Sistem Manajemen *Hotspot* Berbasis Kuota Waktu dan Paket Data

Abdullah Faqih[1], Adian Fatchur Rochim[2], R. Rizal Isnanto[2]
Jurusan Teknik Elektro Fakultas Teknik Universitas Diponegoro

Abstract

Ease offered by wireless technology has resulted in many emerging hotspot area that provides Internet access service. Issues to be faced in the provision of Internet access with wireless LAN is about management of Internet hotspot usage as well as its billing system. Therefore, it require an authentication mechanism to guard hotspot from unauthorized users, one of them is by using freeRadius server which is based on RADIUS (Remote Authentication Dial-in User Service). freeRadius server is then connected to a captive portal Chillispot as an authentication portal for user. Application design and development using DFD modelling which is implemented in PHP as a middleware to build graphical interface and application logic for the management of hotspots. With the utilization of RADIUS-based hotspot management system, it can authenticate registered user which have an access to hotspot, and will reject any unauthorized user. Access control can be made based on the length of usage time (time based) and the use of data packet (volume based) with bandwidth restrictions for each user. Hotspot transaction management is done using prepaid system by voucher and postpaid with membership. Management of users, billing plan, vouchers, and operator can be done more easily and flexible, with the convenience of a centralized web-based control panel which can be accessed from various operating systems and browsers.

Keywords : Internet, hotspot, radius, authentication, 802.1X

1. PENDAHULUAN

1.1 Latar Belakang Masalah

Kemudahan yang ditawarkan oleh teknologi *wireless* LAN mengakibatkan semakin banyak bermunculan area hotspot yang menyediakan jasa akses Internet. Namun kemudahan yang diberikan teknologi nirkabel akan menghadapkan pengelola pada masalah yang berkaitan dengan pengaturan penggunaan jasa Internet serta sistem manajemennya. Isu keamanan juga menjadi salah satu hal yang dipertimbangkan dalam penggunaan fasilitas *hotspot* di area publik karena sifatnya yang terbuka. Oleh sebab itu maka dibutuhkan suatu sistem pengelolaan *hotspot* yang memiliki mekanisme autentikasi pengguna layanan *hotspot*, untuk menjaga agar *hotspot* tidak digunakan oleh pihak yang tidak berhak.

1.2 Tujuan

Tujuan pembuatan Tugas Akhir ini adalah mengimplementasikan mengimplementasikan sistem autentikasi pengguna *hotspot wireless* LAN berbasis RADIUS (802.1X) dengan pembatasan akses berdasarkan kuota waktu pemakaian dan kuota paket data. Sehingga dari sisi pengguna jasa Internet memiliki kemudahan dalam melakukan hubungan ke Internet, dan dari sisi administrator akan memiliki fasilitas untuk membatasi hak akses terhadap jasa Internet yang diberikan, memantau serta mengontrol pengguna jasa Internet, dan melakukan hal administratif lainnya

1.3 Batasan Masalah

Pembatasan masalah pada tugas akhir ini melingkupi sebagai berikut :

1. Prinsip kerja sistem manajemen *hotspot* berbasis FreeRadius *Server*.
2. Prosedur instalasi dan konfigurasi *server* FreeRadius dan Chillispot berikut infrastruktur jaringan *hotspot.*
3. Perancangan sistem manajemen *hotspot* ini menggunakan *webserver* Apache versi 2.2, bahasa pemrograman skrip PHP versi 5, dan database *server* MySQL versi 5 di dalam *platform* sistem operasi Linux Ubuntu Server 8.04 LTS.
4. Perancangan aplikasi antarmuka untuk manajemen pengguna *hotspot*, biling, dan pembuatan *voucher*.
5. Tidak membahas karakteristik sinyal *wireless* dan antena.
6. Tidak membahas proses enkripsi dan manajemen kunci sertifikat pada autentikasi *wireless client.*

2. LANDASAN TEORI

2.1 *Wireless Hotspot*

Wireless atau teknologi nirkabel merupakan media transmisi pengganti media kabel yang menggunakan gelombang radio elektromagnetik untuk berkomunikasi antara satu dengan lainnya. Perkembangan teknologi nirkabel ini kemudian digunakan dalam impelementasi jaringan lokal nirkabel atau biasa dikenal dengan WLAN (*Wireless Local Area Network)*. Maraknya penggunaan WLAN ini kemudian mengakibatkan banyak bermunculan layanan akses Internet *hotspot. Wireless Hotspot* merupakan sebuah area terbuka yang memungkinkan seseorang bisa melakukan akses Internet secara nirkabel, baik secara gratis ataupun dengan melakukan pembayaran untuk jasa penggunaan.

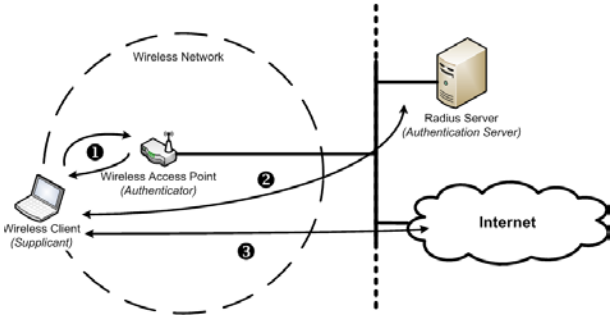
2.2 Standar 802.1X

IEEE 802.1x merupakan protokol kontrol akses jaringan (*network access control*) berbasis port yang memanfaatkan karakteristik infrastruktur LAN IEEE 802 untuk menyediakan media autentikasi dan autorisasi perangkat yang terhubung pada port LAN yang memiliki karakteristik koneksi *point to point*, dan mencegah akses jika autentikasi dan autorisasi gagal[5]. Tujuan standar IEEE

[1] Mahasiswa Teknik Elektro Universitas Diponegoro
[2] Dosen Teknik Elektro Universitas Diponegoro

802.1x adalah untuk menghasilkan kontrol akses, autentikasi, dan manajemen kunci untuk *wireless* LAN.

IEEE 802.1x terdiri dari tiga bagian, yaitu pengguna atau *client* yang akan diautentikasi disebut *wireless node* (*supplicant*), server yang melakukan autentikasi atau disebut *Network Access Server (NAS)*, dan perangkat yang menghubungkan dua bagian tersebut disebut *Authenticator*, dalam hal ini berupa *access point*. *Authentication Server* yang digunakan adalah *Remote Authentication Dial-In User Service* (RADIUS) server dan digunakan untuk autentikasi pengguna yang akan mengakses *wireless* LAN.



Gambar 2.1 Mekanisme Autentikasi 802.1X [6]

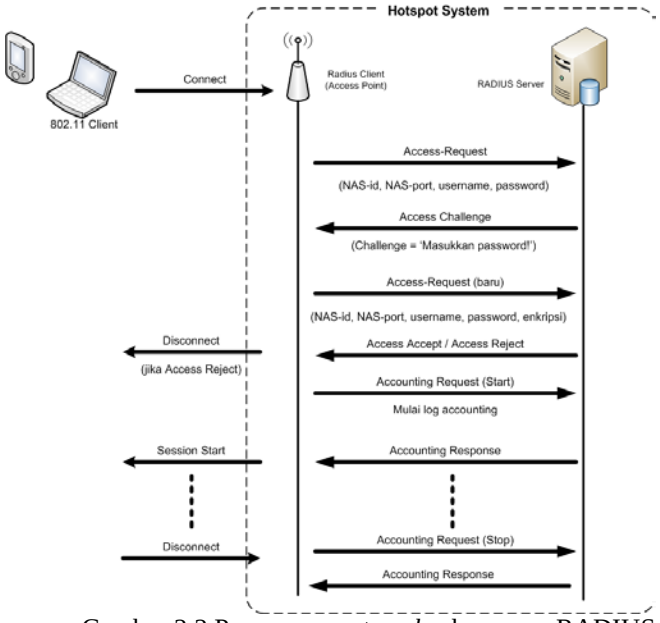
2.3 FreeRADIUS *Server*

RADIUS (*Remote Access Dial-in User Service*) merupakan suatu protokol *client-server* yang dikembangkan untuk mekanisme akses kontrol yang memeriksa dan mengautentikasi pengguna berdasarkan protokol AAA [5].

1. Autentikasi *(Authentication)*
   Yaitu proses memeriksa identitas dari seorang pengguna untuk memastikan apakah *user* tersebut benar telah terdaftar dalam jaringan *wireless* tersebut..
2. Autorisasi *(Authorization)*
   Berperan sebagai suatu kumpulan aturan yang membatasi fasilitas apa yang boleh dan dapat diakses oleh seorang pengguna yang telah terautentikasi.
3. Akuntansi *(Accounting)*
   Suatu proses pencatatan dari awal saat seorang pengguna mengakses jaringan dalam suatu *hotspot*.

FreeRADIUS merupakan salah satu server RADIUS modular berbasis sumber terbuka yang memiliki banyak fitur dan kemampuan yang tidak kalah dengan RADIUS server komersial. Salah satu buktinya adalah sudah mendukung beberapa *Access Point* (AP) / *Network Access Server* (NAS) yang umum, dan mendukung berbagai macam sumber data pengguna dari file teks, LDAP, SQL (MySQL, Oracle, PostgreSQL, MSQL). FreeRADIUS juga dapat berjalan di berbagai sistem operasi, seperti Linux, FreeBSD, OpenBSD, OSF, Sun Solaris, dan lain sebagainya.

Gambar 2.2 menjelaskan proses permintaan akses dari sebuah *client* Radius kepada RADIUS server (*Authentication Server)* melalui proses AAA pada suatu NAS (*Network Access Server).*



Gambar 2.2 Proses *request-reply* akses *user* RADIUS

2.4 *Captive Portal* Chillispot

Chillispot merupakan *captive portal* berbasis sumber terbuka yang difungsikan sebagai *Wireless LAN Access Point Controller*. Digunakan untuk mengautentikasi pengguna dari sebuah jaringan nirkabel. Mendukung sistem login dengan basis web yang merupakan standar untuk *public hotspot*. Chillispot bertindak sebagai portal yang akan memaksa pengguna menuju halaman autentikasi / halaman login pengguna disaat terjadi permintaan akses terhadap suatu alamat (*HTTP Request*). Setiap paket data yang melalui *captive portal* akan ditahan sebelum pengguna berhasil diautentikasi. Informasi login pengguna kemudian diteruskan kepada *Authentication Server* (RADIUS) untuk diperiksa apakah seorang pengguna benar-benar berhak untuk mengakses *hotspot.* Jika suatu pengguna berhasil diautentikasi sebagai pengguna yg berhak, maka paket data akan diteruskan ke pengguna dan penggunaan akan dicatat oleh modul akuntansi RADIUS.

2.5 PHP dan MySQL

PHP merupakan bahasa *server side scripting* yg didesain khusus untuk web, dimana proses eksekusi program secara sepenuhnya dijalankan di sisi server[8]. Dalam struktur pemrogramannya, bahasa skrip PHP disisipkan ke dalam kode HTML (*Hypertext Markup Language*) yang akan dijalankan disaat halaman web tersebut diakses oleh *client*. Disaat sebuah halaman web yang mengandung skrip PHP diminta melalui HTTP *Request* oleh pengguna, modul pemroses PHP akan menerjemahkannya dan mengeksekusinya, kemudian *web server* menyampaikannya kepada *web browser client* dalam halaman HTML.

MySQL merupakan salah satu RDBMS (*Relational Database Management System*) di bawah lisensi GPL yang bersifat sumber terbuka dan bebas untuk didistribusikan[8]. MySQL menggunakan bahasa SQL (*Structured Query*

Language) yang merupakan bahasa query standar yang digunakan luas. MySQL umum digunakan dalam aplikasi berbasis web karena sifatnya yang gratis, stabil dan cepat, kemudahan penggunaan, *cross-platform* berjalan baik di UNIX maupun *platform* Windows, serta dukungan yang luas.

Dalam penggunaannya dengan *server* RADIUS, PHP dipergunakan untuk membangun logika dan antarmuka aplikasi, sedangkan MySQL untuk menyimpan data autentikasi yang berisi data login para pengguna, data autorisasi yang berisi hak akses dari pengguna, dan data-data akuntansi yang mencatat penggunaan setiap *user*. Data ini kemudian akan dipergunakan oleh modul sql FreeRadius untuk mengatur pembatasan akses pengguna.

3. PERANCANGAN SISTEM

3.1 Kebutuhan Sistem

Perancangan Sistem Manajemen *Hotspot* dilakukan dengan melihat kebutuhan akan hal-hal berikut ini.

1. Sistem dapat menyediakan informasi mengenai *hotspot*, cara mengakses, dan lain sebagainya.
2. Sistem dapat menyediakan mekanisme autentikasi yang aman melalui halaman login.
3. Sistem dapat melakukan pengelolaan terhadap pengguna, mengatur akses sesuai hak aksesnya masing-masing, dan masa berlaku akses.
4. Sistem dapat membatasi akses pengguna berdasarkan lama waktu penggunaan.
5. Sistem dapat mengatur dan membatasi kuota unduh dan unggah dengan manajemen *bandwidth*.
6. Sistem dapat memantau pengguna yang sedang *online* dan memutuskan koneksi pengguna jika diperlukan.
7. Sistem dapat memantau sesi penggunaan dari tiap pengguna.
8. Sistem dapat menyediakan informasi mengenai waktu penggunaan, kuota paket data penggunaan, dan *bandwidth* dalam bentuk grafis.
9. Sistem dapat membuat *voucher* akses dan mencetaknya.

3.2 Rancangan Aplikasi Manajemen *Hotspot*

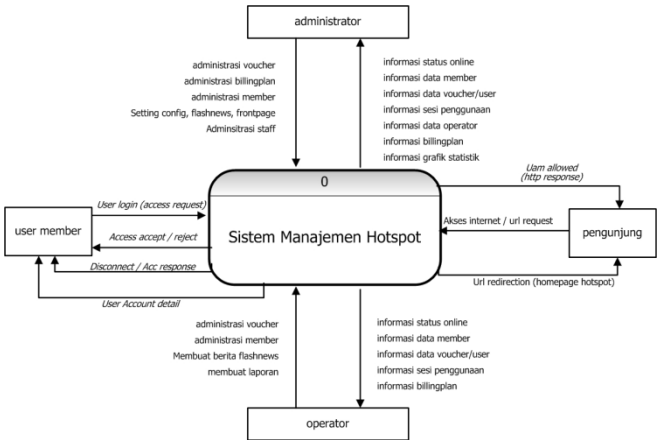
Perancangan Aplikasi Manajemen *Hotspot* ini menggunakan metode terstruktur, dengan beberapa tahapan diantaranya pemodelan DFD (diagram konteks, DFD *zero*, dan DFD detil), Diagram E-R, dan Normalisasi data.

3.3 *Data Flow Diagram* (DFD)

Diagram Aliran Data 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[3]. DFD ini menunjukkan aliran informasi masuk dan keluar pada sistem dengan konsep dekomposisi dimana subbagian dapat dijelaskan lebih rinci pada tingkatan di bawahnya

3.3.1 Diagram Konteks

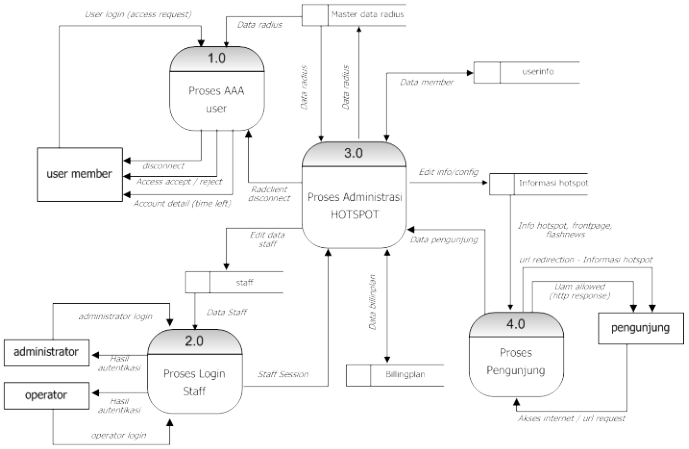
Diagram Konteks merepresentasikan keseluruhan sistem sebagai sebuah proses yang berinteraksi dengan lingkungannya, dengan demikian akan memberikan gambaran umum mengenai sistem tersebut. Pada perancangan sistem manajemen *hotspot*, diagram konteks meliputi empat entitas luar (*terminator)* yang menerima masukan dan memberi masukan terhadap sistem, yaitu *user member* atau pengguna *hotspot*, administrator, operator, dan pengunjung *hotspot.* Gambar 3.1 menunjukkan skema DFD Konteks.



Gambar 3.1 DFD Konteks

3.3.2 Diagram *Zero*

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 4 proses utama yang dijabarkan dari diagram konteks, yaitu proses AAA pengguna (Autentikasi, Autorisasi, dan Akuntansi), proses *login staff*, proses administrasi *hotspot*, dan proses pengunjung *hotspot.* Diagram nol sistem manajemen hotspot ditunjukkan pada gambar 3.2.



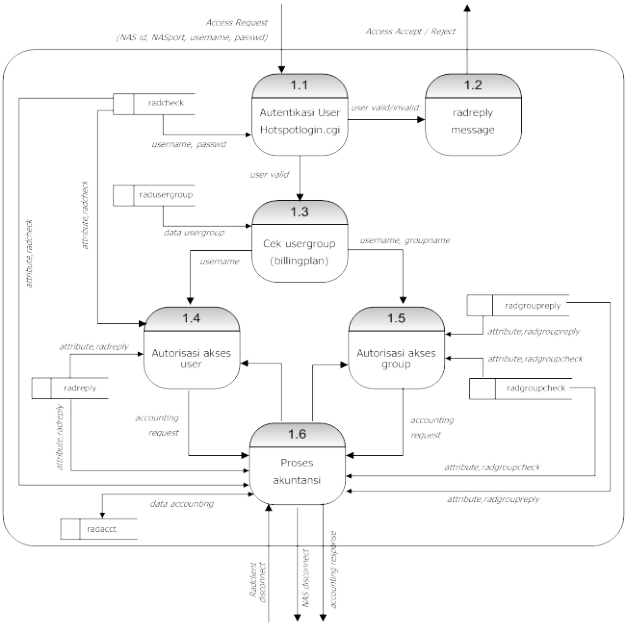
Gambar 3.2 DFD Zero

3.3.3 Diagram Level 1

Diagram detil level 1 merupakan dekomposisi dari diagram nol untuk menjelaskan proses utama pada sistem ke dalam sub-proses yang lebih rinci.

1. DFD Level 1 Proses 1 (Proses AAA *User*)

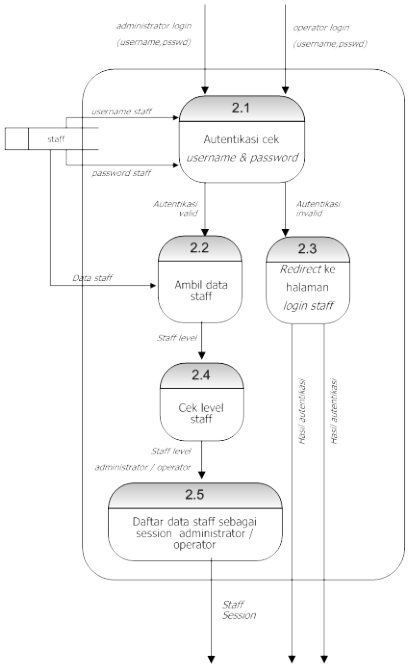
Menjelaskan lebih rinci mengenai proses Autentikasi, Autorisasi, dan Akuntansi dari pengguna *hotspot.* Proses ini berhubungan langsung antara freeradius *server*, NAS, dan basisdata melalui modul *rlm_sql.* DFD *level* 1 proses 1 ditunjukkan pada Gambar 3.3.



Gambar 3.3 DFD *Level* 1 – Proses 1

2. DFD Level 1 Proses 2 (Proses *Login* Staf)

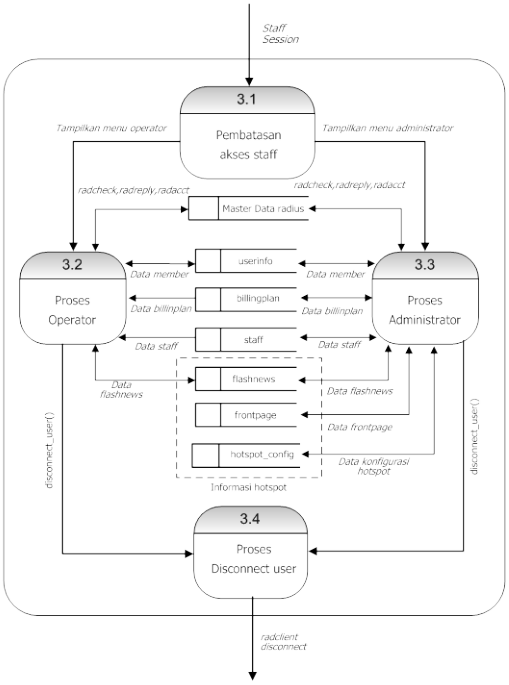
Diagram ini menjelaskan lebih terperinci proses *Login* Staf pada level zero yang berkaitan dengan autentikasi staf dalam pengelolaan *hotspot*. Proses induk didekomposisi menjadi 5 proses seperti ditunjukkan pada Gambar 3.4.



Gambar 3.4 DFD Level 1 Proses 2

3. DFD Level 1 Proses 3 (Proses administrasi *hotspot)*

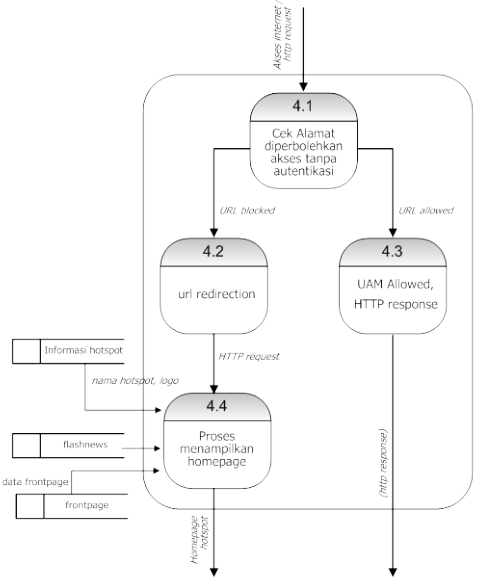
Diagram ini menjabarkan proses administrasi *hotspot* menjadi 5 subproses seperti pada gambar 3.5 berikut.



Gambar 3.5 DFD Level 1 proses 3

4. DFD Level 1 Proses 4 (Proses Pengunjung)

Diagram ini merupakan penjabaran lebih detil pada proses pengunjung pada diagram level zero. Gambar 3.6 menggambarkan DFD level 1 – proses 4.



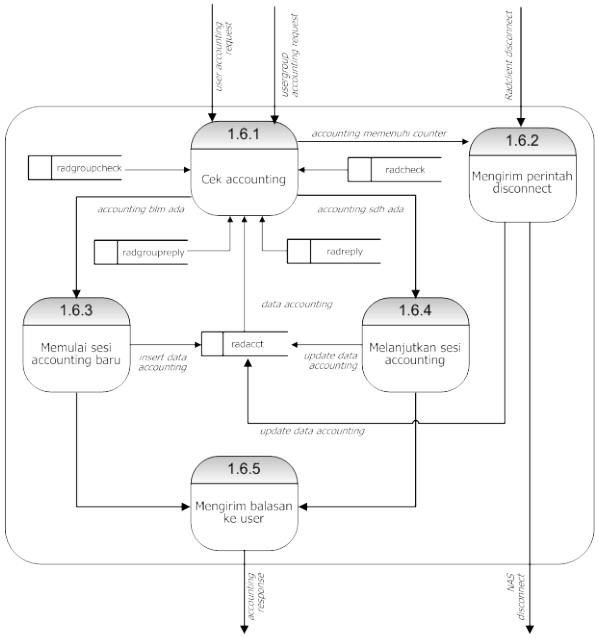
Gambar 3.6 DFD Level 1 proses 4

3.3.4 Diagram Level 2

Diagram ini merupakan dekomposisi dari diagram level 1 karena masih perlu dijabarkan lebih terperinci.

1. DFD Level 2 Proses 1.6

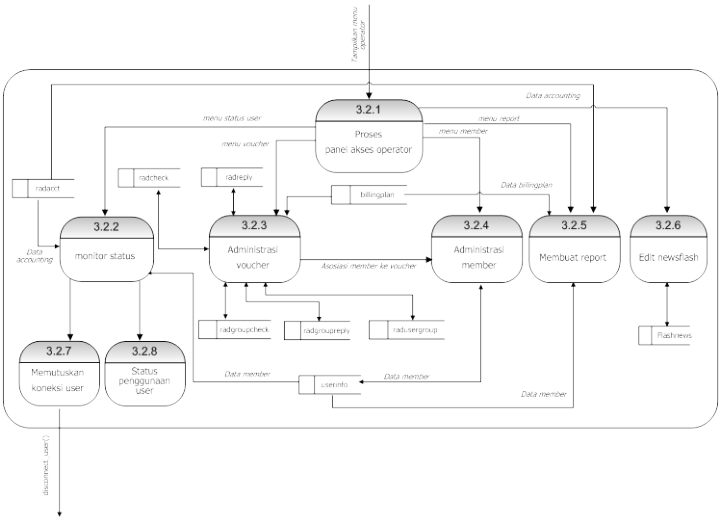
Diagram ini menggambarkan secara rinci proses akuntansi pada proses utama proses AAA *user*, dimana proses induk 1.6 dijabarkan lagi menjadi 5 subproses yang ditunjukkan Gambar 3.7.



Gambar 3.7 DFD Level 2 proses 1.6

2. DFD Level 2 Proses 3.2

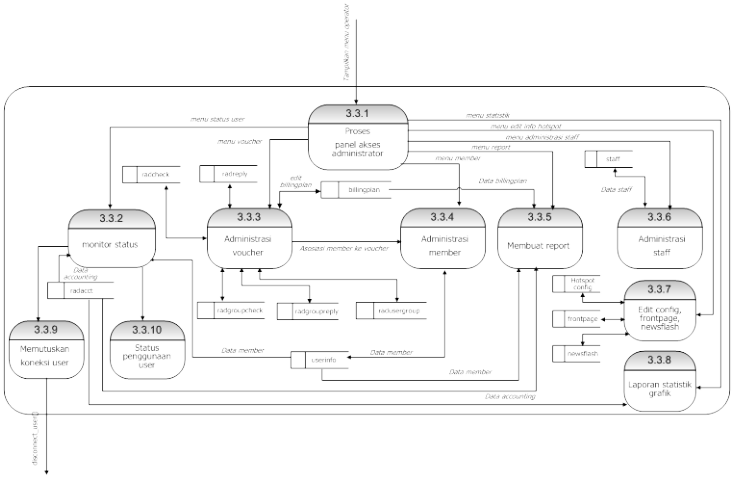
Diagram ini menjelaskan lebih rinci proses Administrasi *hotspot* oleh operator dengan membaginya ke dalam 8 subproses. Gambar 3.8 menunjukkan penjabaran proses 3.2.



Gambar 3.8 DFD Level 2 Proses 3.2

3. DFD Level 2 Proses 3.3

Diagram ini menjelaskan lebih rinci proses Administrasi *hotspot* oleh administrator dengan membaginya ke dalam 8 subproses yang ditunjukkan pada Gambar 3.9.



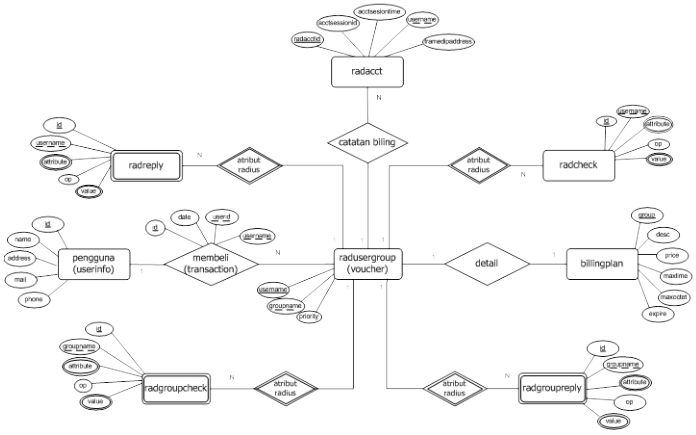
Gambar 3.9 DFD Level 2 Proses 3.3

3.4 Perancangan Basisdata

Perancangan basis data dalam sistem manajemen *hotspot* ini meliputi beberapa tahapan, diantaranya perancangan secara konseptual dengan menggunakan pemodelan diagram E-R (*Entity Relationship*), kemudian memetakannya menjadi model relasional melalui perancangan secara logikal. Model relasional yang dihasilkan kemudian diperbaiki melalui proses normalisasi agar tidak menimbulkan duplikasi dan redundansi data.

3.4.1 Diagram E-R (*Entity Relationship Diagram*)

Diagram E-R merupakan diagram konseptual yang menggambarkan hubungan antar entitas berikut dengan atribut-atribut yang terkait di dalam sebuah sistem[3]. Masing-masing entitas menampilkan atributnya, baik atribut yang mengandung kata kunci (*primary key)*, dan atribut lain yang dijadikan referensial. Gambar 3.10 menunjukkan model diagram E-R pada sistem manajemen *hotspot*.



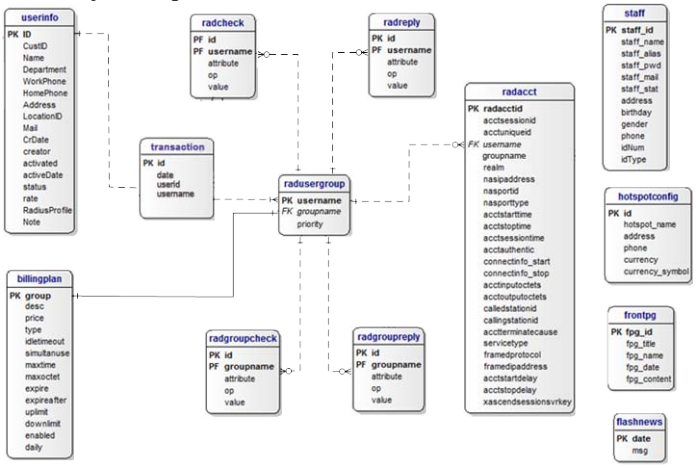
Gambar 3.10 Model Diagram E-R

3.4.2 Skema Basis data Relasional

Basis data yang telah dibuat secara konseptual kemudian dipetakan menjadi skema basis data relasional sehingga didapatkan skema logika dari basis data. Hal ini

akan mempermudah dalam implementasi ke dalam *DBMS* yang akan digunakan.

Proses pemetaan akan menghasilkan tabel-tabel beserta hubungan relasinya antar entitas. Diagram E-R ditunjukkan pada Gambar 3.11.



Gambar 3.11 Model Relasional Basis data

3.4.3 Normalisasi basisdata

Setelah perancangan data secara logikal, dilakukan proses normalisasi agar tidak terdapat pengulangan informasi pada basis data sehingga akan membentuk struktur tabel yang efektif. Hasil dari proses normalisasi adalah himpunan-himpunan data dalam bentuk normal (*normal form).*

4. IMPLEMENTASI DAN PENGUJIAN

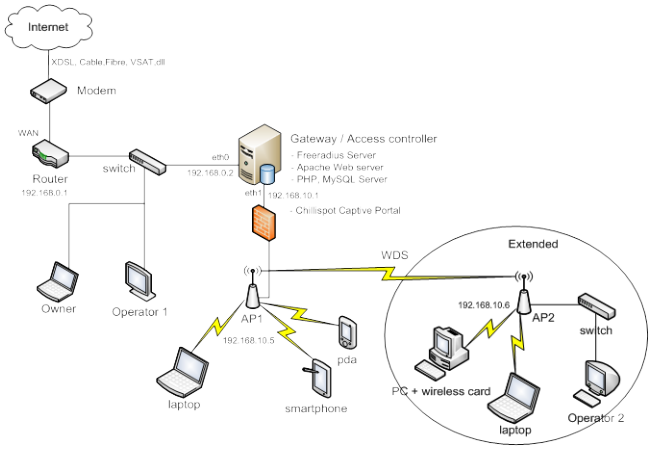
4.1 Implementasi Sistem

Tahap ini mendeskripsikan penerapan perangkat lunak ke dalam tampilan-tampilan sistem sebelum kemudian dilakukan pengujian.

4.2 Batasan Implementasi

Batasan implementasi ditinjau dari 2 aspek yaitu aspek perangkat keras dan aspek perangkat lunak. Dari segi perangkat keras, sistem manajemen *hotspot* menggunakan perangkat dasar berupa koneksi Internet beserta modem, PC Server dengan sistem operasi Linux dan 2 buah *ethernet card*, *wireless access point*, dan perangkat jaringan lainnya jika dibutuhkan untuk pengembangan jaringan. Sedangkan dari aspek perangkat lunak, lingkungan implementasi dilakukan pada *Web Server* Apache, PHP 5, MySQL 5.0, *Server* FreeRadius 2, dan *captive portal* Chillispot.

Gambar 4.1 menunjukkan implementasi infrastruktur jaringan yang digunakan sistem manajemen *hotspot.*



Gambar 4.1 Infrastruktur jaringan *hotspot*

4.3 Implementasi Antarmuka

Hasil perancangan aplikasi kemudian diimplementasikan melalui pengkodean menjadi antarmuka halaman web yang dipergunakan oleh pengunjung sebagai portal mengakses *hotspot*, dan digunakan pengelola untuk memanajemen *hotspot*. Antarmuka aplikasi manajemen *hotspot* ini meliputi beberapa modul diantaranya modul pengunjung sebagai halaman depan dari *hotspot* dan portal *login* pengguna, dan antarmuka bagi *administrator/operator* yang digunakan untuk panel kontrol pengelolaan *hotspot.*

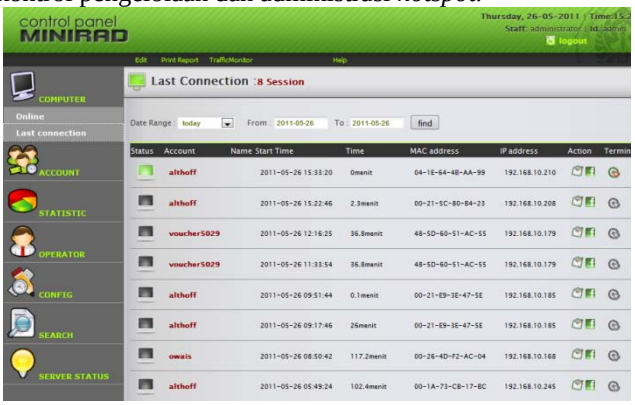
Gambar 4.2 menunjukkan antarmuka halaman depan pengunjung.

Gambar 4.2 Antarmuka halaman depan pengunjung

Gambar 4.3 menunjukkan antarmuka portal login pengunjung. Portal login ini yang akan menghubungkan *captive portal* chillispot dengan server Freeradius.

Gambar 4.3 Antarmuka login pengguna

Gambar 4.4 menunjukkan antarmuka halaman panel kontrol pengelolaan dan administrasi *hotspot.*



Gambar 4.4 Antarmuka panel kontrol pengelola

4.4 Pengujian Sistem

Pengujian perangkat lunak didefinisikan sebagai proses sistem operasi atau komponen menurut kondisi tertentu, pengamatan atau pencatatan hasil dan mengevaluasi beberapa aspek sistem atau komponen[3].

Penelitian ini menggunakan teknik pengujian fungsional atau disebut juga pengujian kotak hitam (*black-box*). Teknik pengujian ini bertujuan untuk menunjukkan fungsi perangkat lunak tentang cara beroperasinya, apakah pemasukan data keluaran telah berjalan sebagaimana yang diharapkan. Tahapan pengujian yang dilakukan meliputi pengujian *alpha* dan pengujian beta. Pengujian *alpha* merupakan tahap pengujian yang dilakukan pada lingkungan pengembangan untuk pengujian pengguna. Pengujian *beta* merupakan tahap pengujian yang bersifat terbuka diluar lingkungan pengembang dengan melibatkan siapa saja sebagai pengguna perangkat lunak.

4.4.1 Kasus Uji (*Test Case*)

Untuk mendapatkan kesesuaian hasil implementasi dengan spesifikasi kebutuhan perangkat lunak, maka dilakukan perancangan serangkaian uji kasus untuk menemukan kesalahan pada perangkat lunak[3].

Tabel 4.2 Kasus uji dan kriteria sukses

No	Skenario Pengujian	Kriteria sukses
1	Modul chillispot, DHCP, *url redirection*, halaman pengunjung.	Sistem secara otomatis dapat memberikan ip pada *client*, dan memindahkan halaman *browser web* pada halaman pengunjung. Semua informasi tentang hotspot, konten dan berita dapat muncul di halaman utama.
2	Autentikasi pengunjung	Sistem dapat melakukan autentikasi yang aman pada pengguna yang berhak mengakses *hotspot.*
3	Administrasi pengguna	Sistem dapat mengelola dan mengatur hak akses sesuai hak akses masing-masing.
4	Pembatasan akses berbasis waktu	Sistem dapat membatasi akses sesuai dengan pembatasan lama waktu penggunaan.
5	Pembatasan akses berbasis kuota data	Sistem dapat membatasi akses jika jumlah kuota unduh dan unggah memenuhi batas yang ditentukan.
6	Panel pemantauan pengguna yang sedang *online*	Sistem dapat memantau secara *realtime* pengguna yang sedang menggunakan akses, dan dapat memutuskan koneksi jika diperlukan.
7	Informasi penggunaan tiap pengguna	Sistem dapat memantau sesi penggunaan, masa aktif, dan informasi jumlah pemakaian tiap pengguna.
8	Grafik dan statistik	Sistem dapat membuat grafik statistik penggunaan dan informasi *hotspot* lainnya.
9	Pencetakan *voucher*	Sistem dapat membuat dan melakukan pencetakan *voucher*
10	Modul Laporan	Sistem dapat membuat laporan terperinci mengenai *hotspot*

4.4.2 Analisis Hasil Pengujian

Secara umum, hasil pengujian yang diperoleh adalah sebagai berikut:

1. Sistem berhasil memberikan alamat ip secara otomatis pada *client* yang terhubung dengan jaringan *hotspot*, dan memindahkan halaman browser menuju halaman pengunjung jika pengguna mengakses sembarang alamat.
2. Sistem berhasil melakukan autentikasi terhadap pengguna yang hanya diperbolehkan untuk mengakses *hotspot*, dan melakukan penolakan terhadap pengguna yang tidak berhak.
3. Sistem berhasil melakukan pengelolaan terhadap pengguna, mengatur akses sesuai hak aksesnya masing-masing, dan masa berlaku akses.
4. Sistem berhasil melakukan pembatasan akses pengguna berdasarkan lama waktu penggunaan dengan memutuskan koneksi saat waktu akses atau masa aktif telah habis.
5. Sistem berhasil melakukan pengaturan pembatasan kuota unduh dan unggah masing-masing pengguna dan dapat membatasi *bandwidth*.
6. Sistem berhasil melakukan pemantauan terhadap pengguna yang sedang *online* dan memutuskan koneksi pengguna.
7. Sistem berhasil melakukan pemantauan sesi penggunaan dari tiap pengguna dalam kurun waktu tertentu dan mencetaknya sebagai laporan.
8. Sistem berhasil menampilkan grafik statistik mengenai *hotspot.*

9. Sistem berhasil membuat *voucher* akses dan mencetaknya.

5. PENUTUP

5.1 Kesimpulan

1. Penggunaan freeRADIUS sebagai server autentikasi dapat mengakomodasi kebutuhan untuk autentikasi dan autorisasi pengguna akses *hotspot* sehingga mencegah akses oleh pihak yang tidak berhak. Pencatatan penggunaan akses oleh modul akuntansi RADIUS dipergunakan lebih lanjut untuk perhitungan biling dan kontrol akses pengguna.
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. 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.
4. Sistem autentikasi dengan menggunakan freeRADIUS dan *captive portal* Chillispot menyediakan proses autentikasi yang cukup aman untuk sistem *hotspot* dengan metode pengamanan SSL dan *uamsecret hash* untuk penyandian *session* antara *client* dan *server* autentikasi. Namun pengujian keamanan yang dilakukan hanya sebatas pada mekanisme autentikasi dan tidak dilakukan pada keamanan keseluruhan sistem *hotspot.*

5.2 Saran

1. Diharapkan sistem manajemen *hotspot* dapat dikembangkan lebih lanjut dengan skema pembatasan akses yang lebih beragam bagi pengguna misal pembatasan kuota tiap hari, pembatasan kecepatan yang akan turun setelah memenuhi kuota paket data, dan lain-lain sehingga pengguna dapat lebih leluasa memilih paket penggunaan Internet.
2. Perlunya dilakukan penelitian lebih lanjut mengenai keamanan sistem *hotspot* dari bahaya serangan penyusup yang berupa *access spoofing*, pencurian *session*, *dictionary attack*, dan eksploitasi kelemahan lainnya. Perlu juga dilakukan analisa mengenai metode pengamanan EAP yang tepat maupun penyandian yang paling baik untuk diimplementasikan dalam jaringan nirkabel.
3. Perlu ditambahkan informasi status dan detail informasi pengguna serta mekanisme pemberitahuan untuk mengingatkan pengguna saat batas nominal penggunaan atau masa berlaku pengguna akan habis, sehingga pengguna dapat mengendalikan penggunaan aksesnya.
4. Perlu dilakukan perubahan pada skema basisdata yang digunakan freeRADIUS, dan modifikasi pada modul sql freeRADIUS sehingga basisdata yang digunakan untuk data AAA memenuhi relasi dan *referential integrity*.

DAFTAR PUSTAKA

[1] Hassel, J. 2002. *RADIUS*. O'Reilly.

[2] IEEE Std 610.12. 1990. *IEEE Standard Glossary of Software Engineering Terminology*. IEEE.

[3] IEEE Std 829. 2008. *IEEE Standard for Software and System Test Documentation*. IEEE.

[4] IEEE Std 802.1X . 2001. *IEEE Standard for Local and Metropolitan area networks – Port-Based Network Access Control*. IEEE.

[5] Interlink Networks. 2004. *Securing Hotspots with RADIUS*. Interlink Networks,Inc.

[6] Rigney, C., S. Willens , A. Rubens, and W. Simpson. 2000. *Remote Authentication Dial In User Service (RADIUS)*. IETF RFC 2865.

[7] Strand, L. *802.1X Port-Based Authentication HOWTO*.http://tldp.org/HOWTO/html_single/8021X-HOWTO/. Januari 2011

[8] Welling, L., and L.Thomson. 2005. *PHP and MySQL Web Development-Third Edition.* Sams Publishing.

BIODATA PENULIS

Abdullah Faqih (L2F306001)
dilahirkan di Surabaya, 1 Mei 1984.
Mahasiswa Teknik Elektro bidang konsentrasi Teknik Informatika dan Komputer, Universitas Diponegoro Semarang.

Email : ab_faqih@yahoo.co.id

Menyetujui dan mengesahkan,

Pembimbing I

Adian Fatchur Rochim, ST, MT.
NIP. 197302261998021001
Tanggal .....

Pembimbing II

R.Rizal Isnanto, S.T., M.M., M.T.
NIP. 197007272000121001
Tanggal .....