

BAB III

DASAR-DASAR JARINGAN

3.1. Protokol Komunikasi

Dalam dunia komputer, terdapat suatu standar bahasa yang memungkinkan tiap-tiap komputer yang berbeda jenis dapat saling berkomunikasi. Standar tersebut disebut sebagai protokol. Protokol mengatur bagaimana sebuah komputer berkomunikasi dengan komputer yang lain.

Protokol standar de facto yang digunakan dalam dunia komputer adalah TCP/IP. Menurut Purbo (Purbo dkk, 1998), Protokol TCP/IP diterima secara luas karena memiliki beberapa sifat sebagai berikut:

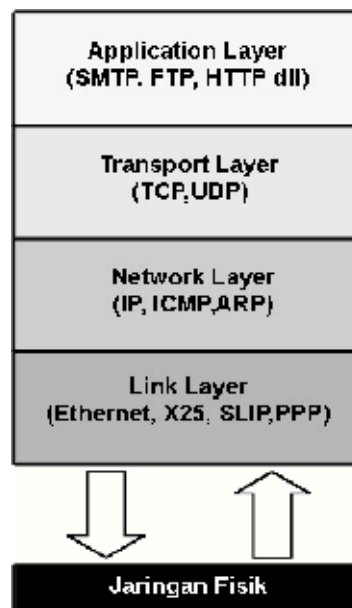
1. Protokol TCP/IP dikembangkan menggunakan standar protokol yang terbuka.
2. Standard protokol TCP/IP dalam bentuk Request for Comment (RFC) dapat diambil oleh siapa saja.
3. TCP/IP dikembangkan dengan tidak bergantung pada perangkat keras atau sistem operasi tertentu.
4. Pengembangan protokol TCP/IP dilakukan dengan konsensus dan tidak tergantung pada vendor tertentu.
5. TCP/IP independen terhadap perangkat jaringan dan dapat dijalankan pada jaringan Ethernet, Token Ring, jalur telepon dial-up dan jenis media transmisi apapun.
6. Pengalamatan pada TCP/IP bersifat unik dalam skala global. Dengan cara ini komputer dapat saling terhubung walaupun jaringannya seluas Internet sekarang ini.
7. TCP/IP memiliki fasilitas routing yang memungkinkan sehingga dapat diterapkan pada internetwork.
8. Protokol TCP/IP memiliki banyak layanan.

3.2. Arsitektur Dasar TCP/IP

TCP/IP sendiri merupakan singkatan dari *Transmission Control Protocol/Internet Protocol*. Dari namanya bisa dilihat kalau TCP/IP bukanlah suatu protokol tunggal, tetapi merupakan suatu kumpulan protokol. Seperti model protokol jaringan yang lain, TCP/IP juga tersusun atas lapisan-lapisan. Tiap lapisan disusun

berdasarkan lapisan di bawahnya dengan cara menambahkan fungsi yang baru. Protokol pada lapisan terendah sepenuhnya berurusan dengan pengiriman dan penerimaan semua jenis data menggunakan perangkat keras jaringan yang telah ditentukan. Protokol pada lapisan tertinggi adalah protokol yang didesain untuk tugas-tugas tertentu seperti mentransfer file, menerima email dan lain-lain. Sedangkan lapisan-lapisan diantara keduanya berhubungan dengan hal-hal seperti routing dan pemeliharaan integritas dan kehandalan data.

Gambar 3.1 memperlihatkan lapisan-lapisan pada arsitektur TCP/IP menurut Purbo (Purbo, 1998).



GAMBAR 3.1 Layer TCP/IP

1. Lapisan Link atau sering disebut lapisan data link. Lapisan ini bertanggung jawab atas pengiriman dan penerimaan data dari media fisik. Wujudnya biasanya berupa network interface dan device driver untuk peralatan tersebut. Lapisan ini menangani jaringan sesungguhnya yaitu berupa sambungan fisik kabel, radio, serat optik dan sebagainya. Contoh yang umum adalah ethernet. Perangkat ini terhubung ke perangkat sejenis melalui sebuah kabel UTP dan hub atau sebuah kabel BNC yang ujungnya diberi terminator. Ethernet mengirim dan menerima blok data yang disebut frame. Ketika sebuah ethernet mengirim data, data tersebut dikirim ke seluruh jaringan. Namun hanya satu ethernet yang menjadi

tujuan pengiriman yang akan merespon data yang terkirim tersebut. Sehingga dalam satu saat, hanya ada satu ethernet yang bisa mengirimkan data.

Apabila ada lebih dari satu ethernet yang mengirimkan data, maka akan terjadi tabrakan atau collision. Untuk itu sebelum mengirimkan data, sebuah *ethernet* akan mengecek apakah ada *ethernet* lain yang sedang memancarkan data. Apabila ada, maka ethernet tersebut akan menunggu dengan selang waktu yang acak untuk memancarkan data kembali.

Karena dalam satu jaringan/kabel terdapat lebih dari satu ethernet, untuk membedakannya tiap-tiap ethernet mempunyai 48 bit alamat unik yang disebut sebagai ethernet address. Selain ethernet, contoh lain adalah SLIP dan PPP.

2. Lapisan Network. Lapisan ini bertanggung jawab untuk menyampaikan data pada alamat yang tepat. Terdapat tiga macam protokol di sini yaitu *Internet Control Message Protokol (ICMP)*, *Address Resolution Protokol (ARP)* dan *Internet Protokol (IP)*.

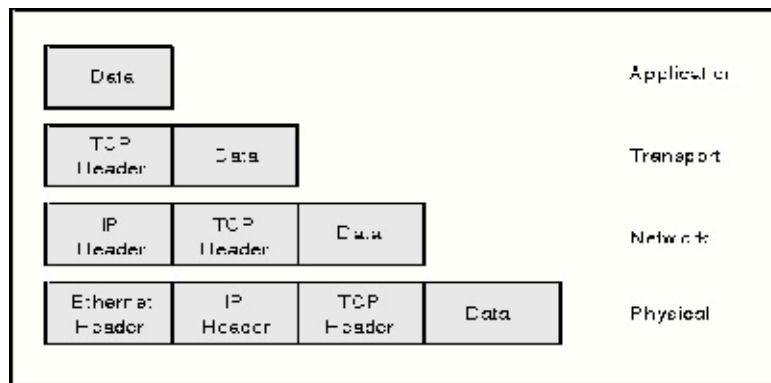
ICMP adalah protokol yang digunakan untuk mengirimkan pesan dan melaporkan kegagalan pengiriman data. ARP digunakan untuk menemukan alamat host atau komputer yang terletak dalam jaringan yang sama. Sedangkan IP digunakan untuk menyampaikan paket data ke alamat yang tepat.

3. Lapisan Transport. Lapisan ini berisi protokol yang bertanggung jawab untuk mengadakan komunikasi antara dua host atau komputer. Protokol yang ada adalah *User Datagram Protocol (UDP)* dan *Transmission Control Protocol (TCP)*.
4. Lapisan Aplikasi. Lapisan ini berisi layanan aplikasi yang digunakan untuk berkomunikasi melalui jaringan. Beberapa contoh aplikasi yang umum pada lapisan ini adalah surat elektronik (email), pengiriman berkas (ftp), pengaksesan halaman-halaman web dan lain-lain.

Pergerakan data dari lapisan yang paling atas ke lapisan di bawahnya dengan cara enkapsulasi data. Aplikasi pada layer paling atas mengirimkan data ke lapisan Transport, kemudian lapisan Transport menambahkan informasi pada header data tersebut dan mengirimnya dalam bentuk paket ke lapisan Network. Lapisan ini juga

menambahkan informasi pada header data tersebut untuk selanjutnya dikirim ke lapisan Link. Demikian pula pada lapisan Link, paket juga mengalami penambahan informasi pada headernya sebelum data benar-benar dikirimkan keluar melalui media transmisi yang ada.

Proses yang berkebalikan terjadi ketika paket diterima pada host tujuan. Tiap-tiap lapisan dari yang paling bawah melepas informasi yang terdapat pada header. Sehingga data yang utuh diterima oleh lapisan aplikasi. Gambar 3.2 memperlihatkan proses enkapsulasi tersebut.



Gambar 3.2 Enkapsulasi Data pada Layer TCP/IP (Fletcher, 2001)

3.3.IP

Protokol ini adalah protokol utama dalam TCP/IP. Seluruh data yang berasal dari protokol pada layer di atas IP harus dilewatkan, diolah oleh protokol IP, dan dipancarkan sebagai paket IP, agar sampai ke tujuan (Purbo, 1998).

Lapisan ini mempunyai sifat *unreliable*, *connectionless* dan *datagram delivery service*. *Unreliable* (ketidakhandalan) artinya bahwa protokol ini tidak menjamin data akan sampai ke tempat tujuan. Protokol hanya akan melakukan usaha sebaik mungkin agar data bisa sampai ke tujuan. Apabila ternyata dalam proses pengiriman terdapat masalah yang mengakibatkan data tidak dapat dikirimkan, protokol hanya akan mengirimkan pesan kepada alamat pengirim menggunakan ICMP bahwa ada masalah dalam peniraman data. *Connectionless* artinya dalam proses pengiriman data pihak pengirim maupun pihak penerima tidak diadakan handshake (perjanjian) terlebih dahulu. Sedangkan *Datagram Delivery Service* artinya adalah setiap datagram yang dikirim tidak bergantung kepada datagram yang lain. Sehingga jalur yang ditempuh oleh masing-masing paket IP bisa berbeda-beda yang menyebabkan urutan kedatangan paket pada tujuan bisa saja menjadi tidak berurutan. Hal ini dilakukan

untuk mengusahakan agar paket data bisa sampai ke tujuan walaupun salah satu jalur ke tujuan ini mengalami masalah.

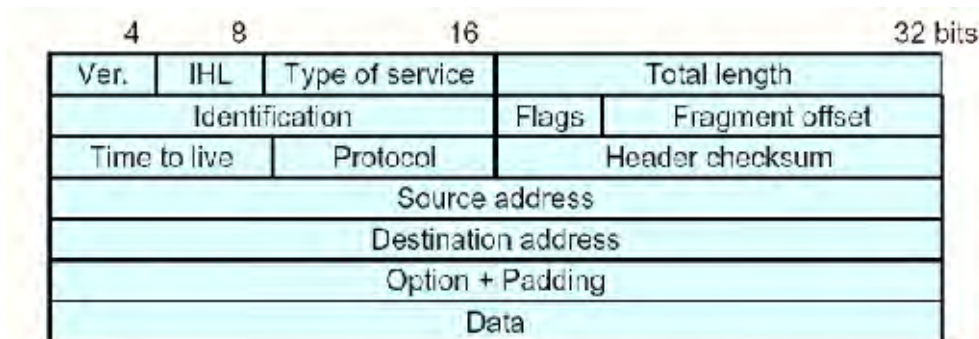
3.3.1. Fragmentasi Paket IP

Dalam proses pengiriman data, TCP/IP memecah data menjadi paket-paket kecil yang disebut sebagai datagram. Protokol IP bertanggung jawab untuk melakukan pemecahan datagram yang berukuran besar menjadi beberapa datagram yang ukurannya sesuai dengan lapisan fisiknya. Proses pemecahan datagram menjadi paket yang lebih kecil disebut fragmentasi. Ukuran datagram IP dapat mencapai 65.535. Namun banyak jaringan tidak mendukung ukuran data sebesar itu. Sebuah frame ethernet, contohnya, hanya dapat diisi 1.500 byte data dari lapisan di atasnya (Heywood, 1996).

Pada host tujuan, terjadi proses sebaliknya. Paket-paket data yang berukuran kecil digabung kembali sehingga menjadi data yang utuh. Proses ini disebut defragmentasi.

3.3.2. Format Header IP

Gambar 3.3 yang diambil dari www.protocols.com, menunjukkan format header paket IP.



Gambar 3.3 Format Header Paket IP

1. Version. Menunjukkan format dari internet header. Versi yang digunakan saat ini adalah versi 4.
2. Internet Header Length (IHL). Menunjukkan panjang dari header menggunakan 32 bit word.
3. Type of Service. Menunjukkan kualitas service yang dapat mempengaruhi cara penanganan paket IP. Beberapa pilihan untuk kualitas layanan adalah waktu tunda yang rendah (low delay), kehandalan yang tinggi (high reliability) atau kecepatan yang tinggi (high throughput).

4. Total Length. Menunjukkan panjang total datagram IP dalam ukuran byte.
5. Identification, Flags dan Fragment Offset. Berisi data yang berhubungan dengan fragmentasi paket. Fragmentasi adalah proses memecah data menjadi paket-paket kecil sesuai besar maksimal data yang bisa dilewatkan melalui suatu jalur.
6. Time To Live. Berisi jumlah router/hop maksimal yang boleh dilewati oleh paket IP. Setiap kali melewati sebuah router, nilai pada TTL berkurang satu. Apabila nilai TTL telah habis, sedangkan paket tersebut belum mencapai tujuan, maka router terakhir akan membuang paket tersebut agar tidak membebani jaringan. Dan selanjutnya router tersebut mengirimkan paket ICMP ke alamat asal yang memberitahu kegagalan pengiriman paket.
7. Protocol. Berisi data tentang protokol lapisan atas yang berhubungan dengan bagian data dari datagram. Nilai assign number telah ditentukan bagi banyak protokol.
8. Header Checksum. Berisi nilai checksum yang dihitung dari seluruh field dari header paket IP. Nilai ini dihitung ulang di tempat tujuan. Apabila terjadi perbedaan, paket dianggap rusak dan dibuang.
9. Source Address dan Destination Address. Berisi alamat IP asal dan alamat IP tujuan. Berupa angka 32 bit.
10. Option + Padding. Beberapa byte option adalah:
 - a. Strict Source Route. Berisi daftar lengkap alamat IP dari router yang harus dilalui oleh paket dalam perjalanannya ke host tujuan. Paket balasan untuk datagram ini juga harus melalui router yang sama.
 - b. Loose Source Router. Juga berisi daftar lengkap alamat IP dari router yang harus dilalui paket untuk sampai ke tujuan. Tetapi jika diantara dua router yang disebutkan terdapat router lain, paket masih diperbolehkan melalui router tersebut.

3.3.3. Pengalamatan Nomor IP

Dalam setiap header paket IP, ada dua field yang memegang peranan sangat vital agar sebuah paket sampai ke tujuan, yaitu source address dan destination address. Alamat yang dimaksud adalah alamat IP. Alamat ini

sebenarnya tidak mengacu ke sebuah komputer, tetapi lebih ke interface jaringan. Sehingga sebuah komputer yang memiliki dua buah interface tentu memiliki dua alamat IP.

Alamat IP berupa bilangan biner 32 bit yang dipisahkan oleh tanda titik setiap 8 bitnya yang disebut oktet.

xxxxxxxx.xxxxxxxxx.xxxxxxxxx.xxxxxxxxx

Setiap simbol x bisa bernilai 0 atau 1. Dan nilai ini kalau dikonversikan ke dalam nilai desimal setiap oktet bisa bernilai antara 0 sampai dengan 255, sehingga dengan kombinasi di atas sebenarnya bisa didapatkan sekitar 4,2 milyar alamat.

IP address terdiri atas dua bagian yaitu network ID dan host ID, di mana network ID menentukan alamat jaringan, sedangkan host ID menentukan alamat dari peralatan jaringan (Wijaya, 2001). Peralatan jaringan yang dimaksud bisa berupa workstation, server, router dan semua host TCP/IP lainnya dalam jaringan tersebut. Alamat IP dikelompokkan dalam lima kelas. Kelas A memiliki jumlah network sedikit tetapi tiap networknya memiliki jumlah host yang banyak. Sedangkan kelas C memiliki jumlah network banyak, tetapi tiap networknya memiliki jumlah host sedikit. Purbo (Purbo, 1998) menyebutkan pembagian kelas alamat IP sebagai berikut:

1. Kelas A : bit pertama selalu bernilai 0, sehingga formatnya
0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh
Dengan begitu kelas A mempunyai range dari 1.xxx.xxx.xxx sampai dengan 126.xxx.xxx.xxx
2. Kelas B : dua bit pertama selalu bernilai 10, sehingga formatnya
10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh
Dengan begitu kelas B mempunyai range dari 128.0.xxx.xxx sampai dengan 191.255.xxx.xxx
3. Kelas C : tiga bit pertama selalu bernilai 110, sehingga formatnya
110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh
Dengan begitu kelas C mempunyai range dari 192.0.0.xxx sampai dengan 223.255.255.xxx
4. Kelas D : empat bit pertama selalu bernilai 1110, sehingga formatnya
1110hhhh.hhhhhhhh.hhhhhhhh.hhhhhhhh

Dengan begitu kelas D mempunyai range dari 224.xxx.xxx.xxx sampai dengan 239.xxx.xxx.xxx. Kelas ini tidak dipergunakan secara umum, tetapi dipergunakan secara khusus untuk keperluan multicasting. Kelas ini tidak mengenal network ID dan host ID.

5. Kelas E : empat bit pertama selalu bernilai 1111, sehingga formatnya 1111hhhh.hhhhhhhh.hhhhhhhh.hhhhhhhh

Dengan begitu kelas E mempunyai range dari 240.xxx.xxx.xxx sampai dengan 255.xxx.xxx.xxx. Seperti halnya kelas D, kelas E juga tidak diperguntukkan bagi kepentingan umum. Kelas ini ditujukan untuk keperluan eksperimental.

Purbo (Purbo, 1998) juga menyebutkan bahwa penggunaan nomor IP selain yang sudah tersebut di atas, harus memperhatikan beberapa aturan khusus yaitu:

1. Network ID dan host ID tidak boleh 0 (nol), karena nilai tersebut berarti menunjuk ke jaringan dan bukan sebuah perangkat. Misalkan 202.152.41.2 artinya jaringan dengan network ID 202.152.41, sedangkan alamat 0.0.0.2 artinya host ID 2 pada jaringan lokal.
2. Network ID 127 merupakan alamat khusus yang disebut loopback. Pesan yang dialamatkan ke network ID 127 tidak diteruskan ke jaringan tetapi akan dikembalikan lagi.
3. Host ID 255 dibatasi penggunaannya. Pesan yang dikirim ke host ID 255 akan disebarkan ke seluruh host dalam jaringan yang dikenal sebagai broadcast.

Pendistribusian alamat IP dikoordinasi oleh IANA, dan untuk mempermudah pengalokasian, distribusi secara regional diserahkan kepada ISP.

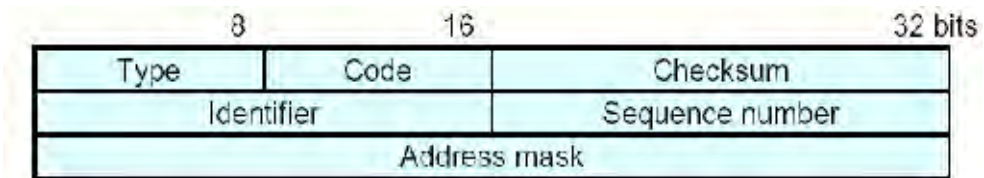
Saat ini alokasi alamat IP kelas A dan B telah habis, sehingga kita hanya bisa mendapatkan alamat IP kelas C, dan itu pun suatu saat akan habis. Untuk itu kita perlu benar-benar melakukan penghematan dalam penggunaan alamat IP.

3.4.ICMP

Protokol IP adalah protokol yang didesain sebagai protokol yang *unreliable*. ICMP adalah protokol yang bertugas mengirimkan pesan-pesan kesalahan dan kondisi

lain yang memerlukan perhatian khusus (Purbo, 1998). Walaupun ICMP dijelaskan secara terpisah, namun ICMP sebenarnya bagian dari IP.

Format header paket ICMP digambarkan pada gambar 3.4, diambil dari www.protocols.com



Gambar 3.4 Format Header Paket ICMP

Ada dua jenis pesan yang disampaikan oleh ICMP yaitu *ICMP Error Message* yang dihasilkan ketika ada masalah dengan jaringan, dan *ICMP Query Message* yang dihasilkan ketika si pengirim paket menginginkan informasi tertentu yang berkaitan dengan kondisi jaringan.

Menurut Purbo (Purbo, 1998) beberapa contoh ICMP Error Message:

1. Destination Unreachable. Pesan ini dihasilkan oleh router ketika terjadi kegagalan pengiriman akibat putusnya jalur baik secara fisik maupun logika. *Destination Unreachable* masih dibagi menjadi beberapa tipe, beberapa diantaranya adalah:
 - a. Network Unreachable jika jaringan tujuan tidak dapat dihubungi.
 - b. Host Unreachable jika host tujuan tidak dapat dihubungi.
 - c. Protokol at Destination is Unreachable jika pada tujuan tidak tersedia protokol tersebut.
 - d. Port is Unreachable jika tidak ada port yang dimaksud pada tujuan.
 - e. Destination Network is Unknown jika network tujuan tidak diketahui.
 - f. Destination Host is Unknown jika host tujuan tidak diketahui.
2. Time Exceeded. Pesan ini muncul jika field TTL pada paket IP sudah habis, sementara paket tersebut belum sampai tujuan.
3. Parameter Problem. Pesan ini muncul jika terdapat kesalahan parameter pada *header paket IP*.
4. Source Quench. Pesan ini muncul bila terjadi jika router atau tujuan mengalami kemacetan yang disebabkan ruang buffer yang terbatas. Sebagai respon atas pesan ini, pengirim harus memperbesar jeda pengiriman pakatnya.

5. Redirect. Pesan ini muncul ketika ketika router menemukan bahwa host mengirim paket melalui router yang salah, sedangkan router tersebut mengetahui router lain yang bisa mengirimkan paket tersebut melalui jalur yang lebih pendek.

Purbo (Purbo, 1998) juga menjelaskan beberapa contoh *ICMP Query Message*:

1. Echo Request dan Echo Reply. Bertujuan untuk mengetahui apakah host tujuan dalam keadaan aktif. Program ping merupakan program pengirim paket ini. Dan jika sistem tujuan aktif, dia akan mengirimkan paket data balasan, kecuali dengan sengaja diatur untuk tidak mengirimkan paket balasan.
2. Timestamp Request dan Timestamp Reply. Pesan ini mengirimkan data mengenai timestamp (penanda waktu) yang diperlukan untuk memproses paket.
3. Address Mask. Untuk mengetahui berapa netmask yang harus digunakan oleh suatu host dalam suatu jaringan.

Sebagai paket pengatur kelancaran jaringan, maka ICMP tidak boleh membebani jaringan. Karenanya, paket ICMP tidak boleh dikirim saat terjadi problem yang disebabkan oleh (Purbo, 1998):

1. Kegagalan pengiriman paket ICMP itu sendiri.
2. Kegagalan pengiriman paket broadcast atau multicast.

3.5.ARP

Dalam sebuah jaringan lokal, host-host saling terhubung menggunakan ethernet. Ethernet memiliki ethernet address sepanjang 48 bit. Untuk mengirim data ke host dengan alamat IP tertentu, sebuah host harus mengetahui di atas *ethernet address* manakah alamat IP yang dituju. Mekanisme untuk mengenali hubungan alamat IP dengan ethernet address adalah Address Resolution Protokol atau ARP. Cara kerja ARP adalah sebagai berikut :

1. Host A pada akan mengirimkan data ke host B dengan alamat IP tertentu dalam jaringan lokal. Diasumsikan dalam cache ARP host A belum ada entry untuk host B.

2. Host A memancarkan paket ARP secara broadcast ke jaringan. Isi paket tersebut menanyakan siapakah pemilik alamat IP B dan berapakah alamat *ethernet*-nya.
3. Setiap host menerima paket ARP tersebut dan mencocokkan dengan alamat IP masing-masing. Jika alamat IP-nya tidak cocok, maka dia akan mengabaikannya.
4. Host B yang merasa alamat IP-nya cocok, akan mengirim paket balasan ke host A. Isi paket balasan tersebut adalah alamat IP dan ethernet address B.
5. Host A menyimpan alamat B ke dalam ARP cache sehingga suatu saat ketika host A ingin mengirimkan paket ke host B, host A tidak perlu melakukan langkah-langkah di atas, tetapi cukup memeriksa ARP cache-nya.

3.6.TCP

Protokol TCP (Transmission Control Protokol) terletak di lapisan transport. Protokol ini bersifat *connection oriented*, *reliable* dan *byte stream service*.

Connection Oriented artinya sebelum melakukan pertukaran data, dua host harus saling melakukan handshake (perjanjian) terlebih dahulu. Reliable berarti menerapkan proses deteksi kesalahan dan pengiriman ulang. Byte Stream Service berarti paket dikirimkan sampai ke tujuan secara berurutan.

Secara sederhana proses handshake dimulai oleh suatu host dengan mengirimkan paket SYN (synchronize). Kemudian host tujuan merespon paket syn dengan mengirimkan paket ACK (acknowledgement). Dengan demikian handshake telah dibangun.

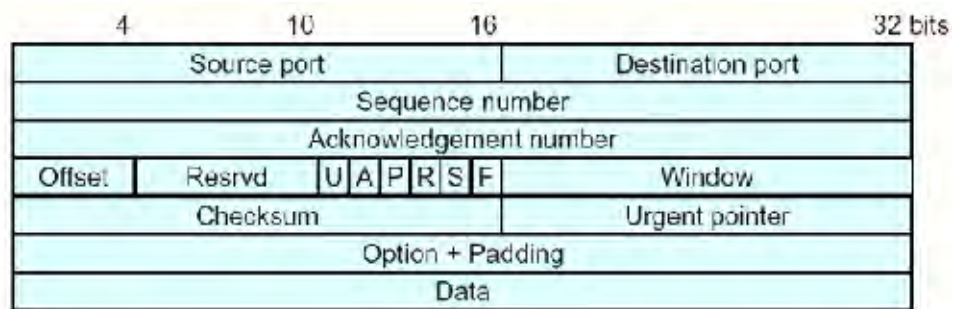
Untuk menjaga kehandalan, TCP menerapkan beberapa hal (Purbo, 1998):

1. TCP memecah data menjadi segmen-segmen yang ukurannya paling sesuai menurut TCP.
2. Ketika suatu host menerima paket TCP dari host lain, dia mengirimkan paket ACK untuk memberitahu bahwa data telah diterima.
3. Pada host pengirim, setelah data dikirimkan, TCP mengaktifkan timer. Jika sampai saat yang ditentukan ACK dari tujuan belum diterima, maka host akan mengirim ulang paket di atas.
4. TCP memiliki proses flow control untuk mencegah server cepat membanjiri server lambat. Setiap koneksi TCP memiliki buffer dengan

ukuran terbatas. Host penerima TCP hanya memperbolehkan host pengirim mengirimkan data sesuai ukuran buffer sebesar yang ia miliki.

3.6.1. Format Header TCP

Gambar 2.5 merupakan format header paket TCP. Gambar tersebut diambil dari www.protocols.com.



Gambar 3.5 Format Header Paket TCP

1. Source Port/Destination Port. Menunjukkan port yang mengidentifikasi aplikasi pengirim dan penerima.
2. Sequence Number. Menunjukkan posisi urutan dari oktet data pertama pada segmen.
3. Acknowledgment number. Setiap kali data sukses terkirim, pihak penerima mengisi field ini dengan sequence number berikutnya yang diharapkan oleh penerima.
4. Offset. Menunjukkan panjang header.
5. Reserved. Bit cadangan, diset nol.
6. Control Bits. Terdapat enam jenis karakter kontrol:
 - a. URG menunjukkan Urgent Pointer bernilai valid.
 - b. ACK menunjukkan Acknowledgement bernilai valid.
 - c. PSH Memulai fungsi push.
 - d. RST me-reset koneksi.
 - e. SYN Melakukan sinkronisasi nomor urutan untuk hubungan.
Bit ini di-set saat sebuah segmen meminta hubungan dibuka.
 - f. FIN menunjukkan pengiriman selesai dan menutup hubungan.
7. Window. Menunjukkan panjang window (semacam buffer) penerimaan segmen TCP, merupakan banyak byte yang bisa diterima tiap saat. Lebarnya 16 bit, sehingga nilai maksimalnya adalah 65.535.

8. Checksum. Digunakan untuk mengontrol error pada header dan field data.
9. Urgent Pointer. Aktif jika flag URG di set. Menunjukkan nomor urutan oktet menyusul data yang mendesak.
10. Option. Berfungsi untuk mengatur berbagai fungsi yang meliputi daftar option, no-operation, ukuran segmen maksimum.

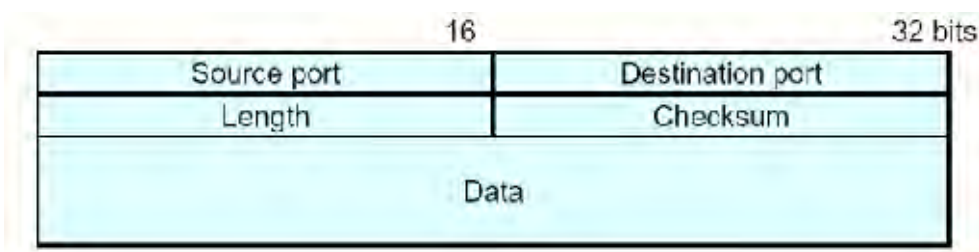
3.7.UDP

User Datagram Protokol (UDP) adalah protokol sederhana. UDP bersifat connectionless dan unreliable. Sebagai protokol datagram, UDP tidak mengurus penerimaan aliran data dan pembuatan segmen yang sesuai untuk IP. Sehingga menjadikan UDP sebagai protokol yang ringkas.

Paket UDP tidak membutuhkan jawaban, sehingga sangat mengurangi overhead jaringan. Berbeda dengan TCP yang harus membuka dan menutup hubungan. UDP biasanya digunakan oleh aplikasi yang secara periodik melakukan aktivitas tertentu misalnya query routing table pada jaringan. Hilangnya satu data dapat diatasi dengan query pada periode berikutnya.

Kemiripan UDP dengan TCP adalah penggunaan nomor port untuk membedakan pengiriman datagram ke beberapa aplikasi yang berbeda dalam komputer yang sama.

Gambar 3.6 menunjukkan format header paket UDP, diambil dari www.protocols.com.



Gambar 3.6 Format Header Paket UDP

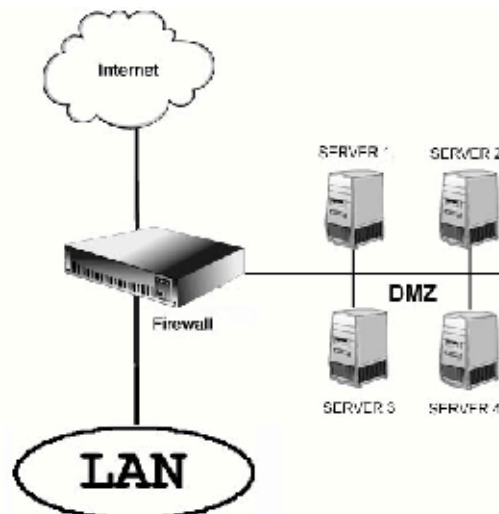
1. Source Port/Destination Port. Menunjukkan port yang mengidentifikasi aplikasi pengirim dan penerima.
2. Length. Menunjukkan panjang header dan data pada datagram.
3. Checksum. Berisi nilai untuk melakukan pengecekan terhadap kesalahan.

3.8.Firewall

Firewall secara bahasa artinya adalah sebuah bangunan yang dibuat untuk mencegah menjalarnya api. Sedangkan Internet Firewall adalah suatu kombinasi perangkat lunak dan perangkat keras yang didesain untuk memeriksa aliran trafik jaringan dan permintaan servis. Kegunannya adalah untuk mencegah keluar/masuknya aliran paket yang tidak memenuhi kriteria keamanan yang didefinisikan oleh organisasi pemilik jaringan (Purbo, 2000).

Firewall yang sederhana adalah sebuah host tanpa fungsi routing yang menghubungkan dua buah jaringan. Sebuah kartu jaringan terhubung ke internet dan sebuah kartu jaringan lain terhubung ke jaringan lokal. Untuk bisa terhubung ke internet, client harus log-on ke host tersebut dari komputer di jaringan lokal, dan dari host tersebut kita menjalankan aplikasi yang mengakses internet. Dengan aplikasi tersebut kita mengakses internet dengan display yang ditampilkan pada komputer lokal kita.

Gambar 3.7 mengilustrasikan desain firewall yang umum digunakan. Firewall tersebut menghubungkan jaringan lokal, internet dan jaringan perimeter. Jaringan perimeter adalah jaringan yang berisi server yang memberikan layanan publik. Jaringan perimeter juga disebut sebagai DMZ (De-Militerized Zone).



Gambar 3.7 Desain Umum Firewall

3.8.1. Proxy Server

Grennan mendefinisikan bahwa Proxy server menyediakan akses internet secara tidak langsung melalui firewall (Grennan, 2000). Ilustrasi dari hal ini adalah seseorang yang melakukan telnet ke suatu mesin, kemudian melakukan telnet lagi ke mesin yang lain di internet. Proxy server mengotomatisasi hal ini. Ketika client melakukan koneksi ke internet, maka client akan terhubung ke proxy

lebih dulu, kemudian proxy akan menghubungi server tujuan dan memberikan data yang diminta ke client.

Karena menangani semua komunikasi, maka proxy bisa melakukan log terhadap semua lalu lintas data. Untuk tipe proxy web, log ini termasuk semua URL yang diakses oleh pengguna. Untuk proxy FTP, log bisa berupa semua file yang di-upload dan donwload oleh user.

3.8.2. Packet Filtering Firewall

Menurut Grennan packet filtering firewall adalah firewall yang berkerja pada lapisan network (Grennan, 2000). Data akan diijinkan untuk lewat/diproses apabila memenuhi kriteria yang ditetapkan. Firewall jenis ini akan menyaring paket berdasarkan informasi tipe, alamat asal, alamat tujuan, dan port dari paket tersebut. Informasi tersebut didapat dari header paket yang diterima.

Data yang dianalisa sangat sedikit, sehingga filtering jenis ini menggunakan sangat sedikit proses CPU, dan menghasilkan beban yang sangat ringan kepada jaringan.

Firewall jenis ini tidak menyediakan mekanisme kontrol dengan password, sehingga kita tidak bisa memilih user yang mana yang kita beri akses. Satu-satunya identitas bagi pengguna adalah alamat IP yang diberikan kepada workstation pengguna. Hal ini bisa menjadi masalah ketika workstation dikonfigurasi menggunakan DHCP, karena alamat IP selalu berubah-ubah. Sehingga aturan baru harus dikonfigurasi ulang untuk menyesuaikan dengan hal ini.