BAB I

PENDAHULUAN

1.1 Latar Belakang

Salah satu perubahan utama di bidang telekomunikasi adalah penggunaan teknologi jaringan *wireless*. Dimana Jaringan *wireless* atau sering disebut *hotspot* ini menjadi daya tarik tersendiri bagi para pengguna komputer yang menggunakan teknologi ini untuk mengakses suatu jaringan komputer atau internet, dikarenakan kemudahan-kemudahan yang ditawarkan oleh teknologi jaringan *wireless*. Pada beberapa tahun terakhir ini pengguna jaringan *wireless* mengalami peningkatan yang pesat. Peningkatan dari pengguna teknologi ini juga diimbangi dengan peningkatan jumlah *hotspot* di tempat-tempat umum, seperti pusat perbelanjaan, Kafe, Bandara, di perkantoran, di Kampus bahkan juga di Sekolah-sekolah. Dengan menggunakan teknologi *wireless* (*hotspot)* kita dapat menikmati akses internet dimanapun kita berada selama di area *hotspot* tanpa harus menggunakan kabel.

Di lingkungan Sekolah SMA Negeri 2 Prabumulih saat ini juga sudah menyediakan layanan internet yang berbasis *wireless (hotspot)*. Layanan Telkom Speedy yang berkecepatan hingga 2 Mbps pun digunakan untuk membuat jaringan *wireless (hotspot)* di SMA Negeri 2 Prabumulih, dan terdapat dua buah *access point* TP-LINK, sehingga *hotspot* pada SMA Negeri 2 Prabumulih dapat

diakses pada dua area, seperti pada ruangan guru-guru, dan area ruangan kelas siswa, jumlah *user* yang mengakses jaringan *wireless* di SMA Negeri 2 Prabumulih berkisar antara 1 sampai dengan 50 *user*, namun didalam jaringan yang tidak mempunyai server yang bertindak sebagai *authentication, authorization, and* a*ccounting* membuat administrator tidak bisa mengetahui identitas yang jelas dari *user*.

Dengan sistem keamanan yang menggunakan WEP (*Wired Equivalent Privacy*) dimana WEP ini menggunakan satu kunci enkripsi yang digunakan bersama-sama oleh para pengguna *wireless* untuk dapat beriternet pada jaringan *wireless* SMA Negeri 2 Prabumulih, seorang *user* juga harus meminta key kepada seorang *administrator*, dan setiap *user* yang ingin berpindah ke *hotspot* yang lain, *user* pun di minta untuk kembali memasukan key, karena setiap titik mempunyai *network* key yang berbeda, tentunya cara yang seperti ini sangat menyulitkan baik bagi *user* maupun *administrator.*

Jaringan *wireless (hotspot)* yang tidak mempunyai server yang dapat melakukan autentikasi, tentunya tidak menjamin keamanan baik dari *user* maupun administrator pada jaringan *wireless* di SMA Negri 2 Prabumulih, sebab seorang *administrator* tidak dapat mengetahui *user-user* yang login dan berinternet pada jaringan, juga tentunya menyulitkan administrator karena tidak dapat memantau serta mengontrol *user* di dalam jaringan *wireless* (*hotspot*) di SMA Negri 2 Prabumulih.

Untuk dapat membuat autentikasi pengguna jaringan *wireless (hotspot)* serta meningkatkan keamanan, dan memberi kenyamanan terhadap pada pengguna jaringan *wireless*, maka dapat dilakukan dengan cara penerapan sistem

autentikasi pengguna *wireless (hotspot)* berbasis radius server, yang mana masalah ini diangkat penulis kedalam skiripsi yang berjudul **"Autentikasi Pengguna Jaringan *Wireless Hotspot* Berbasis Radius Server".**

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka penulis merumuskan permasalah dalam penelitian ini yaitu "Bagaimana membuat autentikasi pengguna jaringan *Wireless (Hotspot)* berbasis radius server" dengan FreeRadius yang akan diinstall pada sistem operasi linuk ubuntu.

1.3 Batasan Masalah

Dalam penelitian ini penulis membatasi permasalahan agar tetap terarah dan tidak menyimpang dari apa yang sudah direncanakan sebelumnya. Adapun batasan masalah pada penelitian ini :

1. Membuat autentikasi pengguna *wireless (hotspot)* yang berbasis Radius Server, yang mana Sistem ini akan deterapkan pada Sistem Operasi Linuk Ubuntu.
2. Membuat *user* yang bisa login pada jaringan hanya *user* yang terdaftar pada server radius, dan memberi laporan tentang aktivitas *user* pada jaringan.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

Penelitian ini bertujuan untuk membuat autentikasi penggunaan *wireless (hotspot)* berbasis radius server di SMA Negri 2 Prabumulih. agar *user* yang mengakses jaringan *wireless* memiliki kemudahan dalam hal melakukan hubungan (konektivitas) kejaringan *wireless (hotspot),* dan juga dapat memberi kemudahan pada administrator jaringan dalam mengelola jaringan *wireless (hotspot)* di SMA Negri 2 Prabumulih.

1.4.2 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut :

1. Bagi sekolah agar dapat meningkatkan keamanan jaringan *wireless* yang ada serta memudahkan administrator dalam mengelola jaringan *wireless*.
2. Bagi penulis dapat menambah pengetahuan dan pemahaman tentang autentikasi pengguna *wireless* yang berbasis radius server.
3. Manfaat bagi dunia akademik dari hasil penelitian ini diharapkan dapat menjadi bahan *referensi* untuk mahasiswa Universitas Binadarma terutama bagi penulis sendiri untuk penelitian selanjutnya dalam mengaplikasikan apa yang selama ini diterima dibangku kuliah kedalam dunia kerja yang sebenarnya.

1.5 Metodologi Penelitian

1.5.1 Waktu dan Tempat Penelitian

Penelitian ini dilaksanakan pada 20 April 2014 sampai dengan bulan 20 Mei 2014, untuk lokasi penelitian ini dilaksanakan di SMA Negeri 2 Prabumulih.

1.5.2 Metode Penelitian

Dalam menyusun skripsi ini penulis Menggunakan metode *Action Research* (Penelitian Tindakan). *Action Research* menurut Davison, Martinsons, dan Kock (2004) yaitu penelitian tindakan yang mendeskripsikan, menginterpretasi dan menjelaskan suatu situasi sosial atau pada waktu bersamaan dengan melakukan perubahan atau *interversi* dengan tujuan perbaikan atau partisipasi. Adapun tahapan penelitian yang merupakan bagian dari *action research* ini, yaitu :

1. Melakukan diagnosa *(Diagnosing)*

   Pada tahapan ini kita melakukan identifikasi masalah-masalah pokok yang ada.

2. Membuat rencana tindakan *(Action Planning)*

   Pada tahapan ini kita memahami pokok masalah yang ada dan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada.

3. Melakukan tindakan *(Action Taking)*

   Pada tahapan ini kita mengimplementasikan rencana tindakan dengan harapan dapat menyelesaikan masalah.

4. Melakukan evaluasi *(Evaluating)*

   Pada tahapan ini kita evaluasi hasil dari implementasi.

5. Pembelajaran *(Learning)*

Pada tahap ini kita melakukan *review* tahapan-tahapan yang telah berakhir dan mempelajari kriteria dalam prinsip pembelajaran.

1.5.3 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam melakukan penelitian adalah sebagai berikut :

1. Observasi (*Observation*)

   Data dikumpulkan dengan melihat secara langsung dari objek yang diteliti.

2. Wawancara (*Interview*)

   Untuk mendapatkan data-data secara langsung dari sumber yang mengerti sehubungan dengan pengamatan yang penulis lakukan. Dalam hal ini penulis mengajukan pertanyaan-pertanyaan kepada pada administrator jaringan komputer di SMA Negeri 2 Prabumulih.

3. Kepustakaan (*Literature*)

   Yaitu dengan cara mengumpulkan data-data yang dilakukan dengan cara membaca dan mempelajari buku-buku yang berkaitan dengan permasalahan yang akan menunjang terhadap materi pembahasan masalah yang diteliti.

1.6 Sistematika Pembahasan

Dalam sistematika pembahasan ini akan menjelaskan mengenai uraian secara singkat isi tiap-tiap bab dalam penelitian ini adalah sebagai berikut :

BAB I PENDAHULUAN

Pada Bab ini menguraikan latar belakang masalah, tujuan dan manfaat pengamatan, rumusan masalah, pembatasan masalah dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada Bab ini menguraikan pengertian mengenai landasan pemikiran yang berisi teori-teori mengenai *autentikasi* radius server.

BAB III TINJAUAN OBJEK

Pada bab ini menguraikan tinjauan objek penelitian yang berisi sejarah dari sebuah objek yang diteliti, visi dan misi, sistem yang sedang berjalan dan permasalahan yang muncul.

BAB IV ANALISIS DAN PERANCANGAN

Pada Bab ini menguraikan rancangan yang akan dibuat untuk menyelesaikan permasalahan yang ada.

BAB V HASIL DAN PEMBAHASAN

Pada bab ini menguraikan tentang hasil dari implementasi pada bab sebelumnya seperti membahas kelebihan sistem yang digunakan serta kekurangannya.

BAB VI SIMPULAN DAN SARAN

Pada Bab ini menguraikan kesimpulan - kesimpulan dari pembahasan bab-bab di atas dan kemudian dilanjutkan dengan saran - saran.

BAB II

TINJAUAN PUSTAKA

2.1 Radius Server

Remote Access Dial-in User Service (RADIUS), merupakan suatu mekanisme akses kontrol yang mengecek dan mengautentikasi (*authentication*) *user* atau pengguna berdasarkan pada mekanisme authentikasi yang sudah banyak digunakan sebelumnya, yaitu menggunakan metode *challenge / response*. *Remote Access Dial In User Service* (RADIUS) dikembangkan di pertengahan tahun 1990 oleh *Livingstone Enterprise* (sekarang *Lucent Technologies*). Yang pada awalnya perkembangan RADIUS menggunakan *port* 1645 yang namun bentrok dengan layanan *datametrics*. Dan sekarang *port* yang dipakai RADIUS adalah *port* 1812 yang format standarnya ditetapakan pada *Request for Command* (RFC) 2138 (C,Rigney, 1997).

Server RADIUS menyediakan mekanisme keamanan dengan menangani autentikasi dan autorisasi 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 autentikasi dan autorisasi berhasil maka proses pelaporan dilakukan, yakni dengan mencatat semua aktivitas koneksi

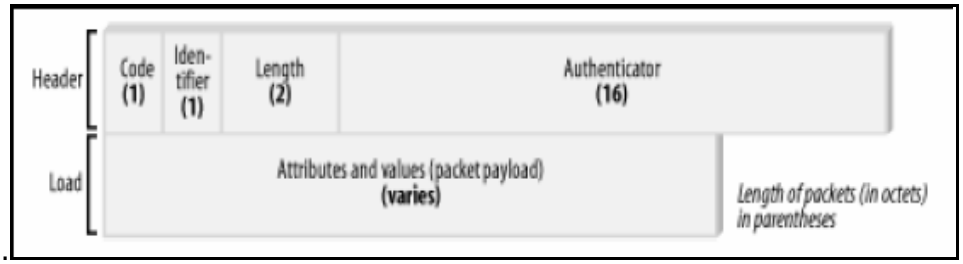
pengguna, menghitung durasi waktu dan jumlah transfer data yang dilakukan oleh pengguna. Proses pelaporan yang dilakukan server RADIUS bisa dalam bentuk waktu (detik, menit, jam) maupun dalam bentuk besar transfer data (*Byte, KByte, Mbyte*) .(Yunus, Amak, 2010)

RADIUS merupakan suatu protokol yang dikembangkan untuk proses AAA (*authentication, authorization, and* a*ccounting*). (Agung S., 2008) Berikut ini adalah RFC (*Request For Comment*) yang berhubungan dengan RADIUS :

- RFC2865 : *Remote Authentication Dial-In User Service* (RADIUS)
- RFC 2866 : RADIUS *Accounting*
- RFC 2867 : RADIUS *Accounting for Tunneling*
- RFC 2868 : RADIUS *Authentication for Tunneling*
- RFC2869 : RADIUS *Extensions*
- RFC 3162 : RADIUS *over* IP6
- RFC 2548 : *Microsoft Vendor-Specific RADIUS Attributes*

2.1.1. Format Paket Data RADIUS

Format paket RADIUS terdiri dari *Code, Identifier, Len gth, Authenticator* dan *Attributes* seperti ditunjukkan pada Gambar 2.4



Gambar 2.1 Struktur paket data RADIUS (J. Hassel, 2002)

1. *Code: Code* memiliki panjang 1 *byte* (8 bit), digunakan untuk membedakan tipe pesan RADIUS yang dikirim. Tipe pesan RADIUS dapat berupa *access request, access accept, access reject* dan *access challenge*.
2. *Identifier:* Memilik panjang 1 *byte* yang digunakan untuk menyesuaikan antara paket permintaan dan respon dari server RADIUS.
3. *Length:* Memiliki panjang 2 *byte*, memberikan informasi mengenai panjang paket. Jika paket kurang atau lebih dari yang diidentifikasikan pada *length* maka paket akan dibuang.
4. *Authenticator:* Memiliki panjang 16 *byte* yang digunakan untuk mengautentikasi tanggapan dari server RADIUS.
5. *Attributes:* Memiliki panjang yang tidak tetap, berisi autentikasi, autorisasi dan informasi. Contoh atribut RADIUS yaitu, *username* dan *password*.

2.1.2 Prinsip Kerja RADIUS

RADIUS merupakan protokol *security* yang bekerja menggunakan sistem *client*-server terdistribusi yang banyak digunakan bersama AAA untuk mengamankan jaringan dari pengguna yang tidak berhak. RADIUS melakukan autentikasi *user* melalui serangkaian komunikasi antara *client* dan server. Bila *user* berhasil melakukan autentikasi, maka *user* tersebut dapat menggunakan layanan yang disediakan oleh jaringan (T.Y. Arif dkk,2007 & Darmariyadi, 2003).

2.1.3 Free Radius Server

Alasan utama kenapa memilih *free* RADIUS server adalah karena mahalnya harga RADIUS server komersial. Sebagai contoh : Interlink's Secure.XS harganya mulai dari $2375 untuk 250 pengguna, Funk Odyssey Server $2500, VOP Radius Small Business mulai dari $995 untuk 100 pengguna. Harga RADIUS server komersial diatas kebanyakan tidak terjangkau bagi para pemilik *hotspot*, terutama bagi kalangan kampus.

Salah satu contoh RADIUS server yang non-komersial adalah FreeRADIUS server. FreeRADIUS server ini tidak kalah dengan RADIUS server yang komersial. Salah satu buktinya adalah freeRADIUS server sudah mendukung beberapa *Access point* (AP)/ (Agung,S 2008) *Network Access Server* (NAS) dibawah ini :

• 3Com/USR Hiper Arc Total Control

• 3Com/USR NetServer

• 3Com/USR TotalControl

• Ascend Max 4000 family

• Cisco Access Server family

• Cistron PortSlave

• Computone PowerRack

• Cyclades PathRAS

• Livingston PortMaster

• Multitech CommPlete Server

• Patton 2800 family

FreeRADIUS dapat berjalan di berbagai sistem operasi, misalnya Linux, FreeBSD, OpenBSD, OSF. Selain FreeRADIUS, ada beberapa RADIUS server non-komersial yang lain, diantaranya adalah:

1. Cistron Radius Server

   Cistron RADIUS dibuat oleh Miguel van Smoorenburg. Merupakan *free software* (dibawah lisensi GNU GPL). Cistron RADIUS dapat diperoleh di

2. ICRadius

   ICRADIUS merupakan varian dari Cistron. ICRADIUS menggunakan MySQL untuk menyimpan *database* nama-pengguna beserta *password*. ICRADIUS sudah berbasis *web*, hal ini akan memudahkan administrator untuk mengelola server ini.

3. JRadius

   Merupakan Java plug-in untuk FreeRADIUS.

4. XtRadius

   XtRadius adalah *freeware* RADIUS server yang berbasiskan pada Cistron RADIUS Server. Perbedaan utama antara XtRadius dengan RADIUS server yang lain adalah kita dapat mengeksekusi *skript* untuk menangani autentikasi.

5. OpenRadius

   OpenRADIUS server dapat berjalan di beberapa sistem operasi unix. OpenRADIUS juga merupakan *free software*, bebas digunakan tanpa harus bayar, pengguna dapat melakukan modifikasi apabila dianggap perlu.

6. YardRadius

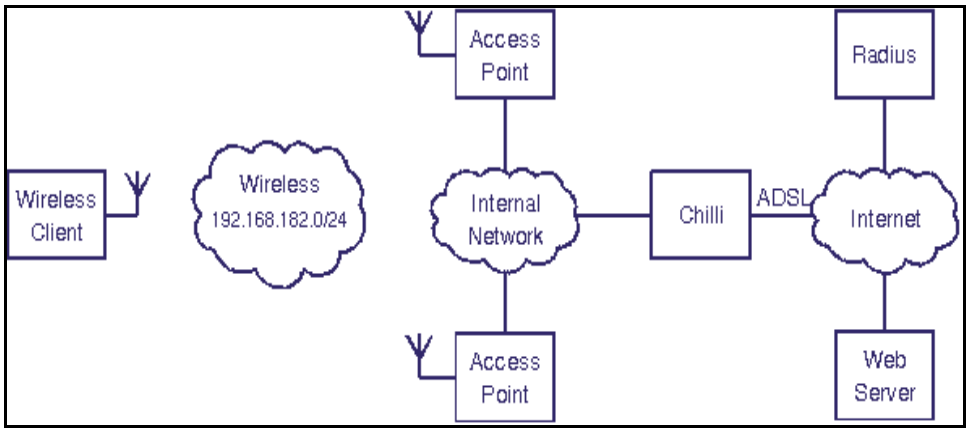
   YARDRRADIUS adalah singkatan dari *Yet Another Radius Daemon* RADIUS. Tulisannya YARDRADIUS, tetapi membacanya Y-A-R-D RADIUS. YARDRADIUS merupakan *free software* yang berasal dari *open source* Livinston RADIUS Server 2.1.

2.1.4 ChilliSpot

ChilliSpot, merupakan *open source captive portal* atau *Wireless LAN access point controller*. Digunakan untuk mengautentikasi *user* dari sebuah jaringan *Wireless LAN*. Mensupport login berbasis web yang merupakan standar untuk public *hotspot* dewasa ini. ChilliSpot juga dapat sebagai media autentikasi, autorisasi dan *accounting* (AAA) yang merupakan framework atau arsitektur kerja dari sebuah RADIUS server (http://www.chillicpot.info/).

Chilli men-*support* dua jenis metode authentikasi, yaitu :

1. Universal Access Method (UAM); dengan UAM, *wireless client* me-*request* sebuah IP address, dan dialokasikan oleh Chilli. Ketika seorang *user* membuka sebuah *web browser*, Chilli akan menangkap koneksi TCP tersebut dan me*redirect* browser tersebut ke autentikasi web server. Web server meminta *user* untuk *user*name dan *password*, *password* di enkripsi dan dikirim kembali ke Chilli.
2. *Wireless Protected Access (WPA)*; dengan WPA, metode autentikasi di*handle* oleh *access point* dan *subsequently* di *forward* dari *access point* ke Chilli. Jika WPA digunakan, maka koneksi yang terjadi antara *access point* dan *user* di enkripsi.



Gambar 2.2 Arsitektur Jaringan ChilliSpot (http://www.chillicpot.info/)

2.1.5 Ubuntu 10.04

Ubuntu merupakan sistem operasi yang bebas *(open source)* yang menekankan komuniti, sokongan, dan kemudahan dari para penggunaan tanpa harus mengorbankan kelajuan, kekuatan, atau fleksibiliti. Linux ini dapat digunkan semua golongan, yang rancang untuk semua orang dari pemula pengguna computer, samapai para ahli. Ubuntu 10.04 merupakan keluaran terbar yang lebih mantap, lebih fleksibel, dan ramah dari versi-versi sebelumnya.

Pada umumnya master distro GNU/Linux tersedia dalam format ISO file yang merupakan format terkompresi dalam bentuk image file. untuk Ubuntu dapat didownload pada http://ubuntu.com/download. adapun File ISO yang disediakan dikategorikan dalam beberapa bagian yaitu:

A. Ubuntu Desktop

   Diperuntukkan untuk komputer-komputer desktop termasuk laptop dan sejenisnya kecuali netbook. Untuk installasi dibutuhkan memory dengan kapasitas minimal 256MB untuk dapat menginstall versi ini, versi Ubuntu Desktop dikategorikan berdasarkan jenis microprocessor yaitu:

- Ubuntu Desktop 32-bit

  Jika menggunakan mikroprocessor keluaran intel maka jenis ini yang harus di download. Ubuntu Desktop 32-bit biasa juga disebut X86 atau i386 dimana merujuk ke code name intel. Jenis ini juga dapat digunakan untuk AMD 32 bit.

- Ubuntu Desktop 64-bit

  Jika menggunakan mikroprocessor keluaran AMD 64 bit pastikan mendownload jenis ini. Juga berlaku untuk jenis arsitektur EM64T seperti Athlon64, Opteron, EM64T Xeon dan Core 2.

B. Ubuntu Server

Ubuntu Server digunkan untuk komputer-komputer kelas server dan tanpa dukungan terhadap lingkungan *Grafical User Interface* (GUI) secara *default*. Ubuntu server juga hadir dengan lingkungan *Command Line Interface* (CLI) secara *default*. Jika telah menginstall Ubuntu Server jangan lagi mencari tampilan grafis. Jenis ini tersedia dalam dua kategori seperti diversi Ubuntu Desktop yaitu Ubuntu Server 32-bit dan Ubuntu Server 64-bit.

C. Ubuntu Alternate

Jika memiliki memory dibawah 256MB dengan spesifikasi hardware yang pas-pasan sebaiknya menggunakan Ubuntu Alternate sebagai solusi karena proses instalasi disajikan dalam mode text menu. Selain itu juga dengan CD alternate, upgarde versi Ubuntu dapat dilakukan tanpa perlu ada koneksi internet ke server Ubuntu. Jenis ini tersedia dalam dua kategori

seperti diversi Ubuntu lainnya yaitu Ubuntu alternate 32-bit dan Ubuntu alternate 64-bit.

D. Ubuntu Netbook

Diperuntukkan untuk netbook yang tersedia 2 versi yaitu:

• Netbook live CD

Jika netbook anda memiliki externel CD drive untuk digunakan live cd/install. Tidak ada perbedaan versi untuk jenis ini karena sudah mendukung intel/amd dan jenis lainnya.

• Netbook live image

Tersedia untuk platforms ARM yang terdiri atas, Marvell Dove netbook live image dan Freescale i.MX51 netbook live image, Kedua jenis ini hanya mendukung booting dengan usb image.

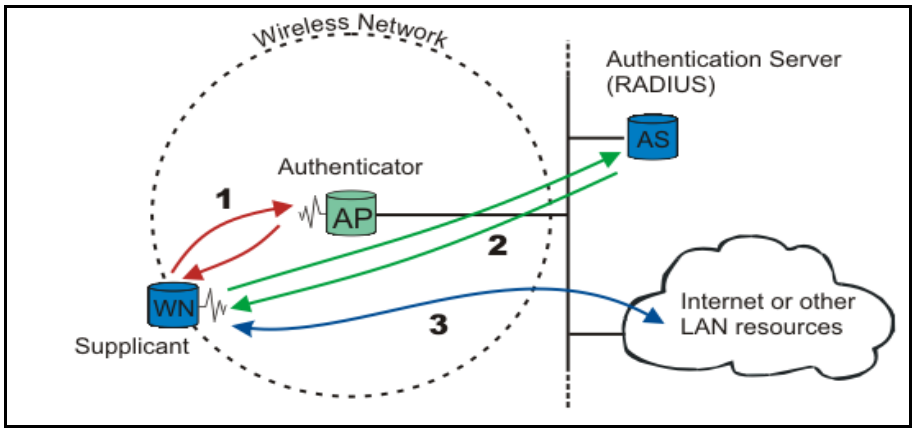
2.2 Autentikasi

Menurut (J, Hassel, 2002), autentikasi adalah proses pengesahan identitas pengguna (*end user*) untuk mengakses jaringan. Proses ini diawali dengan pengiriman kode unik misalnya, *username*, *password*, *pin*, sidik jari oleh pengguna kepada server. Di sisi server, sistem akan menerima kode unik tersebut, selanjutnya membandingkan dengan kode unik yang disimpan dalam *database* server. Jika hasilnya sama, maka server akan mengirimkan hak akses kepada pengguna. Namun jika hasilnya tidak sama, maka server akan mengirimkan pesan kegagalan dan menolak hak akses pengguna.

2.2.1 Mekanisme Autentikasi

Tujuan standar 802.1x IEEE adalah untuk menghasilkan kontrol akses, autentikasi, dan manajemen kunci untuk *wireless* LANs. Standar ini berdasarkan pada *Internet Engineering Task Force* (IETF) *Extensible Authentication Protocol* (EAP), yang ditetapkan dalam RFC 2284. Standar 802.1x IEEE juga mendukung beberapa metode autentikasi, seperti *smart cards, password* yang hanya bisa digunakan oleh satu pengguna pada satu waktu, dan yang lebih baik lagi adalah *biometrics*.(Agung,S ,2008)

802.1x terdiri dari tiga bagian, yaitu *wireless node* (*supplicant*), *access point* (autentikator), autentikasi server. Autentikasi server yang digunakan adalah *Remote Authentication Dial-In Service* (RADIUS) server dan digunakan untuk autentikasi pengguna yang akan mengakses *wireless* LAN. EAP adalah protocol layer 2 yang menggantikan PAP dan CHAP.



Gambar 2.3 Mekanisme Autentikasi menggunakan RADIUS server

Ket:

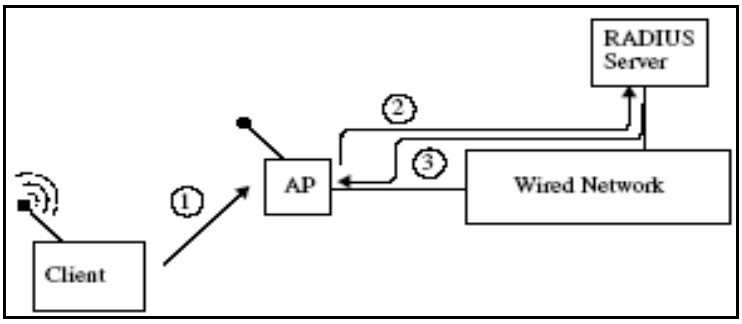
1. *Wireless Node* (WN) / *Supplicant* meminta akses ke *wireless network*, *Access point* (AP) akan menanyakan identitas *Supplicant*. Tidak ada trafik data selain EAP yang diperbolehkan sebelum *Supplicant* terautentikasi.

Access point bukanlah sebuah autentikator, tetapi *access point* berisi autentikator.

2. Setelah nama-pengguna dan *password* dikirim, proses autentikasi dimulai. Protokol yang digunakan antara *Supplicant* dan Autentikator adalah EAP, atau EAP *Protocol over* LAN (EAPoL). Autentikator mengenkapsulasi kembali pesan EAP kedalam format RADIUS, dan mengirimnya ke RADIUS server. Selama proses autentikasi, autentikator hanya menyampaikan paket antara *Supplicant* dan RADIUS server. Setelah proses autentikasi selesai, RADIUS server mengirimkan pesan sukses (atau gagal, apabila proses autentikasinya gagal.)
3. Apabila proses autentikasi sukses, *Supplicant* diperbolehkan untuk mengakses *wireless* LAN dan/atau internet.

2.2.1.1 Pemfilteran alamat MAC

Pengguna *wireless* LAN dapat difilter berdasarkan alamat MAC *wireless card* yang dimiliki pengguna. Hampir semua *access point* telah mempunyai fitur pemfilter alamat MAC. Administrator jaringan dapat memprogram *access point*, program ini yang berisi daftar alamat-alamat MAC yang dapat mengakses *access point* tersebut. Memprogram *access point* untuk memasukkan alamat-alamat MAC akan sangat merepotkan, terutama apabila jumlah alamat MAC yang ingin terhubung ke *access point* sangat banyak. Pemfilteran alamat MAC dapat diimplementasikan pada RADIUS server, alamat MAC beserta identitas pengguna dimasukkan ke dalam RADIUS server. Hal ini tentu akan mempermudah administrator untuk mengelola *wireless* LAN. (Agung,S ,2008).



Gambar 2.4 Pemfilteran alamat MAC dengan menggunakan RADIUS Server

Berikut ini penjelasan dari Gambar 3 mengenai pemfilteran alamat MAC dengan RADIUS server:

1. *Client* (*Wireless Node*) meminta akses ke *Access point* (AP).
2. AP meneruskan permintaan *client* ke RADIUS Server, di RADIUS Server alamat MAC *client* diperiksa apakah ada di *database*.
3. RADIUS memberikan tanggapan ke AP, apabila autentikasi di RADIUS Server berhasil maka *client* diperbolehkan untuk mengakses AP, dan apabila gagal maka *client* tidak diijinkan untuk mengakses AP tersebut.

2.3 Jaringan *Wireless*

Sinyal *Wireless* merupakan sinyal gelombang elektromagnetis yang dapat berjalan tanpa media tetapi melalui ruang hampa atau media seperti udara. Karena tidak dibutuhkan media fisik sebagai perantara, maka hal ini akan sangat menguntungkan pada saat membangun jaringan pada daerah atau area yang luas.

WI-FI (*Wireless Fidelity*) atau jaringan tanpa kabel, yang sering, maka disebut degan jaringan 802.11 karena standar yang biasanya digunakan adalah IEEE 802.11. Keuntungan menggunakan jenis jaringan seperti ini adalah tanpa

menggunakan medium seperti kabel,kita sudah dapat membangun atau melakukan koneksi ke jaringan.

Penggunaan angka 802.11 *(standard wireless network)* dibuat oleh IEEE *(Institute of Electrical and Electronics Engineers).* Penggunaan notasi a,b,dan g, adalah menunjukan versi yang berbeda dalam standar 802.11. versi yang pertama diluncurkan adalah 802.11b beroperasi pada 2,4GHz dan kecepatan 11 Mbps. Kemudian dilanjutkan dengan versi 802.11a dengan beroperasi pada 5GHz dan kecepatan 54Mbps. Versi yang terakhir adalah 802.11g adalah campuran dari kedua versi sebelumnya, beroperasi pada 2,4 GHz dan kecepatan 54Mbps.

Pada dasarnya sistem yang diggunakan pada jaringan WI-FI adalah analogi dengan HT(*Handie-talkie*). Alat ini dapat mengirim dan menerima sinyal radio. Suara yang dikirim akan diterima oleh microphone dan di enkodekan menjadi frekuensi radio dan di transmisikan melalui antana. (Utomo,Eko.2011:74.,)

2.3.1 Macam Jaringan *Wireless.*

Analogi dengan jaringan yang menggunakan kabel,jaringan WI-FI dapat dibedakan dalam beberap macam berdasarkan jarak data yang dapat di transmisikan, yaitu :

a. *Wireless Wide Area Network* (WWANs)

   Koneksi ini dapat mencakup jangkauan yang luas seperti pada sebuah kota atau Negara, melalui beberapa antana atau sistem satelit yang digunakan oleh pnyelengara jasa telekomunikasi.

b. *Wireless Metropolitan Area Network* (WMANs)

Degan teknologi ini akan memungkinkan pengguna untuk membuat koneksi nirkabel antara beberapa lokasi dalam satu daerah metropolitan misalnya antara gedung-gedung yang berbeda dalam satu kota atau dalam satu kampus atau satu universitas.

c. *Wireless Local Area Network* (WLANs)

Teknologi WLAN akan mengijinkan pengguna membangun jaringan nirkabel dalam satu daerah local,misalnya dalam lingkungan satu kantor, gedung, hotel, bandara. Dengan WLAN ini pengguna dapat melakukan aktivitas pekerjaan pada lokasi yang berbeda ,namun masih dalam satu kantor atau satu gedung. pembangunan pengoperasian WLAN dapat dilakukan dengan dua cara ,yatu:

- Sebuah piranti *wireless* (yang dilengkapi dengan network card atau modem external),terhubung dangan *access point* nirkabel yang berfungsi sebagai jembatan *(bridge)* antara *workstation-workstation* dan jaringan *backbone* yang ada.
- Jika sifat peer-to-peer (*ad hoc*) misal dalam satu ruangan rapat,dapat membentuk suatu jaringan sementara tanpa menggunakan *access point*.

d. *Wireless Personal Area Network* (WPANs)

Pada teknologi ini membolehkan pengguna membangun jaringan nirkabel untuk piranti-piranti sederhana,antara lain PDA (*Personal Digital Assistant*), HP/ telepon selular atau laptop. Hal ini dapat dilakukan pada sebuah ruang operasi personal (Personal *Operating Space* atau POS).

Sebuah POS dalah sebuah ruang yang bisa mencapai 10 meter. Dua teknologi yang banyak dipakai dalam penerapan WPANs adalah bluetooth dan infrared (Utomo,Eko.2011:75.)

2.3.2 Teknologi Pengamanan *Wireless*

Sistem keamanan yang paling umum diterapkan pada *wireless* LAN adalah dengan metode enkripsi, yaitu WEP (*Wired Equivalent Privacy*). WEP ini menggunakan satu kunci enkripsi yang digunakan bersama-sama oleh para pengguna *wireless* LAN. Hal ini menyebabkan WEP tidak dapat diterapkan pada *hotspot* yang dipasang di tempat-tempat umum. Dan karena lubang keamanan yang dimiliki WEP cukup banyak, sehingga mudah dibobol oleh pihak ketiga yang tidak berhak, maka penggunaannya tidak disarankan lagi. (Agung S,2008)

Sistem keamanan lainnya adalah WPA (*Wi-Fi Protected Access*), yang menggeser WEP dan menghasilkan keamanan yang lebih baik dari WEP. Implementasi WPA menggunakan 802.1x dan EAP (*Extensible Authentication Protocol*) menghasilkan proses autentikasi pengguna yang relatif lebih aman. Pada proses ini pengguna harus melakukan autentikasi ke sebuah server autentikasi, misalnya RADIUS, sebelum terhubung ke *wireless* LAN atau internet. Pada umumnya proses autentikasi ini menggunakan nama-pengguna dan *password*.

2.3.3 Perangkat *Wireless (Access point)*

Perangkat *wireless* merupakan hal utama yang harus dipersiapkan dalam membuat jaringan *wireless*, seperti *access point*, *access point* merupakan perangkat utama untuk membuat jaringan WLAN *(wirelessLan).* Karena *access*

point merupakan sebuah perangkat jaringan yang terdapat transceiver dan antena untuk transmisi dan menerima sinyal ke dan dari clients remote. Dengan menggunkan *access point*s (AP) clients dari wireless bisa mudah untuk terhubung pada jaringan. karenan Acess point sebuah alat yang dapat menghubungkan alat-alat yang ada dalam suatu jaringan. sedengakan Router dan Acces Point merupakan peralatan jaringan yang mempunyai sistem kerja yang bahu membahu dalam membentuk unit pemancar signal wifi. *Acces Point* berfungsi untuk membentuk *hotspot*, sedangkan Router bekerja dalam mengatur lalu lintas data pada jaringan *wireless*. *access point* juga merupakan pemancar yang dapat menghubungkan komputer-komputer yang koneksi dengan jaringannya untuk dapat menuju jaringan yang lebih besar (internet).

2.3.3.1 *Access point* TP-link TL-WA801ND

Akses Poin merupakan *Repeater Mode* yang befungsi untuk memperluas cakupan dan kekuatan sinyal, dengan Distribusi Layanan Wireless (WDS) teknologi dengan menghubungkan beberapa jalur akses. AP TP-LINK juga mempunyai fitur *Universal Repeater Mode* sehingga AP dan Router tanpa WDS dapat kompatibel. Pengguna dapat menggunakan fitur ini dalam membangun jaringan wireless yang lebih luas dan lebih banyak pengguna, seperti kafe, perkantoran, dan hotel.

Access point Tp-link merupakan perangkat *wireless* yang yang mempunyai kecepatan mencapai 300Mbps dan menggunkan *Power over Ethernet* yang berfungsi untuk untuk menempatkan sebuah perangkat jaringan (seperti

sebuah AP) di lokasi di mana tidak ada stopkontak listrik tersedia, *Passive Power over Ethernet* merupakan solusi terbaik yang tersedia.

QSS atau *Quick Setup* Keamanan merupakan fitur berguna di TL-WA801ND dengan cara menekan tombol QSS pada access point maka secara otomatis TP-link akan membentuk sambungan yang aman dan dapat melindungi jaringan. TP-LINK TL-WA801ND diadopsi secara luas dengan menggunakan teknologi PoE Pasif dalam suatu industri karena memberikan solusi untuk lebih menghemat biaya.

Adapun spesifikasi *access point* Tp-link TL-WA801ND sebagai berikut :

- Kecepatan nirkabel hingga 300Mbps, ideal untuk video streaming, game online
- Mendukung mode operasi: Access Point, Client, Universal / WDS *Repeater, Wireless Bridge*
- Kemudahan setup enkripsi keamanan WPA dengan menekan tombol QSS
- Kemampuan *Power over* Ethernet sampai 30 meter di atas untuk penyebaran fleksibel

2.4 Penelitian Sebelumnya

Penelitian sebelumnya dilakukan oleh (Yesi Novaria Kunang & Ilman Zuhri Yadi, 2008) yang berjudul “Autentikasi Pengguna *Wireless* Lan Berbasis Radius Server” (Studi Kasus WLAN Universitas Bina Darma) pada jurnal ini menjelaskan tentang bangaimana sitem kerja Server Radius yang berfokus pada

tiga aspek dalam mengontrol akses *user*, yaitu autentikasi, autorisasi dan pencatatan.

Penelitan selanjutnya dilakukan oleh (Gesit Singgih Febyatmoko, Taufiq Hidayat, Mukhammad Andri S, 2006) dengan penelitannya yang berjudul "Sistem Otentikasi, Otorisasi, Dan Pelaporan Koneksi *User* Pada Jaringan *Wireless* Menggunakan Chillispotdan Server Radius". yang menjelaskan tentang Penerapan sistem otentikasi dan otorisasi koneksi *user* dengan menggunakan Chillispot dan server Radius memberikan level keamanan jaringan komputer *wireless* yang lebih baik.

BAB III

TINJAUAN OBJEK PENELITIAN

3.1 Gambaran Umum SMA Negeri 2 Prabumulih

SMA Negeri 2 Prabumulih, merupakan salah satu sekolah menengah atas Negeri yang ada di Provinsi Sumatera Selatan, Indonesia. SMA Negri 2 Prabumulih sama dengan SMA pada umumnya yang ada di Indonesia, masa pendidikan sekolah di SMA Negeri 2 Prabumulih ditempuh dalam waktu tiga tahun pelajaran, mulai dari Kelas X (sepuluh) sampai Kelas XII (dua belas).

Sekolah SMA Negeri 2 Prabumulih merupakan sekolah yang Terakreditasi A No. Sertifikasi Ma 007824 Tahun 2010 yang beralamatkan di : Jl Basuki Rahmat Km 4,5 Kel. Tj. Raman Prabumulih Selatan, saat ini SMA Negeri 2 Prabumulih di pimpin oleh Dra. Hj Tin Martini.

Tabel 3.1 Kondisi siswa (3 tahun terakhir) di SMA Negeri 2 Prabumulih

Tahun Pelajaran	Jumlah siswa				Rasio siswa baru
	Kelas 1	Kelas 2	Kelas 3	Jumlah	
2008/2009	223	218	271	712	1 : 3
2009/2010	218	221	216	655	1 : 3
2010/2011	201	216	216	633	1 : 3
2011/2012	189	201	214	604	1 : 3

(Sumber: Staf SMA Negeri 2 Prabumulih)

Tabel 3.2 Kondisi guru saat ini di SMA Negeri 2 Prabumulih

Ijazah tertinggi	Jumlah	
	GT	GTT
S3/S2 S1 D3 D2/D1/SMA	6 63 2 -	- 5 1 -
Jumlah	71	6

(Sumber: Staf SMA Negeri 2 Prabumulih)

3.2 Visi dan Misi SMA Negeri 2 Prabumulih

3.2.1 Visi SMA Negeri 2 Prabumulih

Unggul dalam Prestasi Berwawasan Lingkungan, Berkarakter Bangsa, dan Mampu Bersaing di Era Globalisasi

3.2.2 Misi SMA Negeri 2 Prabumulih

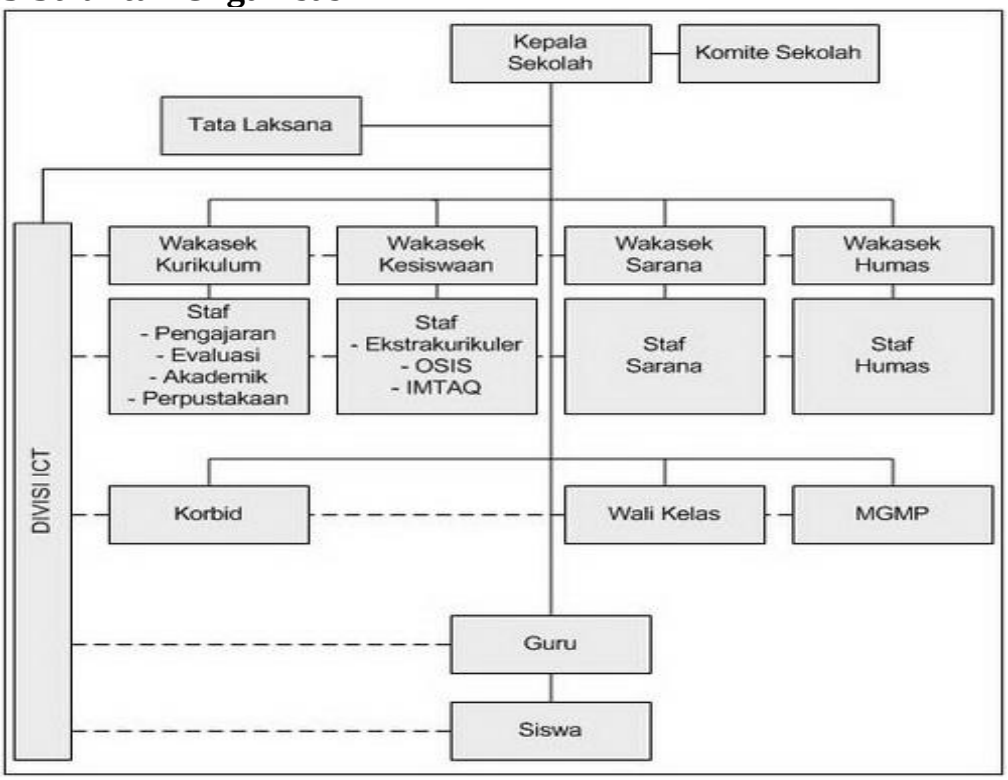
1. Mengoptimalkan Pembelajaran yang Efektif dan Efisien
2. Mengoptimalkan Masuk Perguruan Tinggi Negeri
3. Mengoptimalkan Nilai UN dan US
4. Mengoptimalkan Masuk Perguruan Tinggi Negeri
5. Menjalin Kerja Sama dengan Institusi Terkait
6. Menumbuhkembangkan Program IMTAQ
7. Membekali Siswa dengan IPTEK
8. Membekali Siswa dengan Bahasa Internasional
9. Menegakan Disiplin Tinggi

3.2.3 Tujuan SMA Negeri 2 Prabumulih

1. Mempersiapkan peserta didik yang bertakwa kepada Allah Tuhan Yang Maha Esa dan berakhlak mulia.

2. Mempersiapkan peserta didik agar menjadi manusia yang berkepribadian, cerdas, berkualitas dan berprestasi dalam bidang olahraga dan seni.
3. Membekali peserta didik agar memiliki keterampilan teknologi informasi dan komunikasi serta mampu mengembangkan diri secara mandiri.
4. Menanamkan peserta didik sikap ulet dan gigih dalam berkompetisi, beradaptasi dengan lingkungan dan mengembangkan sikap sportivitas.
5. Membekali peserta didik dengan ilmu pengetahuan dan teknologi agar mampu bersaing dan melanjutkan ke jenjang pendidikan yang lebih tinggi.

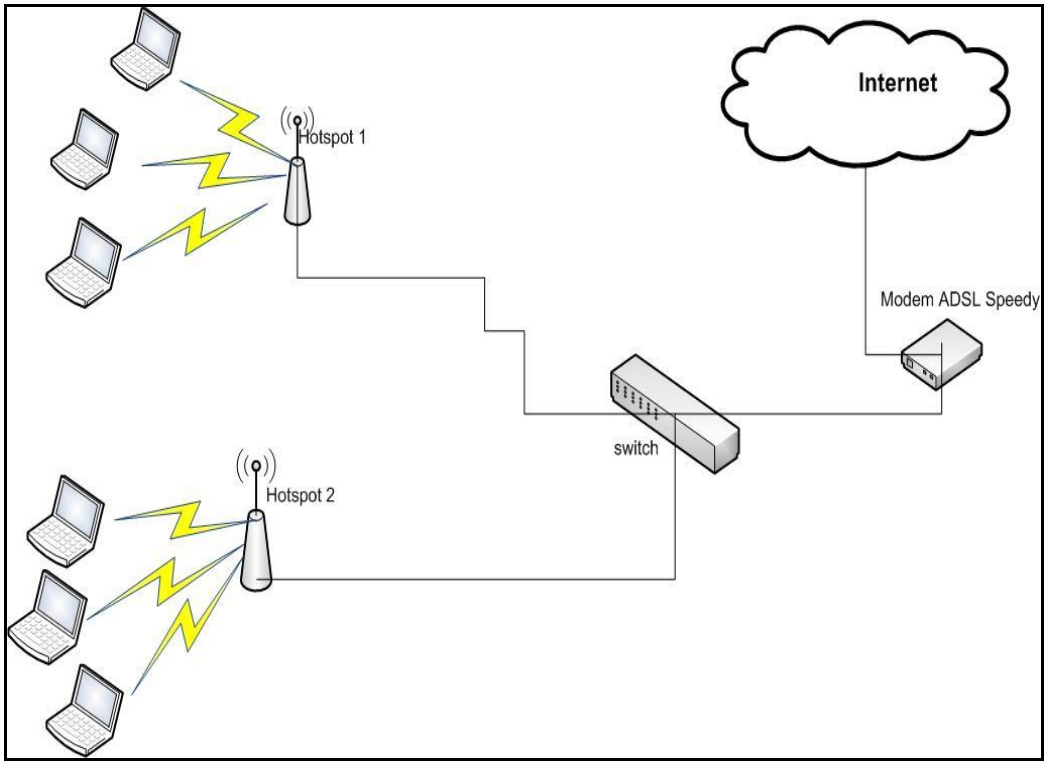
3.3 Struktur Organisasi



Gambar 3.1. Struktur organisasi SMA Negeri 2 Prabumulih
(Sumber : http://www.sman2pbm.sch.id)

3.4 Sistem yang Sedang Berjalan di SMA Negeri 2 Prabumulih

SMA Negeri 2 Prabumulih merupakan salah satu SMA yang hendak menggunakan teknologi informasi dan komunikasi dalam sarana Pendidikan di SMA Negeri 2 Prabumulih. dengan menggunakan layanan Telkom Speedy, SMA Negeri 2 Prabumulih membuat jaringan *wireless hotspot* untuk dapat diakses oleh para guru/staf maupun siswa-siswi.



Gambar 3.2 Skema jaringan *wireless* SMA Negeri 2 Prabumulih

Ket :

Modem yang digunakan pada jaringan ini yaitu Modem Adsl Telkom Speedy 2 Mbps, dimana modem tersebut terhubung dengan sebuah Switch (tanpa ada server autentikasi, autorisasi), dan mempunyai 2 buah access point TP_Link yang bisa di akses oleh pada user yang ada di SMA Negeri 2 Prabumulih.

Dari skema jaringan diatas bahwa pada jaringan wireles yang sedang berjalan saat ini tidak begitu menjamin kaamanan, kemudahan baik dari pengguna maupun administrator jaringan, karna administrator tidak mempunyai media untuk memantau serta mengontrol user disaat terkoneksi kejaringan, tentunya siapapun yang mengetahui password key jaringan, baik itu User SMA Negeri 2 Prabumulih maupun bukan bisa mengakses dan bergabung dengan user-user yang lainnya.

BAB IV

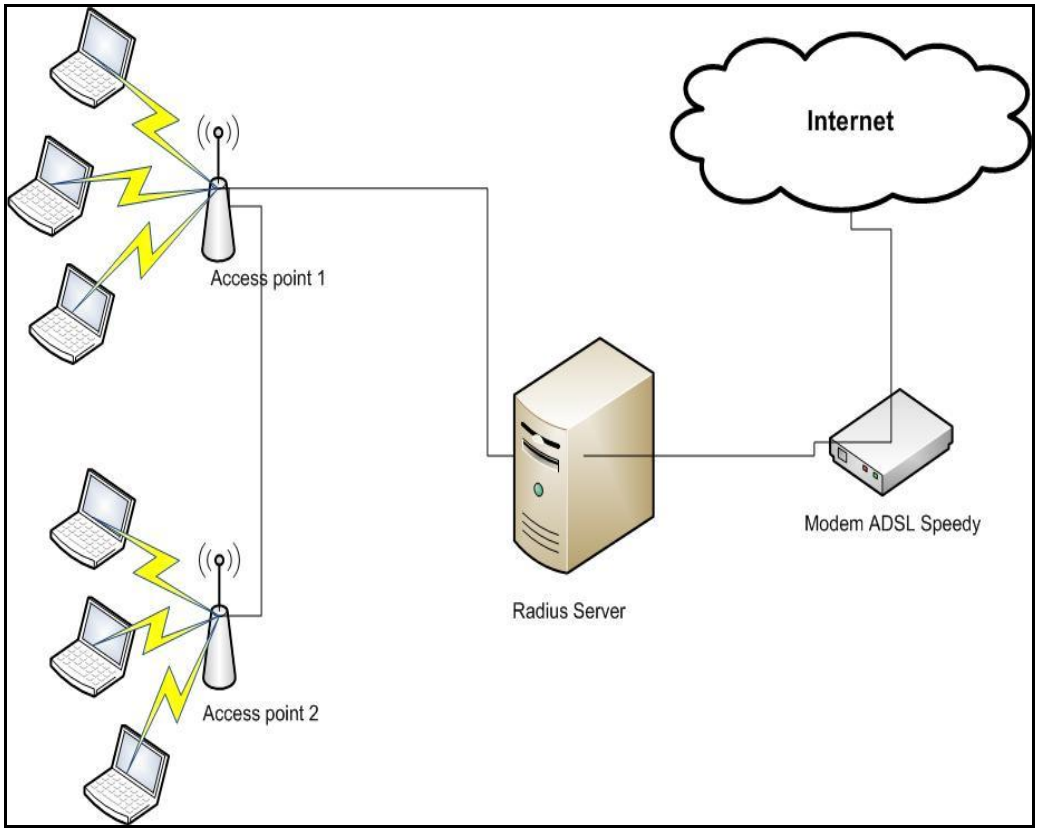
ANALISIS DAN PERANCANGAN

Untuk mendukung penelitian ini diperlukan metode penelitian, dalam Bab ini akan dijelaskan tahap-tahap dari metode penelitian yang digunakan, adapun metode yang digunakan pada penelitian ini adalah *Action Research* menurut Davison, Martinsons, dan Kock (2004) yaitu penelitian tindakan yang mendeskripsikan, menginterpretasi dan menjelaskan suatu situasi sosial atau pada waktu bersamaan dengan melakukan perubahan atau *interversi* dengan tujuan perbaikan atau partisipasi. Adapun tahapan penelitian yang merupakan bagian dari *action research* ini, yaitu :

4.1 Action Planning

Pada tahapan ini merupakan tahap untuk memahami pokok permasalahan dan menyusun rencana tindakan yang tepat untuk dapat meyelesaikan masalah yang ada.

4.1.1 Rancangan Topologi Autentikasi Berbasis Radius Server



Gambar 4.1 Topologi penerapan radius server

Sistem yang akan di uji cobakan di SMA Negeri 2 Prabumulih adalah dengan penerapan Autentikasi Pengguna *Wireless* (*Hotspot*) yang berbasis radius server, yang mana pada sistem diatas akan bangun sebuah server Radius, pada server radius tersebut akan diinstall dengan sistem operasi Ubuntu 10.04 dan juga paket-paket pendukung untuk pembuatan autentikasi dari pengguna jaringan *wireless (hotspot),* seperti : Freeradius mysql, mysql server, apache php, phpmyadmin, paket chilispot, serta paket-paket pendukung lainnya. sehingga setiap *user* yang hendak mengakses jaringan *wireless (hotspot)* dengan *Browser* pada perangkat *wireless user*, maka seorang *user* terlebih dahulu akan dihadapkan dengan *Hotspot login (Captive Portal*) yang telah dibuat pada server radius, pada *Captive Portal* ini seorang *user* akan diminta identitas, seperti *username* dan

password, untuk dapat dicocokkan dengan identitas yang telah dimasukan pada server Radius pada waktu sebelumnya, apabila identitas tersebut terdapat pada server Radius dan identitas yang dimasukan benar maka *user* langsung dapat mengakses internet dengan menggunakan jaringan *wireless (hotspot)* tersebut.

Untuk Chilispot sendiri pada sistem yang akan dibangun ini chilispotnya akan diinstall pada server dan dikonfigurasi pada server, sehingga server yang akan memberi IP *(Internet Protocol)* pada *user* yang sudah melakukan autentikasi dengan benar, untuk konfigurasi pada *access point* ini menggunakan DHCP.

Penerapan sistem ini bertujuan untuk memberikan apa yang dibutuhkan oleh *user* maupun administrator. Untuk *user* sistem ini tentunya akan memudahkan serta memberikan keamanan terhadap *user* yang melakukan koneksi (berinternet) pada jaringan *wireless*, karena pada sistem dengan radius server maka semua identitas *user* akan di *insert* pada database yang ada pada server radius, dan untuk sistem yang tidak dengan server radius, seorang *user* harus selalu meminta *network key* pada administrator jaringan apabila ingin berpindah pada area atau mengakses akses point yang lainnya. Sedangkan untuk kebutuhan *Administrator* tentuntanya dapat memudahkan administrator untuk memanajemen jaringan.

4.1.2 Spesifikasi Sistem *RADIUS Server*

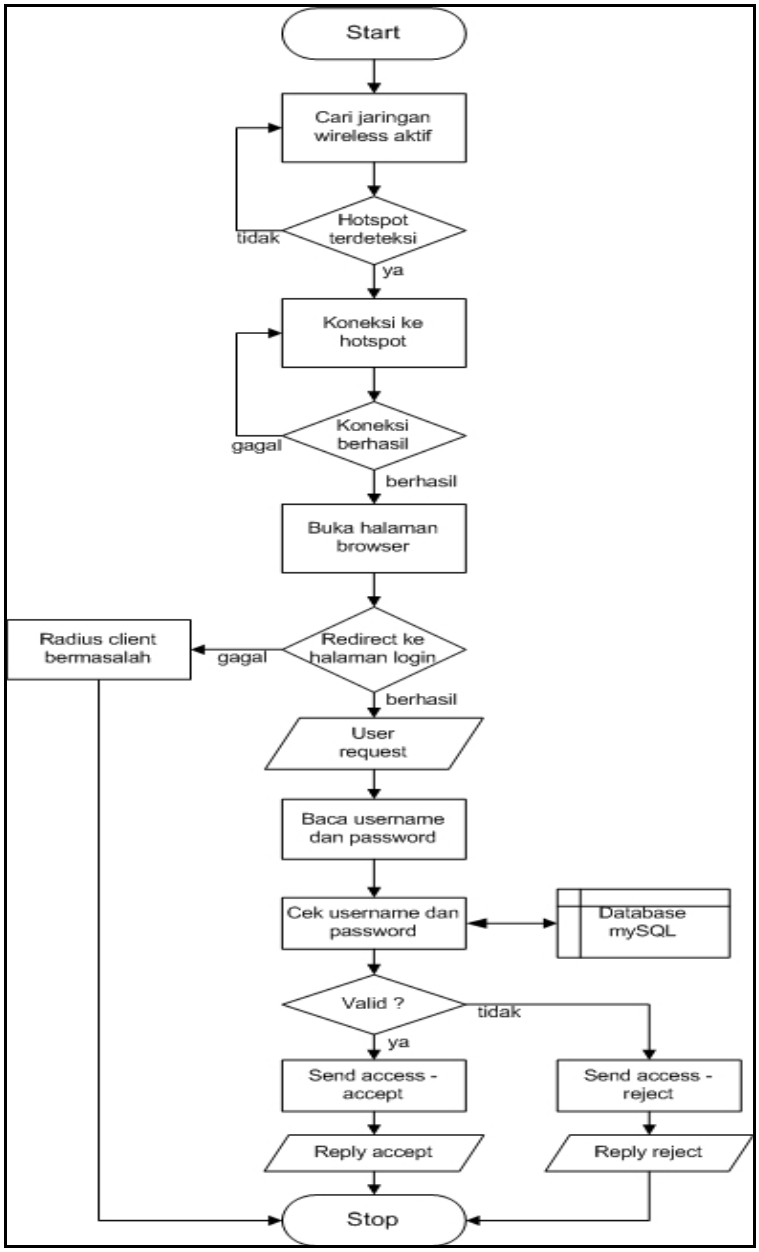
Untuk dapat membuat autentikasi dari pengguna jaringan *wireless (hotspot)* dengan berbasis radius server, terlebih dahulu perlu mempersiapkan perangkat-perangkat pendukung, baik perangkat lunak maupun perangkat keras, yang perangkat tersebut seperti pada tabel dibawah ini .

Tabel 4.1 Spesifikasi *RADIUS* Server

Keterangan	Spesifikasi
Perangkat Lunak OS Server Aplikasi Pendukung	1) Ubuntu 10.04 2) FreeRadius 3) MySql-Server 4) Apache2 php5-mysql 5) Phpmyadmin 6) Paket Chilispot
Perangkat Keras :	
CPU	*7)* Pentium Dual Core
Memory	*8)* 1 GB
Hard Disk	9) 500 GB
Access Point	10) TP-Link
	11) LAN *Card* TP-Link
Kabel	12) UTP (RJ45)

Perangkat lunak yang di install pada server radius agar dapat mendukung sistem yang akan dibangun serta diharapkan dapat membuat autentikasi *user* pada jaringan *wireless*, dapat melakukan autorisasi pada *user* yang terautentikasi dengan baik, dan mampu menyimpan dan memberikan laporan tentang aktivitas yang dilakukan *user* pada jaringan wireless.

4.1.3 Mekanisme Auntentikasi *User*



Gambar 4.2 Mekanisme Autentikasi *User*

Ket :

Setiap *user* yang yang masuk pada jaringan wireless (*hotspot*) dan mencoba untuk browsing internet, sebelumnya akan diredirect ke login *username* dan *password* yang dibuat chiliSpot. Ketika *username* dan *password* telah dimasukkan maka ChilliSpot akan menanyakan ke FreeRADIUS apakah ada *username* dan

password yang dimasukkan oleh *user* sesuai dengan yang ada pada *database*, kemudian FreeRADIUS akan mencocokkan *username* dan *password* yang dimasukkan melalui database yang dibuat di MySQL. Jika ada, FreeRADIUS akan melaporkan kepada ChilliSpot dan ChilliSpot akan memberikan izin sehingga *user* bisa *surfing* di internet, dan jika tidak, maka si FreeRADIUS akan melaporkan ke ChilliSpot bahwa *username* dan *password* yang dimasukkan tidak ada, ChilliSpot tidak akan membuka akses untuk *surfing* internet, dan akan meminta login ulang dan begitu seterusnya.

4.2 Action Taking

Pada tahapan ini akan dijelaskan tentang mengimplementasikan rencana tindakan dengan harapan dapat menyelesaikan masalah.

4.2.1 Proses Instalasi *RADIUS Server Hotspot (Captive Portal)*

Pada bagian ini akan dijelaskan tentang proses autentikasi pengguna *wireless (hotspot)* dengan berbasis radius server. Dalam membuat autentikasi tentunya memerlukan tahap-tahap installasi yang harus dilalui terlebih dahulu, yang mana akan dijelaskan dibawah ini.

RADIUS server bertugas untuk menangani *AAA (Authentication, Authorization, Accounting)*. Yang pada intinya radiusserver bisa menangani autentikasi *user*, autorisasi untuk servis, dan juga penghitungan nilai servis yang digunakan oleh *user*. *RADIUS server* juga merupakan proses pengesahan identitas pengguna (*end user*) untuk mengakses jaringan. pada awalnya seorang *user* akan mengirim kode seperti *username* dan *password* yang ditujukan pada server.

Kemudian server akan menerima kode tersebut dan mencocokan kode (identitas) yang dikirim tersebut dengan identitas yang ada pada *databese* server radius, yang mana identitas tersebut merupakan identitas yang yang dimasukan pada *database* diwaktu sebelumnya. Jika identitas yang dimasukan tadi benar dan cocok dengan identitas yang ada pada *database* maka server kan memberikan hak akses kepada *user* jaringan, namun jika identitas yang dimasukan salah dan tidak terdapat pada *database*, maka server akan meminta agar *user* dapat memasukan identitas dengan benar dan sesuai dengan identitas pada *database*. *Captive Portal* adalah suatu teknik autentikasi dan pengamanan data yang lewat dari *network* internal ke *network* eksternal. Biasanya *Captive Portal* ini digunakan pada infrastruktur *wireless* seperti *hotspot* area, tapi tidak menutup kemungkinan diterapkan pada jaringan kabel. Proses pembuatan *RADIUS Hotspot server* ini, maka yang perlu dilakukan instalasi berikut:

1. Install *Linux Ubuntu* 10.04 *desktop,* yang mana berfungsi sebagai Sistem Operasi untuk Radius Server
2. Install *Fakeroot ssh build-essential rrdtool snmp.* Merupakan paket-paket pendukung untuk membuat Radius Server
3. Install *FreeRADIUS,* Merupakan paket-paket pendukung untuk membuat Radius Server
4. Install *FreeRadius*-mysql, Merupakan paket-paket pendukung untuk membuat Radius Server.
5. Install *Mysql-server,* Merupakan paket-paket pendukung untuk membuat Radius Server

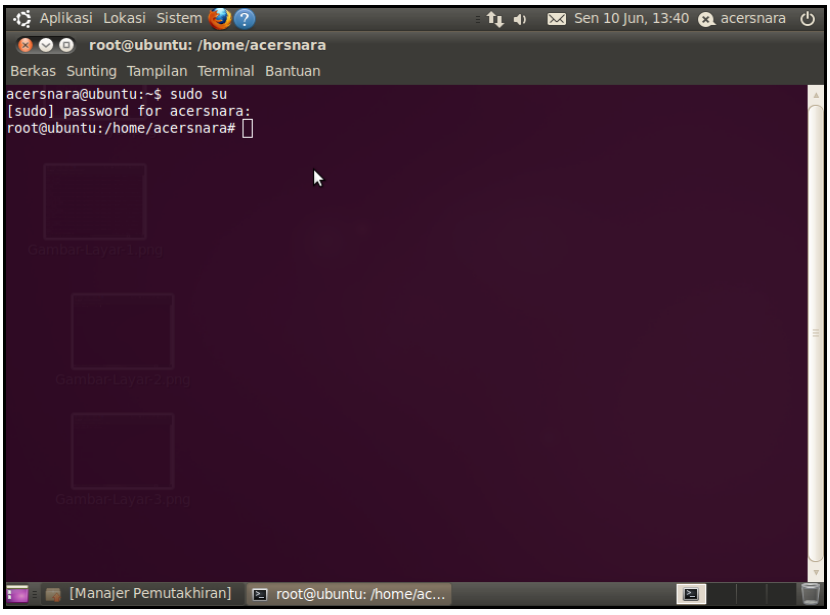
6. Install *Phpmyadmin*, Merupakan paket-paket pendukung untuk membuat Radius Server
7. Install paket *chillispot*_1.0_i386.deb, Merupakan paket-paket pendukung untuk membuat Radius Server
8. Install *Dialup Admin*, Merupakan paket-paket pendukung untuk membuat Radius Server

4.2.2 Proses Konfigurasi

4.2.2.1 Konfigurasi *Freeradius* di *Radius Server Hotspot*

Konfigurasi pada Freeradius di *Radius Server Hotspot* dilakukan berdasarkan langkah berikut :

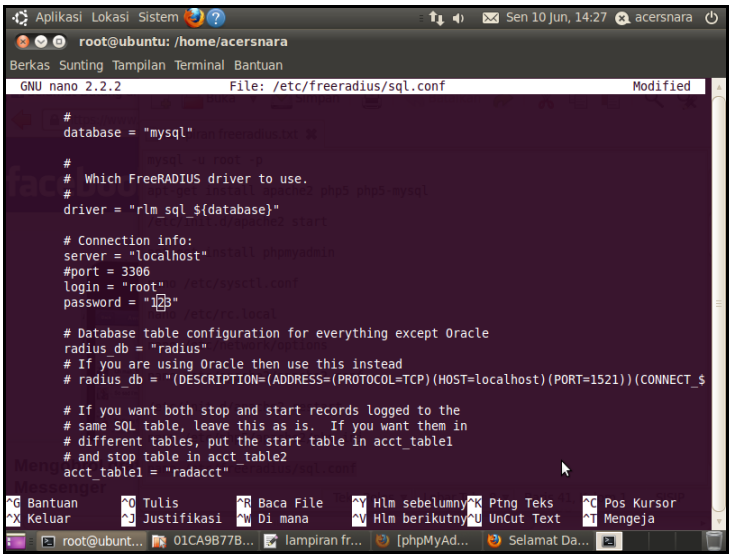
1. Buka terminal di *radius server hotspot* dan *login* sebagai *root*



Gambar 4.3 *Login* sebagai *Root*

Login sebagai *root* untuk melakukan modifikasi *FreeRadius* untuk mengaktifkan *radius server hotspot*.

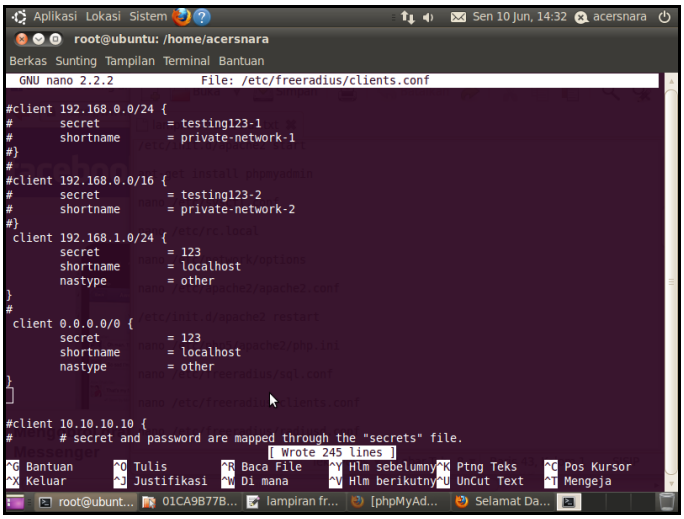
2. Ketik perintah `nano /etc/freeradius/sql.conf`



Gambar 4.4 *Setting freeradius/sql.conf*

Melakukan konfigurasi pada */freeradius/sql.conf*, dimana disini dilakukan perubahan sesuai dengan settingan yang akan dipakai pada database server radius.

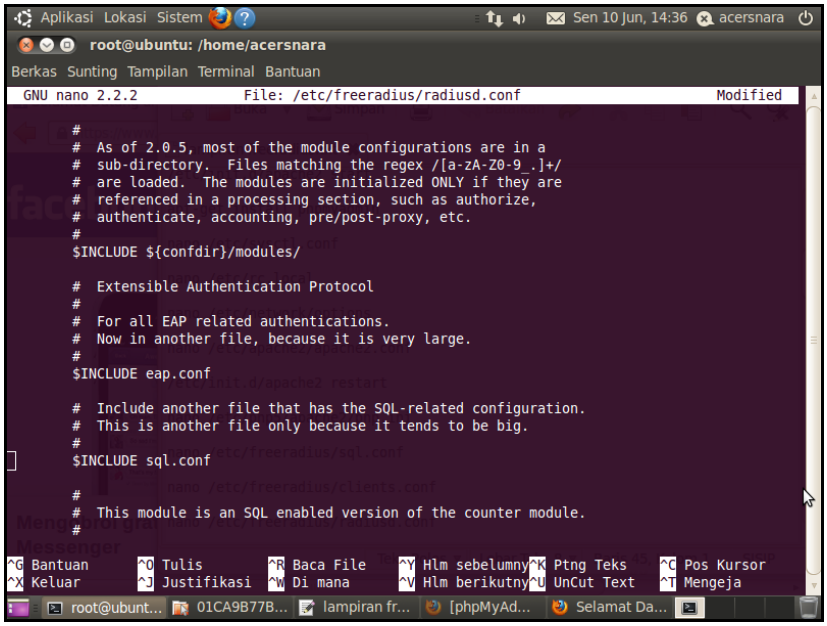
3. *Setting* parameter *client* yang bisa mengakses layanan *radius server hotspot*, ketik perintah `nano /etc/freeradius/client.conf`



Gambar 4.5 *Setting* Parameter *Client*

Melakukan *setting*-an pada *clients.conf* untuk dapat mengatur siapa saja *client* yang bisa mengakses *radius server hotspot*.

4. Ketik perintah `nano /etc/freeradius/radiusd.conf` dan hilangkan tanda # $INCLUDE sql.conf

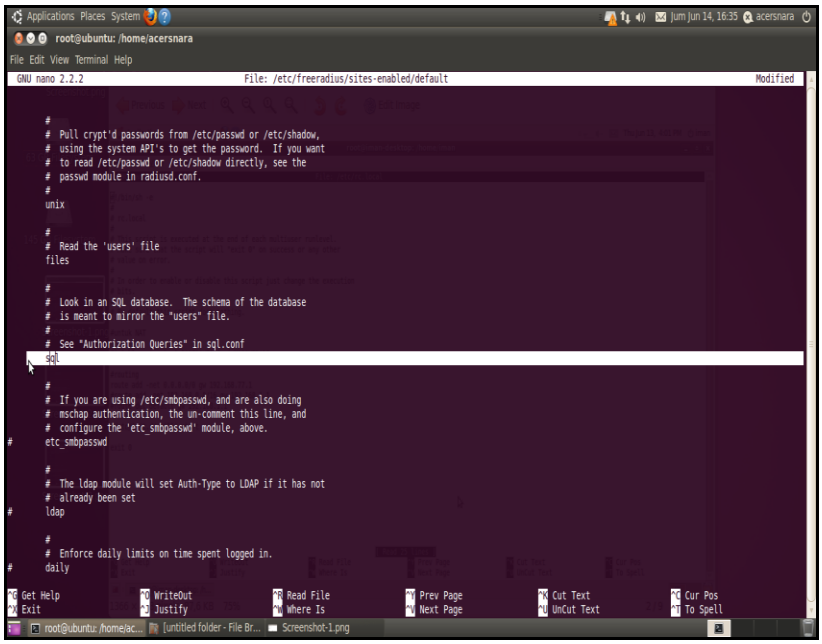


Gambar 4.6 mengaktifkan `radiusd.conf`

5. Jalankan perintah `nano /etc/freeradius/site-enable/default` dan hilangkan tanda # pada

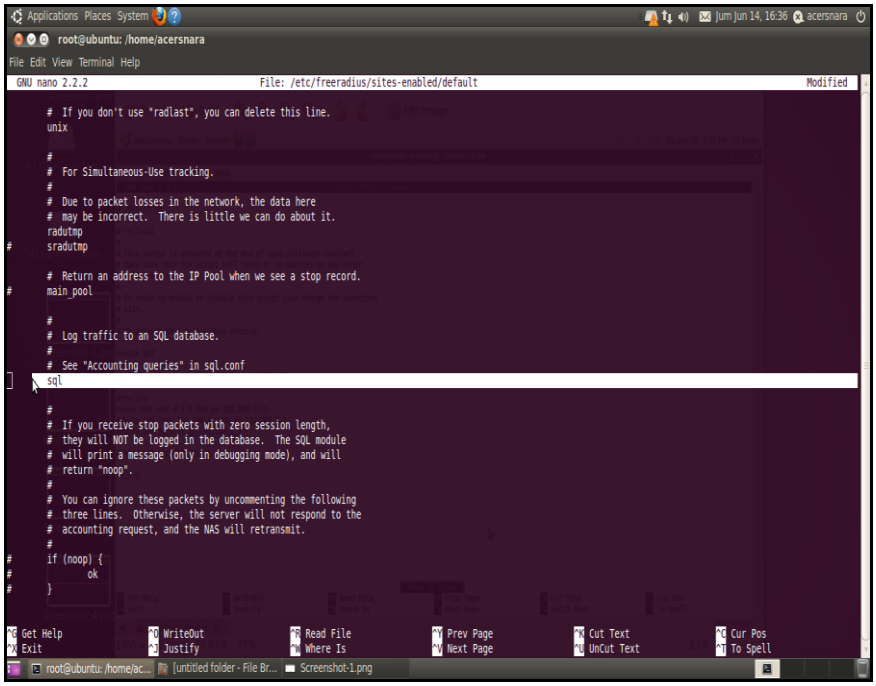
```
See "Authorization Queries" in sql.conf
sql
See "Accounting queries" in sql.conf
sql
See "Simultaneous Use Checking Queries" in sql.conf
Sql
```

Menghilangkan tanda # pada masing-masing perintah `sql` diatas, yang berarti mengaktifkan atau menampilkannya pada server *freeradius*.



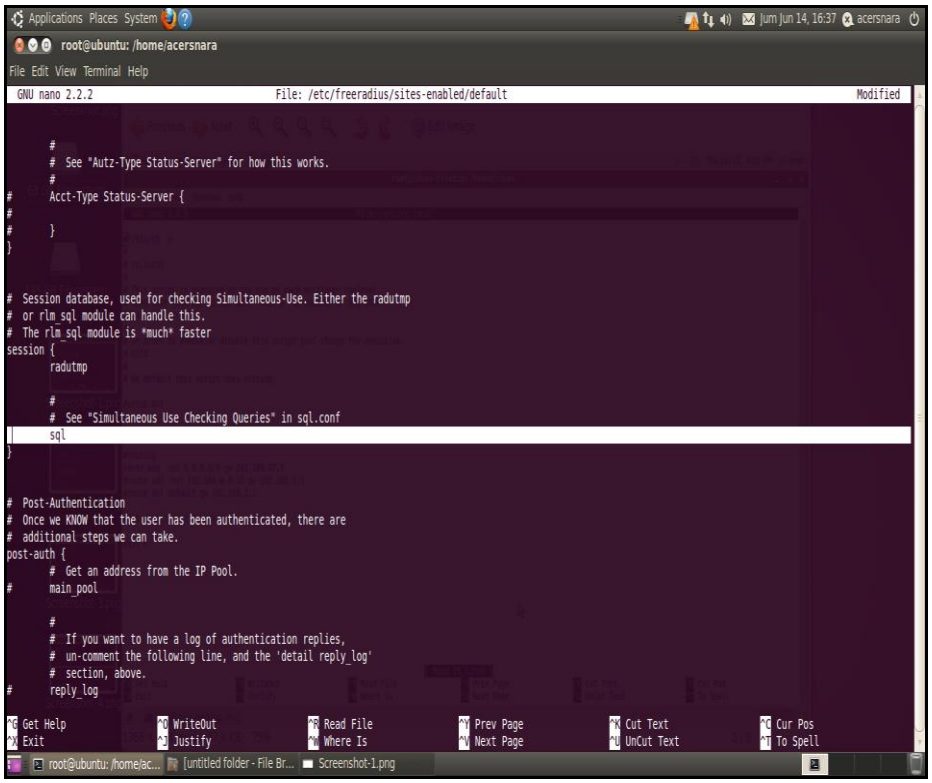
Gambar 4.7 mengaktifkan *Authorization* pada *freeradius*

Menampilakan (mengaktifkan) `Sql` pada `See "Authorization Queries" in sql.conf` di freeradius server



Gambar 4.8 Aktifkan *Acounting* pada *freeradius*

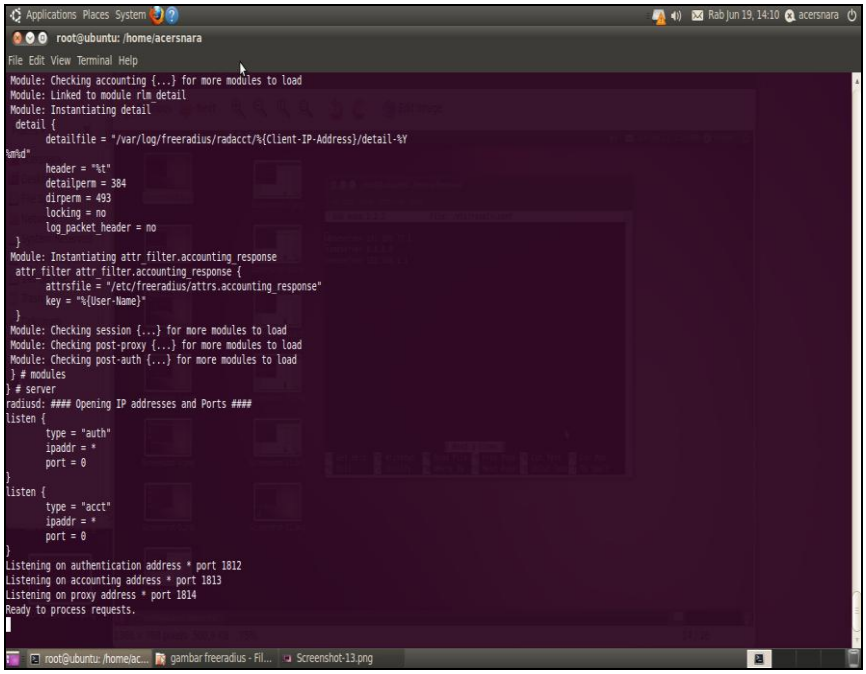
Menampikan (mengaktifkan) dan Sql pada See "Accounting queries" in sql.conf di *freeradius* server.



Gambar 4.9 Aktifkan *simultaneous* pada *freeradius*

Menampilakan (mengaktifkan) Sql pada pada See "Simultaneous Use Checking Queries" in sql.conf di *freeradius* server.

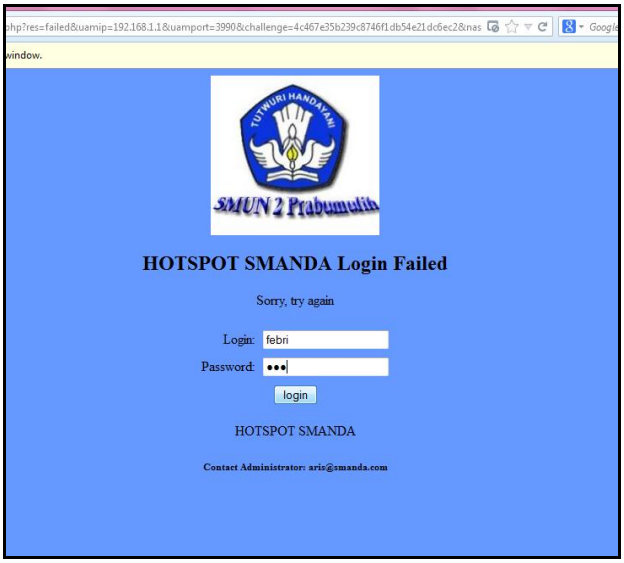
6. Konfigurasi chilispot, konfigurasi ini berfungsi untuk setting Ip *(internet protocol)* yang akan digunkan untuk radiusserver.
7. Kemudian jalankan perintah *freeradius* –X



Gambar 4.10 Cek *Freeradius Running*

Melakukan pengecekan dengan menjalankan perintah *freeradius –X* untuk melihat apakah radiusserver yang dibuat sudah berjalan.

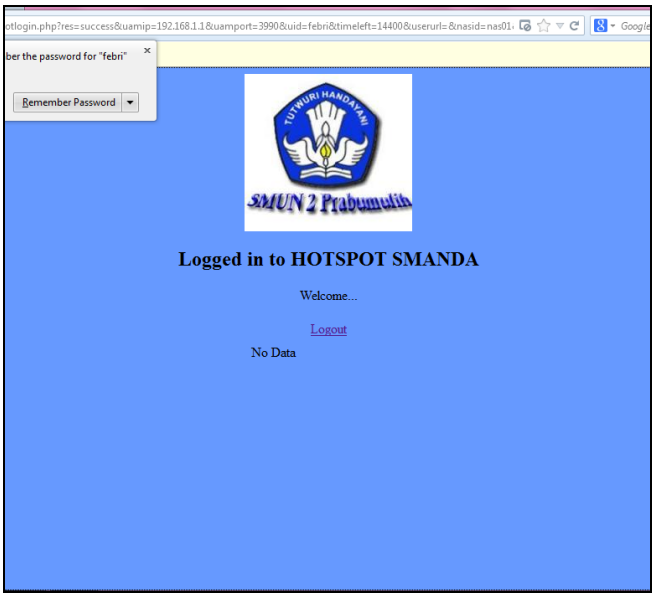
8. Selanjutnya lakukan *login hotspot* dari komputer *client* dengan akun *user* yang telah dibuat pada dialupadmin sebelumnya.



Gambar 4.11 *Login hotspot*

Melakukan *login* dengan menggunakan *username* dan *password* yang telah dibuat pada *dialupadmin* ini merupakan autentikasi.

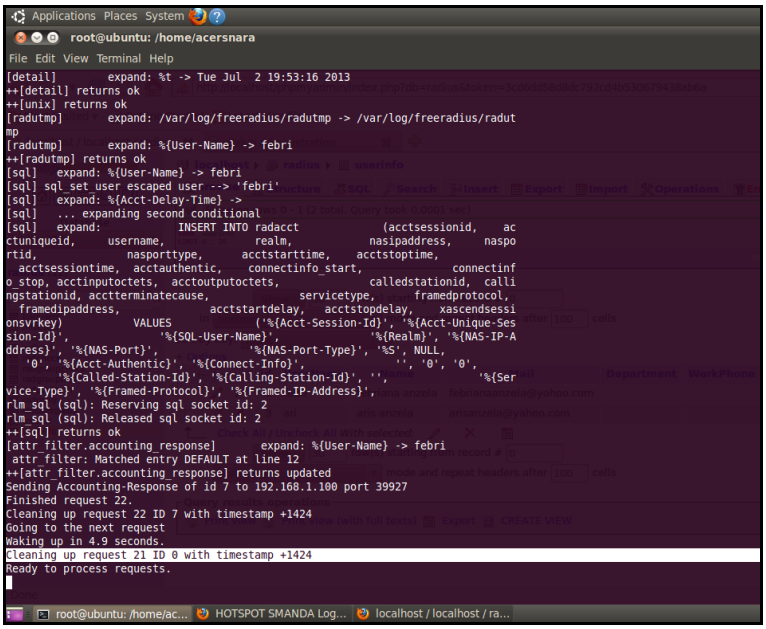
9. *Login* berhasil



Gambar 4.12 *Login* Berhasil di Klien

Username dan *password* yang dibuat di *dialupadmin* berhasil masuk atau *login* di *radius server hotspot*.

10. Jika *login* berhasil maka akan terlihat seperti gambar dibawah ini, pada radius server terdapat laporan, bahwah ada *user* yang m,encoba akses internet, dan *user* telah melalui autentikasi yang di buat server, dan identitas yang dimasukan *user* pun sesuai dengan data yang terdapat pada server.



Gambar 4. 13 *Login* Berhasil di *RADIUS Server*

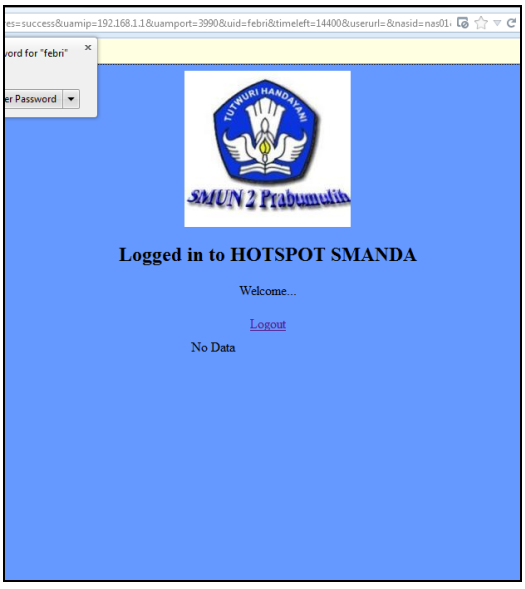
Login yang dilakukan oleh *user* dari komputer client, berhasil terbaca oleh radius server *hotspot* yang menandakan bahwa autentikasi telah berjalan dengan baik.

BAB V

HASIL DAN PEMBAHASAN

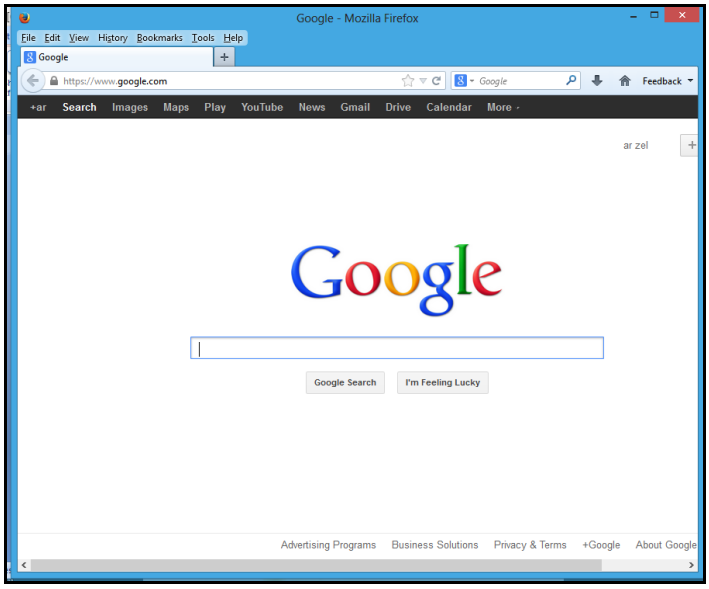
5.1 Hasil

Pada tahapan ini akan dijelaskan mengenai hasil dari implementasi sistem, didalam penerapan autentikasi dengan radius server, hasil yang didapat yaitu *user* yang dapat melakukan *login* dengan benar dan *user*name dan password yang dimasukan sesuai dengan yang ada pada *database*, maka *user* tersebut dapat mengkases internet dengan menggunakkan jaringan *wireless (hotspot).*



Gambar 5.1 berhasil *login*

Pada gambar diatas terlihat bahwa *user* telah melakukan autentikasi dengan benar dan tidak mendapatkan pesan kegagalan, untuk *user* yang sudah melakukan autentikasi dengan benar seperti diatas, *user* tersebut langsung bisa mengakses internet dengan *wireless (hotspot)* dan untuk IP *(Internet Protocol)* yang didpatkan merupakan IP *(Internet Protocol)* yang diberikan server terhadapap *user* yang terkoneksi tersebut.



Gambar 5.2 Terkoneksi ke internet

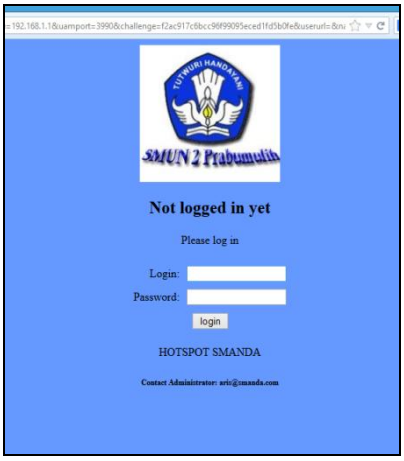
Pada gambar diatas terlihat bahwa *user* yang berhasil melakukan autentikasi dengan benar, *user* tersebut bisa mengakses internet.

5.2 Pembahasan

5.2.1 Ujicoba *login Radius Server*

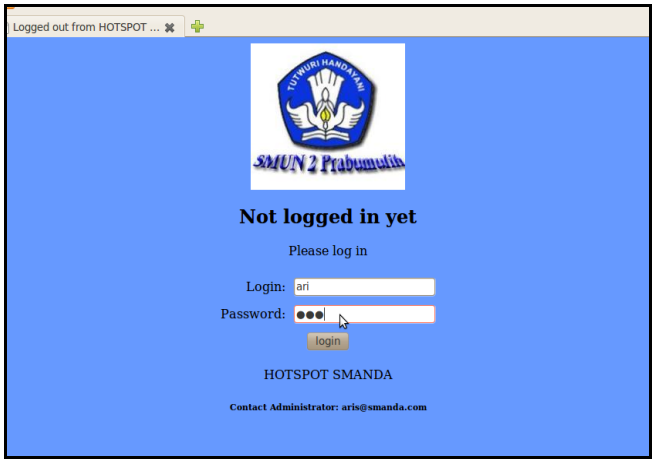
Untuk melakukan ujicoba pada sistem *radius server (freeradius)* telah dibuat *user* pada *database* server, sehingga *user* yang telah di *insert* dapat *login* dan mengakses jaringan *wireless (hotspot)*. Ketika seorang *user* ingin melakukan

koneksi ke internet, *user* tersebut terlebih dahulu akan dihadapkan dengan *hotspotlogin* yang telah dibuat dan dikonfigurasi sebelumnya.



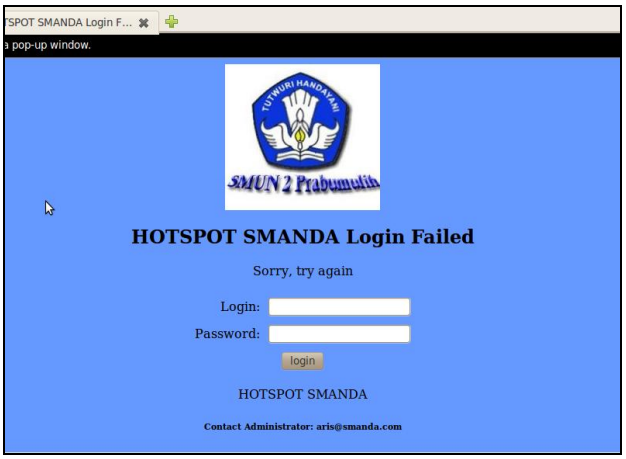
Gambar 5.3 Halaman *Login Hotspot*

Untuk dapat melakukan *login* pada *radius server*, seorang *user* diminta untuk mengisikan *username* dan *password* pada halaman *login hotspot* tersebut.



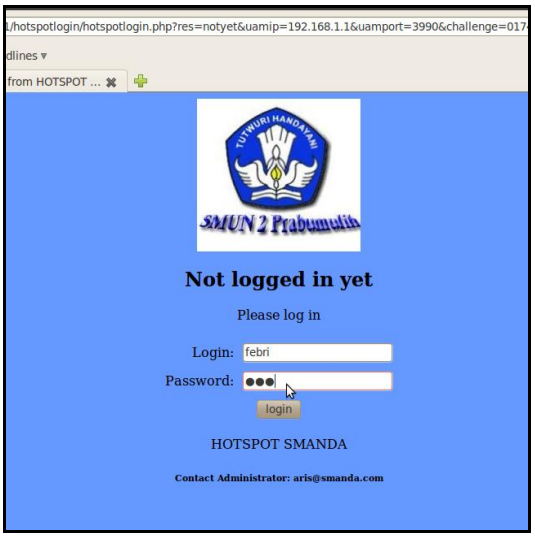
Gambar 5.4 Mencoba untuk *login*

Jika *user* dapat memasukkan *user*name dan *password* sesuai dengan yang terdapat pada *database*, maka *user* dapat mengakses internet, jika salah dan tidak sesuai dengan identitas yang di *insert* pada *database*, maka *user* akan diminta untuk kembali melakukan autentikasi dengan memasukan *user*name dan *password* dengan benar pada halaman *hotspotlogin*.



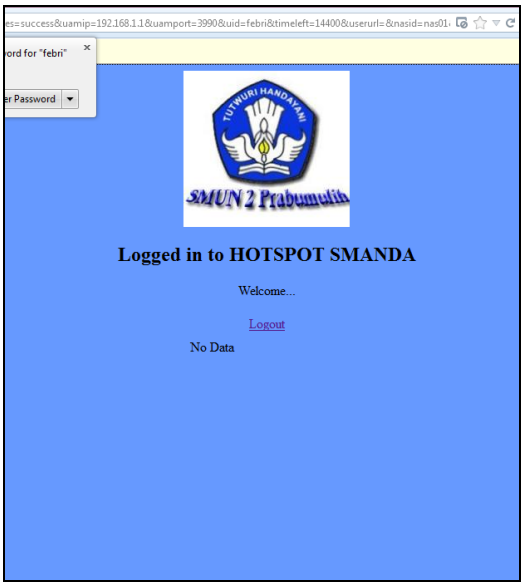
Gambar 5.5 Gagal *Login Hotspot*

User sebaiknya kembali mengisikan *user*name dan *password* yang benar pada saat melakukan autentikasi.



Gambar 5.6 Kembali melakukan autentikasi

Setelah *user* memasukan *user*name dan *password* dengan benar dan identitas yang dimasukan sesuai dengan identitas pada server, maka *user* langsung berinternet pada jaringan *wireless.*



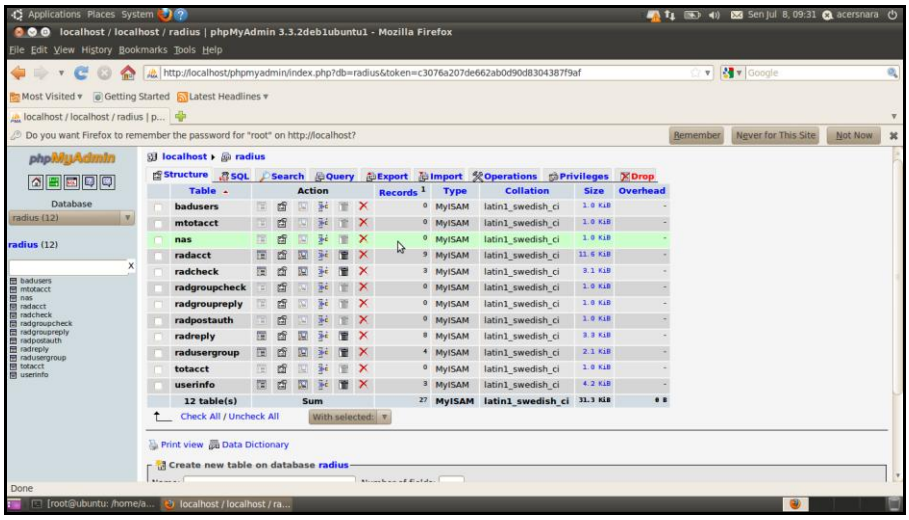
Gambar 5.7 *User* dapat *login* pada jaringan

5.2.2 *Database* pada *Server Radius*

Pada Radius server ini menggunkan *database Phpmyadmin* yang berguna untuk dapat menyimpan tabel-tabel yang ada pada *freeradius* yang nantinya pada tabel tersebut dapat digunakan untuk menyimpan identitas *user* yang diberiwewenang untuk dapat *login* pada jaringan *wireless*. dan juga *PhpMyadmin* dapat berfungsi untuk menambahakan *user*, membagi grup pada *user*, pada server radius. Adapun hal yang harus dilakukan terlebih dahulu adalah bagaimana *login* pada *Phpmyadmin.*

Gambar 5.8 *Login* pada *PhpMyadmin*

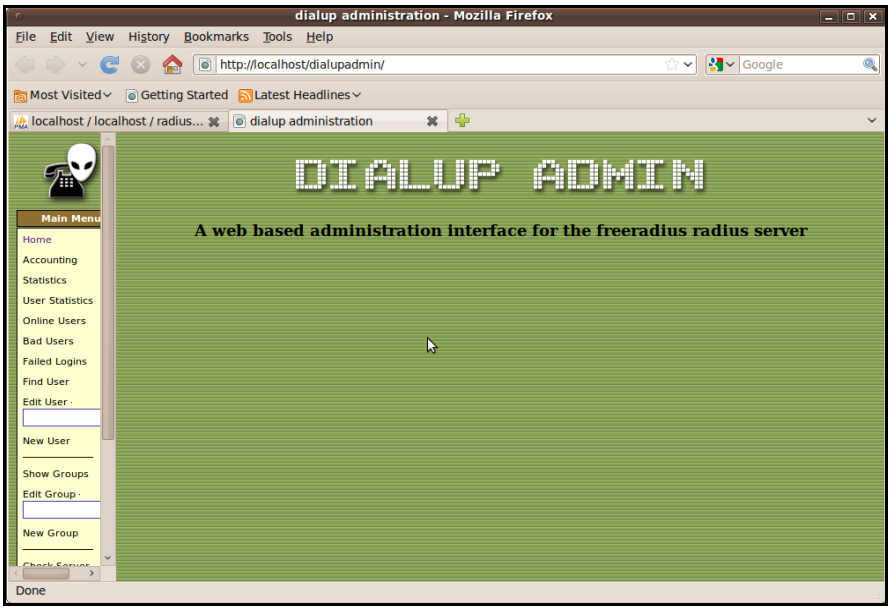
Setelah *login* pada *Phpmyadmin* dengan menggunkan *username* dan *password* yang telah dikonfigurasi sebelumnya. Disini perlu membuat *database* terlebih dahulu, *database* yang dibuat dapat menggunakan nama radius, setelah membuat *database*, perlu melakukan import tabel yang ada pada file *freeradius* untuk mengisi *database*.



Gambar 5.9 Tabel yang ada pada *database* radius

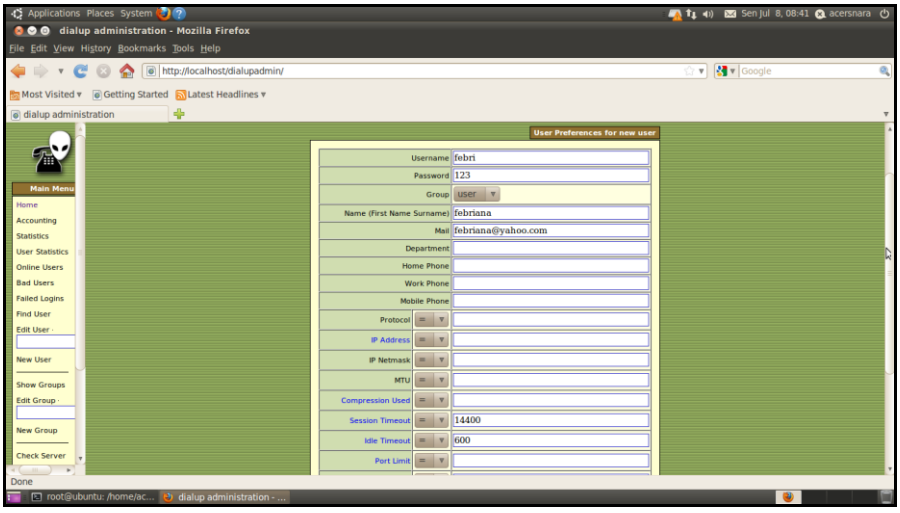
Pada gambar diatas terlihat 12 tabel yang telah di *import* pada *database* radius, tabel ini nantinya mempunyai fungsi masing-masing untuk membuat maupun memberi laporan terhadap *admin* tentang identitas *user*.

Pembuatan *user* dan memasukan seluruh identitas *user* juga dapat dilakukan pada *dialupadmin*, yang juga telah dikonfigurasi pada saat installasi.



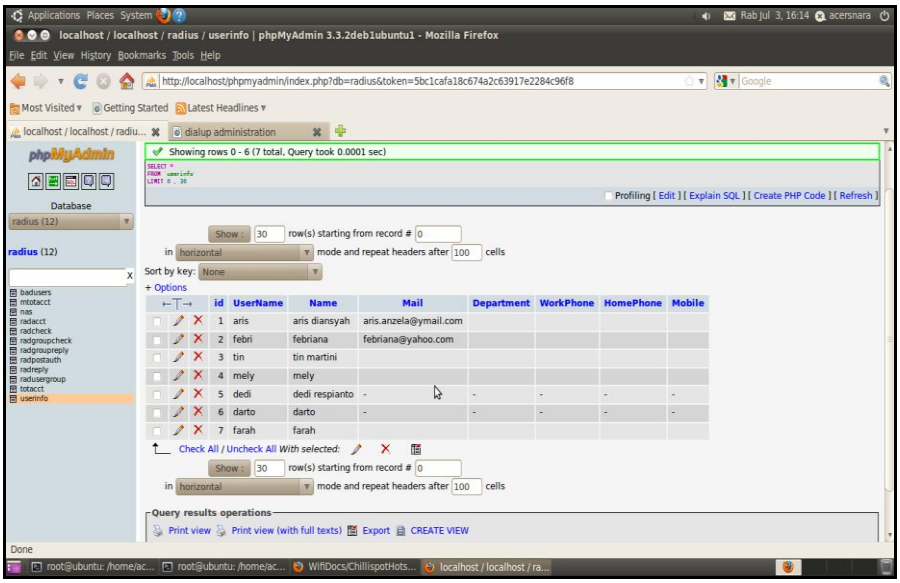
Gambar 5.10 *Home dialupadmin*

Pada *dialupadmin* ini *admin* dapat membuat *user* dan memasukan identitas pada *user* yang di *create* pada dialupadmin ini nantinya akan tersimpan pada *database* radius yang telah dibuat sebelumnya.



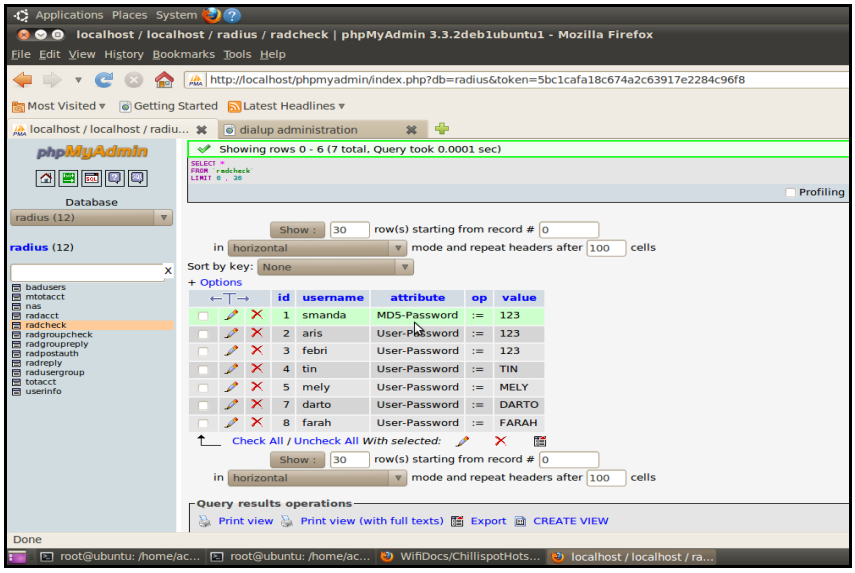
Gambar 5.11 *create user* dengan dialupadmin

Setalah melakukan *create user* maka *user* yang kita masukan tadi, otomatis akan masuk pada *database* radius pada *phpmyadmin.*



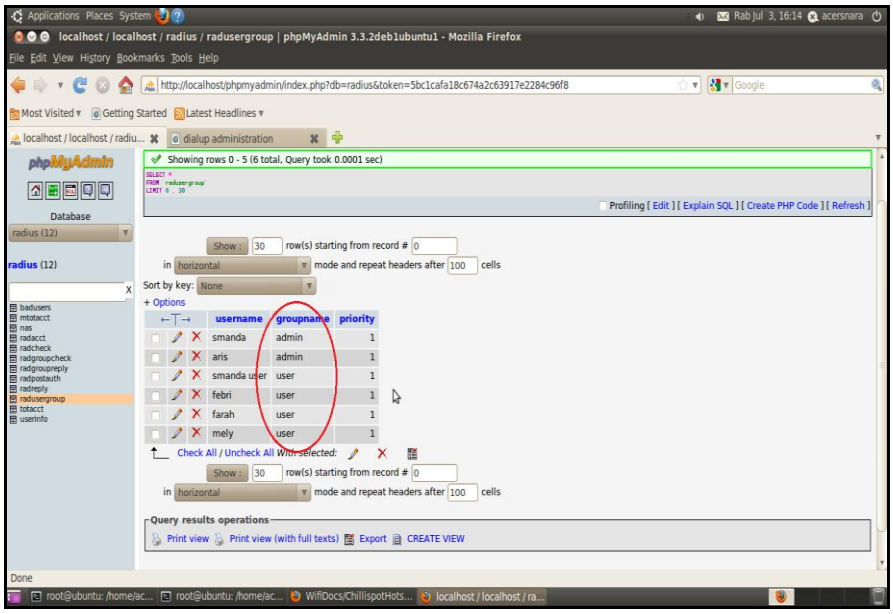
Gambar 5.12 *user*infopada *Phpmyadmin*

Pada gambar diatas terlihat tabel *userinfo*, yang mana diketahui bahwa *user* yang terlihat diatas merupakan *user* yang nantinya dapat melakukan *login* pada *server radius* dan berinternet pada jaringan *wireless (hotspot)*, karena semua identitas telah masukan pada database tersebut, untuk mengecek passwor pada *user* dapat dilihat pada tabel *radchek*



Gambar 5.13 Cek *Password* pada *Radchek Database*

Adapun pembuatan *user* dapat dibagi, dan dimasukan sesuai dengan kriterianya masing-masing seperti yang terlihat pada gambar dibawah ini bahwa pada database radius dibuat 2 kriteria dari *user* yang akan dibuat, yaitu antara client dan server.



Gambar 5.14 *Redusergroup* pada *database*

Gambar diatas menujukan bahwa *user* yang telah berhasil di *create* administrator dengan *dialupadmin* dapat tersimpan pada *database* radius, dan *user* terbagi atas 2 kriteria antara client dan admin. *User* yang telah terdaftar pada database tersebut, apabila bisa melakukan autentikasi dengan benar maka bisa berinternet dengan jaringan *wireless.*

5.3 *Learning*

Pada tahap ini kita melakukan *review* tahapan-tahapan yang telah berakhir dan mempelajari kriteria dalam prinsip pembelajaran.

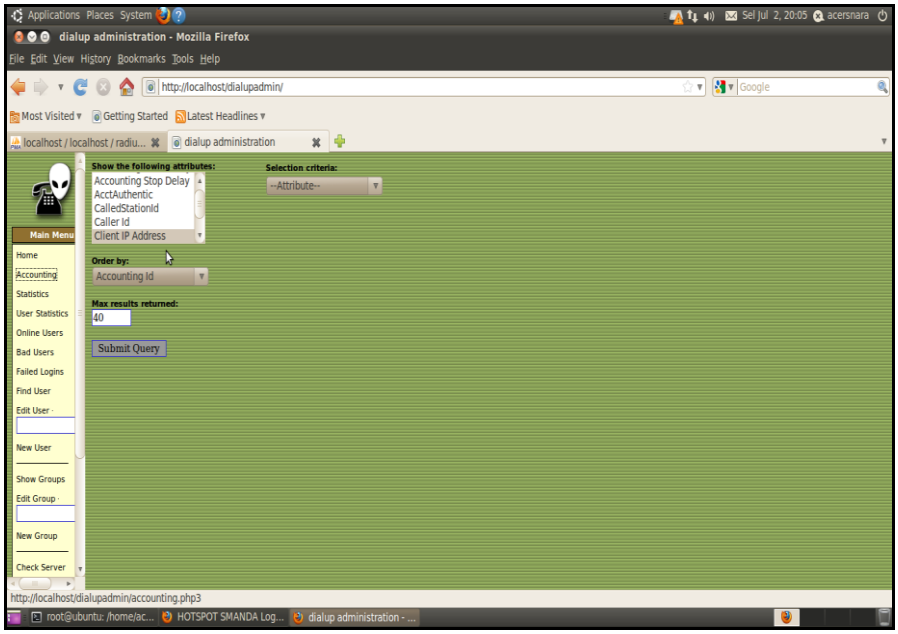
5.3.1 Kelebihan sistem

Dengan Radius server ini memiliki beberapa kelebihan yaitu :

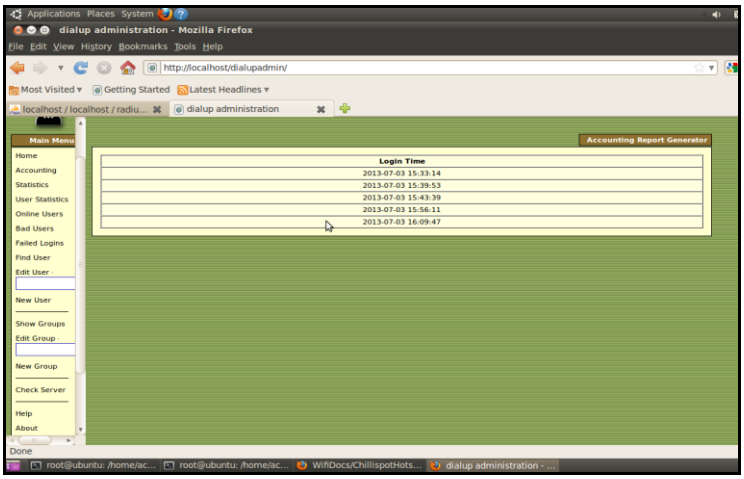
1. Dapat menjalankan sistem administrasi terpusat.
2. Protokol *connectionless* berbasis UDP yang tidak menggunakan koneksi langsung.
3. Mendukung autentikasi *Password Authentication Protocol* (PAP) dan *Challenge Handshake Authentication Protocol* (CHAP) *Password* melalui PPP.

5.3.2 Pelaporan *user*

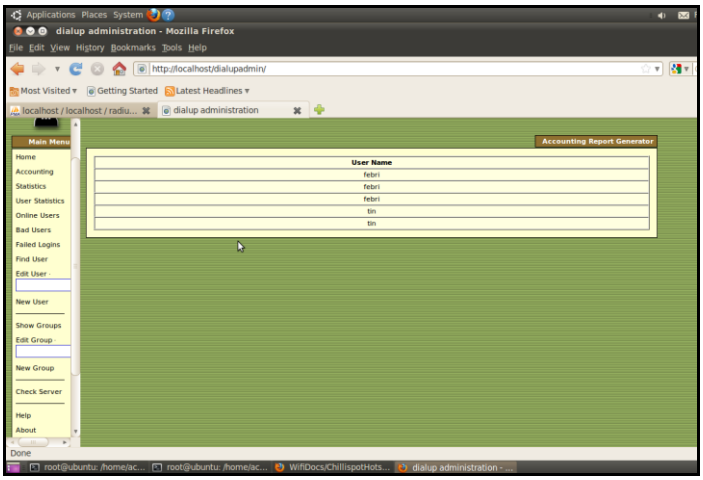
Berikut ini merupakan hasil pelaporan dari *user* yang *login* dan jaringan wireless, pelporan ini dapat dilihat dari dialupadmin dan dilihat dari macam-macam kriteria. Dari laporan tersebut terlihat *user* yang sedang maupun sudah *login* pada jaringan.



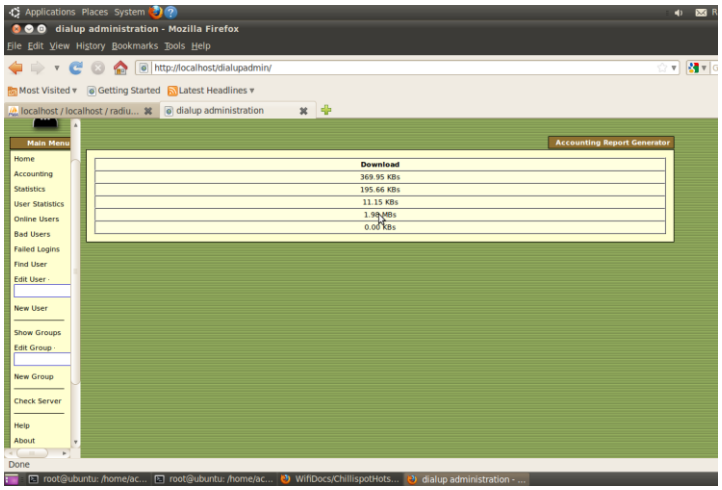
Gambar 5.15 *Accounting*



Gambar 5.16 pelaporan *login time*



Gambar 5.17 pelaporan *username*



Gambar 5.18 pelaporan *download*

BAB VI

SIMPULAN DAN SARAN

6.1 Simpulan

Pada proses *Autentikasi* dari pengguna jaringan *wireless (hotspot)* dengan berbasis radius server, maka dapat disimpukan beberapa point :

1. Dari sisi administrator dan user, dapat membantu administrator dalam mengelola jaringan wireless, karena radius server ini mampu memberikan laporan tentang aktivitas *user* didalam jaringan, administrator juga dapat membedakan kriteria dari *user* antara *client* dan *administrator*. *User* juga mudah untuk dapat melakukan koneksi pada jaringan, cukup dengan memasukan *username* dan *password* yang diminta sever dengan benar.

2. Dari sisi kemanan, penerapan Radius server ini juga mampu memberikan keamanan pada *user* jaringan *wireless (hotspot),* karena Radius server ini mampu memberikan autentikasi yang sulit ditembus oleh pada pengguna yang tidak bertanggung jawab. Karna proses autentikasi ini bisa sukses apabila kode yang diminta server itu bisa dimasukan dengan benar dan sesuai dengan *user* yang di *create* pada *database* radius.

3. Dari hasil yang diuji pada sistem *autentikasi* pengguna wireless berbasis radius server yang diujikan pada *Hotspot* SMA Negeri 2 Prabumulih untuk dapat berinternet cukup cepat hanya membutuhkan waktu kurang dari 10 detik.

6.2 Saran

Untuk pengembangan selanjutnya, beberapa saran yang dapat diberikan adalah sebagai berikut :

1. Untuk pengembangan berikutnya diharapkan agar radius server ini dapat dikombinasikan dengan EAP-TLS untuk lebih menjamin keamanan pada pengguna jaringan wireless, karena dengan menerapkan EAP-TLS user yang bisa mengkases internet selain user yang sudah di *create* pada *database,* user juga harus men-*download* sertifikat TLS terlebih dahulu.
2. Untuk pengembangan berikutnya untuk proses *auntentikasi* dengan berbasis radius server ini jangan hanya diterapkan pada jaringan *wireless,* melainkan juga pada jaringan LAN.

DAFTAR PUSTAKA

Agung S., "*Remote Authentication Dial In User Service (RADIUS) untuk Autentikasi Pengguna Wireless LAN*", Laporan Akhir EC-5010 Institut Teknologi Bandung, 2005, http://br.paume.itb.ac.id:80/courses/ec5010/2005/index.html, (13 Des 2008)

Febyatmoko, dkk. 2006. *Otentikasi, Otorisasi & Pelaporan Koneksi User Wireless Chillispot Dan Server RADIUS.* http://journal.uii.ac.id/index.php/mediainform (akses 21 November 2010)

Kunang,Yesi Novaria dan Zuhri,YadiIlman.*"Autentikasi Pengguna Wireless Lan Berbasis Radius Server (Studi Kasus WLAN Universitas Bina Darma)",* http://blog.binadarma.ac.id/yesinovariakunang/wp, (23 november 2012)

Sudiarta,Pande Ketut, *"Implementasi Sistem Autentikasi Jaringan Hotspot Universitas Udayana Dengan Menggunakan Open Source Freeradius"*. http://ejournal.unud.ac.id/abstrak/pande_10_(1).pdf, (21 November 2012)

Utomo,Eko Priyo.2011.*Membangun Jaringan Komputer dan Server Internet*, Yokyakarta : MediaKom.

Yunus,Amak *"Implementasi Sistem Otentikasi Pada Pengguna Jaringan Hotspot Di Universitas Kanjuruhan Malang Guna Meningkatkan Keamanan Jaringan Komputer"*.

http://ejournal.ukanjuruhan.ac.id/media/paper/Jurnal%20RadiusAmak.pdf,
(22 november 2012).

http://www.sman2pbm.sch.id .(akses 21 november 2012).

Hassel, Jonathan. RADIUS. O'Reilly. 2002.(akses 13 des 2012)

C. Rigney, S. Willens, A. Rubens, W. Simpson, "*Remote Authentication DialIn UserService*(RADIUS)",RFC 2138, 1997, http://www.ietf.org/rfc/rfc2138.txt (13 desember 2012)

Ebook Fui Forum Ubuntu-Indonesia.Com, diakses