BAB 1 – IPv6

Internet Protokol (IP) adalah protokol jaringan yang paling sukses dalam sejarah protokol jaringan. Tidak hanya semua informasi yang mengalir melalui Internet yang terkandung dalam paket yang sesuai dengan Internet Protokol, namun IP juga telah menyingkirkan pasar protokol lain yang digunakan dalam jaringan pribadi selama dua dekade terakhir. Jadi, apa jenis protokol baru mungkin bisa menantang keunggulan IP? Sebuah versi baru dari IP, tentu saja.

Dan persisnya adalah IPv6. Yaitu langkah berikutnya dalam evolusi alami dari Internet Protokol. Dalam hal versi baru dari IP yang diperlukan, para perancang IP original menyertakan bidang yang berisi nomor versi dalam layout paket. Dengan cara ini, tidak akan pernah ada risiko bahwa isi dari paket data akan disalahartikan, karena penerima mengasumsikan versi yang berbeda dari Internet Protokol yang digunakan oleh pengirim. IP hari ini menetapkan nomor versi dalam setiap paket untuk 4, sehingga IPv4. Nomor versi 1, 2, dan 3 dibiarkan tidak terpakai. Nilai-nilai terendah dan tertinggi (0 dan 15 untuk nomor versi IP) terlindungi. IP nomor versi 5 dialokasikan ke protokol non-IP yang harus hidup berdampingan dengan IP dalam kondisi tertentu, jadi 6 adalah pilihan yang logis untuk IP generasi berikutnya.

MENGAPA IPv6?

Pada pertengahan 1980-an, Internet Engineering Task Force (IETF) diciptakan untuk memberikan pengaturan di mana orang-orang yang membangun dan menjalankan jaringan yang berhubungan dengan internet atau peralatan jaringan bisa berinteraksi. Dalam IETF, di sisi lain setiap orang dapat berpartisipasi melalui email dan mendapatkan dokumen RFC secara gratis. Sebagian besar pekerjaan dilakukan melalui email, sehingga bahkan mereka yang tidak mampu bepergian ke pertemuan IETF yang diadakan tiga kali setahun dapat berpartisipasi.

Pada awal 1990, IETF menyadari bahwa ruang alamat IPv4 habis pada tingkat yang berbahaya. Sekitar tahun 1990, sekitar seperdelapan dari 3,7 miliar menggunakan alamat IPv4 yang diberikan, nomor yang dua kali lipat setiap lima tahun. Pada tingkat ini, alamat IP terakhir akan habis pada tahun 2005. Ini rupanya azab yang akan datang mendorong IETF untuk mulai bekerja pada “IP generasi berikutnya” (IPng), yang akhirnya menyebabkan terciptanya standar IPv6. Pertama IPv6 RFC diterbitkan pada tahun 1995 (dengan banyak lagi yang akan datang). Perbedaan utama antara IPv4 dan IPv6 adalah bahwa IPv6 menggunakan alamat yang 128 bit, bukan 32 bit pada IPv4, sehingga tidak kurang dari 3,4 × 1038 alamat individu.

KEUNTUNGAN IPv6

Ruang Alamat Lebih

Keuntungan yang paling jelas dan paling penting dari IPv6 adalah bahwa alamat lebih panjang dan membuat ruang alamat yang jauh lebih besar. Jumlah aktual alamat individu yang mungkin dengan 128 bit melampaui angka siapapun kecuali astronom dan fisikawan partikel akrab dengan: 340.282.366.920.938.463.463.374.607.431.768.211.456
Jumlah alamat IPv4 yang mungkin tampaknya biasa dengan perbandingan: 4294967296

Ruang alamat 128-bit cukup besar untuk memiliki 155 miliar IPv4 Internet pada setiap milimeter persegi permukaan bumi, termasuk lautan. Dalam U.S. measurements, itu cukup untuk memasok setiap inci persegi dari permukaan bumi dengan setara dengan seratus triliun IPv4 Internet.

Tujuan asli memberikan lebih banyak ruang alamat untuk menghindari kehabisan alamat sama sekali tidak mendesak seperti dulu, karena alamat IPv4 tidak lagi digunakan pada tingkat yang eksponensial. Bahkan mungkin ada cukup alamat IPv4 selama beberapa dekade yang akan datang, walaupun itu tentu asumsi yang berbahaya untuk membuatnya. Di sisi lain, tidak cukup ada alamat IPv4 untuk setiap orang di bumi, di Amerika Utara dan Eropa sudah menggunakan banyak lebih dari satu alamat per orang.

Inovasi

NAT pada dasarnya adalah beberapa host berbagi alamat IP yang diterjemahkan, dan memiliki host di tempat lain di Net terhubung ke salah satu host NAT'ed akan menjadi masalah. Hal ini mirip dengan situasi di mana beberapa ponsel yang terhubung ke satu baris untuk panggilan keluar, tidak ada banyak masalah, tetapi tidak ada cara mudah untuk mendapatkan panggilan masuk dikirimkan ke ponsel yang tepat.

Untuk layanan seperti Web dan email, tidak ada banyak masalah. Web browser atau email client selalu kontak server. Untuk layanan ini, jumlahnya terbatas dari server untuk menerima koneksi masuk. Namun, dengan aplikasi jenis lain, setiap orang adalah sebuah server. Contohnya adalah Voice over IP (VoIP), di mana telepon IP-enabled terhubung langsung satu sama lain, dengan aplikasi sejenis seperti konferensi video, dan semua jenis aplikasi peer-to-peer. NAT adalah batu sandungan nyata ketika datang untuk mengadopsi teknologi baru ini. IPv6 dapat memecahkan ini dengan memberikan masing-masing sistem IP-enabled alamat sendiri yang memungkinkan untuk inovasi baru.

Konfigurasi Tanpa State

IPv4 host biasanya menggunakan Dynamic Host Configuration Protocol (DHCP) untuk mendapatkan alamat dari server atau router. Ini umumnya bekerja dengan baik, tapi itu memiliki dua kelemahan, yaitu: tidak ada jaminan bahwa sebuah host akan menerima alamat yang sama ketika mengulang permintaan pada beberapa waktu kemudian. IPv6 menambahkan "stateless autoconfiguration" sebagai sarana untuk host yang akan mengkonfigurasi alamat. Dengan stateless autoconfiguration berlaku (dan biasanya), tuan rumah mendengarkan router untuk menceritakannya tentang 64-bit yang digunakan untuk bagian atas dari alamat IPv6. Semua host terhubung ke jaringan yang sama ini yaitu 64-bit. Host kemudian menurunkan ke bawah 64-bit dari alamat MAC Ethernet mereka untuk sampai pada 128-bit alamat IPv6 penuh. Jika ada beberapa router yang mengiklankan berbagai prefiks 64-bit, host cukup membuat beberapa alamat dengan menggabungkan masing-masing awalan dengan nilai 64-bit MAC yang diturunkan. Ini berarti bahwa kecuali ada keadaan khusus, tuan rumah akan selalu memiliki alamat yang sama tanpa konfigurasi per-host apapun. Dengan IPv6, mengkonfigurasi manual alamat server tidak lagi diperlukan, karena tidak ada lagi "state" (informasi konfigurasi) yang bisa hilang atau rusak.

Renumbering

Mengubah alamat IP untuk sekelompok host menjadi jauh lebih mudah sekarang, karena semua yang diperlukan untuk router untuk menghentikan iklan awalan lama dan memulai iklan yang baru, host secara otomatis akan membuat alamat baru bagi diri mereka sendiri dan melihat bahwa alamat lama tidak lagi "segar". Untuk menghindari gangguan dalam sesi yang sedang berlangsung ketika alamat lama tiba-tiba dihapus, alamat lama hanya "ditinggalkan" pada awalnya, yang berarti mereka mungkin masih digunakan dalam sesi komunikasi yang ada tetapi untuk sesi baru dibentuk tidak menggunakan alamat yang sudah ditinggalkan.

Efisiensi

Peningkatan efisiensi dalam IPv6 adalah sebagai berikut:

- Header IPv6 memiliki panjang tetap.
- Header IPv6 dioptimalkan untuk pengolahan sampai dengan 64 bit pada satu waktu (32 di IPv4).
- Header checksum IPv4 yang dihitung setiap kali paket melewati router telah dihapus dari IPv6.
- Router tidak lagi diperlukan untuk paket kebesaran fragmen, mereka hanya dapat sinyal sumber untuk mengirim paket yang lebih kecil.
- Semua siaran untuk fungsi penemuan digantikan oleh multicast. Hanya host yang aktif mendengarkan multicast terganggu, daripada semua host, seperti siaran.

Keamanan

Mungkin mitos yang paling bertahan lama mengelilingi IPv6 adalah bahwa ia akan lebih aman dibanding IPv4. Mitos ini mungkin dipicu oleh fakta bahwa IPv6 memiliki "keharusan" mendukung IPsec. IPsec memberikan authentikasi dan enkripsi pada tingkat IP, sehingga memungkinkan untuk setiap aplikasi yang berjalan di atas IP harus dilindungi terhadap data yang disadap atau diubah dalam perjalanan Namun, IPsec juga tersedia dalam banyak implementasi IPv4 saat ini, sementara fakta bahwa itu seharusnya disertakan dalam IPv6 tidak berarti bahwa itu tersedia untuk aplikasi secara default, IPsec memerlukan upaya konfigurasi yang luas.

Dalam prakteknya, bagaimanapun, menjalankan IPsec melalui IPv4 adalah sebuah tantangan karena NAT sering menemukan jalannya. IPsec opsi yang dirancang untuk melindungi seluruh paket akan mendeteksi modifikasi paket yang diperkenalkan oleh NAT dan membuang paket tersebut pergi. Pilihan lainnya adalah IPsec dasarnya tidak bertentangan dengan NAT tetapi terhambat oleh kenyataan bahwa mekanisme negosiasi yang dibuat oleh asosiasi keamanan IPsec jadi bingung ketika kedua ujung tidak setuju pada alamat IP masing-masing (karena diterjemahkan di tengah) . Walaupun permasalahan ini dibahas dalam IPv4, itu masih lebih mudah untuk menjalankan IPsec di IPv6. IPv6 tidak memiliki satu keunggulan keamanan atas IPv4, meskipun di IPv6, Ethernet biasanya mendapatkan 64 bit untuk nomor host. Dengan IPv4, tidak pernah lebih dari 16 bit dan sering jauh lebih sedikit. Ini berarti bahwa seorang penyerang atau worm mencari sesuatu untuk hack atau menginfeksi memiliki waktu jauh lebih sulit dalam pemindaian subnet Ethernet tunggal dalam IPv6 dibandingkan pemindaian seluruh Internet IPv4.

Mobilitas

Seperti IPsec, dukungan untuk mobilitas diperlukan untuk IPv6. Dalam konteks ini, mobilitas berarti bahwa host dapat terhubung ke jaringan di tempat yang berbeda pada waktu yang berbeda, menerima IP yang berbeda alamat setiap kali tapi mempertahankan sesi komunikasi untuk "alamat rumah" nya sementara. Namun, berfungsi penuh, jika tidak terlalu efisien, dukungan mobilitas juga tersedia untuk beberapa IPv4 implementasi, sementara itu seringkali masih kurang dalam implementasi IPv6 karena standar Mobile IPv6 belum cukup diselesaikan.

Qos

Dalam hal ini sering dikatakan bahwa IPv6 memiliki dukungan yang lebih baik untuk memberikan tambahan "Quality of Service" (QoS), atau dengan kata lain, mekanisme untuk memprioritaskan lalu lintas tertentu pada lalu lintas lainnya. Ini tidak terjadi. IPv4 dan IPv6 baik dukungan prioritas lalu lintas dengan menggunakan medan kecil di header yang digunakan untuk menahan "Type of Service" dan informasi prioritas.

ROUTING

Telah dikatakan bahwa routing akan ditingkatkan dalam IPv6. Sayangnya, itu persis sama seperti pada IPv4, kecuali bahwa alamat yang lebih besar dan kita bisa menghindari beberapa kesalahan yang dibuat dengan menetapkan address space IPv4.

MASA TRANSISI AKAN JADI TERLALU MAHAL

Dalam kasus-kasus di mana perangkat keras yang ada tidak dapat ditingkatkan untuk mendukung IPv6, transisi ke IPv6 memang akan menjadi mahal. Namun, masalahnya adalah harus mengganti hardware sebagian besar dengan router sangat besar yang digunakan oleh Internet Service Provider dan perusahaan besar. Jika router ini memiliki dukungan hardware khusus untuk routing IPv4 yang tidak kompatibel dengan IPv6, router benar-benar berguna untuk IPv6 atau kinerja secara dramatis lebih rendah karena IPv6 harus diproses dalam perangkat lunak tanpa akselerasi hardware. Namun, Routing hardware mutakhir memiliki umur ekonomi cukup singkat, sehingga masalah ini harus hilang dengan sendirinya dalam beberapa tahun. (Kecuali orang terus terus membeli perangkat keras IPv4-only).

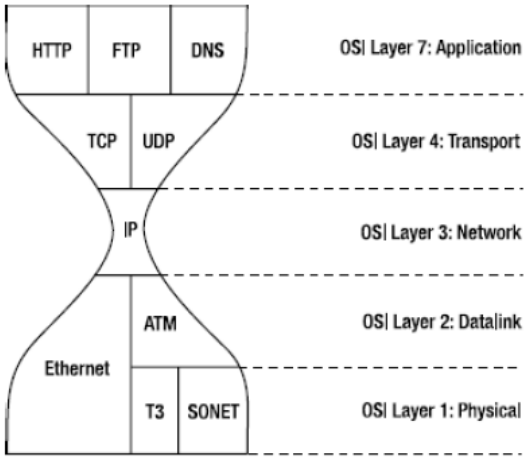
IPv6—When?

Semua protokol jaringan non-IP yang disebutkan dalam bab ini sangat banyak di gunakan 10 sampai 15 tahun yang lalu, tetapi IPv4 telah menggantikan mereka semua. Jadi kita tidak dapat mengesampingkan bahwa IPv4 pada gilirannya akan digantikan oleh IPv6 selama 10 sampai 15 tahun ke depan.

PERBEDAAN ANTARA IPV4, IPV6, DAN PROTOKOL LAINNYA

Telah dikatakan bahwa keluarga protokol IP terlihat seperti jam pasir. Jam pasir yang lebar di bagian atas, di mana terdapat banyak protokol aplikasi, dan menyempit ke satu set yang

lebih kecil dari protokol transport yang digunakan antara dua sistem yang mengambil bagian dalam sesi komunikasi tertentu, seperti TCP dan UDP. Sebuah layer pertama Internet Protocol yang bertanggung jawab untuk mendapatkan paket seluruh infrastruktur dasar membentuk tengah sempit jam pasir. Di bawah IP, kaca akan lebih luas lagi untuk mengakomodasi protokol link layer yang berbeda yang tahu bagaimana untuk mendapatkan paket dari satu IP router ke depan, seperti Ethernet, ATM, dan PPP. Setiap protokol datalink biasanya dapat dijalankan melalui berbagai protokol fisik yang bertanggung jawab untuk mendapatkan bit individu di seluruh kawat.



Gambar 1-1. Model jam pasir IP

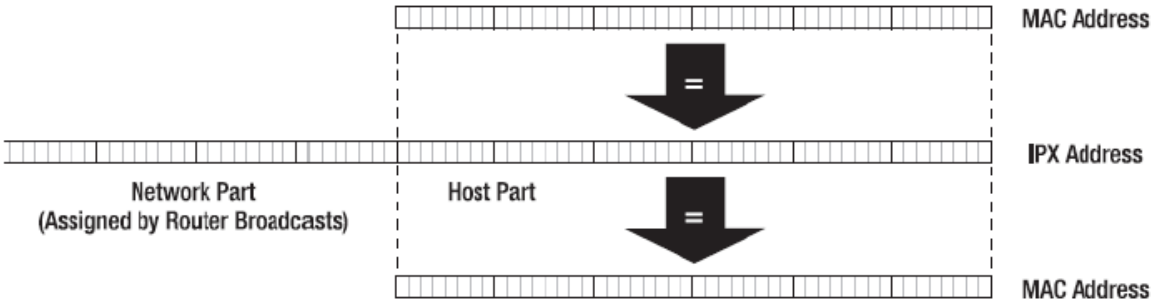
Model jam pasir menempatkan IP tepat di tengah-tengah keluarga protokol, duduk antara protokol tingkat rendah yang berbeda pada setiap hop di sepanjang jalan di satu sisi, dan protokol lapisan tinggi yang berfungsi end-to-end pada sisi lain. Model ini membuat IP- bagian satunya dari keluarga protokol yang harus didukung pada semua host dan semua router. Hal ini tidak berlaku untuk setiap lapisan lainnya. Misalnya, ketika dua host ingin menggunakan protokol SCTP baru di atas IP daripada TCP, mereka hanya dapat pergi ke depan dan melakukannya: router sepanjang jalan tidak harus memahami SCTP. Sebaliknya, hubungan antara dua router dapat ditingkatkan, misalnya dari Ethernet ke paket di atas SONET (POS), tanpa dampak apapun untuk host yang berkomunikasi melalui link ini melalui router yang bersangkutan, sebagai protokol lapisan yang lebih rendah akan dihapus dan diterapkan kembali setiap waktu paket melewati router.

Tugas dari Internet Protocol dan protokol lapisan jaringan alternatif (yang menempati tempat yang sama dalam jam pasir yang berbeda) adalah untuk membuat paket mengalir dari sumber ke tujuan mereka dan untuk mengakomodasi persyaratan yang berbeda protokol lapisan bawah yang ditemui di sepanjang perjalanan. IP mengimplementasikan “unreliable datagram service”, yang berarti bahwa paket (“datagrams”) dapat dikirim dari satu host terhubung ke jaringan ke host lain yang juga terhubung ke jaringan tanpa terlebih dahulu harus melakukan set up koneksi. Dalam kebanyakan kasus, datagram akan disampaikan ke tujuan, namun tidak ada jaminan. Untuk jaringan menyampaikan datagram tersebut ke tujuan mereka, paket harus benar-benar mandiri dan termasuk setidaknya sumber dan alamat tujuan dan protokol layer yang lebih tinggi yang ditujukan paket. Router sepanjang jalan melihat alamat untuk memutuskan arah mana paket harus pergi. Router membuat keputusan ini dengan bantuan tabel routing, yang tidak

lebih dari daftar panjang alamat tujuan berkisar bersama dengan pointer ke router tetangga yang bersedia untuk meneruskan paket untuk memperoleh alamat tersebut ke arah yang benar. Bila alamat tujuan tidak dapat ditemukan pada tabel routing, atau ada masalah lain, router mengirim kembali Internet Control Message Protocol (ICMP) untuk menginformasikan sumber paket menyinggung masalah.

IPX

Internetwork Packet Exchange (IPX) adalah protokol lapisan jaringan yang dikembangkan oleh Novell didasarkan pada pekerjaan oleh Xerox. Menggunakan alamat 80-bit, dengan 32 bit untuk bagian jaringan dari alamat dan 48 bit untuk bagian host. Bagian host dari alamat hanya berisi 48-bit Ethernet MAC address, sehingga pemetaan dari alamat IPX ke alamat Ethernet sangat sederhana. Sebuah host menciptakan alamat IPX untuk dirinya sendiri dengan mengambil alamat jaringan yang router secara berkala menyiarkan dan mengisi nya alamat MAC Ethernet di bagian host dari alamat. Gambar 1-2 menunjukkan bagaimana alamat IPX dibuat dan bagaimana alamat MAC Ethernet ditemukan dalam IPX bila diperlukan.

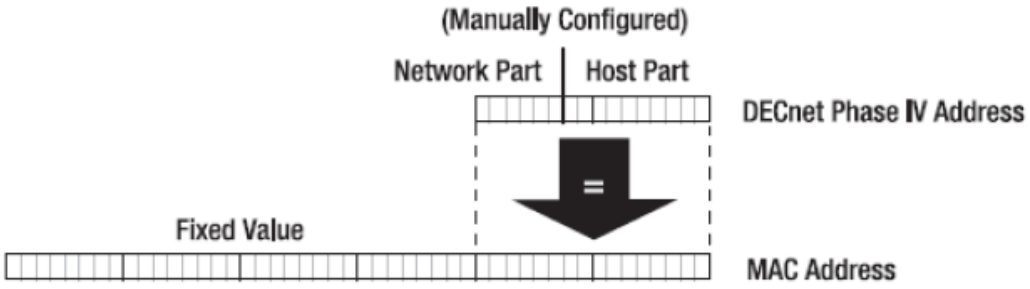


Gambar 1-2. Alamat IPX dan alamat MAC Ethernet

Ketika host IPX ingin berkomunikasi dengan host lain, maka melakukan pengecekan pertama jika koresponden yang dimaksud adalah pada Ethernet lokal dengan memeriksa apakah bagian jaringan host lokal dan alamat remote host yang sama. Jika paket mereka dapat dikirim langsung ke host remote karena itu terhubung ke Ethernet lokal yang sama sebagai tuan rumah. Jika tidak, paket akan dikirim ke router.

DECnet PHASE IV

Digital Equipment DECnet Phase IV menggunakan alamat yang panjangnya hanya 16 bit: 6 bit untuk bagian jaringan dan 10 untuk bagian host. DECnet memecahkan masalah pemetaan sebaliknya, chip Ethernet memprogram untuk mengabaikan alamat terbakar-in dan bukan menggunakan alamat MAC khusus yang mencakup alamat DECnet penuh. Alamat DECnet Phase IV harus dikonfigurasi secara manual. Gambar 1-3 menunjukkan bagaimana alamat DECnet cocok di dalam alamat MAC Ethernet.

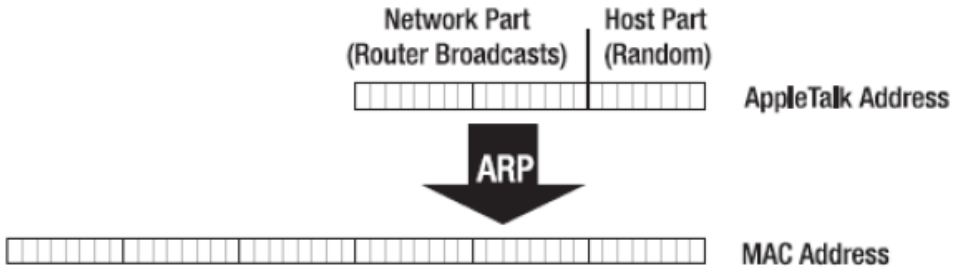


Gambar 1-3. Alamat DECnet Phase IV dan Alamat MAC Ethernet

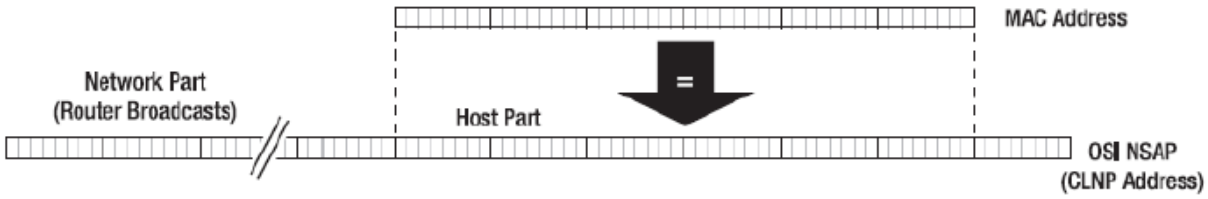
APPLETALK

AppleTalk oleh Apple menggunakan alamat yang tidak lebih lama dari alamat DECnet: 24 bit, dengan 16 bit untuk jaringan dan 8 bit untuk host. Seperti IPX, alamat jaringan dipelajari dari router, tapi tidak seperti IPX dan DECnet Phase IV, AppleTalk tidak menggunakan informasi tetap seperti alamat MAC Ethernet atau konfigurasi nilai secara manual untuk tiba di alamat host. Sebaliknya, tuan rumah hanya mengambil alamat dan memeriksa apakah itu sudah digunakan dengan mengirimkan pesan ke alamat ini. Jika tidak ada jawaban, alamat ini gratis, dan tuan rumah itu mulai menggunakannya. Jika ada jawaban, alamat sudah digunakan, sehingga host baru mengambil alamat lain dan mencoba lagi.

AppleTalk menggunakan protokol resolusi alamat yang sama dengan IP (dibahas kemudian dalam bab ini) untuk menemukan alamat MAC Ethernet lainnya AppleTalk host hanya tahu alamat untuk AppleTalk. Gambar 1-4 menunjukkan bagaimana alamat AppleTalk dibuat dan bagaimana hal itu diselesaikan ke alamat MAC Ethernet.



Pada 1980-an, Open System Interconnection (OSI) protokol keluarga diciptakan oleh International Organization for Standardization (ISO) dan International Telecommunication Union (ITU).Connectionless Network Protocol (CLNP) menyediakan layanan datagram. Pada OSI sejati, di mana bahkan rincian yang paling biasa ditentukan secara hati-hati, ada nama yang berbeda untuk Layanan Jaringan Connectionless (CLNS) dan protokol CLNP aktual yang digunakan untuk menyediakan layanan ini. Namun, nuansa ini hanya dihargai oleh para pecinta, sehingga CLNP dan CLNS sering digunakan secara bergantian. Beberapa orang bahkan hanya mengatakan "OSI," mengabaikan bagian berorientasi koneksi dari keluarga protokol (protokol X.25). Alamat CLNP dapat bervariasi dalam panjang, dengan maksimum 160 bit, dan dilengkapi pengenal sistem yang harus sama panjang untuk semua sistem di dalam jaringan CLNP. Ini berarti bahwa dalam prakteknya, alamat MAC Ethernet sering digunakan di sini, seperti yang ditunjukkan pada Gambar 1-5.



Gambar 1-5. Variabel panjang alamat CLNP dan alamat MAC Ethernet

Tidak seperti IPX, AppleTalk, IP, dan IPv6, CLNP host tidak mencoba untuk mencari tahu alamat yang bisa dijangkau secara lokal tanpa melibatkan router. Sebuah host CLNP hanya mengirimkan paket ke router. Router memungkinkan atau tidak mengirim pesan redirect untuk menginformasikan host yang alamat MAC nya dapat digunakan untuk berkomunikasi dengan host lain.

OSI JARGON

Bagi orang yang awam, OSI jargon bisa sangat membingungkan. Misalnya, sebuah host yang disebut End System (ES) dan sebuah router yang disebut Intermediate System (IS). Sebuah alamat MAC adalah Subnetwork Point of Attachment (SNPA), dan bahkan kata "address" dianggap tidak baik, sehingga Network Service Access Point (NSAP) digunakan sebagai gantinya. Router umumnya ditangani dengan Network Entity Title (NET) daripada NSAP.

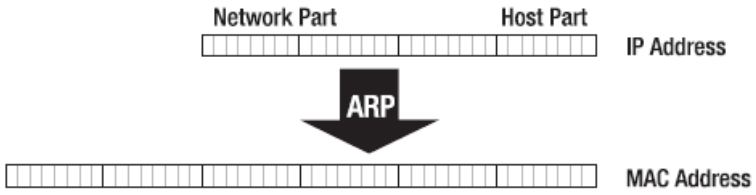
TCP/IP

TCP / IP dikembangkan oleh para peneliti terhubung ke US Department of Defense Advanced Research Projects Agency (ARPA DoD). Awalnya, ARPANET menggunakan Network Control Protocol (NCP) tunggal, tetapi sekitar tahun 1980, fungsi NCP terpecah antara IP dan protokol TCP. Seperti namanya, Internet Protocol ini dimaksudkan untuk menjadi sebuah protokol yang bisa menjadi penghubung beberapa jenis jaringan. Dengan demikian, alamat IP cukup pendek yaitu hanya 32 bit. Jaringan Kelas A memiliki 7 bit untuk penomoran jaringan dan 24 bit untuk penomoran host, jaringan kelas B memiliki 14 bit network dan 16 bit host, dan jaringan kelas C memiliki 21 bit untuk jaringan jumlah dan 8 untuk penomoran host. Sistem dengan tiga kelas alamat yang berbeda memungkinkan IP untuk menghubungkan sejumlah jaringan.

Sayangnya, jaringan kelas B ternyata menjadi pilihan yang paling populer, karena sangat sedikit organisasi perlu untuk menghubungkan lebih dari 65.536 host (yang memerlukan jaringan kelas A), sementara sebagian besar organisasi bisa melihat diri mereka menggunakan lebih dari 256 host, maksimal untuk jaringan kelas C. Ini berarti jaringan kelas B mulai berkurang dan akan habis dalam waktu yang cepat di awal 1990-an. Untuk sementara, kekurangan yang akan datang itu tetap dengan memberikan rentang jaringan kelas C daripada jaringan kelas B tunggal. Namun, solusi ini memiliki efek samping malang yaitu akan menggunakan lebih banyak memori dan kapasitas pengolahan di router: bukannya melacak jaringan kelas B tunggal, router sekarang harus tahu tentang, misalnya, 16 jaringan C kelas individu. Masalah ini pada gilirannya tetap pada tahun 1993 dengan mengadopsi tanpa kelas interdomain routing (CIDR). Dengan CIDR, perbedaan kelas asli sudah tidak relevan lagi, dan nilai yang menunjukkan pembagian antara

jaringan dan bit host secara eksplisit dilakukan dalam routing protokol. Karakteristik ini memungkinkan untuk menggunakan nomor terendah bit ke nomor host, menggunakan kedua ruang alamat IPv4 dan sumber daya router seefisien mungkin.

IP menggunakan Address Resolution Protocol (ARP) untuk mengetahui alamat MAC. Sebuah host yang memiliki paket IP yang ingin mengirimkan ke host lain atau router yang terhubung ke Ethernet yang sama hanya menyiarkan pesan yang meminta untuk pemilik alamat IP yang bersangkutan untuk merespon. Sistem target melihat alamat dalam siaran dan jawaban, dan host melihat alamat MAC itu. Proses ini ditunjukkan pada Gambar 1-6.



Gambar 1-6. Alamat IP dipetakan ke alamat MAC Ethernet dengan ARP

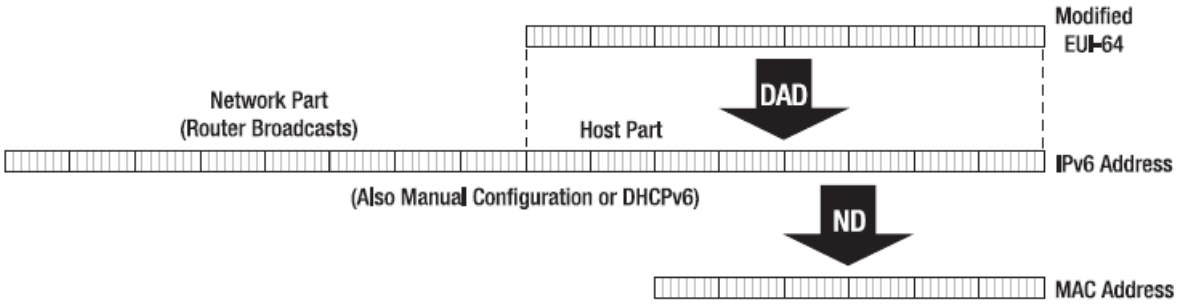
CIDR—AN EXAMPLE

Pada tahun 1988, sebuah organisasi membutuhkan 3.000 alamat yang akan menerima jaringan kelas B, membuang-buang 62.500 alamat tetapi hanya menggunakan satu entri dalam "tabel routing global" yang hadir di router besar di Internet Service Provider. Tiga tahun kemudian, pada tahun 1991, sebuah organisasi membutuhkan jumlah yang sama alamat akan menerima 12 jaringan kelas C, tidak menyia-nyiakan setiap alamat IP untuk berbicara, tetapi menggunakan 12 entri dalam tabel routing seluruh dunia. Tiga tahun kemudian, pada tahun 1994, permintaan untuk 3.000 alamat IP akan menghasilkan 20 / penentuan alamat, yang sama dengan 16 jaringan kelas C atau 1/16th dari jaringan kelas B (4.096 alamat). Namun, alamat ini dengan mudah bisa datang dari kelas A, sebagai perbedaan kelas lama tidak lagi kelas yang relevan dan memegang alamat yang paling tidak terpakai. Digunakan 12 bit untuk nomor host untuk membuat blok 4.096 alamat, yang lebih dari 1.000 lebih dari 3.000 yang diperlukan. Situasi ini masih jauh lebih baik dari itu dengan jaringan kelas B yang penuh, dan hanya satu entri di tabel routing diperlukan.

IP Version 6

Ada banyak perbedaan antara IPv4 dan IPv6, tetapi hal terpenting yaitu bahwa IPv6 masih IP. Semua protokol yang berjalan di atas IPv4 juga dapat menjalankan lebih dari IPv6, dengan asumsi perubahan yang diperlukan dibuat untuk mengakomodasi alamat yang lebih besar. Alamat IPv6 adalah 128 bit (16 byte) panjang dan sepenuhnya tanpa kelas. Dalam prakteknya, di hampir semua kasus, 64 bit yang digunakan untuk jaringan nomor dan 64 bit sisanya adalah bit host. 64 bit host yang secara default diisi dengan Unique Identifier Extended (EUI-64) yaitu alamat MAC 64-bit. Hanya untuk memastikan, IPv6 juga mendukung IPv4 cara-cara tradisional untuk menetapkan alamat: melalui konfigurasi manual dan menggunakan versi IPv6 dari Dynamic Host Configuration Protocol (DHCP). Karena bit host pada alamat IPv6 tidak selalu berisi alamat MAC, IPv6 memiliki mekanisme ARP-seperti untuk menemukan alamat MAC. Tapi ARP adalah protokol yang cukup Ethernet-spesifik dan menggunakan sistem siaran,

yang IPv6 tidak mendukung. Sebaliknya, IPv6 menggunakan multicast secara ekstensif. Multicast seperti siaran ditargetkan: paket dikirim ke semua host yang berlangganan ke alamat grup multicast tertentu. Gambar 1-7 menunjukkan hubungan antara alamat Ethernet MAC, EUI-64, dan alamat IPv6.



Gambar 1-7. Alamat IPv6, EUI-64, dan alamat MAC Ethernet

Gambar diatas menunjukkan gambaran singkat dapat memberikan kesan bahwa IPv6 tidak kompleks, tapi menurut saya, itu tidak terjadi. Ya, dari enam protokol lapisan jaringan, IPv6 adalah yang paling kompleks (atau mungkin sebuah pertalian dengan CLNS), tetapi karena Anda membaca seluruh buku ini, Anda akan menemukan bahwa IPv6 mengambil fitur terbaik yaitu menjadi sesuatu yang elegan dan kuat.