BAB I Pengenalan IP

1.1 Tujuan Praktikum

1. Mahasiswa mampu mengetahui IPv4 dan IPv6
2. Mahasiswa mampu mengetahui bagian atau komponen pada alamat IPv4 dan IPv6
3. Mahasiswa mampu mengetahui perbedaan IPv4 dan IPv6
4. Mahasiswa mampu mengetahui klasifikasi alamat IP

1.2 Indikator/Pencapaian

1. Mahasiswa mampu mengintrepretasikan informasi yang terkandung pada alamat IPv4
2. Mahasiswa mampu menyederhanakan alamat IPv6
3. Mahasiswa mampu membedakan alamat IPv6 yang direkomendasikan dan yang kurang direkomendasikan

1.3 Pendahuluan

Semua komputer di dunia pada jaringan internet berkomunikasi satu sama lain dengan kabel bawah tanah atau kabel bawah air atau nirkabel (wireless). Jika ingin mengunduh file dari internet atau memuat halaman web atau melakukan apa pun yang berhubungan dengan internet, komputer harus memiliki alamat sehingga komputer lain dapat menemukan alamat untuk mengirimkan file atau halaman web tersebut ke komputer yang diminta. Dalam istilah teknis, alamat itu disebut Alamat IP atau Alamat Protokol Internet (Internet Protocol Address).

Mari kita pahami dengan contoh lain, seperti jika seseorang ingin mengirimi surat maka dia harus mengetahui alamat rumah yang dituju. Demikian pula komputer juga memerlukan alamat agar komputer lain di internet dapat berkomunikasi satu sama lain tanpa kebingungan menyampaikan informasi ke komputer orang lain. Dan itulah mengapa setiap komputer di dunia ini memiliki Alamat IP yang unik. Atau dengan kata lain, alamat IP adalah alamat unik yang digunakan untuk mengidentifikasi komputer atau node di internet. Alamat ini hanyalah rangkaian angka yang ditulis dalam format tertentu. Umumnya dinyatakan dalam sekumpulan angka misalnya 192.155.12.1. Di sini, setiap angka dalam himpunan berkisar antara 0 hingga 255. Atau bisa dikatakan alamat IP lengkap berkisar antara 0.0.0.0 hingga 255.255.255.255. Dan alamat IP ini diberikan oleh IANA (dikenal sebagai Internet Corporation For Internet Assigned Numbers Authority).

Tapi apa itu protokol Internet? Protokol internet adalah seperangkat aturan yang membuat internet berfungsi.

Cara kerja alamat IP mirip dengan bahasa lain. Itu juga dapat menggunakan beberapa aturan untuk mengirim informasi. Dengan menggunakan protokol ini, kita dapat dengan mudah mengirim dan menerima data atau file ke perangkat yang terhubung. Ada beberapa langkah di belakang layar.

Perangkat Anda secara langsung meminta Penyedia Layanan Internet (ISP) Anda yang kemudian memberikan perangkat Anda akses ke web.

Dan Alamat IP diberikan ke perangkat Anda dari rentang tertentu yang tersedia.

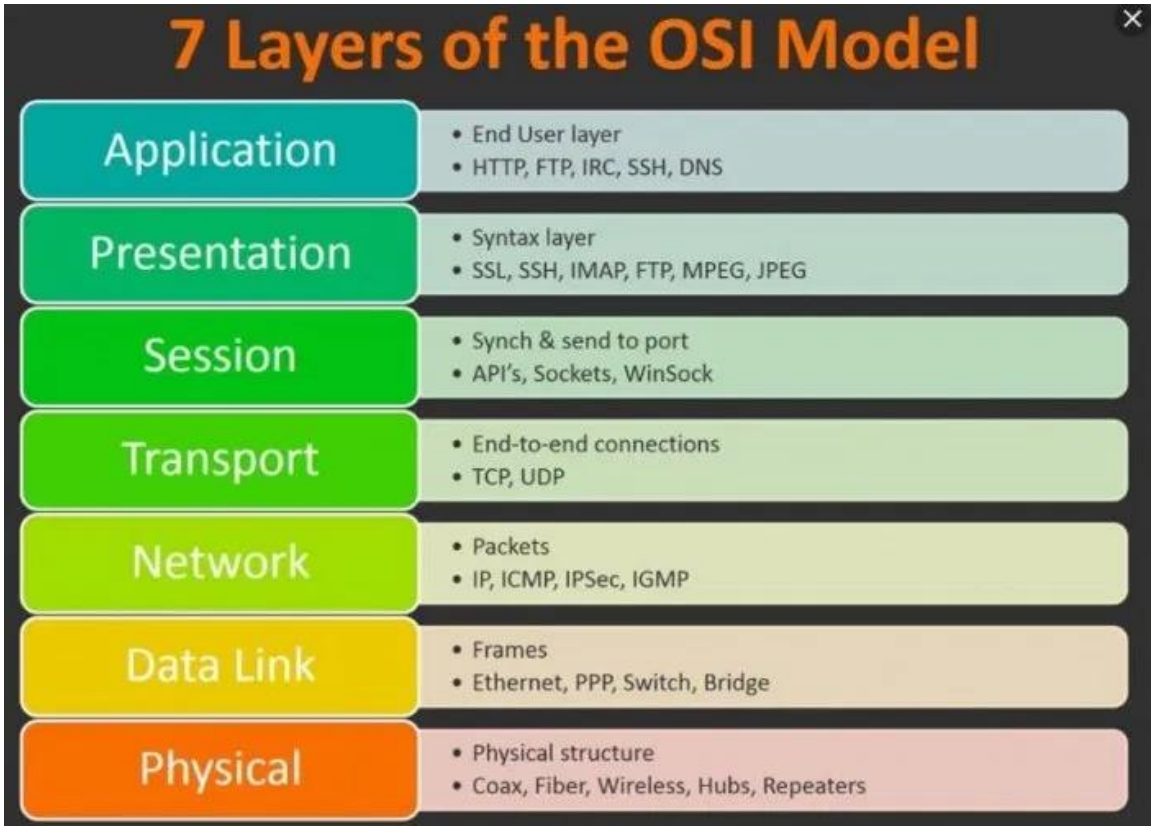
Aktivitas internet Anda melewati penyedia layanan Anda, dan mereka mengarahkannya kembali kepada Anda, menggunakan alamat IP Anda.

Alamat IP Anda dapat berubah. Misalnya, menghidupkan atau mematikan router dapat mengubah Alamat IP Anda.

Saat Anda keluar dari lokasi rumah, alamat IP rumah Anda tidak menyertai Anda. IP berubah saat Anda mengubah jaringan perangkat Anda.

1.4 OSI Layer

Sebelum pembahasan mengenai IP lebih mendalam, pada pembahasan mata kuliah sebelumnya, Anda sudah mempelajari mengenai OSI Layer. Pada modul ini hanya akan diulas secara singkat mengenai OSI Layer.



1. Application Layer (Lapisan ke-7)

Application layer adalah lapisan yang menjadi pusat (center) terjadinya suatu interaksi antara pengguna (end user) dengan aplikasi yang bekerja menggunakan fungsionalitas sebuah jaringan. Selain itu juga mempunyai fungsi untuk melakukan konfigurasi mengenai bagaimana cara aplikasi dapat bekerja menggunakan resource jaringan.

Dan kemudian, dapat memberikan pesan saat terjadi sebuah kesalahan pada proses pengaturan jaringan. Contoh beberapa services dan protokol yang berada pada application layer adalah HTTP, SMTP, FTP, dan lain – lain.

2. Presentation Layer (Lapisan ke-6)

Lapisan yang keenam adalah presentation layer, dimana mempunyai fungsi untuk mentranslasikan format data yang akan ditransmisikan oleh aplikasi melalui jaringan, ke dalam format yang dapat ditransmisikan oleh sebuah jaringan.

Pada layer ini, data juga akan ter- enkripsi dan dekripsi melalui sistem. Contoh protokol yang berada pada presentation layer adalah MIME, SSL, TLS, dan lain sebagainya.

3. Session Layer (Lapisan ke-5)

Session layer merupakan lapisan yang berfungsi untuk mendefinisikan bagaimana sebuah koneksi dapat dibuat, dikelola, dan dikembangkan. Contoh protokol yang berada pada session layer adalah NFS, SMB, RTP, dan lain – lain.

4. Transport Layer (Lapisan ke-4)

Transport layer mempunyai fungsi untuk memecah data menjadi paket – paket data, serta memberikan nomor urut untuk setiap paketnya. Sehingga, nantinya dapat disusun kembali saat sampai pada tujuan. Pada layer ini juga menentukan protokol yang akan digunakan untuk mentransmisikan data, seperti protokol TCP.

Protokol tersebut akan mengirimkan paket data, sekaligus memastikan bahwa setiap paket telah diterima dengan sukses dan tepat sasaran. Selain itu, juga dapat mentransmisikan ulang terhadap paket yang hilang atau rusak ketika proses pengiriman.

5. Network Layer (Lapisan ke-3)

Tugas dari network layer adalah membuat header untuk paket yang berisi informasi IP (Internet Protocol), baik IP pengirim atau IP tujuan data. Pada suatu kondisi, network layer juga melakukan proses routing melalui internetworking dengan menggunakan bantuan router dan switch pada layer ke-3.

6. Data-Link Layer (Lapisan ke-2)

Pada data-link layer memiliki tugas untuk menentukan setiap bit data dikelompokkan menjadi format yang disebut dengan frame. Pada level ini juga terjadi koreksi kesalahan, flow control,

pengalamatan hardware atau perangkat keras (seperti halnya pada MAC Address (Media Access Control Address)).

Serta, menentukan bagaimana perangkat jaringan seperti hub, repeater, bridge, dan switch pada layer 2 dapat beroperasi. Untuk spesifikasi IEEE 802, dapat membagi tingkatan menjadi 2 level, yaitu lapisan Media Access Control (MAC) dan lapisan Logical Link Control (LLC).

7. Physical Layer (Lapisan ke-1)

Dan model OSI Layer terakhir dan yang paling utama adalah physical layer. Fungsinya adalah untuk mendefinisikan media transmisi jaringan, sinkronisasi bit, metode pensinyalan, serta membangun arsitektur jaringan seperti pengkabelan dan topologi jaringan.

1.5 IPv4

IP adalah singkatan dari Internet Protocol dan v4 adalah singkatan dari Version Four (IPv4). IPv4 adalah versi pertama yang digunakan untuk produksi dalam ARPANET pada tahun 1983.

Alamat IP versi empat adalah bilangan bulat 32-bit yang akan dinyatakan dalam notasi desimal.

Contoh- 192.0.2.126 bisa berupa alamat IPv4.

1.5.1 Bagian dari IPv4

- Bagian jaringan:
  Bagian jaringan menunjukkan varietas khas yang ditugaskan ke jaringan. Bagian jaringan juga mengidentifikasi kategori jaringan yang ditetapkan.
- Bagian host:
  Bagian host secara unik mengidentifikasi mesin di jaringan Anda. Bagian dari alamat IPv4 ini ditugaskan ke setiap host.
  Untuk setiap host di jaringan, bagian jaringannya sama, namun separuh hostnya harus berbeda-beda.
- Nomor subnet:

Ini adalah bagian tidak wajib dari IPv4. Jaringan lokal yang memiliki sejumlah besar host dibagi menjadi beberapa subnet dan nomor subnet ditetapkan untuk itu.

1.5.2 Karakteristik IPv4

- IPv4 bisa berupa Alamat IP 32-Bit.
- IPv4 bisa berupa alamat numerik, dan bit-bitnya dipisahkan oleh sebuah titik.
- Jumlah kolom header adalah dua belas dan panjang kolom header adalah dua puluh.
- Ini memiliki gaya alamat Unicast, siaran, dan multicast.
- IPv4 mendukung VLSM (Masker Subnet Panjang Virtual).
- IPv4 menggunakan Protokol Resolusi Alamat Pos untuk memetakan ke alamat MAC.
- RIP mungkin merupakan protokol perutean yang didukung oleh daemon yang dirutekan.
- Jaringan harus dirancang secara manual atau dengan DHCP.
- Izin fragmentasi paket dari router dan menyebabkan host.

1.5.3 Keuntungan IPv4

- Keamanan IPv4 memungkinkan enkripsi untuk menjaga privasi dan keamanan.
- Alokasi jaringan IPV4 cukup besar dan saat ini memiliki lebih dari 85.000 router praktis.
- Menjadi mudah untuk menghubungkan beberapa perangkat di jaringan yang sangat besar tanpa menggunakan NAT.
- Ini adalah model komunikasi yang memberikan layanan berkualitas serta transfer pengetahuan yang ekonomis.
- Alamat IPV4 didefinisikan ulang dan memungkinkan pengkodean tanpa cacat.
- Perutean lebih terukur dan ekonomis karena pengalamatan bersifat kolektif dengan lebih efektif.
- Komunikasi data melalui jaringan menjadi lebih spesifik dalam organisasi multicast.
- Membatasi pertumbuhan bersih bagi pengguna yang sudah ada dan menghambat penggunaan internet bagi pengguna baru.
- Perutean Internet tidak efisien di IPv4.
- IPv4 memiliki harga Manajemen Sistem yang tinggi dan padat karya, rumit, lambat & sering terjadi kesalahan.
- Fitur keamanan tidak wajib.

- Sulit untuk menampilkan dukungan untuk keperluan masa depan karena penambahannya memerlukan biaya overhead yang sangat tinggi karena menghalangi fleksibilitas untuk menghubungkan semuanya melalui IP.

1.5.4 Keterbatasan IPv4

1. IP bergantung pada alamat lapisan jaringan untuk mengidentifikasi titik akhir pada jaringan, dan setiap jaringan memiliki alamat IP unik.
2. Persediaan alamat IP unik di dunia semakin berkurang, dan secara teoritis alamat-alamat tersebut mungkin akan habis.
3. Jika ada beberapa host, kita memerlukan alamat IP kelas berikutnya.
4. Konfigurasi host dan routing yang kompleks, pengalamatan non-hierarki, sulitnya penomoran ulang alamat, tabel routing yang besar, implementasi yang tidak sepele dalam memberikan keamanan, QoS (Quality of Service), mobilitas dan multi-homing, multicasting dll. adalah batasan besarnya. IPv4 jadi itulah mengapa IPv6 muncul.

1.6 IPv6

IPv6 dikembangkan oleh Internet Engineering Task Force (IETF) untuk mengatasi masalah kehabisan IPv4. IPv6 adalah alamat 128-bit yang memiliki ruang alamat 2128, jauh lebih besar dari IPv4. IPv6 menggunakan format Hexa-Desimal yang dipisahkan dengan titik dua (:) .

1.6.1 Komponen dalam Format Alamat

Berbeda dengan IPv4, format alamat IPv6 seperti berikut.

1. Ada 8 grup dan masing-masing grup mewakili 2 Byte (16-bit).
2. Setiap Hex-Digit terdiri dari 4 bit (1 gigitan)
3. Pembatas yang digunakan – titik dua (:)

1.6.2 Penulisan IPv6

Misalkan terdapat Alamat IPv6 sebagai berikut:

2001:0db8:0be0:75a2:0000:0000:0000:0001

Angka 0 yang paling mendahului dapat dihilangkan menjadi:

2001:db8:be0:75a2:0:0:0:1

Field angka 0 berurutan dapat digantikan dengan ::

2001:db8:be0:75a2::1

Contoh 2:

2001:0db8:0000:0000:0010:0000:0000:0001

Jika terdapat beberapa field angka 0 yang berurutan, hanya satu bagian saja yang dapat digantikan dengan ::

Anda dapat memilih salah satu:

2001:db8::10:0:0:1

Atau

2001:db8:0:0:10::1

Catatan:

Kedua bentuk di atas valid, namun bentuk yang pertama (bagian 0 paling awal yang dihilangkan) merupakan yang direkomendasikan berdasarkan RFC 5952.

1.6.3 Kebutuhan IPv6

Alasan utama dari IPv6 adalah penipisan alamat karena kebutuhan akan perangkat elektronik meningkat dengan cepat ketika Internet Of Things (IOT) mulai muncul setelah tahun 1980an & alasan lainnya terkait dengan lambatnya proses karena beberapa pemrosesan yang tidak diperlukan, kebutuhan akan pilihan baru, dukungan untuk multimedia, dan kebutuhan akan keamanan yang sangat mendesak. Protokol IPv6 merespons masalah di atas menggunakan perubahan utama berikut pada protokol:

1. Ruang alamat yang besar
   Alamat IPv6 memiliki panjang 128 bit. Dibandingkan dengan alamat IPv4 32 bit, ini merupakan peningkatan yang sangat besar (2 dimunculkan 96 kali) dalam ruang alamat.

2. Format tajuk yang lebih baik

IPv6 menggunakan format header baru yang opsinya dipisahkan dari header dasar dan disisipkan, bila diperlukan, antara header dasar dan data lapisan atas. Ini menyederhanakan dan mempercepat proses perutean karena sebagian besar opsi tidak perlu diperiksa oleh router.

3. Pilihan baru
   IPv6 memiliki opsi baru untuk memungkinkan fungsionalitas tambahan.
4. Tunjangan perpanjangan
   IPv6 dirancang untuk memungkinkan perluasan protokol jika diperlukan oleh teknologi atau aplikasi baru.
5. Dukungan untuk alokasi sumber daya
   Di IPv6, jenis bidang layanan telah dihapus, tetapi dua bidang baru, kelas lalu lintas dan label aliran telah ditambahkan untuk memungkinkan sumber meminta penanganan khusus terhadap paket. mekanisme ini dapat digunakan untuk mendukung lalu lintas seperti audio dan video real-time.
6. Dukungan untuk keamanan lebih
   Opsi enkripsi dan otentikasi di IPv6 memberikan kerahasiaan dan integritas paket.

Dalam representasi, IPv6 memiliki tiga metode pengalamatan :

1. Unicast
2. Multicast
3. Anycast

1.6.4 Metode Pengalamatan

1. Alamat Unicast
   Alamat Unicast mengidentifikasi single network interface. Paket yang dikirim ke alamat unicast dikirimkan ke interface yang diidentifikasi oleh alamat tersebut.
2. Alamat Multicast
   Alamat Multicast digunakan oleh banyak host, disebut sebagai grup, memperoleh alamat tujuan multicast. Host tidak perlu berada bersama secara geografis. Jika ada paket yang dikirim ke alamat multicast ini, paket tersebut akan didistribusikan ke semua interface yang sesuai dengan alamat multicast tersebut. Dan setiap node dikonfigurasi dengan cara yang sama. Sederhananya, satu paket data dikirim ke beberapa tujuan secara bersamaan.

3. Alamat Anycast

   Alamat Anycast ditetapkan ke sekelompok interface. Setiap paket yang dikirim ke alamat anycast hanya akan dikirim ke satu interface anggota (kebanyakan host terdekat).

   Catatan: Broadcast tidak ada di IPv6.

1.6.5 Jenis alamat IPv6

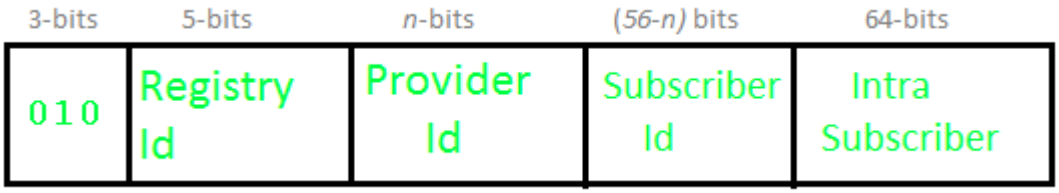
IPv6 memiliki 128 bit dalam alamat IPv6 tetapi dengan melihat beberapa bit pertama kita dapat mengidentifikasi jenis alamatnya.

Prefix	**Alokasi**	**Fraksi dari Ruang Alamat**
Biner: 0000 0000 0000::	Reserved	1/256
0000 0001 0100::	Unassigned (UA)	1/256
Biner: 0000 0010 0200::	Reserved for NSAP	1/128
Biner: 0000 0100 0400::	UA	1/64
Biner: 0000 1000 0800::	UA	1/32
Biner: 0001 1000::	UA	1/16
Biner: 0010 2000:: /3	Global Unicast	1/8
Biner: 0010 0000 0000 0001 0000 1101 1011 1000 2001:db8:: /32	Dokumentasi	
Biner: 0100 4000::	UA	1/8
Biner: 0110	UA	1/8

Prefix	Alokasi	Fraksi dari Ruang Alamat
6000::		
Biner: 1000 8000::	UA	1/8
Biner: 1010 a000::	UA	1/8
Biner: 1100 c000::	UA	1/8
Biner: 1110 e000::	UA	1/16
Biner: 1111 0000 f000::	UA	1/32
Biner: 1111 1000 f800::	UA	1/64
Biner: 1111 1100 fc00:: /7	Unique Local Unicast Address	1/128
Biner: 1111 1110 0 fe00::	UA	1/512
Biner: 1111 1110 1000 fe80:: /10	Link-Local Unicast Addresses	1/1024
Biner: 1111 1110 1100 fec0::	Site-Local Unicast Addresses (Usang)	1/1024
Biner: 1111 1111 ff00:: /8	Multicast Address	1/256

Catatan: Di IPv6, semua angka 0 dan 1 dapat ditetapkan ke host mana pun, tidak ada batasan seperti IPv4.

1. Provider-based Unicast Address:
   Alamat ini digunakan untuk komunikasi global.

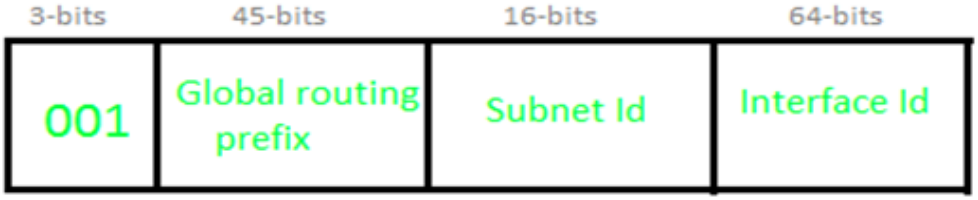


3 bit pertama mengidentifikasinya sebagai tipe ini.

Registry Id	Registry
10000	Multi regional (IANA)
01000	RIPE NCC
11000	INTER NIC
00100	APNIC

a. Id Registri (5-bit): Id Registri mengidentifikasi wilayah tempatnya berada. Dari 32 (yaitu 2^5), hanya 4 ID registri yang digunakan.
b. Id Penyedia: Tergantung pada jumlah penyedia layanan yang beroperasi di suatu wilayah, bit tertentu akan dialokasikan ke bidang Id Penyedia. Bidang ini tidak perlu diperbaiki. Katakanlah jika Provider Id = 10 bit maka Subscriber Id adalah 56 – 10 = 46 bit.
c. Id Pelanggan: Setelah Id Penyedia diperbaiki, sisanya dapat digunakan oleh ISP sebagai alamat IP normal.
d. Intra Pelanggan: Bagian ini dapat dimodifikasi sesuai kebutuhan organisasi yang menggunakan layanan ini.

2. Alamat Unicast berdasarkan geografi :



Awalan perutean global: Awalan perutean global berisi semua detail Lintang (Latitude) dan Bujur (Longtitude). Sampai sekarang, itu tidak digunakan. Dalam peruteannya akan didasarkan pada lokasi.

Id Antarmuka: Di IPv6, alih-alih menggunakan Id Host, digunakan istilah Id Antarmuka.

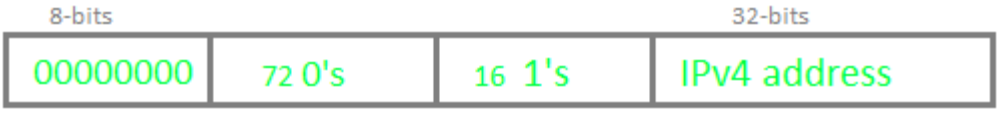
3. Beberapa alamat khusus:

Tidak ditentukan (Undefined)

Loopback (::1/128)

Kompatibel dengan IPv4

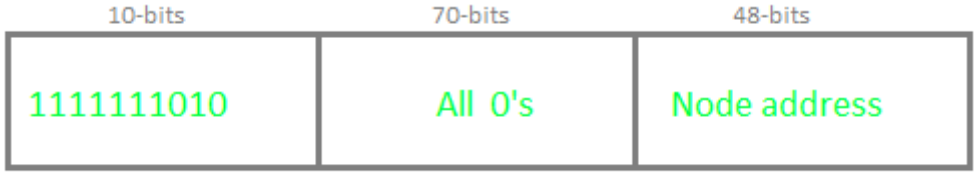
IPv4 dipetakan (IPv4 Mapped)



4. Alamat Unicast Lokal :

   Ini ada dua jenis: Tautan-lokal dan Situs-Lokal

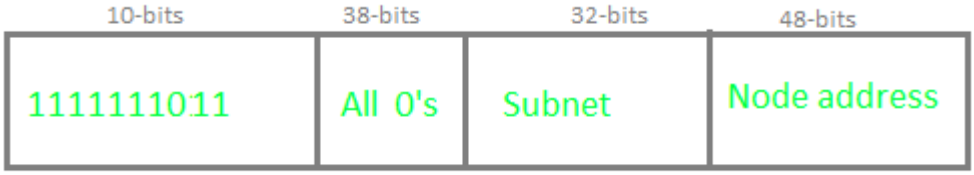
   a. Link-local Address:



Link-local address digunakan untuk mengalamatkan satu link. Itu juga dapat digunakan untuk berkomunikasi dengan node pada link yang sama. Link-local

address selalu diawali dengan 1111111010 (yaitu FE80). Router tidak akan meneruskan paket apa pun dengan Link-local address.

b. Site-local Address:



Site-local address setara dengan alamat IP pribadi di IPv4. Kemungkinan besar, beberapa ruang alamat dicadangkan, yang hanya dapat dirutekan dalam suatu organisasi. 10-bit pertama disetel ke 1111111011, itulah sebabnya site-local address selalu dimulai dengan FEC0. 32 bit berikut adalah ID Subnet, yang dapat digunakan untuk membuat subnet dalam organisasi. Alamat node digunakan untuk mengidentifikasi tautan secara unik. Namun, berkaitan dengan adanya permasalahan pada site-local address dengan koneksi VPN, maka digantikan dengan unique local addresss

1.6.6 Keuntungan IPv6

Berikut beberapa keuntungan dari penggunaan IPv6:

1. Transmisi Data Realtime : Transmisi data realtime mengacu pada proses transmisi data dengan sangat cepat atau segera. Contoh : Layanan live streaming seperti pertandingan kriket, atau turnamen lainnya yang disiarkan di web tepat pada saat kejadian dengan penundaan maksimal 5-6 detik.
2. IPv6 mendukung otentikasi: Memverifikasi bahwa data yang diterima oleh penerima dari pengirim adalah persis apa yang dikirim oleh pengirim dan datang melalui pengirim saja, bukan dari pihak ketiga mana pun. Contoh : Pencocokan nilai hash kedua pesan untuk verifikasi juga dilakukan oleh IPv6.
3. IPv6 melakukan Enkripsi: Ipv6 dapat mengenkripsi pesan pada lapisan jaringan bahkan jika protokol lapisan aplikasi pada tingkat pengguna tidak mengenkripsi pesan yang merupakan keuntungan besar karena menangani enkripsi.
4. Pemrosesan lebih cepat di Router: Router mampu memproses paket data IPv6 lebih cepat karena Base header yang lebih kecil dengan ukuran tetap – 40 byte yang membantu mengurangi waktu pemrosesan sehingga menghasilkan transmisi paket

yang lebih efisien. Sedangkan di Ipv4, kita harus menghitung panjang header yang terletak antara 20-60 byte.

1.7 IPv4 dan IPv6

IPv4	IPv6
Panjang alamat 32-bit	Panjang alamat 128-bit
Mendukung konfigurasi alamat secara manual dan DHCP	Mendukung konfigurasi otomatis dan penomoran ulang alamat
Pada end-to-end, integritas koneksi tidak dapat dicapai	Pada end-to-end, integritas koneksi dapat dicapai
Dapat menghasilkan ruang alamat $4{,}29\times10^{9}$	Ruang alamat IPv6 cukup besar sehingga dapat menghasilkan ruang alamat 3.4×10^{38}
Fitur keamanan bergantung pada aplikasi	IPSEC adalah fitur keamanan bawaan dalam protokol IPv6
Representasi alamat dalam desimal	Representasi alamat dalam heksadesimal
Fragmentasi dilakukan oleh pengirim dan router penerus	Fragmentasi hanya dilakukan oleh pengirim
Identifikasi aliran paket (packet flow) tidak tersedia	Identifikasi aliran paket (packet flow) tersedia dan menggunakan flow label field di header
Tersedia checksum	Tidak tersedia checksum
Memiliki skema transmisi pesan siaran	Skema transmisi pesan multicast dan anycast IPv6 tersedia
Fasilitas enkripsi dan otentikasi tidak disediakan	Enkripsi dan otentikasi disediakan
Memiliki header 20-60 byte.	Memiliki header tetap sebesar 40 byte
IPv4 dapat diubah menjadi IPv6	Tidak semua IPv6 dapat dikonversi ke IPv4
Terdiri dari 4 field yang dipisahkan oleh alamat titik (.)	Terdiri dari 8 field yang dipisahkan dengan titik dua (:)
Alamat IP IPv4 dibagi menjadi lima kelas berbeda. Kelas A, Kelas B, Kelas C, Kelas D, Kelas E.	IPv6 tidak memiliki kelas alamat IP apa pun.
IPv4 mendukung VLSM (Variable Length subnet mask).	IPv6 tidak mendukung VLSM.
Contoh IPv4: 66.94.29.13	Contoh IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB

1.8 Klasifikasi Alamat IP

Alamat IP dapat diklasifikasikan sebagai berikut.

1. Alamat IP Publik: Alamat ini tersedia untuk umum dan ditetapkan oleh penyedia jaringan Anda ke router Anda, yang selanjutnya membaginya ke perangkat Anda. Alamat IP Publik terdiri dari dua jenis,
2. Alamat IP Dinamis (Dynamic IP Address): Saat menghubungkan ponsel cerdas atau komputer ke internet, Penyedia Layanan Internet memberi Alamat IP dari rentang Alamat IP yang tersedia. Sekarang, perangkat memiliki Alamat IP dan cukup menghubungkan perangkat ke Internet dan mengirim serta menerima data ke dan dari perangkat. Saat berikutnya mencoba menyambung ke internet dengan perangkat yang sama, penyedia memberi Alamat IP berbeda untuk perangkat yang sama dan juga dari rentang tersedia yang sama. Karena Alamat IP terus berubah setiap kali terhubung ke internet, ini disebut Alamat IP Dinamis.
3. Alamat IP Statis: Alamat statis tidak pernah berubah. Mereka berfungsi sebagai alamat internet permanen. Ini digunakan oleh server DNS. Apa itu server DNS? Server DNS adalah komputer yang membantu membuka situs web di komputer. Alamat IP Statis memberikan informasi seperti perangkat berada di benua mana, negara mana, kota mana, dan Penyedia Layanan Internet mana yang menyediakan koneksi internet ke perangkat tersebut. Setelah kita mengetahui siapa ISP-nya, kita bisa melacak lokasi perangkat yang terhubung ke internet. Alamat IP Statis memberikan keamanan yang lebih rendah dibandingkan Alamat IP Dinamis karena lebih mudah dilacak.
4. Alamat IP Pribadi: Ini adalah alamat internal perangkat Anda yang tidak dirutekan ke internet dan tidak ada pertukaran data yang dapat dilakukan antara alamat pribadi dan internet.
5. Alamat IP bersama: Banyak situs web menggunakan alamat IP bersama yang lalu lintasnya tidak besar dan sangat terkendali, mereka memutuskan untuk menyewakannya ke situs web serupa lainnya agar ramah biaya. Beberapa perusahaan dan server pengirim email menggunakan alamat IP yang sama (dalam satu server email) untuk mengurangi biaya sehingga mereka dapat menghemat waktu ketika server tidak aktif.
6. Alamat IP khusus: Alamat IP khusus adalah alamat yang digunakan oleh satu perusahaan atau individu yang memberi mereka manfaat tertentu menggunakan sertifikat Secure Sockets Layer (SSL) pribadi yang tidak berlaku untuk alamat IP bersama. Memungkinkan untuk mengakses situs web atau masuk melalui File Transfer Protocol (FTP) berdasarkan alamat IP, bukan nama domainnya. Ini

meningkatkan kinerja situs web ketika lalu lintas tinggi. Ini juga melindungi dari alamat IP bersama yang masuk daftar hitam karena spam.

1.9 Praktikum

1. Pada IPv4 berikut, tentukan a) network address, b) network ID, c) host ID, d) host IP range yang dapat dipakai, e) broadcast address, f) jumlah host, g) jumlah host yang dapat dipakai, h) subnet mask, i) jumlah subnet:
    a. 192.168.1/24
    b. 89.1.9.8/25
    c. 100.90.1.100/30
2. Carilah informasi lebih lanjut mengenai RFC 5952, kemudian tuliskan rekomendasi apa saja yang dituang dalam tulisan tersebut!
3. Pada IPv6 berikut, sederhanakan dan perbaiki alamat IP berdasarkan rekomendasi RFC 5952.
    a. 2001:03ab:0d00:0000:0000:0000:0000:0c01
    b. 2001:0000:A123:0D00:0000:0000:0000:0C01
    c. FE80:0000:0000:8123:AbCd:0000:0000:0123

1.10 Laporan

Laporan Praktikum terdiri dari (Cover, Pembahasan, Daftar Pustaka).

Format Penulisan Laporan :

1. Margin, Paper: A4
    a. Top: 3 cm
    b. Bottom: 3 cm
    c. Left: 4 cm
    d. Right: 3 cm
2. Jenis Font: Times New Roman
    a. Judul Bab: 14 pt, Bold
    b. Subbab dan Paragraf: 12 pt