Evolusi TCP/IP

Dimulai pada tanggal Agustus 1962 oleh J.C.R.Licklider dari MIT yang membahas "Galactic Network" dan bagaimana interaksi sosial dapat terjadi melalui jaringan. Internet memungkinkan infrastruktur komunikasi nasional & global menjadi sangat mungkin.

Sebelum tahun 1960, komunikasi komputer masih sangat langka. Komunikasi komputer yang ada pun tidak efisien menggunakan saluran komunikasi yang ada saat itu, yaitu, circuit switching, yang menggunakan jaringan telepon yang telah ada lebih dari seratus tahun yang lalu di Amerika Utara. Umumnya komunikasi data bersifat burst (sesaat), maka penggunaan jaringan telepon, circuit switching, sangat tidak efisien.

Teknologi fundamental (mendasar) yang mungkinkan Internet beroperasi adalah teknologi packet switching, sebuah jaringan data yang mana semua komponen-nya (host maupun switch) bekerja secara independent, menghilangkan masalah single point-of-failure. Resource jaringan komunikasi tampak seperti dedicated pada pengguna individual, sebetulnya merupakan akumulasi multiplexing dengan batas atas besaran data yang dikirimkan yang pada akhirnya menghasilkan jaringan yang ekonomis.

Di awal tahun 1960-an, packet switching akan di temukan.Tahun 1961, Leonard Kleinrock dari MIT mempublikasi paper pertama tentang teori packet switching dan buku tentang hal tersebut di tahun 1964. Tahun 1962, Paul Baran dari Rand Corporation menjelaskan tentang jaringan data store-and forward yang efisien dan handal bagi Angkatan Udara Amerika Serikat. Pada waktu yang sama, Donald Davies dan Roger Scantlebury menawarkan ide yang sama dari kerja mereka di National Physical Laboratory (NPL) di Inggris. Penelitian di MIT (1961-1967), RAND (1962-1965), dan NPL (1964-1967) terjadi secara independent dan para peneliti tidak saling bertemu sampai saat pertemuan Association for Computing Machinery (ACM) tahun 1967. Istilah packet di adopsi dari pekerjaan di NPL.

Internet modern dimulai pada saat U.S. Department of Defense (DoD) membiayai experimen untuk menyambungkan lokasi penelitian yang didanai oleh DoD di US. Pertemuan ACM 1967 juga merupakan awal design dari ARPANET - nama dari dari Department of Defence Advanced Research Project Agency (ARPA) - yang di publikasikan oleh Larry Roberts. Desember 1968, ARPA memberikan kontrak kepada Bolt Beranek dan Newman (BBN) untuk mendesign dan mengoperasikan jaringan packet switching pada kecepatan 50kbps. September 1969, node pertama APRANET di install di University of California at Los Angeles (UCLA), beberapa bulan berikutnya node di Stanford Research Institute (SRI), University of California at Santa Barbara (UCSB), dan University of Utah. Dengan empat node di akhir 1969, ARPANET berkembang ke seluruh amerika serikat di tahun 1971 dan tersambung ke eropa di tahun 1973.

ARPANET memberikan nyawa bagi beberapa protokol yang baru untuk packet switching. Salah satu hasil dari APRANET yang berumur panjang adalah user-network protocol yang menjadi interface standard antara pengguna dengan jaringan packet switch; yang dikenal sebagai ITU-T (dulu CCITT) rekomendasi X.25. Dengan "standard" interface yang ada memberikan semangat bagi BBN untuk memulai Telenet di tahun 1974, sebuah paket-switched data servis komersial yang kemudian menjadi bagian dari Sprint's X.25 servis.

Protokol komunikasi host-to-host yang pertama kali di gunakan ARPANET disebut Network Control Protocol (NCP). Kemudian hari ternyata NCP tidak sanggup menangani perkembangan beban traffic yang ada. Tahun 1974, protokol komunikasi yang lebih reliable di usulkan dan di implementasikan di seluruh APRANET, berbasis pada Transmission Control Protocol (TCP) untuk komunikasi end-to-end. Akan tetapi protokol ini tampaknya terlalu overkill (canggih) untuk digunakan di gateway perantara (hari ini biasa kita sebut sebagai router), oleh karena itu tahun 1978 sebuah design untuk memisahkan tanggung jawab dari sepasang protocol; protokol baru Internet Protocol (IP) bertanggung jawab untuk me-

routing paket dan komunikasi device-to-device (seperti, host-to-gateway atau gateway-to-gateway) dan TCP untuk komunikasi end-to-end host secara reliable. TCP dan IP awalnya di pikirkan sebagai sebuah protokol, sekumpulan protocol, pada dasarnya terdiri dari kumpulan protocol dan aplikasinya, yang biasanya kita kenal sebagai TCP/IP.

Versi orisinil dari TCP dan IP yang kita gunakan pada hari ini ditulis pada bulan September 1981, walaupun ke dua-nya memperoleh banyak modifikasi dikemdian hari, seperti IP versi 6 (IPv6) yang spesifikasinya di release Desember 1995. Tahun 1993, DoD memerintahkan bahwa semua sistem komputer mereka harus menggunakan TCP/IP untuk komunikasi jarak jauhnya. Hal ini menaikan pentingnya APRANET.

Aplikasi Internet yang pertama kali ditemukan adalah FTP. Menyusul kemudian e-mail, dan telnet. E-mail menjadi aplikasi yang paling populer di masa ARPANET. Tahun 1979 tercatat sebagai tahun berdirinya USENET yang pada awalnya menghubungkan Universitas Duke dan UNC. Grup yang pertama kali dibentuk dalam USENET adalah grup net.*.

Tahun 1983, ARPANET terpisah menjadi dua komponen. Satu komponen, tetap dikenal sebagai ARPANET, yang digunakan untuk menyambungkan pusat penelitian dan akademik. Yang lain, dikenal sebagai MILNET, digunakan untuk membawa trafik militer dan merupakan bagian dari Defence Data Network (DDN). Di tahun yang sama kita melihat kenaikan popularitas TCP/IP dengan dimasukannya kernel komunikasi ke implementasi UNIX dari University of California, 4.2BSD (Berkeley Software Distribution) UNIX.

Pada tahun 1984 jumlah host di Internet melebihi 1000 buah. Pada tahun itu pula diperkenalkan Domain Name System (DNS) yang mengganti fungsi tabel nama host. Sistem domain inilah yang sampai saat ini kita gunakan untuk menuliskan nama host.

Tahun 1986, National Science Foundation (NSF) membangun tulang punggung jaringan komputer untuk menyambungkan National Center for Atmospheric Research (NCAR) dan empat pusat superkomputer regional yang dibiayai oleh NSF. Jaringan ini dikenal sebagai NSFNET, awalnya dimaksudkan sebagai backbone dari network lainnya, dan tidak sebagai mekanisme interkoneksi dari system-system individual.

"Appropriate Use Policy" didefinisikan oleh NSF mem batasi traffic untuk keperluan non-komersial. NSFNET terus berkembang dan memberikan sambungan antara jaringan yang dibiayai NSF dan non-NSF, yang kemudian dikenal sebagai Internet hari ini.

Pada tahun 1987 berdiri UUNET yang saat ini merupakan salah satu provider utama Internet. Tercatat pula pada tahun tersebut jumlah host melewati angka 10.000. Setahun kemudian kecepatan jaringan tulang punggung NSFNET ditingkatkan menjadi T1 (1,544Mbps). Di samping itu juga terdapat beberapa negara di Eropa yang masuk ke jaringan NSFNET.

Awal spesifikasi NSFNET mampu untuk multiprotocol, TCP/IP digunakan untuk interkonektifitas dengan tujuan akhir untuk migrasi ke Open System Interconnection (OSI). NSFNET awalnya terdiri dari sambungan 56Kbps dan berhasil di upgrade ke sambungan T1 1.544Mbps di tahun 1989. Migrasi ke jaringan yang di manage secara professional di supervisi oleh konsorsium yang terdiri dari Merit (Michigan state regional network bermarkas di University of Michigan), IBM, dan MCI. Advanced Network & Services, Inc. (ANS), sebuah perusahaan non-profit dibentuk oleh IBM dan MCI, bertanggung jawab untuk mensupervisi transisi NSFNET backbone ke T3 (44.736 Mbps) di akhir 1991. Pada saat yang sama, NSF mendanai beberapa Internet Servis Provider regional untuk memberikan sambungan ke institusi pendidikan dan berbagai lokasi penelitian yang didanai NSF.

Tahun 1993, NSF memutuskan untuk tidak masuk ke usaha mengoperasikan & mendanai jaringan, tetapi kembali mendanai penelitian bidang supercomputing dan komunikasi kecepatan tinggi. Di samping itu, ada tekanan yang sangat besar untuk mengkomersialkan internet. Tahun 1989, sebuah gateway percobaan berhasil mengkaitkan

MCI, CompuServe, dan Internet mail services. Pada saat itu, untuk pertama kali-nya pengguna komersial non-akademik dan non-hardcore mengetahui kemampuan Internet. Tahun 1991, Commercial Internet Exchange (CIX) Association di bentuk oleh General Atomics, Performance Systems International (PSI), dan UUNET Technologies untuk mempromosikan dan memberikan service backbone Internet komersial. Hal ini semua memberikan tekanan yang sangat besar dari non-NSF ISP untuk membuka jaringan ke semua pengguna.

Tahun 1994, pelaksanaan pengurangan campur tangan NSF di Internet publik. Struktur yang baru terdiri atas tiga bagian, yaitu:

Network Access Points (NAPs), dimana ISP individual melakukan interkoneksi. NSF awalnya mendanai empat (4) dari NAP: Chicago (di operasikan oleh AMeritech), New York (really Pensauken, NJ, di operasikan oleh Sprint), San Francisco (di operasikan oleh Pacific Bell, sekarang SBC), dan Washington, D.C. (MAE-East, dioperasikan oleh MFS, sekarang bagian dari Worldcom).

Very High Speed Backbone Network Service, sebuah jaringan interkoneksi NAPs dan pusat-pusat yang di danai NSF, di operasikan oleh MCI. Jaringan ini di instalasi tahun 1995 dan beroperasi pada kecepatan OC-3 (155.52 Mbps); kemudian di upgrade ke OC-12 (622.08 Mbps) tahun 1997.

Routing Arbiter, untuk menjamin cukupnya routing protokol untuk Internet.

ISP yang dibiayai NSF diberikan waktu lima (5) tahun dengan biaya yang berkurang agar dapat mendanai diri sendiri secara konmersial di tahun ke lima. Pendanaan ini berhenti tahun 1998 dan bermunculan banyak NAP untuk memberikan servis. Terminologi hari ini dikenal sebagai three (3) tier ISP, yaitu:

Tier 1 adalah ISP nasional di Amerika Serikat, atau mereka yang memiliki keberadaan secara nasional dan tersambung pada minimal tiga (3) dari empat (4) NAP awal. ISP nasional (Tier 1) ini termasuk AT&T, Sprint dan Worldcom.

Tier 2 adalah regional ISP, atau mereka yang mempunyai keberadaan regional dan tersambung pada kurang dari tiga regional NAP. Contoh regional ISP adalah Adelphia, BellAtlantic.net, dan BellSouth.net.

Tier 3 adalah ISP lokal, atau mereka yang tidak mempunyai sambungan ke NAP tapi memberikan servis melalui ISP upstream.

Tentunya banyak cerita lainnya tentang NAP terutama agar secara ekonomis dapat mandiri. Salah satunya adalah Metropolitan Fiber Systems (MFS) — memutuskan untuk membuat NAP sendiri. Salah satu NAP pertama MFS adalah MEA-East. MEA kepanjangan dari "Metropolitan Area Ethernet." Melalui fasilitas MEA ini para ISP interkonek router mereka melalui Ethernet saja. Ethernet LAN kemudian hari berubah menjadi 100Mbps FDDI ring, dan "E" menjadi "Exchange".

North American Network Operators Group (NANOG) merupakan forum diskusi dan pertukaran informasi teknis dan koordinasi antar network service provider. Pertemuan mereka tiga (3) kali setahun, NANOG menjadi sangat penting untuk menjaga ke stabilan servis Internet di Amerika Utara. Awalnya memang di danai oleh NFS, saat ini NANOG menerima pendanaan dari registrasi konferens dan donasi vendor.

Di tahun 1988, DoD dan sebagian besar badan pemerintah di Amerika Serikat memilih untuk mengadopsi protokol OSI. TCP/IP mereka lihat sebagai solusi sementara yang hanya beroperasi di peralatan komputer yang terbatas saja. Di samping itu, OSI hanya tertinggal beberapa tahun dari TCP/IP. Pada bulan Agustus 1990, DoD memutuskan untuk menggunakan protokol OSI di semua produk komunikasi komputernya dan penggunaan TCP/IP tidak akan di lanjutkan. Di tambah, dalam definisi U.S. Government OSI Profile

(GOSIP) yang berisi set protocol yang harus di dukung untuk di jual ke pemerintah federal U.S. tidak memasukan TCP/IP ke dalamnya.

Walaupun dalam tekanan yang demikian keras, perkembangan TCP/IP terus berlanjut di akhir 1980-an bersama dengan perkembangan Internet. Perkembangan TCP/IP terjadi di lingkungan yang terbuka (open) walaupun komunitas terbuka ini relatif kecil karena sedikitnya site ARPA/NSF. Terutama di dorong oleh keyakinan "We reject kings, presidents, and voting. We believe in rough consensus and running code" [Dave Clark, M.I.T.]. Keyakinan ini yang ternyata membuahkan para hacker yang militan dan membangun berbagai perangkat yang dibutuhkan dalam pengembangan Internet. Pada akhirnya, di tahun 1994, National Institute for Standards and Technology (NIST) menyarankan agar GOSIP memasukan TCP/IP dan membuang persyaratan "hanya-OSI".

Definisi TCP/IP

TCP/IP (singkatan dari Transmission Control Protocol/Internet Protocol) adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (protocol suite). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut diimplementasikan dalam bentuk perangkat lunak (software) di sistem operasi. Istilah yang diberikan kepada perangkat lunak ini adalah TCP/IP stack.

Layer – layer TCP/IP

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). Jadi dengan demikian para desainer hardware dan jaringan dapat lebih paham dan fleksibel dalam membuat suatu sistem sehingga fungsi setiap mesin dapat berinteroperasi (interoperbility) satu sama lain. Beberapa layer TCP/IP antara lain:

Application Layer

Sesuai namanya, lapisan ini menjembatani interaksi manusia dengan perangkat lunak/software aplikasi. Application layer berisi beberapa protokol dan fungsi yang diperlukan oleh pemakai aplikasi untuk melakukan jenis komunikasi yang diinginkan. Contoh aplikasi Netware pada application layer adalah Netware Control Protocol (NCP) sedangkan untuk TCP/IP adalah FTP, SMTP dan TELNET.

Transport Layer

Transport layer menyediakan perbaikan untuk melayani network layer. Lapisan ini membantu dalam meyakinkan pengiriman data dapat diandalkan dan menggabungkan data yang telah dikirim dari ujung ke ujung. Untuk meyakinkan pengiriman data dapat diandalkan transport layer berdasarkan kepada mekanisme pengontrolan error yang disediakan oleh layer yang lebih rendah, jika layer yang dibawahnya tidah mampu untuk mengerjakan maka transport-layer akan bekerja lebih keras. Pada layer ini merupakan kesempatan terakhir untuk mengatasi error, tetapi pada kenyataannya transport layer menyediakan pengiriman yang bebas error.

Transport layer juga bertanggung jawab untuk membuat hubungan-hubungan secara logis pada sebuah hubungan jaringan, proses ini disebut multiplexing atau time sharing terjadi ketika nomer sambungan transport dibagi pada sambungan jaringan yang sama.

Transport layer adalah layer menengah dalam model OSI, 3 layer dibawahnya menyatakan bagian subnet dari model jaringan, sedangkan 3 layer diatasnya biasanya dipergunakan untuk proses softwering pada node. Transport layer biasanya dipergunakan

pula pada node yang tugasnya untuk merubah subnet yang tidak bisa diandalkan menjadi jaringan yang dapat lebih diandalkan.

Karena adanya multiplexing, beberapa elemen software atau pada OSI disebut dengan protocol-entity untuk membagi address (alamat) network-layer yang sama. Untuk mengidentifikasi setiap elemen software didalam transport layer diperlukan bentuk umum dalam pengalamatan, yang disebut dengan transport address yang biasanya merupakan kombinasi alamat network address dan nomer transport dari service access point. Untuk mengidentifikasi alamat tranport disebut dengan socket atau port-number.

Network Layer

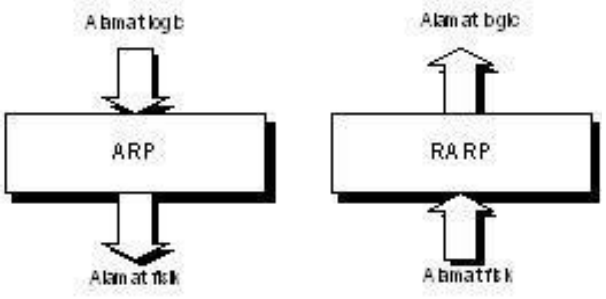
Network layer dibentuk berdasarkan hubungan node-to-node yang disediakan oleh data link layer. Pelayanan data link secara node to node menuju jaringan akan menjadi meningkat dengan adanya layer ini, sehingga data link layer dapat menambah pelayanan untuk rute lintasan sejumlah packet (bagian dari informasi yang berada pada network layer) diantara beberapa node dihubungkan melewati jaringan yang kompleks secara berubah-ubah.

Disamping melayani proses routing, network layer membantu menghilangkan kemacetan dengan cara mengatur aliran data. Disamping itu network layer dapat membuat kemungkinan agar dua jaringan dapat dihubungkan menerapkan uniform addressing mecanism (suatu mekanisme untuk pengalamatan sejenis).

Sebagai contoh jaringan lokal Ethernet dan Token ring memiliki alamat data link yang berbeda tipenya, untuk menghubungkan dua jaringan tersebut maka diperlukan uniform addressing mechanism yang dapat dimengerti oleh Etrhernet maupun Token ring. Untuk jaringan yang berbasis Novel Netware maka digunakan Internet Packet Exchange (IPX) sebagai protokol network layer, sedangkan jaringan berbasis TCP/IP digunakan internet-protocol (IP).

ARP, RARP

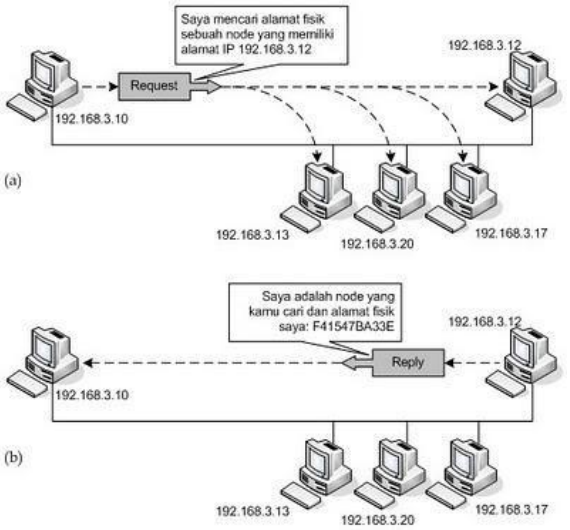
Address Resolution Protocol (ARP) dan Reverse Address Resolution Protocol (RARP) menggunakan alamat fisik unicast dan broadcast. Sebagai contoh Ethernet akan menggunakan alamat FFFFFFFFFFFF16 sebagai alamat broadcast. Sesungguhnya ARP dan RARP adalah proses pemetaan alamat fisik (Physical Address) seperti alamat NIC yang berasosiasi kepada logical address (alamat IP) atau sebaliknya.



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*).



Berikut adalah format paket ARP:

Hardware Type : adalah tipe hardware/perangkat keras. Banyak bit dalam field ini adlah 16 bit. Sebagai contoh untuk Ethernet mempunyai tipe 1.

Protocol Type : adalah tipe protokol di mana banyaknya bit dalam field ini 16 bit. Contohnya, untuk protokol IPv4 adalah 080016.

Hardware Length : field berisi 8 bit yang mendefinisikan panjang alamat fisik. Contohnya, untuk Ethernet, panjang alamat fisik adalah 6 byte.

Protocol Length : field berisi 8 bit yang mendefinisikan panjang alamat logika dalam satuan byte. Contoh : untuk protokol IPv4 panjangnya adalah 4 byte.

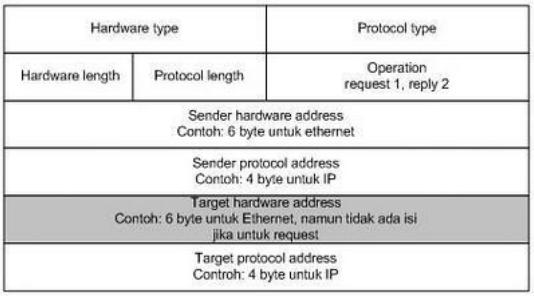
Operation Request & Reply: field berisi 16 bit ini mendefinisikan jenis paket untuk ARP apakah itu berjenis ARP request atau ARP reply.

Sender Hardware Address : banyaknya field adalah variabel yang mendefinisikan alamat fisik dari pengirim. Untuk Ethernet panjang nya 6 byte.

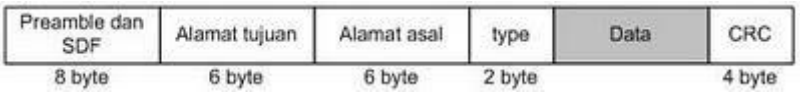
Sender Protocol Address : field ini panjangnya juga variabel dan untuk mendefiniskan alamat logika (alamat IP) dari pengirim.

Target Hardware Address : field ini panjangnya juga variabel yang mendefiniskan alamat fisik daripada target. Pada paket ARP request, field ini isinya 0 semua.

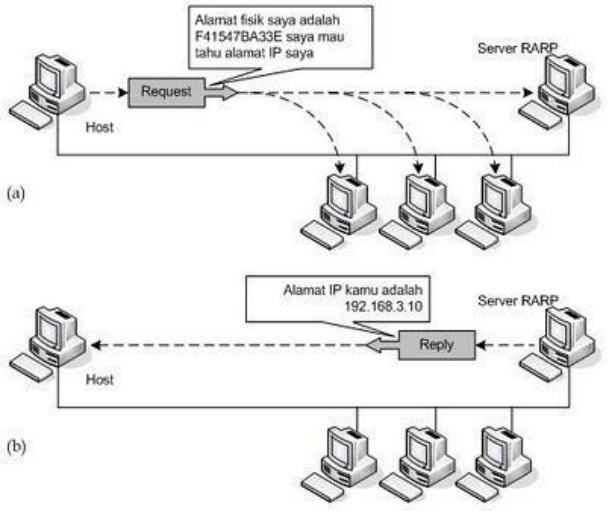
Target Protocol Address : field ini panjangnya juga variabel dan mendefinisikan alamat logika (IP) dari target.



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



RARP didesain 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 tipe 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. Format Paket RARP persis sama dengan format paket ARP.



IPv4 dan IPv6

Internet Protokol Versi 4 (IPv4) adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protocol jaringan TCP/IP yang menggunakan protokol IP versi 4. IP versi ini memiliki keterbatasan yakni hanya mampu mengalamati sebanyak 4 miliar host komputer di seluruh dunia. Contoh alamat IPv4 adalah 192.168.0.3

Pada IPv4 ada 3 jenis Kelas, tergantung dari besarnya bagian host, yaitu kelas A (bagian host sepanjang 24 bit , IP address dapat diberikan pada 16,7 juta host) , kelas B (bagian host sepanjang 16 bit = 65534 host) dan kelas C (bagian host sepanjang 8 bit = 254 host). Administrator jaringan mengajukan permohonan jenis kelas berdasarkan skala jaringan yang dikelolanya. Konsep kelas ini memiliki keuntungan yaitu : pengelolaan rute informasi tidak memerlukan seluruh 32 bit tersebut, melainkan cukup hanya bagian jaringannya saja, sehingga besar informasi rute yang disimpan di router, menjadi kecil. Setelah address jaringan diperoleh, maka organisasi tersebut dapat secara bebas memberikan address bagian host pada masing-masing hostnya.

Pemberian alamat dalam internet mengikuti format IP address (RFC 1166). Alamat ini dinyatakan dengan 32 bit (bilangan 1 dan 0) yang dibagi atas 4 kelompok (setiap kelompok

terdiri dari 8 bit atau oktet) dan tiap kelompok dipisahkan oleh sebuah tanda titik. Untuk memudahkan pembacaan, penulisan alamat dilakukan dengan angka desimal, misalnya 100.3.1.100 yang jika dinyatakan dalam binary menjadi 01100100.00000011.00000001.01100100. Dari 32 bit ini berarti banyaknya jumlah maksimum alamat yang dapat dituliskan adalah 2 pangkat 32, atau 4.294.967.296 alamat. Format alamat ini terdiri dari 2 bagian, net-id dan host-id. Net-id sendiri menyatakan alamat jaringan sedangkan host-id menyatakan alamat lokal (host/router). Dari 32 bit ini, tidak boleh semuanya angka 0 atau 1 (0.0.0.0 digunakan untuk jaringan yang tidak dikenal dan 255.255.255.255 digunakan untuk broadcast). Dalam penerapannya, alamat internet ini diklasifikasikan ke dalam kelas (A-E).

Alasan klasifikasi ini antara lain:
- Memudahkan sistem pengelolaan dan pengaturan alamat-alamat.
- Memanfaatkan jumlah alamat yang ada secara optimum (tidak ada alamat yang terlewat).
- Memudahkan pengorganisasian jaringan di seluruh dunia dengan membedakan jaringan tersebut termasuk kategori besar, menengah, atau kecil.
- Membedakan antara alamat untuk jaringan dan alamat untuk host/router.

Internet Protokol Versi 6 (IPv6) memiliki versi design berbeda dan memiliki kegunaan lebih dibanding IPv4. Disertai dengan tumbuhnya inovasi-inovasi perangkat berteknologi, maka Negara-negara di dunia dituntut mampu bersaing atau setidaknya secara bertahap mulai untuk mengimplementasikan IPv6. Menurut jurnal Internet Protocol, diperkirakan tak sampai tahun 2011, jatah alamat IP yang masih belum digunakan saat ini akan habis. Maka munculah suatu metode pengalamatan baru yang dikenal dengan sebutan IPv6. Di Indonesia, salah satu penyedia jasa Internet, Indosat Mega Media (Indosat M2), sejak 2004 telah siap menyewakan jaringan IPv6 ini.

IPv6 merupakan metode pengalamatan IP yang perlahan-lahan mulai menggantikan IPv4. IPv6 digunakan sebagai pengalamatan karena keterbatasan jumlah IP yang dimiliki oleh IPv4, mengingat semakin bertambahnya perangkat berbasis IP saat ini. IPv6 atau Internet Protocol version 6 adalah protokol Internet terbaru yang merupakan pengembangan lebih lanjut dari protokol yang dipakai saat ini, IPv4 (Internet Protocol version 4). Pengalamatan IPv6 menggunakan 128-bit alamat yang jauh lebih banyak dibandingkan dengan pengalamatan 32-bit milik IPv4. Dengan kapasitas alamat IP yang sangat besar pada IPv6, setiap perangkat yang dapat terhubung ke Internet (komputer desktop, laptop, personal digital assistant, atau telepon seluler GPRS/3G) bisa memiliki alamat IP yang tetap. Sehingga, cepat atau lambat setiap perangkat elektronik yang ada dapat terhubung dengan Internet melalui alamat IP yang unik.

Protokol IPv6 ini memiliki beberapa fitur baru yang merupakan perbaikan dari IPv4, diantaranya:

Memiliki format header baru

Header pada IPv6 memiliki format baru yang didesain untuk menjaga agar overhead header minimum, dengan menghilangkan field-field yang tidak diperlukan serta beberapa field opsional Perbandingan IPv4 dan IPv6 yang ditempatkan setelah header IPv6. Header IPv6 sendiri besarnya adalah dua kali dari besar header dari IPv4.

Range alamat yang sangat besar

IPv6 memiliki 128-bit atau 16-byte untuk masing-masing alamat IP source dan destination. Sehingga secara logika IPv6 dapat menampung sekitar 3.4 x 1038 kemungkinan kombinasi alamat.

Konfigurasi pengalamatan secara stateless dan statefull
IPv6 mendukung konfigurasi pengalamatan secara statefull, seperti konfigurasi alamat menggunakan server DHCP, atau secara stateless yang tanpa menggunakan server DHCP. Pada konfigurasi kedua, host secara otomatis mengkonfigurasi dirinya sendiri dengan alamat IPv6 untuk link yang disebut dengan alamat link-lokal dan alamat yang diturunkan dari prefik yang ditransmisikan oleh router local.

Built-in security
Dukungan terhadap IPsec memberikan dukungan terhadap keamanan jaringan dan menawarkan interoperabilitas antara implementasi IPv6 yang berbeda.

Dukungan yang lebih baik dalam hal QoS
Pada header IPv6 terdapat trafik yang di identifikasi menggunakan field Flow Label, sehingga dukungan QoS dapat tetap diimplementasikan meskipun payload paket terenkripsi melalui IPsec.

Protokol baru untuk interaksi node
Pada IPv6 terdapat Protokol Neighbor Discovery yang menggantikan Address Resolution Protokol.

Ekstensibilitas
IPv6 dapat dengan mudah ditambahkan fitur baru dengan menambahkan header ekstensi setelah header IPv6. Ukuran dari header ekstensi IPv6 ini hanya terbatasi oleh ukuran dari paket IPv6 itu sendiri.

Perbedaan antara IPv4 dan IPv6 menurut Kementerian Komunikasi dan Informatika (Kominfo):

Fitur
IPv4: Jumlah alamat menggunakan 32 bit sehingga jumlah alamat unik yang didukung terbatas 4.294.967.296 atau di atas 4 miliar alamat IP saja. NAT mampu untuk sekadar memperlambat habisnya jumlah alamat IPv4, namun pada dasarnya IPv4 hanya menggunakan 32 bit sehingga tidak dapat mengimbangi laju pertumbuhan internet dunia.

IPv6: Menggunakan 128 bit untuk mendukung 3.4 x 10^38 alamat IP yang unik. Jumlah yang masif ini lebih dari cukup untuk menyelesaikan masalah keterbatasan jumlah alamat pada IPv4 secara permanen.

Routing
IPv4: Performa routing menurun seiring dengan membesarnya ukuran tabel routing. Penyebabnya pemeriksaan header MTU di setiap router dan hop switch.

IPv6: Dengan proses routing yang jauh lebih efisien dari pendahulunya, IPv6 memiliki kemampuan untuk mengelola tabel routing yang besar.

Mobilitas
IPv4: Dukungan terhadap mobilitas yang terbatas oleh kemampuan roaming saat beralih dari satu jaringan ke jaringan lain.

IPv6: Memenuhi kebutuhan mobilitas tinggi melalui roaming dari satu jaringan ke jaringan lain dengan tetap terjaganya kelangsungan sambungan. Fitur ini mendukung perkembangan aplikasi-aplikasi.

Keamanan
IPv4: Meski umum digunakan dalam mengamankan jaringan IPv4, header IPsec merupakan fitur tambahan pilihan pada standar IPv4.

IPv6: IPsec dikembangkan sejalan dengan IPv6. Header IPsec menjadi fitur wajib dalam standar implementasi IPv6.

Ukuran header
IPv4: Ukuran header dasar 20 oktet ditambah ukuran header options yang dapat bervariasi.

IPv6: Ukuran header tetap 40 oktet. Sejumlah header pada IPv4 seperti Identification, Flags, Fragment offset, Header Checksum dan Padding telah dimodifikasi.

Fragmentasi
IPv4: Dilakukan di setiap hop yang melambatkan performa router. Proses menjadi lebih lama lagi apabila ukuran paket data melampaui Maximum Transmission Unit (MTU) paket dipecah-pecah sebelum disatukan kembali di tempat tujuan.

IPv6: Hanya dilakukan oleh host yang mengirimkan paket data. Di samping itu, terdapat fitur MTU discovery yang menentukan fragmentasi yang lebih tepat menyesuaikan dengan nilai MTU terkecil yang terdapat dalam sebuah jaringan dari ujung ke ujung.

Configuration
IPv4: Ketika sebuah host terhubung ke sebuah jaringan, konfigurasi dilakukan secara manual.

IPv6: Memiliki fitur stateless auto configuration dimana ketika sebuah host terhubung ke sebuah jaringan, konfigurasi dilakukan secara otomatis.

Voice Over IP

Voice Over Internet Protocol (juga disebut VoIP, IP Telephony, Internet telephony atau Digital Phone) adalah teknologi yang memungkinkan percakapan suara jarak jauh melalui media internet. Data suara diubah menjadi kode digital dan dialirkan melalui jaringan yang mengirimkan paket-paket data, dan bukan lewat sirkuit analog telepon biasa. VoIP yang disebut juga internet telephon yang merupakan teknologi yang menawarkan solusi teleponi melalui jaringan paket (IP Network). VoIP mereduksi biaya mereduksi biaya percakapan sampai 60%. Sebagai contoh, tarif percakapan lewat telepon kabel di Amerika Serikat Rp 6.000/menit atau US$ 66 sen, sementara tarif VoIP hanya Rp 1.300/menit atau sekitar US$ 14 sen. Selain Reduksi biaya, VoIP juga menyederhanakan sistem, memudahkan OAM dan mendukung aplikasi multimedia.

VoIP sebenarnya adalah aplikasi internet biasa seperti layanan www dan email. VoIP sebagai layanan Internet biasa disebut IP Telephony. Infrastruktur internet dibutuhkan agar dapat menggunakan dann atau menyediakan layanan VoIP. VoIP secara umum berarti mengirimkan informasi suara secara digital dalam bentuk paket data. Dibandingkan secara tradisional, pengiriman informasi suara melalui saluran analog PSTN (Public Switching Telephone Network). VoIP yang disebut juga internet telephony merupakan teknologi yang menawarkan solusi telepon melalui jaringan paket (IP Network). Teknologi yang awalnya dianggap menyimpang dari kelaziman ternyata saat ini menjanjikan suatu kelebihan, sehingga banyak pihak yang ikut melibatkan diri. Secara umum, VoIP didefinisikan sebagai suatu sistem yang menggunakan jaringan internet untuk mengirimkan data paket suara dari suatu tempat ke tempat yang lain menggunakan perantara protokol IP.

Komponen Fungsional VoIP

1. Voice Calling Device

Peralatan untuk membangkitkan dan menerima call.

IP Telephone

- Merupakan peralatan berbentuk telepon yang terhubung langsung ke jaringan internet
- Mempunyai *built-in software* yang bisa berkomunikasi dengan perlatan VoIP lain di jaringan Internet, dan protocol yang bisa mengirim paket data voice
- Terhubung ke jaringan menggunakan jack RJ-45 atau wifi VoIP Phone yang terhubung dengan jaringan wireless IEEE 802.11

Softphone

- Merupakan software yang mengimplementasikan fungsi-fungsi telepon
- Bisa dipasang di PC atau PDA
- Dengan softphone, user VoIP tidak perlu lagi menambahi peralatan telepon dijaringannya.

Telepon Analog

Peralatan telepon analog yang terhubung ke PSTN

Analog Telephone Adapter (ATA)

- Peralatan yang digunakan jika sebuah pesawat telepon analog akan dihubungkan langsung ke jaringan internet
- Peralatan ini mentranslasikan bentuk informasi digital dari jaringan internet ke dalam bentuk informasi analog yang diterima pesawat telepon atau sebaliknya

2. Gateway

Sebagai pembatas dari dua jaringan yang berbeda, dan bertugas membantu agar kedua jaringan tersebut dapat saling berkomunikasi.

Terdiri dari dua komponen utama:

a. Gateway Controller
   - Mentranslasikan sebuah informasi ke dalam format yang dapat dimengerti oleh masing-masing jaringan
   - Mentranslasikan *SIP signaling* di jaringan Internet ke *SS7 signaling* di jaringan PSTN atau sebaliknya

b. Media Gateway

   Melakukan transcoding dari packet-based di jaringan IP ke dalam bentuk frame-frame TDM di PSTN atau sebaliknya.

3. Media Server

Memproses RTP stream dari VoIP untuk mendekodekan nada DTMF, mencampur beberapa media stream kedalam bentuk sebuah conference, membunyikan pengumuman, memproses script Voice XML, speech recognition, konversi text to speech, perekaman audio.

Media ini bisa diintegrasikan bersama gateway.

4. **Session Control Server**

Menyediakan fungsi-fungsi level sesi, seperti otentikasi, otorisasi dan perijinan panggilan.

Merutekan dan memforward panggilan ke jaringan atau service provider yang lain.

Menyediakan layanan caller IP, call waiting dan dapat berinteraksi dengans erver aplikasi.

Merupakan komponen optional pada arsitektur VoIP, bisa menjadi salah satu bagian dari gateway controller.
Juga bisa dianggap sebagai SIP server atau call agent

CIDR

Classless Inter Domain Routing (CIDR) adalah sebuah cara alternatif untuk mengklasifikasikan alamat – alamat IP berbeda dengan sistem klasifikasi ke dalam kelas A, kelas B, kelas C, kelas D, dan kelas E. Disebut juga sebagai supernetting. CIDR merupakan mekanisme routing yang lebih efisien dibandingkan dengan cara yang asli, yakni dengan membagi alamat IP jaringan ke dalam kelas-kelas A, B, dan C. Masalah yang terjadi pada sistem yang lama adalah bahwa sistem tersebut meninggalkan banyak sekali alamat IP yang tidak digunakan. Sebagai contoh, alamat IP kelas A secara teoritis mendukung hingga 16 juta host komputer yang dapat terhubung, sebuah jumlah yang sangat besar. Dalam kenyataannya, para pengguna alamat IP kelas A ini jarang yang memiliki jumlah host sebanyak itu, sehingga menyisakan banyak sekali ruangan kosong di dalam ruang alamat IP yang telah disediakan. CIDR dikembangkan sebagai sebuah cara untuk menggunakan alamat-alamat IP yang tidak terpakai tersebut untuk digunakan di mana saja. Dengan cara yang sama, kelas C yang secara teoritis hanya mendukung 254 alamat tiap jaringan, dapat menggunakan hingga 32766 alamat IP, yang seharusnya hanya tersedia untuk alamat IP kelas B.

CIDR adalah mekanisme routing yang lebih efisien dibandingkan dengan cara yang asli, yakni dengan membagi alamat IP jaringan ke dalam kelas-kelas A, B, dan C.

CIDR merupakan sebuah cara alternatif untuk mengklasifikasikan alamat-alamat IP berbeda dengan sistem klasifikasi ke dalam kelas A, kelas B, kelas C, kelas D, dan kelas E.

Masalah yang terjadi pada sistem yang lama adalah bahwa sistem tersebut meninggalkan banyak sekali alamat IP yang tidak digunakan.

Sebagai contoh, alamat IP kelas A secara teoritis mendukung hingga 16 juta host komputer yang dapat terhubung, sebuah jumlah yang sangat besar. Dalam kenyataannya, para pengguna alamat IP kelas A ini jarang yang memiliki jumlah host sebanyak itu, sehingga menyisakan banyak sekali ruangan kosong di dalam ruang alamat IP yang telah disediakan.

CIDR dikembangkan sebagai sebuah cara untuk menggunakan alamat-alamat IP yang tidak terpakai tersebut untuk digunakan di mana saja. Dengan cara yang sama, kelas C yang secara teoritis hanya mendukung 254 alamat tiap jaringan, dapat menggunakan hingga 32766 alamat IP, yang seharusnya hanya tersedia untuk alamat IP kelas B.

CIDR memakai network prefix dengan panjang tertentu. Network prefix ini menentukan jumlah bit sebelah kiri yang digunakan sebagai network ID. Contoh dari penulisan dari network previx adalah /18 dibelakang ip address. Contoh : 202.168.0.1 /18.

Contoh Kasus TCP/IP

1.) Ip 130.100.160.1 termasuk kedalam kelas mana ?

Penyelesaian:

Pertama kita lihat rentang Ip Adressnya atau octat pertamanya, ternyata masuk kedalam kelas B (128-191)

2.) Ada 3 buah komputer memiliki Ip Address berikut:
a.
130.200.32.2
b.
130.100.32.3
c.
130.200.63.3
Ip manakah yang dapat saling terhubung?

Penyelesaian:

Analisa terlebih dahulu alamat Ip tersebut ternyata kelas B, karena kelas B maka octat
pertama dan kedua merupakan Network ID yang harus sama dan didapat komputer A dan C yang memiliki Network ID yang sama yaitu 130.200 dan Host ID yang berbeda yaitu 32.2 dan 63.3. Kesimpulan komputer A dan C dapat saling berhubungan.