BAB I
PENDAHULUAN

1.1 Latar Belakang

Salah satu perubahan utama di bidang telekomunikasi adalah penggunaan teknologi *wireless*. Teknologi *wireless* juga diterapkan pada jaringan komputer, yang lebih dikenal dengan *wireless* LAN (WLAN). Kemudahan-kemudahan yang ditawarkan *wireless* LAN menjadi daya tarik tersendiri bagi para pengguna komputer menggunakan teknologi ini untuk mengakses suatu jaringan computer atau internet. Beberapa tahun terakhir ini pengguna *wireless* LAN mengalami peningkatan yang pesat. Peningkatan pengguna ini juga dibarengi dengan peningkatan jumlah *hotspot* yang dipasang oleh ISP (*Internet Service Provider*) di tempat-tempat umum, seperti kafe, mal, bandara, Banyak kantor maupun kampus yang telah memiliki hotspot, pada umumnya *hotspot* ini berada di ruangan rapat. Masalah yang akan kita hadapi apabila menerapkan *wireless* LAN adalah isu tentang keamanannya. Banyak pihak yang masih mempertanyakan tentang keamanan *wireless* LAN. [1]

Apabila kita mengimplementasikan *wireless* LAN, maka kita juga harus mengimplementasikan sistem keamanan apa yang akan kita terapkan. Banyak *hotspot* yang tidak menerapkan sistem keamanan yang memadai, sehingga memungkinkan pengguna yang tidak berhak (ilegal) dapat masuk ke jaringan komputer tersebut. Apabila hal ini sampai terjadi, maka pemilik *hotspot* tersebut secara langsung maupun tidak langsung akan dirugikan, penyusup itu dapat saja melakukan perbuatan yang tidak menyenangkan, seperti mengambil data, menyerang komputer-komputer yang ada di jaringan tersebut, kehilangan pendapatan (apabila pemilik *hotspot* adalah ISP.) Sistem keamanan yang paling umum diterapkan pada *wireless* LAN adalah dengan metode enkripsi, yaitu WEP (*Wired Equivalent Privacy*). WEP ini menggunakan satu kunci enkripsi yang digunakan bersama-sama oleh para pengguna *wireless* LAN. Hal ini menyebabkan WEP tidak dapat diterapkan pada *hotspot* yang dipasang di tempat-tempat umum. Dan karena lubang keamanan yang dimiliki WEP cukup banyak, sehingga mudah dibobol oleh pihak ketiga yang tidak berhak, maka penggunaannya tidak disarankan lagi. Sistem keamanan lainnya adalah WPA (*Wi-Fi Protected Access*), yang menggeser WEP dan menghasilkan keamanan yang lebih baik dari WEP. Implementasi WPA menggunakan 802.1x dan EAP (*Extensible Authentication Protocol*) menghasilkan proses autentikasi pengguna yang relatif lebih aman.

Pada proses ini pengguna harus melakukan autentikasi ke sebuah server autentikasi, misalnya RADIUS, sebelum terhubung ke *wireless* LAN atau internet.[1]

Pada umumnya proses autentikasi ini menggunakan nama-pengguna dan *password*. Setting Hotspot dengan menggunakan Mikrotik sebagai RADIUS server sangat mudah dikonfigurasi. Sistem autentikasi hotspot biasa digunakan ketika kita akan menyediakan akses internet pada areal publik, Ketika membuka halaman web maka router akan mengecek apakah user sudah di autentikasi atau belum. Jika belum melakukan autentikasi, maka user akan di arahkan pada hotspot login page yang mengharuskan mengisi username dan password. Jika informasi login yang dimasukkan sudah benar, maka router akan memasukkan user tersebut kedalam sistem hotspot dan client sudah bisa mengakses halaman web. Selain itu akan muncul popup windows berisi status ip address, byte rate dan time live. Penggunaan akses internet hotspot dapat dihitung berdasarkan waktu (time-based) dan data yang di download/upload (volume-based). Selain itu dapat juga dilakukan melimit bandwidth berdasarkan data rate, total data upload/download atau bisa juga di limit berdasarkan lama pemakaian. [2]

1.2 MAKSUD DAN TUJUAN

Adapun Tujuan Penelitian Proyek Akhir ini adalah:

1. Rancang bangun dan menganalisa Hotspot Menggunakan MikroTik sebagai RADIUS Server.

1.3 RUMUSAN MASALAH

Rumusan masalah dari proyek akhir ini adalah sebagai berikut :

1. Perancangan topologi jaringan
2. Hotspot dengan menggunakan Mikrotik sebagai RADIUS Server
3. Access Point Tp –Link tipe TL- WA601G
4. Konfigurasi kartu jaringan (Ethernet),
5. Mengkonfigurasi RADIUS Server melalui WinBox

1.4 PEMBATASAN MASALAH

Ruang lingkup permasalahan dalam laporan proyek akhir ini hanya terbatas pada masalah-masalah sebagai berikut :

1. Tidak membahas Hotspot dengan menggunakan Perangkat lain,
2. Hanya membahas teori dasar Hotspot dan dasar jaringan serta konfigurasi MikroTik sebagai Server RADIUS.
3. Hanya membahas konfigurasi LAN dan MikroTik, perangkat access point adalah merk TP – LINK tipe TL – WA601G
4. Pada saat pengujian PC atau Laptop yang di gunakan hanya 3 buah
5. Pada bagian analisanya yang di bahasa hanya fungsi dari RADIUS server itu sendiri yaitu AAA (autentikasi, authorization, and accounting).

1.5 METODE PENELITIAN

Pada pembuatan proyek akhir ini, penulis melakukan metodologi penelitian dengan menggunakan metode sebagai berikut :

1. Studi literature

   Yaitu dengan melakukan survei pada beberapa sumber bacaan dan situs internet yang mendukung da|am penu|isan proyek akhir ini
2. Perancangan dan realisasi.

   Mefakukan proses perancangan Hotspot berdasarkan pada hasil studi literature dan mengimplementasikan teori-teori dasar komunikasi data dan jaringan komputer kedalam perancangan.

1.6 SISTEMATIKA PENULISAN

Secara garis besar sistematika penulisan proyek akhir ini terdiri dari bab, dengan metode penyampaian sebagai berikut :

BAB I PENDAHULUAN

Menerangkan latar belakang masalah, maksud dan tujuan, pembatasan masalah, metodologi penelitian dan sistematika penulisan dan jadwal kerja proyek akhir.

BAB II TEKNOLOGI HOTSPOT dan MIKROTIK SEBAGAI RADIUS SERVER

Menjelaskan tentang dasar teori Hotspot dan RADIUS Server serta dasar-dasar networking

BAB III INSTALASI DAN KONFIGURASI HOTSPOT MENGGUNAKAN MIKROTIK SEBAGAI RADIUS SERVER

Menjelaskan tentang perancangan topologi jaringan, penginstallasian dan konfigurasi Hotspot dan RADIUS server

BAB IV PENGUJIAN DAN ANALISA

Menjelaskan tentang cara menjalankan sekaligus menganalisa hasil pengujian Hotspot dan RADIUS server

BAB V KESIMPULAN DAN SARAN

Merupakan kesimpulan dari seluruh pembahasan pada penulisan proyek akhir ini. Saran untuk pengembangan lebih lanjut.