Sistem Autentikasi Hotspot Menggunakan LDAP dan Radius pada Jaringan Internet Wireless Prodi Teknik Sistem Komputer

Ahmad Herdinal Muttaqin[1)], Adian Fatur Rochim[2)], Eko Didik Widianto[2)]
Program Studi Sistem Komputer, Fakultas Teknik, Universitas Diponegoro
Jalan Prof. Sudharto, Tembalang, Semarang, Indonesia

Wireless network is a network utilizing radio waves that propagate openly. This network requires security to simplify the process by using user Authentication. One of technology that could be used in order to make it safer is a Lightweight Directory Access Protocol (LDAP) and Remote Authentication Dila In User Service (RADIUS). Computer Systems Engineering Department is one of the study program in the Faculty of Engineering, University of Diponegoro that reserve the internet service everyday for students need. However, internet wireless network in this department is not yet safe enough,for the necessary to secure it's need creating a security system with LDAP and RADIUS.The results of this study is a network authentication server using OpenLDAP and FreeRadius Hotspot that will be integrated with an account of Academic Information System, which is implemented on Prodi Computer Systems Engineering Department of the University of Diponegoro.

Keywords : OpenLDAP, FreeRadius, Wireless, Hotspot, Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial In User Service (RADIUS).

I PENDAHULUAN

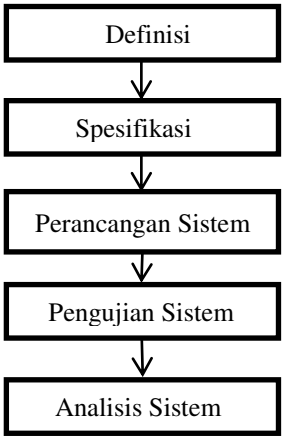
Saat ini beragam cara yang dapat dilakukan untuk memanfaatkan layanan internet mulai dari cara yang konvensional sampai pada pemanfaatan teknologi komunikasi bergerak. Prodi Teknik Sistem Komputer adalah salah satu prodi di Fakultas Teknik Universitas Diponegoro yang mempunyai layanan internet *wireless* untuk kebutuhan mahasiswa sehari-hari dalam mencari data dan informasi Akan tetapi jaringan wireless internet dijurusan ini belum cukup aman.

Berawal dari masalah-masalah tersebut banyak metode pengamanan jaringan wireless dari sekala pengamnan sederhana seperti seperti wpa (*wifi Protected Access)*, wpa2, wpa-psk dan sekala besar seperti metode sejenis yaitu sistem keamanan wireless perhotelan, perkantoran, dan perumahan yang menggunanakn *captive portal*. Selain ituada juga contoh fasilitas *hotspot* cakupan area seperti produk *wifiid* yang diluncurkan oleh ISP (*Internet Service Provider)*Telkomsel untuk bisa menggunakan aksesinternet di berbagai cakupan daerah di Indonesia, informasi ini dikutip di www.wifiid.com yang menjelaskan pengguna diharuskan membeli voucher untuk bisa mendapatkan akses internet di area yang sudah mencakup sinyal *wifiid*.

Berbagai macam bentuk pengamanan jaringan *wireless* sudah ada dan banyak ditemui di sekitar kita akan teteapi bentuk pengamanan jaringan *wirless* ini harus disesuaikan dengan situasi dan kondisi lingkungan yang ada. Seperti halnya pada dilingkungan kampus universitas diponegoro dengan memaanfatkan akun SIA (Sistem Informasi Akademik) yang bisa di integrasikan dengan pengamanan jaringan *hotspot* menggunakan LDAP dan RADIUS.Manfaat yang didapat dalam sistem ini adalah kemudahan bagi setiap mahasiswa Sistem Komputer yang hanya mempunyai satu akun terintegrasi untuk bisa mendapatkan fasilitas internet tanpa mengenyampingkan aspek keamanan yang ada.

II METODOLOGI PENELITIAN

Metodologi penelitian yang digunakan pada sistem autentikasi jaringan hotspot menggunakan Lightweight Directory Access Protocol (LDAP) dan remote authentication dial in user service (RADIUS) pada jaringan internet wireless prodi Teknik Sistem Komputer digambarkan pada Gambar 1 di bawah ini.



Gambar 1 Metode penelitian

Model ini melingkupi aktifitas-aktifitas sebagai berikut,

1 . Definisi Sistem

Mendefinisikan sistem yang akan dibuat dengan penjabaran awal sistem, identifikasi kebutuhan sistem, tujuan dan manfaat sistem, cara kerja sistem dan topologi jaringan sistem.

2 . Spesifikasi Kebutuhan

Proses spesifikasi kebutuhan akan menjabarkan tentang awal perancangan sistem dengan menentukan spesifikasi

kebutuhan yang sesuai definisi sistem. Spesifikasi kebutuhan terdiri atas spesifikasi perangkat keras dan perangkat lunak. Kegiatan ini menentukan arsitektur sistem secara keseluruhan. Perancangan perangkat lunak melibatkan identifikasi dan deskripsi abstraksi sistem perangkat lunak yang mendasar dan hubungan-hubungannya.

3 . Konfigurasi Sistem

Pada tahap ini, spesifiikasi kebutuhan yang telah di tentukan akan di rancang sesuai topologi/desain jaringan dan direalisasikan sebagai serangkaian program atau unit program yang memungkinkan untuk menjalankan tujuan sistem pada cara kerja sistem.

4 . Pengujian Sistem

Unit program diintegrasikan dan diuji sebagai sistem yang lengkap untuk menjamin bahwa persyaratan sistem telah dipenuhi. Setelah pengujian sistem, sistem siap digunakan dan dianalisis.

5 . Analisis Sistem

Unit yang telah diuji akan dilakukan analisis untuk mendapatkan hasil yang diinginkan.

III PERANCANGAN SISTEM

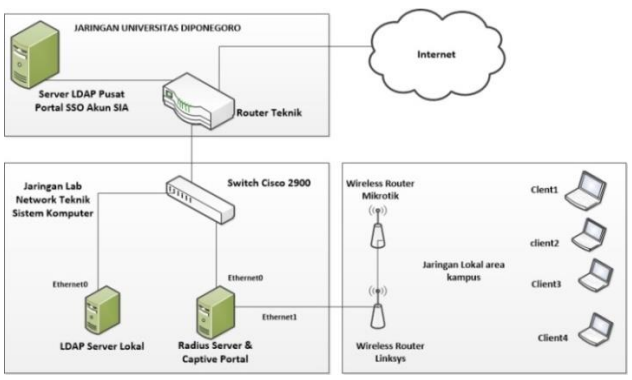
Definisi sistem akan menjabarkan awal sistem dibuat, tujuan, manfaat sistem, topologi jaringan dan cara kerja sistem yang akan digunakan untuk menentukan spesifikasi kebutuhan sistem ke tahapa selanjutnya, beberapa tahapan untuk bisa mendeffinisikan sistem yang telah dibuat adalah sebagai berikut:

A. Inisialisasi awal sistem

Pada tahap ini sistem dibuat sesuai dengan kebutuhan layanan jaringan *wireless* yang ada di kampus Teknik Sistem Komputer dengan pemanfaatan fasilitas komputer yang bisa digunakan untuk kebutuhan peniliatan. Sistem yang digunakandidalam penelitian ini menggunakan LDAP dan RADIUS yang saling terintegrasi dalam pencocokan akun dilengkapi dengan *captive portal* sebagai antarmuka dalam proses *login* jaringan hotspot.

1. Topologi Jaringan

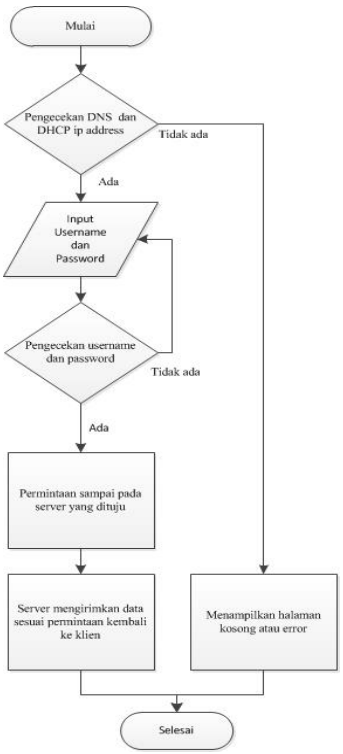
Sistem ini didesain terlebih dahulu menggunakan topologi jaringan. Topologi jaringan merupakan hal yang menjelaskan hubungan geometris antara unsur-unsur dasar penyusun jaringan, yaitu *node*, *link*, dan *station*. Topologi jaringan sistem ini dibuat dengan aplikasi *Microsoft visio* yang disusun sesuai kebutuhan sistem yang akan dibuat. Berikut topologinya



Gambar 2 Topologi Jaringan

2. Cara Kerja Sistem

Sistem autentikasi jaringan *hotspot* menggunakan LDAP dan RADIUS terdiri atas 2 *server* yang tersedia. Dimana LDAP *server* akan menjadi server *directory database* sedangkan *server* RADIUS adalah server autentikasi dan *captive portal* sebgai antarmuka langsung ke jaringa lokal hotspot kampus. tersebut akan diakses oleh klien melalui jaringan lokal. Cara kerja sistem autentikasi *hotspot*menggunakan LDAP dan RADIUS ini akan dijelaskan pada Gambar 3.



Gambar 3 Diagram alir cara kerja sistem

B. Spesifikasi Kebutuhan

1. Spesifikasi Perangkat Keras

Didalam penilitian ini digunakan 2 komputer server yang berada di laboratorium jaringan berikut spesifikasinya:

1. *Server* 1
   Server ini digunanakan sebagai *server* LDAP untuk penyimpanan database accaount user

Gambar 4.Spesifikasi server 1.

Perangkat keras yang digunakan dalam penelitian tugas akhir ini adalah seperti yang terlihat pada Gambar 3 mempunyai sepesifikasi *ProcessorIntel Cori3 Processor, ~2.8GHz; RAM 4 Ghz RAM; SystemManufactureMSI, Lan PCI Xpress* dan penyimpanan *memory Hardisk* sebesar *250 Ghz*

2. *Server* 2
   Server ini digunakan sebagai server RADIUS yang berfungsi melakukan autentikasi data informasi *account* pada *server* LDAP.

Gambar 5 Spesifikasi *server* 2

Perangkat keras yang digunakan dalam server ini meliputi *ProcessorIntel Core 2 duo,* RAM 1Ghz 2 LAN PCI *Xpress* media penyimpanan *Hardisk* 150 Ghz dan *System Manufacture* HP (Hewlett Packard) .

3. Router Linksys WRT54GL

Gambar 6 Router Linksys

Spesifikasi dari router Linksys adalah sebagai berikut *All in one internet sharing router*, 4 *port switch* dan 54 Mbps *wireless-G 802.11g access point. Shares a single internet connection and other resoureces* dengan kabel *Ethernet* dan *Wireless-G High security :*TKIP dan AES *encryption, wireless Mac addrees filtering, powerful* SPI *firewall.*

2. Spesifikasi Perangkat Lunak

1. Sistem Operasi *Ubuntu Server 14.04*
   Pada komputer yang akan menjalankan LDAP *server* telah tertanam sistem operasi Ubuntu berbasisi LINUX 64 *bit*. *Ubuntu* merupakan salah satu distribusi *Linux* yang berbasiskan *Debian* dan didistribusikan sebagai perangkat lunak bebas.*Ubuntu* versi ini dirancang untuk kepentingan penggunaan *server*. Sistem operasi ini digunakan pada LDAP *server* dan RADIUS *server*
2. *OpenLDAP*
   Perangkat lunak yang bersifat *opensource* untuk menjalankan server ldap sebgai pengelola directori database. Perangkat lunak ini release terbaru dengan versi openldap 2.4.4.
3. *PHPLDAPAdmin*
   Selain OpenLDAP didalam server LDAP juga terdapat PHPLDAPAdmin sebagai antarmuka pengelolaan database khusus LDAP berbasis web dengan versi 1.2.
4. *FreeRADIUS*
   FreeRADIUS adalah perangkat lunak yang bersifat opensource untuk menjalankan *server RADIUS* versi yang digunakan yaiut *FreeRADIUS* 2.2.7.
5. *CoovaChilli*
   CoovaChilli merupakan perangkat lunak *captive portal* geratis pegembangan dari *chillispot*.Pada system ini digunakan *covachilli* versi 1.3.0.
6. PHP 5
   PHP adalah bahasa pemrograman dengan semua sintaks yang diberikan akan sepenuhnya dijalankan pada *server* dan hasilnya dikirimkan ke *browser*. Versi PHP yang digunakan dalam tugas akhir ini adalah PHP versi 5.
7. LAMPP
   LAMPP adalah sebuah aplikasi *web serverApache* yang di dalamnya sudah tersedia *database* server MySQL dan *support* php *programming*. Komponen LAMPP yaitu *Apache*, PHP, MySQL dan phpMyAdmin.LAMPP merupakan aplikasi yang mudah digunakan, gratis dan mendukung instalasi di *Linux* dan *Windows*.Keuntungan lainnya adalah cuma menginstal satu kali sudah tersedia *Apache* Web Server, MySQL *DatabaseServer*, PHP *Support* (PHP 4 dan PHP 5) dan beberapa modul lainnya.
8. BIND
   BIND merupakan salah satu implementasi DNS yang paling banyak digunakan pada server di *Internet*. BIND yang digunakan pada virtualisasi jaringan ini adalah BIND9 yang berjalan pada sistem operasi *UbuntuServer* 14.04.
9. *Putty*
   Putty adalah aplikasi terminal akses yang digunakan untuk buat *remoteconnection* komputer melalui *port* SSH atau sebagainya.

III PENGUJIAN UNIT

Berdasarkan perancangan sistem yang telah dibuat pada BAB 3, maka dihasilkan sebuah sistem autentikasi hotspot menggunakan LDAP dan RADIUS.Sistem ini menyediakan infrastruktur keamanan yang berdasarikan autentikasi data informasi akun pada direktori terpusat bertujuan untuk efisiensi pengelolaan jaringan lokal dalam penggunan jaringan internet kampus. Pemanfaatan teknologi ini mengharuskan klien melakukan proses autentikasi terlebih dahulu sebelum menggunakan fasilitas internet, jika tidak maka penggunaan akses internet tidak bisa digunakan. Tahap pengujian pertama dalam sistem ini adalah melakukan pengujian terhadap sistem autentikasi hotspot menggunakan LDAP dan RADIUS. Tahapan ini terbagi menjadi dua skenario pengujian yang dilakukan oleh admin, antara lain sebagai berikut:

1. Skenario pengujian *server* LDAP dan antarmuka Phpldapadmin
2. Skenario pengujian *server* RADIUS dan *Captive portal*

1. Pengujian*Server*LDAP

Tahap pengujian ini dilakukan untuk mengetahui bagaimana cara menggunakan dan mengelola sebuah *Server* LDAP menggunakan OpenLDAP yang berfungsi sebaga *backend* database yang digunakan untuk penyimpanan akun *login user*, selain itu ditambahkan juga antarmuka phpldapadmin yaitu perangkat lunak yang berbasis web yang berfungsi untuk mengatur dan memudahkan pengelolaan akun di dalam LDAP *server* melalu *web browser*. Untuk memulai pengujian *server* ini kita jalankan *server* yangs sudah terinstal *Ubuntu Server* 14.04 dan Openldap. Berikut adalah komputer *server* yang sudah terinstall *Ubuntu Server* 14.04dan Openldap yang ditunjukan pada Gambar 7

```
 * Documentation:  https://help.ubuntu.com/
Last login: Wed Nov 11 05:47:16 2015
ldapserver@192:~$ sudo su
[sudo] password for ldapserver:
root@192:/home/ldapserver# /etc/init.d/slapd start
 * Starting OpenLDAP slapd                                        [ OK ]
root@192:/home/ldapserver#
```

Gambar 7 Pengujian integrasi login sistem

Setelah Openldap dijalankan pengelolaan databases bisa diakses langsung melalui perangkat lunak berbasis web yaitu phpldapadmin yang bisa diakses melalui *web browser* dengan mengetikan alamat url ip address seperti berikut 10.42.12.55/phpldapadmin seperti ditunjukan pada Gambar 8

Gambar 8 Tampilan Phpldapadmin

2. Prngujian Server RADIUS

Pengujian *server* RADIUS dilakukan dengan cara menguji hasil konfigurasi dan sinkronisasi terhadap *server* LDAP untuk proses autentikasi user ketika *login*. Porses ini memungkinkan *server* RADIUS meneruskan paket data akun *user* yang diminta *user* dan melakukan sinkronisasi antara *server* LDAP apakah data *user* yang di *request* teruatentikasi atau tidak.Dalam pengujian ini *server* RADIUS menggunakan perangkat lunak Freeradius yang bersifat *opensource* yang bisa digunakan sebagai radius *server*.Untuk memulai pengujian telah disiapkan sebuah komputer *server* yang sudah terinstal Ubuntu *server* 14.04 dan freeradius *server*. Dalam *server* ini freeradius telah selesai dikonfigurasi pada file modul ldap untuk bisa binding ke *server* ldap seperti pada Gambar 9

```
ldap {
        #
        #  Note that this needs to match the name in the LDAP
        #  server certificate, if you're using ldaps.
        server = "10.42.12.55"
        identity = "cn=admin,dc=test,dc=com"
        password = ldap1234
        basedn = "dc=test,dc=com"
        filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
        #base_filter = "(objectclass=radiusprofile)"

        #  How many connections to keep open to the LDAP server.
        #  This saves time over opening a new LDAP socket for
        #  every authentication request.
        ldap_connections_number = 5

        # seconds to wait for LDAP query to finish. default: 20
        timeout = 4

        #  seconds LDAP server has to process the query (server-side
        #  time limit). default: 20
        #
        #  LDAP_OPT_TIMELIMIT is set to this value.
        timelimit = 3
```

Gambar 9 File Modul Ldap

File modul ldap ini yang berfungsi untuk singkronisasi dengan server ldap agar bisa saling terhubung ketika proses autentikasi berjalan. Dalam file modul LDAP ini kita diminta mengisi sertifikat server agar server RADIUS bisa mengakses server LDAP untuk mengambil data dari database dengan mengisi perintah "`server = "10.42.12.55"`" yaitu IP address server LDAP, *domain component* beserta password *administrator* server LDAP "`identity = "cn=admin,dc=test,dc=com"`', `password = ldap1234`. Selanjutnya setelah semua proses konfigurasi selesai kita menjalankan debug program freeradius agar bisa mengeksekusi file yang telah dimodifikasi. Terlebih dahulu kita harus mengheentikan dengan perintah `/etc/init.d/freeradius stop`, setelah itu jalankan perintah freeradius –X seperti yang ditunukan pada Gambar 10.

```
root@192:/home/radiusserver# freeradius -X
FreeRADIUS Version 2.1.12, for host i686-pc-linux-gnu, built on Feb 24 2014 at 15:00:10
Copyright (C) 1999-2009 The FreeRADIUS server project and contributors.
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE.
You may redistribute copies of FreeRADIUS under the terms of the
GNU General Public License v2.
Starting - reading configuration files ...
including configuration file /etc/freeradius/radiusd.conf
including configuration file /etc/freeradius/proxy.conf
including configuration file /etc/freeradius/clients.conf
including files in directory /etc/freeradius/modules/
including configuration file /etc/freeradius/modules/digest
including configuration file /etc/freeradius/modules/detail
including configuration file /etc/freeradius/modules/soh
```

Gambar 10 Run Freeradius –X

Setelah menjalankan freeradius langkah selanjutnya adalah mencoba melakukan radtest ke server ldap. Radtest adalah perintah yang dilakukan untuk mencoba mengambil data user oleh server radius untuk membuktikan proses binding ke server ldap telah tersambung. Kita akan mencoba melakukan radtest ke akun user yang telah teredaftar di server ldap yaitu akun Asep Unyil. Perintah radtest bisa kita lihat pada Gambar 11

```
root@ubuntu-ldap:/home/ldapserver# radtest aunyil asep1234 localhost 181
g123
Sending Access-Request of id 99 to 127.0.0.1 port 1812
        User-Name = "aunyil"
        User-Password = "asep1234"
        NAS-IP-Address = 10.42.12.33
        NAS-Port = 1812
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=99, len
root@ubuntu-ldap:/home/ldapserver#
```

Gambar 11 Testing Radtest

3. Pengujian *Captive Portal*

Pengujian *captive portal* ini dilakukan bersamaan dengan penjugian RADIUS dikarenakan komputer *server* yang dipakai untuk keduanya sama dalam satu server. Pengujian *captive portal* ini dilakukan dengan menguji proses autentikasi, tampilan antarmuka dan sistem yang dibangun agar semua interkoneksi jaringan dari local ke public berhasil diblok oleh *captive portal*. Selain itu pengujian ini mengharuskan caprive portal bisa terhubung ke server RADIUS dalam mengambil data user di *server* LDAP.Dalam pengujian ini pernagkat lunak yang dipakai untuk membuat *captive portal* adalah coovachilli yang sudah terinstall pada computer server yang memiliki sistem operasi Ubuntu *Server* 14.04 dan syaratnya komputer server ini harus memiliki 2 *ethernet card*.*Ethernet* 1 terhubung ke jaringan internet dan *Ethernet* 2 terhubung ke jaringan local.tahapan pertama dalam pengujian adalah dengan mulai menjalankan coova chilli dengan perintah /etc/init.d/chilli start seperti pada Gambar 12.

```
root@ubuntu-ldap:/home/ldapserver# /etc/ini
Starting chilli: chilli.
root@ubuntu-ldap:/home/ldapserver#
```

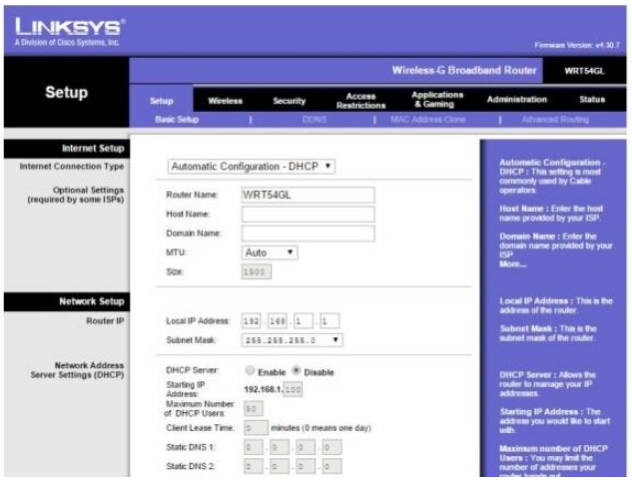
Gambar 12 Menjalankan program chilli

Captive portal mempunyai fungsi untuk memblok smua aliran paket data dan koneksi dari local ke publik dan mengharuskan *client* melakukan autentikasi terlebih dahulu apabaila terhubung ke jaringan publik atau internet. Untuk itu ketika kita menjalankan coovachilli untuk bisa memamkai fasilitas internet covachilli mempunyai fitur untuk membuat *tunel* secara otomatis dari *Ethernet* yang terhubung ke jaringan local dalam kasus ini *Ethernet* yang digunakan adalah eth1 dengan memberikan ip secara DHCP (*Dynamic Host Control Protcol*) dengan range ip 192.168.100.0/24 dan gateway 192.168.100.1 seperti pada Gambar 13

```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-
-00
          inet addr:192.168.100.1  P-t-P:192.168.100.1  Mask:255.255.255.0
          UP POINTOPOINT RUNNING  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Gambar 13 Tunnel Gateway

Gambar 12 menunjukan seteah coovachilli aktif akan menjalankan *tunneling* secara otamtis sesuai dengan konfigurasi yang dibuat. Dalam kasus ini *client* dari jaringan lokal akan di beri rentang ip dari 192.168.100.2 sampai dengan 192.168.100.254 secara DHCP sehingga *client* tidak perlu mensetting ip secara manual baik secara wireless maupun kabel. Langkah selanjutnya mengkonfigurasi *router wireless* Linksys yang berfungsi membrodcast jaringan wifi pada jaringan lokal. Konfigurasi yang dilakukan adalah dengan cara membuant koneksi *bridging* pada lynksis sepert pada Gambar 14



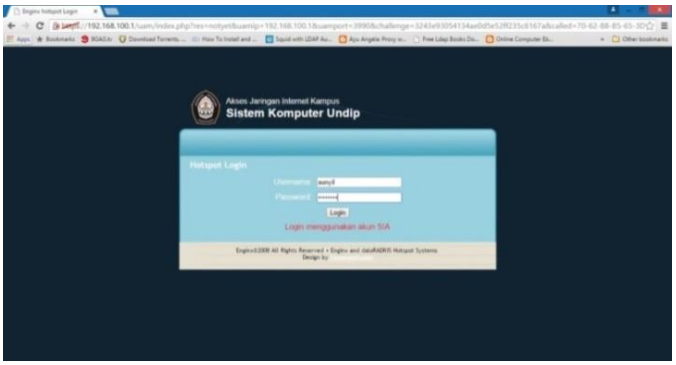
Gambar 14 Konfigurasi Bridge pada Router Linksys

Cara untuk membuat koneksi *bridging* adalah dengan membuat setiingan DHCP disable. Konfigurasi bridging berfungsi untuk bisa meneruskan koneksi dari *captive portal* agar konfigurasi *captive portal*akan diterima *client* secara langung. Saat ini *captive portal* sudah siap menerima *request* dari *client*, untuk mengujinya *router* Linksys harus terhubung dengan jaringan local dan mulai mengkasesnya melalu *web browser* seperti pada Gambar 15

Gambar 16 Captive Portal Login

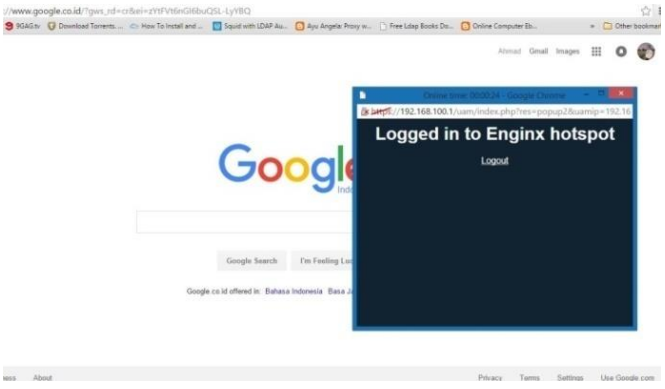
Setelah *Captive portal* berjalan, proses autentikasi akan di minta terus ketika *client* mengakses jaringan internet melalui *web browser*. Selama *client* belum melakukan porses autentikasi dihalaman login ini *client* tidak akan pernah bisa mengakses internet. Setiap kali *client* memasukan alamat url apapun halaman browser akan terus mendirect ke halaman login ini. Pengujian selanjutnya apakah client bisa melakukan autentikasi atau tidak, pada tahap ini akan mencoba dengan

autentikasi dengan data akun Asep Unyil dengan *username* aunyil dan *password* asep1234 seperti pada Gambar 17



Gambar 17 Autentikasi User Aunyil

Jika proses autentikasi berhasil maka *client*sudah bisa mengakses jaringan internet, kemudian pada *web browser* akan menambahkan sesi halaman web baru untuk halaman logout dan lamanya waktu ketika kita menggunakan internet. Seperti pada Gambar 18



Gambar 18 Login berhasil

Tahap pengujian yang dilakukan menunjukkan sistem memiliki fungsi yang bekerja dengan benar.

IV PENUTUP

A Kesimpulan

Selama pengembangan sistem ini terdapat beberapa hal yang bisa disimpulkan. Kesimpulan yang didapatkan antara lain:

1. Rancang bangun Sistem autentikasi hotspot menggunakan LDAP dan RADIUS telah berhasil dibangun pada jaringan internet kampus TEknik Sistem Komputer Univeristas Diponegoro. Sistem ini dibangun denga 2 mesin server dan 1 Router
2. Setiap server saling terintegrasi dan terkoneksi dengan jaringan internet kampus, Server RADIUS bisa melakukan ases ke database LDAP server menggunak Radtest.
3. Pembuatan user akun pada LDAP telah berhasil dengan menggunakan antarmuka phpldapadmin yang diakses melalu we browser
4. Proses autentikasi hotspot menggunakan antarmuka login *captive portal* covachilli yang memblok jaringan lokal sehingga *client* tidak diijinkan masuk pada jaringan internet kampus sebelum *login*.
5. Sistem keamanan pada LDAP server menggunakan SSL (*Secure Socket Layer)* dan autentikasi ganda ketika menggunakan antarmuka phpldapadmin.
6. Antarmuka Captive Portal akan terus melakukan redirect link ketika login gagal, sehingga *client* tidak bisa mengakses laman dan alamat web yang akan diakses.
7. *Server* RADIUS berhasil melakukan binding ke server LDAP pusat yang ada di Universitas Diponegoro untuk bisa melakukan proses autentikasi menggunakan akun SIA melewati perantara portal SSO (*Single Sign On*) Universitas Diponegoro.

B. Saran

1. Penelitian lanjutan untuk menenamkan sistem yang sudah ada dengan menambahkan kapasitas memori dan prosesor untuk diimplementasikan
2. Penelitian lanjutan untuk adanya pengelolaan akun SIA olen admistrator jaringan kampus.
3. Penelitian lanjutan untuk menambahkan kapasitas *acces point* agar lebih stabil ketika diakses oleh banyak mahasiswa.

()

DAFTAR PUSTAKA

[1] Azikin, A. (2011). *Debian GNU/Linux.* Bandung: Informatika Bandung.

[2] Djunawidjaja, J. (2005). Integrasi User Account Dengan LDAP. *Majalah Info Linux*.

[3] Dwi Hantoro, G. (2005). *Wifi (Wireless LAN).* Bandung: Informatika Bandung.

[4] Komputer, Wahana. (2009). *Langkah Mudah Administrasi Jaringan Menggunakan Linux Ubuntu.* Yogyakarta: Andi Publisher Yogyakarta.

[5] Mulyono, H. 2. (2008). *Buku Pintar Komputer.* Jakarta: Kriya Pustaka Jakarta.

[6] S. Mulyanta, E. (2005). *Pengenalan Protokol Jaringan.* Yogyakarta: C.V Andi OFFEST Yogyakarta.

[7] Sugeng, W. (2010). *Jaringan Komputer Dengan TCP/IP.* Bandung: Modula Bandung.

[8] Sukmaji, A. R. (2008). *Jaringan Komputer.* Yogyakarta: Andi Publisher Yogyakarta.

[9] Syafrizal, M. (2008). *Jaringan Komputer.* Yogyakarta: Andi Publisher Yogyakarta.

[10] Wahyono, T. (2003). *Prinsip Dasar Dan Teknologi Komunikasi Data.* Yogyakarta: Amikom Yogyakarta.

[11] *Survey*. (2009, August 3). Retrieved July 14, 2015, from www.freeradius.org: http://freeradius.org/press/survey.html

[12] *Openldap, Kurt D.Zeilenga*. (2014, April 3). Retrieved October 9, 2015, from www.openldap.org: http://www.openldap.org/project/kurt/