KARYA PENELITIAN

IMPLEMENTASI *CAPTIVE PORTAL* UNTUK MENINGKATKAN KINERJA AKSES POINT DI UNIVERSITAS SAM RATULANGI

Oleh : *Meicsy E. I. Najoan, ST. MT.* *

Abstrak.

Penelitian ini membahas impelementasi peningkatan kinerja akses point di Universitas Sam Ratulangi dimana sebelumnya dalam pendistribusian koneksi internet menggunakan jaringan kabel dan tanpa kabel (nirkabel). Untuk implementasi akses point yang tersebar di beberapa titik setiap pengguna mengakses mengunakan perangkat yang memiliki fasilitas *Wi-Fi dengan terlebih dahulu harus meregistrasi MAC address-nya kemudian diberikan alamat IP oleh pengelolah jaringan. Akibatnya memerlukan pendataan langsung terhadap perangkat-perangkat yang akan dikoneksikan melalui access point, yang dari segi jumlah sangat tidak efektif dan efisien dalam mengelolah jaringan nirkabel.*

Pengelolah jaringan dalam memberikan akses ke pengguna dapat memberikan "username" dan "password" untuk lebih efektif dan efisien, tanpa harus meregistrasi MAC address dan melakukan konfiguras alamat IP pada perangkat. Untuk mengimplementasi hal diatas, dapat dibuat dengan teknik autentikasi (pembuktian keaslian dari pengguna) menggunakan captive portal. Dengan teknik ini maka setiap perangkat yang akan terkoneksi ke internet akan melewati perangkat lunak captive portal.

Kata kunci : Access Point, Nirkabel, *Captive portal*

I. Pendahuluan.

Kebutuhan akan koneksi internet terus meningkat, hal ini juga diikuti oleh perkembangan teknologi jaringan semakin berkembang pesat khususnya yang mengunakan teknologi nirkabel. Wi-Fi (Wireless fidelity) merupakan merek dagang wireless LAN yang di perkenalkan dan di standarisasi oleh Wi-Fi Alliance. Standar Wi-Fi didasarkan pada standar 802.11. Sertifikasi Wi-Fi adalah proses untuk memastikan interoperabilitas antar peralatan WLAN 802.11, termasuk Access Point dan kartu-kartu jaringan nirkabel yang biasanya mempunyai form factor yang beragam. Dengan mengunakan teknologi Wireless LAN kita dapat mengakses internet secara mobile tanpa harus dibatasi oleh kabel dengan mengunakan perangkat laptop, PDA, dan sebagainya.

Saat ini di Universitas Sam Ratulangi sudah menggunakan teknologi *Wireless* LAN dengan mengunakan enkripsi WEP dan MAC *filtering* yang tidak efektif dan efisien. Dengan mengunakan enkripsi WEP dapat dengan mudah ditembus keamanannya oleh penyusup (*Hacker*). Untuk itu diperlukan sebuah pembuktian keaslian (melegalisasi), berupa teknik pembatasan koneksi pada client di dalam jaringan dengan menggunakan protokol http*(hypertext transfer protokol)* untuk memberikan hak aksesnya tersebut ke dalam jaringan atau *port-port* tertentu (*Captive Portal*), sehingga keamanan dari Wireless LAN dapat di tingkatkan dan dapat mengatur para pengguna *HotSpot* di Universitas Sam Ratulangi. Dengan mengunakan *Captive Portal* dapat mengontrol pengguna tanpa perlu melakukan konfigurasi apapun di sisi pengguna dan melakukan pembuktian keaslian kepada pengguna, sehingga dapat melakukan bandwidth control, managemen pengguna, dan mengatur *traffic* hanya dengan mengunakan *browser web* biasa sebagai alat pembuktian keaslian yang aman. Sehingga kinerja dari *Access Point* tidak menurun yang di akibatkan oleh enkripsi WEP, WPA, WPA2 yang digunakan pada *Access Point*

* **Staf Pengajar Fakultas Teknik, Jurusan Teknik Elektro Unsrat.**

II. Ruang Lingkup Permasalahan.

Sistem keamanan yang digunakan pada *wireless LAN* di Universitas Sam Ratulangi saat ini masih mengandalkan keamanan dengan mengunakan pembatasan pada MAC *address* dan pemberian alamat IP yang masih manual. Oleh karena itu diperlukan sebuah pembuktian keaslian (authentikasi), berupa teknik pembatasan koneksi pada client didalam jaringan dengan menggunakan protokol *http(Hypertext Transfer Protokol)* untuk memberikan hak akses tersebut kedalam jaringan atau *port-port* tertentu (*Captive Portal*), sehingga keamanan dari Wireless LAN dapat ditingkatkan dan dapat mengatur para pengguna *access point* lebih efektif dan efisien di Universitas Sam Ratulangi.

Lingkup masalah yang akan ditelaah dibatasi pada pembuatan *Wireless LAN* dengan mengunakan C*aptive Portal* sebagai alat pembuktian keaslian yang aman dari para pengguna *Wireless LAN,* dengan mengunakan sistem operasi Mikrotik RoutersOS v.2.9.27 di Universitas Sam Ratulangi

III. Tujuan dan Manfaat Penelitian.

Tujuan yang ingin dicapai dari tugas akhir ini adalah membuat suatu sistem keamanan dengan melakukan pembuktian keaslian para pengguna *wireless LAN* yang ada di Universitas Sam Ratulangi, dengan cara mengatur para pengguna internet melalui server *captive portal.* Sehinga mengharuskan pengguna untuk membuktikan keabsahan/keasliannya dalam mengakses ke *wireless LAN* yang membuat keamanan tiap pengguna terjamin dan dapat melakukan akses dengan mudah, yang pada akhirnya membuat *access point* di universitas sam ratulangi semakin efektif dan efisien.

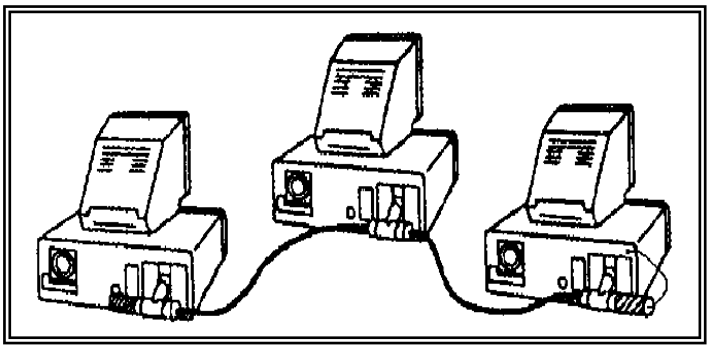
Mengoptimalkan penggunaan jaringan nirkabel agar lebih efektif dan efisien dalam mengakses internet di Universitas Sam Ratulangi..

IV. Tinjauan Pustaka.

4. 1. Pengertian Umum jaringan Komputer

Perkembangan teknologi Komputer dan Komunikasi suatu model komputer yang melayai seluruh tugas-tugas komputasi menjadi sekumpulan komputer yang terpisah tetapi saling berhubungan dalam melaksanakan tugas-tugas komputer. Sekumpulan komputer ini saling terkoneksi satu sama lain melalui media transmisi tertentu. Bentuk koneksinya tidak hanya melalui kawat tembaga saja melainkan dapat mengunakan serat optik, gelombang radio, dan satelit komunikasi. Jaringan komputer pada dasarnya merupakan pengabungan antara dua teknologi, yaitu:teknologi komputer dan teknologi telekomunikasi, dimana pengabungan tersebut menghasilkan sebuah teknologi komunikasi data yang diaplikasikan dalam komputer.

Awalnya jaringan komputer adalah sambungan komputer ke komputer dalam bentuk topologi bus. Topologi ini menhubungkan peralaan jaringan ke kabel tunggal yang berjalan sepanjang jaringan, seperti yang ditunjukan pada gambar 1.



Gambar 1. Jaringan Kompute topologi bus

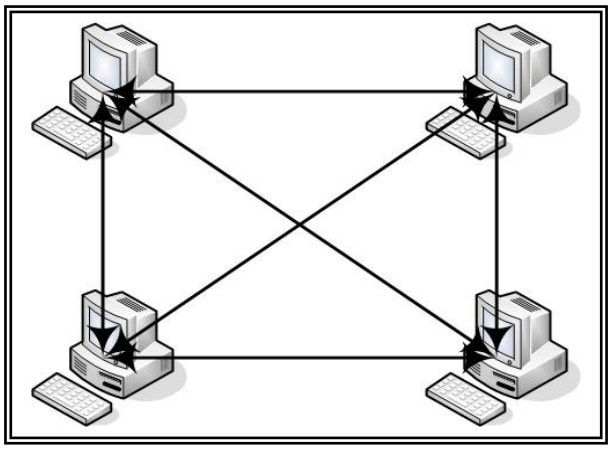
4.2 Wireless Local Area Network (Wireless LAN)

Jaringan *Wireless* LAN merupakan suatu sistem komunikasi data tanpa kabel yang merupaka solusi alternatif dari jaringan komputer yang mengunakan kabel (*Wired* LAN). Dengan kata lain jaringan *Wireless* LAN

merupakan salah satu pengembangan media transmisi dari teknologi jaringan komputer dengan menggunakan perangkat radio komunikasi data yang dapat menghubungkan sebuah komputer ke jaringan *Local Area Network* (LAN).jaringan *Wireless* LAN dapat dipasang didalam gedung *(Indoor)* maupun diluar gedung *(Outdoor)*.

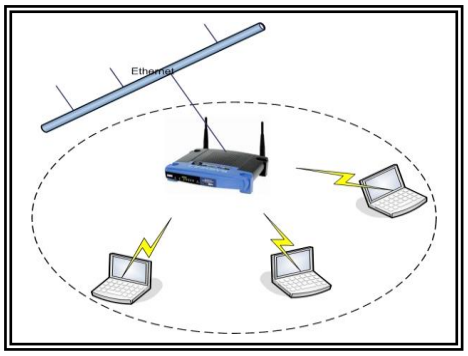
Teknik jaringan berbasis *wireless* LAN bertumpu pada konsep yang ditentukan dengan standar IEEE 802.11.standar ini mendukung tiga topologi dasar untuk jaringan *wireless* LAN, yaitu: *Independent Basic Sevice Set* (IBSS), *Basic Service Set* (BSS*),* dan *Extended Service Set* (ESS)**.**

- Konfigurasi ***I****ndependent Basic Sevice Set* (IBSS) dikenal sebagai konfigurasi independent atau jaringan ad-hoc, yang merupakan konfigurasi jaringan *wireless* yang sangat sederhana, dimana dalam menghubungkan beberapa komputer kita tidak perlu menambahkan *access point* sehinggan komputer dapat berkomunikasi secara langsung satu dengan yang lainya. Tampak seperti gambar 2 dibawah ini:



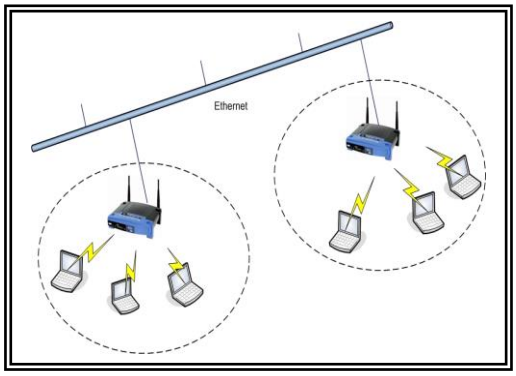
Gambar 2. Topologi *Independent Basic Service Set* (IBSS/Ad-hoc)

- Jenis yang lain adalah *Basic Service Set* (BSS*)*, terdiri dari minimal satu buah a*ccess point* yang dihubungkan ke infrastruktur jaringan kabel.jenis ini dikenal juga sebagai man*aged network* di jaringan *wireless* LAN, dimana access point bertindak sebagai server logical di sebuah sel jaringan komputer *wireless* LAN. Sehinga client tidak lagi dapat berhubungan langsung, tetapi harus melalui *access point* yang berfungsi seperti *switch*/*hub* dalam jaringan kabel, seperti pada gambar 3.

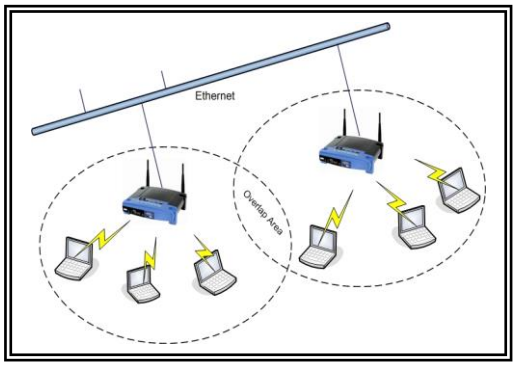


Gambar 3. Topologi *Basic set service* (BSS)

- *Extended Service Set* (ESS) terdiri dari beberapa BSS dalam suatu jaringan. Pada ESS, jaringan BSS tidak harus mengunakan SSID yang sama namun tanpa SSID yang sama fungsi *roaming* tidak dapat dimanfaatkan. *Roaming* adalah feature yang memungkinkan client berpindah dari BSS ke jaringan BSS yang lainsecara otomatis tanpa terputus koneksinya. Untuk mengunakan *feature roaming,* harus terdapat *Overlaping Area* atau area dimana kedua signal dapat diakses. Untuk lebih jelasnya dapat dilihat pada gambar 4 dan gambar 5.



Gambar 4. Topologi *Extended Service Set* (ESS)



Gambar 5. Topologi *Basic set service* (BSS) dengan fungsi *Roaming*

4.3. Standarisasi *Wireless* LAN

Wi-Fi sebenarnya merupakan merek dagang *wireless* LAN yang diperkenalkan dan distandarisasi oleh Wi-Fi Alliance. Standar Wi-Fi didasarkan pada standar 802.11. Sertifikasi Wi-Fi adalah adalah proses untuk memastikan interoperabilitas antar peralatan WLAN 802.11, termasuk access point dan kartu-kartu jaringan wireless yang biasanya mempunyai beberapa form factor yang beragam. Perusahaan-perusahaan produsen peralatan *wireless* harus menjadi anggota Wi-Fi Alliance(Purbo, 2006). Secara teknis peralatan *wireless* yang biasa digunakan mengunakan standar IEEE 802.11x. Di mana x adalah sub standard yang dapat dilihat pada Table 1 di bawah ini.

Tabel 1. Standar IEEE 802.11x

Protocol	Frekuensi	Maksimum Transfer
IEEE 802.11	2,4GHZ	2Mbps
IEEE 802.11a	5GHZ	54Mbps
IEEE 802.11a 2x	5GHZ	108Mbps
IEEE 802.11b	2,4GHZ	11Mbps
IEEE 802.11b+	2,4GHZ	22Mbps
IEEE 802.11g	2,4GHZ	54Mbps
IEEE 802.11n	2,4GHZ	120Mbps

4.4. Infrastuktur *Wireless* LAN

Fungsi utama dari *wireless* LAN adalah untuk menjangkau wilayah jaringan area lokal yang sulit dicapai dengan kabel, juga untuk menjangkau pengguna bergerak (*mobile users*). Dalam mengembangkan serta melakukan instalasi *wireless* LAN, diperlukan beberapa perangkat penting, antara lain

- *Access Point :* Inti dari sebuah jaringan *wireless* adalah pengunanan *Access Point* (AP), alat ini berbentuk kotak kecil, terkadang dilengkapi satu atau dua antena. Peralatan ini merupakan radio *based*, berupa *receiver* dan *transmiter* yang akan terkoneksi dengan LAN *wired* atau dapat pula terkoneksi pada *broadband* menggunakan *ethernet* dengan mengunakan kabel UTP.
- Adapter *Wireless* : Bentuk fisik kartu jaringan *wireless* mempunyai kemiripan dengan jaringan *wired*, hanya media transmisinya yang berlainan. Bentuk fisik *Wireless Network Interface Card* (WNIC) pada jaringan *wireless* merupakan *interface* fisik dan bus elektrikal yang menjadikan WNIC dapat berkomunikasi dengan peralatan yang lain. Secara umum, sebuah kartu mempunyai bentuk fisik standar yang disesuaikan secara fisik dengan bagian interkoneksi pada komputer.
- Antenna : Beberapa WNIC dan *Access Point* secara permanen mempunyai antena yang menyatu dan terintegrasi, sehingga tidak dapat diubah-ubah. Namun ada beberapa WNIC dan *Access Point* memiliki antenna eksternal yang dapat diubah-ubah. Dalam merencanakan untuk membangun jaringan *wireless* LAN dengan cakupan area yang lebih luas.
- *Pig Tail* : Untuk menghubungkan access point ke antenna yang berbeda tipe konektornya, maka digunakan kabel penghubung antara access point dengan antenna (*Pig tail)*.

4.5. Authentikasi *Wireless* LAN

Authentikasi *Wireless* pada dasarnya mempersilahkan atau memblokir pelanggan yang masuk melalui jaringan *Wireless*. Secara alami *wireless* LAN membutuhkan authentikasi pada *Workstation* ke *Access Point.* Proses authentikasi ini memberikan hak akses pada *access point* untuk membatasi *workstation* yang ingin bergabung atau berasosiasi dengannya. Bagaimana pun juga,authentikasi ini tidak cukup untuk dapat menjamin keamanan di wireless LAN. Integritas sebuah pesan merupakan kelemahan dalam WEP dan hal ini merupakan unsur utama dalam keamanan.(Geier, 2005)

Pemeriksaan integritas pesan per-paket (disebut authentikasi per-paket) merupakan salah satu cara *access point* untuk menentukan paket authentikasi dari *workstation,* atau sebaliknya dari *access point.* Semua pesan tersebut mempunyai kunci yang di-*share* diantara dua sistem tersebut.

Untuk mengantisipasi penggunaan oleh pengguna yang tidak berhak, maka *Access Point* menyediakan beberapa pengamanan diantaranya adalah:

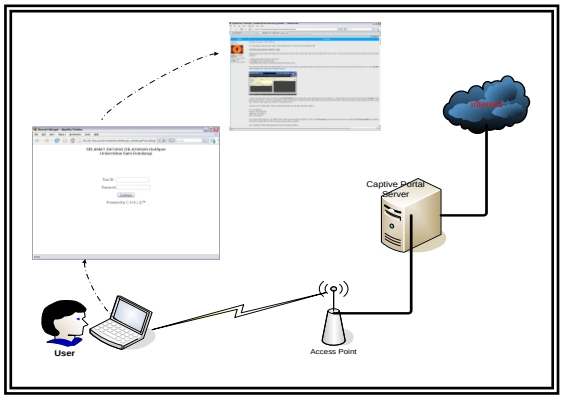
- *Wired Equivalen Privacy (WEP)* : merupakan metode otentikasi yang membutuhkan kunci, kunci dimasukan ke klien maupun access point, kunci ini harus cocok antara yang dimasukan ke access point dan kunci yang dimasukan ke klien. Kunci ini akan dikirimkan dalam bentuk enkripsi sehingga akan lebih aman dari usaha penyadapan data
- *Wifi Protected Access (WPA)* : Merupakan teknik pengmanan jaringan wireless yang menggunakan teknik enkripsi yang lebih baik dibandingkan dengan teknik WEP, selain itu juga teknik ini disertai pengamanan berupa otentikasi pengguna. Setiap Wifi memiliki area jangkauan tertentu tergantung power dan antenna. Tidak mudah untuk melakukan pembatasan area jangkauan wifi. Hal ini memungkinkan pengguna yang tidak berhak untuk mendapatkan atau masuk ke jaringan wireless selama masih dalam jangkauan sehingga memungkinkan terjadi aktifitas-aktifitas perusakan atau pemanfaatan sumberdaya yang tidak semestinya.

4.6. Captive Portal

Captive portal bekerja dengan cara mengalihkan semua permintaan akses http dari klien menuju ke sebuah halaman khusus yang biasanya berupa halaman autentikasi pengguna atau halaman kesepakatan antara pengguna dengan penyedia jaringan wireless yang berfungsi untuk melakukan autentikasi, sebelum user atau klien mengakses sumber daya jaringan atau jaringan internet.(Purbo, 2006)

Pengalihan permintaan http tersebut dilakukan dengan menginterupsi semua paket dengan mengabaikan setiap alamat dan nomor port yang dituju. Pada halaman autentikasi, user akan disuguhi variable-variabel yang harus di isi untuk authentikasi, biasanya berupa kode pengguna dan kata kunci.

Pada saat pengguna berusaha mem-*browse* ke *web* di Internet, *Captive Portal* akan memaksa pengguna yang belum di authentikasi untuk masuk ke Web authentikasi dan memberikan pertanyaan *username password* dan informasi tentang jaringan yang mereka masuki. Jika gateway wireless berhasil menghubungkan diri dengan server authentikasi dan berhasil memperoleh identifikasi pengguna, *gateway* dapat mengubah aturan firewall-nya dan mengijinkan pengguna untuk mengakses jaringan dan internet, termasuk mengatur jumlah *bandwidth* dan *port* yang dapat digunakan. Gambar 6 menunjukkan mekanisme captive portal.

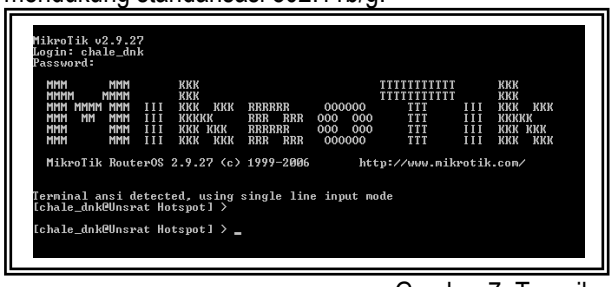


Gambar 6. Mekanisme *Captive Portal*.

V. Implementasi Captive Portal Untuk Meningkatkan Kinerja Akses Point

5. 1. Implementasi Captive Portal.

Implementasi *captive portal* di Universitas Sam Ratulangi mengunakan sistem operasi Mikrotik RoutersOS sebagai perangkat lunak berbasis CLI (*Command Line Interface*), seperti pada gambar 7 dan Linksys WRT54G sebagai *Access Point*. Untuk perangkat *Access Point* sebaiknya mengunakan perangkat yang mendukung standarisasi 802.11b/g.



Gambar 7. Tampilan Mikrotik Router OS

5.1.1. Konfigurasi Gateway

Untuk konfigurasi *gateway* mengunakan 2 buah NIC (*Network Interface Card)* yang digunakan untuk membagi jaringan menjadi WAN dan LAN. Untuk disisi WAN mengunakan *interface 'ether1'* dengan mengunakan IP 192.168.4.197 dan subnet 255.255.255.0 dan untuk LAN mengunakan *interface 'ether2'* dengan mengunakan IP 192.168.10.0 dengan subnet 255.255.255.0.

Untuk memasukan IP *address* di Mikrotik dengan mengunakan perintah sebagai berikut:

[chale_dnk@Unsrat Hotspot] > ip address add address=192.168.4.197 netmask=255.255.255.0 interface=ether1
[chale_dnk@Unsrat Hotspot] > ip address add address=192.168.10.0 netmask=255.255.255.0 interface=ether2

selanjutnya membuat *default gateway* untuk melakukan koneksi internet, dalam hal ini mengunakan IP 192.168.4.2, dengan mengunkan perintah:

[chale_dnk@Unsrat Hotspot] > ip route add gateway=192.168.4.2

5.1.2. Konfigurasi DHCP Server

Agar *client* hotspot mendapatkan IP *address* secara otomatis maka server perlu di setting menjadi DHCP server. Dalam pemberian IP *address* perlu dibuat DHCP *Pool* untuk penyewaan IP kepada *client*, untuk *range* IP yang digunakan yaitu 192.168.10.100 - 192.168.10.200.seperti dibawah ini :

[chale_dnk@Unsrat Hotspot] > ip pool add name=dhcp-poll ranges = 192168.10.100-192.168.10.200

Selanjutnya membuat DHCP *Network* dan *Gateway* yang akan di distribusikan kepada *client*. Pada kasus ini *network*-nya mengunakan 192.168.10.0 dengan subnet 255.255.255.0 dan gateway 192.168.10.1

[chale_dnk@Unsrat Hotspot] >ip dhcp-server network add address=192.168.10.0/24 gateway=192.168.10.1

Setelah membuat dhcp pool dan dhcp network, langkah selanjutnya adalah membuat dhcp server dengan mengunakan konfigurasi-konfugurasi seperti yang telah dibuat.

[chale_dnk@Unsrat Hotspot] >add name=Doank interface=ether2 address-pool=dhcp-pool lease-ti

5.1.3. Konfigurasi Captive Portal

Untuk konfigurasi *captive portal*, mengunakan interface ether2 dengan IP 192.168.10.2 sebagai server *captive portal*. Seperti yang di tampilakan pada gambar 8 di bawah ini:

```
Terminal ansi detected, using single line input mode
[chale_dnk@Unsrat Hotspot] > ip hotspot
[chale_dnk@Unsrat Hotspot] ip hotspot> set
set  setup
[chale_dnk@Unsrat Hotspot] ip hotspot> setup
hotspot interface: ether2
local address of network: 192.168.10.2/24
masquerade network: yes
address pool of network: 192.168.10.100-192.168.10.200
select certificate: none
ip address of smtp server: 0.0.0.0
dns servers: 203.130.254.140,202.134.2.5
dns name:
[chale_dnk@Unsrat Hotspot] ip hotspot> _
```

Gambar 8. Tampilan konfigurasi Captive Portal

5.1.4. Proses Pembuatan Profil User Hotspot

Untuk proses pembuatan profil *user* hotspot berdasarkan tingkatan dan otoritas *user* dalam mengakses internet mengunakan perintah seperti contoh dibawah ini:

[chale_dnk@Unsrat Hotspot] > ip hotspot user profile add name="Limeted User kuota download" address-Pool="dhcp-pool" session-timeout="5m" idle-timeout="none" keepalive-timeout="2m" status-autorefresh="1m" shared-users="50" rate-limit="128/32" transparent-proxy="yes"

5.1.5. Proses Pembuatan Pengguna Hotspot

Untuk proses pembuatan pengguna hotspot berdasarkan tingkatan dan otoritas pengguna dalam mengakses internet mengunakan perintah seperti contoh dibawah ini:

add name=charles password=doank profile="Limited User time limit" limit-uptime=30d

perintah diatas merupakan perintah untuk membuat pengguna dengan profile pengguna "*Limeted User* Mahasiswa", dimana untuk pengguna tersebut dibatasi pengunaan internet selama 30 hari atau satu bulan.

5.1.6. Konfigurasi Radius Server

Pengunaan radius server pada jaringan *wireless* yang mengunakan *captive portal* dimaksudkan agar para pengguna jaringan *wireless* di Universitas Sam Ratulangi dapat melakukan *login* dengan mengunankan satu *account (user id)*, tanpa perlu memiliki beberapa *account* jika para pengguna melakukan *roaming*. Untuk itu diperlukan sebuah *server* yang terpisah dari server *captive portal,* yang di tempatkan sejajar dengan Router yang memiliki IP global.

Pengunaan radius server pada jaringan *wireless* yang mengunakan *captive portal* dimaksudkan agar para pengguna jaringan *wireless* di Universitas Sam Ratulangi dapat melakukan *login* dengan mengunankan satu *account (user id)*, tanpa perlu memiliki beberapa *account* jika para pengguna melakukan *roaming*. Untuk itu diperlukan sebuah *server* yang terpisah dari server *captive portal,* yang di tempatkan sejajar dengan Router yang memiliki IP global.

Untuk jenis radius yang digunakan, penulis mengunakan radius yang terdapat pada Mikrotik RoutersOS v2.9.27, dengan konfigurasi mengunakan IP global yaitu 203.130.254.137. Untuk menghubungkan server *captive portal* dengan Radius server, harus mengkonfigurasi server *captive portal* menjadi radius *client* dengan mengunakan perintah sebagai berikut:

[chale_dnk@Unsrat Hotspot] > radius add service=login,hotspot address=203.130.254.137 secret=132936

5. 2. Pengoperasian Sistem

Dalam pengoperasian sistem ini diatur oleh administrator, dalam mengakses sistem dapat dilakukan secara langsung atau melalui remote, mengunakan telnet atau SSH (*Secure Shell*). Sedangkan pengguna *wireless* LAN dibagi menjadi 3 jenis pengguna (*user*) yang masing-masing memiliki otoritas dan tingkatan tertentu dalam mengakses internet mengunakan sistem *captive portal* yang berjalan, yaitu *Unlimited User, Limited User,* dan *Guest.* Sedangkan untuk pengguna yang melakukan *roaming* mengunakan account dari radius server,sehingga dapat mengakses koneksi internet melalui server *captive portal*

5.2.1. Unlimited user

Unlimited user memiliki otoritas penuh dalam mengakses jaringan *wireless* LAN sistem *captive portal* berupa, *bandwith* internet yang tidak dibatasi, tidak adanya batasan waktu dalam mengakses internet *(time limit)*, serta kuota *Download* dan *Upload* tidak di batasi. *Unlimited user* ini diperuntukan bagi para petinggi Unsrat, misalnya Rektor, Pembantu-Pembantu Rektor,serta Dekan-dekan fakultas yang ada di Universitas Sam Ratulangi.

5.2.2.. Limited user

Untuk *Limited user* dibagi menjadi dua jenis:

- *Limited user* berdasarkan waktu (*time limit*)
  Untuk *limited user* berdasarkan waktu *(time limit)* dibatasi pengunaan internet dengan mengunakan waktu yang dilakukan oleh *user* (penguna) yang mekakukan koneksi inernet. *Limited user* berdasarkan waktu ditujukan kepada dosen-dosen serta para pegawai yang ada di lingkungan Universitas Sam Ratulangi. Untuk *bandwith* internet yang diberikan sebesar 128 kbps untuk *upload* dan 128 kbps *download* per-*user.*
- *Limited user* berdasarkan kuota *download* dan *upload*.
  Untuk *limited user* berdasarkan kuota *download* dan *upload* ke internet
  dibatasi berdasarkan paket-paket data yang telah di *download* dan *upload*.

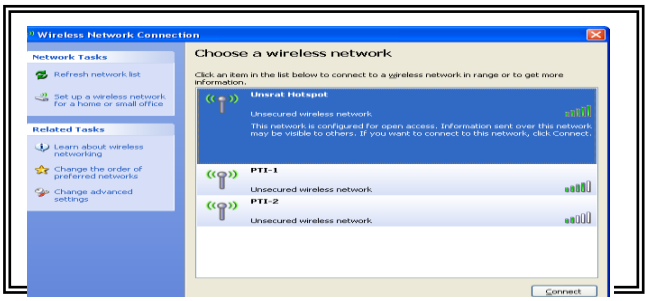
5.2.3. Guest

Untuk guest (tamu) memiliki otoritas yang terbatas, pengguna ini tidak melakukan login untuk mengakses internet. Pengguna ini hanya memiliki otoritas untuk melakukan *browsing* pada situs-situs yang ditentukan, misalnya situs Universitas Sam Ratulangi (http://www.unsrat.ac.id), situs detik (http://www.detik.com) ,serta situs yahoo (http://www.yahoo.com).

5. 3. Tampilan Sistem Captive Portal

5.3.1. Tampilan Konfigurasi Jaringan pada Sisi Client

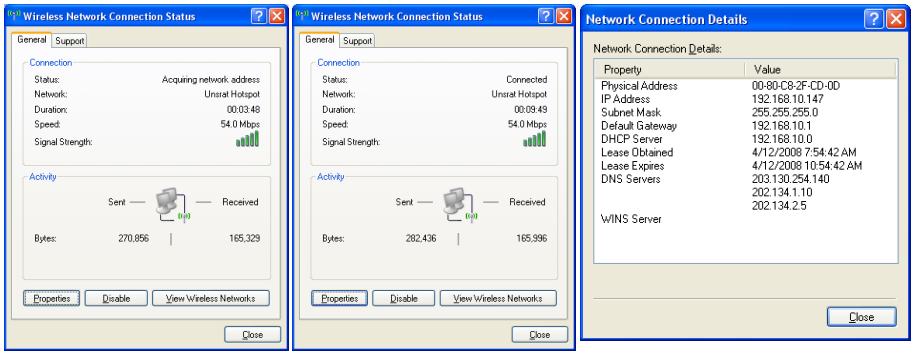
Sebelum client terhubung ke jaringan Unsrat Hotspot, Pastikan perangkat wireless telah terpasang dan diaktifkan. Untuk melihat jaringan *wireless* mana yang aktif dapat mengunakan *software wireless client* dari system operasi Windows XP, yang mempunyai kemampuan sangat terbatas dalam hal menampilakan informasi mengenai jaringan *wireless* yang aktif, seperti pada gambar 9.



Gambar 9. Scanning Jaringan Wireless

5.3.2. Proses Pemberian IP

Setelah terhubung dengan jaringan wireless client akan me-*request* IP ke dhcp server, selajutnya server akan memberikan ip yang tersedia kepada komputer *client*.tambak pada gambar 10 (a) komputer *client* sedang melakukan proses pencarian IP ke DHCP Server, sedangkan pad gambar 10 (b) dan 10 (c) komputer client telah mendapatkan IP *address* dari DHCP Server

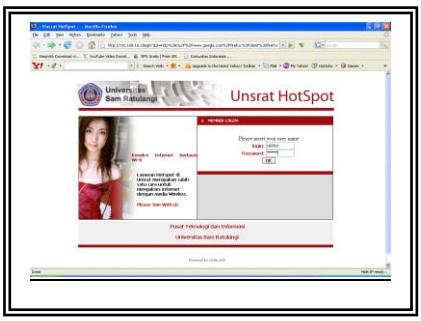


(a) *(b)* *(c)*

Gambar 10. Proses Pemberian IP

5.3.3. Halaman Login

Ketika pengguna akan melakukan koneksi ke internet mengunakan web browser, server captive portal akan mengarahkan ke halaman login, seperti pada gambar 11.



Gambar 11. Tampilan Halaman Login

Pengguna akan memasukan "*user name*"dan "*password"* untuk mendapatkan akses ke internet berdasarkan hak akses tiap-tiap pengguna. Setelah berhasil *login, server* akan menampilkan status koneksi, berupa IP *address* yang digunakan, aktifitas data yang diterima dan yang keluar, serta waktu koneksi yang dilakukan.

5. 4. Analisa Kinerja Akses Point.

Hasil pengujian yang dilakukan, dimana pada *access point* fitur keamanan diaktifkan, ketika mengirimkan paket dalam jumlah yang banyak, sebagian dari paket yang dikirimkan akan megalami kerusakan yang diakibatkan oleh enkripsi dan dekripsi yang dilakukan pada *access point*. Pada gambar 12 dan 13 pengujian dilakukan dengan mengirimkan paket sebesar 65500 byte dari laptop ke komputer lain melalui *access point* dengan mengunakan perintah *ping* selama 5 menit dan fitur keamanan akses pint diaktifkan..

Gambar 12. Pengujian Akses Point dengan mengaktfikan fitur keamanan pada akses point.

Gambar 13 Pengjujian Akses Point dengan TIDAK mengaktifkan fitur keamanan pada akses point

Berdasarkan gambar diatas terdapat perbedaan antara *access point* yang menerapakan sistem keamanan dengan yang tidak. Dimana *access point* yang tidak mengaktifkan fitur keamanan memiliki tingkat keberhasilan yang lebih besar dalam mengirimkan paket. Hal ini disebabkan *access point* tidak melakukan proses dekripsi dan enkripsi dalam setiap pengiriman paket, melainkan dilakukan pada server captive portal dengan melakukan pembuktian keabsahan (*authentication)* para pengguna jaringan WLAN, melalui web browser tanpa perlu melakukan konfigurasi apa pun di sisi pengguna. Serta mengatur pengunaan bandwith berdasarkan jenis-jenis pengguna yang ada di Universitas Sam Ratulangi

VI. Penutup / Kesimpulan.

- Dalam perancangan sistem *Captive Portal* di Universitas Sam Ratulangi menggunakan sistem operasi Mikrotik RoutersOS yang berbasis CLI (*Command Line Interface*)

- Dengan mengunakan sistem *Captive Portal* di jaringan *wireless* LAN pengelolah jaringan dapat mengatur para pengguna jaringan *wireless* LAN yang terhubung dengan *access point,* sehingga lebih efektif dan efisien.
- Dengan mengunakan sistem *Captive Portal* Keamanan di jaringan *wireless* LAN dapat ditingkatkan.
- Untuk dapat mengakses *wireless* LAN pengguna*(user)* harus melakukan authentikasi melalui *web browser.*
- Dengan menghubungkan radius server dengan server captive portal, para pengguna *wireless* LAN dapat melakukan *roaming* atau berpindah tempat tanpa perlu memiliki beberapa *account*
- Kinerja dari *access point* dapat meningkat, hal ini dapat dilihat dari pengujian yang dilakukan,dimana *access point* yang mengaktifkan fitur keamnaan akan selalu gagal dalam mengirimkan paket, hal ini disebabkan oleh adanya proses *enkripsi* dan *dekripsi* di *access point.*

Daftar Pustaka:

[1] Anonimous, " *Mikrotik RoutersOS 2.9 Reference Manuals*. http://www.mikrotik.com," 2 februari 2008.

[2] Geier, J., "*Wireless Networks First-Step*." Terjemahan tim penerjemah ANDI. Yogyakarta: ANDI Yogyakarta, 2005.

[3] Faisal, Lisa., "*Wireless Hacking Di Windows & Teknik Pengamanannya*". Jakarta: InfoKomputer, 2007

[4] Purbo, Onno W., *"Buku Pegangan Internet Wireless dan Hotspot.",* Jakarta: PT Elex Media Komputindo, 2006

[5] Satya, Ika A., "*Mengenal dan Mengunakan Mikrotik Winbox Router Moderen Berbasis PC (Windows dan Linux)*", Jakarta: Datakom Lintas Buana, 2006

[6] S'to., "*Menguasai Windows Server 2003*". Jakarta: PT Elex Media Komputindo, 2004.

[7] S'to., "*Wireless Kung Fu : Networking & Hacking",* Jakarta: Jasakom, 2007.

[8] Sugiardi, Michael S. , " *WLAN Seminar*" , Ritzy Hotel. Manado, 2006.

[9] Stallings, William., "*Komunikasi Data dan Komputer: Jaringan Komputer*". Jakarta: Salemba Teknika, 2002.