IP Next Generation

Oleh : Mulyo Sanyoto
NIM : 23298044

Dikarenakan adanya keterbatasan pada protokol Internet versi 4, IEFT (The Internet Engineering Task Force) mengadopsi Protokol Internet versi 6 (IPv6 dikenal sebagai IP Next generation) untuk menggantikan Protokol Internet versi 4 (IPv4).

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) merupakan suatu protokol standar yang sudah umum kita pakai, spesifikasi teknis dari protokol ini sudah diterbitkan untuk umum sehingga setiap orang bisa mengimplementasikan protokol ini dalam hardware/software-nya.
Keadaan 'open' ini membuat protokol ini menjadi sangat populer, sehingga protokol inilah yang paling banyak dipakai pada jaringan komputer di dunia kita saat ini. Apapun platform perangkat keras dan sistem operasinya, asalkan mempunyai protokol TCP/IP, akan memungkinkan terjadinya interkoneksi dalam jaringan komputer terbesar di dunia, Internet.

TCP/IP sendiri bukan merupakan satu protokol yang berdiri sendiri, tetapi terdiri dari banyak protokol, dimana masing masing protokol mengatur suatu task yang berbeda beda. Transmission Control Protocol dan Internet Protocol merupakan protokol yang utama dalam keluarga TCP/IP. Beberapa protokol dan servis yang membentuk keluarga TCP/IP bisa dikelompokkan tergantung dari tujuannya.

Berikut ini adalah pengelompokkan protokol TCP/IP :

Transpor

Protokol ini mengontrol pergerakkan data diantara dua mesin.

TCP (Transmission Control Protocol)
Servis yang berbasis koneksi, berarti bahwa pengirim dan penerima saling berkomunikasi dalam seluruh waktu

UDP (User Datagram Protocol)
Servis yang berbasis tanpa koneksi, berarti nahwa tidak saling berkomunikasi.

Routing

Protokol ini menangani pengalamatan data,dan menentukan routing terbaik ke tujuan. Juga menangani cara cara bagaimana data paket yang besar dibagi bagi dan disusun lagi di penerima.

IP (Internet Protocol)
Menangani pengiriman data yang sebenarnya.

ICMP (Internet Control Message Protocol)

Menangani status message dari IP, contohnya ‘error’ dan perubahan network yang akan mempengaruhi routing.

RIP (Routing Information Protocol)
Salah satu dari protokol yang menentukan cara routing terbaik.

OSPF (Open Shortest Path Fisrt)
Protokol alternatif untuk menentukan routing.

Network Addresses

Servis ini menangani pengalamatan suatu komputer, dengan cara penomoran yang unik atau dengan simbol nama.

ARP (Address Resolution Protocol)
Menentukan alamat suatu komputer dalam jaringan dengan suatu nomor yang unik.

DNS (Domain Name System)
Menentukan alamat numerik dari suatu nama komputer.

RARP (Reverse Address Resolution Protocol)
Menentukan alamat suatu komputer dalam jaringan, tetapi berkebalikan dengan ARP.

BOOTP (Boot Protocol)
Protocol ini akan menjalankan suatu komputer dengan membaca informasi boot dari suatu server. BOOTP ini umumnya digunakan pada workstation yang tidak mempunyai disk.

User Services

Berikut ini adalah aplikasi aplikasi yang bisa diakses oleh pemakai :

FTP (File Transfer Protocol)
Protokol ini akan memindahkan file dari satu komputer ke komputer lain . FTP menggunakan TCP sebagai transport-nya.

TFTP (Trivial File Transfer Protocol)
Pemindah file sederhana yang mempergunakan UDP sebagai transport-nya.

TELNET
Memungkinkan untuk melakukan login dari jauh (remote) sehingga pemakai komputer bisa melakukan login ke komputer lain (remote) dan bisa melakukan perintah perintah seolah olah pemakai tersebut duduk dihadapan remote komputer.

Gateway Protocols

Servis ini memungkinkan jaringan untuk mengkomunikasikan routing dan status informasi .

EGP (Exterior Gateway Protocol)
Memindahkan informasi routing jaringan eksternal.

GGP (Gateway to Gateway Protocol)
Memindahkan informasi routing antar gateway Internet.

IGP (Interior Gateway Protocol)
Memindahan informasi routing untuk jaringan internal.

Lain lain

Kategori ini tidak termasuk dalam kategori sebelumnya tetapi menyediakan servis yang penting dalam jaringan.

NFS (Network File System)
Memungkinkan suatu direktori dari komputer lain di baca oleh komputer kita sehingga seolah olah direktori tersebut terdapat pada komputer kita.

NIS (Network Information Service)
Menjaga account pemakai dalam jaringan, menyederhanakan perawatan login dan password.

RPC (Remote Procedure Call)
Memungkinkan aplikasi remote saling berkomunikasi menggunakan prosedur call.

SMTP (Simple Mail Transfer Protocol)
Protokol untuk memindahkan email elektronik antar komputer.

SNMP (Simple Network Management Protocol)
Digunakan untuk mendapatkan status message tentang konfigurasi TCP/IP dan software.

Semua definisi protokol TCP/IP dipelihara oleh suatu badan standardisasi yang merupakan bagian dari organisasi Internet. Walaupun terdapat perubahan perubahan bila ada features baru /tambahan atau metoda baru, tetapi protokol yang baru tersebut akan selalu kompatibel dengan protokol lama.

Internet Protokol Versi 6

Beberapa keuntungan

Kemampuaan kapasitas pengalamatan

Pada IPv6 area untuk alamat diubah menjadi 128 bit (pada IPv4 ukuran ini adalah 32 bit), sehingga memungkinkan lebih banyak lagi node yang bisa saling terhubung. Kemampuan routing multicast telah diperbaiki dengan menambahkan area “scope” dalam alamat multicast.

Didefinisikan juga tipe baru yang disebut “anycast address” yang digunakan untuk pengiriman paket ke siapa saja dalam kelompok node.

Penyederhanaan format header

Beberapa header IPv4 tidak dipakai lagi atau dibuat optional, untuk mengurangi biaya proses untuk kasus umum dari penanganan paket dan untuk membatasi biaya bandwidth dari heared IPv6.

Perbaikan dalam hal support untuk extension dan option

Perubahan dalam hal pengkodean opsi pada header IP memungkinan penerusan message yang lebih efisien, berkurangnya batas opsi, dan fleksibilitas yang lebih besar untuk menambahkan opsi baru di masa mendatang.

Kemampuan Flow Labeling

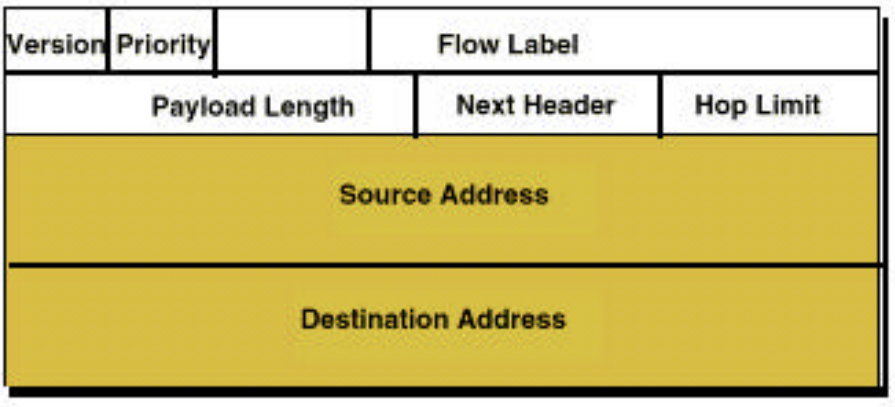
Kemampuan baru ditambahkan untuk memungkinkan pemberian label terhadap paket milik aliran “flow” yang tertentu dimana pengirim meminta penanganan yang khusus, misalnya servis kualitas yang khusus ataupun servis real time.

Kemampuan Autentifikasi dan Privasi

IPv6 menyediakan kemampuan autentifikasi, integritas data, dan kerahasiaan data.

Format Header IPv6

Berikut adalah format header dari IPv6 :



Penjelasan dari masing masing area adalah sebagai berikut :

Version
4-bit, nomor versi dari Internet Protocol (= 6).

Prio.
4-bit, nilai prioritas.
Flow Label
24-bit flow label.

Payload Length
16-bit unsigned integer. Panjang dari payload, misal, sisa paket setelah header IPv6, dalam oktet.

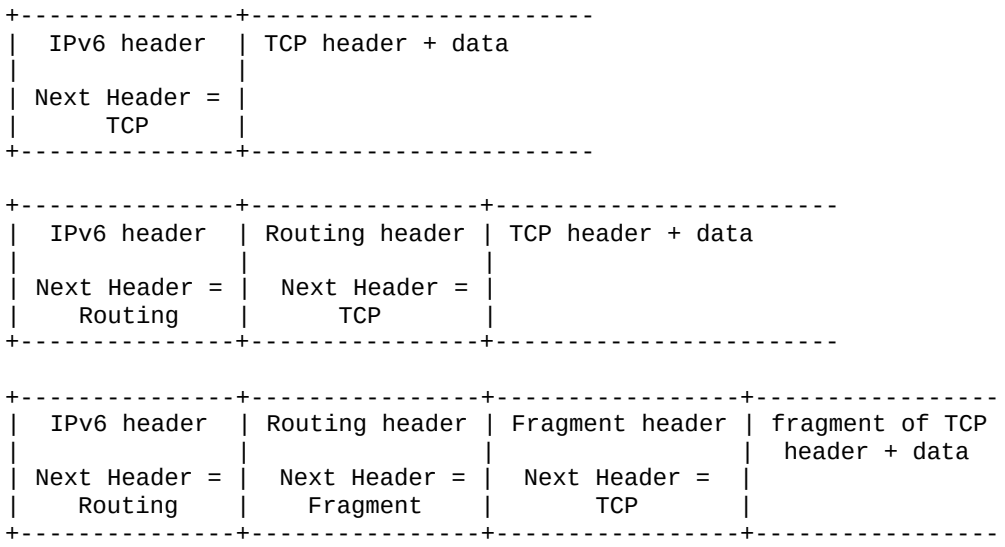
Next Header
8-bit selector. Menandakan tipe header setelah header IPv6. Menggunakan nilai yang sama dengan are protokol IPv4.

Hop Limit
8-bit unsigned integer. Berkurang satu setiap kali paket diteruskan oleh suatu node. Bila nilainya nol paket dibuang.

Source Address
128-bit alamat pengirim paket.

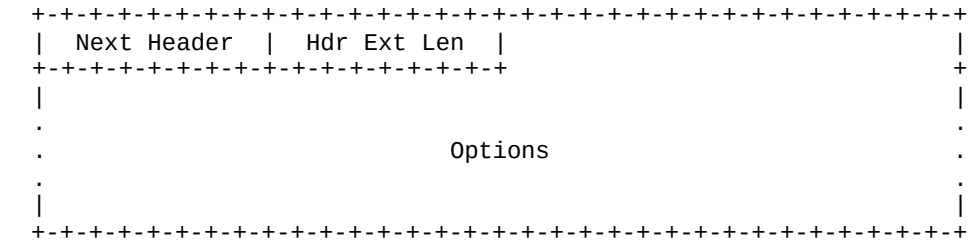
IPv6 Extension Headers

Dalam IPv6, informasi layer internet opsional dikodekan dalam header yang berbeda yang bisa ditempatkan diantara header IPv6 dan header Upper-layer dalam suatu paket. Terdapat beberapa header extension yang seperti itu, masing masing dibedakan oleh Next Header Value. Paket IPv6 bisa sama sekali tidak membawa header extension, bisa juga membawa satu atau lebih header extension, masing masing diidentifikasikan dalam area ‘Next Header’ yang sebelumnya.



Hop-by-Hop Options Header

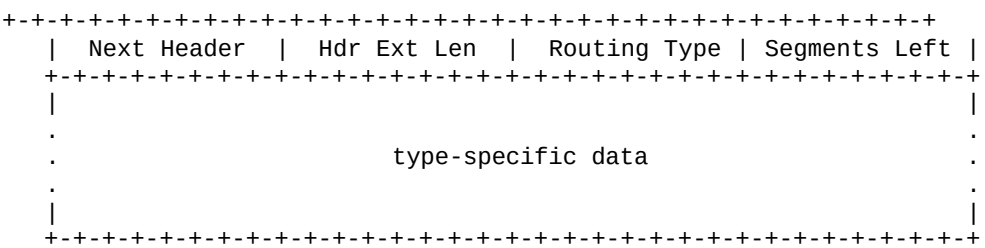
Header opsi ‘Hop-by-hop’ digunakan untuk membawa informasi opsional yang harus diuji oleh setiap node sepanjang alur pengiriman paket. Header ini dikenali oleh nilai 0 dari ‘Next Header’ dalam header IPv6, dan mempunyai format seperti berikut :



Next Header	8-bit selector. Mengidentifikasi tipe header setelah opsi header Hop-by-hop. Menggunakan nilai yang sama seperti pada area protokol IPv4.
Hdr Ext Len	8-bit unsigned integer. Panjang dari opsi header Hop-by-Hop dalam unit 8 -oktet, Tidak termasuk 8 oktet yang pertama.
Options	bervariasi-panjang area, sedemikian sehingga panjang dari header ini kelipatan dari 8 oktet.

Routing Header

Header ini digunakan oleh pengirim paket Ipv6 untuk mendaftarkan satu atau lebih node antara yang bisa dilalui paket ke arah tujuan. Fungsi in sangat mirip dengan opsi Source Route pada Ipv4. Header ini diidentifikasi oleh nilai 43 dari ‘Next Header’ pada header sebelumnya. Formatnya adalah sebagai berikut :



Next Header	8-bit selector. Identifikasi tipe header setelah Routing Header. Menggunakan nilai yang sama dengan protokol Ipv4.
Hdr Ext Len	8-bit unsigned integer. Panjang dari Routing header dalam satuan 8-octet , tidak Termasuk 8 oktet yang pertama.

```
Routing Type          8-bit identifier untuk routing tertentu.

Segments Left         8-bit unsigned integer.  Jumlah rute segmen
                      Yang masih tersisa, misal, jumlah node antara yang
                      Harus dilewati sebelum mencapai tujuan.

type-specific data    panjangnya variabel, dimana formatnya ditentukan
                       oleh tipe routing.
```

Apabila dalam penerimaan paket, suatu node menemukan header routing yang tidak dikenal nilainya, yang harus dilakukan oleh node tersebut adalah bergantung pada nilai dari segmen sisa :

Apabila sisa segmen adalah nol, node tersebut harus mangabaikan Routing Header dan meneruskan memproses header dalam paket berikutnya, dimana tipenya diidentifikasikan oleh area Next Header dalam Routing Header.

Apabila sisa segmen tidak nol, node tersebut harus membuang paket tersebut dan mengirimkan problem parameter ICMP, kode 0, message ke pengirim paket dan menunjukkan Routing type mana yang tidak dikenal.

Fragment Header

Fragment header digunakan oleh pengirim Ipv6 untu kmengirimkan paket yang lebih besar yang tidak cukup dalam pat hMTU.. Fragment header diidentifikasikan oleh nilai 44 pada Next Header dan formatnya adalah seperti berikut :

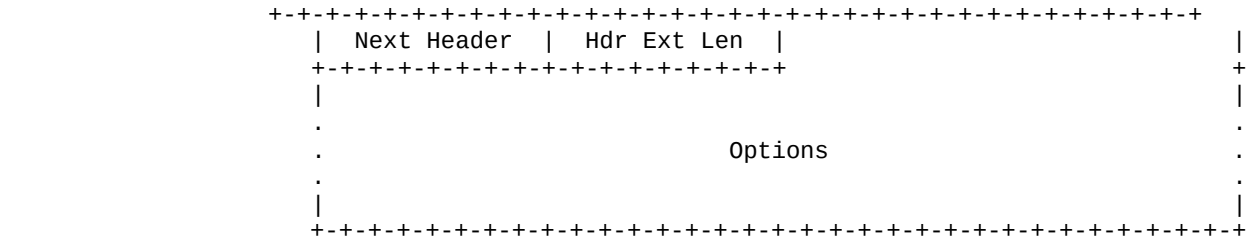
```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Next Header  |   Reserved    |      Fragment Offset    |Res|M|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Identification                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
Next Header           8-bit selector. Mengidentifikasikan tipe dari
                      Header awal dari bagian suatu paket. Menggunakan
                      Nilai yang sama seperti pada Ipv4.

Reserved              8-bit reserved field. Diisi nol pada saat
                      Pengiriman dan diabaikan di penerima.

Fragment Offset       13-bit unsigned integer. Ofset, dalam satuan 8 oktet
                      Dari data setelah header, relatif terhadap awal dari
                      bagian fragmen tersebut dalam paket aslinya.

Res                   2-bit reserved field. Diisi nol pada saat
                      Pengiriman dan diabaikan di penerima.

M flag                1 = fragmen antara ; 0 = fragmen terakhir.

Identification        32 bits.
```

Apabila paket yang dikirim terlalu besar untuk dimasukkan dalam MTU pada alur ke penerima, suatu node bisa membagi bagi paket tersebut menjadi beberapa fragmen dan mengirimkan masing masing fragmen tersebut dalam paket yang terpisah, kemudaian fragmen fragmen tersebut disatukan kembali di sisi penerima.

Destination Options Header

Destination Options header digunakan untuk membawa informasi opsonal yang harus diuji hanya oleh node penerima. Nilai dari identifier ini adalah 60 dan formatnya adalah sebagai berikut :



Next Header	8-bit selector. Mengidentifikasi tipe header Berikutnya. Menggunakan nilai yang sama dengan Yang digunakan pada protokol Ipv4
Hdr Ext Len	8-bit unsigned integer. Panjang dari Destination Options header dalam unit 8-oktet, Tidak termasuk 8 oktet yang pertama.
Options	Variable-panjang field, panjang dari Destination Options header yang lengkap, kelipatan 8 oktet.

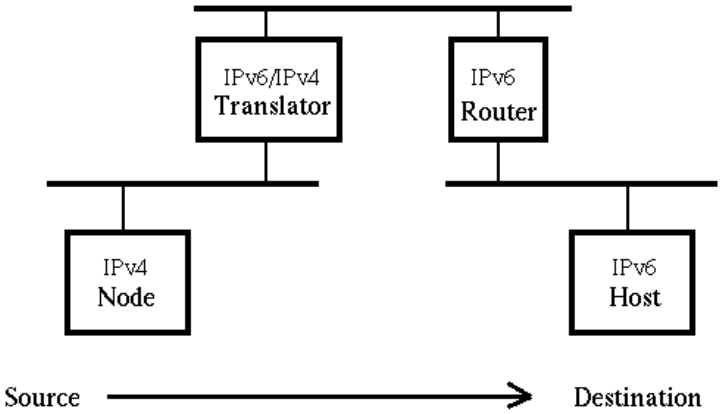
Header Translation

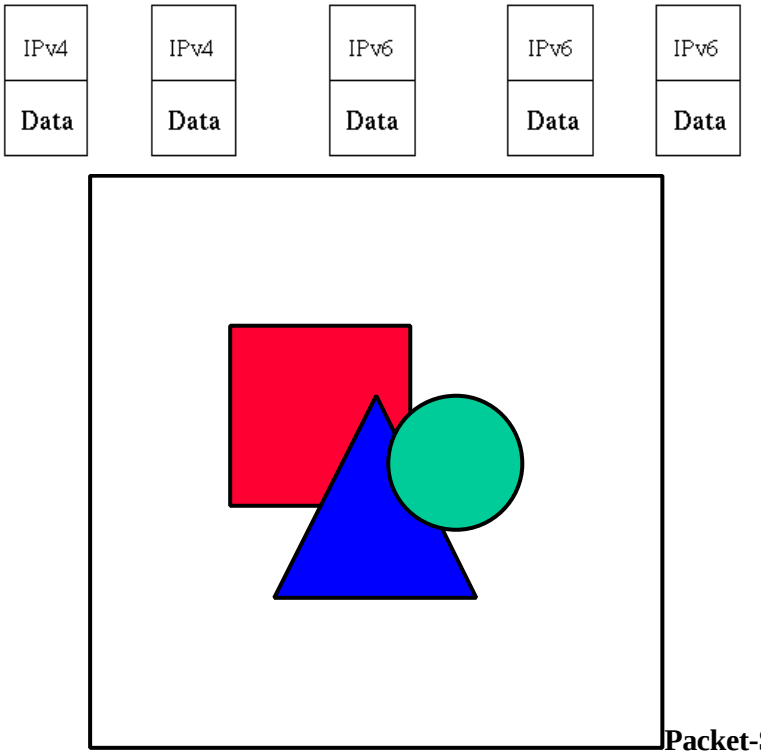
Beberapa cara diperlukan untuk mengimplementasikan IPv6 supaya bisa dipakai dalam infrastrukture IPv4 yang sekarang dipakai, diantaranya adalah translasi header..
Translasi header digunakan untuk menjembatani infrastruktur IPv4 dan infrastruktur IPv6. Ada dua macam trafic yang membutuhkan jembatan, paket IPv4 dan paket IPv6 yang dibungkus dengan header IPv4 yang dikirimkan diantara node IPv6.

Fungsi dari translator IPv6/IPv4 adalah seperti berikut :

1. Mengubah header IPv4 ke header IPv6.

Net Structure





Packet-Structure

2. Mengubah header IPv6 ke IPv4.

3. Membungkus kembali semua paket IPv6 kedalam paket IPv4. Hal ini dibutuhkan apabila IPv6/IPv4 header translating router bukan merupakan tujuan akhir dari data.