PERANCANGAN MEDIA OTENTIKASI MENGGUNAKAN *CAPTIVE PORTAL* PADA JARINGAN *WIRELESS* LABORATORIUM KOMPUTER TEKNIK ELEKTRO UNIVERSITAS DIPONEGORO

Mochamad Arif Haryadi[*)], Maman Somantri, and Yuli Christyono

Departemen Teknik Elektro Fakultas Teknik Universitas Diponegoro
Jl. Prof. Sudharto, Tembalang, Semarang, Indonesia

[*)]*Email: moch.arif.hr@gmail.com*

Abstrak

Penggunaan media Internet pada lingkungan kampus semakin hari semakin meningkat. Para mahasiswa menggunakan media internet melalui Access Point. Dimana dalam mengakses melalui Access Point tidak menggunakan otentikasi apapun sehingga kita tidak dapat mengetahui siapakah pengguna media internet pada lingkungan kampus. Hal ini dapat menyebabkan penggunaan internet yang tidak sebanding dengan ketersediaan bandwidth yang diberikan untuk Access Point. Karena itulah diperlukan adanya sistem otentikasi untuk menjaga dari pengguna yg tidak merupakan warga dari fakultas teknik elektro. Dalam penelitian ini melakukan perancangan sistem otentikasi dengan menggunakan *captive portal* sebagai portal otentikasi dengan sistem operasi menggunakan ubuntu. Dimana *captive portal* terhubung dengan server RADIUS sebagai media otentikasi. RADIUS yang dipakai menggunakan freeradius. Hasil penelitian menunjukkan bahwa sistem otentikasi berjalan sesuai dengan yang direncanakan. Dimana hanya yang memiliki user yang dapat mengakses jaringan internet kampus, dan pembatasan bandwidth yang berjalan sesuai jenis user yang ada.

Kata kunci : Access Point, bandwidth, captive portal, RADIUS, FreeRADIUS

Abstract

Internet use in campus enviroment is increase rapidly. Many college students using the internet via Access Point. In which many of the Access Point doesn't use any authentication. And because of that we didn't know who is the one only using or abusing the use of internet on campus. This may lead to the use of the internet which is not comparable with the availability of bandwidth given by University. Because of that we need to secure our internet network from people outside electrical engineering. In this study perform authentication system design by using *captive portal* as a portal authentication with the operating system using ubuntu. Where a *captive portal* to connect with the RADIUS server as the authentication media. RADIUS is used using FreeRADIUS. The results showed that the authentication system goes as planned. *captive portal* can be used to handle user authentication using a username and password registered in the server. Where only a user with acess that can use internet in the campus, and bandwidth restrictions that go according to the existing user.

Keywords : Access Point, Bandwidth, Captive portal, RADIUS, FreeRADIUS

1. Pendahuluan

Pengguna Internet pada kampus semakin hari semakin banyak. Pada laboratorium masing-masing jurusan memiliki pengguna yang sedikit. Namun pengguna Internet pada jaringan umum seperti pada Access Point semakin hari semakin banyak sehingga setiap harinya terdapat aktifitas lalu lintas jaringan yang tinggi. Dalam kesehariannya terkadang pemakaian bandwidth yang ada bisa berlebihan dan tidak sesuai dengan kebutuhan dari masing-masing pengguna Internet.

Adanya ketidakseimbangan antara ketersediaan bandwidth dengan meningkatnya pengguna Internet akan mengakibatkan makin lambatnya akses Internet, disamping itu bebasnya penggunaan *Wireless* Acces Point juga mempengaruhi. Dengan adanya masalah ini maka diperlukan sebuah sistem yang dapat melakukan penyaringan pengguna pada *Wireless Access Point* ketika akan mengakses Internet sehingga jaringan tidak penuh oleh pengguna-pengguna yang bukan merupakan bagian dari teknik elektro UNDIP.

Captive portal merupakan salah satu metode yang digunakan untuk mengamankan dan membatasi akses pada suatu jaringan *Internet*. Dimana *Server* bekerja sebagai router atau gateway yang memproteksi atau tidak mengizinkan adanya trafik jaringan sebelum user melakukan registrasi. Pada perkembangannya *Captive portal* terintegrasi dengan alat lain seperti Mikrotik.

Pada Penelitian sebelumnya telah banyak implementasi *captive portal* sebagai pengaman jaringan. Diantaranya penggunaan *captive portal* dengan menggunakan Pfsense yang berbasis freebsd[5]. Serta penggunaan mikrotik sebagai *captive portal*[1]. Terdapat juga yang menggunakan aplikasi EasyHotspot sebagai *captive portal*[8]. Ada juga penelitian lain yang menggunakan ChilliSpot sebagai *captive portal*[4] Penelitian lain adalah tentang penggunaan bandwidth management pada *captive portal* untuk membatasi besarnya pertukaran data pada pengguna[7].

Pada perancangan ini dibuat *captive portal* yang menggunakan sistem operasi Ubuntu 15.04 yang terintegrasi dengan CoovaChilli, dan FreeRADIUS. Dimana pengguna mengakses melalui *Wireless Access Point* yang dirancang dengan metode bridge dimana lebih dari satu *Wireless* access point namun tetap memiliki network yang sama.

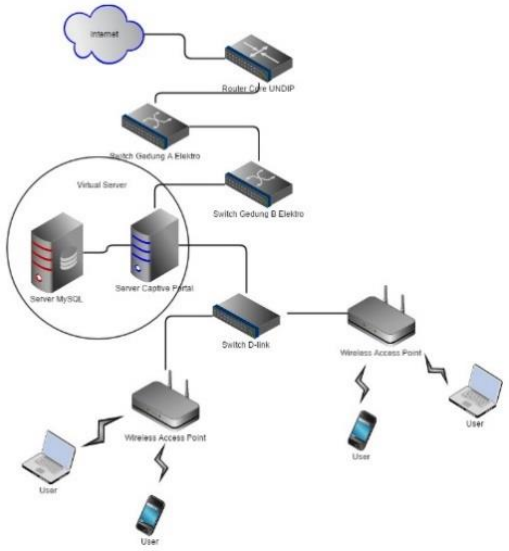
2. Metode

2.1. Deskripsi Sistem

Server gateway captive portal merupakan server yang menyediakan layanan RADIUS untuk autentikasi dalam penggunaan jaringan Internet. RADIUS memungkinkan autentikasi bisa dilakukan dengan mengambil data *username* dan *password* dari *server* MySQL yang telah dibuat sebelumnya. RADIUS hanya menyediakan fasilitas untuk autorisasi dan autentikasi saja, sehingga diperlukan CoovaChilli sebagai *walled-garden* untuk bisa mencegat dan mengarahkan pengguna yang ingin terhubung ke Internet ke sebuah halaman yang mengharuskan pengguna untuk *login* menggunakan username dan password yang terdaftar di *server* MySQL.

CoovaChilli juga menggunakan aplikasi *web captive portal* Enginx yang digunakan untuk mengirimkan parameter *access controller* yang terhubung ke *server* RADIUS. Parameter ini digunakan untuk mengirimkan dan menampilkan status dari pengguna melalui tampilan *web*. Enginx *website* akan mempermudah pengguna untuk melakukan *login* dan *logout* karena *interface web*-nya yang berbasis GUI, sehingga tinggal mengisi *field* yang disediakan.

Gambar 1 merupakan topologi fisikal yang menunjukkan rancangan sistem *captive portal* yang akan digunakan. Topologi fisikal menjelaskan mengenai tata letak secara fisik tentang perangkat yang terkoneksi ke jaringan. Topologi fisikal dibuat sesuai dengan pengkabelan dan komponen yang dipakai pada jaringan yang sebenarnya, sehingga memuat tipe perangkat , model dan pabrikan dari perangkat , lokasi, dan pengkabelan dari *point* ke point.



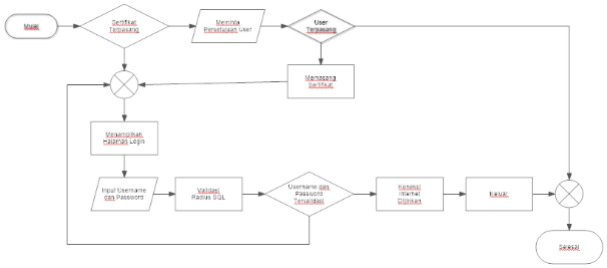
Gambar 1. Topologi Fisikal perancangan *server gateway captive portal*

2.2. Proses Autentikasi pada *Server Gateway Captive portal*

Web browser pengguna harus memasang sertifikat yang dimiliki *server* untuk dapat memasuki halaman HTTPS *login CoovaChilli*. Permintaan pemasangan sertifikat sesuai dengan persetujuan pengguna akan muncul, bila belum terpasang sertifikat. *CoovaChilli* akan menampilkan halaman *login* untuk memasukkan *username* dan *password* bagi pengguna. Proses autentikasi ini nantinya akan divalidasi oleh FreeRADIUS ke *server MySQL*. Alur autentikasi sistem ini dapat dilihat pada diagram alir yang ditunjukkan pada Gambar 2.

Diagram alir pada Gambar 2 dapat dijelaskan sebagai berikut:

1. Memeriksa sertifikat yang terpasang di dalam *web browser*.
2. Jika sertifikat belum terpasang maka akan muncul permintaan pemasangan sertifikat.
3. Sesuai dengan persetujuan pengguna maka sertifikat akan dipasang didalam aplikasi *web browser* pengguna. Jika pengguna tidak setuju maka tidak akan dapat memasuki halaman *login*.
4. Pada halaman *login user* memasukan *username* dan *password.*
5. *Username* dan *password* akan divalidasi oleh FreeRADIUS yang sudah terhubung dengan *server MySQL* sebagai media penyimpanan informasi *user* FreeRADIUS.
6. Jika *username* dan *password* tervalidasi maka autentikasi berhasil dan koneksi Internet diijinkan.
7. Jika autentikasi gagal maka kembali ke halaman *login*.



Gambar 2. Diagram alir autentikasi pada *server gateway captive portal*

2.3. Perancangan *Wireless Router* dengan mode *Bridge* dan SSID Tunggal

Sistem ini memerlukan 2 *Wireless Router* dimana *Wireless Router* tersebut akan digunakan sebagai *access point* untuk para mahasiswa. Setting yang akan digunakan yaitu mode *Bridge* , mode *Bridge* ini membuat *Wireless Router* hanya berfungsi sebagai *access point*, sehingga *network* yang diakses oleh mahasiswa pada 2 *Wireless router* tersebut merupakan satu network dengan Server *Captive portal*. Hal ini dapat terlihat pada Gambar 1 dimana 2 *Wireless router* tersambung dengan kabel ke *switch* kemudian *switch* ke *Server Captive portal*.

Dua *Wireless* AP tersebut menggunakan SSID (*Service Set Identifier*) yang sama yaitu "Labkom" namun *channel Wireless* yang akan digunakan berbeda, Penggunaan SSID yang sama bertujuan agar ketika mahasiswa berpindah dari satu tempat dengan *access point* pertama ke tempat dengan *access point* kedua tidak perlu untuk memutuskan koneksi dan otomatis berpindah dari *access point* pertama ke kedua dan mahasiswa tidak perlu untuk *login* kembali ke *captive portal* karena ip address yang digunakan masih sama.

3. Hasil dan Analisa

3.1. Pengujian Otentikasi *Captive portal*

Pengujian autentikasi *captive portal* memerlukan sebuah pengguna dengan pengaturan *interface* ke mode DHCP, agar mendapatkan alamat IP, *subnet mask*, dan *server* DNS dari *interface* yang digunakan pada *server gateway captive portal* secara automatis. Pengguna masih belum bisa terhubung ke jaringan luar atau Internet meskipun telah diberikan pengaturan alamat IP dan sebagainya.

3.2. Pengujian *redirecting* halaman web

Pada pengujian *redirecting* dilakukan dengan menggunakan *web browser* untuk mengakses sebuah situs di *Internet* dan mengecek respon dari *captive portal* untuk mengalihkan ke halaman *login captive portal*. Gambar 3 menunjukkan tampilan halaman *redirecting* dari *captive portal*.

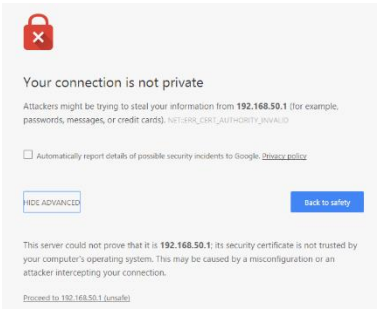
Gambar 3 Halaman *redirecting*

Telah dilakukan 10 kali uji coba mengakses situs web didapatkan hasil seperti pada Tabel 1.

Tabel 1. Pengujian *redirecting page*

Uji Coba	Hasil yang Diharapkan	Halaman website yang dicoba	Status
1	Dialihkan ke halaman *login*	www.novelupdates.com	Berhasil
2	Dialihkan ke halaman *login*	www.yahoo.com	Berhasil
3	Dialihkan ke halaman *login*	www.facebook.com	Berhasil
4	Dialihkan ke halaman *login*	www.twitter.com	Berhasil
5	Dialihkan ke halaman *login*	www.elektro.undip.ac.id	Berhasil
6	Dialihkan ke halaman *login*	www.detik.com	Berhasil
7	Dialihkan ke halaman *login*	www.kompas.com	Berhasil
8	Dialihkan ke halaman *login*	www.youtube.com	Berhasil
9	Dialihkan ke halaman *login*	www.viva.co.id	Berhasil
10	Dialihkan ke halaman *login*	www.cnnindonesia.com	Berhasil

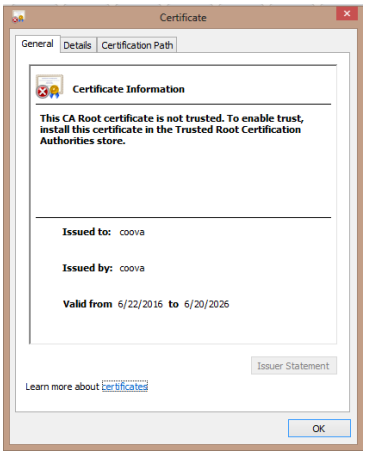
Gambar 4 menunjukkan tampilan pada *web browser* pengguna pada saat mengakses halaman HTTPS dimana akan ada pertanyaan mengenai kesediaan pengguna untuk memasang sertifikat.



Gambar 4. Tampilan saat sertifikat belum terpasang

Sertifikat yang dibuat pada *web browser* akan dikenal sebagai sertifikat pribadi yang tidak terdaftar sebagai badan yang membuat sertifikat SSL. Hal ini mengakibatkan sertifikat tersebut tidak dapat langsung dipasang pada *web browser*. Pengguna harus menyetujui untuk memasang sertifikat tersebut agar bisa mengakses

halaman *login* Enginx *website* seperti ditunjukkan pada Gambar 5.



Gambar 5. Tampilan pemasangan sertifikat pada *web browser*

Halaman *login* Enginx *website* akan langsung ditampilkan setelah proses pemasangan sertifikat selesai seperti ditunjukkan pada Gambar 6. Proses *login* akan dinyatakan berhasil setelah memasukkan *username* dan *password* yang terdaftar pada *server* MySQL dengan benar. Hubungan menuju jaringan Internet akan diizinkan, ketika proses *login* berhasil.

Gambar 6. Halaman *login captive portal*

3.3. Pengujian *Login* Berhasil

Pada pengujian *login* dilakukan dengan cara memasukkan username yang berupa NIM dan password yang benar pada halaman *login*. Pengujian ini dilakukan dengan 10 kali uji coba. Gambar 7 berikut merupakan hasil pengujian *login* berhasil.

Gambar 7. Pesan keberhasilan *login captive portal*

Pada Gambar 7 terlihat hasil pengujian *login* berhasil. Dimana parameter keberhasilannya adalah muncul notifikasi berhasilnya *login* setelah menekan tombol *Login*.

Setelah dilakukan 10 kali uji coba didapatkan hasil seperti pada Tabel 2.

Tabel 2. Pengujian *login* berhasil

Uji coba	Hasil yang Diharapkan	Username	*Password*	Status
1	Notifikasi tertampi	2601	2601elektro	Berhasil
2	Notifikasi tertampil	2602	Elektrojaya	Berhasil
3	Notifikasi tertampil	2603	Elektro	Berhasil
4	Notifikasi tertampil	2604	3l3ktr0	Berhasil
5	Notifikasi tertampil	L2F009123	Labkombkt1	Berhasil
6	Notifikasi tertampil	L2F009124	4f1fr0h1k1	Berhasil
7	Notifikasi tertampil	L2F009100	TyTy12345	Berhasil
8	Notifikasi tertampil	L2F009101	sandaljepit	Berhasil
9	Notifikasi tertampil	21060112120001	Sy4r1f	Berhasil
10	Notifikasi tertampil	21060110141033	Iy4nnDuT	Berhasil

3.4. Pengujian *Login* Gagal

Pada pengujian *login* dilakukan dengan cara memasukkan username yang berupa NIM dan password yang salah pada halaman *login*. Pengujian ini dilakukan dengan 10 kali uji coba. Gambar 8 berikut merupakan hasil pengujian *login* gagal.

Gambar 8. Notifikasi gagal *login* ke *captive portal*

Parameter keberhasilannya adalah munculnya notifikasi peringatan bahwa *login* gagal. Berdasarkan Tabel 3 dilakukan pengujian 10 kali uji coba didapatkan hasil sebagai berikut.

Tabel 3. Pengujian *login* gagal

No	Hasil	Username	*Password*	Status
1	Notifikasi tertampil	2601	2601elektr0	berhasil
2	Notifikasi tertampil	2602	Elektr0j4y4	berhasil
3	Notifikasi tertampil	2603	3l3ktr0	berhasil
4	Notifikasi tertampil	2604	Elektro	berhasil
5	Notifikasi tertampil	L2F009123	Labkombkti	berhasil
6	Notifikasi tertampil	L2F009124	Afifrohiki	berhasil
7	Notifikasi tertampil	L2F009100	tyty12345	berhasil
8	Notifikasi tertampil	L2F009101	SandalJepit	berhasil
9	Notifikasi tertampil	21060112120001	Syarif	berhasil
10	Notifikasi tertampil	21060110141033	Iyanndut	berhasil

Pengguna bisa membuka *tab* yang baru untuk memulai *browsing*. Pengguna bisa mengakses *link* keluar untuk memutuskan sesi koneksi. Notifikasi keluar dari *captive portal* akan muncul seperti pada Gambar 9. Pengguna bisa melakukan *login* lagi dengan mengakses *link* masuk.

Gambar 9. Pesan keberhasilan *logout captive portal*

Gambar 10 menunjukkan bahwa *server* sedang melakukan koneksi ke *server* MySQL untuk mengecek ketersediaan akun.

Gambar 10. Notifikasi mencoba masuk ke *captive portal*

3.5. Pengujian Halaman Administrator

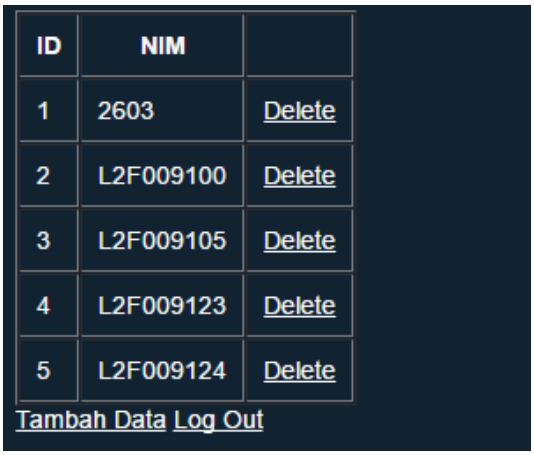
Pengujian pada halaman administrator dari *captive portal* akan dilakukan dengan menggunakan *web browser*. Halaman administrator dapat di kunjungi setelah *web browser* mengakses halaman *login captive portal*. Dapat dilihat terdapat menu Admin di kiri atas halaman *login*.

Gambar 11. Menu Admin pada halaman *login captive portal*

Administrator tidak perlu untuk *login* ke dalam *captive portal* untuk mengakses halaman admin. Halaman admin memiliki halaman *login* sehingga hanya admin yang dapat masuk. Gambar 12 menunjukkan halaman *Login* untuk Administrator.

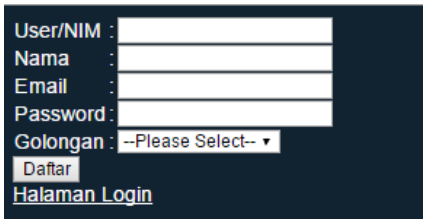
Gambar 12. Halaman *login* Administrator

Setelah *login* maka Admin akan dapat melihat terdapat halaman web sederhana yang berisi list user yang terdaftar dalam sistem *Captive portal*. Admin dapat menambah user dengan menekan link pada Tambah Data.



Gambar 13. Halaman List User

Setelah itu kita akan masuk ke dalam form untuk pendaftaran user baru seperti yang terlihat pada Gambar 14. Pada form pendaftaran hanya terdiri dari 3 info yaitu Username, Password ,dan Golongan. Opsi golongan membedakan antara Dosen dengan mahasiswa dimana, Dosen mendapatkan bandwidth internet yang lebih besar daripada mahasiswa yaitu dengan maksimum bandwidth 5Mbps, sedangkan mahasiswa mendapatkan 1Mbps.

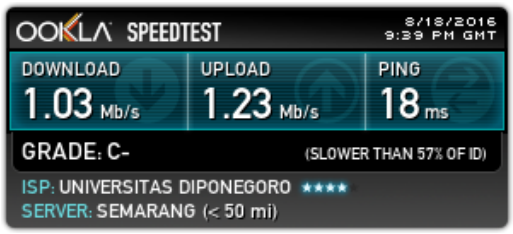


Gambar 14. Halaman Form Pendaftaran

3.6. Pengujian *Bandwitdh Limiter*

Pada sistem *captive portal* yang dirancang memiliki 2 jenis pengguna , yaitu Mahasiswa dan Dosen. Ada perbedaan dari kedua username ini adalah besarnya bandwidth yang disediakan, untuk Username Mahasiswa hanya diberi bandwidth sebesar 1Mbps baik download maupun upload sedangkan untuk username Dosen memiliki bandwidth sebesar 5Mbps baik download maupun upload.

Penyettingan bandwidth limiter pada username mahasiswa dilakukan dengan cara memberikan attribute tambahan pada tabel di database MySQL pada bagian tabel *radreply*. Pada tabel tersebut kita memberi input database. Pengujian *bandwidth limiter* pada username mahasiswa, pengujian dilakukan menggunakan website speedtest.net.



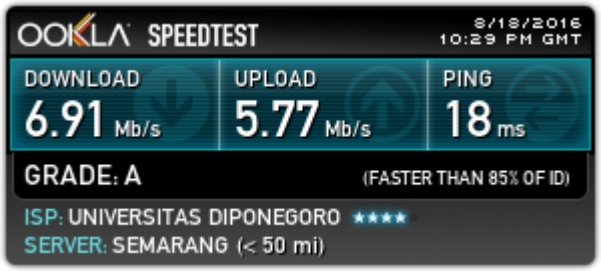
Gambar 15. Bandwitdh user Mahasiswa pada speedtest

Pada gambar diatas terlihat bahwa username mahasiswa hanya mendapatkan bandwidth untuk upload dan download sekitar 1 Mbps. Sudah dilakukan tes sebanyak 10 kali menggunakan speedtest pada 10 lokasi server yang berbeda dapat dilihat pada Tabel 4.

Tabel 4. Pengujian *bandwidth* user Mahasiswa

Lokasi Server	Download (Mbps)	Upload (Mbps)
Semarang (GMedia Tech)	1.03	1.19
Semarang (UNNES)	0.96	1.09
Surabaya (PT.Telkom)	1.17	1.15
Surakarta (UNS)	1.06	1.18
Yogjakarta (UGM)	1.04	1.28
Jakarta (MNC)	1.03	1.15
Bandung (PT.Telkom)	1.10	1.21
Bekasi (PT.Cyberplus Media Pratama)	1.12	1.15
Bali (PT.Telkom)	1.05	1.12

Pengujian *bandwidth limiter* pada username Dosen, pengujian dilakukan menggunakan *website* speedtest.net



Gambar 16. Bandwitdh user Dosen pada speedtest

Pada gambar diatas terlihat bahwa username dosen hanya mendapatkan bandwidth untuk upload dan download sekitar 5 Mbps. Sudah dilakukan tes sebanyak 10 kali menggunakan speedtest pada 10 lokasi server yang berbeda dapat diliat pada Tabel 5.

Tabel 5. Pengujian *bandwidth* user Dosen

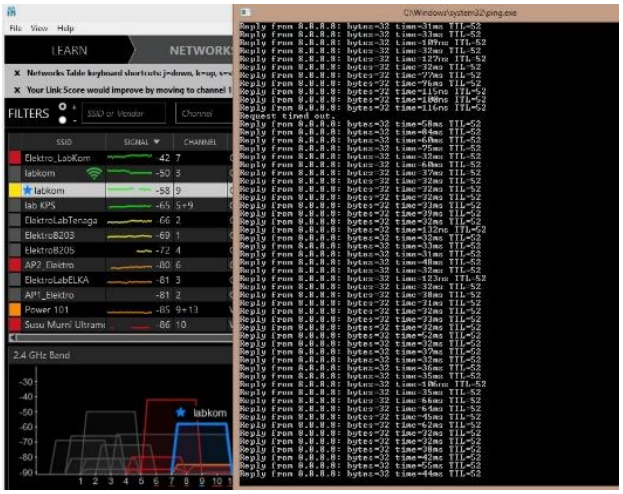
Lokasi Server	Download (Mbps)	Upload (Mbps)
Semarang(GMedia Tech)	5.91	5.77
Semarang(UNNES)	5.38	6.23
Surabaya(PT. Telkom)	5.73	2.29
Surakarta(UNS)	6.02	1.67
Yogjakarta(UGM)	5.32	5.01
Jakarta(MNC)	5.92	1.86
Bandung(PT.Telkom)	6.14	3.84
Bekasi(PT.Cyberplus Media Pratama)	6.12	2.93
Bali(PT.Telkom)	5.76	2.06

Terjadinya perbedaan yang cukup besar pada download dan upload dari User pada golongan Dosen. Hal ini dikarenakan oleh beberapa sebab, salah satu diantaranya dikarenakan Server yang digunakan sebagai *captive portal* bukan merupakan sebuah dedicated server melainkan sebuah Server Virtual, sehingga respon server ketika me-limit Bandwidth tidak secepat yang di harapkan sehingga limiter tidak bekerja secara optimal.

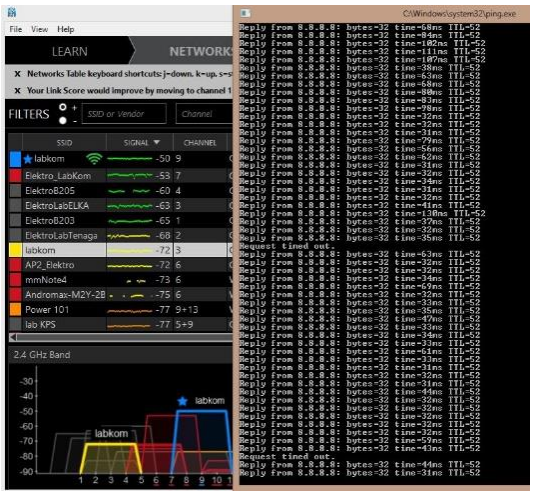
Terjadinya perbedaan yang cukup besar pada upload, hal ini dikarenakan ada beberapa server yang tidak memiliki cukup bandwidth upload sehingga hanya mendapatkan pembacaan di sekitar 2-3 Mbps. Sedangkan pembacaan diatas 5Mbps terjadi karena lebih cepatnya respon server dibandingkan kecepatan respon dari limiter server.

3.7. Pengujian Multiple *Wireless* AP dengan SSID (Service Set Identifier) Tunggal

Sistem menggunakan 2 *Wireless Router* yang di setting sebagai *access point* dengan metode bridge. Yang bertujuan agar ketika user berpindah dari satu access point ke lokasi *access point* yang lain tidak perlu untuk *login* kembali ke sistem *captive portal*. Pengujian menggunakan laptop yang dipindah dari satu lokasi *access point* ke *access point* yang lain.



Gambar 17. Laptop terkoneksi pada Acces Point labkom ke-1



Gambar 18. Laptop terkoneksi pada Acces Point labkom ke-2

Dari gambar terlihat bahwa ketika laptop berpindah dari acces point labkom channel 3 ke labkom channel 9. Otentikasi *captive portal* masih tetap berjalan dan tidak perlu untuk reconnect kembali. Hal ini dikarenakan *Wireless* AP dengan metode bridge walau acess point berbeda namun network masih sama.

Pengujian dilakukan dengan dua *Wireless access point* yang diletakkan 10 meter antara satu dengan yang lain. Kemudian pengguna dengan menggunakan laptop atau smartphone berpindah posisi dari satu *Wireless access point* ke yang lain. Tabel 6 berikut ini merupakan hasil pengujian perpindahan *Wireless access point*.

Tabel 6. Pengujian *roaming Wireless access point*

Uji coba	Hasil yang Diharapkan	Jarak (meter)	Status
1	device berpindah wap	11	Berhasil
2	device berpindah wap	7	Berhasil
3	device berpindah wap	6.5	Berhasil
4	device berpindah wap	9	Berhasil
5	device berpindah wap	9	Berhasil
6	device berpindah wap	10	Berhasil
7	device berpindah wap	10	Berhasil
8	device berpindah wap	11	Berhasil
9	device berpindah wap	7.2	Berhasil
10	device berpindah wap	6.5	Berhasil

Pada pengujian yang dilakukan 10 kali perpindahan. Terjadinya perbedaan jarak pada saat perpindahan disebabkan oleh bedanya kuat sinyal pada *Wireless access point* satu dengan yang lain dikarenakan dua wap tersebut berbeda seri dan produsen, dan dipengaruhi juga oleh network card yang dimiliki pengguna.

4. Kesimpulan

Media otentikasi dibuat menggunakan FreeRADIUS versi 2.2 dan CoovaChilli 1.3.0 pada Server gateway *captive portal*, sehingga akses internet jaringan *Wireless* Labkom teralihkan ke halaman *captive portal*. Penggunaan *captive portal* membatasi akses Internet hanya untuk pengguna yang terdaftar di server MySQL. Jika pengguna tidak terdaftar maka akan teralihkan ke halaman *captive portal*. Hasil uji menunjukkan bahwa pengujian *login* berhasil, *login* gagal, dan halaman pengalihan yang dilakukan berhasil 100% tanpa ada kegagalan dalam pengujian. Pengujian dilakukan dengan 10 pengguna dengan pengguna golongan dosen sebanyak 5 pengguna dan pengguna golongan mahasiswa 5 pengguna. Bandwidth yang didapat user mahasiswa sama dengan bandwitdh limiter yang terpasang yaitu 1Mbps dengan toleransi perbedaan sebesar 0.1 sampai 0.2 Mbps. Bandwidth yang didapat user dosen sama dengan bandwitdh limiter yang terpasang 5Mbps dengan toleransi perbedaan sebesar 1Mbps. Pengujian dilakukan pada perangkat *Wireless* dengan standar 802.11b/g/n dengan radius pengujian 10meter di sekitar laboratorium komputer. *Wireless Access Point* metode bridge memungkinkan pengguna untuk berpindah antar *Access Point* tanpa perlu *login* ke *captive portal* kembali.

Referensi

Journal:

[1]. Aldila Prasandika, 2014, *"Perancangan Hotspot Area Berbasis Mikrotik dan RADIUS",* AMIKOM Yogyakarta.

[2]. Gesit Singgih Febyatmoko, 2006, "*Sistem Otentikasi Otorisasi dan pelaporan koneksi user pada jaringan Wireless Chillispot dan server Radius*", Universitas Ahmad Dahlan.

[3]. Lilik Suheri, 2009, "*Analisis Manajemen Hotspot dengan Captive portal*", AMIKOM Yogyakarta.

[4]. Permadhi Santosa, 2011,"*Perancangan Prototype Radius Server dan Chillispot untuk Otentikasi Pengguna Jaringan Wireless*". Institut Pertanian Bogor.

[5]. Widhargo, 2009, "*Autentikasi Jaringan LAN dan Wireless menggunakan Router Pfsense dengan Radius*", Universitas Sebelas Maret.

[6]. Yuswira Efendi,2008 *" Desain Dan Implementasi Autentikasi jaringan Hotspot menggunakan Chillispot autentikasi system dan radius server pada GNU/Linux 4.0 r3 ETH",* Universitas Sebelas Maret.

[7]. Dani Kusuma Hermawan,2011 "*Implementasi Bandwidth Management Captive portal pada Jaringan Wireless di PENS-ITS",* Institut Teknologi Sepuluh Nopember.

[8]. Agus Supriyono,2013 *"Rancang Bangun Sistem Hotspot Menggunakan Captive portal",* Universitas Ahmad Dahlan.

Texbooks:

[9]. Hassell, Jonathan. *RADIUS*. O'Reilly. USA. 2002.

[10]. Nakhjiri. *AAA based Keying for Wireless Handovers: Problem Statement*. Network Working Group. 2006.

Internet:

[11]. Anonymous. *CoovaChilli*. "http://www.coova.org/CoovaChilli". 2010.

[12]. Purbo, Onno. W. 2003.*Captive portal*, http://kambing.ui.ac.id/onnopurbo/oraridiklat/ teknik/2.4ghz/wifi-advanced/captive-portal-11-2003.doc , diakses tanggal 7 November 2012

[13]. David. *CoovaChilli JSON Interface*. "http://coova.org/CoovaChilli/JSON". 2008.

[14]. Novell. *SUSE Linux Administration Guide*. "http://www.novell.com/documentation/suse91/ suselinux-adminguide/html/". 2012.

[15]. Ranch, David A. *Linux IP Masquerade HOWTO*. "http://www.tldp.org/HOWTO/IP-Masquerade-HOWTO/". 2005.

[16]. Technet Microsoft. *RADIUS Protocol*. "http://technet.microsoft.com/en-us/library/cc781821(WS.10).aspx". 2005.