



I PENDAHULUAN

1.1 Latar Belakang

Pertumbuhan jaringan komputer dari waktu ke waktu sangat cepat, seiring dengan perkembangannya maka perlu adanya pengamatan pada suatu jaringan komputer. Hal ini untuk menghindari adanya *user* yang tidak berhak menggunakan jaringan komputer dapat dengan leluasa masuk ke jaringan komputer. Pada saat ini banyak *user* yang dapat mengakses suatu jaringan komputer tanpa melalui ijin yang si pemilik jaringan, untuk masuk ke suatu sistem jaringan seharusnya diperlukan otentikasi agar *user* yang tidak berhak tidak dapat terhubung ke jaringan (Martin *et al.* 2013).

Hotspot merupakan suatu area dimana suatu koneksi internet dapat berlangsung tanpa kabel. Jaringan *Wi-Fi (Wireless Fidelity)* menjadi teknologi alternatif dan relatif lebih mudah untuk diimplementasikan di lingkungan kerja. *Hotspot* juga merupakan salah satu bentuk pemanfaatan teknologi pada lokasi-lokasi publik seperti taman, perpustakaan, restoran, kampus ataupun bandara, beberapa diantaranya bahkan dapat diakses secara cuma-cuma. Internet terkoneksi biasanya dilakukan melalui perangkat notebook/ laptop/ PDA. *Hotspot* pertama kali digagas tahun 1993 oleh Breet Stewart. Dengan teknologi ini, individu dapat mengakses jaringan seperti internet melalui komputer atau laptop yang *user* miliki di lokasi-lokasi dimana *hotspot* (Ardianto *et al.* 2018).

Radius server memberikan fungsi AAA (*Authentication, Authorization, dan Accounting*). Dengan ini seorang administrator jaringan mampu menambah keamanan pada layanan internet karena setiap *user* yang akan berhubungan dengan NAS (*Network Access Server*) akan di tahan oleh *Radius* Server dan melakukan autentikasi. *Radius* juga memaksimalkan performance dari jaringan dengan memanfaatkan fungsi *Accounting* dengan cara menyimpan log aktifitas setiap *user*, sehingga seorang administrator jaringan mampu mengambil keputusan hak akses yang perlu diberikan kepada setiap users selain itu juga server AAA juga dapat memberikan fungsi *Authorize* yang mana seorang administrator mampu memberikan hak akses dan kewenangan pada setiap *user* yang ada, sehingga *Access user* atau *client* dapat dibatasi oleh administrator jaringan (Haq *et al.* 2017).

Badan Standardisasi Instrumen Lingkungan Hidup dan Kehutanan menggunakan internet sebagai sarana pertukaran informasi. Kondisi instansi memiliki jaringan *wireless* dengan manajemen *user* yang kurang memadai, yang mengakibatkan para pegawai mempertanyakan tentang keamanannya. Penulis mengangkat judul tugas akhir yaitu “Penerapan *Authentication Hotspot* Menggunakan *Radius* Server” yang mana bertujuan untuk memberikan keamanan pada jaringan *hotspot* serta memudahkan admin jaringan dalam mengelola pengguna yang terhubung pada jaringan *hotspot*.

1.2 Rumusan Masalah

Bagaimana cara mengimplementasikan sistem *Authentication* menggunakan *Radius* Server di *Router* Mikrotik.



1.3 Tujuan

Merancang Sistem *Authentication Hotspot* Menggunakan *Radius* Server di Router Mikrotik memiliki tujuan:

- a Untuk membuat mikrotik *hotspot* dengan menggunakan sistem login untuk para pengguna.
- b Untuk membuat sistem yang memudahkan dalam mengelola pengguna pada *hotspot* sehingga administrator jaringan dapat melakukan *accounting*.

1.4 Manfaat

Dari penerapan Sistem *Authentication Hotspot* Menggunakan *Radius* Server Router Mikrotik adalah:

- a Menjaga kestabilan koneksi internet.
- b Memudahkan dalam mengelola pengguna.
- c Memberikan keamanan pada setiap pengguna.

1.5 Ruang Lingkup

Batasan-batasan dalam penerapan Sistem *Authentication Hotspot* Menggunakan *Radius* Server Router Mikrotik yang digunakan adalah Mikrotik dan *Radius* Server yang terdapat pada mikrotik itu sendiri.



Sekolah Vokasi
College of Vocational Studies