BAB I
PENDAHULUAN

1.1 Latar Belakang

Dunia teknologi dan ilmu pengetahuan pada saat ini berkembang pesat, mengakibatkan banyak perubahan yang terjadi dalam kehidupan manusia. Salah satunya perkembangan teknologi. Adanya perkembangan teknologi ini setiap pekerjaan akan dapat direalisasikan secara lebih efisien dan efektif (Djaelangkara dkk.,2015). Salah satu perubahan yang bisa dirasakan adalah perkembangan komunikasi yaitu pada penggunaan *hotspot*. Penggunaan *hotspot* sudah marak sekali digunakan hampir setiap tempat mempunyai *hotspot* seperti sekolah, Kampus, pengkantoran, mall, restoran, dan lain-lain yang mempunyai jaringan *wireless*.

Pada *wireless* keamanan yang paling umum digunakan adalah dengan menggunakan metode enkripsi yaitu WEP *(Wired Equivalent Privacy)*(Geier, 1999). Pada WEP system keamanan menggunakan satu kata kunci enkripsi untuk semua pengguna wireless yang digunakan bersama-sama. Hal ini menyebabkan metode WEP menjadi tidak cocok dipasang ditempat-tempat umum karena memiliki keamanan yang kurang baik karena dapat dimasuki oleh pihak-pihak yang berhak sehingga tidak disarankan lagi untuk menggunakan metode keamanan ini. Sistem keaman selain WEP adalah WPA *(Wi-Fi Protected Access)*, sistem keaman WPA telah mampu menggeser metode WEP dan menghasilkan keamanan yang lebih baik. Implementasi WPA menggunakan 802.1x dan EAP *(Extensible Authentication Protocol)* (Josh, 2009). Sehingga menghasilkan keamanan yang lebih baik dengan proses *auntetifikasi* pengguna. Pada proses ini setiap pengguna harus melakukan proses autentikasi ke *serverauntetifikasi*sebelum terhubung ke internet. Pada umumnya proses autentikasi ini menggunakan *username* dan *password*.

Berdasarkan hasil pengamatan yang dilakukan oleh penulis di Universitas Katolik Musi Charitas Palembang, bahwa UKMC sudah menggunakan sistem autentifikasi untuk melakukan koneksi ke jaringan hotspot mahasiswa. Dalam hasil wawancara dengan kepala kantor KSITK(dapat dilihat di lampiran 1), mengatakan bahwa sistem autentifikasi di UKMC masih mengunakan *username* dan *password* yang sama, jadi setiap mahasiswa yang ingin *login* memasukan *username* dan *password* untuk koneksi ke *internet.* Masalahnya ada pada tidak semua mahasiswa mengetahui *username* dan *passwordwi-fi* mahasiswa tersebut dan admin jaringan juga tidak dapat mengkontrol dan *Memanagemant* user yang login di wi-fi mahasiswa. Karena masalah yang ada makanya penulis diminta untuk mendesain dan mensimulasikan sistem autentifikasi menggunakan server RADIUS *(Remote Authentication Dial-In User Service).*

Radius server yang digunakan adalah *FreeRADIUS. FreeRADIUS* merupakan *radius server* gratis yang cukup popular. *FreeRADIUS* dikembangkan pada tahun 1999 oleh Alan DeKok dan Miquel van Smoorenburg. Sebelum mengembangkan *FreeRADIUS,* Miquel pernah mengembangkan *Cistron RADIUS,* namun tidak dilanjutkan dan dilanjutkan dengan mengembangkan *FreeRADIUS. FreeRADIUS* dimulai untuk membuat *RADIUS Server* dengan menggunakan desain modular. Seiring perkembangan waktu *FreeRADIUS* semakin banyak digunakan, sehinga *FreeRADIUS* terus dikembangkan, sehingga selain *support text file, FreeRADIUS* juga *support* LDAP, SQL, *PostgreSQL*, *Oracel* dan banyak *database* lainnya. Selain itu *FreeRADIUS* mendukung semua autentikasi PAP popular termasuk PEAP dan EAP-TTLS. Dalam *FreeRADIUS* juga telah dimasukkan hingga lebih dari 100 *dictionaries* vendor dan kompabilitas dengan berbagai jenis perangkat NAS serta dapat berjalan dibanyak platform OS seperti keluarga Linux/Unix, Windows, Mac OS dan Sun Solaris. Hingga *FreeRADIUS* diklaim cukup cepat, kaya fitur, skalabel dan dapat diandalkan (Dekok Alan, 2014).

FreeRADIUS akan di install dan dikonfigurasi pada PC yang telah di install Ubuntu server 14.04 LTS. Sehingga PC tersebut akan menjadi *Radius Server* yang akan memanagemen dalam mengatur koneksi mahasiswa ke jaringan internet. Dengan demikian, sistem RADIUS akan menjadi sebuah keamanan yang penting untuk menggatur aktivitas mahasiswa dalam melakukan koneksi kejaringan internet. Dari urian di atas, maka penulis tertarik mengangkat sebuah judul "DESAIN DAN SIMULASI *AUNTETIFIKASI HOTSPOT* MAHASISWA MENGUNAKAN *FREERADIUS*".

1.2 Tujuan

Berdasarkan latar belakang masalah yang ada maka tujuan dalam kerja pratik ini adalah:

1. Mendesain dan mensimulasikan jaringan hotspot mahasiswa mengunakan radius server dan mikrotik di Universitas Katolik Musi Charitas.
2. Menjadi referensi penelitian selanjutnya (merancang jaringan hostpot menggunkaan radius server).

1.3 Manfaat

Manfaat yang didapatkan setelah kerja pratik ini selesai adalah

1. Dapat merancang dan mensimulasikan jaringan hotspot mengunakan radius server dan mikrotik di jaringan *hotspot* mahasiswa. Jadi mahasiswa akan mempunyai satu akun *hotspot* sendiri dengan *bandwith* sendiri juga , jadi tidak menggangu jaringan internet akun mahasiswa lainnya.
2. Hasil dari penelitian ini juga dapat dimanfaatkan sebagai referensi untuk penelitian selanjutnya.

1.4 Waktu Pelaksanaan

Jadwal pelaksanaan menunjukkan daftar kegiatan serta waktu dimulainya suatu kegiatan hingga kegiatan selesai. Penulis memulai penelitian ini pada tanggal 2Maret 2016 sampai 23 Juli 2016. Dengan jadwal setiap hari Senin pukul 07.15 – 14.00 WIB