LAPORAN KERJA PRAKTEK

AUTENTIKASI PENGGUNA *WIRELESS* UIN SUNAN KALIJAGA DENGAN CAPTIVE PORTAL BERBASIS RADIUS SERVER

Diajukan sebagai salah satu syarat

untuk memperoleh gelar sarjana Teknik Informatika

Disusun oleh:

Nama : Muhammad Asfarudin

NIM : 09650051

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
YOGYAKARTA

2012

PENGESAHAN LAPORAN KERJA PRAKTEK

PENGESAHAN LAPORAN KERJA PRAKTEK

AUTENTIKASI PENGGUNA *WIRELESS* UIN SUNAN KALIJAGA DENGAN CAPTIVE PORTAL BERBASIS RADIUS SERVER

Disusun Oleh

Nama : Muhammad Asfarudin

NIM : 09650051

Telah diseminarkan pada tanggal : 1 Juni 2012

Pembimbing,

M. Taufiq Nuruzzaman, S.T., M.Eng.

NIP. 19791118 200501 1 003

Penguji,

Aulia Faqih Rifa'I, M.Kom.

NIP. 19860306 201101 1 009

Mengetahui,

a.n. Dekan

Ketua Program Studi

Agus Mulyanto, S.Si., M.Kom.

NIP. 19710823 199903 1 003

KATA PENGANTAR

Puji dan syukur kami panjatkan ke hadirat Allah SWT, karena hanya atas berkat dan rahmat-Nya, sehingga Laporan Kerja Praktek yang berjudul "AUTENTIKASI PENGGUNA *WIRELESS* UIN SUNAN KALIJAGA DENGAN CAPTIVE PORTAL BERBASIS RADIUS SERVER" dapat diselesaikan dengan baik dan tepat waktu. Adapun tujuan penulisan laporan ini adalah untuk memenuhi persyaratan dalam menyelesaikan Kerja Praktek Program Studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta.

Penyusunan laporan ini tidak terlepas dari bantuan beberapa pihak, oleh karena itu penulis hendak mengucapkan terima kasih kepada :

1. Orang tua tercinta, yang telah memberikan doa, cinta, sayang, semangat, dukungan, dan motivasi selama melakukan studi.
2. Bapak Agus Mulyanto, S.Si., M.Kom. selaku Kepala Program Studi Teknik Informatika.
3. Bapak M. Taufiq Nuruzzaman, S.T., M.Eng. selaku Dosen Pembimbing Kerja Praktek.
4. Bapak Agung Fatwanto, S.Si., M.Kom., Ph.D. selaku Dosen Pembimbing Lapangan Kerja Praktek.
5. Abdul Hafidh Sidiq, teman satu kelompok Kerja Praktek yang telah berjuang untuk menyelesaikan Kerja Praktek ini bersama-sama.

6. Teman-teman Teknik Informatika 2009, yang selalu berbagi canda, tawa, dan kesedihan bersama selama ini.
7. Staff PKSI, yang dengan sabar membantu dan memberi dukungan selama kerja praktek.
8. Semua pihak yang tidak dapat disebutkan satu per satu yang terlibat dalam penyusunan Laporan Kerja Praktek ini sehingga dapat selesai dengan baik.

Akhir kata, penulis menyadari bahwa pelaksanaan kerja praktek dan penyusunan laporan ini belumlah sempurna. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan. Semoga penyusunan laporan ini bermanfaat bagi semua pihak dan perkembangan Prodi Teknik Informatika UIN Sunan Kalijaga khususnya.

Yogyakarta, 14 Mei 2012

Penulis

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 Latar Belakang

Universitas Islam Negeri Sunan Kalijaga saat ini sudah menyediakan layanan *free hotspot* yaitu sebuah area dimana pada area tersebut tersedia koneksi internet *wireless* yang dapat diakses melalui *Notebook* maupun PDA. Dengan adanya layanan tersebut mahasiswa dosen maupun karyawan yang berada dalam area tersebut dapat menikmati fasilitas internet dengan *gadget* mereka secara geratis.

Layanan tersebut dapat diakses secara langsung oleh siapa saja melalui *Notebook, PDA* dan perangkat lain yang mendukung penggunaan *wifii* di area *hotspot*. Hal inilah yang akhirnya menjadi masalah dikemudian hari seperti penggunaan fasilitas oleh pihak-pihak diluar civitas akademika UIN Sunan Kallijaga sampapi dengan masalah yang berkaitan dengan *bandwidth*.

Oleh sebab itu diperlukan sistem *autentikasi*, *user management* dan *monitoring* pada jaringan *hotspot* UIN Sunan Kallijaga untuk meminimalisasi atau menghilangkan sama sekali masalah tersebut. Dengan sistem tersebut diharap hanya civitas akademik UIN Sunan Kalijaga saja yang dapat mengakses fasilitas *free hotspot* tersebut.

1.2 Batasan Masalah Kerja Praktek

Agar pembahasan nantinya tidak menyimpang dari tugas kerja praktek yang dikerjakan maka permasalahan akan dibatasi pada beberapa aspek :

1. Penulis hanya membahas tentang *captive portal*.
2. *Captive portal* akan dibuat dengan menggunakan *free radius* dan *chillispot*.

1.3 Tujuan Kerja Praktek

Tujuan dari kerja praktek ini adalah mendesain dan mengimplementasikan autentikasi pada jaringan *hotspot* di UIN Sunan Kalijaga dengan menggunakan *captive portal*. Diharapkan dengan adanya *captive portal* tersebut penggunaan fasilitas *hotspot* bisa dioptimalkan.

1.4 Manfaat Kerja Praktek

Manfaat yang dapat diambil dari kerja praktek ini adalah:

1. Mempermudah dalam *management* dan *monitoring* jaringan *hotspot* di UIN Sunan Kalijaga.
2. Membatasi pemakaian *hotspot* karena hanya *user* yang memiliki *account* saja yang bisa menggunakan fasilitas tersebut.
3. Pengguna *wifii* tidak perlu mendaftarkan setiap *gadget* yang akan digunakan kepada admin.
4. Manfaat umum yaitu dapat digunakan sebagai acuan dalam penelitian berikutnya.

BAB II

TEMPAT KERJA PRAKTEK

2.1 Gambaran Umum Instansi

Pusat Komputer dan Sistem Informasi (PKSI) Universitas Islam Negeri Sunan Kalijaga, sebagaimana tercantum dalam Keputusan Menteri Agama Republik Indonesia Nomor 390 Tahun 2004 tanggal 3 September 2004 adalah gabungan dari dua lembaga sebelumnya yaitu Pusat Komputer dan Sistem Informasi. Pusat Komputer (PUSKOM) adalah salah satu dari dua Unit Pelaksana Teknis atau unsure penunjang IAIN Sunan Kalijaga (Statuta IAIN Sunan Kalijaga Yogyakarta Tahun 2001 Pasal 121 ayat 3). Unit Pelaksana Teknis lainnya adalah Perpustakaan. Sistem Informasi, semula merupakan sub bagian dari bagian Perencanaan dan Sistem Informasi (PSI).

Secara yuridis, Pusat Komputer sudah ada sejak diberlakukannya Keputusan Menteri Agama RI Nomor 385 Tahun 1993 tanggal 29 Desember 1993, tentang Organisasi dan Tata Kerja IAIN Sunan Kalijaga Yogyakarta. Pasal 60 memuat tentang Pusat Komputer yang menjelaskan bahwa Pusat Komputer adalah unsure penunjang IAIN Sunan Kalijaga di bidang komputer (pasal 60 ayat 1). Pusat Komputer dipimpin oleh seorang kepala, yang ditunjuk di antara pranata komputer senior di lingkungan Pusat Komputer yang bertanggungjawab kepada Rektor dan pembinaannya dilakukan oleh Pembantu Rektor I (pasal 60 ayat 2).

Pusat Komputer sebagai unit pelaksana teknis atau unsur penunjang di IAIN Sunan Kalijaga dimuat juga dalam Keputusan Menteri Agama RI Nomor 399 Tahun 1993 tentang statute Institut Agama Islam Negeri Sunan Kalijaga Yogyakarta.

Dalam upaya meningkatkan kualitas pelayanan administrasi di IAIN Sunan Kalijaga Yogyakarta diperlukan adanya sarana pendukung berupa pusat computer yang berkemampuan tinggi, teruji tingkat validitasnya, efisien, efektif dan didukung oleh keakuratan data, kecepatan pengolahan serta keamanan yang terjamin, maka Rektor, Prof. Dr. H. M. Atho Mudzhar, membentuk tim pelaksana penyiapan Program Pusat Komputer IAIN Sunan Kalijaga Yogyakarta.

Visi PKSI UIN Sunan Kalijaga Yogyakarta

Mewujudkan UIN Sunan Kalijaga Yogyakarta sebagai universitas digital (cyber campus)

Strategi

1. Otomasi proses administrasi (Akademik, Kemahasiswaan, dan Umum)
2. Digital lifestyle experience (e-learning, digital information dissemination, dan digital payment)

Prinsip PKSI UIN Sunan Kalijaga Yogyakarta

1. Layanan
   a. One Day Service
   b. One Stop Service

c. 3S (Senyum, Salam, Sapa)

2. Teknis

a. One Account for All Access

b. One Entry for All Database

c. ADAP (As Digital As Posible)

2.2 Ruang Lingkup Kerja Praktek

Ruang lingkup kerja praktek pada laporan ini menjelaskan tentang struktur organisasi dari PKSI UIN Sunan Kalijaga. Berikut ini adalah struktur organisasi PKSI UIN Sunan Kalijaga:

1. Kepala : Agung Fatwanto, S.Si, M.Kom, Ph.D
2. Divisi :
   a. Divisi Infrastruktur : Hendra Hidayat, S.Kom

      Angota : Rahmadhan Gatra, ST

   b. Divisi Pengembangan Sistem Informasi : Mustaqim, MT.

      Anggota :

      - Salim Athari, S.Kom
      - Adi Wirawan, S.Kom
      - Prihanto Dwi Rahmanto, S.Kom

   c. Divisi SDM : Ratna Windah Lestari, SIP

      Anggota : Rohyati, S.Ag.

   d. Divisi Media : M. Arif Wibisono

Anggota : Daru Prasetyawan, ST

e. Divisi Layanan IT : Siti Mutmainah, S.Kom

Anggota :

- Novi Praci Putri
- Mellyana Cahya Ningrum

Bendahara : Ratna Windah Lestari, SIP

BAB III

HASIL DAN PEMBAHASAN

3.1 Analisis

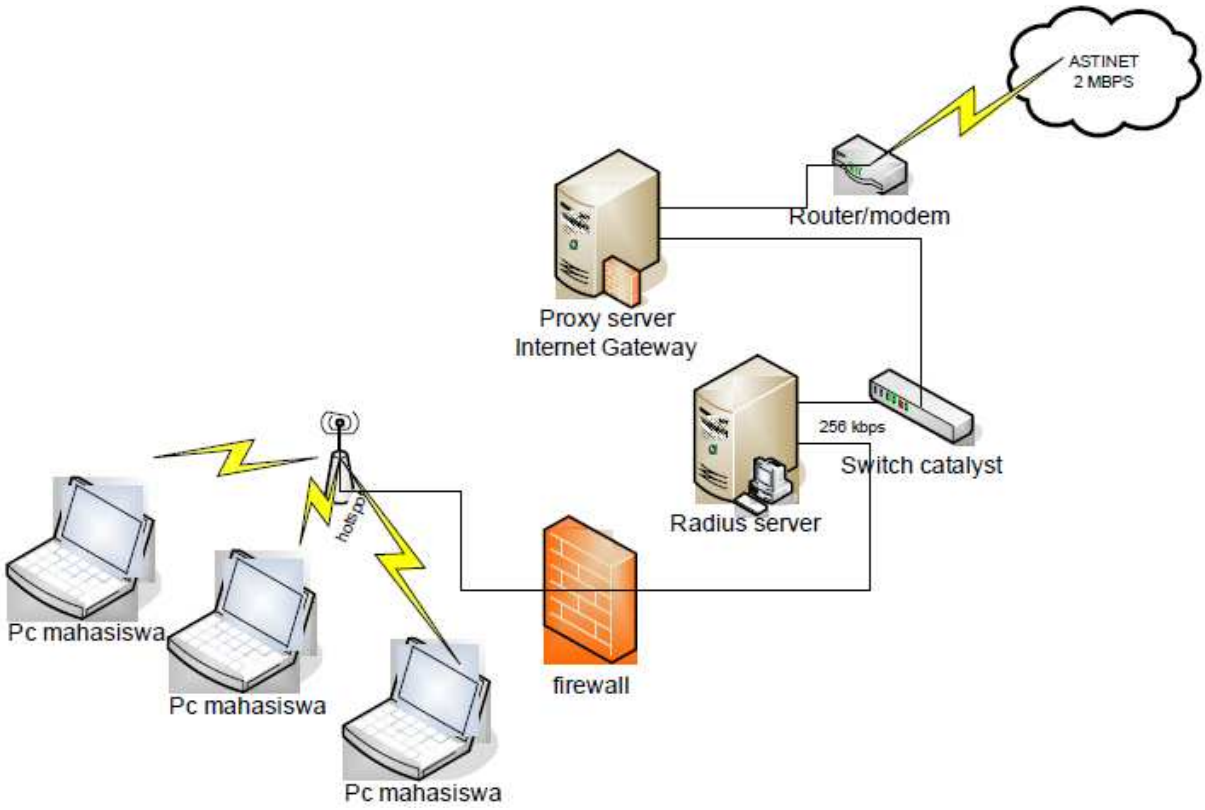
Tujuan dalam analisis ini adalah untuk mendapatkan informasi tentang apa yang dibutuhkan oleh sistem berdasarkan pada aspek kebutuhan *user* dan *admin*. Dari analisis tersebut didapat bahwa kebutuhan pengguna (*user*) adalah kemudahan dan kepraktisan dalam melakukan konektivitas internet dengan memanfaatkan fasilitas *free hotspot* yang disediakan oleh kampus Universitas Islam Negeri Sunan Kalijaga tanpa harus mendaftarkan setiap perangkat wireless yang ingin dikoneksikan. Kebutuhan Admin (*administrator*) pada sistem yang akan dikembangkan: 1) Membatasi *user* yang dapat menggunakan fasilitas internet terbatas pada user yang memiliki akun dan terdaftar sebagai civitas akademika UIN Sunan Kalijaga 2) Memberikan informasi *user* dan *bandwidth monitoring*; 3) Dapat membatasi penggunaan *bandwidth* terhadap *user*.

Berdasarkan hasil analisa tetrsebut, maka dapat dipaparkan spesifikasi kebutuhan sistem, sebagai berikut:

1. Layanan yang harus disediakan: autentifikasi, *monitoring*, dan *management user*.
2. Kriteria-kriteria yang harus dipenuhi: Autentifikasi *via* web login dengan menggunakan *web browser*, Media untuk *management user*.
3. Pembatasan penggunaan *bandwidth* terhadap *user wireless*

3.2 Kegiatan KP

Penilitian ini merupakan penelitian mengkaji tindak (*action research*) yang ditujukan untuk membuat *captive portal* berbasis *radius server* dengan topologi seperti di tunjukkan dalam Gambar 3.1.



Gambar 3.1

3.2.1 Pengembangan Captive Portal

Dalam pembuatan captive portal ini Sistem Operasi yang digunakan adalah Sistem Operasi Linux Ubuntu versi 11.10. Spesifikasi hardware untuk radius server yang digunakan sebagai berikut:

· Intel Pentium IV 2,4 GHz

· RAM 1024Mb

· *Hardisk* 40 Gb

· *Network Interface Card (NIC)* .

Pada Server tersebut diinstal beberapa software antara lain apache server, PHP, database MySQL, FreeRADIUS, CoovaChili, SSL dan Dialup Admin.

FreeRadius akan digunakan sebagai aplikasi yang akan melakukan fungsi-fungsi *radius server*. Dimana fungsi utamanya disebut sebagai protocol AAA. Protokol AAA (*Authentication, Authorization, Accounting*) adalah mekanisme bagaimana mengatur tata cara berkomunikasi, baik antara *client* ke domain-domain jaringan maupun antar *client* dengan domain yang berbeda dengan tetap menjaga keamanan pertukaran data (Warsito, 2004) . Protokol ini memiliki tiga fungsi utama (J.Hassel, 2002) :

a. **Autentikasi (*Authentication*)**; yaitu proses pengesahan identitas pengguna (*end user*) untuk mengakses jaringan. Proses ini diawali dengan pengiriman kode unik misalnya, *username*, *password*, *pin*, sidik jari oleh pengguna kepada server. Di sisi server, sistem akan menerima kode unik tersebut, selanjutnya membandingkan dengan kode unik yang disimpan dalam *database* server. Jika hasilnya sama, maka server akan mengirimkan hak akses kepada pengguna. Namun jika hasilnya tidak sama, maka server akan mengirimkan pesan kegagalan dan menolak hak akses pengguna
b. **Autorisasi (*Authorization*);** merupakan proses pengecekan wewenang pengguna, mana saja hak-hak akses yang diperbolehkan dan mana yang tidak.
c. **Pencatatan (*Accounting*);** merupakan proses pengumpulan data informasi seputar berapa lama *user* melakukan koneksi dan *billing time* yang telah dilalui

selama pemakaian. Proses dari pertama kali seorang user mengakses sebuah sistem, apa saja yang dilakukan user di sistem tersebut dan sampai pada proses terputusnya hubungan komunikasi antara user tersebut dengan sistem, dicatat dan didokumentasikan di sebuah database MySQL server.

3.2.2 Implementasi dan Pengujian

Dalam Penelitian Server Radius ini berfokus pada tiga aspek dalam mengontrol akses user, yaitu autentikasi, autorisasi dan pencatatan

11.2.2.1. Autentikasi (*Authentication*)

Proses pengesahan identitas pengguna (*end user*) untuk mengakses jaringan. Proses ini diawali dengan pengiriman kode unik *username* dan *password*) oleh pengguna kepada server. Di sisi server, sistem akan menerima kode unik tersebut, selanjutnya membandingkan dengan kode unik yang disimpan dalam *database* server. Jika hasilnya sama, maka server akan mengirimkan hak akses kepada pengguna. Namun jika hasilnya tidak sama, maka server akan mengirimkan pesan kegagalan dan menolak hak akses pengguna. Mekanisme Autentikasi dapat dilihat pada gambar 3.2

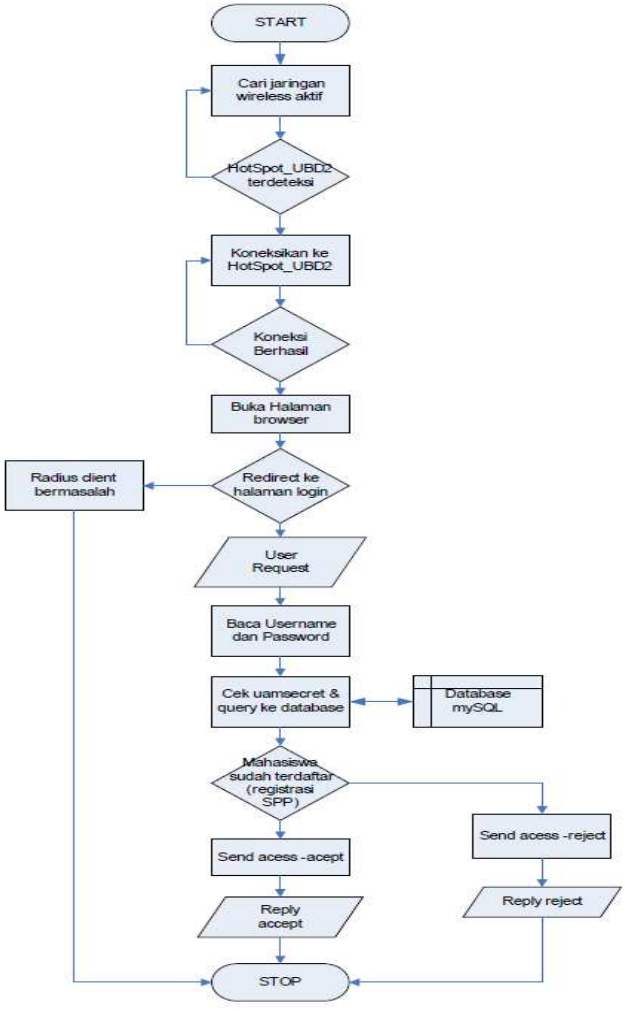
Server akan memeriksa apakah user adalah mahasiswa yang sudah terdaftar di dalam database. Jika sudah terdaftar maka akan ada pesan sukses.Jika tidak maka akan tampil kembali menu login. Di server sendiri akan mencatat semua transaksi login yang disimpan di var/log/freeradius/radius.log.

Untuk proses autentikasi dalam penelitian ini dibuat *script* untuk menambahkan user mahasiswa yang sudah registrasi (membayar SPP). Data mahasiswa yang sudah registrasi (membayar SPP) tersebut diambil dari data krs bidar yang

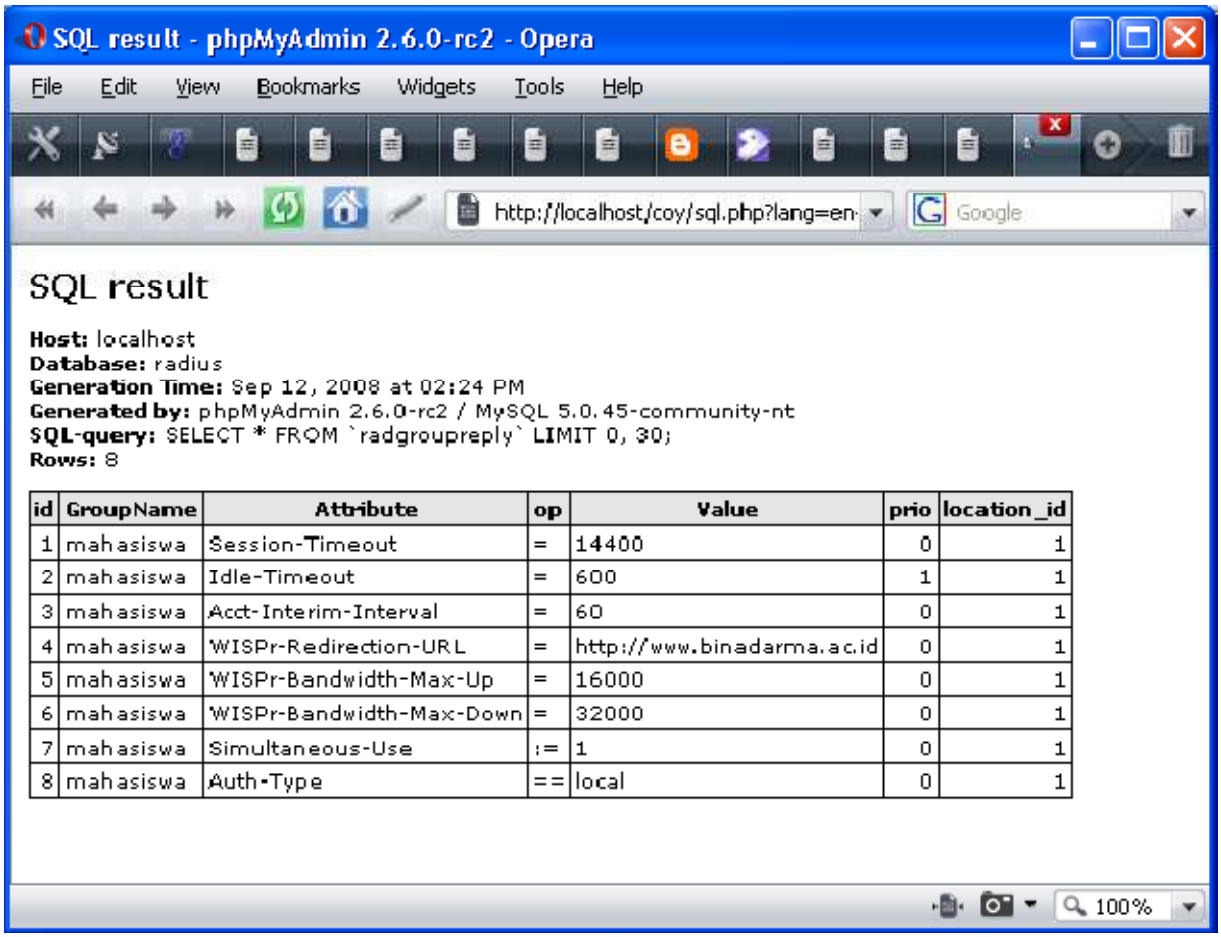
ditampung di tabel krs_aktif. Dengan menggunakan script php user tersebut di*generate* untuk disimpan di tabel userinfo, radcheck dan tabel usergroup.

11.2.2.2. Autorisasi (Authorization)

Merupakan proses pengecekan wewenang pengguna, mana saja hak-hak akses yang diperbolehkan dan mana yang tidak. Khusus untuk mahasiswa autorisasinya dibatasi di tabel radgroupreply (gambar 3.3)



Gambar 3.2 Mekanisme Autentikasi



id	GroupName	Attribute	op	Value	prio	location_id
1	mahasiswa	Session-Timeout	=	14400	0	1
2	mahasiswa	Idle-Timeout	=	600	1	1
3	mahasiswa	Acct-Interim-Interval	=	60	0	1
4	mahasiswa	WISPr-Redirection-URL	=	http://www.binadarma.ac.id	0	1
5	mahasiswa	WISPr-Bandwidth-Max-Up	=	16000	0	1
6	mahasiswa	WISPr-Bandwidth-Max-Down	=	32000	0	1
7	mahasiswa	Simultaneous-Use	:=	1	0	1
8	mahasiswa	Auth-Type	==	local	0	1

Gambar 3.3. Aturan otorisasi bagi user mahasiswa

Keterangan:

· Session-Timeout = 14400; berarti maksimal dalam 1 sesi login adalah 4 jam atau 14400 s.

· Idle-Timeout = 600; maksimal waktu idle adlah 600 s atau 10 menit

· Acct-Interim-Interval = 60; interval request adalah 60 s atau 1 menit

· WISPr-Redirection-URL; Halaman default yang akan dibuka.

· WISPr-Bandwidth-Max-Up = 16000; maksimal *upload* kecepatannya 16000 bps.

· WISPr-Bandwidth-Max-Down = 32000; maksimal kecepatan *download* 32000 bps.

· Simultaneous-Use := 1; hanya mengizinkan 1 orang 1 kali login saat bersamaan.

· Auth-Type == local; mengizinkan hanya autentikasi local

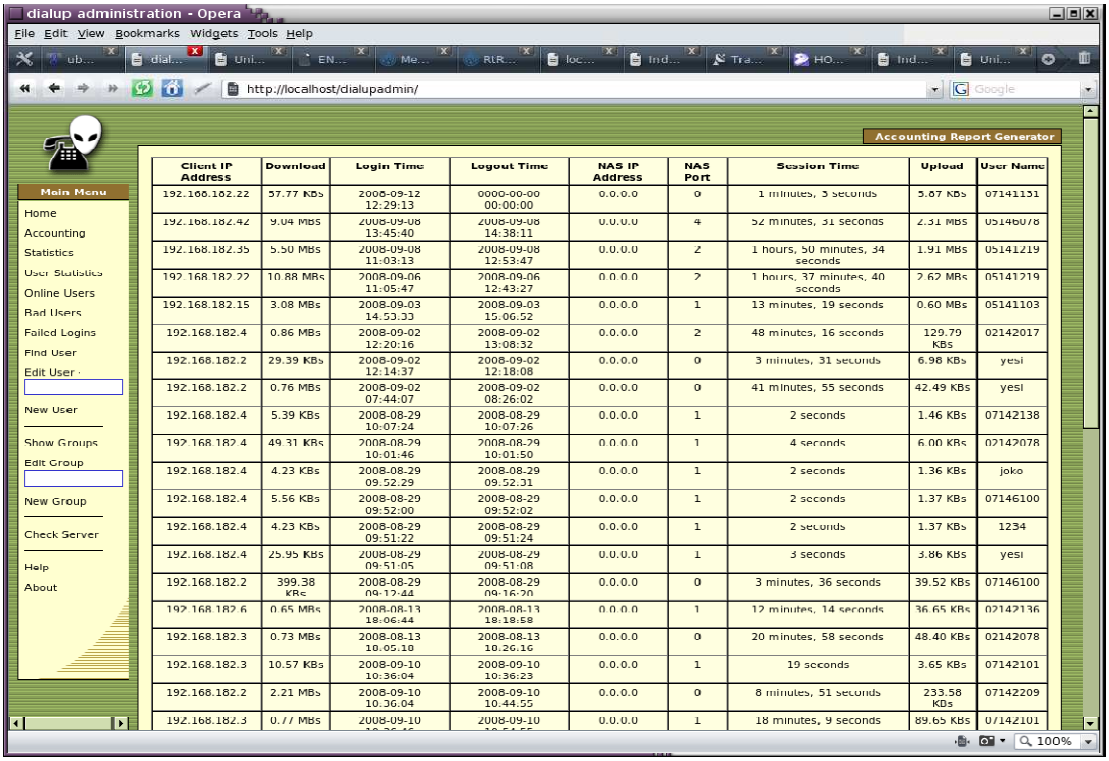
11.2.2.3. Pencatatan (*Accounting*)

Untuk proses pengumpulan data informasi seputar berapa lama *user* melakukan koneksi dan *billing time* yang telah dilalui selama pemakaian digunakan *tools* Dialup Admin. Proses dari pertama kali seorang user mengakses sebuah sistem, apa saja yang dilakukan user di sistem tersebut dan sampai pada proses terputusnya hubungan komunikasi antara user tersebut dengan sistem, dicatat dan didokumentasikan di database MySQL server.

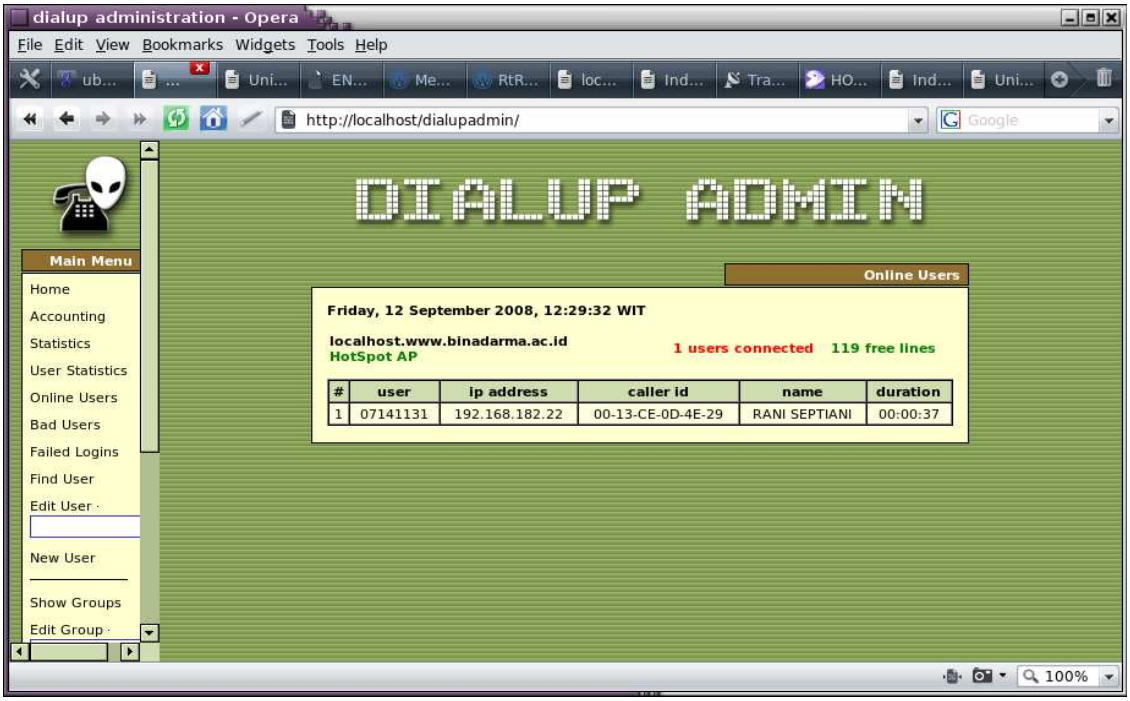
Dialup Admin untuk melihat *user accounting* Pada gambar 3.4 merupakan menu interface untuk melihat user accounting. Dengan menu tersebut bisa terlihat tanggal dan jam login serta logout, user yang login, ipnya serta jumlah upload dan downlod.

Dialup Admin juga memiliki fasilitas untuk melihat user *online* seperti pada gambar 3.5.. Dengan fasilitas tersebut kita dapat melihat jumlah user yang sedang *online* dan siapa saja mereka.

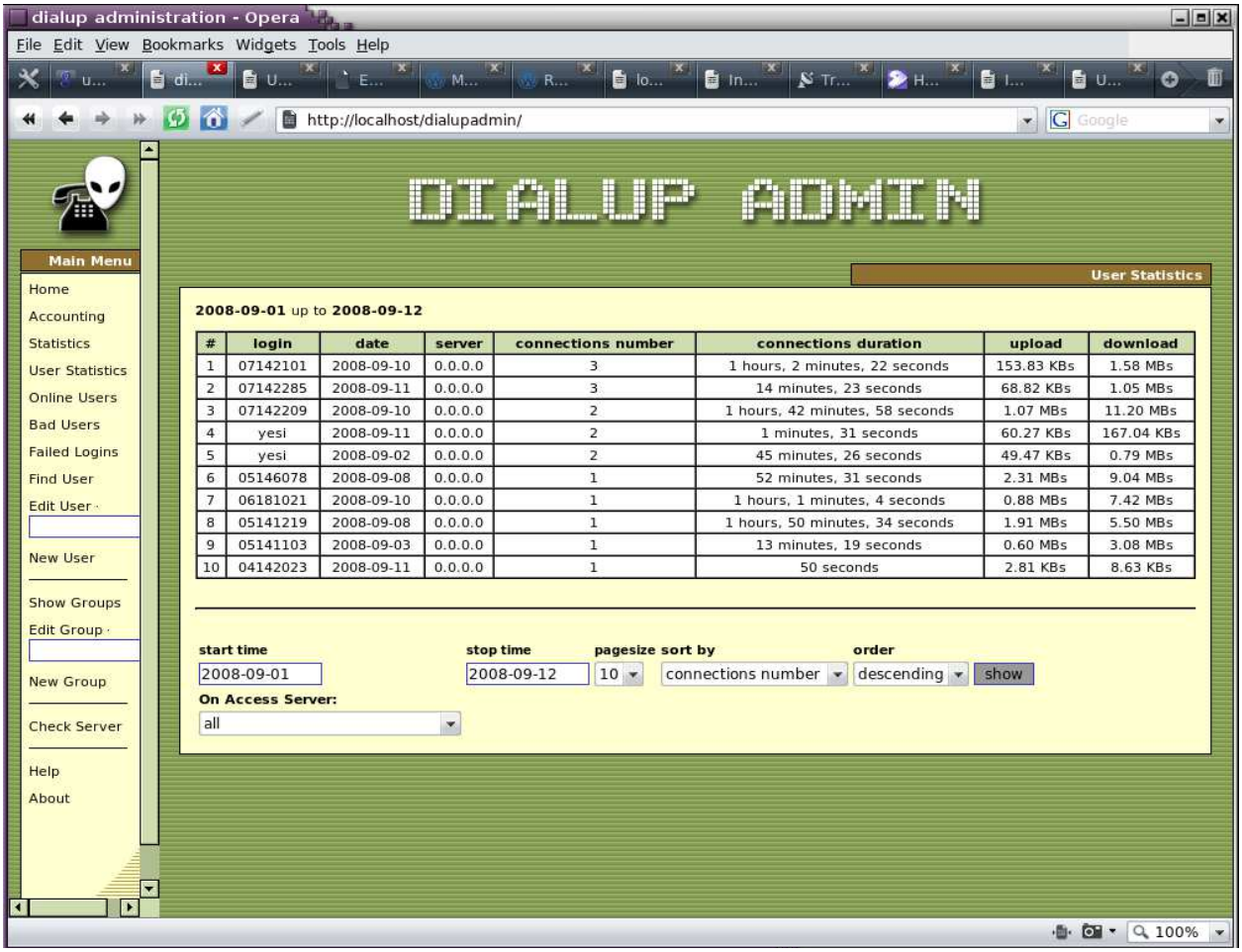
Pada Gambar 3.6 kita dapat melihat statistik user meliputi durasi koneksi, volume download dan volume upload masing-masing didasarkan pada tanggal pengaksesan.



Gambar 3.4 Menu *Interface*



Gambar 3.5 Menu *Interface* Dialup Admin untuk melihat user yang *online*.



Gambar 3.6 Menu *Interface* Dialup Admin untuk melihat statistik user

3.3 Rekomendasi

Untuk implementasi dan penelitian lebih lanjut akan lebih baik lagi jika *captive portal* yang dikembangkan dapat menyempurnakan penelitian ini dan memiliki beberapa komponen berikut:

1. Penggunaan *database* yang lebih baik seperti Oracle
2. Setelah terautentikasi halaman bisa langsung di *redirect* ke halaman tujuan, bukan ke *home page.*

BAB IV PENUTUP

4.1 Kesimpulan

Dari hasil penelitian dapat di ambil beberapa kesimpulan:

1. Di sisi kenyamanan pengguna, pengguna dimudahkan dengan sistem autentikasi ini karena pengguna tidak perlu mendaftarkan setiap *gadget* yang akan koneksikan ke wifii.
2. Dengan adanya sistem autentikasi yang dikembangkan memudahkan administrator dalam memantau dan mengontrol user-user yang terhubung ke jaringan serta dapat membatasi penggunaan *bandwidth*.
4. Dapat membatasi pengguna, terbatas pada civitas akademik UIN Sunan Kalijaga.
3. Dari sisi keamanan penggunaan sistem autentikasi ini juga relatif aman bagi data pengguna, karena memanfaatkan sistem *tunelling* dengan SSL yang akan mengenkrip semua data yang dikirim *client* maupun server hotspot.