BAB II

TINJAUAN PUSTAKA

2.1 Profil Tempat Kerja Praktek

PT. Rajawali Citra Televisi Indonesia atau yang biasa disingkat *"RCTI"* adalah salah satu perusahaan dan stasiun televisi swasta di Indonesia yang bergerak dalam bidang penyiaran. PT. Rajawali Citra Televisi Indonesia juga merupakan salah satu bagian dari MNC GROUP.

2.1.1 Sejarah PT. Rajawali Citra Televisi Indonesia

PT. Rajawali Citra Televisi Indonesia adalah stasiun Televisi Swasta pertama di Indonesia yang lahir pada tanggal 24 Agustus 1989 dari gagasan perusahaan besar yaitu Bimantara Citra Tbk dan Rajawalo *Corporations.*

Pembangun PT. Rajawali Citra Televisi Indonesia ditandai dengan peletakan batu pertama oleh Gubernur DKI Jakarta, Wiyog Atmodarminto pada tanggal 23 Juni 1988. Pada tanggal 14 November 1988, PT. Rajawali Citra Televisi Indonesia melakukan siaran percobaan untuk wilayah jakarta selama 4jam sehari dengan menggunakan *decorder* yang saat itu berjumlah 30.000 pelanggan.

Setelah PT. Rajawali Citra Televisi Indonesia diresmikan oleh Presiden RI-Soeharto, jumlah pelanggan meningkat menjadi 125.000. Penggunaan *decorder* untuk menangkap siaran PT. Rajawali Citra Televisi Indonesia tidak berlangsung lama karena tepat satu tahun hari jadinya , PT. Rajawali Citra Televisi Indonesia melakukan pelepasan penggunaan alat tersebut. Hal ini bertujuan agar semakin banyak pemirsa yang dapat menikmati siaran PT. Rajawali Citra Televisi Indonesia.

Tetapi sebagai konsekuensinya, maka pendapatan PT. Rajawali Citra Televisi Indonesia hanya bersumber dari iklan sebesar 20%. Sedangkan 18% untuk berita dan dialog serta 62% untuk hiburan, sports dan budaya. Iklan tersebut mencakup lokal break yaitu iklan yang hanya ditayangkan di kota-kota tertentu saja seperti jakarta (9 kota), Bandung (3 kota), Jawa Timur (9 kota), Jawa Tengah (22 kota), Sumatera Utara (7 kota) dan 39 kota lainnya.

Pada Agustus 1990-1992, PT. Rajawali Citra Televisi Indonesia bersama-sama dengan Surya Citra Televisi indonesia (*SCTV)* melakukan beberapa program kerja sama yaitu pemberitaan, sales dan marketing serta produksi dan teknik. Tidak sampai dengan meresmikan stasiun PT. Rajawali Citra Televisi Indonesia Bandung pada tanggal 01 Mei 1991 dan mulai bersiaran secara nasional dua tahun kemudian tepatnya pada tanggal 24 Agustus 1993.

Untuk meningkatkan kualitas penyiaran, PT. Rajawali Citra Televisi Indonesia memindahkan siaran dari *Satelit Palapa C2* pada Maret 1996, disamping itu pada tanggal 01 Februari 2000, sistem siaran PT. Rajawali Citra Televisi Indonesia diubah dari analog menjadi digital. Penajaman logo PT. Rajawali Citra Televisi Indonesia juga dilakukan tepat hari jadi PT. Rajawali Citra Televisi Indonesia yang ke-11 guna menggambarkan penampilan dan semangat baru.

Dengan meresmikan stasiun transmisi PT. Rajawali Citra Televisi Indonesia yang ke-47 di Kota baru, Kalimantan Selatan pada 10 Februari 2001, praktis PT. Rajawali Citra Televisi Indonesia telah mengoperasikan 47 buah stasiun transmisi yang mencakup 289 kota diseluruh Indonesia hingga saat ini. Secara populasi mencakup lebih dari 162, 3 juta penduduk Indonesia. Untuk itulah PT. Rajawali Citra Televisi Indonesia selalu menjadi pilihan para cakupan terluas.

Sejak lahir, PT. Rajawali Citra Televisi Indonesia identik dengan beragam program yang popular dan merupakan *Trensdsetter* bagi televisi-televisi lainnya dimana pembagian program tayangnya adalah 51,2 program lokal dan sisanya, 48,8 program asing yang ditayangkan 20-24 jam setiap hari.

Hingga kini baru saja menginjak ulang tahunnya yang ke-17, PT. Rajawali Citra Televisi Indonesia kembali melakukan perubahan logo dengan garis-garis biru terputus ditambah dengan penebalan pada garis merah yang menandakan bahwa PT. Rajawali Citra Televisi Indonesia kini lebih bersatu dan tegas untuk melangkah menghadapi persaingan di industri penyiaran, serta semakin menjadi kebanggaan bangsa Indonesia.

2.1.2 Visi, Misi, Pilar Utama dan Logo Perusahaan

Visi merupakan keadaan masa depan (nyata dan terukur) yang diinginkan terjadi sebagai hasil dari perusahaan. Visi harus dirasakan oleh seluruh pihak yang terlibat. Visi juga harus mudah untuk dikomunikasikan dan dimengerti oleh seluruh organisasi.

Misi merupakan rumusan umum mengenai upaya-upaya yang akan dilaksanakan untuk mewujudkan visi.

1. Visi

"Media Utama Hiburan dan Informasi", kalimat ini mengandung makna mencerminkan unsur kemuliaan karena melibatkan aspek aktualitas, kualitas, integritas dan dedikasi kepada masyarakat. Media utama hiburan dan informasi memiliki makna :

a) PT. Rajawali Citra Televisi Indonesia unggul dalam hal kualitas materi dan penyajian program hiburan dan informasi.

b) PT. Rajawali Citra Televisi Indonesia memperhatikan keseimbangan faktor bisnis dan bertanggung jawab sosial atas sajian program-programnya.

c) PT. Rajawali Citra Televisi Indonesia menjadi pilihan yang utama dari para *"stakeholder"* (karyawan, pemirsa, pengiklan, pemegang saham, pemasok, pesaing, perusahaan afiliasi, mitra strategis, masyarakat dan penyelenggara negara)

2. Misi

"Bersama Menyediakan Layanan Prima". Dalam profesinya interaksi kerja diperusahaan lebih mengutamakan semangat kebersamaan sebagai tim kerja yang kuat. Hal ini memungkinkan seluruh komponen perusahaan mulai dari level teratas sampai dengan level terbawah mampu bersama-sama tertimulasi, terkoodinasi dan tersistematisasi memberikan karya terbaiknya demi mewujudkan pelayanan terbaik dan utama kepada *"Stakeholder"*.

3. Pilar Utama

Untuk mewujudkan visi dan misi, terdapat 3 (tiga) tata nilai yang perlu diketahui sebagai pilar utama PT. Rajawali Citra Televisi Indonesia, yaitu :

1. Keutamaan dan Kebersamaan.
2. Bersatu Padu.
3. Oke.

Proses kerja dilakukan dengan semangat kebersamaan untuk dapat mencapai hasil yang diakui oleh para *"Stakeholder"* baik dari segi kualitas, integritas maupun dedikasi yang ditampilkan.

4. Logo

RCTI memiliki logo sebagai lambang perusahaannya sebagaimana tertera pada gambar dibawah ini :



Gambar 2.1 Logo RCTI

Dalam logo RCTI terbaru ini menggambarkan pesan kepada masyarakat dengan memiliki fungsi sebagai perusahaan media massa yang mengkontrol tatanan kehidupan politik, ekonomi, sosial dan budaya bangsa. Secara lambang, perusahaan RCTI mengandung makna dari setiap huruf yang tertera pada logo, berikut arti pesannya :

a) 'R' berarti Rajawali, digunakan sebagai lambang burung rajawali, sebagaimana seekor burung rajawali merupakan pemaknaan sebagai penguasa udara.
b) 'C' sebaga Citra, mempunyai pemaknaan dalam mewujudkan citra terbaik untuk perusahaan dimata khalayak. Hal ini digunakan RCTI dalam menjaga *image* sebagai media televisi swasta senior, harus hampu memberikan contoh bagi televisi swasta baru lainnya.
c) 'T' sebagai Televisi, menegaskan RCTI merupakan media massa elektronik berbentuk Televisi.
d) 'I' berarti Indonesia, RCTI ingin dijadikan sebagai televisi kebanggaan bersama milik Bangsa Indonesia.

Warna biru pada logo perusahaan digunakan karena memberi kesan yang elegan, cerdas, informatif dan komunikatif. Sedangkan warna merah pada mata rajawali, menegaskan sebagai pemancar yang tajam, akurat dan terpercaya.

2.1.3 Struktur Organisasi Perusahaan

RCTI memiliki jajaran direksi dan struktur organisasi yang melingkupi tugas dan peran di perusahaan seperti dibawah ini :



Gambar 2.2 Struktur Organisasi RCTI

Uraian Struktur Organisasi :

a) Direktur Utama RCTI : Bpk. Harry Tanoesodibjo, M.BA

b) Direktur RCTI : Bpk.Ir. Syafril Nasution

c) Kepala Bidang Siaran : Bpk. Arif Suditomo, S.sos., M.Sas

d) Kepala Bidang Pemberitaan : Bpk. Putra Nababan, M.si

e) Kepala Bidang Teknik : Ibu. Uun Billah, M.Si

f) Kepala Bidang Keuangan dan Umum : Ibu. Citra Melati, M.BA

g) Kepala Bidang Usaha : Ibu. Betty Suratni, M.SE

2.1.4 Sarana dan Prasana

PT. Rajawali Citra Televisi Indonesia memiliki sarana dan prasana yang tersedia untuk mendukung kinerja karyawan dalam pencapaian visi dan misinya. Fasilitas-fasilitasnya adalah sebagai berikut :

1. Fasilitas Gedung

Terdapat 12 gedung dan digunakan untuk beberapa acara program dibagi atas :

a) Gedung Utama (Gedung A)
b) Gedung Operasional Teknik (Gedung B)
c) Gedung Pemancar (Gedung TX)
d) Gedung Annex (Gedung C)
e) Gedung Produksi Studio 4 (Gedung D)
f) Gedung Klinik dan Koperasi
g) Gedung Produksi dan Feb.I
h) Gedung Produksi Set
i) Gedung ME 1 dan ME 2
j) Gedung Car Pool
k) Gedung Pergudangan (Gedung G)
l) Gedung Ex. Koperasi

Sumber : (Bagian Teknik, RCTI 2012)

2. Fasilitas Studio

Terdapat 7 studio dan OB Van dan SNG studio digunakan untuk beberapa acara program dibagi atas :

Tabel 2.1 Studio RCTI

Studio	Keterangan
1 & 4	Studio terbesar di Komplek RCTI, dan biasanya dipergunakan untuk acara yang memerlukan setting luas seperti, "FIFA World Cup 2010, Ketoprak Canda, New Star Ramadhan, Selera Nusantara, Kuis Kata Berkait, Kuis Piramida, Musik 2 Warna, Gita Fitri, Sahara, Hitam Putih, Sabuk Emas RCTI, Joged, Senggal Senggol, Duel, Impresario dll".
2	Studio yang sedang luasnya ini khusus untuk set virtual yang digunakan untuk Acara MP3, TALA dll.
3	Studio terkecil yang dipergunakan untuk pembawa acara siaran RCTI.
5	Studio khusus acara berita dan dialog.
6	Studio khusus siaran langsung dipergunakan untuk "Selamat Datang Pagi" Program Religius, Resep Oke Rudy dll.
7	Studio khusus untuk siaran langsung sepakbola
OB van	Studio berjalan untuk diluar komplek RCTI.
SNG	Satelite News Gathering (siaran langsung dari lokasi dimana saja).

3. Fasilitas lainnya

a) Ruang Control, Ruang Audio dan Video.

b) Ruang Terjemahan.

c) Ruang Pengisian Suara.

d) Antena Pemancar Stasiun Pusat Jakarta Setinggi 275 meter (baru) dan 151 meter (lama).

e) Koperasi Karyawan.

f) Masjid Raudathul Jannah.

g) Kantin Karyawan.

h) Klinik Umum, Klinik Gigi

i) Bengkel dan Garasi Lapangan Mobil Karyawan RCTI.

j) Radio Trijaya FM, Radio ARH FM.

k) Stasiun Televisi Global TV.

l) Lapangan Sepakbola RCTI

m) Lapangan Basket RCTI.

n) Halte Taksi.

Sumber : (*Bagian Teknik, RCTI. 2012)*

2.2 Landasan Teori

Dalam melaksanakan kerja praktek ini digunakan dasar-dasar teori jaringan komputer sebagai bahan acuan. Berisi teori-teori yang bisa dijadikan dasar dan acuan dalam pergantian Core*switch*.

2.2.1 Model OSI

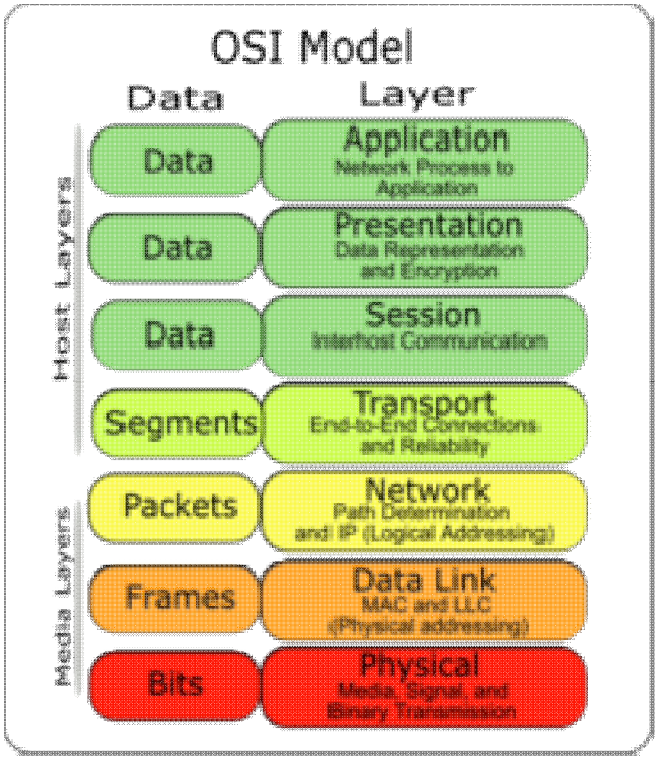
Siapa saja yang menekuni dunia jaringan komputer (*Computer Networks*) sudah selayaknya meluangkan waktu untuk mempelajari model referensi standar yang disebut *Open System Interconnection* (OSI) *seven-layer model* atau model OSI tujuh *layer*. Model OSI sering digunakan untuk menjelaskan cara kerja jaringan komputer secara logika.

Secara umum model OSI membagi berbagai fungsi *network* menjadi 7 lapisan. Sedangkan lembaga yang mempublikasikan model OSI adalah *international for Standardization* (ISO). Model OSI diperkenalkan pada tahun 1984.

Model OSI menjadi semacam referensi atau acuan bagi siapa saja yang ingin memahami cara kerja jaringan komputer. Walaupun OSI merupakan sebuah model yang diakui dunia saat ini, namun tidak ada paksaan bagi pengembang *hardware atau software* dan *user* untuk menggunakannya. Sebagai contoh, jaringan internet menggunakan model DARPA (*Defence Advanced Research Projects Agency*) yang berbeda dengan model OSI. Bahkan internet bisa berkembang sangat pesat walaupun tidak menggunakan model OSI.

Peril dipahami bahwa model OSI bukanlah sebuah protokol. Protokol adalah sekumpulan aturan yang digunakan pada komunikasi data. Protokol untuk jaringan komputer cukup banyak, beberapa yang popular seperti TCP/IP, IPX, NetBIOS, PPP, AppleTalk dan sebagainya. model OSI terdiri atas *layer-layer* atau lapisan-lapisan yang berjumlah 7 buah. Ketujuh layer tersebut yaitu :

1. Physical
2. Data Link
3. *Network*
4. Transport
5. Session
6. Presentation
7. Application



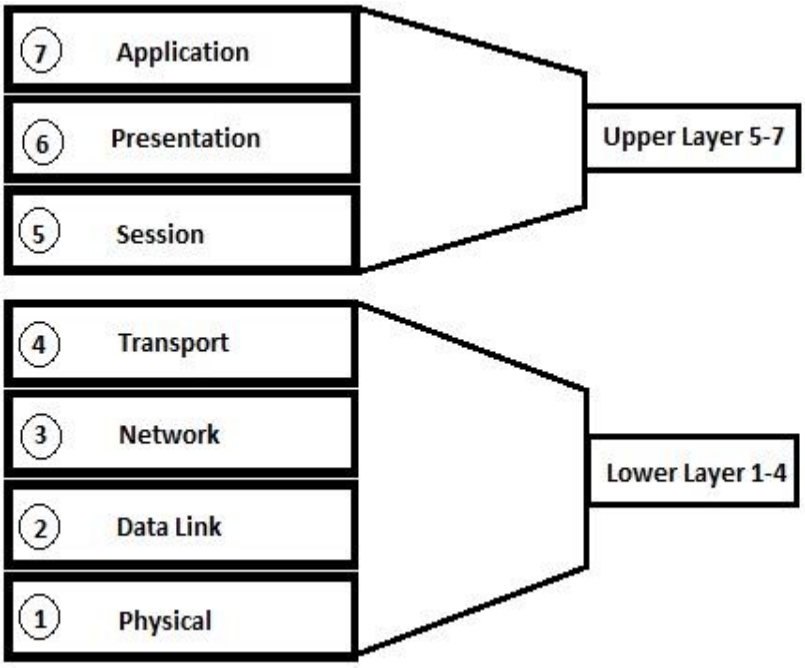
Gambar 2.3 Model OSI

Beberapa keuntungan atau alasan model OSI dibuat berlapis-lapis, diantaranya :

- Memudahkan siapa saja (khususnya pemula) untuk memahami cara kerja jaringan komputer secara menyeluruh.
- Memecahkan persoalan komunikasi data yang rumit menjadi bagia-bagian kecil yang lebih sederhana. Sehingga dapat memudahkan proses *trouble shooting.*
- Memungkinkan *vendor* atau pakar *network* mendesain dan mengembangkan *hardware/software* yang sesuai dengan fungsi *layer* tertentu (modular).
- Menyediakan standar *interface* bagi pengembangan perangkat yang melibatkan *multivendor*.
- Adanya abstraksi *layer* memudahkan pengembangan teknologi masa depan yang terkait dengan *layer* tertentu.

Ketujuh layer ini jika dilihat secara fungsional dapat dikelompokkan menjadi dua bagian saja, yaitu :

- *Layer* 5 sampai 7 dikelompokkan sebagai *application layer* atas *upper layer*. Segala sesuatu yang berkaitan dengan *user interface,* data *formatting*dan *communication session* ditangi *layer* ini.
- Layer 1 sampai 4 dikelompokkan sebagai data flow layers atau lower layers. Lower layer dapat diimplementasikan dalam bentuk hardware maupun software.



Gambar 2.4 Uper layers dan Lower layers

Tabel 2.2 OSI layer

Layer	Fungsi	Contoh Protokol
Application	Menyediakan servis bagi berbagai aplikasi *network*	NNTP, HL7, Modbus, SIP, SSI, DHCP, FTP, Ghoper, HHTP, NFS, NTP, RTP, SMPP, SMTP, SNMP, Telnet
Presentation	Mengatur konversi dan translasi berbagai format data, seperti kompresi data dan enkripsi data	TDI, ASCII, EBCDIC, MIDI, MPEG, ASCII7
Session	Mengatru sesi yang meliputi establishing (memulai sesi), maintaining (mempertahankan sesi) dan terminating (mengakhiri sesi) antar entitas yang dimiliki oleh presentation layer	SQL, X Window, Named Pipes (DNS), NetBios, ASP, SCP, OS Scheduling, RPC, NFS, ZIP
Transport	Menyediakan End-to-end communication protocol. Layer ini bertanggung jawab terhadap “keselamatan data” dan “segmentasi data”, seperti : mengatur flow control (kendali aliran data), error detection (deteksi error) and correction (koreksi), data	TCP, SPX, UDP, SCTP, IPX

	sequencing (urutan data) dan size of the packet (ukuran paket)	
Network	Menentukan rute yang dilalui oleh data. Layer ini menyediakan logical addressing (pengalamata logika) dn path determination (penentuan rute tujuan)	IPX, IP, ICMP, IPsec, ARP, RIP, IGRP, BGP, OSPF, NBF, Q.931
Data Link	Menentukan pengalamatan fisik (hardware address), error notification (pendeteksi error), frame flow control (kendali aliran frame) dan topologi *network*. Ada dua sublayer pada datalink : Logical Link Control (LLC) dan media Access Control (MAC). LLC mengatur komunikasi seperti error notification dan flow control. Sedangkan MAC mengatur pengalamatan fisik yang digunakan dalam proses komunikasi antar-adapter	802.3 (Ethernet), 802,11a/b/g/n MAC/LLC, 802.1Q (VLAN), ATM, CDP, HDP, FDDI, Fibre chanel, Frame Relay, SDLC, HDLC, ISL, PPP, Q.921, Token Ring
Physical	Layer ini menentukan masalah kelistrikan/gelombang/medan dan berbagai prosedur/fungsi yang	RS-232, V.35, V.34, I.430, I.431, T1, E1, 10BASE-T, 100BASE-

	berkaitan dengan link fisik, seperti besar tegangan (arus listrik), panjang maksimal media transmisi, pergantian fasa, jenis kabel, dan konektor	TX, POTS, SONET, DSL, 802.11 a/b/g/n PHY, hub, repeater, fibre optics

2.2.2 Jaringan Komputer

Sejarah *network* atau jaringan komputer berawal dari time-sharing *network*s, yaitu "rangkaian" terminal yang terhubung dengan komputer sentral yang disebut mainframe. Contoh time-sharing *network*s adalah IBM's System *Network* Architecture (SNA) dan digital's *network* architecture.

Kemudian komputer berskala kecil yang disebut Personal Computer atau PC mulai "menggeser" komputer-komputer mainframe. Beberapa buah PC dapat membentuk *network* yang disebut LAN (Local Area *Network*). LAN menyediakan pemakaian resource bersama, seperti sharing file dan sharing printer. LAN cukup efektif digunakan pada area tertutup dengan luas area terbatas, seperti dirumah, kantor, laboratorium dan sebagainya.

Setiap tahun selalu dikembangkan teknologi jaringan komputer. Dengan semakin luasnya infrastruktur jaringan telepon seluler maka jaringan komputer telah memasuki area yang selama ini belum pernah dijangkau, yaitu perkawinan antara mobile *network* dan computer *network*. Setipa orang dapat mengakses internet dimanapun dia berada dengan hanya berbekal sebuah laptop dan modem GSM atau CDMA. Jaringan komputer dapat dibedakan berdasarkan beberapa kriteria. Seperti luas area, media transmisi, pola operasi, dan sebagainya.

Berdasarkan luas areanya maka jaringan komputer dapat dibedakan menjadi :

a) PAN *(Personal Area Network)*

b) LAN (*Local Area Network)*

c) MAN (*Metropolitan Area Network)*

d) WAN *(Wide Area Network)*

Beberapa suimber lain membedakan jaringan komputer menjadi :

a) PAN

b) LAN

c) NAN (Neighborhood Area *Network*)

d) CAN (Campus Area *Network*)

e) MAN

f) WAN

g) GAN (Global Arean *Network*)

h) RAN (Regional Area *Network*)

i) SAN (Storage Area *Network*)

Berikut terdapat tabel 2.3 yang sedikit memberikan gambaran beberapa kira-kira luas area untuk masing-masing jaringan komputer. Tentu saja nilai yang ada pada table 2.3 hanya merupakan nilai kisaran saja. Dalam praktiknya cukup sulit untuk membuat batasan yang tegas.

Tabel 2.3 Jaringan komputer berdasarkan area

Jarak (meter)	*Network*	Contoh area
1 s.d 10	PAN	Ruangan
10 s.d 1000	LAN	Gedung
10 s.d 1000	NAN	RT/RW
1000 s.d 10.000	CAN	Universitas
10.000 s.d 100.000	MAN	Kota
100.000 s.d 1.000.000	WAN	Negara
Diatas 1.000.000	Internet	Antar Negara

Berdasarkan media penghantar yang digunakan, jaringan komputer dapat dibagi menjadi 2, yaitu :

a) *Wire network* atau *Wireline network*

Wire *network* adalah jaringan komputer yang menggunakan kabel sebagai media penghantar. Jadi, data dialirkan melalui kabel. Kabel yang umum digunakan pada jaringan komputer biasanya mengunakan bahan dasar tembaga. Ada juga jenis kabel lain yang menggunakan *fiber optis* atau serat optic. Biasanya bahan tembaga banyak digunakan pada LAN. Sedangkan untuk MAN atau WAN menggunakan gabungan kabel tembaga dan serat optic.

b) Wireless network (network nirkabel)

Wireless network adalah jaringan komputer yang menggunakan media penghantar berupa gelombang radio atau cahaya (infrared atau laser). Saat ini sudah semakin banyak pusat perbelanjaan, airport, rumah sakit dan lokasi lain yang menyediakan

layanan *wireless network* . Sehingga pengguna dapat dengan mudah melakukan akses internet menggunakan *handphone,* laptop, PDA dan perangkat *mobile* lainnya. Frekuensi yang digunakan *wireless network* biasanya 2.4 GHz dan 5.8 GHz. Sedangkan pengguna *infrared* dan laser umumnya hanya terbatas untuk jenis jaringan yang hanya melibatkan dua buah titik saja (disebut point to point).

Berdasarkan pola pengoperasian atau fungsi masing-masing komputer maka jaringan komputer dapat dibagi menjadi 2, yaitu :

a) *Peer to peer*

Peer to peer adalah jenis jaringan komputer dimana setiap komputer bisa menjadi *server* sekaligus *client*. Setiap komputer dapat menerima dan memberikan *acces* dari atau ke komputer lain. *Peer to peer* banyak diimplementasikan pada LAN. Walaupun dapat juga diimplementasikan pada MAN, WAN atau Internet, namun hal ini kurang lazim. Salah satu alasannya adalah masalah manajemen dan *security*. Cukup sulit mengawasi *security* pada jaringan *peer to peer* mana kala pengguna jaringan komputer sudah banyak.

b) *Client Server*

client server adalah jaringan komputer yang salah satu (boleh lebih) komputernya difungsikan sebagai *server* untuk melayani komputer lain. Komputer yang dilayani oleh *server* disebut *client*. Layanan yang diberikan bisa berupa akses Web, E-mail, file atau yang lain. *Client server* banyak dipakai oleh *Internet* dan Intranet.

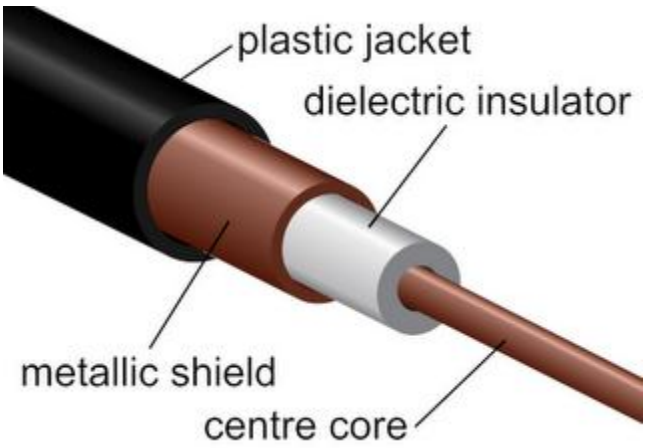
2.2.3 Kabel Jaringan Komputer

Kabel atau media penghubung jaringan merupakan komponen pokok dalam sebuah jaringan karena tanpa adanya media ini sebuah jaringan tidak bisa berjalan dan tidak bisa

disebut sebagai sebuah jaringan. Tiap-tiap kabel memiliki karakteristiknya sendiri. Mengingat karakteristik kabel satu dengan lainnya berbeda, maka masing-masing jenis kabel memiliki kegunaan masing-masing dan memiliki proses instalasi yang berbeda pula. Pada bagian ini akan dibahas berbagai jenis kabel berikut karakteristiknya.

1. Kabel Coaxial

Kabel coaxial banyak digunakan untuk instalasi jaringan, terutama jaringan ethernet dan ArcnNet. Kabel ini banyak digunakan karena mudah dalam instalasinya. Beberapa tipe *kabel coxial*, disamping mdah instalasinya, juga murah harganya, sehingga dapat menekan biaya instalasi jaringannya. Itu pula sebabnya pada jaringan Ethernet dengan menggunakan *kabel coaxial* jenis RG-58A/U sering disebut dengan *cheaper-net* atau jaringan yang murah.



Gambar 2.5 Kabel Coaxial

Semua tipe *kabel coaxial* memiliki bagian-bagian sebagai berikut :

a) Konduktor (centre core), berupa kabel tunggal atau kabel serabut yang merupakan inti dari kabel coaxial. Bagian ini merupakan bagian kabel yang digunakan untuk transmisi data atau sebagai kabel data.

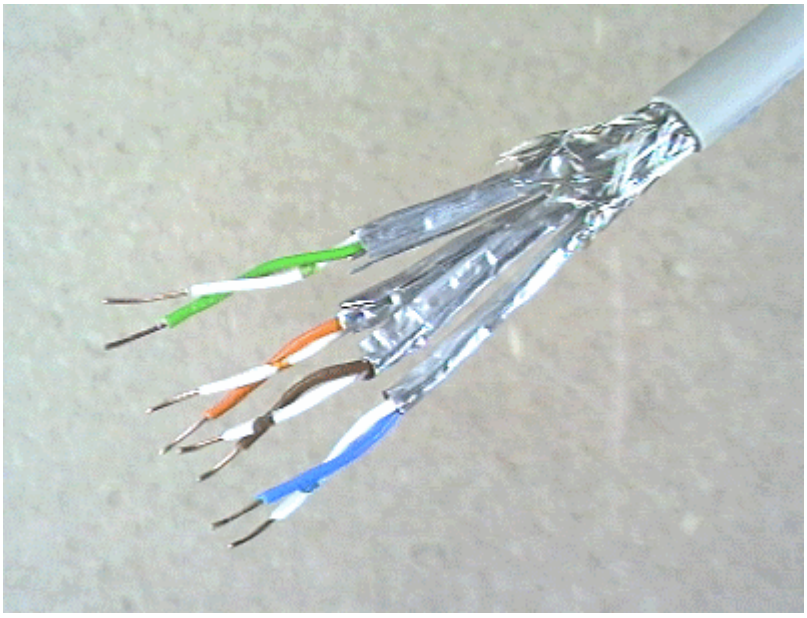
b) Isolator Dalam (*dielectric insulator*), merupakan lapisan isolator antara konduktor dengan *grounding*, yang juga berfungsi sebagai pelindung kabel inti (konduktor).

c) Pelindung (*Grounding*), Bagian ini berupa kabel serabut yang dirangkai secara bersilang mengelilingi isolator bagian dalam. Disamping sebagai pelindung juga berfungsi sebagai *grounding* dari pengaruh interferensi frekuensi-frekuensi liar yang menganggu.

d) Isolator Luar (*plastic jacket),* bagian berupa lapisan isolator yang juga merupakan kulit tabel.

2. Kabel STP (Sheilded Twisted Pair)

Kabel STP (*Shielded Twisted Pair)* merupakan salah satu jenis kabel yang digunakan dalam jaringan komputer. Kabel ini banyak digunakan pada jaringan Token-Ring. Kabel ini berisi dua *pair* kabel (enpat kabel) yang masing-masing *pair* dipilin (*Twisted).*Masing-masing kabel berupa kabel dengan inti kawat tembaga tunggal yang berisolator. Keempat kabel tersebut dibungkus dengan anyaman kabel serabut yang berfungsi sebagai pelindung dan *grounding* (Shielded). Sebagai pelindung luar adalah lapisan *isolator* yang merupakan kulit kabel. Kabel ini mampu mentransmisikan data hingga 16Mbps dengan jarak maksimal mencapai 100 meter. Itulah sebabnya kabel ini banyak digunakan pada jaringan Token-Ring yang mampu berjalan pada kecepatan 16 Mbps.



Gambar 2.6 Kabel STP

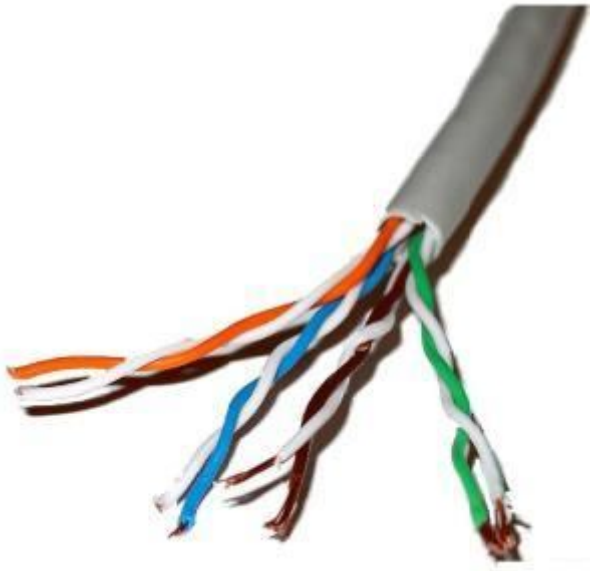
3. Kabel UTP (Unsheilded Twisted Pair)

Kabel UTP (*Unshielded Twisted Pair)* merupakan salah satu jenis kabel yang paling banyak digunakan dalam jaringan komputer saat ini. Sesuai namanya, kabel ini berisi empat pasang (*pair)* kabel yang tiap *pair*-nya dipilin (*Twisted)*. Berbeda dengan kabel STP, kabel ini tidak dilengkapi dengan pelindung (*Unshielded)*. Keempat pasang kabel (delapan kabel) yang menjadi isi kabel berupa kabel tembaga tunggal yang berisolator.

Sampai saat ini terdapat lima kategori kabel UTP, yaitu kabel UTP kategori satu sampai dengan kategori lima. Kabel UTP kategori satu dan dua tidak digunakan dalam jaringan komputer karena kemampuan transfer datanya sangat rendah. Kabel kategori ini banyak digunakan untuk komunikasi telepon, atau berfungsi sebagai kabel telepon. Sedangkan untuk jaringan komputer digunakan kabel kategori tiga sampai lima. Kabel kategori tiga bisa dipergunakan untuk komunikasi pada jaringan dengan kecepatan 10 Mbps,

seperti Ethernet. Itulah sebabnya Ethernet dengan kabel UTP disebut dengan 10 BaseT. Sedangkan untuk jaringan token ring bisa menggunakan kabel UTP kategori empat dan lima. Kabel UTP kategori lima bisa dipergunakan untuk kedua jaringan diatas, bahkan kabel ini bisa pula dipergunakan untuk jaringan komputer dengan kecepatan 100Mbps atau Fast Ethernet (100BaseT).

Gambar dibawah menunjukkan bentuk kabel dari kabel UTP. Sedangkan untuk menghubungkan kabel UTP ini digunakan konektor RJ-45, yaitu *Modular Jack* yang berisi 8 pin, seperti ditunjukkan pada gambar 2.7 dibawah ini :



Gambar 2.7 Kabel UTP

4. Kabel Fiber Optic

Fiber optic merupakan salah satu jenis media transfer data dalam jaringan komputer. Sekilas bentuknya seperti sebuah kabel, namun berbeda dengan kabel lainnya karena media ini mentransfer data dalam bentuk cahaya. Untuk menggunakan fiber optic dibutuhkan kartu

jaringan yang memiliki konektor tipe ST (*ST Connector)*. Kelebihan utama fiber optic dibanding media kabel adalah dalam hal kecepatan transfer datanya yang tinggi. Selain itu, fiber optic mampu mentransfer data pada jarak yang cukup jauh, yaitu mencapai 1 kilometer tanpa bantuan perangkt repeater. Fiber optic juga memiliki kelebihan dalam hal ketepatan dan keamanan transmisi data. Hal ini dimungkinkan karena fiber optic tidak terpengaruh oleh interferensi dari frekuensi-frekuensi liar yang mungkin ada di sepanjang jakur instalasi.

Kelemahan fiber optic ada pada tingginya tingkat kesulitan proses instalasinya. Mengingat bahwa media ini mentransmisikan data dalam bentuk gelombang cahaya, maka anda tidak bisa menginstalasi media ini dalam jalur yang berbelok secara tajam atau menyudut. Jika terpaksa harus berbelok, maka harus betul-betulterhindar dari kemungkinan terjadinya tekanan fisik pada media tersebut.



Gambar 2.8 Kabel Fiber Optic

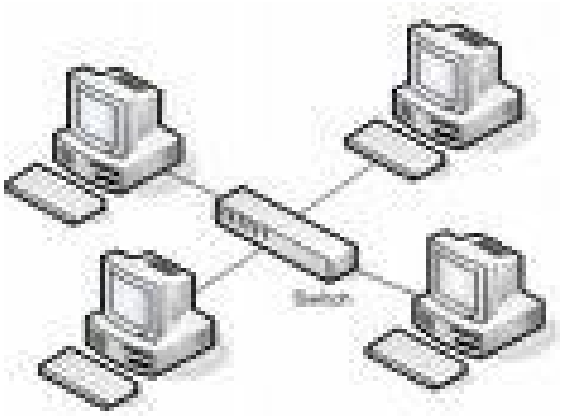
2.2.4 Topologi Jaringan Komputer

Topologi Jaringan adalah susunan lintasan aliran data didalam jaringan yang secara fisik menghubungkan simpul yang satu dengan simpul lainnya. Berikut ini adalah beberapa topologi jaringan yang ada dan dipakai hingga saat ini, yaitu:

1. **Topologi Star**

Beberapa simpul/node yang dihubungkan dengan simpul pusat/host, yang membentuk jaringan fisik seperti bintang, semua komunikasi ditangani langsung dan dikelola oleh host yang berupa mainframe komputer seperti *Switch* hub.Topologi star digunakan dalam jaringan yang padat, ketika endpoint dapat dicapai langsung dari lokasi pusat, kebutuhan untuk perluasan jaringan, dan membutuhkan kehandalan yang tinggi. Topologi ini merupakan susunan yang menggunakan lebih banyak kabel daripada bus dan karena semua komputer dan perangkat terhubung ke central point. Jadi bila ada salah satu komputer atau perangkat yang mengalami kerusakan maka tidak akan mempengaruhi yang jaringan yang lainnya.

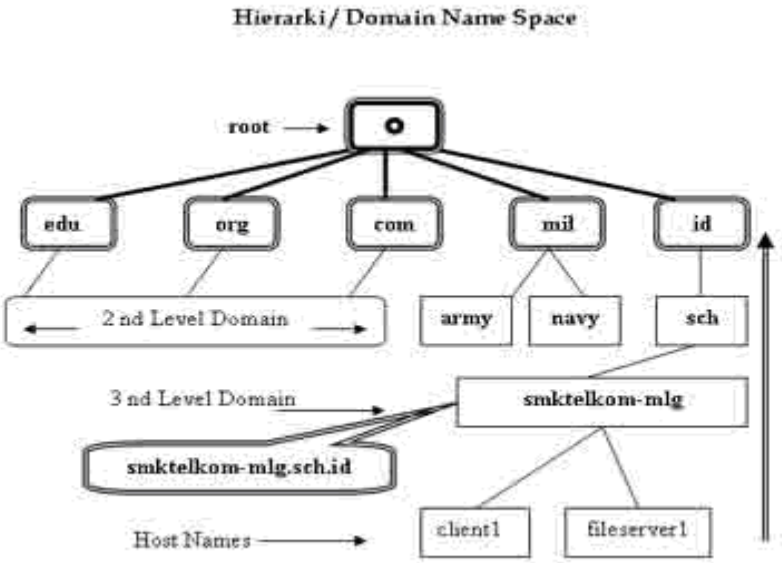
berikut ini gambar 2.9 merupakan gambaran topologi star :



Gambar 2.9 Topologi Star

2. Topologi Tree

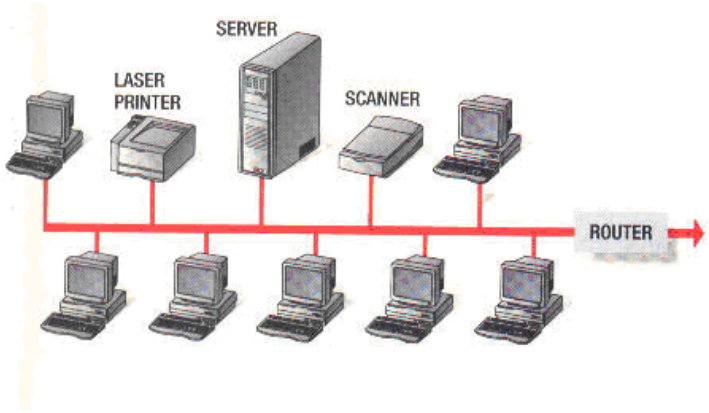
Berbentuk seperti pohon bercabang yang terdiri dari komputer induk (host) yang dihubungkan dengan simpul atau node lain secara berjenjang, jenjang yang lebih tinggi berfungsi sebagai pengetur kerja jenjang dibawahnya, biasanya topologi ini digunakan oleh perusahaan besar atau lembaga besar yang mempunyai beberapa cabang daerah, sehingga data dari pusat bisa didistribusikan ke cabang atau sebaliknya.



Gambar 2.10 Topologi Tree

3. Topologi Bus

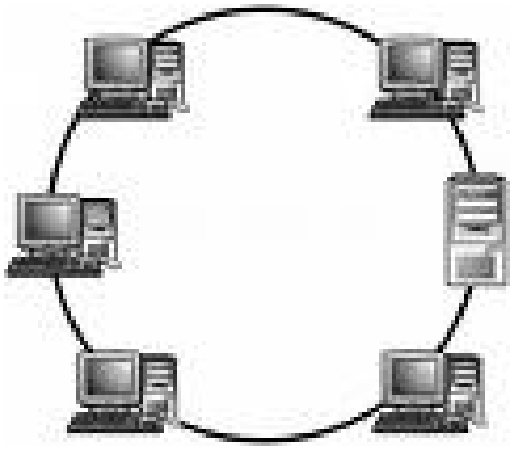
Beberapa simpul/node dis*witch*ungkan dengan jalur data (bus). Masing2 node dapat melakukan tugas-tugas dan operasi yang berbeda namun semua mempunyai hierarki yang sama. Topologi ini biasanya menggunakan kabel Coaxial, yang sekarang sudah sangat jarang digunakan atau di implementasikan. berikut ini gambar 2.11 merupakan gambaran topologi Bus :



Gambar2.11 Topologi Bus

4. Topologi Ring

Di dalam topologi Ring semua workstation dan server dihubungkan sehingga terbentuk suatu pola lingkaran atau cincin. 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. 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, dan yang lainnya menggu hingga pengiriman data selesai.



Gambar 2.12 topologi Ring

2.2.5 *Switch*

Cara kerja *Switch* mirip dengan bridge dan memang sesungguhnya *Switch* adalah bridge yang memiliki banyak port. Sehingga *Switch* disebut sebagai multiport bridge. *Switch* berfungsi sebagai sentral atau konsentrator pada sebuah *network*.

Switch dapat mempelajari alamat hardware host tujuan, sehingga informasi bisa langsung dikirim ke host tujuan. *Switch* yang lebih cerdas dapat mengecek frame yang error dan dapat mem-blok frame yang tersebut.

Informasi tentang produk bridge buatan Cisco agak sulit ditemukan. Hal ini disebabkan karena fungsi maupun interface sebuah bridge telah tersedia pada router Cisco. Untuk membuat sebuah router menjadi bridge tinggal memanfaatkan interface tersebut. Saat ini orang sudah semakin jarang membeli perangkat bridge. Semua fitur yang dimiliki oleh bridge telah tersedia pada *Switch*.

Selain itu, *Switch* juga dapat dikelompokkan berdasarkan kapasitas atau ukuran *network*. Dalam hal ini, Cisco membagi *switch* menjadi :

1. *Are Switch Cisco Series 2960*

   Switch yang dibuat sebagai pengganti hub tradisional. Biasanya digunakan pada workgroups atau small office. Spesifikasi pada Cisco Catalyst 2960 Series dengan perangkat lunak Dasar LAN antara lain :

   a) Fast Ethernet dan Gigabit Ethernet konektivitas ke desktop untuk memberikan kinerja aplikasi yang superior.
   b) Power over Ethernet (PoE) untuk memberikan 15.4W secara bersamaan pada semua port PoE.
   c) Kemampuan keamanan yang canggih, termasuk layanan identitas dan kontrol akses yang canggih untuk melindungi aset penting.
   d) Kualitas layanan (QoS) intelijen untuk mendukung delay-sensitif suara IP dan aplikasi video untuk mengoptimalkan bandwidth pada jaringan User.
   e) Redundansi dan ketahanan fitur untuk melindungi ketersediaan aplikasi kritis User setiap saat.
   f) Manajemen yang sederhana untuk menggunakan antarmuka baris perintah (CLI) atau berbasis GUI Cisco dan Asisten Jaringan dengan antarmuka Smartports Cisco
   g) Skalabilitas untuk dapat mengakomodasi aplikasi baru dan layanan sebagai bisnis berkembang.
   h) Garansi Cisco IOS Software update Spesifikasi cisco series 2960 :



Gambar 2.13 Switch Catalyst series 2960

Fitur dan Manfaat Cisco Catalyst 2960 Series

a) Mengungkapkan Penataan menyederhanakan konfigurasi awal dengan browser web.
b) Menghilangkan kebutuhan untuk lebih kompleks emulasi terminal program dan pengetahuan CLI.
c) Memudahkan penyebaran saklar Autoconfiguration DHCP dari beberapa switch melalui server boot.

Tabel 2.4 Model Cisco 2960

Model	2960C-8TC-L	2960C-8TC-S	2960CPD-8TT-L	2960C-8PC-L	2960CPD-8PT-L	2960C-12PC-L	2960CG-8TL-L
Total Ethernet Ports	8 x 10/100 Fast Ethernet					12 x 10/100 Fast Ethernet	8 x 10/100/1000 Gigabit Ethernet
Total PoE/PoE+ Output Ports	N/A			8 PoE	8 PoE	12 PoE	N/A
Available PoE Power	N/A			124W	Up to 22.4W*	124W	N/A
Uplinks	2 x 1G copper or 1G SFP		2 x 1G (PoE+ input)	2 x 1G copper or 1G SFP	2 x 1G (PoE+ input)	2 x 1G copper or 1G SFP	
MACsec	N/A						

2. Distribusi Switch type Cisco 3700

Cisco 3700 Series adalah keluarga modular, platform akses multiservice untuk kantor menengah dan berukuran besar ataupun kecil dalam menyediakan layanan Internet Service. Dengan lebih dari 70 pilihan antarmuka modular, keluarga Cisco 3700 menyediakan solusi untuk data, suara, video akses dial hybrid, jaringan privat virtual (VPN), dan multiprotocol Data routing. Kinerja tinggi, arsitektur modular melindungi investasi pelanggan dalam teknologi jaringan dan mengintegrasikan fungsi beberapa perangkat ke satu solusi yg dikelola. Cisco Series 3700 dengan platform akses multiservice. 3700 Cisco menyediakan densitas yang lebih tinggi, kinerja yang lebih besar, dan kemampuan ekspansi lebih. Kekuatan tambahan dan kinerja dari platform Cisco 3660 memungkinkan aplikasi baru, seperti agregasi suara packetized dan kantor cabang akses ATM mulai dari T1/E1 IMA hingga OC-3. Antarmuka dan Modul Cisco 3700 series platform multiservice telah ditingkatkan dengan kemampuan untuk Voice over Frame relay (VoFR) dan Voice over ATM (VoATM-AALs) pada antarmuka

suara digital (T1 dan E1). QSIG juga sekarang didukung pada semua interface digital, termasuk T1/E1 dan BRI. Perangkat tambahan lain termasuk perpanjangan Premise (OPX) dan VoIP melalui Frame Relay. Selain itu, fitur yang bekerja dengan versi softwars Call Manager membuat produk-produk gateway seperti PBX dan PSTN untuk IP telephony. Memungkinkan aplikasi seperti transfer panggilan dan konferensi.



Gambar 2.14 Cisco Switch Series 3700

3. Data center and Backbone Switches

Switch yang dibuat untuk keperluan *network* berskala besar atau *network* yang dinamikanya tinggi. Contoh *Switch* jenis ini antara lain :

a) 6500 *Switch*es

lihat dari sisi kemampuan Enginesnya, Cisco series 6500 dapat dikategorikan sebagai berikut :

Tabel 2.5 Kategori kemampuan Engines Coreswitch Cisco series 6500

	Supervisor 2E	Supervisor 2	Supervisor 1
CPU	Dual Quad-Core Xeon	Quad-Core Xeon	Dual-Core Xeon
Speed (GHz)	2.13	2.13	1.66
Memory (GB)	32	12	8
Flash memory	USB	USB	Compact Flash
Fibre Channel over Ethernet on F2 module	Yes	Yes	No
CPU share	Yes	Yes	No
Virtual Device Contexts (VDCs)	8+1 admin VDC	4+1 admin VDC	4
Cisco Fabric Extender (FEX) support	48 FEX/1536 ports	32 FEX/1536 ports	32 FEX/1536 ports
Connectivity Management Processor (CMP)	Not supported	Not supported	Supported

Dilihat dari sisi kemampuan Slot, Cisco series 6500 dapat dikategorikan sebagai berikut :

Tabel 2.6 Kategori kemampuan Slot Coreswitch Cisco series 6500

-slot	9-slot	10-slot	18-slot
Supervisor redundancy	Yes	Yes	Yes
I/O module slots	2	7	8
Bandwidth per slot (Gbps)	440	550	550
Switching capacity (Tbps)	1.92	7.7	8.8
1 GE port density	96	336	384
10 GE port density	96	336	384

40 GE port density	12	42	48
100 GE port density	4	14	16
Rack space (RU)	7	14	21
Airflow	Side-rear	Side-side	Front-back

b) 7000 *Switch*es

Cisco Nexus 7000 Series Switches adalah seri pertama dari switch yang dirancang khusus untuk memenuhi data center kelas persyaratan dan terukur sampai 15 terabit per detik (Tbps). Cisco Nexus 7000 Series Switches terdiri dari data center modular kelas lini produk yang dirancang untuk menyediakan scalable 10 Gigabit Ethernet jaringan dengan dukungan 40 dan 100 Ethernet Gigabit interface. Tujuan dibangun untuk memenuhi persyaratan dari mission-critical sebagian besar pusat data dan memberikan sistem operasi yang uptodate. Cisco Nexus 7000 Series didasarkan pada sistem operasi terbukti (Cisco NX-OS), dengan fitur yang disempurnakan untuk memberikan sistem *real-time upgrade* dengan pengelolaan servis yang handal. Desain yang inovatif dibangun untuk mendukung end-to-end konektivitas data center, IP konsolidasi, penyimpanan, dan komunikasi interprocess (IPC) jaringan pada jaringan Ethernet tunggal. Berikut tabel spesifikasi Cisco Nexus 7000 yang akan digunakan pada Data Center :

Tabel 2.7 Spesifikasi Cisco Nexus 7000 (Double Power Supply with Quad Source)

Number of slots	4, 9, 10, and 18
Bandwidth per slot	**550 Gbps**
Max switching capacity	**17.6 Tbps**
Max packets per second	**11.5 billion**
1 GE density	Up to 768 ports
1 GE density with Cisco Nexus 2000	Up to 1536 ports
Line-rate 10 GE density	Up to 768 ports
40GE and 100GE	Up to 96 40GE ports and 32 100GE ports
Redundant supervisors	Yes
Hitless software upgrade	Yes: In Service Software Upgrade (ISSU)
Switch virtualization	Yes: Virtual Device Context (VDC)
Programming interface	XML and CLI script
Management tool	Cisco Data Center Network Manager



Gambar 2.15 Cisco Nexus 7000 (Double Power Supply with Quad Source)

Umumnya *Switch* buatan Cisco dapat dikendalikan melalui komputer. Seperti halnya router Cisco, dapat menggunakan kabel rollover dan melakukan koneksi dari komputer ke *switch*. Dilihat dari cara kerjanya maka *switch* dapat dikelompokkan menjadi beberapa jenis, yaitu :

1. *Cut through atau fast forward*

   Switch jenis ini hanya mengecek alamat tujuan (yang ada pada header frame). Selanjutnya frame akan diteruskan ke host tujuan. Kondisi ini dapat mengurangi "waktu tunggu" atau latency. Inilah jenis *switch* "tercepat" diantara jenis lainnya. Kelemahan *Switch* jenis ini yaitu tidak dapat mengecek frame-frame yang error. Frame yang error akan tetap diteruskan ke host tujuan.

2. *Store and forward*

   Switch jenis ini akan menyimpan semua frame untuk sementara waktu sebelum diteruskan ke host tujuan. Seluruh frame akan dicek melalui mekanisme CRC (Cyclic Redudancy Check). Jika ditemukan error maka frame akan "dibuang" dan tidak diteruskan ke host tujuan. *Switch* jenis ini paling " terpercaya" diantara jenis *Switch* lainnya. Kelemahan *switch* jenis ini adalah meningkatkan latency akibat adanya proses Fragment free atau modified cut through pengecekan seluruh frame yang melalui *Switch*.

3. *Fragment free atau modified cut through*

   Switch akan membaca 64 byte dari frame sebelum meneruskannya ke host tujuan. Nilai 64 bytre ini merupakan jumlah minimum byte yang dianggap penting untuk menentukan apakah frame error atau tidak. Sehingga *Switch* jenis ini memiliki unjuk kerja yang cukup baik dan tetap dapat diandalkan.

Seiring dengan semakin meningkatnya kebutuhan, maka *switch* telah diberi beberapa fitur tambahan yang tidak dijumpai pada *switch* jenis lama. Inilah yang disebut multi layer *switch* (MLS). *Switch* jenis berfungsi sama dengan *Switch* tradisional, hanya saja memiliki fitur lain seperti QoS (Quality of Service), ToS (Type os Service), IP Security, IP DSCP o VLAN, VLAN to IP DSCP, dan sebagainya.

Selain itu, Cisco juga mengeluarkan berbagai jenis *switch* untuk berbagai jenis *network* yang berbeda, seperti *Switch* untuk ethernet, token ring, frame relay, ATM, dan sebagainya.

2.2.6 LAN (Local Area *Network*)

Local Area Network (LAN) adalah sejumlah komputer yang saling dihubungkan bersama di dalam satu areal tertentu yang tidak begitu luas, seperti di dalam satu kantor atau gedung. 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 *client* maupun *server*. Sedangkan pada jaringan *Client-Server*, hanya satu komputer yang bertugas sebagai *server* dan komputer lain berperan sebagai *client*.

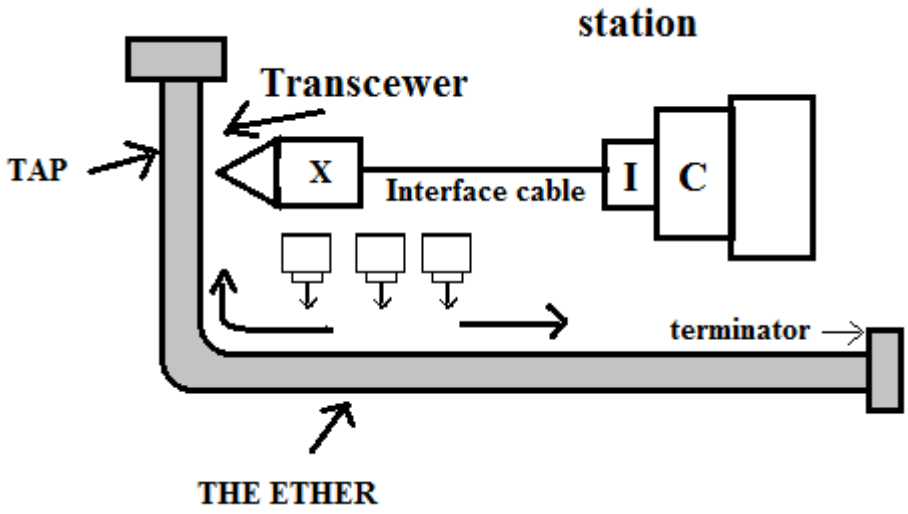
2.2.6.1 Protokol pada LAN (Local Area *Network*)

Protokol adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer. **Protokol** dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi dari keduanya. Pada tingkatan yang terendah protokol mendefinisikan koneksi perangkat keras. Berikut beberapa protokol yang ada pada LAN :

a) **Ethernet 802.3**

Saat ini teknologi *Ethernet* secara *de facto* telah menjadi standar pada jaringan lokal (LAN). *Ethernet* dapat dipandang sebagai perangkat keras, protokol dan jenis *network*. Sebagai sebuah protokol, *Ethernet* dibuat dengan prinsip saling berbagi media kabel dengan komputer lain dan merupakan sebuah "broadcast protocol", artinya data akan dikirim ke semua komputer pada jaringan yang satu *segmen* atau satu *broadcastdomain.*

Ethernet bekerja pada *layer Data Link* dan menggunakan metode CSMA/CD. Semua komputer dapat menggunakan *network* sepanjang media *network* tidak digunakan oleh komputer lain. Sebelum mengirim data, setiap komputer akan "melihat" kondisi *network* untuk mengetahui *network* sudah layak pakai atau belum. Data hanya akan dikirim jika komputer pengirim tidak melihat data lain sedang mengalir di media *network* pada saat itu.

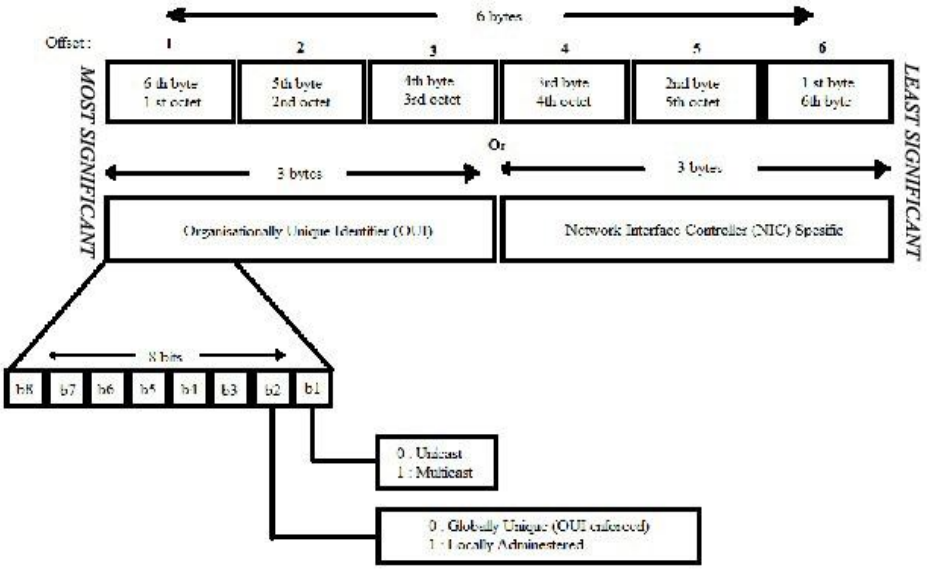


Gambar 2.16 Diagram yang menjelaskan asal katla Ethernet (karya Robert M. Metcalfe 1976)

Mungkin saja pada saat yang bersamaan ada komputer lain yang kuga mengirim data. Hal ini bisa terjadi karena setiap komputer menganggap *network* sedang bebas (tidak digunakan). Akibatnya, bisa terjadi tabrakan data disepanjang media *network.* Kondisi semacam ini disebut *collision.*

Untuk mengantisipasi terjadinya *collisison,* perangkat *Ethernet* telah dilengkapi sensor yang disebut *collision detection.* Jika *collisison* terdeteksi maka data yang *colliding* (tumpang tindih/tabrakan) akan diabaikan oleh semua komputer.kemudian masing-masing komputer akan diberi kesempatan (yang waktunya ditentukan secara *random)* untuk mengirim ulang data.

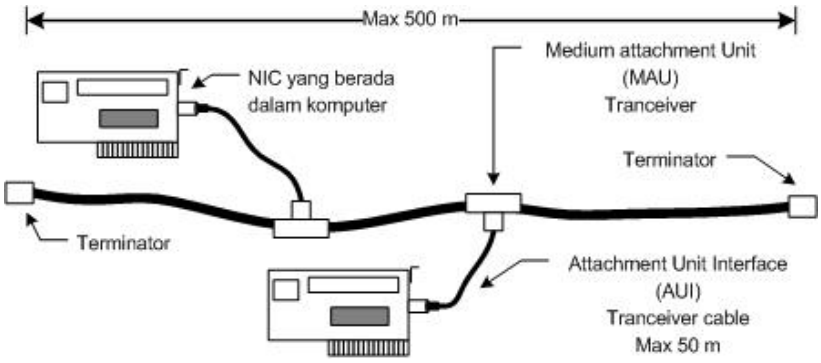
Setiap *Ethernet* memilki *Media Access Control (*MAC) yang berbeda-beda. Panjang MAC *address* adalah 48 bit. Sehingga jumlah total alokasi MAC *address* untuk seluruh dunia adalah 2^{48} atau 281.474.976.710.656 buah. Contoh MAC *address :* 00:16:d4:c9:e8:48. MAC *address* sepanjang ini dibagi menjadi 2 bagian, bagian sepanjang 24 bit menyatakan ID dari *vendor* pembuat *Ethernet.* Kemudian 24 bit yang kedua merupakan nomor serial yang ditentukan oleh masing-masing *vendor.*



Gambar 2.17 Bagan MAC address

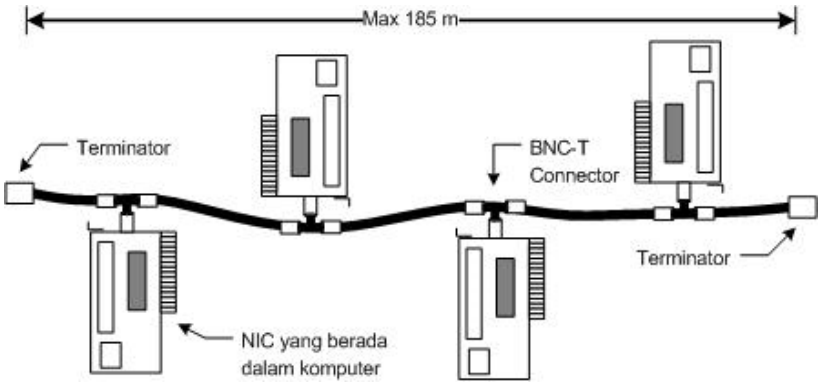
Seluruh Ethernet LAN dikonfigurasikan sebagai *logical bus* dan secara fisik dapat diimplementasikan dalam bentuk topologi bus atau star.

c) 10BASE5 : Implementasi ini disebut ***thick ethernet*** atau *thick-net*. Adalah LAN topologi bus yang menggunakan baseband sinyal dan memiliki panjang kabel maksimum 500 meter. Lihat Gambar 2.18 mengenai Thick Ethernet :



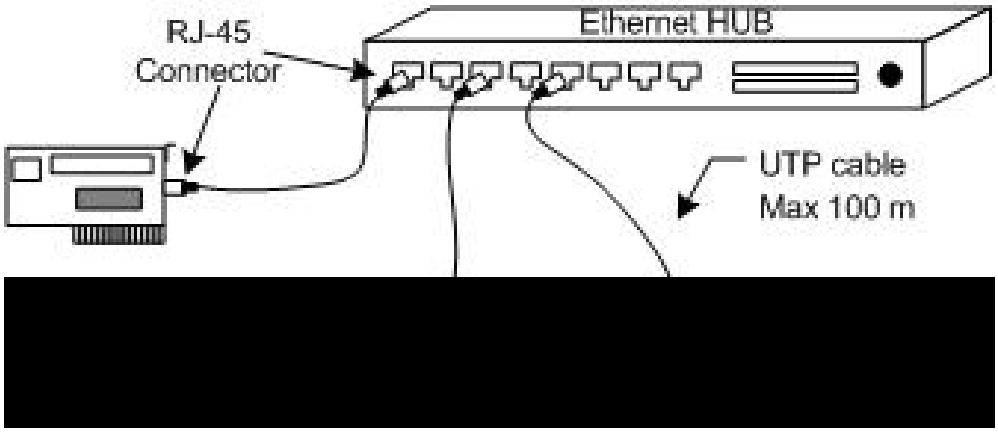
Gambar 2.18 Implementasi thick ethernet

d) 10BASE2 : Implementasi ini disebut ***thin ethernet***. Ada yang menyebutnya: *thin-net*, *cheap-net* atau *thin-wire Ethernet*. Konsepnya sama dengan 10BASE5, namun *thin-net* ini lebih murah dan lebih ringan kabelnya sehingga lebih luwes dibanding *thick-net*. Kelemahannya dibanding *thick-net* adalah jarak kabel yang tidak melebihi 185 meter dan hanya mampu mengakomodasi sedikit komputer. Gambar di bawah ini memperlihatkan contoh thin-net.



Gambar 2.19 Contoh dari thin-net

e) 10BASE-T : Implementasi LAN ini adalah yang sangat populer, disebut **Twisted-pair Ethernet**. Topologi yang digunakan pada implementasi LAN ini adalah topologi star. 10BASE-T ini mampu mendukung data hingga 10 MBps untuk panjang kawat maksimum 100 meter. Lihat Gambar berikut.



Gambar 2.20 Implementasi Twisted-pair Ethernet.

Semakin berkembangnya aplikasi lewat LAN seperti CAD, image processing, audio dan video di mana dibutuhkan transportasi data yang menuntut kapasitas yang lebih besar dalam LAN maka ada implementasi LAN lagi yang disebut **Fast Ethernet** atau disimbolkan dengan 100BASE-T. Fast Ethernet mampu mentransfer data hingga 100 MBps. Topologi Fast Ethernet tidak jauh beda dengan 10BASE-T.

Versi-versi terbaru Fast Ethernet ini pun sudah banyak macam ragamnya. Misal: 100BASE-T4 (menggunakan UTP 4 pair seperti 10BASET), 100BASE-XT (menggunakan STP atau UTP 2 pair) dan 100BASE-XF (menggunakan dua kabel serat optik pada masing2 jalur pengirim dan penerima).

b) **Local Talk**

LocalTalk adalah sebuah protokol *network* yang dikembangkan oleh Apple Computer, Inc. untuk 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 computer 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**. Kecepatan transmisinya **hanya 230 Kbps**.

Prosedur CSMA/CD antara lain :

f) Jika media transmisi dalam keadaan **idle**, lakukan **transmit**, jika tidak lakukan step 2.

g) Jika media transmisi sibuk, tetap *mendengarkan* sampai media idle, kemudian segera transmit.

h) Jika **tubrukan** terdeteksi selama transmisi data, transmit sebuah **sinyal jamming** singkat untuk meyakinkan bahwa semua station mengetahui bahwa telah terjadi tubrukan dan menghentikan transmisi.

i) Setelah melakukan transmit sinyal jamming, tunggu selama beberapa waktu, kemudian coba untuk melakukan transmit kembali **(ulangi dari step 1)**.

Metoda akses yang digunakan ethernet dalam LAN disebut carrier sense *multiple access with collision detection* disingkat CSMA/CD. Maksudnya, sebelum komputer/device mengirim data, komputer tersebut “menyimak/mendengar” dulu media yang akan dilalui sebagai pengecekan apakah komputer lain sedang menggunakannya, jika tidak ada maka komputer/device akan mengirimkan data nya. Terkadang akan terjadi dua atau lebih komputer yang mengirimkan data secara bersamaan dan itu akan mengakibatkan *collision* (tabrakan). Bila *collision* terjadi maka seluruh komputer yang ada akan mengabaikan data yang hancur tersebut. Namun bagi komputer pengirim data, dalam periode waktu tertentu maka komputer pengirim akan mengerim kembali data yang hancur akibat tabrakan tersebut.

Setiap komputer, device atau stasion dalam LAN memiliki NIC (*Network Interface Card*). NIC ini memiliki 6-byte alamat fisik (*physical address*). Ethernet LAN dapat mendukung laju data antara 1 sampai 10 Mbps, sedangkan Fast Ethernet mendukung hingga 100 Mbps dan yang terakhir GigaBit Ethernet hingga 1Gbps. Sebagai catatan tambahan, bahwa Ethernet tidak menyediakan suatu mekanisme untuk *acknowledge* frame yang diterima, sehingga hal ini bisa dikatakan sebagai media yang unreliabel. Namun demikian *acknowledgement* diimplementasikan pada layer di atasnya. Sebagai keterangan isi bingkai ethernet adalah sbb:

a) **Preamble** : memuat 7 byte (56 bit) rangkaian bolak-balik bit 0 dan 1. Kegunaannya untuk sinkronisasi pada komputer penerima.

b) **Start frame delimiter** : berisi 1 byte dengan nilai (10101011). Digunakan sebagai *flag* dan sinyal mulainya *frame*.

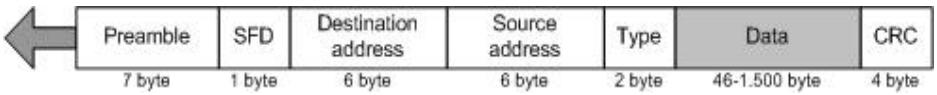
c) **Destination address** : Berisi 6 byte yang memuat *physical address* untuk komputer yang dituju.

d) **Source address** : Berisi 6 byte yang memuat *physical address* untuk komputer pengirim.

e) **Type** : berisi informasi yang menentukan jenis data yang dibungkus (*encapsulated*) pada *frame*.

f) **Data** : berisi data dari lapisan di atasnya. Panjang data harus berkisar antara 46 dan 1500 byte. Apabila data yang didapat dari lapisan di atasnya kurang dari 46 byte, maka ditambahkan byte2 yg disebut *padding* sehingga melengkapi jumlah minimum yakni 46 byte. Namun apablia besar data lebih dari 1500 byte, maka lapisan di atasnya harus mengfargmentasikannya dalam pecahan-pecahan 1500 byte.

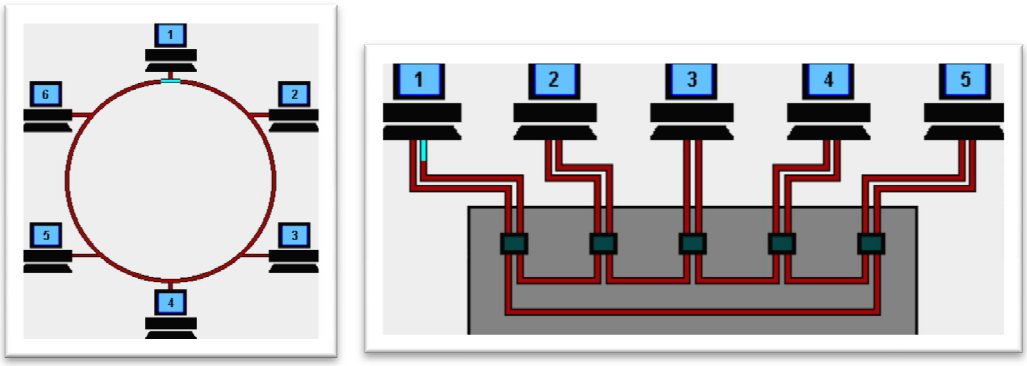
g) **Cyclic redudancy check** : berisi 4 byte sebagai error detection. Jenis CRC yang digunakan adalah CRC-32.



Gambar 2.21 Identifikasi CRC-32

c) **Token Ring**

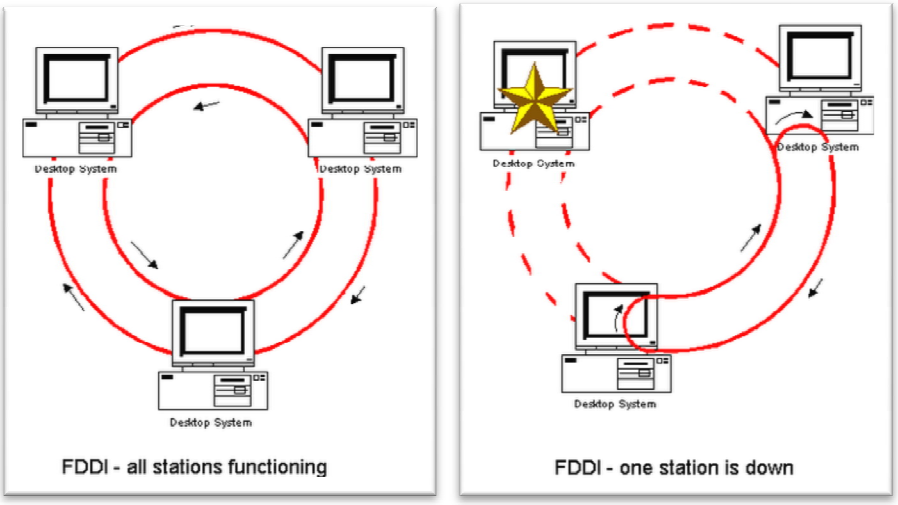
Protokol **Token** di kembangkan oleh IBM pada pertengahan tahun 1980. Metode Aksesnya melalui lewatnya sebuah token dalam sebuah lingkaran seperti **Cincin**. Dalam lingkaran token, komputer-komputer dihubungkan satu dengan yang lainnya seperti sebuah cincin. Sebuah Sinyal token bergerak **berputar** 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 di antara masing-masing komputer.



Gambar 2.22 (a)Token Ring dan (b)Token Bus

d) **FDDI**

Fiber Distributed Data Interface (FDDI) adalah sebuah protokol jaringan yang menghubungkan antara dua atau lebih jaringan bahkan pada **jarak yang jauh**. Metode akses yang digunakan oleh FDDI adalah **model token ring**. FDDI menggunakan **dua buah topologi ring** secara **fisik**. **Proses transmisi** biasanya 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 cable **kecepatan 100 Mbps**.



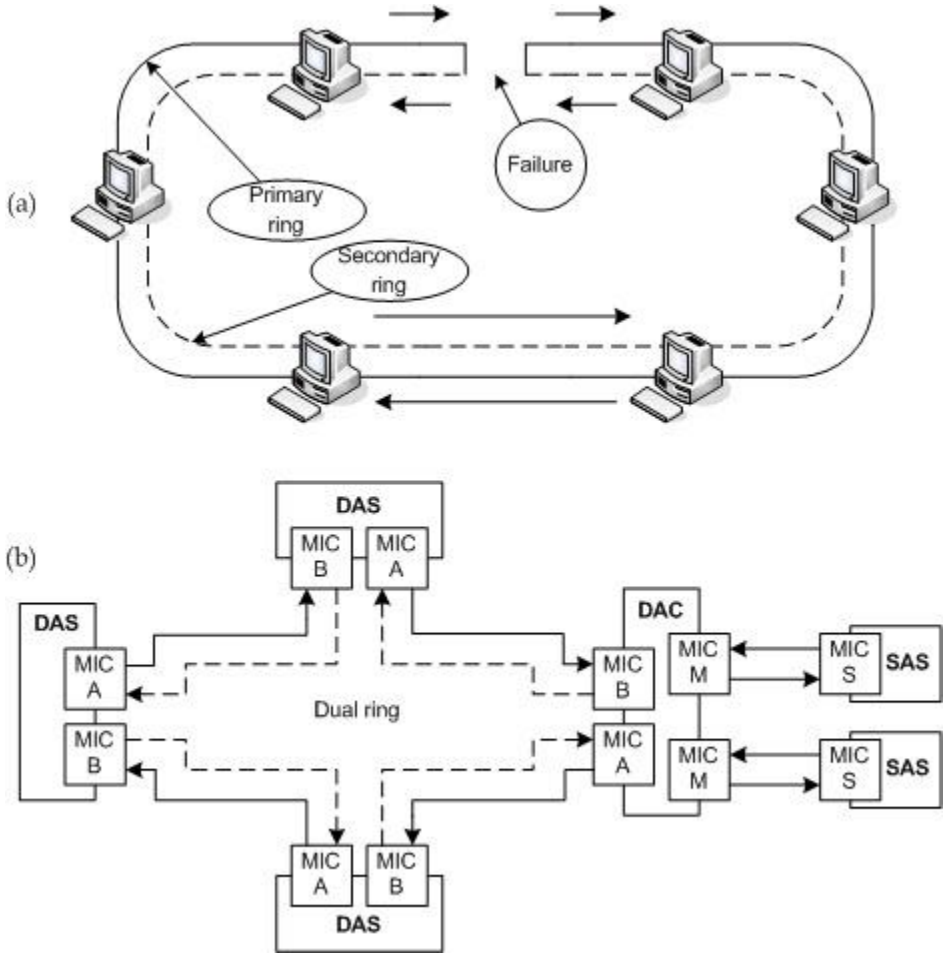
Gambar 2.23 Kecepatan FDDI

e) ATM

ATM adalah singkatan dari Asynchronous Transfer Mode (ATM) yaitu sebuah protokol jaringan yang mentransmisikan pada kecepatan 155 Mbps atau lebih. ATM mentransmisikan 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 . ATM juga banyak dipakai oleh Internet Service Providers (ISP) untuk meningkatkan kecepatan akses Internet untuk klien mereka. Untuk mencapai kecepatan transfer yang tinggi, sebuah jaringan ATM menggunakan perangkat keras dan tehnik perangkat lunak yang spesial, yaitu :

1. Sebuah jaringan ATM memiliki satu atau lebih *switch* berkecepatan tinggi, yang terhubung ke host-host komputer atau *switch-switch* ATM lainnya.
2. ATM menggunakan fiber optikal untuk koneksi, termasuk koneksi dari host komputer ke ATM *switch*, yang menyediakan *transfer rate* yang lebih tinggi dibanding kabel tembaga. Biasanya koneksi antara host komputer dengan ATM *switch* berkisar antara 100-155 Mbps.
3. Layer terbawah pada jaringan ATM menggunakan *fixed-size* frame yang disebut *cells*. Karena tiap sel panjangnya sama, perangkat keras ATM *switch* dapat memproses sel-sel secara cepat.



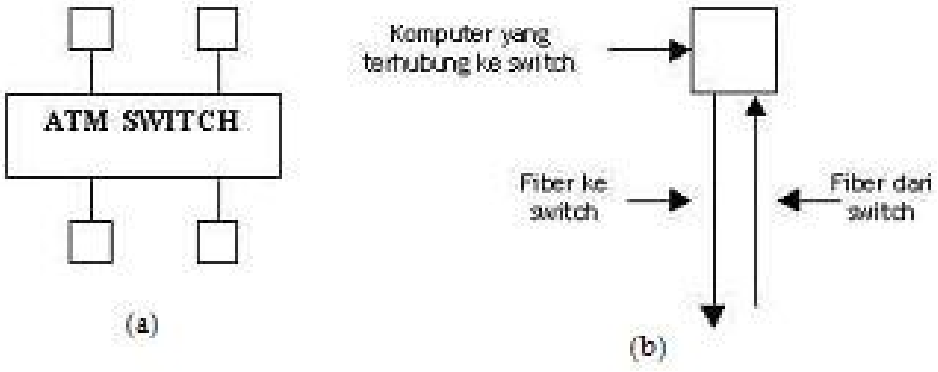
Gambar 2.24 Jaringan ATM menggunakan fixed-size *frame*

ATM berbeda dari jaringan *packet-switching* karena menawarkan layanan *connection-oriented*. Sebelum sebuah host komputer yang terhubung ke ATM dapat mengirim *cells,* host tersebut terlebih dahulu berinteraksi dengan *switch* untuk menentukan sebuah tujuan. Interaksi tersebut dapat dianalogikan seperti membentuk sambungan telepon. Host tersebut menspesifikasikan alamat remote komputer, dan menunggu ATM *switch* untuk mengontak sistem remote tersebut dan membentuk sebuah path. Jika komputer yang dituju (remote) menolak permintaan tersebut, tidak merespon, atau ATM *switch* tidak dapat menjangkaunya, permohonan untuk komunikasi tersebut gagal.

Ketika sebuah koneksi berhasil, ATMN *switch* lokal memilih sebuah *identifier* untuk koneksi tersebut, dan meneruskan *identifier* tersebut ke komputer host dengan sebuah pesan yang memberitahukan sukses ke host tersebut. Komputer host menggunakan *identifier* tadi ketika mengirim dan menerima *cells*.

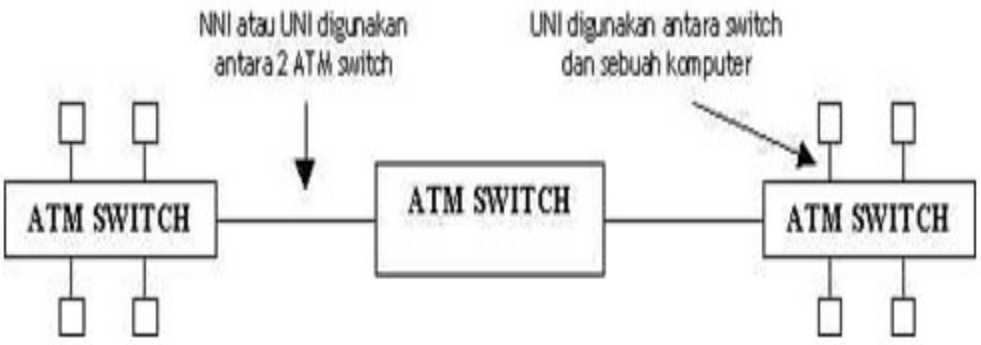
Ketika selesai menggunakan koneksi, host kembali berkomunikasi dengan ATM *switch* untuk meminta pemutusan koneksi. *Switch* kemudian memutuskan kedua komputer. Pemutusan ini sama dengan pemutusan sambungan telepon di akhir sambungan telepon. Sesudah pemutusan, *switch* dapat menggunakan kembali *identifier* koneksi yang tadi.

Komponen dasar sebuah jaringan ATM adalah suatu *special-purpose electronic switch* yang dirancang untuk mentransfer data pada kecepatan yang sangat tinggi. *Switch* yang kecil biasanya dapat menghubungkan antara 16 dan 32 komputer. Untuk menyediakan komunikasi data pada kecepatan tinggi, setiap koneksi antara komputer dengan ATM *switch* menggunakan sepasang fiber optikal. Gambar berikut memperlihatkan koneksi antara komputer host dengan ATM *switch*.



Gambar 2.25 (a) merupakan skema sebuah ATM switch dengan 4 buah komputer yang terhubung. (b) memperlihatkan detail dari setiap koneksi

Walaupun sebuah ATM *switch* memiliki kapasistas terbatas, banyak *switch* dapat dihubungkan untuk membangun jaringan yang lebih besar. Untuk menghubungkan komputer pada dua sisi ke dalam jaringan yang sama, sebuah *switch* dapat dipasang pada tiap sisi, dan kedua *switch* tersebut kemudian dapat dihubungkan. Koneksi antara dua *switch* agak berbeda dengan koneksi antara *switch* dengan host komputer. Koneksi antar *switch* dapat dilakukan pada kecepatan yang lebih tinggi dan dapat menggunakan protokol yang dimodifikasi. Gambar berikut mengilustrasikan topologi tersebut dan perbedaan antara sambungan antar jaringan atau *Network to Network Interface* (NNI), dan sambungan antara pengguna dengan jaringan atau *User to Network Interface* (UNI).



Gambar 2.26 Beberapa ATM switch membentuk jaringan besar

Gambar diatas memperlihatkan 3 buah ATM *switch* yang digabungkan membentuk sebuah jaringan besar. Meskipun antar muka NNI dirancang untuk digunakan antar *switch*, koneksi UNI dapat digunakan antar ATM *switch* dalam sebuah jaringan privat. Walaupun arsitektur fisikal memperbolehkan sebuah jaringan ATM terdiri dari banyak *switch*, perangkat keras ATM menyediakan layanan sambungan komputer dengan suatu jaringan fisik. Komputer yang terhubung dalam jaringan ATM tidak perlu mengetahui struktur fisik dari jaringan sehingga jaringan ATM secara logis dapat dilihat pada level yang paling bawah,

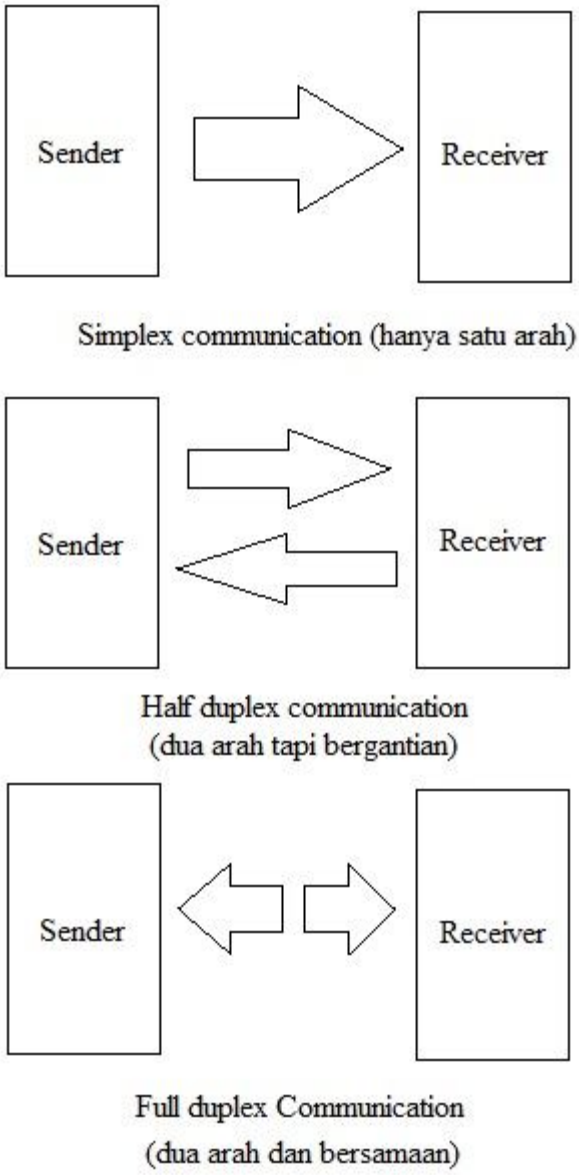
sebuah jaringan ATM menggunakan *fixed-size* frane yang disebut *cells* untuk membawa data. ATM membutuhkan semua sel berukuran sama karena dengan demikian memungkinakan untuk membuat perangkat keras untuk *switch*ing yang lebih cepat. Setiap sel ATM panjangnya 53 oktet, yang terdiri dari 5 oktet *header* dan 48 oktet data.

2.2.6.2 Peranan *Switch* pada LAN

Umumnya LAN bekerja secara *half duplex.* Artinya pada saat sebuah komputer sedang mengirim data, maka komputer yang lain hanya bisa "mendengarkan" hingga proses pengiriman data selesai. Kondisi semacam ini meirip dengan alay *walkie-talkie.* Dimana proses komunikasi dilakukan secara bergantian.

Namun setelah perangkat *switch* diperkenalkan dan teknologi *Ethernet* dikembangkan lebih maju, maka komunikasi data dapat dilakukan secara *full duplex. Switch* akan mengatur pemakaian media *network*. Secara teori keepatan dapat ditingkatkan hingga batas maksimal yang dapat dicapai, yaitu seuserr 100 Mbps atau lebih (bergantung pada jenis perangkatnya).

Komputer dapat mengirim dan menerima data secara bersamaan dengan kecepatan penuh. *full duplex* dapat dianalogikan dengan telepon rumah. Dimana dapat berbicara dan mendengarkan pada saat yang sama.

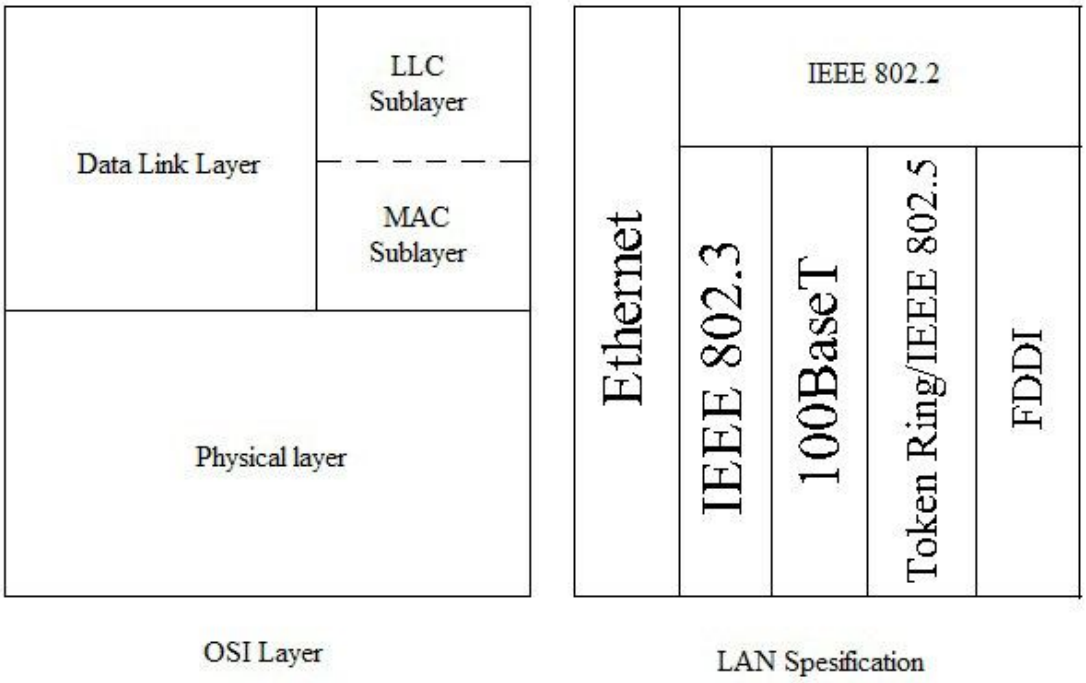


Gambar 2.27. Ilustrasi simplex, half-duplex dan full duplex

Manfaat lain dari *switch* adalah memecah sebuah *network* menjadi beberapa segmen atau dalam istilah teknis disebut sebagai *multiple collision domains.* Sementara alamat *broadcast-nya* masih tetap satu. Istilah yang biasa digunakan untuk menggambarkan kondisi ini yaitu *multiple collision domainsand single broadcast domain.*

2.2.6.3 Hubungan LAN dengan Model OSI

jika dikaitkan dengan model OSI, maka teknologi dan protokol yang diimplementasikan pada LAN hanya berhubungan dengan *layer Physical* dan *Data Link.* Tidak berarti bahwa LAN tidak berhubungan sama sekali dengan *layer* yang lain. Dalam prakteknya LAN tetap memerlukan aplikasi yang bekerja pada layer *Application*dan seterusnya.



Gambar 2.28 Hubungan LAN dengan OSI Layer

2.2.6.4 VLAN (*Virtual Local Area Network)*

Salah satu masalah yang dihadapi oleh LAN adalah tidak adanya mekanisme pengaturan yang fleksibel. *Administrator* akan cukup sulit mengelompokkan masing-masing host berdasarkan kategori tertentu. Seperti mengelompokkan beberapa *host* berdasarkan

kelompok kerja, berdasarkan departemen, aplikasi atau servis yang disediakan dan sebagainya.

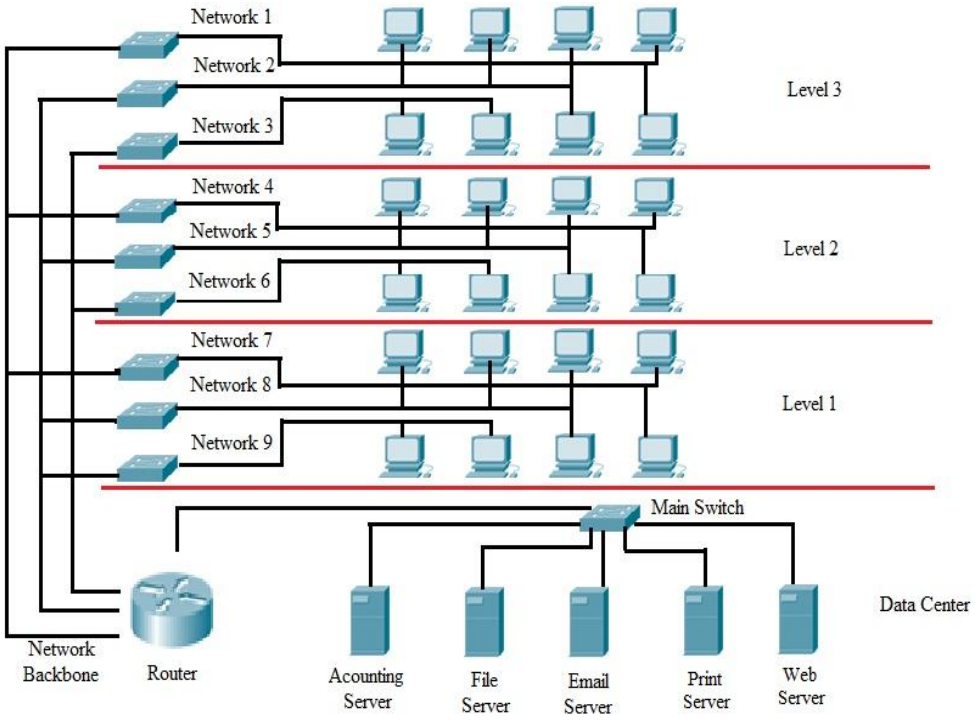
Apalagi jika ukuran LAN sudah cukup besar, misalkan sebesar kampus atau lebih besar lagi. Dimana masing-masing *host* berada ditempat yang cukup jauh. Akan sulit membuat kelompok berdasarkan kategori tertentu jika lokasi host terpencar-pencar atau berjauhan.

Untuk mengatasi hal tersebut, VLAN atau Virtual Local Area *Network* dapat menjadi solusinya. VLAN dapat mengatasi beberapa kesulitan yang tidak dapat diselesaikan oleh LAN. VLAN juga disebut mirip dengan *subnetwork* karena memeliki tujuan yang sama yaitu untuk membuat kelompok atau *group* yang terdiri atas beberapa komputer atau perangkat *network*.

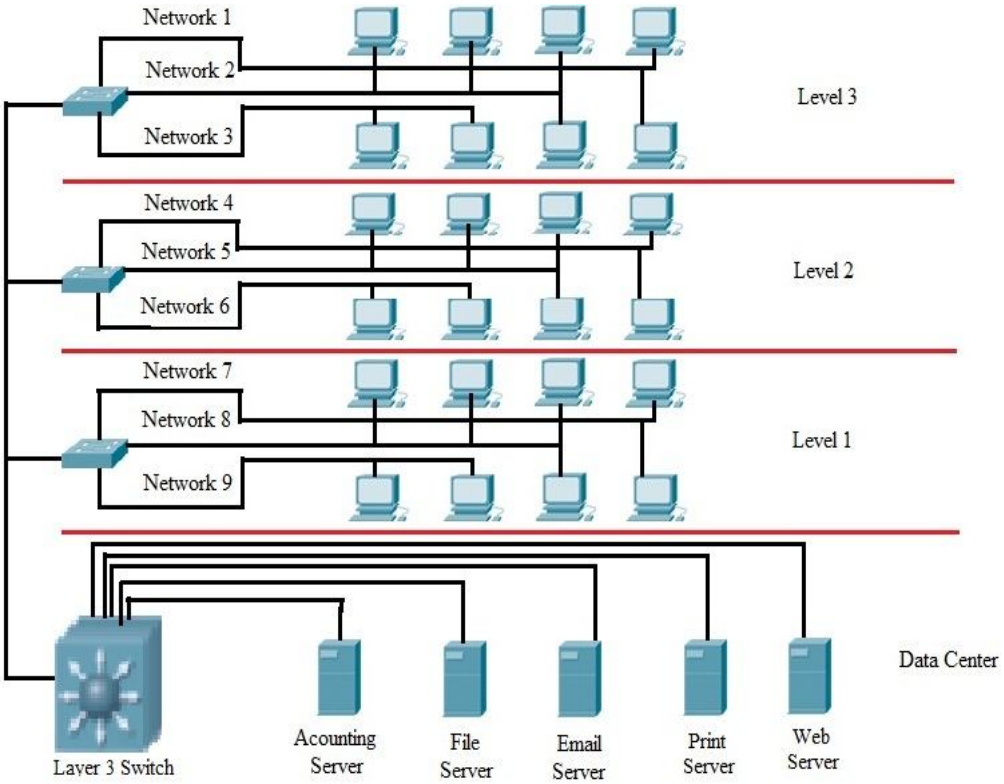
Ketika topologi fisik suatu LAN sudah ditentukan maka akan cukup sulit untuk merombaknya menjadi bentuk yang lain. Biasanya media fisik *network* akan ditanamkan pada pipa khusus yang suka dibongkar dan ditata ulang. Sehingga tidak dapat secara fleksibel Mengelompokkan kembali beberapa komputer yang lokasinya berjauhan (misal beda ruangan atau gedung) tanpa melalui proses bongkar pasang hardware.

VLAN dapat mengatasi keterbatasan ini. *Administrator* dapat secara fleksibel mengatur ulang "layout" *network* secara virtual. Artinya user tidak perlu membongkar media *network* dan mencabut kabel-kabel *switch*. Cukup mengatur ulang menggunakan *software* untuk menentukan komputer mana saja yang akan dikelompokkan. Selain itu, kebuthan *hardware,* kususnya *switch* dan *router* akan lebih sedikit dibandingkan LAN. Dengan memanfaatkan VLAN maka user tidak lagi dibatasi oleh kendala lokasi. Bahkan komputer-komputer yang berbeda pemakaian *switch* masih dapat dikelompokkan menjadi sebuah LAN.

VLAN dapat ditentukan berdasarkan lokasi, fungsi, departemen, aplikasi dan protokol yang digunakan. Sebagai contoh, terdapat dua VLAN. VLAN 1 digunakan untuk semua pengguna aplikasi A dan VLAN 2 digunakan untuk semua pengguna aplikasi B. untuk memahami apa yang dimaksudkan perhatikan gambar ilustrasi dibawah ini.



Gambar 2.29 Desain network tanpa VLAN



Gambar 2.30 Desain network dengan VLAN

Keuntungan lain pemakaian VLAN adalah untuk meningkatkan keamanan dan membagi broadcast domain menjadi beberapa broadcast domain yang lebih kecil. Dengan memanfaatkan VLAN, seorang *Administrator network* kini dapat mengontrol setiap *port switch* dan *user*. *User* tidak bisa dengan mudah menghubungkan kabel *network* pada *switch* untuk mengakses semua *resource network*. Sebab VLAN akan membatasi area berdasarkan *resource network* tertentu. Selain itu, switch dapat member tahu *network workstation* agar selalu meminta *user* untuk memasukkan login atau password ketika mulai mengakses network. Secara garis besar manfaat VLAN sebagai berikut :

1. Meningkatkan Performa Network

VLAN mampu meningkatkan performa network dengan cara memblok paket atau frame yang tidak perlu.

2. Desain Network yang Fleksibel

   VLAN memungkinkan anggota berpindah-pindah lokasi tanpa harus merombak ulang perangkat jaringan. Cukup melakukan konfigurasi secara software. VLAN dapat mengatasi persoalan lokasi.

3. Mengurangi Biaya Instalasi

   Jika hendak merubah VLAN maka tidak memerlukan biaya instalasi mauun penambahan perangkat baru.

4. Keamanan

   VLAN dapat mebatasi *user* yang boleh mengakses suatu aplikasi atau data berdasarkan *access list* yang bisa ditentukan.

2.2.6.5 Keanggotaan VLAN

Jika dilihat dari sisi keanggotaan maka VLAN dapat dibagi menjadi dua yaitu :

- *Static VLAN*

  Static VLAN merupakan tipe VLAN yang paling umum dan paling *secure*. Setiap anggota dari suatu VLAN ditentukan berdasarkan nomor *port switch*. Keanggotaan akan tetap selamanya seperti itu hingga penentuan yang lain. Biasanya dengan memindahkan kabel network ke port yang lain. Kadangkala static VLAN disebut sebagai *port based* VLAN.

- *Dynamic VLAN*

  Pada dynamic VLAN, keanggotaan akan ditentukan secara default (otomatis) menggunakan software yang diinstal pada *server* pusat, yang disebut VLAN

Management Policy Server (VMPS). Dengan menggunakan VMPS, *Administrator* dapat menentukan keanggotaan VLAN berdasarkan MAC *address*, protokol dan aplikasi untuk membentuk *dynamic* VLAN. Pada VMPS akan dilakukan *mapping* VLAN dan MAC *address.*

Tabel 2.8 Mapping VLAN ke MAC address

Entry	Keanggotaan VLAN	MAC address
1	2	00:16:D4:C9:E8:48
2	4	FE:DA:D1:C0:00:10
3	4	10:12:E4:A9:B8:09
4	12	DD:0D:26:52:78:35
5	4	C4:42:25:1F:DA:94
6	4	5B:90:09:BB:BC:25
7	12	E4:8E:FA:C4:A2:61
8	12	16:00:C9:D4:48:E8
9	2	BC:1A:00:1C:10:01
10	2	3F:C1:A3:10:09:C1

2.2.6.7 *Link* VLAN

VLAN dibangun menggunakan berbagai perangkat, seperti *switch, router, PC* dan sebagainya. tentunya diperlukan hubungan atau link diantara perangkat-perangkat tersebut. *Link* terkadang disebut sebagai sebagai *interface.* Ada dua jenis *link* yang digunakan yaitu :

- *Access Link*

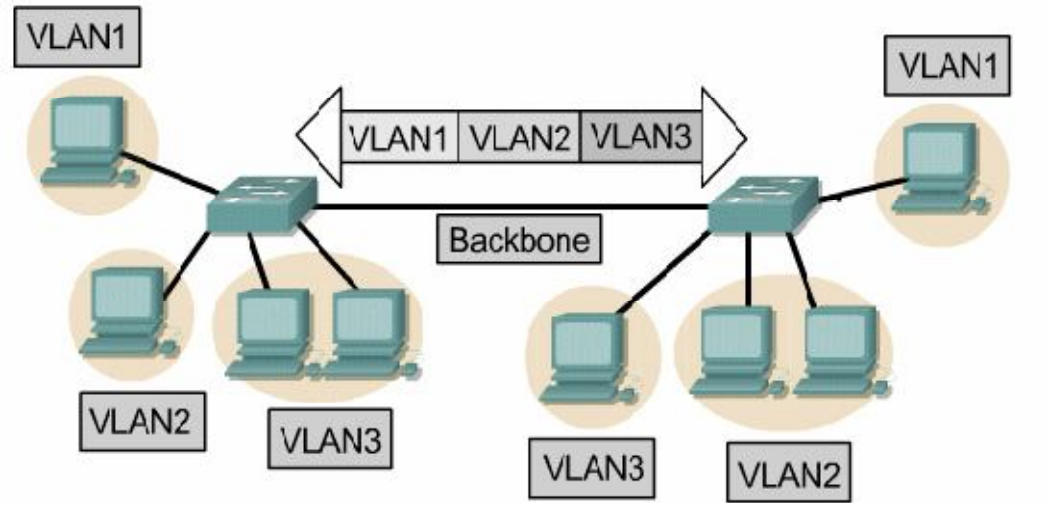
Access Link merupakan tipe *link* yang umum dan dimiliki oleh hamper semua jenis *switch* VLAN. *Acces Link* lazimnya digunakan untuk menghubungkan komputer dengan *switch. Access Link* tidak lain merupakan *port switch yang sudah terkonfigurasi.* Selama proses transfer data, *switch* akan membuang informasi tentang VLAN. Anggota suatu VLAN tidak bisa berkomunikasi dengan anggota VLAN yang lain, kecuali jika dihubungkan oleh *router*. *Access Link* mendukung teknologi *Ethernet* biasa (10Mbps) hingga *FastEthernet (*100Mbps).

- *Trunk Link*

  Isitlah *trunk* diambil dari system telepon yang dapat mengangkat beberapa percakapan sekaligus (*multipe conversation). Trunk Link* digunakan untuk menghubungkan *switch* dengan *switch* yang lain, *switch* dengan *router* atau *switch* dengan *server*. Jadi port telah dikonfigurasi untuk dilalui berbagai VLAN (tidak hanya sebuah VLAN). *Trunk Link* hanya mendukung teknologi *fast (*100Mbps) atau Gigabit (1000Mbps) *Ethernet.* Sebab *Trunk Link* biasanya dihubungkan dengan *Network Backbone* berkecepatan tinggi.

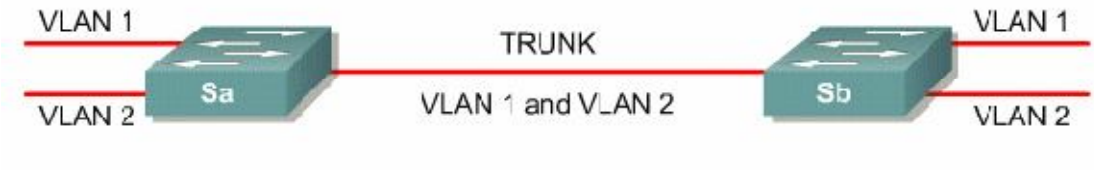
2.2.6.8 Trunking

Trunk adalah hubungan fisik dan logik antara dua switch melalui rute jaringan. Beberapa trunk akan ada pada satu backbone jaringan. Router, Switch dan Server dapa dihubungkan ke Trunk VLAN. Perhatikan gambar 2.31 dibawah ini :



Gambar 2.31. Trunk VLAN

Pada perangkat switching VLAN, trunk adalah link point-to-point yang mendukung beberapa VLAN. Berikut Gambar konsep yang diterapkan Trunking pada switching VLAN :

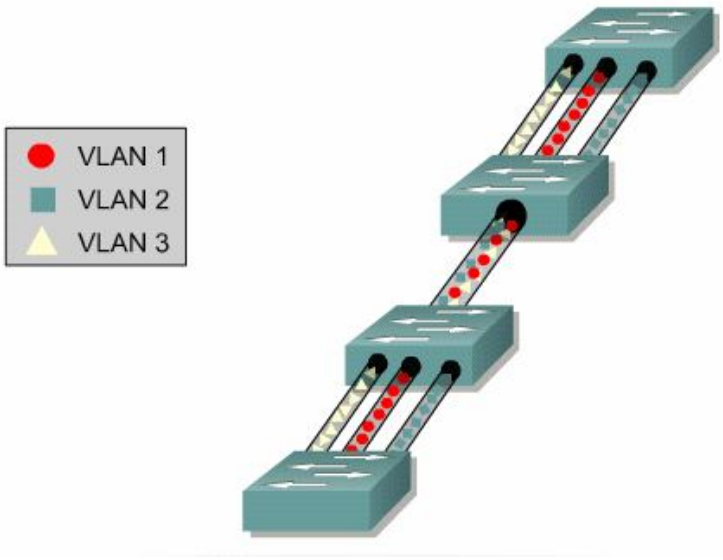


Gambar 2.32 Konsep Trunking pada switching VLAN

Protokol Trunking yang dikembangkan berfungsi untuk mengefektifkan pengelolaan transfer frame dari VLAN yang berbeda pada jalur fisik tunggal. Sekarang terdapat dua tipe mekanisme Trunking, yaitu *Frame Filtering* dan *Frame Tagging.*

2.2.6.9 Frame Taging

Frame taging adalah suatu cara yang digunakan untuk mengidentifikasi frame. Secara unik frame akan diberi ID *user*. setiap *switch* yang dilalui oleh frame akan membaca VLAN ID, kemudian menentukan "nasib frame" sesuai dengan daftar yang tersedia pada filter *table*. Terkadang *switch* dapat mengidentifikasi bahwa frame harus menempuh *Trunk Link* yang lain maka *switch* akan *memforward* frame tersebut ke *Trunk Link* yang berbeda.



Gambar 2.33 Konsep Frame Taging

Oleh IEEE, *Frame Tagging* diadopsi sebagai mekanisme *Trunking* standar. Protokol *Trunking* yang menggunakan mekanisme *Frame Tagging* ditandai satu *frame* identitas untuk memudahkan pengelolaan dan untuk mencapai penyampaian *frame* tercepat. Untuk mencapainya tiap *frame* dikirimkan pada link ber-tag untuk mengetahu identitas VLAN. Ada skema perbedaan tagging. Secara umum skema tagging untuk segmen *Ethernet* adalah ISL (protokol milik Cisco Inter-Swicth Link) dan 802.1Q (standar IEEE).

2.2.6.10 VLAN *Trunk Protocol* (VTP)

VTP merupakan protokol milik (*proprietary)* Cisco yang memungkinkan *switch-switch* Cisco yang terhubung saling bertukar informasi. VTP memudahkan proses konfigurasi secara otomatis antar sesame *switch*. Bayangkan jika sebuah *network* memiliki puluhan *switch* yang saling terhubung. Setiap *switch* menggunakan minimal sebuah port yang ditempatkan pada satu VLAN.

Tanpa VTP, seorang *Administrator* harus *login* satu per satu ke semua *switch* dan melakukan konfigurasi yang sama untuk membentuk sebuah VLAN. Dengan VTP , seorang *Administrator* cukup membuat suatu VLAN dengan hanya melakukan konfigurasi pada salah satu *switch* . sedangkan *switch* yang lainnya akan secara otomatis membuat VLAN yang sama.

VTP bekerja pada *layer* 2. *Administrator* dapat menambah, menghapus, mengedit, mengubah konfigurasi VLAN. Jika salah satu *switch* dirubah konfigurasinya, maka VTP akan melakukan *Sinkronisasi* kofigurasi terhadap *switch-switch* yang lain. Agar fitur VTP dapat dimanfaatkan maka harus ditentukan mode salah satu *switch* menjadi *Server mode.* Sedangkan *switch* lainnya harus disetting menjadi *Client Mode.* Ada 3 mode VTP yang disediakan, yaitu :

a) Server Mode

b) Client Mode

c) Transparent Mode

Konfigurasi VLAN harus dilakukan pada *switch server*. Sementara *switch-switch* lain (*client mode)* akan menyesuaikan konfigurasinya secara otomatis dengan *server*. Jika ada

switch tersebut hanya dapat *memforward* informasi VTP. *Switch* pada *transparent mode* tidak akan melakukan *sinkronisasi.* Berikut syarat-syarat agar fitur VTP dapat berfungsi :

a. *Switch-switch* harus memiliki VTP *domain name* yang sama

b. Menggunakan *Trunk* ISL atau 802.1q

c. Jika konfigurasi dilakukan pada beberapa *switch,* maka *switch-switch* tersebut harus memiliki *password* yang sama.

2.2.7 TCP/IP

Cukup sulit untuk mendefinisikan secara tepat apa yang disebut protokol. Protokol memiliki banyakk variasi dan banyak tujuan penggunaan. Secara sederhana dapat dijelaskan, protokol adalah sekumpulan aturan dalam komunikasi data. Protokol mengatur terjadinya hubungan dan perpindahan data antara dua atau lebih komputer. Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi keduanya. Pada tingkatan yang terendah, protokol mendefiniskan koneksi perangkat keras. Sebagian besar protokol memiliki karakteristik sebagai berikut :

a) Melakukan deteksi apakah ada koneksi fisik atau tidak yang dilakukan oleh komputer atau mesin lain.
b) Melakukan *handshaking.*
c) Menjadi negosiator berbagai macam karakteristik koneksi.
d) Mengatur bagaimana mengawali dan mengakhiri suatu pesan.
e) Menentukan format pesan.
f) Melakukan *error detection* dan *error correction* saat terjadinya kerusakan pesan.
g) Mengakhiri suatu koneksi.

Secara umum format protokol meliputi :

a) Format informasi
b) Pewaktuan (*timing)*
c) Urutan (*sequencing)*
d) Control kesalahan (*erro control)*

Pada masa ARPANET protokol yang digunakan untuk komunikasi data adalah NCP (*Network Communication Protocol)*. Semakin lama ukuran ARPANET semakin besar dan NCP tidak sanggup menampung node komputer yang lebih besar. DARPA kemudian mendanai pembuatan protokol komunikasi yang lebih umum. Protokol itu dinamakan TCP/IP. Departemen pertahanan amerika menyatakan TCP/IP menjadi standar untuk jaringannya pada tahun 1982. Protokol ini kemudian diadopsi menjadi standar ARPANET pada tahun 1983. Perusahaan Bolt Beranek Newman (BBN) membuat protokol TCP/IP supaya dapat berjalan di atas komputer dengan system operasi UNIX.

TCP/IP memiliki karakteristik yang membedakannya dari protokol-protokol komunikasi yang lain, diantaranya :

a) Bersifat standar, terbuka dan tidak bergantung pada perangkat keras atau system operasi tertentu.
b) Bebas dari jaringan fisik tertentu, memungkinkan integrasi berbagai jenis jaringan (*Ethernet, token ring, dial-up)*
c) Mempunyai skema pengalamatan yang umum bagi setiap *device* yang terhubung dengan jaringan.
d) Menyediakan berbagai layanan bagi *user*.

Berikut ini penjelasan secara singkat masing-masing *layer* protokol TCP/IP beserta fungsinya :

1. Lapisan pertama adalah ***Network Access Layer*** (identik dengan lapisan Physical dan Data Link layer pada OSI). Pada lapisan ini, didefinisikan bagaimana penyaluran data dalam bentuk frame-frame data pada media fisik yang digunakan secara handal. Lapisan ini biasanya memberikan servis untuk deteksi dan koreksi kesalahan dari data yang ditransmisikan. Beberapa contoh protokol yang digunakan pada lapisan ini adalah X.25 untuk jaringan public, *Ethernet* untuk jaringan *Ethernet* dan sebagainya.
2. Lapisan kedua adalah ***Internet Layer*** (identik dengan network layer pada OSI). Lapisan ini bertugas untuk menjamin agar suatu paket yang dikirimkan dapat menemukan tujuannya. Lapisan ini memiliki peranan penting terutama dalam mewujudkan *Internetworking* yang meliputi wilayah luas (worldwide *internet)*. Beberapa tugas penting pada lapisan ini adalah :
    a) ***Addressing,*** yakni melengkapi setiap paket data dengan alamat internet atau yang dikenal dengan *Internet Protocol address* (IP *address)*. Karena pengalamatan (*addressing)* berada pada level ini, maka jaringan TCP/IP independen dari jenis media, system operasi dan komputer yang digunakan.
    b) **Routing,** yakni menentukan rute atau arah paket data yang akan dikirim kan agar mencapai tujuan yang diinginkan. Routing merupakan fungsi penting dari *internet protocol* (IP). Proses routing sepenuhnya ditentukan oleh jaringan. Pengirim tidak memiliki kendali terhadap paket yang

kirimkannya. Router-router pada jaringan TCP/IP yang menentukan penyampaian paket data dari pengirim ke penerima.

3. Lapisan ketiga adalah ***Transport Layer*** (identik dengan *Tranport Layer pada OSI)*. Pada lapisan ini didefinisikan cara-cara untuk melakukan pengiriman data antar *end* to *end host*. Lapisan ini menjamin bahwa informasi yang diterima pada sisi penerima akan sama dengan informasi yang dikirim oleh pengirim. Lapisan ini memili beberapa fungsi penting antara lain :

    a) **Flow Control.** Pengiriman data yang telah dipecah menjadi paket-paket data harus diatur sedemikian rupa agar pengirim tidak sampai mengirimkan data dengan kecepatan yang melebihi kemampuan penerima dalam menerima data.

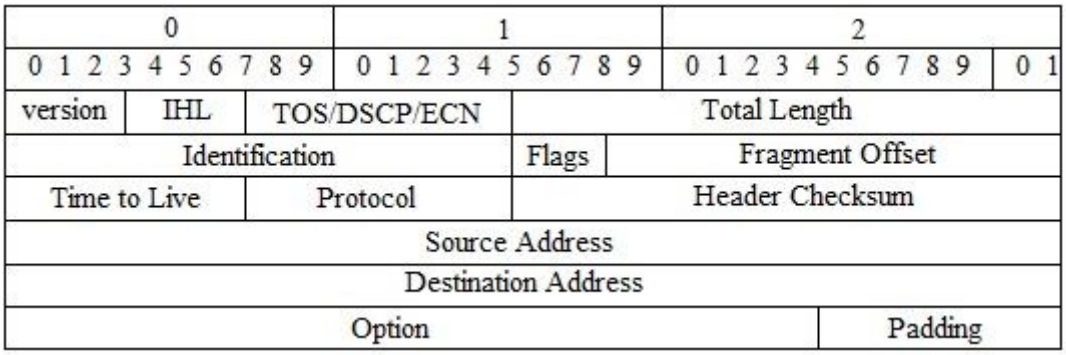
    b) **Error Detection.** Pengirim dan penerima melengkapi data dengan sejumlah informasi yang bisa digunakan untuk memeriksa data yang dikirimkan telah bebas dari kesalahan atau tidak. Jika ditemukan kesalahan pada paket data yang diterima, maka penerima tidak akan menerima paket data tersebut. Pengirim akan mengirim ulang paket data yang mengandung kesalahan sampai penerima menerima paket data tersebut. Dengan demikian, data dijamin bebas dari kesalahan (*error free)* pada saat diteruskan ke lapisan aplikasi. Konsekuensi dari mekanisme ini adalah timbulnya *delay* yang cukup berarti. Namun selama aplikasi tidak bersifat *real-time, delay* ini tidak akan menjadi masalah karena yang lebih diutamakan adalah data yang bebas dari kesalahan. Ada dua buah protokol yang digunakan pada *layer* ini, yaitu *Transmission Control Protocol* (TCP) dan *User Program Protocol* (UDP). TCP digunakan oleh aplikasi-aplikasi yang membutuhkan

keandalan data. Sedang UDP digunakan untuk aplikasi yang tidak menuntut keandalan tinggi. Beberapa aplikasi lenih sesuai dengan menggunakan UDP sebagai protokol *transport*. Contohnya aplikasi *database* yang hanya bersifat *query* dan *response* atau aplikasi lain yang sangat sensitif terhadap delay seperti *video conference.* Aplikasi seperti ini dapat mentolerir sedikit kesalahan karena gambar atau suara masih tetap bisa dimengerti.TCP memiliki *flow control* dan *error detection* yang bersifat *connectionless,* tidak ada mekanisme pemeriksaan data dan *flow control,* sehingga UDP disebut juga *unreliable proyocol.*

4. Lapisan ke empat adalah ***Application Layer*** (identik dengan *Application, Presentation, Session Layer pada* OSI). Sesuai dengan namanya, lapisan mendefinisikan aplikasi-aplikasi yang dijalan pada jaringan. Cukup banyak protokol yang telah dikembangkan pada lapisan ini. Contohnya adalah SMTP (*simple mail transfer protocol)* untuk pengiriman Email, FTP (*file transfer protocol*) untuk transfer file, HTTP (*hyper text transfer protocol)* untuk apliasi berbasis web atau WWW (*wide world web),* NTTP (*network news transfer protocol)* untuk distribusi *news group* dan sebagainya,

2.2.8 IP Address

Pada *Layer* internet dapat ditemukan sebuah protokol yang popular yaitu *Internet Protocol* (IP). IP merupakan protokol yang bersifat *Connectionless* dan *Unreliable.* IP (*internet protocol)* juga termasuk inti dari protokol TCP/IP. Pada *header* IP terdapat field berisi informasi *internet address* atau IP *address.* IP *address* asal dan tujuan dari paket data. Perhatikan diagram *header* protokol IP berikut.



Gambar 2.34 Header Protocol IP

IP *address* dibentuk oleh sekumpulan bilangan biner sepanjang 32 *bit,* yang dibagi atas 4 bagian. Setiap bagian panjangnya 8 *bit.* IP *address* nerupakan identifikasi setiap host pada jaringan internet. Artinya tidak boleh ada host lain menggunakan IP *address* yang sama. Contoh IP *address* sebagai berikut :

0100 0100 1000 0001 1111 1111 0000 0001

Apabila setiap bagian user konversikan kebilangan decimal maka IP *address* diatas menjadi

68.129.255.1

Bentuk penulisan IP *address* diatas dikenal dengan notasi "*doted decimal*". IP jenis inilah yang biasa digunakan sebagai alamat *host.* IP address dibagi menjadi lima kelas, A sampai E. IP *address* yang dipakai secara umum dibagi dalam 3 kelas, sementara 2 kelas lainnya dipakai untuk kepentingan khusus. Ini untuk memudahkan pendistribusian IP *address* ke seluruh dunia. Berikut penjelasan masing-masing kelas IP *address:*

1. KELAS A :
    a) Format : 0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh
    b) Bit pertama : 0
    c) Panjang Network ID : 8 bit

d) Panjang Host ID : 24 bit

e) Byte pertama : 0 – 127

f) Jumlah : 126 kelas A (0 dan 127 dicadangkan)

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

h) Jumlah IP : 16.777.214 IP address pada tiap kelas A

i) IP address kelas ini diberikan kepada suatu jaringan yang berukuran sangat besar, yang pada tiap jaringannya terdapat sekitar 16 juta host.

2. KELAS B :

a) Format : 10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh

b) 2 bit pertama : 10

c) Panjang Network ID : 16 bit

d) Panjang Host ID : 16 bit

e) Byte pertama : 128 – 191

f) Jumlah : 16.384 kelas B

g) Range IP : 128.0.xxx.xxx sampai 191.155.xxx.xxx

h) Jumlah IP : 65.535 IP address pada tiap kelas B

i) IP address kelas ini diberikan kepada jaringan dengan ukuran sedang-besar.

3. KELAS C

a) Format : 110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh

b) 3 bit pertama : 110

c) Panjang Network ID : 24 bit

d) Panjang Host ID : 8 bit

e) Byte pertama : 192 – 223

f) Jumlah : 2.097.152 kelas C

g) Range IP : 192.0.0.xxx sampai 223.255.255.xxx

h) Jumlah IP : 254 IP address pada tiap kelas C

i) IP kelas ini dialokasikan untuk jaringan berukuran kecil.

IP kelas D digunakan sebagai alamat multicast yaitu sejumlah komputer memakai bersama suatu aplikasi. Contohnya adalah aplikasi real-time video conference yang melibatkan lebih dari dua host. Ciri IP kelas D adalah 4 bit pertamanya 1110. IP kelas E (4 bit pertama 1111) dialokasikan untuk keperluan eksperimental.

Yang perlu diperhatikan dalam pemilihan IP address adalah aturan dasar pemilihan Network ID dan Host ID :

a) Network ID tidak boleh bernilai 127. Karena Network ID 127 digunakan sebagai alamat loopback yaitu alamat yang digunakan komputer untuk menunjuk dirinya sendiri.
b) Network ID dan Host ID tidak boleh seluruhnya bernilai 255 (seluruh bit diset 1). Nework ID atau Host ID yang seluruhnya bernilai 255 adalah alamat broadcast jaringan tersebut. Apabila dikirimkan pesan kepada alamat broadcast maka seluruh host pada jaringan tersebut akan menerima pesan itu.
c) Network ID dan Host ID tidak boleh seluruhnya bernilai 0 (seluruh bit diset 0). Alamat IP dengan host id semuanya bernilai 0 diartikan sebagai alamat network yang menunjuk ke jaringan, bukan ke host.
d) Host ID harus unik dalam satu network.

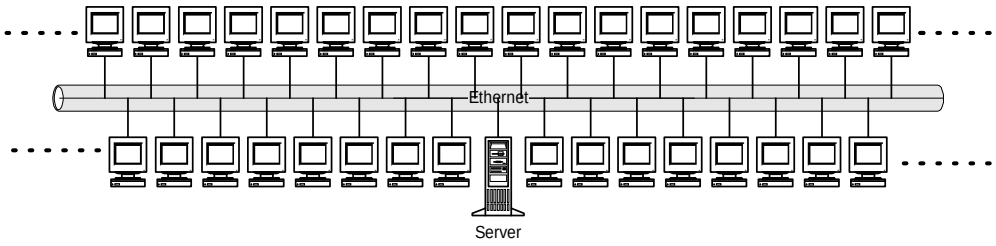
2.2.9 Subnetting

Jumlah IP Address sangat terbatas, apalagi jika harus memberikan alamat semua host di Internet. Oleh karena itu, perlu dilakukan efisiensi dalam penggunaan IP Address supaya dapat mengalamati semaksimal mungkin host yang ada dalam satu jaringan. Konsep subnetting dari IP Address merupakan teknik yang umum digunakan di Internet untuk mengefisienkan alokasi IP Address dalam sebuah jaringan supaya bisa memaksimalkan penggunaan IP Address. Routing & konsekuensi logis lainnya akan terjadi dengan lebih effisien dengan metoda subnetting yang baik.

Untuk beberapa alasan yang menyangkut efisiensi IP Address, mengatasi masalah topologi network dan organisasi, network administrator biasanya melakukan subnetting. Esensi dari subnetting adalah “memindahkan” garis pemisah antara bagian network dan bagian host dari suatu IP Address. Beberapa bit dari bagian host dialokasikan menjadi bit tambahan pada bagian network. Address satu network menurut struktur baku dipecah menjadi beberapa subnetwork. Cara ini menciptakan sejumlah network tambahan dengan mengurangi jumlah maksimum host yang ada dalam tiap network tersebut.

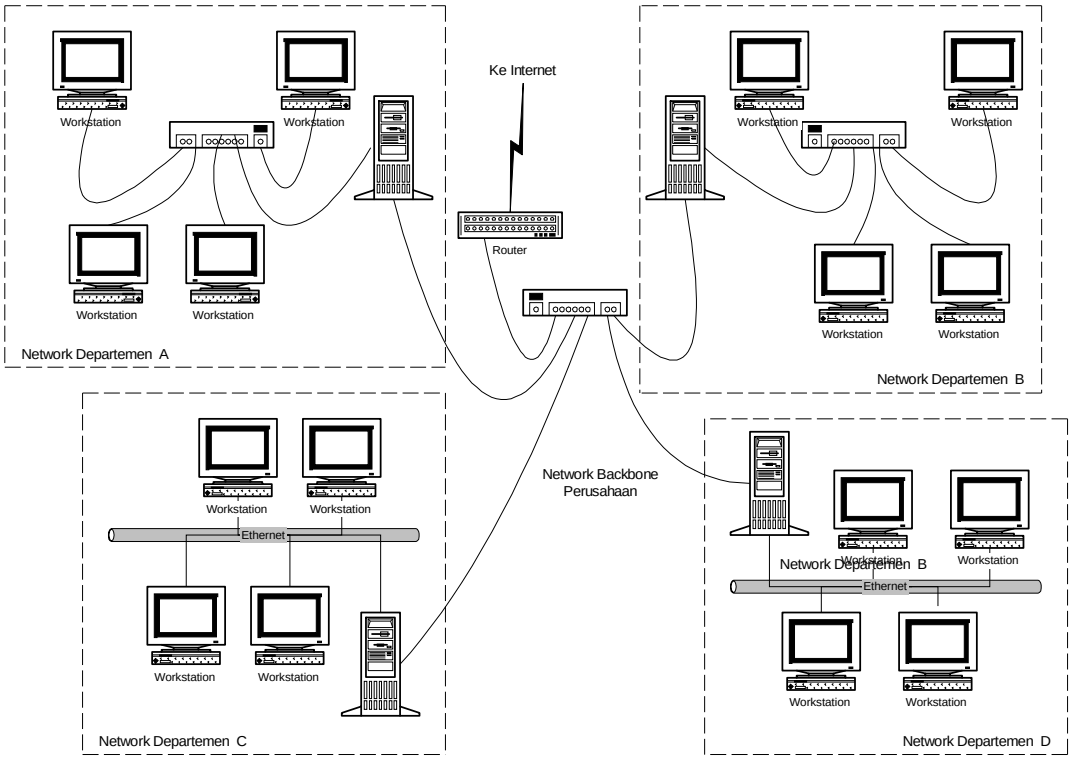
Tujuan lain dari subnetting yang tidak kalah pentingnya adalah untuk mengurangi tingkat congesti dalam suatu network. Perhatikan bahwa pengertian satu network secara logika adalah host-host yang tersambung pada suatu jaringan fisik. Misalkan pada suatu LAN dengan topologi bus, maka anggota suatu network secara logika haruslah host yang tersambung pada bus tersebut. Jika menggunakan hub untuk topologi star, maka keseluruhan network adalah semua host yang terhubung dalam hub yang sama. Bayangkan jika network kelas B hanya dijadikan satu network secara logika, maka seluruh host yang jumlahnya dapat mencapai puluhan ribu itu akan “berbicara” pada media yang sama. Jika user perhatikan

ilustrasi pada Gambar 3.34, hal ini sama dengan ratusan orang berada pada suatu ruangan. Jika ada banyak orang yang berbicara pada saat bersamaan, maka pendengaran user terhadap seorang pembicara akan terganggu oleh pembicara lainnya. Akibatnya, user bisa salah menangkap isi pembicaraan, atau bahkan sama sekali tidak bisa mendengarnya. Artinya tingkat kongesti dalam jaringan yang besar akan sangat tinggi, karena probabilitas "tabrakan" pembicaraan bertambah tinggi jika jumlah yang berbicara bertambah banyak.



Gambar 2.35 Satu Physical Network dengan Host yang Sangat Banyak

Untuk menghindari terjadinya kongesti akibat terlalu banyak host dalam suatu physical network, dilakukan segmentasi jaringan. Misalkan suatu perusahaan yang terdiri dari 4 departemen ingin memiliki LAN yang dapat mengintegrasikan seluruh departemen. Masing-masing departemen memiliki Server sendiri-sendiri (bisa berupa Novell Server, Windows NT atau UNIX). Cara yang sederhana adalah membuat topologi network perusahaan tersebut ditampilkan pada Gambar 2.35. User membuat 5 buah physical network (sekaligus logical network), yakni 4 buah pada masing-masing departemen, dan satu buah lagi sebagai jaringan backbone antar departemen. Dengan kata lain, user membuat beberapa subnetwork (melakukan subnetting). Keseluruhan komputer tetap dapat saling berhubungan karena Server juga berfungsi sebagai router. Pada server terdapat dua network interface, masing-masing tersambung ke jaringan backbone dan jaringan departemennya sendiri



Gambar 2.36 Subnetting secara Fisik

Subnetting juga dilakukan untuk mengatasi perbedaan hardware dan media fisik yang digunakan dalam suatu network. Router IP dapat mengintegrasikan berbagai network dengan media fisik yang berbeda hanya jika setiap network memiliki address network yang unik. Selain itu, dengan subnetting, seorang network administrator dapat mendelegasikan alokasi IP address untuk host di seluruh departemen dari suatu perusahaan besar kepada setiap departemen, untuk memudahkannya dalam mengatur keseluruhan network. Setelah membuat subnet secara fisik, user juga harus membuat *subnet logic*. Masing-masing subnet fisik setiap departemen harus mendapat *subnet logic* yang berbeda, berupa network address yang merupakan bagian (sub) dari network address perusahaan.

2.2.10 DHCP

DHCP (Dynamic Host Configuration Protocol) adalah protokol yang berbasis arsitektur client/server yang dipakai untuk memudahkan pengalokasian alamat IP dalam satu jaringan. Sebuah jaringan lokal yang tidak menggunakan DHCP harus memberikan alamat IP kepada semua komputer secara manual. Jika DHCP dipasang di jaringan lokal, maka semua komputer yang tersambung di jaringan akan mendapatkan alamat IP secara otomatis dari server DHCP. Selain alamat IP, banyak parameter jaringan yang dapat diberikan oleh DHCP, seperti default gateway dan DNS server. DHCP dibuat bertujuan sebagai berikut :

a. Tidak ada manual konfigurasi pada klien
b. Satu server dapat menangani banyak subnet. (Administrator jaringan tidak perlu menyediakan sebuah komputer per subnet untuk memberikan layanan DHCP, karena itu DHCP hanya perlu bekerja melalui router melalui banyak subnet.)
c. Banyak server diijinkan. (Untuk redundansi dan reliabilias, server dan klien harus dapat berhubungan dengan banyak server aktif pada satu jaringan)
d. Host-host yang terkonfigurasi secara statis harus berdampingan. (Host-host yang untuk beberapa alasan memerlukan alamat IP yang sama, atau yang tidak dapat berpartisipasi dalam protokol DHCP, harus dapat bekerja dalam jaringan yang sama secara harmonis).
e. BOOTP berdampingan. (Implementasi-implementasi DHCP harus beroperasi dengan agen relai BOOTP dan memberikan layanan pada klien BOOTP.)
f. Jaminan alamat yang unik (DHCP tidak boleh memberikan alamat IP yang sama pada banyak klien)

g. Menjaga informasi klien. (DHCP harus menjaga parameterparameter setiap klien dalam penyimpanan yang stabil sehingga server yang beroperasi lama tidak akan mempengaruhi integritas informasi) DHCP didefinisikan dalam RFC 2131 dan RFC 2132 yang dipublikasikan oleh Internet Engineering Task Force. DHCP merupakan ekstensi dari protokol Bootstrap Protocol (BOOTP).

Karena DHCP merupakan sebuah protokol yang menggunakan arsitektur client/server, maka dalam DHCP terdapat dua pihak yang terlibat, yakni DHCP Server dan DHCP Client.

1. DHCP server merupakan sebuah mesin yang menjalankan layanan yang dapat "menyewakan" alamat IP dan informasi TCP/IP lainnya kepada semua klien yang memintanya. Beberapa sistem operasi jaringan seperti Windows NT Server, Windows 2000 Server, Windows Server 2003, atau GNU/Linux memiliki layanan seperti ini.
2. DHCP client merupakan mesin klien yang menjalankan perangkat lunak klien DHCP yang memungkinkan mereka untuk dapat berkomunikasi dengan DHCP Server. Sebagian besar sistem operasi klien jaringan (Windows NT Workstation, Windows 2000 Professional, Windows XP, Windows Vista, atau GNU/Linux) memiliki perangkat lunak seperti ini. DHCP server umumnya memiliki sekumpulan alamat yang diizinkan untuk didistribusikan kepada klien, yang disebut sebagai DHCP Pool. Setiap klien kemudian akan menyewa alamat IP dari DHCP Pool ini untuk waktu yang ditentukan oleh DHCP, biasanya hingga beberapa hari. Manakala waktu penyewaan alamat

IP tersebut habis masanya, klien akan meminta kepada server untuk memberikan alamat IP yang baru atau memperpanjangnya.

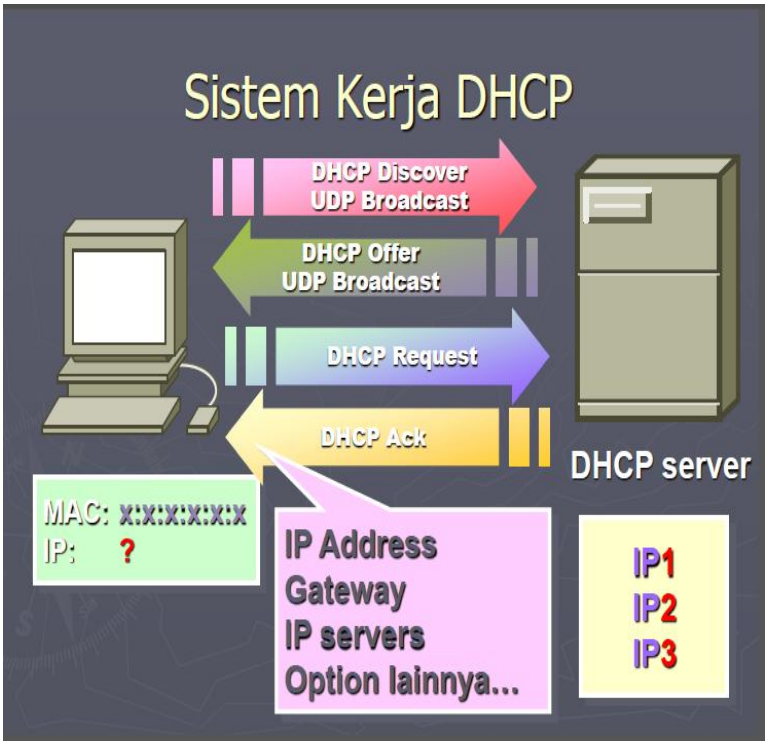
DHCP Client akan mencoba untuk mendapatkan “penyewaan” alamat IP dari sebuah DHCP server dalam proses empat langkah berikut (dengan catatan DHCP server harus memiliki alamat IP yang statis) :

1. DHCPDISCOVER: DHCP client akan menyebarkan request secara broadcast untuk mencari DHCP Server yang aktif.
2. DHCPOFFER: Setelah DHCP Server mendengar broadcast dari DHCP Client, DHCP server kemudian menawarkan sebuah alamat kepada DHCP client.
3. DHCPREQUEST: Client meminta DCHP server untuk menyewakan alamat IP dari salah satu alamat yang tersedia dalam DHCP Pool pada DHCP Server yang bersangkutan.
4. DHCPACK: DHCP server akan merespons permintaan dari klien dengan mengirimkan paket acknowledgment. Kemudian, DHCP Server akan menetapkan sebuah alamat (dan konfigurasi TCP/IP lainnya) kepada klien, dan memperbarui basis data database miliknya. Klien selanjutnya akan memulai proses binding dengan tumpukan protokol TCP/IP dan karena telah memiliki alamat IP, klien pun dapat memulai komunikasi jaringan.

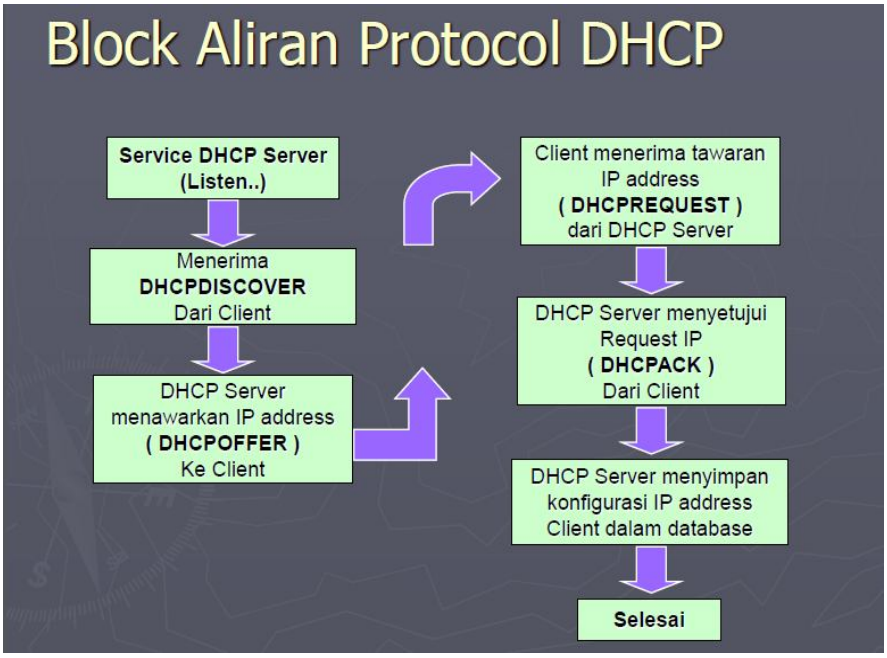
Empat tahap di atas hanya berlaku bagi klien yang belum memiliki alamat. Untuk klien yang sebelumnya pernah meminta alamat kepada DHCP server yang sama, hanya tahap 3 dan tahap 4 yang dilakukan, yakni tahap pembaruan alamat (address renewal), yang jelas lebih cepat prosesnya. Berbeda dengan sistem DNS yang terdistribusi, DHCP bersifat stand-

alone, sehingga jika dalam sebuah jaringan terdapat beberapa DHCP server, basis data alamat IP dalam sebuah DHCP Server tidak akan direplikasi ke DHCP server lainnya. Hal ini dapat menjadi masalah jika konfigurasi antara dua DHCP server tersebut berbenturan, karena protokol IP tidak mengizinkan dua host memiliki alamat yang sama. Selain dapat menyediakan alamat dinamis kepada klien, DHCP Server juga dapat menetapkan sebuah alamat statik kepada klien, sehingga alamat klien akan tetap dari waktu ke waktu. Contoh Cara kerja sistem ini adalah:

1. pada suatu LAN, cukup ada SATU DHCP server. DHCP server ini diset untuk membagikan alamat IP dengan rentang tertentu, misal 192.168.0.100 - 192.168.0.199.
2. Ada banyak komputer client. Setiap komputer diset agar TCP/IP nya memakai mode AUTO.
3. Saat komputer client dihidupkan, dia akan menyebarkan permintaan alamat IP.
4. DHCP server akan menangkap permintaan ini, lalu memberikan nomor IP unik dalam rentang yang telah ditentukan. Bersamaan dengan itu, juga dapat diberikan informasi lain seperti netmask, alamat dns server, maupun gateway.
5. Si client bisa men-set TCP/IP-nya sesuai informasi yang diberikan dan mulai bekerja.
6. Alamat IP ini hanya pinjaman. Setelah selang waktu yang ditentukan, DHCP server akan menagihnya kembali agar dapat dipinjamkan ke client lain. Jadi si client harus memperbaharui pinjamannya (leasing) secara berkala.



Gambar 2.37 Sistem kerja DHCP



Gambar 2.38 Block aliran Protokol DHCP

DHCP Scope adalah alamat -alamat IP yang dapat disewakan kepada DHCP client. Ini juga dapat dikonfigurasikan oleh seorang administrator dengan menggunakan peralatan konfigurasi DHCP server. Biasanya, sebuah alamat IP disewakan dalam jangka waktu tertentu, yang disebut sebagai DHCP Lease, yang umumnya bernilai tiga hari. Informasi mengenai DHCP Scope dan alamat IP yang telah disewakan kemudian disimpan di dalam basis data DHCP dalam DHCP server. Nilai alamat -alamat IP yang dapat disewakan harus diambil dari DHCP Pool yang tersedia yang dialokasikan dalam jaringan. Kesalahan yang sering terjadi dalam konfigurasi DHCP Server adalah kesalahan dalam konfigurasi DHCP Scope.

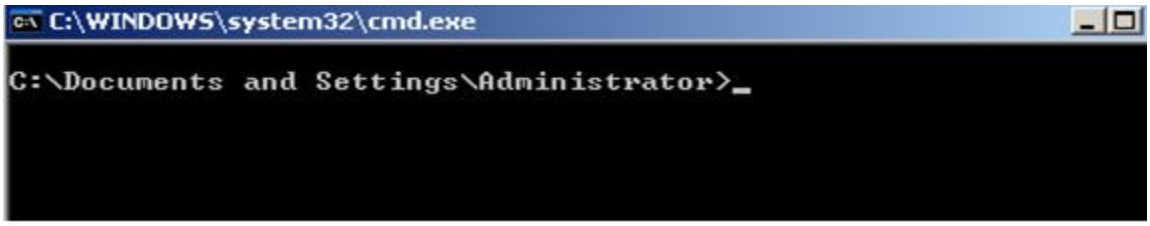
DHCP Lease adalah batas waktu penyewaan alamat IP yang diberikan kepada DHCP client oleh DHCP Server. Umumnya, hal ini dapat dikonfigurasikan sedemikian rupa oleh seorang administrator dengan menggunakan beberapa peralatan konfigurasi (dalam Windows NT Server dapat menggunakan DHCP Manager atau dalam Windows 2000 ke atas dapat menggunakan Microsoft Management Console [MMC]). DHCP Lease juga sering disebut sebagai Reservation.

DHCP Options adalah tambahan pengaturan alamat IP yang diberikan oleh DHCP ke DHCP client. Ketika sebuah klien meminta alamat IP kepada server, server akan memberikan paling tidak sebuah alamat IP dan alamat subnet jaringan. DHCP server juga dapat dikonfigurasikan sedemikian rupa agar memberikan tambahan informasi kepada klien, yang tentunya dapat dilakukan oleh seorang administrator. DHCP Options ini dapat diaplikasikan kepada semua klien, DHCP Scope tertentu, atau kepada sebuah host tertentu dalam jaringan.

2.2.11 Putty dan Telnet

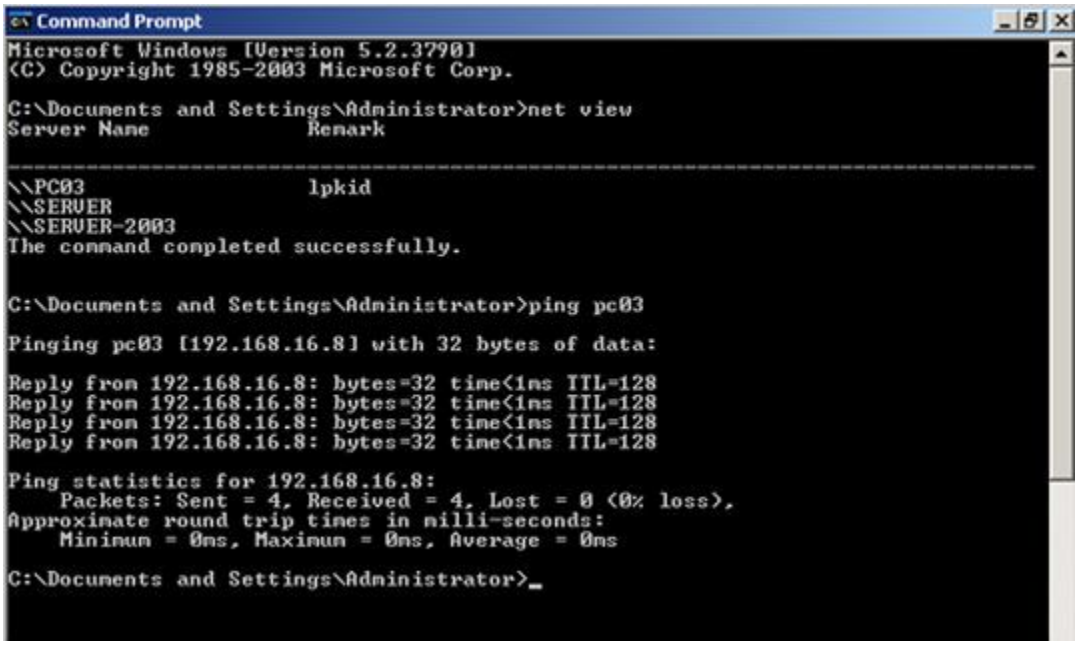
Putty merupakan software remote console atau terminal berbasis open source yang berfungsi untuk melakukan remote ke suatu server (komputer) yang membuka port 21 (telnet), port 22 (SSH). Telnet adalah salah satu fasilitas yang sering digunakan untuk meremote computer dalam suatu jaringan melalui underdos (CMD). Perintah Telnet dapat dinyatakan gagal koneksi bila konfigurasi Telnet tersebut tidak aktif. Perintah Telnet merupakan perintah remote desktop yang artinya bisa melakukan pengendalian komputer secara otomatis. Sebagai contoh penulis akan memberikan capture cara melakukan telnet pada komputer User :

Langkah awal cek konfigurasi telnet pada komputer dengan menekan tombol windows + R (klik Run – ktikan CMD terus klik OK) sampai muncul tampilan Dos :



Gambar 2.39 Tampilan DOS dalam pengecekan konfigurasi telnet

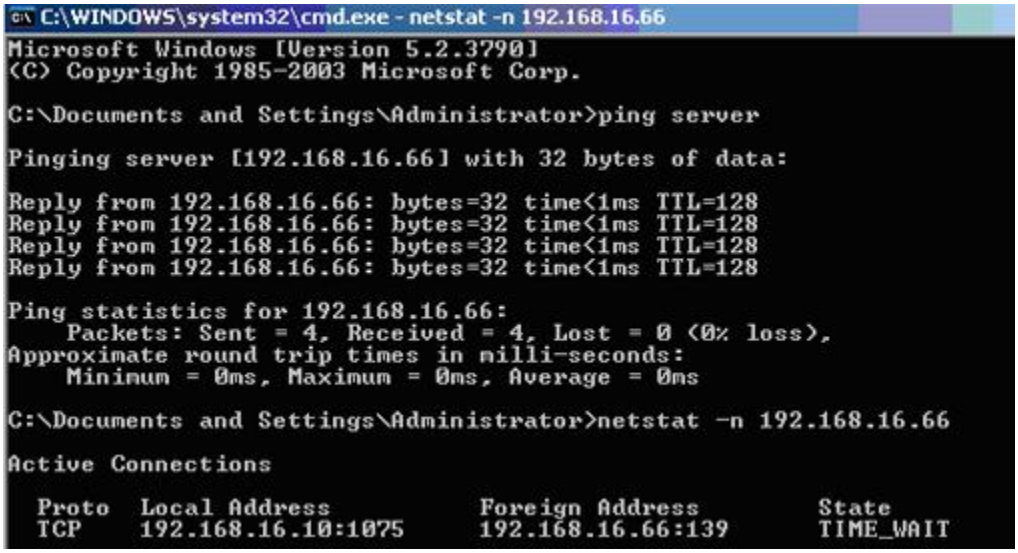
Untuk mengecek apakah fungsi telnet sudah bisa dilakukan atau belum sebaiknya cek terlebih dahulu komputer mana saja yang sedang berjalan.



Gambar 2.40 Tampilan DOS dalam pengecekan port yang terhubung ke server.

Pada tampilan diatas server akan mencoba dengan beberapa perintah **-net view**, tujuannya adalah untuk mengecek jaringan (host) mana saja yang sedang aktif. Pada gambar 2.40 terdapat beberapa host yang sedang terkoneksi dengan computer server yaitu **PC-03.**

Kemudian server akan mencoba melakukan ping ke PC -03 , pada gambar 2.40 ternyata dihasilkan **IP 192.168.16.8**. Selanjutnya akan melakukan pengecekan port mana saja yang bisa disusupi ke computer tersebut misalnya user ingin mengechek computer **SERVER** yang lain.



Gambar 2.41 Tampilan DOS port yang terhubung ke server.

Perhatikan pada Bagian Foreign Address! Disitu terdapat sebuah Port yang terbuka dengan **port 139,** jika sudah seperti keterangan yang ada pada gambar 2.41 maka coba lakukan **telnet** (spasi) **IP** tujuan(spasi)**noPort:** ***telnet 192.168.16.66 139***. jika benar maka akan menghasilkan :



Gambar 2.42 Tampilan sukses login telnet.