

## BAB II

### ANALISIS DAN PERANCANGAN

#### 2.1. IP Addressing

IP atau *Internet Protocol* adalah sederetan angka biner sejumlah 32 bit yang terbagi menjadi 4 kelompok, masing-masing kelompok terdiri atas biner 8 bit yang dipisahkan dengan tanda titik (*dot*). Masing-masing kelompok tersebut disebut *oktet*. IP beroperasi pada lapisan 3 atau lapisan *network* pada sistem OSI (*Open System Interconnection*). *IP Address* bersifat unik, artinya tidak ada peralatan jaringan yang berupa *station*, *host* atau *router* yang memiliki IP yang sama. Tetapi sebuah *host*, *komputer* atau *router* dapat memiliki lebih dari 1 *IP Address*.

Informasi yang terkandung pada sebuah alamat IP yang dimiliki oleh sebuah *host* terbagi dua buah bagian, yakni:

- *Network Identifier / NetID* atau *Network Address* (alamat jaringan) adalah sebuah alamat IP yang digunakan khusus untuk mengidentifikasi alamat jaringan di mana *host* tersebut berada.
- *Host Identifier / Host ID* atau *Host address* (alamat *host*) adalah alamat IP yang digunakan khusus untuk mengidentifikasi alamat *host* tersebut (dapat berupa *workstation*, *server* atau sistem lainnya yang berbasis teknologi TCP/IP) di dalam jaringan. Nilai *host identifier* tidak boleh bernilai 0 atau 255 dan harus

bersifat unik di dalam *network identifier*/segmen jaringan di mana ia berada.

### 2.1.1. Kelas pada Alamat IP

Menurut dokumen RFC791, alamat IP dibagi ke dalam kelas-kelas untuk mengakomodasi kebutuhan jumlah jaringan maupun jumlah *host*. Adapun pembagian kelas tersebut adalah sebagai berikut :

Tabel 2.1 Kelas Alamat IP

Kelas Alamat IP	Oktet pertama		Kebutuhan
	Bentuk Desimal	Bentuk Biner	
Kelas A	0–127	00000000 s/d 01111111	Jumlah jaringan sedikit, dengan jumlah <i>host</i> banyak pada masing-masing jaringan
Kelas B	128–191	10000000 s/d 10111111	Jumlah jaringan sedang dengan jumlah <i>host</i> sedang pada masing-masing jaringan
Kelas C	192–223	11000000 s/d 11011111	Jumlah jaringan banyak dengan jumlah <i>host</i> sedikit pada masing-masing jaringan

Namun ada beberapa alamat yang tidak dipergunakan karena beberapa hal.

Misalnya:

- Alamat dengan *oktet* pertama 0 digunakan untuk menunjuk alamat jaringan.
- Alamat dengan *oktet* pertama bernilai 127 digunakan untuk keperluan *loopback*, yaitu alamat yang digunakan untuk menunjuk dirinya sendiri.

### 2.1.2. *Netmask*

*Netmask* merupakan cara untuk membedakan *network identifier* dari *host identifier* di dalam sebuah alamat IP sebuah jaringan komputer. *Netmask* merupakan sebuah nilai sebesar 32 bit. Adapun penulisan *netmask* diatur sebagai berikut:

- Semua bit yang ditunjukkan agar digunakan oleh *network identifier* diberi nilai 1.
- Semua bit yang ditunjukkan agar digunakan oleh *host identifier* diberi nilai 0.

Berdasarkan dokumen RFC791, maka dengan *netmask* pada masing-masing kelas, maka didapatkan jumlah jaringan maupun jumlah *host* sebagai berikut:

Tabel 2.2 Jumlah jaringan dan *host* pada tiap Kelas Alamat IP

Kelas	Oktet Pertama	Netmask	Jumlah Jaringan	Jumlah Host
A	1 s/d 126	255.0.0.0	126	16.777.214
B	128 s/d 191	255.255.0.0	16.384	65.534
C	192 s/d 223	255.255.255.0	2.097.152	254

Catatan: Pada kelas A, alamat jaringan dengan *oktet* pertama bernilai 0 dan 127 tidak dipergunakan / dicadangkan sehingga jumlah yang seharusnya 128, dikurangi 2 menjadi 126 jaringan.

### 2.1.3. Alamat Publik

Alamat Publik adalah alamat-alamat yang telah ditetapkan oleh InterNIC dan berisi beberapa buah *network identifier* yang telah dijamin unik (artinya, tidak ada dua *network* yang menggunakan alamat yang sama) jika alamat tersebut telah terhubung ke *Internet*.

Ketika beberapa alamat Publik telah ditetapkan, maka beberapa rute / tujuan dapat diprogramkan ke dalam sebuah router sehingga lalu lintas data yang menuju alamat Publik tersebut dapat mencapai lokasi yang dituju. Di *internet*, lalu lintas ke sebuah alamat Publik tujuan dapat dicapai, selama masih terkoneksi dengan *internet*.

### 2.1.4. Alamat Privat

Alamat IP Privat adalah sebuah alamat IP yang berada di dalam ruangan alamat pribadi tidak akan digunakan sebagai sebuah alamat publik.

Alamat ini tidak terhubung dengan alamat IP Publik atau tidak di-*routing*. Alamat IP Privat digunakan untuk membentuk jaringan yang sifatnya lokal, dalam pengertian tidak terhubung ke jaringan publik secara langsung. Ketentuan tentang alamat IP privat diatur dalam dokumen RFC 1918 (*Request for Comments* 1918). Inti isi dokumen tersebut adalah bahwa IANA (*Internet Assigned Numbers Authority*) menyediakan tiga blok alamat IP berikut untuk alamat IP Privat.

Tabel 2.3 Alamat IP Privat

Kelas IP	Rentang Alamat IP privat
A	10.0.0.0 s/d 10.255.255.255
B	172.16.0.0 s/d 172.31.255.255
C	192.168.0.0 s/d 192.168.255.255

## 2.2. Jaringan Komputer

Jaringan komputer merupakan kumpulan komputer, *printer* dan peralatan lainnya (biasa disebut *node*) yang terhubung dalam satu kesatuan, dan dapat saling berkomunikasi, saling bekerjasama untuk mencapai suatu tujuan tertentu, misalnya:

- Berbagi sumber daya: contohnya berbagi pemakaian *printer*, *file sharing*, dll.
- Komunikasi: contohnya *e-mail*, *instant messaging*, *chatting*
- Akses informasi: contohnya *web browsing*, *streaming*

Untuk mencapai tujuan tersebut, maka diperlukan adanya pihak yang memberikan layanan dan pihak yang meminta/menerima layanan. Pihak yang meminta/menerima layanan disebut *client* dan yang memberikan/mengirim layanan disebut *server*. Arsitektur ini disebut dengan sistem *client-server*.

## **2.3. Virtual Private Networking**

### **2.3.1. Pengertian dan cara kerja VPN**

*Virtual Private Networking* adalah sistem yang memungkinkan seseorang mengakses sumberdaya pada jaringan lokal melalui jaringan *internet*. Di dalam sebuah sistem VPN, maka mutlak diperlukan adanya sebuah NAS ( *Network Access Server* ) atau seringkali juga disebut *VPN gateway* yang berfungsi untuk menghubungkan jaringan lokal ke jaringan *internet*. Selain NAS, sistem VPN juga membutuhkan keberadaan sistem autentikasi. Salah satu contoh sistem autentikasi adalah RADIUS ( *Remote Authentication Dial In Service* ).

Ketika NAS menerima permintaan koneksi dari *user*, NAS akan mengirimkan informasi yang diperolehnya dari *user* ke RADIUS *server*. Kemudian RADIUS *server* akan memeriksa apakah informasi tentang *user* tersebut cocok dengan data yang dimilikinya. Jika informasi tersebut cocok, maka RADIUS *server* akan menyatakan bahwa *user* tersebut sah dan memberitahukan ke NAS. Jika tidak,

maka RADIUS *server* akan menyatakan bahwa *user* tersebut tidak sah dan memberitahukan ke NAS. Berdasarkan informasi dari RADIUS *server* tersebut, NAS akan memutuskan untuk melanjutkan atau menghentikan permintaan koneksi dari *user*.

Ketika *user* tersebut dinyatakan mempunyai hak akses ke jaringan lokal, maka kemudian oleh NAS akan diberikan alokasi alamat IP pada jaringan lokal tersebut. Alokasi ini dapat dilakukan oleh NAS tersebut atau NAS hanya melakukan relay dari DHCP *server* yang lain. Dengan demikian, maka *user* tersebut akan seolah-olah berada pada jaringan lokal tersebut. Inilah yang kemudian dinamakan VPN.

### **2.3.2. DHCP (*Dynamic Host Configuration Protocol*)**

*Dynamic Host Configuration Protocol* (DHCP) adalah suatu protokol jaringan yang digunakan oleh DHCP *server* untuk memberikan alokasi alamat IP pada komputer *client*. Setiap DHCP *client* akan terkoneksi secara terpusat pada suatu DHCP *Server* dimana DHCP *Server* ini akan memberikan alokasi alamat IP kepada komputer *client* yang melakukan permintaan (*request*) alokasi alamat IP, yang termasuk didalamnya antara lain : IP *address*, *netmask*, *gateway* dan DNS *server*.

*Client* dalam melakukan permintaan alokasi alamat IP akan menjalani proses sebagai berikut:

- **DHCPDISCOVER:** DHCP *client* akan menyebarkan request secara *broadcast* untuk mencari DHCP Server yang aktif.
- **DHCPOFFER:** Setelah DHCP Server mendengar *broadcast* dari DHCP Client, DHCP server kemudian menawarkan sebuah alamat kepada DHCP *client*.
- **DHCPREQUEST:** Client meminta DHCP server untuk menyewakan alamat IP dari salah satu alamat yang tersedia dalam DHCP Pool pada DHCP Server yang bersangkutan.
- **DHCPACK:** DHCP server akan merespons permintaan dari *client* dengan mengirimkan paket *acknowledgment*. Kemudian, DHCP Server akan menetapkan sebuah alamat (dan konfigurasi TCP/IP lainnya) kepada *client*, dan memperbarui basis data miliknya. Setelah *client* mendapatkan alokasi alamat IP, maka *client* pun dapat memulai komunikasi

### 2.3.3. RADIUS Server

RADIUS ( *Remote Authentication Dial In User Service* ) adalah sebuah protokol keamanan komputer yang digunakan untuk melakukan autentikasi, otorisasi, dan pendaftaran akun pengguna secara terpusat untuk mengakses jaringan. RADIUS didefinisikan di dalam dokumen RFC 2865 dan RFC 2866



RADIUS dijalankan oleh sebuah RADIUS server. Di dalam melakukan tugasnya, RADIUS server bekerjasama dengan NAS. Database yang dimiliki oleh RADIUS server ada 2 yaitu:

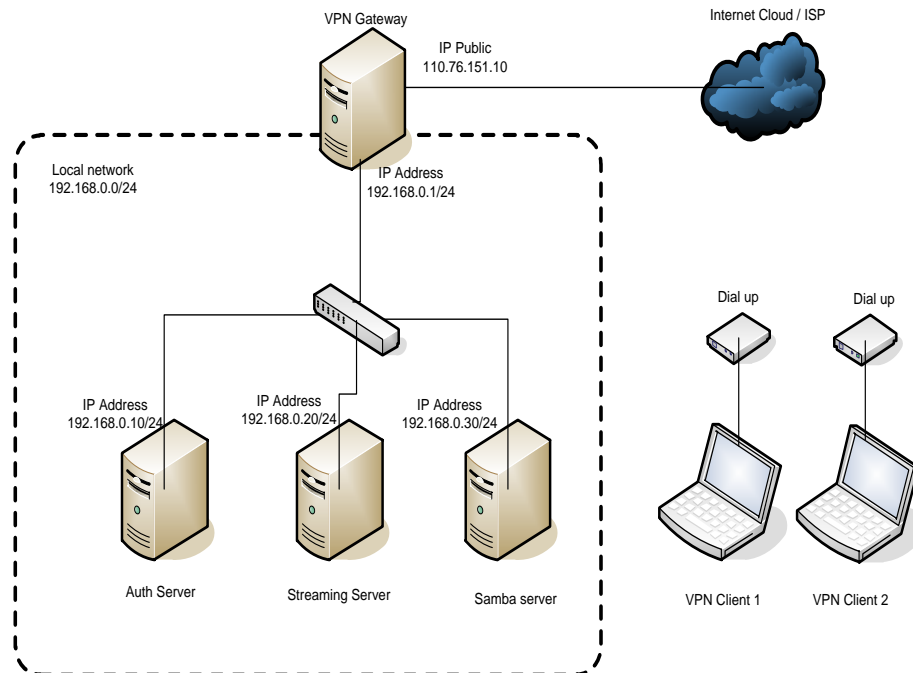
- *Database client* yang berisi nama atau alamat IP *client* beserta *shared secret*-nya. *Client* ini berupa NAS.
- *Database user* yang berisi *username* dan *password* untuk pengguna (*user*).

Saat sebuah NAS meminta layanan dari RADIUS server, maka oleh RADIUS server akan dilakukan pemeriksaan nama dan atau alamat IP beserta *shared secret* yang dikirimkan oleh NAS tersebut. Jika informasi yang diterima cocok dengan *database client* yang dimilikinya, maka *client* tersebut dinyatakan sah dan dicatat dalam *log file* RADIUS server tersebut.

Ketika kemudian ada permintaan layanan dari *user* melalui NAS tersebut, maka informasi *user* yang dikirimkan oleh NAS, akan diperiksa dan dicocokkan dengan *database user*. Jika cocok, maka *user* tersebut dinyatakan sah dan dicatat di dalam *log file* RADIUS server.

#### **2.4. Rancangan Topologi Jaringan**

Berikut ini rancangan topologi jaringan secara penuh yang akan dibangun dalam tugas akhir.



Gambar 2.1. Topologi jaringan VPN

Adapun kebutuhan untuk membangun sebuah DHCP server dan sebuah RADIUS server adalah:

1. Sebuah komputer dengan spesifikasi :
  - Prosesor Pentium 4 atau yang setara
  - Memori 1 GB
  - *Interface ethernet*
  - *DVD drive*
  - *Hard disk 4 GB.*
2. *Master linux distro Centos 5.5 dalam bentuk DVD*
3. *Software DHCP server ( bawaan dari Centos 5.5 )*
4. *Software FreeRADIUS versi 2 ( yang akan diinstal melalui yum )*