

Mengenal IP Versi 6

Irvan Nasrun

irvann@excelcom.co.id

Lisensi Dokumen:

Copyright © 2005 IlmuKomputer.Com

Seluruh dokumen di **IlmuKomputer.Com** dapat digunakan, dimodifikasi dan disebarluaskan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari **IlmuKomputer.Com**.

Pada tulisan ini saya akan menjelaskan mengenai IP versi 6 dan bagaimana cara pengalokasiannya, dimana artikel ini pernah dimuat di majalah Infokomputer.

Saat ini untuk request IP address dilakukan melalui lembaga yang telah ditunjuk oleh IANA (Internet Assigned Numbers Authority) yang ditentukan berdasarkan wilayah, diantaranya adalah APNIC (Asia Pacific Network Information Center) yang khusus menangani request IP address untuk wilayah Asia Pasifik, diantaranya wilayah yang dilayani oleh APNIC adalah Indonesia. Organisasi serupa yang menangani kawasan Amerika Utara, Amerika Selatan, Karibia, dan Afrika Sub Sahara adalah ARIN, sedangkan di Eropa, Timur Tengah, dan sebagian Afrika adalah RIPE-NCC.

IP address yang bahasa awamnya bisa disebut dengan kode pengenal komputer pada jaringan/Internet memang merupakan komponen vital pada Internet, karena tanpa IP address sudah pasti tidak akan dikenal Internet. Setiap komputer yang terhubung ke Internet setidaknya harus memiliki sebuah IP address pada setiap interfacenya dan IP address sendiri harus unik karena tidak boleh ada komputer/server/perangkat network lainnya yang menggunakan IP address yang sama di Internet. IP address adalah sederetan bilangan binary sepanjang 32 bit, yang dipakai untuk mengidentifikasi host pada jaringan. IP address ini diberikan secara unik pada masing-masing komputer/host yang tersambung ke internet. Packet yang membawa data, dimuati IP address dari komputer pengirim data, dan IP address dari komputer yang dituju, kemudian data tersebut dikirim ke jaringan. Packet ini kemudian dikirim dari router ke router dengan berpedoman pada IP address tersebut, menuju ke komputer yang dituju. Seluruh host/komputer yang tersambung ke Internet, dibedakan hanya berdasarkan IP address ini, jadi jelaslah bahwa tidak boleh terjadi duplikasi. Sehingga IP address ini dibagikan oleh beberapa organisasi yang memiliki otoritas atas pembagian IP address tersebut, seperti APNIC (Asia Pacific Network Information Center).

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, netid dan hostid. Netid sendiri menyatakan alamat jaringan sedangkan hostid 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).

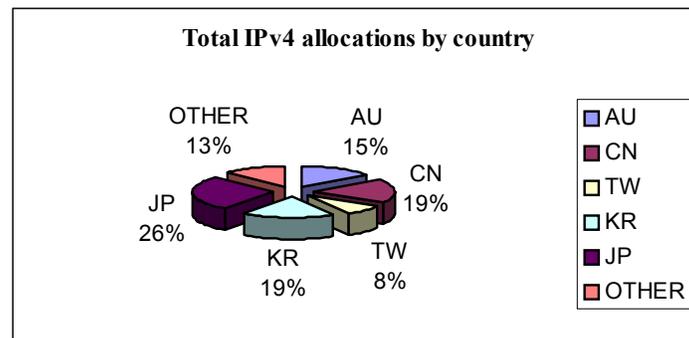
Alasan klasifikasi ini antara lain :

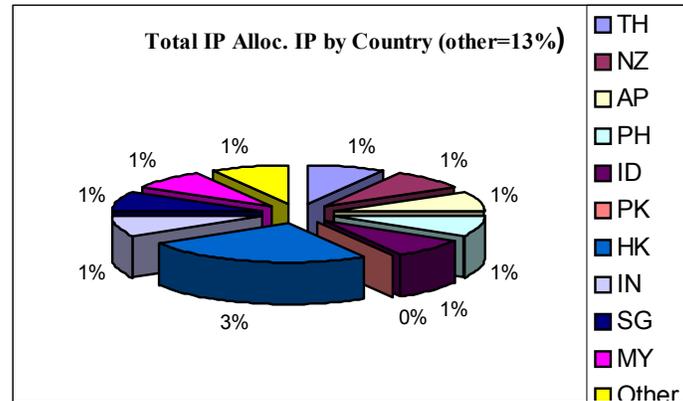
- ◆ Memudahkan sistem pengelolaan dan pengaturan alamat-alamat.
- ◆ Memanfaatkan jumlah alamat yang ada secara optimum (tidak ada alamat yang terlewat).
- ◆ Memudahkan pengorganisasian jaringan di seluruh dunia dengan membedakan jaringan tersebut termasuk kategori besar, menengah, atau kecil.
- ◆ Membedakan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

Pada tabel dibawah dijelaskan mengenai ketersediaan IPv4 berdasarkan data dari APNIC sampai akhir tahun 1999 yang lalu dan total IP yang sudah dialokasikan ke tiap – tiap negara di Asia Pasifik..

IPv4 address space allocated and free

Network	Allocated	Total	% Allocated	% Free
061	1089536	16777216	6.5%	93.5%
169	0	1048576	0.0%	100.0%
202	10659072	16777216	63.5%	36.5%
203	9958912	16777216	59.4%	40.6%
210	13174272	16777216	78.5%	21.5%
211	3932416	16777216	23.4%	76.6%
Total	38814208	84934656	45.7%	54.3%





Perkembangan Internet dan network akhir-akhir ini telah membuat Internet Protocol (IP) yang merupakan tulang punggung networking berbasis TCP/IP dengan cepat menjadi ketinggalan zaman, saat ini berbagai macam aplikasi yang menggunakan Internet, diantaranya transfer file (ftp), surat elektronik (e-mail), akses jarak jauh (remote access), Multimedia menggunakan Internet, dan lain sebagainya. Perkembangan ini telah membuat terlampainya kapasitas jaringan berbasis IP untuk mensuplai layanan dan fungsi yang diperlukan. Sebuah lingkungan seperti Internet membutuhkan dukungan pada lalu-lintas data secara real-time maupun fungsi sekuriti. Kebutuhan akan fungsi sekuriti ini saat ini sangat sulit dipenuhi oleh IP versi 4 atau sering disebut IPv4. Hal ini mendorong para ahli untuk merumuskan Internet Protocol baru untuk menanggulangi keterbatasan resource Internet Protocol yang sudah mulai habis serta menciptakan Internet Protocol yang memiliki fungsi sekuriti yang reliability.

Pada tanggal 25 Juli di Toronto pada saat pertemuan IETF telah direkomendasikan penggunaan IPv6 atau ada yang menyebutnya dengan IPng (IP next generation) yang dilatarbelakangi oleh keterbatasan IPv4 yang saat ini memiliki panjang 32 bit, akibat ledakan pertumbuhan jaringan. Pengembangan IPv6, atau ada yang menyebutkan dengan nama IP Next Generation yang direkomendasikan pada pertemuan IETF di Toronto tanggal 25 Juli 1994 dilatarbelakangi oleh kekurangan IP address yang saat ini memiliki panjang 32 bit, akibat ledakan pertumbuhan jaringan. IPv6 merupakan versi baru dari IP yang merupakan pengembangan dari IPv4.

Keunggulan IPv6 :

a. Otomatisasi berbagai setting / Stateless-less auto-configuration (plug&play)

Address pada IPv4 pada dasarnya statis terhadap host. Biasanya diberikan secara berurut pada host. Memang saat ini hal di atas bisa dilakukan secara otomatis dengan menggunakan DHCP (Dynamic Host Configuration Protocol), tetapi hal tersebut pada IPv4 merupakan fungsi tambahan saja, sebaliknya pada IPv6 fungsi untuk mensetting secara otomatis disediakan secara standar dan merupakan defaultnya. Pada setting otomatis ini terdapat 2 cara tergantung dari penggunaan address, yaitu **setting otomatis stateless dan statefull**.

♦ **Setting otomatis stateless**, pada cara ini tidak perlu menyediakan server untuk pengelolaan dan pembagian IP address, hanya mensetting router saja dimana host yang telah tersambung di jaringan dari router yang ada pada jaringan tersebut memperoleh prefix dari address dari jaringan tersebut. Kemudian host menambah pattern bit yang diperoleh dari informasi yang unik terhadap host, lalu membuat IP address sepanjang 128 bit dan menjadikannya sebagai IP address dari host tersebut. Pada informasi unik bagi host ini, digunakan antara lain address MAC dari jaringan interface. Pada setting otomatis stateless ini dibalik kemudahan pengelolaan, pada Ethernet atau FDDI karena perlu memberikan paling sedikit 48 bit (sebesar address MAC) terhadap satu jaringan, memiliki kelemahan yaitu efisiensi penggunaan address yang buruk.

- ◆ **Setting otomatis statefull** adalah cara pengelolaan secara ketat dalam hal range IP address yang diberikan pada host dengan menyediakan server untuk pengelolaan keadaan IP address, dimana cara ini hampir mirip dengan cara DHCP pada IPv4. Pada saat melakukan setting secara otomatis, informasi yang dibutuhkan antara router, server dan host adalah ICMP (Internet Control Message Protocol) yang telah diperluas. Pada ICMP dalam IPv6 ini, termasuk pula IGMP (Internet Group management Protocol) yang dipakai pada multicast pada IPv4.

Keamanan (IP layer privacy and authentication)

Saat ini metode dengan menggunakan S-HTTP(Secure HTTP) untuk pengiriman nomor kartu kredit, ataupun data pribadi dengan mengenkripsinya, atau mengenkripsi e-mail dengan PGP (Pretty Good Privacy) telah dipakai secara umum. Akan tetapi cara di atas adalah securiti yang ditawarkan oleh aplikasi. Dengan kata lain bila ingin memakai fungsi tersebut maka kita harus memakai aplikasi tersebut. Jika membutuhkan securiti pada komunikasi tanpa tergantung pada aplikasi tertentu maka diperlukan fungsi securiti pada layer TCP atau IP, karena IPv4 tidak mendukung fungsi securiti ini kecuali dipasang suatu aplikasi khusus agar bisa mendukung securiti. Dan IPv6 mendukung komunikasi terenkripsi maupun Authentication pada layer IP. Dengan memiliki fungsi securiti pada IP itu sendiri, maka dapat dilakukan hal seperti packet yang dikirim dari host tertentu seluruhnya dienkripsi. Pada IPv6 untuk Authentication dan komunikasi terenkripsi memakai header yang diperluas yang disebut AH (Authentication Header) dan payload yang dienkripsi yang disebut ESP (Encapsulating Security Payload). Pada komunikasi yang memerlukan enkripsi kedua atau salah satu header tersebut ditambahkan.

Fungsi securiti yang dipakai pada layer aplikasi, misalnya pada S-HTTP dipakai SSL sebagai metode encripsi, sedangkan pada PGP memakai IDEA sebagai metode encripsinya. Sedangkan manajemen kunci memakai cara tertentu pula. Sebaliknya, pada IPv6 tidak ditetapkan cara tertentu dalam metode encripsi dan manajemen kunci. Sehingga menjadi fleksibel dapat memakai metode manapun. Hal ini dikenal sebagai SA (Security Association).

Fungsi Securiti pada IPv6 selain pemakaian pada komunikasi terenkripsi antar sepasang host, dapat pula melakukan komunikasi terenkripsi antar jaringan dengan cara mengenkripsi packet oleh gateway dari 2 jaringan yang melakukan komunikasi tersebut.

Perbaikan utama lain dari IPv6 adalah:

- ◆ Streamlined header format and flow identification
- ◆ Expanded addressing capability
- ◆ More efficient mobility options
- ◆ Improved support for options/extensions,

Kegunaan perbaikan tersebut dimaksudkan agar dapat merespon pertumbuhan Internet, meningkatkan reliability, maupun kemudahan pemakaian.

Perubahan terbesar pada IPv6 adalah perluasan IP address dari 32 bit pada IPv4 menjadi 128 bit. 128 bit ini adalah ruang address yang kontinyu dengan menghilangkan konsep kelas. Selain itu juga dilakukan perubahan pada cara penulisan IP address. Jika pada IPv4 32 bit dibagi menjadi masing-masing 8 bit yang dipisahkan dengan "." dan dituliskan dengan angka desimal, maka pada IPv6, 128 bit tersebut dipisahkan menjadi masing-masing 16 bit yang tiap bagian dipisahkan dengan ":" dan dituliskan dengan hexadesimal. Selain itu diperkenalkan pula struktur bertingkat agar pengelolaan routing menjadi mudah. Pada CIDR (Classless Interdomain Routing) tabel routing diperkecil dengan menggabungkan jadi satu informasi routing dari sebuah organisasi.

Tabel 1 Pembagian ruang address pada IPv6

Allocation	Prefix (binary)	Fraction of Address Space
Reserved	0000 0000	1/256
Unassigned	0000 0001	1/256
Reserved for NSAP Allocation	0000 001	1/128
Reserved for IPX Allocation	0000 010	1/128
Unassigned	0000 011	1/128
Unassigned	0000 1	1/32
Unassigned	0001	1/16
Unassigned	001	1/8
Provider based Unicast Address	010	1/8
Unassigned	011	1/8
Reserved for Neutral-Interconnect- Based Unicast Addresses	100	1/8
Unassigned	101	1/8
Unassigned	110	1/8
Unassigned	1110	1/16
Unassigned	1111 0	1/32
Unassigned	1111 10	1/64
Unassigned	1111 1101	1/128
Unassigned	1111 1110	1/512
Link Local Use Addresses	1111 1110 10	1/1024
Site Local Use Addresses	1111 1110 11	1/1024
Multicast Addresses	1111 1111	1/256

Untuk memahami tentang struktur bertingkat address pada IPv6 ini, dengan melihat contoh pada address untuk provider. Pertama-tama address sepanjang 128 bit dibagi menjadi beberapa field yang dapat berubah panjang. Jika 3 bit pertama dari address adalah "010", maka ini adalah ruang bagi provider. Sedangkan n bit berikutnya adalah registry ID yaitu field yang menunjukkan tempat/lembaga yang memberikan IP address. Misalnya IP address yang diberikan oleh InterNIC maka field tersebut menjadi "11000". Selanjutnya m bit berikutnya adalah provider ID, sedangkan o bit berikutnya adalah Subscriber ID untuk membedakan organisasi yang terdaftar pada provider tersebut. Kemudian p bit berikutnya adalah Subnet ID, yang menandai kumpulan host yang tersambung secara topologi dalam jaringan dari organisasi tersebut. Dan yang $q=125-(n+m+o+p)$ bit terakhir adalah Interface ID, yaitu IP address yang menandai host yang terdapat dalam grup-grup yang telah ditandai oleh Subnet ID. Subnet ID dan Interface ID ini bebas diberikan oleh organisasi tersebut.

Organisasi bebas menggunakan sisa $p+q$ bit dari IP address dalam memberikan IP address di dalam organisasinya setelah mendapat $128-(p+q)$ bit awal dari IP address. Pada saat itu, administrator dari organisasi tersebut dapat membagi menjadi bagian sub-jaringan dan host dalam panjang bit yang sesuai, jika diperlukan dapat pula dibuat lebih terstruktur lagi. Karena panjang bit pada provider ID dan subscriber ID bisa berubah, maka address yang diberikan pada provider dan jumlah IP address yang dapat diberikan oleh provider kepada pengguna dapat diberikan secara bebas sesuai dengan kebutuhan. Pada IPv6 bagian kontrol routing pada address field disebut prefix, yang dapat dianggap setara dengan jaringan address pada IPv4.

Address IPv6 dapat dibagi menjadi 4 jenis, yaitu :

- ◆ Unicast Address (one-to-one) digunakan untuk komunikasi satu lawan satu, dengan menunjuk satu host.

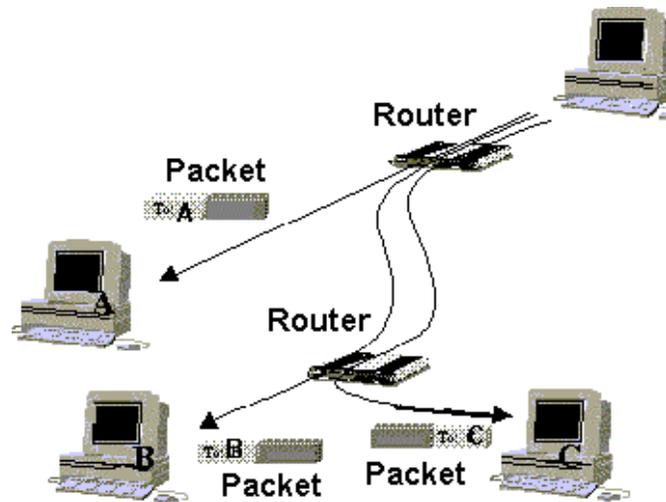
Pada Unicast address ini terdiri dari :

- ❖ Global, address yang digunakan misalnya untuk address provider atau address geografis.
- ❖ Link Local Address adalah address yang dipakai di dalam satu link saja. Yang dimaksud link di sini adalah jaringan lokal yang saling tersambung pada satu level. Address ini dibuat secara otomatis oleh host yang belum mendapat address global, terdiri dari 10+n bit prefix yang dimulai dengan "FE80" dan field sepanjang 118-n bit yang menunjukkan nomor host. Link Local Address digunakan pada pemberian IP address secara otomatis.
- ❖ Site-local, address yang setara dengan private address, yang dipakai terbatas di dalam site saja. Address ini dapat diberikan bebas, asal unik di dalam site tersebut, namun tidak bisa mengirimkan packet dengan tujuan alamat ini di luar dari site tersebut.
- ❖ Compatible.

Panjang bit						,PQTI {{{j					
,R											
,OPO		Registry ID		Provider ID		Subscriber ID		Subnet ID		interface ID	
Provider - based global unicast address											
Panjang bit						,PPWI					
,PO											
,PPPPPPPOP				,O						Interface ID	
Link - lokal address											
Panjang bit						,PPWI					
,PO											
,PPPPPPPOP				,O		Subnet ID				Interface ID	
Site - local address											

Struktur Unicast Address

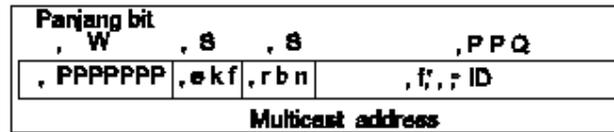
Pada gambar di bawah dijelaskan mengenai cara kerja pengiriman packet pada Unicast Address :



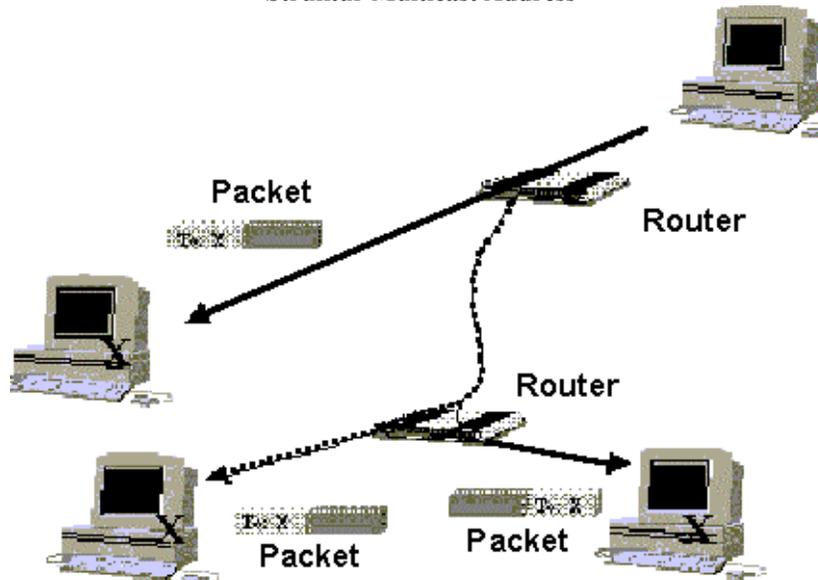
Gambar Pengiriman packet pada Unicast Address

- ◆ Multicast (one-to-many) yang digunakan untuk komunikasi 1 lawan banyak dengan menunjuk host dari group. Multicast Address ini pada IPv4 didefinisikan sebagai kelas D, sedangkan pada IPv6 ruang yang 8 bit pertamanya di mulai dengan "FF" disediakan untuk multicast Address. Ruang ini kemudian dibagi-bagi lagi untuk menentukan range berlakunya. Kemudian Blockcast address pada IPv4 yang address bagian hostnya didefinisikan sebagai "1", pada IPv6 sudah termasuk di dalam multicast Address ini. Blockcast address untuk

komunikasi dalam segmen yang sama yang dipisahkan oleh gateway, sama halnya dengan multicast address dipilah berdasarkan range tujuan.

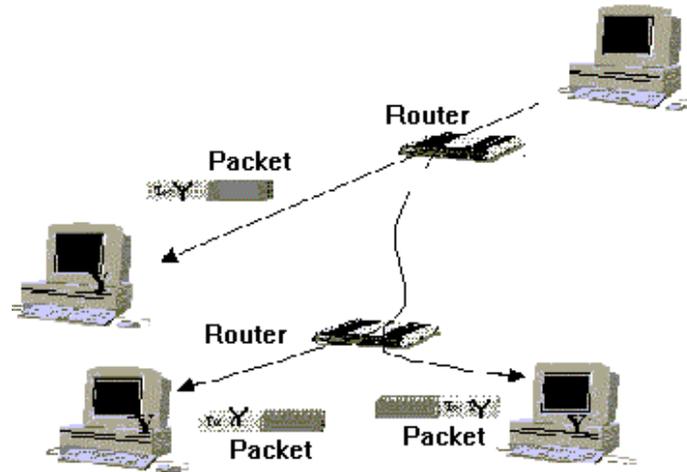


Struktur Multicast Address



Gambar Pengiriman packet pada multicast address

- ◆ Anycast Address, yang menunjuk host dari group, tetapi packet yang dikirim hanya pada satu host saja. Pada address jenis ini, sebuah address diberikan pada beberapa host, untuk mendefinisikan kumpulan node. Jika ada packet yang dikirim ke address ini, maka router akan mengirim packet tersebut ke host terdekat yang memiliki Anycast address sama. Dengan kata lain pemilik packet menyerahkan pada router tujuan yang paling "cocok" bagi pengiriman packet tersebut. Pemakaian Anycast Address ini misalnya terhadap beberapa server yang memberikan layanan seperti DNS (Domain Name Server). Dengan memberikan Anycast Address yang sama pada server-server tersebut, jika ada packet yang dikirim oleh client ke address ini, maka router akan memilih server yang terdekat dan mengirimkan packet tersebut ke server tersebut. Sehingga, beban terhadap server dapat terdistribusi secara merata. Bagi Anycast Address ini tidak disediakan ruang khusus. Jika terhadap beberapa host diberikan sebuah address yang sama, maka address tersebut dianggap sebagai Anycast Address.

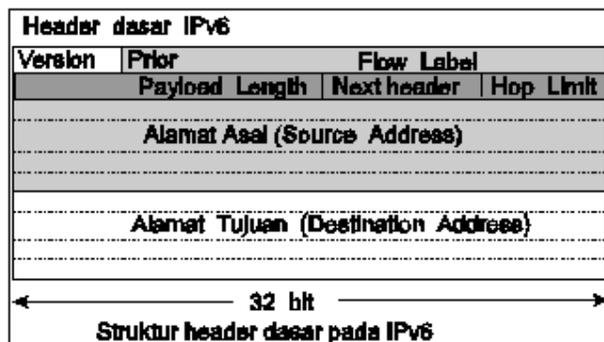


Gambar Pengiriman packet pada anycast address

- ◆ Reserved, digunakan untuk keperluan dimasa yang akan datang.

Struktur Packet pada IPv6

Dalam pendesignan header packet ini, diupayakan agar cost/nilai pemrosesan header menjadi kecil untuk mendukung komunikasi data yang lebih real time. Misalnya, address awal dan akhir menjadi dibutuhkan pada setiap packet. Sedangkan pada header IPv4 ketika packet dipecah-pecah, ada field untuk menyimpan urutan antar packet. Namun field tersebut tidak terpakai ketika packet tidak dipecah-pecah. Header pada Ipv6 terdiri dari dua jenis, yang pertama, yaitu field yang dibutuhkan oleh setiap packet disebut header dasar, sedangkan yang kedua yaitu field yang tidak selalu diperlukan pada packet disebut header ekstensi, dan header ini didefinisikan terpisah dari header dasar. Header dasar selalu ada pada setiap packet, sedangkan header tambahan hanya jika diperlukan diselipkan antara header dasar dengan data. Header tambahan, saat ini didefinisikan selain bagi penggunaan ketika packet dipecah, juga didefinisikan bagi fungsi sekuriti dan lain-lain. Header tambahan ini, diletakkan setelah header dasar, jika dibutuhkan beberapa header maka header ini akan disambungkan berantai dimulai dari header dasar dan berakhir pada data. Router hanya perlu memproses header yang terkecil yang diperlukan saja, sehingga waktu pemrosesan menjadi lebih cepat. Hasil dari perbaikan ini, meskipun ukuran header dasar membesar dari 20 bytes menjadi 40 bytes namun jumlah field berkurang dari 12 menjadi 8 buah saja.



Struktur header dasar pada IPv6

Label Alir dan Real Time Process

Header dari packet pada IPv6 memiliki field label alir (flow-label) yang digunakan untuk meminta agar packet tersebut diberi perlakuan tertentu oleh router saat dalam pengiriman (pemberian 'flag'). Misalnya pada aplikasi multimedia sedapat mungkin ditransfer secepatnya walaupun kualitasnya sedikit berkurang, sedangkan e-mail ataupun WWW lebih memerlukan sampai dengan akurat dari pada sifat real time.

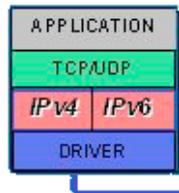
Tabel Label Alir pada IPv6

Label	Kategori
0	Uncharacterized Traffic
1	"Filler" traffic (e.g., netnews)
2	Unattended data transfer (e.g., e-mail)
3	Reserved
4	Attended bulk transfer (e.g., FTP, HTTP, NFS)
5	Reserved
6	Interactive traffic (e.g., Telnet, X)
7	Internet control traffic (e.g., routing protocols, SNMP)
8-15	Realtime communications traffic, non-congestion-controlled traffic

Router mengelola skala prioritas maupun resource seperti kapasitas komunikasi atau kemampuan memproses, dengan berdasar pada label alir ini. Jika pada IPv4 seluruh packet diperlakukan sama, maka pada IPv6 ini dengan perlakuan yang berbeda terhadap tiap packet, tergantung dari isi packet tersebut, dapat diwujudkan komunikasi yang aplikatif.

IPv6 Transition (IPv4 – IPv6)

Untuk mengatasi kendala perbedaan antara IPv4 dan IPv6 serta menjamin terselenggaranya komunikasi antara pengguna IPv4 dan pengguna IPv6, maka dibuat suatu metode Hosts – dual stack serta Networks – Tunneling pada hardware jaringan, misalnya router dan server.



Gambar Hosts – dual stack (IPv6 Transition)



Gambar Networks – Tunneling (IPv6 Transition)

Jadi setiap router menerima suatu packet, maka router akan memilah packet tersebut untuk menentukan protokol yang digunakan, kemudian router tersebut akan meneruskan ke layer di atasnya.

Allokasi IPv6

Kebijakan alokasi IPv6:

- Regular allocations
 - ◆ Peering dengan ≥ 3 subTLA (Top Level Agregator) dan
 - ◆ Merencanakan untuk menyediakan pelayanan IPv6 tidak lebih dari 12 bulan, atau
 - ◆ Mempunyai ≥ 40 SLA (Site Level Agregator) customer.
- Bootstrap
 - ◆ Peering dengan ≥ 3 AS (Autonomous System Number) dan
 - ◆ Merencanakan untuk menyediakan pelayanan IPv6 tidak lebih dari 12 bulan, atau
 - ◆ Mempunyai ≥ 40 IPv4 customer, atau
 - ◆ Mempunyai kemampuan 6bone experience.

Untuk mendapatkan alokasi IPv6 dari Asia Pacific Network Information Center (APNIC), anda harus mengirimkan permohonan IPv6 menggunakan form <http://www.apnic.net/apnic-bin/ipv6-subtla-request.pl>, untuk wilayah Indonesia anda bisa mengirimkan form permohonan IPv6 yang juga bisa diambil dari homepage APNIC: <http://www.apnic.net/apnic-bin/ipv6-subtla-request.pl>, kemudian mengirimkan form tersebut ke ip-request@apjii.or.id, tapi sebelumnya anda mendaftarkan sebagai anggota APJII untuk mendapatkan pelayanan ini.

Saat ini telah terdapat beberapa vendor yang telah mendukung IPv6, diantaranya:

- ❖ IPv6 Ready: 3Com, Epilogue, Ericsson/Telebit, IBM, Hitachi, KAME, Nortel, Trumpet
- ❖ Beta Testing: Apple, Cisco, Compaq, HP, Linux community, Sun, Microsoft.
- ❖ Implementing: Bull, BSDI, FreeBSD, Mentat, Novell, SGI, dan lain sebagainya.

Berdasarkan data dari 6BONE (<http://www.6bone.net>) saat ini telah terdapat 200 situs yang terdapat di 39 negara yang telah bertarsipasi dalam pengembangan tentang IPv6 ini, dan terdapat berbagai lembaga yang turut berpartisipasi mengadakan riset mengenai IPv6 ini, diantaranya adalah: CAIRN, Canarie, CERNET, Chunghwa Telecom, DANTE, Esnet, Internet2, IPFNET, NTT, Renater, Singren, Sprint, SURFnet, vBNS, WIDE.

IANA sebagai lembaga tertinggi untuk pembagian Internet Resource telah mengalokasikan IPv6 resource ke 3 Regional Internet Registries (RIR), dengan perincian sebagai berikut:

- APNIC : 2001:0200::/23
- ARIN : 2001:0400::/23
- RIPE NCC : 2001:0600::/23

Pada saat ini terdapat 3 Regional Internet Registries (RIR) yang telah mengalokasikan 49 allocate IPv6 dengan perincian sebagai berikut :

- APNIC telah mengalokasikan 19 alokasi IPv6.
- RIPE NCC telah mengalokasi 21 alokasi IPv6.
- ARIN telah mengalokasikan 9 alokasi IPv6.

Untuk mendapatkan status daftar dari alokasi IPv6 oleh Regional Internet Registries anda bisa mendapatkan informasi ini di situs 6Bone (<http://www.6bone.net>).

Kesimpulan & Saran

IPv4 yang merupakan pondasi dari Internet telah hampir mendekati batas akhir dari kemampuannya, dan IPv6 yang merupakan protokol baru telah dirancang untuk dapat menggantikan fungsi IPv4. Motivasi utama untuk mengganti IPv4 adalah karena keterbatasan dari panjang addressnya yang hanya 32 bit saja serta tidak mampu mendukung kebutuhan akan komunikasi yang aman, routing yang fleksibel maupun pengaturan lalu lintas data.

IPv6 yang memiliki kapasitas address raksasa (128 bit), mendukung penyusunan address secara terstruktur, yang memungkinkan Internet terus berkembang dan menyediakan kemampuan routing baru yang tidak terdapat pada IPv4. IPv6 memiliki tipe address anycast yang dapat digunakan untuk pemilihan route secara efisien. Selain itu IPv6 juga dilengkapi oleh mekanisme penggunaan address secara local yang memungkinkan terwujudnya instalasi secara Plug&Play, serta menyediakan platform bagi cara baru pemakaian Internet, seperti dukungan terhadap aliran data secara real-time, pemilihan provider, mobilitas host, end-to-end security, ataupun konfigurasi otomatis.

Untuk informasi mengenai IPv6, kami sarankan anda untuk mengakses situs 6BONE (<http://www.6bone.net>), pada situs ini anda bisa mendapatkan informasi mengenai status dan hasil riset dari berbagai partisipan yang tergabung di 6BONE ini.

Selain itu anda bisa mendapatkan informasi mengenai IPv6 dengan mengunjungi situs berikut ini:

- <http://www.6ren.net>
- <http://www.6tap.net>
- <http://www.ipv6.org>
- <http://www.ipv6forum.com>

Selain itu, anda bisa mendapatkan informasi tentang IPv6 melalui RFC (Request for Comment), sebagai berikut:

- RFC 2374, an IPv6 Aggregatable Global Unicast Address Format
- RFC 2373, IPv6 Addressing Architecture
- RFC 2460, IPv6 Specification
- RFC 2461, Neighbor Discovery for IPv6
- RFC 2462, IPv6 Stateless Address Autoconfiguration
- RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification
- RFC 1886, DNS Extensions to support IPv6
- RFC 1887, An Architecture for IPv6 Unicast Address Allocation
- RFC 1981, Path MTU Discovery for IP version 6
- RFC 2023, IP version 6 over PPP
- RFC 2080, RIPng for IPv6
- RFC 2452, IP version 6 Management Information Base for the User Datagram Protocol
- RFC 2464, Transmission of IPv6 Packets over Ethernet Networks
- RFC 2465, Management Information Base for IP version 6: Textual Conventions and General Group
- RFC 2466, Management Information Base for IP version 6: ICMPv6 Group
- RFC 2467, Transmission of IPv6 Packets over FDDI Networks
- RFC 2470, Transmission of IPv6 over Token Ring Networks
- RFC 2472, IP version 6 over PPP
- RFC 2473, Generic Packet Tunneling in IPv6 Specification
- RFC 2507, IP Header Compression
- RFC 2526, Reserved IPv6 Subnet Anycast Addresses
- RFC 2529, Transmission of IPv6 over IPv4 Domains without Explicit Tunnels
- RFC 2545, Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
- RFC 2590, Transmission of IPv6 Packets over Frame Relay
- RFC 2675, IPv6 Jumbograms
- RFC 2710, Multicast Listener Discovery (MLD) for IPv6

- RFC 2711, IPv6 Router Alert Option
- RFC 1888, OSI NSAPs and IPv6
- RFC 2292, Advanced Sockets API for IPv6
- RFC 2375, IPv6 Multicast Address Assignments
- RFC 2450, Proposed TLA and NLA Assignment Rules
- RFC 2471, IPv6 Testing Address Allocation
- RFC 2553, Basic Socket Interface Extensions for IPv6

Daftar Pustaka

- ❖ <http://playground.sun.com/ipng>
- ❖ <http://www.6ren.net>
- ❖ <http://www.6tap.net>
- ❖ <http://www.ipv6.org>
- ❖ <http://www.ipv6forum.com>
- ❖ <http://www.apnic.net/policies.html>
- ❖ <http://www.apnic.net/drafts/ipv6/IPv6-FAQ.html>
- ❖ <http://www.apnic.net/drafts/ipv6/ipv6-policy-280599.html>
- ❖ <http://www.6bone.net/misc/case-for-ipv6.html>
- ❖ Robert M. Hinden, IP Next Generation Overview,
<http://playground.sun.com/pub/ipng/html/INET-Ipng-Paper.html>

© Irvan Nasrun
Account Manager
PT. Excelcomindo Pratama (XL)
Email. irvann@excelcom.co.id
Yahoo Messenger: cybermatrixid