ANALISA IMPLEMENTASI KEAMANAN AKSES WIFI CAPTIVE PORTAL DENGAN MENAMBAHKAN FITUR *PASSWORD LOGIN REQUEST* MELALUI SMS

Oleh

Agustini Rodiah Machdi

Abstrak

Jaringan Wifi (*Wireless Fidelity*) memiliki lebih banyak kelemahan dibanding dengan jaringan kabel. Untuk mengatasinya, dilakukan pengaturan terhadap fasilitas jaringan *wireless* agar dapat terbentuk sebuah jaringan *wireless* yang aman dengan menggunakan aplikasi *captive portal*. Untuk meningkatkan keamanan akses, dimana user akan memiliki password yang berubah-ubah pada setiap akan login memasuki wifi, dengan menambahkan fitur *password request* melalui SMS.

Melengkapi proses analisa, dilakukan simulasi menggunakan OPNET Modeller untuk mengukur *delay otentikasi Captive Portal* - SMS dan *throughput* jaringan, yaitu membandingkan antara tanpa *otentikasi* dan yang menggunakan proses *otentikasi*.

Hasil pengukuran waktu dari proses otentikasi wifi dengan menerapkan *captive portal* - SMS waktu rata-rata yang dibutuhkan dalam proses keseluruhan alur kerja ini adalah 2 menit 9,752 detik.

Perbedaan pada saat simulasi adalah waktu respon untuk proses otentikasi, yang mencapai waktu 2 menit sebelum akhirnya memulai proses *download* maupun *upload*. Sedangkan simulasi yang tanpa menggunakan proses otentikasi, *download* dan *upload* langsung terjadi pada saat menit pertama dalam rentang waktu simulasi.

Implementasi dari captive portal dapat memaksimalkan pengaturan bandwidth, sehingga dapat diimplementasikan di jaringan Wifi Internet Service Provider dan kampus.

Kata Kunci : *wifi, hotspot, captive portal, IEEE 802.1X, radius, sms, opnet.*

1. PENDAHULUAN

Jaringan Wifi (*Wireless Fidelity*) memiliki lebih banyak kelemahan dibanding dengan jaringan kabel. Saat ini perkembangan teknologi wifi sangat signifikan sejalan dengan kebutuhan system informasi yang mobile.Banyak penyedia jasa wireless seperti hotspot komersil, ISP, Warnet, kampus maupun perkantoran sudah mulai memanfaatkan wifi pada jaringan masing-masing, tetapi sangat sedikit yang memperhatikan keamanan komunikasi data pada jaringan wireless tersebut.

Kelemahan jaringan wireless secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Salah satu contoh penyebab kelemahan pada konfigurasi karena saat ini untuk membangun sebuah jaringan wireless cukup mudah. Banyak vendor yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan wireless yang masih menggunakan

konfigurasi wireless default bawaan vendor. Sering ditemukan wireless yang dipasang pada jaringan masih menggunakan setting default bawaan vendor seperti SSID, IP Address , remote manajemen, DHCP enable, kanal frekuensi, tanpa enkripsi bahkan user/password untuk administrasi wireless tersebut. WEP (*Wired Equivalent Privacy*) yang menjadi standar keamanan wireless sebelumnya, saat ini dapat dengan mudah dipecahkan dengan berbagai tools yang tersedia gratis di internet. WPAPSK dan LEAP yang dianggap menjadi solusi menggantikan WEP, saat ini juga sudah dapat dipecahkan dengan metode dictionary attack secara offline.

Untuk mengatasinya, pada jurnal ini akan dibahas untuk melakukan pengaturan terhadap fasilitas jaringan wireless agar dapat terbentuk sebuah jaringan wireless yang aman dengan menggunakan server RADIUS untuk authentifikasi dan otorisasi hak akses. Serta implementasi aplikasi captive portal pada jaringan wireless untuk lebih meningkatkan keamanan dan kenyamanan saat pengguna melakukan koneksi dan otentikasi terhadap penggunaan jaringan wireless, yang selanjutnya diperkuat dengan proses password request melalui SMS yang harus dilakukan masing-masing user sebelumnya untuk mendapat password login melalui captive portal dan analisa sistem menggunakan simulasi *software* simulator OPNET Modeler versi 14.

2. TEORI

2.1. Wireless dan WiFi

Wireless menggunakan gelombang radio (*electromagnetic*) untuk berkomunikasi dengan lainnya. Sebagai media transmisi menggantikan media kabel. Semakin jauh jangkaun dari wireless maka sinyal dan kecepatan yang didapat akan semakin rendah. Wi-Fi (atau Wi-fi, WiFi, Wifi, wifi) merupakan kependekan dari Wireless Fidelity, memiliki pengertian yaitu sekumpulan standar yang digunakan untuk Jaringan Lokal Nirkabel (*Wireless Local Area Networks* - WLAN) yang didasari pada spesifikasi IEEE 802.11. [17]

Sekarang ini ada empat variasi dari 802.11, yaitu: 802.11a, 802.11b, 802.11g, and 802.11n. Spesifikasi b merupakan produk pertama Wi-Fi. Variasi g dan n merupakan salah satu produk yang memiliki penjualan terbanyak pada 2005. [20]
Spesifikasi kecepatan dan frekuensi band yang digunakan : [3]

1. 802.11b 11 Mb/s 2.4 GHz b
2. 802.11a 54 Mb/s 5 GHz a
3. 802.11g 54 Mb/s 2.4 GHz b, g
4. 802.11n 100 Mb/s 2.4 GHz b, g, n

2.2. Kelemahan Wireless

Di bawah ini adalah macam-macam kelemahan dari wireless terdiri dari :

1. Interception atau penyadapan
2. Injection
3. Jamming
4. Locating Mobile Nodes
5. Access Control
6. Hijacking

2.3. Teknik Keamanan pada Wireless LAN

Di bawah ini beberapa kegiatan dan aktifitas yang dilakukan untuk mengamanan jaringan *wireless*, yaitu :

1. Menyembunyikan SSID
2. Keamanan wireless dengan kunci WEP
3. Keamanan wireless dengan WPA
4. MAC Filtering
5. Captive Portal

2.4. Captive Portal

Infrastruktur *Captive Portal* awalnya di design untuk keperluan komunitas yang memungkinkan semua orang dapat terhubung (*open network*). *Captive portal* sebenarnya merupakan mesin router atau gateway yang memproteksi atau tidak mengizinkan adanya *trafik* hingga *user* melakukan *registrasi/ otentikasi.*

Fungsi utama *Captive Portal* adalah : [16]

1) Manajemen member (user) *wireless hotspot*
2) Authentifikasi AAA RADIUS *server*
3) Hotspot anti mac address spoofing
4) Mengatur pembatasan pengguna *wireless, (time based, quota data dan date expire)*
5) *Hotspot user interface* berbasis web

Captive portal menggunakan standar *web browser* untuk memberikan pengguna wifi untuk dapat mengotentikasi dirinya, biasanya berupa username & password. *Captive portal* juga dapat memberi informasi (seperti Kebijakan Penggunaan Jaringan yang Dapat di Terima / *Acceptable Use Policy*) kepada pemakai sebelum memberi akses lebih lanjut. Dengan memakai web browser, captive portal dapat bekerja pada semua laptop dan sistem operasi. Captive portal biasanya dipakai di jaringan terbuka yang tidak mempunyai metode otentikasi lain (seperti WEP atau MAC filter).

2.5. MikroTik RouterOS™

MikroTik RouterOS™ adalah sistem operasi dan yang dapat digunakan untuk menjadikan komputer manjadi router network yang handal, mencakup berbagai fitur lengkap untuk network dan wireless, salah satunya adalah sebagai *Authentication Server Hotspot.*

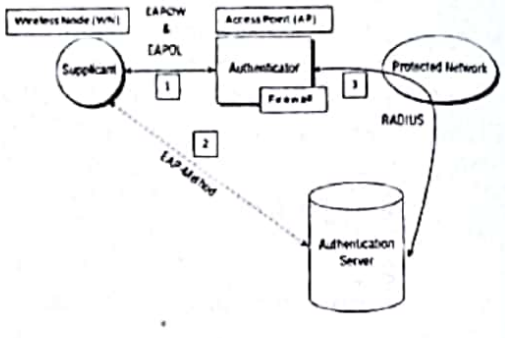
Untuk instalasi Mikrotik tidak dibutuhkan piranti lunak tambahan atau komponen tambahan lain. Mikrotik didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks sekalipun.

2.6. IEEE 802.1x

IEEE 802.1x merupakan salah satu standar keamanan jaringan yang cukup dikenal dan sudah banyak digunakan untuk jaringan *wireless*.

Standar 802.1x merupakan standar keamanan jaringan yang mempunyai banyak mekanisme untuk *autentifikasi*.

IEEE 802.1x atau sering disebut juga "*port based authentication*" merupakan standar yang pada awal rancangannya digunakan pada koneksi dialup. Tetapi pada akhirnya, standar 802.1x digunakan pula pada jaringan IEEE 802 standar. Gambar 1. berikut ini merupakan skema dasar dari standar 802.1x. [9]



Gambar 1. Skema 802.1x

2.7. Remote Authentication Dial-In User Service (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*.
Server RADIUS menyediakan mekanisme keamanan dengan menangani otentikasi 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 otentikasi 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). RADIUS merupakan suatu protokol yang

dikembangkan untuk proses AAA (*authentication, authorization, and accounting*).

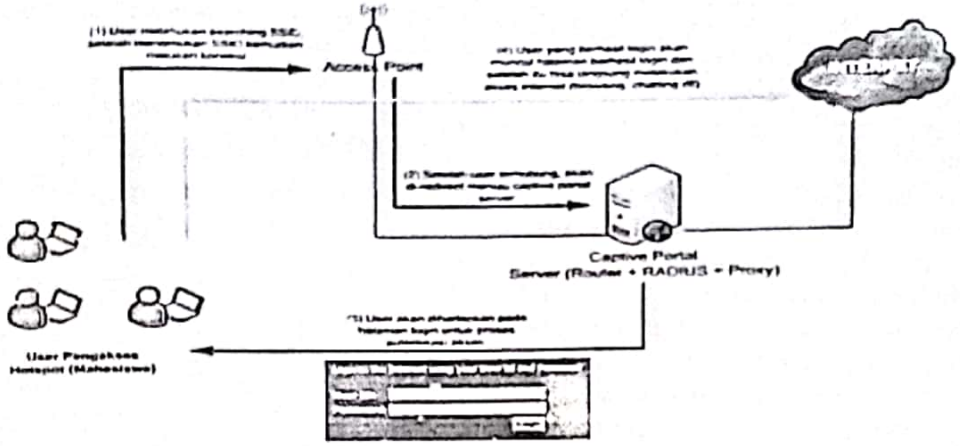
3. IMPLEMENTASI CAPTIVE PORTAL

3.1. *Captive Portal Dengan Fitur Password Login Request* SMS

Untuk membangun *hotspot* dengan *otentikasi* yang ditambah dengan sms password request memerlukan beberapa item:

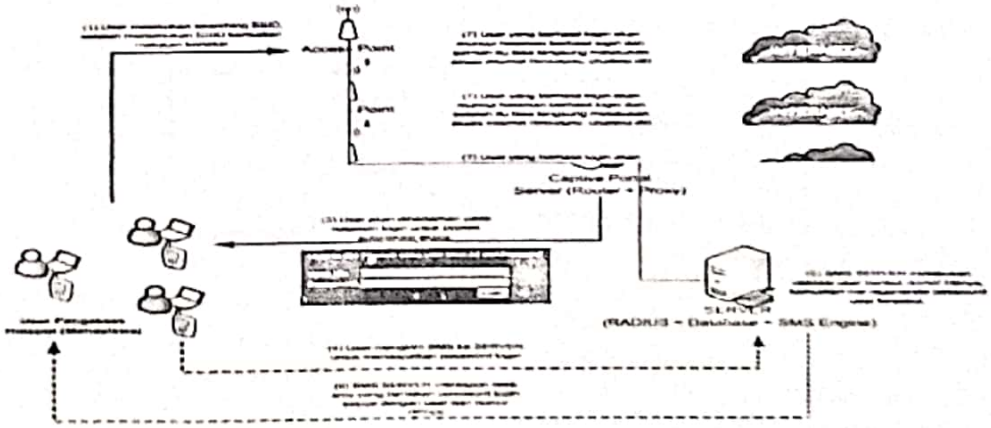
1) Koneksi Internet
2) Wireless LAN Access Point
3) *Captive portal dan Radius Server (Mikrotik RouterOS)*
4) Database *Server*
5) SMS Engine *Server*

Implementasi secara keseluruhan dari keamanan akses wifi dengan menggunakan *Captive Portal* adalah seperti ditunjukkan pada gambar 2 .



Gambar 2. Implementasi keamanan akses wifi dengan menggunakan *Captive Portal*

Kemudian untuk memperkuat keamanan akses dimana *user* akan memiliki *password* yang berubah-ubah pada setiap akan login memasuki wifi, dikembangkan dengan menambahkan fitur *password request* melalui SMS ini seperti yang dapat dilihat pada gambar 3.



Gambar 3. Implementasi keamanan akses wifi dengan menggunakan Captive Portal ditambah SMS Request Password

Mekanisme alur kerja dari implementasi pada gambar 3 adalah sebagai berikut :

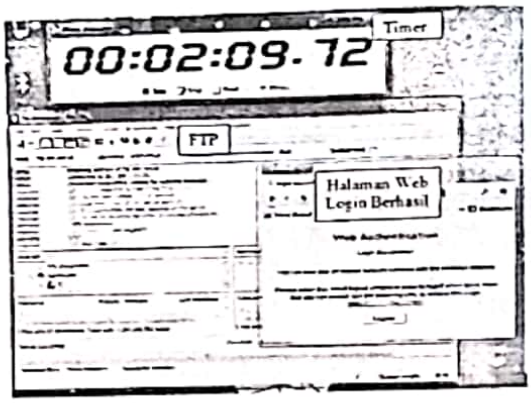
1) User pengakses hotspot yang merupakan supplicant mencari nama SSID dari akses poin yang akan diakses, kemudian user melakukan koneksi pada akses poin yang dituju
2) Akses poin yang berisi otentikator akan meneruskan otentikasi ke *server captive portal*
3) Kemudian server captive portal yang juga berfungsi sebagai router menampilkan halaman login yang harus diisi berupa informasi User ID dan *password* dari user yang akan diotentikasi oleh *authentication server*.
4) Agar dapat melakukan login user kemudian melakukan *request password* melalui SMS ke SMS Server.
5) Kemudian SMS server membalas sms yang berisi password yang baru saja di-generate secara otomatis oleh server sesuai dengan user ID dan nomor Handphone user tersebut.
6) *Authentication server* melakukan pemeriksaan mengenai user dan password yang dimasukan oleh user tersebut, bila validasi sesuai dengan yang ada di database authentication server maka user tersebut berhak mengakses wifi dan internet.

4. ANALISA

4.1. Analisa Kondisi Dari Proses *Otentikasi* Wifi Menggunakan *Captive Portal –SMS.*

Pada bagian ini akan diperlihatkan berapa besar waktu yang dibutuhkan untuk proses otentikasi Wifi dengan menggunakan Captive Portal – SMS. Skenario yang digunakan adalah satu client dengan satu access point dan melakukan pembebanan traffik dengan menjalankan file transfer (FTP).

Pertama pengguna membuka aplikasi FTP , kemudian menuliskan alamat dari server ftp yang dituju, setelah itu koneksi dijalankan kemudian pengguna langsung di-redirect menuju halaman login untuk proses otentikasi, selanjutnya pengguna mengirimkan SMS untuk meminta password, dengan format isi SMS adalah "*pass*" (tidak case sensitive). Setelah mendapatkan balasan SMS yang berisi *password*, Kemudian pengguna memasukan nama login berikut password yang didapat dari SMS Server, bila login berhasil maka pengguna akan di-redirect menuju halaman web yang menyatakan proses otentikasi berhasil dan pengguna dapat menggunakan fasilitas yang tersedia didalam jaringan, termasuk internet. Proses login ini berlangsung selama 2 menit 9,72 detik. Seperti yang terlihat pada gambar 4. berikut ini.



Gambar 4. Proses Otentikasi Pengguna Berhasil

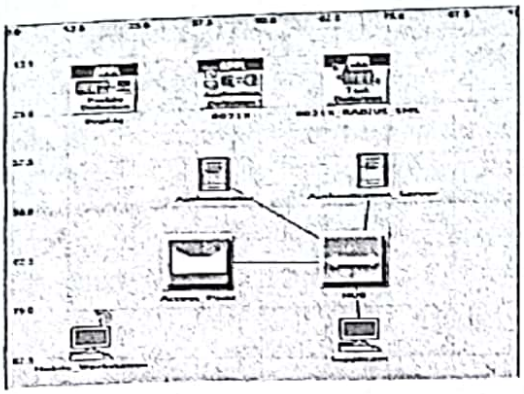
Setelah 10 kali dilakukan pengujian seperti proses diatas, nilai rata-rata waktu yang didapat adalah 2 menit 9,752 detik.

4.2. Simulasi Proses Otentikasi Wifi Dengan Menggunakan Captive Portal – SMS Menggunakan *OPNET Modeller.*

4.2.1. Topologi Jaringan Simulasi Pertama

Arsitektur ini, seperti yang ditunjukkan pada gambar 5, terdiri dari tiga objek (*Profile, Application* dan *Task Definition*) serta 5 node (*workstation*, dua *server, access point* dan sebuah *switch Ethernet*), *link wireless* 802.11g menghubungkan *workstation* dan *access point*, sedangkan link ethernet

100BaseT menghubungkan *access point* dengan kedua *server*.



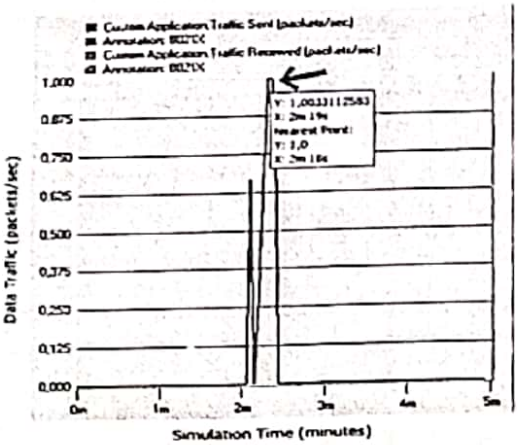
Gambar 5. Topologi Simulasi Satu Access Point dan Satu Workstation

4.2.2. Hasil dan Analisa Statistik Simulasi WiFi Menggunakan *OPNET Modeller*

Grafik-grafik yang dihasilkan merupakan hasil setelah tools statistik dijalankan pada *OPNET*.

4.2.2.1. Trafik Data Pengaplikasian *Captive Portal – SMS*

Hasil dari simulasi untuk *traffik* data untuk Pengaplikasian *Captive Portal* – SMS dapat dilihat pada gambar 6 di bawah ini :

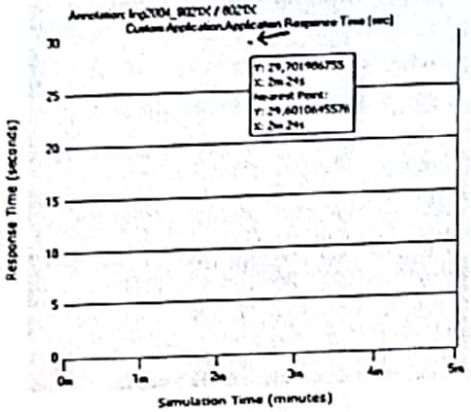


Gambar 6. Grafik Traffic Data Pengaplikasian Captive Portal – SMS

Grafik pada gambar 6 menjelaskan bahwa paket yang diterima dan dikirim dalam jaringan wireless selalu ada kaitannya dengan proses otentikasi 802.1X (garis grafik berwarna biru), jadi data tidak akan diterima (garis grafik berwarna merah) sebelum mengalami proses otentikasi.

4.2.2.2. Waktu Respon IEEE 802.1X

Gambar 7 merupakan hasil dari simulasi untuk waktu respon IEEE 802.1X

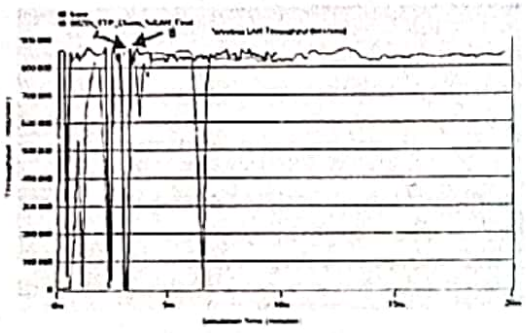


Gambar 7. Waktu Respon 802.1X

Gambar 7 menunjukkan grafik waktu respon dari proses otentikasi 802.1X yang disimulasikan, yang diberi tanda panah, dimana didapat hasil 29,702 detik, angka ini diatas angka teoritis, dimana secara teoritis waktu respon bernilai 29,6 detik.

4.2.2.3. Throughput Wireless LAN

Hasil dari simulasi untuk throughput wireless LAN dapat dilihat pada gambar 8 berikut ini:



Gambar 8. Grafik Throughput Wireless LAN

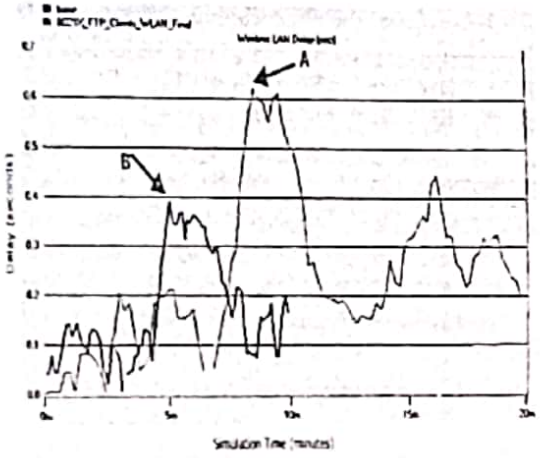
Dari grafik pada gambar 8 menunjukan troughput pada kecepatan implementasi

Captive Portal-SMS (garis grafik warna merah) tidak menyebabkan perbedaan yang sangat jauh jika dibandingkan dengan tanpa Captive Portal-SMS (base, garis grafik warna biru).

Troughput maksimum yang mampu dicapai pada saat simulasi ini, dengan mengimplementasikan proses otentikasi adalah 850.000 bits/sec (titik A merah), dan tanpa proses otentikasi adalah 865.000 bits/sec (titik B biru), kedua *throughput* ini sama-sama dicapai pada menit ke 4 selama rentang waktu simulasi.

4.2.2.4. Delay Wireless LAN

Hasil dari simulasi untuk delay wireless LAN dapat dilihat pada gambar 9 di bawah ini:



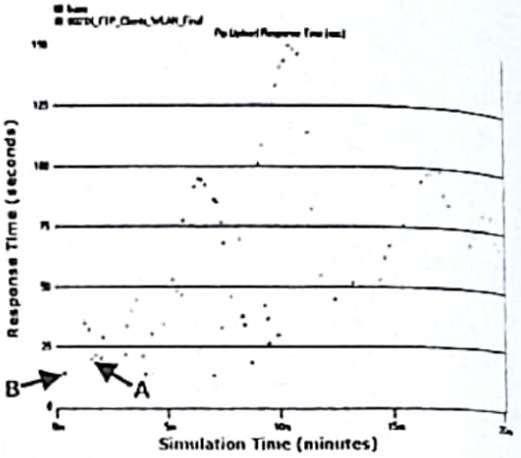
Gambar 9. Grafik Delay Wireless LAN

Dari grafik pada gambar 9, terlihat dalam hal waktu secara keseluruhan pada Captive Portal –SMS (garis grafik warna merah) terdapat delay lebih tinggi bila dibandingkan dengan tanpa Captive Portal-SMS (garis grafik warna biru).

Delay maksimum yang dicapai pada saat simulasi ini, dengan mengimplementasikan proses otentikasi adalah 0,61 detik (titik A merah), dan tanpa proses otentikasi adalah 0,4 detik (titik B biru), tetapi dari sisi keamanan jaringan dengan proses otentikasi lebih terjamin.

4.2.2.5. Upload Respon Time FTP

Hasil dari simulasi untuk upload respon time dapat dilihat pada gambar 10 di bawah ini:

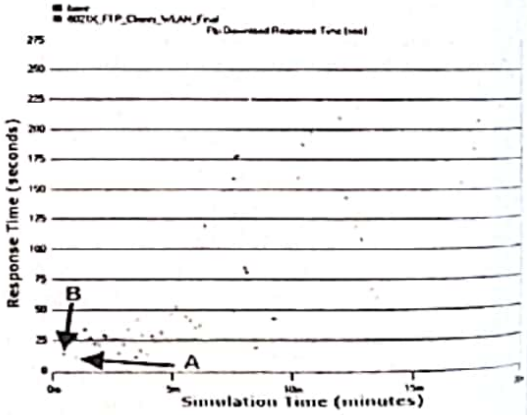


Gambar 10. Grafik Upload Respon Time FTP

Dari grafik pada gambar 10 terlihat penundaan waktu inisiasi upload FTP. Dari simulasi didapat grafik waktu upload FTP dimulai 2 menit kemudian (titik A merah), ini dikarenakan adanya proses otentikasi Captive Portal–SMS. Sedangkan inisiasi upload FTP tanpa otentikasi dimulai pada rentang waktu kurang dari 1 menit (titik B biru).

4.2.2.6. Download Respon Time FTP

Hasil dari simulasi untuk download respon time dapat dilihat pada gambar 11 berikut ini:



Gambar 11. Grafik Download Respon Time FTP

Dari grafik pada gambar 11 terlihat penundaan waktu download FTP. Dari

simulasi didapat grafik waktu inisiasi download FTP dimulai sekitar 2 menit kemudian, ini dikarenakan adanya proses *otentikasi Captive Portal* – SMS (titik A merah).

Sedangkan *inisiasi download* FTP tanpa otentikasi dimulai pada rentang waktu 1 menit (titik B biru).

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Dari hasil analisa dan simulasi jaringan Wifi menggunakan OPNET Modeler, dengan kondisi dari proses otentikasi dengan menggunakan Wifi, satu *Acces point* satu *client* dan satu *Acces point* enam *client*, maka dapat disimpulkan :

1) Waktu otentikasi Wifi rata-rata dengan menggunakan Captive Portal – SMS adalah 2 menit 9,752 detik.
2) Pada simulasi menggunakan Opnet waktu respon dari proses otentikasi 29,702 detik.
3) Pada simulasi Opnet, *troughput* maksimum yang mampu dicapai pada saat simulasi, dengan mengimplementasikan proses otentikasi adalah 860.000 bits/sec.
4) Pada Opnet, *delay* maksimum yang dicapai dengan mengimplementasikan proses otentikasi adalah 0,4 detik.
5) Implrmentasi dari pengaturan *bandwidth* untuk bandwidth internasional dibatasi sebesar 64 Kbps. Sedangkan untuk *bandwidth local* bandwidth minimum 1 Mbps dan maksimum 2 Mbps.

5.2. Saran

Untuk mempercepat proses SMS di *server* disarankan menggunakan spesifikasi yang lebih tinggi, baik dari sisi *processor*, RAM, maupun *hardisk*, karena semua layanan yang menggunakan *data base* (RADIUS, SMS *engine*, MySQL) lebih banyak menggunakan *resources* dari RAM dan *processor*.

DAFTAR PUSTAKA

1) Aboba, Bernard., Moore, Tim., 2000, IEEE 802.1X For Wireless LANs, doc. IEEE 802.11-00/035
2) Barnes, Christian., 2002, Hack Proofing Your Wireless Network. Syngress, Rockland, page. 201, 239-361.
3) Briere, Danny., 2003, Wireless Home Networking for Dummies, Wiley Publishing Inc., Indianapolis, page. 16. 17, 28, 29.
4) Cabral, Sheeri K., 2009, MySQL Administrator's, Wiley Publishing Inc., Indianapolis, page 31, 114.
5) Ding, P, Holliday J, and Celik A., 2004. Improving the Security of Wireless LANs by Managing 802.1x Disassociation. Proceedings of the IEEE Consumer Communications and Networking Conference, Las Vegas. NV., page. 10.
6) Distribusi, 2009, Bikin Gateway Murah Pakai Mikrotik, Info Komputer, Jakarta, halaman 37
7) Earle, Aaron E., 2006, Wireless Security Handbook, Auberbach Publication, New York, page. 181, 190. 227.
8) Febyatmoko, Gesit Singgih., Hidayat. Taufiq., Andri S. Mukhammad., 2006. Sistem Otentikasi, Otorisasi, Dan Pelaporan Koneksi User Pada Jaringan Wireless Menggunakan Chillispot Dan Server RADIUS, Media Informatika. Vol. 4, No. 1, Juni 2006, Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia, Jogjakarta
9) Geier, Jim., 2008, Implementing 802.1X Security Solutions for Wired and Wireless Networks, Wiley Publishing Inc., Indianapolis, page. 14. 22, 38, 39, 49.
10) IEEE, 1999, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications 802.11 Standard, page. 29.
11) IEEE, 2001, IEEE 802.1x – Port-based network access control.

12) Janevski, Toni., 2003, Traffic Analysis and Design of Wireless IP Networks, Artech House, Boston, page 15, 17.
13) M. Tara., Elden, Charles R., 2002, Wireless Security and Privacy: Best Practices and Design Techniques, Addison Wesley, Boston, Chapter 2, 3.
14) Macaulay, Tyson., 2002, Hardening IEEE 802.11 Wireless Networks, EWA, Canada, page. 4, 17.
15) Nugroho M. Agung, 2009, Studi Kasus Celah Keamanan pada Jaringan Nirkabel yang Menerapkan Wired Equivalent Privacy (WEP), Prosiding Seminar Nasional Open Source Software III ISSN 1978-7510 page A-8, Pusat Penelitian Informatika Lembaga Ilmu Pengetahuan Indonesia, Jakarta.
16) Nugroho M. Agung, 2009, Analisa dan Studi Kasus Manajemen Hotspot dengan Aplikasi Captive Portal pada Jaringan Nirkabel untuk Layanan Hotspot UPT STMIK AMIKOM YOGYAKARTA, Prosiding Seminar Nasional Open Source Software III ISSN 1978-7510, Pusat Penelitian Informatika Lembaga Ilmu Pengetahuan Indonesia, Jakarta, halaman B-18
17) Priyambodo, Tri Kuntoro., 2005, Jaringan Wi-Fi Teori dan Implemetasi, Penerbit Andi, Jogjakarta, halaman 22, 27.
18) Ross, John., 2008, The Book of Wireless 2nd Edition, No Starch Press, San Fransisco, page. 141, 195, 211.
19) Soyinka, Wale., 2010, Wireless Network Administration A Beginner's Guide, McGraw Hill, New York, page. 74, 142.
20) Stallings, William., 2005, Wireless Communication and Networks, Pearson Prentice Hall, New Jersey, page. 2, 264.
21) Zhang, Cathy, Chau, Ricky, Sun, Wenqi, Wi-Fi Network Simulation OPNET, Simon Fraser University Offset, Vancouver Canada, page 7.
22) http://www.analysis.com, diakses tanggal 5 Februari 2011
23) http://www.activexperts.com/activsms, diakses tanggal 12 Januari 2011

PENULIS :

Agustini Rodiah Machdi, ST., MT., Staf Dosen Program Studi Teknik Elektro FT-Unpak Bogor