

ARSITEKTUR PROTOKOL TCP/IP

1.	Umum.....	2
2.	Transport Control Protocol (TCP).....	6
3.	User Datagram Protocol (UDP).....	8
4.	Internet Protocol (IP).....	10
5.	Internet Control Message Protocol (ICMP).....	13
6.	Routing pada IP.....	15

ARSITEKTUR PROTOKOL TCP/IP

1. Umum

Pada dasarnya jika dua komputer akan melakukan pertukaran data/informasi memerlukan sebuah protokol yang bertugas untuk mengatur bagaimana komunikasi antar komputer tersebut. Sekelompok komputer yang terhubung satu sama lain dengan *network interface* (antar-muka jaringan) yang kemudian disebut *computer network* (jaringan komputer) dapat menggunakan banyak macam protokol, agar dua buah komputer dapat berkomunikasi maka diperlukan protokol yang sama. Protokol berfungsi mirip bahasa manusia, dimana untuk dapat berbicara dan mengerti satu sama lain diperlukan bahasa yang sama.

TCP/IP Suite (*Transport Control Protocol/Internet Protocol*) merupakan sekelompok protokol yang mengatur komunikasi data komputer dan memungkinkan komputer berbagai jenis dan berbagai *vendor* serta berbeda sistem operasi untuk berkomunikasi bersama dengan baik. TCP/IP ini dikembangkan pertama kali oleh lembaga riset Departemen Pertahanan Amerika, DARPA (*Defense Advance Research Project Agency*) pada akhir 1960-an dengan berlanjut pada keberhasilan ARPANET pada tahun 1972. Pada tahun 1982 DARPA mendanai pembuatan protokol komunikasi yang lebih umum yang kemudian dinamakan TCP/IP. Berikutnya pada tahun 1986 lembaga ilmu pengetahuan nasional Amerika Serikat U.S. *National Science Foundation* (NSF) mendanai pembuatan jaringan TCP/IP yang dinamai NSFNET, jaringan inilah yang menjadi embrio berkembangnya Internet. Perkembangan pun tidak berhenti begitu saja dan terus berlanjut pada tahun-tahun berikutnya. Hingga akhirnya pada awal tahun 1990-an TCP/IP menjadi protokol yang paling banyak dan luas digunakan. Dengan perkembangan dan fungsi yang sedemikian kemudian TCP/IP digunakan secara luas dalam dunia Internet yang sekarang ini telah kita gunakan bersama.

Perkembangan TCP/IP yang cepat dan diterima secara luas tidak hanya dikarenakan rekomendasi DARPA, melainkan fitur-fitur penting yang ada pada TCP/IP, diantaranya:

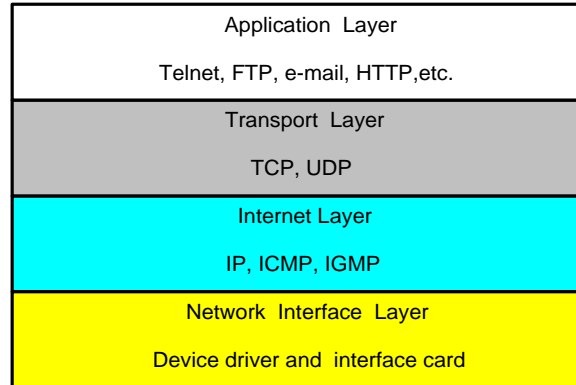
- TCP/IP dikembangkan menggunakan standar protokol yang terbuka. Tersedia secara bebas dan dikembangkan tanpa bergantung pada perangkat keras ataupun sistem operasi tertentu.
- Tidak tergantung pada spesifik perangkat jaringan tertentu. Hal ini memungkinkan TCP/IP untuk mengintegrasikan berbagai macam jaringan.
- TCP/IP menggunakan pengalamatan yang unik dalam skala global. Dengan demikian memungkinkan komputer dapat saling berhubungan walaupun jaringannya seluas Internet sekarang ini.
- Standarisasi protokol TCP/IP dilakukan secara konsisten dan tersedia secara luas untuk siapapun tanpa biaya. Hal ini diwujudkan dalam RFC (Request For Comment).

TCP/IP terdiri atas sekumpulan protokol yang masing-masing bertanggung jawab atas bagian-bagian tertentu dalam komunikasi data dan didesain untuk melakukan fungsi-fungsi komunikasi data pada LAN (*Local Area Network*) maupun WAN (*Wide Area Network*). Dengan prinsip pembagian tersebut TCP/IP menjadi protokol komunikasi data yang fleksibel dan dapat diterapkan dengan mudah di setiap jenis komputer dan antar-muka jaringan, karena sebagian besar isi kumpulan protokol ini tidak spesifik terhadap satu komputer atau peralatan jaringan tertentu. Agar TCP/IP dapat berjalan pada antar-muka jaringan tertentu, hanya diperlukan perubahan pada bagian protokol yang berhubungan dengan antar-muka jaringan saja.

Sekumpulan protokol TCP/IP ini dimodelkan dalam empat lapisan/layer yang bertingkat. Keempat layer tersebut ialah:

1. *Application Layer*, merupakan layer program aplikasi yang menggunakan protokol TCP/IP. Beberapa diantaranya adalah: Telnet, FTP (*File Transfer Protocol*), SMTP (*Simple Mail Transport Protocol*), SNMP (*Simple Network Management Protocol*), HTTP (*Hypertext Transfer Protocol*).
2. *Transport Layer*, berisi protokol yang bertanggung jawab untuk mengadakan komunikasi antar dua komputer. Pada layer ini terdiri atas dua protokol, yaitu: TCP (*Transport Control Protocol*) dan UDP (*User Datagram Protocol*).
3. *Internet Layer*, berfungsi untuk menangani pergerakan paket data dalam jaringan dari komputer pengirim ke komputer tujuan. Protokol yang berada dalam fungsi ini antara lain: IP (*Internet Protocol*), ICMP (*Internet Control Message Protocol*), dan IGMP (*Internet Group Management Protocol*).
4. *Network Layer*, merupakan layer paling bawah yang bertanggung jawab mengirim dan menerima data dari dan ke media fisik.

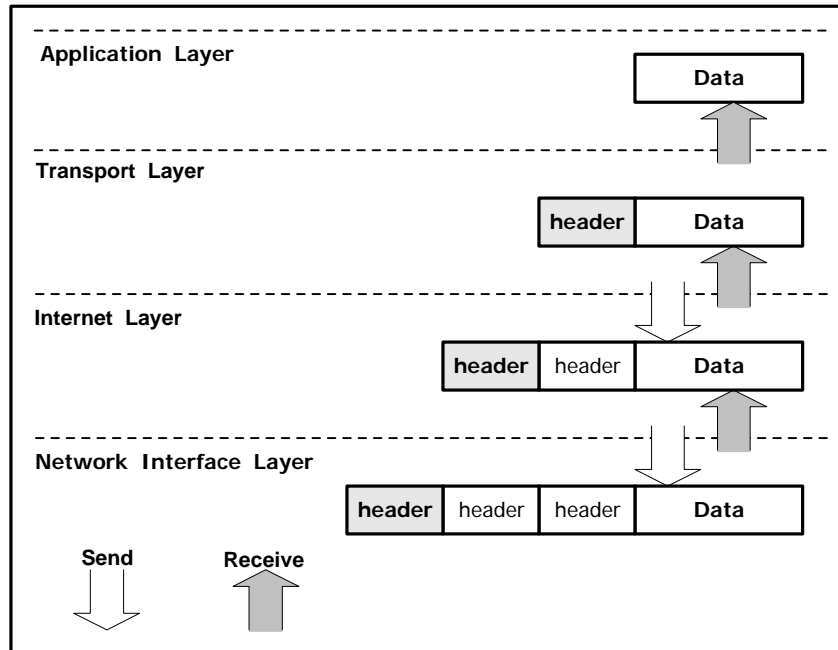
Model sekumpulan protokol TCP/IP tersebut dapat digambarkan sebagaimana terlihat pada gambar 1.1.



Gambar 1.1. Layer pada TCP/IP
(Sumber: W. Richard Steven. 1994: 2)

Pada TCP/IP terjadi penyampaian data dari protokol di satu layer ke protokol di layer lain. Setiap layer memiliki struktur data yang tidak saling bergantung. Secara konseptual sebuah layer tidak memperhatikan struktur data yang digunakan oleh layer-layer di atas dan di bawahnya. Pada kenyataannya struktur data didesain untuk kompatibel antar layer dengan tujuan efisiensi transmisi data. Setiap protokol pada masing-masing layer memperlakukan semua informasi yang diterimanya dari protokol lain sebagai data.

Setiap protokol pada masing-masing layer akan menambahkan informasi tambahan miliknya pada data, jika protokol tersebut menerima data dari protokol lain di layer atasnya. Tambahan informasi tersebut disebut *header*, yang berfungsi sebagai kontrol informasi protokol tersebut. Proses penambahan informasi tersebut dinamakan *encapsulation*. Proses tersebut ditunjukkan pada gambar 1.2. Proses sebaliknya akan terjadi jika sebuah protokol menerima data dari protokol lain pada layer di bawahnya. Jika data tersebut dianggap benar, protokol tersebut akan membuang *header*-nya dan meneruskan data tersebut ke protokol lain di layer atasnya.



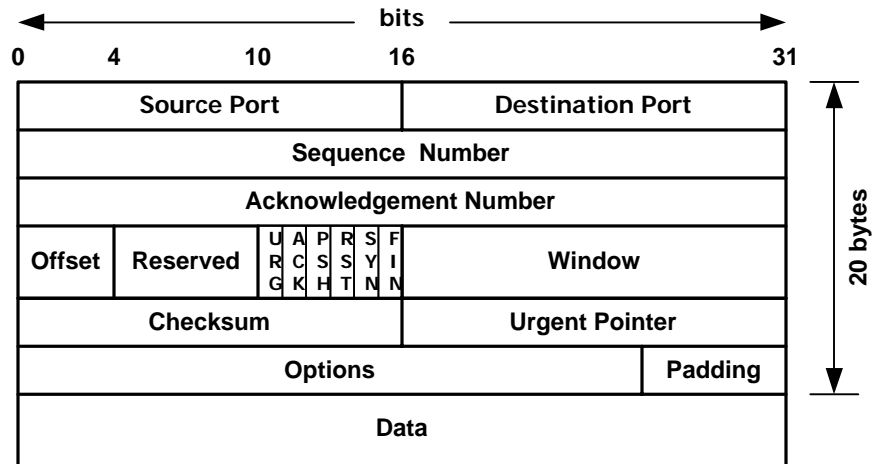
Gambar1.2. Pergerakan data dalam layer TCP/IP
(Sumber: Craig Hunt. 1992: 10)

2. Transport Control Protocol (TCP)

TCP (Transport Control Protocol) merupakan protokol yang berada pada layer *transport* dari layer TCP/IP. TCP adalah protokol yang bersifat *byte stream*, *connection-oriented* dan *reliable* dalam pengiriman data. TCP menggunakan komunikasi *byte-stream*, yang berarti bahwa data dinyatakan sebagai suatu urutan-urutan byte. *Connection-oriented* berarti sebelum terjadi proses pertukaran data antar komputer terlebih dahulu harus dibentuk suatu hubungan. Hal ini dapat dianalogikan dengan proses pendialan nomor telepon dan akhirnya terbentuk suatu hubungan.

Keandalan TCP dalam mengirim data didukung oleh mekanisme yang disebut *Positive Acknowledgement with Re-transmission* (PAR) [Craig Hunt. 1992: 20]. Data yang dikirim dari layer aplikasi akan dipecah-pecah dalam bagian-bagian yang lebih kecil dan diberi nomor urut (*sequence number*) sebelum dikirimkan ke layer berikutnya. Unit data yang sudah dipecah-pecah tadi disebut segmen (*segment*). TCP selalu meminta konfirmasi setiap kali selesai mengirimkan data, apakah data tersebut sampai pada komputer tujuan dan tidak rusak. Jika data berhasil sampai mencapai tujuan, TCP akan mengirimkan data urutan berikutnya. Jika tidak berhasil,

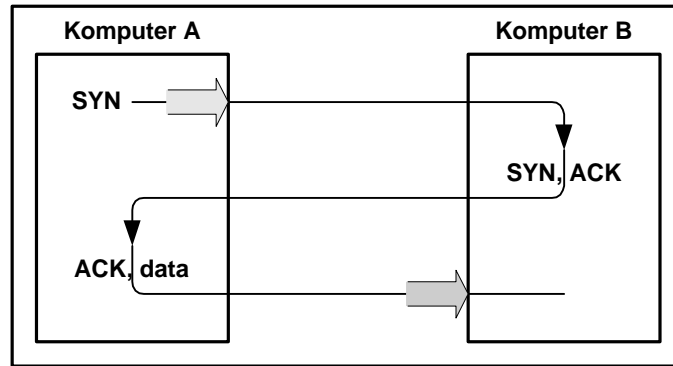
maka TCP akan melakukan pengiriman ulang urutan data yang hilang atau rusak tersebut. Dalam kenyataannya TCP menggunakan sebuah *acknowledgement* (ACK) sebagai suatu pemberitahuan antara komputer pengirim dan penerima. Format segmen TCP diperlihatkan pada gambar 2.1.



Gambar 2.1. Format *header* TCP
(Sumber: Steven, W. Richard. 1994: 225)

Data yang diterima pada sisi penerima akan disusun berdasarkan nomor urut yang diberikan oleh sisi pengirim. Untuk mengatasi kerusakan data yang diterima, TCP menggunakan sebuah *checksum* untuk memastikan bahwa data tersebut tidak rusak.

Model komunikasi dua arah antara komputer sisi kirim dan sisi terima sebelum terjadi proses pengiriman data disebut *handshake*. Tipe *handshake* yang digunakan TCP adalah *three-way handshake*, karena menggunakan tiga segmen. Tujuan *three-way handshake* ini adalah untuk pembentukan koneksi, sinkronisasi segmen, dan pemberitahuan besar data yang bisa diterima pada suatu saat antara sisi kirim dan sisi terima. Proses sederhana *three-way handshake* tersebut dapat ditunjukkan pada gambar 2.2.



Gambar 2.2. Three-way Handshake

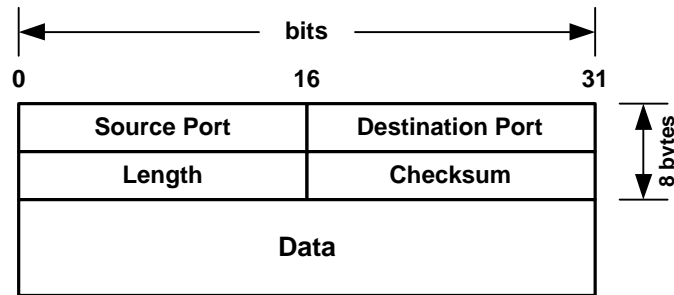
(Sumber: Craig Hunt. 1992: 21)

Komputer A memulai hubungan dengan mengirimkan segmen sinkronisasi nomor urut (SYN) pada komputer B. Segmen tersebut merupakan pemberitahuan pada komputer B bahwa komputer A ingin melakukan sebuah hubungan dan menanyakan nomor urut berapa yang akan digunakan sebagai awal urutan segmen yang akan dikirim. (Nomor urut tersebut digunakan agar data tetap berada pada urutan yang benar). Komputer B memberikan respon pada komputer A dengan sebuah segmen yang memberikan ACK dan SYN. Dengan demikian komputer A akan tahu informasi nomor urut yang digunakan untuk komputer B. Akhirnya, komputer A pun mengirimkan sebuah segmen sebagai balasan dari segmen yang dikirim komputer B, sekaligus melakukan pengiriman data yang sebenarnya pertama kali. Setelah terjadi proses tersebut komputer A mendapati bahwa komputer B siap menerima data dan segera setelah hubungan dipastikan dapat terjadi data pun dikirim sepenuhnya ke komputer B. Pada saat seluruh data telah selesai dikirim, proses *three-way handshake* untuk mengakhiri hubungan pun terjadi untuk memastikan bahwa tidak ada lagi data yang dikirim.

3. User Datagram Protocol (UDP)

UDP (*User Datagram Protocol*) merupakan protokol yang juga berada pada layer *transport* selain TCP. Protokol ini bersifat *connectionless* dan *unreliable* dalam pengiriman data. *Connectionless* berarti tidak diperlukannya suatu bentuk hubungan terlebih dahulu untuk mengirimkan data. *Unreliable* berarti pada protokol ini data tidak dijamin akan sampai pada

tujuan yang benar dan dalam kondisi yang benar pula. Keandalan pengiriman data pada protokol ini menjadi tanggung jawab dari program aplikasi pada layer di atasnya. Gambar 3.1. menunjukkan format *header* UDP.



Gambar 3.1. Format Header UDP
(Sumber: Steven, W. Richard. 1994: 144)

Jika dibandingkan dengan TCP, UDP adalah protokol yang lebih sederhana dikarenakan proses yang ada di dalamnya lebih sedikit. Dengan demikian aplikasi yang memanfaatkan UDP sebagai protokol transport dapat mengirimkan data tanpa melalui proses pembentukan koneksi terlebih dulu. Hal ini pun terjadi pada saat mengakhiri suatu koneksi, sehingga dalam banyak hal proses yang terjadi sangatlah sederhana dibanding jika mengirimkan data melalui protokol TCP. Secara teknis protokol UDP memiliki header yang lebih kecil dibanding protokol TCP seperti terlihat pada format header masing-masing.

Bila suatu program aplikasi memanfaatkan protokol UDP untuk mengirimkan informasi, protokol UDP melakukan fungsi multiplexing/demultiplexing seperti yang dilakukan protokol TCP dengan menentukan nomor port pengirim (*source port*) dan nomor port penerima (*destination port*), kemudian menambahkan sedikit fungsi koreksi kesalahan lalu meneruskan segmen yang terbentuk ke protokol layer Internet. Pada layer internet segmen tersebut ditambahi informasi dalam bentuk datagram IP dan kemudian ditentukan cara terbaik untuk mengantarkan segmen tersebut ke sisi penerima. Jika segmen tersebut tiba pada sisi penerima, protokol UDP menggunakan nomor port informasi IP pengirim dan penerima untuk mengantarkan data dalam segmen ke proses program aplikasi yang sesuai.

Beberapa hal yang harus diperhatikan jika suatu program aplikasi akan menggunakan protokol UDP sebagai protokol transport:

- Tidak ada pembentukan koneksi. Protokol UDP hanya mengirim informasi begitu saja tanpa melakukan proses awal sebelumnya.
- Tidak ada pengkondisian koneksi. Protokol UDP tidak melakukan penentuan kondisi koneksi yang berupa parameter-parameter seperti buffer kirim dan terima, kontrol kemacetan, nomor urutan segmen dan *acknowledgement*.
- Memiliki header yang kecil. Protokol UDP memiliki 8 byte header dibanding 20 byte header pada TCP.
- Tidak ada pengaturan laju pengiriman data. Protokol UDP hanya menekankan kecepatan kirim pada laju program aplikasi dalam menghasilkan data, kemampuan sumber kirim data (berdasarkan CPU, laju pewaktuan, dll) dan *bandwidth* akses menuju Internet. Jika terjadi kemacetan jaringan sisi penerima tidak perlu menerima seluruh data yang dikirim. Dengan demikian laju penerimaan data dibatasi oleh faktor kemacetan jaringan yang terjadi walaupun pada sisi kirim tidak memperhatikannya.

Protokol UDP lebih sering diimplementasikan untuk aplikasi-aplikasi yang mengarah proses *real-time* seperti aplikasi multimedia, dimana rugi-rugi paket data yang kecil lebih ditoleransi daripada nilai *delay* yang terjadi [Keith W. Ross and Jim Kurose: 1996].

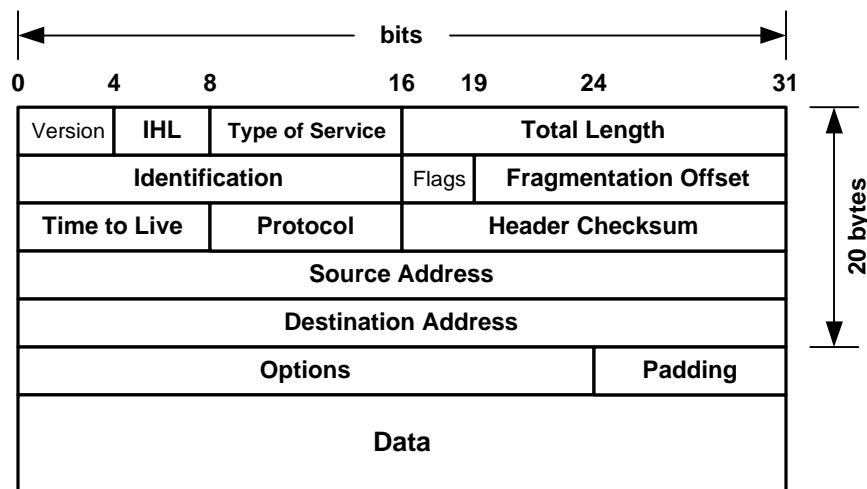
4. Internet Protocol (IP)

IP (*Internet Protocol*) merupakan protokol yang paling penting yang berada pada layer *Internet* TCP/IP. Semua protokol TCP/IP yang berasal dari layer atasnya mengirimkan data melalui protokol IP ini. Seluruh data harus dilewatkan, diolah oleh protokol IP dan dikirimkan sebagai datagram IP untuk sampai ke sisi penerima. Dalam melakukan pengiriman data, protokol IP ini bersifat *unreliable*, *connectionless* dan *datagram delivery service*.

Unreliable berarti protokol IP tidak menjamin datagram yang dikirim pasti sampai ke tujuan. Protokol IP hanya melakukan cara terbaik untuk menyampaikan datagram yang dikirim ke

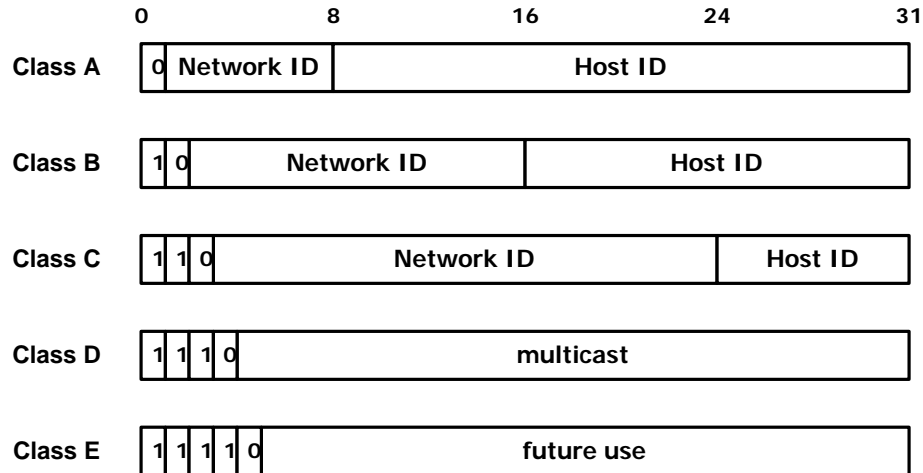
tujuan. Jika pada perjalanan datagram tersebut terjadi hal-hal yang tidak diinginkan (putusnya jalur, kemacetan, atau sisi penerima yang dituju sedang mati), protokol IP hanya memberikan pemberitahuan pada sisi kirim kalau telah terjadi permasalahan pengiriman data ke tujuan melalui protokol ICMP. *Connectionless* berarti tidak melakukan pertukaran kontrol informasi (*handshake*) untuk membentuk koneksi sebelum mengirimkan data.

Datagram delivery service berarti setiap datagram yang dikirim tidak tergantung pada datagram lainnya. Akibatnya jalur yang ditempuh oleh masing-masing datagram IP ke tujuan bisa berbeda satu sama lainnya. Dengan demikian kedatangan datagram pun bisa jadi tidak berurutan. Metode ini dipakai untuk menjamin sampainya datagram ke tujuannya walaupun salah satu jalur menuju ke tujuan mengalami masalah.



Gambar 4.1. Format datagram IP
(Sumber: Steven, W. Richard. 1994: 34)

Pada bagian header dari protokol IP seperti terlihat pada gambar 4.1 terdapat bagian pengalamatan sumber kirim dan tujuan masing-masing sebesar 32-bit. Pengalamatan (IP *addressing*) adalah bagian yang terpenting dalam jaringan TCP/IP. Alamat inilah yang sering dinamakan sebagai alamat Internet yang harus dimiliki setiap node yang terhubung dalam jaringan Internet. Format IP *address* yang dinyatakan dalam bilangan 32-bit dimana tiap 8 bitnya dipisahkan oleh tanda titik. Untuk memudahkan distribusinya, IP *address* dibagi dalam kelas-kelas. Pembagian kelas dalam IP *address* diperlihatkan pada gambar 4.2.



Gambar 4.2. Format pembagian kelas IP Address

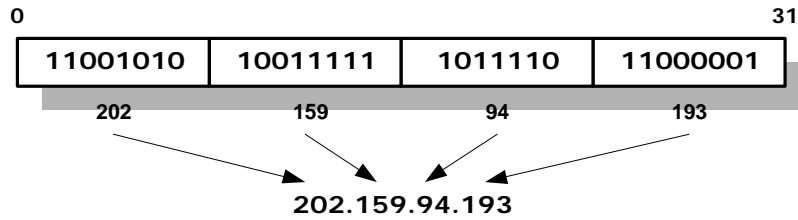
(Sumber: Steven, W. Richard. 1994: 8)

Tabel 4.1. Pembagian IP address dalam format bilangan desimal

(Sumber: Steven, W. Richard. 1994: 8)

Kelas	Alokasi
A	0.0.0.0 – 127.255.255.255
B	128.0.0.0 – 191.255.255.255
C	192.0.0.0 – 223.255.255.255
D	224.0.0.0 – 239.255.255.255
E	240.0.0.0 – 247.255.255.255

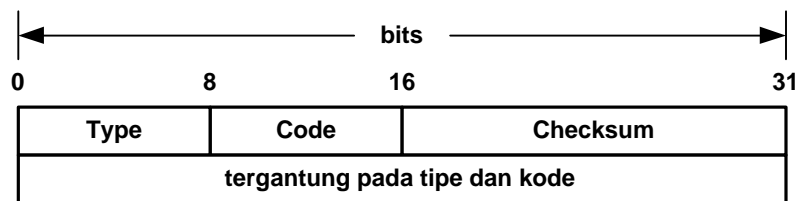
Pembagian tersebut di atas didasarkan pada dua hal, yakni: *Network ID* dan *Host ID* dari suatu *IP address*. *Network ID* adalah bagian dari *IP address* yang digunakan untuk menunjukkan jaringan tempat komputer itu berada. *Host ID* adalah bagian dari *IP address* yang digunakan untuk menunjukkan *host*/komputer itu sendiri. Pada satu jaringan, *host ID* ini harus unik (tidak boleh ada yang sama). Format *IP address* yang dinyatakan dalam bentuk biner kemudian ditulis sebagai 4 bilangan desimal yang masing-masing dipisahkan tanda titik. Format seperti ini disebut *dotted-decimal notation*. Setiap bilangan desimal tersebut merupakan nilai dari 8 bit *IP address* seperti terlihat pada gambar 4.3.



Gambar 4.3. Notasi desimal bertitik dari IP address

5. Internet Control Message Protocol (ICMP)

ICMP (*Internet Control Message Protocol*) merupakan bagian dari layer IP, dimana protokol ini bertugas mengirimkan pesan-pesan kesalahan atau kondisi lain yang memerlukan perhatian khusus. Pesan ICMP ini akan dikirim jika terjadi masalah layer IP dan layer atasnya (TCP atau UDP). Gambar 5.1 menunjukkan format dari sebuah pesan ICMP.



Gambar 5.1. Format Pesan ICMP
(Sumber: Steven, W. Richard. 1994: 70)

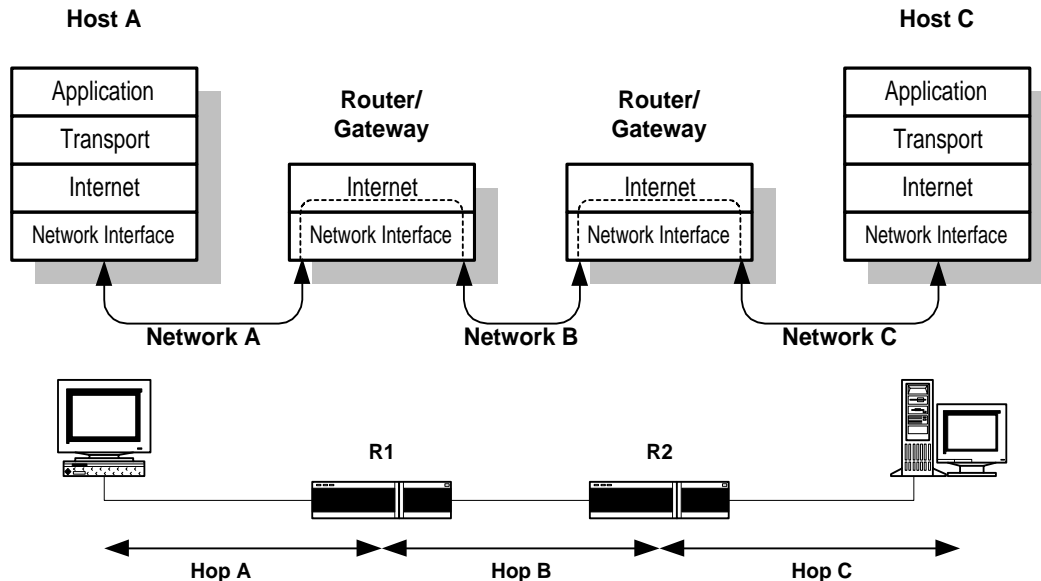
Pesan ICMP tersebut ditentukan dari kombinasi tipe dan kodenya. Pesan kesalahan yang mungkin dikirimkan dengan ICMP diantaranya adalah:

- *Destination unreachable*. Pesan ini dikirim oleh *router* jika pengiriman paket data mengalami kegagalan akibat masalah putusnya jalur, baik secara fisik maupun logik.
- *Time exceeded*. Pesan ini dikirim oleh *router* jika batas waktu (*life-time*) sebuah paket data dalam jaringan sudah habis. Hal ini dapat terjadi jika sampai batas waktu yang ditentukan paket data tersebut belum dapat mencapai alamat tujuannya.
- *Parameter problem*. Pesan ini dikirim jika terdapat kesalahan parameter pada *header* datagram IP.
- *Source Quench*. Pesan ICMP ini dikirim jika *router* atau tujuan mengalami kemacetan/kongesti proses dan sebagai respon balik atas pesan ini pada sisi pengirim paket data harus memperlambat pengiriman paket datanya.
- *Redirect*. Pesan yang dikirim jika pada *router* merasa pengirim melewati data pada *router* yang salah, sehingga harusnya dikirimkan melalui *router* lain.
- *Echo* dan *Echo reply*. Merupakan pesan yang menyediakan mekanisme pengujian keaktifan alamat pengirim dan alamat tujuan.
- *Timestamp* dan *Timestamp-reply*. Menyediakan mekanisme untuk mengetahui informasi waktu yang diperlukan sistem tujuan untuk memproses suatu paket data.
- *Address mask request* dan *address mask reply*. Untuk mengetahui pengalamatan yang harus digunakan oleh *host*/komputer dalam suatu alamat jaringan.

IP tidak didesain dengan keandalan pengiriman data yang mutlak. Tujuan dari ICMP ini adalah untuk memberikan pesan balik terhadap permasalahan yang terjadi dalam jaringan komunikasi IP, bukan untuk membuat protokol IP menjadi andal (*reliable*) [RFC 792]. Pesan ICMP sendiri dikirim dalam beberapa situasi, misal: jika sebuah datagram tidak dapat mencapai tujuannya, jika *gateway/router* tidak mampu meneruskan datagram dikarenakan penuhnya kapasitas buffer yang ada, dan jika *gateway/router* tidak dapat menemukan alamat tujuan.

6. Routing pada IP

Routing pada IP adalah suatu proses penentuan jalur untuk melewatkan datagram IP dari alamat pengirim ke alamat tujuan. Alat yang berfungsi melakukan *routing* IP disebut *router*. Proses *routing* dilakukan pada setiap *hop*. *Hop* adalah perjalanan paket data dari satu *router* atau *host* ke *router* atau *host* lainnya.



Gambar 6.1. Routing paket data dalam jaringan IP
(Sumber: Craig Hunt. 1992: 15)

Pada gambar 6.1 diperlihatkan proses *routing* paket data dari *host*/komputer A ke *host*/komputer C, dimana paket data dari komputer A tersebut melalui dua *router/gateway* sebelum sampai di komputer C. *Routing* paket data berkerja berdasarkan informasi yang terdapat pada tabel informasi *routing* pada setiap *host* atau *router*. Sebagai contoh pada gambar 2.10, sebelum komputer A mengirimkan data terlebih dahulu melihat informasi tabel *routing* yang ada padanya, kemudian diketahui untuk mengirimkan data ke komputer C harus lewat *router* R1. Pada saat data sampai di R1, data tersebut diperiksa alamat tujuannya dan dikonfirmasi dengan informasi tabel *routing*-nya. Oleh *router* R1 data tersebut diteruskan melalui R2 sampai akhirnya data tadi ditujukan ke komputer C oleh *router* R2.

Proses *routing* ini menjadi sangat penting sekali dalam jaringan Internet yang menghubungkan berbagai jenis jaringan LAN, MAN maupun WAN. Pada TCP/IP terdapat pula

protokol *routing* yang bertugas melakukan proses pemilihan jalur data dari pengirim ke tujuannya. Protokol *routing* tersebut diantaranya: *Routing Information Protocol* (RIP), *Open Shortest Path Protocol* (OSPF), dan *Border Gateway Protocol* (BGP). Protokol-protokol *routing* tersebut dimasukkan dalam dua kategori yang berbeda. RIP dan OSPF masuk dalam kategori *Interior Gateway Protocol* (IGP), sedang BGP berada dalam kategori *Exterior Gateway Protocol* (EGP). IGP adalah protokol *routing* yang menangani *routing* jaringan Internet pada sebuah *autonomous system* sementara EGP menangani *routing* antar *autonomous system*. *Autonomous system* (AS) secara umum didefinisikan sebagai jaringan internet yang berada dalam satu kendali administrasi dan teknis. Internet merupakan kumpulan dari ribuan *autonomous system*.