MANAJEMEN JARINGAN WIRELESS MENGGUNAKAN SERVER RADIUS

Raymond Powers Tenggario; Jonathan Lukas

Computer Engineering Department, Faculty of Engineering, Binus University
Jln. K.H. Syahdan No. 9, Palmerah, Jakarta Barat 11480
jonathanlukas@binus.ac.id

ABSTRACT

Security is very critical in a network. Therefore, the wireless hotspot system designed at this occasion uses a radius server with EAP authentication method for authorization and authentication in a network and usage limitation of each user. The application designed is also equipped with a hotspot user management, billing, voucher-making and usage limitation of time/quota per user. This study aims to implement a user authentication system of LAN hotspot wireless based on RADIUS (802.1X) with access limitation on based on both time usage quota and data packet quota. The results obtained help simplify the wireless hotspot network management. It is concluded that this hotspot management system can perform a variety of access limitation schemes including the use of time limitation (time-based) and the amount of packet data use (volume-based) with bandwidth limitation for each user.

Keywords: *hotspot, wireless, radius server, EAP authentication*

ABSTRAK

Keamanan sangat penting dalam suatu jaringan. Oleh karena itu, sistem wireless hotspot yang dirancang kali ini menggunakan radius server dengan metode EAP authentication untuk autorisasi dan autentikasi dalam suatu jaringan dan pembatasan pemakaian tiap user. Perancangan aplikasi ini juga dilengkapi dengan manajemen pengguna hotspot, biling, pembuatan voucher dan pembatasan pemakaian waktu/kuota per user. Penelitian ini bertujuan untuk mengimplementasikan sistem autentikasi pengguna hotspot wireless LAN berbasis RADIUS (802.1X) dengan pembatasan akses berdasarkan kuota waktu pemakaian dan kuota paket data. Hasil yang dicapai membantu mempermudah manajemen jaringan wireless hotspot. Dapat disimpulkan bahwa sistem manajemen hotspot ini dapat melakukan berbagai skema pembatasan akses, di antaranya pembatasan berdasarkan lama penggunaan waktu (time based) dan jumlah penggunaan paket data (volume based) dengan pembatasan bandwidth untuk tiap pengguna.

Kata kunci: *hotspot, wireless, radius server, EAP authentication*

PENDAHULUAN

Jaringan komputer adalah sekelompok komputer yang saling berhubungan satu sama lain dengan memanfaatkan media komunikasi dan suatu protokol komunikasi, sehingga antar komputer dapat saling berbagi dan bertukar informasi. Pada saat ini, manfaat dari jaringan komputer sudah sangat banyak dirasakan. Apalagi dalam dunia komunikasi yang serba cepat ini, jaringan komputer sering kali berperan vital dalam kegiatan pendistribusian informasi yang cepat tersebut. Semua dari komponen yang tergabung dalam jaringan komputer tersebut haruslah mampu saling mendukung untuk menghasilkan satu sistem yang kokoh dan handal untuk melayani setiap permintaan informasi yang dibutuhkan oleh pengguna.

Pemanfaatan teknologi jaringan komputer sebagai media komunikasi data hingga saat ini semakin meningkat. Kebutuhan atas penggunaan bersama resource yang ada dalam jaringan baik software maupun hardware telah mengakibatkan timbulnya berbagai pengembangan teknologi jaringan itu sendiri. Seiring dengan semakin tingginya kebutuhan dan semakin banyaknya penggunaan jaringan yang menginginkan suatu bentuk jaringan yang dapat memberikan hasil maksimal baik dari segi efisiensi maupun peningkatan keamanan jaringan itu sendiri. Berlandaskan pada keinginan-keinginan tersebut, maka upaya-upaya penyempurnaan terus dilakukan oleh berbagai pihak.

Teknologi *wireless* memberikan kemudahan dan fleksibilitas yang cukup tinggi dan nyaman digunakan. Selama berada dalam *hotspot wireless*, *user* dapat mengakses internet dimana pun. Untuk membuat sebuah jaringan terkoneksi ke internet yang aman dan *user friendly*, kita bisa membuat sebuah sistem menggunakan Radius *Server* untuk melakukan autorisasi dan autentikasi dalam sebuah jaringan, membatasi pemakaian tiap *user* yang ada di dalam sebuah jaringan.

Ruang lingkup dari penelitian mencakup analisis, perancangan dan implentasi jaringan. Ruang lingkup yang akan dibahas sebagai berikut: (1) jaringan komputer yang dipakai adalah jaringan secara nirkabel; (2) pembahasan mencakup bagaimana membatasi pemakaian waktu/kuota per *user*; (3) untuk meningkatkan keamanan ber-*internet,* jaringan nirkabel akan menerapkan metode *EAP authentication* dengan *RADIUS Servers*; (4) perancangan aplikasi antarmuka untuk manajemen pengguna *hotspot*, biling, dan pembuatan *voucher*; (5) evaluasi dilakukan menggunakan beberapa *network tools* yang ada, yaitu *RADIUS Servers(freeRADIUS), Firefox browser, iperf.*

METODE

Perancangan

Perancangan aplikasi manajemen *hotspot* ini menggunakan metode terstruktur, dengan beberapa tahapan diantaranya pemodelan DFD (diagram konteks dan DFD zero), dan Normalisasi data.

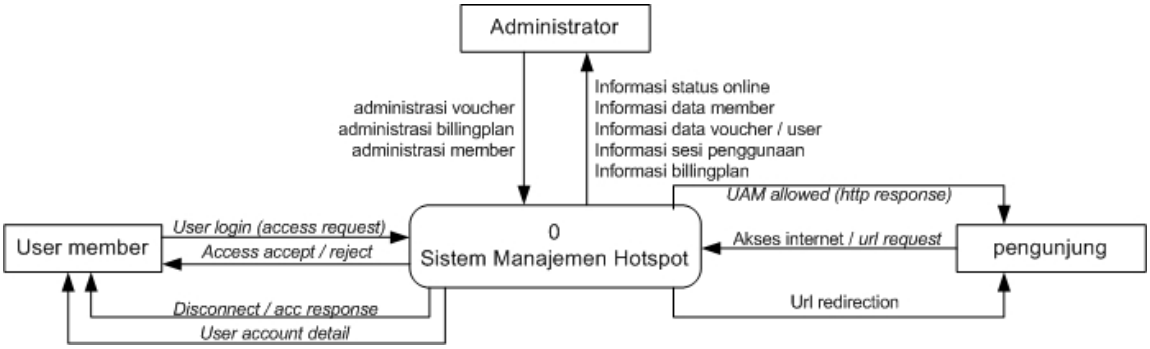
Data Flow Diagram (DFD)

Data Flow Diagram merupakan alat pembuatan model yang digunakan untuk menggambarkan sistem sebagai suatu jaringan proses fungsional yang dihubungkan satu sama lain dengan aliran data, baik secara manual maupun komputerisasi. DFD ini menunjukkan aliran

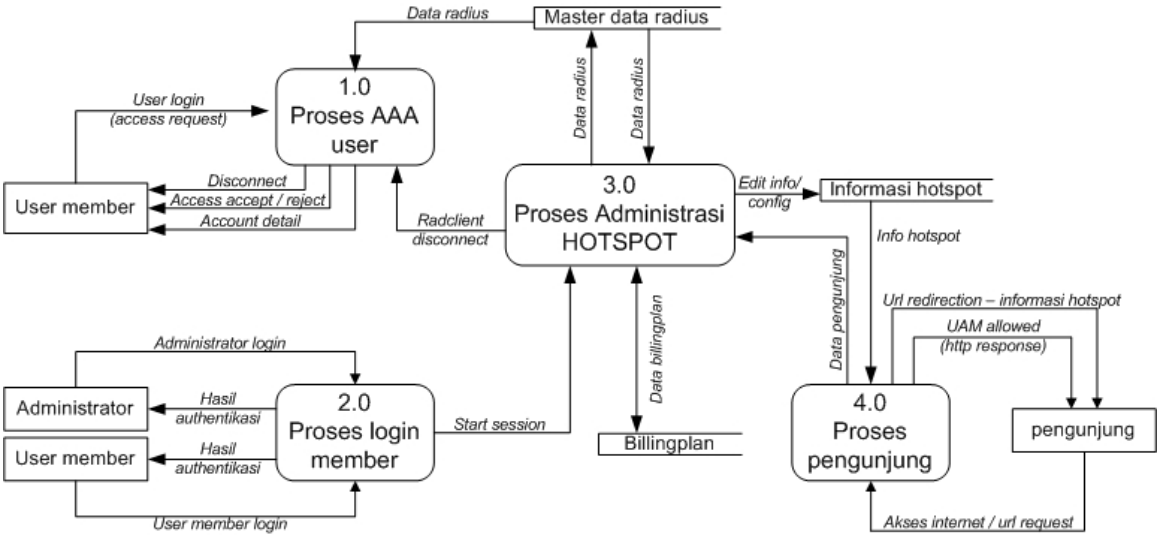
informasi masuk dan keluar pada sistem dengan konsep dekomposisi dimana subbagian dapat dijelaskan lebih rinci pada tingkatan di bawahnya.

Diagram Konteks merepresentasikan keseluruhan sistem sebagai sebuah proses yang berinteraksi dengan lingkungannya, dengan demikian akan memberikan gambaran umum mengenai sistem tersebut. Pada perancangan sistem manajemen *hotspot*, diagram konteks meliputi tiga entitas luar (terminator) yang menerima masukan dan memberi masukan terhadap sistem, yaitu *user* member atau pengguna *hotspot*, administrator, dan pengunjung *hotspot*. Diagram konteks sistem manajemen *hotspot* ditunjukkan pada Gambar 1.

Diagram nol (*zero*) merupakan dekomposisi dari diagram konteks untuk penjabaran aliran data yang lebih terperinci dengan proses utama pada sistem. Dalam sistem manajemen *hotspot* ini terdapat empat proses utama yang dijabarkan dari diagram konteks, yaitu proses AAA pengguna (Autentikasi, Autorisasi, dan Akuntansi), proses *login administrator/member*, proses administrasi *hotspot*, dan proses pengunjung *hotspot*. Diagram nol sistem manajemen *hotspot* ditunjukkan pada Gambar 2.



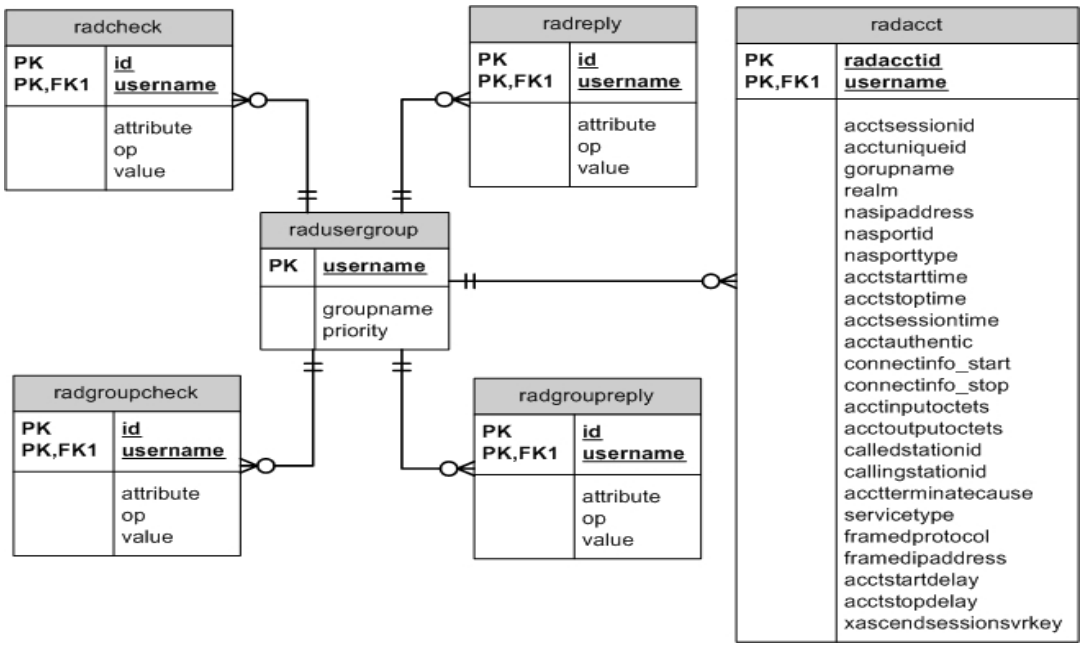
Gambar 1. DFD konteks.



Gambar 2. DFD *zero*.

Skema Basis Data Relational

Proses pemetaan akan menghasilkan tabel-tabel beserta hubungan relasinya antar entitas. Diagram E-R ditunjukkan pada Gambar 3.



Gambar 3. Model relasional basis data.

Mekanisme Authentikasi User

Web page *login* ini digunakan sebagai perantara antara *user* dan RADIUS *server* di mana RADIUS client sebagai medianya, dengan memiliki *uamsecret* untuk authorisasi (Gambar 4).

Cara kerja *server* autentikasi ini sebagai berikut, pertama setiap *user* yang masuk kedalam *wireless hotspot* dan mencoba untuk browsing internet, semuanya akan di-*redirect* ke halaman *login user*name dan *password* yang dibuat oleh CoovaChilli. Ketika *username* dan password telah dimasukkan, CoovaChilli akan menanyakan ke FreeRADIUS apakah ada *username* dan *password* yang dimasukkan oleh *user*. FreeRADIUS akan mencocokkan *username* dan *password* yang dimasukkan melalui *database* yang dibuat di MySQL. Jika ada, FreeRADIUS akan mengecek batas pemakaian *user* tersebut. Jika *user* tersebut valid, FreeRADIUS akan melaporkan kepada CoovaChilli dan CoovaChilli akan memberikan izin sehingga *user* bisa *surfing* di internet. Jika tidak, FreeRADIUS akan melaporkan ke CoovaChilli bahwa *user*name dan *password* yang dimasukkan tidak mendapatkan hak akses ke jaringan. ChilliSpot tidak akan membuka akses untuk *surfing* internet, dan akan meminta *login* ulang dan begitu seterusnya.

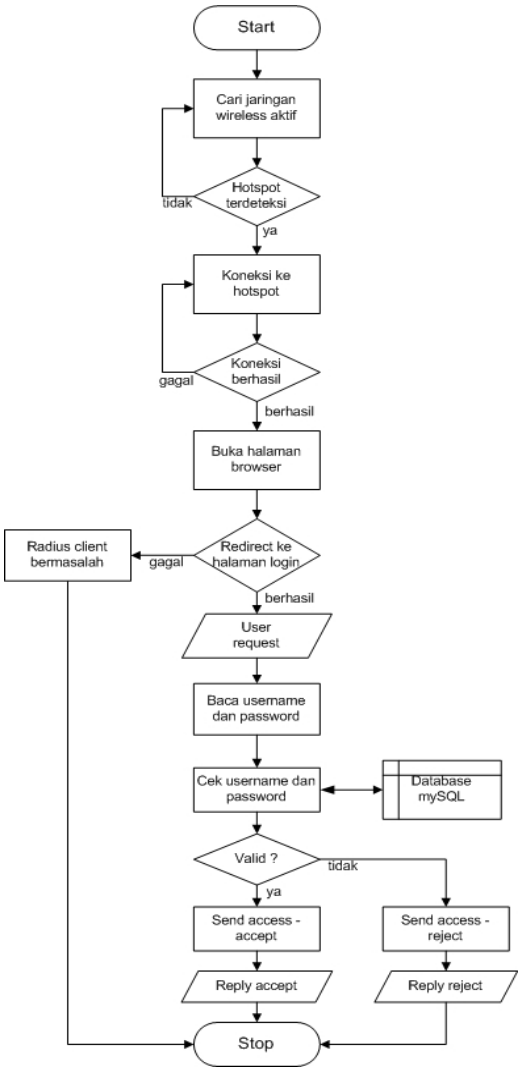
Evaluasi

Evaluasi Pemakaian *Bandwidth*

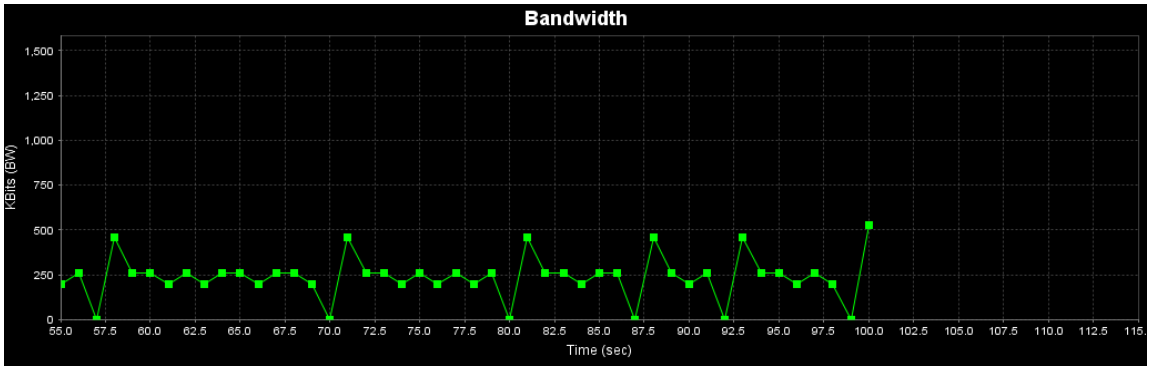
Untuk membuktikkan bahwa pembatasan pemakaian *bandwidth* bekerja dengan baik, dilakukan pengambilan data selama 100 detik setiap percobaan dalam bentuk grafik (Gambar 5-7).

Evaluasi Batas Pemakaian

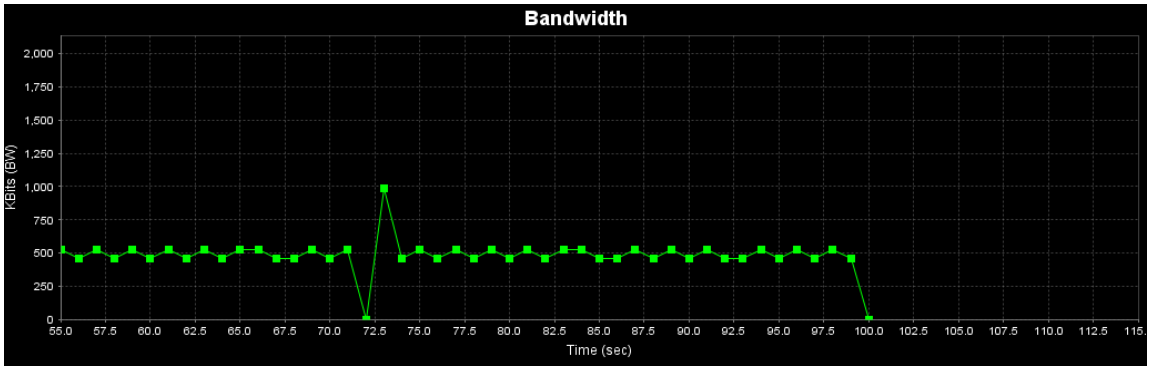
Berikut adalah halaman yang akan muncul ketika *user* telah mencapai batas maksimum pemakaian (Gambar 8 – 10).



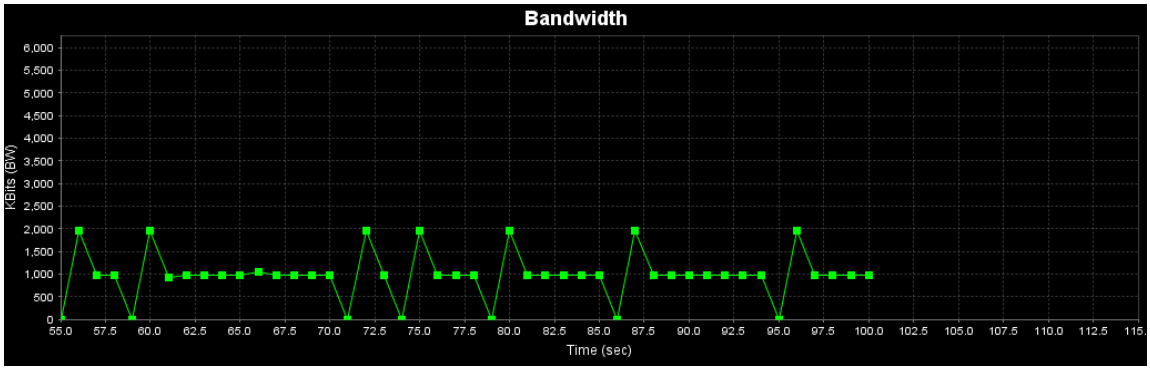
Gambar 4. Mekanisme autentikasi *user*.



Gambar 5. Hasil percobaan pembatasan *bandwidth* 256kbps.



Gambar 6. Hasil percobaan pembatasan *bandwidth* 512kbps.



Gambar 7. Hasil percobaan pembatasan *bandwidth* 1024kbps.

Evaluasi Keseluruhan Sistem

Dari hasil pengujian sistem autentikasi pengguna *wireless* berbasis radius *server* untuk konektivitas cukup efisien dan praktis. Untuk terkoneksi ke *hotspot* seorang *user* membutuhkan waktu kurang dari sepuluh detik. Sistem autentikasi ini juga memungkinkan adanya monitoring dan manajemen *bandwidth* baik *upload* maupun *download*. Sistem autentikasi ini juga relatif aman bagi data pengguna, karena memanfaatkan sistem tunelling seperti VPN yang akan mengenkrip semua data yang dikirim *client* maupun *server hotspot*. Semua data yang dikirim via *wireless* semuanya akan dienkrip sehingga lebih aman untuk aksi penyadapan. Sistem autentikasi ini juga memudahkan bagi pengguna untuk terkoneksi ke *hotspot* tanpa adanya prosedur yang berbelit-belit (seperti meminta *password* WEP/WPA KEY).

PENUTUP

Kesimpulan yang didapat dari hasil implementasi adalah sebagai berikut: (1) sistem manajemen *hotspot* ini dapat melakukan berbagai skema pembatasan akses termasuk diantaranya pembatasan berdasarkan lama penggunaan waktu (time based) dan jumlah penggunaan paket data (volume based) dengan pembatasan bandwidth untuk tiap pengguna. Skema pembatasan didefinisikan di dalam modul RADIUS sesuai dengan atribut yang didukung oleh perangkat; (2) dengan penggunaan sistem berbasis RADIUS, mekanisme autentikasi dapat dilakukan lebih mudah dengan kontrol akses secara terpusat pada satu *server*, dibandingkan dengan melakukan pengaturan

keamanan pada tiap-tiap perangkat jaringan; (3) pengaturan kecepatan *bandwidth* setiap pengguna cukup stabil; (4) pengaturan pembatasan pemakaian waktu/kuota per *user* dapat berfungsi dengan baik.

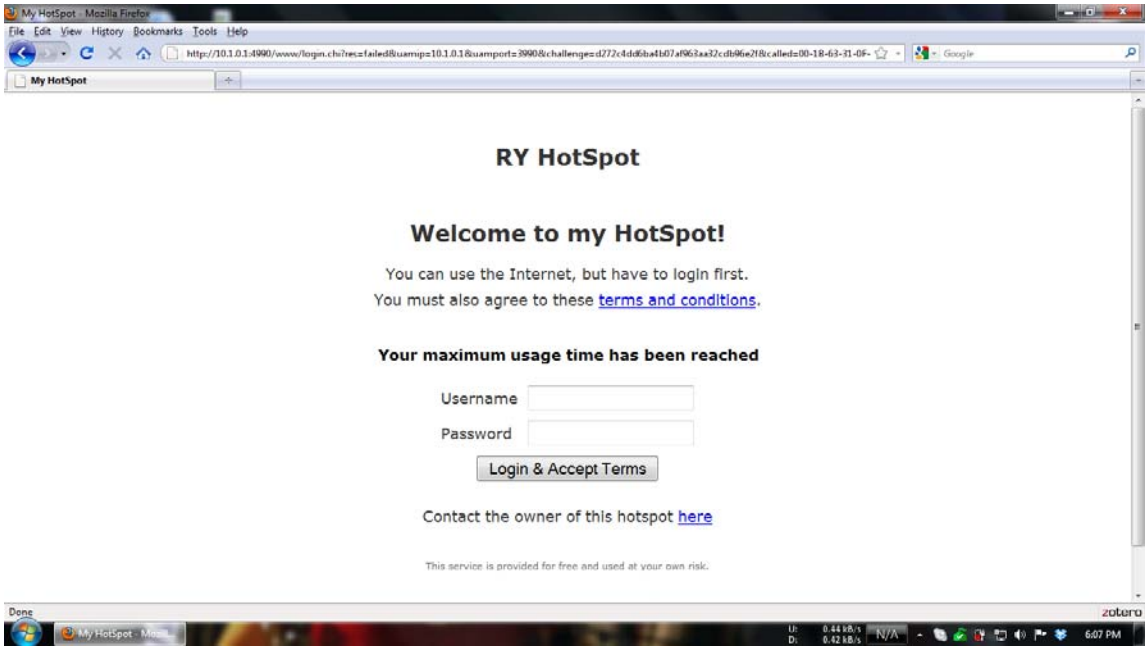
DAFTAR PUSTAKA

Burdick, William. (2005). *Extensible Authentication Protocol (EAP)*. Diakses dari http://searchmobilecomputing.techtarget.com/definition/Extensible-Authentication-Protocol.

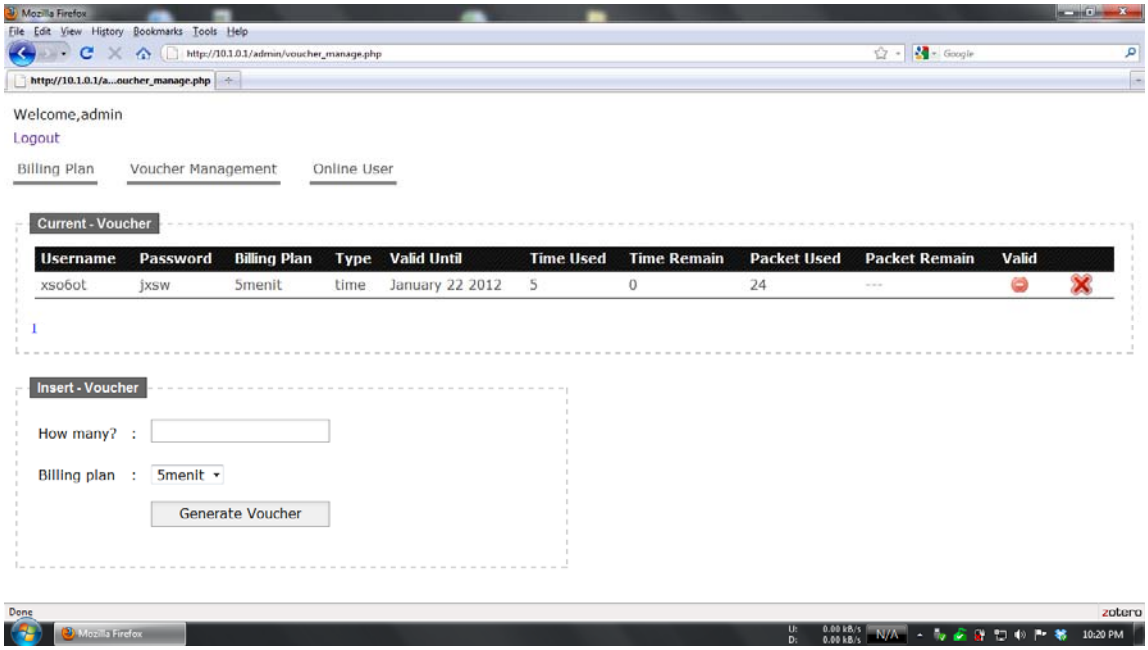
Felix Ivan, dkk. (2010). *Redesign Jaringan Komputer pada Binus Center Untuk Meningkatkan Perfoma dengan Menerapkan Quality of Service pada Layer 3 dan Keamanan pada Jaringan Nirkabel* Skripsi S1. Jurusan Teknik Informatika. Jakarta: Universitas Bina Nusantara.

Teare, D. (2008). *Authorized self-study Guide Designing for Cisco Internetwork Solutions*, (edisi ke-2). Indianapolis: Cisco Press.

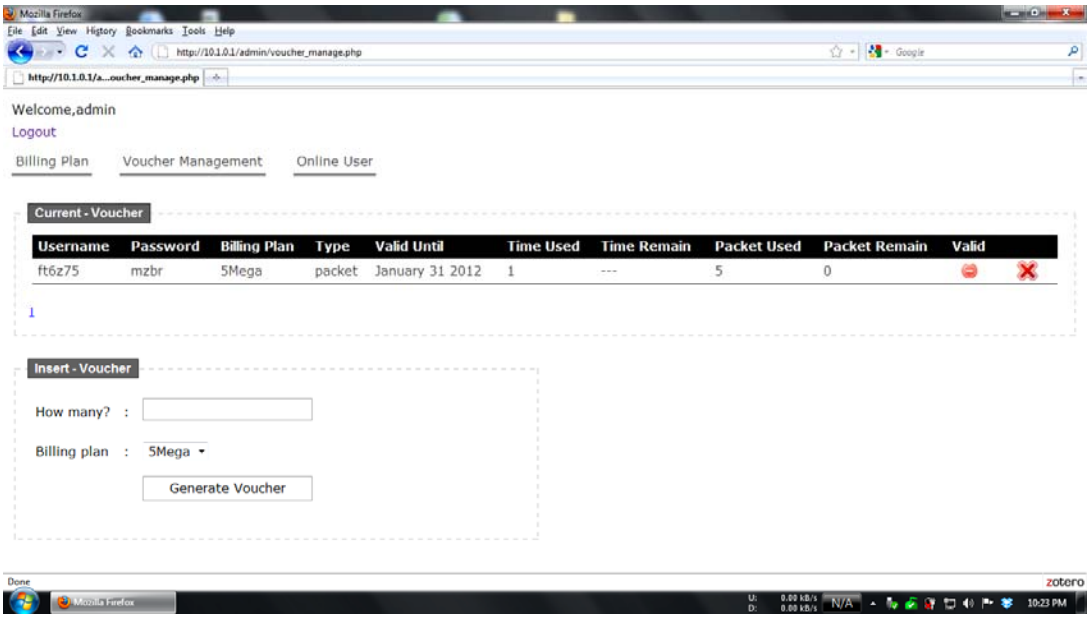
APPENDIX



Gambar 8. Halaman ini merupakan halaman ketika *user* telah mencapai batas pemakaian *bandwidth*.



Gambar 9. Hasil dari pembatasan pemakaian kuota waktu selama lima menit.



Gambar 10. Hasil dari pembatasan pemakaian kuota paket data sebanyak lima MByte.