

MSIM4316
Edisi 1

MODUL 01

Network Enterprise dan Sistem Pengalamatan IP

Zaenal Arifin, S.T., M.Kom.

Daftar Isi

| | |
|---|------------|
| Modul 01 | 1.1 |
| <i>Network Enterprise</i> dan Sistem Pengalamatan IP | |
| Kegiatan Belajar 1 | 1.4 |
| <i>Network Enterprise</i> | |
| Latihan | 1.9 |
| Rangkuman | 1.11 |
| Tes Formatif 1 | 1.11 |
| Kegiatan Belajar 2 | 1.14 |
| Sistem Pengalamatan IP <i>(Internet Protocol)</i> | |
| Latihan | 1.28 |
| Rangkuman | 1.29 |
| Tes Formatif 2 | 1.29 |
| Kunci Jawaban Tes Formatif | 1.32 |
| Daftar Pustaka | 1.33 |



Pendahuluan

Sebagai dasar dalam mempelajari *Network Administration*, perlu dipelajari dan dipahami terlebih dahulu konsep dan prinsip-prinsip merancang sistem jaringan *enterprise*.

Selanjutnya, dalam modul ini akan dibahas pula tentang sistem pengalamatan IP. Pada bagian ini mempersyaratkan Anda untuk **sudah** menguasai konversi bilangan desimal dan *hexadecimal* ke dalam bentuk sistem bilangan biner dan sebaliknya.

Pada modul ini Anda akan mempelajari konsep desain jaringan *enterprise* dan memanfaatkan serta menerapkan sistem pengalamatan IPv4 dan IPv6 pada suatu sistem jaringan.

Setelah mempelajari modul ini diharapkan Anda mampu:

1. menjelaskan pengertian tentang jaringan *enterprise*,
2. menyebutkan definisi tentang jaringan *enterprise*,
3. menjelaskan tentang berbagai konsep desain jaringan *enterprise*,
4. merancang desain jaringan *enterprise*,
5. menjelaskan pengalamatan ipv4 untuk jaringan *enterprise*,
6. menjelaskan pengalamatan ipv4 untuk jaringan *enterprise*,
7. menerapkan penggunaan pengalamatan ipv4 untuk jaringan *enterprise*,
8. menerapkan penggunaan pengalamatan ipv4 untuk jaringan *enterprise*.

Network Enterprise

A. PENGERTIAN *NETWORK ENTERPRISE*

Saat ini pemanfaatan teknologi semakin tinggi, khususnya teknologi yang terkait dengan interkoneksi. Akibatnya, penggunaan jaringan pun semakin tinggi dan menyebabkan bertambahnya infrastruktur, layanan, serta protokol pada lalu lintas jaringan, sehingga perlu dilakukan perencanaan dan perancangan sistem jaringan yang bersifat *enterprise*.

Terdapat beberapa pengertian terkait dengan *network enterprise* antara lain:

- *network enterprise* menurut Manual Castell merupakan jaringan yang terbentuk dari beberapa kelompok jaringan antar perusahaan, atau beberapa bagian dari beberapa perusahaan, atau sebagian internal dari beberapa perusahaan;
- menurut Cisco, *network enterprise* merupakan suatu desain arsitektur yang dibangun dengan latar belakang *multi platform*, *multi services*, *multi protocols* untuk memenuhi kebutuhan terhadap pemanfaatan teknologi informasi yang semakin tumbuh pesat. *Multi platform* mengandung arti infrastruktur yang terdiri atas beberapa perangkat *hardware* dan *software*. *Multi services* yang terdiri atas layanan yang banyak dan beragam. Sistem yang terdiri atas *multi platform* dan *multi services* umumnya membutuhkan *multi protocols*.

Dalam merancang suatu jaringan, terlepas dari ukuran atau persyaratan jaringan, faktor fundamental untuk implementasi yang benar dari setiap desain jaringan adalah dengan mengikuti prinsip-prinsip teknik terstruktur yang baik berikut ini.

- **Hierarki**, model jaringan hierarki merupakan rancangan infrastruktur jaringan yang membagi masalah kompleksitas dari desain jaringan menjadi area yang lebih kecil dan lebih mudah untuk dikelola.
- **Modular**, desain jaringan yang modular dengan mudah mendukung pertumbuhan dan perubahan. Dengan memisahkan dalam modul berbagai fungsi yang ada dalam jaringan, pengembangan jaringan dapat relatif lebih mudah, beberapa modul, antara lain blok layanan, *data center*, dan perimeter internet.

- **Resistensi dan *resilient***, desain jaringan harus memiliki karakteristik *high availability* (HA) yang memiliki waktu aktif mendekati 100 persen. Jaringan harus tersedia agar dapat digunakan, baik dalam kondisi normal, maupun kondisi abnormal (kegagalan *hardware* atau *software*).
- **Fleksibel**, merupakan kemampuan untuk memodifikasi bagian-bagian jaringan, menambah layanan baru atau meningkatkan kapasitas tanpa perlu pembaruan besar. Jaringan yang dibangun harus mampu untuk beradaptasi dengan cepat sesuai kebutuhan perkembangan/perubahan bisnis.

B. DESAIN JARINGAN MODEL HIRARKI

Desain jaringan model hierarki dirancang terdiri atas beberapa lapisan untuk menyederhanakan arsitekturnya. Setiap lapisan fokus secara spesifik berdasarkan fungsi, sehingga memungkinkan perancang jaringan untuk memilih sistem dan fitur yang tepat untuk setiap lapisan. Model ini menyediakan kerangka modular yang memungkinkan fleksibilitas dalam implementasi dan pemecahan masalah desain fasilitas jaringan. Salah satu arsitektur jaringan yang menggunakan model hierarki ini adalah arsitektur jaringan Cisco yang secara fundamental membagi jaringan atau blok modular ke dalam beberapa lapisan berikut.

- **Lapisan akses**, menyediakan akses jaringan untuk kelompok kerja dan pengguna. Perangkat jaringan pada lapisan ini digunakan untuk memberi akses pada pengguna, *server*, atau perangkat *edge* lainnya ke jaringan. Lapisan akses umumnya menghubungkan perangkat *switch* dengan *workstation*, *server*, *printer*, *access point wireless*, dan sebagainya. Di lingkungan WAN, lapisan akses untuk perangkat *telecommuters* atau *remote site* menyediakan akses ke jaringan perusahaan melintasi teknologi WAN. Lapisan akses merupakan lapisan yang paling kaya fitur jaringan yang mencakup teknologi keamanan, kontrol akses, dan sebagainya.

Beberapa fungsi pada lapisan akses, di antaranya berikut ini.

- *Layer 2 Switching*.
- *High availability*.
- *Port Security*.
- Klasifikasi dan penandaan *Quality of Services* (QoS).
- Pemeriksaan *Address Resolution Protocol* (ARP).
- *Virtual Access Control List* (VACL).
- Penerapan *Virtual Local Area Network* (VLAN).

- **Lapisan distribusi**, menyediakan konektivitas berbasis kebijakan dan mengontrol batas antara lapisan akses dan *core*. Lapisan distribusi merupakan *aggregator* dari lapisan akses, menggunakan *switch* atau *router* untuk melakukan segmentasi terhadap jaringan. Pada lapisan ini dilakukan proses *routing* dan *filtering*.

Lapisan distribusi dapat menyediakan yang berikut ini.

- Agregasi link LAN atau WAN.
 - Keamanan berbasis kebijakan dalam bentuk daftar kontrol akses (ACL) dan penyaringan.
 - Layanan *routing* antar jaringan LAN dan VLAN, dan antara *domain routing* (misalnya, EIGRP ke OSPF).
 - Redudansi dan *load balancing*.
 - Batas untuk agregasi dan *summarization* rute yang dikonfigurasi di *interface* ke lapisan *core*.
 - Mengatur *broadcast domain*, karena *router* maupun *switch multilayer* tidak melewatkan *broadcast*. Perangkat berfungsi sebagai titik demarkasi antara *broadcast domain*.
- **Lapisan core (backbone)**, menyediakan transportasi cepat antara *switch* distribusi. Lapisan *core* merupakan *backbone* yang berkecepatan tinggi, dirancang untuk mengalihkan paket secepat mungkin. Lapisan *core* merupakan lapisan yang sangat penting untuk konektivitas, maka harus menyediakan tingkat ketersediaan yang tinggi dan dapat beradaptasi dengan perubahan dengan cepat. Desain lapisan ini juga menyediakan skalabilitas dan konvergensi yang cepat.

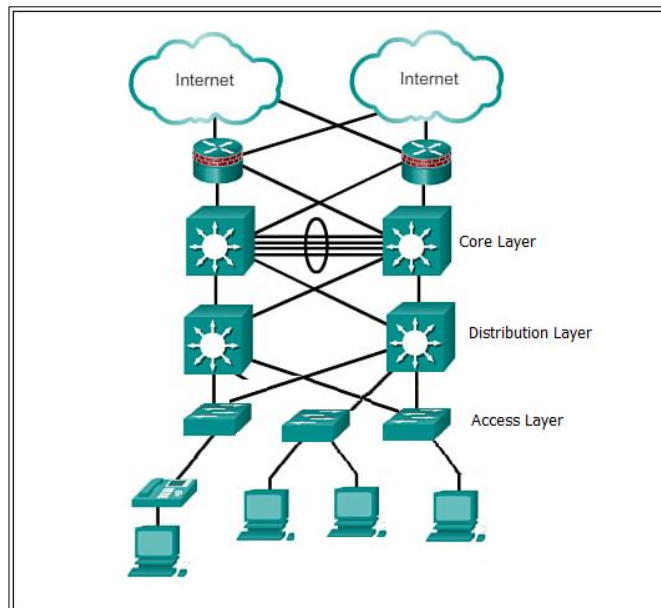
Beberapa pertimbangan mengenai penerapan pada lapisan *core* sebagai berikut:

- harus menyediakan mekanisme peralihan dengan kecepatan tinggi;
- harus menyediakan kehandalan dan *fault tolerance*;
- harus menghindari penanganan paket yang memerlukan kebutuhan yang tinggi terhadap CPU akibat adanya mekanisme pengamanan, inspeksi, klasifikasi kualitas layanan (QoS), atau proses lainnya.

Keuntungan yang dapat diperoleh dengan menerapkan rancangan jaringan yang bersifat hierarki, antara lain:

- menyediakan modularitas,
- lebih mudah dipahami,
- meningkatkan fleksibilitas,
- memudahkan pertumbuhan dan skalabilitas,
- mengurangi kerumitan pemecahan masalah.

Gambar 1.1 Mengilustrasikan model hierarki pada suatu jaringan.



Gambar 1.1
Model Jaringan Hierarki

Desain hierarki tiga tingkat memaksimalkan kinerja, ketersediaan jaringan, dan kemampuan untuk mengukur desain jaringan. Namun, untuk jaringan yang kecil dan tidak berkembang pesat dapat menggunakan desain hierarki dua tingkat. Pada desain tersebut, lapisan *core* dan distribusi digabungkan menjadi satu lapisan dan lebih praktis dan lebih efisien, dengan tetap mempertahankan sebagian besar manfaat dari model jaringan hierarki.

C. DESAIN JARINGAN MODULAR

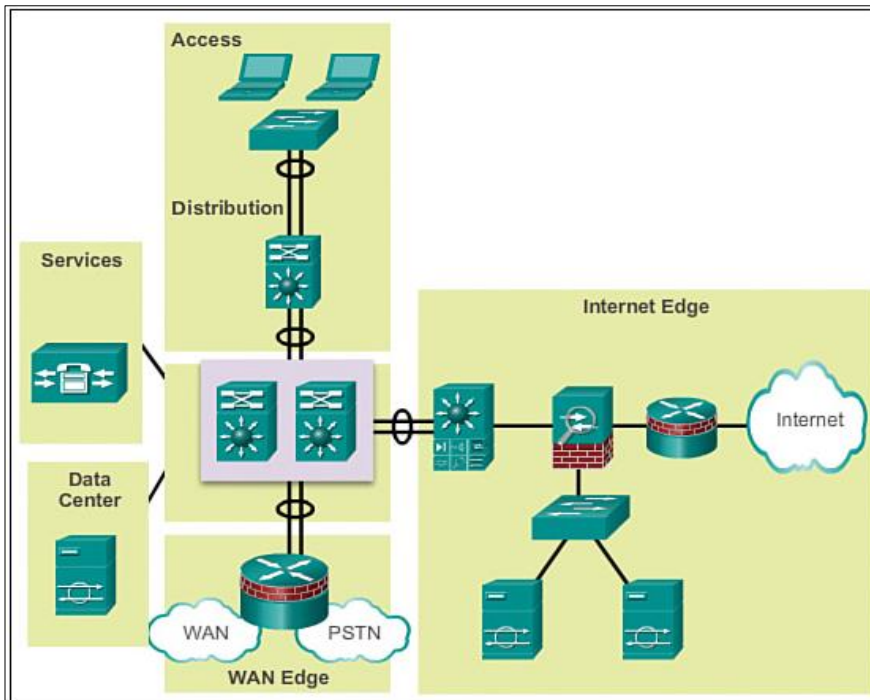
Dengan berkembangnya pemanfaatan teknologi informasi saat ini, kompleksitas jaringan pun meningkat, untuk memenuhi tuntutan tersebut, maka desain jaringan perlu disesuaikan dengan yang menggunakan pendekatan yang lebih modular. Penerapan model desain hierarki di beberapa blok fungsional jaringan, arsitektur jaringan yang lebih *scalable* dan modular dapat dicapai. Arsitektur jaringan modular ini menawarkan fleksibilitas desain tingkat tinggi yang membuatnya lebih responsif terhadap kebutuhan bisnis yang terus berkembang. Desain modular membuat jaringan dikelola dengan melakukan isolasi domain kesalahan dan pola lalu lintas yang lebih deterministik. Akibatnya, perubahan dan peningkatan jaringan dapat dilakukan dengan cara yang terkontrol dan bertahap, sehingga memungkinkan stabilitas dan fleksibilitas yang lebih besar dalam pemeliharaan dan pengoperasian jaringan.

Desain jaringan modular memisahkan jaringan menjadi berbagai modul jaringan fungsional, masing-masing menargetkan tempat atau tujuan tertentu dalam jaringan. Modul mewakili area yang memiliki konektivitas fisik atau logis yang berbeda. Mereka menunjuk di mana fungsi yang berbeda terjadi di jaringan. Menggunakan pendekatan modular memiliki beberapa keuntungan, di antaranya sebagai berikut.

- Kegagalan yang terjadi dalam modul dapat diisolasi dari jaringan lainnya, menyediakan deteksi masalah yang lebih sederhana dan ketersediaan sistem keseluruhan yang lebih tinggi.
- Perubahan, peningkatan, atau pengenalan layanan baru jaringan dapat dilakukan dengan cara yang terkontrol dan bertahap, memungkinkan fleksibilitas yang lebih besar dalam pemeliharaan dan pengoperasian jaringan.
- Ketika modul tertentu tidak lagi memiliki kapasitas yang cukup atau kehilangan fungsi atau layanan baru, itu dapat diperbarui atau diganti dengan modul lain yang memiliki peran struktural yang sama dalam desain hierarki keseluruhan.
- Keamanan dapat diterapkan secara modular yang memungkinkan kontrol keamanan yang lebih terperinci.
- Penggunaan modul dalam desain jaringan memungkinkan fleksibilitas dan memfasilitasi implementasi dan pemecahan masalah.

Jaringan modular ini terdiri atas modul-modul yang saling terhubung dengan jaringan *core*, di antaranya berikut ini.

- ***Access-distribution***, dikenal pula dengan istilah blok distribusi.
- ***Services***, merupakan blok yang umum digunakan untuk mengidentifikasi layanan.
- ***Data center***, dikenal juga dengan istilah *server farm*. Blok ini bertanggung jawab untuk mengelola dan memelihara banyak sistem data yang penting pengguna mengandalkan data dan sumber daya di pusat data untuk membuat, berkolaborasi, dan berinteraksi secara efektif.
- ***Enterprise Edge***, merupakan blok yang terdiri atas ujung jaringan internet dan WAN. Blok-blok ini menawarkan konektivitas ke layanan suara, video, dan data di luar jaringan internal.



Sumber: ciscopress

Gambar 1.2
Desain Jaringan Modular



Latihan

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

- 1) Sebutkan dan jelaskan lapisan pada model jaringan hierarki!
- 2) Sebutkan dan jelaskan modul-modul jaringan pada model jaringan modular!
- 3) Sebutkan dan jelaskan prinsip-prinsip terstruktur dalam merancang jaringan!

Petunjuk Jawaban Latihan

- 1) Desain jaringan model hierarki dirancang terdiri atas beberapa lapisan untuk menyederhanakan arsitekturnya. Setiap lapisan fokus secara spesifik berdasarkan fungsi, sehingga memungkinkan perancang jaringan untuk memilih sistem dan fitur yang tepat untuk setiap lapisan.
 - a) **Lapisan akses**, menyediakan akses jaringan untuk kelompok kerja dan pengguna. Perangkat jaringan pada lapisan ini digunakan untuk memberi akses pada pengguna, *server* atau perangkat *edge* lainnya ke jaringan.

- Lapisan akses umumnya menghubungkan perangkat *switch* dengan *workstation*, *server*, *printer*, *access point wireless*, dan sebagainya.
- b) **Lapisan distribusi**, menyediakan konektivitas berbasis kebijakan dan mengontrol batas antara lapisan akses dan *core*. Lapisan distribusi merupakan *aggregator* dari lapisan akses, menggunakan *switch* atau *router* untuk melakukan segmentasi terhadap jaringan. Pada lapisan ini dilakukan proses *routing* dan *filtering*.
 - c) **Lapisan core (backbone)**, menyediakan transportasi cepat antara *switch* distribusi. Lapisan *core* merupakan *backbone* yang berkecepatan tinggi, dirancang untuk mengalihkan paket secepat mungkin. Lapisan *core* merupakan lapisan yang sangat penting untuk konektivitas, maka harus menyediakan tingkat ketersediaan yang tinggi dan dapat beradaptasi dengan perubahan dengan cepat.
- 2) Model jaringan modular: Arsitektur jaringan modular ini menawarkan fleksibilitas desain tingkat tinggi yang membuatnya lebih responsif terhadap kebutuhan bisnis yang terus berkembang. Desain modular membuat jaringan dikelola dengan melakukan isolasi domain kesalahan dan pola lalu lintas yang lebih deterministik.
- a) **Access-distribution**, dikenal pula dengan istilah blok distribusi.
 - b) **Services**, merupakan blok yang umum digunakan untuk mengidentifikasi layanan.
 - c) **Data center**, dikenal juga dengan istilah *server farm*. Blok ini bertanggung jawab untuk mengelola dan memelihara banyak sistem data yang penting pengguna **mengandalkan** data dan sumber daya di pusat data untuk membuat, berkolaborasi, dan berinteraksi secara efektif.
 - d) **Enterprise Edge**, merupakan blok yang terdiri dari ujung jaringan internet dan *WAN*. Blok-blok ini menawarkan konektivitas ke layanan suara, video, dan data di luar jaringan internal.
- 3) Prinsip-prinsip teknik terstruktur yang baik, yang terdiri dari berikut ini.
- a) **Hierarki**, model jaringan hierarki merupakan rancangan infrastruktur jaringan yang membagi masalah kompleksitas dari desain jaringan menjadi area yang lebih kecil dan lebih mudah untuk dikelola.
 - b) **Modular**, desain jaringan yang modular dengan mudah mendukung pertumbuhan dan perubahan. Dengan memisahkan dalam modul berbagai fungsi yang ada dalam jaringan, pengembangan jaringan dapat relatif lebih mudah, beberapa modul, antara lain blok layanan, *data center*, dan perimeter internet.
 - c) **Resistensi dan resilient**, desain jaringan harus memiliki karakteristik *high availability* (HA) yang memiliki waktu aktif mendekati 100 persen. Jaringan harus tersedia agar dapat digunakan, baik dalam kondisi normal, maupun kondisi abnormal (kegagalan *hardware* atau *software*).

- d) **Fleksibel**, merupakan kemampuan untuk memodifikasi bagian-bagian jaringan, menambah layanan baru atau meningkatkan kapasitas tanpa perlu pembaruan besar. Jaringan yang dibangun harus mampu untuk beradaptasi dengan cepat sesuai kebutuhan perkembangan/perubahan bisnis.



Rangkuman

Network enterprise merupakan suatu jaringan yang terbentuk dari beberapa kelompok jaringan yang terdiri atas *multi platform*, *multi services*, dan *multi protocols*.

1. Dalam merancang suatu jaringan perlu mengikuti prinsip-prinsip teknik terstruktur yang baik, yang terdiri atas hierarki, modular, resistansi, dan fleksibel.
2. Model jaringan hierarki merupakan jaringan yang terdiri atas beberapa lapisan, di antaranya *access*, distribusi, dan *core*.
3. Model jaringan modular merupakan jaringan yang terdiri atas beberapa modul, di antaranya adalah: *access-distribution*, *services*, *data center*, dan *enterprise edge*.



Tes Formatif 1

Pilihlah satu jawaban yang paling tepat!

- 1) Perangkat *switch layer 2* pada jaringan hierarki berada pada lapisan
 - A. *core*
 - B. *access*
 - C. distribusi
 - D. jawaban A, B, dan C salah
- 2) Berikut ini merupakan prinsip-prinsip terstruktur yang perlu diperhatikan dalam merancang jaringan, *kecuali*
 - A. hierarki
 - B. modular
 - C. fleksibel
 - D. *services*
- 3) Mekanisme *routing* pada jaringan hierarki diimplementasikan pada lapisan
 - A. *core*
 - B. *access*
 - C. distribusi
 - D. *services*

- 4) Pemasangan fitur *port security* pada jaringan hierarki diterapkan pada lapisan
 - A. *core*
 - B. *access*
 - C. distribusi
 - D. *services*

- 5) Desain jaringan harus memiliki karakteristik *high availability*, merupakan prinsip
 - A. modular
 - B. hierarki
 - C. fleksibel
 - D. resistansi

- 6) Infrastruktur yang terdiri atas beberapa perangkat *hardware* dan *software*, merupakan maksud dari istilah
 - A. *multi platform*
 - B. *multi services*
 - C. *multi protocols*
 - D. jawaban A, B, dan C salah

- 7) Pada jaringan modular, *server farm* akan terdapat pada modul
 - A. *data center*
 - B. *access-distribution*
 - C. *services*
 - D. *enterprise edge*

- 8) Teknologi VLAN pada jaringan hierarki diterapkan pada lapisan
 - A. *access*
 - B. distribusi
 - C. *data center*
 - D. *core*

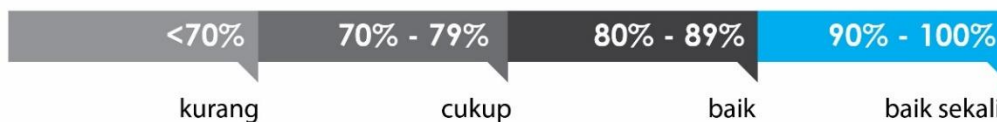
- 9) Berikut ini adalah hal-hal yang harus diperhatikan pada lapisan *core*, kecuali
 - A. menyediakan kebijakan *routing* dan *filtering*
 - B. menyediakan mekanisme peralihan dengan kecepatan tinggi
 - C. menyediakan kehandalan dan *fault tolerance*
 - D. menghindari penanganan paket yang memerlukan kebutuhan yang tinggi terhadap CPU

- 10) Pada jaringan modular, koneksi internet akan terdapat pada modul
- A. *data center*
 - B. *access-distribution*
 - C. *services*
 - D. *enterprise edge*

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 1 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 1.

$$\text{Tingkat Penguasaan} = \frac{\text{Jumlah Jawaban yang Benar}}{\text{Jumlah Soal}} \times 100$$

Arti tingkat penguasaan



Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan Kegiatan Belajar 2. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 1, terutama bagian yang belum dikuasai.

Sistem Pengalamatan IP (*Internet Protocol*)

Alamat merupakan suatu elemen yang sangat diperlukan dalam sistem jaringan. Alamat pada jaringan merupakan identitas berupa angka dari suatu *host* dan jaringan agar dapat dikenali dan saling berkomunikasi. Sistem pengalamatan pada jaringan umumnya terdiri atas dua jenis, yakni alamat logik dan alamat fisik. Sistem pengalamatan logik yang digunakan pada sistem jaringan juga beragam jenisnya, tetapi yang paling umum digunakan sistem pengalamatan IP (*Internet Protocol*).

IP merupakan salah satu protokol pada jaringan internet yang digunakan agar komputer dapat saling berkomunikasi. IP bekerja pada *network layer* dan bersifat *connectionless protocol*. Sistem pengalamatan berbasis IP yang digunakan saat ini terdiri dari 2 versi, yakni: IPv4 dan IPv6.

A. SISTEM PENGALAMATAN IPV4

Sistem bilangan yang digunakan pada IPv4 adalah sistem bilangan desimal, yang terdiri atas angka 0 hingga 255. Sistem pengalamatan IPv4 merupakan suatu alamat yang dibentuk dari 32 bit bilangan biner. Format alamat IPv4 membagi 4 bagian dari 32 bit tersebut, masing-masing bagian terdiri dari satu *byte* (8 bit).

XXXXXXXX.XXXXXXXXXX.XXXXXXXXXX.XXXXXXXXXX

dimana x merupakan bilangan 0 atau 1 (bilangan biner).

Suatu alamat IP terdiri dari dua komponen berikut.

- *Network ID*, sejumlah bit bagian depan dari format alamat IP secara unik menandai alamat suatu kelompok jaringan. Jumlah bit bagian *Network* tergantung pada banyaknya nilai bit 1 pada *subnet mask*.
- *Host/node ID*, sejumlah bit bagian belakang dari format alamat IP secara unik menandai identitas setiap mesin yang terpasang pada suatu jaringan. Jumlah bit bagian *host/node* tergantung pada banyaknya nilai bit 0 pada *subnet mask*.

Contoh 1:

IP = 192.168.10.5 : 11000000. 10101000. 00001010. 00000101
 SM = 255.255.255.0 : 11111111. 11111111. 11111111. 00000000
NETWORK ID HOST ID

Contoh 2:

IP = 172.16.10.5 : 10101100. 00010000. 00001010. 00000101
 SM = 255.255.0.0 : 11111111. 11111111. 00000000. 00000000
NETWORK ID HOST ID

Subnet mask (SM) merupakan suatu teknik yang digunakan untuk membagi bagian *network* dan *host* pada suatu alamat IPv4. Penulisan *subnet mask* selain menggunakan cara desimal, dapat juga dilakukan dengan menggunakan teknik *bit-count* (menuliskan berdasarkan banyaknya bit 1 yang terdapat di subnet mask).

Contoh:

SM : 255.255.255.0 = /24 (banyaknya bit 1 di subnet mask 24 bit)
 SM : 255.255.0.0 = /16 (banyaknya bit 1 di subnet mask 16 bit)
 SM : 255.0.0.0 = /8 (banyaknya bit 1 di subnet mask 8 bit)

IP address terbagi dalam lima kelas, sebagai berikut:

| | | | | |
|-----------|---------|-------|-------|-------|
| Kelas A → | 1-126 | 1-255 | 1-255 | 1-255 |
| Kelas B → | 128-191 | 1-255 | 1-255 | 1-255 |
| Kelas C → | 192-223 | 1-255 | 1-255 | 1-255 |
| Kelas D → | 224-239 | 1-255 | 1-255 | 1-255 |
| Kelas E → | 240-255 | 1-255 | 1-255 | 1-255 |

angka yg digunakan untuk menentukan Kelas

Gambar 1.3
IPv4 Berdasarkan Kelas

Kelas dari suatu alamat dapat ditentukan berdasarkan angka pada oktet pertama. Jika angka pada oktet pertama suatu alamat IP berkisar dari 1 sampai dengan 126 berarti alamat tersebut termasuk dalam kelas A. Begitu pun jika angka pada oktet pertama suatu alamat IP berkisar dari 192 sampai dengan 223 berarti alamat tersebut termasuk dalam kelas C, seperti terlihat pada gambar 1.x. Alamat 127.x.x.x tidak digunakan untuk mengalami suatu *host* atau *network*, alamat ini digunakan sebagai fasilitas *utility*. Contohnya alamat 127.0.0.1 digunakan untuk memeriksa koneksi ke diri sendiri, dengan menggunakan perintah ping 127.0.0.1.

Secara administrasi alamat IP dibagi menjadi berikut ini.

- Alamat IP Publik, alamat IP yang biasa digunakan pada jalur publik (internet). Penggunaan alamat IP publik harus melalui proses registrasi ke suatu organisasi yang menangani masalah penggunaan IP agar tidak terdapat *host* yang memiliki alamat IP yang sama.
- Alamat IP Privat, alamat IP yang digunakan pada jaringan lokal. Penggunaannya tidak memerlukan proses registrasi. Alamat-alamat IP yang tergolong ke dalam IP privat dapat terlihat pada Gambar 1.4 berikut:

| | | | | |
|-----------|-----|---------|-------|-------|
| Kelas A → | 10 | 1-255 | 1-255 | 1-255 |
| Kelas B → | 172 | 16 - 31 | 1-255 | 1-255 |
| Kelas C → | 192 | 168 | 1-255 | 1-255 |

Gambar 1.4
IP Privat

Alamat-alamat yang termasuk dalam kelas A, B, dan C biasa digunakan untuk mengalami secara eksplisit suatu *host* sehingga penggunaannya perlu diatur oleh *subnet mask*. Masing-masing kelas memiliki *subnet mask default*, sebagai berikut.

- Kelas A menggunakan *subnet mask default*: 255.0.0.0
- Kelas B menggunakan *subnet mask default*: 255.255.0.0
- Kelas C menggunakan *subnet mask default*: 255.255.255.0

Alamat IP yang termasuk dalam kelas D digunakan untuk sistem pengalamatan secara *multicast* (alamat kelompok), sedangkan alamat-alamat IP yang termasuk dalam kelas E digunakan untuk keperluan perangkat-perangkat militer dan kebutuhan riset.

Berdasarkan korelasi AND antara nilai *subnet mask* dengan suatu alamat IP dapat ditentukan alamat *network* dari suatu jalur.

$$\text{Network Address} = \text{IPAddress AND Subnet mask}$$

Contoh 1:

$$\begin{aligned} \text{IP Address} &= 192.168.10.5 : 11000000.10101000.00001010.00000101 \\ \text{Subnet Mask} &= 255.255.255.0 : 11111111.11111111.11111111.00000000 \\ \text{Network Add} &= 192.168.10.0 : 11000000.10101000.00001010.00000000 \end{aligned} \text{ AND}$$

Contoh 2:

$$\begin{aligned} \text{IP Address} &= 172.16.10.5 : 10101100.00010000.00001010.00000101 \\ \text{Subnet Mask} &= 255.255.255.0 : 11111111.11111111.00000000.00000000 \\ \text{Network Add} &= 172.16.0.0 : 10101100.00010000.00000000.00000000 \end{aligned} \text{ AND}$$

Contoh 3:

Sebuah *host* yang terpasang alamat IP = 172.16.15.1 dan *subnetmask* = 255.255.0.0 dapat disimpulkan bahwa *host* tersebut berada di *network* 172.16.0.0.

| | Desimal | Biner | | | |
|-----------------|-------------|----------|----------|----------|----------|
| IP Address | 172.16.15.1 | 10101100 | 00010000 | 00001111 | 00000001 |
| Subnet Mask | 255.255.0.0 | 11111111 | 11111111 | 00000000 | 00000000 |
| Network Address | 172.16.0.0 | 10101100 | 00010000 | 00000000 | 00000000 |

⏟
⏟
 Bagian Network Bagian Host

Suatu alamat IP dikatakan sebagai ***network address*** **JIKA** bagian *host*-nya bernilai **0 semua** (perhatikan tiga contoh yang telah dibahas sebelumnya). Sebaliknya, **JIKA** bagian *host* bernilai **1 semua** dikenal sebagai ***broadcast address***. *Broadcast address* digunakan untuk mengirimkan trafik ke seluruh *host*.

Broadcast address terdiri atas dua jenis.

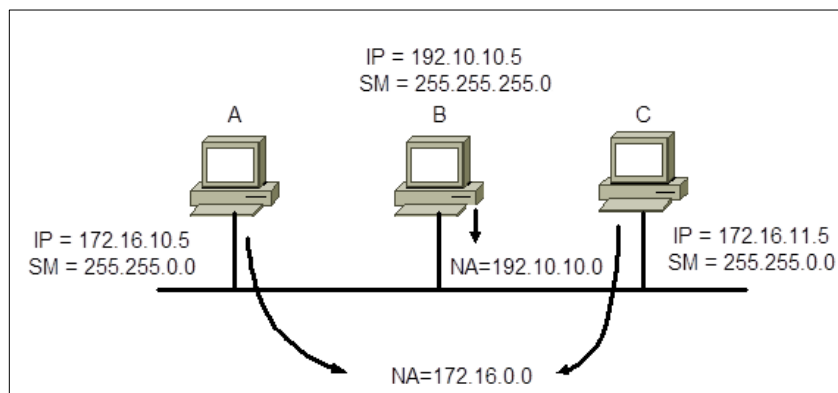
- ***Local Broadcast***, pengiriman yang dilakukan ke seluruh *host* yang terdapat di *subnet* yang sama dengan *host* pengirim. *Local broadcast* tidak bisa melewati *router*. Alamat *local broadcast* adalah 255.255.255.255

- **Directed Broadcast**, pengiriman yang dilakukan ke seluruh *host* yang terdapat pada *subnet* tertentu. *Directed broadcast* dapat melewati *router*. Alamat *directed broadcast* memiliki ciri bahwa seluruh bit yang dimiliki oleh bagian *host* selalu bernilai 1 semua, contoh 172.16.255.255

Jadi dalam 1 blok alamat IP terdiri atas 3 komponen sebagai berikut.

- 1 *Network address* (misal: 172.16.0.0)
- 1 *Broadcast address* (misal: 172.16.255.255)
- 1 blok alamat *host* (*range host address*), (misal: 172.16.0.1 s/d 172.16.255.254)

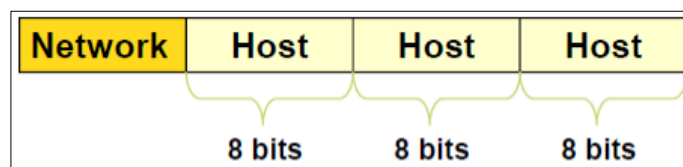
Dua atau beberapa *host* dapat saling berkomunikasi secara langsung jika memiliki *host address* yang berbeda dan berada dalam satu *network address* yang sama. Seperti yang terlihat pada Gambar 1.5, *host* A dapat berkomunikasi hanya dengan *host* C karena membentuk *network address* yang sama, yakni 172.16.0.0. Sedangkan *host* B tidak dapat berkomunikasi dengan *host* A dan *host* C karena secara logik berada pada jalur yang berbeda, yakni 192.10.10.0



Gambar 1.5
Network Address

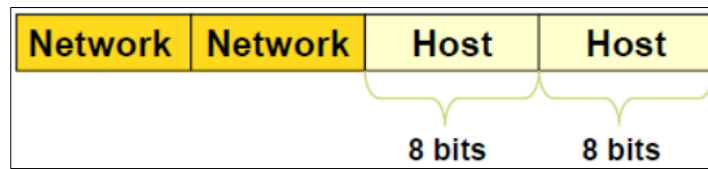
Berdasarkan *subnet mask default*, dalam satu *network address* kelas A terdiri atas:

$$2^{24} - 2 = 16.777.216 \text{ host address}$$



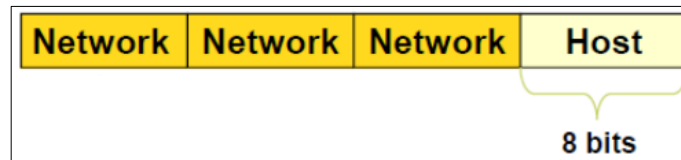
dalam satu *network address* kelas B terdiri atas:

$$2^{16} - 2 = 65.534 \text{ host address}$$



dalam satu *network address* kelas C terdiri atas:

$$2^8 - 2 = 254 \text{ host address}$$



Untuk menghitung jumlah *host address* pada suatu *network address* dapat dihitung dengan menggunakan rumus berikut:

$$\text{Jumlah Host} = 2^{\text{banyaknya bit 0 di subnet mask}} - 2$$

B. SUBNETTING

Subnetting merupakan suatu teknik yang digunakan untuk mengubah nilai *subnet mask* yang bertujuan untuk memperbanyak jumlah *sub network* dan memperkecil jumlah *host/network* dengan memperbanyak bit 1 pada *subnet mask*.

Dalam merancang suatu jaringan IP terdapat beberapa hal yang perlu dipertimbangkan sebelum Anda memberikan alamat terhadap suatu jaringan dan *host*, antara lain sebagai berikut.

- Jumlah **network ID** yang diperlukan, berikut ini.
 - Satu untuk setiap *subnet*.
 - Satu untuk setiap koneksi jaringan WAN.
- Jumlah **host ID** yang diperlukan dalam tiap *subnet*, berikut ini.
 - Satu untuk setiap *host*.
 - Satu untuk setiap *interface* yang terdapat pada *router*.
- Berdasarkan kebutuhan di atas, buat:
 - satu *subnet mask* untuk seluruh jaringan;
 - *subnet ID* yang bersifat unik untuk setiap *segment* secara fisik;
 - kisaran dari *host ID* untuk setiap *subnet*.

Berikut contoh penerapan *subnetting*.

Contoh 1:

Anda ditugaskan untuk merancang sistem pengalamatan jaringan yang terdapat di kantor cabang yang terdiri atas 5 bagian dan masing-masing bagian terdapat 20 pengguna jaringan. Pengelola kantor pusat memberi satu alamat *network* = 201.222.5.0 dengan *subnet mask* 255.255.255.0. Masing-masing bagian harus memiliki *network address* yang berbeda. Tentukan *subnet mask* yang harus digunakan di kantor cabang dan tentukan *subnet address* yang terbentuk!

Secara singkat informasi yang kita peroleh pada kasus tersebut sebagai berikut.

- *Network Address* = 201.222.5.0
- *Default Subnet Mask* = 255.255.255.0
- Jumlah minimal *subnet* yang harus dibentuk = 5 *Subnet*
- Jumlah minimal *host* pada tiap-tiap *Subnet* = 20 *Host*

Tahapan yang perlu dilakukan untuk menyelesaikan kasus tersebut sebagai berikut.

1. Tentukan Nilai *Subnet Mask* yang akan Digunakan

Untuk menentukan nilai *subnet mask* yang digunakan, dapat dilakukan dengan langkah berikut.

- a. Kebutuhan jumlah *subnet* yang akan dibentuk minimal 5 *subnet*, sehingga Anda perlu memodifikasi nilai subnet mask yang semula bernilai 255.255.255.0
- b. Ubah *subnet mask* ke dalam bentuk biner.

255.255.255.0 → 11111111.11111111.11111111.00000000

- c. Untuk memenuhi kebutuhan sejumlah *subnet* yang harus dibentuk, Anda dapat mengubah sejumlah bit 0 menjadi bit 1.
- d. Banyaknya bit 0 yang Anda ubah menjadi bit 1 dapat ditentukan dengan menggunakan rumus berikut:

$$\text{Banyaknya subnet terbentuk} \geq 2^x - 2$$

Di mana:

x: banyaknya bit 0 yang diubah menjadi bit 1

- e. Berdasarkan rumus di atas, kita bisa tentukan banyaknya bit 0 yang harus diubah agar dapat memenuhi kebutuhan 5 *subnet*.

$$2^x - 2 \geq 5$$

$$2^x \geq 5 + 2$$

Jika x kita ganti menjadi 3 maka akan menghasilkan

$$8 \geq 7$$

Sehingga sudah memenuhi syarat dan dapat kita simpulkan bahwa banyaknya bit 0 yang diubah menjadi bit 1 sebanyak 3 bit.

- f. Sehingga *subnet mask* berubah menjadi:

11111111. 11111111. 11111111.11100000

- g. Konversikan ke desimal menjadi:

255.255.255.224

- h. Dengan menggunakan *subnet mask*: 255.255.255.0 maka akan terbentuk:

- *subnet* sebanyak : $2^3 - 2 = 6$ *subnet*;
- masing-masing *subnet* terdiri atas $2^5 - 2 = 30$ *host*.

Jumlah *host* dalam 1 *subnet* dapat dihitung dengan menggunakan rumus berikut:

$$\text{Banyaknya } \mathbf{host} = 2^y - 2$$

di mana:

y: banyaknya bit 0 pada *subnet mask*

- i. Dari hasil perhitungan di atas sudah memenuhi persyaratan jumlah *subnet* yang harus dibentuk minimal 5 dan masing-masing *subnet* dapat menampung minimal 20 *host*. Sehingga pada tahap 1 ini kita bisa tentukan *subnet mask* yang akan digunakan adalah:

255.255.255.224

2. Tentukan *Subnet Address* yang Terbentuk

- a. Perhatikan nilai *subnet mask* yang telah diperoleh.

255.255.255.224

- b. Perhatikan octet ke-4 pada kasus ini bernilai 224.
c. Lakukan pengurangan terhadap 256 (nilai yang berasal dari 2 pangkat banyaknya bit dalam 1 octet (8 bit)).

$$256 - 224 = 32$$

- d. Hasil dari pengurangan di atas mengindikasikan bahwa alamat *subnet* selalu kelipatan 32.
- e. Jadi *subnet* yang terbentuk mulai:
 - **subnet 1 : 201.222.5.0** → tidak digunakan (*major network*)
 - **subnet 2 : 201.222.5.32**
 - **subnet 3 : 201.222.5.64**
 - **subnet 4 : 201.222.5.96**
 - **subnet 5 : 201.222.5.128**
 - **subnet 6 : 201.222.5.160**
 - **subnet 7 : 201.222.5.192**
 - **subnet 8 : 201.222.5.224** → tidak bisa digunakan (224 nilai maksimal).

Contoh 2:

Diketahui suatu *host* memiliki alamat IP = 192.16.2.125 dan *subnet mask* 255.255.255.248 (kelas C di *subnetting* 5 bit). Tentukan *subnet address*, *directed broadcast address*, dan *range host address* dari *host* tersebut?

Untuk menjawab soal tersebut, lakukan langkah-langkah berikut.

- Menentukan *subnet address*, hal tersebut dilakukan dengan melakukan operasi AND antara *IP address* dan *subnet mask*.

| | | | | | |
|--------------|---|-----------------|-----------------|-----------------|-----------------|
| IP (desimal) | = | 192 | 16 | 2 | 125 |
| SM (desimal) | = | 255 | 255 | 255 | 248 |
| IP (biner) | = | 1 1 0 0 0 0 0 0 | 0 0 0 1 0 0 0 0 | 0 0 0 0 0 0 1 0 | 0 1 1 1 1 0 1 |
| SM (biner) | = | 1 1 1 1 1 1 1 1 | 1 1 1 1 1 1 1 1 | 1 1 1 1 1 1 1 1 | 1 1 1 1 1 0 0 0 |
| AND | | | | | |
| NA (biner) | = | 1 1 0 0 0 0 0 0 | 0 0 0 1 0 0 0 0 | 0 0 0 0 0 0 1 0 | 0 1 1 1 1 0 0 0 |
| NA (desimal) | = | 192 | 16 | 2 | 120 |

Network address yang dihasilkan adalah 192.16.2.120

- Menentukan *broadcast address*, hal tersebut dilakukan dengan cara

| | | | | | |
|--|---|-----------------|-----------------|-----------------|-----------------|
| IP (desimal) | = | 192 | 16 | 2 | 125 |
| SM (desimal) | = | 255 | 255 | 255 | 248 |
| IP (biner) | = | 1 1 0 0 0 0 0 0 | 0 0 0 1 0 0 0 0 | 0 0 0 0 0 0 1 0 | 0 1 1 1 1 1 0 1 |
| SM (biner) | = | 1 1 1 1 1 1 1 1 | 1 1 1 1 1 1 1 1 | 1 1 1 1 1 1 1 1 | 1 1 1 1 1 0 0 0 |
| nilai IP pada bagian host diubah 1 semua | | | | | |
| BA (biner) | = | 1 1 0 0 0 0 0 0 | 0 0 0 1 0 0 0 0 | 0 0 0 0 0 0 1 0 | 0 1 1 1 1 1 1 1 |
| BA (desimal) | = | 192 | 16 | 2 | 127 |

Broadcast address merupakan alamat IP di mana bagian *host* nya bernilai 1 semua. Bagian *host* pada kasus ini adalah 3 bit paling akhir. Sehingga *Broadcast address* yang terbentuk adalah: 192.168.2.127

- Menentukan *range host address*, merupakan alamat yang berada di antara *network address* dan *broadcast address*.

Network Address = 192.168.2.120

Broadcast Address = 192.168.2.127

Range host address = 192.168.2.121 s/d 192.168.2.126

Contoh 3:

Diketahui suatu *host* memiliki alamat IP = 172.16.121.125/21 (IP 172.16.121.125 dengan *subnet mask* 255.255.248.0). Tentukan *subnet address*, *directed broadcast address*, dan *range host address* dari *host* tersebut?

Untuk menjawab soal tersebut, lakukan langkah-langkah berikut:

- Menentukan *subnet address*, hal tersebut dilakukan dengan melakukan operasi AND antara *IP address* dan *subnet mask*.

| | | | | | |
|--------------|---|-----------------|-----------------|-----------------|-----------------|
| IP (desimal) | = | 172 | 16 | 121 | 125 |
| SM (desimal) | = | 255 | 255 | 248 | 0 |
| IP (biner) | = | 1 0 1 0 1 1 0 0 | 0 0 0 1 0 0 0 0 | 0 1 1 1 1 0 0 1 | 0 1 1 1 1 0 1 |
| SM (biner) | = | 1 1 1 1 1 1 1 1 | 1 1 1 1 1 1 1 1 | 1 1 1 1 1 0 0 0 | 0 0 0 0 0 0 0 0 |
| AND | | | | | |
| NA (biner) | = | 1 0 1 0 1 1 0 0 | 0 0 0 1 0 0 0 0 | 0 1 1 1 1 0 0 0 | 0 0 0 0 0 0 0 0 |
| NA (desimal) | = | 172 | 16 | 120 | 0 |

Network address yang dihasilkan adalah 172.16.120.0

- Menentukan *broadcast address*, hal tersebut dilakukan dengan cara

| | | | | | |
|--|---|-----------------|-----------------|-----------------|-----------------|
| IP (desimal) | = | 172 | 16 | 121 | 125 |
| SM (desimal) | = | 255 | 255 | 248 | 0 |
| IP (biner) | = | 1 0 1 0 1 1 0 0 | 0 0 0 1 0 0 0 0 | 0 1 1 1 1 0 0 1 | 0 1 1 1 1 0 1 |
| SM (biner) | = | 1 1 1 1 1 1 1 1 | 1 1 1 1 1 1 1 1 | 1 1 1 1 1 0 0 0 | 0 0 0 0 0 0 0 0 |
| nilai IP pada bagian host diubah 1 semua | | | | | |
| BA (biner) | = | 1 0 1 0 1 1 0 0 | 0 0 0 1 0 0 0 0 | 0 1 1 1 1 1 1 1 | 1 1 1 1 1 1 1 1 |
| BA (desimal) | = | 172 | 16 | 127 | 255 |

Broadcast address merupakan alamat IP di mana bagian *host* nya bernilai 1 semua. Bagian *host* pada kasus ini adalah 11 bit paling akhir. Sehingga *Broadcast address* yang terbentuk adalah: 172.16.127.255

- Menentukan *range host address*, merupakan alamat yang berada di antara *network address*, dan *broadcast address*.

Network Address = 172.16.120.0

Broadcast Address = 172.16.127.255

Range host address = 172.16.120.1 s/d 172.16.127.254

C. SISTEM PENGALAMATAN IPV6

Perkembangan internet yang sangat besar menyebabkan penggunaan alamat IPv4 sudah tidak dapat mencukupi kebutuhan pengguna. IETF (*Internet Engineering Task Force*) memperkenalkan sistem pengalamatan *IP address next generation* (IPng) atau IPv6.

Bilangan pembentuk IPv6 sebesar 128-bit. Sistem bilangan yang digunakan IPv6 adalah hexadecimal, dibagi dalam 8 bagian yang terdiri atas 16 bit. 16-bit tersebut membentuk 4 digit angka hexadesimal.

1. Format Penulisan IPv6

Penulisan alamat IPv6 dapat dilakukan dengan beberapa cara.

- *Format Preferred*, merupakan cara formal, yaitu menggunakan 8 segmen bilangan heksadesimal yang masing-masing dipisahkan oleh *colon* (titik dua vertikal) atau symbol “:”.

Contoh:

2000:1234:0000:0000:ABCD:1234:1234:0001

FE00:0000:0000:6789:0000:0000:0000:0001

- *Format Compressed*, merupakan cara penulisan alamat IPv6 yang dikompres, umumnya penulisan ini digunakan untuk alamat IPv6 yang beberapa segmennya menggunakan sejumlah bilangan 0. **Kompresi terhadap sederetan segmen angka 0 pada suatu alamat IPv6 hanya boleh dilakukan satu kali, tidak boleh lebih.**

Contoh 1:

2000:1234:0000:0000:ABCD:1234:1234:0001

menjadi

2000:1234:0:0:ABCD:1234:1234:1

atau

2000:1234::ABCD:1234:1234:1

Contoh 2:

FE00:0000:0000:6789:0000:0000:0000:0001

menjadi

FE00:0:0:6789:0:0:0:1

atau

FE00::6789:0:0:0:1

atau

FE00:0:0:6789::1

Contoh 3:

Berikut **contoh penulisan yang salah** dari alamat IPv6

FE00:0000:0000:6789:0000:0000:0000:0001

menjadi

FE00::6789::1

Penulisan alamat IPv6 di atas **tidak diperbolehkan** karena mengandung “ :: “ lebih dari 1 kali.

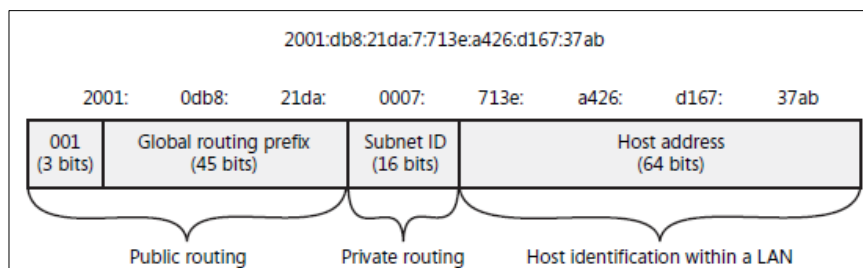
2. Jenis Alamat IPv6

Jenis pengalamatan IPv6 terdiri atas berikut ini.

- 1) Alamat *unicast* merupakan jenis IP address yang digunakan untuk mengidentifikasi suatu *host*. Alamat jenis ini digunakan untuk transmisi paket secara *unicast* yakni paket dikirimkan hanya untuk diterima oleh satu *host*. Secara umum, *unicast address* pada IPv6 berfungsi sama dengan *unicast address* pada IPv4.

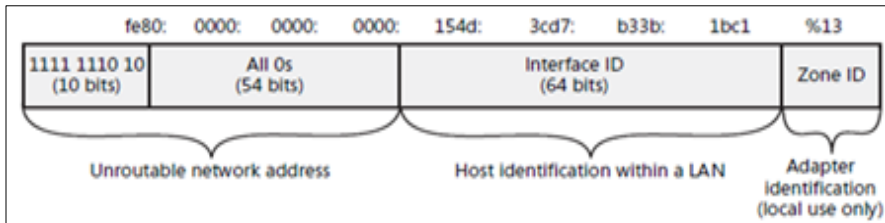
Alamat *unicast* dibagi menjadi beberapa jenis:

- a) Alamat *unicast global* merupakan alamat IP publik pada IPv4. *Global unicast address* memiliki ciri bit-bit awal bernilai **001**. *Prefix* yang digunakan oleh alamat ini adalah 2000::/3.



Gambar 1.6
IPv6 Global Address

- (a) 48 bit pertama dari alamat IPv6 *Global* mewakili bagian topologi publik dari alamat tersebut, yang mewakili kumpulan ISP besar dan kecil di Internet IPv6 dan yang dikontrol oleh ISP ini melalui penugasan oleh IANA. Struktur dari 48 bit tersebut dapat dirinci sebagai berikut:
- 3 bit awal (001) sebagai penanda bahwa IPv6 tersebut merupakan *IPv6 global address*,
 - 13 bit berikutnya (TLA ID - *Top-Level Aggregation Identifier*) merupakan level tertinggi dalam hierarki routing. TLA ID diatur oleh *Internet Assigned Name Authority* (IANA), yang mengalokasikannya ke dalam daftar *Internet registry*, yang kemudian mengalokasikan sebuah TLA ID ke suatu ISP global,
 - 8 bit (resevasi), diresevasikan untuk kebutuhan teknologi di masa yang akan datang,
 - 24 bit (NLA ID - *Next Level Aggregation Identifier*), merupakan tanda pengenalan *site customer* tertentu.
- (b) 16 bit berikutnya adalah *subnet ID* (*Site Level Aggregation Identifier* (SLA ID)). Organisasi Anda dapat menggunakan bagian ini untuk menentukan hingga 65.536 *subnet* unik untuk tujuan *routing* di dalam situs organisasi Anda. 16 bit ini mewakili bagian topologi situs dari alamat tersebut, yang dikontrol oleh organisasi Anda.
- (c) 64 bit terakhir adalah *Interface ID* unik dalam setiap *subnet*. *Interface ID* ini setara dengan *host ID* pada IPv4.
- b) Alamat *unicast link-local* merupakan jenis alamat yang mengizinkan suatu *host* yang mengaktifkan IPv6 untuk dapat saling berkomunikasi dengan *host* lainnya yang berada dalam satu *subnet*, alamat ini berfungsi sebagai *neighbor discovery*. Setiap *host* yang mengaktifkan IPv6 akan terpasang secara otomatis *IPv6 link local address*. Alamat ini mirip dengan APIPA (*Automatic Private Internet Protocol Addressing*) pada IPv4. *IPv6 link-local address* memiliki ciri 10 bit awal bernilai **1111 1110 10**. Prefix yang digunakan oleh *unicast link-local* adalah **FE80::/10** dan 64-bit *interface identifier*.

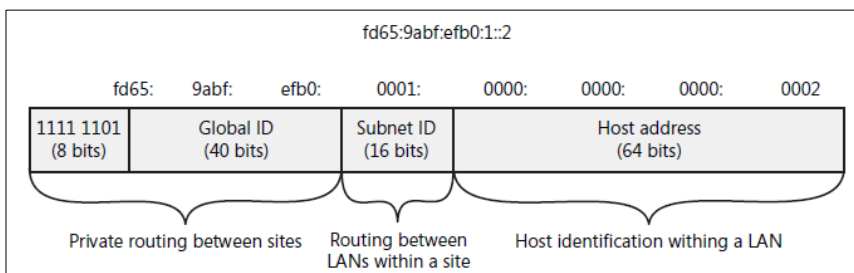


Gambar 1.7
IPv6 Link Local Address

- c) Alamat *unicast unique local* mirip alamat privat pada IPv4. Alamat ini dapat dirutekan antar *subnet* di jaringan pribadi, tetapi tidak dapat dirutekan di jaringan internet atau publik.

Struktur ULA (*unique local address*) sebagai berikut.

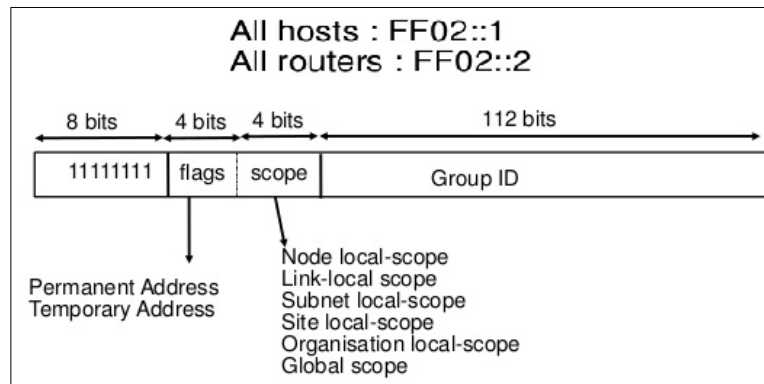
- 7 bit pertama dari alamat selalu bernilai **1111 110** (biner), menunjukkan alamat lokal. Ini berarti prefiks alamatnya adalah **fd00::/8** dan **fc00::/8**.
- 40 bit berikutnya mewakili ID global dan merupakan nilai yang diidentifikasi secara acak situs tertentu dalam organisasi Anda.
- 16 bit berikutnya mewakili ID *subnet* dan dapat digunakan untuk pengelompokan jaringan internal situs Anda untuk tujuan *routing*.
- 64 bit terakhir adalah ID *interface* unik dalam setiap *subnet*.



Gambar 1.8
IPv6 Unique Local Address

- d) Alamat *unicast loopback* merupakan alamat yang digunakan untuk mekanisme *interprocess communication* (IPC) pada suatu *host*. Dalam IPv4 alamat *loopback* adalah 127.0.0.1. Sedangkan pada IPv6 adalah 0:0:0:0:0:0:0:1 atau ::1. Alamat ini hanya dapat diberikan pada *virtual interface*.

- 2) Alamat *multicast* digunakan untuk mengidentifikasi sekumpulan *host*. Alamat *multicast* IPv6 sama seperti alamat *multicast* pada IPv4. Paket yang dikirim ke alamat *multicast* akan diterima oleh semua *host* yang menggunakan alamat tersebut. Alamat *multicast* IPv6 memiliki ciri **FF00::/8**. Alamat *multicast* adalah FF00:: sampai FF0F::.



Gambar 1.9
IPv6 Multicast Address

- 3) Alamat *Anycast*, merupakan alamat yang digunakan untuk penyampaian paket ke anggota terdekat dari suatu grup (*one-to-one-of-many*). Alamat *anycast* menyampaikan paket kepada salah satu dari banyak penerima. Alamat *anycast* pada IPv6 mirip dengan alamat *anycast* dalam IPv4. Alamat *anycast* pada IPv6 diimplementasikan dengan cara yang lebih efisien dibandingkan dengan IPv4. IPv6 menggunakan alamat *anycast* untuk mengidentifikasi beberapa *interface* yang berbeda. Alamat *anycast* tidak mempunyai alokasi khusus, sebab jika beberapa *node/interface* diberikan *prefix* yang sama maka alamat tersebut sudah merupakan alamat *anycast*.



Latihan

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

- 1) Tentukan *network address*, *broadcast address*, dan *range host address* dari alamat berikut:
- a. 192.168.10.100/26
 - b. 172.16.45.40/21
 - c. 10.18.134.40/19

- 2) Sederhanakan penulisan IPv6 berikut:
 - a. 2001:0000:0000:1235:0000:0000:0000:0001
 - b. 0000:0000:0000:0000:0000:0000:0000:0001
 - c. 000A: 0000:0000:1235:AB00:7000:00AB:0001

Petunjuk Jawaban Latihan

- 1) Anda harus mengingat kembali tentang cara melakukan perhitungan *subnetting* dan format penulisan IP.
Lakukan penghitungan dengan menggunakan kaidah yang telah dijelaskan di atas.
Lakukan pemeriksaan kebenaran jawaban Anda dengan menggunakan *software* IP-Kalkulator yang tersedia secara daring, unduh ataupun aplikasi pada *PlayStore*.
Misal:
<http://jodies.de/ipcalc> atau
<https://www.calculator.net/ip-subnet-calculator.html>
- 2) Ingat kaidah penghapusan nilai 0000 secara rinci.



Rangkuman

Pengalamatan IP terbagi menjadi 2, yaitu: IPv4 dan IPv6. Perbedaan antara IPv4 dan IPv6, antara lain:

1. IP Versi 4 memiliki panjang 32 bit, sedangkan untuk IP Versi 6 memiliki panjang 128 bit.
2. IPv4 mendukung representasi alamat menggunakan *subnet mask*, sedangkan IPv6 tidak mendukung *subnet mask*.
3. IPv4 menggunakan *dotted-decimal format*, sedangkan IPv6 menggunakan *colon-hexadecimal format*.



Tes Formatif 2

Pilihlah satu jawaban yang paling tepat!

- 1) Berikut ini merupakan alamat IP Privat, *kecuali*
 - A. 192.168.10.5
 - B. 172.16.10.5
 - C. 10.10.31.5
 - D. 192.167.10.5

- 2) Alamat *network* dari host yang memiliki IP:171.168.100.20 dengan menggunakan *subnet mask default* adalah
 - A. 171.168.100.0
 - B. 171.168.0.0
 - C. 171.0.0.0
 - D. 171.168.80.0

- 3) Jumlah *host* yang dapat digunakan pada alamat *network* 172.16.0.0/16 adalah
 - A. 254
 - B. 65534
 - C. 1024
 - D. 65536

- 4) Jumlah *subnet* yang terbentuk pada alamat *network* 172.16.0.0/20 adalah
 - A. 14
 - B. 240
 - C. 30
 - D. 6

- 5) Berikut ini merupakan alamat yang termasuk pada alamat *unique local address*, kecuali
 - A. FD01:0:0:0:1200::5
 - B. FD00:0001:1234:1010::0002:4c
 - C. 2000:0001:abcd:abcd:1234::1
 - D. FCE1::1

- 6) *Global address* yang benar adalah
 - A. FD01:0:0:0:1200::5
 - B. 2000:100:1:1234:1010:12:0:0002:4c
 - C. 2000:0001:abcd:abcd:1234::1
 - D. FCE1::1

- 7) Alamat *link local* yang benar adalah
 - A. FE80:1234:1234:1234:a:b:c:d
 - B. FE70:1234:1234:1234:a:b:c:d
 - C. FF80:1234:1234:1234:a:b:c:d
 - D. FE60:1234:1234:1234:a:b:c:d

- 8) Alamat *network* dari suatu *host* yang memiliki alamat 192.168.100.75/28 adalah
- A. 192.168.100.32
 - B. 192.168.100.48
 - C. 192.168.100.0
 - D. 192.168.100.64
- 9) Alamat *host* dari suatu alamat *network* 172.168.96.0/28 adalah
- A. 172.16.96.1 s/d 172.16.96.254
 - B. 172.16.96.1 s/d 172.16.112.0
 - C. 172.16.96.1 s/d 172.16.111.254
 - D. 172.16.96.1 s/d 172.16.111.255
- 10) *Subnet mask* yang digunakan jika Anda akan membangun minimal 12 *subnet* yang berisi 10 *host* adalah
- A. 192.168.10.32/28
 - B. 192.168.10.32/27
 - C. 192.168.10.32/26
 - D. 192.168.10.32/29

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 2 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 2.



Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan modul selanjutnya. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 2, terutama bagian yang belum dikuasai.

Kunci Jawaban Tes Formatif

Tes Formatif 1

- 1) B
- 2) D
- 3) C
- 4) B
- 5) D
- 6) A
- 7) A
- 8) A
- 9) A
- 10) D

Tes Formatif 2

- 1) D
- 2) B
- 3) B
- 4) A
- 5) C
- 6) C
- 7) A
- 8) D
- 9) C
- 10) A

Daftar Pustaka

Academy, C. N. (2014). *Connecting networks companion guide*. Cisco Press.

Froom, R., Sivasubramanian, B., & Frahim, E. (2010). *Implementing cisco IP switched network (SWITCH) foundation learning guide*. Cisco Press.

Odom, W. (2020). *CCNA 200-301 official cert guide, Vol 1*. Cisco Press.