BAB II – Memulai IPv6

Dalam bab ini, kita akan memungkinkan IPv6, tapi sebelum itu, penting untuk memahami IPv6. Mata kuliah ini agak lebih kompleks daripada IPv4 pengalamatan. Pertama-tama, alamat IPv6 ditulis berbeda: delapan nilai heksadesimal 16-bit yang dipisahkan oleh titik dua bukan sebagai empat nilai desimal 8-bit yang dipisahkan oleh periode. Sebuah alamat IPv6 khas terlihat seperti ini:

2001: db8: 31:1:20 a: 95ff: fef5: 246e

Perhatikan bahwa nol terdepan biasanya ditinggalkan. Untuk mengurangi angka nol yang tidak perlu bahkan lebih, satu (dan hanya satu) urutan nilai nol dipisahkan oleh titik dapat dihapus. Jadi alamat 2001: db8: 31:0:0:0:0:1 juga dapat ditulis sebagai 2001: db8: 31 :: 1. Fakta bahwa alamat sekarang terdiri dari hanya empat nilai menunjukkan bahwa empat nilai nol telah dihapus di tempat kolon ganda, sehingga mereka dengan mudah dapat dikembalikan ketika alamat harus dikonversi ke representasi 128-bit internal. Ini "zero compression" yang membuat singkatan berikut sangat legal:

:: (0:0:0:0:0:0:0:0), yang merupakan alamat tidak ditentukan.

:: 1 (0:0:0:0:0:0:0:1), yang merupakan alamat loopback IPv6.

2001: db8: 31 :: (2001: db8: 31:0:0:0:0:0), yang (hampir) alamat biasa.

IPv6 tidak menggunakan netmasks (beberapa pengecualian membuktikan aturan), melainkan menggunakan notasi awalan yang umum di IPv4 routing yang juga. Jadi, ketika Ethernet memiliki kisaran alamat IPv6 2001: db8: 31:1 :: 2001: db8: 31:1: ffff: ffff: ffff: ffff ditugaskan untuk itu, ini ditulis sebagai 2001: db8: 31:1: :/ 64. The "/ 64" berarti bahwa pertama (atas atau kiri) 64 bit dari alamat yang ditugaskan oleh otoritas dari beberapa macam, dan isi dari bit yang tersisa (juga 64 dalam kasus ini) yang ditugaskan secara lokal. Alamat bagian dalam awalan harus alamat IPv6 berlaku dengan semua bit yang bukan merupakan bagian dari awalan diatur ke nol. Jadi 2001: db8: 31:1 :: / 64 dan 2001: db8: 31:1 :: / 127 adalah awalan yang valid, tapi 2001: db8: 31:1 / 64 atau 2001: db8: 31:1 :: / 48 tidak. Dalam kasus pertama, bagian alamat tidak 128-bit alamat IPv6 yang valid, dalam kasus kedua ": 1 ::" bagian berada di luar 48 bit awalan, sehingga seharusnya nol: 2001: db8: 31 :: / 48. Namun, meskipun itu bukan awalan valid, 2001: db8: 31:1:20 a: 95ff: fef5: 246e/64 adalah istilah untuk "alamat 2001: db8: 31:1:20 a: 95ff: fef5: 246e di subnet 2001: db8:. 31:1 :: / 64" Sebuah alamat tanpa slash dan nilai awalan selalu hanya alamat, tidak pernah awalan atau kisaran alamat. Jadi 2001: db8: 31 :: / 48 adalah awalan, tapi 2001: db8: 31 :: adalah alamat yang kebetulan berakhir dalam banyak nol bit. Lihat RFC 3513 untuk informasi lebih lanjut. Lampiran A memiliki informasi lebih lanjut tentang RFC dan bagaimana cara mendapatkannya.

HEXADECIMAL AND BINARY REPRESENTATION

Nomor disimpan dalam representasi biner dalam memori komputer, dengan kata lain, sebagai string dari nol dan satu. Nilai-nilai biner dengan mudah dapat dikonversi bolak-balik ke representasi desimal reguler kami bila diperlukan. Tapi ketika nomor tersebut menjadi cukup besar, konversi antara biner dan desimal menjadi nyaman karena angka desimal terlalu besar. Pada

IPv4, ketidaknyamanan ini dihindari dengan mengubah alamat 32-bit ke desimal sebagai empat kelompok 8 bit. Solusi ini memiliki manfaat tambahan yang memungkinkan kita untuk dengan mudah menentukan bahwa 192.168.0.69 dan 192.168.0.95 jatuh dalam kisaran alamat yang sama. Me lakukan hal yang sama untuk 3221291245 dan 3221291271 (alamat 32-bit yang sama dikonversi ke angka desimal) akan jauh lebih sulit. IPv6, di sisi lain, mengambil keuntungan dari fakta bahwa angka heksadesimal mewakili bahkan jumlah bit, seperti yang ditunjukkan dalam tabel berikut.

Binary	Hexadecimal	Decimal	Binary	Hexadecimal	Decimal
0000	0	0	1000	8	8
0001	1	1	1001	9	9
0010	2	2	1010	A	10
0011	3	3	1011	B	11
0100	4	4	1100	C	12
0101	5	5	1101	D	13
0110	6	6	1110	E	14
0111	7	7	1111	F	15

Dalam heksadesimal, itu juga lebih mudah untuk melihat bahwa dua alamat IP berbagi bagian pertama umum atau awalan: C0A80045 dan C0A8005F. Apakah mereka benar-benar bagian dari subnet yang sama, tentu saja, tergantung pada ukuran subnet.

PENGALAMATAN IPv6

IPv6 memiliki tiga jenis alamat: unicast, multicast, dan anycast. Alamat Unicast adalah alamat biasa digunakan untuk satu-ke-satu komunikasi. Alamat multicast adalah “group address”; paket yang dikirim ke alamat tersebut dikirim ke semua sistem yang tertarik dan telah bergabung dengan grup. Semua fungsi yang dilakukan oleh siaran di IPv4 dilakukan dengan menggunakan multicast pada IPv6. Anycasts mirip dengan multicast, perbedaan adalah bahwa paket yang dikirim ke alamat anycast hanya dikirimkan ke satu sistem dalam kelompok anycast daripada mereka semua.

Pada tingkat tertinggi, ruang alamat IPv6 128-bit dibagi menjadi enam bagian, seperti yang ditunjukkan pada Tabel 2-1.

Tabel 2-1. Sekilas IPv6 Address Space

Start bits	IPv6 prefix notation	Use
000	::/3	Special addresses types
001	2000::/3	Allocated global unicast addresses
01 - 1111 1110 0	4000::/2 - FE00::/9	Reserved global unicast addresses
1111 1110 10	FE80::/10	Link-local unicast addresses
1111 1110 11	FEC0::/10	Site-local unicast addresses
1111 1111	FF00::/8	Multicast addresses

Alamat link-lokal untuk digunakan pada subnet tunggal, mereka akan kita bicarakan nanti bab ini. Dalam nada yang sama, alamat situs-lokal dimaksudkan untuk digunakan dalam satu situs. Kisaran alamat situs-lokal agak mirip dengan RFC 1918 rentang alamat IPv4 (10.0.0.0 / 8,

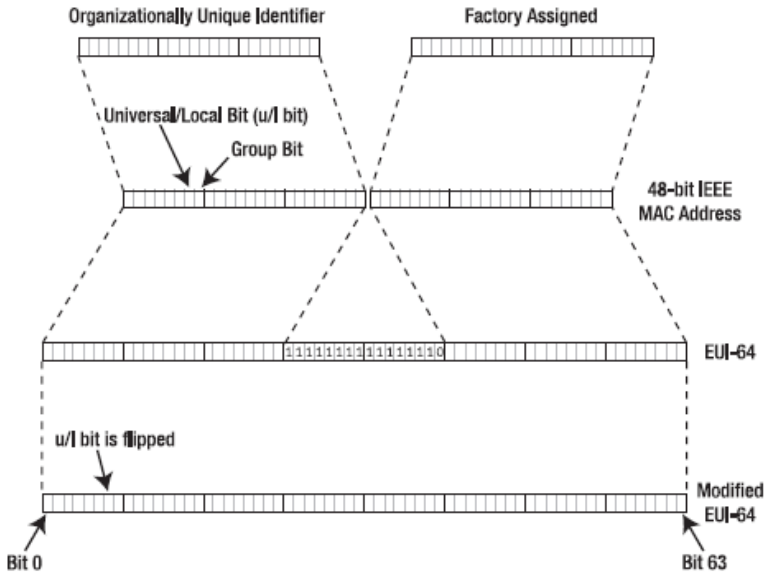
172.16.0.0/12, dan 192.168.0.0/16). Namun, IETF telah mengidentifikasi sejumlah kekhawatiran mengenai penggunaan alamat situs-lokal. Lihat Bab 4 untuk diskusi yang lebih rinci.

Yang hilang dari Tabel 2-1 adalah alamat anycast, karena alamat anycast adalah "secara sintaktis tidak bisa dibedakan" dari alamat unicast. Dengan kata lain, alamat anycast terlihat sama seperti alamat unicast dan berbagi ruang alamat yang sama, dan tuan rumah tidak memiliki cara untuk mengetahui apakah itu mengirimkan sebuah paket ke alamat unicast biasa atau ke alamat kelompok anycast. Sebuah sistem yang sudah diatur untuk menerima paket anycast harus secara eksplisit dikonfigurasi sehingga tahu itu berurusan dengan alamat anycast untuk mengaktifkan diperlukan perilaku link layer khusus.

Interface Identifiers

Semua alamat unicast, kecuali mereka yang memulai dengan tiga bit nol (awalan :: / 3), seharusnya menggunakan interface pengenal 64-bit di bawah 64 bit dari alamat IPv6. Seperti disebutkan dalam Bab 1, interface identifier biasanya berasal dari perangkat keras alamat MAC. Pada gilirannya, alamat MAC dan EUI-64 diperpanjang Identifier unik yang terdiri dari 24-bit Organizationally Unique Identifier (OUI), atau "company_id," seperti yang dikelola oleh Institute of Electrical and Electronics Engineers (IEEE), bersama dengan 24 atau 40 bit yang pemilik oui memberikan. Meskipun IEEE biasa mengacu pada oui sebagai 24 bit panjang, pada kenyataannya, itu hanya 22 bit panjang, sebagai dua bit digunakan untuk menunjukkan apakah alamat MAC atau EUI-64 adalah unik secara global (bit yang universal / lokal) dan apakah alamat MAC adalah kelompok (multicast) alamat atau alamat unicast biasa (sedikit kelompok).

Bahkan dalam kasus-kasus di mana tidak ada alamat hardware tidak tersedia atau alamat diatur secara manual, langkah dari interface pengenal ke alamat IPv6 masih konseptual hadir. Dalam hal ini, bit yang universal / lokal di EUI-64 diatur ke satu, menunjukkan bahwa alamat tidak unik secara global dan dengan demikian tidak dapat digunakan secara universal. Namun, untuk menghindari kerumitan ketika secara manual mengkonfigurasi alamat, bit yang universal / lokal (u / l bit) membalik ketika membuat sebuah alamat IPv6 dari awalan routing dan interface identifier. Sebuah EUI-64 dengan bit yang universal / lokal membalik disebut sebagai "dimodifikasi EUI-64". Gambar 2-1 menunjukkan hubungan antara OUI, alamat MAC, EUI-64, dan EUI-64 yang telah dimodifikasi.



Gambar 2-1. Hubungan antara OUI, alamat MAC, EUI-64, dan dimodifikasi EUI-64

Sebagai contoh, alamat MAC 00:00 A: 95: F5: E9: 6E mengandung OUI 000A95, yang terdaftar ke Apple. Ini 48-bit MAC address berubah menjadi EUI-64 dengan memasukkan nilai FFFE heksadesimal antara oui dan bit-organisasi ditugaskan, yang membuat untuk 64-bit nilai 00:00 A: 95: FF: FE: F5: E9 : 6E. Dengan membalik bit 6 dan menambahkan awalan 64-bit, misalnya, 2001:db8:31:1 :: / 64, ini untuk membuat alamat lengkap: 2001: db8: 31:1:20 a: 95ff: fef5: e96e di kasus ini.

MULTICAST SCOPING

Lebih sering daripada tidak, itu perlu untuk membatasi penyebaran paket multicast. Misalnya, tidak akan baik jika semua router yang terhubung ke Internet adalah untuk menerima semua paket hello yang router OSPF gunakan untuk menemukan tetangga mereka. Paket ini adalah untuk digunakan pada subnet lokal saja. Dan pidato CEO harus mungkin hanya akan multicast seluruh perusahaan, bukan ke Internet. Pembatasan penyebaran paket multicast dikodekan dalam alamat multicast dalam bentuk nilai lingkup 4-bit, seperti yang tercantum dalam Tabel 2-2.

Tabel 2-2. Nilai Lingkup Multicast IPv6

Value (binary)	Value (hexadecimal)	Scope
0000	0	Reserved
0001	1	Interface-local (for the transmission of loopback multicast packets)
0010	2	Link-local
0011	3	Reserved
0100	4	Admin-local
0101	5	Site-local
1000	8	Organization-local
1110	E	Global
1111	F	Reserved

Nilai-nilai lingkup yang tersisa (6, 7, dan 9 - C) dapat digunakan oleh administrator

jaringan untuk menentukan lingkup tambahan bila diperlukan. Empat bit lingkup dalam alamat didahului oleh empat "flag" bit. RFC 3513 hanya mendefinisikan penggunaan yang terakhir ini untuk menunjukkan apakah 112 bit yang membentuk sisa alamat multicast adalah permanen, nilai terkenal ditugaskan oleh Internet Assigned Numbers Authority (IANA), atau beberapa nilai yang ditentukan secara lokal . Jika bit diatur ke nol, nilai 112-bit adalah IANA-yang ditugaskan. Jika bit diatur ke satu, alamat multicast adalah "transient". Jadi FF12 :: / 16 adalah awalan untuk penggunaan multicast link-local sementara, sedangkan ff0e :: / 16 adalah awalan untuk alamat multicast global permanen.

fec0 :: / 10 adalah awalan untuk alamat situs-lokal. Alamat ini dimaksudkan untuk digunakan dalam satu situs, mirip dengan RFC 1918 alamat di IPv4 (10.0.0.0 / 8, 172.16.0.0/12, dan 192.168.0.0/16). Lihat Bab 4 untuk informasi lebih lanjut tentang alamat situs-lokal.

FF02 :: 1 adalah bentuk paling umum dari alamat multicast semua-host. Alamat ini, hal yang paling dekat yang IPv6 memiliki ke alamat broadcast, biasanya ditemukan dengan lingkup link-lokal (FF02 :: 1) tetapi banyak juga host mengimplementasikannya dengan lingkup interface lokal (FF01 :: 1), di mana fungsinya sangat mirip dengan alamat loopback. Router mengatasi pesan iklan router periodik mereka mengirimkan untuk kepentingan semua host pada link ke FF02 :: 1.

FF02 :: 2 adalah alamat multicast semua-router. Ini mirip dengan alamat semua host, kecuali bahwa (tentu saja) hanya router mengikuti alamat multicast. Selain lingkup link-lokal biasa (FF02 :: 2), alamat ini juga dapat ditemui dengan lingkup interface lokal dan situs-lokal, FF01 :: 2 dan ff05 :: 2, berturut-turut.

Semua-nol alamat multicast untuk lingkup apapun (misalnya, FF02 :: untuk lingkup link- lokal) yang dilindungi dan tidak dapat digunakan.Alamat semua-nol dalam subnet apapun (misalnya, 2001: db8: 31:1 ::) adalah subnet semua- router alamat anycast. Namun, tidak ada gunanya nyata untuk alamat anycast, dan beberapa vendor router (seperti Cisco) tidak menerapkannya. Namun, menggunakan alamat ini pada bahaya Anda, karena tidak akan bekerja andal jika ada router di subnet yang tidak menerapkan alamat anycast semua router dengan benar.

128 interface identifiers tertinggi dengan universal / lokal bit set ke satu atau pengalamatan 128 tertinggi untuk alamat subnet yang tidak menggunakan interface identifiers (yaitu, mereka termasuk dalam :: / 3) disediakan untuk alamat anycast terkenal (RFC 2526).

CATATAN : Secara teknis, menggunakan sintaks % interface untuk menunjukkan "scope zone" tidak menentukan interface, tapi sebuah link, sebagai dua atau lebih interface dapat terhubung ke link yang sama.

ALOKASI ALAMAT

Secara formal, ruang alamat IP berada di bawah tanggung jawab Internet Corporation for

Assigned Names and Numbers (ICANN). Namun, fokus ICANN adalah pada nama domain, sehingga pengelolaan ruang alamat IP yang tersisa untuk IANA, yang pada gilirannya mengutus hari demi hari untuk alokasi IPv4 dan alamat IPv6 lima Regional Internet Registries (RIR):

- The African Network Information Centre (AfriNIC, http://www.afrinic.net/), mengurus Africa dan the Indian Ocean.
- The Asia Pacific Network Information Centre (APNIC, http://www.apnic.net/), mengurus Australia, Oceania, dan Asia.
- The American Registry for Internet Numbers (ARIN, http://www.arin.net/), mengurus Amerika Utara.
- The Latin American and Caribbean Internet Addresses Registry (LACNIC, http://www.lacnic.net/), melayani Amerika Latin dan Caribbia.
- The Résaux IP Européens Network Coordination Centre (RIPE NCC, sering dipanggil"RIPE", http://www.ripe.net/), mengurus Europe, Uni Soviet, dan Timur Tengah.

RIR kemudian mengalokasikan blok ruang alamat IP untuk Local Internet Registries (LIR), kadang-kadang melalui perantara National Internet Registry (NIR). ISP yang meminta alamat blok IPv6 dan memenuhi persyaratan ini diberikan alokasi / 32, yang untuk pengguna akhir dapat dibuat. (ISP yang berharap untuk menghubungkan benar-benar angka besar pengguna IPv6 dapat menerima alokasi yang lebih besar dari / 32.) Perbedaan antara alokasi dan penugasan adalah bahwa pemegang alokasi tidak dapat memulai menggunakan alamat. RIR mengalokasikan / 32 prefiks ke ISP untuk membatasi jumlah entri individu dalam IPv6 global yang tabel routing yang menentukan aliran paket di antara ISP.

Dalam dokumentasi IPv6, istilah Top-Level Aggregator (TLA), Next-Level Aggregator (NLA), Situs-Level Aggregator (SLA), dan sub-TLA sering muncul. Istilah-istilah ini mengacu pada gagasan bahwa ruang alamat IPv6 harus didistribusikan dalam tetap, secara hirarkis. Pada penerbitan RFC 3587, terminologi ini usang, ruang alamat IPv6 didistribusikan seperti diuraikan di atas, yang sangat mirip dengan IPv4 kecuali untuk minimal ISP ukuran alokasi tetap 32 bit dan juga sebagus ukuran penugasan tetap untuk end users 48 bit.

6bone ini didirikan oleh IETF sebagai IPv6 global yang testbed pada tahun 1996. Karena RIR sekarang menyediakan "produksi" ruang alamat IPv6, 6bone dan yang 3ffe :: / 16 prefix akan dihapus. Namun sementara itu ruang alamat 6bone mungkin muncul di berbagai tempat bersama ruang alamat RIR sebagai 6bone dan jaringan produksi interkoneksi atau bahkan tumpang tindih di banyak tempat. Menyarankan tanggal 6bone untuk berhenti pada 6 Juni 2006.

MENGAKTIFKAN IPV6

IPv6 berisi fitur lengkap untuk konfigurasi otomatis, hanya memungkinkan protokol membuat terjangkau atas IPv6. Jika tidak ada router IPv6 yang tersedia pada subnet lokal, tuan

rumah masih akan membuat alamat link-local untuk dirinya sendiri (pada setiap interface), yang cukup untuk memungkinkan host lain yang hidup di subnet yang sama untuk terhubung ke lebih dari IPv6. Ini berarti bahwa penting untuk menggunakan firewall IPv6 di mana tepat ketika IPv6 diaktifkan.

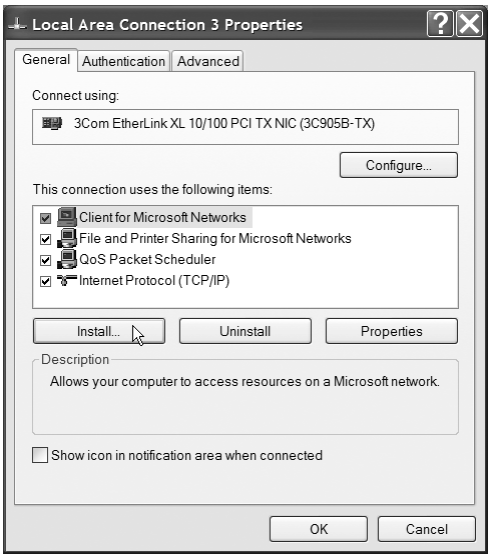
WINDOWS

IPv6 pada Windows dimulai dengan Windows XP 3. Dalam rilis awal, IPv6 tidak tersedia melalui interface pengguna grafis tetapi hanya dengan menggunakan perintah agak tersembunyi yang harus dimasukkan.

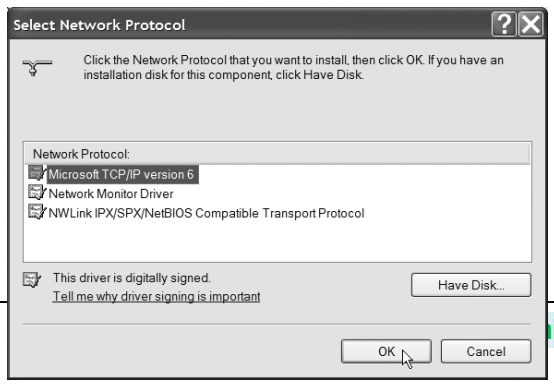
Artikel Basis Pengetahuan membahas pembaruan panjang lebar dan berisi petunjuk tentang men-download dan menginstal itu (tapi ini cukup banyak mendidih ke "Use Windows Update"). Setelah menginstal pembaruan, IPv6 tersedia sebagai protokol tambahan dengan nama "Microsoft TCP / IP versi 6." Anda dapat menginstalnya dengan memilih Mulai ➤ Control Panel ➤ Jaringan dan Koneksi Internet ➤ Network Connections dan kemudian mengklik kanan setiap interface jaringan dan memilih Properties, yang akan membuka jendela yang ditunjukkan pada Gambar 2-2.

Dalam jendela ini, klik tombol Install dan pilih installing an additional protocol. Kemudian pilih

"Microsoft TCP / IP version 6", seperti yang ditunjukkan pada Gambar 2-3.



Gambar 2-2. Windows XP jaringan jendela pengaturan interface



Gambar 2-3. Windows XP jaringan jendela pengaturan interface

ALAMAT PRIVASI

Dalam contoh ini, komputer memiliki tiga alamat: alamat link-local (jenis alamat "link"), alamat yang berasal EUI-64 biasa (tipe "public", dikenali oleh FF: FE urutan di tengah babak kedua dari alamat). Alamat sementara yang digunakan untuk keluar koneksi TCP, sementara alamat publik yang stabil tersedia untuk menerima koneksi masuk. Hal ini dilakukan untuk mengurangi kekhawatiran privasi yang berasal dari kehadiran alamat MAC dalam alamat IPv6

FREE BSD

Sistem FreeBSD dengan dukungan IPv6 di kernel (yang merupakan default untuk versi terbaru)

memiliki pengolahan IPv6 dan penciptaan alamat link-local diaktifkan secara default, tetapi autoconfiguration alamat lingkup global yang menggunakan iklan router dinonaktifkan. Untuk mengaktifkan konfigurasi otomatis, tambahkan baris :

```
ipv6_enable="YES"
ipv6_network_interfaces="auto"
```

ke file / etc / rc.conf dan reboot.

Dengan pengaturan sysctl baru, alamat IPv6 global dikonfigurasi untuk semua interface yang menerima iklan router. Penjelasan yang paling mungkin untuk cara ini konfigurasi akan bahwa di beberapa titik, fungsi yang digunakan untuk disediakan oleh skrip startup dipindahkan ke kernel, tetapi skrip startup tetap.

Penciptaan alamat IPv6 dapat dipantau dengan menggunakan perintah ifconfig, seperti ditunjukkan pada Listing 2-2. Ini tidak perlu menjadi root untuk menjalankan ifconfig dengan cara ini.

Listing 2-2. *Using* ifconfig *to Monitor IPv6 Addresses on FreeBSD*

```
# ifconfig xl0
xl0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu
1500 inet 192.0.2.123 netmask 0xffffff00 broadcast 192.0.2.255
inet6 fe80::201:2ff:fe29:2640%xl0 prefixlen 64 scopeid
0x1 inet6 2001:db8:31:2:201:2ff:fe29:2640 prefixlen 64
autoconf ether 00:01:02:29:26:40
media: Ethernet autoselect (100baseTX <full-duplex>)
status: active
```

TRIGGERING ROUTER SOLICITATIONS

Pesan solicitation router masih dikirim oleh skrip startup atau program eksternal, sehingga ketika perubahan konektivitas IPv6, mungkin diperlukan beberapa saat sebelum alamat IPv6

global yang baru dikonfigurasi, sebagai sistem menunggu untuk iklan router diminta periodic

ALAMAT PRIVASI

Alamat privasi tidak diaktifkan secara default pada FreeBSD dan implementasi IPv6 lainnya KAME yang diturunkan (termasuk MacOS X). Anda dapat mengaktifkannya dengan pengaturan sysclt berikut (sebagai root):

```
sysctl -w net.inet6.ip6.use_tempaddr=1
```

Pengaturan baru mungkin tidak berlaku sampai setelah ulang interface, misalnya, setelah reboot atau ketika interface sebelumnya tidak terhubung terhubung ke jaringan dengan router IPv6.

LINUX

IPv6 pertama menjadi tersedia di Linux kernel versi 2.1.8 pada tahun 1998. Sejak saat itu, implementasi Linux IPv6 telah maju, dan sekarang banyak, tapi tentu tidak semua, distribusi Linux memiliki dukungan IPv6 dibangun di kernel. Dalam buku ini, kita akan membahas secara spesifik IPv6 dari Red Hat 9 dan Red Hat Enterprise Linux ES4 distribusi. Karena IPv6 implementasi itu sendiri ditemukan dalam kernel, banyak informasi yang diberikan juga berkaitan dengan distribusi Linux lainnya, tapi jelas program pendukung yang berbeda dari distribusi ke distribusi. Perhatikan bahwa di samping "biasa" Linux implementasi IPv6, ada lagi IPv6 Linux pelaksanaan oleh proyek Usagi (Playground Universal untuk IPv6, http://www.linux-ipv6.org/), yang bekerja sama erat dengan KAME.

Perhatikan bahwa *rtsold* harus dijalankan sebagai root. Program ini juga dapat dijalankan sebagai daemon:

```
rtsold xl0
```

Argumen xl0 adalah interface yang akan digunakan untuk mengirimkan pesan solicitation router.

ALAMAT PRIVASI

Alamat privasi tidak diaktifkan secara default pada FreeBSD dan implementasi IPv6 lainnya. Anda dapat mengaktifkannya dengan pengaturan sysclt berikut (sebagai root):

```
sysctl -w net.inet6.ip6.use_tempaddr=1
```

Pengaturan baru mungkin tidak berlaku sampai setelah ulang interface, misalnya, setelah reboot atau ketika interface sebelumnya tidak terhubung terhubung ke jaringan dengan router IPv6.

LINUX

IPv6 pertama tersedia di Linux kernel versi 2.1.8 pada tahun 1998. Sejak saat itu, implementasi Linux IPv6 telah maju, dan sekarang banyak didistribusikan. Linux mendukung IPv6 dan berada di kernel. Dalam buku ini, kita akan membahas secara spesifik IPv6 dari distribusi Red Hat 9 dan Red Hat Enterprise Linux ES4. Karena implementasi IPv6 itu sendiri ditemukan dalam kernel, banyak informasi yang diberikan juga berkaitan dengan distribusi Linux lainnya.

Distribusi Red Hat telah mendukung IPv6 sejak versi 7.1, dan pada ES4, telah diaktifkan secara default. Di bawah Red Hat 9 (dan setidaknya Linux lainnya),bisa digunakan IPv6 dengan menambahkan perintah:

NETWORKING_IPV6="yes"

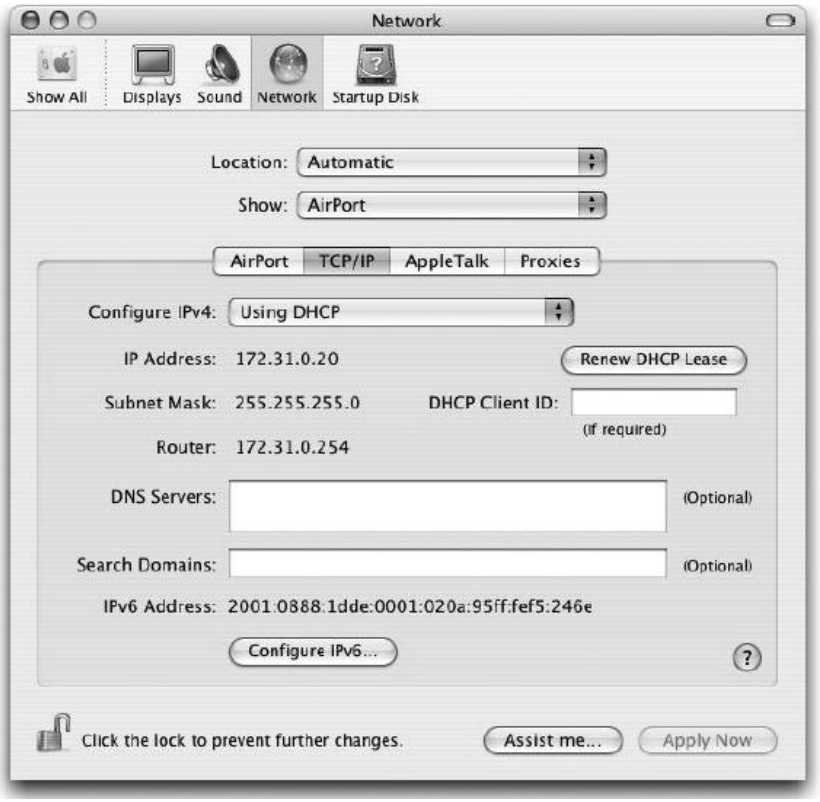
ke file / *etc* / *sysconfig* / *network*. Setelah reboot, sistem kemudian secara otomatis mengkonfigurasi alamat link-lokal dan mengirim pesan solicitation router sehingga dapat auto-configure ke alamat global untuk interface yang terhubung ke router IPv6 yang membalas dengan router yang lain. Linux mengirimkan solicitation router hanya pada startup, namun utilitas solicitation router tidak tersedia. Seperti dengan FreeBSD, perintah ifconfig dapat digunakan untuk mengetahui alamat IPv6 yang dikonfigurasi. Hal ini ditunjukkan pada Listing 2-3. Path ke perintah ifconfig (/ sbin /) diberikan karena direktori ini tidak dalam path pencarian default untuk pengguna non-root.

Listing 2-3. Menggunakan ifconfig ke Monitor Alamat IPv6 di Linux

```
# /sbin/ifconfig eth0
eth0 Link encap:Ethernet HWaddr 00:01:02:29:23:B6
inet addr:192.0.2.8 Bcast:192.0.2.255 Mask:255.255.255.0
inet6 addr: fe80::201:2ff:fe29:23b6/64 Scope:Link
inet6 addr: 2001:db8:1dde:1:201:2ff:fe29:23b6/64 Scope:Global
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:226 errors:0 dropped:0 overruns:0 frame:0
TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:27348 (26.7 Kb) TX bytes:13251 (12.9 Kb)
Interrupt:10 Base address:0xd000
```

MAC OS

Di bawah MacOS X, IPv6 sudah tersedia sejak versi 10.2 Jaguar. MacOS berbeda dari sistem operasi lain dalam IPv6 diaktifkan secara default. Namun, karena MacOS X tidak mengekspos layanan apapun untuk jaringan secara default, ada sedikit kebutuhan untuk firewall IPv6. Dukungan IPv6 di Jaguar cukup marjinal karena tidak ada cara untuk mengaktifkan / menonaktifkan dan mengkonfigurasi protokol dengan menggunakan alat konfigurasi sistem biasa (grafis). Hal ini telah berubah di MacOS 10.3 Panther, di mana IPv6 dikendalikan dengan Jaringan preferensi panel di System Preferences. Pilih interface yang sesuai dan klik TCP / IP, yang membawa sebuah jendela di mana IPv4 dan IPv6 dapat dikonfigurasi, seperti yang ditunjukkan pada Gambar 2-4. Jika IPv6 diaktifkan dan interface yang aktif, alamat IPv6 akan hadir di “IPv6 Address” Ini bisa menjadi alamat global jika seseorang dapat dikonfigurasi dari iklan router atau alamat link-lokal jika alamat global tidak tersedia.



Gambar 2-4. MacOS 10.3 jaringan panel preferensi, Bagian TCP / IP

Karena alat System Configuration hanya akan menampilkan alamat IPv6 tunggal dan tidak selalu mencerminkan informasi terkini, dapat berguna untuk menjalankan perintah ifconfig di Terminal (terletak di Aplikasi ➤ Utilities), seperti ditunjukkan pada Listing 2 - 4.

Listing 2-4. Menggunakan ifconfig ke Monitor Alamat IPv6 pada MacOS

```
% ifconfig en1
en1:    flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST>
mtu 1500
        inet6 fe80::20a:95ff:fef5:246e prefixlen 64 scopeid 0x5
        inet6 2001:db8:1dde:1:20a:95ff:fef5:246e prefixlen 64 autoconf
        inet 172.31.0.20 netmask 0xffffff00 broadcast 172.31.0.255
        ether 00:0a:95:f5:24:6e
        media: autoselect status: active
        supported media: autoselect
```

Di bawah MacOS X, built-in interface Ethernet biasanya en0, sedangkan Bandara (802.11b) atau Airport Extreme (802.11g) interface en1. Tanpa argumen, ifconfig menunjukkan informasi untuk semua interface. Karena banyak dari MacOS UNIX inti berasal dari FreeBSD, banyak perintah UNIX bekerja hampir identik dengan rekan-rekan mereka FreeBSD. Jadi untuk informasi lebih lanjut tentang output ifconfig, lihat penjelasan untuk versi FreeBSD dari perintah sebelumnya.

THE DNS PROBLEM

Sama seperti IPv4, IPv6 menggunakan Domain Name System (DNS) untuk menyelesaikan nama host menjadi alamat yang membuat komunikasi yang diinginkan mungkin. Meminta informasi dari server DNS juga hampir sama dalam IPv4, kecuali satu masalah: pada IPv6, ada aren, AOT benar-benar mekanisme untuk secara otomatis menemukan alamat server DNS lokal. Secara teori, host IPv6 dapat alamat autoconfigure dan

informasi lainnya dalam dua cara: stateless dan stateful (lihat Bab 8). Autoconfiguration stateless adalah mekanisme yang didefinisikan dalam RFC 2462. Namun, bukannya memasok prefiks alamat sendiri, router juga dapat menunjukkan bahwa host harus menggunakan mekanisme stateful untuk mengkonfigurasi alamat dan / atau informasi konfigurasi lainnya dengan menetapkan, Di MacOS X Panther, TCP / IP panel konfigurasi grafis menerima alamat IPv6, seperti yang disebutkan sebelumnya. Dalam FreeBSD dan Linux, hal ini dilakukan dengan menambahkan baris seperti berikut ini ke file / etc / resolv.conf:

nameserver 2002:a00:1:5353:20a:95ff:fef5:246e

Pada Windows XP, mungkin untuk mengkonfigurasi nameserver dengan interface ipv6 add perintah dns netsh, tapi ini tidak mengakibatkan Windows benar-benar query sehingga dikonfigurasi DNS server IPv6. Lihat Bab 5 untuk informasi lebih lanjut tentang menempatkan informasi IPv6 dalam DNS dan menjalankan nameserver IPv6.

DIAGNOSA

Tes terbaik untuk melihat apakah upaya konfigurasi IPv6 yang sukses adalah untuk menjalankan browser Web dan kunjungi situs Web IPv6-enabled. Versi lama Apple Safari browser Web akan terhubung ke IPv6-only server melalui IPv6 tapi lebih suka IPv4, sehingga KAME tidak akan menari. Lihat Bab 6 untuk informasi lebih lanjut tentang browser Web IPv6-enabled dan aplikasi lainnya.

PING AND TRACEROUTE

Jaringan debugging alat ping dan traceroute tentu saja juga tersedia untuk IPv6. Namun, pada kebanyakan sistem, tidak ada ping IPv4/IPv6 terintegrasi atau traceroute, sehingga ping dan tracerouting dalam IPv6 harus dilakukan dengan perintah yang terpisah: ping6 dan traceroute6. Pada Windows, traceroute adalah “tracert” dan versi IPv6 “tracert6.” Biasa tracert juga mendukung IPv6, dan tracert6 kini ditinggalkan di bawah Windows sekalipun. Pada semua sistem, ping6 dan traceroute6 adalah utilitas baris perintah. Pada Windows, memulai command prompt dengan memilih Mulai ➤ All Programs ➤ Aksesoris ➤ Command Prompt, dan di bawah MacOS, gunakan aplikasi Terminal Aplikasi ➤ Utilities. Listing 2-5 menunjukkan output dari perintah traceroute6 bawah FreeBSD.

Listing 2-5. traceroute6 pada FreeBSD

```
% traceroute6 www.ipv6forum.com
traceroute6 to www.ipv6forum.com (2001:630:d0:131:a00:20ff:feb5:ef1e) from
2001:db8:31:2:201:2ff:fe29:2640, 30 hops max, 12 byte packets
1 46.ge-0-2-0.xr1.pbw.xs4all.net 0.984 ms 0.967 ms 0.798 ms
2 2001:db8:0:106::2 0.959 ms 0.93 ms 1.04 ms
3 0.ge-1-3-0.xr1.tc2.xs4all.net 1.35 ms 1.199 ms 1.125 ms
4 eth10-0-0.xr1.ams1.gblx.net 3.345 ms 1.299 ms 1.637 ms
5 2001:798:2014:20dd::5 19.015 ms 16.712 ms 17.752 ms
6 de.nl1.nl.geant.net 24.046 ms 23.325 ms 22.973 ms
7 nl.uk1.uk.geant.net 33.594 ms 31.715 ms 30.407 ms
8 janet-gw.uk1.uk.geant.net 29.726 ms 31.023 ms 28.623 ms
9 po3-0.lond-scr3.ja.net 28.85 ms 33.616 ms 28.204 ms
10 po6-0.lond-scr.ja.net 28.483 ms 28.863 ms 28.46 ms
11 po0-0.london-bar1.ja.net 29.143 ms 29.582 ms 28.813 ms
12 fe0-1-0.ulcc.ipv6.ja.net 24.845 ms 24.751 ms 24.918 ms
13 fa1-0.rtr1.ipv6.ja.net 24.844 ms 24.966 ms 24.565 ms
14 po2-0.rtr2.ipv6.ja.net 24.841 ms 24.639 ms 26.232 ms
15 zaphod.6core.ecs.soton.ac.uk 33.2 ms 32.621 ms 35.53 ms
16 2001:630:d0:131:a00:20ff:feb5:ef1e 32.953 ms 31.756 ms 30.08 ms
```

Tidak seperti IPv4, traceroute6 seperti yang diterapkan dalam FreeBSD, MacOS, dan Linux tidak secara default menunjukkan kedua nama host dan alamat untuk setiap hop, sebagai garis terlalu panjang seperti itu. Sebaliknya, perintah menunjukkan nama host jika tersedia, dan alamat sebaliknya. Dengan opsi-l, traceroute6 menunjukkan kedua nama host dan alamat, dan seperti biasa, opsi-n menunjukkan alamat saja. Bahkan lebih dari dengan IPv4, itu umum bahwa traceroute6 probe tidak menerima jawaban karena host tujuan atau router di tengah adalah tingkat membatasi jumlah pesan ICMP pihaknya siap untuk kembali. Implementasi IPv6 tua cenderung membatasi jumlah pesan ICMP mereka kirim ke satu per detik, implementasi baru sering memiliki batas satu per 100 atau 200 milidetik. Ketika traceroute6 tidak menerima jawaban, ia mencetak tanda ke layar bukannya waktu dalam milidetik.

Listing 2-6. *The Windows XP* ping6 *Command*

```
C:\>ping6 www.hitachi.co.jp
Pinging www.hitachi.co.jp [2001:240:400::101]
from 2001:db8:1dde:1:59eb:57:32ff:b6f4 with 32 bytes of data:
Reply from 2001:240:400::101: bytes=32 time=395ms
Reply from 2001:240:400::101: bytes=32 time=396ms
Reply from 2001:240:400::101: bytes=32 time=398ms
Reply from 2001:240:400::101: bytes=32 time=397ms
Ping statistics for 2001:240:400::101:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 395ms, Maximum = 398ms, Average = 396ms
```

Sistem akan menampilkan pilihan yang tersedia untuk traceroute6 (atau tracert6) dan ping6 perintah dengan mengetikkan perintah tanpa argumen. Di Linux, FreeBSD, dan MacOS, informasi lebih lanjut tersedia di halaman manual, untuk mengaksesnya, tipe man ping6 atau man traceroute6.