BAB II

ANALISIS DAN PERANCANGAN

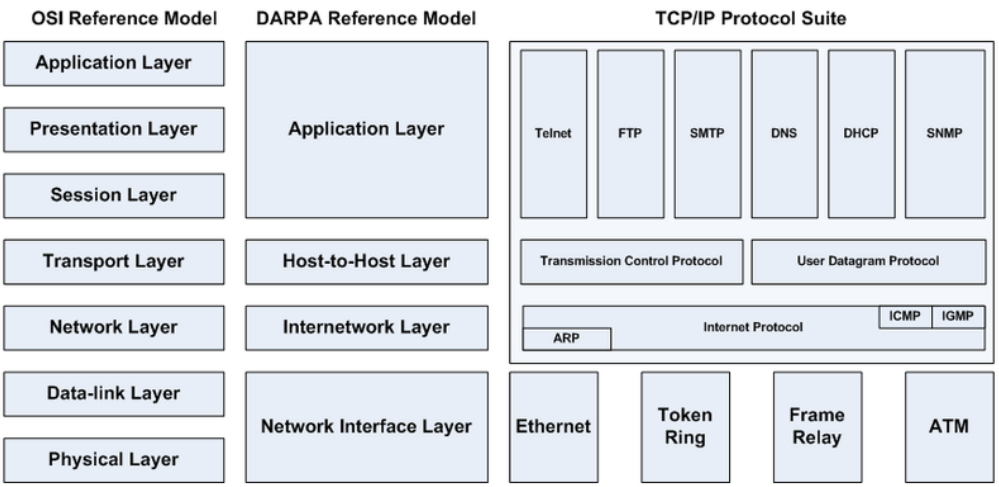
2.1 Jaringan Komputer

2.1.1 Pengertian Jaringan Komputer

Jaringan komputer merupakan sekelompok komputer yang saling berhubungan antara satu dengan yang lainya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, program-program, penggunaan bersama perangkat keras seperti printer, hardisk dan sebagainya.

2.1.2 Protokol TCP/IP

Sebuah jaringan memiliki suatu standar bahasa yang memungkinkan tiap-tiap komputer yang berbeda jenis dapat saling berkomunikasi. Standar tersebut adalah protokol yang berfungsi mengatur sebuah *host* berkomunikasi dengan *host* yang lain pada jaringan tersebut. TCP/IP (*Transmission Control Protocol/Internet Protocol*) merupakan standar komunikasi data yang digunakan dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan.



Gambar 2.1 OSI dan TCP/IP

2.2 IP Address

2.2.1 Pengertian IP Address

Alamat IP (*Internet Protocol Address*) adalah deretan angka *biner* antara 32-bit (untuk IPv4 atau IP versi 4) sampai 128-bit (untuk IPv6 atau IP versi 6) yang dipakai sebagai alamat identifikasi untuk tiap host dalam jaringan internet berbasis TCP/IP.

2.2.2 Kelas Dalam IP Address

Dalam RFC 791, alamat IP versi 4 dibagi dalam 5 kelas, berikut merupakan tabel penjelasan tentang kelas tersebut jika dilihat dari oktet pertamanya :

Tabel 2.1 Kelas IP

Kelas Alamat IP	Oktet pertama (desimal)	Oktet pertama (biner)	Digunakan oleh
Kelas A	1–126	0xxxxxxx	Alamat *unicast* untuk jaringan skala besar
Kelas B	128–191	10xxxxxx	Alamat *unicast* untuk jaringan skala menengah hingga skala besar

Kelas C	192–223	110xxxxx	Alamat *unicast* untuk jaringan skala kecil
Kelas D	224–239	1110xxxx	Alamat *multicast* (bukan alamat *unicast*)
Kelas E	240–255	1111xxxx	Direservasikan; umumnya digunakan sebagai alamat percobaan (eksperimen); (bukan alamat unicast)

2.2.3 Pengertian Subnet Mask

S*ubnet mask* berfungsi untuk memanajemen jumlah host. Dengan *subnet mas*k, sebuah Router dapat menentukan bagian mana yang menunjukkan alamat host (Host ID).

S*ubnet mask* terdiri dari 32-*bit* yang setiap 8-*bit*nya dipisahkan dengan tanda titik (*dot*). Pada Subnet *Mask Default* , bit yang menunjukkan alamat jaringan diisi dengan biner 1 semua, sedang bit yang menunjukkan alamat host diisi dengan biner 0 semua.

Tabel 2.2 Pembagian Kelas Subnet Mask

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

2.2.4 Menentukan Alamat Jaringan dan Alamat Broadcast

Menentukan alamat jaringan dapat dilakukan dengan konversi bilangan desimal ke biner terlebih dahulu pada alamat IP dan *netmask*. Misalkan sebuah komputer dengan alamat IP 192.168.0.30 dan *netmask* 255.255.255.0 maka hasil konversinya yaitu :

Alamat IP : 11000000.10101000.00000000.00011110

Netmask : 11111111.11111111.11111111.00000000

Alamat jaringan diperoleh dengan cara melakukan operasi *AND* pada bilangan biner IP dan *netmask,* sehingga mendapatkan hasil : 11000000.10101000.00000000.00000000.

Bilangan biner tersebut jika dikonversi ke bilangan desimal maka akan mendapatkan hasil : 192.168.0.0. Nilai tersebut merupakan Alamat Jaringan.

Menentukan *broadcast* dengan cara melakukan operasi *OR* pada alamat jaringan dengan nilai pembalikan (*NOT*) dari nilai biner *netmask*, yaitu:

Network Address: 11000000.10101000.00000000.00000000,

NOT Subnet Mask: 00000000.00000000.00000000.11111111. Kemudian dilakukan operasi OR kedua bilangan biner tersebut maka akan mendapatkan hasil: 1100000.10101000.00000000.11111111. Nilai biner tersebut jika dikonversikan menjadi nilai desimal adalah : 192.168.0.255. Nilai tersebut adalah alamat *broadcast.*

2.3 VPN (Virtual Private Network)

VPN (*Virtual Private Network)* adalah suatu jaringan pribadi yang memberikan akses komunikasi menggunakan jaringan *internet* untuk menghubungkan *remote-site* secara aman, sehingga VPN banyak digunakan untuk teknologi keamanan akses jaringan komputer. Komputer yang mendapatkan akses ke VPN berpotensi dapat mengakses semua sumber daya pada jaringan, karena seolah-olah tersambung secara jaringan lokal (LAN).

Sebuah sistem VPN secara mutlak memerlukan sebuah NAS (*Network Acces Server*) dan keberadaan sistem otentikasi. Salah satu contoh dari sistem otentikasi adalah RADIUS (*Remote Authentication Dial In User Service*).

2.3.1 Cara Kerja VPN *Server*

Cara kerja VPN *server* ditunjukkan dengan kerjasama antara NAS dan RADIUS *server* sebagai berikut :

1. NAS menerima permintaan koneksi dan mengirimkan informasi yang diterima dari *client* ke RADIUS *server*.
2. RADIUS *server* melakukan verifikasi otentikasi mengenai informasi *client* dan mengirimkan informasi ke NAS setelah menyatakan sah atau tidak sah mengenai keaslian informasi dari *client*.
3. Berdasarkan informasi dari RADIUS *server*, maka NAS memutuskan untuk mempersilahkan atau menghentikan permintaan dari *client*.
4. Jikalau *client* mendapatkan akses ke jaringan, maka alamat IP pada *client* dialokasikan NAS dengan melakukan *relay* dari *database* RADIUS *server*.

2.3.2 NAS

NAS (*Network Access Server*) dalam sistem jaringan VPN dikenal sebagai RAS (*Remote Access Server*) yang berfungsi sebagai *gateway* yang menghubungkan antara *client* yang berada pada

jaringan publik dengan jaringan lokal. *Gateway* merupakan istilah yang mengacu kepada pintu keluar atau titik perpindahan dalam jaringan komputer yang menghubungkan satu jaringan dan jaringan lainnya.

2.3.3 RADIUS *Server*

RADIUS (*Remote Authentication Dial In User Service*) adalah sebuah protokol yang digunakan untuk melakukan otentikasi, otorisasi dan pendaftaran akun pengguna demi keamanan akses jaringan. RADIUS dijalankan oleh sebuah RADIUS *server* yang mengerjakan tugasnya bekerjasama dengan NAS.

Kerjasama antara NAS dan RADIUS *server* melibatkan *database* RADIUS *server*. *Database* yang dimiliki RADIUS *server* ada dua yaitu :

1. *Database client*, berisi nama atau alamat IP *client* beserta *shared secret*-nya.
2. *Database user*, berisi *username* dan *password* untuk pengguna (*user*).

2.4 Linux Backtrack

Linux secara umum adalah Sistem *Multiuser*, artinya komputer dapat dipakai oleh beberapa user pada saat bersamaan. Setiap user mempunyai kondisi dan lingkungan kerja sendiri. Agar hal ini bisa terselenggara dengan baik user-user tersebut harus dibuatkan *account* oleh Administrator Sistem Linux. Administrator pada Linux adalah *root*.

2.4.1 Hak Akses Pada Linux

Sistem Linux terdapat kepemilikan file atau *ownership* dan *hak akses permission*. Hak Akses merupakan sistem keamanan file dalam sistem Linux. Setiap file dan direktori yang ada dalam sistem linux memiliki tiga hak akses. Contoh :

```
total 8
drwxrwx--- 2 root root 4096 2011-07-08 11:46 Data
drwxrwxr-x 5 root root 4096 2011-07-08 11:48 Public
```

Gambar 2.2 Hak akses Direktori

Karakter pertama menunjukkan jenisnya, jika berisi karakter *d* berarti adalah direktori sedangkan jika kosong berarti file. Sembilan karakter berikutnya menunjukkan hak akses pemilik file, group, dan untuk user lain.

Tabel 2.3 Karakter Nilai Hak Akses

Karakter	Arti	Nilai
r (read)	Hak akses untuk membaca	4
w (write)	(write) Hak akses untuk menulis	2
x (exec)	(exec) Hak akses untuk menjalankan	1

Linux menyediakan beberapa perintah untuk menentukan hak akses, yaitu:

a. Perintah *chown* digunakan untuk mengganti pemilik sebuah file,
b. Perintah *chattr* untuk melindungi sebuah file sehingga tidak akan dapat dihapus atau dirubah dengan perintah apapun
c. Perintah *chmod* digunakan untuk memberikan hak akses *read*, *write*, *execute* pada sebuah file ataupun direktori.

2.5 Samba

Samba merupakan serangkaian aplikasi *UNIX* yang berkomunikasi dengan protokol *Server Message Block* (SMB). SMB adalah protokol komunikasi data yang juga digunakan oleh *Microsoft* dan *OS/2* untuk menampilkan fungsi jaringan client-server yang menyediakan sharing berkas dan printer serta tugas-tugas lainnya yang berhubungan.

Beberapa kegunaan Samba server yaitu:

a. Sharing berkas/direktori antar Unix/Linux dengan windows
b. Printer sharing pada Samba server dengan windows client
c. Memudahkan proses *network browsing*
d. Menyediakan proses *Autentikasi* komputer windows client ketika *login* ke Windows *domain*
e. Menyediakan dan membantu proses *netbios name resolution* dengan *Windows Internet name Service* (WINS).

Komunikasi *client-server* pada jaringan yang berbeda sistem operasi dilakukan melalui port SMB pada protokol TCP. SMB digunakan dalam interaksi *request* dan *respon* antara *client-server*.

Ketika *client* dan *server* terhubung pada level *NetBIOS*, *client* siap untuk mengirimkan *request* ke *server*. *Client* dan *server* harus saling mengidentifikasi protokol mana yang akan digunakan. Setelah protokol SMB terhubung, *client* akan meneruskan untuk *login* ke *server* jika dibutuhkan. Server me-*respon* dengan memberitahukan apakah *username* dan *password* yang dimasukan benar atau salah. Kemudian

client dapat melanjutkan untuk mengakses folder yang di-*share* yaitu: membuka file dengan *open SMB*, membaca file dengan *read SMB*, menulis file dengan *write SMB*, dan menutupnya dengan *close SMB*.

Samba memiliki beberapa apikasi server yaitu *smbd* dan *nmbd*. *Smbd* adalah aplikasi *server* atau *daemon* yang menangani proses sharing berkas/direktori dan *printer*, juga menangani proses *autentikasi* dan *otorisasi* dengan SMB *client*. Sedangkan *nmbd* adalah aplikasi server atau daemon yang mendukung *Netbios name service* dan WINS, juga membantu proses *network browsing* pada windows *client*.

2.5.1 File Konfigurasi Samba

Dalam file konfigurasi *smb.conf* pada dasarnya terdapat dua buah variable, yaitu :

1. [global]

Variabel [global] mendefinisikan tentang konfigurasi server samba, seperti *workgroup, netbios*, *security* dan sebagainya. Bagian ini menyediakan empat macam jenis security yang bisa digunakan yaitu:

1. *User*

   Client terlebih dahulu harus melakukan *login* dengan nama *user* dan *password* yang *valid*.

2. *Share*

   Client tidak perlu melakukan *login* sebelum menggunakan sumberdaya jaringan .

3. *Server*

   Samba akan mencoba melakukan validasi nama *user* dan passwordnya dengan cara melakukanya ke server smb yang lainya.

4. *Domain*

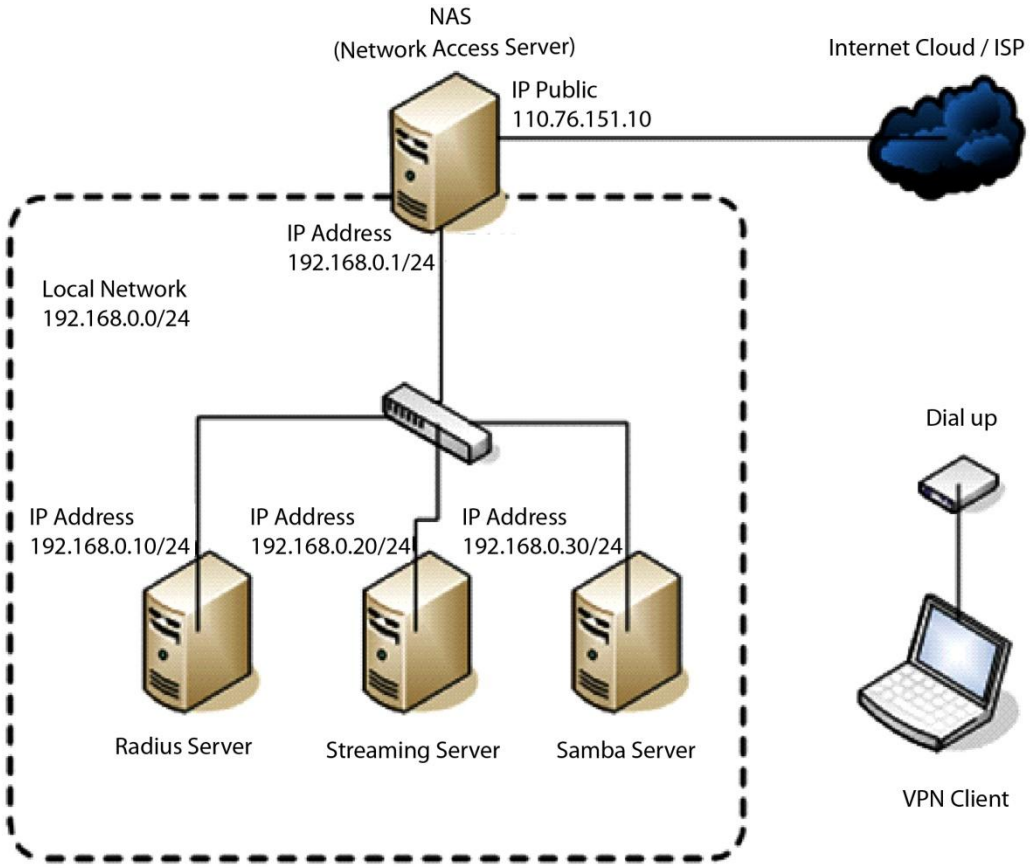
   Security ini akan bekerja jika *account* mesin akan ditambahkan ke windows NT domain dengan menggunakan smb password. Hal ini juga memerlukan parameter *encrypted password* di-set *true.*

2. [share]

Variabel [share] mendefinisikan akses direktori atau file yang akan di-*share* melalui samba server. Pada bagian ini terdapat pengaturan direktori dan hak akses terhadap direktori tersebut.

2.6 Rancangan Sistem Jaringan

Jaringan lokal dengan alamat jaringan 192.168.0.0/24 ini merupakan serangkaian server, yaitu: *Radius Server, Streaming Server,* dan *Samba Server* yang terhubung pada NAS melalui sebuah *switch*.



Gambar 2.3 Rancangan Jaringan

VPN Gateway (NAS) terhubung ke internet melalui alamat IP *public:* 110.76.151.10 dan *netmask:* 255.255.255.255 dari ISP. Namun untuk sekedar melakukan pengujian pada tugas akhir ini VPN digunakan pada jaringan lokal dengan menggunakan alamat IP *private:* 172.17.42.133 dengan *netmask:* 255.255.255.0.