PERANCANGAN JARINGAN HOTSPOT BERBASIS RADIUS SERVER *UNTUK MANAJEMEN PENGGUNAAN INTERNET* DI SMK NEGERI 3 PEKALONGAN

Arief Agung Gumelar[1)]

[1)] *Teknik Informatika STMIK AMIKOM Yogyakarta*
Jl Ring road Utara, Condongcatur, Sleman, Yogyakarta 55281
Email : mail@ariefagung.com[1)]

Abstrak

Keamanan sangat penting dalam suatu jaringan. Oleh karena itu, sistem wireless hotspot yang dirancang kali ini menggunakan radius server dengan metode EAP authentication untuk autorisasi dan autentikasi dalam suatu jaringan dan pembatasan pemakaian tiap user. Perancangan aplikasi ini juga dilengkapi dengan manajemen pengguna hotspot, biling, pembuatan voucher dan pembatasan pemakaian waktu/kuota per user.

Penelitian ini bertujuan untuk mengimplementasikan sistem autentikasi pengguna hotspot wireless LAN berbasis RADIUS (802.1X) dengan pembatasan akses berdasarkan kuota waktu pemakaian dan kuota paket data. Hasil yang dicapai membantu mempermudah manajemen jaringan wireless hotspot. Dapat disimpulkan bahwa sistem manajemen hotspot ini dapat melakukan berbagai skema pembatasan akses, di antaranya pembatasan berdasarkan lama penggunaan waktu (time based) dan jumlah penggunaan paket data (volume based) dengan pembatasan bandwidth untuk tiap pengguna.

Kata kunci : *mikrotik, user manager, radius, hotspot.*

1. Pendahuluan

1.1. Latar Belakang

Salah satu perubahan utama dibidang telekomunikasi adalah penggunaan teknologi wireless. Teknologi wireless juga diterapkan pada jaringan komputer, yang lebih dikenal dengan Wireless Lokal Area Network *(WLAN)*. Kemudahan yang ditawarkan wireless LAN menjadi daya tarik tersendiri bagi para pengguna komputer yang menggunakan teknologi ini untuk mengakses suatu jaringan komputer atau internet. Hal ini dibarengi pula dengan harga sebuah laptop yang dilengkapi teknologi wifi sudah sangat terjangkau, sehingga ada kecenderungan orang untuk memilih laptop dari pada PC Desktop[2].

Beberapa tahun terakhir ini pengguna wireless LAN mengalami peningkatan yang pesat. Peningkatan pengguna ini juga dibarengi dengan peningkatan jumlah hotspot yang dipasang oleh ISP (*Internet Service Provider*) di tempat-tempat umum, seperti kafe, mal, bandara dll. Teknologi Wireless LAN memang cocok untuk membangun jaringan komputer secara temporal (*Ad-hoc*), yaitu infrastruktur yang mudah dibangun dan dibongkar sehingga sangat cocok untuk tempat-tempat umum, sekolah, kampus dan lainnya.

1.2. Permasalahan

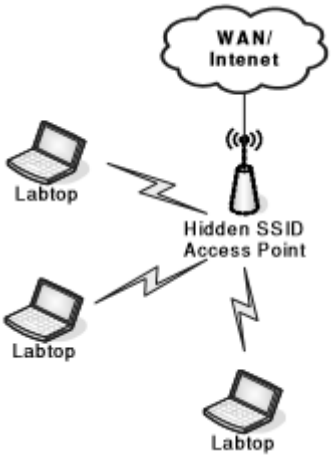
Banyak pihak yang masih mempertanyakan tentang keamanan *WLAN*, maka kita juga harus memikirkan sistem keamanan apa yang akan diterapkan. Banyak hotspot yang tidak menerapkan sistem keamanan yang memadai, sehingga memungkinkan pengguna yang tidak berhak (ilegal) dapat masuk ke jaringan komputer tersebut. Apabila hal ini sampai terjadi, maka pemilik hotspot tersebut secara langsung maupun tidak langsung akan dirugikan, penyusup itu dapat saja melakukan perbuatan yang tidak menyenangkan, seperti mengambil data, menyerang komputer yang ada pada jaringan tersebut, kehilangan pendapatan (apabila pemilik hotspot adalah *ISP*) dll.

Memang tidak mudah untuk memanajemen user dalam jaringan hotspot. Semakin banyak user dan semakin luas jangkauan wilayah dari jaringan wireless, maka diperlukan penerapan manajemen keamanan jaringan yang semakin bagus.

1.3. Pemecahan

Banyak paper yang mencoba membahas mengenai bagaimana memanajemen user dan mengamankan jaringan hotspot. Diantaranya teknologi itu adalah :

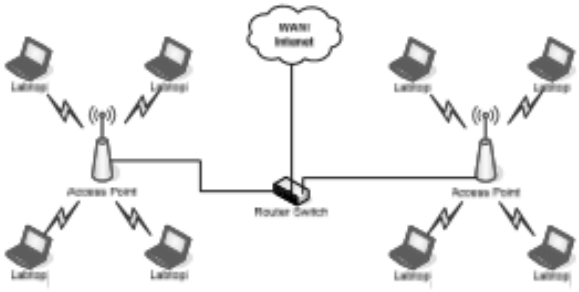
- **SSID (Service Set ID)** dilakukan dengan menyembunyikan *SSID* namun kenyataannya cara ini tidak efektif sebab client akan tetap mengirimkan *SSID* dalam bentuk plain text (meskipun menggunakan enkripsi). Beberapa tools yang dapat digunakan untuk mendapatkan *SSID* yang dihidden antara lain, *kismet (kisMAC), ssid_jack (airjack), aircrack, void 1.1* dan lainnya[1].



Gambar 1. *Bagan Hidden SSID Access Point*

• **WEP (Wired Equivalent Privacy)** metode ini adalah sistem keamanan dan enkripsi pertama yang digunakan pada wirelees, namun kelemahannya Karena enkripsi algoritma *RC4* mempunyai kunci yang lemah yaitu kunci *WEP* bersifat statis. Beberapa bentuk serangan yang dilakukan misalnya *FMS Attack* (*Fluhrer, Martin dan Shamir*), atau dengan *Traffict Injection*. *WEP* juga menggunakan satu kunci enkripsi yang digunakan bersama-sama oleh para pengguna WLAN. Hal ini menyebabkan *WEP* tidak dapat diterapkan pada hotspot yang dipasang ditempat-tempat umum[1].

• **Mac Filtering** adalah sistem keamanan bawaan yang sudah melekat pada perangkat wireless Access Point maupun Router. Hal ini sebenarnya tidak banyak membantu mengamankan komunikasi wireless, Karena MAC address sangat mudah *dispoofing* atau bahkan diubah. Tools yang biasa digunakan network utilities, regedit, smac, machange[1].



Gambar 2. *Bagan Wifi Dengan Mac Filter*

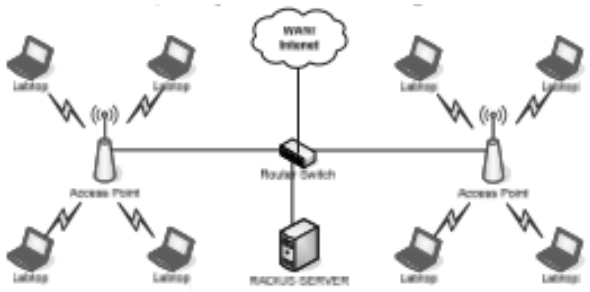
• **DHCP Server** hanya mengindentifikasi MAC Address kemudian memberikan IP ke klien. Tidak ada proses autentikasi selama proses permintaan IP namun punya kelebihan yaitu effective cost penggunaan resource network[5].

• **PPPoe dan PPTP**, biasanya digunakan untuk proses autentikasi untuk jaringan ATM, Membutuhkan client resource seperti software client sehingga kostumer masih perlu intervensi[5].

• **Proxy Server,** teknologi sudah mendukung multi user dan roaming (perpindahan user) dalam jaringan, namun autentikasi yang diberikan hanya ketika user mau akses ke jaringan luar/internet. Sedangkan jika pengguna hanya ingin membuat koneksi dijaringan lokal/internet, maka autentikasi ini tidak akan muncul[5].

Gambar 3. *Bagan Wifi dengan Proxy*

• **RADIUS (Remote Authentication Dial In User Service)**, teknologi sudah mendukung banyak pengguna (multiuser) dan perpindahan user (roaming) dalam jaringan, baik untuk koneksi jaringan intranet maupun internet.



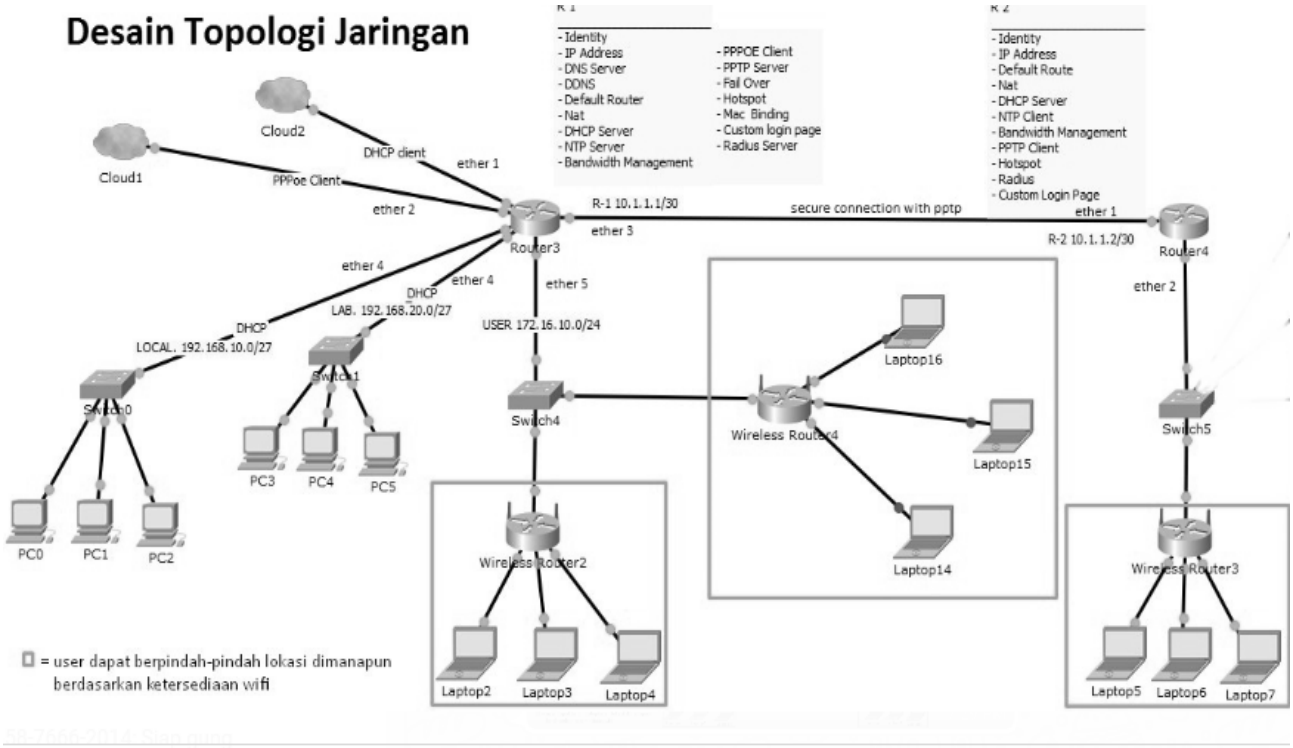
Gambar 4. *Bagan Wifi dengan RADIUS*

2. Pembahasan

2.1. Protokol Radius

Remote Authentication Dial In User Service (*RADIUS*), adalah protokol yang dikembangkan untuk proses AAA (authentication, authorization and accounting). Protokol *AAA* ini sendiri adalah sebuah model akses jaringan yang memisahkan tiga macam fungsi kontrol, yaitu Authentication, Authorization dan Accounting, untuk diproses secara independen[2].

Pada dasarnya terdapat tiga komponen yang membentuk model ini yaitu Remote User, Network Access Server (*NAS*) dan *AAA* server. Proses yang terjadi dalam sistem ini adalah user meminta hak akses ke suatu jaringan (internet atau WLAN misalnya) kepada Network Access Server. Network Access Server kemudian mengindentifikasi user tersebut melalui *AAA server*. Jika server *AAA* mengenali user tersebut, maka server *AAA* akan memberikan informasi kepada *NAS* bahwa user tersebut berhak menggunakan jaringan, dan layanan apa saja yang dapat diakses olehnya.



Gambar 4. *Desain Topologi Jaringan*

Selanjutnya, dilakukan pencatatan atas beberapa informasi penting mengenai aktivitas user tersebut, seperti layanan apa saja yang digunakan, berapa besar data (dalam ukuran bytes) yang diakses oleh user, berapa lama user menggunakan jaringan, dan sebagainya.

2.2. Desain Topologi Jaringan

Dalam Gambar 4. Terlihat detail topologi untuk desain jaringan yang nantinya akan diterapkan pada implementasi perancangan jaringan hotspot di Smk 3 Pekalongan. Penerapan radius yang akan digunakan pada desain jaringan diatas menggunakan *2 buah router, 3 buah access point, 2 buah switch, 6 buah PC client dan 9 buah laptop*. Pada router 1 terdapat 2 line internet dengan kecepatan line 1 100mbps dan line 2 200 mbps sehingga total dari akumulasi bandwith yang akan didistribusikan pada jaringan sebesar 300 mbps, nantinya akan ada pembagian jalur antara kebutuhan lokal seperti (kantor, lab, perpustakaan, ruang tata usaha) menggunakan line 1, sedangkan untuk line 2 didistribusikan untuk kebutuhan jaringan hotspot. Dalam router otentifikasi yang digunakan untuk terhubung ke jaringan internet menggunakan fasilitas dhcp client dan salah satu protokol tunneling yang sering digunakan yaitu, pppoe clientdiantara ke-2 router tersebut di hubungkan dengan media wireless karena letaknya yang tidak memungkinkan di jangkau dengan dilakukan instalasi media kabel sehingga perlu perangkat tambahan yang digunakan untuk mengkoneksikan antara ke-2 router, metode pengamanan yang digunakan dalam kasus ini selain menggunakan tipe authentikasi *WP2/PSK dengan enkripsi AES* juga menggunakan salah satu fitur tunneling dari router mikrotik yaitu *PPTP*. Fitur ini mampu untuk membuat pengenkripsian dalam pengiriman data sehingga baik data yang keluar maupun yang masuk ke dalam router sudah dalam bentuk terenkripsi sehingga dalam kasus ini terjadi 2 kali pengenkripsian data.

Fitur *PPTP* yang ada pada router mikrotik merupakan salah satu service yang sering digunakan untuk membangun jaringan *VPN* atau jaringan pribadi dengan menggunakan jaringan publik sebagai media penghubungnya sehingga nantinya seolah-olah walaupun berada pada beda network namun seperti terhubung pada jaringan lokal, analoginya adalah seperti membuat jaringan pipa yang ada di dalam pipa yang mana pipa terluar adalah jaringan publik (internet) dan pipa terdalam adalah jaringan lokal yang telah kita bangun sehingga dengan penerapan seperti ini mamapu untuk mengantisipasi jaringan yang dibangun dari serangan penyadapan karena dalam proses tunneling terdapat proses transmisi, enkapsulasi dan dekapsulasi paket data yang dikomunikasikan dengan demikian penerapan fitur ini cocok di aplikasikan diantara 2 router diatas.

2.3. Implementasi

Dari desain permodelan jaringan yang ada pada topologi diatas memanfaatkan 2 buah jalur koneksi untuk terhubung ke jaringan internet, masing-masing jalur memiliki kecepatan baik download maupun upload yang berbeda sehingga nantinya router akan dikonfigurasikan untuk dapat menentukan pembagian jalur berdasarkan pembagian yang telah ditentukan oleh administrator, sehingga sebelum penentuan pembagian jalur di buat sebelumnya telah dilakukan perhitungan dari banyaknya jumlah user yang akan menggunakan termasuk didalamnya bukan hanya jumlah user yang

menggunakan jaringan hotspot namun juga jumlah pemakaiaan bandwidth yang dibutuhkan untuk menunjang pembelajaran disekolah seperti; ruang lab, ruang kantor, perpustakaan dan lainnya sehingga dari akumulasi tersebut dapat dilakukan perhitungan untuk penentuan jalur yang cocok apakah semua user hotspot akan dialihkan ke jalur internet 1 sedangkan aktifitas penunjang pembelajaran dialihkan untuk menggunakan jalur internet 2 ataupun sebaliknya, dengan demikian akan tercapai pembagian bandwidth yang simetris berdasarkan kebutuhan yang harus dipenuhi, nantinya ketika semua pengguna aktif secara bersamaan maka setiap user akan tetap dapat terhubung ke jaringan internet dengan mendapatkan kecepatan minimal yang telah di tentukan oleh administrator berdasarkan akumulasi perhitungan diatas dan apabila kondisi pengguna jaringan sekolah tidak terlalu padat maka setiap user akan dapat mencapai batas kecepatan maksimalnya, selain itu dari kedua jalur internet yang digunakan memiliki fitur auto backup link, dimana jalur internet pertama terputus akan digantikan oleh jalur internet kedua dan begitu pula sebaliknya, fasilitas yang digunakan untuk menentukan terhubung dan tidaknya jalur internet 1 ataupun 2 adalah menggunakan parameter ping yang ada pada fitur router mikrotik, melalui fitur ini router akan mempunyai sebuah algoritma sederhana yakni jika jalur 1 dilakukan ping tidak menjawab selama sekian detik maka jalur 1 akan dianggap mati dan router akan secara otomatis mengalihkan semua trafik internet melalui jalur 2, namun ketika kedua jalur internet berjalan normal masing-masing link memiliki jalur untuk menangani trafik yang sudah dibagi berdasarkan routing yang sudah diterapkan pada router.

Parameter yang menjadi patokan dalam penentuan jalur *back up link* selain menggunakan fasilitas ping adalah menggunakan *distance*, semakin kecil *distance* yang di terapkan maka *distance* tersebut yang akan di jadikan prioritas utama dalam penentuan jalur routing, selain itu beberapa parameter lain yang digunakan selain distance adalah firewall yang berfungsi untuk menandai paket data yang keluar masuk dari jalur lokal menuju internet ataupun sebaliknya dari internet menuju jaringan lokal sehingga dengan penandaan ini akan bisa memisahkan antara trafik hotspot yang harusnya mengarah ke jalur internet 2 dan trafik pemakain pada ruang lab,perpustakaan dan kantor yang mengarah ke jalur internet satu.

Peran router 2 dalam topologi jaringan diatas berfungsi sebagai router distribusi ke client sehingga router harus mampu melakukan singkronisasi ke router utama, karena semua database user tersimpan pada router pertama, router ke-dua juga akan memudahkan dalam melakukan segmentasi jaringan bagi administrator yang menangani jaringan karena hal ini akan memudahkan dalam management pengelompokan terhadap pembagian IP Address, mencegah broadcast domain dan troubleshooting ketika terjadi masalah.

Bagi user dapat mengakses jaringan hotspot dimanapun selama berada didalam jangkauan (*coverage area*), karena sistem jaringan yang dibuat mampu melakukan sinkronisasi terhadap user, sejumlah akses point yang dipasang di sekeliling lokasi baik yang berada di bawah router 1 langsung maupun yang berada di bawah router distribusi telah di support dengan fitur wds layaknya jaringan seluler yang kita gunakan sekarang, artinya kemanapun user berpindah selama dalam lingkungan sekolah yang tercover jaringan hotspot bisa langsung terhubung tanpa melakukan pemindaain jaringan wifi baru yang tersedia, selain itu disetiap titik akses point yang dipasang dikonfigurasikan dengan *SSID* yang sama untuk lebih memudahkan user yang benar-benar awam dalam menggunakan jaringan hotspot. Setiap user nantinya akan mendapatkan 1 username dan password yang bersifat unik artinya mereka dapat menggunakan user tersebut untuk login ke jaringan hotspot baik melalui perangkat smartphone ataupun leptop namun hanya bisa digunakan untuk 1 device saja, sehingga ketika sudah ada 1 device yang terhubung melalui jaringan dengan username dan password tersebut device lain yang mencoba melakukan login dengan user yang sama akan secara otomatis di blok oleh router utama dengan demikian ini bisa menghemat pemakaian bandwidth yang ada serta bandwidth dapat di distribusikan secara tepat efektif.

Dalam implementasi ini penulis menggunakan sample sebanyak 2000 user yang nantinya dapat terhubung kejaringan hotspot dengan jumlah total bandwidth yang tersedia sebesar 200mbps yang akan di distribusikan ke jaringan oleh karena itu di butuhkan manejemen bandwidth yang bisa mengatur secara sama rata kepada 2000 user yang ada yang menggunakan, dalam kasus ini penulis menggunakan fitur menejemen bandwidth *queuetree* yang kombinasikan dengan *PCQ* melalui perhitungan sebagai berikut :

Jumlah user (x) = 2000 orang

Jumlah Bandwidth tersedia (y) = 200 mbps

A = 1 Mbps = 1024 Kbps

$$\Sigma QT = \frac{Y * A}{X} \quad \ldots\ldots (1)$$

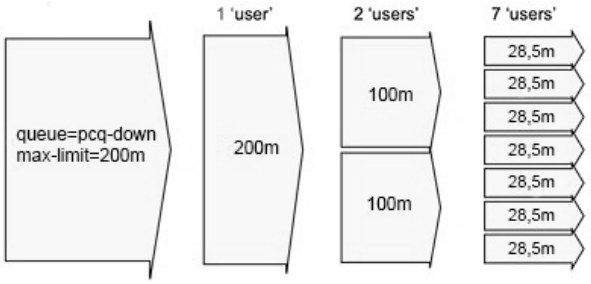
$$\Sigma QT = \frac{200 * 1024}{2000} = 102.4\ kbps$$

Gambar 5. *Perhitungan PCQ*

Gambar 5 merupakan hasil dari perhitungan PCQ dengan rumus pada persamaan 1 dapat kita simpulkan bahwa setiap user yang terkoneksi ke jaringan hotspot dengan alokasi total bandwidth yang tersedia sebesar 200mbps setidaknya user akan mendapat minimal 102.4 kbps ketika terhubung ke jaringan pada saat traffic jaringan padat sekalipun, namun ketika hanya beberapa user saja yang menggunakan maka setiap user dapat

mencapai batas pemakaian maksimalnya sebesar 512 kbps. Analogi ini memanfaatkan dari fitur *PCQ* yang bisa membagi jaringan secara sama rata ketika semua user aktif menggunakan namun ketika hanya beberapa user sistem mampu menyesuaikan ke batas maksimal kecepatan yang telah ditentukan.

Berikut ini adalah analogi penggunaan fitur *PCQ* yang diterapkan pada topologi diatas, fitur ini mampu melakukan pembagian bandwidth secara rata berdasarkan banyaknya jumlah user yang sedang menggunakan internet.



Gambar 6. *Cara Kerja PCQ*

Dari gambar diatas terlihat jelas bagaimana cara kerja *PCQ* dalam melakukan pembagian bandwidth kepada user yang sedang aktif menggunakan internet, ketika hanya 1 user yang aktif maka user tersebut dalam analogi diatas akan mendapatkan seluruh jumlah bandwidth yang tersedia, ketika ada 2 user yang aktif maka algoritma pcq akan langsung membagi jumlah bandwidth yang tersedia dibagi 2 seperti pada gambar diatas diaman tersedia bandwidth 200mbps akan otomatis di bagi menjadi 2 dengan masing-masing user mendapatkan alokasi bandwidth 100mbps.

3. Kesimpulan

Dari hasil penyajian data mengenai perancangan jaringan hotspot berbasis radius server di SMKN 3 Pekalongan dapat ditarik kesimpulan bahwa dengan menerapkan radius server pada jaringan hotspot dapat memudahkan management bandwidth maupun management user pada jaringan hostpot tersebut, serta dapat memudahkan administrator jaringan untuk melakukan segmentasi jaringan antar divisi pada lingkup area jaringan hotspot tersebut.

Karena dalam perancangan ini kami menggunakan 2 router yang dapat membagi antar lokal server dengan jaringan hotspot. *Lokal server* disini ditunjukan untuk segmentasi ruang guru, lab, ruang TU, ruang kepala sekolah, dan perpustakaan. Sedangkan untuk jaringan hotspot ditunjukkan untuk para siswa dengan menggunakan username dan password masing – masing.

Fitur *auto backup link* yang diterapkan pada perancangan jaringan hotspot diatas akan sangat bermanfaat karena sebuah algoritma sederhana yang diterapkan mampu mengenali keadaan jaringan baik dalam kondisi tersedia ataupun terputus sehingga dengan memanfaatkan fitur ini akan menjaga performa jaringan internet agar tetap terhubung.

Daftar Pustaka

[1] A.W. Setiawan. *Remote Authentication Dial In User Service (RADIUS) untuk Autentikasi Pengguna Wireless LAN*, Bandung : FTI-ITB, 2005.
[2] A. Yani. *Panduan Membangun Jaringan Komputer*, Jakarta : Kawan Pustaka, 2007
[3] R. Frinkel, R. Taylor, R. Bolles, and R. Paul. "An overview of AL, programming system for automation," in *Proc. Fourth Int. Join Conf Artif.Intel.*, pp. 758-765, Sept. 3-7, 2006.
[4] L. Phifer. Using RADIUS for WLAN Authentication, Part II (December 10,2003).

Biodata Penulis

Arief Agung Gumelar, merupakan mahasiswa aktif Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta, angkatan tahun 2014.

ISSN : 2302-3805