SISTEM MANAJEMEN USER LOGIN HOTSPOT MIKROTIK DENGAN RADIUS SERVER MENGGUNAKAN RASPBERRY PI

Erik Hendarto
Program Studi Teknik Informatika S1, Fakultas Teknologi Industri
Institut Teknologi Nasional Malang, Jalan Raya Karanglo km 2 Malang, Indonesia
erikhendarto96@gmail.com

ABSTRAK

Hotspot saat ini sudah sangat dikenal oleh banyak masyarakat umum, dari anak-anak hingga orang dewasa sering memakai layanan ini. Namun terkadang hotspot juga memiliki masalah seperti keamanan pada penerapan metode autentifikasi nya. Freeradius merupakan server Remote Authentication Dial-In User Service (RADIUS) yang menggunakan metode portal captive untuk mendapatkan akses hotspot .

Metode ini mengharuskan user yang tehubung ke jaringan hotspot tersebut untuk melakukan login, freeradius ini menggunakan protokol AAA (Authentication, Authorization, Accounting) melalui data yang sudah tersimpan pada database MySql. Pada rancangan penelitian ini dibuatlah manajemen user berbasis website yang dilakukan oleh admin dan server login hotspot yang tersedia pada mikrotik dengan menerapkan metode autentifikasi username dan password (portal captive).

Penelitian ini menjelaskan bahwa perangkat hotspot (mikrotik) sekedar cukup memberikan akses hotspot (SSID dan ip Address), sedangkan NAS (Network Attach Storage) dan login autentifikasi akan dilakukan oleh radius server (freeradius).

Kata kunci : *hotspot . Radius, freeradius, portal captive, MySql, mikrotik.*

1. PENDAHULUAN

Layanan *hotspot* tidak asing lagi di kehidupan sehari-hari. Layanan ini biasa di temukan pada rumah sakit, tempat makan, pusat hiburan, instansi pendidikan dan diberbagai tempat umum lainnya. Penyedia layanan *hotspot* ini banyak menggunakan *password* yang di akses bersama dan memakai enkripsi WEP, WPA ataupun menggunakan *portal captive* dalam segi autentifikasi yang digunakan penyedia *hotspot* . Sebagian besar instansi saat ini menggunakan layanan *hotspot* yang menggunakan *password* bersama yang dapat diakses oleh semua pengguna di instansi.

Bahkan bisa jadi orang dari luar instansi juga dapat menggunakan layanan *hotspot* dengan bebas, penelitian ini melakukan uji coba pada jaringan *hotspot* informatika, dan jaringan hanya di khususkan untuk mahasiswa informatika dengan menggunakan *server freeradius* pada *raspberry pi*.

Penelitian ini di desain dan di implementasikan untuk membuat proses autentifikasi *portal captive* yaitu pada layanan *hotspot* yang menggunakan autentifikasi *user*name dan *password*, *user* harus memiliki *user*name dan *password* terlebih dahulu yang telah dibuat oleh administrator. Administrator secara manual membuatkan *user*name dan *password* untuk setiap *user*, dan pengguna juga dapat melakukan pendaftaran sendiri yang di verifikasi oleh administrator. Penerapan sistem manajemen *user* dilengkapi fitur *create, reset, update, delete* (CRUD) pada layanan *hotspot* untuk administrator mengolah data pengguna *hotspot* , serta memungkinkan pengguna layanan *hotspot* melakukan pendaftaran secara mandiri. Dan aktifitas pelaporan pengguna (*log*) yang *login* juga akan dicatat dan ditampilkan dihalaman admin.

2. TINJAUAN PUSTAKA

2.1. Hotspot

Pengguna layanan *hotspot* dengan metode akses *user*name/*password* harus memiliki *user*name dan *password* yang telah terdaftar. Proses pembuatan *user*name dan *password* dilakukan oleh administrator atau pengelola *hotspot* . Untuk terkoneksi ke *access point hotspot* , pengguna perangkat keras tidak perlu melakukan autentifikasi. Saat pengguna perangkat melakukan permintaan alamat *web* di *browser*, secara otomatis *hotspot* akan menampilkan halaman autentifikasi dimana pengguna memasukkan *user*name dan *password*.[1]

2.2. Mikrotik

Mikrotik sebagai produsen perangkat jaringan komputer menghadirkan Mikrotik *Router* OS yang merupakan sistem operasi khusus untuk kebutuhan jaringan komputer. Mikrotik memiliki banyak fitur, salah satunya sebagai *port*al *captive* hotspot *gateway*, dengan fitur tersebut mikrotik dapat mengarahkan pengguna yang terhubung dengan jaringan *hotspot* ke alamat *login*. Mikrotik hadir dalam bentuk suatu kesatuan perangkat keras dan sistem operasi mikrotik *router* os.[1]

2.3. Radius

Radius (Radial *Authentication* Dial In *User* Service) merupakan *server* yang digunakan untuk autentifikasi *login* dimana didalamnya terdapat protokol AAA (*Authentication*, Authorized,

Accounting) yang dibuat dari bebepara protokol untuk memungkinkan administrator mengamankan dan memonitor jaringan.[2] Sistem apapun selalu butuh keamanan, akutansi dan administrasi pengguna dalam jaringan yang terhubung ke internet.[3] Layanan internet telah menciptakan permintaan yang kuat dalam mendapatkan ip *Address* dengan kemampuan jelajah yang tinggi.[4]

Radius adalah protokol autentifikasi akses *server* dan akutansi yang telah memperoleh dukungan luas. *Server* autentifikasi *radius* menjaga autentifikasi pengguna dan informasi akses jaringan. Klien akan berjalan ke akses *server* dan mengirim permintaan autentifikasi untuk *radius server*. Protokol AAA diproses secara independen. *Authentication* adalah proses *user* diidentifikasi oleh *server* sebelum *user* menggunakan jaringan, pada proses ini *user* meminta akses kepada NAS (*Network Access Server*) yang kemudian mengirimkan kepada AAA. Authorized adalah pengalokasian layanan apa aja yang berhak diakses oleh *user* dan *Accounting* merupakan proses mencatat aktivitas *user*.[2]

2.4. Freeradius

Freeradius adalah salah satu penyedia perangkat lunak *radius server* dengan jumlah yang sangat luas. *Freeradius* menonjolkan kecepatan dan modularitas. *Freeradius Server* daemon untuk sistem operasi Unix yang memungkinkan seseorang untuk membuat *server* protokol *radius*, yang biasanya digunakan untuk otentikasi dan akuntansi pengguna dial-up. *Freeradius* adalah produk open source, dan memiliki semua manfaat yang disediakan open source.

Perangkat lunak ini menangani Accounting Server Functionalities and Authenticators yang menggunakan jalur akses berbasis *hotspot* dalam penyiapan otentikasi IEEE 802.11i. *Freeradius* juga merupakan *server* yang kuat dan dapat dikonfigurasi sesuai administrator jaringan. Semua konfigurasi *freeradius server* tersimpan dalam direktori Linux /*etc*/*freeradius*, konfigurasi sedikit rumit dan dipecah menjadi beberapa file secara default.

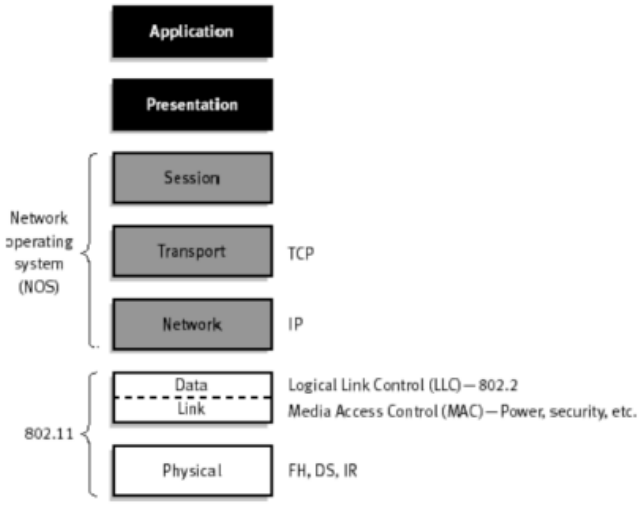
Server otentikasi dapat berfungsi baik sebagai *server* penerusan dan *server* jarak jauh, berfungsi sebagai *server* penerusan untuk beberapa wilayah dan *server* jarak jauh untuk wilayah lainnya. Satu *server* forwarding dapat bertindak sebagai forwarder untuk sejumlah *server* jarak jauh. *Server* jarak jauh dapat memiliki sejumlah *server* yang meneruskannya dan dapat memberikan otentikasi untuk sejumlah wilayah. Satu *server* penerusan dapat meneruskan ke *server* penerusan lain untuk membuat rangkaian proxy. Layanan pencarian diperlukan untuk menemukan *server* jarak jauh.[6]

2.5. Logger

Sistem memiliki kemampuan pengumpulan data informasi seputar waktu *user login* dan billing yang telah dilalui selama pemakaian. Proses dari pertama kali seorang mengakses sebuah sistem, apa saja yang dilakukan *user* di sistem tersebut dicatat dan didokumentasikan pada sebuah *database server*. Dengan demikian admin bisa memantau aktivitas *user* untuk menentukan kebijakan manajemen jaringan.[10]

2.6. WLAN

Wireless Local Area Network (WLAN) adalah sebuah jaringan komputer yang menggunakan media transmisi berupa gelombang radio. WLAN menggunakan spesifikasi versi 802.11 yang merupakan standrasisasi ditetapkan oleh IEEE (Institute of Electrical and Electronics Engineers). Penggunaan versi 802.11 memberikan kecepatan transfer data 1 Mbps dan 2Mbps yang berfokus pada OSI model level physical dan datalink layer.



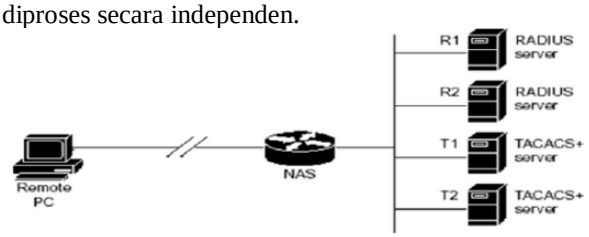
Gambar 1 802.11 IEEE OSI Model

WLAN memberikan kuntungan jika dibandingkan dengan *Local Area Network* (LAN). Keuntungan yang diberikan oleh WLAN adalah sebagai berikut:

1. Meningkatkan mobilitas komputer
2. Biaya instalasi yang lebih murah
3. Efektif diterapkan pada lingkungan yang dinamis. [7]

2.7. AAA

AAA (*Authentification*,*Authorization*,*Accounting*) adalah sebuah model akses jaringan yang memisahkan tiga macam fungsi kontrol, yaitu *Authentication*, *Authorization*, dan *Accounting*, untuk diproses secara independen.



Gambar 2 Proses AAA

Pada gambar 2 terlihat komponen-komponen yang terlibat dalam model AAA. 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 ialah *user* meminta hak akses ke suatu jaringan misalnya WLAN kepada *Network Access Server*. *Network Access Server* kemudian mengidentifikasi *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. Selanjutnya, dilakukan pencatatan atas beberapa informasi penting mengenai aktivitas *user* tersebut, seperti layanan apa saja yang digunakan, berapa besar data dalam ukuran byte yang diakses oleh *user*, berapa lama *user* menggunakan jaringan, dan sebagainya.

Authentication adalah suatu proses dimana *user* diidentifikasi oleh *server* AAA sebelum *user* menggunakan jaringan. Pada proses ini, *user* meminta hak akses kepada NAS untuk menggunakan suatu jaringan. NAS kemudian menanyakan kepada *server* AAA apakah *user* yang bersangkutan berhak untuk menggunakan jaringan atau tidak. *Authorization* adalah pengalokasian layanan apa saja yang berhak diakses oleh *user* pada jaringan. *Authorization* dilakukan ketika *user* telah dinyatakan berhak untuk menggunakan jaringan. *Accounting* merupakan proses yang dilakukan oleh NAS dan AAA *server* yang mencatat semua aktivitas *user* dalam jaringan, seperti kapan *user* mulai menggunakan jaringan, kapan *user* mengakhiri koneksinya dengan jaringan, berapa lama *user* menggunakan jaringan, berapa banyak data yang diakses *user* dari jaringan, dan lain sebagainya. Informasi yang diperoleh dari proses *accounting* disimpan pada AAA *server* dan dapat digunakan untuk berbagai keperluan seperti billing, auditing, atau manajemen jaringan.

Koneksi antara *user* dengan NAS dapat melalui jaringan telepon WLAN. Koneksi tersebut, seperti telah disebutkan di atas, menggunakan bermacam-macam jaringan akses dengan protokol komunikasi yang berbeda-beda, tergantung perangkat yang digunakan oleh *user* dan NAS. Koneksi antara NAS dengan *server* AAA menggunakan beberapa macam protokol yang terstandarisasi seperti *RADIUS*.[7]

2.8. Raspberry pi

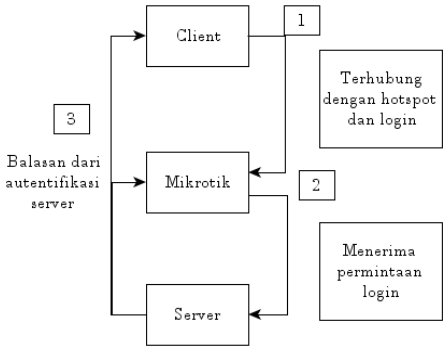
Raspberry pi adalah komputer mikro berukuran seperti kartu kredit yang dikembangkan oleh *Raspberry pi Foundation*, Inggris. Komputer *single board* ini dikembangkan dengan tujuan untuk mengajarkan dasar-dasar ilmu komputer dan pemrograman untuk siswa sekolah di seluruh dunia. Meskipun mikrokontroler yang memiliki fisik seperti Arduino dimana lebih dikenal untuk proyek-proyek *prototyping*, tidak demikian dengan *Raspberry pi* yang sangat berbeda dari mikrokontroler kebanyakan, dan sebenarnya, lebih seperti komputer daripada Arduino.

Raspberry pi terdiri dari banyak bagian perangkat keras yang penting dengan beberapa fungsi yang penting. Bagian utama dari *Raspberry pi* adalah processor nya. Setiap *Raspberry pi* memiliki BCM2835 Chip Broadcom yang mewujudkan suatu CPU inti ARM1176JZF-S. Chip ini memiliki clock speed 700MHz dan merupakan sistem 32-bit. *Raspberry pi* memiliki slot kartu SD untuk kartu SD yang bertindak sebagai media penyimpanan yang semuanya termasuk sistem operasi dan file lainnya disimpan dalam kartu SD. *Port* HDMI digunakan sebagai audio dan video output. Sebuah HDMI ke DVI (Digital Visual *Interface*) converter dapat digunakan untuk mengkonversi sinyal HDMI ke DVI yang biasanya digunakan oleh monitor. *Raspberry pi* mebutuhkan catu tegangan 5V DC melalui micro USB. Perangkat ini juga memiliki konektor video komposit RCA untuk output video serta jack stereo 3,5 mm untuk output audio. *Raspberry pi* memiliki 26 GPIO pin yang membantu untuk terhubung ke peripheral tingkat rendah dan expansion boards.[5]

3. METODE PENELITIAN

3.1. Diagram Blok Sistem

Diagram blok pernyataan sistem dalam bentuk gambar yang ringkas dari masukkan dan keluaran pada sistem *login*. Diagram blok sistem ditunjukkan pada Gambar 3.



Gambar 3 Diagram Blok Sistem

Merupakan gambaran umum sistem dimana *client* terhubung ke mikrotik untuk mendapatkan ip *Address* dan halaman *login*, dari halaman *login* mikrotik *server freeradius* menerima permintaan untuk diautentifikasi. *Reply* dari *server* akan diarahkan ke *client* dan mikrotik, *client* menerima *reply login* dan mikrotik untuk memberikan aturan-aturan yang sudah dikonfigurasi oleh admin kepada *client*. Berikut urutan proses pada sistem:

1. *Client* terhubung dengan *hotspot* yang berasal dari mikrotik.
2. Pada saat *client login* dengan *user* dan *password* mikrotik meneruskan permintaan melalui konfigurasi *radius* menggunakan IP *Address*.
3. *Server* akan menerima request *login*, melakukan autentifikasi dan memberikan *reply* autorisasi.

3.2. Topologi

Konsep yang menghubungkan beberapa perangkat jaringan untuk menjadi suatu jaringan yang saling terhubung pada sistem. Topologi jaringan ditunjukkan pada Gambar 4

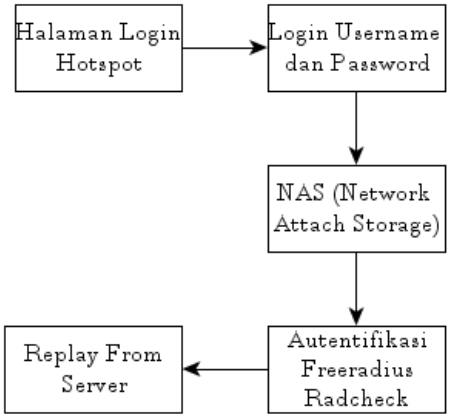
Gambar 4 Topologi Jaringan

Merupakan topologi jaringan dari sistem *login* menggunakan *hotspot* mikrotik dan *raspberry pi* sebagai *server freeradius*. *Ethernet* 2 digunakan sebagai sumber internet (opsional) karena untuk *login hotspot* saja tidak membutuhkan konek internet, *Ethernet* 5 merupakan koneksi antara mikrotik dan *freeradius* dengan ip *Address* satu jaringan, sedangkan untuk hotpot sendiri menggunakan *interface* WLAN yang merupakan koneksi untuk ke *user* atau *client*. Berikut keterangan *port* mikrotik yang digunakan:

1. *Ethernet* 2 = Sumber Internet
2. *Ethernet* 5 = *server freeradius*. IP *Address* 10.10.10.1/24
3. WLAN = *hotspot* . IP *Address* 192.168.20.1/24

3.3. Diagram Alur

Gambaran alur dari langkah-langkah atau proses saat *login hotspot* pada sistem. Diagram alur *login* ditunjukkan pada Gambar 5.

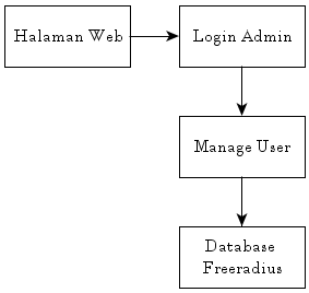


Gambar 5 Diagram Alur Login

Merupakan diagram alur dari sistem *login* dimana alur dimulai pada halaman *login* yang kemudian *user* memasukkan *user*name dan *password* yang telah diberikan admin. Data *login* tersebut akan masuk ke dalam *Network Attach Storage* (NAS) untuk pencocokan dan diautentifikasi oleh *server freeradius* sebelum diberi hak akses.

1. Membuka halaman *login* mikrotik
2. Input *user* dan *password*
3. Pencocokan data dengan NAS
4. Proses autentifikasi *freeradius*
5. *Reply* dari *freeradius*

Gambaran alur dari langkah-langkah atau proses manajemen *user* pada sistem Diagram alur manajemen *user* ditunjukkan pada Gambar 6

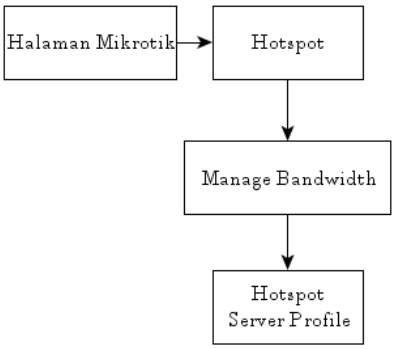


Gambar 6 Diagram Alur Manajemen User

Merupakan diagram alur untuk manajemen *user* pada sistem, setelah membuka halaman web admin akan diminta memasukkan *user*name dan *password* untuk *login*. Jika *login* berhasil akan diteruskan menuju halaman manajemen *user* dimana admin dapat memanajemen *user hotspot* yang kemudian data tersebut tersimpan pada *database freeradius*.

1. Membuka halaman *web* dan *login*.
2. Melakukan manajemen pada *user*.
3. Hasil manajemen *user* tersimpan pada *database*.

Gambaran alur dari langkah-langkah atau proses manajemen *bandwidth* pada sistem Diagram alur manajemen *bandwidth* ditunjukkan pada Gambar 7

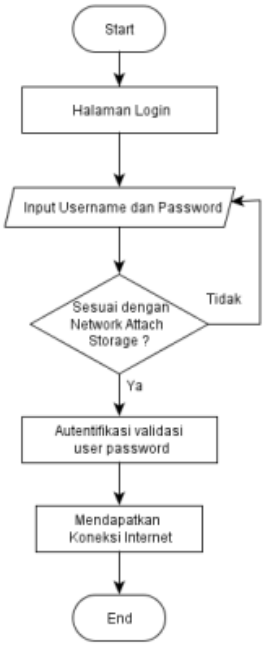


Gambar 7 Diagram Alur Manajemen Bandwidth

Merupakan diagram alur untuk manajemen *bandwidth* pada sistem, setelah membuka halaman mikrotik admin akan menuju menu *hotspot*. Kemudian dapat manajemen pada *Hotspot Server Profile* untuk mennetukan berapa *bandwidth* yang akan diberikan pada *user hotspot*.

3.4. Flowchart

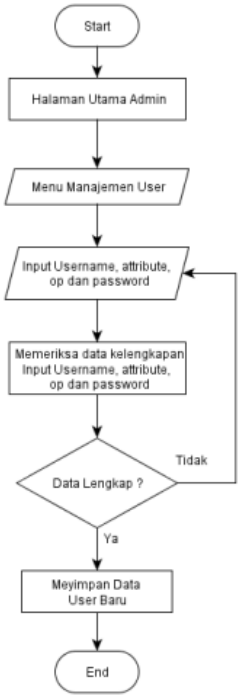
Diagram dengan simbol-simbol grafis yang menyatakan algoritma beserta dengan urutan yang saling terhubung untuk *login hotspot* ditunjukkan pada Gambar 8



Gambar 8 Flowchart Login

Pengguna masuk ke halaman *login*, melakukan input *user*name dan *password*, jika data *login user* tidak sama dengan data NAS (*Network Attach Storage*) akan berhenti pada halaman *login hotspot* dan jika data *login* sama dengan data NAS maka akan di autentifikasi untuk mendapatkan akses koneksi.

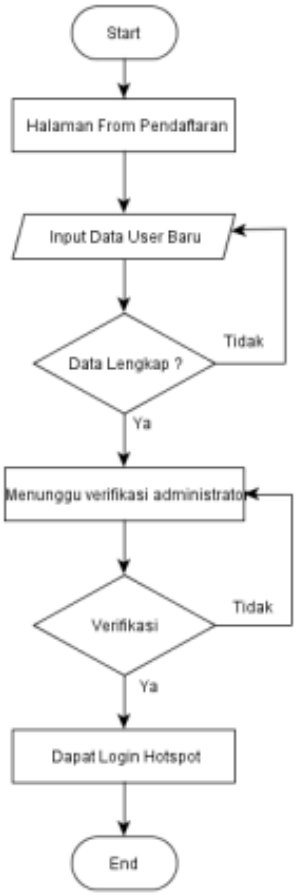
Diagram dengan simbol-simbol grafis yang menyatakan algoritma beserta dengan urutan yang saling terhubung untuk proses manajemen *user* pada sistem ditunjukkan pada Gambar 9



Gambar 9 Flowchart Manajemen User

Pada saat admin masuk halaman admin, kemudian masuk pada menu manajemen *user*, di manajemen *user* atau pendaftaran *user* baru yang membutuhkan kelengkapan data berupa *user*name, attribute, op dan *password* yang dilakukan oleh admin. Jika data *user* tidak lengkap maka akan kembali ke manajemen *user* dan jika data *user* lengkap makan data akan tersimpan.

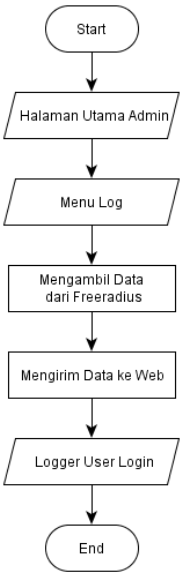
Diagram dengan simbol-simbol grafis yang menyatakan algoritma beserta dengan urutan yang saling terhubung untuk proses *user* melakukan pendaftaran mandiri ditunjukkan pada Gambar 10



Gambar 10 Flowchart Pendaftaran oleh User

Merupakan proses dimana *user* dapat melakukan sebuah pendaftaran untk mendapatkan *user*name dan *password* tanpa didaftarkan oleh admin. *User* masuk pada form pendaftaran, kemudian *user* melakukan input data, jika data tidak lengkap maka melakukan input data lagi dan jika data lengkap akan menunggu verifikasi administrator, jika sudah diverifikasi makan *user* dapat melakukan *login hotspot* .

Diagram dengan simbol-simbol grafis yang menyatakan algoritma beserta dengan urutan yang saling terhubung untuk proses mendapatkan data *user* yang *login* ditunjukkan pada Gambar 11



Gambar 11 Flowchart Logger

Merupakan proses untuk mendapatkan data *user* yang *login*, kemudian menampilkan data tersebut pada halaman web. Data *log*ger diambil dari *freeradius* yang sudah tersimpan di *database* pada setiap ada *user login*.

3.5. Perbandingan WEP, WPA dan Radius pada keamanannya

WEP *(Wired Equivalent Privacy)* merupakan enkripsi opsional yang dimasukkan (oleh administrator) ke klien maupun access point. Kunci ini harus cocok dari yang diberikan akses point ke client, dengan yang dimasukkan client untuk authentikasi menuju access point.

Kelebihannya Saat user melakukan koneksi ke jaringan, user tidak perlu melakukan perubahan settingan. Hanya pada saat pertama kali browsing user diminta untuk memasukkan username dan password. Kelemahannya keamanan password yang mudah dipecahkan.

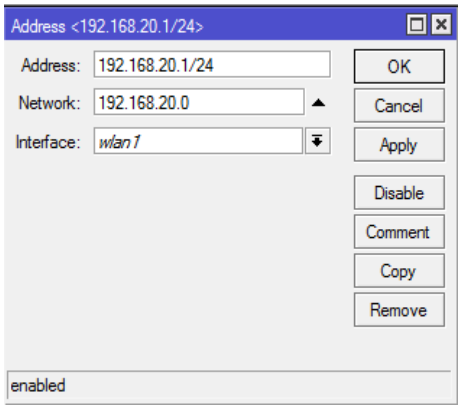
WPA (WI-FI Protected Accsess) merupakan pengembangan dari WEP , WPA menggunakan metode TKIP (Temporal Key Integrity Protocol) yang mampu berubah secara dinamis. Kelebihan, menggunakan enkripsi TKIP (Temporal Key Integrity Protocol). Kelemahan, proses kalkulasi data yang lama.

Radius digunakan untuk mengontrol user-user atau customer yang ada jauh dari jangkauan, jadi kita hanya pantau dari server radius tersebut untuk security authenticnya. Kelebihan :Menjalakan sistem administrasi terpusat.[2]

4. HASIL DAN PEMBAHASAN

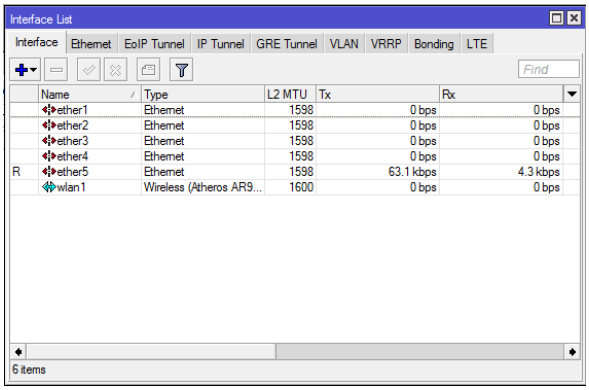
4.1. Konfigurasi WLAN Hotspot

Konfigurasi IP *Address* pada *interface* wlan di mikrotik. Konfigurasi dilakukan agar *interface* dapat terhubung dengan *client* yang akan menggunakan *hotspot* . Konfigurasi ditunjukkan pada Gambar 12.



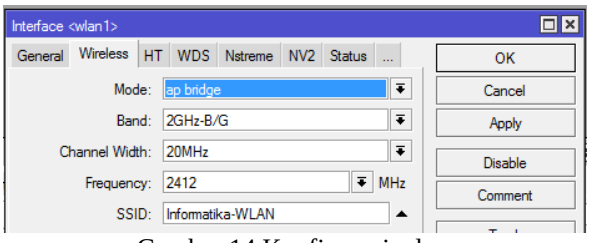
Gambar 12 Konfigurasi ip wlan

Konfigurasi *interface* atau *port* yang ada pada mikrotik. Konfigurasi ini dilakukan untuk mengaktifkan *interface* wlan yang akan digunakan sebagai sumber *hotspot* , cara mengaktifkan *interface* dengan memilih *interface* kemudian klik button check list. Konfigurasi ditunjukkan pada Gambar 13



Gambar 13 Konfigurasi interface

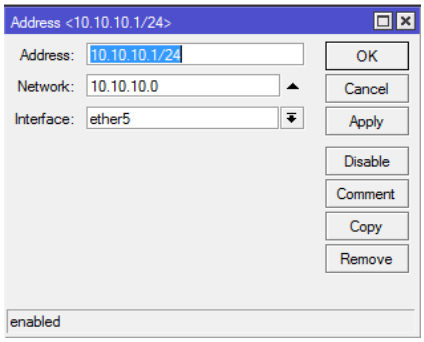
Konfigurasi wlan *hotspot* . Konfigurasi dilakukan untuk memilih mode *interface* wlan menjadi ap bridge dan SSID (Service Set Identifier) atau nama dari *hotspot* agar mudah dikenali. Konfigurasi ditunjukkan pada Gambar 14



Gambar 14 Konfigurasi wlan

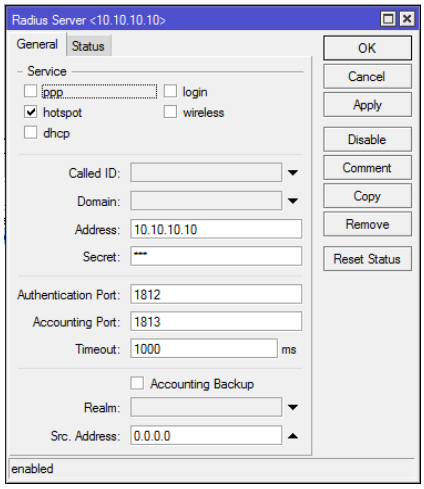
4.2. Konfigurasi Radius pada Mikrotik

Konfigurasi IP *Address* untuk *interface* yang terhubung dengan *server freeradius.* Konfigurasi ditunjukkan pada Gambar 15



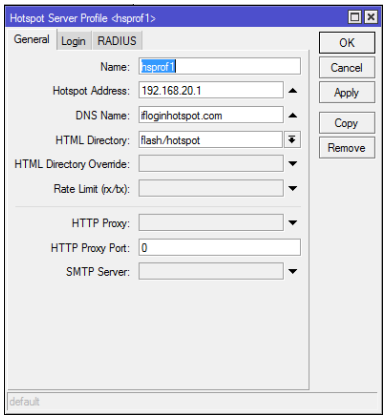
Gambar 15 Konfigurasi ip server

Konfigurasi *radius* pada mikrotik. Konfigurasi dilakukan untuk menghubungkan antara mikrotik sebagai *hotspot* dan *server freeradius* dimana konfigurasi membutuh IP *Address* dari *server* dan secret key yang terdapat pada *server*. Konfigurasi ditunjukkan pada Gambar 16



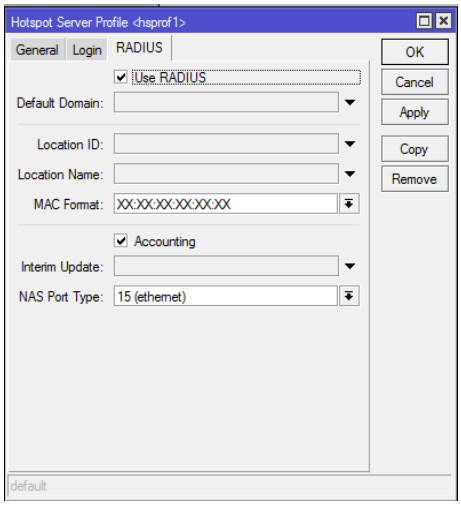
Gambar 16 Konfigurasi Radius

Konfigurasi *hotspot server* profile pada menu general. Konfigurasi dilakukan untuk mengganti nama alamat atau DNS (Domain Name System) halaman *login* mikrotik sehingga mudah diakses. Konfigurasi ditunjukkan pada Gambar 17



Gambar 17 Konfigurasi DNS halaman login

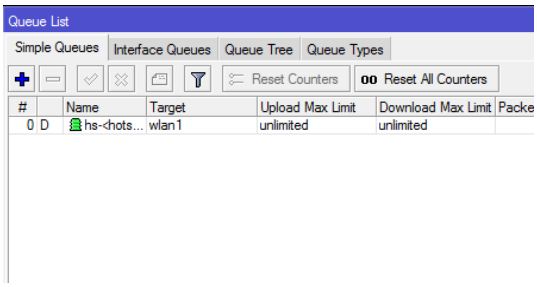
Konfigurasi *hotspot server* profile pada menu *RADIUS*. Konfigurasi dilakukan untuk mengaktifkan *radius server* pada *server* profile. Konfigurasi ditunjukkan pada Gambar 18



Gambar 18 Konfigurasi enable radius

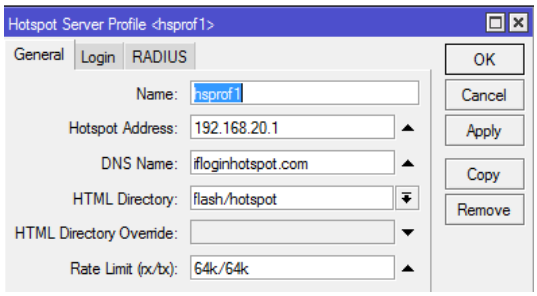
4.3. Konfigurasi Management Bandwidth Hotspot

Proses dimana belum di manajemen bandwidth. Seperti ditunjukkan pada Gambar 19



Gambar 19 Sebelum management bandwidth

Kemudian setelah dilakukan manajemen bandwidth pada hotspot seperti pada Gambar 20

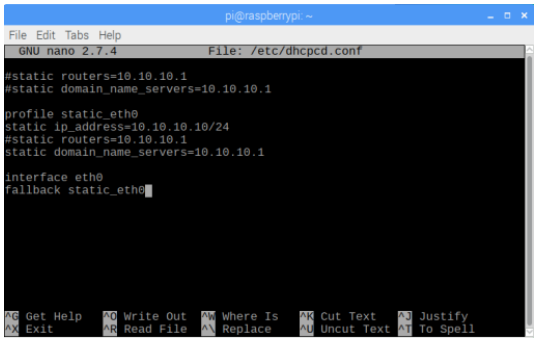


Gambar 20 Konfigurasi rate limit bandwidth hotspot

Penggunaan *Rate Limit* pada *hotspot server profile* ini, secara otomatis akan membatasi total *traffic* pada jaringan *Hotspot* Mikrotik. Pada gambar di atas, besarnya *rate limit* yang diset pada jaringan *hotspot* adalah sebesar 64K/64K, yang berarti 64 Kbps untuk total *traffic Upload* dan 64 Kbps untuk total *traffic Download* pada jaringan *hotspot* tersebut.

4.4. Konfigurasi Server

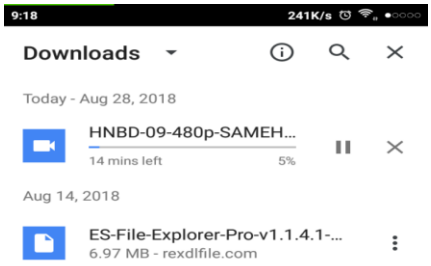
Konfigurasi IP *Address* pada *server Raspberry pi*. Konfigurasi IP *Address* pada *Raspberry pi* dilakukan pada file dhcpcd.conf. Konfigurasi menggunakan IP *Address* static namun pada fungsi fallback static jika *interface* mendapatkan IP *Address* dynamic dari DHCP (Dynamic Host Configuration Protocol) *server* akan tetap menggunakan IP dynamic Konfigurasi ditunjukkan pada Gambar 21



Gambar 21 Konfigurasi ip Address pada server

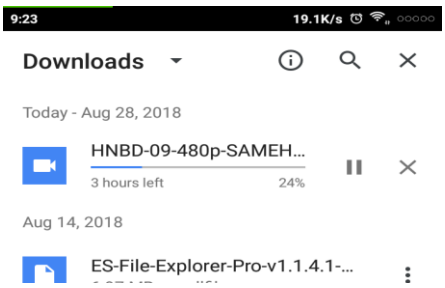
4.5. Pengujian Management Bandwidth Hotspot

Jika pada manajemen *bandwidth* tidak di konfigurasi maka *Upload Download Max Limit* otomatis akan *Unlimited.* Ditunjukkan pada Gambar 22



Gambar 22 Hasil download sebelum management bandwidth

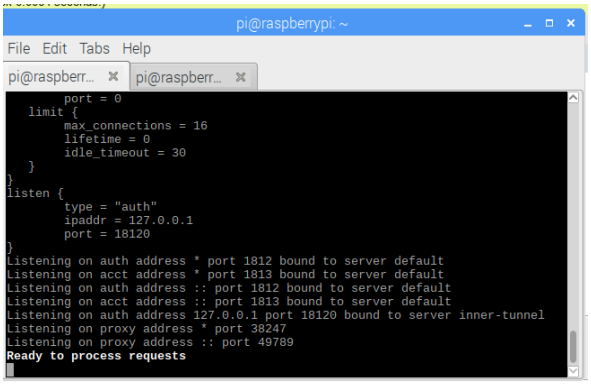
Dan *user hotspot* dapat melakukan *download* dengan tidak ada batasan *bandwidth*. Dengan hasil download seperti pada Gambar 23



Gambar 23 Hasil download setelah management bandwidth

4.6. Pengujian Server

Jika *port radius* dan proxy sudah bound (terhubung) dan terdapat keterangan Ready to process request maka *server* berhasil dijalankan. Ditunjukkan pada Gambar 24



Gambar 24 Menjalankan server freeradius

4.7. Pengujian Manajemen User

Pengujian halaman *login* admin dimana *interface* . Ditunjukkan pada Gambar 25

Gambar 25 Halaman login admin

Pengujian menambahkan *user* baru. Ditunjukkan pada Gambar 26

Gambar 26 Menambah user baru

Pengujian edit *user*. Ditunjukkan pada Gambar 27

Gambar 27 Edit user

4.8. Pengujian Login

Pengujian *login* pada sistem operasi. Ditunjukkan pada Tabel 1

Tabel 1 Pengujian login pada sistem operasi

No.	Sistem operasi	Hasil
1	Windows	Berhasil
2	Android (Mobile)	Berhasil
3	Windows 7	Berhasil
4	Windows 8	Berhasil
5	Windows 10	Berhasil
6	Android (Jelly Bean)	Berhasil
7	Android (KitKat)	Berhasil
8	Android (Marshmellow)	Berhasil
9	Android (Nougut)	Berhasil

Pengujian *login hotspot* dengan 12 *user*. Ditunjukkan pada Tabel 2

Tabel 2 Pengujian login hotspot

No.	Jumlah *Client*	Hasil
1	1 *User*	Berhasil
2	2 *User*	Berhasil
3	3 *User*	Berhasil
4	4 *User*	Berhasil
5	5 *User*	Berhasil
6	6 *User*	Berhasil
7	7 *User*	Berhasil
8	8 *User*	Berhasil
9	9 *User*	Berhasil
10	10 *User*	Berhasil
11	11 *User*	Berhasil
12	12 *User*	Berhasil

Halaman *login* mikrotik. Ditunjukkan pada Gambar 28

Gambar 28 Halaman login mikrotik

5. PENUTUP

5.1. Kesimpulan

Berdasarkan pembahasan yang telah dilakukan maka didapat beberapa kesimpulan sebagai berikut:

1. Dari pengujian server yang dilakukan, Freeradius berjalan dengan baik dan dapat melayani permintaan login dari user pada perangkat raspberry pi dengan sistem operasi Linux turunan Debian.
2. Fungsionalitas manajemen *user* pada sistem mampu berjalan dengan baik pada menu *create, edit* dan *delete* dalam pengujian menggunakan 12 data *user*.
3. Dapat berjalannya pelaporan (*logger*) *user*.

5.2. Saran

Adapun saran yang dapat diberikan setelah pengujian adalah sebagai berikut:

1. Dapat dibuatkan hak akses *user* khusus untuk mahasiswa informatika.
2. Pendaftaran *user* baru dapat di verifikasi melalui *email*.

DAFTAR PUSTAKA

[1] Wicahyanto, A., & Sumirat, E. W. (2012). Pendaftaran pengguna layanan *hotspot* berbasis web Pada *hotspot* mikrotik dan *freeradius*. IJNS-Indonesian Journal on Networking and Security, 1(1).

[2] Stiawan, D., Rini, D. P., Sriwijaya, J. S. K. U., & Sriwijaya, J. T. K. U. (2009). Analisis Perbandingan Sistem Keamanan WEP/WPA/*RADIUS* Pada Jaringan Publik Wireless *Hotspot* .

[3] Saliu, A. M., Kolo, M. I., Muhammad, M. K., & Nafiu, L. A. (2013). Internet *Authentication* and billing (*hotspot*) system using MikroTik router operating system. International Journal of Wireless Communications and Mobile Computing, 1(1), 51-57.

[4] Ala-Laurila, J., Mikkonen, J., & Rinnemaa, J. (2001). Wireless LAN access network architecture for mobile operators. IEEE Communications Magazine, 39(11), 82-89.

[5] Shadiq, H. M., Sudjadi, S., & Darjat, D. (2015). Perancangan Kamera Pemantau Nirkabel Menggunakan *Raspberry pi* Model B. Transient, 3(4), 546-551.

[6] Fernandez, E. B., & Warrier, R. (2003). *Remote* authenticator/authorizer. Procs. of PLoP.

[7] Hidayat, R. N. (2010, June). Implementasi Tomato Firmware Pada Linksys Wireless Router Dengan Proses *Authentification*, *Authorization*, *Accounting* Menggunakan *Radius Server*. In Seminar Nasional Aplikasi Tekno*log*i Informasi (SNATI).

[8] Rachman, A., & Aminullah, M. (2013). RANCANG BANGUN PROXY *SERVER* DAN ANALISIS PEMAKAIAN INTERNET DENGAN MENGGUNAKAN SARG (STUDI KASUS DI BMKG JUANDA SURABAYA). Jurnal IPTEK Vol, 17(1).

[9] Jumri, J. P. (2013). Perancangan Sistem Monitoring Konsultasi Bimbingan Akademik Mahasiswa dengan Notifikasi Realtime Berbasis SMS Gateway. Jurnal Sistem dan Tekno*log*i Informasi (JustIN), 1(1), 21-25.

[10] Stiawan, D., Rini, D. P., Sriwijaya, J. S. K. U., & Sriwijaya, J. T. K. U. (2009). Analisis Perbandingan Sistem Keamanan WEP/WPA/RADIUS Pada Jaringan Publik Wireless Hotspot.