INTERNET PROTOCOL VERSION 4 (IPv4)

Internet Protocol addresss (alamat IP) merupakan suatu komponen vital dalam dunia internet, karena lamat IP dapat di katakana sebagai identitas dari pemakai internet, sehingga antara satu alamat dengan alamat lainnya tidak boleh sama. Pada awal perkembanagn internet di gunakan IPv4 yang penggunaanya masih di rasakan sampai sekarang.

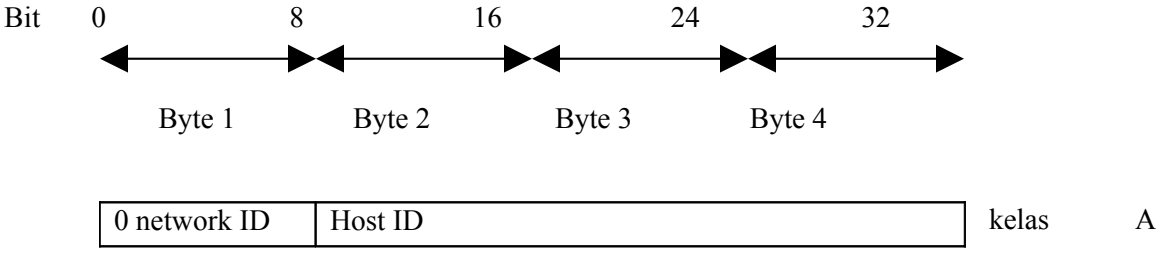
Internet Protocol (IP) pada awalnya di rancang untuk memfasilitasi hubungan antara bebrapa organisasi yang tergabung dalam departemen pertahanan Amerika yaitu Advanced Research Project Agency(ARPA). Sebelum terciptanya internet protocol, jaringna memiliki peralatan dan protocol tersendiri yang di gunaka nuntuk saling berhubungan, sehingga mainframe vendor A tidak dapat berkomunikasi dengan minicomputer pada vendor Begitupun sebaliknya. Dari permasalahan tersebut, kemudian di buatlah suatu protocol yang dapat di gunakan secara umum untuk menyatukan berbagai perbedaan dalam penggunaan perangkat yang terhubung di dalam jaringan. Protocol tersebutlah yang sampai saat ini masih mendominasi dalam pemakaiannya oleh masyarakat banyak, yaitu internet protocol versi 4 (IPv4).

Pembagian Kelas IPv4

Pada IPv4 dapat di bagi menjadi 3 kelas yang tergantung dari besarnya bagian host, yaitu :

- Kelas A (bagian host sepanjang 24 bit, terdiri dari 16,7 juta host)
- Kelas B (bagian host sepanjang 16 bit, terdiri dari 65534 host)
- Kelas C (bagian host sepanjang 8 bit , terdiri dari 254 host)

Alamat IPv4 dapat juga di bagi menjadi 5 bagian, yaitu kelas A, kelas B, kelas C, kelas D, dan kelas E. Akan tetapi kelas yang paling banyak digunakan adalah kelas A, B dan C saja, karena kelas E di gunakan untuk alamat multicase yang tidak memilki network ID dan host ID, sedangkan kelas E di gunakan untuk penggunaan khusu. Berikut adalah gambar pembagian kelas dari alamat IPv4 .



10 Network ID	Host ID	kelas	B
110 Network ID	Host ID	kelas	C
1110 Multicast Address		kelas	D
1111 Digunakan untuk keperluan masa depan		kelas	E

Untuk lebih jelasnya lagi dalam pembagian kelas dalam IPv4, maka dapat dilihat melalui table pembagian kelas IPv4

Table pembagian kelas IPv4

Bit Inisial a	Format	Range a	Jumlah Kelas	Kelas	Bagian Network	Bagian Host	Guna
0…	0hhhhhhh.hhhhhhhh. hhhhhhhh. hhhhhhhh	0-127	126	A	A	b,c,d	Jaringan besar
10…	10hhhhhh.hhhhhhhh. hhhhhhhh. hhhhhhhh	128-191	16.384	B	a,b	c,d	Jar.menengah
110…	110hhhhh.hhhhhhhh. hhhhhhhh. hhhhhhhh	192-223	2.097.152	C	a,b,c	d	Jar. kecil
1110…	1110mmmm. mmmmmmmm. mmmmmmmm. mmmmmmmm	224-247	-0	D	a,b,c	d	Cadangan:IP multicasting
1111…	1111rrrr.rrrrrrrr.rrrrrrrr. rrrrrrrr	248-255	-	E	a,b,c	d	Cadangan : eksperimen

Untuk keperluan alokasi alamat Ip yang di gunakan untuk jaringan pribadi (Private network), yang tidak di gunakan dalam internet (Public network), menurut RFC 1597 di atur sebagai berikut :

The internet assigned number authority (IANA) has reserved the three blocks of the IP address space for private network :			
10.0.0.0	-	10.255.255.255	For class A
172.16.0.0	-	172.31.255.255	For class B
192.168.0.0	-	192.168.255.255	For class C

Subnetting IPv4

Subnet mask ialah angka biner 32 bit yang di gunakan untuk :

- membedakan network ID dan host ID
- menentukan letak suatu host, apakah berada di jaringan local atau di jaringan luar.

Kelas A	255.0.0.0	FF.00.00.00
Kelas B	255.255.0.0	FF.FF.00.00
Kelas C	255.255.255.0	FF.FF.FF.00

Catatan :

Aturan RFC 950 adalah, subnet-ID 0 (alamat subnet) dan subnet-ID tertinggi (alamat broadcast) tidak boleh di gunakan. daftar subnet yang di alokasikan adalah sebagai berikut :

Alamat Subnet	Alamat Broadcast	Range IP address
192.168.0.0	192.168.0.31	192.168.0.1 s/d 192.168.0.30
192.168.0.32	192.168.0.63	192.168.0.33 s/d 192.168.0.62
192.168.0.64	192.168.0.95	192.168.0.65 s/d 192.168.0.94
192.168.0.96	192.168.0.127	192.168.0.97 s/d 192.168.0.126
192.168.0.128	192.168.0.159	192.168.0.129 s/d 192.168.0.158
192.168.0.160	192.168.0.191	192.168.0.161 s/d 192.168.0.190
192.168.0.192.	192.168.0.223	192.168.0.193 s/d 192.168.0.222
192.168.0.224	192.168.0.255	192.168.0.225 s/d 192.168.0.254

Jika dengan subnet

11111111.11111111.1111111.00000000 =
FF.FF.FF.00 =
255.255.255.000

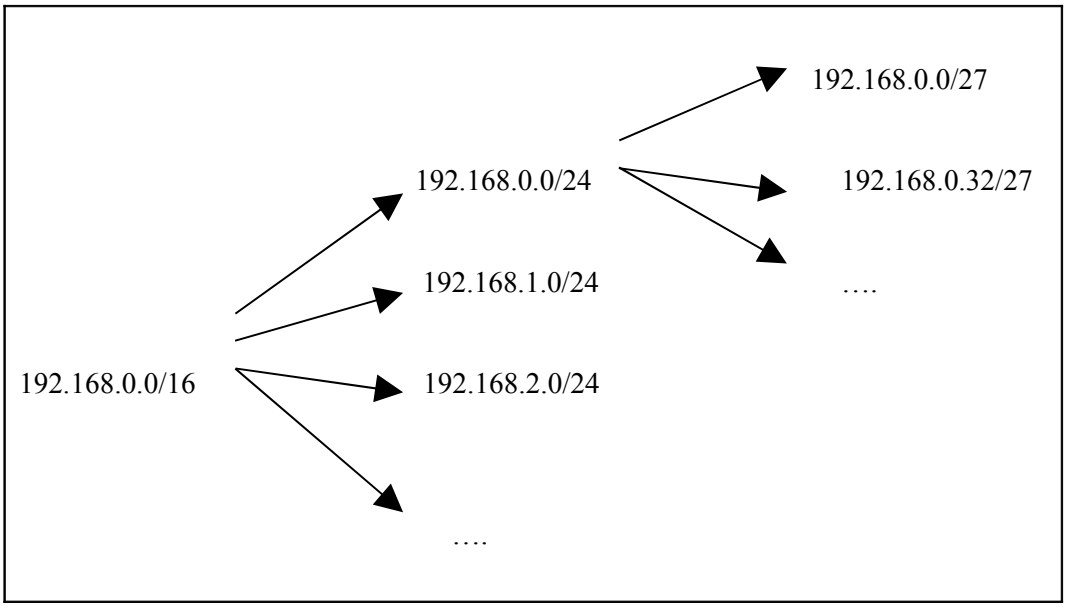
Pada subnet ID

192.168.0.0 / 24

Subnet yang dialokasikan adalah sebagai berikut :

Alamat Subnet	Alamat Broadcast	Range IP address
192.168.0.0	192.168.0.255	192.168.0.1 s/d 192.168.0.254

VLSM (Variabel Length Subnet Mask) memungkinkan pembagian ruang IP address secara rekrusif, contoh agregasi routingnya sebagai berikut :



Untuk memperoleh alamat jaringan tersebut, maka administrator jaringan harus mengajukan permohonana jenis kelas berdasarkan skala jaringan yang di kelolanya. Konsep kelas ini memiliki keuntungan yaitu pengelolaaan route informasi tidak memerlukan seluruh 32 bit tersebut, melainkan cukup hanya bagian jaringan nya saja, sehingga besar informasi route yang di simpan di router, menjadi kecil. Setelah alamat jaringan di peroleh, maka organisasi tersebut dapat secara bebas memeberikan alamat bagian host pada masing-masing hostnya. Alasan pembagian kelas tersebut adalah :

- 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 memebedakan jaringan tersebut kategori besar, menengah, atau kecil.
- membedakan antara untuk jaringan dan alamat untuk host/router.

Format Alamat IPv4

Pemberian alamat dalam internet mengikuti format alamat IP (RFC1166). Alamat ini di nyatakan dengan 32bit(bilangan 0 dan 1) yang di bagi atas 4 bagian (setiap bagian terdiri dari 8 bit/octet) dan tiap kelompok di pisahkan dalam sebuah tanda titik. Untuk memudahkan pembacaan, penulisan alamat di lakukan dengan angka decimal, misalnya alamat IP 192.168.1.2 yang jika dinyatakan dalam bilangan biner menjadi 1100 0000.1010 1000.0000 0001.0000 0010.

Dari 32 bit ini berarti banyaknya jumlah maksimum alamat yang dapat di tuliskan adalah 2 pangkat 32 atau 4.294.967.296 alamat.

Adapun format alamat IPv4 terdiri dari 2 bagian, netid dan hosted. Netid sendiri menyatakan alamat jamringan sedangkan hosted menyatakan alamat local(host/router). Akan tetapi dari 32 bit ini tidak boleh semuanya angka 0 atau 1(0.0.0.0 digunakan untuk jaringan yang tidak di kenal dan 255.255.255.255 digunakn untuk broadcast).

Sebagai contoh adalah :

Alamat IPv4 dalam bilangan biner :

11000000.10101000.00000001.00000010

Setelah di konversi ke bilangan decimal menjadi :

192.168.1.2

Pengalamatan IPv4

Alamat IP (dalam hal ini adalah IPv4) di gunakan untuk mengidentifikasi interface jaringan pada host computer. Untuk memudahkan kita dalam membaca dan mengingat suatu alamat IPv4, maka umumnya penamaan yang di gunakan adalah berdasarkan bilangan decimal atau sering di sebut sebagai notasi dotted decimal.

IPv4 memilki sifat yang di kenal sebagai : unriable, connectionless, datagram delivery service. IP address merupakan bilanagan biner 32 bit yang di pisahkan dengan oleh tanda pemisah berupa titik setiap 8 bit nya. Tiap 8 bit ini di sebut sebagai octet. Bentuk IP address adalah sebagai berikut :

(setiap symbol ”x” dapat di gantikan dengan angka 0 atau 1)

xxxxxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx.

Alamat IP dapat dibagai menjadi 2 bagian, yaitu :

Network ID	Host ID

Network Address Translation (NAT)

Keterbatasan alamat pada IPv4 merupakan maslah pada jaringan global atau internet. Untuk memksimalkan menggunakqn alamat IP yang di berikan oleh internet service provider (ISP) maka dapat digunakan Network Address Translation atau sering di singkat dengan NAT. NAT membuat jaringan yang menggunakan alamat local(private), alamat yang tidak boleh ada dalam table routing internet dan di khusukan untuk jaringan local/internet, agar dapat berkomunikasi ke internet dengan jalan meminjam alamat IP internet yang di alokasikan oleh ISP.

Dengan teknologi NAT maka di mungkinkan alamat IP local/private terhubung dengan jaringan public seperti internet sebuah router NAT di tempatkan antara jaringan local(inside

network) dan jaringan public (outside network), dan mentranslasikan alamat local/internal menjadi alamat IP global yang unik sebelum mengirimkan paket ke jaringan luar seperti internet. Sehingga dengan NAT,jaringan internal/local tidak akan terlihat oleh dunia luar/internal.

a. Pembagian Nat

Nat dapat di bagi menjadi 2, yaitu :

1). Static

Translasi static terjadi ketika sebuah alamat local (inside) di petakan kepada sebuah alamat global/internet(outside). Alamat local dan global tersebut di petakan 1 lawan 1 secara statistic.

2). Dinamik

- NAT dengan kelompok

Translasi dinamik terjadi ketika router NAT di set untuk memahami alamat local yang harus di translasikan, dan kelompok (POOL) alamt global yang akan di gunakan untuk terhubung ke internet. Proses NAT dinamik ini dapat memetakan beberap kelompok alamat local ke beberapa kelompok alamat global.

- Nat overload

Sejumlah IP local internal dapat di translasikan ke suatu alamat IP global(outside). Hali ini sangat menghemat penggunaan alokasi IP dari ISP. Sharing/pemakaian bersama 1 alamat Ip ini menggunakan methode port multiplexing, atau perubahan port ke packet outbound.

b. Keuntungan dan Kerugian NAT

Nat sangan berguna/penting untuk mentranslasikan alamat IP. sebagai contoh apabila akan berganti ISP atau menggabungkan 2 internet(2 perusahaan) maka di harmuskan untuk merubah alamat IP internal. Akan tatapi dengan menggunkan teknologi Nat maka di mungkinkan untuk menambah alamat IP tanpa merubah alamat IP pada host atau computer. Dengan demikian akan menghilangkan duplicate IP tanpa pengalamatan kembali host atau computer.

Berikut adalah table keuntungan dan Kerugian dari penggunaan NAT :

Keuntungan	**Kerugian**
Menghemat alamat IP legal yang di tetapkan oleh NIC atau servis provider	Translasi menimbulkan delay switching
Mengurangi terjadinya duplicate alamat jaringan	Menghilangkan kemampuan trace(traceability) end to endip
Meningkatkan fleksibilitas untuk koneksi ke internet	Aplikasi tertentu tidak dapat langsung berjalan jika menggunkan NAT, perlu

	penyesuaian
Menghindarkan proses pengalamatan kembali (readdressing) pada saat jaringan berubah	

DHCP (Dynamic Host Configuratio Protocol)

DHCP merupakan salah satu keunggulan dari teknolohi IPv4, dimana dengan DHCP tersebut alamat IP dan subnet mask dapat di berikan secara otomatis oleh server ketika computer baru akan terhubung ke dalam suatu jaringan. DHCP sendiri berfungsi untuk memberikan IP address secara otomatis paad computer yang menggunak protocol TCP/IP. DHCP berkerja dengan relasi client-server, dimana DHCP server menyediakan suatu kelompok IP address yang dapat di berikan pada DHCP client. Dalam memberika IP address ini DHCP hanya meminjamkan IP address tersebut. Jadi pemberian Ip address ini berlangsung secara dinamis.

Keamanan IPv4

Saat ini metode dengan menggunakan S-HTTP(Secure-HTTP) untuk pengiriman nomor kartu kredit, ataupun data pribadi dengan mengenkripsinya, mengenkripsi email dengan PGP (Pretty Good Privacy) telah dipakai secara umum. Akan tetapi cara di atas adalah security yang di tawarkan oleh aplikasi. Dengan kata lain bila ingin memakai fungsi tersebut maka kita harus memakai aplikasi tersebut. Jika membutuhkan security pada komunikasi tanpa tergantung pada aplikasi tertentu maka di perlukan fungsi security pada layer TCP atau IP, karena IPv4 tidak mendukung fungsi keamanan ini kecuali di pasang suatu aplikasi khusus agar bisa mendukuing security.

Modul IPv4

Pada Redhat Linux versi 9, modul IPv4 telah terinstal secara langsung dengan status enabled. Oleh karena itu tidak di perlukan teknik tamabahan lagi untuk melakukan pengkonfigurasian pada modul IPv4.

Setting alamat IPv4

Untuk melakukan setting atau melakukan perubahaan alamat IPv4 dapat dilakukan melalui terminal Linux dengan memasukkan format perintah sebagai berikut :

```
/ifconfig <interface> <alamat IPv4 baru> netmask <subnet IPv4 baru>
```

Pada format perintah di atas berfungsi untuk melakukan perintah perubahan alamat IPv4dan subnetnya pada interface yang digunakan. Adapun interface yang di gunakan pada komputer1 dan 2 adalah eth0, sehingga perintah perubahan alamat IPv4 dapat menjadi :

```
[root@localhost root]# ifconfig eth0 192.168.2.1
netmask 255.255.255.0
```

Pada perintah perubahan alamat IPv4 tersebut, dimasukkan alamat IPv4baru dengan alamat 192.168.2.1 serta alamat subnet 255.255.255.0 karena menggunakan kelas C pada suatu interface bernama eth0.

Setelah memasukkan perintah untuk merubah alamat IPv4 tersebut, maka selanjutnya dapat di lakukan pengecekjan apakah alamat IPv4 yang telah di masukkan telah berhasil atau tidak denga menggunakan perintah “ifconfig” sebagai berikut :

```
[root@localhost root]#ifconfig
eth0      link encap : Ethernet HWaddr 00:11:95:60:24:08
          inet addr :192.168.2.1 Bcast : 192.168.2.255
          Mask : 255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU : 1500
          Metric : 1
          RX packets : 23 errors:0 dropped:0 overruns : 0
          Frame : 0
          TX packets : 10 errors:0 dropped:0 overruns : 0
          Carrier : 0
          Collisions : 0 txquelen : 100
          RX bytes :2572 (2.5 Kb) TX bytes:700 (700.0 b)
          Interupt : 10 Base address:0x3000
```

```
lo        link encap : Local Loopback
          inet addr :127.0.0.1   Mask : 255.255.255.0
          UP LOOPBACK RUNNING MTU : 16436
          Metric : 1
          RX packets :8565 errors:0 dropped:0 overruns : 0
          Frame : 0
          TX packets : 8565 errors:0 dropped:0 overruns : 0
          Carrier : 0
          Collisions : 0 txquelen : 100
          RX bytes :584702 (570.9 Kb) TX bytes: 584702 (570.9 Kb)
```

Dengan perintah ifconfig tersebut,maka jelas terlihat bahwa proses perubahan alamat IPv4 yang dilakukan sebelumnya telah berhasil (di tinjukkan pada karakter panah).

Untuk perubahan alamat pada computer 2, dapat dilakukan dengan perintah yang sama pada computer 1, akan tetapi dengan alamat IPv4 yang berbeda yaitu 192.168.2.2 dan subnet 255.255.255.0

Akhir dari IPv4

Dengan perkembangan Internet dan jaringan 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 apliksi yang menggunakan internet, di antaranya transfer file (FTP), surat elektronik(e-mail), akses jarak jauh(telnet), multimedia menggunakan internet, Voice Over Internet Protocol (VOIP), dan lain senagainya, membuat pemakainy dapat melampaui kapasitas jaringan berbasis IP untuk mensuplai layanana dan fungsi yang di perlikan tersebut. Sehingga di pekirakan bahwa 7 tahun mendatang alamat IPv4 Akan habis terpakai dan secara perlahan akan di kurangi penggunaanuya Karena tidak mampu lagi menfasilitasi perkembangan internet yang terbaru.

Hal ini mendorong para ahli untuk merumuskan internet protocol baru untuk menaggulangi keterbatasan resource Internet Protocol yang sudah muali habi serta menciptakan suatu Internet Protocol yang memiliki fungsi security yang dapat di andalkan (reliability).

INTERNET PROTOCOL VERSION 6 (IPv6)

Penggunaan IPv6 yang memilki nama lain IPng (IP next generation) pertama kali di rekomendasikan pada tanggal 25 juli di Toronto pada saat pertemuan IETF. Perancanagan dari IPv6 ini di latarbelakangi oleh keterbatasan pengalamatan IPv4 yang saat ini memiliki panjang 32 bit dirasa tidak dapat menangani seluruh pwngguna internet di masa depan akibat dari pertumbuhan jaringan pengembangan jaringan khususnya internet.

Keunggulan IPv6

IPv6 memiliki berbagai keunggulan di bandingkan denga IPv4. Adapun keunggulan dari IPv6 adalah :

a. Otomatisai setting(stateless less auto configuration).

Alamat pada IPv4 pada dasaranya statis terhadap host. Biasanya di berikan secara berurut pada host. Memang saat ini hal ini bias di lakukan secara otomatis dengan menggunakan DHCP, tetapi hal tersebut pada IPv4 merupakan fungsi tambahan saja, sebaliknya pada IPv6 fungsi untuk mensetting secara otomatis di sediakan secara standard dan merupakan default nya. Pada setting otomatis ini terdapata 2 cara tergantung dari penggunaan address, yaitu setting otomatis stateless dan statefull.

b. Setting otomatis stateless

   Cara ini tidak perlu menyediakan server untuk pengelolaan dan pemabgian IP address, hanya mensetting router saja di mana host yang telah tersambung di jaringan dari router yang ada pada jaringan tersebut memperoleh prefix alamat dari jaringan tersebut. Kemudian host menambah pattern bit yang di peroleh dari informasi yang unik terhadap host, lalu membuat IP address sepanjang 128 bit dan menjadikannya sebagai alamat IP dari host tersebut.

c. Setting otomatis statefull

   Merupakan pengelolaan secara ketat dalam hal range IP address yang di berikan pada host dengan menyediakan server untuk pengelolaan keadaan alamat IP, Dimana cara ini hamper mirip dengan cara DHCP pada IPv4. Pada saat melakukan setting secara otomatis, informasi yang di butuhkan antara router, server dan host adalah ICMP(Internet Control Message Protocol) yang telah di perluas. Pada ICMP dalam IPv6 ini termasuk pula IGMP(Internet Group Management Protocol) yang di pakai pada multicast dalam IPv4.

Keamanan IPv6

Pada IPv6 telah mendukung komunikasi komunikasi terenkripsi maupun authentification pada layer IP. Dengan memilki fungsi security pada IP itu sendiri, maka dapat di lakukan hal seperti packet yang di kirim dari host tertentu seluruhnya di enkripsi. Pada IPv6 untuk authentification dan komunikasi terenkripsi memakai header yang di perluas ynag di sebut AH (Authentification Header) dan payload yang di enkripsi yang disebut ESP (Encapsulating Security Payload). Pada komunikasi yang memerlukan enkripsi kedua atau salah satu header tersebut di tambahkan.

Fungsi security yang di pakai pada layer aplikasi, mislnya pada S-HTTP dipaakai SSL sebagai metode enkripsi, sedangkan pada PGP memakai IDEA sebagai metode enkripsinya.

Sedangkan manajemen kunci memakai cara tertentu pula. Sebaliknya, pada IPv6 tidak di tetapkan cara tertentu dalam metode enkripsi dan manajemen kunci, sehingga mnejadi fleksibel dapat memakai metode manapun.Hal ini di kenal sebagai Sh(Security Assocaition). Fungsi Security pada IPv6 selain pemakaian pada komunikasi terenkripsi antar sepasang host dapat pula melakukan komunikasi terenkripsi antar jaringan dengan cara menenkripsi paket oleh gateway dari 2 jaringan yang melakukan komunikasi tersebut.

Pengalamatan IPv6

Seperti diketahui sebelumnya, IPv6 di ciptakan untuk menangani masalah-masalah yang terdapat pada IP, akan tetapi perubahan dan penambahan pada IPv6 tersebut di buat tanpa melakukan perubahan pada core sebenarnya dari IP itu sendiri. Addressing atau pengalamatan merupakan perubahan yang mencolok yang dapat di lihat dari perbedaan antara IPv6dengan IPv4, akan tetapi perubahan tersebut merupakan hal bagaimana pengalamatan tersebut di implemntasikan dan di gunakan.

a. Karakteristik Model pengalamatan IPv6

   Secara umum karakteristik model pengalamatan model pada IPv6 memiliki dasar yang sama dengan pengalamatan IPv4. Berikut adalah karakteristik model dari pengalamatan IPv6 :

   - Core Function of Addressing (Fungsi Inti dari Pengalamatan)

     2 Fungsi utama dari pengalamatan adalah network interface identification dan routing. Routing merupakan suatu kemudahan untuk melakukan proses struktur dari pengalamatan pada internetwork.

   - Network Layer Addressing (Pengalamatan Layer Jsaringan)

     Pengalamatan IPv6 masih berhubungan satu dengan yang lainnya dengan network layer pada jaringan TCP/IP dan langsung dari alamat data link layer (sering disebut phsycal).

   - Jumlah pengalamatan IP per device (alat)

     Pengalamatan biasanya di gunakan untuk menandai perangkat jaringan sehingga setiap computer yang terhubung biasanya akana memilki 1 alamat(unicase), dan router dapat memilki lebih dari satu alamat untuk masing-masing physical network yang terhubung.

   - Address Innerpretation and Prefix Representation

     Alamat IPv6 memiliki kesamaan kelas dengan alamat IPv4 dimana masing-masing memiliki bagian network identifier dan bagian host identifier. Jumlah

panjang prefix digunakan untuk menyatakan panjang dari network ID itu sendiri(prefix length)

- Private and Public Address

  Kedua type dari alamat tersebut terdapat pada IPv6, walaupun kedua type tersebut di definisikan dan di gunakan untuk keperluan yang berbeda.

b. Type Alamat Pendukung IPv6

Satu perubahan penting yang terdapat pada model pengalamatan dari IPv6 adalah type alamat yang di dukungnaya. Pada IPv4 hnaya mendukung 3 type alamat seperti : unicast, multicast, dan broadcast dengan actual traffic yang paling banyak di gunakan adalah alamat unicast. IP multicast pada IPv4 tidak di kembangkan untuk keperluan luas sampai beberapa tahun setelah internet di luncurkan dan terus berlanjut dengan beberapa isu yang menghambat dari perkembangannya. Sedangkan IP broadvast memiliki beberapa alas an yang di tolak dengan alas an performansi (performance).

Pada IPv6, juga memiliki 3 type alamat seperti IPv4 akan tetapi dengan beberapa perubahan. Type alamat IPv6 terbagi mnjadi 3, yaitu : unicast, multicast, dan anycast. Selain ke tiga pembagian type alamat tersebut, IPv6 juga memilki 1 type alamat lagi yang di gunakan untuk keperluan di masa yang akan dating yang dinamakan dengan reserved.

a. Alamat Unicast

   Alamat Unicast digunakan untuk komunikasi 1 lawan 1 dengan menunjuk 1 host. Alamat Unicast dapat di bagi menjadi 4 bagian yaitu :

   >>. Alamat Global

   >>. Alamat Link Lokal

   >>. Site Lokal

   >>. Compatible

b. Alamat Multicast

   Alamat Multicast di gunakan untuk komunikasi 1 lawan banyak dengan menunjuk host dari group.

c. Alamat Anycast

   Alamat Anycast digunkan ketika suatu paket harus dikirimkan kebeberapa member dari group dan bukan mengirimkan ke seluruh member dari group atau dapat juga di katakana menunjuk host dari group, tetapi paket yang dikirim hanya pada satu host saja.

c. Ukuran Alamat IPv6

Secara teori ukuran/panjang dari alamat IP mempengaruhi jumlah alamat yang tersedia. Semakin panjang alamat IP maka semakin banyak pula ruang alamat yang tersedia untuk pemakainya. Seperti diketahui bahwa jumlah lamat IPv4 sangatlah kecil untuk mendukung teknologi Internet di mass depan dimana hal ini merupakan implikasi dari bagaimana alamat internet tersebur di gunakan.

Berbeda dengan IPv6. dengan alas an utnuk mengatasu kekurangan akan alamat pada internet, maka IPv6 menggunakan ukuran alamt sebesar 128 bit yang di bagi menjadi 16 oktet dan masing-masing octet terdiri dari 8 bit. Jika semua alamat digunakan, maka dapat dilakukan perhitungan sebagai berikut :

$2^{128\ bit} =$ 340.282.366.920.938.463.374.607.431.768.211.456
Alamat

Apabila di tulis dalam bentuk scientific, maka sekitar $3.4 * 10^{38}$, atau sekitar 340 triliun triliun triliun. Melebihi kapasitas pendududk di dunia yang akan terhubung internet di masa depan.

Akan tetapi terdapat beberapa kelemahan untuk mendapatkan atau menciptakan kapasitas ruang alamat yang besar. dengan pertimbangan menggunakan 64 bit sekalipun maka akan di dapatkan jumlah alamat sebesra 18 juta triliun. Dengan jumlah alamat sebanyak itu maka masih memungkinkan penggunaan internet di masa mendatang. Akan tetapi penggunaan lebar alamat 128 bit pada IPv6 adalah untuk alas an fleksibilitas bila dibandingkan dengan lebar alamat 64 bit.

Modul IPv6

Setelah melakukan hubungan antara kedua computer dengan menggunakan alamat IPv4, maka selanjutnya akan dibahas mengenai penggunaan IPv6 sebagai migrasi dari IPv4.

a. Memuat modul IPv6

Sebelum memuat modul IPv6, maka dapat di lkukan pengecekan terlebih dahulu terhadap system opreasi Redhat Linux 9 yang di gunakan. Hal ini tidak lah waajib, karena pada Redhat Linux versi 9 sendiri sebetulnya telah menyertakan modul IPv6 pada kernel yang di gunakan nya yaitu kernel versi 2.4.20-8. Semua tulisan yang berada pada kotak/table berwarna abu-abu berisi perintah yang diketikkan pada terminal redhat Linux

9 beserta dengan hasil keluaran atau output dari terminal. Perintah yang di gunakan untuk melakukan pengecekana modul IPv6 tersebut adalah sebagai berikut :

```
[root@localhost root]# test –f /proc/net/if_net6 &&
echo " kernel Linux telah mendukung  IPv6"
kernel Linux telah mendukung IPv6
```

Perintah di atas di gunakan untuk melihat apakah pada /proc/file-system terdapat entry/proc/net/if_net6 atau tidak dengan penambahan && echo " kernel Linux telah mendukung IPv6", maka apabila kernel linux telah mensukung modul IPv6 akan menghasilakan output tulisan kernel Linux telah mendukung IPv6.

b. Membuat Modul IPv6

Memuat modul IPv6 bertujuan untuk mengaktifkan modul yang akan di gunakan untuk menangani IPv6 baik konfigurasi maupun interkoneksi. Perintah yang di gunakan untuk memuat modul IPv6 tersebut adalah sebegai berikut :

```
[root@localhost root]# insmood IPv6
using / lib/modules/2.4.20-8/kernel/net/ipv6/ipv6.0
```

Dengan menggunakan perintah "insmood", maka semua aplikasi dan perangkat lunak yang mendukung IPv6 akan di aktifkan.Dengan menggunakan perintah "ifconfig" pada terminal linux, maka dapat di lihat hasil aktivitas modul IPv6 sebelum dan sesudah aktivitas, sebagai berikut :

- Sebelum Aktifasi

```
[root@localhost root]#ifconfig eth0
eth0      link encap : Ethernet HWaddr 00:11:95:60:24:08
          inet addr :192.168.2.1 Bcast : 192.168.2.255
          Mask : 255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU : 1500
          Metric : 1
          RX packets : 15 errors:0 dropped:0 overruns : 0
          Frame : 0
          TX packets : 63 errors:0 dropped:0 overruns : 0
          Carrier : 0
          Collisions : 0 txquelen : 100
```

```
RX bytes :1128 (1.1 Kb) TX bytes:4008 (3.9 b)
Interupt : 10 Base address:0x3000
```

- Sesudah Aktifasi

```
[root@localhost root]#ifconfig eth0
eth0    link encap : Ethernet HWaddr 00:11:95:60:24:08
        inet addr :192.168.2.1 Bcast : 192.168.2.255
        Mask : 255.255.255.0
        UP BROADCAST RUNNING MULTICAST  MTU : 1500
        Metric : 1
        RX packets : 372 errors:0 dropped:0 overruns : 0
        Frame : 0
        TX packets : 244 errors:0 dropped:0 overruns : 0
        Carrier : 0
        Collisions : 0 txquelen : 100
        RX bytes :22320 (21.7 Kb) TX bytes:14740 (14.3 b)
        Interupt : 10 Base address:0x3000
```

c. Memuat Modul IPv6 secara otomatis

Modul IPv6 yang di aktifkan sebelumnya, sebetulnya belum secara otomatis di load, sehingga apabila computer di restart, maka modul IPv6 akan kembali nonaktif. Untuk membuat modul IPv6 dapat secara otomatis di load ketika redHat Linux pertama kali start Up, maka perlu di tambahkan 1 baris perintah pada file/etc/modules.conf.
Perintah tersebut adalah :

```
Alias net-pf-10     IPv6 # load Ipv6 secara otomatis
```

Selain itu di mungkinkan juga untuk me-nonaktifkan proses load modul IPv6 secara otomatis dengan cara menambahkan baris perintah pada file/otc/modules.conf sebagai berikut :

```
Alias net-pf-10     off  # Un-load Ipv6 secara otomatis
```

Interkoneksi IPv6 dengan IPv4

Ipv6 mempunyai format alamat dan header yang berbeda dengan IPv4. Sehingga secar langsung IPv4 tidak bias melakukan interkoneksi dengan IPv6. Hal ini tentunya akan menimbulakan masalah implementasi pada IPv6 pada jaringan internet IPv4 yang telah ada. Sebagai solusi dalam masalah implementasi IPv6, maka diperlukan suatu mekanisme transisi IPv6. Tujuan pembuatan mekanisme pembuatan transisi ini adalah supaya paket IPv6 dapat di lewatkan pada jaringan IPv4 yang telah ada ataupun sebaliknya.

Pada interkoneksi IPv6 dengan IPv4 tersebut, menggunakan mekanisme automatic tunneling yang berfungsi untuk melewatkan paket IPv6 melalui jaringan IPv4 yang telah ada, tanpa merubah infrastruktur jaringna IPv4. mekanisme automatic tunneling mempunyai prinsip kerja mengenkapsulasi paket IPv6 dengan header IPv4, kemudian paket tersebut langsung di kirimkan ke jaringan IPv4.