitted over the network
5	Remote users on the same network can gain write and/or execution access to non–root-owned files on the system or transmitted over the network
6	Remote users on the same network can gain write and/or execution access to root-owned files on the system.
7	Remote users across a firewall can gain read access to files on the system or transmitted over the network.
8	Remote users across a firewall can gain write and/or execution access to non–root-owned files on the system or transmitted over the network
9	Remote users across a firewall can gain write and/or execution access to root-owned files on the system.

Tabel 2.4 Skala Internet Threat Level (ITL)

Seberapa besar tingkat ancaman dapat diukur dengan melihat beberapa faktor, antara lain :

• Kegunaan sistem
• Kerahasiaan data dalam sistem.
• Tingkat kepetingan dari integritas data
• Kepentingan untuk menjaga akses yang tidak boleh terputus
• Profil pengguna
• Hubungan antara sistem dengan sistem yang lain.

3. *Enkripsi*

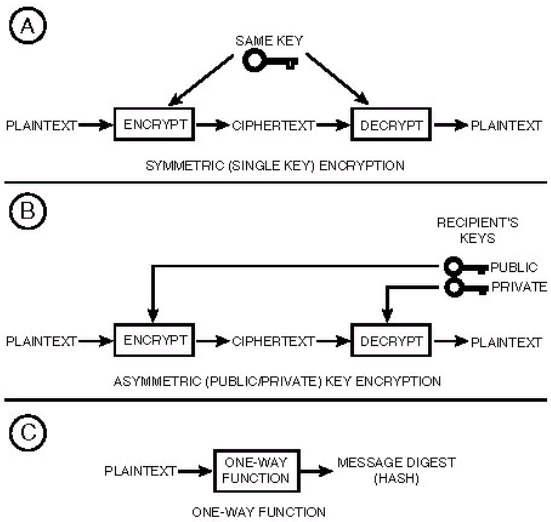
Setiap orang bahwa ketika dikehendaki untuk menyimpan sesuatu secara pribadi, maka kita harus menyembunyikan agar orang lain tidak tahu. Sebagai misal ketika kita megirim surat kepada seseorang, maka kita membungkus surat tersebut dengan amplop agar tidak terbaca oleh orang lain. Untuk menambah kerahasiaan surat tersebut agar tetap tidak secara mudah dibaca orang apabila amplop dibuka, maka kita mengupayakan untuk membuat mekanisme tertentu agar isi surat tidak secara mudah dipahami. Cara untuk membuat pesan tidak mudah terbaca adalah enkripsi. Dalam hal ini terdapat tiga kategori enkripsi antara lain :

- Kunci enkripsi rahasia, dalam hal ini terdapat sebuah kunci yang digunakan untuk meng-enkripsi dan juga sekaligus men-dekripsi informasi.
- Kunci enksripsi public, dalam hal ini dua kunci digunakan, satu untuk proses enkripsi dan yang lain untuk proses dekripsi.
- Fungsi one-way, di mana informasi di-enkripsi untuk menciptakan “signature”dari informasi asli yang bisa digunakan untuk keperluan autentifikasi.

Enkripsi dibentuk dengan berdasarkan suatu algoritma yang akan mengacak suatu informasi menjadi bentuk yang tidak bisa dibaca atau tak bisa dilihat. Dekripsi adalah proses dengan algoritma yang sama untuk mengembalikan informasi teracak menjadi bentuk aslinya. Algoritma yang digunakan harus terdiri dari susunan prosedur yang direncanakan secara hati-hati yang harus secara efektif menghasilkan sebuah bentuk terenkripsi yang tidak bisa dikembalikan oleh seseorang bahkan sekalipun mereka memiliki algoritma yang sama. Algoritma sederhana dapat dicontohkan di sini. Sebuah algoritma direncanakan, selanjutnya disebut algoritma (karakter+3), agar mampu mengubah setiap karakter menjadi karakter nomor tiga setelahnya. Artinya setiap menemukan huruf A, maka algoritma kanmengubahnya menjadi D, B menjadi E, C menjadi F dan seterusnya.

Sebuah pesan asli, disebut *plaintext* dalam bahasa kripto, dikonversikan oleh algoritma karakter+3 menjadi *ciphertext* (bahasa kripto untuk hasil enkripsi). Sedangkan untuk mendekripsi pesan digunakan algoritma dengan fungsi kebalikannya yaitu karakter-3 Metode enkripsi yang lebih umum adalah menggunakan sebuah algoritma dan sebuah kunci. Pada contoh di atas, algoritma bisa diubah menjadi karakter+x, di mana x adlah variabel yang berlaku sebagai kunci. Kunci bisa bersifat dinamis, artinya kunci dapt berubahubah sesuai kesepatan untuk lebih meningkatkan keamanan pesan. Kunci harus diletakkan terpisah dari pesan yang terenkripsi dan dikirimkan secara rahasia. Teknik semacam ini disebut sebagai symmetric (single key) atau secret key cryptography. Selanjutnya akan muncul permasalahn kedua, yaitu bagaimana mengirim kunci tersebut agar kerahasiaannya terjamin. Karena jika kunci dapat diketahui oleh seseorang maka orang tersebut dapat membongkar pesan yang kita kirim. Untuk mengatasi permasalahan ini, sepasang ahli masalah keamanan bernama Whitfield Diffie dan Martin Hellman mengembangkan konseppublic-key cryptography. Skema ini, disebut juga sebagai asymmetric encryption, secara konsep sangat sederhana, tetapi bersifat revolusioner dalam cakupannya. Kunci privat dijaga kerahasiaanya oleh pemiliknya atau diterbitkan pada server kunci publik apabila dihendaki. Apabila kita menginginkan untuk mengirimkan sebuah pesan terenkripsi, maka kunci publik dari penerima pesan harus diberitahukan untuk mengenkripsi pesan. Saat pesan tersebut sampai, maka penerima akan mendekripsi pesan dengan kunci privatnya. Jadi konsep sederhana yang diaplikasikan di sini adalah bahwa sebuah pesan hanya bisa didekripsi dengan sebuah kunci privat hanya apabila ia sebelumnya telah dienskripsi dengan kunci public dari pemilik kunci yang sama. Enkripsi ini memiliki bersifat one-way function. Artinya proses enkripsi sangat mudah dilakukan, sedangkan proses dekripsi sangat sulit dilakukan apbila kunci tidak diketahui. Artinya untuk membuat suatu pesan terenkripsi hanya dibutuhkan waktu beberapa detik, sedangkan mencoba mendekripsi dengan segala kemungkinan membutuhkan waktu ratusan, tahuanan bahkan jutaan tahun meskipun menggunakan komuter yang handal Sekalipun Enkripsi one-way digunakan untuk bebearap kegunaan.

Misalkan kita memliki dokumen yang akan dikirimkan kepada seseorang atau menyimpan untuk kita buka suatu saat, kita bisa menggunakan teknik one-way function yang akan menghasilkan nilai dengan panjang tertentu yang disebut hash.. Hash merupakan suatu signature yang unik dari suatu dokumen di mana kita bisa menaruh atau mengirimkan bersama dengan dokumen kita. Penerima pesan bisa menjalankan one-way function yang sama untuk menghasilkan hash yang lain. Selanjutnya hash tersebut saling dibanding. Apabila cocok, maka dokumen dapat dikembalikan ke bentuk aslinya.



Gambar 2.22 Tiga teknik kriptografi

3 Tujuan Kriptografi

Tujuan dari sistem kriptografi adalah :

- Confidentiality : memberikan kerahasiaan pesan dan menyimpan data dengan menyembuyikan informasi lewat teknik-teknik enkripsi.
- Message Integrity : memberikan jaminan untuk tiap bagian bahwa pesan tidak akan mengalami perubahan dari saat ia dibuat samapai saat ia dibuka.
- Non-repudiation : memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang apabila ia mencoba menyangkal memiliki dokumen tersebut.
- Authentication : memberikan dua layanan. Pertama mengidentifikasi keaslian suatu pesan dan memberikan jaminan keotentikannya. Kedua

untuk menguji identitas seseorang apabila ia kan memasuki sebuah sistem.

Dengan demikian menjadi jelas bahwa kriptografi dapat diterapkan dalam banyak bidang . Beberapa hal di antaranya :

- Certificates (Digital IDs) .
- Digital signatures.
- Secure channels.