

IMPLEMENTASI SISTEM OTENTIKASI PADA PENGGUNA JARINGAN *HOTSPOT* GUNA MENINGKATKAN KEAMANAN JARINGAN KOMPUTER

Oleh: Irma T

Pendidikan Matematika IAIN Palopo

e-mail: irmaikom@yahoo.co.id

Abstrak:

Semakin banyaknya aplikasi yang menggunakan *client server* baik *desktop* maupun *WEB Application* membuat setiap user harus memiliki banyak *user id* dan *password* yang harus dihapalkan, karena setiap aplikasi pasti membutuhkan otentikasi agar dapat memanfaatkan aplikasi tersebut dengan alasan keamanan. Selain itu perkembangan media jaringan juga semakin berkembang baik penggunaan kabel maupun nirkabel. Dari penjelasan diatas teknologi RADIUS sangatlah dibutuhkan dalam kasus yang telah dijelaskan diatas, karena dengan metode RADIUS ini memungkinkan seorang user cukup memiliki satu *user id* untuk mengakses ke beberapa aplikasi, baik *desktop* maupun *WEB application*. Metode RADIUS juga dapat diintegrasikan terhadap media kabel dan nirkabel.

Kata kunci: Nirkabel, WEP, otentikasi, RADIUS, *database*, *server*, *client*

I. Pendahuluan

Penggunaan jaringan saat ini pada umumnya tanpa adanya otentikasi pengguna. Dengan tanpa adanya otentikasi pengguna ini maka jaringan dapat diakses oleh siapa saja ketika pengguna bergabung dalam jaringan. Untuk media transmisi menggunakan *wireless access point* otentikasi menggunakan *Wired Equivalent Privacy* (WEP). *Key* pada WEP harus dipasang pada tiap *access point* dan tiap *client access point*, sehingga merepotkan administrator karena harus mendatangi masing-masing *client*. *Key* WEP juga bersifat statik sehingga mudah diketahui dengan melihat komputer *client* yang lain. Sekarang sudah ada beberapa aplikasi yang bisa membaca *key* WEP sehingga pengguna yang tidak berhak bias masuk ke jaringan, yang bisa membahayakan sistem didalamnya. Otentikasi WEP hanya diberikan kepada jalur koneksi untuk staf, sedangkan jalur koneksi untuk mahasiswa (*hostspot*) yang menggunakan mediatransmisi *wireless access point* tanpa menggunakan otentikasi sehingga dapat diakses oleh siapa saja.

Padamedia transmisi kabel yang menggunakan HUB sebagai pemecah koneksi tidak menggunakan otentikasi, sehingga dengan menancapkan kabel kita bisa langsung terhubung ke jaringan. Oleh karena itu dalam penelitian ini dibuat sistem untuk otentikasi pengguna, baik yang menggunakan media transmisi kabel maupun nirkabel.

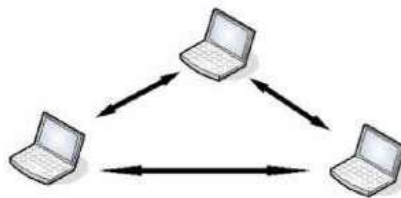
Dalam artikel ini akan diketahui bagaimana pengembangan manajemen sistem keamanan jaringan yang lebih baik, serta mengintegrasikan manajemen *user* untuk beberapa aplikasi

II. Mode Jaringan dan Protokol Route

Jaringan Wireless Jaringan Wireless Local Area Network (WLAN) merupakan salah satu bentuk jaringan wireless. Jaringan WLAN adalah jaringan yang memungkinkan dua mesin atau lebih untuk berkomunikasi menggunakan protokol jaringan standar tetapi tanpa menggunakan media transmisi kabel. Media transmisi yang digunakan komunikasi pada jaringan WLAN adalah gelombang elektromagnetik yang dapat berupa sinar infra-merah (infrared, IR), gelombang mikro (microwave) atau gelombang radio (radio frequency, RF). Mode Jaringan WLAN, antara lain:

1. Mode Ad-Hoc

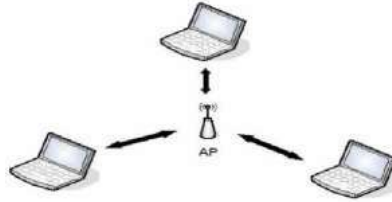
Mode Ad-hoc sering disebut sebagai jaringan peer to peer atau disebut juga jaringan point to point. Mode Ad-hoc memungkinkan hubungan antar computer pada jaringan WLAN tanpa melalui suatu access point.



Gambar 1. Mode Ad-hoc

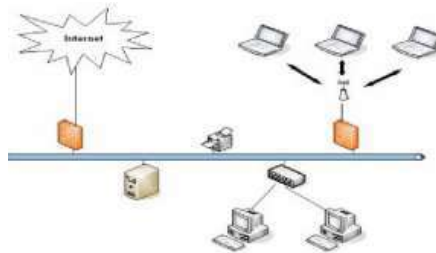
2. Mode Infrastruktur

Untuk menghubungkan banyak computer jaringan WLAN harus dijalankan menggunakan mode Infrastruktur. Pada mode Infrastruktur diperlukan peralatan tambahan berupa wireless access point (WAP) atau disebut secara singkat dengan access point. Access point berlaku seperti HUB atau switch pada jaringan kabel, sehingga access point akan menjadi pusat dari jaringan WLAN.



Gambar 2. Mode Infrastruktur

Jaringan WLAN yang bekerja pada mode Infrastruktur dapat dihubungkan dengan jaringan lain misalnya jaringan Ethernet. Untuk berhubungan dengan jaringan lain diperlukan bridge. Access point yang beredar di pasaran umumnya sudah dapat difungsikan sebagai bridge.



Gambar 3. Jaringan WLAN dan Ethernet

Routing adalah proses membawa paket data dari satu host asal ke host tujuan melalui satu atau beberapa host node lainnya. Secara umum mekanisme koordinasi routing dapat dibagi menjadi dua, yaitu routing statis dan routing dinamis, dengan penjelasan sebagai berikut:

1. Routing Statis

Pada routing statis, entri-entri dalam forwarding tabel routing diisi dan dihapus secara manual sedangkan pada routing dinamis perubahan dilakukan melalui protokol routing. Routing statis adalah pengaturan routing paling sederhana yang dapat dilakukan pada jaringan komputer. Menggunakan routing statis murni dalam sebuah jaringan berarti mengisi setiap entri dalam forwarding table di setiap router yang berada dalam jaringan tersebut.

Penggunaan routing statis dalam sebuah jaringan yang kecil bukanlah sebuah masalah hanya beberapa entri yang perlu diisikan pada forwarding table di setiap router. Sebaliknya jika harus melengkapi forwarding table di setiap router yang jumlahnya tidak sedikit dalam jaringan yang besar.

2. Routing Dinamis

Routing dinamis adalah cara yang digunakan untuk melepaskan kewajiban mengisi entri-entri forwarding table secara manual. Protokol routing mengatur router-router sehingga dapat berkomunikasi satu dengan yang lain dan saling memberikan informasi routing yang dapat mengubah isi forwarding table, tergantung keadaan jaringannya. Dengan cara ini, router-router mengetahui keadaan jaringan yang terakhir dan mampu meneruskan datagram ke arah yang benar.

RADIUS adalah sebuah protokol keamanan komputer yang digunakan untuk melakukan otentikasi, otorisasi, dan pendaftaran akun pengguna secara terpusat untuk mengakses jaringan. RADIUS didefinisikan di dalam RFC 2865 dan RFC 2866, yang pada awalnya digunakan untuk melakukan otentikasi terhadap akses jaringan secara jarak jauh dengan menggunakan koneksi dial-up. RADIUS, kini telah diimplementasikan untuk melakukan otentikasi terhadap akses jaringan secara jarak jauh dengan menggunakan koneksi selain dial-up, seperti halnya VPN (Virtual Private Networking), access point nirkabel, switch Ethernet, dan perangkat lainnya.

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

WEP (Wired Equivalent Privacy) adalah suatu metode pengamanan jaringan nirkabel, disebut juga dengan Shared Key Authentication. Shared Key Authentication adalah metode otentikasi yang membutuhkan penggunaan WEP. Enkripsi WEP menggunakan kunci yang dimasukkan (oleh administrator) ke client maupun access point. Kunci ini harus cocok dari yang diberikan akses point ke client, dengan yang dimasukkan client untuk otentikasi menuju access point.

III. Rancang Sistem

Perangkat Keras (Minimal) yang dibutuhkan adalah sebagai berikut:

1. Motherboard x86 300 MHZ Pentium
2. RAM 64 MB
3. Hardisk 40 GB

Kebutuhan hardware untuk menginstal Router OS, dalam hal ini menggunakan Mikrotik OS

1. CPU dan motherboard 100 MHz Pentium.
2. RAM 32 MB
3. Hardisk ATA/IDE 1 GB.

Media instalasi Linux Ubuntu dan MikroTik adalah:

1. CD Linux Ubuntu Server 8.04 LTS
2. CD MikroTik
3. Software FreeRADIUS Server
4. Software LAMP (Linux Apache MySQL Php)

Pada dasarnya, Pengguna melihat bahwa jaringan yang diperlukan cukup sederhana dan tidak rumit. Ini dikarenakan client memandang jaringan hanya digunakan untuk share informasi yang umum dan koneksi internet.

Aplikasi Desktop adalah suatu aplikasi yang dapat berjalan sendiri atau independen tanpa menggunakan browser pada suatu komputer otonom dengan sistem operasi tertentu. Penggunaan aplikasi desktop dengan cara meng-install aplikasi ini pada masing-masing pengguna. Penggunaan aplikasi desktop untuk proses administrasi.

Beberapa aplikasi berbasis WEB yang ada di laboratorium dapat mengakses aplikasi desktop dan elearning, aplikasi WEB, sedangkan hotspot hanya mengakses ebook, ejournal, WEB mail client, aplikasi WEB saja. line, SIAKAD yang bisa diakses baik melalui jaringan lokal maupun jaringan internet.

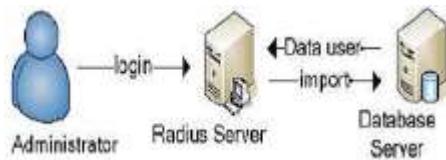
Perancangan Sistem

Beberapa aplikasi server yang digunakan di WEB server pada database server, mail server, FTP server, DNS server, proxy server dan firewall.

Untuk administrasi dan akses internet. Untuk menghubungkan antar gedung kabel yang digunakan adalah kabel STP (Shield Twister Pair). Untuk menghubungkan client dalam satu ruangan digunakan media transmisi kabel UTP (Unshield Twister Pair) dan wireless. Sedang-kan media transmisi untuk hostspot area Untuk memecah antar client digunakan HUB yang diletakan ditiap gedung atau ruangan disesuaikan dengan jumlah client.

Secara sederhana desain topologi dengan RADIUS Server. Server RADIUS berfungsi menyimpan username dan password secara terpusat. Pengguna memasukan username dan password melalui interface yang disediakan oleh NAS (Network Access Server), selanjutnya NAS akan menanyakan ke RADIUS server apakah username dan password ada dalam database. Jika username dan password ada maka pengguna akan diijinkan menggunakan jaringan.

Arsitektur sistem otentikasi seperti terlihat pada menggambarkan arsitektur sistem otentikasi, terlihat bahwa pengguna agar terhubung ke dalam jaringan harus menggunakan PC atau Laptop. Pengguna dapat memanfaatkan jaringan apabila memiliki username dan password pada RADIUS server. Apabila pengguna sudah berhasil login, maka pengguna bisa terhubung ke jaringan. Username dan password yang digunakan untuk login adalah user dan password yang digunakan untuk login pada aplikasi bits.



Gambar 4. Arsitektur pengambilan Data Pengguna

Test ID	TR – TS04		
Tujuan Test	Mengetahui hasil tool importer		
Kondisi Awal	Data belum ter import		
Prosedur pengujian	Hasil yang diharapkan	Hasil yang diperoleh	Kesimpulan
<ul style="list-style-type: none"> Masuk ke server Radius Gunakan mysql client, ketik mysql -u user -p Masukkan query untuk mengecek data sudah masuk atau belum Query: Select * from radcheck where username like "040403%" 	Pada database radius table radcheck berisi data pengguna yang diambil menggunakan importer	Data masuk ke database Radius table radcheck	Tool importer berjalan sesuai dengan keinginan



Gambar 5. RedCheck

Test ID	TR – TS05		
Tujuan Test	Mengetahui apakah pengguna dapat terhubung Dengan system radius		
Kondisi Awal	Pengguna radius kosong		
Prosedur pengujian	Hasil yang diharapkan	Hasil yang diperoleh	Kesimpulan
User radius kosong			
<ul style="list-style-type: none"> Masuk ke server Radius Menggunakan tool radiest Langkah: radiest pengguna password (ppost password) Radrec (040430)10016 null 127.0.0.1 1812 testing123 	Rad_recv menampilkan pesan Access-Accept	Rad_recv menampilkan pesan Access-Accept	Pengguna sudah dapat terhubung ke radius server
User tidak bisa terhubung			
<ul style="list-style-type: none"> Masuk ke server Radius Menggunakan tool radiest Langkah: radiest pengguna password (ppost password) Radrec (040430)10016 null 127.0.0.1 1812 testing123 	Rad_recv menampilkan pesan Access-Reject	Rad_recv menampilkan pesan Access-Reject	Pengguna sudah dapat terhubung ke radius server karena password yang dimasukkan salah

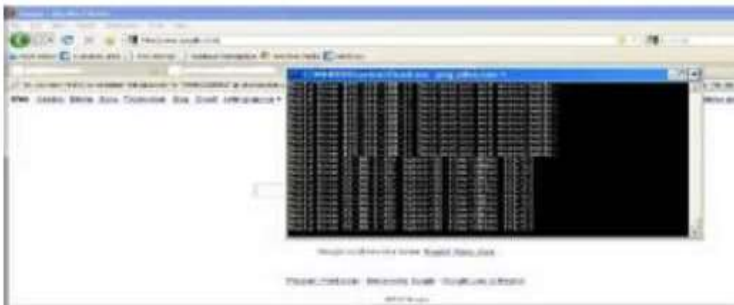
Gambar 6. Pengujian Pengguna

Test ID	TR – TS03		
Tujuan Test	Mengetahui fungsi user pada Mikrotik NAS		
Kondisi Awal	User tidak ada		
Prosedur pengujian	Hasil yang diharapkan	Hasil yang diperoleh	Kesimpulan
User disable pada Mikrotik			
<ul style="list-style-type: none"> • Login ke Mikrotik dengan winbox • Masuk menu ip hotspot user • Disable semua user yang ada 	User cepat melakukan login	User dapat melakukan login	Komunikasi Mikrotik NAS berjalan dengan normal
User Aktif pada Mikrotik NAS			
<ul style="list-style-type: none"> • Login ke Mikrotik dengan winbox • Masuk menu ip hotspot user • Perlihatkan user yang ada 	List pengguna muncul pada tab active	List pengguna muncul pada tab active	Komunikasi NAS berjalan normal sehingga pengguna dari radius server muncul pada <i>list active</i>

Gambar 7. Pengujian Mikrotik HotsPot User

Username	User Name	Domain	Address	Uptime	Idle Time	Session E.	Profile
panasul	2040030001		192.168.102.23	00:00:06	00:00:00		256 Kbps
panasul	2040030018		192.168.102.24	00:00:05	00:00:00		3 Kbps
panasul	2040030036		192.168.102.25	00:01:57	00:00:00		1320 Kbps
panasul	2040030053		192.168.102.27	00:02:00	00:00:04		3 Kbps
panasul	2040030070		192.168.102.28	00:12:28	00:00:02		3 Kbps

Gambar 8. User Aktif Pengguna Jaringan



Gambar 9. Uji Coba Login Sukses

IV. Kesimpulan

Berdasarkan pengujian dan implementasi system yang telah dilakukan, dapat disimpulkan bahwa dengan menggunakan RADIUS dengan software free RADIUS yang dihubungkan dengan Mikrotik sebagai network access server dapat digunakan untuk otentikasi pengguna pada jaringan. Dengan adanya otentikasi user ini diharapkan dapat meningkatkan keamanan jaringan komputer.

DAFTAR PUSTAKA

- Arifin, Zaenal. 2008. Sistem Pengamanan Jaringan Wireless LAN Berbasis Protokol 8.02.1x dan Sertifikat. Penerbit Andi. Yogyakarta.
- Febyatmoko, dkk. 2006. Otentikasi, Otorisasi & Pelaporan Koneksi User Wireless Chillispot dan Server RADIUS. <http://journal.uii.ac.id/index.php/mediainformatika/article/viewFile/122/83> (akses 20 januari 2010).
- Kelompok 123P IKI-83408T MTI UI. 2005. Keamanan Jaringan Komputer. http://bebas.vlsm.org/v06/Kuliah/MTIKeamananSistem-Informasi/2005/123/123P-03-final1.0-network_security.pdf (akses 20 januari 2010).
- Linto, Herlambang Moch., dan Catur L. Azis. 2008. Panduan Lengkap Menguasai Router Masa Depan Menggunakan Mikrotik RouterOSTM. Penerbit Andi. Yogyakarta.
- Rigney, et al. 2000. Remote Authentication Dial In User Service (RADIUS). <http://www.ietf.org/rfc/rfc2865.txt> (akses 19 januari 2010).
- Wagito. 2007. Jaringan Komputer Teori dan Implementasi Berbasis Linux. Gava Media. Yogyakarta.