BAB IV

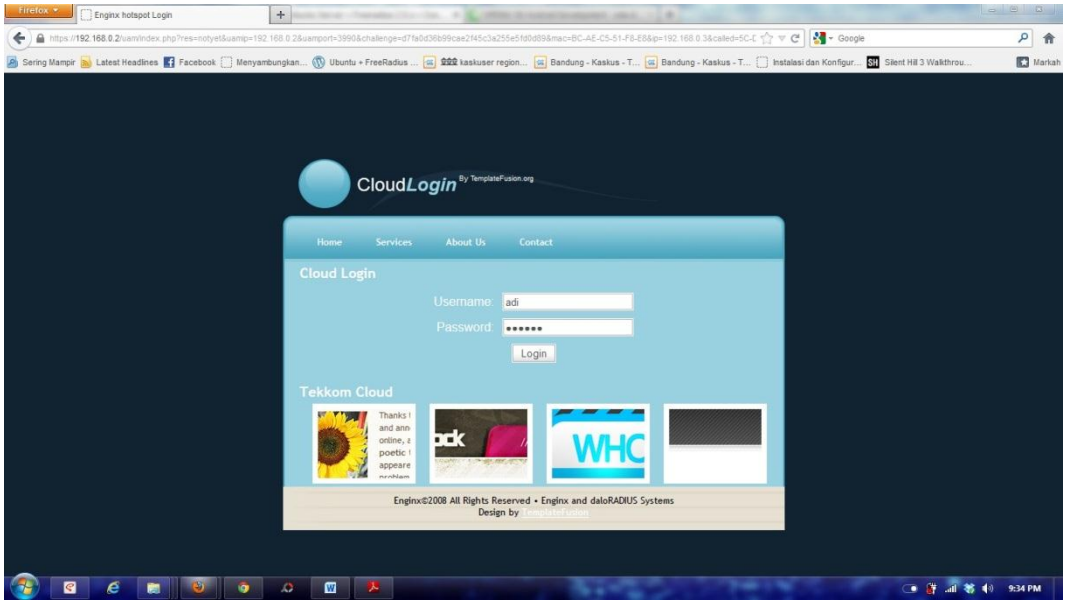
PENGUJIAN DAN ANALISA

Setelah dilakukan perancangan sistem RADIUS pada PC *Router* yang bertindak sebagai server, dihubungkan dengan layanan aplikasi web *private cloud computing* yang berada di *web server cloud* dan dihubungkan lagi dengan beberapa *user client*, sesuai dengan topologi yang telah dibuat sebelumnya (liat gambar 3.1). Pada bab ini dilakukan pengujian dan analisa fungsi RADIUS terhadap *user* yang mengakses layanan aplikasi web, yaitu otentikasi, otorisasi, dan akuntansi *user*. Lalu dilakukan juga pengujian pada sisi administrator yang mengatur RADIUS dan memonitoring kegiatan *user*. Adapun analisa perbandingan otentikasi pada saat input *login username* dan *password*.

4.1 Pengujian Pada RADIUS

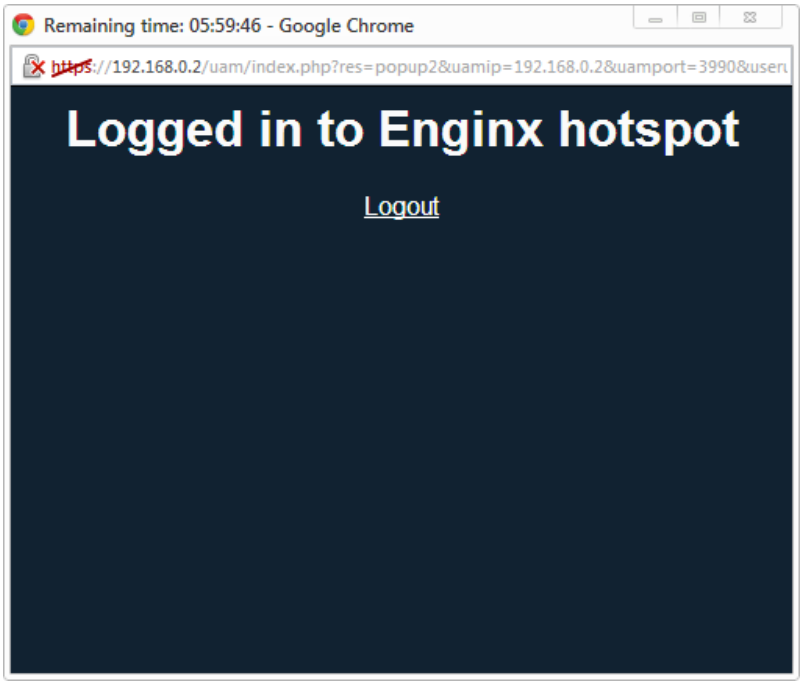
4.1.1 Pengujian Otentikasi *User*

Proses awal pengaksesan aplikasi web merupakan otentikasi *login* yang dilakukan oleh *user client* dengan membuka *web browser*. Hal pertama yang dilakukan *user* agar dapat mengakses layanan aplikasi *web cloud* adalah *user* diharuskan memberikan identitas kode unik seperti *username* dan *password*, atau *login* terlebih dahulu. Caranya dengan membuka *web browser* dan nantinya akan langsung diteruskan ke halaman portal otentikasi. Sistem otentikasi pada halaman portal ini dikendalikan oleh *CoovaChilli* yang berada di *web server Apache* dan *MySQL* sebagai basis datanya. Halaman otentikasi ini disimpan pada server di direktori */var/ww/hotspot*. Tampilan halaman *web portal login* dapat dilihat pada gambar 4.1.



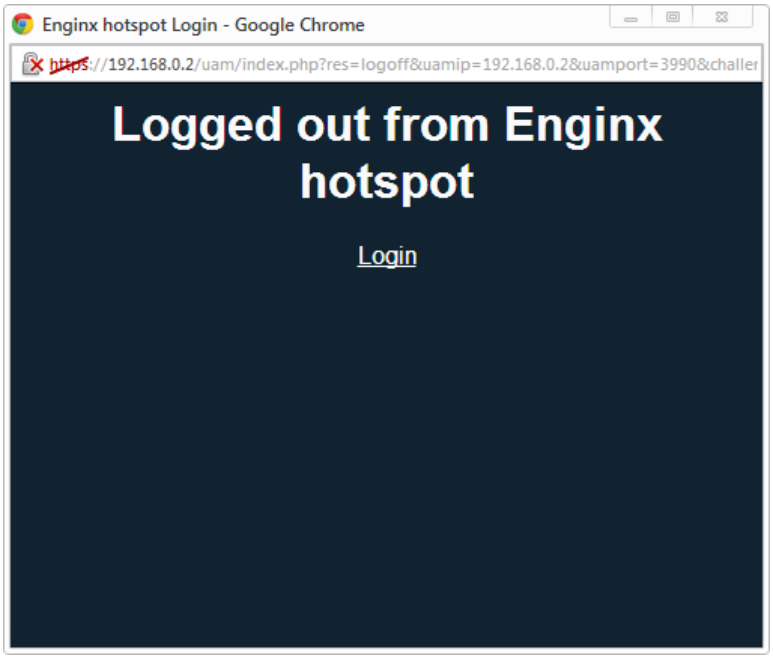
Gambar 4.1. Tampilan Halaman *Login User Client*

Gambar 4.1 merupakan tampilan halaman login *user* ketika pertama kali membuka *web browser*, di halaman *login* ini *user* diharuskan untuk memasukan kode unik berupa *username* dan *password* pada form yang sudah disediakan. Di sisi server, sistem akan menerima kode unik tersebut dan selanjutnya membandingkan dengan kode otentik yang disimpan dalam *database* di MySQL, jika hasilnya sama maka *user* akan diberikan hak akses dan *user* akan dapat mengakses halaman aplikasi web, tapi jika hasilnya tidak sesuai maka tidak dapat mengakses halaman aplikasi web. *Username* dan *password* ini didapat dengan mendaftarkan terlebih dahulu dari adminstrator yang mengelola akun *user* dengan memasukannya kedalam *database* di tabel *radcheck*. Berikut ini adalah gambar tampilan ketika user telah berhasil *login*.



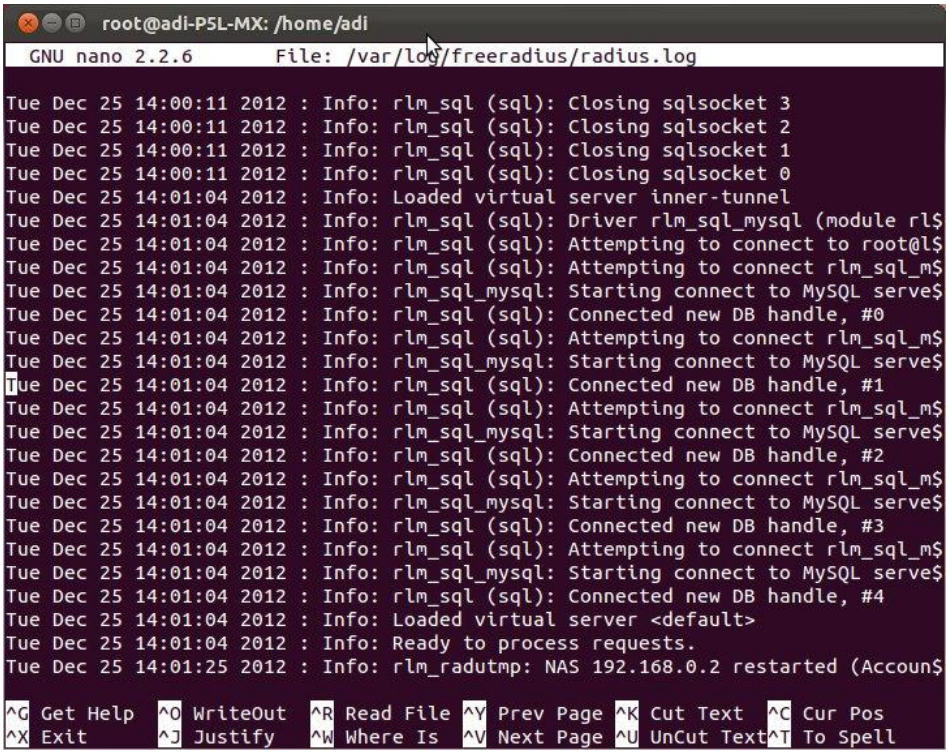
Gambar 4.2 Tampilan Saat *User* Berhasil *Login*

Pada gambar 4.2 ini berarti user telah *login* dan dapat mengakses aplikasi web *cloud*. Jika seorang *user* berkehendak ingin melakukan *logout* maka *user* dapat mengklik tulisan "Logout" pada jendela yang telah *login* tersebut, maka tampilannya akan seperti gambar 4.3 dibawah ini.



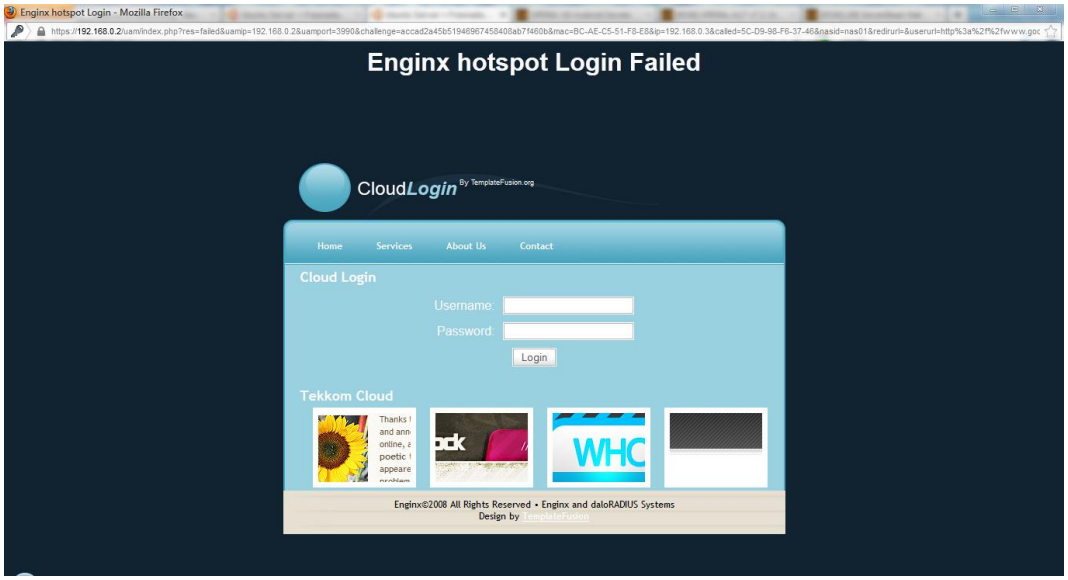
Gambar 4.3 Tampilan Saat *User* Berhasil *Logout*

Pada gambar 4.3 terlihat bahwa *user* berhasil *logout*, akan tetapi jika *user* tersebut ingin kembali *login* maka *user* dapat mengklik tulisan “Login” dan kemudian akan diminta kembali memasukan identitas *username* dan *password* seperti halaman web *login* pada gambar 4.1. Disisi server transaksi *login* maupun *logout* dapat tercatat jika melihat data pada direktori */var/log/freeradius/radius.log*. Berikut merupakan gambar tampilan radius.log di Ubuntu.



Gambar 4.4 Transaksi *Login* dan *Logout* Pada Radius.log

Selanjutnya apabila *user* salah dalam memasukan *username* dan *password*, hal tersebut karena tidak sesuai atau tidak sama dengan *username password* yang ada dalam *database* pada tabel *radacct*, maka *user* mendapat pesan bahwa *login* gagal sebagaimana ditampilkan seperti pada gambar 4.5.



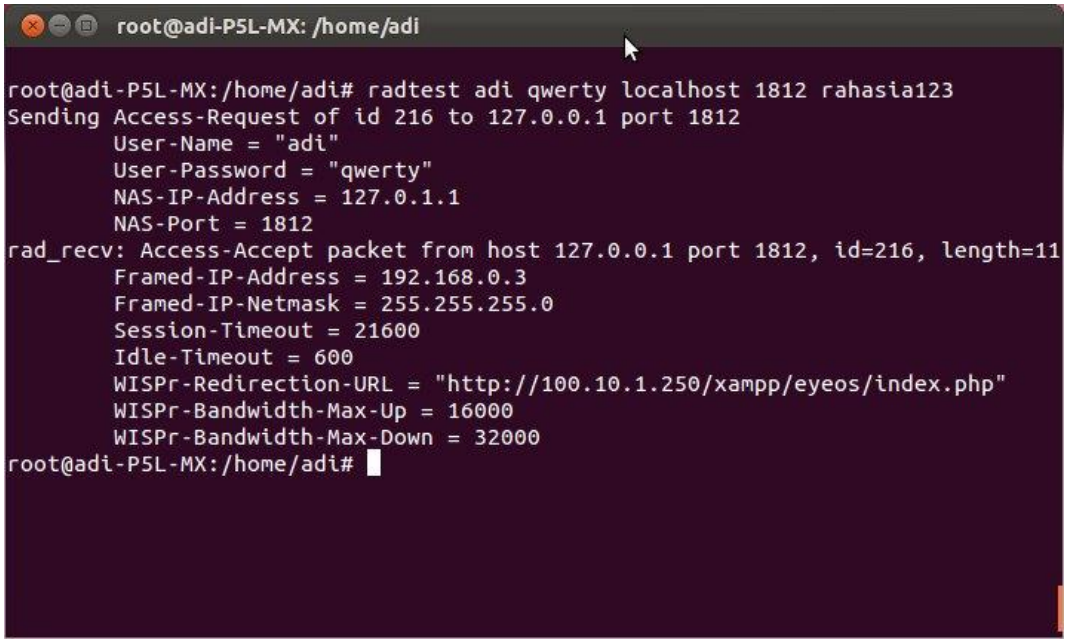
Gambar 4.5. Pesan Kesalahan Pada Halaman *Login User*

Pada gambar 4.5. merupakan pesan kesalahan karena *username* atau *password* tidak cocok dengan yang ada dalam *database*, sehingga berarti *user client* tidak dapat mengakses layanan aplikasi web, namun *user client* dapat mencoba kembali sampai berhasil *login*. Jika salah seorang *user* tidak ingat/lupa akan *username* atau *password*, maka user tersebut harus memberitahu kepada admin dan meminta kembali *username password* atau membuatkan akun *user* yang baru.

Di sisi server pengujian otentikasi juga dapat dilakukan dengan menggunakan perintah *radtest* dengan mengetikannya di jendela terminal.

```
# radtest adi qwerty localhost 1812 rahasia123
```

Pada keterangan perintah diatas, “radtest” merupakan perintah untuk menguji akun *user*, “adi” “qwerty” merupakan *user-name* dan *user-password*, “localhost” disini adalah IP *Address* server. “1812” adalah kode port untuk otentikasi, dan “rahasia123” adalah penamaan *radius secret*. Jika berhasil maka tampilannya akan seperti gambar 4.6.



Gambar 4.6. Pengujian Otentikasi Menggunakan Perintah *Radtest*.

Pada gambar 4.6 dapat dijelaskan bahwa *client* mengirimkan pesan *Access-Request* ke server untuk meminta otentikasi dan otorisasi untuk percobaan koneksi, lalu pesan tersebut diterima oleh server RADIUS, dan server menerimanya dengan kode pesan *Access-Accept*, artinya kode pesan tersebut menginformasikan kepada *client* RADIUS bahwa percobaan koneksi telah diotentikasi dan diotorisasi.

4.1.2 Pengujian Otorisasi *User*

Salah satu fungsi kontrol RADIUS adalah otorisasi. Otorisasi disini merupakan perijinan *user* yang mengakses layanan aplikasi *web cloud*, mana saja hak-hak akses yang diperbolehkan dan mana saja yang tidak. Dalam pembatasan hak akses dapat di kendalikan oleh seorang administrator melalui *tool management user DaloRadius* atau *DialupAdmin*, saat ketika menambah atau mengubah suatu *user*. *User* dapat dibedakan menjadi *personal user* dan kelompok/*group*, dimana masing-masing *group* memiliki hak akses yang berbeda-beda. Pada *database* kelompok ini disimpan dalam tabel *radgroupcheck*,

dan personal *user* disimpan pada tabel *radcheck*. Sedangkan hak-hak aksesnya disimpan pada tabel *radgroupreply* dan *radreply*.

Administrator dapat membatasi hak akses suatu *group user* dan *personal user*, misalnya lama waktu koneksi (*session time*), maksimal *bandwidth upload* maupun *download*, batas waktu *idle*, dan lain-lain. Semua itu dapat disesuaikan menurut kebutuhan pada masing-masing kelompok/*group* atau personal.

Berikut adalah pengujian terhadap *personal user* dengan nama user "Adi" yang telah diberikan hak akses, dengan urutan hak-hak aksesnya sebagaimana ditampilkan pada tabel 4.1.

Tabel 4.1 Hak Akses *User* Bernama "Adi"

NO	ATTRIBUTE	OP	VALUE
1	Simultaneous-Use	:=	1
2	Acct-Interim-Interval	=	60
3	Session-Timeout	=	21600
4	Idle-Timeout	=	600
5	WISPr-Bandwidth-Max-Down	=	256000
6	WISPr-Bandwidth-Max-Up	=	128000
7	WISPr-Redirection-URL	=	http://100.10.1.253/xampp/eyeos/index.php

Keterangan:

1. *Simultaneous-Use* := 1, artinya attribut ini hanya mengijinkan 1 kali login untuk satu *user* pada saat yang bersamaan.
2. *Acct-Interim-Interval*, artinya waktu interval *request*, diberikan sebanyak 60 detik.
3. *Session-Timeout*, adalah attribut berapa lama waktu sesi koneksi untuk *user* tersebut, diberikan waktu selama 21600 detik atau 6 jam.

4. *Idle-Time*, waktu *idle* yang diberikan selama 600detik/10menit, artinya jika *user* tidak melakukan apapun selama yang telah ditentukan maka secara otomatis akan menutup sesi *login*.
5. *WISPr-Redirection-Max-Down*, atribut ini berfungsi membatasi besar *bandwidth* pengguna untuk melakukan *downstream*, dalam hal ini *user* akan dibatasi *downstream* sebesar 256000bps/256kbps.
6. *WISPr-Bandwidth-Max-Up*, attribut ini berfungsi untuk membatasi besar *bandwidth* pengguna untuk melakukan *upstream*, dalam hal ini *user* akan dibatasi *upstream* sebesar 128kbps.
7. *WISPr-Redirection-URL*, atribut yang berfungsi ketika saat *user* berhasil login akan langsung diteruskan ke halaman web yang telah ditentukan, dalam hal ini user akan masuk ke halaman utama aplikasi *web cloud computing* yang berada di web server beralamat http://100.10.1.253 /xampp/eyeos/index.php

User yang telah diberikan hak akses dengan atribut *Session-Timeout*, ketika berhasil *login*, maka pada jendela *login* akan terdapat indikator yang menginformasikan bahwa *user* diberikan tenggang waktu akses yang telah ditentukan. Dalam hal ini *user* yang bernama "Adi" diberikan hak akses selama 6 jam, dapat dilihat pada gambar 4.7

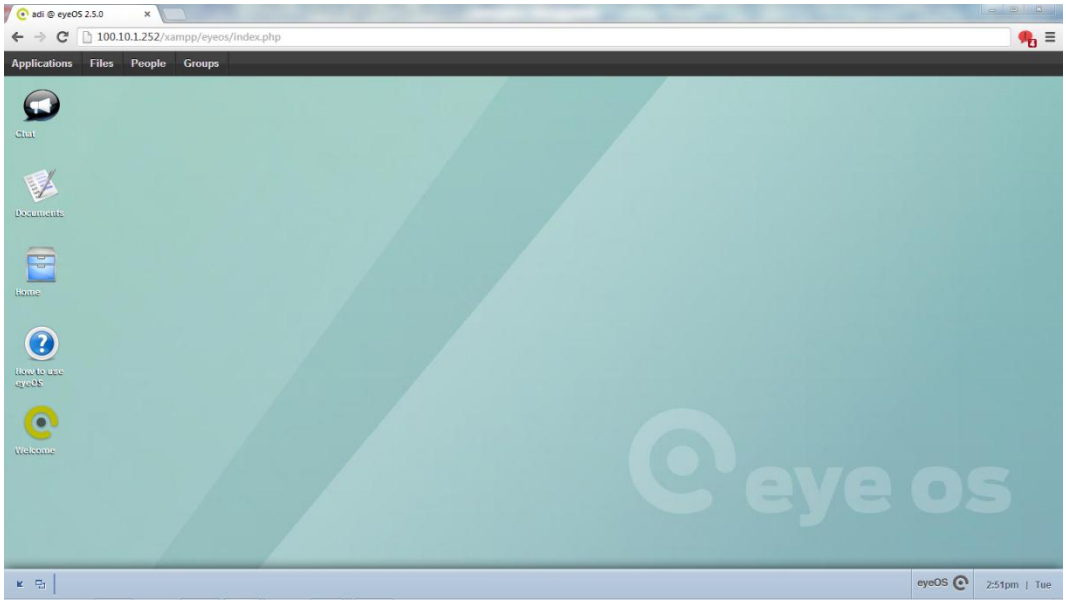


Gambar 4.7 *User* Diberikan Tenggang Waktu Akses Selama 6 Jam

Pada gambar 4.7 yang ditandai kurung merah menyatakan bahwa *user* diberikan jatah akses selama kurang lebih 6 jam. Jika waktu akses telah habis maka secara otomatis sistem akan keluar/*logout* dengan sendirinya, dan pencatatan waktu/akuntansi pada sistem akan berhenti. Disisi server dapat dilihat

apabila waktu akses user yang ditetapkan telah habis maka statusnya pada *user* tersebut adalah "*Session-Timeout*"

User yang diberikan hak akses dengan atribut *WISPr-Redirection-URL* ,ketika berhasil *login* maka secara otomatis akan diteruskan ke halaman aplikasi web *cloud* yang beralamat http://100.10.1.253/xampp/eyeos/. Berikut adalah tampilan *home page* dari aplikasi web *cloud* yang sudah diinstal kedalam *web server*.



Gambar 4.8 Tampilan *Home Page Web Application Cloud*.

Pada gambar 4.8 merupakan tampilan dari aplikasi *web cloud computing*, di aplikasi ini seorang *user* dapat memanfaatkan fitur-fitur yang ada, misalnya *chatting*, *file sharing*, *mail*, menyimpan data, kalkulator dan terlebihnya lagi terdapat *teks editor* yang dimana media penyimpanan sepenuhnya berada di dalam *web server cloud*. Dengan kata lain, *user* tidak harus menginstal aplikasi-aplikasi tersebut kedalam komputernya, *user* hanya membuka jendela *web browser* saja tanpa harus menggunakan sumber daya dari komputernya sendiri. Aplikasi web *cloud computing* ini dapat digunakan secara bersama-sama (*Multi-Tenant*) oleh sejumlah *user*.

4.1.3 Pengujian Pencatatan *User*

Salah satu fungsi kontrol selain otentikasi dan otorisasi dari RADIUS adalah pencatatan. Sistem RADIUS memiliki kemampuan untuk mengumpulkan data informasi statistik dalam hal lamanya *user* melakukan koneksi dan *billing time* yang telah dilalui selama pemakaian digunakan. Proses ini dicatat mulai dari pertama kali *user* mengakses layanan web sampai pada proses terputusnya hubungan *user* dengan sistem. Putusnya hubungan ini berarti user telah *logout*. Semua itu dicatat dan didokumentasikan ke dalam *database* tepatnya di tabel *radaact*. Dengan demikian, seorang admin dapat mengetahui dan memantau aktivitas *user* tersebut, dan untuk memantaunya dapat digunakan tool *management user* seperti *DaloRadius* atau *DialupAdmin*. Berikut adalah tampilan akunting salah satu *user* pada *Daloradius*.

CSV Export

1 2 3 4

ID	HotSpot	Username	IP Address	Start Time	Stop Time	Total Time	Upload (Bytes)	Download (Bytes)	Termination	NAS IP Address
55		andi	192.168.0.4	2012-12-25 14:41:10	2012-12-25 14:41:13	3 seconds	24.7 Kb	21.17 Kb	User-Request	192.168.0.2
56		adi	192.168.0.4	2012-12-25 14:44:07	2012-12-25 14:46:06	1 minutes, 59 seconds	79.95 Kb	61.74 Kb	User-Request	192.168.0.2
57		andi	192.168.0.4	2012-12-25 14:46:12	2012-12-25 14:46:15	3 seconds	3.84 Kb	3.77 Kb	User-Request	192.168.0.2
58		andi	192.168.0.4	2012-12-25 14:47:23	2012-12-25 14:47:56	33 seconds	35.56 Kb	36.39 Kb	User-Request	192.168.0.2
59		andi	192.168.0.4	2012-12-25 14:48:20	2012-12-25 14:53:44	5 minutes, 24 seconds	585.25 Kb	199.85 Kb	User-Request	192.168.0.2
60		andi	192.168.0.4	2012-12-25 14:55:09	2012-12-25 14:58:28	3 minutes, 19 seconds	659.32 Kb	150.71 Kb	User-Request	192.168.0.2
61		agung	192.168.0.4	2012-12-25 15:06:34	2012-12-25 15:12:36	6 minutes, 2 seconds	126.05 Kb	126.69 Kb	Session-Timeout	192.168.0.2
62		adi	192.168.0.4	2012-12-26 14:20:19	2012-12-26 15:33:16	1 hours, 12 minutes, 57 seconds	12.36 Mb	2.04 Mb	User-Request	192.168.0.2
63		andi	192.168.0.5	2013-01-05 13:02:47	2013-01-05 13:05:43	2 minutes, 56 seconds	503.73 Kb	87.73 Kb	User-Request	192.168.0.2
64		adi	192.168.0.5	2013-01-05 13:08:23	2013-01-05 13:08:32	9 seconds	5.63 Kb	5.06 Kb	User-Request	192.168.0.2
65		adi	192.168.0.5	2013-01-05 13:08:57	2013-01-05 13:20:31	11 minutes, 34 seconds	952.14 Kb	164.86 Kb	User-Request	192.168.0.2
66		adi	192.168.0.5	2013-01-05 13:20:38	2013-01-05 13:22:45	2 minutes, 7 seconds	1.52 Mb	104.64 Kb	User-Request	192.168.0.2
67		andi	192.168.0.4	2013-01-05 13:32:59	2013-01-05 13:39:00	6 minutes, 1 seconds	1.52 Mb	99.6 Kb	Session-Timeout	192.168.0.2
68		adi	192.168.0.5	2013-01-05 13:33:14	2013-01-05 14:02:20	29 minutes, 6 seconds	388.25 Kb	200 Kb	User-Request	192.168.0.2
69		agung	192.168.0.4	2013-01-05 13:48:07	2013-01-05 13:54:09	6 minutes, 2 seconds	1.57 Mb	129.62 Kb	Session-Timeout	192.168.0.2
70		adi	192.168.0.3	2013-01-08 18:11:30	2013-01-08 18:14:07	2 minutes, 37 seconds	10.12 Kb	15.69 Kb	User-Request	192.168.0.2
71		adi	192.168.0.3	2013-01-08 18:14:45	2013-01-08 18:20:23	5 minutes, 38 seconds	9.36 Kb	18.23 Kb		192.168.0.2
72		adi	192.168.0.3	2013-01-08 18:21:36	2013-01-08 18:33:08	11 minutes, 32 seconds	1.53 Mb	143.4 Kb	User-Request	192.168.0.2
75		bayu	192.168.0.3	2013-01-08 19:25:49	2013-01-08 20:18:12	52 minutes, 23 seconds	992.83 Kb	71.23 Kb	User-Request	192.168.0.2
76		adi	192.168.0.3	2013-01-08 20:18:57	2013-01-08 20:21:20	2 minutes, 23 seconds	1.5 Mb	99.11 Kb	User-Request	192.168.0.2
77		adi	192.168.0.3	2013-01-08 20:53:15	2013-01-08 21:03:33	10 minutes, 18 seconds	1.54 Mb	136.37 Kb	User-Request	192.168.0.2

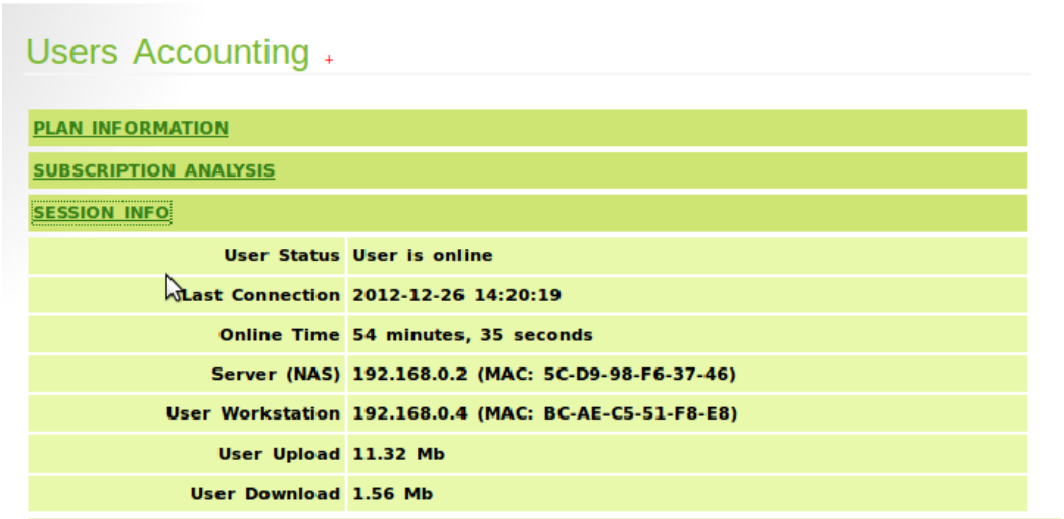
Gambar 4.9. Tampilan Pencatatan Statistik Penggunaan *User*

Pada gambar 4.9. menampilkan data statistik pada beberapa *user*. Di tampilan ini bisa terlihat berapa IP *address*, waktu mulai, waktu berhenti, jumlah waktu, besar *upload* serta *download* (dalam hitungan *byte*), terminasi, dan IP address nas server dari *user* tersebut yang digunakan.



Gambar 4.10 Tampilan Pencatatan Analisis Akses *User*

Pada gambar 4.10 menampilkan data statisik berapa banyak waktu penggunaan (*Session Used*), sesi *download* (*Session Download*), serta sesi *upload* (*Session Upload*), *session traffic*, dan banyak login dalam hitungan perhari, minggu, bulan, dan keseluruhannya pada salah satu *user*.



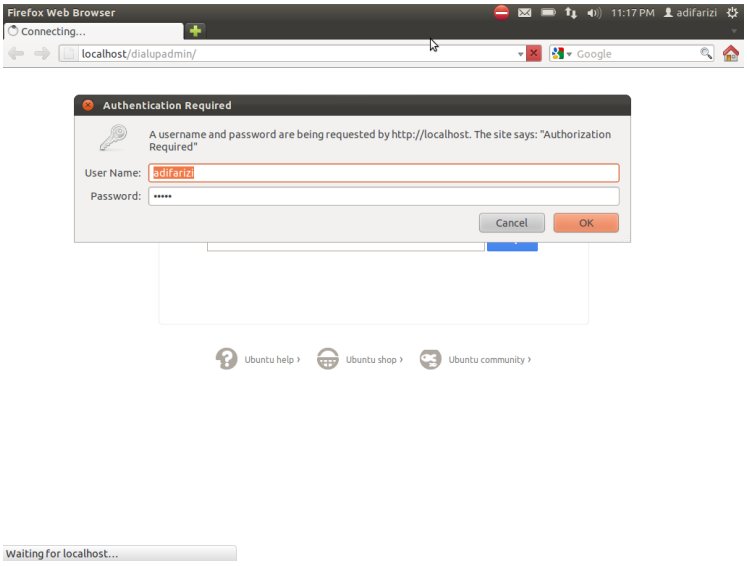
Gambar 4.11 Tampilan Informasi Sesi *Login User*

Pada gambar 4.11 menampilkan data *status user* apakah sedang *online* atau *offline*, menampilkan kapan waktu koneksi terakhir, berapa lama waktu *online*, alamat Server NAS dan MAC address yang dipakai, IP address dan MAC address pengguna (*user workstation*), serta besar *upload*, dan besar *download*.

4.2 Manajemen *User*

Salah satu peranan administrator pada jaringan *private cloud computing* dalam hal ini adalah pengelolan akun *user* RADIUS. Seorang admin diberikan hak penuh untuk mengatur akun *user* baik menambah, menghapus atau mengubah data-data akun *user*. Untuk mengatur *user* disini menggunakan *tool management user* berbasis web seperti DialupAdmin atau yang lebih lengkap fungsi-fungsinya yaitu DaloRADIUS.

Sebelum admin *user* masuk ke halaman DialupAdmin untuk kegiatan manajemen *user* dibutuhkan otentikasi terlebih dahulu, karena secara *default* DialupAdmin tidak terproteksi tanpa *username* dan *password*, hal ini tentu saja berbahaya karena bisa diakses oleh siapa saja, setelah diberikan fitur *.htaccess* dan di konfigurasi maka tampilan *login admin user* untuk DialupAdmin seperti pada gambar dibawah ini.

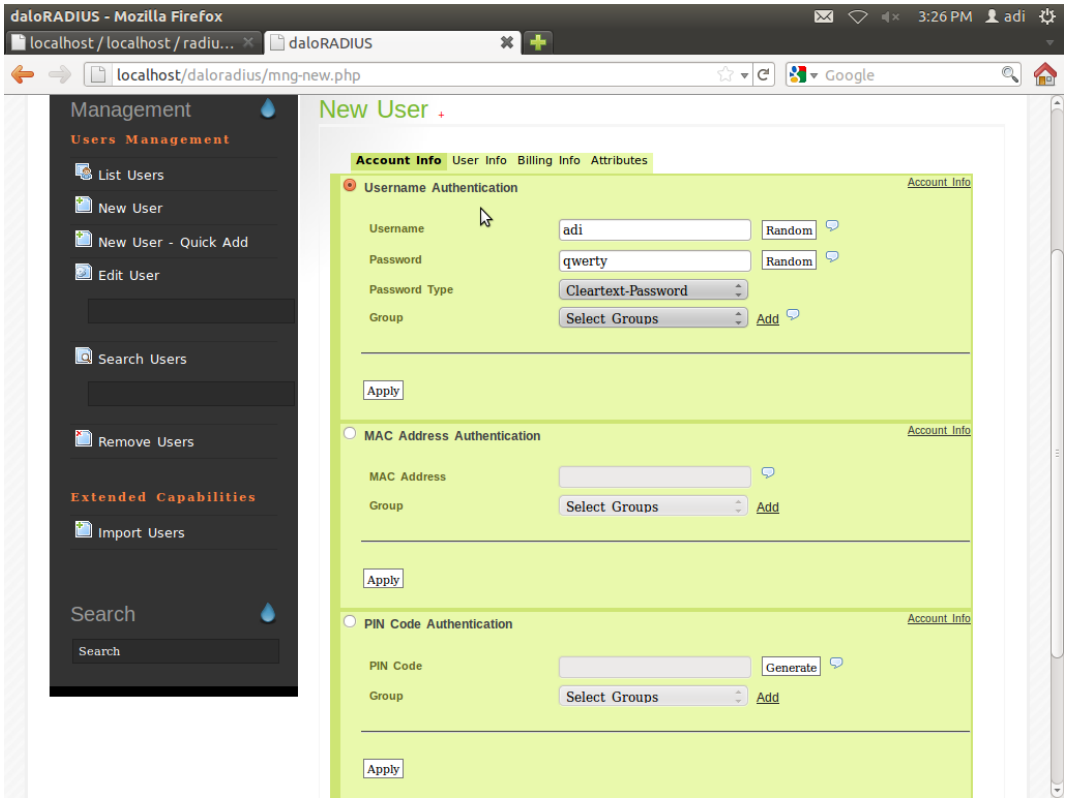


Gambar 4.12. Tampilan Jendela *Login Dialup Admin*

Pada gambar 4.12 diatas adalah otentikasi dimana admin *user* diharuskan *login* terlebih dahulu, apabila otentikasi berhasil maka dapat masuk ke halaman *DialupAdmin* sedangkan apabila salah memasukan *username* atau *password* tidak dapat masuk ke halaman *DialupAdmin*. Di server *DialupAdmin* ini disimpan pada *file system* di direktori */usr/local/dialup_admin*. Sedangkan DaloRADIUS disimpan didalam direktori */var/www/daloradius*. Pada DaloRADIUS sudah disediakan fitur otentikasi sehingga tidak perlu lagi diberikan fitur *.htaccess*.

4.2.1 Menambah Akun *User*

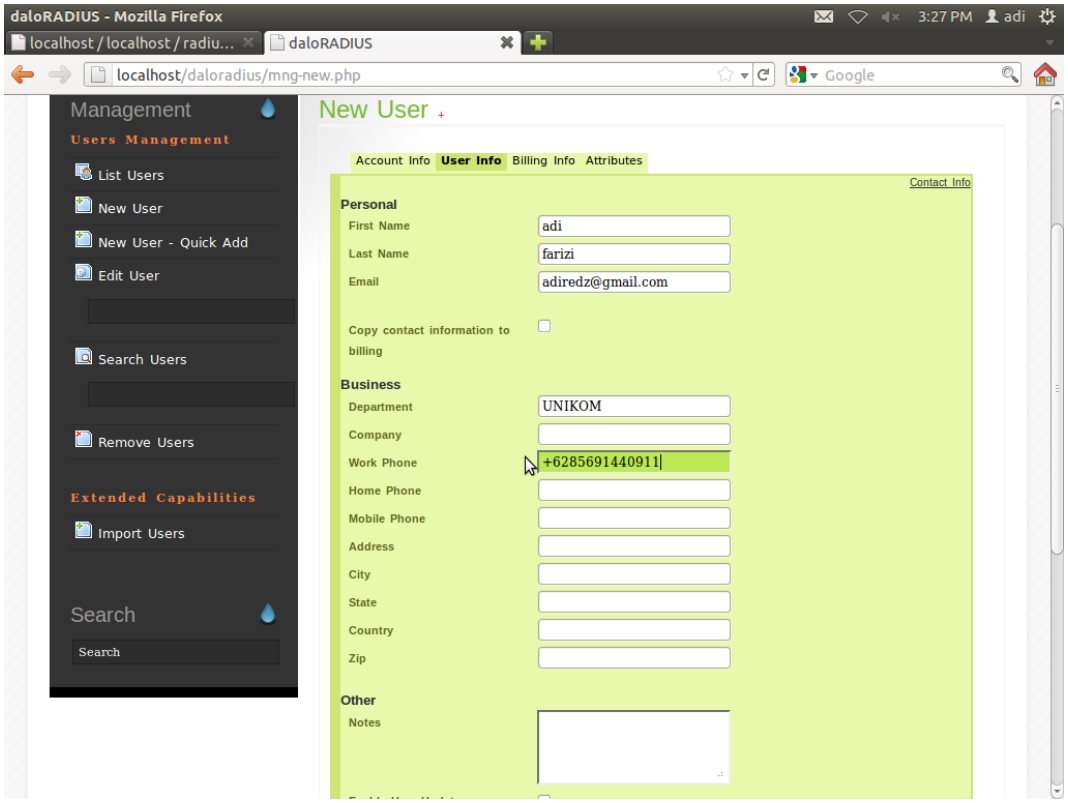
Dalam DaloRADIUS, untuk penambahan akun *user* terdapat beberapa sub menu yang diisikan diantaranya *account info*, *user info*, *billing info*, dan attribut yang dipakai.



Gambar 4.13 *Form* Pengisian Informasi Akun

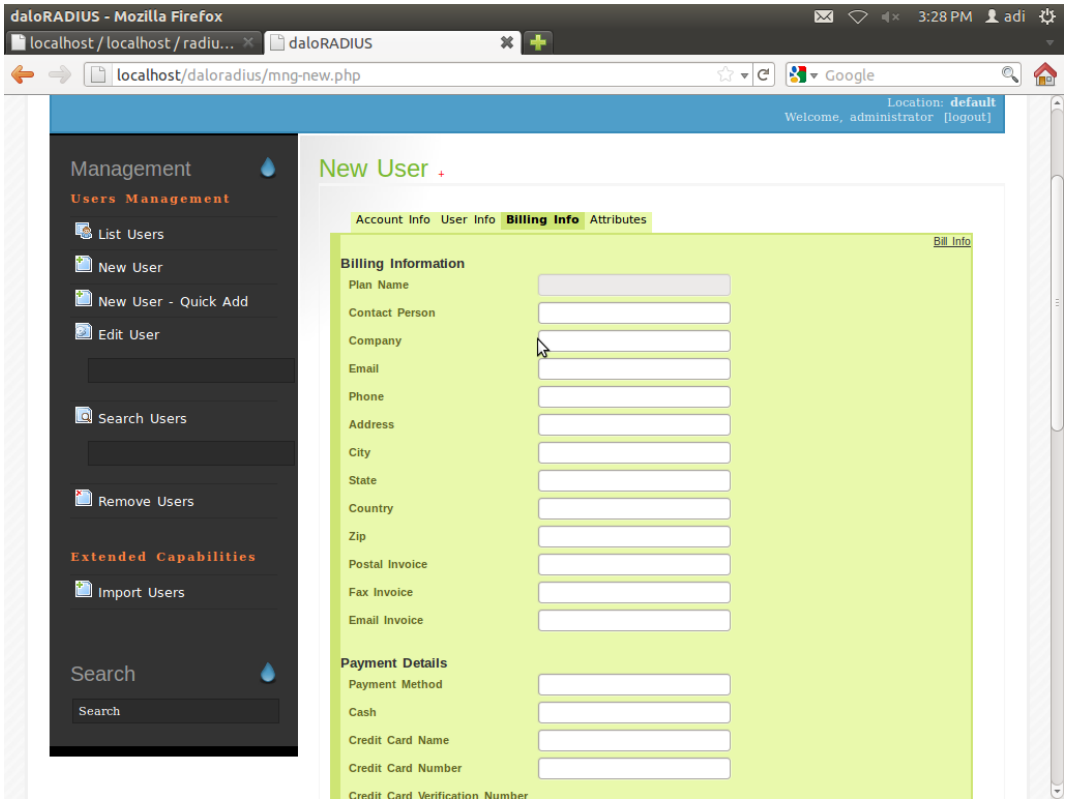
Pada form ini untuk menentukan *username* dan *password* dari akun RADIUS yang wajib diisi, karena nantinya akan disimpan dalam tabel radcheck.

Metode *password*-nya dapat dipilih, diantaranya *ClearText-Password*, *MD5-Password*, *CHAP-Password*, dan lain-lain.



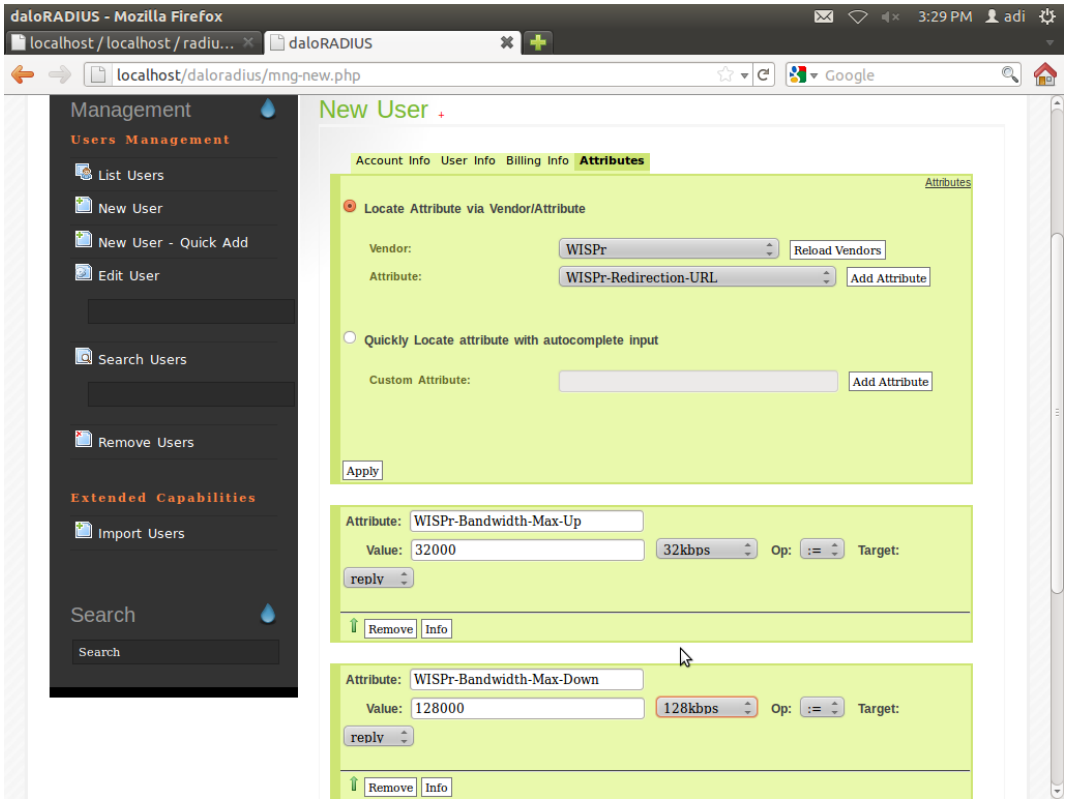
Gambar 4.14. *Form* Pengisian Info *User*

Pada form ini dipergunakan untuk menambahkan identitas agar memberikan informasi yang lebih detail di masing-masing akun *user*.



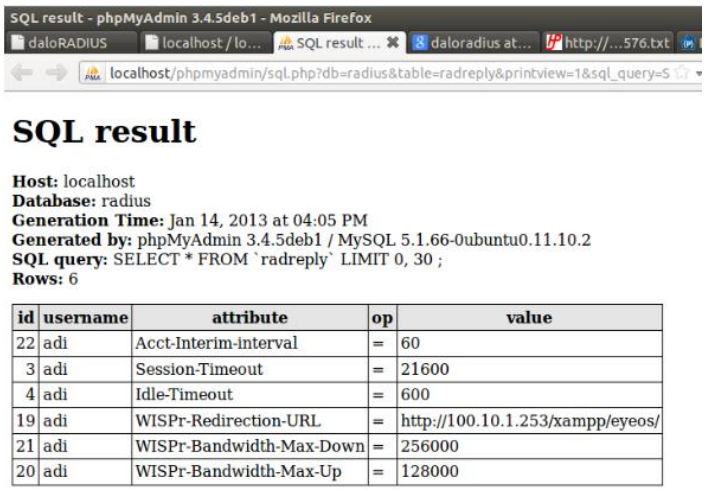
Gambar 4.15. *Form* Pengisian Info *Billing*

Form ini sebagai infomasi pembayaran (*billing*) dari akun seorang *user*, form ini tidak diisi karena dalam penelitian ini *user* tidak melakukan pembayaran atas penggunaan apapun.



Gambar 4.16. *Form* Pemberian Hak Akses *User*

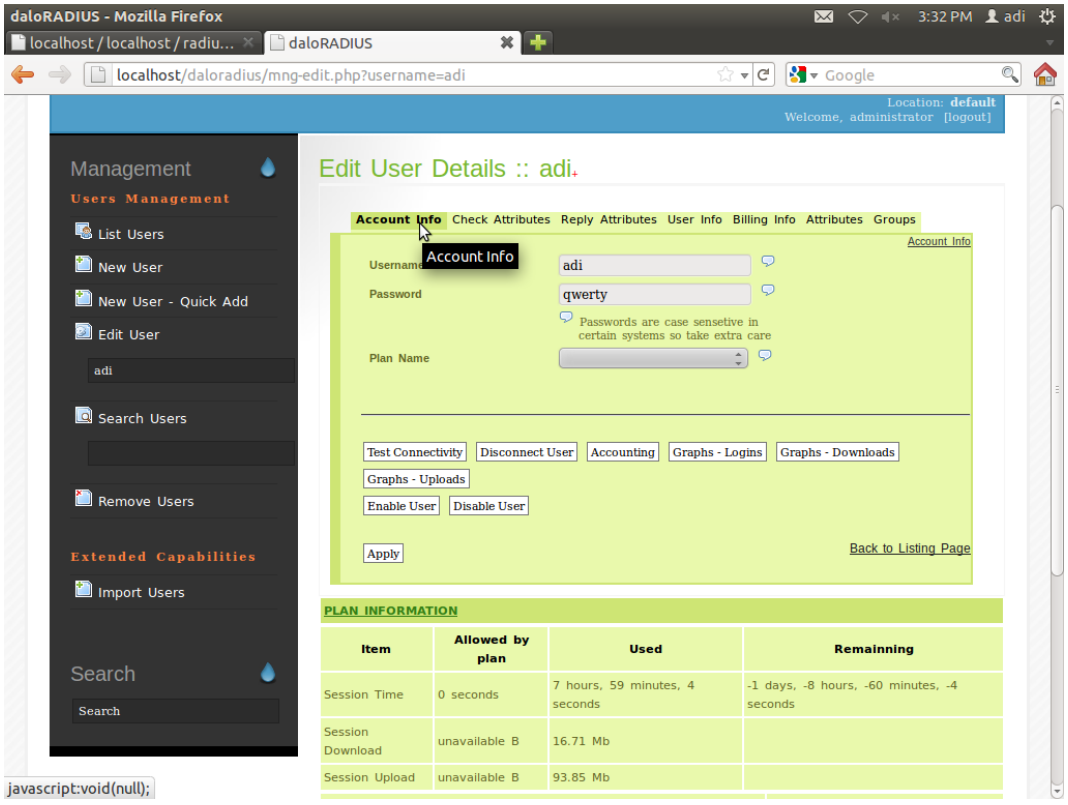
Form ini merupakan pemberian hak akses untuk akun seorang *user*, hak-hak apa saja yang dapat ditambahkan disesuaikan menurut kebutuhan masing-masing *user*. Daftar pemberian hak akses *user* dapat dilihat di halaman PhpMyAdmin seperti yang ditunjukan pada gambar 4.17.



Gambar 4.17. Daftar Hak Akses *User* Pada *PhpMyAdmin*

4.2.2 Mengubah Akun *User*

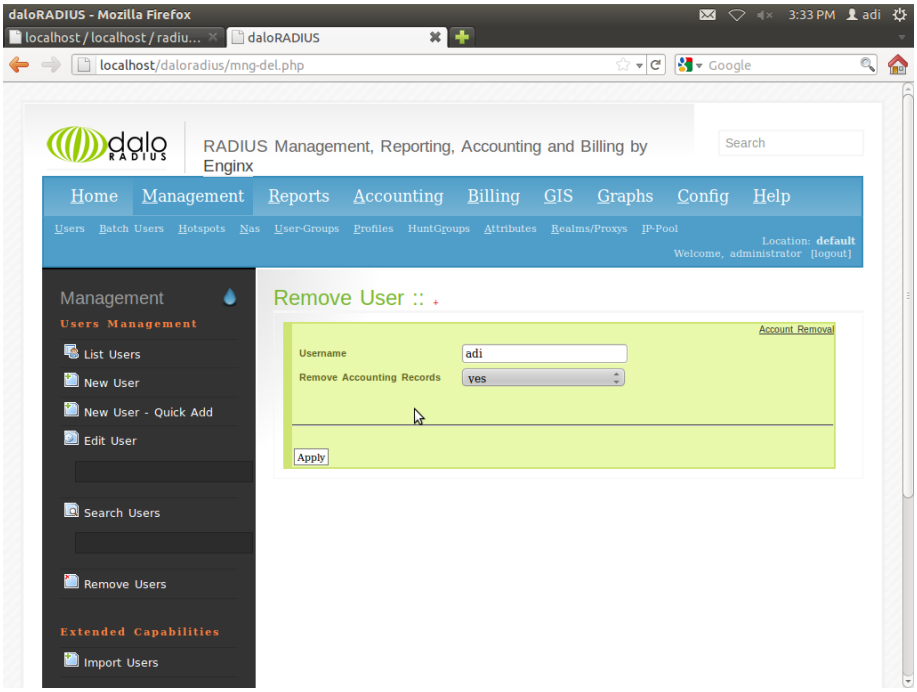
Daloradius memilik fitur untuk mengubah akun *user*. Informasi yang dapat diubah mulai dari pergantian *username* atau *password*, informasi akun *user*, attribut yang dipakai dan lain-lain. Berikut merupakan gambar dari tampilan mengubah *user*.



Gambar 4.18. *Form* Untuk Mengubah Akun *User*

4.2.3 Menghapus Akun *User*

DaloRADIUS menyediakan fungsi untuk menghapus akun *user* dan menghapus semua catatan akuntansi dari *user* tersebut. Tampilan fungsi untuk menghapus dapat dilihat pada gambar 4.19.



Gambar 4.19. Tampilan Untuk Menghapus Akun *User*.

4.3 Analisa *User*

4.3.1 Analisa Otentikasi *User*

Berikut ini adalah analisa dari pengujian otentikasi *login user* berhasil atau tidaknya, dilihat dari cara *user* meng-input *username* atau *password*. Hasil analisa dapat dilihat pada tabel dibawah ini.

Tabel 4.2 Analisa Otentikasi RADIUS *user*

Username	Password	Accest-Accept	Accest-Reject
adi	qwerty	✓	
adi	Qwerty		✓
Adi	Qwerty		✓
Adi	qwerty	✓	
ADI	qwerty	✓	
adi	QWERTY		✓
ADI	QWERTY		✓

Pada tabel 4.2 dapat dijelaskan, ketika *username* diketikan benar atau tidak sesuai baik besar kecil jenis hurufnya akan tetap terotentikasi, sedangkan *password*-nya apabila tidak sesuai baik besar kecilnya jenis huruf, maka akses untuk *login* akan gagal. Disebabkan pada *login* otentikasi, terutama pada *password* aksesnya telah dipasangkan *sensitive font*. Sedangkan pada *username* tidak mempengaruhi besar kecilnya jenis *font* proses *login* dan akan tetap cocok.

4.3.2 Analisa Manajemen *Bandwidth User*

User mendapatkan hak akses dengan diberikan atribut dalam tabel *radreply* atau *radgroupreply* di *database* salah satu namanya adalah *WISPr-Bandwidth-Max-Down* dan *WISPr-Bandwidth-Max-Up*. Atribut tersebut berfungsi sebagai manajemen *bandwidth* dengan diberikan batasan nilai (*limit*) *download* dan *upload* pada *user*. Tabel 4.3 merupakan daftar *user* yang diberikan batasan *bandwidth*.

Tabel 4.3. Daftar *User* Yang Dibatasi *Bandwidth*

Username	**Download**	**Upload**
Adi	32KBps	25KBps
Andi	16KBps	16KBps
Agung	16KBps	16KBps

User tersebut di analisa dengan membuktikan apakah atribut tersebut berfungsi dengan baik, maka hasilnya dapat ditampilkan ke dalam tabel berikut.

Tabel 4.4. Hasil Analisa Perbandingan *Bandwidth* Akses *User*

Username	**Bandwidth Downstream**		**Bandwidth Upstream**	
	User Limit (KBps)	**User Non-Limit (KBps)**	**User Limit (KBps)**	**User Non-Limit (KBps)**
Adi	31.4	56.4	23.4	44.3
Andi	15.3	60.3	15.3	32.1
Agung	15.7	58.1	15.2	32.8

Dari hasil tabel diatas dapat disimpulkan bahwa *user* yang dibatasi *bandwidth*-nya oleh RADIUS akan memiliki rata-rata sesuai dengan yang ditentukan pada masing-masing *user* meski data yang dihasilkan tidak terlalu signifikan.