IMPLEMENTASI KEAMANAN JARINGAN WIRELESS ENTERPRISE MENGGUNAKAN REMOTE AUTHENTICATION DIAL IN USER SERVICES

Nanang Sadikin[1)]

[1),] *Teknik Informatika Universitas Islam Attahiriyah Jakarta*
Email : nanang_sadikin@yahoo.com[1),]

Abstrak

Jaringan komputer wireless menawarkan kemudahan. Namun hal ini rentan terhadap ancaman serangan. Oleh karena itu jaringan wireless ini perlu diamankan. Di dalam makalah ini akan dijelaskan bagaimana mengamankan jaringan wireless menggunakan metode WPA2 Enterprise. Di dalam makalah ini WPA2 Enterprise implementasikan menggunakan Remote Authentication Dial-In User Services (RADIUS) yang merupakan fungsi Network Policy Server (NPS) yang terdapat pada Windows Server. Metode WPA2 Enterprise ini memiliki keunggulan dibandingkan metode keamanan WEP, WPA, atau WPA2 yang hanya mengandalkan security key.

Kata kunci:Wireless LAN, RADIUS, Network Policy Server, WEP, WPA, WPA2 .

1. Pendahuluan

Saat ini jaringan wireless semakin banyak digunakan di berbagai organisasi. Jaringan nirkabel memberikan berbagai keunggulan atas jaringan kabel. Keunggulana jaringan nirkabel antara lain adalah kemudahan bagi pengguna untuk berpindah dari satu tempat ke tempat lain. Selain itu jaringan nirkabel juga mudah dipasang karena tidak harus menarik kabel yang pemasangannya terkendala oleh berbagai rintangan. Keunggulan lainnya adalah jaringan nirkabel hemat biaya karena kita tidak membutuhkan banyak kabel. Karena berbagai keunggulan tersebut maka jaringan nirkabel berpotensi untuk menggantikan jaringan kabel secara luas.

Sebagai acuan ada beberapa penelitian yaitu dari Deris Stiawan yang berjudul ***Analisis Perbandingan Sistem Keamanan WEP/WPA/RADIUS Pada Jaringan Publik Wireless Hotspot***[3], penelitian dari Raymond Powers Tenggario yang berjudul ***Manajemen Jaringan Wireless Menggunakan Server Radius***[4], penelitian dari William Susanto yang berjudul ***Pengembangan Jaringan Lokal PT SVW Berbasis Teknologi Wireless LAN***[5], penelitian dari Firmansyah yang berjudul ***Membangun Komunikasi Data dengan Wireless Lan di RSUDR Syamsudin SH Kota Sukabumi***[6], penelitian dari Abdullah Faqih yang berjudul ***Sistem Manajemen Hotspot Berbasis Kuota Waktu dan Paket Data***[7], penelitian dari Aji Supriyanto yang berjudul ***Analisis Kelemahan Keamanan pada Jaringan Wireless***[8], penelitian dari Christina Megawati yang berjudul ***Implementasi dan Analisa Unjuk Kerja Sistem Keamanan Jaringan Wireless Berbasis Linux Platform dan DD-WRT Firmware***[9], penelitian dari Wildan Angga Yogantara yang berjudul ***Perancangan Jaringan Wireless Local Area Network Pada Dinas Pemerintah Kota Semarang***[10], dan penelitian dari Ahmad yang berjudul ***Membangun Jaringan Wireless pada SMA Negeri 1 Woja***[11] yang digunakan untuk membuat paper ini.

Di dalam paper ini Penulis akan memaparkan arsitektur jaringan wireless enterprise yang aman yang berbeda dengan rancangan jaringan wireless yang terdapat pada beberapa penelitian sebelumnya yang disebutkan di atas.

Wireless pada dasarnya terdiri atas dua kata, yaitu wire yang artinya kawat dan less yang bermakna tiada, tidak ada, tanpa. Jadi, jika diartikan wireless berarti tanpa kabel atau tidak menggunakan kabel. Secara lengkap jaringan wireless merupakan sebuah teknologi komunikasi yang tidak menggunakan kabel untuk menghubungkan antar perangkat, melainkan dengan menggunakan gelombang radio sebagai media yang digunakan.

Gelombang radio atau frekuensi radio adalah sarana transmisi umum yang digunakan pada jaringan wireless. Frekuensi radio menunjuk ke spektrum elektromagnetik dimana gelombang elektromagnetik dapat dihasilkan dari pemberian arus bolak-balik ke sebuah antena.

Gelombang ini dapat melintasi jarak yang jauh, menembus dinding. Karakteristik dari frekuensi radio sangat dipengaruhi oleh frekuensinya, seperti pada frekuensi tinggi, gelombang ini cenderung merambat pada garis lurus dan terpantul oleh permukaan objek. Sedangkan pada frekuensi rendah, gelombang ini cenderung dapat menembus dinding, namun jarak rambatnya jauh lebih pendek.

Gelombang ini dapat melintasi jarak yang jauh, dan menembus dinding. Karakteristik frekuensi radio sangat dipengaruhi oleh frekuensinya. Pada frekuensi tinggi gelombang ini cenderung merambat pada garis lurus dan terpantul oleh permukaan objek. Sedangkan frekuensi rendah, gelombang ini cenderung dapat menembus dinding, namun jarak rambatnya jauh lebih pendek. Frekuensi radio ini berada pada jangkauan frekuensi 10 Hertz (Hz) sampai dengan beberapa Giga Hertz (Ghz).

Jaringan Wireless bekerja pada frekeunsi yang sama dengan Bluetooth yaitu pada 2.4 Ghz. Bedanya, Bluetooth menggunakan Frequency Hopping Spread Spectrum (FHSS), sedangkan jaringan wireless yang disebut dengan Wifi menggunakan Direct Sequence Spread Spectrum (DSSS). Spread Spectrum adalah metode komunikasi dimana semua sinyal komunikasi disebar di seluruh spektrum frekuensi yang tersedia.

Standarisasi jaringan wireless dikeluarkan oleh IEEE (Institute of Electrical and Electronics Engineers). Saat ini terdapat empat spesifikasi jaringan wireless 802.11 yang umum dikenal. Tabel di bawah ini menunjukkan spesifikasi jaringan wireless tersebut.

Tabel 1. *Spesifikasi Jaringan Wireless*

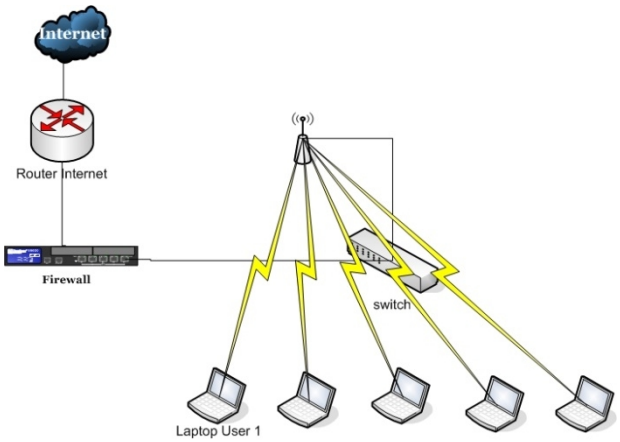
Spesifikasi	Rilis	Kecepatan max	Kecepatan actual	Frekuensi	Jarak (indoor)	Outdoor	coco k	Modulasi	MIMO
802.11a	September 1999	54	23	5	35	120	a	OFDM	1
802.11b	September 1999	11	4,3	2.4	35	140	b	DSSS	1
802.11g	Juni 2003	54	19	2,4	38	140	b,g	OFDM, DSSS	1
802.11n	Oktober 2009	150	74	2,4 dan 5	70	250	b,g,n	OFDM	4

Topologi pada jaringan wireless terbagi dua yaitu AdHoc dan Infrastruktur. Dalam topologi AdHoc komputer yang terhubung melalui wireless tidak menggunakan perantara atau peer to peer. Topologi ini dikenal dengan nama Independent Basic Service Sets (IBSS). Dalam topologi Infrastruktur, komputer yang terhubung dengan jaringan wireless menggunakan perantara yang disebut dengan Access Point atau Wireless Access Point. Topologi infrastruktur dikenal dengan nama Basic Service Sets (BSS).

SSID (Service Set Identifier) merupakan ID atau nama untuk jaringan wireless. Nama ini dapat diatur sesuai dengan keinginan administrator. SSID in bersifat case sensitive dan tidak boleh lebih dari 32 karakter. Secara default SSID akan di broadcast, sehingga akan membuat orang lain bisa menemukan jaringan

2. Pembahasan

Dari beberapa penelitian sebelumnya, sistem jaringan wireless yang diimplementasikan dapat dilihat pada gambar 1 di bawah ini:

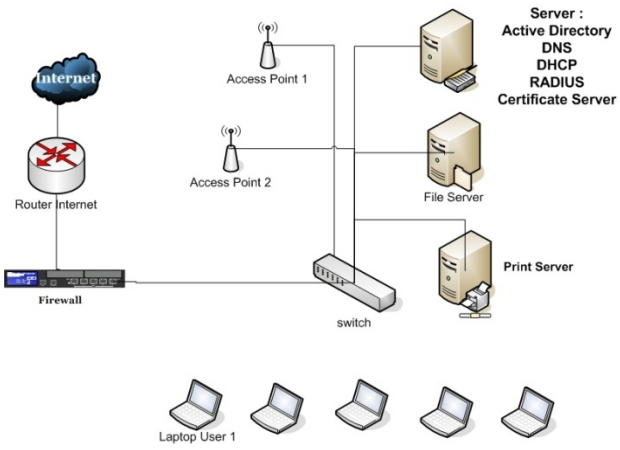


Gambar 1. *Skema jaringan wireless biasa*

Pada gambar di atas ditunjukkan skema jaringan wireless yang membentuk sebuah jaringan LAN. Jika jumlah komputer yang tergabung dalam jaringan LAN tersebut tidak terlalu banyak, konfigurasi jaringan LAN tersebut tidak bermasalah. Namun jika jumlah komputer yang tergabung dalam jaringan wireless LAN tersebut mencapai angka ratusan, maka hal tersebut akan menyulitkan.

1. Untuk bisa terhubung ke jaringan setiap wireless client harus memasukkan key
2. Jika key diganti pada access point maka semua key di semua laptop juga harus diganti
3. Semakin banyak jumlah laptop yang bergabung dengan jaringan wireless akan menyulitkan pergantian key.

Di dalam paper ini Penulis mengusulkan rancangan skema jaringan wireless enterprise untuk memperbaiki rancangan jaringan wireless biasa sebelumnya.
Rancangan jaringan wireless enterprise tersebut dapat dilihat pada gambar 2 di bawah ini:



Gambar 2. *Skema Jaringan Wireless Enterprise*

Pada gambar 2 di atas ditunjukkan beberapa komponen yang menjadi bagian dari jaringan wireless enterprise.

Pada gambar dua di atas ditunjukkan beberapa buah server yang menjadi bagian jaringan wireless enterprise.

Server yang pertama kali kita install adalah server yang memiliki fungsi sebagai server Active Directory, DHCP Server, DNS, RADIUS, dan Certificate Server.

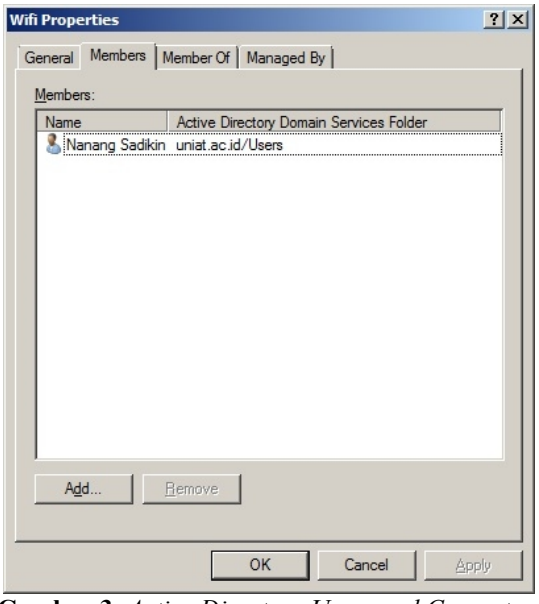
Server Active Directory merupakan server yang memiliki fungsi paling penting di jaringan. Server Active Directory ini disebut juga domain controller atau pengendali domain. Server ini merupakan server yang fungsinya pertama kali harus ada di jaringan, sebelum server yang lain dipasang. Setelah server Active Directory dipasang, baru fungsi yang lain diaktifkan pada server tersebut.

Sebelum server Active Directory dipasang maka ada beberapa hal yang harus dilakukan terlebih dahulu. Hal yang pertama kali harus dilakukan adalah memberikan IP Address untuk server tersebut. IP Address yang akan dipasang umumnya IP Address kelas C, karena jaringan kita jumlah komputernya paling banyak sekitar 200 komputer. Selain IP Address untuk Active Directory, kita juga harus memberikan IP Address untuk semua perangkat yang terhubung ke jaringan.Tabel di bawah ini menunjukkan pembagian IP Address.

Tabel 1. *IP Address*

No	IP Address	Fungsi
1	192.168.0.2	Server Active Directory
2	192.168.0.254	Access Point
3	192.168.0.3	Server File Sharing
4	192.168.0.4	Server Print Sharing
5	192.168.0.21-200	Client Access Point

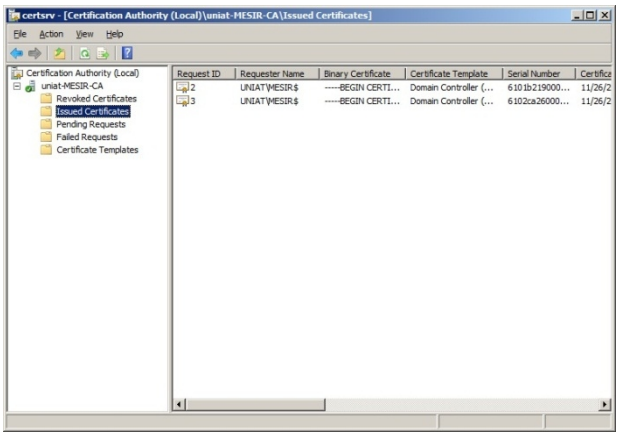
Setelah melakukan pembagian IP Address langkah selanjutnya adalah kita melakukan instalasi Active Directory. Sebelum melakukan instalasi Active Directory kita harus menentukan terlebih dahulu nama domain yang akan kita gunakan. Misalnya domain yang akan kita gunakan adalah uniat.ac.id. setelah itu kita bisa mulai melakukan instalasi Active Directory dengan menggunakan server manager.



Gambar 3. *Active Directory Users and Computers*

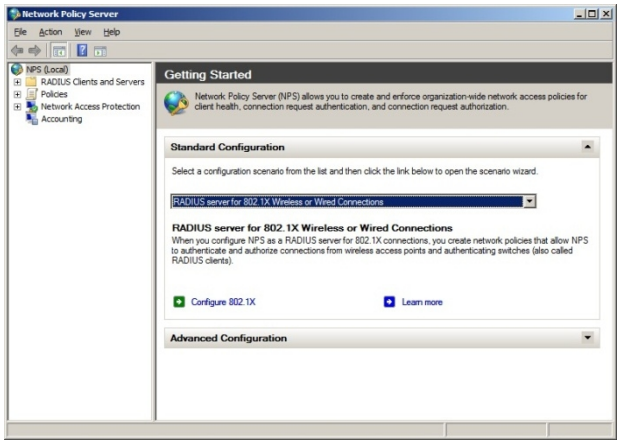
Setelah melakukan instalasi Active Directory, langkah selanjutnya adalah kita mengkonfigurasikan user dan group yang akan digunakan untuk melakukan otentikasi. Untuk mengkonfigurasikan user dan group kita bisa menggunakan console Active Directory Users and Computers. Di sana kita memasukkan parameter yang diperlukan untuk membuat user yaitu antara lain nama login atau account name, nama lengkap, dan password yang digunakan oleh user tersebut untuk login. Setelah selesai membuat user langkah selanjutnya adalah membuat group. Untuk membuat group langkahnya sama dengan membuat user yaitu menggunakan Active Directory users and computers. Parameter yang perlu diisi saat membuat group adalah nama groupnya. Setelah group terbentuk, langkah selanjutnya adalah menambahkan user tadi ke dalam group tersebut. Selanjutnya kita menggabungkan komputer client ke dalam domain dan menggunakan user tersebut untuk login.

Setelah melakukan instalasi active directory beserta mengkonfigurasi user dan group, langkah selanjutnya adalah melakukan instalasi certificate services. Certificate services merupakan service yang akan mengeluarkan sertifikat untuk server dan client. Dengan cara ini maka client bisa memverifikasi server sebelum melakukan proses otentikasi. Sama seperti fungsi lainnya pada Windows Server, certificate services ini merupakan sebuah roles yang kita install melalui server manager. Saat melakukan instalasi certificate services ada beberapa pilihan yang harus dipilih yaitu tipe certificate services yang dipilih adalah Enterprise karena menggunakan Active Directory, membuat certificate yang baru, nama certification authority serta masa berlakunya.



Gambar 4. *Certificate Services*

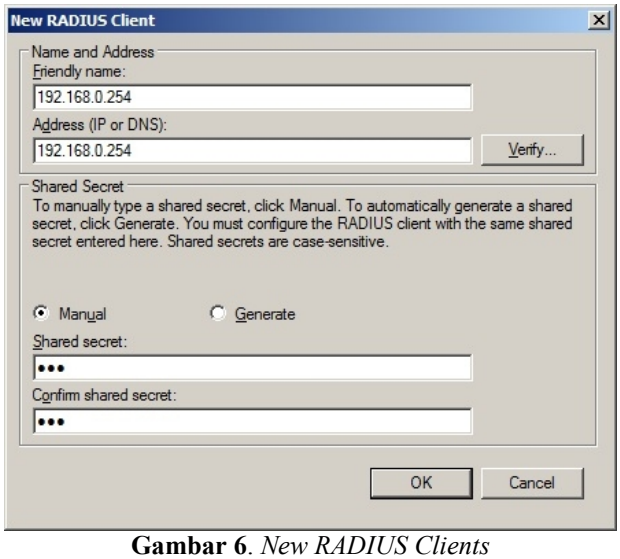
Langkah selanjutnya adalah kita melakukan instalasi network policy server. Network Policy Server merupakan salah fungsi yang terdapat pada Windows Server. Network Policy Server diinstall menggunakan roles yang terdapat pada Server Manager. Setelah sukses maka kita bisa membuka console Network Policy Server yang terdapat pada start Menu.



Gambar 5. *Network Policy Server*

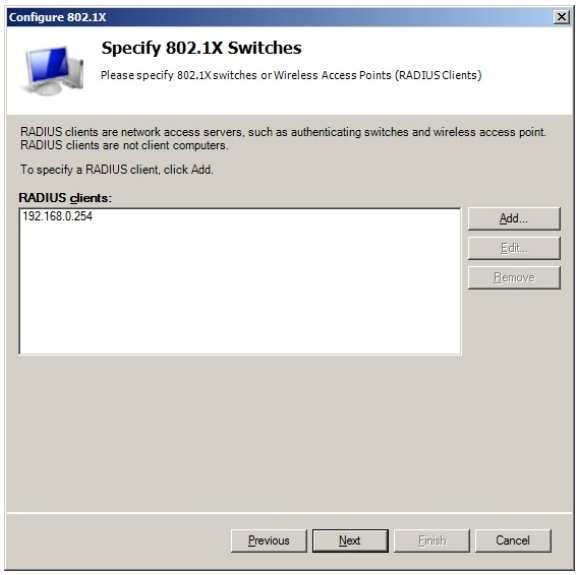
Langkah selanjutnya adalah kita melakukan konfigurasi terhadap Network Policy Server. Disini akan melakukan registrasi Network Policy Server pada Active Directory. Tujuan registrasi ini adalah agar Network Policy Server (NPS) bisa membaca konfigurasi Active Directory seperti nama login dan group yang akan digunakan untuk otentikasi wireless.

Langkah selanjutnya adalah kita mengkonfigurasi setting 802.1x yang terdapat pada Network Policy Server untuk melakukan otentikasi terhadap client yang akan menggunakan koneksi wireless. Disini kita juga akan menambahkan RADIUS Client. RADIUS Client adalah IP Address dari Access Point.



Gambar 6. *New RADIUS Clients*

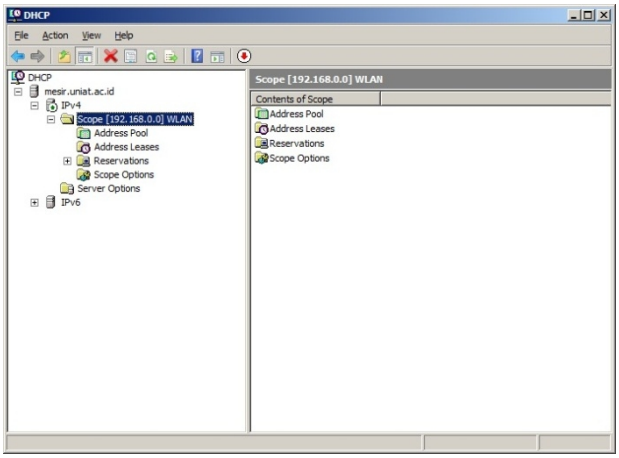
Shared secret adalah password yang diperlukan oleh Access Point (AP) untuk mengakses RADIUS Server. Masukkan password yang sama pada kolom Shared secret dan Confirm shared Secret. Password yang sama juga dimasukkan pada Access point.



Gambar 7. *Configure 802.1X*

Selain itu setting yang juga dimasukkan adalah group yang bisa mengakses menggunakan jaringan wireless LAN yang tadi sudah dibuat menggunakan Active Directory Users and Computers.

Langkah selanjutnya adalah kita melakukan instalasi dan konfigurasi DHCP Server. DHCP Server merupakan salah satu fungsi yang terdapat pada Windows Server. DHCP Server diinstall menggunakan Roles yang terdapat pada Server manager.



Gambar 8. *DHCP Server*

Setelah itu kita akan mengkonfigurasikan Scope di DHCP Server. Scope merupakan kumpulan IP Address yang nantinya akan digunakan oleh client yang menggunakan wireless.

Langkah terakhir adalah kita mengkonfigurasikan Access Point dan computer client. Pada Access point kita memberikan nama jaringan wireless tersebut pada setting SSID. Selanjutnya kita memilih metode keamanan WPA2 Enterprise, sehingga nanti akan muncul setting untuk RADIUS Server. Masukkan IP Address RADIUS server beserta Shared secret key yang sama seperti pada langkah

sebelumnya yaitu saat melakukan setting RADIUS Server.

Langkah terakhir adalah mengkonfigurasikan komputer client dengan memasukkan certificate yang sudah dibuat di server, membuat profile jaringan wireless dan login menggunakan nama pemakai yang sudah didaftarkan pada Active Directory. User selain dari pemakai active Directory dan pemakai yang tergabung dalam group Wifi tidak akan bisa terhubung menggunakan jaringan wireless. Dengan cara ini maka, jaringan wireless akan lebih aman, karena tidak ada security key yang digunakan bersama seperti pada metode WEP, WPA, dan WPA2.

3. Kesimpulan dan Saran

Dari pembahasan di atas dapat disimpulkan hal-hal sebagai berikut:

1. Jaringan yang menggunakan wireless lebih baik diterapkan jika pegawai yang bekerja di perusahaan memiliki mobilitas yang tinggi
2. Jaringan wireless dengan model WPA2 enterprise akan meningkatkan keamanan jaringan karena tidak menggunakan security key seperti yang digunakan pada jaringan wireless dengan metode keamanan WEP.

Adapun saran dari hasil penelitian ini sebagai berikut:

1. Penelitian ini belum menguji perbandingan kecepatan antara jaringan wireless dengan jaringan biasa yang menggunakan kabel.
2. Perlu dilakukan penelitian lebih lanjut jika menggunakan beberapa access point agar jaringan lebih handal

Daftar Pustaka

[1] Efvy Zamidra Zam, *Cara Mudah Membuat Jaringan Wireless,* Jakarta: Elex Media Komputindo, 2014
[2] Sto, *Wireless Kung Fu Networking & Hacking*, Jakarta: Jasakom, 2007.
[3] Deris Setiawan, *Analisis Perbandingan Sistem Keamanan WEP/WPA/RADIUS Pada Jaringan Publik Wireless Hotspot,* Palembang: Universitas Sriwijaya, 2009.
[4] Raymond Powers Tenggario, *Manajemen Jaringan Wireless Menggunakan Server Radius*, Jakarta: Universitas Bina Nusantara, 2011.
[5] William Susanto, *Pengembangan Jaringan Lokal PT SVW Berbasis Teknologi Wireless LAN*, Jakarta: Universitas Bina Nusantara, 2005.
[6] Firmansyah, *Membangun Komunikasi Data dengan Wireless LAN di RSUDR Syamsudin SH Kota Sukabumi*, Sukabumi: SMK Teknologi Plus Padjajaran, 2007.
[7] Abdullah Faqih, *Sistem Manajemen Hotspot Berbasis Kuota Waktu dan Paket Data*, Semarang: Universitas Diponegoro, 2012.
[8] Aji Supriyanto, *Analisis Kelemahan Keamanan pada Jaringan Wireless,* Semarang: Universitas Stikubank, 2006.
[9] Christina Megawati, *Implementasi dan Analisa Unjuk Kerja Sistem Keamanan Jaringan Wireless Berbasis Linux Platform dan DD-WRT Firmware*, Depok : Universitas Indonesia, 2012
[10] Wildan Angga Yogantara, *Perancangan Jaringan Wireless Local Area Network Pada Dinas Pemerintah Kota Semarang*, Semarang: Universitas Dian Nuswantoro, 2014.
[11] Ahmad, *Membangun Jaringan Wireless pada SMA Negeri 1 Woja*, Mataram: Akademi Manajemen Informatika Komputer, 2013.

Biodata Penulis

Nanang Sadikin, memperoleh gelar Sarjana Teknik (ST), Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Gunadarma, lulus tahun 2000. Memperoleh Gelar Magister Teknologi Informasi (MTI) Program Pasca Sarjana Fakultas Ilmu Komputer Universitas Indonesia, lulus tahun 2013. Saat ini menjadi dosen di Jurusan Teknik Informatika Fakultas Teknik Universitas Islam Attahiriyah Jakarta

ISSN : 2302-3805