ABSTRAK

Perkembangan teknologi informasi yang semakin pesat telah mengubah sistem konvensional menjadi sistem yang modern, terutama dengan adanya *internet*. *Internet* memberikan konstribusi yang sedemikian besar bagi masyarakat, perusahaan, dan pemerintahan. Kebutuhan akan *internet* sudah dirasakan oleh masyarakat, hal ini terbukti dengan banyaknya fasilitas tempat umum seperti *café*, *mall*, kampus, perkantoran dan lain sebagainya yang menyediakan fasilitas *internet*. Salah satu masalah yang sering terjadi adalah penggunaan jaringan *internet* dari *user illegal* atau yang tidak memberikan autentikasi kepada *client*. *Captive portal* adalah salah satu cara untuk tidak memberi izin adanya *traffic* sebelum *user* melakukan registrasi pada suatu *web*. Biasanya *Captive Portal* digunakan pada infrastruktur *wireless* seperti *hotspots area*, tetapi tidak menutup kemungkinan diterapkan pada jaringan kabel.

Penggunaan *Captive Portal* tidak tergantung dengan mekanisme keamanan *built-in* peralatan *WiFi* 802.11b untuk mengontrol siapa saja yang dapat bersosialisasi ke *access point*. Penggunaan *Captive Portal* agar *access point* berkerja tanpa *WEP*, sehingga tidak membebani kerja dari *access point* itu sendiri. *Access point* berkerja pada *mode bridge* (bukan *router*) dan tersambung ke *computer server* yang sudah terkonfigurasi sebagai *router* linux. *Router* linux akan berfungsi sebagai *gateway* penghubung antara jaringan lokal dengan jaringan *internet*.

Pada penelitian ini dilakukan penelitian *Captive Portal* di jaringan *wireless*. Dalam tugas kali ini akan mengimplementasikan *Captive Portal* menggunakan *gateway* dimana *user* yang belum terauntikasi akan dipaksa menuju ke *aunthentication web* dan mengamati tingkat performansinya. Parameter-parameter yang dianalisis pada penelitian kali ini adalah *time login,respon server, throughput*,dan keamanan pada *Captive Portal (MAC spoofing).* Hasil análisis menunjukan *Captive Portal* memiliki waktu *login* mínimum sebesar 6 ms, *Captive Portal* ini mampu melayani 4738 *user* dengan maksimal transaksi sebesar 1.342.738 tidak sebaik mikrotik dalam melakukan *management bandwidth*, namun sudah cukup adil untuk membagi *bandwidth* untuk masing-masing *user*, dan *Captive Portal* kali ini mampu menangani *MAC spoofing*. Adapun hasil dari perancangan kali ini diharapkan dapat diterapkan pada suatu badan atau instalasi.

Kata kunci : *Captive Portal, time login, bandwidth management, response time server, dan MAC spoofing.*