

IPv6 : Internet Protocol Generasi Mendatang

Oleh : Sudarmawan

Pendahuluan

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. Jika dua dekade yang lalu IP merupakan penyambung jutaan komputer, maka saat ini IP harus mampu menghubungkan milyaran komputer.

Selama ini Internet dan network TCP/IP yang lainnya dirancang untuk mendukung penggunaan-terdistribusi sederhana seperti transfer file (ftp), surat elektronik (e-mail), akses jarak jauh (remote access) dengan menggunakan TELNET. Akan tetapi saat ini, akibat ledakan popularitas World Wide Web beberapa tahun terakhir ini, Internet telah tumbuh menjadi multimedia. Pada saat yang sama jaringan di perusahaan telah beralih dari e-mail dan penggunaan transfer file sederhana kepada lingkungan client/server yang kompleks.

Perkembangan ini telah membuat terlampauinya 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 ini saat ini sangat sulit dipenuhi oleh IP versi 4 atau sering disebut IPv4.

Pengembangan IPv6, IP Generasi berikut atau IPng (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.

Kekurangan IP address versi 4

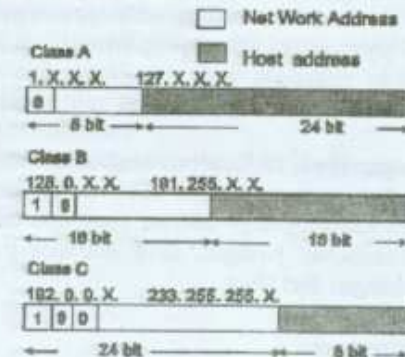
IP address adalah sederetan bilangan *binary* sepanjang 32 bit, yang dipakai untuk mengidentifikasi host pada jaringan. IP address ini diberikan secara unik pada masing-masing komputer/host yang tersambung ke internet. Packet yang membawa data, dimuati IP address dari komputer pengirim data, dan IP address 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 Inter-NIC (*Network Information Center*). Pada mulanya, address dengan 32 bit ini dianggap cukup untuk dibagikan pada host.

Tetapi dengan perkembangan internet yang luar biasa beberapa tahun terakhir ini, muncul kekhawatiran akan habisnya IP address ini, akibat permintaan yang luar biasa.

Selama ini inter-NIC memberi IP address dengan menggunakan konsep kelas. Maksudnya, IP address sepanjang 32 bit ini dibagi menjadi 2, yaitu bagian jaringan dan bagian host, Inter-NIC hanya mengelola bagian jaringan saja. Dengan kata lain pada saat memberi IP address pada sebuah organisasi, Inter-NIC hanya memberi bagian jaringannya saja, sedang sisanya, pemberian IP address pada masing-masing host diserahkan pada organisasi tersebut.

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.



Gambar 1. Konsep Kelas

Setelah address jaringan diperoleh, maka organisasi tersebut dapat secara bebas memberikan address bagian host pada masing-masing hostnya. Tetapi tidak pasti seluruh address yang diperoleh dapat dipakai. Pada kenyataannya banyak yang tidak terpakai. Contohnya, organisasi yang tersambung ke internet dengan jumlah host sebanyak 1000 buah, karena jumlah host tersebut lebih dari 256, maka akan memilih kelas B. Akibatnya hanya sebagian kecil dari 65536 address yang diperoleh yang dipakai. Sementara itu, address yang tersisa tidak dapat digunakan oleh organisasi lain.



Gambar. 2 Contoh tabel rute

Address pada IPv4 pada dasarnya statis terhadap host. Biasanya diberikan secara berurut pada host. Misalnya ketika menggunakan komputer note, jika tersambung pada satu jaringan maka IP address yang dipakai adalah IP address pada jaringan tersebut. Jika tersambung pada jaringan yang lain lagi, maka IP address pun harus di set ulang ke IP address di jaringan tersebut. Pada koneksi dialup pun, karena IP address berganti-ganti maka harus diset ulang.

Memang saat ini hal di atas bisa dilakukan secara otomatis dengan menggunakan DHCP (*Dynamic Host Configuration Protocol*). Tetapi, hal tersebut sesungguhnya tidak termasuk dalam spesifikasi IPv4, merupakan fungsi tambahan yang bersifat optional. Pada kenyataannya DHCP hanya terbatas pada OS baru saja, sehingga DHCP harus diload secara tersendiri. Karena itu, tetap diperlukan adanya mekanisme pemberian address yang fleksibel pada layer IP.

Sama-rata

Salah satu ciri khas Internet adalah pemakaian bersama jaringan, khususnya backbone. Walaupun bandwidth (lebar-pita) provider sebesar 1.5 Mbps, dan begitu pula dengan routing antaranya, namun belum tentu kita dapat senantiasa menggunakan seluruh lebar-pita tersebut. Jika pada saat itu ada pengguna lain yang menggunakan line tersebut, maka lebar-pita yang dapat kita pakai pun berkurang sebanyak yang dipakai oleh pengguna tersebut. Dengan kata lain tidak ada jaminan besar lebar-pita yang dapat dipakai pada waktu tertentu. Walaupun sudah menggunakan line ke provider cukup besar, ketika akan mengirim atau menerima

suara atau gambar, namun tidak dapat dipastikan akan berlangsung dengan lancar sebelum terlaksana. Atau secara ekstrim, ketika kita melakukan TV conference di dalam LAN, tiba-tiba ada pengguna lain yang mengirim data yang sangat besar, maka gambar dan suara yang diterima/dikirim akan terputus-putus. Karenanya diperlukan satu sistem baru yang dapat memenuhi pemakaian baru tersebut.

Keamanan

Agar pemakaian Internet dapat meluas ke bidang bisnis dan berbagai bidang lainnya, fungsi sekuriti adalah salah satu kuncinya. Konsekuensi dari Internet sebagai jaringan publik, tidak dapat dipungkiri kemungkinan data dilihat selama dalam perjalanan. Atau perlu dicegah akses yang dapat merusak, seperti hacker ataupun cracker.

Fungsi sekuriti dapat diwujudkan pada berbagai layer. Meskipun telah ada banyak sekuriti pada layer aplikasi seperti untuk surat elektronik, maupun WWW, tetap diperlukan fungsi sekuriti pada layer jaringan. Pada IPv4 sendiri tidak terdapat fungsi sekuriti ini.

Perubahan pada IPv6

Kemudian apa yang berubah dengan IPv6 ini? Perbaikan utama adalah pada : perluasan ruang alamat (IP address), penyederhanaan header dari packet, Plug&Play, fungsi Sekuriti. Masing-masing perbaikan tersebut dimaksudkan agar dapat merespon pertumbuhan Internet, meningkatkan reliability, maupun kemudahan pemakaian.

Perluasan Address

Seperti telah dijelaskan di atas, perkembangan Internet yang demikian pesat beberapa tahun terakhir ini telah mengakibatkan kelangkaan IP address. 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 dipisah kan dengan "." dan di tuliskan dengan angka desimal, misalnya 150.7.7.250. Maka pada IPv6, 128 bit tersebut dipisahkan menjadi masing-masing 16 bit yang tiap bagian dipisahkan dengan ":" dan dituliskan dengan hexadesimal. Contohnya, "4FE5:2F21:3512:77BB:AF23:3201:55AA:2F33".

Disamping itu, bukan hanya sekedar memperbesar ruang address saja, tapi juga diperkenalkan struktur bertingkat, agar pengelolaan routing menjadi mudah. Pada CIDR (*Classless Interdomain Routing*) tabel routing diperkecil dengan menggabungkan jadi satu informasi routing dari sebuah organisasi. Pada IPv4, sama sekali tidak memperhatikan hubungan antar organisasi maupun negara. Sementara itu pada IPv6, beberapa organisasi dengan provider yang sama, atau memiliki

hubungan geografis, dihubungkan dan dicerminkan pada routing. Dengan kata lain, jika beberapa organisasi berada dalam satu provider pada saat pemberian IP address diupayakan agar address tersebut bisa berada dalam satu ruang address.

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

Misalnya ada dua organisasi pada sebuah provider, maka kedua organisasi ini jaraknya dekat jika dilihat dari jaringan. Sehingga pada pemberian address, diupayakan agar bagian atas dari address sedapat mungkin tidak berbeda jauh. Dengan demikian di luar provider tersebut, informasi routing dari kedua organisasi ini dapat dijadikan satu.

Dengan cara tersebut, saat ini sudah dilakukan pembagian ruang IP address pada IPv6. Dan yang banyak menempati ruang tersebut adalah Address untuk provider dan address untuk wilayah. masing-masing menempati 1/8 dari ruang address yang tersedia. Kemudian saat ini masih sekitar 70% yang belum didefinisikan, yang dibiarkan sebagai cadangan bagi cara pemberian address baru.

Selanjutnya, mari kita lihat 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.

3 Jenis address yang disediakan

Address IPv6 dapat dibagi menjadi 3 jenis. Yang pertama, disebut unicast Address, digunakan untuk komunikasi satu lawan satu, dengan menunjuk satu host. Kemudian multicast yang digunakan untuk komunikasi 1 lawan banyak. Ini dengan menunjuk host dari grup. Kemudian yang terakhir adalah fungsi baru pada IPv6 yaitu anycast Address, yang menunjuk host dari grup, tetapi packet yang dikirim hanya pada satu host saja.

Pada sebuah host tidak selalu hanya diberikan satu address dari ketiga tipe address di atas, tapi bisa saja diberikan beberapa address. Misalnya memiliki sekaligus Unicast address, link local address, dan Anycast Address.

Unicast Address

Pada unicast address, ditetapkan address yang bersifat global seperti address untuk provider, address geografis. Selain itu juga link local address maupun site local address. Masing-masing yaitu Link-local address dan Site-local address.

hubungan geografis, dihubungkan dan dicerminkan pada routing. Dengan kata lain, jika beberapa organisasi berada dalam satu provider pada saat pemberian IP address diupayakan agar address tersebut bisa berada dalam satu ruang address.

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

Misalnya ada dua organisasi pada sebuah provider, maka kedua organisasi ini jaraknya dekat jika dilihat dari jaringan. Sehingga pada pemberian address, diupayakan agar bagian atas dari address sedapat mungkin tidak berbeda jauh. Dengan demikian di luar provider tersebut, informasi routing dari kedua organisasi ini dapat dijadikan satu.

Dengan cara tersebut, saat ini sudah dilakukan pembagian ruang IP address pada IPv6. Dan yang banyak menempati ruang tersebut adalah Address untuk provider dan address untuk wilayah. masing-masing menempati 1/8 dari ruang address yang tersedia. Kemudian saat ini masih sekitar 70% yang belum didefinisikan, yang dibiarkan sebagai cadangan bagi cara pemberian address baru.

Selanjutnya, mari kita lihat 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.

3 Jenis address yang disediakan

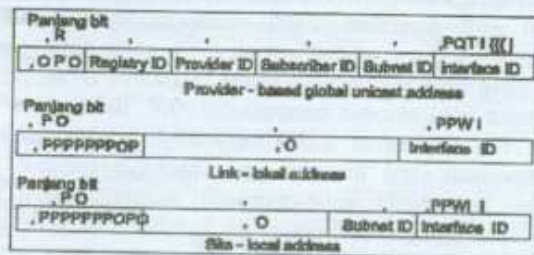
Address IPv6 dapat dibagi menjadi 3 jenis. Yang pertama, disebut unicast Address, digunakan untuk komunikasi satu lawan satu, dengan menunjuk satu host. Kemudian multicast yang digunakan untuk komunikasi 1 lawan banyak. Ini dengan menunjuk host dari grup. Kemudian yang terakhir adalah fungsi baru pada IPv6 yaitu anycast Address, yang menunjuk host dari grup, tetapi packet yang dikirim hanya pada satu host saja.

Pada sebuah host tidak selalu hanya diberikan satu address dari ketiga tipe address di atas, tapi bisa saja diberikan beberapa address. Misalnya memiliki sekaligus Unicast address, link local address, dan Anycast Address.

Unicast Address

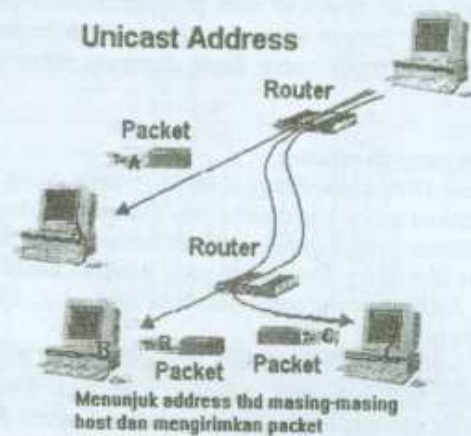
Pada unicast address, ditetapkan address yang bersifat global seperti address untuk provider, address geografis. Selain itu juga link local address maupun site local address. Masing-masing yaitu Link-local address dan Site-local address,

dimasukkan dalam ruang address IPv6 yang memakan masing-masing sekitar 1/1024 dari ruang address yang tersedia.



Gambar 3. Struktur Unicast Address

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.



Gambar 4. Pengiriman packet pada Unicast Address

Sedang Site Local Address setara dengan private address, 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.

Multicast Address

Sedangkan Multicast Address pertama-tama menset address untuk sebuah grup host. Kemudian bila ada packet yang dikirim ke address tersebut, maka packet tersebut akan dikirim ke seluruh host pada grup tersebut.



Gambar 5. Struktur Multicast Address

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.



Gambar 6. Pengiriman packet pada multicast address

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.

Anycast Address

Pada IPv6 ini ditambahkan satu jenis address baru yang tidak terdapat pada IPv4, yaitu Anycast Address. 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

Cara yang kedua yaitu 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. Cara ini mirip dengan cara DHCP pada IPv4, walaupun harus memelihara server dan address, namun karena IP address dapat dipakai secara efektif, cara ini memiliki karakteristik administrator dapat mengelola secara mendetil seperti dapat menstruktur address di dalam organisasi dan lain-lain.

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.

Fungsi Sekuriti

Saat ini pada masa transaksi dengan menggunakan internet telah menjadi kenyataan, sekuriti pada saat komunikasi merupakan hal yang tidak bisa ditawar lagi. 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 sekuriti yang ditawarkan oleh aplikasi. Dengan kata lain bila ingin memakai fungsi tersebut maka kita harus memakai aplikasi tersebut. Jika membutuhkan sekuriti pada komunikasi tanpa tergantung pada aplikasi tertentu maka diperlukan fungsi sekuriti pada layer TCP atau IP.

Dan IPv6 mendukung komunikasi terenkripsi maupun Authentication pada layer IP. Dengan memiliki fungsi sekuriti 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 sekuriti yang dipakai pada layer aplikasi, misalnya pada S-HTTP dipakai SSL sebagai metode enkripsi, sedangkan pada PGP memakai IDEA sebagai metode encripsinya. Sedangkan manajemen kunci memakai cara tertentu pula. Sebaliknya, pada IPv6 tidak ditetapkan cara tertentu dalam metode enkripsi dan manajemen kunci. Sehingga menjadi fleksibel dapat memakai metode manapun. Hal ini dikenal sebagai SA (*Security Association*).

Fungsi Sekuriti 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.

Label Alir dan Real Time Process

Header dari packet pada IPv6 memiliki field label alir (*flow-label*). Label ini, digunakan untuk meminta agar pakect tersebut diberi perlakuan tertentu oleh router saat dalam pengiriman. Dengan kata lain label ini dapat memberi tanda jenis dari packet tersebut. Misalnya pada suara atau gambar bergerak (*motion picture*) 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	Categories
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.

Penutup

Internet Protocol versi 4 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. Selain itu IP adalah protokol yang sudah sangat tua yang tidak mampu mendukung kebutuhan akan komunikasi yang aman, routing yang fleksibel maupun pengaturan lalu lintas data.

Alasan-alasan inilah yang mendorong munculnya IPv6, Internet protocol generasi berikut. IPv6 yang memiliki kapasitas address raksasa, 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.

IPv6 juga 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.

Daftar Pustaka

Yan Ryanto, ELEKTRO INDONESIA Edisi ke Sembilan, Oktober 1997