SISTEM AUTENTIKASI, OTORISASI, DAN PELAPORAN KONEKSI USER PADA JARINGAN WIRELESS MENGGUNAKAN CHILLISPOT DAN SERVER RADIUS

Mukhammad Andri Setiawan[1], Gesit Singgih Febyatmoko[2]
Cisco Networking Academy, Informatics Department, Faculty of Industrial Technology,
Universitas Islam Indonesia, Jl. Kaliurang Km. 14 Yogyakarta 55584
Phone. (0274) 895287 ext. 150, Fax. (0274) 895007 ext. 148
E-mail: andri@fti.uii.ac.id[1], gesitsigh@yahoo.com[2]
URL: http:// cisco.or.id

ABSTRAKSI

Jaringan komputer nirkabel atau yang lebih dikenal dengan WLAN (Wireless Local Area Network) adalah salah satu teknologi yang saat ini sudah digunakan secara luas diberbagai institusi. Selain banyaknya keuntungan dengan memakai teknologi jaringan komputer nirkabel, terdapat juga kekurangan yaitu keamanan transfer data dan pembagian hak akses karena menggunakan media udara (gelombang elekromagnet). Isu keamanan dalam penerapan teknologi jaringan komputer nirkabel menjadi rawan dikarenakan mekanisme enkripsi menggunakan WEP yang mempunyai banyak kelemahan. Chillispot adalah perangkat lunak Captive Portal yang akan memaksa user yang menggunakan layanan WLAN untuk melakukan autentikasi. Apabila user sudah terautentikasi oleh sistem, user diijinkan menggunakan layanan WLAN, seperti file sharing, web dan koneksi internet. Server Radius digunakan untuk meningkatkan level keamanan WLAN karena server Radius menerapkan mekanisme autentikasi dan otorisasi layanan jaringan yang tersedia. Server Radius juga mampu untuk melakukan pencatatan, penghitungan, dan pelaporan aktifitas koneksi WLAN yang dilakukan user. Penerapan aplikasi Sistem Administrasi Hotspot berbasis web memberikan solusi terpusat dan disertai dengan tool-tool yang memudahkan administrator dalam mengelola sistem. Sistem yang dibuat meliputi tiga bagian. Bagian yang pertama adalah membangun server UAM (Universal Access Method) dengan chillispot. Bagian sistem yang kedua adalah konfigurasi server Radius menggunakan software Freeradius. Bagian sistem yang ketiga adalah membangun aplikasi Sistem Administrasi Hotspot berbasis web menggunakan bahasa pemrograman PHP yang memberikan abstraksi pembangun antarmuka dan pengaksesan basis data menjadi lebih mudah.

Kata kunci: *Captive Portal, Chillispot, Hotspot, Radius*

1. LATAR BELAKANG

Sebuah institusi yang besar terutama institusi yang tulang punggung eksistensinya menggunakan teknologi informasi membutuhkan penanganan yang baik agar sistem informasi yang ada dapat berjalan dengan optimal. Banyak faktor yang mempengaruhi keoptimalan kinerja sistem informasi, salah satu yang terpenting adalah keamanan sistem.

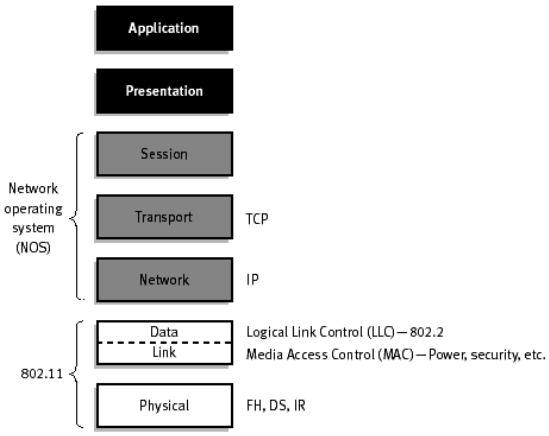
Jaringan komputer nirkabel atau disebut WLAN (Wireless Area Network) adalah salah satu teknologi yang saat ini sudah digunakan secara luas di berbagai institusi. Selain banyaknya keuntungan dengan memakai teknologi jaringan komputer nirkabel, terdapat juga kekurangan yaitu keamanan dan pembatasan hak akses yang sulit. Isu keamanan dalam penerapan teknologi jaringan komputer nirkabel menjadi rawan dikarenakan mekanisme enkripsi (WEP) yang mempunyai banyak kelemahan.

Selain isu keamanan, praktek bisnis yang mengandalkan penyewaan akses WLAN (hotspot) juga membutuhkan sebuah sistem yang mampu mengakomodasi kebutuhan untuk mengelola user, semisal pada kasus, yang bisa mengakses internet adalah user yang terdaftar sebagai anggota (*member*).

2. WIRELESS LOCAL AREA NETWORK (WLAN)

Wireless LAN (WLAN atau WIFI) adalah sistem transmisi data yang didesain untuk menyediakan akses jaringan yang tidak terbatas tempat atau lokasi antar device komputer dengan menggunakan gelombang radio.

Spesifikasi 802.11 [IEEE Std 802.11 (ISO/IEC 8802-11: 1999)] [1] adalah standar untuk WLAN yang disahkan oleh Electrical and Electronics Engineers (IEEE) pada tahun 1997. Versi 802.11 ini menyediakan kecepatan transder data 1 Mbps dan 2 Mbps. Versi ini juga menyediakan dasar-dasar metode pensinyalan dan layanan lainnya. Seperti semua standar 802 IEEE, standar 802.11 berfokus pada 2 level model OSI yang paling bawah, yaitu physical layer dan link layer. Aplikasi-aplikasi LAN, sistem operasi jaringan, protocol TCP/IP dan Novel NetWare, dapat berjalan pada 802.11-compliant WLAN seperti halnya pada ethernet.



Gambar 1. 802.11 IEEE dan ISO Model

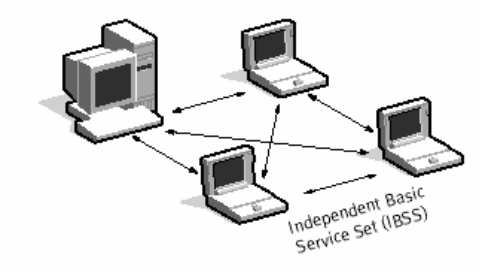
WLAN mempunyai kelebihan daripada LAN konvensional (menggunakan kabel), diantaranya adalah:

1. Meningkatkan mobilitas device komputer.
   Tidak seperti koneksi jaringan konvensional yang menggunakan kabel, pengguna jaringan dapat berpindah-pindah tempat dengan batasan jangkauan sinyal gelombang perangkat WLAN.
2. Biaya instalasi lebih murah.
   Instalasi WLAN tidak memerlukan konfigurasi kabel yang sulit. Pada kasus instalasi LAN pada gedung dengan struktur dinding yang kokoh, maka wireless merupakan solusi yang lebih baik daripada menggunakan kabel.
3. Efektif diterapkan pada lingkungan yang dinamis.
   Pada kasus kantor yang sering berpindah-pindah, maka penggunaan wireless sangat efektif karena pada saat berpindah tempat maka tidak diperlukan instalasi kabel baru.

2.1 Arsitektur WLAN

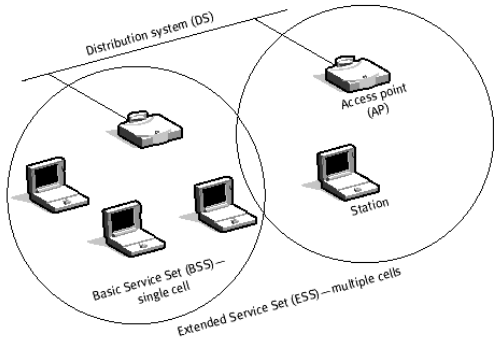
Terdapat dua macam arsitektur yang dipergunakan dalam membangun jaringan WLAN, yakni arsitektur jaringan Ad hoc dan arsitektur jaringan Infrastruktur.

Ad hoc atau *peer-to-peer* WLAN terdiri dari sejumlah komputer yang dilengkapi dengan *wireless interface card*. Tiap komputer dapat berkomunikasi secara langsung dengan semua komputer yang dilengkapi dengan peralatan wireless. Ad hoc memungkinkan dilakukannya sharing file dan printer, tetapi tidak dapat digunakan untuk menghubungkan WLAN dengan *wired LAN*, kecuali apabila salah satu komputer dikonfigurasi sebagai *bridge* untuk menghubungkan ke *wired LAN* dengan menggunakan software khusus.



Gambar 2. Arsitektur Jaringan Ad hoc

WLAN dapat menggunakan *Access Point*, atau *Base Station*. Pada arsitektur jaringan ini, *Access Point* bertindak seperti halnya hub pada *wired LAN*. *Access Point* menyediakan konektivitas pada komputer-komputer yang dilengkapi dengan peralatan wireless. *Access Point* dapat menghubungkan WLAN dengan wired LAN, dan mengijinkan WLAN untuk mengakses resource pada wired LAN, seperti server file atau koneksi internet.



Gambar 3. Arsitektur Jaringan Infrastruktur

3. CHILLISPOT

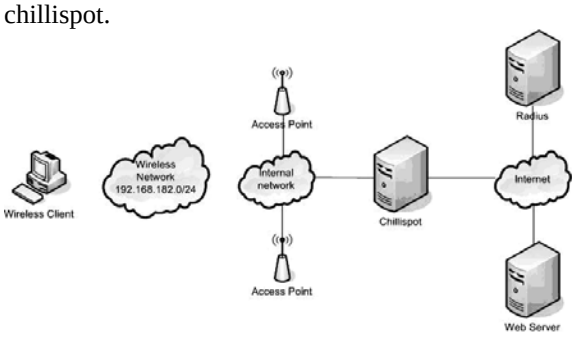
Chillispot adalah Wireless Access Point Controller berbasis open source. Chillispot merupakan software Captive Portal yang digunakan untuk autentikasi user Wireless LAN [3]. Cara kerja Chillispot adalah dengan cara mengcapture request halaman web client dan kemudian di-redirect ke halaman web chillispot untuk login autentikasi. Data user dan password yang dimasukkan user akan ditransfer ke server Radius untuk proses autentikasi dan otorisasi hak akses. Apabila data user dan password ter-autentikasi oleh server radius maka user dapat mengakses halaman web di internet.

Chillispot dikembangkan pada platform sistem operasi Linux tetapi juga dapat di-compile pada sistem operasi FreeBSD, OpenBSD, Solaris, dan bahkan MAC OS X. Chillispot dikembangkan menggunakan bahasa pemrograman C untuk meningkatkan portabilitas platform sistem operasi yang digunakan. Beberapa fitur yang dimiliki oleh Chillispot antara lain server UAM, layanan DHCP, dan Captive Portal [4].

Untuk membangun hotspot dengan autentikasi, chillispot memerlukan beberapa item, yakni:

a. Koneksi internet
b. Wireless LAN Access Point
c. Radius Server
d. Database Server

Gambar berikut menunjukkan sebuah struktur jaringan hotspot yang mempergunakan chillispot.



Gambar 4. Struktur jaringan Chillispot

4. SERVER RADIUS

Radius adalah singkatan dari *Remote Authentication Dial-in User Service* yang berfungsi untuk menyediakan mekanisme keamanan dan manajemen user pada jaringan komputer. Radius diterapkan dalam jaringan dengan model client-server [2].

Server Radius menyediakan mekanisme keamanan dengan menangani autentikasi dan otorisasi koneksi yang dilakukan user. Pada saat komputer client akan menghubungkan diri dengan jaringan maka server Radius akan meminta identitas user (username dan password) untuk kemudian dicocokkan dengan data yang ada dalam database server Radius untuk kemudian ditentukan apakah user diijinkan untuk menggunakan layanan dalam jaringan komputer. Jika proses autentikasi dan otorisasi berhasil maka proses pelaporan dilakukan, yakni dengan mencatat semua aktifitas koneksi user, menghitung durasi waktu dan jumlah transfer data dilakukan oleh user. Proses pelaporan yang dilakukan server Radius bisa dalam bentuk waktu (detik, menit, jam, dll) maupun dalam bentuk besar transfer data (Byte, KByte, Mbyte) [6].

Software server Radius yang digunakan dalam penelitian ini adalah Freeradius yang bersifat modular dan memiliki banyak fitur. Freeradius merupakan software server yang berbasis pada open source dan berlisensi GPL [5].

5. ANALISIS PERMASALAHAN

Masalah yang dimunculkan pada kasus ini adalah bagaimana menerapkan sistem keamanan pada jaringan wireless dengan mekanisme autentikasi, otorisasi, dan pelaporan aktifitas koneksi user.

Secara garis besar, sistem yang akan diwujudkan mampu menangani mekanisme keamanan koneksi jaringan yang dilakukan user. Mekanisme keamanan menggunakan autentikasi sehingga user yang diperbolehkan menggunakan layanan dalam WLAN adalah user yang terdaftar dan dikenali oleh sistem.

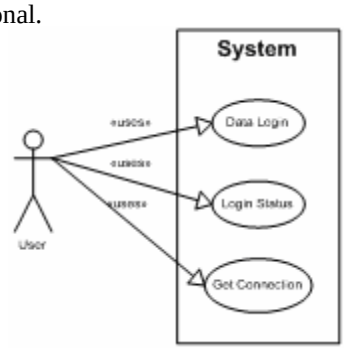
Proses autentikasi dan otorisasi menggunakan mekanisme login yang secara otomatis dilakukan oleh sistem dengan cara me-redirect halaman web yang diakses oleh user ke halaman autentikasi. Setelah proses autentikasi dan otorisasi berhasil, maka layanan hotspot untuk user akan disediakan oleh sistem. Jika proses autentikasi tidak berhasil, maka layanan WLAN tidak akan disediakan untuk user.

Sistem mengelola user yang terdaftar dengan dua cara, yaitu dengan model *Card* dan *Subscribers*. *User*. Dengan mempergunakan model Card, maka tidak dibutuhkan keanggotaan dan hanya berlaku selama durasi waktu akses tertentu (30 menit, 60 menit dan 120 menit). User dengan model Subscriber memerlukan keanggotaan dan untuk menggunakan user ini harus memberikan identitas diri untuk didaftarkan ke dalam sistem. Keanggotaannya dibatasi dengan masa kadaluarsa selama jangka waktu tertentu.

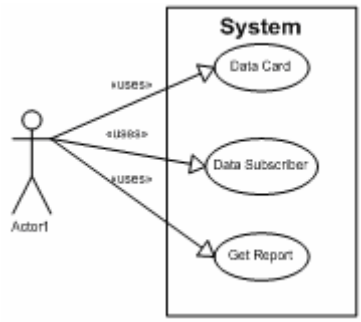
6. PERANCANGAN

6.1 Use Case Diagram

Diagram use case di gunakan untuk mendekripsikan apa yang seharusnya di lakukan oleh sistem. Diagram use case menyediakan cara mendeskripsikan pandangan eksternal terhadap sistem dan interaksi-interaksinya dengan dunia luar. Dengan cara ini, diagram use case menggantikan diagram konteks pandangan pendekatan konvensional.



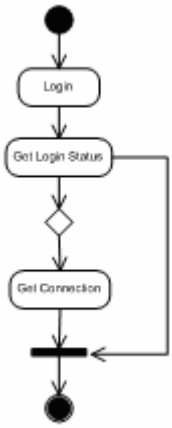
Gambar 5. Use Case Diagram User



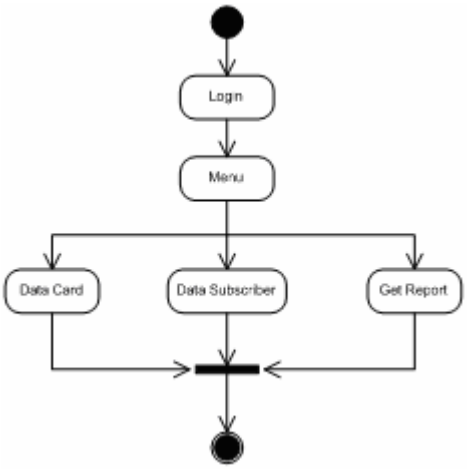
Gambar 6. Use Case Diagram Administrator

6.2 Activity Diagram

Activity diagram menggambarkan berbagai alir aktifitas dalam aplikasi yang sedang di rancang, bagaimana masing masing alir berawal, keputusan yang mungkin terjadi dan bagaimana mereka berakhir.



Gambar 7. User Activity Diagram



Gambar 8. Administrator Activity Diagram

7. IMPLEMENTASI

7.1 Arsitektur Perangkat Lunak

Perangkat lunak yang dikembangkan menggunakan Arsitektur sebagai berikut :

1. Software Freeradius berjalan dalam sistem operasi Linux Fedora Core 4.
2. Software Chillispot berjalan dalam sistem operasi Linux Fedora Core 4. Chillispot dan Freeradius dikonfigurasi dalam satu komputer.
3. Software administrasi sistem berjalan diatas web dengan bahasa pemrograman PHP dan dukungan basis data MySQL.
4. Lingkungan operasi client tidak terbatas dengan sistem operasi tertentu (Linux atau Microsoft Windows).

7.2 Prosedur autentikasi client

Agar client dapat terautentikasi dan dapat mempergunakan layanan yang diberikan dalam Hostspot, dibutuhkan beberapa langkah sebagai berikut:

1. Import certificate SSL komputer server Radius
   Certificate SSL server UAM (Universal Access Method), di-import dengan menyalin certificate SSL yang di-generate server UAM. Certificate pada sistem Linux digenerate dengan perangkat lunak OpenSSL.
2. Konfigurasi peralatan wireless komputer client
   Konfigurasi peralatan wireless komputer client supaya mendapat alamat IP secara DHCP.
3. User membuka web browser, kemudian membuka halaman web. Chillispot akan mem-blok akses koneksi dan me-redirect halaman web ke halaman autentikasi yang terletak di server UAM. Chillispot sendiri dikonfigurasi sebagai UAM server. Chillispot bekerja di komputer gateway untuk meng-capture paket data dari client wireless LAN yang belum terautentikasi untuk di-redirect ke halaman web yang menampilkan form untuk login. Data username dan password yang diisikan oleh user akan diforward ke server Radius untuk diproses apakah username tersebut terautentikasi dan diberikan otorisasi untuk menggunakan layanan hotspot. Chillispot memberikan layanan DHCP (Dynamic Host Configuration Protocol) kepada client WLAN, sehingga setiap client WLAN yang aktif akan mendapat alamat IP yang ditentukan oleh Chillispot.
   Berikut contoh konfigurasi chili.conf dalam server Chilispot:

```
# alamat jaringan untuk WLAN
net 10.10.0.0/24
# alamat server DNS primary untuk WLAN
dns1 192.168.0.1
# alamat server DNS secondary u/ WLAN
dns2 202.162.32.6
#  alamat IP server Freeradius
radiusserver1 192.168.0.50
# shared key server Freeradius
radiussecret sharedkey
# interface jaringan layanan DHCP WLAN
dhcpif eth1
#   alamat   IP   server   UAM,   untuk
menampilkan form autentikasi uamserver
https://192.168.0.50/hotspotlogin.php
```

4. Login sistem
   Melakukan pengecekan data user dan password yang dimasukkan oleh user. Proses ini dilakukan oleh server Radius dengan data user dan password yang ada dalam database.

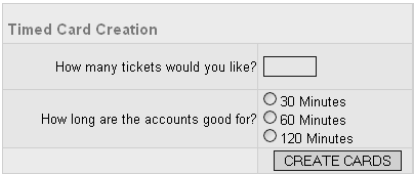
7.3 Administrasi Account

Login aplikasi administrasi menggunakan fasilitas yang disediakan server web Apache, menggunakan file .htacess dan .htpasswd.

Gambar 9. Aplikasi phpMyPrepaid untuk Membuat Account

7.4 Create Timed Cards

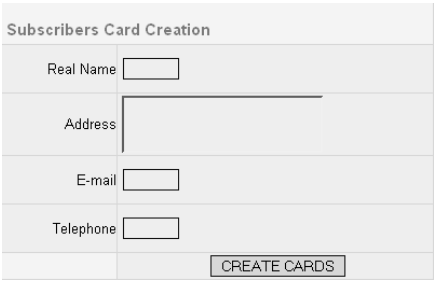
Bagian ini dipergunakan untuk untuk membuat Card yang terdiri dari Username dan Password digunakan untuk autentikasi. Username ini nanti dapat dipergunakan oleh client. Timed Cards dipergunakan seperti penggunaan kartu pra bayar dalam komunikasi seluler.



Gambar 10. Create New Cards

7.5 Create New Subscribers

Bagian ini digunakan untuk membuat Subscribers baru. Subscriber adalah pengguna yang tercatat sebagai pelanggan dengan ketentuan tertntu. Username ini nantinya akan dapat mempergunakan layanan hotspot sampai dengan accountnya dihentikan. Pengguna ini seperti pengguna pasca bayar dalam komunikasi seluler.



Gambar 11. Create New Subscribers

8. KESIMPULAN

Penerapan sistem autentikasi dan otorisasi koneksi user dengan menggunakan Chillispot dan server Radius memberikan level keamanan jaringan komputer wireless yang lebih baik. User yang dapat menggunakan layanan jaringan harus terdaftar dalam sistem sehingga tidak semua orang dapat menggunakan layanan jaringan.

Dengan mekanisme pelaporan detail tentang koneksi yang dilakukan user, memudahkan administrator dalam memonitor penggunaan layanan jaringan dan dapat dijadikan dasar bagi pengembangan aplikasi billing yang dapat diterapkan pada institusi komersial seperti Penyedia Jasa Internet.

DAFTAR PUSTAKA

[1] Anonymous, *802.1x Port Based Network Authentication*, http://www.tldp.org/HOWTO/8021X-HOWTO/, diakses tanggal 14 Januari 2006.

[2] Anonymous, *GNU Radius Reference Manual*, http://www.gnu.org/software/radius/manual/index.html, diakses tanggal 14 Januari 2006.

[3] Anonymous, *Chillispot Forum*, http://www.chillispot.org/forum/, diakses tanggal 20 Februari 2006.

[4] Anonymous, *Swarm Internet Hotspots Forum*, http://topup.ie/phpBB2/, diakses tanggal 20 Februari 2006.

[5] Anonymous, *Freeradius Mail Archives*, http://www.mail-archive.com/freeradius-users@lists.freeradius.org/, diakses tanggal 20 Februari 2006.

[6] Sean, Bracken, *How To Setup Wi-Fi Hotspot*, http://howtoforge.com/wifi_hotspot_setup, diakses tanggal 20 Februari 2006.