Protokol TCP/IP
Bagian 1

PRASIMAX

TECHNOLOGY DEVELOPMENT CENTER

Revision 1.0

PRASIMAX Product Research Division
Jl. Margonda Raya 494E
Depok 16424, Indonesia
Tel : +62-21-7888-0672
Fax: +62-21-7888-3379
E-mail : info@prasimax.com

BAB 1

Pendahuluan

INTERNET

Di akhir milenium kedua perkembangan internet sungguh revolusioner karena internet telah merasuki segala aspek kehidupan manusia. Dengan internet kita dapat melakukan bisnis lebih efisien, melakukan komunikasi antara manusia dengan manusia, manusia dengan komputer atau komputer dengan komputer.

Internet sendiri adalah sebuah sistem yang memberikan informasi yang terorganisir dan terkelola dengan baik. Jadi internet itu sendiri adalah sebuah sistem yang terstruktur dan terorganisir. Untuk memahami bagaimana hubungan internet dengan TCP / IP, mula-mula kita harus mendefinisikan konsep *protokol* dan *standar*. Tentu saja kita dituntut untuk proaktif mengamati dan mempelajari standar-standar yang dikeluarkan oleh organisasi-organisasi yang berkompeten dalam pengembangan internet menjadi suatu standar bersama. Mengapa? Dapat dibayangkan jika ratusan organisasi baik ilmiah maupun komersil membuat standarnya sendiri-sendiri akan menjadi tidak mungkin bila mengaplikasikan perangkat komunikasi yang berbeda standar satu dengan yang lainnya.

PROTOKOL dan STANDAR

Apa yang dimaksud dengan protokol? Tidak lain adalah sebuah sinonim yang bisa kita sinonimkan sebagai *rule* atau “aturan main”. Dan apa pula yang dimaksud dengan standar? Standar adalah *rule* yang telah disepakati untuk diaplikasikan.

Protokol

Dalam suatu jaringan komputer, terjadi sebuah proses komunikasi antar entiti atau perangkat yang berlainan sistemnya. Entiti atau perangkat ini adalah segala sesuatu yang mampu menerima dan mengirim. Untuk berkomunikasi mengirim dan menerima antara dua entiti dibutuhkan pengertian di antara kedua belah pihak. Pengertian ini lah yang dikatakan sebagai protokol. Jadi protokol adalah himpunan aturan-aturan main yang mengatur komunikasi data. Protokol mendefinisikan apa yang dikomunikasikan bagaimana dan kapan terjadinya komunikasi. Elemen-elemen penting daripada protokol adalah : *syntax*, *semantics* dan *timing*.

- **Syntax** mengacu pada struktur atau format data, yang mana dalam urutan tampilannya memiliki makna tersendiri. Sebagai contoh, sebuah protokol sederhana akan memiliki urutan pada delapan bit pertama adalah alamat pengirim, delapan bit kedua adalah alamat penerima dan *bit stream* sisanya merupakan informasinya sendiri.
- **Semantics** mengacu pada maksud setiap section bit. Dengan kata lain adalah bagaimana bit-bit tersebut terpola untuk dapat diterjemahkan.
- **Timing** mengacu pada 2 karakteristik yakni kapan data harus dikirim dan seberapa cepat data tersebut dikirim. Sebagai contoh, jika pengirim memproduksi data sebesar 100 Megabits per detik (Mbps) namun penerima hanya mampu mengolah data pada kecepatan 1 Mbps, maka transmisi data akan menjadi *overload* pada sisi penerima dan akibatnya banyak data yang akan hilang atau musnah.

Standar

Standar adalah suatu hal yang penting dalam penciptaan dan pemeliharaan sebuah kompetisi pasar daripada manufaktur perangkat komunikasi dan menjadi jaminan *interoperability* data dalam proses komunikasi.

Standar komunikasi data dapat dikategorikan dalam 2 kategori yakni kategori *de facto* (konvensi) dan *de jure* (secara hukum atau regulasi).

ORGANISASI STANDAR

Di bawah ini adalah beberapa organisasi yang concern dengan perkembangan standar teknologi telekomunikasi dan data internasional maupun dari Amerika.

- International Standards Organization (ISO).
- International Telecommunications Union-Telecommunication Standards Section (ITU-T).
- American National Standards Institute (ANSI).
- Institute of Electrical and Electronics Engineers (IEEE).
- Electronic Industries Association (EIA).

Selain itu terdapat pula organisasi yang bersifat forum ilmiah seperti Frame Relay Forum dan ATM Forum.

Kemudian ada pula organisasi yang berfungsi sebagai agen regulasi, misalnya Federal Communications Commision (FCC).

STANDAR INTERNET

Standar internet adalah sebuah proses jalan panjang yang teruji dan terspesifikasi sehingga menjadi berguna bagi siapa yang bekerja dengan internet. Tentu saja spesifikasi ini dimulai dengan sebuah *draft*. Kemudian draft internet ini menjadi dokumen acuan kerja yang memiliki umur 6 bulan. Setelah itu akan mendapatkan rekomendasi dari otoritas Internet dan dipublikasikan sebagai Request for Comment (RFC).

ADMINISTRASI INTERNET

Internet yang pada mulanya merupakan jaringan komputer skala kecil di kalangan akademisi makin bertambah luas bahkan untuk kepentingan militer, komersial dan hiburan. Semakin luasnya aktivitas internet tersebut diperlukan koordinasi dan administrasi untuk mengaturnya. Mulai dari tingkat pengorganisasian nama domain dari root sampai organisasi yang mengatur nama domain untuk root negara. Juga ada organisasi yang mengadministratif standar teknis internet dan mendistribusikan atau mengumpulkan informasi tentang TCP/IP.

Di antaranya adalah :

- Internet Society (ISOC)
- Internet Architecture Board (IAB)
- Internet Engineering Task Force (IETF)

- Internet Research Task Force (IRTF)
- Internet Asigned Number Authority (IANA) dan Internet Corporation for Asigned Names and Numbers (ICANN)

SEJARAH SINGKAT INTERNET

- 1969, empat node ARPANET dioperasikan.
- 1970, host-host ARPA mengimplentasikan NCP.
- 1973, penelitian dan pengembangan TCP/IP dimulai.
- 1977, sebuah pengujian penting menggunakan TCP/IP.
- 1978, UNIX mulai menyebar di kalangan akademis dan riset.
- 1981, CSNET didirikan.
- 1983, TCP/IP menjadi protokol resmi untuk ARPANET.
- 1983, MILNET dilahirkan.
- 1986, NSFNET didirikan.
- 1990, ARPANET digantikan dan dikelola oleh NSFNET.
- 1995, NSFNET kembali menjadi lembaga penelitian jaringan atau network.

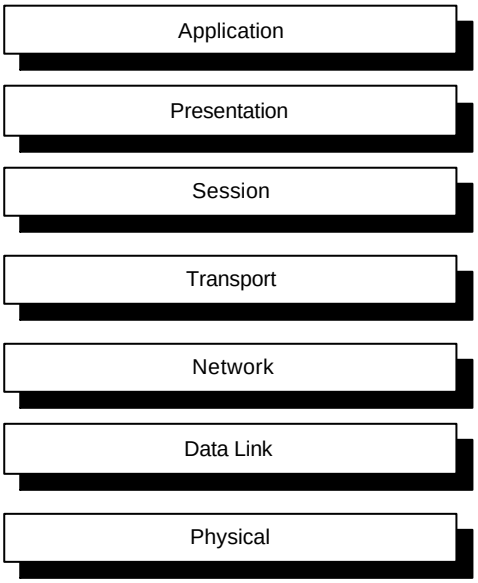
BAB 2

Model OSI dan Protokol TCP/IP

Model lapisan / *layer* yang mendominasi literatur komunikasi data dan jaringan sebelum 1990 adalah Model **Open System Interconnection** (OSI). Setiap orang yakin bahwa model OSI akan menjadi standar terakhir untuk komunikasi data, namun nampaknya hal itu tidak pernah terjadi. Justru protokol TCP / IP yang telah menjadi arsitektur model lapisan dari protokol internet yang sangat dominan bahkan terus menerus diuji, dikembangkan dan diperluas standarnya.

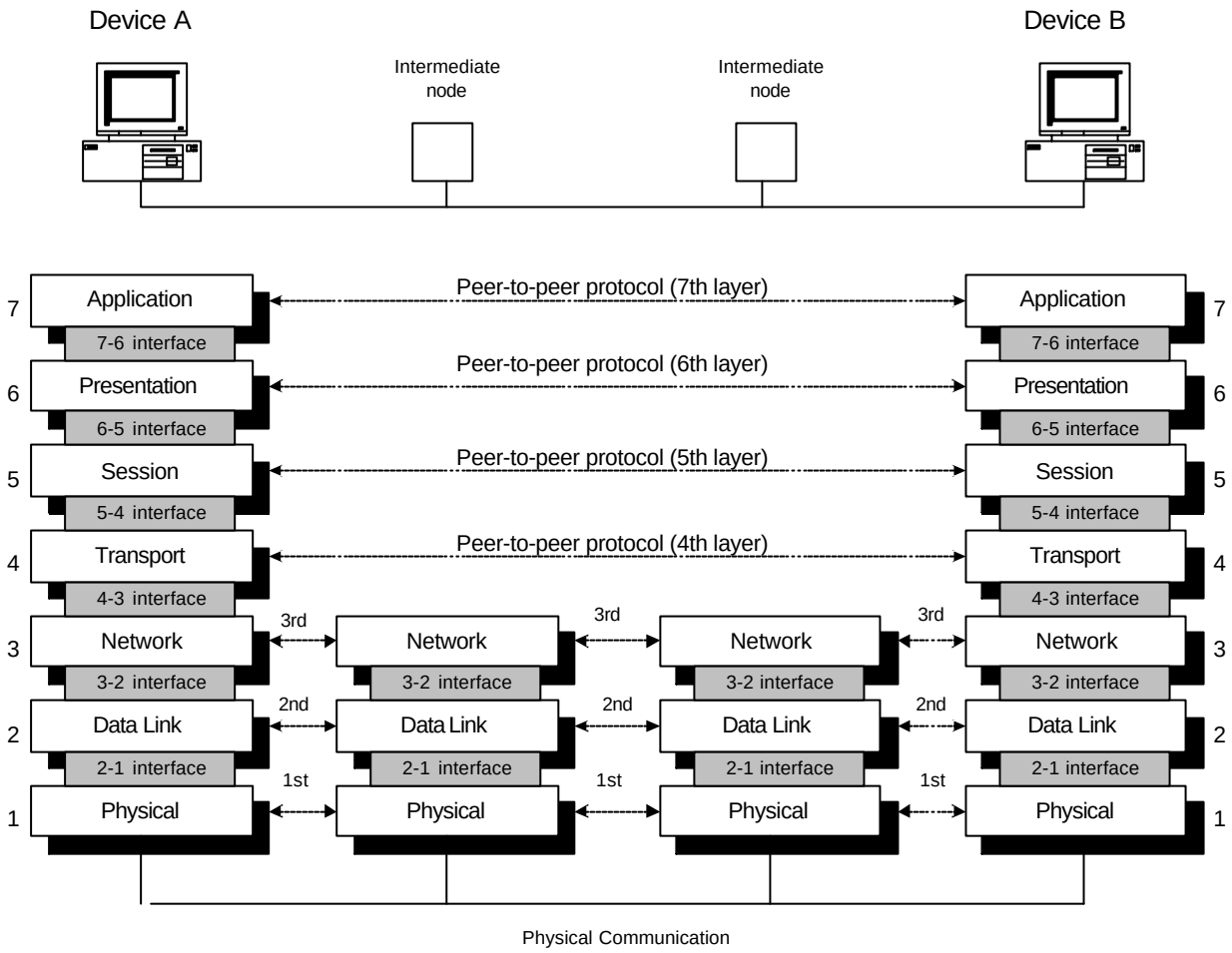
MODEL OSI

Adalah sebuah badan multinasional yang didirikan tahun 1947 yang bernama International Standards Organization (ISO) sebagai badan yang melahirkan standar-standar standar internasional. ISO ini mengeluarkan juga standar jaringan komunikasi yang mencakup segala aspek yaitu model OSI. OSI adalah *open system* yang merupakan himpunan protokol yang memungkinkan terhubungnya 2 sistem yang berbeda yang berasal dari *underlying architecture* yang berbeda pula. Jadi tujuan OSI ini adalah untuk memfasilitasi bagaimana suatu komunikasi dapat terjalin dari sistem yang bebeda tanpa memerlukan perubahan yang signifikan pada *hardware* dan *software* di tingkat underlying. Pada Gambar 2.1 diperlihatkan lapisan model OSI.



Gambar 2.1 Model OSI

Model OSI disusun atas 7 lapisan; fisik (lapisan 1), data link (lapisan 2), network (lapisan 3), transport (lapisan 4), session (lapisan 5), presentasi (lapisan 6) dan aplikasi (lapisan 7). Pada Gambar 2.2, Anda dapat juga melihat bagaimana setiap lapisan terlibat pada proses pengiriman pesan / *message* dari *Device* A ke *Device* B. Terlihat bahwa perjalanan message dari A ke B melewati banyak intermediasi *node*. Intermediasi *node* ini biasanya hanya melibatkan tiga lapisan pertama model OSI saja.



Gambar 2.2 Lapisan-lapisan OSI

Jadi dengan demikian para disainer hardware dan jaringan dapat lebih paham dan flexibel dalam membuat suatu sistem sehingga fungsi setiap mesin dapat ber-interoperasi (*interoperbility*) satu sama lain.

Setiap mesin / komputer hanya dapat memanfaatkan *service* lapisan yang terdapat tepat di lapisan bawahnya. Contoh: Lapisan 3 menggunakan service yang disediakan oleh lapisan 2 dan menyediakan *service* untuk lapisan 4.

Proses peer-to-peer

Bila dua mesin / komputer berinteraksi melakukan proses harus mematuhi aturan dan konvensi yang disebut protokol. Proses yang terjadi pada setiap mesin pada lapisan tertentu disebut **peer-to-peer processes** (proses peer-to-peer). Jadi dengan demikian jika 2 mesin akan dapat berkomunikasi jika pada lapisan tertentu menggunakan protokol yang sama. Dilihat pada Gambar 2.2, *message* atau pesan yang dikirim oleh device A menuju device B harus melalui lapisan-lapisan yang paling atas menuju lapisan bawah berikutnya sampai lapisan terbawah kemudian kembali menuju lapisan yang lebih tinggi dan seterusnya melewati lapisan tepat diatasnya. Pesan-pesan yang dikirim adalah berupa informasi yang dibentuk dalam paket-paket di mana pada layer tepat di bawahnya informasi tersebut “dibungkus”. Jadi pada sisi

penerima informasi yang sampai berupa paket-paket yang telah “dibuka” bungkusannya dan dikonstruksi kembali.

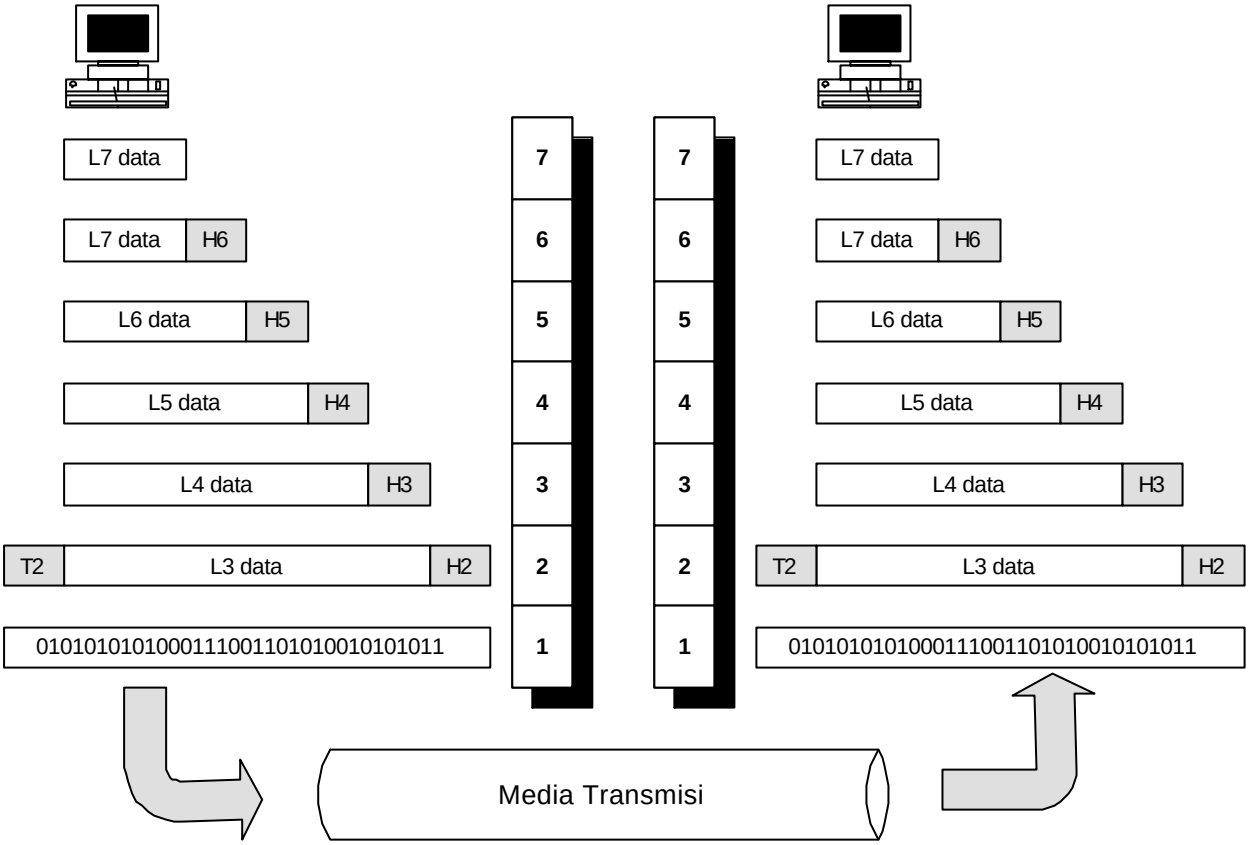
Antarmuka antara lapisan terdekat

Pada saat pengiriman dan penerimaan pesan, lapisan memerlukan antarmuka dengan lapisan atas dan bawahnya yang berdekatan. Sepanjang sebuah lapisan menyediakan layanan yang dimaksud pada layer tepat di atas atau di bawahnya, dapat diimplementasikan fungsi yang termodifikasi atau diganti tanpa memerlukan perubahan di seluruh lapisan.

Pengorganisasian lapisan

Tujuh lapisan yang telah dijelaskan dapat dibagi menjadi 3 sub-kelompok (*subgroups*). Lapisan 1, 2 dan 3 adalah ***network support layer*** (lapisan-lapisan pendukung jaringan). Lapisan 5, 6 dan 7 merupakan ***user support layer*** (lapisan-lapisan pendukung pengguna). Lapisan 4 adalah **transport layer**, yang maksudnya adalah lapisan yang menghubungkan 2 subgroup sehingga lapisan ***user support layer*** dapat “mengerti” pesan yang dikirim ***network support layer***.

Gambar 2.3 memperlihatkan seluruh lapisan OSI dengan dimulai pada lapisan 7 yang merupakan **data asli**.



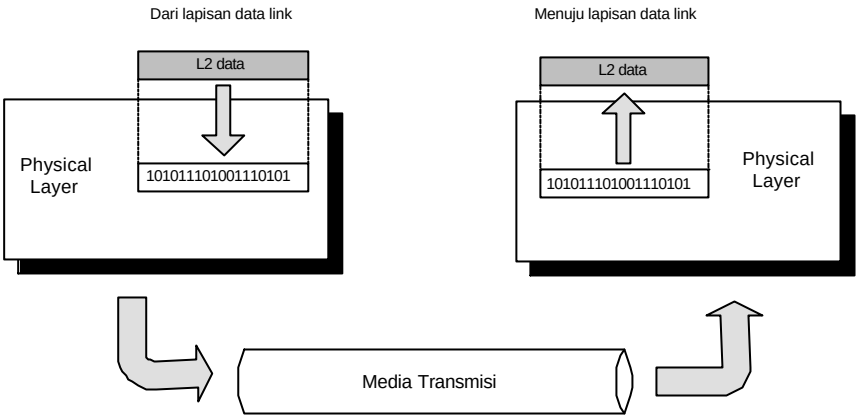
Gambar 2.3 Pertukaran data menggunakan model OSI

LAYER/LAPISAN MENURUT OSI

Physical Layer (Lapisan Fisik)

Lapisan fisik melakukan fungsi pengiriman dan penerimaan *bit stream* dalam medium fisik. Dalam lapisan ini kita akan mengetahui spesifikasi mekanikal dan elektrikal daripada media transmisi serta antarmukanya. Hal-hal penting yang dapat dibahas lebih jauh dalam lapisan fisik ini adalah :

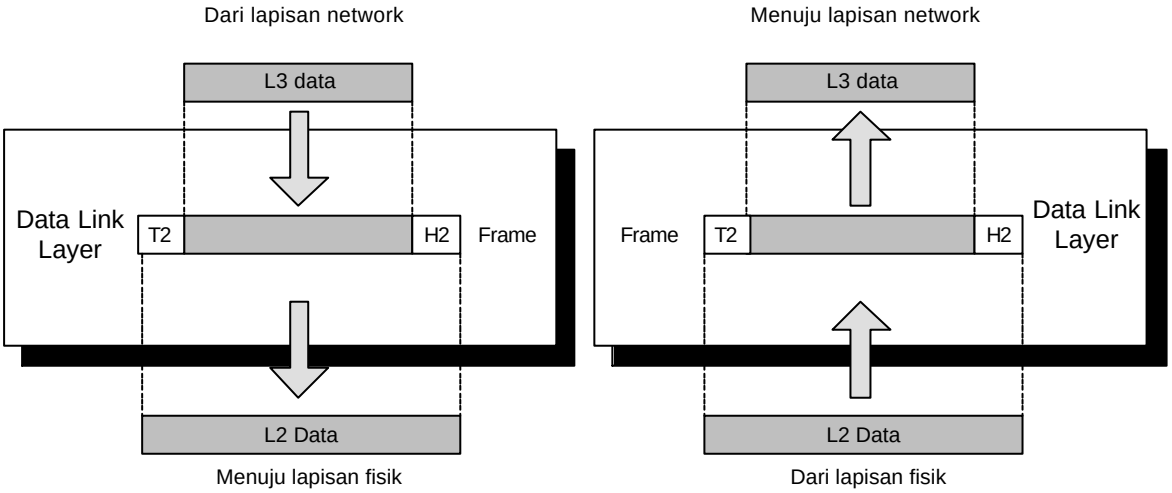
- Karakteristik fisik daripada media dan antarmuka.
- Representasi bit-bit. Maksudnya lapisan fisik harus mampu menterjemahkan bit 0 atau 1, juga termasuk pengkodean dan bagaimana mengganti sinyal 0 ke 1 atau sebaliknya.
- *Data rate* (laju data).
- Sinkronisasi bit.
- Line configuration (Konfigurasi saluran). Misalnya: *point-to-point* atau *point-to-multipoint configuration.*
- Topologi fisik. Misalnya: *mesh topology*, *star topology*, *ring topology* atau *bus topology*.
- Moda transmisi. Misalnya : half-duplex mode, *full-duplex* (*simplex*) *mode*.



Gambar 2.4 Lapisan fisik/physical layer

Data Link Layer (Lapisan Data Link)

Lapisan data link berfungsi mentransformasi lapisan fisik yang merupakan fasilitas transmisi data mentah menjadi link yang reliabel. Dalam lapisan ini menjamin informasi bebas *error* untuk ke lapisan di atasnya.



Gambar 2.5 Lapisan Data Link/Data link layer

Tanggung jawab utama lapisan data link ini adalah sebagai berikut :

- *Framing*. Yaitu membagi bit stream yang diterima dari lapisan network menjadi unit-unit data yang disebut *frame*.
- *Physical addressing*. Jika frame-frame didistribusikan ke sistem lainpada jaringan, maka data link akan menambahkan sebuah *header* di muka *frame* untuk mendefinisikan pengirim dan/atau penerima.
- *Flow control*. Jika *rate* atau laju *bit stream* berlebih atau berkurang maka flow control akan melakukan tindakan yang menstabilkan laju bit.
- *Error control*. Data link menambah reliabilitas lapisan fisik dengan penambahan mekanisme deteksi dan retransmisi frame-frame yang gagal terkirim.

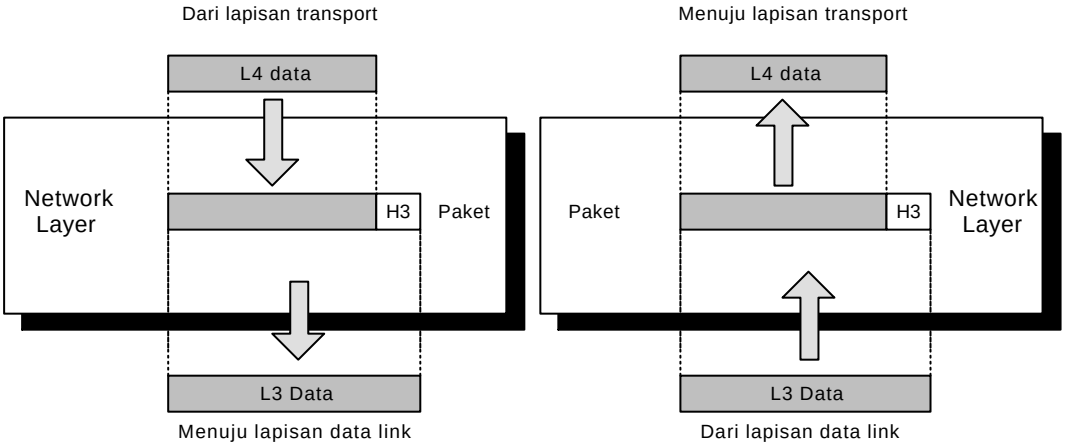
✍✍*Access control*. Jika 2 atau lebih device dikoneksi dalam link yang sama, lapisan data link perlu menentukan device yang mana yang harus dikendalikan pada saat tertentu.

Network Layer (Lapisan Network)

Lapisan network bertanggung jawab untuk pengiriman paket dengan konsep *source-to-destination*. Adapun tanggung jawab spesifik lapisan network ini adalah:

✍✍*Logical addressing*. Bila pada lapisan data link diimplementasikan *physical addressing* untuk penangan pengalamatan / *addressing* secara lokal, maka pada lapisan network problematika addressing untuk lapisan network bisa mencakup lokal dan antar jaringan / network. Pada lapisan network ini *logical address* ditambahkan pada paket yang datang dari lapisan data link.

✍✍*Routing*. Jaringan-jaringan yang saling terhubung sehingga membentuk internetwork diperlukan metoda *routing* / perutean. Sehingga paket dapat ditransfer dari satu device yang berasal dari jaringan tertentu menuju device lain pada jaringan yang lain.



Gambar 2.6 Lapisan nertwork / network layer

Transport Layer (Lapisan Transpor)

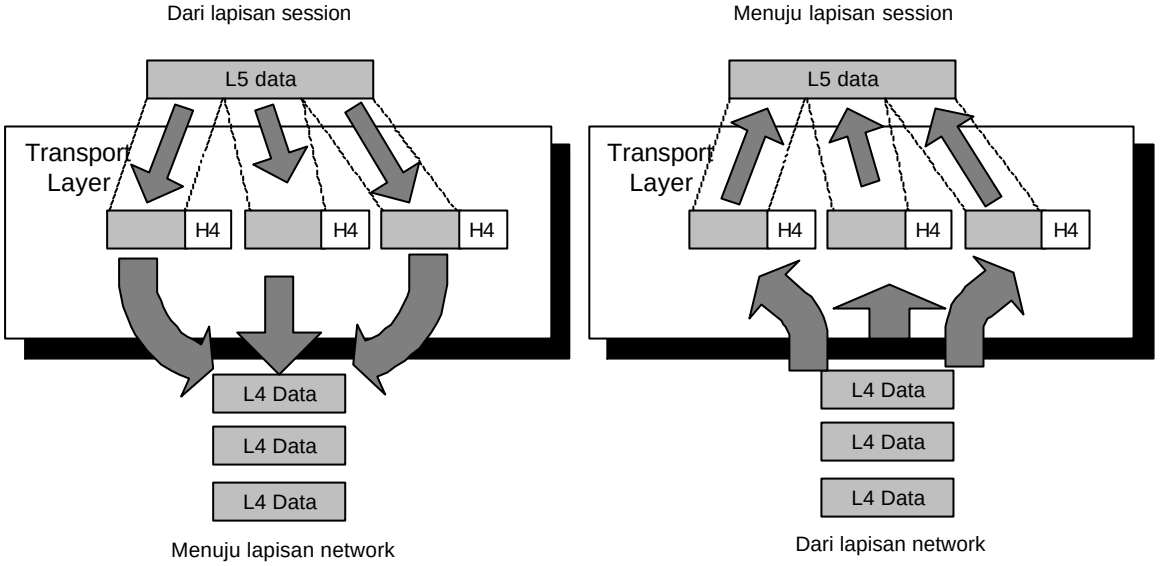
Lapisan transpor bertanggung jawab untuk pengiriman *source-to-destination* (*end-to-end*) daripada jenis *message* tertentu. Tanggung jawab spesifik lapisan transpor ini adalah:

✍✍*Sevice-point addressing*. Komputer sering menjalankan berbagai macam program atau aplikasi yang berlainan dalam saat bersamaan. Untuk itu dengan lapisan transpor ini tidak hanya menangani pengiriman / delivery *source-to-destination* dari computer yang satu ke komputer yang lain saja namun lebih spesifik kepada delivery jenis *message* untuk aplikasi yang berlainan. Sehingga setiap message yang berlainan aplikasi harus memiliki alamat / *address* tersendiri lagi yang disebut *service point address* atau *port address*.

✍✍*Segmentation* dan *reassembly*. Sebuah message dibagi dalam segmen-segmen yang terkirim. Setiap segmen memiliki *sequence number*. *Sequence number* ini yang berguna bagi lapisan transpor untuk merakit / reassembly segmen-segman yang terpecah atau terbagi tadi menjadi message yang utuh.

✍✍*Connection control*. Lapisan transpor dapat berperilaku sebagai *connectionless* atau *connection-oriented*.

- *Flow control.* Seperti halnya lapisan data link, lapisan transpor bertanggung jawab untuk kontrol aliran (flow control). Bedanya dengan flow control di lapisan data link adalah dilakukan untuk end-to-end.
- *Error control.* Sama fungsi tugasnya dengan error control di lapisan data link, juga berorientasi end-to-end.



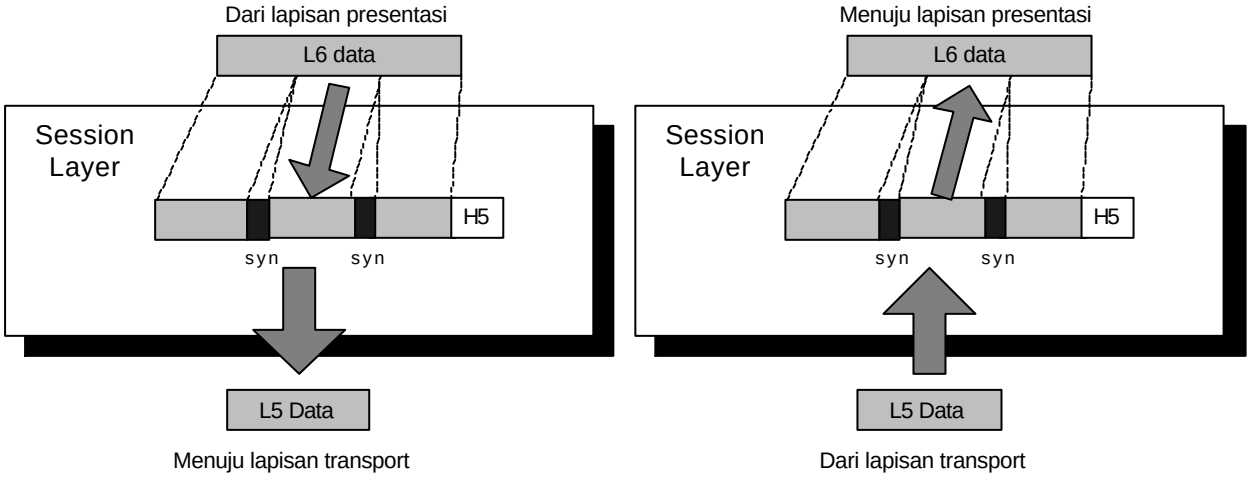
Gambar 2.7 Lapisan Transport/Transport Layer

Session Layer (Lapisan Session)

Layanan yang diberikan oleh tiga layer pertama (fisik, data link dan network) tidak cukup untuk beberapa proses. Maka pada lapisan session ini dibutuhkan *dialog controller*.

Tanggung jawab spesifik:

- Dialog control.
- Sinkronisasi

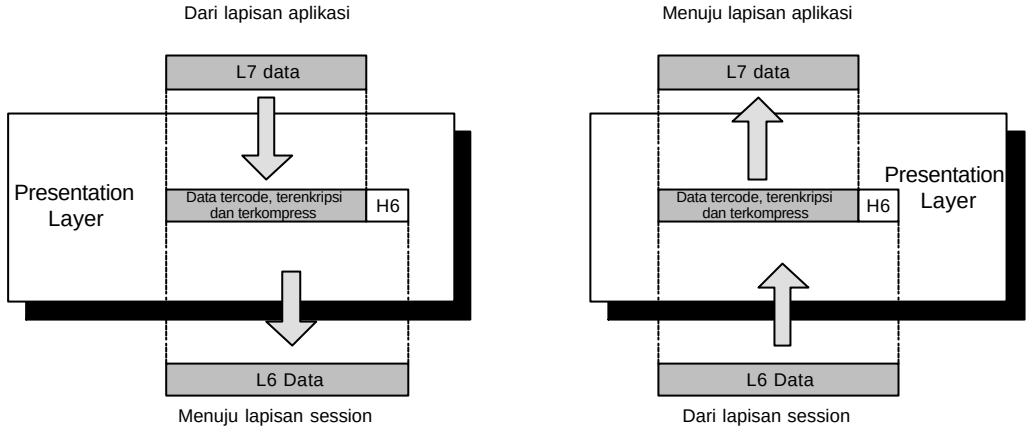


Gambar 2.8 Lapisan Session/Session Layer

Presentation Layer (Lapisan presentasi)

Presentation layer lebih cenderung pada *syntax* dan *semantic* pada pertukaran informasi dua sistem. Tanggung jawab spesifik :

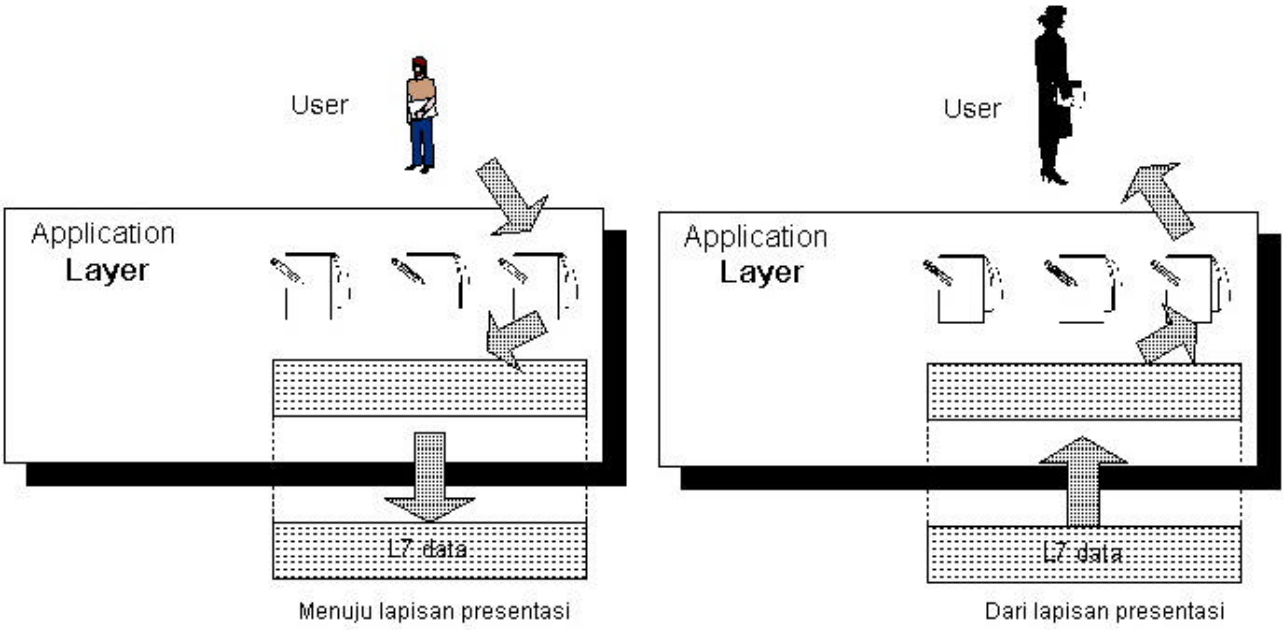
- Translasi
- Enkripsi
- Kompresi



Gambar 2.9 Lapisan Presentasi/Presentation Layer

Application Layer (Lapisan Aplikasi)

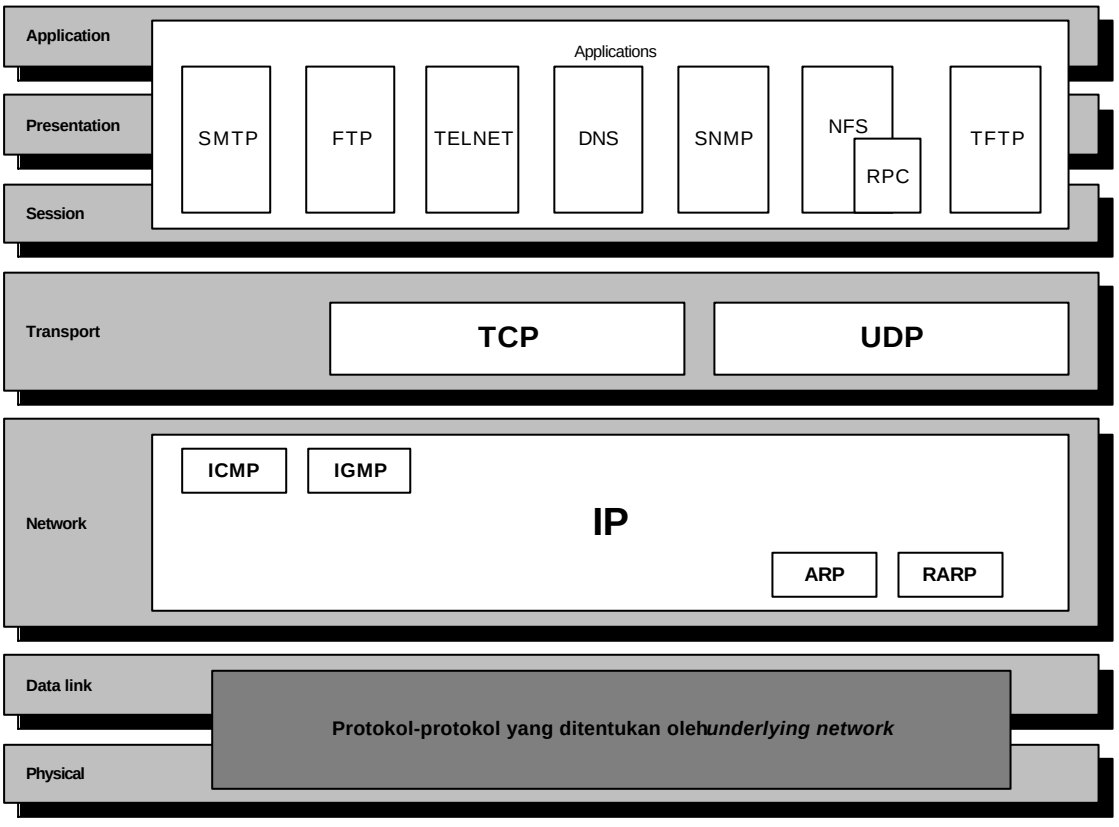
Sesuai namanya, lapisan ini emnjembatani interaksi manusia dengan perangkat lunak / *software* aplikasi.



Gambar 2.10 Lapisan Aplikasi/Application Layer

TCP/IP PROTOCOL SUITE

TCP/IP dikembangkan sebelum model OSI ada. Namun demikian lapisan-lapisan pada TCP/IP tidaklah cocok seluruhnya dengan lapisan-lapisan OSI. Protokol TCP/IP hanyadibuat atas lima lapisan saja: physical, data link, network, transport dan application. Cuma hanya lapisan aplikasi pada TCP/IP mencakupi tiga lapisan OSI teratas, sebagaimana dapat dilihat pada Gambar 2.11. Khusus layer keempat, Protokol TCP/IP mendefinisikan 2 buah protokol yakni Transmission Control Protocol (TCP) dan User Datagram Protocol Protocol (UDP). Sementara itu pada lapisan ketiga, TCP/IP mendefiniskan sebagai Internetworking Protocol (IP), namun ada beberapa protokol lain yang mendukung pergerakan data pada lapisan ini.



Gambar 2.11 Susunan Protokol TCP/IP dan model OSI

Physical dan Data Link Layer

Pada lapisan ini TCP/IP tidak mendefinisikan protokol yang spesifik. Artinya TCP/IP mendukung semua standar dan proprietary protokol lain.

Network Layer

Pada lapisan ini TCP/IP mendukung IP dan didukung oleh protokol lain yaitu RARP, ICMP, ARP dan IGMP.

Internetworking Protocol (IP)

Adalah mekanisme transmisi yang digunakan oleh TCP/IP. IP disebut juga *unreliable* dan *connectionless datagram protocol-a besteffort delivery service*. IP mentransportasikan data dalam paket-paket yang disebut *datagram*.

Address Resolution Protocol (ARP)

ARP digunakan untuk menyesuaikan alamat IP dengan alamatfisik (*Physical address*).

Reverse Address Resolution Protocol (RARP)

RARP membolehkan host menemukan alamat IP nya jika dia sudah tahu alamat fiskinya. Ini berlaku pada saat host baru terkoneksi ke jaringan.

Internet Control Message Protocol (ICMP)

ICMP adalah suatu mekanisme yang digunakan oleh sejumlah host dan gateway untuk mengirim notifikasi datagram yang mengalami masalah kepada host pengirim.

Internet Group Message Protocol (IGMP)

IGMP digunakan untuk memfasilitasi transmisi message yang simultan kepasa kelompok/group penerima.

Transport Layer

User Datagram Protocol (UDP)

UDP adalah protokol process-to-process yang menambahakan hanya alamat port, c*heck-sum error control,* dan panjang informasi data dari lapisan di atasnya.

Transmission Control Protocol (TCP)

TCP menyediakan layanan penuh lapisan transpor untuk aplikasi. TCP juga dikatakan protokol transpor untuk *stream* yang reliabel. Dalam konteks ini artinya TCP bermakna connection-oriented, dengan kata lain: koneksi end-to-end harus dibangun dulu di kedua ujung terminal sebelum kedua ujung terminal mengirimkan data.

Application Layer

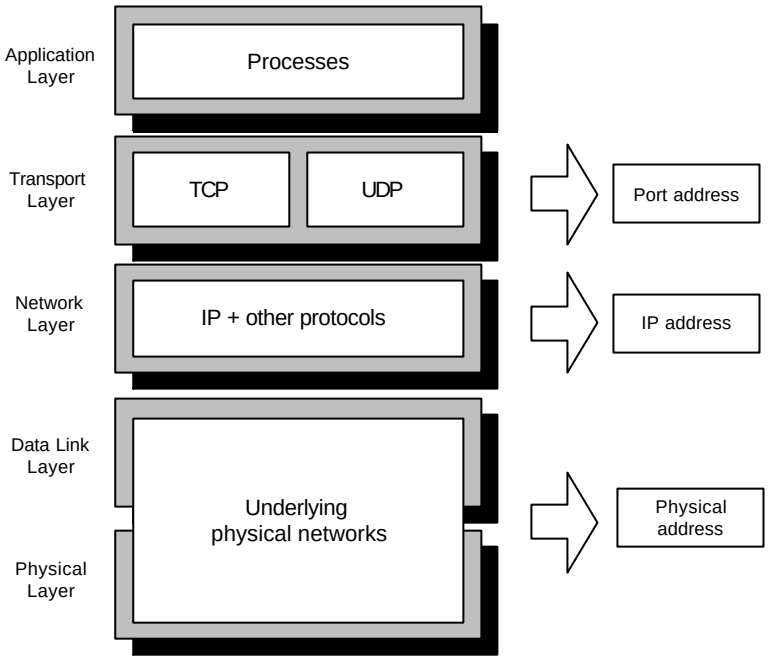
Application Layer dalam TCP/IP adalah kombinasi lapisan-lapisan *session, presentation* dan *application* pada OSI.

ADDRESSING (PENGALAMATAN)

Dalam TCP/IP dikenal 3 alamat yakni: *physical address*, *IP address* dan *port address*. Physical address kerap disebut sebagai link address. Ukuran address/alamat fisik ini tergantung jenis hardwarenya. Alamat fisik dapat berupa unicast, multicast atau broadcast.

Internet address perlu untuk layanan komunikasi yang aspeknya universal. Saat ini besarnya *Internet address* adalah 32 bit.

Port address sangat diperlukan untuk komunikasi yang berorientasi terhadap proses aplikasi.



Gambar 2.12 Pengalamatan pada Protokol TCP/IP

VERSI-VERSI TCP/IP

TCP/IP menjadi protokol secara resmi untuk aplikasi internet adalah tahun 1983. Sejak itu hingga sekarang telah digunakan secara luas hingga versi 4 atau disebut IPv4 seperti yang kita gunakan saat ini. Pernah versi 5 diajukan sebagai proyek namun akhirnya gagal karena berbagai sebab. Namun pada saat ini pula sudah mulai disosialisasikan IP vesrsi *next generation*, banyak kalangan menyebutnya IPv6. Di mana pada IPv4 alamat IP menggunakan 32 bit (4 byte) tapi IPv6 menggunakan 128 bit (16 byte). Pada IPv6 konon sudah dilengkapi dengan dukungan *authentication*, data *integrity* dan *confidentiality*. Dalam materi kursus Protokol TCP/IP kita akan hanya membahas IPv4 saja.

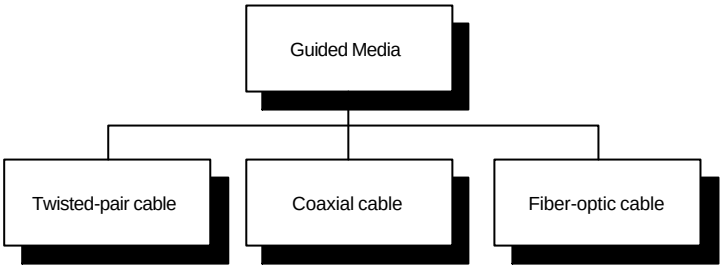
BAB 3

Teknologi Underlying

Protokol TCP/IP didisain untuk mendukung bermacam-macam teknologi jaringan.

MEDIA TRANSMISI

Secara garis besar ada dua kategori media transmisi, yakni : *guided* (terpandu) dan *unguided* (tidak terpandu).



Gambar 3.1 Media terpandu

Media yang terpandu (Guided)

Media transmisi yang terpandu maksudnya adalah media yang mampu mentransmisikan besaran-besaran fisik lewat materialnya. Contoh: kabel *twisted-pair*, kabel *coaxial* dan serat optik.

Kabel Twisted-pair

Kabel twisted-pair memiliki beberapa jenis utama yaitu *shielded* (berselimut) biasa disebut STP dan *unshielded* (tidak memiliki selimut) biasa disebut UTP. Untuk UTP terdapat pula pembagian jenis yakni:

- Category 1 : sifatnya mampu mentransmisikan data kecepatan rendah. Contoh: kabel telepon.
- Category 2 : sifatnya mampu mentransmisikan data lebih cepat dibanding category 1. Dapat digunakan untuk transmisi digital dengan bandwidth hingga 4 MHz.
- Category 3 : mampu mentransmisikan data hingga 16 MHz.
- Category 4 : mampu mentransmisikan data hingga 20 MHz.
- Category 5 : digunakan untuk transmisi data yang memerlukan bandwidth hingga 100 MHz.

Kabel Coaxial

Kabel coaxial mampu mengangkut sinyal frekuensi yang lebih tinggi daripada kabel twisted-pair.

Serat Optik

Serat optik terbuat dari material gelas atau plastik dan mampu mentransmisikan sinyal dalam bentuk cahaya.

Media yang tidak terpandu (Unguided)

Media *unguided* mentransmisikan gelombang electromagnetic tanpa menggunakan konduktor fisik seperti kabel atau serat optik. Contoh sederhana adalah gelombang radio seperti microwave, wireless mobile dlsb.

LOCAL ARE NETWORK (LAN)

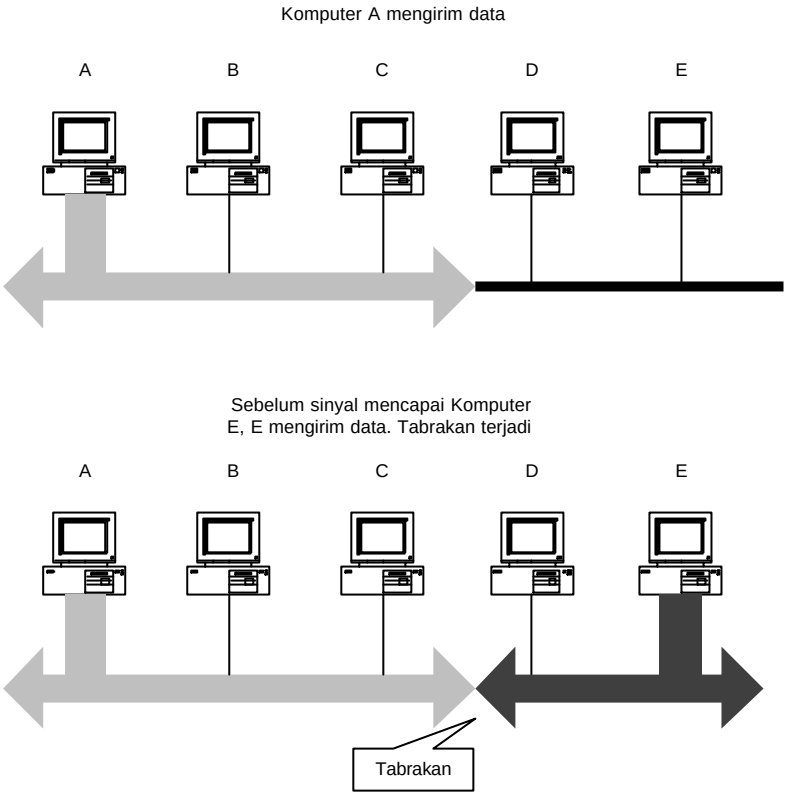
LAN adalah sebuah sistem komunikasi data yang membolehkan sejumlah device atau komputer yang terangkai untuk berkomunikasi langsung satu sama lainnya. Di dalam LAN dikenal ada 3 macam arsitektur: Ethernet, token ring dan *fiber distributed data interface* (FDDI).

Ethernet

Ethernet adalah standar LAN yang pertama kali dikembangkan oleh XEROX dan kemudian diperluas pengembangannya oleh Digital Equipment Corp, Intel Corp dan Xerox juga.

Metoda akses : CSMA/CD

Metoda akses yang digunakan dalam LAN disebut carrier sense *multiple access with collision detection* (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 2 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.



Gambar 3.2 CSMA/CD

Addressing (pengalamatan)

Setiap komputer, device atau stasion dalam LAN memiliki NIC (*Network Interface Card*). NIC ini memiliki 6-byte alamat fisik (*physical address*).

Data rate (laju data)

Ethernet LAN dapat mendukung laju data antara 1 sampai 10 MBps, sedangkan Fast Ethernet mendukung hingga 100 MBps.

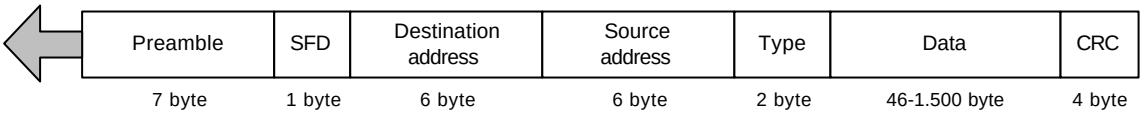
Frame Format (format bingkai)

Pada Gambar 3.3 dapat dilihat sebuah *Ethernet frame*. 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:

- **Preamble** : memuat 7 byte (56 bit) rangkaian bolak-balik bit 0 dan 1. Kegunaannya untuk sinkronisasi pada komputer penerima.
- **Start frame delimiter** : berisi 1 byte dengan nilai (10101011). Digunakan sebagai *flag* dan sinyal mulainya *frame*.
- **Destination address** : Berisi 6 byte yang memuat *physical address* untuk komputer yang dituju.

- **Source address** : Berisi 6 byte yang memuat *physical address* untuk komputer pengirim.
- **Type** : berisi informasi yang menentukan jenis data yang dibungkus (*encapsulated*) pada *frame*.
- **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.
- **Cyclic redudancy check** : berisi 4 byte sebagai error detection. Jenis CRC yang digunakan adalah CRC-32.

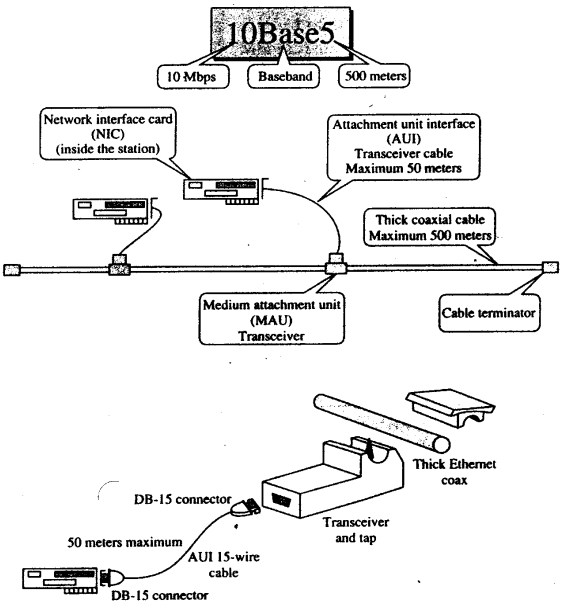


Gambar 3.3 Ethernet Frame

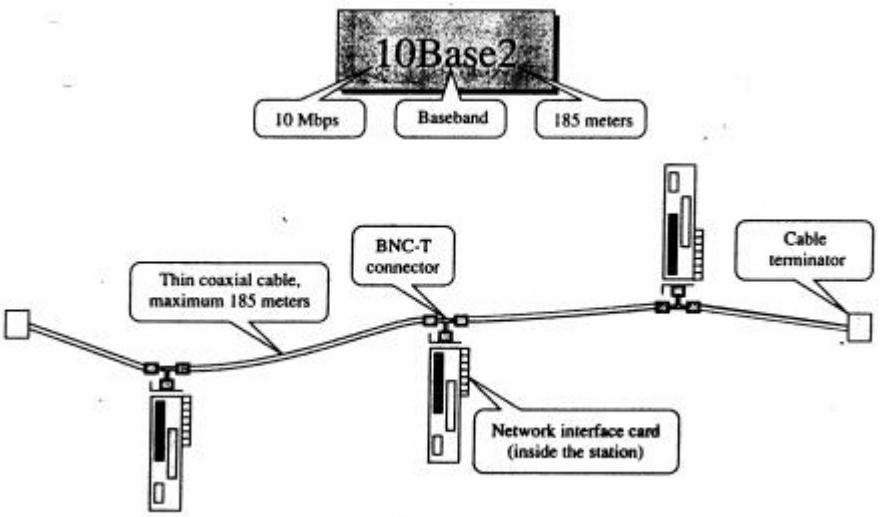
Implementasi LAN

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

- 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 3.4.
- 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 kabelnyasehingga lebih luwes dibanding *thick-net*. Kelemahannya dibanding *thick-net* adalah jarak kabel yang tidak melebihi 185 meter dan hanya mampu mengakomodasi sedikit komputer. Gambar 3.5 memperlihatkan contoh thin-net.

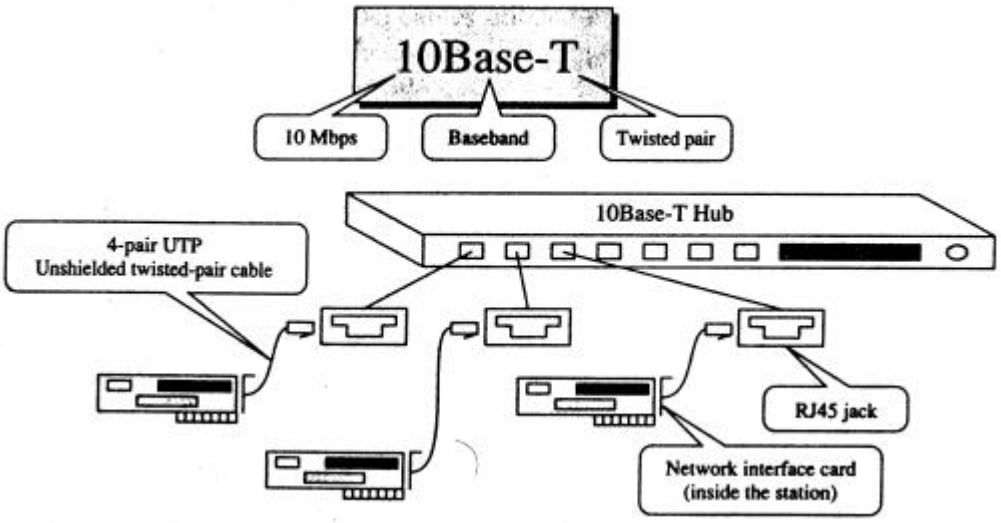


Gambar 3.4 Thick Ethernet



Gambar 3.5 Thin Ethernet

- 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 3.6 (Figure 3.13).



Gambar 3.6 Twisted-pair Ethernet

Fast 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.

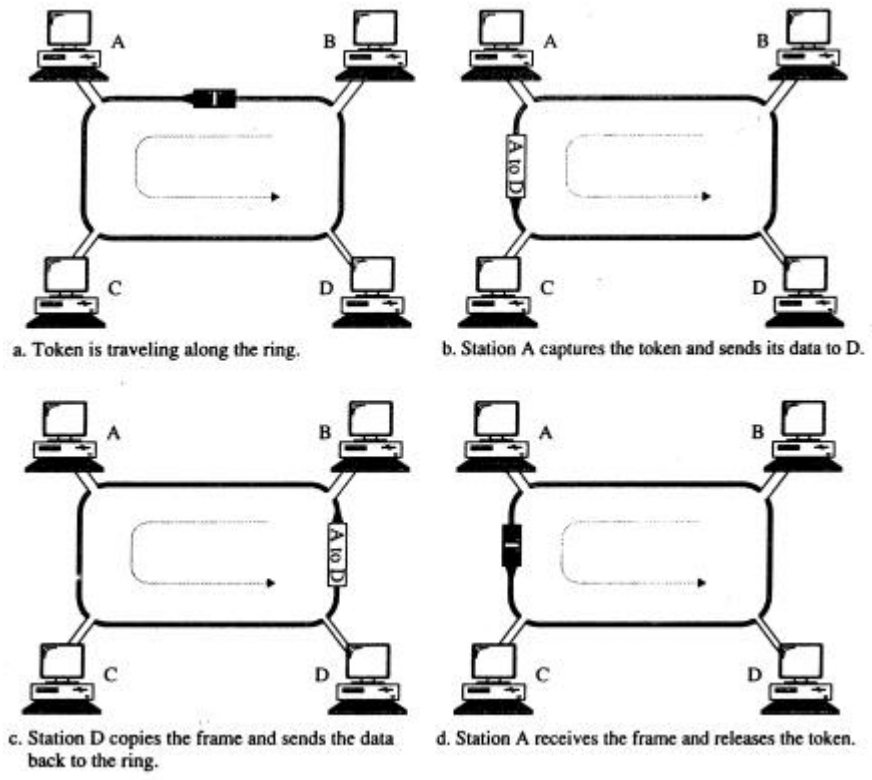
Versi-versi terbaru Fast Ethernet ini pun sudah banyak macam ragamnya. Misal: 100BASE-T4 (menggunakan UTP 4 pair seperti 10BASET), 100BASE-XT (menggunakan STP atau UTP 2 pair) dan 100BASE-XF (menggunakan dua kabel serat optik pada masing2 jalur pengirim dan penerima).

Token Ring

Token Ring adalah permulaan standar LAN yang pernah dikembangkan oleh IBM.

Metoda akses: token passing

Pada Gambar 3.7 dapat dilihat bahwa dalam *token passing*, token dilewatkan dari station / komputer satu ke station / komputer lain dalam urutan hingga token meng-*encounter* sebuah data yang dilewatkan token itu. Station lain menunggu hingga token terkirim. Topologi ini mutlak harus berbentuk ring. Untuk menghindari maslaah terhadap token yang tidak berguna atau token yang hilang maka diletakkan sebuah komputer / station yang bertugas sebagai pengontrol atau monitor.



Gambar 3.7 Metode akses Token-passing

Addressing (pengalamatan)

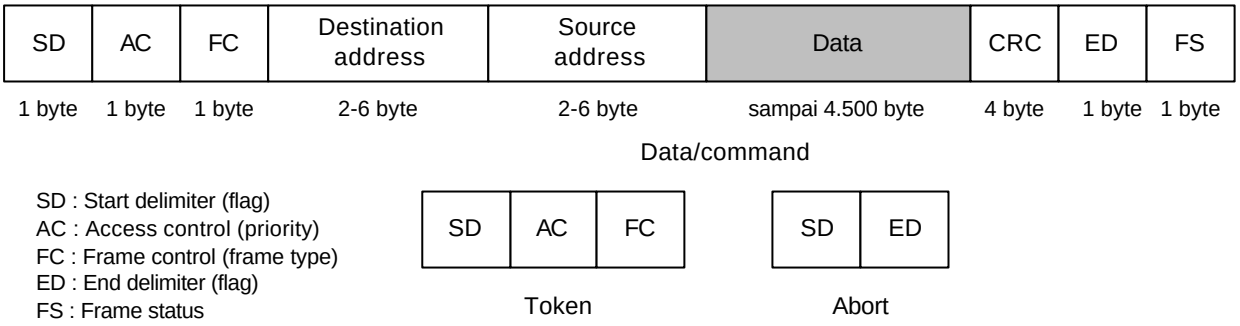
Token ring menggunakan sistem pengalamatan / addressing 6 byte.

Data rate (laju data)

Token ring mampu mendukung dua laju data : 4 dan 16 MBps.

Farme Format

Protokol token ring memiliki 3 jenis frame : data, token, dan abort, lihat Gambar 3.8.



Gambar 3.8 Frame Token ring

Di mana :

Data frame adalah bingkai / *frame* yang hanya untuk mengangkut data. Isi field dalam Data

Farem ini adalah sbb :

- Start delimiter (SD). Berisi 1 byte yang digunakan untuk memberitahu komputer penerima ketika frame sampai.
- Access control (AC). Berisi 1 byte yang memuat informasi tentang prioritas dan reservasi.
- Frame control (FC). Field ini berisi 1 byte yang memuat jenis informasi yang dimuat dalam *data field*.
- Destination address (DA). Field ini panjangnya variabel antara 2 sampai 6 byte. Memuat physical address komputer / station berikutnya.
- Source address (SA). Field ini panjangnya variabel antara 2 sampai 6 byte. Memuat physical address komputer / station sebelumnya.
- Data. *Field* ini memuat data. Data dapan memuat hingga 4500 byte.
- CRC. Field ini berisi 4 byte CRC-32
- End delimiter (ED). Berisi 1 byte yang mengindikasikanahir dari *frame*.
- Frame status (FS). *Field* ini di-set oleh penerima untuk mengindikasikan bahwa frame sudah dibaca. Atau station monitor mengindikasikan bahwa frame ini sudah mengelilingi ring.

Token Frame hanya berisi 3 field yaitu: SD, AC dan ED.

Abort Frame hanya ada 2 field: SD dan ED. Digunakan oleh monitor untuk mengabaikan mekanisme token ketika ada masalah.

Implementasi Token Ring

Terdiri dari penggunaan kabel 150-ohm. Setiap station dihubungkan ke output port pada sebuah station sebelah dan input port pada station yang di sebelahnya yang lain lagi. Aliran token ring ini adalah unidirectional, atau satu arah.. Jadi akan menjadi problem besar jika kabel2 yg menghubungkan 2 sation putus atau rusak.

Fiber Distributed Data Interface (FDDI)

FDDI adalah protokol LAN yang distandarisasikan oleh ITU-T. FDDI mendukung laju data 100 MBps, sehingga menjadi laternatif pengganti ethernet dan token ring. FDDI dalam implementasinya harus menggunakan kabel serat optik, sehingga dari segi biaya adalah sangat mahal.

Metoda akses : Token passing

FDDI dalam metoda akses sama dengan *Token Ring* yakni *token passing*.

Addressing (pengalamatan)

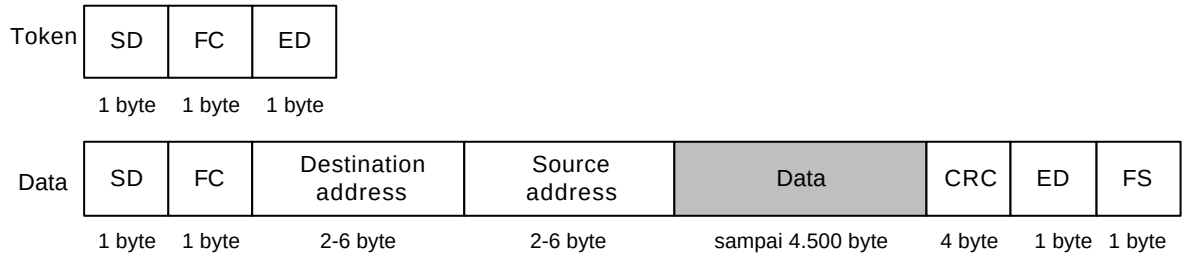
FDDI menggunakan 2 hingga 6 byte alamat fisik.

Data Rate (laju data)

FDDI mendukung laju data pada 100 MBps.

Frame Format (format bingkai)

FDDI hanya menggunakan 2 jenis frame: data dan token, lihat Gambar 3.9.

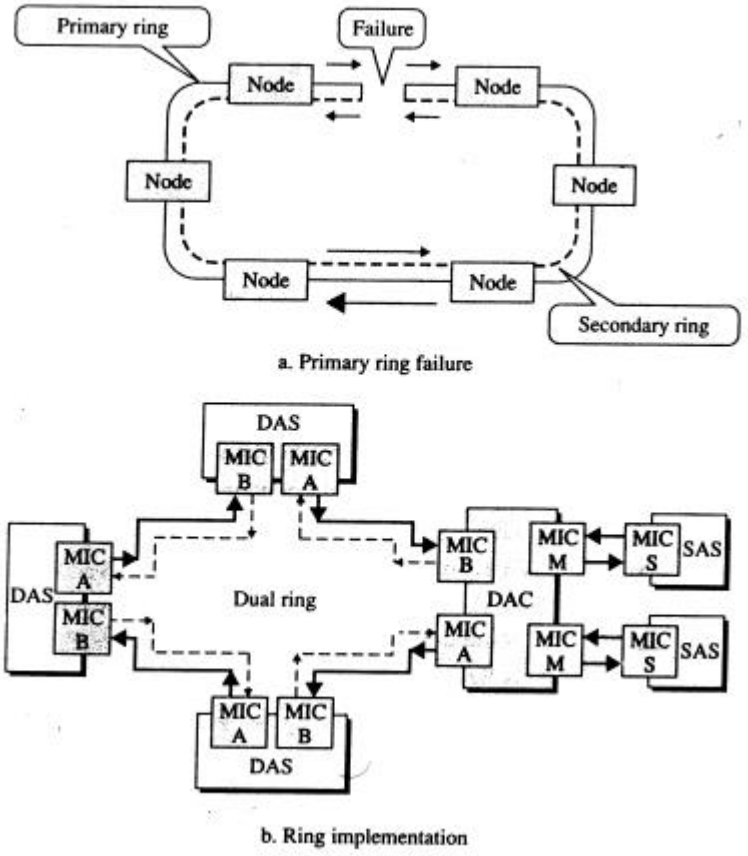


Gambar 3.9 Frame FDDI

Implementasi FDDI

FDDI diimplementasikan menggunakan ring ganda (dual ring). Dalam banyak kasus data ditransmisikan pada ring pertama (*primary ring*). Jika ring pertama mengalami masalah, maka ring kedua (*secondary ring*) melakukan recovery.

Setiap station atau node atau komputer dikoneksi dengan device yang bernama media transfer connector (MIC). Setiap MIC memiliki 2 *fiber port*. FDDI memiliki 3 tipe node: dual attachment station (DAS), single attachment station (SAS), dan dual attachment concentrator (DAC). Untuk DAS memiliki 2 MIC (MIC A dan MIC B) lihat gambar 3.10.



Gambar 3.10 Implementasi FDDI

WIDE ARE NETWORK (WAN)

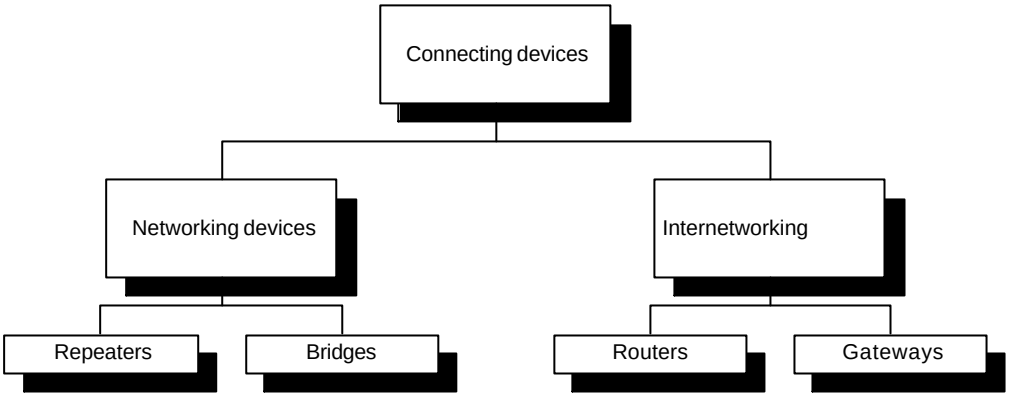
Pada WAN menyediakan layanan transmisi data berjarak jauh secara geografis antar kota, pulau dan benua.

Jadi perbedaan dengan LAN adalah bergantung pada perangkat keras yang dimilikinya. Jadi WAN dapat menggunakan fasilitas publik seperti sirkuit sewa (*leased line*), frame relay, VSAT dlsb.

Untuk mengetahui teknologi pendukung WAN ini lebih dalam perlu mengetahui konsep **Point-to-Point Protocol (PPP)**, **X.25**, **Frame Relay** dan **ATM**.

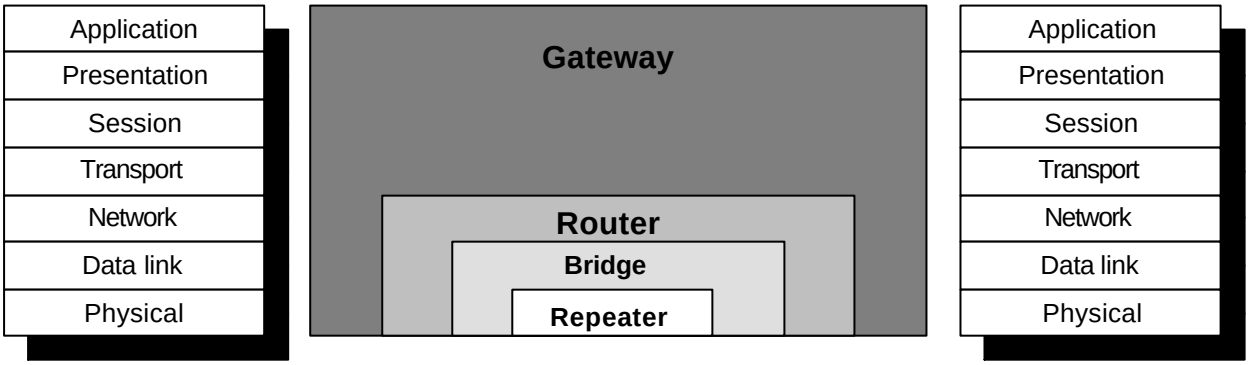
CONNECTING DEVICE

Connecting device digunakan untuk menghubungkan segmen-segmen atau perangkat dalam jaringan untuk menhasilakan apa yang disebut internetwork / internet. Dapat diklasifikasikan dalam Gambar 3.11 mengenai klasifikasi connecting device ini.



Gambar 3.11 Connecting devices

Terlihat bahwa dalam connecting device ini terdapat jenis-jenis device sbb : *repeater*, *bridge*, *router* dan *gateway*. Masing-masing connecting device ini terlibat dalam cakupan lapisan OSI yang berbeda seperti dapat dilihat pada Gambar 3.12.



Gambar 3.12 Connecting devices dan model OSI

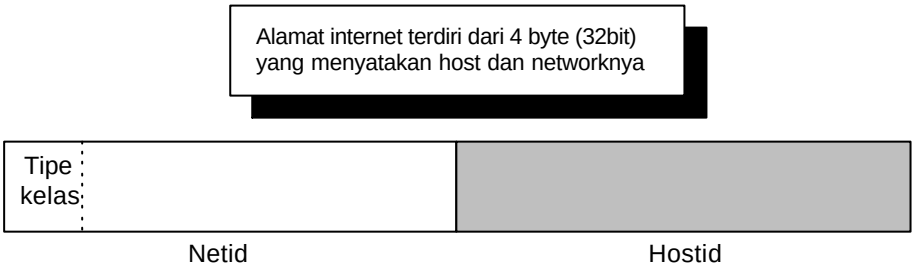
BAB 4

IP Address

IP address memiliki 32 bit angka yang merupakan *logical address*. *IP address* bersifat unique, artinya tidak ada device, station, host atau router yang memiliki *IP address* yang sama. Tapi setiap host, komputer atau router dapat memiliki lebih dari *IP address*. Setiap alamat IP memiliki makna netID dan hostID. Netid adalah pada bit-bit terkiri dan hostid adalah bit-bit selain netid (terkanan).

Notasi Desimal

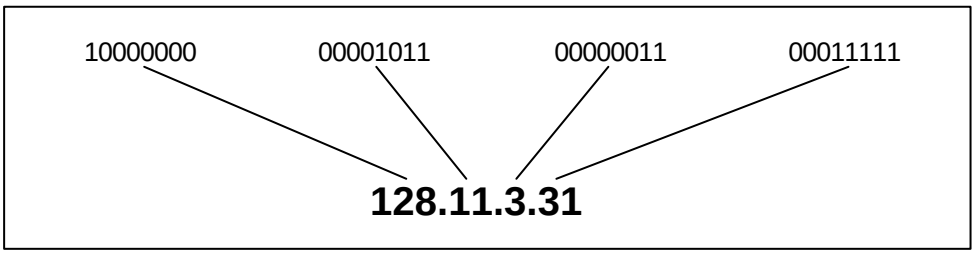
Untuk membuat pembacaan lebih mudah alamat internet yang merupakan *logical address* ini maka dibuatlah dalam bentuk desimal di mana setiap 8 bit diwakili satu bilangan desimal. Masing-masing angka desimal ini dipisahkan oleh tanda titik (Gambar 4.1).



Gambar 4.1 Alamat Internet

Notasi Desimal

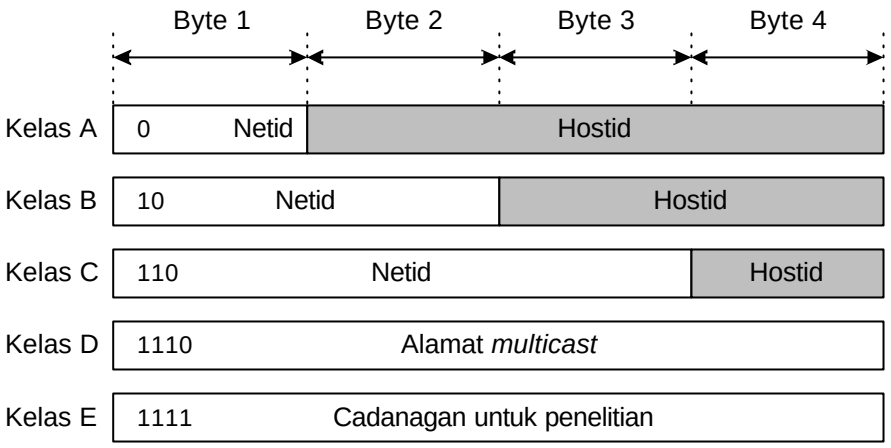
Untuk mempermudah pembacaan, 32 bit alamat internet direpresenatsikan dengan notasi desimal.



Gambar 4.2 Notasi desimal

kelas

Dalam IP address adal 5 peng-kelas-an yakni kelas A, kelas B, kelas C, kelas D dan kelas E. Semua itu didisain untuk kebutuhan jenis-jenis organisasi.



Gambar 4.3 kelas-kelas alamat internet

Kelas A

Dalam kelas A ini oktet (8 bit) pertama adalah netid. Di mana bit yang tertinggal pada netid kelas A ini adalah nol (0) semua. Secara teori, kelas A ini memiliki 2^7 jaringan atau 128 jaringan yang tersedia. Secara aktual hanya ada 126 jaringan yang tersedia karena ada 2 alamat yang disisakan untuk tujuan tertentu. Dalam kelas A, 24 bit digunakan sebagai hostid. Jadi secara teori pula setiap netid memiliki 2^{24} host atau 16.777.216 host / router. Kelas A cocok untuk mendisain organisasi komputer yang jumlahnya sangat besar dalam jaringannya.

Kelas B

Dalam kelas B, 2 oktet digunakan sebagai netid dan 2 oktet sisanya untuk hostid. Secara teori pula, kelas B memiliki 2^{14} netid atau 16.384 jaringan. Sedangkan banyaknya host setiap jaringan adalah 2^{16} host atau 65.536 host / router. Dikarenakan ada 2 alamat yang akan digunakan untuk tujuan khusus, maka hostid yang tersedia efektif adalah sebanyak 65.534. Kelas B ini cocok untuk mendisain organisasi komputer dalam jumlah menengah.

Kelas C

Dalam kelas C, 3 oktet sudah dimiliki untuk netid dan hanya 1 oktet untuk hostid. Sehingga secara teori banyaknya jaringan yang bisa dibentuk oleh kelas C ini adalah 2^{21} atau terdapat 2.097.152 jaringan. Sedangkan banyaknya host / router di setiap jaringan adalah 2^8 host / router atau setara dengan 256 host. Juga dikarenakan penggunaan 2 hostid untuk tujuan khusus maka hostid yang tersedia efektif adalah sebanyak 254 host atau router.

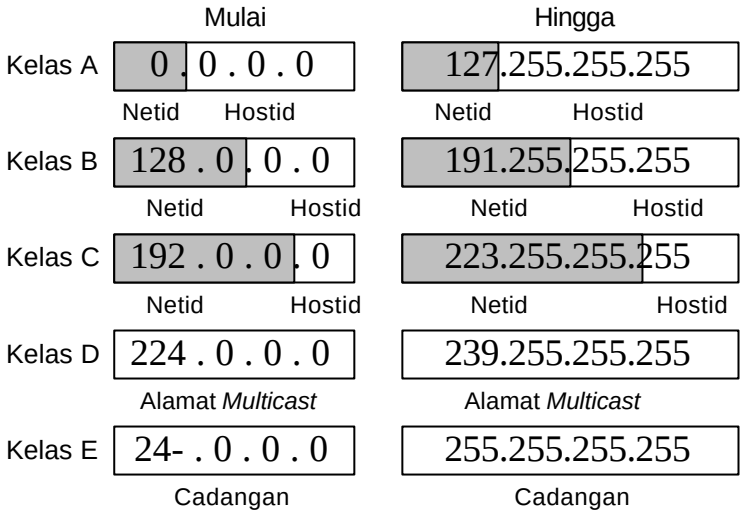
Kelas D

Khusu kelas D ini digunakan untuk tujuan *multicasting*. Dalam kelas ini tidak lagi dibahas mengenai netid dan hostid.

Kelas E

Kelas E disisakan untuk pengunaan khusus, biasanya untuk kepentingan riset. Juga tidak ada dikenal netid dan hostid di sini.

Secara keseluruhan penentuan kelas dapat dilihat di Gambar 4.4.



Gambar 4.4 Kelas-kelas dengan menggunakan notasi desimal

alamat khusus

Beberapa bagian alamat dalam kelas A, B dan C digunakan untuk lamat khusus (lihat tabel 4.1).

Alamat khusus	Netid	Hostid	Asal atau Tujuan
Alamat network	Spesifik	0 semua	Tidak ada
Alamat broadcast langsung	Specific	1 semua	Tujuan
Alamat broadcast terbatas	1 semua	1 semua	Tujuan
Host dalam network / jaringan	0 semua	0 semua	Asal
Host spesifik dalam jaringan	0 semua	spesifik	Tujuan
Alamat loopback	127	sembarang	Tujuan

Tabel 4.1 Alamat khusus

Network Address (alamat jaringan)

Dalam kelas A, B dan C sebuah alamat dengan hostid yang bernilai 0 semua tidak diperuntukkan kepada host manapun. Alamat demikian dicadangkan untuk mendefinisikan alamat jaringan. Namun patut diingat bahwa netid berbeda dengan alamat jaringan (*network address*). Karena netid adalah bagian dari IP address, sedangkan *network address* adalah sebuah alamat di mana hostid nya di set 0 semua. Tamabahan juga, alamat jaringan atau *network address* ini tidak dapat digunakan sebagai alamat asal dan tujuan dalam sebuah paket IP.

Direct Broadcast Address

Dalam kelas A, B dan C, jika hostid semuanya di-set 1, alamat tersebut disebut sebagai *direct broadcast address*. Alamat ini digunakan router untuk mengirim sebuah paket ke seluruh host dalam jaringan tertentu / khusus, sehingga seluruh host pada jaringan tertentu tersebut menerima paket dengan alamat ini.

Limited Broadcast Address

Dalam kelas A, B dan C, sebuah alamat dengan semua di set 1 baik netid maupun hostid digunakan untuk menentukan apakah *broadcast address* dalam jaringannya.

Host ini ada di dalam jaringannya

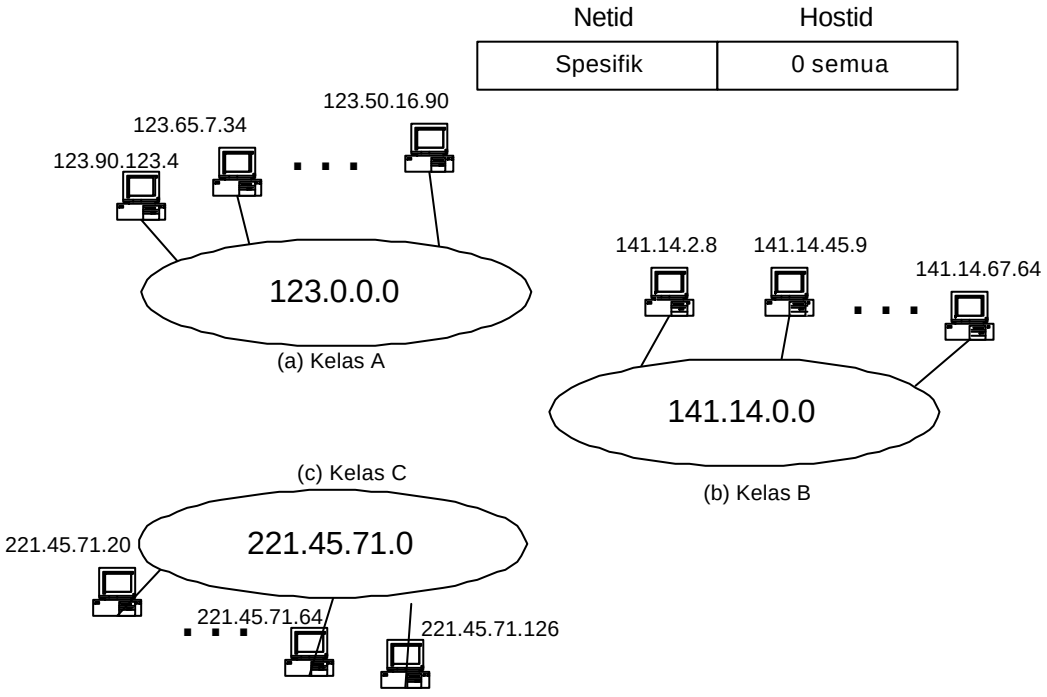
Jika semua IP di-set 0 semua, berarti host ini pada jaringannya. Teknik ini digunakan oleh sebuah host yang baru melakukan bootstrap dan inisialisasi karena host tidak tahu alamat IP nya. Alamat IP ini hanya dapat digunakan sebagai alamat asal (*source address*).

Specific Host dalam jaringannya

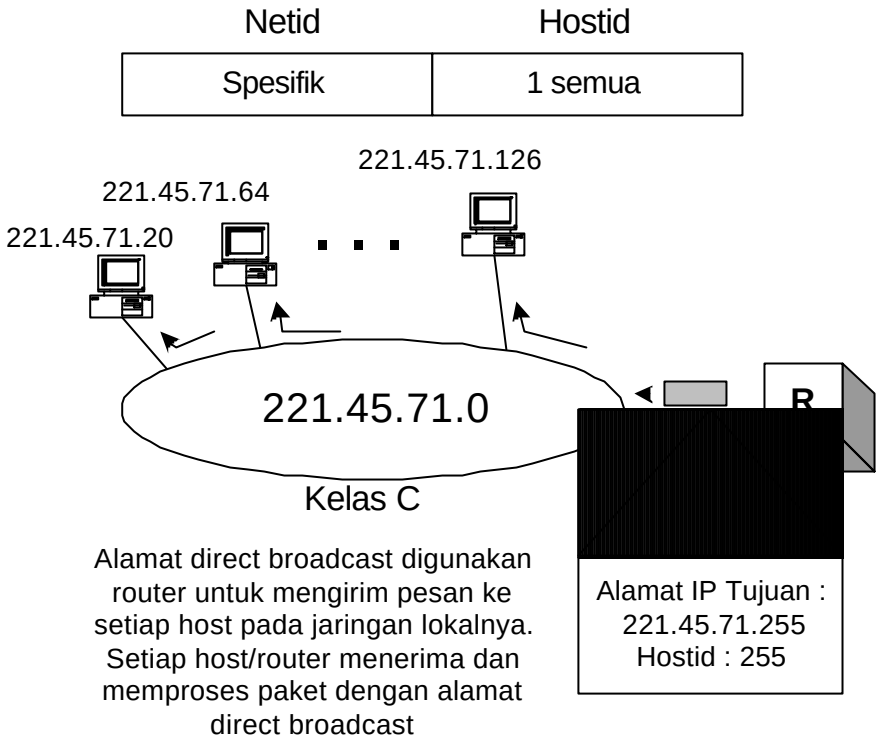
Alamat IP dengan netid yang 0 semua berarti sebuah host yg spesifik dalam jaringannya. Alamat ini digunakan oleh sebuah host untuk mengirim pesan ke host lain dalam jaringan yang sama. Catatan: alamat ini hanya digunakan untuk alamat tujuan (*destination address*).

Loopback Address

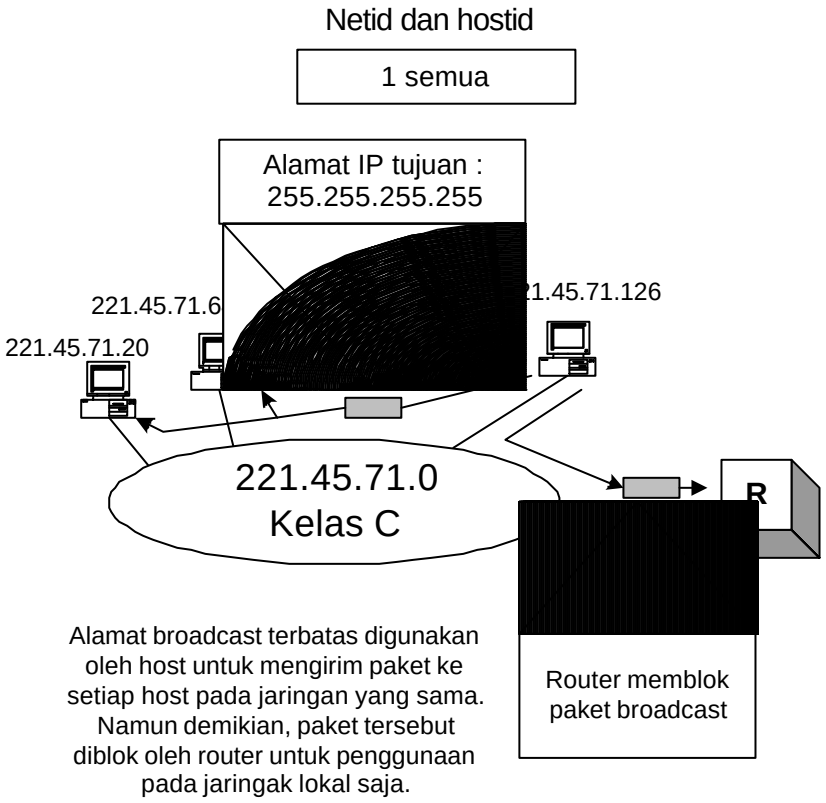
Alamat IP yang dimulai dengan desimal 127 digunakan sebagai *loopback address*. Alamat ini digunakan untuk menguji perangkat lunak pada komputer atau host.



Gambar 4.5 Contoh alamat jaringan / network address



Gambar 4.6 Contoh *direct broadcast address*



Gambar 4.7 Contoh *limited broadcast address*

UNICAST, *multicast* dan broadcast

Alamat Unicast

Paket yang dikirim oleh satu host menuju sebuah host yang lain menggunakan alamat unicast di mana pada paketnya terdapat alamat asal dan alamt tujuan. Komunikasi ini juga disebut *one-to-one*. Alamat unicast dimiliki kelas A, B dan C saja.

Alamat *Multicast*

Alamat *multicast* adalah komunikasi *one-to-many*. Paket yang dikirim oleh sebuah host menuju kelompok tujuan (*group of destination*). Alamat ini hanya ada di kelas D.

Alamat Broadcast

Broadcast bermakna sebagai komunikasi *one-to-all*. Alamat broadcast ini hanya bisa terjadi pada jaringan lokalnya saja.

jaringan private

Jika sebuah organisasi ingin membangun jaringan komputer dan tidak membutuhkan terkoneksi pada jaringan internet, ada 3 pilihan untuk pembuatan alamat-alamat IP nya :

1. Dapat menggunakan sebuah alamat yang unique tanpa menghubungkan ke internet. Namun ini akan sangat menguntungkan apabila di kemudian hari berniat untuk menghubungkan jaringan private-nya ke internet tidak akan timbul masalah lagi. Namun nampaknya untuk kelas A dan B sudah tidak memungkinkan lagi karena sudah dimiliki oleh organisasi yang terhubung ke internet.
2. Bisa juga menggunakan sembarang alamat IP dari kelas A, B dan C. Namun ini akan sanagat menyulitkan apabila organisasi tersebut berniat terhubung ke internet.
3. Pilihan 1 dan 2 masih memiliki masalah, maka otoritas pencatatan alamat internet telah mencadangkan range alamat-alamat tertentu dari kelas A, B dan C yang bisa digunakan oleh organisasi manapun sebagai jaringan private. Tentu saja, di dalam internet, alamat khusus ini tidak akan dikenal dan diabaikan. Singkat kata, alamat ini adalah unique bagi jaringan lokalnya namun tidak unique bagi jaringan global. Lihat Tabel 4.2

Kelas	Alamat Netid	Total
A	10.0.0	1
B	172.16 sampai 172.31	16
C	192.68.0 sampai 192.68.255	256

Tabel 4.2 Alamat yang dicadangkan untuk jaringan private

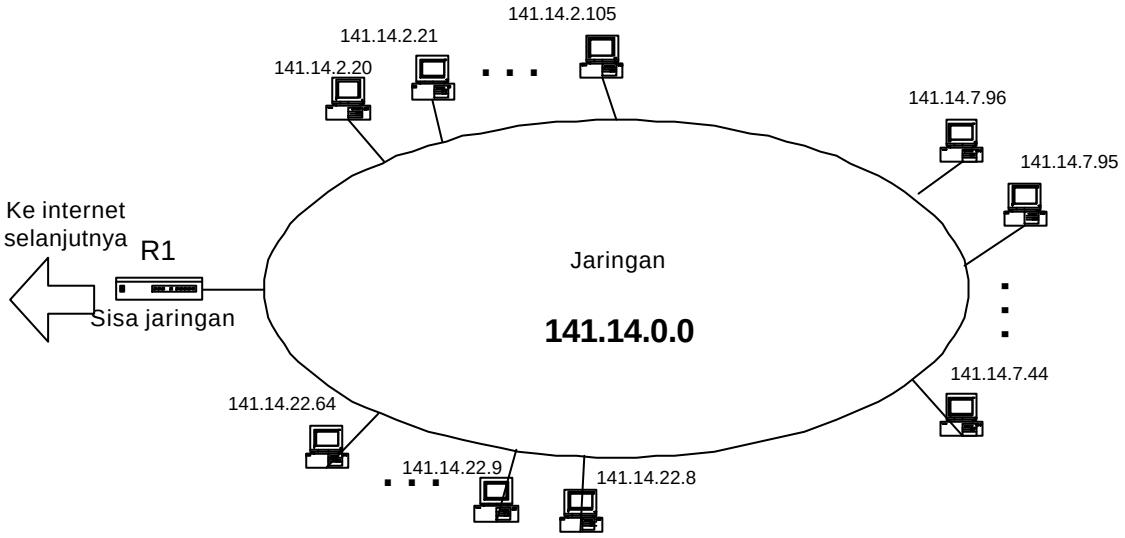
BAB 5

Subnetting dan Supernetting

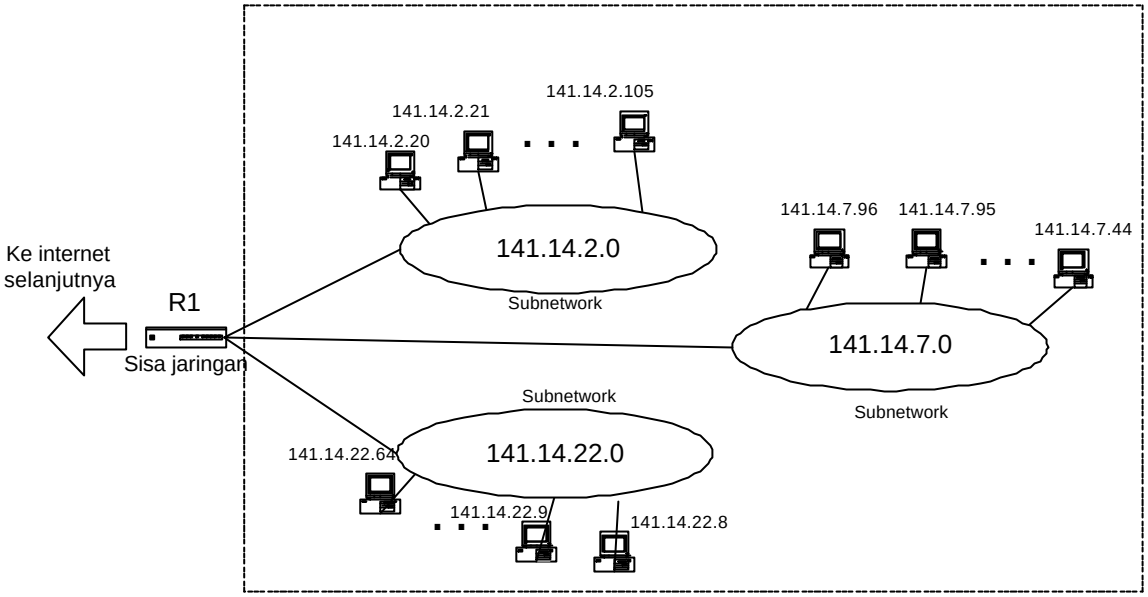
subnetting

Subnetting merupakan teknik memecah network menjadi subnetwork yang lebih kecil. Subnetting hanya dapat dilakukan pada kelas A, B dan C.

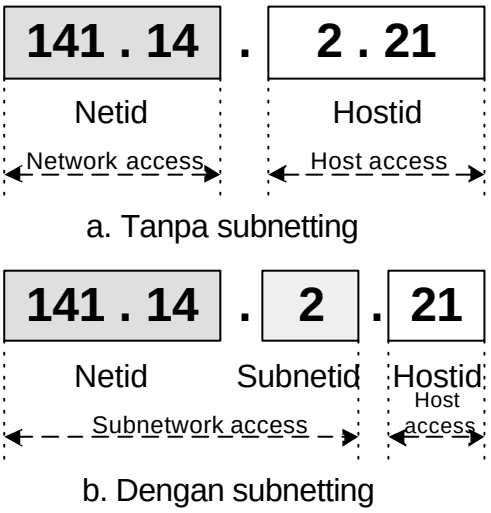
Bila kita perhatikan alamat IP terdiri dari netid dan hostid. Jadi jika kita menuju suatu host artinga kita mencari netidnya baru mencari hostidnya. Mekanisme itu melalui 2 level hierarki. Namun bila sudah mendapatkan netid dari organisasi dan ingin membuat organisasi tersebut menjadi sub kelompok perlu dilakukan pemecahan network dengan teknik subnetting. Dapat dilihat pada Gambar 5.1, 5.2 dan 5.3.



Gambar 5.1 Jaringan dengan 2 tingkat hierarki (tanpa subnetting)

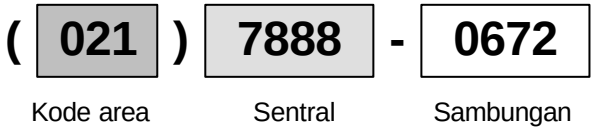


Gambar 5.2 Jaringan dengan 3 tingkat hierarki (dengan subnetting)



Gambar 5.3 Alamat-alamat dalam jaringan dengan atau tanpa subnetting

Konsep hierarki ini bisa dianalogikan dengan nomor telepon, Gamabar 5.4.

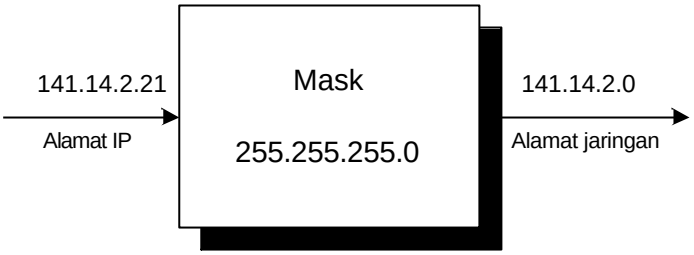


Gambar 5.4 Konsep hierarki dalam nomor telepon

masking

Masking adalah suatu proses yang mengekstrak alamat jaringan fisik dari sebuah alamat IP. Lihat Gambar 5.5.

a. Tanpa subnetting

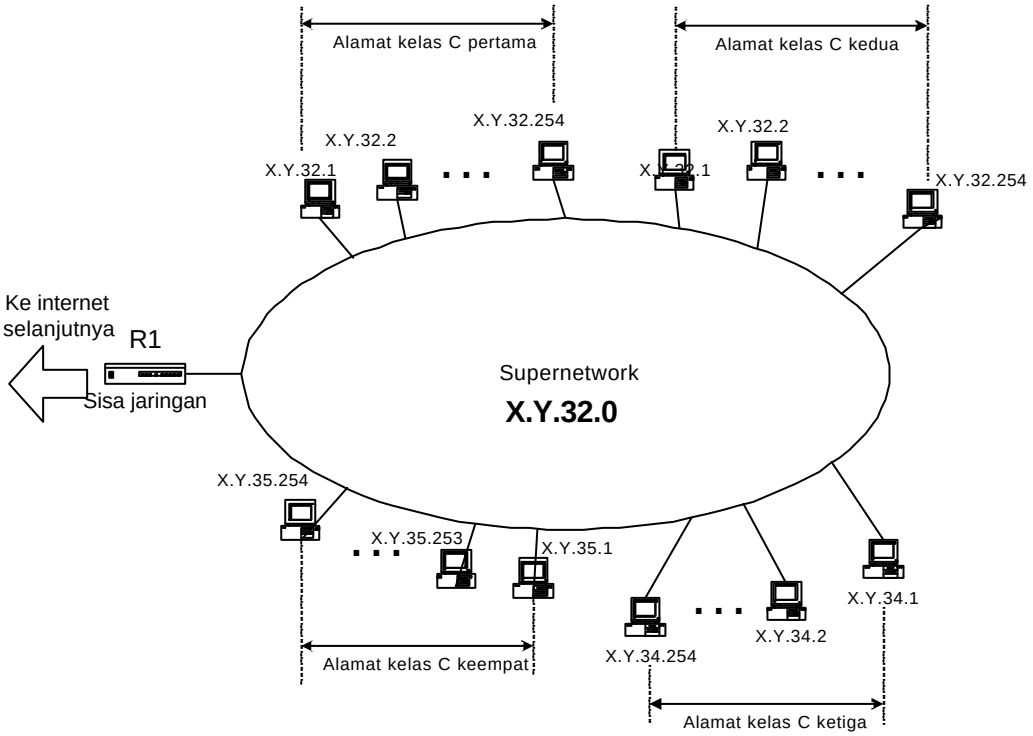


b. Dengan subnetting

Gambar 5.5 Masking

supernetting

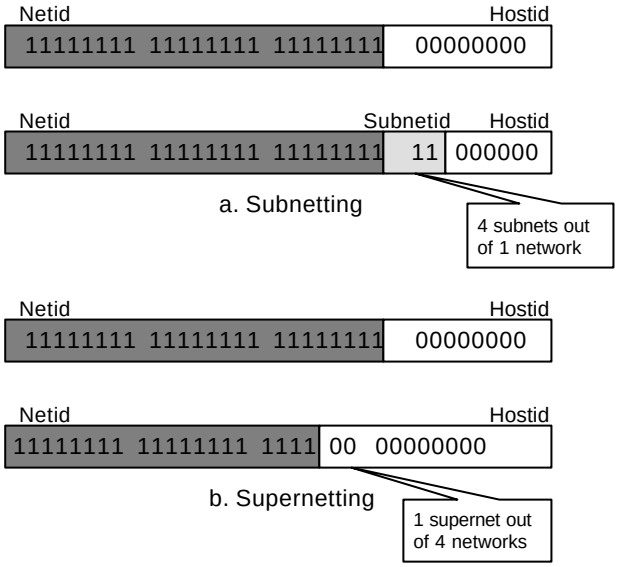
Alamat-alamat kelas A dan kelas B sudah hampir terpakai semua, namun kelas C masih memberikan ketersediaan awalaupun juga sangat terbatas. Walaupun demikian kelas C yang setiap netid memeiliki maksimum 254 host masih tidak memuaskan bagi kebutuhan suatu organisasi. Solusinya adalah *supernetting*. Contoh, suatu organisasi membutuhkan 1.000 alamat yang diambil dari 4 alamat kelas C. Maka organisasi tersebut dapat menggunakan lamat-alamat tersebut dalam 1 supernetwork dalam 4 jaringan. Gambar 5.6 memeperlihatkan bagaiman 4 alamat kelas C berkombinasi menjadi satu supernetwork.



Gambar 5.6 Supernetwork

Supernet Mask

Supernet mask dapat dibuat untuk membentuk sebuah blok kelas C jika banyak alamat jaringan adalah pangkat dari 2 (2, 4, 8, 16, ..). *Default mask* untuk kelas C adalah 255.255.255.0, artinya ada 24 digit 1 kemudian diikuti 8 digit 0. Jika beberapa digit 1 digantimenjadi 0, maka kita mendapatkan sebuah *mask* untuk kelompok alamat kelas C. Seperti pada Gambar 5.7 terlihat bahwa proses mask di supernetting berlawanan dengan mask di subnetting.



Gambar 5.7 Supernet mask

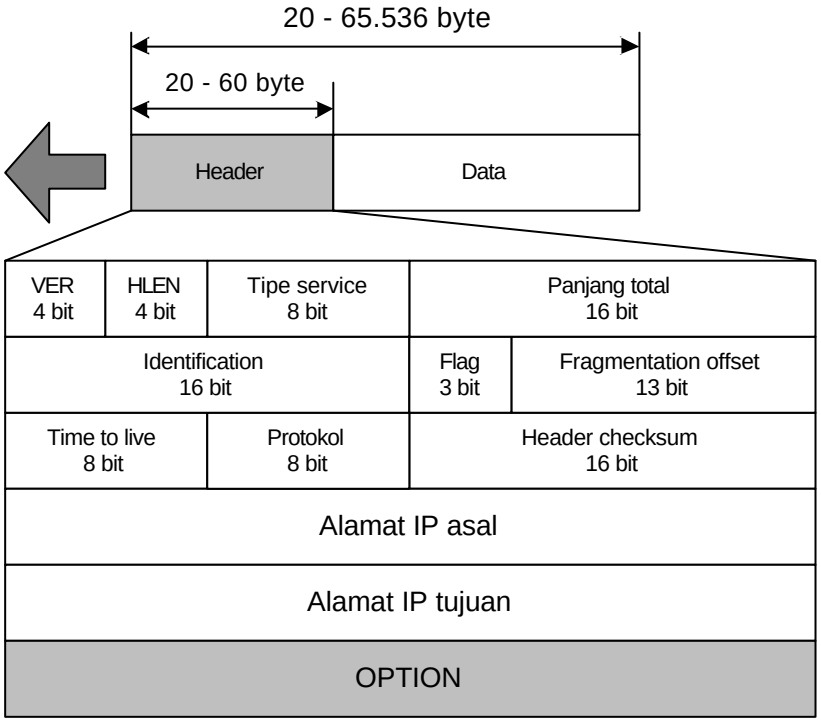
BAB 6

Internet Protocol (IP)

Internet Protocol (IP) adalah mekanisme transmisi yang digunakan oleh TCP / IP yang sifatnya *unreliable* dan *connectionless*. Banyak yang mengistilahkan dengan *best effort delivery*, artinya: bahwa IP menyediakan *no error checking* atau *tracking*. Jika diperlukan reliabilitas maka IP mesti dipasangkan dengan protokol yang reliabel misalnya TCP. Contoh alama dari IP adalah, kantor pos mengirimkan surat tapi tidak selalu sukse dikirimkan. Jika surat tersebut tidak lengkap maka terserah pengirim ingin mengantarkannya atau tidak. Juga kantor pos tidak pernah menjejaki ke mana surat-surat yang jumlahnya jutaan itu terkirim.

datagram

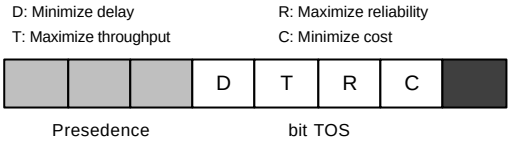
Paket dalam lapisan IP disebut dengan *datagram*. Gambar 6.1 memperlihatkan datagram sebuah IP.



Gambar 6.1 Datagram IP

Datagram IP panjangnya variabel yang terdiri dari data dan header. Panjang header bisa antara 20 sampai 60 byte. Header ini memuat informasi yang penting sekali untuk keperluan ruting dan pengiriman. Berikut penjelasn tentang isi daripada header.

- Version (VER) : Ada 4 bit yang menginformasikan versi IP. Saat ini versi yang digunakan adalah versi 4. Jadi dengan demikian mesin yang memproses datagram ini harus melakukan mekanisme IP versi 4.
- Header Length (HLEN) : Ada 4 bit yang menginformasikan panjang header datagram dalam 4 byte word.
- Service type : Ada 8 bit yang menginformasikan bagaimana datagram harus ditangani oleh router. Field ini dibagi menjadi 2 subfield yakni: *precedence* (3 bit) dan *sevice type (TOS=type of service)* (4 bit). Sisa bit tidak digunakan, lihat Gambar 6.2.



Gambar 6.2 Jenis layanan/service

Bit TOS	Penjelasan
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

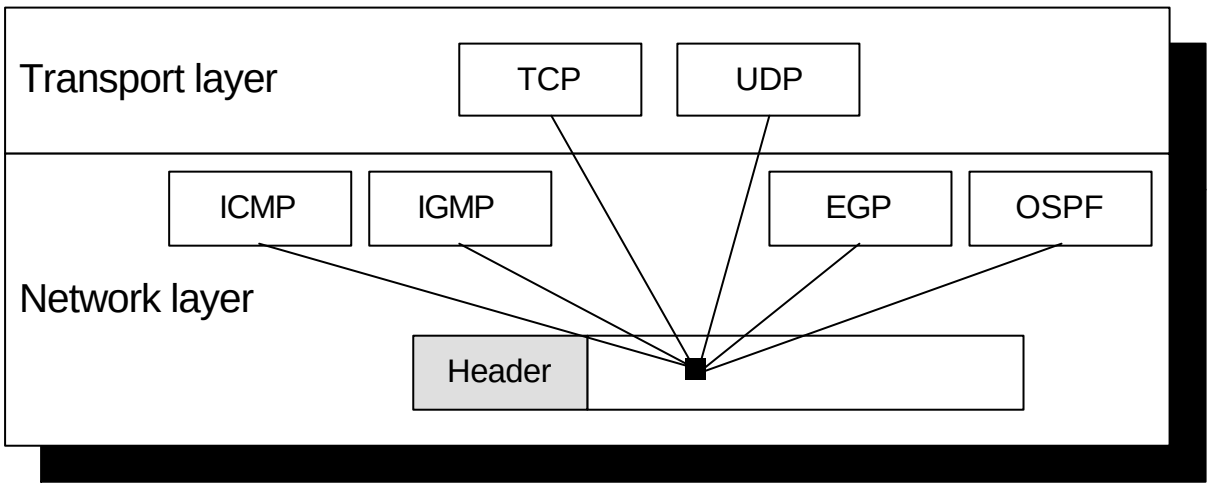
Tabel 6.1 Jenis layanan/service

Protokol	Bit TOS	Penjelasan
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimize cost
IGP	0010	Maximize reliability
SNMP	0010	Maximize reliability
TELNET	1000	Minimize delay
FTP (data)	0100	Maximize throughput
FTP (control)	1000	Minimize delay
TFTP	1000	Minimize delay
SMTP (command)	1000	Minimize delay
SMTP (data)	0100	Maximize throughput
DNS (UDP query)	1000	Minimize delay
DNS (TCP query)	0000	Normal
DNS (zone)	0100	Maximize throughput

Tabel 6.2 Jenis layanan default

- Total length : memiliki 16 bit yang menentukan panjang total (header plus data) daripada datagram IP dalam satuan byte. Karena panjang field ini adlah 16 bit maka total panjang datagram IP dibatasi sampai 65.535 (2^{16}-1) byte saja. Melihat perkembangan teknologi yang mampu mentransimiskan data yang lebar bandwidthnya, maka ada lagi proses yang disebut fragmentasi yakni memecah besar data yang tidak muat diangkut oleh datagram IP.

- Identification : field ini memiliki 16 bit yang digunakan dalam fragmentasi. Akan dibahas lebih lanjut.
- Flags : field ini juga digunakan dalam proses fragmentasi.
- Fragmentation offset : field ini digunakan juga untuk fragmentasi.
- Time to live (TTL) : Ternyata dalam protokol TCP/IP datagram yang melakukan perjalanan antar jaringan melalui router atau agteway memiliki batasan waktu. Field TTL ini beris 8 bit. Bisa saja mesin pengirim yang menghendaki datagram ini melakukan perjalanan di lokal jaringannya men-set TTL adlah 1.
- Protocol : field ini berisi 8 bit yang mendefinisikan lapisan protokol di atasnya menggunakan layanan lapisan IP. Sebuah datagram IP dapat membeungkus data dari beberapa tingkat protokol di atasnya seperti TCP, UDP, ICMP dan IGMP. Ketika protokol I me-*multiplex* dan men-*demultiplex* data dari tingkatan protokol di atasnya, nilai field ini menolong proses ketika datagram sampai ke tujuan alamat akhir, Gambar 6.3.



Gambar 6.3 Multiplexing

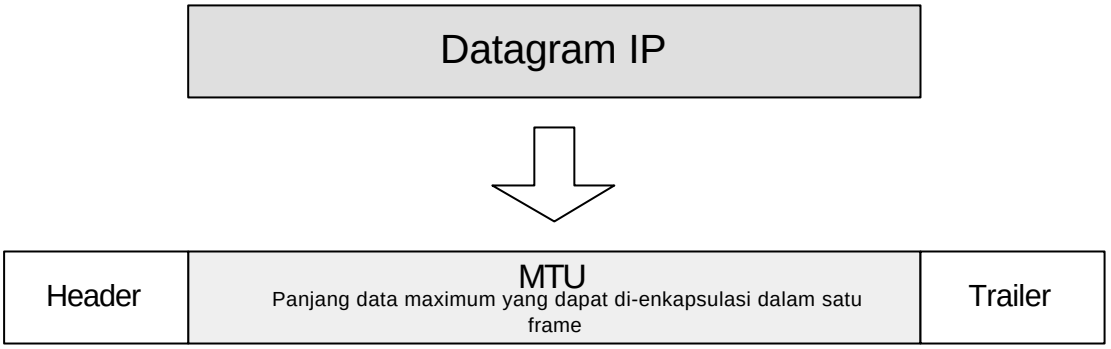
- Checksum : Adalah filed yg berisi 16 bit yang melakukan proses *error correction.*
- Source address : 32 bit yang berisi informasi alamat IP dari host pengirim.
- Destination address : 32 bit yang berisi informasi alamat IP tujuan.

fragmentasi

Maximum Transfer Unit (MTU)

Setiap lapisan protokol data link memiliki format frame nya sendiri. Salah satu field frame tersebut didefinisikan dalam bentuk atau format ukuran maksimum untuk field data. Ketika datagram dibungkus (*encapsulated*) dalam sebuah frame, total ukuran datagram harus kurang

dari ukuran maksimumnya. Hal ini disebabkan oleh persyaratan perngkat keras dan lunak yang digunakan dalam jaringan, Lihat Gambar 6.4.



Gambar 6.4 MTU

Tabel 6.4 memperlihatkan bagaimana ukuran MTU berbeda-beda untuk setiap jenis protokol lapisan fisik.

Protokol	MTU
Hyperchannel	65.535
Token ring (16 Mbps)	17.914
Token ring (4 Mbps)	4.464
FDDI	4.352
Ethernet	1.500
X.25	576
PPP	296

Tabel 6.4 MTU untuk bermacam jenis sistem jaringan

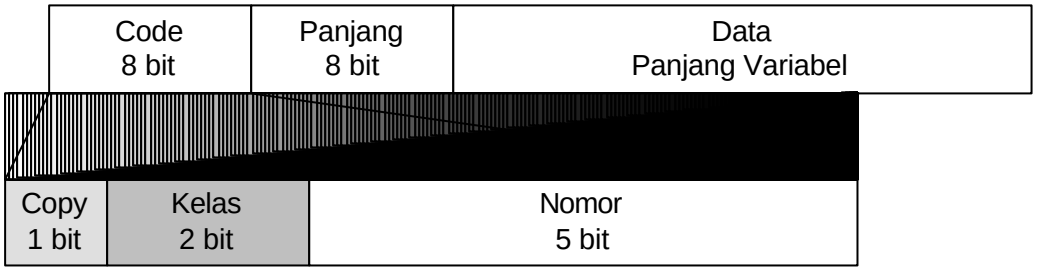
Setiap sebuah datagram yang difragmentasi akan memiliki header sendiri. Sebuah datagram dapat difragmentasi beberapa kali sebelum mencapai tujuan akhirnya jika melewati banyak jenis fisik jaringan. Fragmen-fragmen ini dapat saja menempuh perjalanan atau rute yang berbeda-beda. Jadi tentu saja perakitan / *reassembly* terjadi di alamat tujuan akhir.

option

Di awal bab dijelaskan bahwa header datagram IP mempunyai panjang yang tetap yakni 20 byte. Sedangkan panjang header yang variabel adalah 40 byte. Oleh sebab itu header datagram IP berkisar antara 20 hingga 60 byte. Panjang header variabel ini adalah option. Yang digunakan untuk kepentingan pengetesan dan debugging.

Format

Format OPTION ini terdiri dari Code, Length dan Data, lihat Gambar 6.5.



Copy
0 Copy hanya pada fragment pertama
1 Copy ke dalam semua fragmen

Kelas
00 Kontrol datagram
01 Cadangan
10 Debugging dan manajemen
11 Cadangan

Nomor
00000 Akhir dari option
00001 No opertion
00011 Loose source route
00100 Timestamp
00111 Record route
01001 Strict source code

Gambar 6.5 Format option

Jenis Option

Option memeiliki 6 jenis yang dikategorikan dalam 2 kategori, yakni byte tunggal dan multi byte. Kategori byte tunggal adalah *No operation* dan *end of option.*

- **No operation** : adalah 1-byte yang digunakan sebagai pengisi antara option.
- **End of option** : digunakan untuk *padding* pada akhir field option.
- **Record route** : digunakan untuk mencatat router internet yang menangani datagram. Record route ini dapat mencatat hingga 9 router alamat IP.
- **Strict source route** : digunakan oleh host asal untuk menentukan sebuah rute bagi datagram yang akan menempuh perjalan di internet. Pengirim dalam hal ini dapat menentukan rute dengan TOS, seperti waktu tunda minimum atau maximum *throughput*.
- **Loose source route** : mirip dengan strict source route, namun agak lebih luwes. Setiap router dalam list harus dikunjungi, namun datagram dapat mengunjungi router yang lain juga.
- **Timestamp** : digunakan untuk mencatat waktu yang dilakukan oleh router. Waktu ditampilkan dalam milidetik dari saat tengah malam, *Universal Time*. Waktu ini bermanfaat untuk menolong pengguna menjejaki perilaku router di internet.

checksum

Metode deteksi error digunakan TCP/IP yang disebut *checksum*.

Kalkulasi *checksum* pada sisi pengirim

Pada sisi pengirim, paket dibagi menjadi *n*-bit bagian (n biasanya 16). Bagian-bagian tersebut ditambahkan dengan metode aritmetika *one's complement*. Caranya :

✍✍Paket dibagi dalam *k* bagian, masing-masing terdiri dari *n* bit.

✍✍Seluruh bagian ditambahkan bersama dengan menggunakan metoda aritmatika *one's complement*.

✍✍Hasil akhir dikomplementasikan membentuk *checksum*.

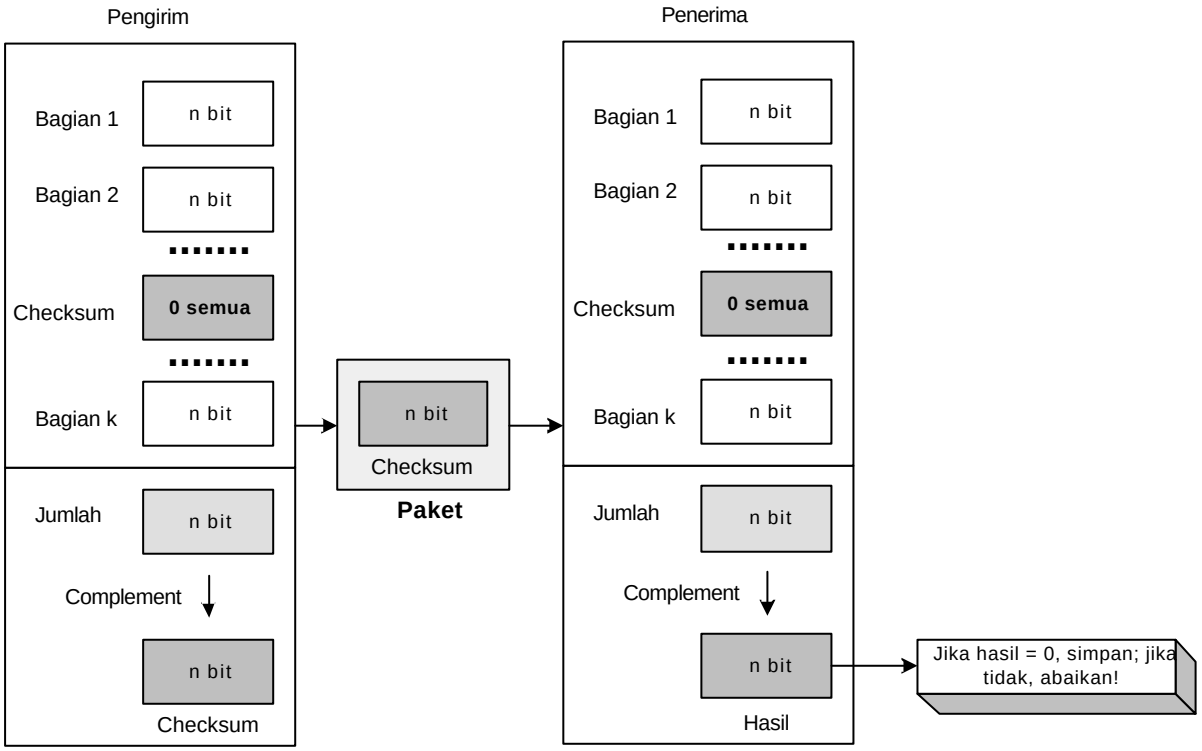
Kalkulasi *checksum* pada sisi penerima

✍✍Paket dibagi menjadi *k* bagian, masing-masing terdiri dari *n* bit.

✍✍Seluruh bagian tadi ditambahkan bersama-sama menggunakan aritmatika *one's complement*.

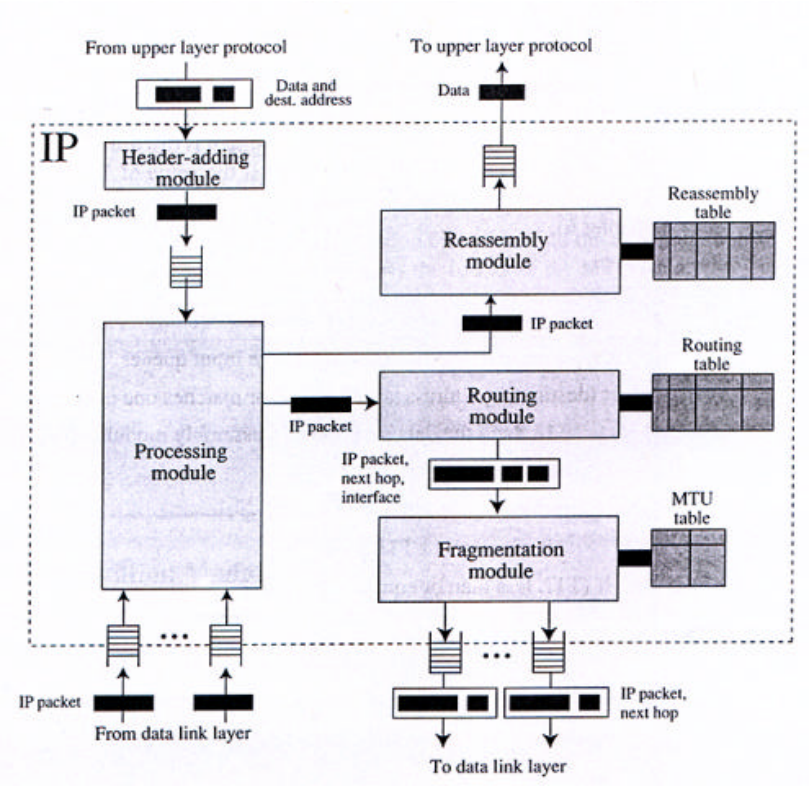
✍✍Hasilnya dikomplementasi.

✍✍Hasil akhir adalah 0, maka paket tidak rusak dan dapat diterima, jika tidak akan ditolak.



Gambar 6.6 Konsep *checksum*

Untuk lebih lanjut mengetahui komponen-komponen protokol IP dapat dilihat pada Gambar 6.7.

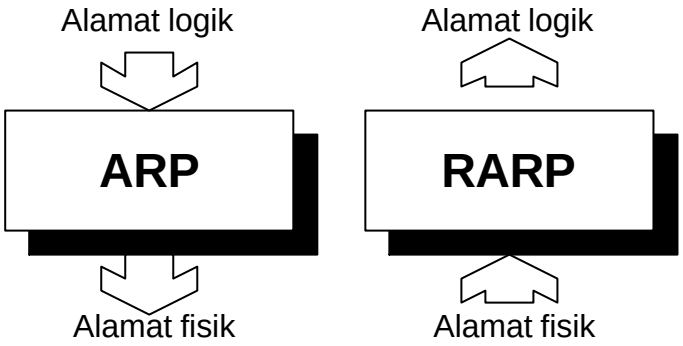


Gambar 6.7 Komponen Protokol IP

BAB 7

ARP dan RARP

Address Resolution Protocol (ARP) dan *Reverse Address Resolution Protocol* (RARP) menggunakan alamat fisik *unicast* dan *broadcast*. Sebagai contoh Ethernet akan menggunakan alamat $FFFFFFFFFFFF_{16}$ sebagai alamat *broadcast*. Sesungguhnya ARP dan RARP adalah proses pemetaan alamat fisik (*Physical Address*) seperti alamat NIC yang berasosiasi kepada *logical address* (alamat IP) atau sebaliknya.

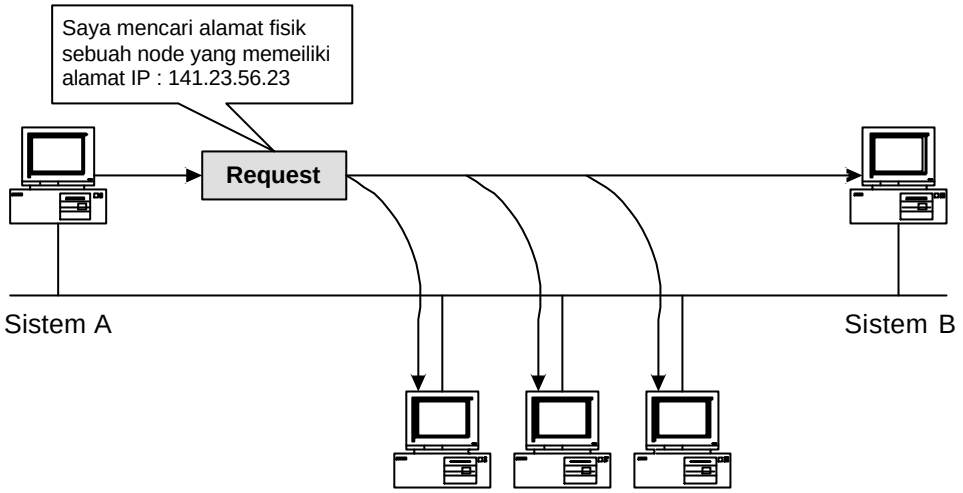


Gambar 7.1 ARP dan RARP

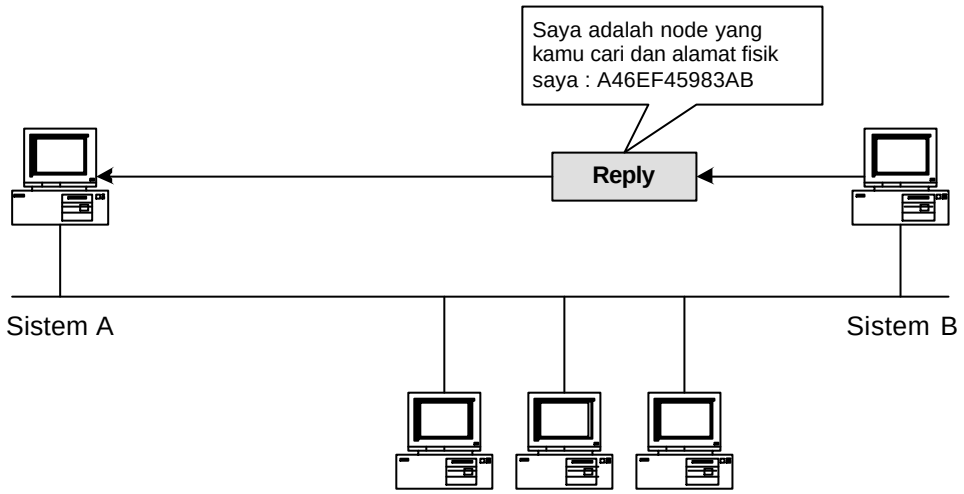
ARP

ARP berasosiasi antara alamat fisik dan alamat IP. Pada LAN, setiap device, host, station dll diidentifikasi dalam bentuk alamat fisik yang didapat dari NIC.

Setiap host atau router yang ingin mengetahui alamat fisik daripada host atau router yang terletak dalam jaringan lokal yang sama akan mengirim paket *query* ARP secara *broadcast*, sehingga seluruh host atau router yang berada pada jaringan lokal akan menerima paket query tersebut. Kemudain setiap router atau host yang menerima paket query dari salah satu host atau router yang mengirim maka akan diproses hanya oleh host atau router yang memiliki IP yang terdapat dalam paket query ARP. Host yang menerima respons akan mengirm balik kepada pengirim query yang berisi paket berupa informasi alamat IP dan alamat fisik. Paket ini balik (reply ini sifatnya *unicast*. Lihat Gambar 7.2.



a. ARP request adalah broadcast



b. ARP reply adalah unicast

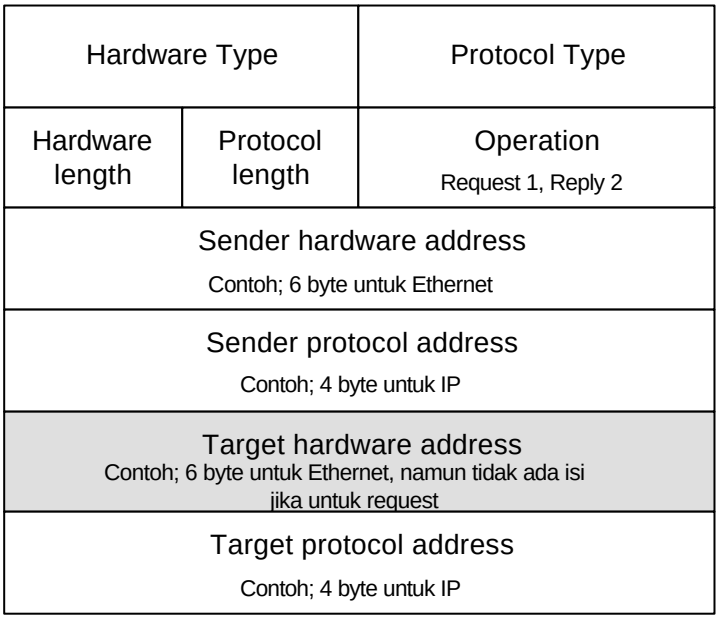
Gambar 7.2 Operasi ARP

Format Paket

Gambar 7.3 memperlihatkan format paket ARP.

- **HTYPE** : adalah tipe hardware / perangkat keras. Banyak bit dalam field ini adlah 16 bit. Sebagai contoh untuk Ethernet mempunyai tipe 1.
- **PTYPE** : adalah tipe protokol di mana banyaknya bit dalam field ini 16 bit. Contohnya, untuk protokol IPv4 adalah 0800_{16}.
- **HLEN** : field berisi 8 bit yang mendefinisikan panjang alamat fisik. Contohnya, untuk Ethernet, panjang alamat fisik adalah 6 byte.
- **PLEN** : field berisi 8 bit yang mendefinisikan panjang alamat logika dalam satuan byte. Contoh : untuk protokol IPv4 panjangnya adalah 4 byte.

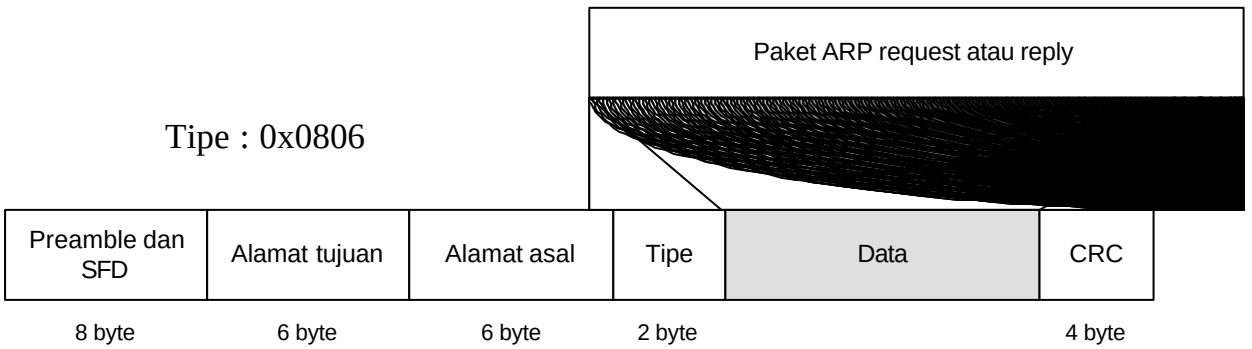
- **OPER**: field berisi 16 bit ini mendefinisikan jenis paket untuk ARP apakah itu berjenis ARP request atau ARP reply.
- **SHA** : banyaknya field adalah variabel yang mendefinisikan alamat fisik dari pengirim. Untuk Ethernet panjang nya 6 byte.
- **SPA** : field ini panjangnya juga variabel dan untuk mendefiniskan alamat logika (alamat IP) dari pengirim.
- **THA** : field ini panjangnya juga variabel yang mendefiniskan alamat fisik daripada target. Pada paket ARP request, field ini isinya 0 semua.
- **TPA** : field ini panjangnya juga variabel dan mendefinisikan alamat logika (IP) dari target.



Gambar 7.3 Paket ARP

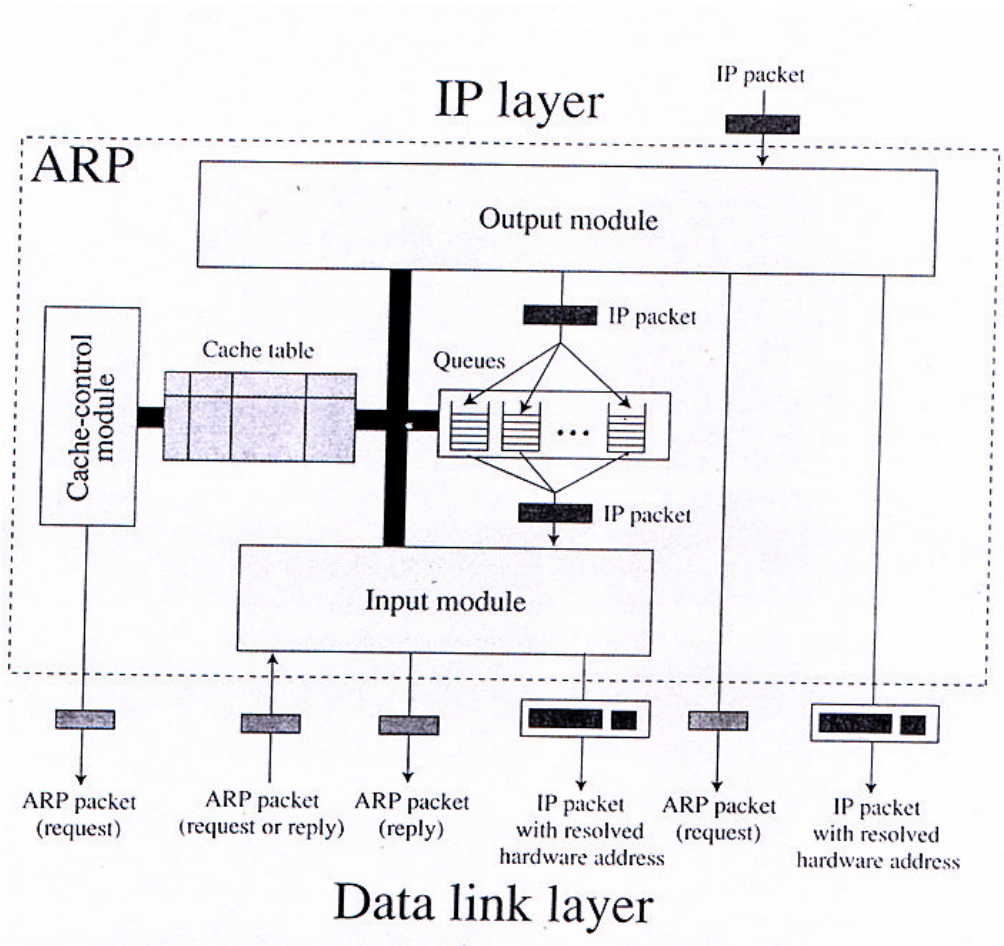
Enkapsulasi (pembungkusan)

Sebuah paket ARP dienkapsulasi langsung ke *frame data link*. Lihat Gambar 7.4.



Gambar 7.4 Enkapsulasi pada paket ARP

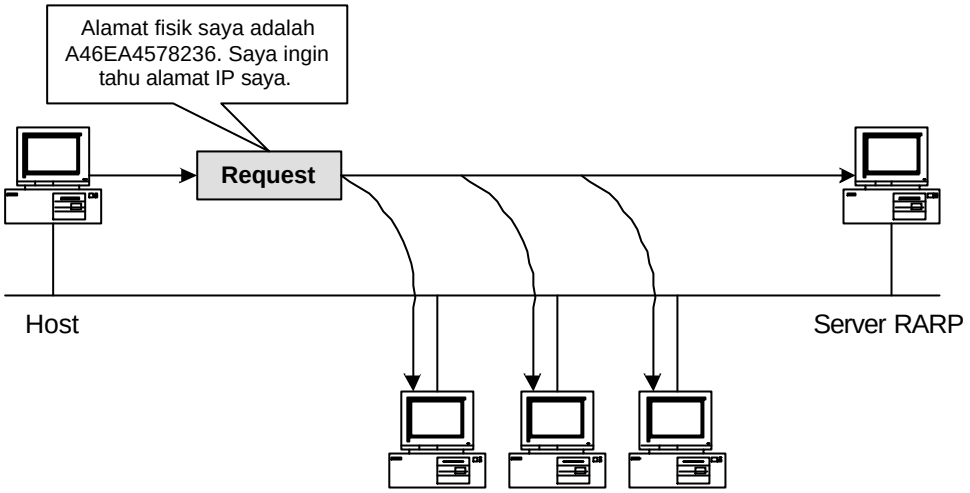
Untuk lebih lanjut mengetahui komponen ARP, dapat dilihat pada Gambar 7.5.



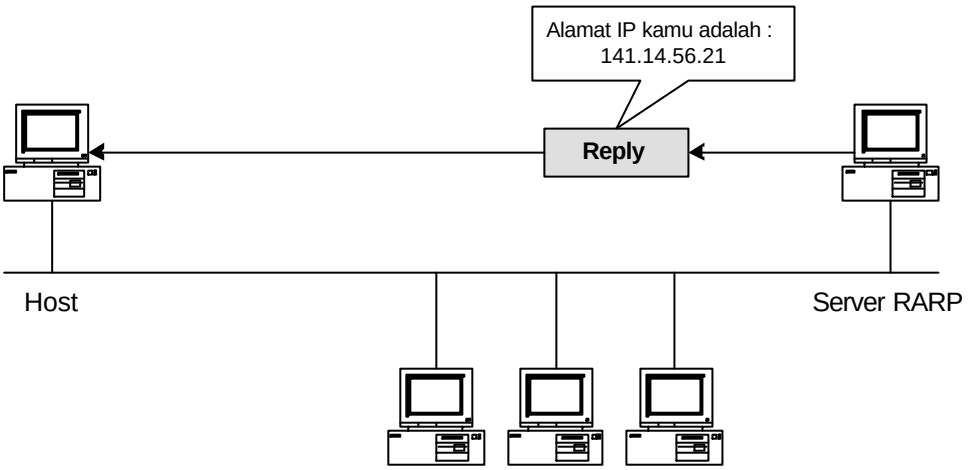
Gambar 7.5 (8.7)

RARP

Sesungguhnya RARP didisain untuk memecahkan masalah mapping alamat dalam sebuah mesin/komputer di mana mesin/komputer mengetahui alamat fisiknya namun tidak mengetahui alamat logikanya. Cara kerja RARP ini terjadi pada saat mesin seperti komputer atau router yang baru bergabung dalam jaringan lokal, kebanyakan tipr mesin yang menerapkan RARP adalah mesin yang *diskless*, atau tidak mempunyai aplikasi program dalam disk. RARP kemudian memberikan request secara broadcast di jaringan lokal. Mesin yang lain pada jaringan lokal yang mengetahui semua seluruh alamat IP akan akan meresponsnya dengan RARP reply secara *unicast*. Sebagai catatan, mesin yang merequest harus menjalankan program klien RARP, sedangkan mesin yang merespons harus menjalankan program server RARP. Lihat Gambar 7.6.



a. RARP request adalah broadcast



b. RARP reply adalah unicast

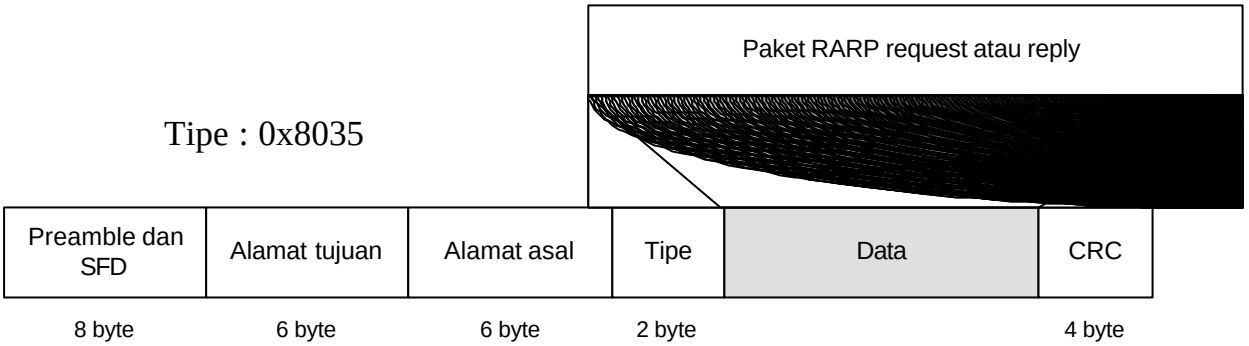
Gambar 7.6 Operasi RARP

Format Paket

Format Paket RARP persis sama dengan format paket ARP.

Enkapsulasi (pembungkusan)

Paket RARP dibungkus secar langsung ke dalam *frame* data link. Lihat Gambar 7.7.



Gambar 7.7 Enkapsulasi pada paket RARP

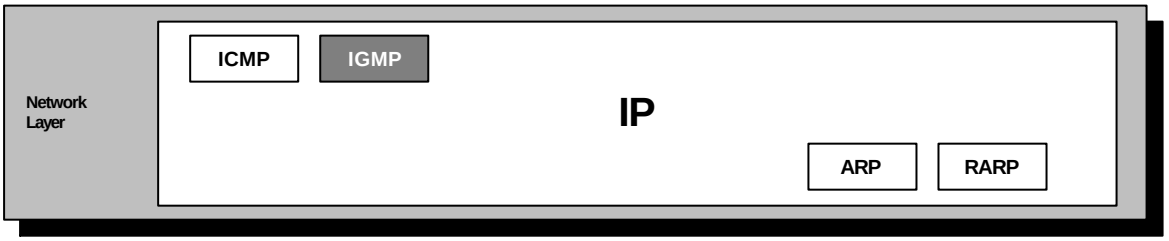
BAB 8

Internet Control Message Protocol (ICMP)

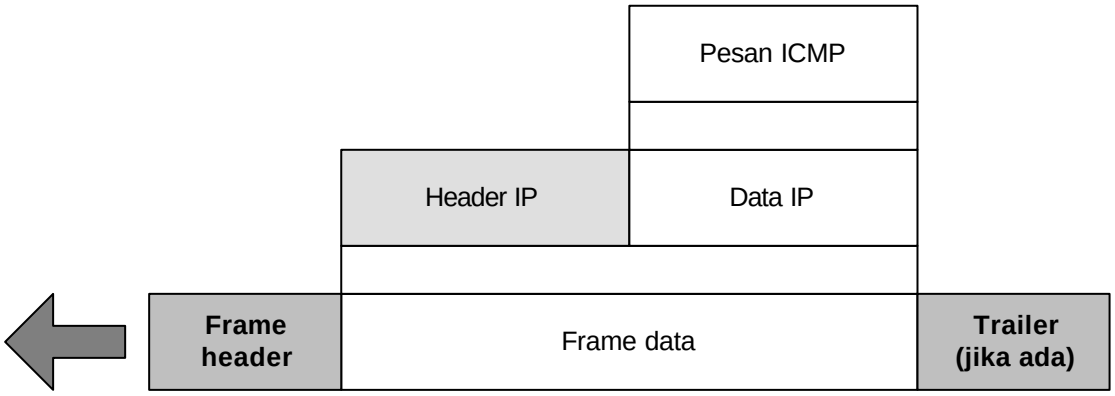
Protokol IP merupakan datagram yang tidak reliable dan *connectionless*. Karena didisain sedemikian adalah untuk membuat sumber daya jaringan lebih efisien. Walaupun demikian IP memiliki 2 defisiensi yaitu : *lack of error control* dan *lack of assistance mechanism*.

Protokol IP tidak memiliki *no error-reporting* atau *error-corecting mechanism*. Lalu apa yang terjadi apabila sesuatu masalah berlaku?

ICMP didisain untuk mengkompensasi 2 defisiensi tersebut. ICMP sebenarnya adalah protokol yang mendukung dan mendampingi protokol IP. Gambar 8.1 adalah pemetaan posisi ICMP dalam *network layer* (lapisan network). Jadi ICMP itu sendiri adalah *network layer*. Gambar 8.2 memperlihatkan bagaiman ICMP dienkapsulasi.



Gambar 8.1 Posisi ICMP dalam lapisan network



Gambar 8.2 Enkapsulasi sebuah ICMP

Jenis-jenis message/pesan

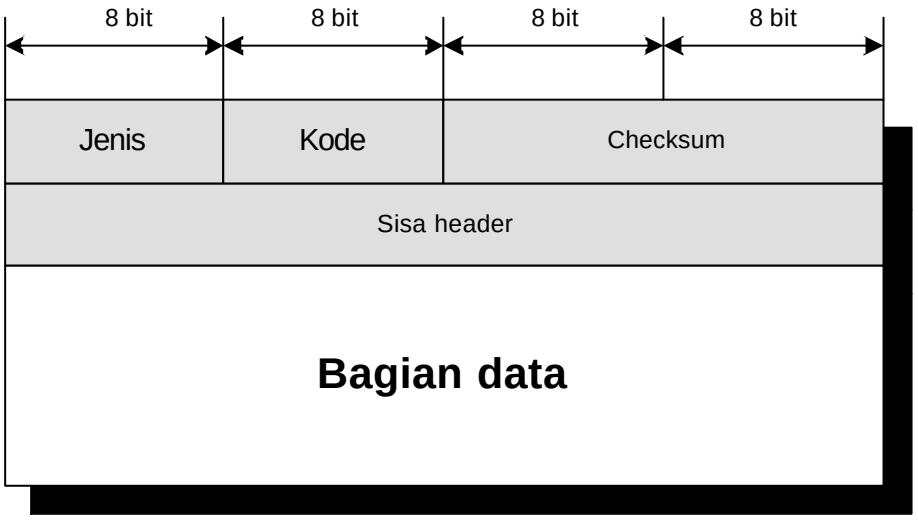
Pesan ICMP dibagi dalam 2 jenis : *error-reporting message* dan *query message*. Lihat Tabel 8.1.

Kategori	*Tipe*	*Pesan/Message*
Pesan *Error-reporting*	3	Destination unreachable
	4	Source quench
	11	Time exeeded
	12	Parameter problem
	5	Redirection
Pesan *Query*	8 atau 0	Echo request or reply
	13 atau 14	Timestamp request and reply
	17 atau 18	Address mask request and reply
	10 atau 9	Router solicitation and advertisement

Tabel 8.1 Pesan-pesan ICMP

Format Message/pesan

Pesan ICMP memiliki 8 byte untuk header dan untuk data besarnya variabel. Format umum pesan ICMP dapat dilihat pada Gambar 8.3.



Gambar 8.3 Format umum pesan ICMP

Error reporting

Tanggung jawab utama ICM adalah melaporkan terjadinya error. Namun ICMP tidak memperbaiki error. Perbaikan error hanya dilakukan pada lapisan protokol yang lebih tinggi. Pesan error selalu di kirim ke alamat asal.

Ada 5 jenis error yang ditangani oleh ICMP, yakni :

✍✍Destination unreachable

✍✍Source Quence

✍✍Time exeeded

✍✍Parameter Problem

✍✍Redirection

query

Jenis pesan yang lain untuk ICMP adalah *query*. Dalam pesan jenis ini, node mengirim pesan yang dijawab dalam format spesifik oleh node tujuan. Jenis-jenis query pada ICMP adalah :

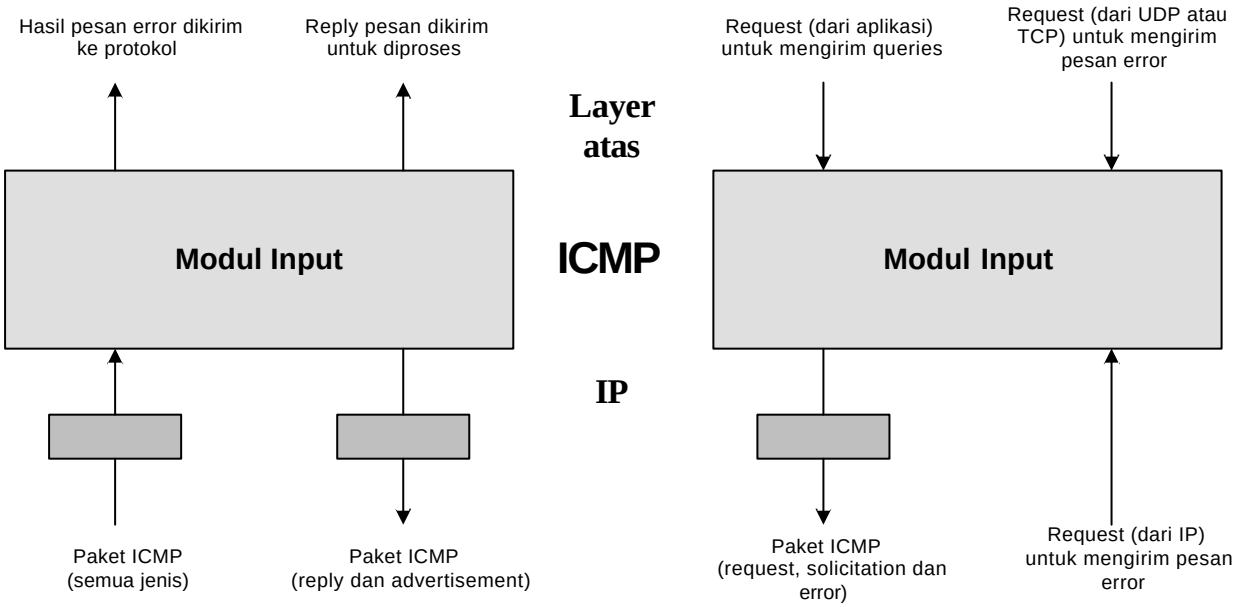
✍✍Echo request and reply

✍✍Timestamp request and reply

✍✍Address mask request and reply

✍✍Router solicitation and advertisement.

Untuk melihat disain dan komponen ICMP dapat dilihat pada Gambar 8.4.



Gambar 8.4 Disain ICMP

BAB 9

Internet Group Management Protocol (IGMP)

*multicast*ing

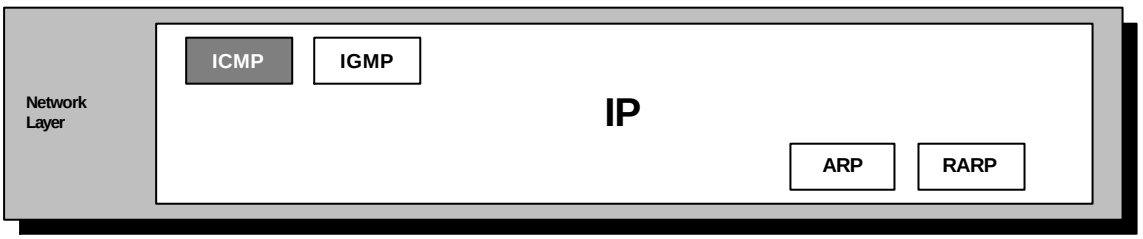
Beberapa proses kadang kala perlu mengirim pesan kepada sejumlah tujuan secara bersamaan. Ini yang disebut *multicasting*. Aplikasi daripada *multicast*ing ini misalnya pembatalan rencana perjalanan, informasi saham yang selalu berganti, belajar jarak jauh dan lain sebagainya.

Alamat *Multicast*

Seperti pada Bab terdahulu, alamat IP untuk keperluan *multicast* berada di kelas D. Dan alamat *multicast* dapat digunakan hanya sebagai alamat tujuan saja. Banyak kalangan yang menyebut alamat *multicast* sebagai *groupid*.

IGMP

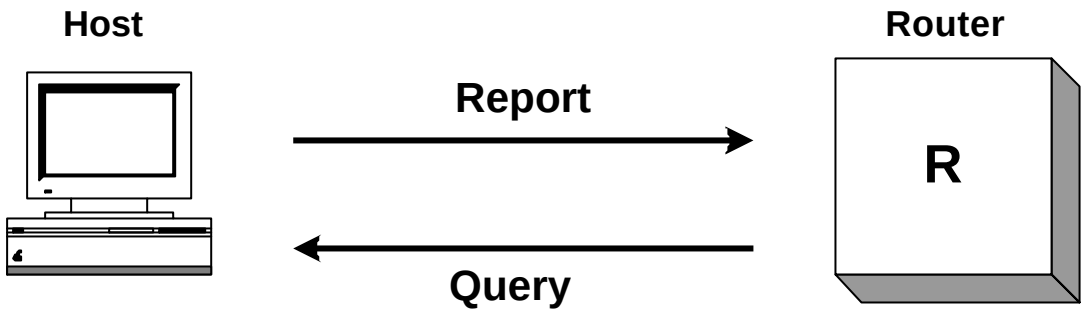
IGMP didisain untuk membantu router mengidentifikasi host-host yang berada dalam LAN yang merupakan anggota kelompok *multicast*. IGMP juga merupakan protokol yang mendukung ikut bersama protokol IP serta sama-sama berada di lapisan network / *network layer*.



Gambar 9.1 Posisi IGMP dalam lapisan network

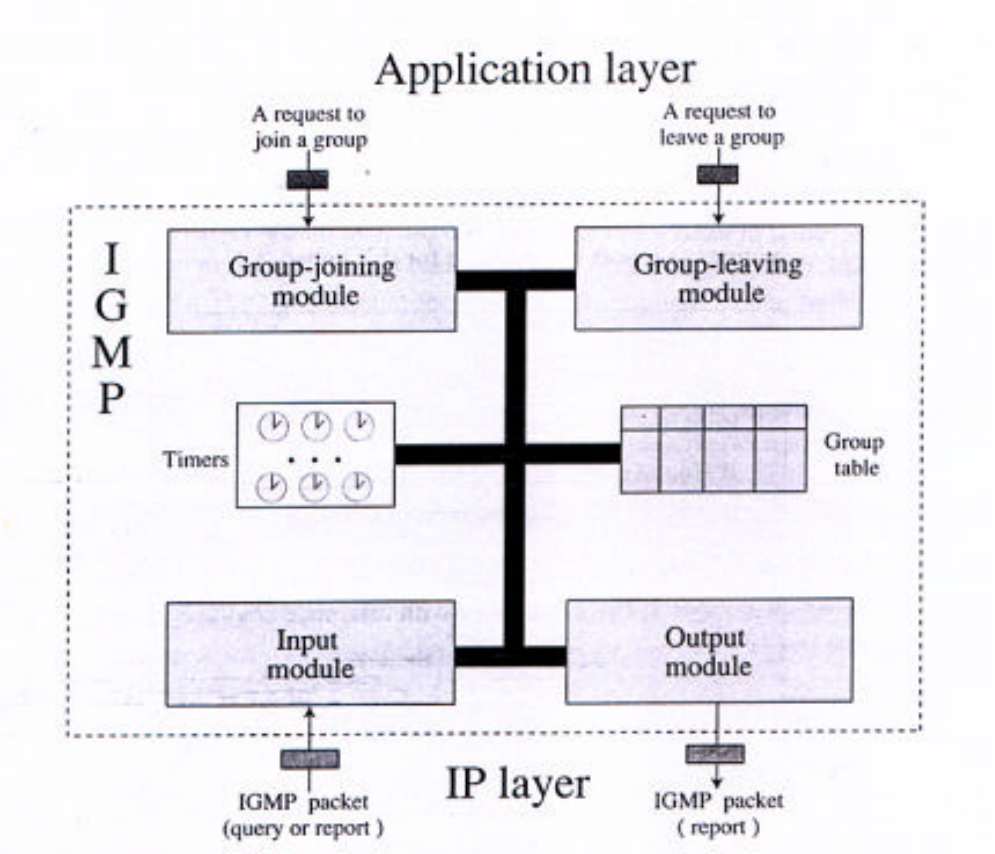
Jenis Message/Pesan

IGMP hanya mempunyai 2 jenis pesan yakni *report* dan *query*. Di mana pesan *report* dikirim dari host ke router sedangkan pesan *query* dikirim dari router ke host. Lihat Gambar 9.1.



Gambar 9.2 Pesan IGMP

Untuk melihat disain komponen IGMP lihat Gambar 9.3.

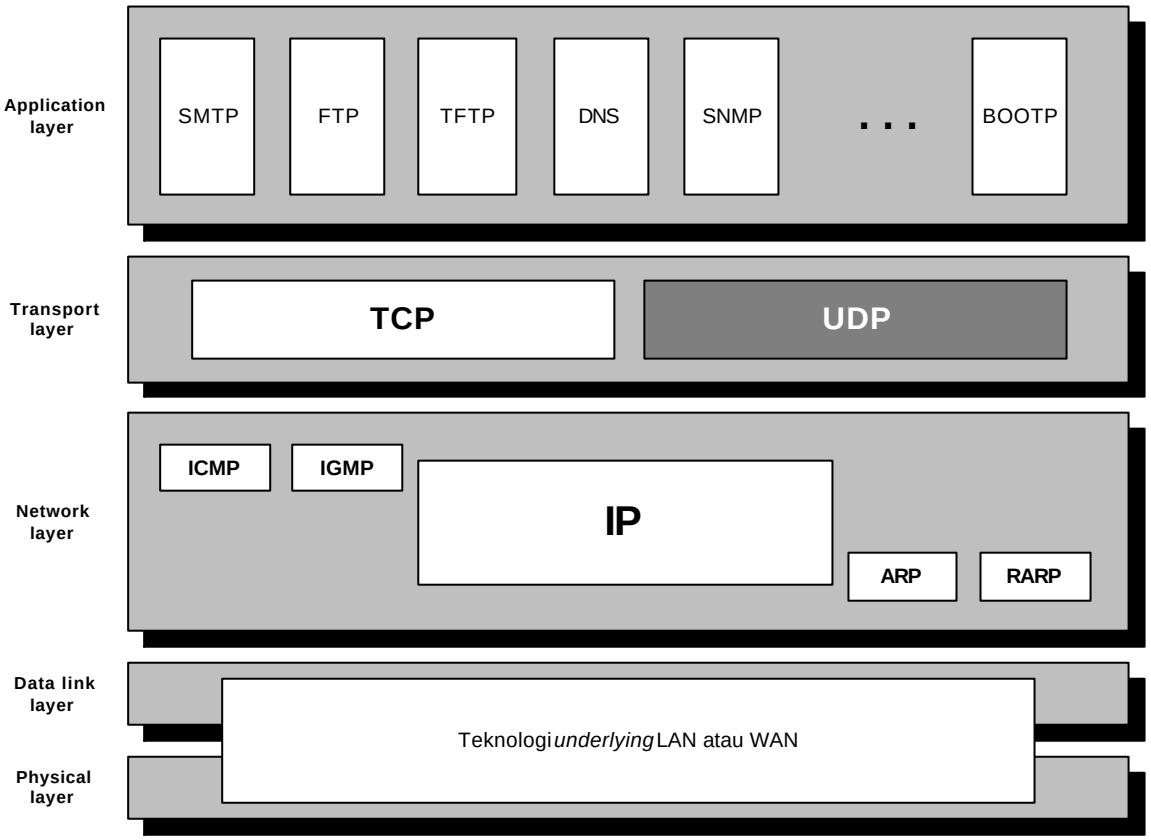


Gambar 9.3 Komponen IGMP

BAB 10

User Datagram Protocol (UDP)

Protokol TCP/IP memiliki 2 protokol pada lapisan transport, yakni UDP dan TCP. Pada bab ini kita membicarakan UDP dahulu. Gambar 10.1 mendemonstrasikan posisi UDP dalam rangkaian protokol TCP/IP.

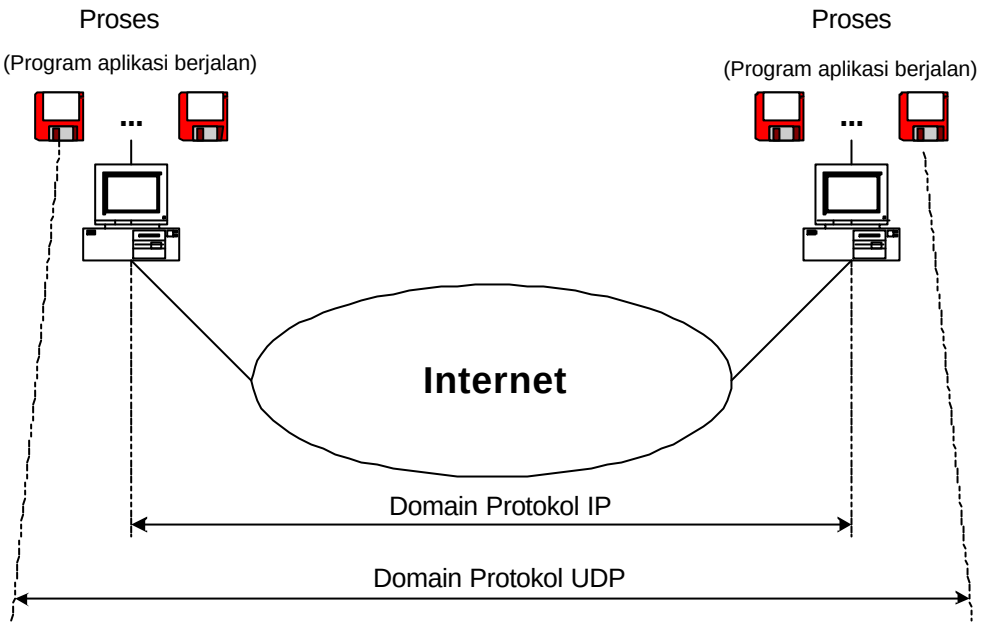


Gambar 10.1 Posisi UDP dalam Protokol TCP/IP

komunikasi process-to-process

Sbeelum mendalam membahas UDP ada baiknya memahami komunikasi host-to-host dan komunikasi process-to-process serta perbedaannya.

Protokol IP hanya bertanggung jawab membangun komunikasi antara host dengan host. Padahal setelah komunikasi ini terbentuk belumlah lengkap tanpa disertai proses yang benar. Maka pada lapisan network, *message* yang berpindah antara host ke host lain akan diproses lebih lanjut pada lapisan transport, lihat Gambar 10.2. Bentuk proses bisa saja membentuk proses *client-server*.



Gambar 10.2 UDP vs IP

Nomor Port

Proses yang terjadi pada host lokal disebut *client*, *client* ini membutuhkan layanan / *service* untuk sebuah proses pada sebuah host yang lain, host tersebut yang dimaksud adalah *server*. Proses yang dilakukan berdua oleh client dan server memiliki jenis dan proses yang bernama sama.

Sistem operasi yang sekarang digunakan sudah mendukung lingkungan yang *multiuser* dan *multiprogramming*. Tentu saja ini bisa melakukan multi proses dalam satu buah host baik itu *server* maupun *client*. Sebelum melangkah lebih jauh perlu ditentukan titik-titik komunikasi ini :

- Local host
- Local process
- Remote host
- Remote process

Local host dan *remote host* memanfaatkan alamat IP. Sedangkan untuk mendefinisikan proses, kita membutuhkan identifier khusu yang disebut, **nomor port**. Dalam protokol TCP / IP nomor port adalah berupa bilangan integer dari 0 samapai 65.535.

Protokol TCP / IP telah memutuskan untuk menetapkan penggunaan nomor port yang digunakan untuk server yang spesifik, nomor port tersebut adalah **well-known port numbers**. IANA membagi nomor port dalam 3 kelompok yakni:

- **Well-known ports** : nomor port ini bermula dari 0 sampai 1.023.
- **Registered ports** : nomor ini ini bermula dari 1.024 samapai 49.151.
- **Dynamic ports** : nomor port dimulai dari 49.152 sampai 65.535.

Well-known port untuk UDP

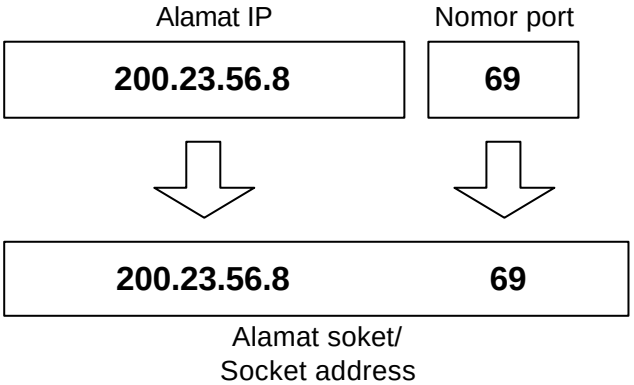
Tabel 10.1 memperlihatkan beberapa *well-known port* untuk UDP. Beberapanya lagi dapat digunakan juga bagi TCP.

Port	*Protokol*	*Penjelasan*
7	Echo	Datagram Echo yang diterima kembali ke pengirim
9	Discard	Abaikan sembarang datagram yang diterima
11	Users	User aktif
13	Daytime	Return tanggal dan waktu
17	Quote	Return kutipan hari
19	Chargen	Return sebuah string karakter
53	Nameserver	Domain name service
67	Bootps	Port server mendownload informasi bootstrap
68	Bootpc	Port client mendownload informasibottstrap
69	TFTP	Trivial File Transfer Protocol
111	RPC	Remote Procedure Call
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management Protocol
162	SNMP	Simple Network Management Protocol

Tabel 10.1 Port Well-known yang digunakan oleh UDP

Socket Address (Alamat Soket)

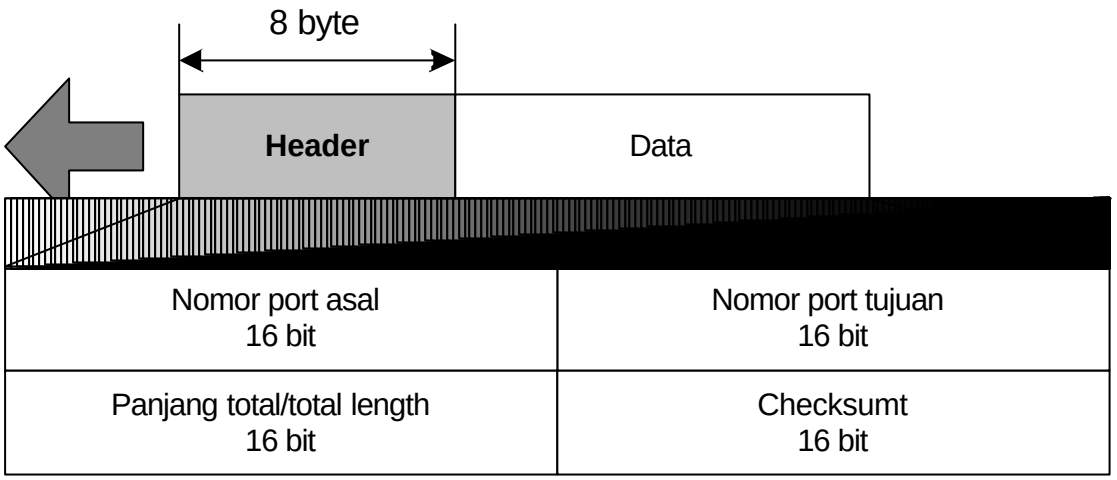
Seperti diketahui bahwa UDP membutuhkan 2 identifier, yakni alamat IP dan nomor port. Keduanya jika dikombinasikan akan membentuk **socket address**.



Gambar 10.3 Alamat soket/*socket address*

USER DATAGRAM

Paket UDP disebut user datagram. User datagram ini memiliki ukuran header yang tetap sebesar 8 byte, Gambar 10.4.



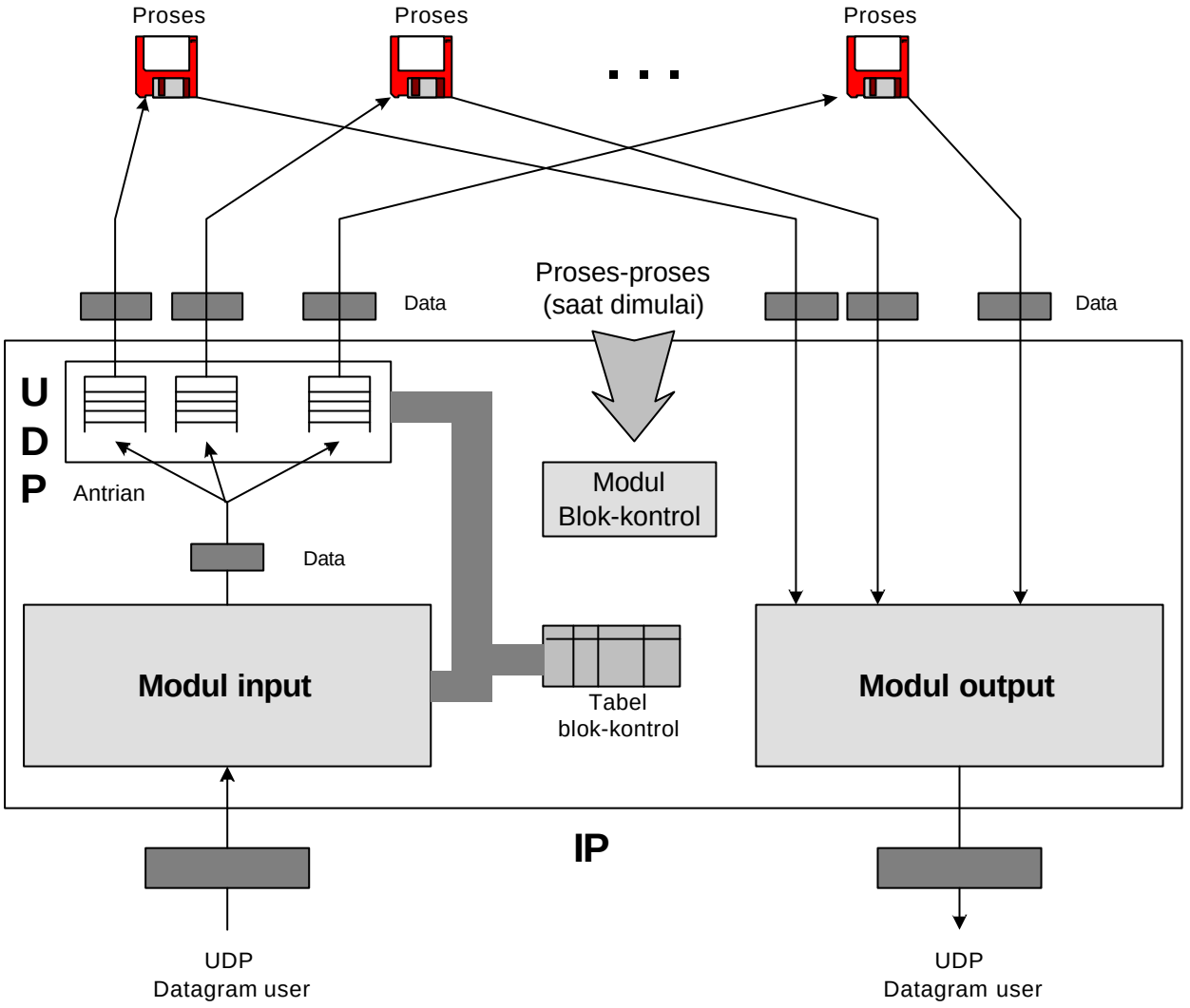
Gambar 10.4 Format datagram user (UDP)

kegunaan udp

Berikut ini kegunaan protokol UDP :

- UDP cocok untuk proses yang memerlukan request-respons communication dan sedikit sekali memperhatikan masalah *flow control* dan *error control.*
- UDP yang melakukan proses dengan mekanisme internal *flow control* dan *error control* hanya untuk proses TFTP (*Trivial File Transfer Protocol*).
- UDP cocok untuk multicasting dan broadcasting pada lapisan transport.
- UDP digunakan untuk manajemen proses seperti aplikasi SNMP.
- UDP digunakan pengupdate protokol ruting seperti pada RIP (*Routing Informastion Protocol*).

Untuk mengetahui disain yang lebih jelas perihal UDP, silakan Gambar 10.5

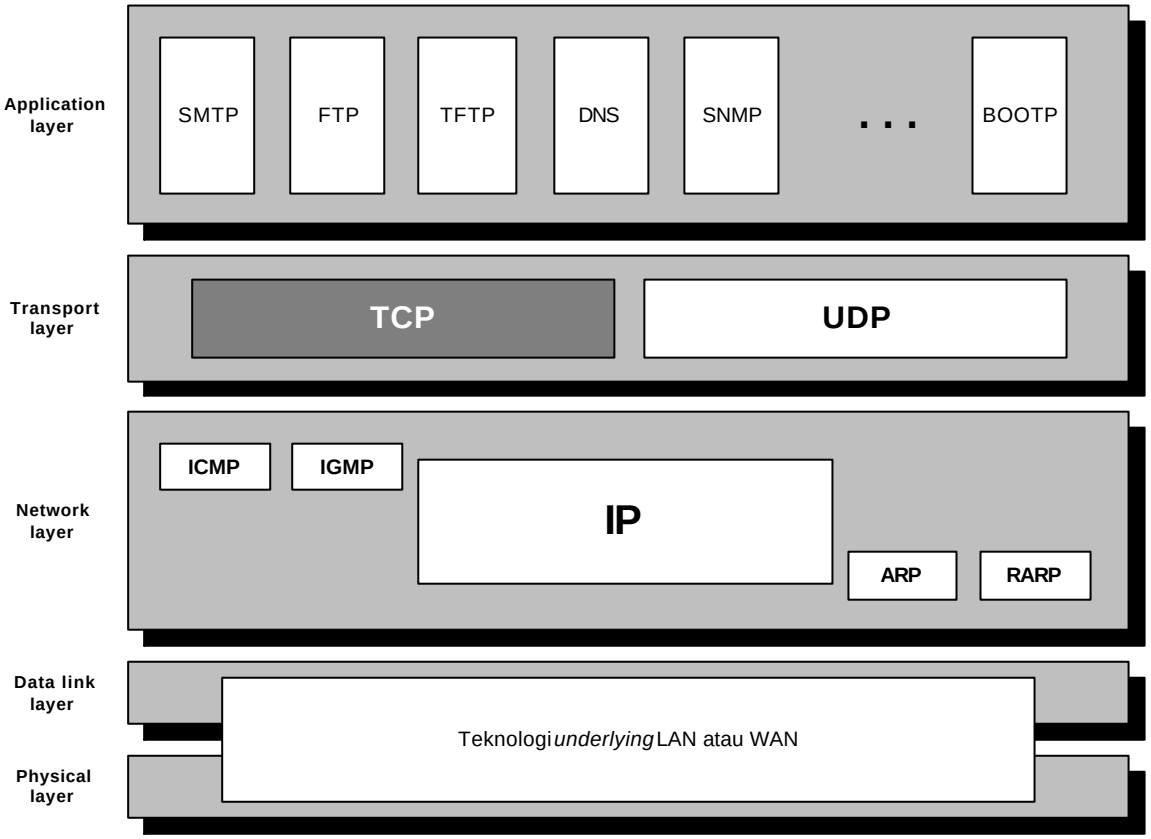


Gambar 10.5 Disain UDP

BAB 11

Transmission Control Protocol (TCP)

Gambar 11.1 memperlihatkan posisi TCP dalam protokol TCP/IP dan OSI.



Gambar 11.1 Posisi TCP dalam Protokol TCP/IP

Seperti halnya UDP, TCP melakukan *process-to-process communication.* Adapun dilihat daripada alamat port yang berkaitan dengan proses yang dilakukan oleh TCP dapat dilihat pada Tabel 11.1.

Dalam tabel tersebut terlihat bahwa alamat port yang digunakan TCP masuk dalam kategori alamat port yang disebut *Well-known port*.

Port	*Protokol*	*Penjelasan*
7	Echo	Datagram Echo yang diterima kembali ke pengirim
9	Discard	Abaikan sembarang datagram yang diterima
11	Users	User aktif
13	Daytime	Return tanggal dan waktu
17	Quote	Return kutipan hari
19	Chargen	Return sebuah string karakter
20	FTP data	File Transfer Protocol (koneksi data)
21	FTP Control	File Transfer Protokol (Koneksi kontrol)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

Tabel 11.1 Port *well-known* yang digunakan pada TCP

Layanan TCP

Stream Data Service

TCP melakukan layanan stream data pada lapisan transport. Untuk pengiriman stream, pengirim dan penerima TCP menggunakan buffer. Data yang dilalukan secara streaming itu berupa segmen-segmen.

Layanan Full-Duplex

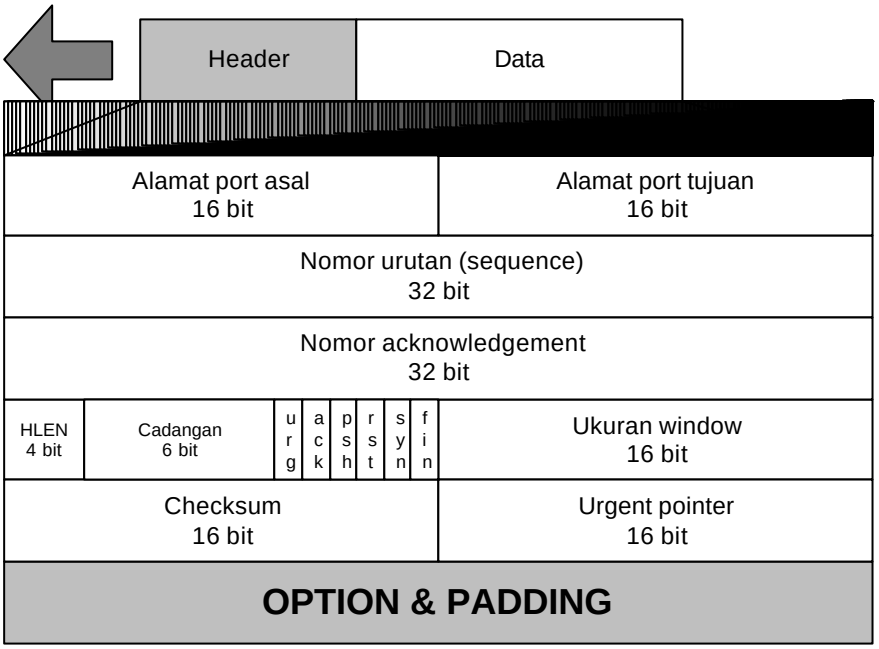
TCP memberikan juga layanan full-duplex, di mana dta dapat berpindah dalam dua arah pada saat bersamaan.

Layanan Reliabel

TCP merupakan protokol di lapisan transport yang sifatnya reliabel. Karena TCP menggunkan mekanisme acknowledgment.

SEGMEN

Unit data yang ditransfer melalui TCP disebut dengan **Segmen**. Segmen memuat 20-60 byte header. Jika tanpa option, besar header hanya 20 byte.



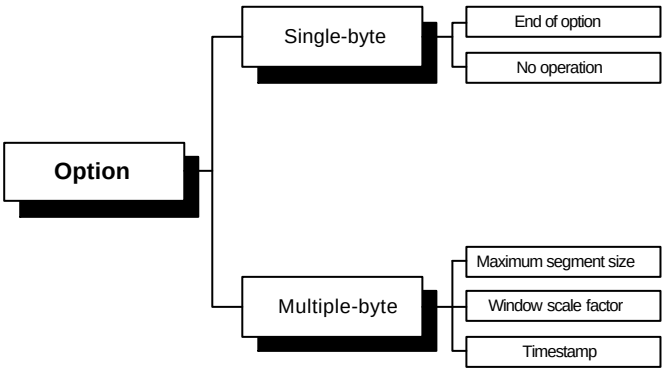
Gambar 11.2 Format segmen TCP

Flag	*Penjelasan*
URG	Nilai *urgent pointer* adalah valid
ACK	Nilai *acknowledgement* adalah valid
PSH	Push data
RST	Koneksi harus di-reset
SYN	Sinkronisasi nomor urutan (*squence*) selama koneksi terjadi
FIN	Putuskan koneksi

Tabel 11.2 Penjelasan flag dalam field kontrol

Option

Header TCP dapat bertambah besar sampai penambahan maksimal 40 byte yang disebut header option. Kategori option dapat dilihat pada Gambar 11.3.



Gambar 11.3 Option

Timer TCP

Untuk melaksanakan operasional dengan baik, TCP menggunakan 4 timer yakni :

- Retransmission
- Persistence
- Keepalive
- Time-waited

Koneksi dalam TCP

TCP adalah protokol yang berorientasi kepada konksi dalam virtual path asal dan tujuan. Jadi, seluruh segmen akan melalui virtual path.

Ada 2 prosedur dalam orientasi koneksi dalam TCP yakni :

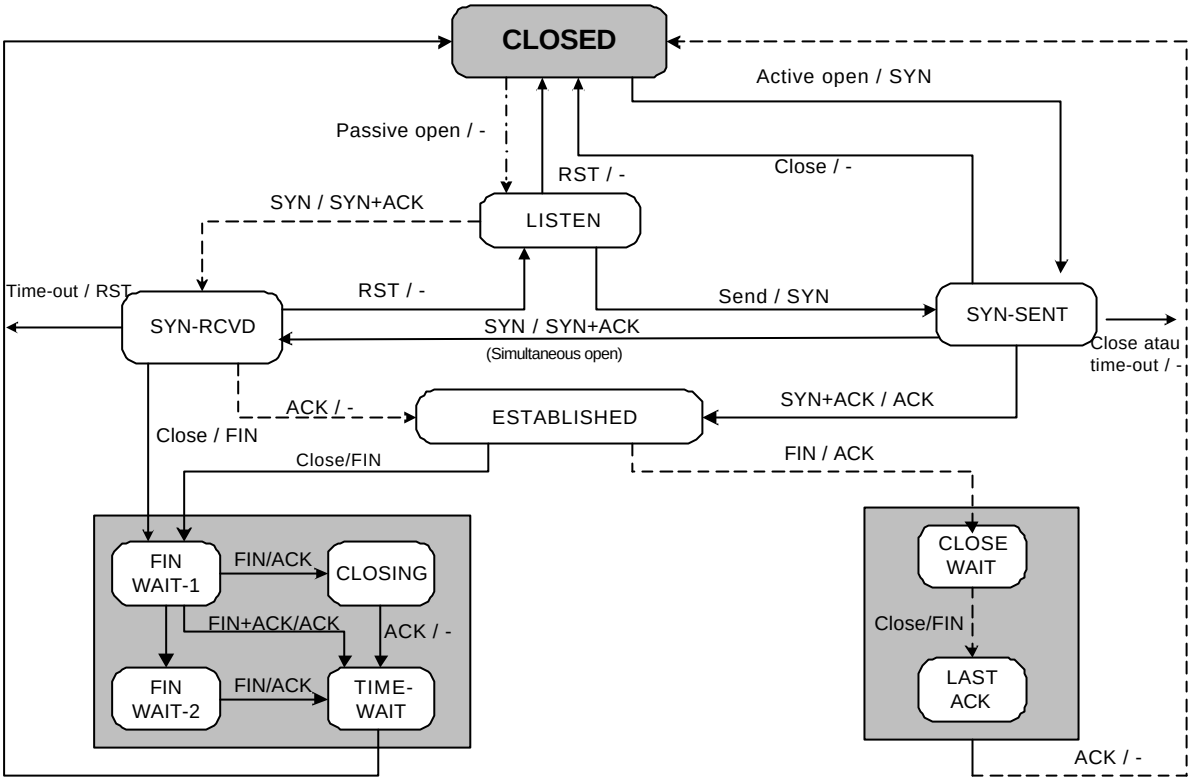
- Connection establishment
- Connection termination

State transition diagram (DIAGRAM KEADAAN TRANSISI)

Perangkat lunak TCP dibuat sebagai sebuah *finite state machine* (Keadaan batasan mesin). Maksudnya, mesin yang melakukan proses dengan TCP ini melewati sejumlah keadaan suatu proses. Tabel 11.2 dan Gambar 11.5 memperlihatkan Diagram Keadaaan Transisi.

Keadaan	*Penjelasan*
CLOSED	Tidak ada koneksi
LISTEN	Server menunggu *call* dari client
SYN-SENT	Request koneksi dikirim, menunggu ack
STN-RCVD	Request koneksi diterima
ESTABLISHED	Koneksi terjalin
FIN-WAIT-1	Aplikasi menginginkan penutupan koneksi
FIN-WAIT-2	Sisi lain menerima penutupan koneksi
CLOSING	Kedua sisi memutuskan untuk menutup koneksi bersama-sama
TIME-WAIT	Menunggu pengiriman ulang segmen2 sampai selesai
CLOSE-WAIT	Server menunggu aplikasi ditutup
LAST-ACK	Server menunggu ack terakhir

Tabel 11.2 Tabel keadaan dalam TCP



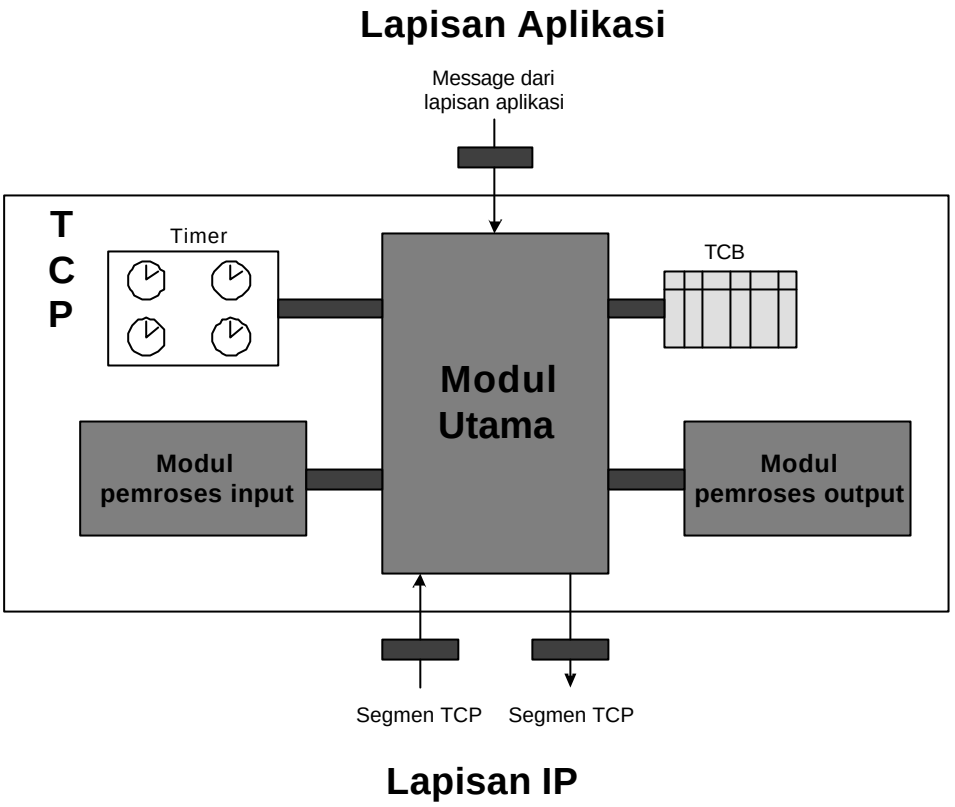
Gambar 11.5 Diagram keadaan transisi

tcp beroperasi

Beberapa poin yang didapat dalam TCP adalah melakukan operasional sbb :

- Enkapsulasi dan dekapsulasi (pembungkusan dan pembukabungkusan)
- Queuing (pengantrian)
- Multiplexing dan demultiplexing
- Pushing Data

Untuk melihat lebih jelas disain TCP dapat diperhatikan pada Gambar 11.6.



Gambar 11.6 Disain TCP

Bab 12

Protokol-protokol di lapisan ke 7

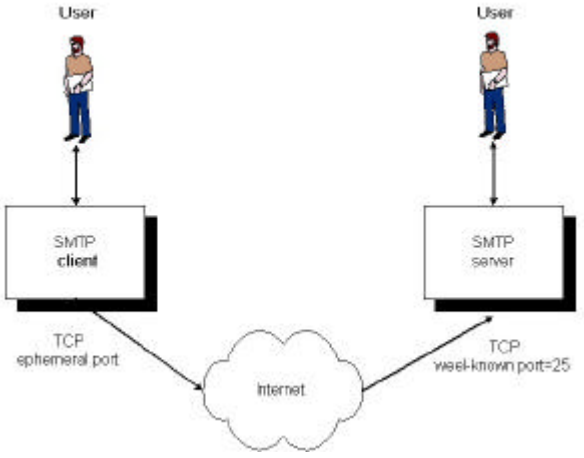
Bab ini akan menerangkan secara ringkas sekali untuk memperkenalkan protokol TCP/IP yang berada pada lapisan teratas. Untuk seterusnya kita menyebutkan sebagai protokol aplikasi. Protokol-protokol pada lapisan ini mempunyai perbedaan command syntax untuk berbagai ragam sistem operasi yang ada saat ini dan mendukung Protokol TCP/IP. Seperti Microsoft Windows 9x/2000, Linux, Unix/Solaris, Novell dan lain sebagainya. Oleh sebab itu dalam modul ini tidak dipelajari secara spesifik yang berasosiasi pada sistem operasinya. Namun sesungguhnya, protokol-protokol di lapisan 7 ini ditambah metode ruting akan diberikan dalam modul tersendiri sebagai lanjutan Protokol TCP/IP.

SMTP & POP

SMTP singkatan dari *Simple Mail Transfer Protocol.* SMTP adalah suatu protokol aplikasi yang merupakan sistem pengiriman *message*/pesan atau e-mail. SMTP dapat mendukung 3 jenis pengiriman pesan:

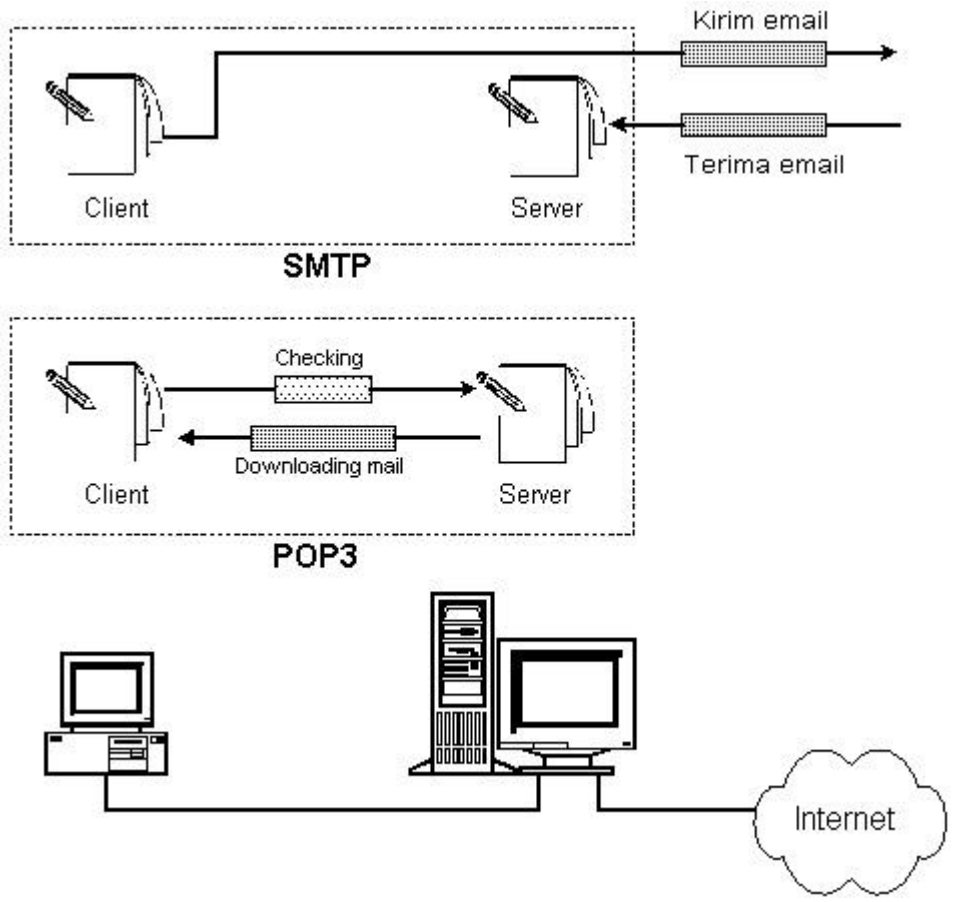
1. Pengiriman pesan saja kepada 1 atau lebih penerima.
2. Pengiriman pesan yang termasuk dalamnya teks, suara, video atau grafik.
3. Pengiriman pesan ke pengguna-pengguna yang di luar jaringan/internet.

Untuk melakukan operasinya SMTP memanfaatkan layanan protokol TCP (lapisan 4) dengan menggunakan alamat port = 25.



Gambar 12.1 Konsep SMTP

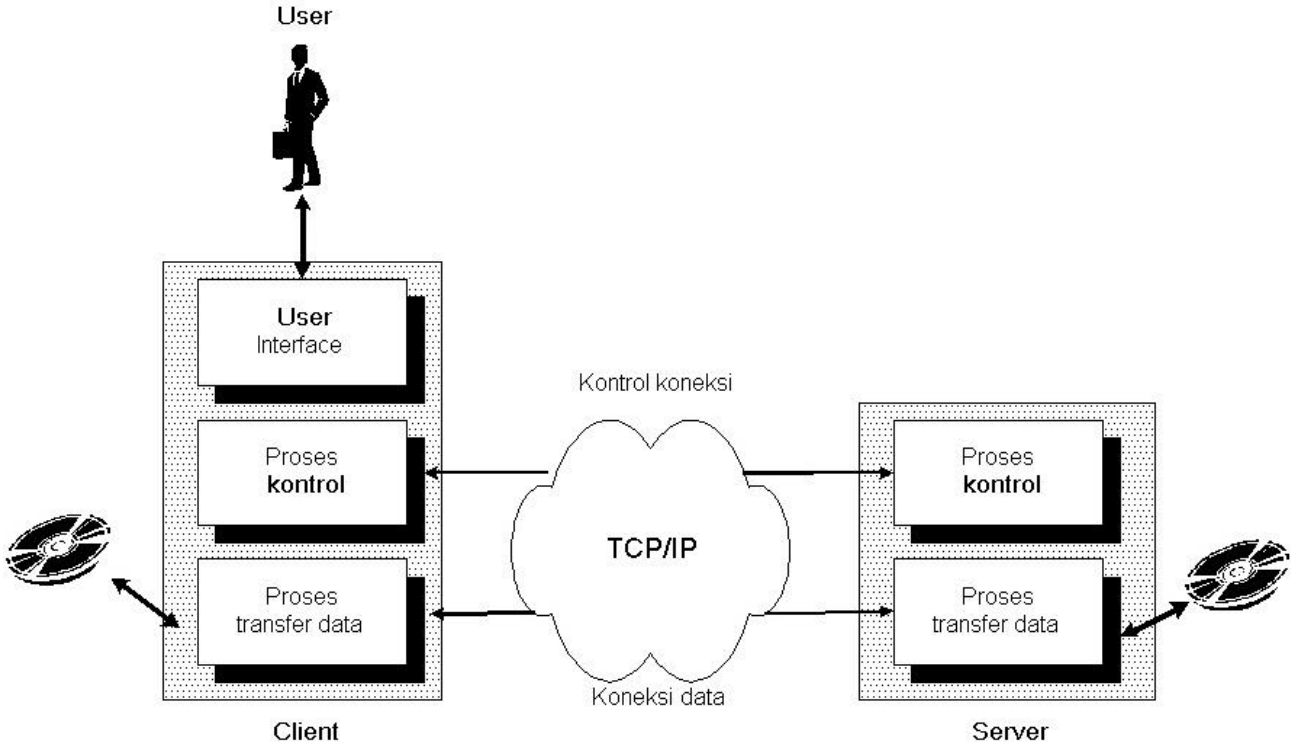
Dalam beberapa organisasi komputer, mail diterima oleh server SMTP yang selalu on-line. Server menerima email atas nama setiap nama host dalam organisasinya. Di mana workstation berinteraksi dengan host SMTP untuk "menarik" pesan dengan menggunakan protokol client-server yang disebut Post Office Protocol ver 3 (POP3). POP3 ini menggunakan alamat port = 110.



Gambar 12.2 POP3 dan SMTP

FTP

FTP singkatan dari *File Transfer Protocol*. FTP merupakan mekanisme standar yang dimiliki Protokol TCP/IP untuk keperluan penyalinan (copying) file dari satu host ke host yang lain. FTP ini memanfaatkan layanan protokol TCP (lapisan 4) untuk melakukan operasinya. Sebagai proses, FTP memanfaatkan alamat port 21 (untuk kontrol) dan 20 (untuk transfer data).



Gambar 12.3 FTP

TFTP

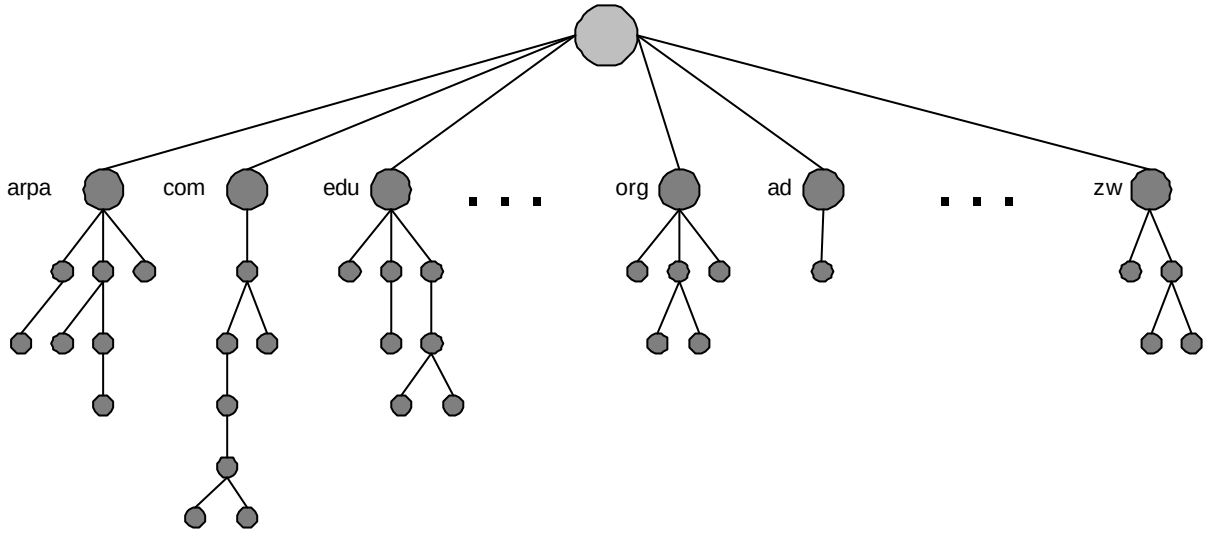
TFTP singkatan dari *Trivial File Transfer Protocol.* TFTP ini mirip dengan FTP namun banyak fungsi pada FTP yang dihilangkan untuk kegunaan booting sebuah *diskless workstation* pada jaringan lokal. Misalnya, ruter atau switch Cisco ingin melakukan bootp.

TFTP ini menggunakan layanan UDP (lapisan 4) dengan alamat port = 69.

Dalam TFTP, ada 5 jenis pesan / *message* yang dikenal, yakni : RRQ, WRQ, DATA, ACK dan ERROR.

DNS

Untuk mengidentifikasi suatu entitas, protokol TCP / IP menggunakan alamat IP. Namun apabila dalam aplikasi setiap orang harus menghafal alamat IP untuk melakukan komunikasi bisa berakibat timbulnya kesulitan untuk mengingat. Apalagi jika perkembangan internet sudah demikian pesat. Untuk itiu protokol TCP / IP memiliki suatu metode untuk membuat suatu map yang menterjemhkan nama kepada alamat IP atau sebaliknya. Metode ini disebut juga sebagai *Domain Name System* (DNS).



Gambar 12.4 Domain name system

telnet & Rlogin

TELNET Singkatan dari **TERminal NETwork**. Dalam tugas utamanya protokol TCP/IP dalam internet adalah menyediakan layanan-layanan kepada pengguna seperti layanan FTP, TFTP, SMTP dst. Namun apabila telah terjadi suatu kominkasi yang spesifik di luar standar Protokol TCP/IP seperti FTP, TFTP, SMTP, DNS, dlsb, maka TELNET & Rlogin memberikan solusi bagi pengguna untuk melakukan proses aplikasi secara client-server. TELNET & Rlogin ini juga disebut sebagai *general-purpose client/server application program*.

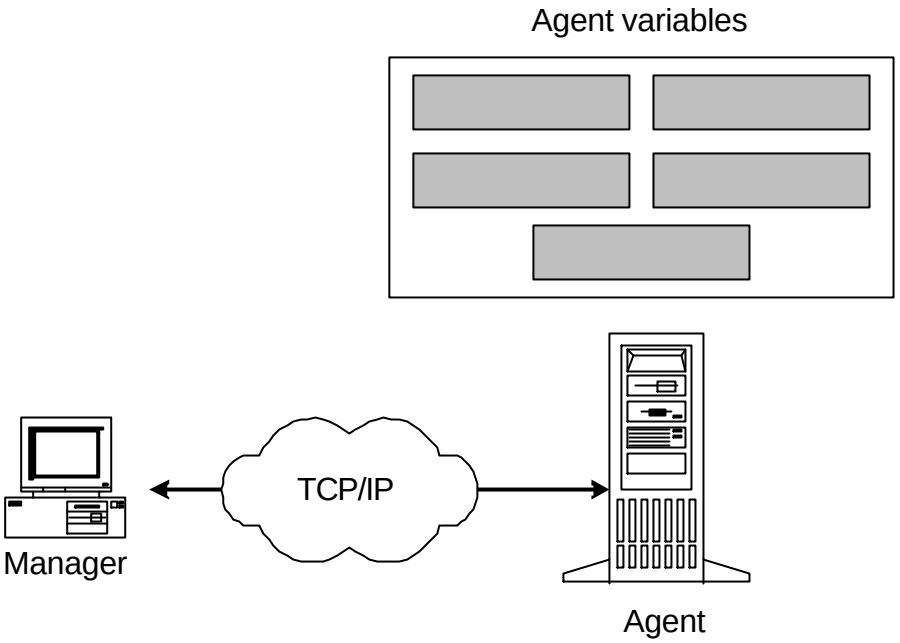
TELNET dan Rlogin dalam pengoperasiannya memanfaatkan layanan TCP (lapisan 4) dengan menggunakan alamat port 23 sedangkan Rlogin menggunakan alamat port 513.

Dalam perkembangannya, TELNET dan Rlogin dianggap rawan terhadap aspek keamanan. Namun saat ini banyak perangkat lunak yang melindunginya dengan perangkat lunka snooper. Metode lain adalah dengan melakukan proses enkripsi (pengacakan) pola data, teruatam untuk username dan password.

TELNET, kecuali Rlogin, dapat memanfaatkan authentication yang sudah dikeluarkan standarnya oleh IANA seperti Kerberos v4 atau Kerberos v5.

SNMP

SNMP singkatan dari *Simple Network Management Protocol.* SNMP menyediakan sejumlah operasi fundamental untuk memonitor dan memelihara internet yang sudah besar organisasinya dan heterogen sifatnya. Konsep SNMP adalah *manager* dan *agent*. Selain itu SNMP memiliki komponen yakni : SMI (Structure of Management Information), MIB (Management Informastion Base) dan SNMP sendiri.



Gambar 12.5 Konsep SNMP