**BAB II**

**DASAR TEORI**

Bab II akan diterangkan mengenai beberapa teori yang menjadi acuan dalam tugas akhir ini diantaranya alamat IP (*Internet Protocol*), NAT(*Network Address Translation*) dan DHCP (*Dynamic Host Configuration Protokol*).

**2.1 Alamat IP**

 Alamat IP (*IP Address*) merupakan deretan angka biner antara 32-bit sampai 128-bit yang dipakai sebagai alamat identifikasi untuk tiap komputer dalam sebuah jaringan. Saat ini ada dua tata cara pemberian alamat IP yaitu dengan menggunakan IP Address versi 4 panjang 32-bit dan yang terbaru adalah IP Address versi 6 panjang 128-bit. Pada tugas akhir ini menggunakan format alamat IP versi 4 dengan panjang 32-bit format ini dibagi menjadi 4 kelompok, masing – masing kelompok terdiri dari 8-bit yang dipisahkan dengan tanda titik (dot). Format ini dibagi menjadi 2 bagian identifikasi sebagai berikut :

1. Bagian identifikasi identitas jaringan (NetID), menunjukkan identitas kelompok jaringan yang terhubung terdiri dari banyak komputer host.
2. Bagian identifikasi identitas Host (HostID), memberikan tanda pengenal yang unik pada setiap komputer host yang terhubung pada sebuah kelompok jaringan.

Pada terminologi TCP/IP satu NetID terdiri dari sekelompok host yang dapat berkomunikasi secara langsung tanpa harus menggunakan router. Komputer host harus memiliki paling tidak satu alamat IP. Host yang memiliki identitas jaringan yang berbeda untuk berkomunikasi dengan komputer host lainnya harus melewati sebuah proses routing. Jaringan diatasnya adalah jaringan *Internetwork* yaitu sebuah struktur jaringan yang terdiri dari beberapa NetID, digunakan untuk menggabungkan dan mengatur komunikasi antar beberapa jaringan yang berbeda. Seperti halnya host, anggota dari internetwork harus memiliki identitas yang unik pula.

**2.1.1 Kelas Alamat IP**

 Untuk keperluan pengelolaan pengalokasian alamat jaringan, alamat host, jumlah jaringan dan jumlah host alamat IP dibagi menjadi lima kelas, yang mana masing – masing kelas akan mempunyai fungsi bit yang berbeda – beda. Alamat – alamat kelas yang digunakan secara umum sebagai berikut .

1. Alamat Kelas A

Alamat IP kelas A mempunyai 8-bit yang dialokasikan sebagai alamat jaringan atau NetID dan sisanya ada 24-bit untuk keperluan alokasi alamat HostID. Bit yang memiliki nilai paling tinggi MSB (*Most Signification Bit*) berada di posisi paling kiri dengan nilai biner yang selalu 0 dan sisanya adalah NetID, 24-bit selanjutnya adalah HostID yang merupakan LSB (*Least Signification Bit*) sehingga alamat unik alamat IP yang bisa dialokasikan adalah sebanyak 224 = 16.777.214 host untuk setiap jaringan. .

1. Alamat Kelas B

Alamat IP kelas B mempunyai 16-bit yang dapat dialokasikan sebagai alamat jaringan atau NetID. Bit yang memiliki nilai paling tinggi MSB (*Most Signification Bit*) berada di posisi paling kiri dengan nilai biner yang selalu 10. Untuk alokasi HostID disediakan sebanyak 16-bit pada posisi LSB (*Least Signification Bit*) sehingga alamat unik alamat IP yang bisa dialokasikan adalah sebanyak 216 = 65532 host untuk setiap jaringan.

1. Alamat Kelas C

Alamat IP kelas C mempunyai 24-bit yang dapat dialokasikan sebagai alamat jaringan atau NetID. Bit yang memiliki nilai paling tinggi MSB LSB (*Least Signification Bit*). Berada diposisi paling kiri dengan nilai biner yang selalu 110. Sedangkan untuk alokasi HostID disediakan sebanyak 8 bit pada posisi LSB (*Least Signification Bit*) sehingga alamat unik alamat IP yang bisa di alokasikan adalah sebanyak 28 = 256 host untuk setiap jaringan.

1. Alamat Kelas D

IP address kelas D digunakan untuk keperluan multicasting. 4 bit pertama IP address kelas D selalu diset 1110 sehingga byte pertamanya berkisar antara 224-247, sedangkan bit-bit berikutnya diatur sesuai keperluan multicast group yang menggunakan IP address ini. Dalam multicasting tidak dikenal istilah network ID dan host ID.

1. Alamat Kelas E

IP address kelas E tidak diperuntukkan untuk keperluan umum. 4 bit pertama IP address kelas ini diset 1111 sehingga byte pertamanya berkisar antara 248-255.

Selain dari alamat IP kelas diatas, ada beberapa alamat IP yang nilainya telah dikhususkan sehingga tidak boleh dipakai.

1. Alamat 0.0.0.0 tidak boleh digunakan untuk menunjukkan host atau komputer.
2. Alamat 255. 255. 255. 255 tidak boleh digunakan untuk alamat host karena alamat ini menunjuk pada alamat broadcast pada jaringan.
3. Alamat 127.0.0.1 adalah alamat khusus yang digunakan untuk local host(*loopback*) sehingga tidak boleh digunakan untuk alamat HostID.
4. Alamat 224.0.0.0 – 239.255.255.255 digunakan untuk teknologi multicasting.
5. Alamat 240.0.0.0 – 247.255.255.255 digunakan untuk keperluan alamat IP dimasa yang akan datang.
6. Nilai bit dalam format alamat IP yang menunjukkan alamat host, tidak boaleh diisi dengan biner 0 semua atau dengan nilai 1 semua. Karena jika bit 0 semua akan secara otomatis akan menunjuk pada alamat NetID dan bila dengan nilai 1 semua maka secara otomatis akan menunjuk pada alamat broadcast.

Dalam pengelolaan alamat IP baik itu untuk alokasi jaringan LAN ataupun jaringan WAN maka alamat IP dibedakan menjadi 2 kategori yaitu alamat IP yang terintergrasi ke internet langsung atau lebih sering disebut IP Public dan alamat IP yang tidak terintergrasi langsung ke internet atau sering disebut IP privat. Dikatakan IP privat karena tidak dapat diakses oleh internet dan dapat digunakan untuk jaringan LAN saja. Ini dimaksudkan untuk membatasi banyak IP yang bisa mengakses langsung ke internet. Range IP private adalah sebgai berikut :

|  |  |
| --- | --- |
| **Kelas** | **Kelompok Private Address** |
| A | 10.0.0.1 – 10.255.255.254 |
| B | 172.16.0.1 – 172.31.255.254 |
| C | 192.168.0.1 – 192.168.255.254 |

 Tabel 2.1 IP Private

**2.1.2. Format Pengalamatan IPv4**

1. Classfull Addressing

Format pengalamatan dengan metode Classfull merupakan pembagian IP address berdasarkan kelas, dimana IP address seperti yang telah dijelaskan sebelumnya dibagi kedalam lima kelas yakni:

* 1. Kelas A
* Nilai 1 bit pertama IP address adalah = 0.
* Menggunakan 8 bit alamat jaringan dan 24 bit bit untuk alamat host.

|  |  |
| --- | --- |
| NNNNNNN | HHHHHHHH. HHHHHHHH. HHHHHHHH. |
| NetID | HostID |

* Mempunyai 126 jaringan ( 0 dan 127 dicadangkan ) dengan 16.777.214 host untuk setiap jaringan.
* Dialokasikan untuk jaringan dengan jumlah host yang besar.
	1. Kelas B
* Nilai 2 bit pertama IP address adalah = 10.
* Menggunakan 16 bit alamat jaringan dan 16 bit alamat untuk host.

|  |  |  |
| --- | --- | --- |
| 10 | NNNNNNN.NNNNNNNN | HHHHHHHH. HHHHHHHH. |
| NetID | HostID |

* Mempunyai 16.384 jaringan dengan 65.532 host untuk setiap jaringan.
* Dialokasikan untuk jaringan besar dan sedang
	1. Kelas C
* Nilai 3 bit pertama IP address adalah = 110.
* Menggunakan 24 bit alamat jaringan dan 8 bit untuk alamat host.

|  |  |  |
| --- | --- | --- |
| 110 | NNNNNNN.NNNNNNNN. NNNNNNNN | HHHHHHHH. |
| NetID | HostID |

* Mempunyai 2.097.152 jaringan dan 254 host untuk setiap jaringan.
* Dialokasikan untuk jaringan dengan jumlah host yang tidak sampai 254.
	1. Kelas D
* Nilai 4 bit pertama IP address adalah = 1110.

|  |  |
| --- | --- |
| 1110 | MMMM.MMMMMMMM. MMMMMMMM. MMMMMMMM. |
| Multicast  |

* Digunakan untuk keperluan multicastting.
	1. Kelas E
* Nilai 4 bit pertama IP address adalah =1111.

|  |  |
| --- | --- |
| 1111 | RRRR.RRRRRRRR. RRRRRRRR. RRRRRRRR.  |
| Research |

* Keals E dicadangkan untuk keperluan eksperimen ( *research*).

2. Classless Addressing

 Sistem ini telah dikembangkan pada awal tahun 1990-an dan resmi pada tahun 1993 di RFCs 1517, 1518, 1519 dan 1520. Metode ini mulai banyak diterapkan ,yakni pengalokasian alamat IP dalam Classless Inter Domain Routing (CIDR). Dalam implementasinya tidak terlepas dari network prefix yaitu sebuah istilah untuk menunjukkan suatu jaringan secara lebih spesifik.

Penulisan NetID dalam implemetasi network prefix menggunakan garis miring ‘/’ lalu diikuti dengan nilai desimal yang menunjukkan panjang network prefix dalam bit.

**2.1.3 Subnet Mask**

 Subnet mask digunakan untuk memanajemen jumlah host. Setiap host dijaringan TCP/IP membutuhkan subnet mask. Secara default subnet mask telah diset jika jaringan tidak dibagi lagi menjadi beberapa sub – sub jaringan. Namun subnet mask tertentu digunakan ketika jaringan dibagi menjadi beberapa subnet. Subnet mask default digunakan di jaringan TCP/IP yang dibagi menjadi subnet – subnet. Subnet mask sendiri merupakan alamat IP 32-bit yang digunakan sebagai berikut.

1. Memisahkan bagian alamat IP untuk membedakan bagian NetID dan HostID.
2. Menyatakan apakah alamat IP host tujuan terletak dijaringan lokal atau jaringan remote.

Seluruh bit yang berkaitan dengan NetID di set ke nilai 1 atau nilai desimal 255, sedangkan seluruh bit yang berkaitan dengan HostID diset ke 0. Berikut adalah tabel dari subnet mask default.

|  |  |  |
| --- | --- | --- |
| **Kelas** | **Subnet Mask dalam biner** | **Subnet Mask dalam desimal** |
| A | 11111111.00000000. 00000000. 00000000 | 255.0.0.0 |
| B | 11111111. 11111111. 00000000. 00000000 | 255.255.0.0 |
| C | 11111111. 11111111. 11111111. 00000000 | 255.255.255.0 |

Tabel 2.2 Subnet maskIP Private

* 1. **Network Address Translation (NAT)**

Keterbatasan alamat IPv.4 merupakan masalah pada jaringan global atau Internet. Untuk memaksimalkan penggunakan alamat IP yang diberikan oleh *Internet Service Provider* (ISP) dapat digunakan *Network Address Translation* atau NAT. NAT membuat jaringan yang menggunakan alamat lokal (*private*), alamat yang tidak boleh ada dalam tabel routing Internet dan dikhususkan untuk jaringan lokal/intranet, dapat berkomunikasi ke Internet dengan jalan meminjam alamat IP Internet yang dialokasikan oleh ISP.

**2.2.1 Dua Tipe NAT**

Dua tipe NAT adalah Static dan Dinamik yang keduanya dapat digunakan secara terpisah maupun bersamaan.

**2.2.2 Statik NAT**

Translasi Static terjadi ketika sebuah alamat lokal (inside) di petakan ke sebuah alamat global/internet (*outside*). Alamat lokal dan global dipetakan satu lawan satu secara Statik.

**2.2.3 Dinamik NAT dengan Pool**

Translasi Dinamik terjadi ketika router NAT diset untuk memahami alamat lokal yang harus ditranslasikan, dan kelompok (*pool*) alamat global yang akan digunakan untuk terhubung ke internet. Proses NAT Dinamik ini dapat memetakan bebarapa kelompok alamat lokal ke beberapa kelompok alamat global.

**2.2.4. NAT Overload**

NAT Overload adalah sebuah metode translasi sejumlah IP lokal/internal ditranslasikan ke satu alamat IP global/inside. Pemakaian bersama satu alamat IP ini disertai dengan *port* *multiplexing* atau disebut juga dengan *Network Address Port Translation*. Metode ini memungkinkan sejumlah ip privat pada jaringan lokal berkomunikasi dengan jaringan global dengan satu alamat publik dan melewati port tertentu. Mekanisme NAT overload dengan membuat Dua-jalur komunikasi untuk paket TCP dan UDP yang berisi kedua sumber alamat IP dan nomor port sumber serta tujuan alamat IP dan nomor port tujuan. Keempat informasi tersebut, dilakukan bersama-sama, membentuk sebuah socket

**2.2.5. Cara kerja NAT**

Network Address Translation atau yang lebih biasa disebut dengan NAT adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP. Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat IP yang terbatas, kebutuhan akan keamanan (security), dan kemudahan serta fleksibilitas dalam administrasi jaringan. Berikut adalah ilustrasi cara kerja NAT yang digunakan untuk mentranslasikan alamat dari dalam privat ke

jaringan ke publik.



Gambar 2.1 Network Address Translasi

* Langkah 1:

Pengguna pada klien C pada inside local membuat koneksi keluar yaitu ke host B.

* Langkah 2:

Perjalanan paket pertama – tama diterima oleh router dari klien C, selanjutnya akan dicocokkan dengan tabel NAT. Tabel NAT berisi alamat translasi dari alamat inside lokal ke inside global. Tabel NAT terbentuk pada saat administrator melakukan konfigurasi NAT pada router untuk melakukan translasi alamat – alamat inside lokal ke alamat inside global.

* Langkah 3:

Router mengganti alamat IP klien C inside local dengan alamat inside global yang telah dipilih dan meneruskan paket data.

* Langkah 4:

Host B menerima paket dan merespon ke node yang menggunakan alamat IP inside global atau alamat publik router.

* Langkah 5:

Ketika router menerima paket dengan alamat IP inside global, router kembali memeriksa tabel NAT dengan alamat IP inside global sebagai

referensi.

* Langkah 6:

Router kemudian mentranslasikan alamat tersebut ke klien C yang menggunakan alamat inside local, dan meneruskan paket data ke klien C.

* 1. **Dynamic Host Configuration Protocol (DHCP)**

Dynamic Host Configuration Protocol (DHCP) adalah protokol yang berbasis arsitektur client/server yang dipakai untuk memudahkan pengalokasian alamat IP dalam satu jaringan. Sebuah jaringan lokal yang tidak menggunakan DHCP harus memberikan alamat IP kepada semua komputer secara manual. Jika DHCP dipasang dijaringan lokal , maka semua komputer yang tersambung dijaringan akan mendapat alamat IP

 secara otomatis dari server DHCP. Jaringan DHCP dimasa kini semakin diminati terutama pada jaringan wireless.

Selain alamat IP, banyak parmeter jaringan yang dapat diberikan oleh DHCP, seperti *default gateway* dan *DNS server.*

Karena DHCP merupakan sebuah protool yang menggunakan konsep client/server, maka dalam DHCP terdapat 2 pihak yang terlibat yaitu DHCP server dan DHCP client.

1. DHCP server merupakan sebuah mesin yang menjalankan layanan yang mengalokasikan alamat IP dan informasi TCP/IP lainya kepada pihak klient yan memintanya.
2. DHCP client merukan mesin klien yang menjalankan perangkat lunak klien DHCP yang memungkinkan mereka untuk dapat berkomunikasi dengan DHCP server.

DHCP klien akan mencoba untuk mendapat alokasi alamat IP dari sebuah DHCP server dalam proses 4 langkah berikut :

1. DHCPDISCOVER : DHCP klien akan meyebarkan request untuk mencari DHCP server yang aktif.
2. DHCPOFFER : setelah DHCP server mendapat request dari DHCP klien maka DHCP server akan menawarkan sebuah alamat kepada DHCP klien.
3. DHCPREQUEST : klien meminta DHCP server untuk menyewakan alamat IP dari salah satu alamat yang tersedia dalam DHCP pool (range) pada DHCP server yang bersangkutan.
4. DHCPPACK : DHCP server akan merespon permintaan dari klient dengan mengirimkan paket acknowledgment. Kemudian DHCP server akan menetapkan sebuah alamat IP beserta konfigurasi TCP/IP lainya kepada klient, lalu memperbaharui database miliknya.

Empat tahap diatas hanya berlaku bagi klien yang belum memiliki alamat IP. Untuk klien yang sebelumnya telah pernah *merequest* alamat kepada DHCP server yang sama hanya akan menempuh sampai pada tahap 3 dan tahap 4 yang dilakukan, yakni tahap pembaruan alamat IP (*address renewal*) .

Berbeda dengan sistem DNS yang terdistribusi, DHCP bersifat standalone sehingga jika dalam sebuah jaringa terdapat beberapa DHCP server maka database alamat IP yang dialokasikan pada DHCP server tidak akan direplikasikan ke DHCP server lainnya. Hal ini dapat menjadi masalah jika konfigurasi antara dua DHCP server tersebut berbenturan, karena protokol IP tidak mengijinkan dua host memiliki alamat yang sama.

* DHCP scope

DHCP scope adalah alamat – alamat IP yang dialokasikan kepada DHCP klien. Ini dikonfigurasikan oleh seorang administrator pada mesin DHCP server. Nilai alamat – alamat IP yang dapat dilaokasikan harus diambil dari DHCP pool yang tersedia yang selanjutnya dialokasikan ke jaringan.

* DHCP lease

DHCP lease adalah batas waktu penyewaan alamat IP yang diberikan kepada DHCP klien oleh dhcp server. Umumnya hal ini dapat dikonfigurasikan sedemikian rupa oleh seorang administrator dengan menggunakan bebrapa utilitas konfigurasi. DHCP lease juga sering disebut sebgai reservation.

* DHCP options

DHCP options adalah tambahan pengaturan alamat IP yang diberikan oleh DHCP ke DHCP klien. Ketika klien meminta alamat IP ke server , dari sisi server akan merespon dengan memberikan alamat IP dan subnet jaringan.DHCP server juga dapat dikonfigurasikan sedemikina rupa agar mmeberikan tambahan informasi kepada klien yang tentunya dapat dilakukan oleh seorang administrator. DHCP options ini dapat diaplikasikan kepada semua klien, DHCP scope tertentu atau kepada sebuah host tertentu dalam jaringan.