

IMPLEMENTASI SISTEM AUTENTIKASI JARINGAN *HOTSPOT* UNIVERSITAS UDAYANA DENGAN MENGGUNAKAN *OPEN SOURCE FREERADIUS*

Pande Ketut Sudiarta

Staff Pengajar Teknik Elektro, Fakultas Teknik Universitas Udayana
Kampus Bukit Jimbaran, Bali, tlp. 0361 703315
Email : sudiarta@unud.ac.id

Abstrak

Universitas Udayana sudah menyediakan layanan akses *hotspot* di beberapa Fakultasnya baik yang berada di Kampus Denpasar, Kampus Nias, maupun di Kampus Bukit Jimbaran. Untuk dapat memanfaatkan layanan *hotspot*, *user* harus login terlebih dahulu dan melewati proses autentikasi *username* dan *password*. Saat ini *user account* di-generate dari *ticket printer* yang terpasang ke masing-masing akses poin yang ada di Universitas Udayana. Melihat banyaknya layanan *hotspot* yang ada di Universitas Udayana, tentunya akan menyulitkan *user* karena masing-masing *hotspot* mempunyai *account* yang berbeda-beda. Sehingga dilakukan penelitian bagaimana mengimplementasikan sistem autentikasi terpusat menggunakan *open source freeradius* dan *mysql* sebagai *database user* serta mengimplementasikan manajemen sistem yang berbasis *web interface* untuk memudahkan *administrator* atau *operator* dalam mengelola *user*.

Hasil penelitian ini akan dipakai sebagai sistem yang akan menangani autentikasi *user* jaringan *hotspot* secara terpusat di Universitas Udayana. Metode analisis yang digunakan pada penelitian ini yaitu dengan metode analisis deskriptif yaitu menganalisis data-data hasil pengujian yang dilakukan dan menarik kesimpulan dari hasil analisis tersebut. Pengujian dilakukan dengan menguji kestabilan sistem dalam menangani permintaan autentikasi dalam jumlah yang banyak yang login dalam waktu yang bersamaan, menerapkan *secondary server*, melakukan pengujian seberapa signifikan pengaruh jarak terhadap *time latency* autentikasi *user* dengan *account radius*, pengujian *time latency* autentikasi *user* yang akses ke *extended* akses poin baik yang menggunakan gelombang radio dan fiber optik dengan *account radius*. Dalam mengimplementasikan sistem autentikasi *radius* diperlukan server *radius* yang akan menangani proses autentikasi, otorisasi dan *accounting user*. Semua *hotspot* yang terintegrasi dengan *server radius* akan melakukan autentikasi ke sebuah *server radius*.

Dengan menerapkan *web based administration interface*, maka *administrator* atau *operator* dapat dengan mudah dalam mengelola *user* karena berbasis *web interface* dan bisa diakses dari mana saja dalam satu jaringan Universitas Udayana. *Administrator* bisa membuat laporan dan menganalisis pemakaian *hotspot* berdasarkan *accounting record* yang ditampilkan melalui *web based*. *Time latency* autentikasi antara menggunakan *account ticket* dengan *account radius* tidak menunjukkan selisih yang signifikan, jarak dan media transmisi juga tidak berpengaruh signifikan terhadap *time latency* autentikasi *user*. Setelah dilakukan pengujian, sistem *radius* mampu menangani autentikasi *user* dalam jumlah yang banyak yang login secara bersamaan dan dengan menerapkan *secondary server*, sistem autentikasi bisa tetap berjalan dengan stabil. Dari sistem *radius*, *administrator* bisa mendapatkan data-data yang diperlukan untuk pengembangan layanan jaringan *hotspot* di Universitas Udayana menjadi lebih baik untuk kedepannya.

Kata Kunci : *Radius, Authentication, Authorization, Accounting and Hotspot*

1. PENDAHULUAN

Salah satu perubahan utama dibidang telekomunikasi adalah penggunaan teknologi *wireless*. Kemudahan-kemudahan yang ditawarkan *wireless LAN* menjadi daya tarik tersendiri bagi para pengguna komputer menggunakan teknologi ini mengakses suatu jaringan komputer atau *internet*. Beberapa tahun terakhir ini pengguna *wireless LAN* mengalami peningkatan yang sangat pesat. Peningkatan pengguna ini juga dibarengi dengan peningkatan jumlah *hotspot* yang dipasang oleh ISP (*Internet Service Provider*) di tempat-tempat umum, seperti kafe, mall, bandara dan tempat umum lainnya. Perkantoran dan kampus pun sudah banyak menggunakan atau memasang *hotspot*.

Sistem keamanan yang paling umum digunakan pada *wireless LAN* adalah dengan metode enkripsi yaitu, WEP (*Wired Equivalent Privacy*).[1] WEP ini menggunakan satu kunci enkripsi yang digunakan bersama-sama oleh para pengguna *wireless LAN*. Hal ini menyebabkan metode WEP tidak cocok diterapkan pada *hotspot* yang dipasang di tempat-tempat umum. Dan karena lubang keamanan yang dimiliki WEP cukup banyak, sehingga jaringan mudah dimasuki oleh pihak-pihak yang tidak berhak, maka penggunaan metode ini sudah tidak disarankan lagi. Sistem keamanan lainnya adalah WPA (*Wi-Fi Protected Access*), yang menggeser WEP dan menghasilkan keamanan yang lebih baik dibandingkan dengan WEP. Implementasi WPA

menggunakan 802.1x dan EAP (*Extensible Authentication Protocol*)[2] menghasilkan proses autentikasi pengguna yang relatif aman. Pada proses ini pengguna harus melakukan autentikasi ke sebuah server autentikasi sebelum terhubung ke internet. Pada umumnya proses autentikasi ini menggunakan *username* dan *password*.

Universitas Udayana adalah salah satu pengguna jaringan *hotspot* dengan jumlah lebih dari satu karena terdiri dari beberapa Fakultas. Saat ini Universitas Udayana sudah menerapkan sistem keamanan yang sudah disebutkan di atas yaitu autentikasi *user* dengan *username* dan *password*. Namun untuk saat ini perangkat yang digunakan untuk membuat *user account* adalah dengan menggunakan tiket *printer*. Dengan melihat banyaknya jaringan *hotspot* yang ada di Universitas Udayana maka tentunya akan sangat menyulitkan bagi mahasiswa sebagai pengguna jaringan ini, karena setiap jaringan *hotspot* mempunyai perangkat tiket *printer* yang berbeda, sehingga mahasiswa harus meminta tiket kepada masing-masing *operator* jaringan *hotspot* setiap kali mengakses jaringan *hotspot* di tempat yang berbeda.

Melihat permasalahan di atas maka diperlukan suatu sistem yang mampu menangani proses autentikasi *user* pada satu sistem tertentu. *Radius* atau *Remote Authentication Dial-In User Service* [3] merupakan sebuah protokol yang memungkinkan keamanan jaringan *wireless* untuk melakukan autentikasi, otorisasi, dan akuntansi untuk meremote *user* yang ingin mengakses suatu sistem atau layanan dari pusat server jaringan komputer. *Radius* menjalankan sistem administrasi yang terpusat, sistem ini akan mempermudah tugas *administrator/operator* dalam mengelola *user* atau pengguna *wireless* LAN. Dengan sistem ini *user* sebagai pengguna jaringan *hotspot* dapat menggunakan *hotspot* di tempat yang berbeda-beda dengan melakukan autentikasi ke sebuah server *radius* tanpa harus meminta *account* kepada *operator* setiap menggunakan jaringan *hotspot* di tempat yang berbeda karena satu *user* menggunakan satu *username* dan *password* untuk semua jaringan *hotspot* yang menggunakan sistem autentikasi terpusat[4]. Maka pada penelitian ini akan membahas bagaimana mengimplementasikan sistem autentikasi jaringan *hotspot* di Universitas Udayana dengan menggunakan *Freeradius* dan *MySQL* sebagai *database user*[5]

2. METODE PENELITIAN

Tujuan standar 802.1x IEEE adalah untuk menghasilkan kontrol akses, autentikasi, dan manajemen kunci untuk *wireless* LAN. Standar ini berdasarkan pada *Internet Engineering Task Force* (IETF), yang ditetapkan dalam RFC 2284. Standar 802.1x IEEE juga mendukung beberapa metode

autentikasi, seperti *smart cards*, *password* yang hanya bisa digunakan oleh satu pengguna pada satu waktu, dan yang lebih baik lagi adalah *biometrics*.

Standar 802.1x [1] terdiri dari tiga bagian, yaitu *wireless node* (*supplicant*), *access point* (*autentikator*), server autentikasi yang digunakan adalah *radius* untuk autentikasi pengguna yang akan mengakses *wireless* LAN. Pada penelitian ini akan menggunakan 2 buah komputer sebagai server *radius* yang digunakan untuk server autentikasi, 4 *access point*, dan beberapa *laptop* yang akan digunakan sebagai komputer *client*. Dari 4 buah akses poin tersebut dapat dibagi dimana 2 buah akses poin terletak di lantai dua gedung GDLN Unud Denpasar, 1 buah akses poin di gedung Teknik Ekstensi Denpasar dan 1 buah akses poin di kampus Teknik Elektro Bukit Jimbaran. 4 akses poin ini akan melakukan autentikasi ke sebuah server *radius* yang diletakkan di lantai dua gedung GDLN Unud Denpasar. Pada penelitian ini akan menggunakan dua buah server autentikasi, hal ini dilakukan untuk menjaga kestabilan sistem dimana seandainya pada server autentikasi *primer* dalam keadaan *down* atau mati, maka akses poin selaku *NAS* (*Radius client*) akan secara otomatis akan merutekan proses autentikasi ke server *secondary* sesuai dengan setingan pada *NAS*, sehingga proses autentikasi tetap bisa berlangsung disaat server *primer* *down*

3. PEMBAHASAN

3.1 Konfigurasi Server Radius [6]

```
[root@radius ~]# updatdb
```

Install paket *freeradius* dan *freeradius-mysql* dengan command *yum*

```
[root@radius ~]# yum install -y freeradius
[root@radius ~]# yum install -y freeradius-mysql
[root@radius ~]# cd /etc/raddb/
```

Jalankan service *mysql*

```
[root@www raddb]# service mysqld start
```

Buat service *mysql* jalan untuk setiap kali booting

```
[root@radius ~]# chkconfig mysqld on
```

Buat password *mysql* untuk user *root*

```
[root@radius ~]# mysqladmin -uroot password
987654xxxxx
[root@radius raddb]# mysql -u root -p987654xxxxxx
mysql> exit
```

Buat database untuk server *radius* dengan nama database *radiusdb*. Username database *radiusdb* adalah "radius" dan passwordnya "radpass"

```
[root@radius raddb]# mysql -u root -p
Enter password:
mysql> create database radiusdb;
```

```
mysql> grant all on radiusdb.* to
      radius@localhost identified by
      "radpass";
mysql> flush privileges;
mysql> exit;
[root@radius raddb]# mysql -u root -p
Enter password:
mysql> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| dblogin       |
| mysql         |
| radiusdb      |
| test          |
+-----+
5 rows in set (0.01 sec)
```

Buatkan skema tabel untuk database server radiusnya

```
[root@radius raddb]# mysql -u radius -p radiusdb <
/usr/share/doc/freeradius-1.1.7/examples/mysql.sql
Enter password:
[root@radius raddb]# mysql -u radius -pradpass
radiusdb
```

```
mysql> show tables;
+-----+
| Tables_in_radiusdb |
+-----+
| nas                 |
| radacct             |
| radcheck            |
| radgroupcheck       |
| radgroupreply       |
| radippool           |
| radpostauth         |
| radreply            |
| usergroup           |
+-----+
9 rows in set (0.00 sec)
mysql> exit;
```

Rubah konfigurasi file radiusd.conf seperti di bawah ini (d disesuaikan dengan kebutuhan jaringan)

```
[root@radius local]# cd /etc/raddb/
[root@radius raddb]# vi radiusd.conf
....
port = 1812
....
log_auth = yes
....
log_auth_badpass = yes
log_auth_goodpass = yes
....
Modules {
pap {
    encryption_scheme = md5
    }
}
$INCLUDE ${confdir}/sql.conf
```

```
....
checkval {
    notfound-reject = yes
}
....
authorize {
    preprocess
    chap
    suffix
    files
    sql
    pap
}
....
authenticate {
    Auth-Type PAP {
        pap
    }
    Auth-Type CHAP {
        chap
    }
    Unix
....
accounting {
    detail
    unix
        radutmp
    sql
}
....
session {
    radutmp
    sql
}
....
post-auth {
    sql
}
....
```

Rubah konfigurasi file sql.conf seperti di bawah ini

```
[root@radius raddb]# vi sql.conf
sql {
    ...
    driver = "rlm_sql_mysql"
    server = "localhost"
    login = "radius"
    password = "radpass"
    radius_db = "radiusdb"
    acct_table1 = "radacct"
    acct_table2 = "radacct"
    postauth_table =
"radpostauth"
    authcheck_table =
"radcheck"
    authreply_table =
"radreply"
```

```

groupcheck_table =
"radgroupcheck"
groupreply_table =
"radgroupreply"
usergroup_table =
"usergroup"
nas_table = "nas"
deletestalesessions = yes
sqltrace = yes
sqltracefile =
${logdir}/sqltrace.sql
num_sql_socks = 5
connect_failure_retry_dela
y = 60
readclients = yes
...

```

Rubah konfigurasi file clients.conf seperti di bawah ini (disesuaikan dengan kebutuhan jaringan)

```

[root@radius raddb]# vi clients.conf
....
client 127.0.0.1 {
    secret    = wias1000g
    shortname = localhost
    nastype   = other
}
client 172.16.0.0/16 {
    secret    = wias1000g
    shortname = 172.16.0.0
    nastype   = other
}
client 172.15.0.0/16 {
    secret    = wias1000g
    shortname = 172.15.0.0
    nastype   = other
}
....

```

Jalankan debug mode radiusd dengan command seperti di bawah ini

```

[root@radius raddb]# radiusd -Xxx
...
Fri Jun 5 16:14:51 2009 : Debug: radutmp:
username = "%{User-Name}"
Fri Jun 5 16:14:51 2009 : Debug: radutmp:
case_sensitive = yes
Fri Jun 5 16:14:51 2009 : Debug: radutmp:
check_with_nas = yes
Fri Jun 5 16:14:51 2009 : Debug: radutmp:
perm = 384
Fri Jun 5 16:14:51 2009 : Debug: radutmp:
callerid = yes
Fri Jun 5 16:14:51 2009 : Debug: Module:
Instantiated radutmp (radutmp)
Fri Jun 5 16:14:51 2009 : Debug: Listening
on authentication *:1812
Fri Jun 5 16:14:51 2009 : Debug: Listening
on accounting *:1813

```

```

Fri Jun 5 16:14:51 2009 : Info: Ready to
process requests.

```

```

[root@radius raddb]# service radiusd start
Starting RADIUS server: Wed Jul 1
17:45:22 2009 : Info: Starting - reading
configuration files ...
[ OK ]
[root@radius raddb]# chkconfig radiusd on

```

3.2 Konfigurasi Web Radius [7]

Instal paket-paket php yang diperlukan seperti di bawah ini

```

[root@radius ~]# yum install php php-mysql php-
pear php-gd php-pear-DB -y

```

Pindahkan file-file php web based ke dalam direktori /var/www/ dan selanjutnya adalah mengubah hak akses direktori radius

```

[root@radius www]# chmod 644 /var/www/radius

```

Tambahkan skema tabel pada database server radius supaya bisa diintegrasikan dengan web based administration interface

```

[root@radius www]# mysql -u radius -pradpass
radiusdb < /var/www/radius/contrib/db/radius.sql
[root@radius www]# mysql -u radius -pradpass
radiusdb

```

```

mysql> show tables;
+-----+
| Tables_in_radiusdb |
+-----+
| billing_history |
| billing_paypal |
| billing_plans |
| billing_rates |
| dictionary |
| hotspots |
| nas |
| operators |
| proxys |
| radacct |
| radcheck |
| radgroupcheck |
| radgroupreply |
| radippool |
| radpostauth |
| radreply |
| realms |
| userbillinfo |
| usergroup |
| userinfo |
+-----+
20 rows in set (0.00 sec)

```

Buatkan file untuk log web radius dan rubah hak aksesnya

```

[root@radius www]# touch /tmp/webradius.log

```

```
[root@radius www]# chmod 644 /tmp/webradius.log
```

Rubah konfigurasi file php web radius supaya bisa diintegrasikan dengan database mysql yang sudah dibuat untuk server radius (sesuaikan dengan database yang sudah dibuat)

```
[root@radius www]# vi
/var/www/radius/library/webradius.conf.php
....
$configValues['CONFIG_DB_ENGINE'] =
'mysql';
$configValues['CONFIG_DB_HOST'] =
'127.0.0.1';
$configValues['CONFIG_DB_USER'] =
'radius';
$configValues['CONFIG_DB_PASS'] =
'radpass';
$configValues['CONFIG_DB_NAME'] =
'radiusdb';
$configValues['CONFIG_DB_TBL_RADC
HECK'] = 'radcheck';
$configValues['CONFIG_DB_TBL_RADR
EPLY'] = 'radreply';
$configValues['CONFIG_DB_TBL_RADG
ROUPREPLY'] = 'radgroupreply';
$configValues['CONFIG_DB_TBL_RADG
ROUPCHECK'] = 'radgroupcheck';
$configValues['CONFIG_DB_TBL_RADU
SERGROUP'] = 'usergroup';
$configValues['CONFIG_DB_TBL_RADN
AS'] = 'nas';
$configValues['CONFIG_DB_TBL_RADP
OSTAUTH'] = 'radpostauth';
$configValues['CONFIG_DB_TBL_RADA
CCT'] = 'radacct';
$configValues['CONFIG_DB_TBL_RADIP
POOL'] = 'radippool';
$configValues['CONFIG_DB_TBL_OPER
ATOR'] = 'operators';
$configValues['CONFIG_DB_TBL_HOTS
POTS'] = 'hotspots';
$configValues['CONFIG_DB_TBL_USERI
NFO'] = 'userinfo';
$configValues['CONFIG_PATH_RADIUS_
DICT'] = '/usr/share/freeradius';
$configValues['CONFIG_DB_PASSWORD
_ENCRYPTION'] = 'md5';
$configValues['CONFIG_LOG_FILE'] =
'/tmp/webradius.log';
$configValues['CONFIG_IFACE_TABLES
_LISTING'] = '25';
$configValues['CONFIG_IFACE_TABLES
_LISTING_NUM'] = 'yes';
$configValues['CONFIG_IFACE_AUTO_C
OMplete'] = 'yes';
$configValues['CONFIG_MAINT_TEST_U
SER_RADIUSSEVER'] = '127.0.0.1';
$configValues['CONFIG_MAINT_TEST_U
SER_RADIUSPORT'] = '1812';
```

```
$configValues['CONFIG_MAINT_TEST_U
SER_NASPORT'] = '1';
$configValues['CONFIG_MAINT_TEST_U
SER_RADIUSSECRET'] = 'wias1000g';
....
```

Tambahkan alias pada file konfigurasi httpd.conf supaya bisa diakses dari web browser seperti di bawah ini

```
[root@radius www]# vi /etc/httpd/conf/httpd.conf
....
Alias /hotspot "/var/www/radius/"
<Directory /var/www/radius/>
    Options None
    order deny,allow
    allow from 127.0.0.1
    allow from all
</Directory>
```

Tambahkan beberapa script pada file konfigurasi radiusd.conf untuk pemberian hak durasi waktu untuk user seperti di bawah ini

```
[root@radius www]# vi /etc/raddb/radiusd.conf
....
sqlcounter noresetcounter {
    counter-name = Max-All-Session-
Time
    check-name = Max-All-Session
sqlmod-inst = sql
    key = User-Name
    reset = never
    query = "SELECT
SUM(AcctSessionTime) FROM radacct
WHERE Username=% { %k }"
}
sqlcounter accessperiod {
    counter-name = Max-Access-
Period-Time
    check-name = Access-Period
sqlmod-inst = sql
    key = User-Name
    reset = never
    query = "SELECT
UNIX_TIMESTAMP() -
UNIX_TIMESTAMP(AcctStartTime)
FROM radacct WHERE Username =
' { %k }' ORDER BY AcctStartTime LIMIT
1"
}
sqlcounter accessperiodmonthly {
    counter-name = Max-Access-
Period-Time
    check-name = Access-Period-
Monthly
    sqlmod-inst = sql
    key = User-Name
    reset = monthly
    query = "SELECT
UNIX_TIMESTAMP() -
```

```

UNIX_TIMESTAMP(AcctStartTime)
FROM radacct WHERE Username =
'% { %k }' ORDER BY AcctStartTime LIMIT
1"
}
sqlcounter accessperiodweekly {
counter-name = Max-Access-
Period-Time
check-name = Access-Period-
Weekly
sqlmod-inst = sql
key = User-Name
reset = weekly
query = "SELECT
UNIX_TIMESTAMP() -
UNIX_TIMESTAMP(AcctStartTime)
FROM radacct WHERE Username =
'% { %k }' ORDER BY AcctStartTime LIMIT
1"
}
sqlcounter accessperioddaily {
counter-name = Max-Access-
Period-Time
check-name = Access-Period-
Daily
sqlmod-inst = sql
key = User-Name
reset = daily

```

```

query = "SELECT
UNIX_TIMESTAMP() -
UNIX_TIMESTAMP(AcctStartTime)
FROM radacct WHERE Username =
'% { %k }' ORDER BY AcctStartTime LIMIT
1"
}
....
Authorize {
...
noresetcounter
dailycounter
monthlycounter
accessperiod
...
}

```

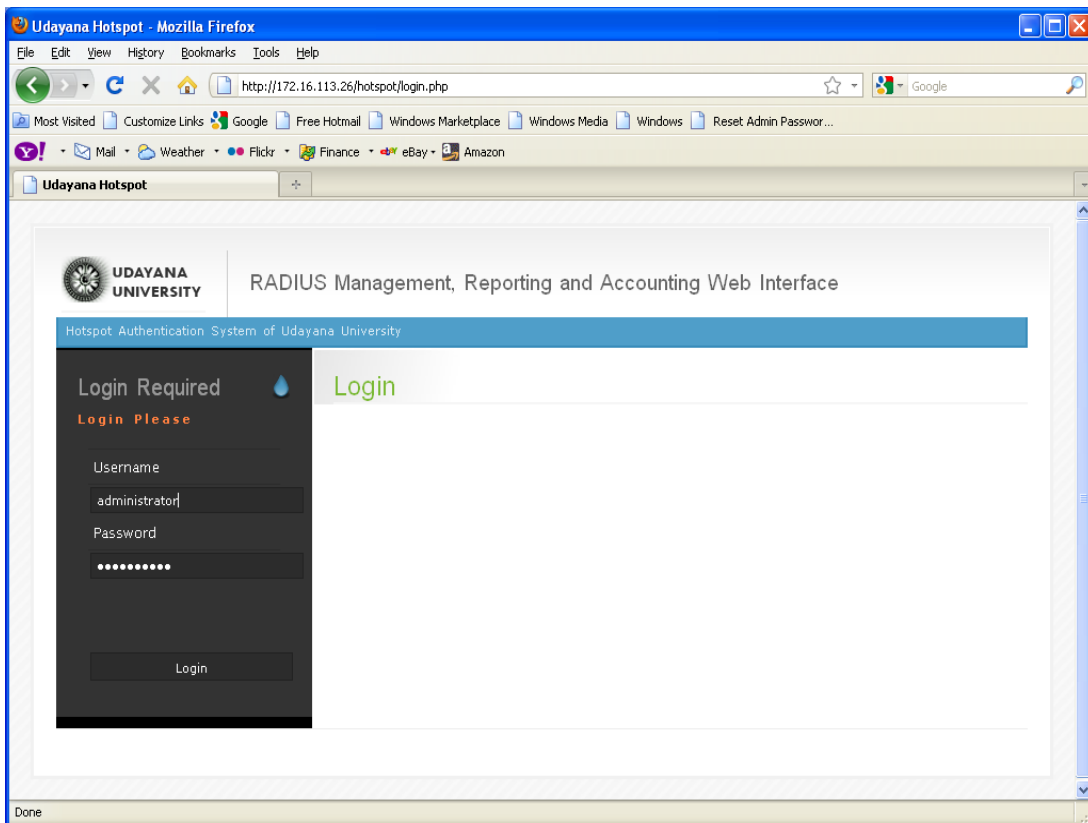
Setelah menambahkan script di atas maka restart service apache :

```

[root@radius www]# service httpd restart
Stopping httpd:
OK ]
Starting httpd:
OK ]

```

Kemudian akses web radius dari web browser anda dengan alamat <http://IPLocalhost/hotspot> dengan tampilan seperti di bawah ini



4. KESIMPULAN

Kesimpulan yang dapat ditarik dari pembahasan di atas adalah sebagai berikut:

1. Dalam mengimplementasikan sistem autentikasi *user* jaringan *hotspot* dengan sistem *radius*, diperlukan dua buah *server radius* yaitu satu untuk *server* utama dan satu untuk *server* cadangan yang terintegrasi dengan akses poin yang ada di Universitas Udayana, *server* ini yang akan menangani proses autentikasi, otorisasi dan *accounting* terpusat dengan spesifikasi *server* sebagai berikut :
 - Spesifikasi *PC* minimum *pentium IV*, *hardisk 80 GB*, *RAM 512 MB*
 - Sistem operasi yang digunakan yaitu *linux fedora core 8*
 - *MySQL-Server* sebagai *database user*
 - *Freeradius* sebagai protokol yang menangani autentikasi, otorisasi dan *accounting user*.
2. Dalam mengimplementasikan manajemen sistem yang berbasis *web interface*, diperlukan *web server* yang dalam penelitian ini dijadikan satu dengan *server radius*. Adapun spesifikasi *web based administration interface* yang digunakan pada sistem *radius* ini yaitu :
 - *Web server* dengan menggunakan *Apache*
 - *Web Based Administration Interface* dibuat dengan menggunakan bahasa pemrograman *PHP* dan *java script*.

5. DAFTAR PUSTAKA

- [1] Jim Geier, *Wireless Lans Implementing Interoperable Networks*, Macmillan Technical Publisig USA, 1999.
- [2] Josh. 2009. "*Implementasi 802.1x EAP-TLS & PEAP-MSCHAPv2*", *FreeRADIUS*
- [3] Hassell, J. "*O'Reilly : RADIUS*". 2002. O'Reilly.USA
- [4] Rody. 2009. "*Membangun Server Hotspot dengan Chillispot dan Freeradius*".
- [5] *Authentication, Authorization & Accounting With FreeRadius & MySQL Backend & Web Based Management with Daloradius*". Available <http://www.howtoforge.com>
- [6] *HowTo Use FreeRadius and MySQL*. Available <http://smallwhitecube.com>
- [7] *Install FreeRadius & MySQL*". available <http://www.tatang.web.id/>