KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
PALCOMTECH PALEMBANG

SKRIPSI

Desain Dan Implementasi Pengamanan Jaringan *Nirkabel* Menggunakan *Radius Server* Pada Pengadilan Tinggi Palembang

Oleh :
SLAMET RIYADI
012080776

Untuk Memenuhi Sebagian Dari Syarat-Syarat
Guna Mencapai Gelar Sarjana Komputer
Palembang
2012

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
PALCOMTECH PALEMBANG

HALAMAN PERSETUJUAN PEMBIMBING SKRIPSI

NAMA	**: Slamet Riyadi**
NOMOR POKOK	**: 012080776**
PROGRAM STUDI	**: Teknik Informatika**
JENJANG PENDIDIKAN	**: Strata I (TI)**
KONSENTRASI	**: Jaringan**
JUDUL SKRIPSI	**: Desain dan Implentasi Pengamanan Jaringan *Nirkabel* Menggunakan *Radius Server* Pada Pengadilan Tinggi Palembang**

Tanggal : 06 Agustus 2012 **Mengetahui,**
Pembimbing : **Ketua,**

Benny Wijaya, S.T **Rudi Sutomo, S.Kom., M.Si**
NIDN :0202097902 **NIP : 028.PCT.08**

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
PALCOMTECH PALEMBANG

HALAMAN PENGESAHAN PENGUJI

NAMA	**: Slamet Riyadi**
NOMOR POKOK	**: 012080776**
PROGRAM STUDI	**: Teknik Informatika**
JENJANG PENDIDIKAN	**: Strata I (TI)**
KONSENTRASI	**: Jaringan**
JUDUL SKRIPSI	**: Desain dan Implementasi Pengamanan Jaringan Nirkabel Menggunakan Radius Server Pada Pengadilan Tinggi Palembang**

Tanggal : 20 September 2012	**Tanggal : 20 September 2012**
Penguji 1,	**Penguji II,**
Rudi Sutomo, S.Kom., M.Si	**AtinTriwahyuni, ST., M.Emg**
NIDN : 0222057501	**NIDN :0215028002**

Menyetujui,
Ketua STMIK,

Rudi Sutomo, S.Kom., M.Si.
NIP : 028.PCT.08

MOTTO :

Bismillahirohmannirohim

- Tiada daya dan upaya melainkan usaha dan do'a
- Sukses bukan datang menghampiri namun sukses adalah untuk kita raih
- Ilmu yang bermanfaat adalah ilmu yang diamalkan, berguna bagi dirinya sendiri dan bermanfaat bagi orang lain.
- Teori tanpa disertai dengan praktek sama saja dengan minum dari gelas yang kosong, begitu juga sebaliknya.

(*Slamet Riyadi*)

Kupersembahkan kepada :

- *Allah SWT yang selalu memberikan kemudahan dalam segala hal*
- *Ayah dan ibu tercinta yang selalu mendo'akan dan memberikan dukungan.*
- *Mutiara Hatiku "Rere Resia"*
- *Pembimbing dan para dosen yang telah Ikhlas memberi pengajaran yang berharga bagiku.*
- *Adik-adikku yang selalu ku sayangi*
- *Sahabat – Sahabat ku yang selalu memberikan motivasi.*
- *Almamaterku*

KATA PENGANTAR

Alhamdulillahi Rabbil'alamin, puji syukur atas ridho dan nikmat yang senantiasa Allah SWT limpahkan kepada kita. Karena dengan nikmatnya yang indah penulis dapat menyelesaikan penyusunan dan penulisan skripsi ini dengan judul: **"Desain dan Implementasi Pengamanan Jaringan *Nirkabel* Menggunakan *Radius Server* Pada Pengadilan Palembang".** Penulis sangat menyadari bahwa dalam penulisan dan penyusunan skripsi ini masih banyak kekurangan dan kelemahan.

Dalam penulisan skripsi ini, penulis menyadari bahwa penulisan ini banyak mendapat bantuan dari berbagai pihak, baik dari pihak akademik, keluarga, maupun teman-teman seperjuangan. Oleh karena itu, penulis mengucapkan banyak terimakasih yang tulus serta do'a dan harapan semoga semua bantuan yang penulis dapatkan dapat di balas kebaikan oleh Allah SWT, Amin.

Tak lupa penulis ucapkan rasa terimakasih kepada semua pihak yang telah membantu dan membimbing dengan ikhlas dan sungguh-sungguh. Penulis banyak mengucapkan terimakasih kepada Bapak Rudi Sutomo, S.Kom., M.Si selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palcomtech, Bapak Benny Wijaya, ST. selaku Pembimbing, Para Dosen dan Staff pegawai Palcomtech, kedua orang tuaku tercinta (Ibu dan Bapak) yang memberikan dukungan baik moril maupun materil. Teman–teman seangkatan penulis yang sudah banyak membantu dan memberi dukungan dalam penulisan skripsi ini.

Semoga Allah SWT senantiasa melimpahkan rahmat dan karunianya kepada kita semua, kritik dan saran yang sifatnya membangun juga penulis

harapkan. Akhirnya, penulis berharap semoga skripsi ini dapat bermanfaat bagi penulis dan pembaca sekalian.

Palembang, 20 September 2012

Penulis

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

.

ABSTRAK

Slamet Riyadi (NPM 012080776). Desain dan Implementasi Pengamanan Jaringan *Nirkabel* Menggunakan *Radius Server* Pada Pengadilan Tinggi Palembang.

Salah satu perubahan utama dibidang telekomunikasi adalah penggunaan teknologi wireless. Kemudahan-kemudahan yang ditawarkan wireless LAN menjadi daya tarik tersendiri bagi para pengguna komputer untuk menggunakan teknologi ini dalam mengakses suatu jaringan komputer atau internet.

Teknologi ini akan memberikan jaringan akses yang mudah bagi pengguna. Namun, kita perlu sistem yang canggih manajemen informasi untuk mengontrol *bandwidth* untuk tujuan administratif. Pada penelitian ini, penulis akan menerapkan Pengamanan Jaringan *Nirkabel* sebagai media sharing *internet* serta keamanannya. dalam Pembuatan *authentikasi wireless* penulis menggunakan satu unit perangkat PC yang dipasang *wireless card* sebagai *Access Point.*

Access point yang digunakan adalah access point yang dibuat dengan menggunakan kartu jaringan *wireles*s. *Software* yang dipakai adalah *chillispot* sebagai *captive portal* dan *Freeradius* sebagai mekanisme keamanannya dan *MySql* sebagai *databasenya* Sebagai hasilnya dapat disimpulkan bahwa dengan menggunakan Authentikasi user mampu menerapkan jaringan wireless yang baik dan aman.

Kata kunci: Chillispot, Freeradius, Phpmyprepaid.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Sebuah institusi yang besar terutama Pengadilan Tinggi Palembang yang tulang punggung eksistensinya menggunakan teknologi informasi membutuhkan penanganan yang baik agar sistem informasi yang ada dapat berjalan dengan optimal. Banyak faktor yang mempengaruhi keoptimalan kinerja sistem informasi, salah satu yang terpenting adalah keamanan sistem. Jaringan komputer Nirkabel atau disebut WLAN (*Wireless local Area Network)* adalah salah satu teknologi yang saat ini sudah digunakan secara luas di berbagai institusi. Selain banyaknya keuntungan dengan memakai teknologi jaringan komputer nirkabel, terdapat juga kekurangan yaitu keamanan dan pembatasan hak akses. Hal itulah yang saat ini dihadapi oleh pihak Pengadilan Tinggi Palembang yang mana masih minimnya keamanan.

Pengadilan Tinggi khusus Palembang memberikan pelayanan Hukum yang Berkeadilan sebelumnya telah memiliki jaringan computer yang sudah terkoneksi ke jaringan *internet* dan memanfaatkan teknologi *wireless* sebagai infrastruktur jaringan akan tetapi pemanfaatan teknologi *wireless* tersebut tidak berlangsung lama di karenakan sistem keamanannya yang masih lemah maka yang tadinya telah dibangunlah sistem jaringan *wireless* dimplementasikan kembali tetapi terdapat penambahan pada infrastruktur jaringan yaitu dengan menggunakan *Radius server* untuk *autentifikasi user.*

Berdasarkan pengamatan penulis bahwa system keamanan *wireless* pada Pengadilan Tinggi Palembang masih lemah terutama dilihat dari sisi pengamanan karena menggunakan metode enkripsi *WEP (Wired Equivalent Privacy)*. WEP menggunakan kunci yang bersifat statis sehingga siapapun bisa mengakses *hotspot.* Hal ini sangat beresiko sekali untuk keamanan jaringan maka dari itu diperlukan metode lain yang lebih baik untuk mengatasi kelemahan tersebut. Salah satunya menggunakan Sistem keamanan lainnya adalah *WPA* (*Wi-Fi Protected Access*), yang menggeser *WEP* dan menghasilkan keamanan yang lebih baik dibandingkan dengan *WEP*. Implementasi *WPA* menggunakan 802.1x dan *EAP* (*Extensible Authentication Protocol*) menghasilkan proses autentikasi pengguna yang relatif aman. Pada proses ini pengguna harus melakukan autentikasi ke sebuah server autentikasi sebelum terhubung ke internet. Pada umumnya proses autentikasi ini menggunakan *username* dan *password*. dengan system ini tidak sembarangan *user* bisa mengakses jaringan,sehingga *user* memerlukan *autentikasi* ketika akan mengakses *wireless* atau yang lebih dikenal *hot-spot.* Hanya *user* yang telah diberikan hak akses oleh administrator jaringan yang bisa mengakses hotspot sehingga sistem keamanan lebih terjamin yaitu menggunakan *radius server*. Berdasarkan uraian hal tersebut maka judul skripsi yang penulis angkat adalah " ***Desain dan Implementasi Pengamanan Jaringan Nirkabel Menggunakan Radius Server Pada Pengadilan Tinggi Palembang".***

1.2 Rumusan Masalah

Berdasarkan latar belakang yang diatas, maka penulis merumuskan permasalahan dalam penelitian ini yaitu sebagai berikut; “bagaimana mendesain dan mengimplementasi pengamanan Jaringan Nirkabel menggunakan Radius Server pada Pengadilan Tinggi Palembang”.

1.3 Batasan Masalah

Untuk menghindari meluasnya materi yang dibahas pada penelitian ini, maka penulis memberikan batasan masalah sebagai berikut:

a. *Aplikasi Captive Portal* yang digunakan adalah *Chillispot* dan *Freeradius* yang disertai dengan *mysql* yang digunakan untuk mekanisme keamanan dan database.
b. *Aplikasi PHPMyprepaid* yang digunakan untuk *management user* dan *bandwidth*, *Quota User* untuk membatasi jumlah kapasitas penyimpanan file pada *File Server,* serta pemasangan tanda area *Wirelless* pada tempat-tempat tertentu.
c. *Sistem operasi* yang digunakan adalah *Centos Server 5.3* yang merupakan salah satu *sistem operasi* yang *Open Source.*

1.4 Tujuan Penelitian

Adapun dari penelitian ini adalah untuk mendesain dan mengimplementasin pengamanan jaringan Nirkabel menggunakan Radius Server pada Pengadilan Tinggi Palembang.

1.5 Manfaat Penelitian

Adapun manfaat yang diperoleh dari penelitian ini adalah :

1. **Bagi Penulis**

   Agar dapat menerapkan pengetahuan yang didapat didalam perkuliahan seperti mata kuliah praktik jaringan komputer.

2. **Bagi Perusahaan**

   Penelitian ini diharapkan dapat mempermudah proses autentikasi user dan sistem keamanan jaringan *wireless* pada Pengadilan Tinggi Palembang.

3. **Bagi Akademik**

   Dapat menambah informasi dan bisa dijadikan perbandingan bagi penelitian selanjutnya serta dapat dijadikan arsip atau dokumen yang diharapkan akan bermanfaat untuk proses kegiatan perkuliahan mahasiswa nantinya.

1.6 Sistematika Penulisan

Agar penyusunan dalam penulisan skripsi ini lebih sistematis sesuai dengan ketentuan yang diberikan, sistematika penulisan tersebut antara lain sebagai berikut:

BAB I PENDAHULUAN

Bab ini penulis akan menguraikan tentang latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, dan sistematika penulisan.

BAB II GAMBARAN UMUM

Bab ini penulis akan membahas tentang sejarah singkat perusahaan, visi misi dan tujuan organisasi, struktur organisasi, pembagian tugas, dan wewenang serta perancang jaringan *wireless.*

BAB III TINJAUAN PUSTAKA

Bab ini akan membahas tentang landasan teori yang digunakan dalam pembuatan autentikasi jaringan nirkabel.

BAB IV METODE PENELITIAN

Bab ini penulis akan membahas tentang metodologi penulisan, lokasi dan waktu riset yang telah dilakukan.

BAB V HASIL DAN PEMBAHASAN

Bab ini penulis akan membahas mengenai Desain jaringan beserta implementasi, hasil penelitian dan pembahasan.

BAB VI SIMPULAN DAN SARAN

Bab ini berisi simpulan dan saran yang penulis kemukakan dari penelitian yang penulis lakukan.

BAB II

GAMBARAN UMUM PERUSAHAAN

1.1 Profil Perusahaan

1.1.1 Sejarah Perusahaan

Sebelum Pengadilan Tinggi Palembang dibentuk merupakan wilayah hukum Pengadilan Tinggi Medan dan Pengadilan Tinggi Jakarta, namun setelah terbit Undang Undang Nomor 11 Tahun 1964 Tanggal 08 Agustus 1964 Tentang Pembentukan Pengadilan Tinggi Palembang, maka terbentuklah Pengadilan Tinggi Palembang yang wilayah hukumnya meliputi Propinsi Jambi, Propinsi Sumatera Selatan dan Propinsi Lampung. Pada tahun 1980 terbit Undang – Undang No. 9 Tahun 1980 tanggal 29 Juli 1980 Tentang Pembentukan Pengadilan Tinggi Tanjung Karang yang meliputi wilayah hukum Propinsi Lampung, pada tahun 1982 terbit Undang – Undang No. 14 Tahun 1982 tanggal 20 Agustus 1982 Tentang Pembentukan Pengadilan Tinggi Jambi yang meliputi wilayah hukum Propinsi Jambi dan pada tahun 2004 dibentuk pula Pengadilan Tinggi Bangka Belitung yang meliputi wilayah Propinsi Bangka Belitung dengan Undang – Undang No. 13 Tahun 2004 tanggal 06 Juli 2004. Dengan terbitnya ketiga Undang - Undang tersebut diatas wilayah hukum Propinsi Lampung, Propinsi Jambi dan Propinsi Bangka Belitung tidak lagi termasuk dalam wilayah hukum Pengadilan Tinggi Palembang.

Pengadilan Tinggi Palembang yang terletak di Jalan Jenderal Sudirman KM 3,5 Palembang meliputi wilayah hukum Propinsi Sumatera Selatan dan hingga saat ini membawahi 8 (delapan) Pengadilan Tinggi yaitu :

No	Nama	Wilayah
1	Pengadilan Tinggi Palembang	Kota Palembang
2	Pengadilan Tinggi Kayu Agung	Kabupaten Ogan Komering Ilir dan Kabupaten Ogan Ilir
3	Pengadilan Tinggi Sekayu	Kabupaten Bayuasin dan Kabupaten Musi Bayuasin
4	Pengadilan Tinggi Muara Enim	Kabupaten Muara Enim
5	Pengadilan Tinggi Baturaja	Kabupaten OKU Selatan, OKU Timur, Ogan Komering Ulu
6	Pengadilan Tinggi Lahat	Kabupaten Epat Lawang, Lahat, Pagar Alam
7	Pengadilan Tinggi Lubuk Linggau	Kabupaten Lubuk Linggau, Musi Rawas
8	Pengadilan Tinggi Prabumulih	Kabupaten Prabumulih

Sumber : Pengadilan Tinggi Palembang

1.1.2 Visi dan Misi

a. Visi

Dalam menjalankan tugas dan fungsinya, Pengadilan Tinggi Palembang sebagai Peradilan Tingkat Banding dilandasi oleh visi ke depan, sebagaimana Visi Mahkamah Agung Republik Indonesia yaitu **"Terwujudnya Badan Peradilan Indonesia Yang Agung".**

b. Misi

Dalam menjalankan tugas dan wewenangnya, Pengadilan Tinggi Palembang juga membawa ***misi***, yaitu:

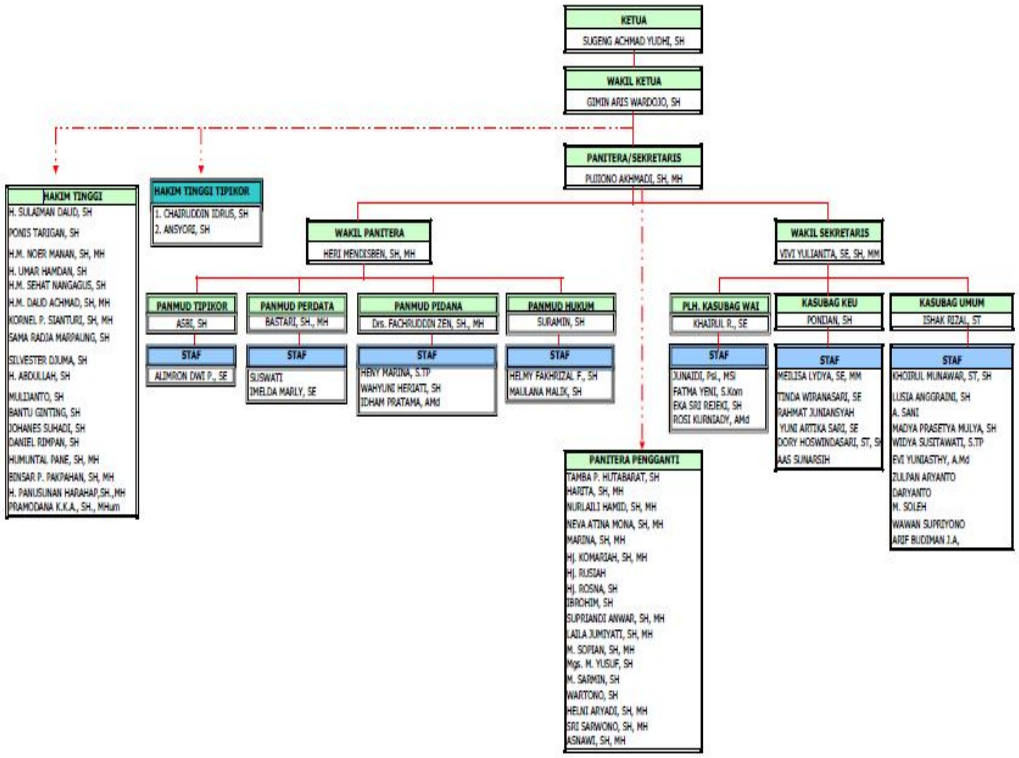
1. Menjaga Kemandirian Badan Peradilan.
2. Memberikan Pelayanan Hukum yang Berkeadilan.
3. Meningkatkan Kualitas Kepemimpinan Badan Peradilan.
4. Meningkatkan Kredibilitas dan Transparansi Badan Peradilan.

1.2 Struktur Organisasi

Dalam menjalankan perusahaan atau instansi dengan baik, maka sangat dibutuhkan adanya struktur organisasi perusahaan yang dapat menggambarkan secara jelas tentang uraian tugas dari masing-masing pegawai. Serta dapat memberikan gambaran yang nyata mengenai wewenang dan tanggung jawab masing-masing bagian sesuai dengan tugas yang diberikan. Susunan organisasi Pengadilan Tinggi Palembang terdiri dari Ketua Pengadilan, Hakim, Panitera dan Staf.

Susunan organisasi ini memungkinkan adanya koordinasi yang baik dari level yang teratas hingga yang terendah guna menciptakan suatu kerjasama yang baik untuk mencapai tujuan Instansi. Dan susunan yang baik diharapkan dapat meningkatkan efektivitas kerja suatu organisasi.

Struktur Organisasi Pengadilan Tinggi Palembang



Gambar 2.1 Struktur Organisasi Pengadilan Tinggi Palembang

1.3 Tugas dan Wewenang

Untuk menjelaskan megenai tugas dan tanggung jawab dari masing-masing bagian yang tertera pada struktur organisasi pada Pengadilan Tinggi Palembang adalah sebagai berikut:

A. Ketua Pengadilan

1. Melakukan pengawasan terhadap jalannya peradilan yang ditangani oleh Pengadilan Tinggi Palembang.
2. Melakukan pengawasan terhadap tingkah laku para hakim pada Pengadilan Tinggi Palembang.
3. Melakukan pengawasan/memonitor terhadap pekerjaan-pekerjaan baik administrasi tekhnis maupun non tekhnis Pengadilan Tinggi Palembang.
4. Memberikan peringatan, teguran, dan petunjuk yang diperlukan.
5. Tugas-tugas lain yang menurut Undang-undang di wajibkan kepadanya.

B. Wakil Ketua Pengadilan

1. Membantu ketua dalam melakukan pengawasan terhadap jalannya peradilan yang ditangani oleh Pengadilan Tinggi Palembang.
2. Tugas-tugas lain yang menurut Undang-undang di wajibkan kepadanya.

C. Panitera/Sekretaris

1. Membantu Ketua Pengadilan Tinggi Palembang dalam membuat program kerja jangka pendek dan jangka panjang, pelaksanaannya dan pengorganisasiannya.
2. Melakukan penilaian dan mengesahkan penilaian pelaksanaan pekerjaan pejabat bawahan.
3. Melakukan bimbingan pegawai di lingkungan Pengadilan Tinggi Palembang.
4. Mengatur pembagian tugas pejabat kepaniteraan.
5. Dengan dibantu oleh Wakil Panitera dan Panitera Muda menyelenggarakan administrasi secara cermat mengenai jalannya perkara perdata dan pidana maupun situasi keuangan perkara perdata.
6. Mengkoordinasikan ketatausahaan di lingkungan Pengadilan Tinggi Palembang.
7. Melakukan pengawasan melekat dilingkungan Pengadilan Tinggi Palembang.
8. Mengkoordinasikan pengelolaan anggaran rutin Pengadilan Tinggi Palembang sesuai dengan ketentuan dan perundang-undangan yang berlaku.
9. Bertanggung jawab atas pengurusan berkas perkara, putusan, dokumen, akta, buku daftar, biaya perkara, uang titipan, pihak ketiga, surat-surat bukti dan surat-surat lainnya yang disimpan di kepaniteraan.

10. Membuat akta dan salinan putusan.
11. Menerima dan mengirimkan berkas perkara.
12. Mengkoordinasikan pengelolaan perlengkapan Pengadilan Tinggi Palembang.
13. Melakukan pengelolaan kebutuhan formasi dan pengelolaan administrasi kepegawaian pegawai Pengadilan Tinggi Palembang.
14. Melakukan pengendalian administrasi kepegawaian dalam lingkungan Pengadilan Tinggi Palembang.
15. Mengkoordinasikan pembuatan dan penyusunan laporan pelaksanaan tugas Pengadilan Tinggi Palembang.
16. Menyetujui, menolak atau merubah nilai apabila ada keberatan atas penilaian DP3 yang dibuat pejabat bawahan.
17. Mengesahkan DP3 yang dibuat oleh pejabat bawahan.
18. Memberi petunjuk dan pengarahan pelaksanaan tugas pada bawahan.
19. Menegakkan disiplin pegawai dilingkungan Pengadilan Tinggi Palembang.
20. Melaksanakan eksekusi putusan perkara perdata (yang telah berkekuatan hukum tetap) yang diperintahkan Ketua Pengadilan Tinggi Palembang dalam jangka waktu yang ditentukan.
21. Menyelenggarakan administrasi perkara dan mengurus tugas wakil Panitera, panitera muda dan panitera pengganti. (Pasal 96 Undang-undang No. 7 Tahun 1989, pasal 58 Undang-undang No. 2 Tahun 1986).

22. Bertanggung jawab atas kepengurusan berkas perkara, putusan, dokumen, akta, buku daftar, biaya perkara, uang titipan pihak ketiga, surat-surat bukti kepaniteraan (pasal 63 Undang-undang No. 2 Tahun 1986) dan pasal 101 Undang-undang No. 7 Tahun 1989.
23. Membuat semua daftar perkara yang diterima di kepaniteraan dan pasal 99 Undang-undang No. 7 tahun 1989. (pasal 61 Undang-undang Nomor 2 Tahun 1986.
24. Membuat salinan atau turunan penetapan atau putusan Pengadilan Tinggi Palembang menurut peraturan Perundang-undangan yang berlaku pasal 100 Undang-undang Nomor 7 Tahun 1989.
25. Pemungutan biaya-biaya Pengadilan dan menyetorkan ke kas negara.
26. Menerima uang titipan pihak ketiga dan melaporkannya kepada ketua pengadilan.
27. Membuat akta-akta.
28. Permohonan banding.
29. Pemberitahuan adanya permohonan banding.
30. Penyampaian salinan memori/kontra memori banding.
31. Pemberitahuan membaca/memerikasa berkas perkara (inzage).
32. Pemberitahuan putusan banding.
33. Pencabutan permohonan banding.
34. Pemberitahuan adanya permohonan kasasi.
35. Pemberitahuan memori kasasi.
36. Penyampaian salinan memori kasasi/kontra memori kasasi.

37. Penerimaan kontra memori kasasi.
38. Tidak menerima memori kasasi.
39. Pencabutan permohonan kasasi.
40. Pemberitahuan putusan kasasi.
41. Permohonan peninjauan kembali.
42. Pemberitahuan adanya peninjauan kembali.
43. Penerimaan/penyampaian jawaban permohonan peninjauan kembali.
44. Pencabutan permohonan peninjauan kembali.
45. Penyampaian salinan putusan Peninjauan kembali.
46. Pembuatan akta yang menurut Undang-undang peraturan diharuskan dibuat oleh panitera.
47. Dimana tugas-tugas Panitera tersebut diatas yang menyangkut tentang tugas-tugas diluar pengadilan, sudah barang tentu dibantu oleh Petugas Fungsional lainnya, seperti hanya Jurusita dan Jurusita Pengganti sebagai perpangjangan tangan dari Panitera itu sendiri.

D. Wakil Panitera

1. Mengadakan pembinaan, pengawasan dan mengkoordinir pelaksanaan tugas-tugas Panitera Muda Perdata.
2. Mengadakan pembinaan, pengawasan dan mengkoordinir pelaksanaan tugas-tugas Panitera Muda Pidana.
3. Mengadakan pembinaan, pengawasan dan mengkoordinir pelaksanaan tugas-tugas panitera muda hukum.

4. Menerima surat-surat masuk yang berhubungan dengan tugas kepaniteraan yang telah didisposisi oleh Ketua/Wakil Ketua dan Panitera/Sekretaris untuk diteruskan ke masing-masing panitera muda untuk penyelesaiannya.
5. Menerima berkas perkara perdata dan pidana yang telah terdaftar dari Penitera Muda Perdata dan Panitera Muda Pidana untuk diserahkan kepada Ketua Pengadilan Tinggi Palembang melalui Panitera/Sekretaris untuk ditetapkan Majelis Hakimnya.
6. Evaluasi Laporan bulanan perkara perdata dan pidana.
7. Tugas-tugas lain yang menurut Undang-undang di wajibkan kepadanya.

E. Wakil Sekretaris

1. Menyelenggarakan tertib administrasi dalam hal surat-menyurat dalam Pengadilan Tinggi Palembang.
2. Mengadakan pembinaan, pengawasan dan mengkoordinir pelaksanaan tugas pada sub bagian umum.
3. Mengadakan pembinaan, pengawasan dan mengkoordinir pelaksanaan tugas pada sub bagian keuangan.
4. Mengadaan pembinaan, pengawasan dan mengkoordinir pelaksanaan tugas pada sub bagian kepegawaian.
5. Koordinasi dengan bagian Kepaniteraan dalam pelaksanan tugas kedinasan.

6. Tugas-tugas lain yang menurut Undang-undang di wajibkan kepadanya.

F. Panitera Muda Perdata

1. Melakukan administrasi perkara.

2. Mempersiapkan persidangan perkara.
3. Melaksanakan formalitas kelengkapan perkara.
4. Melaksankan pendaftaran berkas perkara.
5. Menyerahkan berkas perkara yang telah diregister dan dengan dilengkapi formulir penetapan penunjukan Majelis Hakim kepada Wakil Panitera untuk diserahkan kepada Pengadilan Tinggi Palembang melalui Panitera/Sekretaris.
6. Menerima berkas perkara perdata yang telah diminutasi oleh Panitera Pengganti.
7. Menyimpan surat dan memelihara arsip surat-surat yang berkaitan dengan perkara perdata.
8. Menyimpan berkas perkara yang masih berjalan.
9. Tugas-tugas lain yang menurut Undang-undang di wajibkan kepadanya.

G. Panitera Muda Pidana

1. Menerima berkas perkara yang dikirim oleh Kejaksaan Tinggi Palembang.

2. Melaksanakan formalitas kelengkapan berkas perkara pidana.

3. Menyerahkan berkas perkara pidana yang telah diregister dan dilengkapi dengan formulir penetapan penunjukan Majelis Hakim kepada Wakil Panitera untuk diserahkan kepada Ketua Pengadilan Tinggi Palembang melalui Panitera/ Sekretaris.
4. Menyerahkan berkas perkara pidana kepada ketua Majelis Hakim yang telah ditunjuk oleh Ketua Pengadilan Tinggi Palembang.
5. Secara teratur mengisi kolom buku register dengan tertib, cermat, lengkap dan tepat waktu.
6. Menyelenggarakan perpanjangan penahanan.
7. Melaksana-kan register-register barang bukti dan register putusan.
8. Membuat Laporan bulanan perkara pidana.
9. Menyimpan dan memelihara surat-surat yang berhubungan dengan perkara pidana.
10. Melaksanakan administrasi perkara.
11. Mempersiapkan persidangan perkara.
12. Menyimpan berkas perkara yang masih berjalan.
13. Tugas-tugas lain yang menurut Undang-undang di wajibkan kepadanya.

H. Panitera Muda Hukum

1. Mengevaluasi laporanan bulanan perkara perdata dan pidana.
2. Menata kembali arsip perkara perdata dan pidana yang sudah in aktif.
3. Mengumpulkan, mengolah dan mengkaji data.

4. Menyajikan statistik perkara.
5. Menyusun Laporan perkara.
6. Menyimpan arsip berkas perkara.
7. Melakukan administrasi pendaftaran notaris.
8. Melakukan administrasi pendaftaran Penasehat hukum.
9. Melakukan administrasi pendaftaran Badan Hukum.
10. Melakukan administrasi kewarganegaraan.
11. Melakukan administrasi balai harta peninggalan.
12. Menyimpan dan memelihara surat-surat yang berkaitan dengan tugas-tugas Panitera Muda Hukum.
13. Tugas-tugas lain yang menurut Undang-undang di wajibkan kepadanya.

I. Urusan Kepegawaian

1. Menyusun rencana kerja kepala sub bagian kepegawaian.
2. Menyusun formasi pengangkatan pegawai baru pada Pengadilan Tinggi Palembang.
3. Membuat laporan tutup tahun anggaran kepegawaian.
4. Menyiapkan data kepegawaian untuk mengikuti ujian dinas tingkat I dan tingkat II.
5. Mengadakan usulan kenaikan pangkat.
6. Menyelesaikan urusan permintaan pensiun pegawai, pensiun janda/laporan pensiun.
7. Menganalisa data pegawai untuk menyiapkan DUK pegawai.

8. Menyelesaikan dan menghimpun DP.3.
9. Menghimpun dan menyelesaikan Bezetting pegawai.
10. Mempersiapkan dan mengusulkan Karpeg, Karis/Karsu, Taspen.
11. Menyiapkan dan mengusulkan kenikan gaji berkala pegawai.
12. Menyimpan SK para pegawai Kantor Pengadilan Tinggi Palembang
13. Menyelenggarakan kegiatan administrasi yang berkaitan dengan kepegawaian di Pengadilan Tinggi Palembang.
14. Membuat rekapitulasi jumlah pegawai Tinggi Sipil dan Calon Pegawai Tinggi Sipil menurut Pendidikan, jenis kelamin dan golongan.
15. Hukuman Disiplin.
16. Keadaan tenaga teknis peradilan.
17. Rekapitulasi daftar hadir hakim dan pegawai.
18. Tugas-tugas lain yang menurut Undang-undang Pokok Kepegawaian Nomor 43 Tahun 1999 yang di wajibkan kepadanya.

J. Urusan Keuangan

1. Membuat, menyusun rencana penggunaan anggaran dan rencana kebutuhan fisik/perlengkapan kantor yang dituangkan dalam RKL – KL.

2. Menyusun DIPA Pengadilan Tinggi Palembang.
3. Melaksanakan tugas kebendaharaan pengeluaran APBN Pengadilan Tinggi Palembang.

4. Membuat dan mengirim Lapbul, Labtrin, Lapsemester, Laptah, dan Laporan BAP Kas penerimaan dan kas pengeluaran APBN Pengadilan Tinggi Palembang.
5. Menyusun rekapitulasi anggaran/Laporan keuangan.
6. Menyusun daftar pemasukan dan pengeluaran.
7. Membuat dan menatausahakan daftar gaji pegawai.
8. Membuat SKPP Pegawai pindah/pensiun.
9. Melaksanakan tugas petugas penerimaan SPP.
10. Menerima/menyimpan KP4/SPMT/SPMJ Pengadilan Tinggi Palembang.
11. Menyimpan arsip surat yang berkaitan dengan keuangan.
12. Tugas-tugas lain yang menurut Undang-undang di wajibkan kepadanya.

K. Urusan Umum

1. Membuat Daftar Inventaris Barang (DIR).
2. Menempatkan karyawan pada tempat yang benar sesuai dengan ilmu, bakat, kemampuan serta status (SK pengankatannya).
3. Penataan arsip keluar/masuk sesuai dengan jenis klasifikasi surat.
4. Mengelola dan menatausahakan Barang Milik Megara.
5. Mengusulkan pengadaan dan penghapusan barang Milik Negara.
6. Menyimpan dan memelihara barang-barang yang ada dalam penguasaan Pengadilan Tinggi Palembang.

BAB III

TINJAUAN PUSTAKA

3.1 Teori Pendukung

3.1.1 Jaringan Komputer

Jaringan komputer (*computer network)* adalah merupakan gabungan antara teknologi computer dan teknologi telekomunikasi. sehingga computer kita dapat berinteraksi atau berkomunikasi dengan computer lain maka dikatakan computer kita sudah terkoneksi dalam sebuah jaringan computer. Bentuk koneksinya tidak harus melalui kabel saja melainkan dapat menggunakan jaringan Nirkabel. (Sopandi, 20010:02).

Dua buah komputer dikatakan "interkoneksi" apabila keduanya bisa berbagi *resources* yang dimiliki, seperti saling bertukar data/informasi,berbagi printer, berbagi media penyimpanan (*hard disk, floppy disk, CD ROM, dan* sebagainya) yang mengalir melalui media jaringan (baik kabel atau nirkabel). Yang saling terhubung dalam jaringan.

3.1.2 Jenis-Jenis Jaringan

Pada dasarnya LAN dan WAN merupakan desain original jaringan komputer, seiring dengan kemajuan teknologi konsep ini mengalami perkembangan. (Sopandi,2008:2).

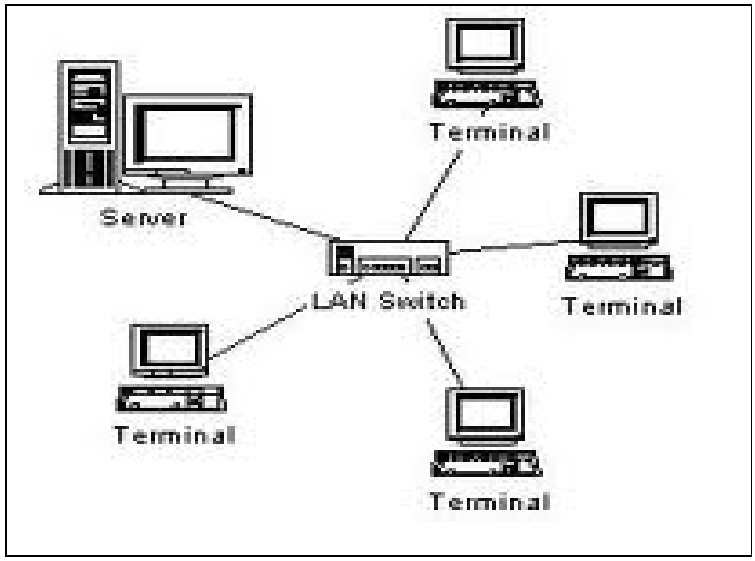
Menurut Sopandi (2008:2), saat ini kita mengenal beberapa jenis *Network Area*, seperti :

1. *Local Area Network* (LAN)
2. *Wide Area Network* (WAN)
3. *Metropolitan Area Network* (MAN)

1. LAN (*Local Area Network)*

LAN adalah suatu jaringan komputer yang dibangun pada area yang terbatas atau relative kecil, seperti ruangan, rumah, kantor, gedung, kampus. Sebuah LAN dapat terdiri atas puluhan hingga ratusan buah computer. LAN mendukung kecepatan transfer data cukup tinggi. Semua computer yang terhubung ke server pada jaringan disebut dengan Workstation. Workstation merupakan computer standar yang dikonfigurasi menggunakan kartu jaringan. (Wagito,2007:09).

LAN merupakan jaringan yang bersifat internal dan biasanya miliki pribadi di dalam perusahaan kecil atau menengah dan biasanya berukuran sampai beberapa kilometer dan seringkali digunakan untuk menghubungkan computer-komputer pribadi dsn *workstation* dalam suatu kantor perusahaan sebagai sarana tukar-menukar informasi (Sopandi,2010:02). Berikut contoh Topologi jaringan LAN, yaitu



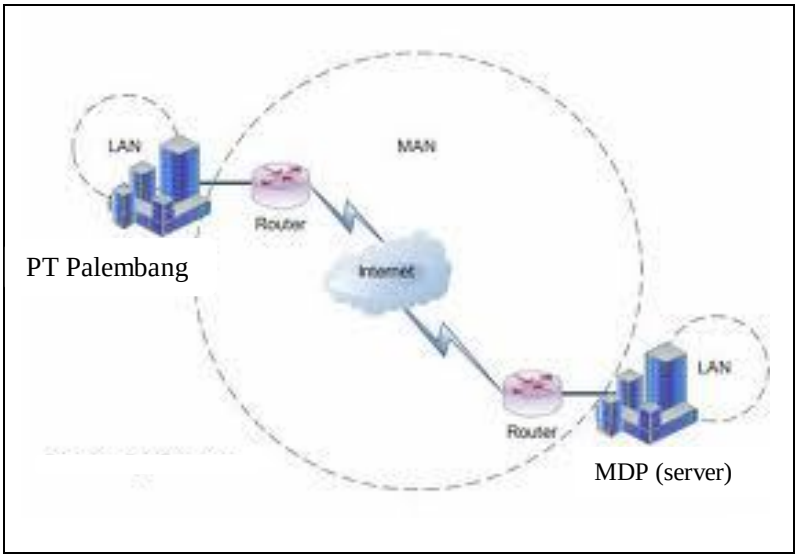
(Sumber : Sopandi,2010:20)

Gambar 3.1 Jaringan *LAN*

2. MAN (*Metropolita Area Network)*

MAN merupakan jaringan computer yang meliputi area sebuah kota, bisa berupa beberapa buah sekolah atau beberapa buah kampus. MAN telah diimplementasikan menggunakan teknologi *wire* maupun *wireless network. Wireless* MAN dapat menjangkau area yang sulit dijangkau oleh kabel.(Sofana,2011:27).

Jaringan MAN adalah gabungan dari beberapa LAN. Jangkauan dari MAN berjarak 10 km hingga 50 km, MAN dapat dimanfaatkan jaringan TV kabel jenis *coaxial* dan serat optic, sehingga dapat mengangkut data berukuran gigabit dengan sangat cepat (Sopandi, 2010:04).



(Sumber : Sopandi,2010:04)

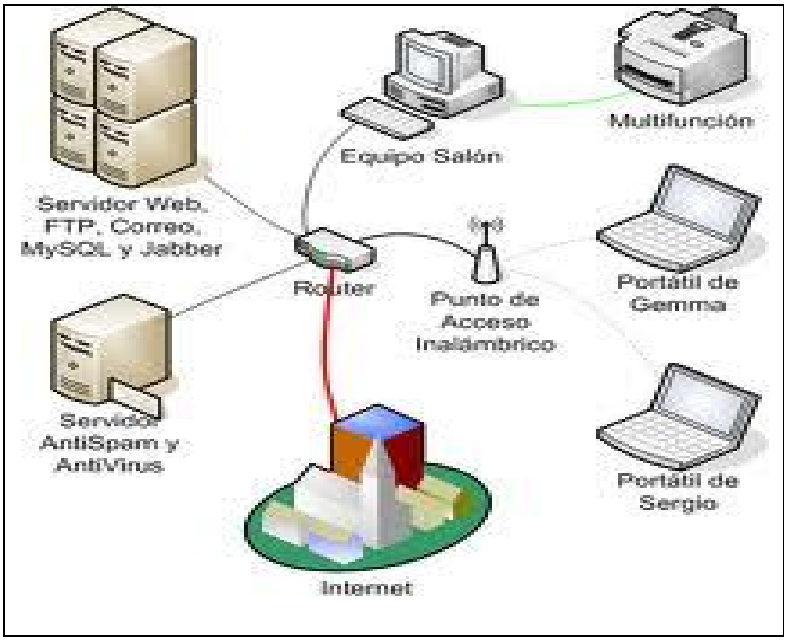
Gambar 3.2 Jaringan *MAN*

3. WAN (*Wide Area Network)*

WAN merupakan jaringan computer yang meliputi area geografis sangat besar, sepeti antarkota, antarnegara, antarbenua. Dimana dapat menghubungkan LAN dan MAN yang dipisahkan oleh jarak yang sangat jauh. Sehingga untuk menghubungkan kedua jarak yang berjauhan biasanya digunakan saluran telepon atau saluran komunikasi public (umum) atau satelit (Sofana,2011:29).

Pada sebagaian besar WAN, jaringan terdiri dari sejumlah banyak kabel atau saluran telepon yang menghubungkan sepasang *Router*. Bila dua *router* yang tidak mengandung kabel yang sama akan melakukan komunikasi, keduannya harus berkomunikasi secara tidak langsung melalui router lainnya. Ketika sebuah paket

dikirimkan dari sebuah *router* ke *router* lainnya melalui *router* perantara atau lebih, maka paket akan diterima *router* dalam keadaan lengkap (Sopandi ,2010:04)



Sumber : Sopandi,2009:40)

Gambar 3.3 Jaringan WAN

3.1.3 Teknologi Jaringan Komputer

Peralatan yang dibutuhkan dalam suatu jaringan sangat tergantung pada konfigurasi dan media transmisi data yang digunakan untuk menjangkau jaringan. (Wagito,2007:23).

Secara umum suatu jaringan dapat terdiri dari beberapa perangkat keras diantaranya sebagai berikut:

1. Server.
2. Workstation.

3. NIC (*Network Interfaces Card)* .
4. HUB.
5. Switch.
6. WAP (*Wireless Access Point).*
7. Repeater
8. Bridge
9. Router

1. Server

Merupakan hati dari jaringan. Server biasanya merupakan computer berkecepatan tinggi dengan kapasitas memori (RAM) dan simpanan yang besar, dan dihubungkan dengan kartu jaringan yang cepat yang berkualitas tinggi. Sehingga server mampu beroprasi terus-menerus untuk melayani permintaan. (Wagito,2007:24).

2. Workstation

Merupakan computer standar yang dikonfigurasi menggunakan kartu jaringan serta perangkat lunak jaringan dan kabel-kabel yang diperlukan.(Wagito,2007:24).

3. NIC

Merupakan peralatan yang memungkinkan terjadinya hubungan antara jaringan dengan computer workstation atau jaringan dengan computer server. NIC merupakan peralatan internal yang

dipasangkan pada slot ekspensi dalam computer (baik ekspansi ISA atau PCI).

NIC merupakan factor yang sangat menentukan dalam penentuan kecepatan serta kinerja suatu jaringan. Berikut beberapa macam NIC yang sering digunakan dalam jaringan:

a. Kartu Token Ring

   Digunakan untuk protocol jaringan yang dibangun IBM yang mana computer mengakses jaringan melalui token passing. Topologi yang biasanya digunakan adalah star-wired-ring.

b. Kartu Localtalk

   Digunakan untuk protocol yang dimiliki oleh Apple Cor-Poration yang menggunakan skema media akses CSMA/CA dan mendukung tranmisi data pada kecepatan 230 Kbps.

c. Kartu Ethernet

   Digunakan untuk protocol jaringan yang menggunakan CSMA/CD dan bekerja pada beberapa tipe kabel yang sangat tergantung pada jenis jaringan.

d. Kartu WLAN

   Digunakan pada jaringan WLAN, dan di lengkapi dengan antenna yang digunakan untuk memancarkan dan menerima data sebagai media pengganti media kabel. (Wagito,2007:24-25).

4. HUB

Hub merupakan sebuah *central conennection point* untuk komputer pada network. *Hub* tidak memiliki fasilitas routing, sehingga semua informasi yang datang akan dikirim kesemua komputer (*broadcast*). (Sopandi,2008:18),

5. Switch

Merupakan penghubung beberapa LAN yang terpisah serta menyediakan filter paket antar LAN dan multi port yang mana dapat menyediakan *dedicated bandwitch* pada masing-masing port. Switch juga dapat mendukung banyak tranmisi secara serentak. (Wagito,2007:29).

6. WAP (*Wireless Access Point)*

Pada *wireless* LAN, *device transceiver* disebut sebagai *access point* dan terhubung dengan jaringan (LAN) melalui kabel (biasanya berupa UTP). Diman fungsi dari *access point* tersebut adalah mengirim dan menerima data, serta berfungsi sebagai buffer data antara *wireless* LAN dan *wired* LAN. Satu *access point* dapat melanyani sejumlah *user* (beberapa literature menyatakan bahwa satu akses point maksimal meng-*handle* sampai 30 *user).* Karena dengan semakain banyaknya *user* terhubung ke *access point* maka kecepatan yang diperoleh tiap *user* juga akan semakin berkurang. (Hantoro,2009:19)

7. Repeater

Merupakan fungsi utamanya *repeater* adalah untuk memperkuat sinyal. Sinyal yang diterima dari salah satu segmen kabel LAN ke segmen LAN berikutnya akan dipancarkan kembali dengan kekuatan sinyal asli pada segmen LAN pertama, sehinngga dengan adanya *repeater* ini, jarak antara dua jaringan komputer dapat diperluas. (Sopandi,2008:24),

8. Bridge

Merupakan perangkat yang digunakan untuk menghubungkan beberapa buah segmen jaringan komputer (LAN) yang sama ataupun yang bebeda, misalnya jaringan *Ethernet* dengan *Token Ring*, lebih cepat daripada *ROUTER* dan lebih handal, karena paket yang didapat akan langsung dikirimkan kealamat yang dituju tanpa ada proses penganalisisan/pengecekan dan tanpa ada *routing* kembali. (Sopandi,2008:24),

9. Router

Menurut Sopandi (2008:25), router memiliki kemampuan melewatikan paket IP dari satu jaringan kejaringan lain yang mungkin memiliki banyak jalur diantara keduanya. Router juga dapat digunakan untuk menghubungkan sejumlah LAN, sehingga trafik yang dibangkitkan oleh suatu LAN terisolasikandengan baik dari trafik yang dibangkitkan oleh LAN lain. Jika dua atau lebih LAN terhubung dengan *router*, setiap LAN dianggap sebagai

subnetwork yang bebeda. Mirip dengan *bridge*, *router* dapat menghubungkan *network interface* yang berbeda.

3.1.4 Topologi Jaringan Komputer

Menurut Wagito (2007:15) topologi dalam jaringan mengandung dua pengertian dilihat dari sisi pengkabelan dan dari sisi aliran data. Jika dilihat dari aliran data pada jaringan maka topologi yang dimaksud adalah topologi logika *(logical topologi)* yaitu gambaran bagaimana aliran data dalam suatu jaringan. Jika dilihat dari fisik pengkabelan maka topologi yang dimaksud adalah topologi fisik *(physical topologi)* yaitu bentuk layout pengkabelan yang diimplementasikan pada jaringan atau dapat juga dikatakan konfigurasi semua komputer baik *workstation* maupun *server*, peralatan serta kabel dalam suatu jaringan.

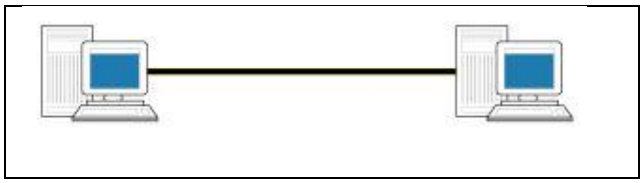
3.1.4.1 Topologi Fisik Jaringan

Menurut Wagito (2007:16), Bentuk-bentuk topologi fisik yang ada dalam sistem jaringan dapat dikelompokkan dalam dua topologi fisik dasar yaitu:

1. **Point to Point**

   Topologi fisik *point to point* adalah topologi yang menggambarkan bentuk hubungan antara dua komputer atau lebih tepatnya antara dua titik. Dua komputer dapat dihubungkan dengan beberapa cara antara lain sebagai

berikut : Jika jarak antara dua komputer tersebut tidak jauh maka dapat dihubungkan langsung menggunakan media transmisi kabel *koaksial* atau *UTP*. Jarak terjauh dari hubungan ini tergantung pada jenis media transmisi yang digunakan. Jika jarak antara komputer jauh maka hubungan dilakukan menggunakan media transmisi kabel telepon, kabel serat optik atau gelombang elektromagnetik. Dalam hubungan ini biasanya digunakan modem yang tipenya disesuaikan dengan media transmisi yang digunakan. Berikut adalah gambar visualisasinya:



(Sumber : Wagito, 2007:16)

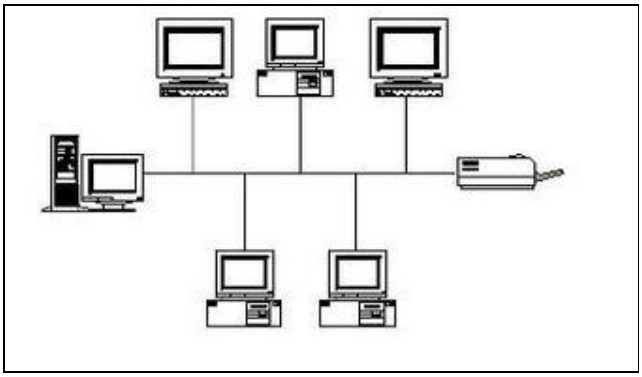
Gambar 3.4 *Point to Point*

2. *Multi Point*

Topologi fisik *multi point* adalah topologi yang menggambarkan bagaimana beberapa komputer (lebih dari dua) terhubung menggunakan media transmisi. Ada beberapa tipe topologi multi point dalam jaringan yaitu:

a. Topologi Bus

Topologi bus menggunakan sebuah kabel *backbone* dan *host* yang terhubung secara langsung pada kabel tersebut.



(Sumber : Wagito,2007:17)

Gambar 3.5 Topologi Bus

Masing-masing topologi ini mempunyai ciri khas, dengan kelebihan dan kekurangannya sendiri, yaitu sebagai berikut:

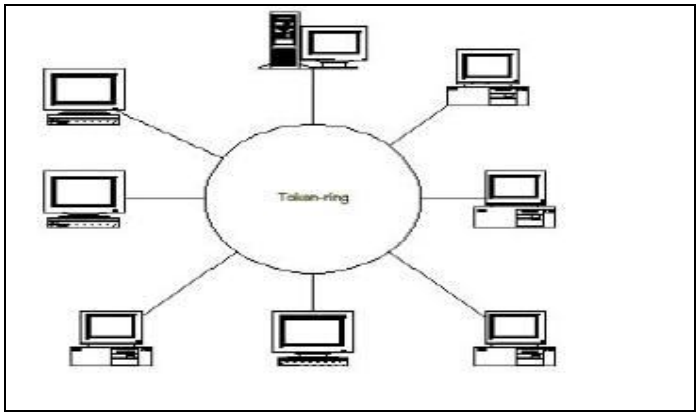
Tabel 3.1 kelebihan dan kekurangan topologi bus

Kelebihan	Kekurangan
Hemat kabel Layout kabel sederhana Mudah dikembangkan	repeater untuk jarak jauh Kepadatan lalu lintas Bila salah satu client rusak, maka jaringan tidak bisa berfungsi.

(Sumber : Wagito,2007:17)

b. Topologi Ring

Topologi Ring menghubungkan *host* dengan *host* lainya membentuk lingkaran tertutup atau *loop.* Artinya informasi dan data serta *traffic* disalurkan sedemikian rupa sehingga masing-masing *node.* Umumnya fasilitas ini memanfaatkan *fiber optic* sebagai sarananya (walaupun ada juga yang menggunakan *twisted pair).*



(Sumber : Wagito,2007:18)

Gambar 3.6 Topologi Ring

Berikut kelebihan dan kekurangan pada Topologi Ring yaitu sebagai berikut:

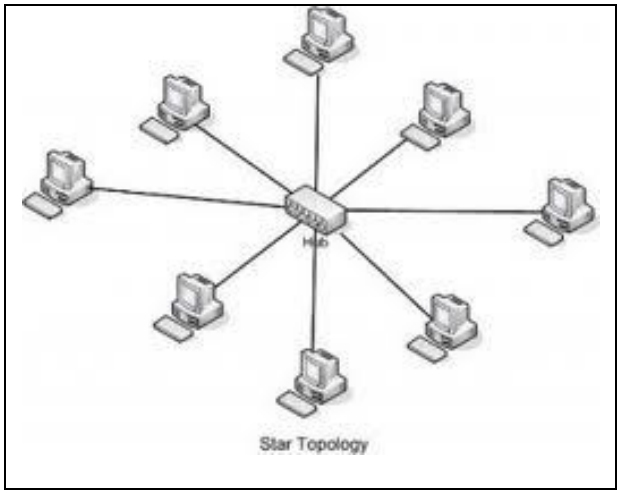
Tabel 3.2 Kelebihan dan kekurang topologi Ring

Kelebihan	Kekurangan
Proses installasi mudah Biaya install relatife murah Penambahan *node* dapat dilakukan dengan mudah Bekerja baik pada network skala kecil	Merupakan teknologi lama yang *out of date* Jika kabel putus atau rusak maka network lumpuh total Manajemen pada *netwoerk* skala besar tidak dapat dilakukan.

(Sumber : Wagito,2007:18)

c. Topologi Star

Topologi star menghubungkan semua computer pada sentral atau kosentrator. Biasanya kosentrator berupa perangkat *hub* atau *switch.*



(Sumber : Wagito,2007:19)

Gambar 3.7 Topologi Star

Berikut kelebihan dan kekurangan pada Topologi Star yaitu sebagai berikut:

Tabel 3.3 kelebihan dan kekurangan Topologi Star

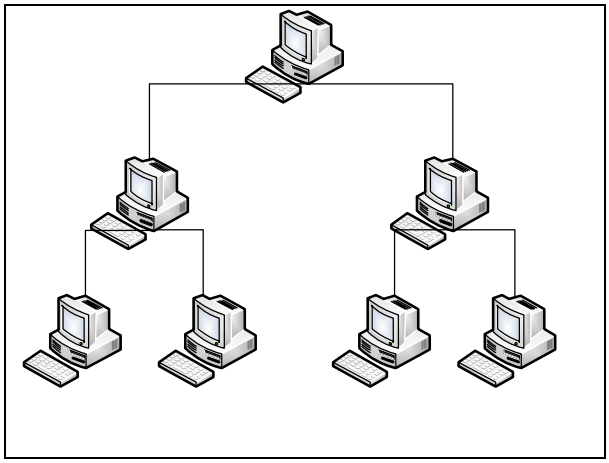
Kelebihan	Kekurangan
proses install mudah Penambahan *node* padat dilakukan dengan mudah Jika salah satu kabel rusak atau putus maka network masih dapat berfungsi manajemen network terpusat dan mudah memudahkan untuk skala besar	Biaya install cukup mahal Jika *hub* atau *switch* rusak maka *network* akan lumpuh total

(Sumber : Wagito,2007:19)

d. Topologi Tree

Merupakan gabungan dua topologi yaitu topologi bus dan topologi star yang mana meliputi beberapa kelompok konfigurasi workstation bertopologi star yang kemudian

dihubungkan dalam kabel utama sebagai bus linear. Dalam topologi tree dimungkinkan melakukan perluasan jaringan secara mudah. (Wagito,2007:19)



(Sumber : Wagito,2007:20)

Gambar 3.8 Topologi Tree

a. Topologi Logika Jaringan

Topologi logikal jaringan adalah gambaran bagaimana aliran data dalam suatu jaringan. Topologi logikal dalam jaringan dapat dikelompokkan menjadi dua macam yaitu:

1. Topologi Logika Bus

Dalam topologi logika *bus* dimana transmisi data melewati masing-masing *workstation* pada jaringan. Masing-masing transmisi dipancarkan kedalam jaringan. Dan masing-masing *workstation* menggunakan alamat untuk menentukan apakah *workstation* harus menanggapi transmisi tersebut. Dalam topologi logika *bus* setiap waktu

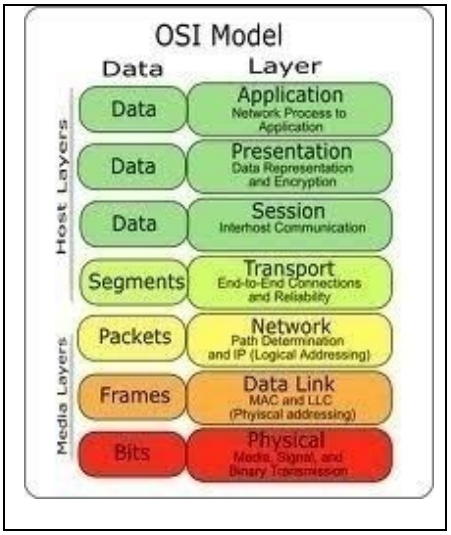
masing-masing *workstation* pada jaringan dapat menerima transmisi. (Wagito,2007:20).

2. Topologi Logika Ring

Dalam topologi logika *ring* dimana transmisi data dilakukan dari suatu *workstation* ke *workstation* berikutnya. Tranmisi data akan lebih bagus apabila topologi fisik yang digunakan juga topologi ring. Suatu cara untuk menentukan apakah topologi logika suatu jaringan menggunakan ring adalah dengan cara melihat apakah rangkaian penerima data dan pengirim data terpisah. Jika terpisah, maka workstation tersebut berfungsi sebagai repeater dan mungkin terhubung secara logika dengan topologi ring. (Wagito,2007:21).

3.1.5 Model Referensi ISO OSI Layer

Menurut Siregar, edison (2010:11), intenational Organization For Standardization (ISO) pada tahun 1997 membuat sebuah model referensi, yaitu *Open Systems Interconnection* (OSI) yang menjadi acuan untuk *network communication*. Model OSI dikatakan *Open Systems architecture* karena medel ini menghubungkan satu komputer dengan komputer yang lain menggunakan komunikasi terbuka. Komputer yang terhubung tidak harus menggunakan pabrikan dan sistem operasi yang sama.



(Sumber : Siregar,2010:15)

Gambar : 3.9 Model OSI Layer

OSI Model layer terdiri atas tujuh layer seperti gambar 3.7 masing-masing layer mengambarkan fungsi yang akan dilakukan ketika data ditransfer antara dua aplikasi yang saling berkomunikasi. OSI Model akan menjadi rujukan untuk pengembang aplikasi pada saat menggembangkan aplikasi yang akan digunakan pada jaringan. Berikut ini adalah Tujuh model OSI layer;

1. ***physical Layer***

   Layer ini bertanggung jawab untuk mengirimkan dan menerima bit-bit data dari satu komputer kekomputer lain melalui media komunikasi. Layer ini tidak harus mengerti data apa yang ada pada bit-bit tersebut. (Siregar,2010:12),

2. *Data-Link Layer*

Menurut Siregar, (2010:12), layer ini berfungsi adalah untuk mengatur aliran bit-bit data yang akan dikirimkan. Layer ini menerima paket data dari layer yang diatasnya, yaitu Network layer dan mengubahnya menjadi frame-frame. Frame-frame inilah yang selanjutnya diatur untuk dikirimkan melalui *physical* layer. Pada layer ini juga dilakukan *error checking* sebelum dikirimkan menggunakan CRC (*Cylic Redudancy Checking*). Data CRC tersebut akan ditambah ke dalam data sebenarnya yang nantinya berfungsi untuk memeriksa apakah ada frame yang rusak. Jadi layer ini memastikan bahwa data yang dikirim tidak rusak atau salah. Data-Link Layer terdiri dari 2 jenis yaitu :

a. *Logical Link Control* (LLC)

Berguna untuk melakukan dan memelihara link komunikasi secara logical antara dua media komunikasi.

b. *Media Access Control* (MAC)

Layer ini akan mengatur peralatan-peralatan agar bisa berbagi satu media yang sama ketika melakukan komunikasi.

3. *Network Layer*

Menurut Siregar, (2010:13), layer ini berfungsi akan bertanggung jawab untuk menanggani perpindahan paket-paket data antara dua peralatan yang terhubung secara kompleks. Layer ini akan bertugas untuk memutuskan apakah sebuah paket data

harus di-*routing* atau harus di-*forwarding* hingga data tersebut menemukan alamat tujuan yang diinginkan. *Network* layer juga bertanggung jawab membagi-bagi paket data yang besar kedalam porsi yang lebih kecil bila paket data yang besar terssbut lebih besar dari frame data yang diterima oleh data link-layer. Pada sisi penerima, *network* layer juga akan menggabungkan frame data tersebut ke paket yang sebenarnya. Paket layer ini akan terjadi hal-hal berikut :

a. Pengalamatan, alamat logical jaringan dan alamat *services*
b. Switching (*Circuit, Message, Packet*)
c. Menemukan atau memilih route
d. Layanan koneksi, termasuk *Network Layer Flow Control, Network Layer Error Control,* dan *Packet Squence Control*
e. Layanan *Gateway.*

4. *Transport Layer*

Layer ini berfungsi akan memastikan data yang terkirim bebas dari kesalahan, urutannya benar, dan tidak ada data yang hilang atau terduplikasi. Layer ini juga bertugas memecah data yang data dari sesi layer menjadi paket-paket kecil untuk dikirim kekomputer tujuan. Layer ini juga mengirimkan *acknowledgment* (ACK) setiap pengiriman data. (Siregar,2010:13),

5. *Session Layer*

layer ini berfungsi untuk memperbolehkan aplikasi pada komputer yang berbeda untuk berbagi koneksi yang biasa disebut *session*. Layer ini menyediakan layanan seperti *name lookup* dan *security* sehingga dua program bisa mengadakan link komunikasi. Session layer juga bertanggung jawab untuk melakukan sinkronisasi data dan *checkpointing* sehingga jika terjadi kegagalan pada *network*, hanya data yang dikirim setelah terjadi kegagalan saja yang akan dikirim ulang. Pada layer ini juga terjadi dialog antara dua proses dan menentukan siapa yang bisa mengirim data dan siapa yang harus menerima selama terjadi komunikasi. (Siregar,2010:14),

6. *Presentation Layer*

Layer ini berfungsi menerjamahkan format data yang diperlukan dan diharapkan oleh komputer. Pada layer ini akan dilakukan *translation, compression, dan encryption* terhadap data. Yang terjadi pada *presentation* layer adalah manipulasi data bukan fungsi komunikasi. (Siregar,2010:14),

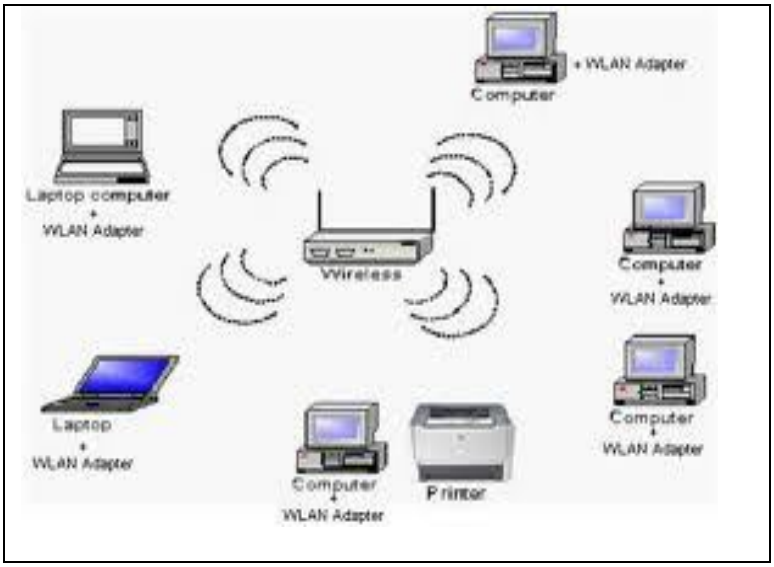
7. *Application Layer*

Layer ini berfungsi menyediakan layanan untuk pengguna akhir misalnya *database*, file *transfer*, dan email. Jadi layer ini merupakan *user interface* (antarmuka pengguna). (Siregar,2010:14),

3.1.6 Jaringan WLAN (*Wireless Local Area Network)*

Jaringan WLAN merupakan salah satu bentuk jaringan *wireless.* Media transmisi yang digunakan untuk berkomunikasi pada jaringan *WLAN* adalah gelombang *elektromagnetik* yang dapat berupa sinar - infra-meraj (*infrared),* gelombang mikro (*mikro move),* atau gelombang radio (*radio frequensi).* Teknologi *WLAN* membolehkan pengguna untuk membangun jaringan *nirkabel* dalam suatu area yang bersifat local (dalam lingkungan gedung kantor, kampus, atau area public, seperti bandara atau kafe). Jaringan WLAN dapat melakukan transfer data hingga 108 Mbps.

Jaringan WLAN memerlukan peralatan NIC khusus yang dapat dipasang pada slot PCI, USB ataupun PCMCIA. NIC untuk jaringan WLAN dilengkapi dengan antenna sebagai pengganti port kabel. Masing-masing peralatan yang terhubung dalam jaringan WLAN dapat melakukan hubungan secara add-hoc antara peralatan atau melalui WAP (*Wireless Access Point)* yang berlaku sebagai Hub atau konsentrator. (Wagito,2007:14)



(Sumber : Wagito,2007:73)

Gambar : 3.10 Jaringan WLAN

Ada 3 (tiga) metode keamanan yang diterapkan dalam jaringan *WLAN* sebagai berikut:

1. WEP (*Wired Equivalent Privacy)*

   Metode ini dimaksudkan untuk enkripsi untuk *autentikasi user* dan enkripsi data payload yang dilewatkan lewat jaringan *wireless.* WEP menggunakan algoritma *Pseudo Radom Number Generator (*PRNG) dan RC4 *stream chipper* atau *block chipper*. Kedua tipe *chipper* ini akan memunculkan sebuah *key stream* dari kunci rahasia tersebut. *Key stream* ini dicampur dengan data untuk memunculkan *output* yang telah terenkripsi (Hantoro, 2009:80)

2. SSID (*Service Set Identifier)*

   SSID merupakan nama *network* dari suatu jaringan WLAN, dan dapat diset sesuai dengan keinginan *administrator*. SSID

dikenal juga dengan istilah ESSID. Fungsi dari SSID dikaitkan dengan keamanan WLAN adalah merupakan garda terdepan terhadap system keamanan WLAN. Setiap *client* yang akan masuk jaringan WLAN atau ter hubung ke AP (*access point)* maka harus mengetahui SSID dari AP tersebut. (Hantoro, 2009:77).

3. Filter Alamat MAC (*Metode Access Kontrol).*

   Metode ini biasanya digunakan untuk memfilter semua *station* yang akan melakukan koneksi ke AP sehingga *station* yang MAC *address-nya* tidak terdapat dalam setingan AP tersebut tidak dapat melakukan koneksi, dan dapat menyaring *client* mana saja yang bias masuk ke jaringan setelah proses *Open Sistem Authentication* dan *Shared Key Authentication.(*Hantoro,2009:78).

3.1.7 Wi-Fi (*Wireless Fidelity)*

Wi-Fi adalah satu standar *Wireless Networking* tanpa kabel, hanya dengan komponen yang sesuai dapat terkoneksi ke jaringan. Yang didasari pada spesifikasi sebagai berikut:

1. IEEE 802.11a yaitu Wi-Fi dengan frekuensi 5 Ghz yang memiliki kecepatan 54 Mbp dan jangkauan jaringan 300 m.
2. IEEE 802.11b yaitu dengan frekuensi 2,4 Ghz yang memiliki kecepatan 11 Mbp dan jangkauan jaringan 100 m.
3. IEEE 802.11g yaitu dengan frekuensi 2,4 Ghz yang memiliki kecepatan 54 Mbp dan jangkauan jaringan 300 m.

Teknologi Wi-Fi yang akan diimplementasikan adalah standar . (Priyambodo, 2005:01).

3.1.8 Standar *Wireless* LAN

Berikut ini adalah dua standar utama dari IEEE untuk *wireless LAN* yang digunakan saat ini.

1. 802.11 standar *indoor* (Hantoro,2009:40)
   a. 802.11 2,4 GHz 2 Mbps
   b. 802.11a 54 Mbps
   c. 802.11b 11 Mbps
   d. 802.11g 54 Mbps
   e. 802.11n 600 Mbps
2. 802.16 standar *outdoor* salah satunya adalah WiMAX (*World Interoperbility For Microwaver Access).*

Secara umum perbandingan di antara ke empat standar dimaksudkan dapat dijabarkan seperti pada tabel di bawah ini :

Tabel 3.4 Perbandingan Standar Wireless LAN

	802.11a	**802.11b**	**802.11g**	**802.11n**
Standard Approved	July 1999	July 1999	June 2003	Not yet ratified
Maximum data rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Modulation	OFDM	DSSS or CCK	DSSS or CCK or OFDM	DSSS or CCK or OFDM
RF Band	5 Ghz	2.4 Ghz	2.4 Ghz	2.4 or 5 Ghz
Nomber of Spatial Streams	1	1	1	1,2,3,4
Channel Widht	20 MHz	20 MHz	20 MHz	20 or 40 MHz

Sumber : (Hantoro,2009:43)

3.1.9 Topologi *Wireless* LAN

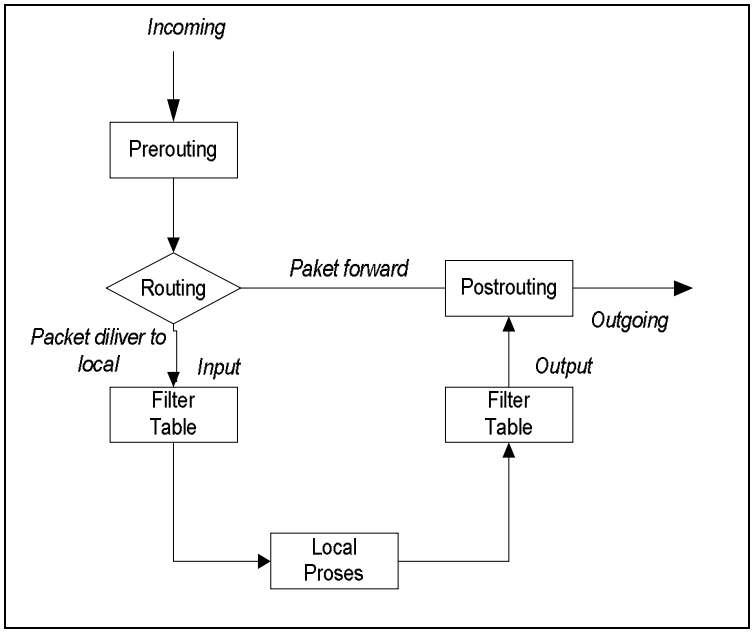
Wireless LAN terdiri dari 2 (dua) jenis topologi (Wagito,2005:71-72)

1. *Ad hock (peer to peer wireless)* yakni setiap computer dengan terpasang *wireless* LAN *card* dapat saling terhubung tanpa melalui perangkat *Access Point (*AP).
2. Topologi *Infrastruktur (Point To Multi Point Wireless)* yakni setiap computer dapat saling terhubung dengan computer lain melalui perangkat *Access Point* sebagai jalur pusat komunikasi. Setiap *Access Poin* memiliki IP *address, SSID, User Nama* dan *password* default.

3.1.10 IP*Tables*

IP*Table* merupakan suatu program yang digunakan untuk memasukkan dan menghapus isi tabel tersebut filter paket kernel. Dengan demikian, apapun yang dituliskan dalam tabel tersebut akan hilang ketika dilakukan reboot terhadap system. Supaya system dapat selalu mempunyai kemampuan filter paket yang diinginkan, aturan-aturan yang diberikan dapat ditulis dalam skrip inisialisasi. Dapat juga digunakan perintah iptables-save untuk menyimpan aturan yang diberikan dan perintah *iptables-restore* untuk menjalankan semua aturan yang sudah ditulis. (Wagito,2007:146)

Sebenarnya IPTable tidak hanya bisa digunakan untuk membangun Firewall, tetapi juga dapat dionfigurasikan menjadi sebuah router unuk menghubungkan subnet network yang berbeda. (Siregar, 2007:109).



(Sumber : Siregar,2007:109)

Gamabar 3.11 Aliran Paket Data

Pada diagram tersebut, *chain* merupakan sebuah aturan atau *rule* yang digunakan firewall ketika melakukan peyaringan paket data yang dating dan yang dikirim. Bila paket tidak memenuhi criteria chain pertama, maka chain berikutnya akan diperiksa. Bila semua chain tidak terpenuhi, maka paket data tersebut akan ditolak (*rejected)*. Chain pada filter table ada 3, yaitu : INPUT, OUTPUT dan FORWAD. (Siregar,2007:110).

3.1.11 Pengalamatan Ip *Address*

IP *Address* adalah alamat yang diberikan pada jaringan dan peralatan jaringan yang menggunakan *protocol* TCP/IP, IP *address* terdiri dari 32 Bit angka *biner* yang dapat ditulis sebagai empat kelompok angka decimal yang dipisahkan oleh tanda titik seperti 192.160.42.1 oleh karena *protocol* IP adalah *protocol* yang paling banyak dipakai untuk meneruskan (*routing*) informasi didalam jaringan computer.

Tabel 3.5 IP Address

Network ID			**Host ID**
192	160	42	1

(Sumber : Wagito,2007:75)

3.1.12 Kelas-kelas IP *Address*

IP *Address* terdiri atas 32 bit angka biner, yang dapat ditulis dalam empat kelompok, terdiri dai 8 bit (octet) decimal yang dipisahkan oleh tanda titik, 11000000.10100000.10101000.00000001 dan dapat ditulis dalam bentuk empat kelompok decimal (0-255) dan dapat juga ditulis dengan simbolik dapat ditulis dengan angka w.x.y.z. IP address terdiri dari 3 bagian yaitu *Network* ID dan *Host* ID, dimana *Network* ID menentukan alamat dari peralatan jaringan, sedangkan *Host* ID diibaratkan sebagai nama rumah, nomor rumah, nama jalan.

Untuk mempermudah pemakaian, tergantung kebutuhan pemakai, maka IP *address* dibagi 3 kelas.

Tabel 3.6 Kelas-Kelas IP Address

Kelas	Network ID	Host ID	Defaul Subnet Mask
A	W	X.Y.Z	255.0.0.0
B	W.X	Y.Z	255.255.0.0
C	W.X.Y	Z	255.255.255.0

(Sumber : Wagito, 2007:81)

Tabel 3.7 Jumlah *Network* dan *Host* dari Kelas-Kelas IP *address*

Kelas	**Range**	**Jumlah Maksimum Network**	**Jumlah Maksimum Host Per Network**
A	1-126	126	167777214
B	128-191	16384	65534
C	192-223	2097152	254

(Sumber : wagito, 2007:79)

Dari tabel di atas terdapat 3 (tiga) kelas IP *address* yaitu A,B,C yang sering dipakai.

Agar suatu jaringan dapat mengetahui kelas mana yang dipakai oleh IP *address*, dipergunakan *default subnet mask.* Setiap IP *address* harus memiliki default *subnet mask.* Angka decimal 255 (11111111) dari *default subnet mask* menandakan bahwa octet (8 bit) yang bersangkutan dai IP *address* adalah untuk *network* ID. Sedangkan angka decimal 0 (00000000) dai *default subnet mask* menandakan bahwa octet yang bersangkutan dari IP *address* adalah untuk *host* ID.

Contoh :

IP *address*	: 20.0.0.1
Default subnet mask berada di kelas A	: 255.0.0.0
IP *address*	: 172.100.0.1
Default subnet mask berada di kelas B	: 255.255.0.0
IP *address*	: 192.100.10.1
Default subnet mask berada di kelas C	:255.255.255.0

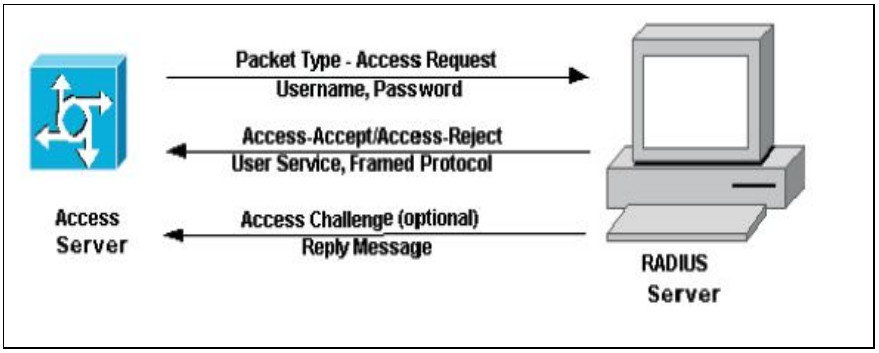
Pada kelas A jumlah *network* ID sangat sedikit dibandaingkan *host* ID-nya dikarnakan octet pertamanya dipakai untuk *host* ID. Kelas B memberikan jumlah yang sama untuk *network* ID dan *Host* ID, sedangkan kelas C memberikan jumlah paling banyak untuk *Network* ID dan sedikit *Host* ID.

3.2 RADIUS (*Remote Authentication Dial-in User Service)*

RADIUS adalah system berbasis *client-server* yang menggunakan *cisco* dari para penyusup. RADIUS adalah *protocol* yang diimplementasikan pada *Cisco IOS Softwere* yang mengerim otentikasi *request ke radius server*. Radius *server* biasanya merupakan *server* yang mengerjakan dengan berbagai *flatform,* termasuk *Microsoft NT Server* atau UNIX *host. Radius* dapat mengotentikasi pengguna *router, vendor,* dan bahkan IP *router* yang sah. (Thomas, 2005:141).

3.2.1 Prinsip Kerja Radius

RADIUS merupakan protocol *security* yang bekerja menggunakan system *clien-server* terdistribusi yang banyak digunakan bersama AAA untuk mengamankan jaringan pengguna yang tidak berhak. RADIUS melakukan autentikasi *user* melalui serangkaian komunikasi antara *client-server.* Bila *user* berhasil melakukan autentikasi, maka *user* tersebut dapat menggunakan lanyanan yang disediakan oleh jaringan. (Lukman dan yadi :06)



Gambar : 3.12 Autentikasi Antara NAS dengan Radius Server

Keterangan :

a. *User* melakukan *deal-in* menggunkan *modem* pada *network Access server (NAS).* NAS akan meminta *user* memasukkan nama dan *password* jika koneksi *modem* berhasil dibangun.

b. NAS akan membangun paket data berupa informasi, yang dinamakan *access-request.* Informasi ini diberikan NAS pada server RADIUS berisi informasi spesifikasi dari NAS itu sendiri yang miminta *access-request, port* yang digunakan untuk koneksi modem serta nama dan *password.* untuk proteksi dari *huckers,* NAS

yang bertindak sebagai RADIUS *client*. Melakukan enkripsi *password* sebelum dikirim pada RADIUS *server*. *Access-request* ini dikirimkan pada jaringan dari RADIUS client ke RADIUS server. Jika RADIUS server tidak terjangkau, RADIUS *client* dapat melakukan pemindahan rute pada server alternative pada konfigurasi NAS.

c. Ketika *access-request* diterima, Server autentikasi akan memvalidasi permintaan tersebut dan melakukan dekripsi paket data untuk memperoleh informasi nama dan *password*. Jika nama dan *password* sesuai dengan basis data pada server, server akan mengirim *access-accept* yang berisi informasi kebutuhan system *network* yang harus disediakan oleh *user,* missal Radius Server akan menyampaikan pada NAS bahwa *user* memerlukan TCP/IP dan *Netware* menggunakan PPP (*Point-to-Point Protocol)* atau *user* memerlukan SLIP (*Serial Line Internet Protocol)* untuk dapat terhubung dengan jaringan. Selain itu *access-accep* ini dapat berbasis informasi untuk membatasi akses *user* pada jaringan. Jika proses *login* tidak memenuhi kesesuaian, maka Radius Server akan mengirim *access-reject* pada NAS dan *user* tidak dapat mengakses jaringan.

d. Untuk menjamin permintaan *user* benar-benar diberikan pada pihak yang benar, Radius Server mengirim *authentication key* atau *signature* yang menandakan keberadaan Radius *client.*

Ketika *user* akan melakukan koneksi maka radius server akan melakukan filter terhadap paket-paket data yang dikirim apakah *user*

dan password sudah terdaftar pada *dialup admin* yang dilakukan oleh *administrator* jaringan. Bila sudah terdaftar maka autentikasi *user* yang akan melakukan akses akan di teruskan dan bila belum terdaftar maka *user* akan ditolak, easyhotspot merupakan *tools* pencatata (*accounting*) yang berfungsi sebagai proses dari pertama kali *user* mengakses sebuah sistem, apa saja yang di lakukan *user* di system tersebut dan sampai proses terputusnya hubungan komunikasi antara *user* tersebut dengan sistem, dicatat dan didokumentasikan disebuah database *MySQL*. Jadi pembatasan hak akses bagi karyawan digunakan autentikasi yaitu pengecekan wewenang pengguana, mana saja hak-hak akses yang diperbolehkan dan yang tidak. Khusus untuk karyawan *autorisasi* dibatasi dengan mengguanakan *rodgroupreply*, seperti keterangan dibawah ini;

a. *Session-Timeout* = 14400; berarti maksimal dalam 1 sesi logi adalah jam atau 28800 s.
b. *Idle-Timeout* = 600; maksimal waktu idle adalah 600 s atau 10 meneti.
c. *Acc-Interim-Interval* = 60; *Interval Request* adalah 60 s atau 1 menit.
d. *WISPr-Redirection-URL* = http://www.google.com; saat *login* maka halamat *web* yang pertama kali muncul adalah halaman *web* www.google.com.

e. *WISPr-Bsndwidth-Max-Up* = 16000; maksimal *upload* kecepatannya 16000 *bps.*

f. *WISPr-Bsndwidth-Max-Down* = *32000;* maksimal kecepatan *Download* 32000 *bps.*

g. *Simultaneous-Use* = 1; hanya mengizinkan 1 orang 1 kali *login*.

h. *Aunth-Type* = mengizinkan hanya *autentikasi* local.

Berdasarkan gambaran topologi di atas terdapat perbedaan dari rancangan jaringan yang sebelum dan yang akan di bangun yaitu adanya *Radius Server* dan *wireless access point* sebagai media komunikasi data.

3.2.2 Aspek Keamanan Radius

Protocol Radius yang digunakan sebagai salah satu system keamanan *wireless* LAN melalui autentikasi pengguna *wireless* LAN, ternyata memiliki beberapa lubang keamanan. Mekanisme proteksi menggunakan nama pengguna dan *password* ternyata tidak cukup aman untuk diterapkan. Paket *access-request* yang tidak di autentikasi oleh Radius Server. Beberapa lubang keamanan protocol Radius adalah sebagai berikut;

a. MD5 dan *Shared Secret*

Metode *Shared Secret* sudah sangat beresiko untuk di terapkan dari *client* ke Radius *server.* Hal ini dikarenakan lemahnya MD5 *hash* yang menyimpan tanggapan autentikator. *Hecker* atau penyusup dapat dengan mudah mengetahui paket *access-request*

beserta tanggapannya. Penyusup dapat dengan mudah mengetahui *Shared Secret* dengan cara melakukan perhitungan awal terhadap perhitungan MD5.

b. Paket *Access-request*

Tidak adanya autentikasi dan verifikasi terhadap paket *Access-request* merupakan salah satu kelemahan dari protocol RADIUS. Paket *Access-request* harus berisi atribut IP *access point (*AP), nama pengguna beserta *password* atau CHAP-*Password, port* yang digunakan oleh *access point* nama pengguna beserta *password* disembunyikan dengan memakai metode RSA *Message Digest Algorithm* MD5. RADIUS Server akan memeriksa dan memastikan bahwa pesan yang dikirim oleh alamat IP adalah salah satu dari *client* yang terdaftar. Sehingga penyusup dapat mengetahui dan menggunakan alamat IP yang menjadi *client* dan Radius Server ini. Hal ini merupakan salah satu keterbatasan dari rangcangan *protocol* Radius.

c. Pemecahan *Password*

Skema proteksi password yang dipakai adalah *stream-chiper*, dimana MD5 digunakan sebagai sebuah ad hoc *pseudorandom number generator* (PRNG). 16 oktet pertama bertindak sebagai sebuah *synchronous stream chipper*. MD5 *hash* secara umum digunakan untuk *crypthographic hash*, bukan *stream chipper*. Ada kemungkinan masalah keamanan yang ditimbulkan dari pengguan

MD5 *hash* tersebut. Seperti yang dijelaskan diatas bahwa atribut *password* diamankan dengan metode *stream chipper*. Hal ini memungkinkan penyusup mendapatkan informasi *shared secret* apabila mereka melakukan *sniffing* ke jaringan *wereless* dan mencoba masuk ke RADIUS *Server*.

d. Request Authenticator

Keamanan RADIUS bergantung pada pembangkitan *Request Authenticator*. *Request Authenticator* ini harus unik dan tidak diprediksi untuk menjaminm keamanan. Protocol RADIUS tidak menekankan pada pentingnya pembangkitan *Request Authenticator*, sehingga banyak implementasi yang menggunakan PRNG yang kurang dalam membangkitkan *Request Authenticator*.

3.2.3 Sistem Keamanan

1. Standar Keamanan 802.11

RADIUS (*Remote Access Dial-in User Service*) merupakan suatu protokol *client-server* yang dikembangkan untuk mekanisme akses kontrol yang memeriksa dan mengautentikasi pengguna berdasarkan protokol AAA (Autentikasi, Autorisasi, Akutansi). (Sumber: Deris Stiawan, 2008 http://www.ilkom.unsri.ac.id/deris.

a. Autentikasi *(Authentication)*

Yaitu proses memeriksa identitas dari seorang pengguna untuk memastikan apakah *user* tersebut benar telah terdaftar dalam jaringan *wireless* tersebut.

b. Autorisasi *(Authorization)*

Berperan sebagai suatu kumpulan aturan yang membatasi fasilitas apa yang boleh dan dapat diakses oleh seorang pengguna yang telah terautentikasi.

c. Akuntansi *(Accounting)*

Suatu proses pencatatan dari awal saat seorang pengguna mengakses jaringan dalam suatu *hotspot*.

FreeRADIUS merupakan salah satu server RADIUS modular berbasis sumber terbuka yang memiliki banyak fitur dan kemampuan yang tidak kalah dengan RADIUS server komersial. Salah satu buktinya adalah sudah mendukung beberapa *Access Point* (AP) / *Network Access Server* (NAS) yang umum, dan mendukung berbagai macam sumber data pengguna dari file teks, LDAP, SQL (MySQL, Oracle, PostgreSQL, MSQL). FreeRADIUS juga dapat berjalan di berbagai sistem operasi, seperti Linux, FreeBSD, OpenBSD, OSF, Sun Solaris, dan lain sebagainya.

Berikut beberapa kelebihan dan kekurangan Radius Server:

Tabel : 3.8 kelebihan dan kekurangan Radius

Kelebihan	Kekurangn
Menjalankan sistem administrasi terpusat Protokol *connectionless* berbasis UDP yang tidak menggunakan koneksi langsung Mendukung autentikasi *Password Authentication Protocol* (PAP) dan *Challenge Handshake Authentication Protocol* (CHAP) *Password* melalui PPP	Tidak adanya utentikasi dan erifikasi terhadap *access request* lak sesuai digunakan pada jaringan ngan skala yang besar D5 dan *shared ecret*; metode *ared secret* sudah berisiko untuk erapkan, hal ini karenakan nahnya MD5 hash yang nyimpan tanggapan autentikator ingga *acker* / penyusup dapat ngan mudah mengetahui paket *cess-request* beserta tanggapannya ngan cara melakukan penghitungan al terhadap perhitungan MD5

(Sumber :Deris, 2008 http://www.ilkom.unsri.ac.id/deris)

2. SSID (Services Set Identifier)

SSID merupakan nama network dari suatu jaringan WLAN, dan dapat diset sesuai dengan keinginan administrator. SSID dikenal juga dengan istilah ESSID. Fungsi SSID dikaitkan dengan keamanan WLAN adalah merupakan garda terdepan terhadap sistem keamanan WLAN. Setiap client yang akan masuk jaringan WLAN atau terhubung ke AP maka harus mengetahui SSID dari AP tersebut.

SSID pada dasarnya dapat diset broadcast maupun tidak. Bila diset broadcast maka sangat mudah diketahui oleh pengguna yang mempunyai WLAN card. Semua device (notebook atau PDA) dengan scanning jaringan WLAN baik dengan software bawaan WLAN card maupun software tambahan lainnya.

3. MAC Filtering

Sistem pengamanan yang ketiga adalah dengan memanfaatkan filtering MAC (Medium Access Control) address. Teknik ini biasanya digunakan untuk memfilter semua station yang akan melakukan koneksi ke Access Point sehingga station yang MAC Address-nya tidak terdapat dalam settingan AP tersebut tidak dapat melakukan koneksi. Teknik ini juga membantu menyaring client mana saja yang bisa masuk ke jaringan setelah proses *Open System Authentication dan Shared Key Authentication.*

4. WEP (Wired Equivalent Privacy)

WEP adalah algoritma enkripsi (shared key authentication proses) untuk autentikasi user dan enkripsi data payload yang dilewatkan lewat jaringan wireless. Dengan demikian seperti namanya, maka sistem WLAN dirancang agar sama amannya dengan jaringan Wired LAN. WEP menggunakan algoritma *Pseudo Random Number Generator (PRNG)* dan RC4 *stream* chiper atau *block chiper.* Kedua tipe chiper ini akan memunculkan sebuah key stream dari kunci rahasia tersebut. *Key Stream* ini dicampur dengan data untuk memunculkan output yang telah terenkripsi.

5. WPA (Wi-Fi Protectes Access)

WPA merupakan perbaikan di sisi WEP di kalangan industri, nama WPA juga dikenal dengan nama 803.11i. beberapa

hal yang menjadi pertimbangan dalam menggunakan WPA adalah WEP menggunakan sebuah kunci statis yang terpisah untuk transmisi global seperti paket broadcast. Namun kunci ini tidak diperbaharui secara regular. Meskipun data-data penting tidak ditransmisikan secara broadcast, penggunaan kunci statis untuk transmisi global memberikan kesempatan pada penyerang untuk mengetahui kunci-kunci tersebut dan dapat masuk ke dalam jaringan.

6. Autentikasi

Dalam Penggelaran WLAN yang biasa, maka user tidak perlu melakukan autentikasi terlebih dahulu. Asal dapat mengetahui SSID-nya, maka user akan langsung dapat tersambung ke jaringan WLAN. Dengan peambahan level security autentikasi, maka user diwajibkan untuk memasukkan username dan password agar bisa tersambung ke jaringan WLAN. Teknis dari penerapan sistem autentikasi dapat dilakukan secara lcal (data base terletak di AP) atau dilakukan secara remote (menggunakan server radius). Untuk jaringan yang besar dan butuh pengamanan yang lebih tinggi maka lebih baik menggunakan autentikasi remote. Jadi database user diinstall di server radius.

3.3 Chillispot

Chillispot adalah software *access controller open source*, berbasis pada Chillispot project yang sekarang sudah tidak aktif. Lebih tepatnya,

Chillispot aktif dikembangkan oleh kontributor Chillispot. Chillispot juga bisa diartikan sebagai sebuah *software access control* yang kaya akan fitur, yang dapat memberikan captive portal / walled-garden environment dan menggunakan RADIUS untuk mengontrol akses dan akunting. Chillispot adalah bagian integral dari firmware CoovaAP OpenWRT.

Cara Kerja Chillispot adalah Chillispot akan mengambil alih control dari internal interface (eth1) menggunakan socket raw promiscuous. Chillispot kemudian akan menggunakan kernel modul vtun untuk membangun interface virtual (bisa tun au tap) untuk meneruskan packet yang di terima atau di kirim ke WAN. Pada dasarnya, kernel modul vtun digunakan untuk memindahkan paket IP dari kernel ke mode user, sedemikkan hingga Chillispot dapat berfungsi tanpa non-standard kernel module. Chillispot kemudian akan memberikan DHCP, ARP, and HTTP Hijacking pada interface "dhcpif". Sebuah client / laptop akan tersambung ke Interface ini akan di batasi oleh "walled garden" sampai di authorisasi. Client / laptop hanya akan dapat memperoleh DNS dan Web site yang sudah di approved oleh "walled garden". Authentikasi (dan authorisasi) di Chillispot akan dilakukan menggunakan salah satu dari dua cara berikut. Apakah itu menggunakan MAC based authentication (menggunakan pilihan macauth di chilli.conf) atau menggunakan cara "Universal Access Method" (UAM). Metoda yang ke dua menggunakan captive portal yang akan menginisiasi proses authentikasi. Saat sebuah client yang tidak ter-authentikasi berusaha untuk mengakses Web (pada port 80), permohonan

untuk menyambung ke Web akan di tangkap oleh Chillispot dan akan di redirect ke captive portal. Dalam kasus kita, kita akan menggunakan sebuah perl-script dengan nama hotspotlogin.cgi (yang di jalankan oleh apache melalui https).

Hotspotlogin.cgi akan menyajikan halaman ke user dengan kolom username dan password. Data authentikasi ini akan di forward ke Freeradius server, yang akan kemudian mencocokkan informasinya ke back end menggunakan PAP, CHAP, atau MSCHAPv2. Freeradius *back-end* disini adalah mysql. User kemudian akan ditentukan apakah ditolak atau diijinkan oleh Freeradius, yang akan disampaikan oleh hotspotlogin.cgi dalam bentuk message/pesan penolakan atau pemberitahuan sudah sukses. (Sumber :Wirawan DEA, http://oc.its.ac.id, 2008)

3.4 MySQL

MySQL merupakan salah satu RDBMS (*Relational Database Management System*) di bawah lisensi GPL yang bersifat sumber terbuka dan bebas untuk didistribusikan. MySQL menggunakan bahasa SQL (*Structured Query Language*) yang merupakan bahasa query standar yang digunakan luas. MySQL umum digunakan dalam aplikasi berbasis web karena sifatnya yang gratis, stabil dan cepat, kemudahan penggunaan, *cross-platform* berjalan baik di UNIX maupun *platform* Windows, serta dukungan yang luas. Dalam penggunaannya dengan *server* RADIUS, PHP dipergunakan untuk membangun logika dan antarmuka aplikasi, sedangkan MySQL untuk menyimpan data autentikasi yang berisi data login para pengguna, data

autorisasi yang berisi hak akses dari pengguna, dan data-data akuntansi yang mencatat penggunaan setiap *user*. Data ini kemudian akan dipergunakan oleh modul SQL FreeRadius untuk mengatur pembatasan akses pengguna.

MySQL merupakan salah satu SQL database *open source* yang sangat popular saat ini dan menawarkan fitur dan fungsi yang sangat berguna, termasuk aspek keamanan. (Hantoro, 2010:102).

Berikut fitur-fitur yang mendukung MySQL, yaitu ;

a. Multi – threading, mendukung query *multiple simultaneous.*
b. Mendukung penggunaan *password* pada system dan kepemilikan yang fleksibel.
c. Dapat mencapai 16 keys per tabel. Setiap key dapat dipakai samapail 15 field.
d. Mendukung *field primery key, field-field key* dan unik pada *create.*
e. Dukungan terhadap satu sampai empat *bit int, fload, double, fixed* dan panjang *string variable, time stamps.*

3.5 Penelitian Terdahulu

3.5.1 Penelitian 1

Berjudul “Sistem Otentikasi,Otorisasi dan Pelaporan Koneksi *User* Pada Jaringan *Wireless* menggunakan Chillipspot dan Radius Server di Fakultas Teknologi Industri Jurusan Teknik Informatika Universitas Islam Indonesia” disusun Oleh : **Gesit Singgih Febyatmoko, Taufiq Hidayat, Mukhammad Andri S.**

Sistem otentikasi, otorisasi, dan pelaporan koneksi user pada jaringan *wireless* dalam penelitian ini meliputi tiga bagian. Bagian yang pertama adalah membangun server UAM (Universal Access Method) dengan chillispot. Kedua adalah konfigurasi server Radius menggunakan software Freeradius. Ketiga adalah membangun aplikasi Sistem Administrasi Hotspot berbasis web menggunakan bahasa pemrograman PHP yang memberikan abstraksi pembangun antarmuka dan pengaksesan basis data menjadi lebih mudah. Studi kasus diimplementasikan pada jaringan Fakultas Teknik Industri UII dan juga diterapkan pada NOC UIINET (percobaan). Setelah dilakukan pengujian terhadap system ini, terbukti bahwa level keamanan WLAN dan pembagian akses layanan dapat menjadi lebih baik. Penggunaan layanan jaringan juga dapat dimonitor oleh administrator melalui aplikasi berbasis web.

3.5.2 Penelitian 2

Berjudul “Sistem Autentikasi Pengguna *Wireless* LAN Berbasis Radius Server” Dosen Tetap Universitas Bina Darma Jurusan Teknik Informatika Universitas Bina Darma” disusun Oleh : **Yesi Novaria Kunang & Ilman Zuhri Yadi.**

Teknologi ini akan memberikan jaringan akses yang mudah bagi pengguna. Namun, kita perlu sistem yang canggih manajemen informasi untuk mengontrol *bandwidth* untuk tujuan *administratif*. Pada

penelitian ini, kami akan merancang otentikasi LAN nirkabel menggunakan server yang sistem informasi dan basis data. Sistem ini juga dirancang mampu untuk membatasi pemakaian *bandwidth* di jaringan server otentikasi LAN nirkabel. studi kasus akan dilakukan di Bina Darma University. Sebuah analisis kebutuhan bagi pengguna (staf dan siswa), administrator dan sistem rekayasa akan dilakukan untuk mengembangkan desain sistem otentikasi dan identifikasi nirkabel LAN server untuk hot-spot pengguna di lingkungan Universitas Bina Darma.

BAB IV

METODE PENELITIAN

4.1 Lokasi dan Waktu Penelitian

4.1.1 Lokasi

Penelitaian ini berlokasi di Pengadilan Tinggi Palembang Jl. Jendral sudirman KM 3.5 palembang.

4.1.2 Waktu Penelitian

waktu yang dibutuhkan dalam melakukan penelitian di mulai dari bulan Maret 2012 sampai dengan April 2012.

4.2 Jenis Data

Data merupakan sesuatu bentuk informasi yang sangat penting dalam melakukan penelitian. Dalam penulisan skripsi ini Penulis menggunakan beberapa jenis data dalam pengumpulan data, yang terdiri dari:

4.2.1 Data Primer

Menurut Umar (2007:42), Data primer merupakan data yang didapat dari sumber pertama baik secara individu atau perseorangan seperti hasil dari wawancara atau hasil pengisian kuesioner yang biasa dilakukan oleh peneliti.

Data primer tersebut didapat Penulis secara langsung dari Pegawai Pengadilan Tinggi Palembang khususnya pada bagian umum, yang menjelaskan jalannya program, topologi yang dipakai serta

permasalahan yang sering terjadi khususnya dalam jaringan di Pengadilan Tinggi Palembang.

4.2.2 Data Sekunder

Menurut Umar (2007:42), data sekunder merupakan data primer yang telah diolah lebih lanjut dan disajikan baik oleh pihak pengumpul data primer atau oleh pihak lain, biasanya berupa sejarah instansi, visi dan misi, aktivitas organisasi dan struktur organisasinya.

. Data primer tersebut didapat Penulis secara langsung dari Pegawai Pengadilan Tinggi Palembang khususnya pada bagian umum, yang menjelaskan bagaimana aktivitas rutinitas Pengadilan Tinggi Palembang.

4.3 Teknik Pengumpulan Data

Metode penelitian yang digunakan adalah:

1. Studi *Literatur*, yaitu teknik yang dilakukan dengan cara mempelajari teori-teori yang berkaitan dengan pengetahuan dalam membangun suatu jaringan *Wireless* LAN.
2. Studi Lapangan, yaitu teknik yang dilakukan dengan cara mendatangi langsung tempat penelitian dan mengumpulkan data. Metode yang digunakan oleh penulis adalah sebagai berikut:

a. Wawancara

Adalah metode pengumpulan data dengan cara bertanya langsung dengan responden yaitu kepada pegawai Pengadilan Tinggi Palembang.

b. Dokumentasi

Dokumentasi adalah pengumpulan data dengan cara melakukan penyelidikan melalui sumber dokumen.

c. Pengamatan (*Observasi)*

Pengamatan (*observasi)* adalah pengumpulan data dengan terjun langsung dan melihat ke lapangan terhadap objek yang diteliti.

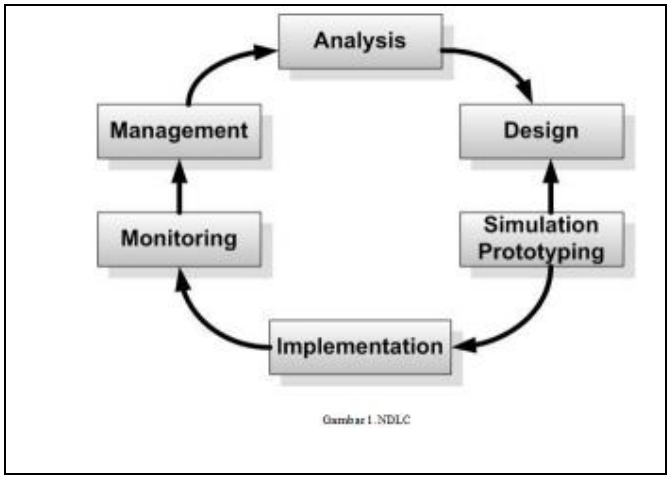
4.4 Jenis Pengumpulan Data

Adapun jenis penelitian yang digunakan penulis pada penelitian ini yaitu penulis menggunakan jenis penelitian Terapan (*applied reaserch*). Penelitian Terapan bertujuan untuk meningkatkan pengetahuan ilmiah dengan suatu tujuan praktis. Hasilnya diharapkan segera dapat dipakai untuk keperluan praktis. Misalnya penelitian untuk menunjang kegiatan pembangunan yang sedang berjalan, penelitian untuk melandasi kebijakan pengambilan keputusan atau administrator.

Dilihat dari segi tujuannya, penelitian terapan berkepentingan dengan penemuan-penemuan yang berkenan dengan aplikasi dan sesuatu konsep-konsep teoritis tertentu.

4.5 Teknik Pengembangan Sistem

Dalam pengembangan aplikasi ini digunakan metode pengembangan *Network Development Life Cycle Model* (NDLC Model) atau juga dikenal dengan metodelogi *Classic Life Cycle Model* (CLCM)/ *Linear Sequential Model* (LSM)/*Waterfall Method*. Pada metode ini terdapat enam tahap untuk mengembangkan suatu perangkat lunak. Keenam tahapan itu tersusun dari atas kebawah, diantaranya : *Analysis, Design, Simulation prototyping, Implementation, Monitoring, Managemen*.



(Sumber : Goldman, James E Rawles 2001:470)

Gambar 4.1 Model NDLC

1. **Analysis**

   Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan user, dan analisa topologi / jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap ini diantaranya, Wawancara, survey langsung kelapangan, membaca manual atau blueprint

dokumentasi, dan menelaah setiap data yang didapat dari data-data sebelumnya.

2. Design

Dari data-data yang didapatkan sebelumnya, tahap Design ini akan membuat gambar design topology jaringan interkoneksi yang akan dibangun, diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. Design bisa berupa *design struktur topology, design akses data, design tata layout perkabelan, dan sebagainya* yang akan memberikan gambaran jelas tentang project yang akan dibangun. Biasanya hasil dari design berupa, Gambar-gambar topology (server farm, firewall, datacenter, storages, lastmiles, perkabelan, titik akses dan sebagainya).

3. Simulation Prototype

Beberapa networker's akan membuat dalam bentuk simulasi dengan bantuan Tools khusus di bidang network. hal ini dimaksudkan untuk melihat kinerja awal dari network yang akan dibangun dan sebagai bahan presentasi dan sharing dengan team work lainnya

4. Implementation

Dalam implementasi networker's akan menerapkan semua yang telah direncanakan dan di design sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil /

gagalnya project yang akan dibangun dan ditahap inilah Team Work akan diuji dilapangan untuk menyelesaikan masalah teknis dan non teknis.

5. Monitoring

setelah implementasi tahapan monitoring merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari user pada tahap awal analisis, maka perlu dilakukan kegiatan monitoring. Monitoring bisa berupa melakukan pengamatan pada ;

a. Infrastruktur hardware : dengan mengamati kondisi reliability / kehandalan system yang telah dibangun (reliability = performance + availability + security).
b. Memperhatikan jalannya packet data di jaringan (pewaktuan, latency, peektime, troughput)
c. Metode yang digunakan untuk mengamati ”kesehatan” jaringan dan komunikasi secara umum secara terpusat atau tersebar.

6. Management

Manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah Policy, kebijakan perlu dibuat untuk membuat / mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur Reliability terjaga.

BAB V

HASIL DAN PEMBAHASAN

5.1 Hasil

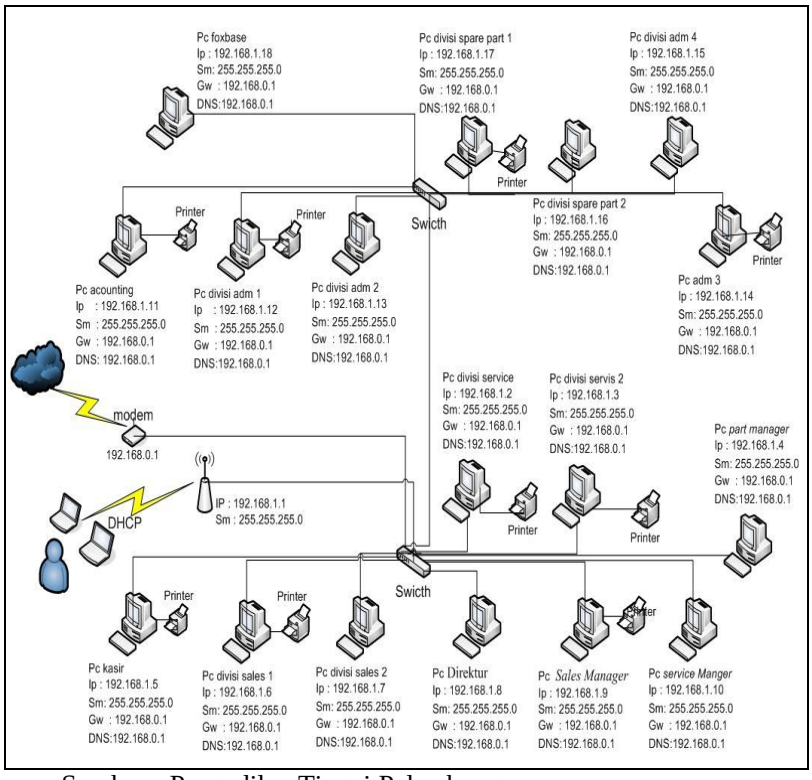
5.1.1 Analisis dan Keadaan Jaringan

Jaringan yang ada pada Pengadilan Tinggi Palembang sebelumnya telah memiliki jaringan computer yang sudah terkoneksi ke jaringan *internet* dan memanfaatkan teknologi *wireless* sebagai infrastruktur jaringan akan tetapi pemanfaatan teknologi *wireless* tersebut masih jauh dari sistem keamanan, maka yang tadinya telah dibangunlah sistem jaringan *wireless* dimplementasikan kembali dengan penambahan jaringan menggunakan *Radius* sebab dengan adanya system *radius* tersebut *autentifikasi user* yang akan mengakses *internet* di manajemen oleh *server radius* sebagai pusat pelanyanan yang mengatur seluruh fisik jaringan *wireless.* Hanya *user* yang telah diberikan hak akses oleh administrator jaringan yang bisa mengakses hotspot sehingga sistem keamanan lebih terjamin yaitu menggunakan *radius server*. Untuk lebih jelasnya pada gambar 5.1 dapat dilihat infrastruktur topologi jaringan yang akan diimplementasikan dan yang digunakan pada Pengadilan Tinggi Palembang.

5.1.1.1 Topologi Jaringan Yang Digunakan

Setelah melalui pengamatan yang di lakukan penulis pada Pengadilan Tinggi Palembang, maka penulis mendapatkan

data mengenai infrastruktur model *topologi* jaringan yang digunakan, untuk lebih jelasnya maka penulis telah membuat topologi jaringan sebelum di bangun pada Pengadilan Tinggi Palembang seperti di bawah ini;



Sumber : Pengadilan Tinggi Palembang

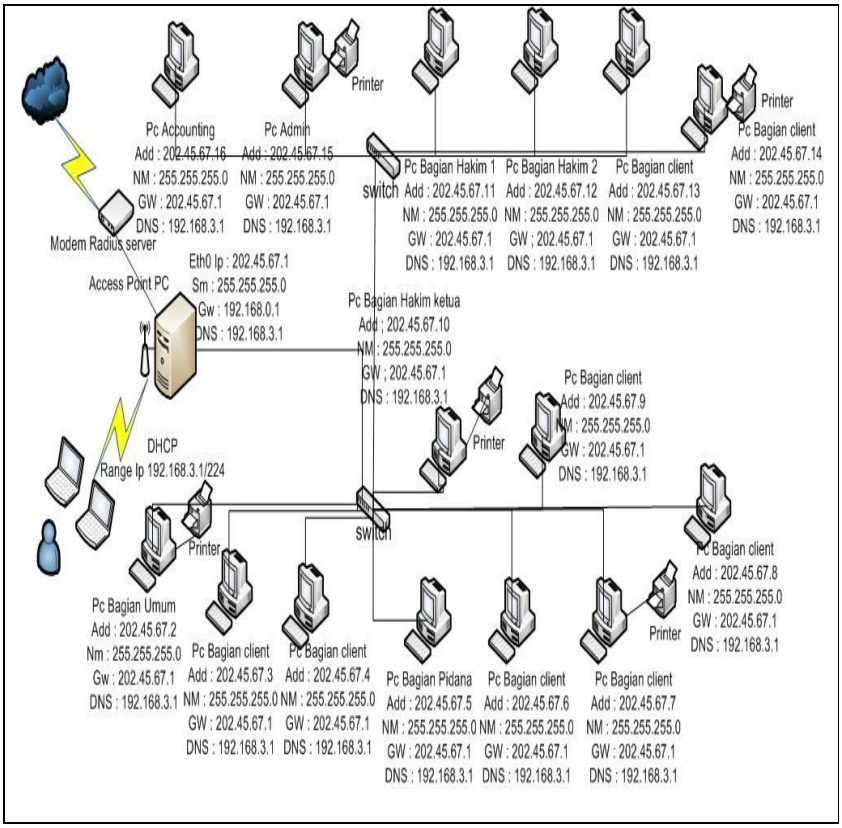
Gambar 5.1 Topologi Jaringan Sedang Berjalan.

Topologi jaringan pada Pengadilan Tinggi Palembang seperti yang terlihat pada gambar 5.1 diatas menggunakan topologi star sebagai infrastruktur jaringannya, alokasi *id address* untuk PC menggunakan kelas C yaitu 192.160.42.2 sampai dengan 192.160.42.21, dan sudah berbasis *wireless*

yang mana masih minimnya dalam segi keamanan data yang terdapat pada Pengadilan Tinggi Palembang.

5.1.1.2 Topologi Jaringan yang Disarankan

Dari hasil topologi jaringan sebelum dibangun maka dalam pembuatan *Radius Server* topologi mengalami perubahan hampir 80 %, hal tersebut dikarenakan kebutuhan dalam pengembangan jaringan *Wifi* meskipun untuk beberapa bagian infrastruktur tidak mengalami perubahan yaitu untuk computer admin dan computer manager. Untuk lebih jelasnya dapat dilihat pada gambar topologi jaringan yang akan dibangun.



(Sumber : Pengelolahan Sendiri)

Gambar 5.2 Topologi Jaringan Yang Disarankan

Berdasarkan gambar 5.2 topologi jaringan diatas menunjukkan pengalamatan *ip address modem* adalah 202.45.67.1. sehingga untuk server radius harus mengguanakan *network id* yang sama yaitu 202.45.67.0 untuk komputer admin dan 202.45.67.15 untuk komputer manager. Angka 1 dan 15 bit terakhit menyatakan *host id, switch* berfungsi untuk menghubungakan antara radius ke *access point*, dimana pengalamatan *access point* menggunakan DHCP atau pengalamatan IP *address* secara otomatis.

5.1.2 Perancang Jaringan

Perancang jaringan meliputi kebutuhan *Hardwere* dan *Softwere*, adapun kebutuhan tersebut sebagai berikut;

5.1.2.1 Kebutuhan Perangkat Keras (*Hardwere*)

Agar pembuatan jaringan dapat terlaksana maka dibutuhkan perangkat keras (*Hardwere)* yang menunjang sehingga hasil yang diperoleh susuai dengan yang diharapkan, adapun kebutuhan perangkat keras adalah sebagai berikut;

1. Satu komputer server untuk *back-end authentication* server (RADIUS server).
2. *Access Point Linkysy WAP54G*
3. dua (2) bauh NIC

5.1.2.2 Kebutuhan Perangkat Lunak (*Softwere)*

Kebutuhan perangkat lunak merupakan bagian yang sangat penting setelah adanya perangkat keras, karena perangkat lunak adalah sebuah program yang dirancang untuk memenuhi kebutuhan pemakai (*user)* sesuai spesifikasi yang di butuhkan, adapun kebutuhan perangkat lunak adalah sebagai berikut;

1. System Oprasi Centos5.3.
2. System Oprasi Windows 7 dan *free Radius Server Open Source.*

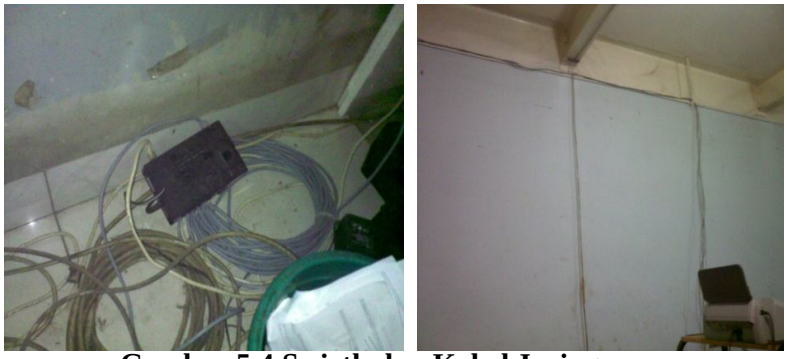
5.1.2.3 Komputer Client / Komputer Karyawan

Komputer ini digunakan oleh staf karyawan untuk kegiatan mereka sehari-hari seperti pengolahan data Perkara, data administrasi dan lain-lain. Berikut adalah gambar komputer client yang dipakai karyawan Pengadilan Tinggi Palembang.

Gambar 5.3 Komputer Client Pengadilan

5.1.2.4 Swicth dan Kabel Jaringan

Switch digunakan untuk menghubungkan semua komputer yang ada di Pengadilan Tinggi Palembang, Kabel jaringan dihubungkan ke Switch yang terletak di beberapa titik. Berikut gambar switch digunakan pada Pengadilan Tinggi Palembang.



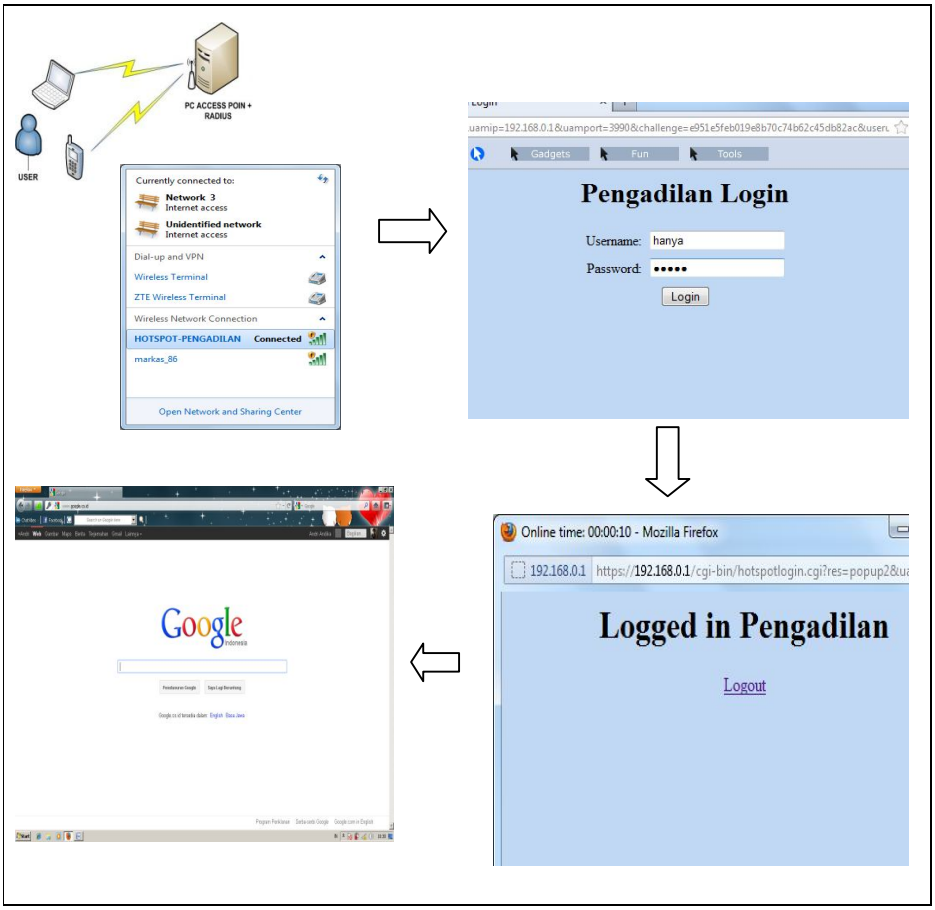
Gambar 5.4 Swicth dan Kabel Jaringan

5.2 Pembahasan

Dalam membangun sebuah *access point server* berbasis PC ini dibutuhkan langkah-langkah Instalasi mulai dari Installasi Sistem Operasi yang digunakan, Installasi *software*, konfigurasi *software-software*, konfigurasi database dan uji coba sistem.

Desain jaringan yang penulis usulkan dalam penelitian ini adalah penulis membuat sebuah *access point* yang dibuat dari personal computer dan dapat juga dijadikan wireless router. Di dalam *access point* ini juga terdapat autentikasi user menggunakan captive portal *chillispot* dan juga *freeradius* sebagai server radius. Cara kerja *chillispot* adalah dengan cara meng-capture request halaman *web client* dan kemudian di-*redirect* ke

halaman *web chillispot* untuk *user authentication*. Data *username* dan *password* yang dimasukkan *user* akan ditransfer ke *server radius* untuk proses *user authentication* dan *prefilarge authentication*.



Gambar 5.5 Ilustrasi cara kerja user autentikasi.

Konsep keamanan *wireless* yang digunakan dibagi dua, yaitu keamanan wireless untuk staf/pelanggan menggunakan user authentication dan keamanan wireless untuk karyawan menggunakan MAC filtering.

Pelanggan atau tamu yang akan mengakses internet menggunakan jaringan wireless akan melapor kepada admin untuk kemudian diberi

username dan password tersendiri. Username dan password tersebut akan digunakan pada saat login *autentikasi*. Dalam skripsi ini penulis mencontohkan beberapa user yang telah didaftarkan oleh administrator. Berikut adalah tabel user pelanggan.

Tabel 5.1 User tamu/pelanggan yang didaftarkan pada hotspot

No	Nama Jelas	Username	Password	Bandwitch	Masa aktif
1	Eko	Eko	12345	32/32 Kbps	5000 hari
2	jayak	Jayak	12345	32/32 Kbps	5000 hari
3	joe	Joe	12345	32/32 Kbps	5000 hari
4	fairin	Fairing	12345	32/32 Kbps	5000 hari
5	lim	Lim	12345	32/32 Kbps	5000 hari

Contoh disini eko memiliki username eko dan password 12345, memiliki kapasitas untuk download sebesar 32 Kbps dan upload sebesar 32 Kbps dan masa aktif 5000 hari. Masa aktif dapat kita atur sesuai keinginan sesuai dengan berapa lama user yang bersangkutan ingin mengaktifkan accountnya.

Dan keamanan wireless kedua adalah MAC filtering, MAC filtering ini digunakan untuk autentikasi perangkat wireless staf atau karyawan. Jadi karyawan yang perangkat wireless seperti laptop atau PDA yang MAC addressnya telah didaftarkan maka tidak akan dibatasi oleh user autentikasi tetapi akan langsung dilewatkan dan dapat mengakses internet. Perangkat

wireless Staf atau karyawan yang belum didaftarkan MAC addressnya akan dibatasi oleh user login dan tidak dapat mengakses internet. Berikut adalah tabel MAC address staf yang telah didaftarkan.

Tabel 5.2 MAC Address karyawan yang didaftarkan

No	Nama Staf/Karyawan	MAC Address
1	M.Anwar,SH	002185BFFD4B
2	Yarma Esti,S.H	00216BA98585
3	Darmawansyah,S.H	002186BFDF5B
4	Arifin.S.H	00216BA9753B
5	Hermansyah.S.H	002185BFDE4C

Karena keterbatasan akses penulis untuk dapat melihat MAC address laptop karyawan secara langsung, maka penulis disini hanya menuliskan contoh dari MAC address yang didaftarkan.

5.3 Install Server

Langkah awal yang harus dilakukan adalah menginstall Sistem Operasi, dimana dalam implementasi ini penulis menggunakan Linux *Centos 5.8* kemudian install Paket-paket pendukung di antaranya sebagai berikut.

```
[root@hotspot~]# Chillispot freeradius sshd
httpd
```

5.3.1 Konfigurasi IP Address

Setelah melakukan proses install server (dalam penelitian ini menggunakan Centos5.8*)* maka selanjutnya penulis akan melakukan konfigurasi IP *address* pada computer Radius *server*. IP *address* merupakan pengalamatan komunikasi antar jaringan yang lebih dikenal dengan istilah protocol, konfigurasi dapat dilakukan dengan cara mengedit *files* yang bernama ifcfig-eth0, seperti dibawah ini:

```
[root#hotspot-login] vi ifconfig-eth0
 static
        address 202.45.67.20
        netmask 255.255.255.0
        gateway 202.45.67.1

eth1 DHCP
        address 192.168.0.1
        netmask 255.255.255.0
        network 192.168.0.0
        broadcast 192.168.10.255
```

Untuk Eth0 (*Network card* yang pertama) diberikan IP computer yang disesuaikan dengan jaringan, pada penelitian ini IP yang digunakan 202.45.67.20, *Netmask 255.255.255.0* dan *gateway* 202.45.67.1 yang disesuaikan dengan jaringan LAN dan Eth1 menggunakan IP *static* 202.45.67.21 dengan *subnetmask* 255.255.255.0/240. agar jarigan bias terkoneksi maka diperlukan DNS

(*Domain Name Server) google* yang sudah diberikan oleh ISP. Caranya dengan mengedit file *resolv.conf* pada direktori ***/etc/resolv.conf.***

```
NameServer 127.0.0.1
NameServer 127.0.0.1
```

Kemudian aktifkan IP forward dengan menghilangkan tanda pagar pada file sysctl.conf, hilangkan tanda pagar di depan net.ipv4.ip forward=1.

```
#net.ipv4.conf.default.forwarding=1
Menjadi :
net.ipv4.conf.default.forwarding=1
```

Simpan dan keluar dengan perintah (esc) => (shift + ;) => wq

Selanjutnya restart network dengan perintah;

 # service network restart.

Sesudah restart maka lakukan ping untuk melihat komfigurasi ip address sudah benar, penulis melakukan tes ping ke google.com tampak seperti di bawah ini ;

```
root@pengadilan:/# ping www.google.com
#============================================
PING any-fp3-real.wa1.b.Google.com
(98.137.149.56) 56(84) bytes of data.
64 bytes from ir1.fp.vip.sp2.Google.com
(98.137.149.56): icmp_seq=1 ttl=49 time=357 ms
```

```
64 bytes from ir1.fp.vip.sp2.Google.com
(98.137.149.56): icmp_seq=2 ttl=49 time=304 ms
^C
--- any-fp3-real.wa1.b.Google.com ping
statistics ---
2 packets transmitted, 2 received, 0% packet
loss, time 1000ms
rtt min/avg/max/mdev =
304.324/331.099/357.875/26.781 ms
```

5.3.2 Install Freeradius dan Paket Tambahan

System autentikasi Hospot ini setiap user yang masuk ke dalam hotspot kita lewat wireless dan mencoba untuk browsing internet, semuanya akan diredirect ke login username dan password chillispot. Untuk mendukung halaman login dan halaman untuk manajemen user dan bandwidth dibutuhkan webserver dan database. Dalam penelitian ini menggunakan webserver apache dan database mysql.

1. Install paket pendukung

   Sebelum menginstall dan komfigurasi webserver sendiri dibutuhkan beberapa tools yang sebaiknya juga diinstall untuk menunjang kerja server. Install paket-paket tersebut dengan perintah sebagai berikut :

```
[root@hotspot]# yum install freeradius
sshd httpd iptraf iftop whois sysstat snmp
snmpd rrdtool dbconfig-common libphp-adodb
php5-cli php5-gd php5-gmp php-pear php5-
snmp
```

Gambar diatas merupakan proses intall paket pendukung yang dibutuhkan dalam pembuatan server radius, adapun keterangan dari paket-paket tersebut diantaranya sebagai berikut;

1. Paket enzip dibutuhkan untuk mengextrak file-file yang berekstensi zip.
2. Paket fakeroot dibutuhkan untuk menjalankan suatu perintah dengan berpura-pura sebagai root
3. Paket buld-essential akan menginstall paket-paket yang diperlukan dikala kita mau kompilasi suatu program
4. Paket rrdtool dibutuhkan untuk menampilkan grafik di webserver

Setelah selesai proses instalasi paket pendukung system radius maka diperlukan apache,php dan mysql.

#**yum install mysql-server**

```
[root@hotspot]# yum install mysql-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be
installed:
  libdbd-mysql-perl libdbi-perl libhtml-
template-perl libmysqlclient16
  libnet-daemon-perl libplrpc-perl
mysql-client-5.1 mysql-common
  mysql-server-5.1 mysql-server-core-5.1
Suggested packages:
  libipc-sharedcache-perl libterm-
readkey-perl tinyca
The following NEW packages will be
installed:
  libdbd-mysql-perl libdbi-perl libhtml-
template-perl libmysqlclient16
  libnet-daemon-perl libplrpc-perl
mysql-client-5.1 mysql-common mysql-
```

```
server
  mysql-server-5.1 mysql-server-core-5.1
0 upgraded, 11 newly installed, 0 to
remove and 270 not upgraded.
Need to get 23.3 MB of archives.
After this operation, 54.9 MB of
additional disk space will be used.
Do you want to continue [Y/n]?
```

Perintah tersebut menginstall serve maysql, server apache2, php5 dan library php5-mysql. Sewaktu menginstall mysql –server biasanya akan di minta password untuk root mysql. Untuk memasukkan password anda dapat membuat sendiri dengan perintah mysqladmin u root password “rahasia”dengan perintah tersebut maka untuk admin mysql dengan user root passwordnya adalah rahasia. Kemudian download paket chillispot-1.1.0.i386.rpm .

```
[root@hotspot]# wget
http://www.chillispot.info/download/chill
ispot-1.1.0.i386.rpm
```

Kemudian install paket yang kita download, masih di dalam directory tempat kita mendownload. Kemudian install dengan perintah.

```
[root@hotspot]# rpm -ivh chillispot-
1.1.0.i386.rpm
```

5.3.3 Membuat database hotspot

Langkah pertama adalah membuat user mysql yaitu dengan perintah berikut :

```
[root@hotspot ~]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor. Commands end
with ; or \g.
Your MySQL connection id is 5140
Server version: 5.0.45 Source distribution
Type 'help;' or '\h' for help. Type '\c' to
clear the buffer.
mysql> GRANT ALL PRIVILEGES ON radius.* to
'radius'@'localhost' IDENTIFIED BY '123456';
Query OK, 0 rows affected (0.01 sec)
mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.02 sec)
mysql>
```

Kemudian buat user sebagai login, dengan perintah sebagai berikut;

```
mysql>; INSERT INTO radcheck (UserName, Attribute, Value)
VALUES ('ibnu', 'User-Password', 'ibnu');
```

5.3.4 Konfigurasi Radius Server

Setelah anda membuat account baru tersebut, anda harus menyesuaikan settingnya dengan setting database freeradius dan

chillispot untuk itu anda perlu merubah file **/etc/freeradius/sql.conf** dan ubah setting server, login, password dan radius_db menjadi :

```
sql {
#
#  Set the database to one of:
#
#    mysql, mssql, oracle, postgresql
#
database = “mysql”
#
#  Which FreeRADIUS driver to use.
#
driver = “rlm_sql_${database}”
# Connection info:
server = “localhost”
#port = 3306
login = “root”
password = “testing123”
# Database table configuration for
everything except Oracle
radius_db = “hotspot”
```

Langkah selanjutnya adalah membuat chilli sebagai client dari freeradius, untuk itu kita harus merubah file **/etc/freeradius/clients.conf** dan pastikan anda memiliki baris setting seperti dibawah :

```
ipaddr = 127.0.0.1

secret = testing123

nastype = other
```

Berikutnya memberitahu freeradius untuk menggunakan MySql dalam authentikasi user. ubah file **/etc/freeradius/radiusd.conf**. dibagian **modules** (sekitar baris 648) dan uncommen :

```
$INCLUDE sql.conf

begitu juga bebrapa baris berikutnya,
uncomment pada :

$INCLUDE sql/mysql/counter.conf

Kemudian cari di bagian instantiate (sekitar
baris 715) dan tambahkan didalamnya :

max_all_mb

noresetcounter
```

kemudian save file tersebut dan buka file **/etc/freeradius/sites-enabled/default.** Pada bagian **authorize accounting, session** dan **post-auth**, kemudian save perhatikan baris yang berisi **sql** yang mungkin di”comment” anda harus meng-”uncomment” baris tersebut dan menambahkan baris sehingga menjadi seperti dibawah ini :

```
Sql

max_all_mb

noresetcounter
```

Tahap selanjutnya adalah merubah file **/etc/freeradius/sql/mysql/counter.conf**, buka file tersebut dan lihat pada bagian akhir file, terdapat parameter.

```
sqlcounter noresetcounter {       counter-name =
Max-All-Session-Time
```

```
check-name = Max-All-Session
sqlmod-inst = sql
key = User-Name
reset = never
query = “SELECT IFNULL(SUM(AcctSessionTime),0)
FROM radacct WHERE User$
}
```

Hapus semua baris diatas hingga tanda **}** dan gantikan dengan :

```
sqlcounter noresetcounter {

counter-name = Session-Timeout

check-name = Session-Timeout

reply-name = Session-Timeout

sqlmod-inst = sql

key = User-Name

reset = never

query = “SELECT SUM(Acctsessiontime) FROM
radacct WHERE UserName=’%{%k}’”

}

sqlcounter max_all_mb {

counter-name = Max-All-MB

check-name = Max-All-MB

reply-name = ChilliSpot-Max-Total-Octets

sqlmod-inst = sql

key = User-Name

reset = never

query = “SELECT SUM(AcctInputOctets)/(1024*1024)
```

```
+ SUM(AcctOutputOctets)/(1024*1024) FROM radacct
WHERE UserName='%{%k}'"

}
```

Selanjutnya manjalankan freeradius dengan mode debug.

$service radius restart

$servece mysqld restart

5.3.5 Install dan konfigurasi Chillispot

Chillispot merupakan open source captive portal atau *wireless* lan *access point controller*. Digunkan untuk meng-auntentikasi user dari sebuah jaringan wireless lan. File chillispot bias diperoleh melalui situs http://www.chillispot.info/. Perintah untuk mendowload adalah sebagai berikut

```
# [root@hotspot~]# wget
http://www.chillispot.info/download/chillispot
-1.1.0.i386.rpm
```

Setelah selesai melakukan download maka selanjutnya melakukan install dengan perintah dpkg –I chillispot_1.0_i386.rpm, dengan perintah tersebut linux debian otomatis akan memeriksa dependency paket kemudain menginstall paket chillispot dan juga paket-paket yang dibutuhkan chillispot.

```
[root@hotspot ~]# rpm -ivh chillispot-
1.1.0.i386.rpm
```

Setelah selesai proses install kemudian perlu dilakukan konfigurasi pada file Chilli Secara default, Chillispot di set dalam keadaan tidak aktif, anda harus mengaktifkan dengan cara merubah isi file **/etc/default/chilli** dan cari

START_CHILLI=0 ubah menjadi **START_CHILLI=1**

Kemudian buka file vim **/etc/chilli.conf** dan sesuaikan parameter sesuai setting-setting diatas, berikut adalah setting **/etc/chilli.conf** saya :

```
[root@hotspot]/# vim  /etc/chilli.conf
#=========================================================

net 192.168.0.0/25
dynip 192.168.0.0/25
dns1 192.168.0.1
radiusserver1 127.0.0.1
radiusserver2 127.0.0.1
radiusauthport 1812
radiussecret testing123
dhcpif eth1
uamserver https://192.168.0.1/cgi-
bin/hotspotlogin.cgi
uamsecret ht2eb8ej6s4et3rg1ulp
uamallowed
www.chillispot.org,202.45.67.2,192.168.0.3,
192.168.0.17
```

Pada bagian ini kita mengaktifkan MAC address Filtering. Hilangkan tanda pagar pada *HS_MACAUTHMODE=local*

```
#=====================================================
#                   Setting MAC Address Filtering
#=====================================================
###
#   Features not activated per-default (default to off)
#
#HS_RADCONF=on     # Get some configurations from RADIUS or a URL ('on'
and 'url' respectively)
#
# HS_ANYIP=on             # Allow any IP address on subscriber LAN
#
# HS_MACAUTH=on           # To turn on MAC Authentication
#
#HS_MACAUTHDENY=on        # Put client in 'drop' state on MAC Auth
Access-Reject
#
HS_MACAUTHMODE=local      # To allow MAC Authentication based on
macallowed, not RADIUS
#
#=====================================================
#                   Pendaftaran MAC Address Client
#=====================================================
HS_MACALLOW="002185BFFD4B, 00216BA98585, 002185BFFD4B ,
00216BA98585, 002186BFDF5B, 00216BA9753B, 002185BFDE4C "      # List of
MAC addresses to authenticate (comma seperated)
#
# HS_USELOCALUSERS=on     # To use the /etc/chilli/localusers file
#=====================================================

#   Standard configurations
#
HS_MODE=hotspot
HS_TYPE=chillispot
```

```
# HS_RADAUTH=1812
# HS_RADACCT=1813
# HS_ADMUSR=chillispot
# HS_ADMPWD=chillispot

#   .jpg, .gif, .png, .js are allowed. See below for using .chi as a
#   CGI extension.
HS_WWWDIR=/etc/chilli/www

#   to chilli with url /www/filename.chi
HS_WWWBIN=/etc/chilli/wwwsh
#   Some configurations used in certain user interfaces
HS_PROVIDER=Pengadilan #untuk Informasi
HS_PROVIDER_LINK=http://www.pengadilanunion.com/

HS_LOC_NAME="HotSpot Pengadilan"          # WISPr Location Name and
used in portal

#   WISPr settings (to form a proper WISPr-Location-id)
```

Setelah di save, jalankan chilli dengan perintah :

```
root@:/# service chilli restart
#============================================
Starting chilli: chilli.                    Ok
```

Test hotspot dengan menjalankan perintah ifconfig apabila dalam reslut ifconfig telah muncul **tun0** dimana Tun0 memiliki ip 192.168.0.1 maka server hotspot sudah bisa digunakan.

```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-
inet addr:192.168.0.1  P-t-P:192.168.0.1  Mask:255.255.255.0
UP POINTOPOINT RUNNING  MTU:1500  Metric:1
```

```
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tun1      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-
00-00-00-00-00-00-00-00-00
inet addr:192.168.0.1  P-t-P:192.168.0.1  Mask:255.255.255.0
UP POINTOPOINT RUNNING  MTU:1500  Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

5.3.6 Membuat File Hotspotlogin.cgi

Masuk ke direktori /usr/share, lalu kopikan file chilli ke direktori /var/www/cgi-bin dengan perintah berikut :

```
[root@hotspot]# cp
/usr/share/doc/chillispot-
1.1.0/hotspotlogin.cgi /var/www/cgi-bin/
[root@FTPSVR radius_server]# chmod 755
/var/www/cgi-bin/hotspotlogin.cgi
```

Kemudian Jalankan edit file hotspotlogin.cgi, dengan perintah;

```
[root@hotspot]# vim /var/www/cgi-
bin/hotspotlogin.cgi
```

Lalu ganti seperti di bawah ini;

```
#$uamsecret = "ht2eb8ej6s4et3rg1ulp ";
menjadi $uamsecret = " ht2eb8ej6s4et3rg1ulp
";
#$userpassword=1; menjadi $userpassword=1;
```

5.3.7 Configurasi PhpMyprepaid

Pastikan bahwa mysql server sudah terinstal di server anda.

Download file phpmyprepaid:

Lalu masuk direktori html dengan cara;

```
[root@hotspot] #Cd /var/www/html
```

Kemudian install paket phpmyprepaid dengan perintah;

[root@hotspot html] # `wget`

```
http://waix.dl.sourceforge.net/
sourceforge/phpmyprepaid/phpmyprepaidRC3.tgz
```

Kemudian extrak

```
[root@hotspot html]#tar -zxvf
phpmyprepaidRC3.tgz
[root@hotspot html]# chmod 777
```

```
/var/www/html/phpmyprepaid/www/
```

5.3.8 Akses Keamanan Hotspot

Hapus file install di /var/www/html/phpmyprepaid/www/install/ seperti dibawah ini;

```
[root@hotspot html]# rm -rf
/var/www/html/phpmyprepaid/www/install/
Ganti permission untuk
var/www/html/phpmyprepaid/www
[root@hotspot html]# chmod 755
/var/www/html/phpmyprepaid/www/
```

5.3.9 Setting Firewall

Untuk menjalankan Firewall kita harus meng non altifkan iptables terlebih dahulu, seperti perintah dibawah ini;

```
[root@hotspot]# /etc/init.d/iptables stop
[[root@hotspot]# /usr/share/doc/chillispot-1.0/firewall.iptables
[root@hotspot]# /etc/init.d/iptables save
```

Perhatikan : setiap service network melakukan restart, jika ada gangguan maka jalankan lagi perintah diatas, karena sering terjadi firewall bermasalah saat service network di restart.

Kemudian aktifkan IP forward dengan menghilangkan tanda pagar pada file sysctl.conf, hilangkan tanda pagar di depan net.ipv4.ip forward=1.

```
[root@hotspot]# vim /etc/sysctl.conf
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
```

Apabila semua proses configurasi sudah selesai, maka selanjutnya kita menjalankan chilli dan radius dengan perintah;

```
root@hotspot]#chkconfig chilli on
[root@hotspot ~]#chkconfig radiusd on
```

Jika ada perubahan konfigurasi restart chilli dan radiusd

```
[root@hotspot ~]#service chilli restart
[root@hotspot~]# service radiusd restart
```

5.3.10 Pembuatan Account Hotspot Login

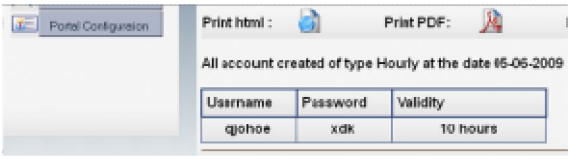
Pembuatan account bisa dilakukan dengan dua cara, yaitu lewat console linux dan lewat phpmyprepaid.

Cara pertama lewat console :

```
[root@hotspot]# mysql -u radius -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 228
Server version: 5.0.45 Source distribution
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
mysql> INSERT INTO radcheck (UserName, Attribute, Value)
VALUES ('ibnu', 'User-Password', 'ibnu');
mysql> quit
```

Cara kedua lewat phpMyPrePaid.

Pilih menu : Subscriber Expiration



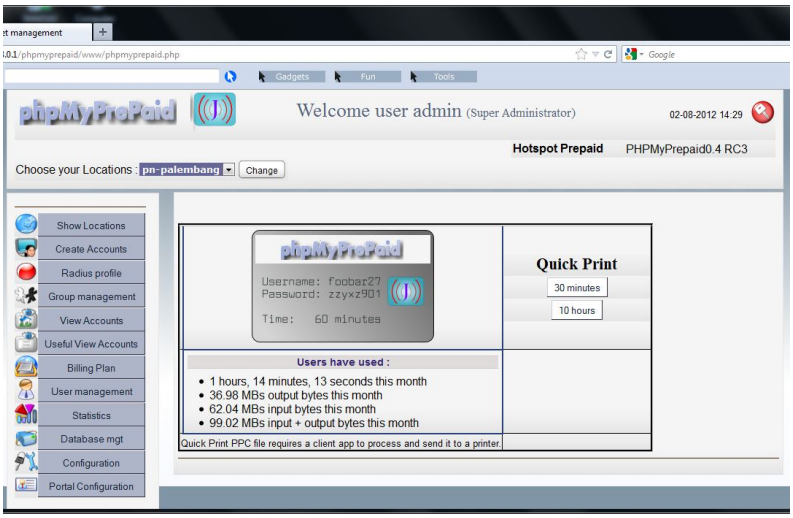
Gambar 5.6 Create Account Dari Phpmyprepaid

5.3.11 Test Login Admin dari Client

Gunakan web browser lalu ketik halaman Https://Pengadilanhotspot.net maka akan tampil halaman login admin seperti berikut,

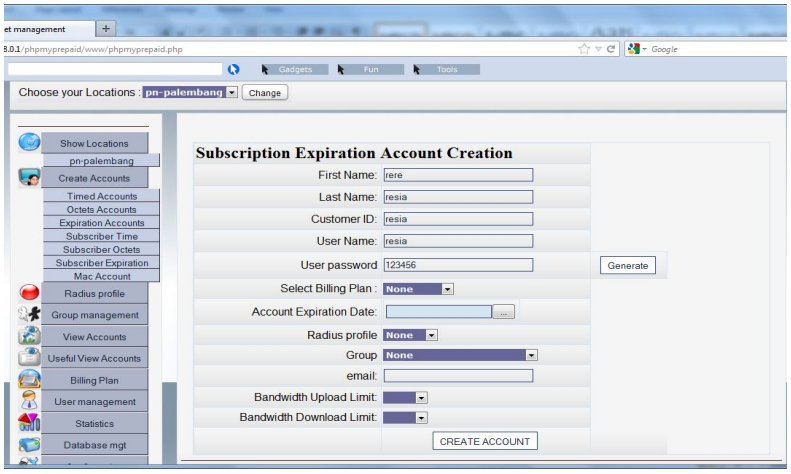
Gamabar 5.7 Tampilan Web HTTPS login admin

Masukkan User Name : admin dan password : qwerty123 lalu klick Login. Maka akan tampil halaman home admin seperti dibawah ini;



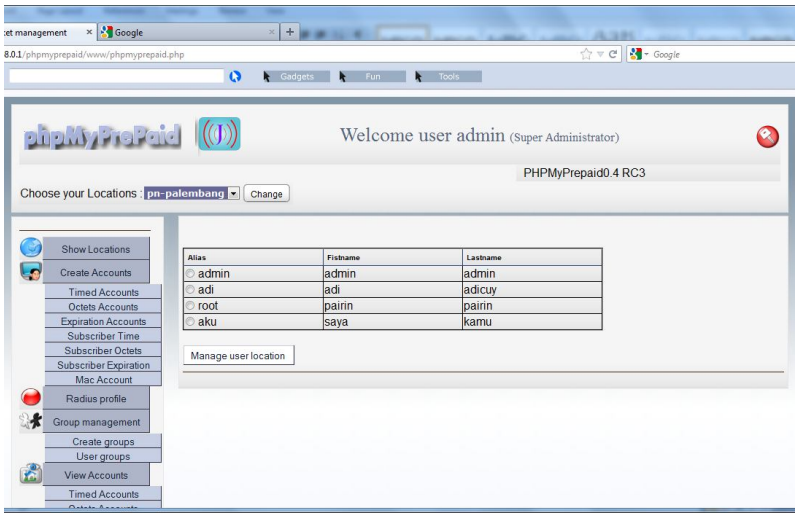
Gambar 5.8 Tampilan halaman Home Admin

Untuk membuat user baru atau menambahkan user baru masuk ke menu Create Account. Disini kita dapat memanagement user hotspot.



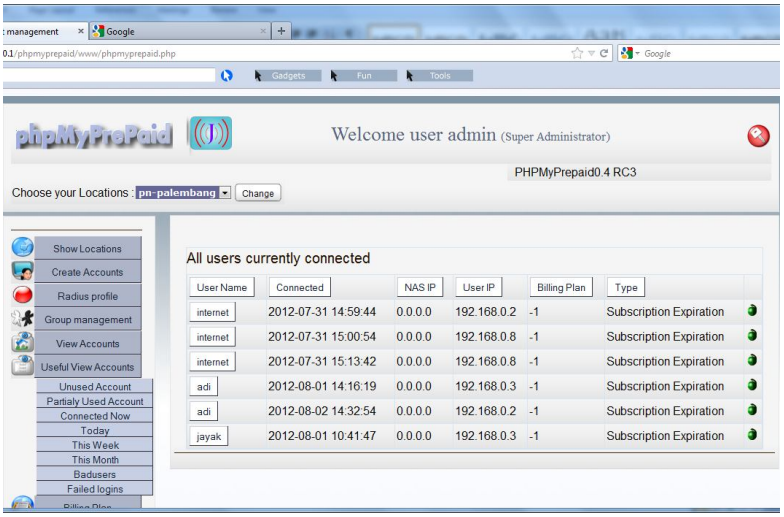
Gambar 5.9 Tampilan halaman penambahan user

Gambar dibawah ini menunjukkan jumlah user yang terdaftar pada hotspot Admin.



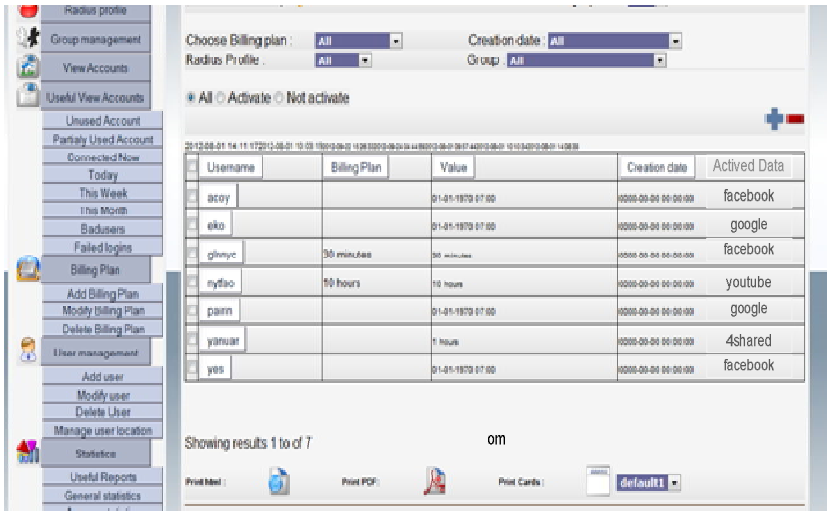
Gambar 5.10 Tampilan halaman user yang telah terdaftar

Untuk melihat user yang sedang online kita dapat melihatnya pada menu user online.



Gambar 5.11 Tampilan jumlah user yang sedang online

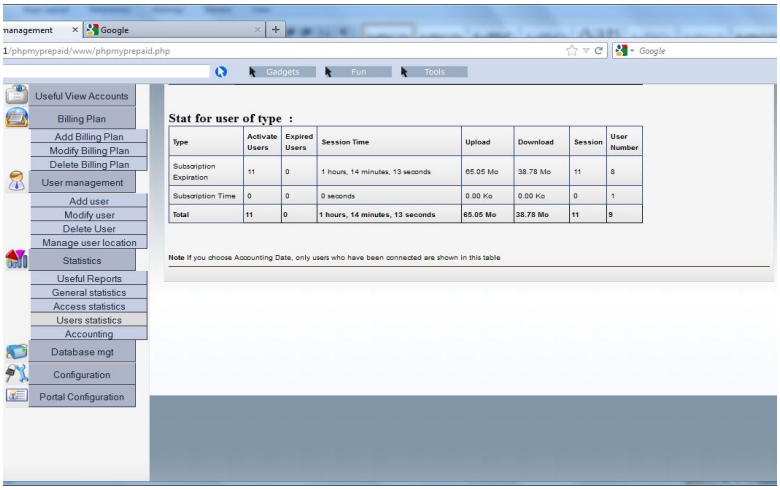
Selanjutnya kita dapat memonitoring apa saja yang di lakukan setiap user, dapat di lihat pada gambar berikut ini:



Gambar 5.14 aktivitas Data

5.3.12 Setting Limit Bandwicth User Hotspot

Langkah pertama adalah masuk ke Login admin. Lalu pilih postpaid setting seperti gambar dibawah.



Gambar 5.12 Tampilan halaman pengaturan bandwidh user

Masukkan berapa limit untuk download rate dan berapa limit untuk upload rate, Kemudian restart chilli dengan perintah

```
[root@hotspot ~] #service chillispot restart

[root@hotspot ~] #reboot
```

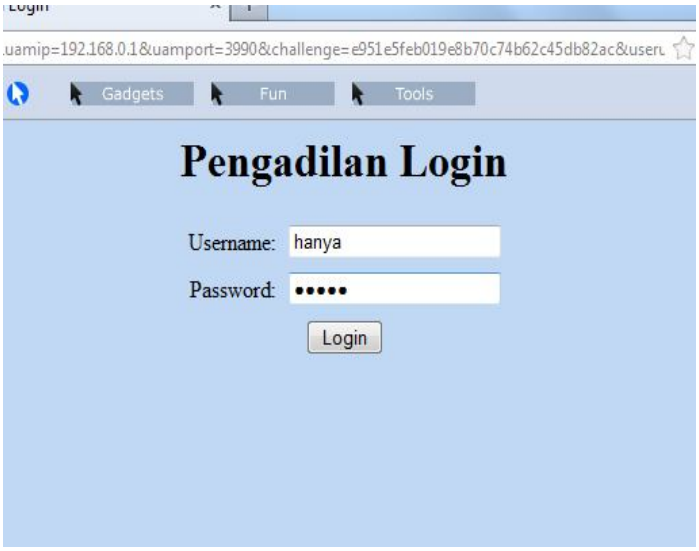
5.3.13 Hasil Halaman User Authentication

Terdapat dua pengaturan pengamanan *wireless* yang diterapkan pada Pengadilan Tinggi Palembang, yang pertama adalah Pengamanan menggunakan user authentication yang digunakan untuk user pelanggan atau tamu yang ingin mengakses internet via

wireless. User tamu akan diberikan *username* dan *password* untuk dapat mengakses internet pada jaringan *wireless* Pengadilan Tinggi Palembang seperti pada gambar berikut :

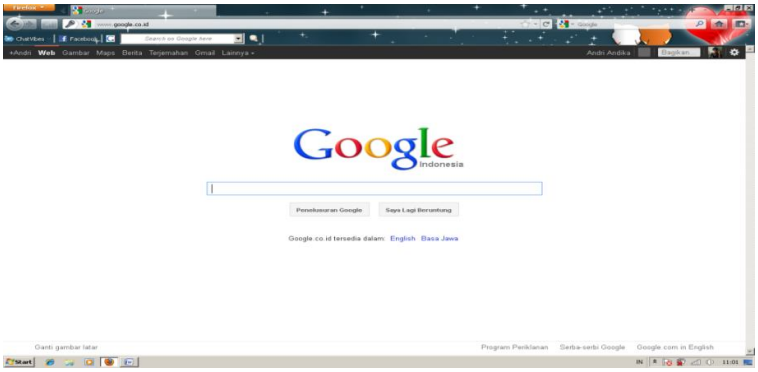
Gambar 5.13 SSID Pengadilan Tinggi Palembang

Setelah laptop atau perangkat *wireless* lainnya menangkap sinyal wireless SSID Pengadilan Tinggi Palembang, pilih atau koneksikan ke jaringan tersebut. Setelah terkoneksi akses halaman web contohnya dengan mengetikkan 192.168.0.1 pada browser maka secara otomatis halaman browser akan dialihkan ke halaman login seperti gambar berikut,



Gambar 5.14 Tampilan Halaman l*ogin user authentication*

Masukkan User Name : adi dan password : 123456 lalu klick Login. Maka akan tampil halaman browser seperti dibawah ini;



Gambar 5.15 Tampilan halaman website google

Password user hanya dapat digunakan untuk satu client yang online, jika kita menggunakan password user yang sedang online maka akses akan kembali ke halaman login, sedangkan jika client menggunakan username yang belum terdaftar atau salah

memasukkan username dan password maka akan terdapat pemberitahuan bahwa *username and/or password was not valid*.

Pengamanan kedua adalah untuk staf karyawan, sebelumnya MAC Address dari perangkat wireless mereka harus didaftarkan ke administrator untuk dapat mengakses internet tanpa harus melakukan user authentication pada saat mengkoneksikan perangkat wireless mereka dengan kata lain bagi staf karyawan yang MAC Address perangkat wirelessnya sudah terdaftar maka akan langsung terkoneksi dan dapat melakukan browsing halaman web.

5.3.14 Konfigurasi *Access Point*

dalam penelitian ini *Access Point* yang digunakan adalah A*ccess Point model Linksys WAP500G.* untuk melakukan konfigurasi *Access Point* jenis ini sediakan kompuer atau leptop untuk mengkonfigurasinya. Hubungkan kabel UTP antara *Access Point* dan computer atau leptop dan masukkan CD *Setup-nya.* Yang perlu dilakukan adalah mengkonfigurasi ;

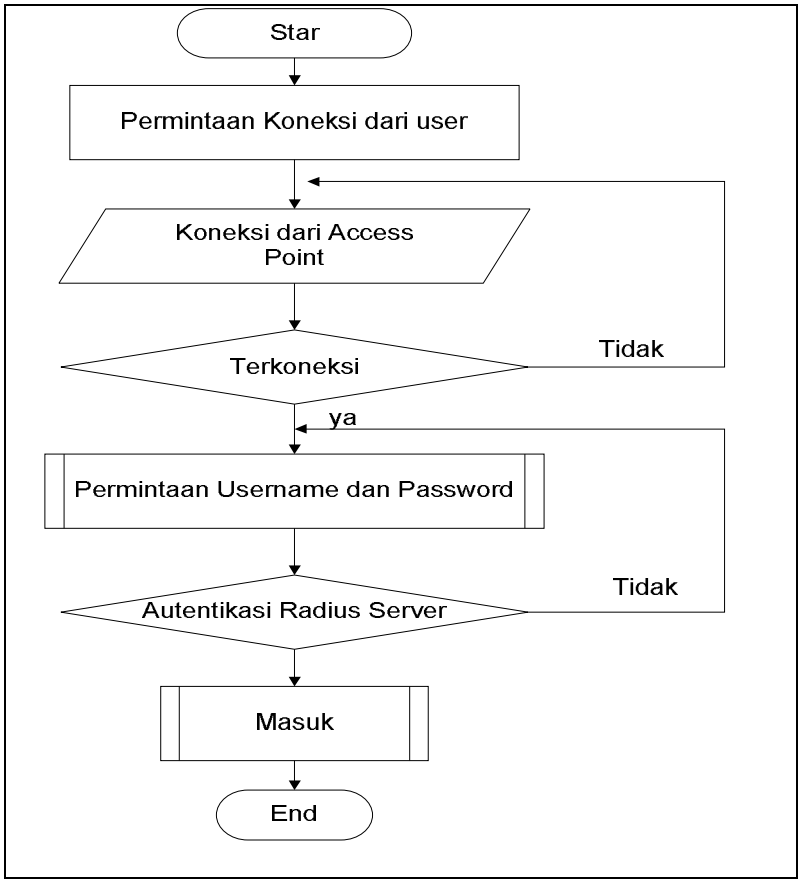
a. SSID : nama *Wifi* HOTSPOT-PENGADILAN
b. Untuk bagian *network* silahkan pilih *Autoconfiguration DHCP*.
c. Untuk bagian *security disable* fitur tersebut (*no encryption).*

Fungsi chillispot disini adalah sebagai pemberi IP *address*, sebagai *security,* dan sebagai pemberi izin dalam melakukan *surfing internet*. Jika semuanya sudah selesai configurasinnya, tahap terakhir

adalah menghubungkan PC *server Radius* yang telah kita configurasi. Selanjutnya restart semua system yang dikonfigurasi .

5.3.15 Alur Sistem Yang digunakan

Dimana alur permintaan koneksi dari *client* ke *Access point* kemudian *Access Point* akan menanyakan ke Radius server apabila antara *client* terdapat kecocokan, maka *client* akan diijinkan masuk atau *login* menggunakan *username* dan *password*. selanjutnya Radius Server akan bekerja untuk mengautentikasi *client* yang akan mengakses permintaan data dari server. Jika autentikasi berhasil selanjutnya *client* diijinkan mengakses data dari server. Kemudian dilakukan proses *authorisasi* (semacam pengalokasian *client*) untuk memberikan hak akses apa saja yang diperbolehkan diakses oleh *client*, dari server sendiri akan memonitoring kegiatan *client* dengan aplikasi *chillispot*.



Gambar 5.16 Flochat Radius

BAB VI

SIMPULAN DAN SARAN

6.1 Simpulan

Setelah melakukan pembahasan, maka penulis dapat menyimpulkan bahwa penggunaan *Access Point* berbasis *PC* sebagai media *Sharing Koneksi Internet* menggunakan *Wireless* serta menggunakan dua sistem keamanan yaitu menggunakan *User Authentication* untuk *User* pegawai atau tamu dan *MAC Address Filtering* untuk staf Pegawai Pengadilan Tinggi Palembang sangat baik dan dapat diterapkan pada jaringan komputer di Pengadilan Tinggi Palembang. *Freeradius* memiliki kemampuan yang sangat baik didalam sistem keamanan *Wireless* sehingga dapat mencegah *user* yang tidak diinginkan masuk dengan leluasa tanpa melewati sistem keamanan yang ada. Pembuatan *Access Point* berbasis *PC (Personal Computer)* dapat berjalan dengan menggunakan Sistem *Operasi Mikrotik*, aplikasi *Freedius* dan *mysql* sebagai *database server*, aplikasi *Web PHP* sebagai *captive portal* sebagai *web interfaces* untuk *memanagement user hotspot.*

6.2 Saran

Penulis juga memberikan saran guna meningkatkan kinerja *Access Point* pada jaringan komputer Pengadilan Tinggi Palembang antara lain:

1. Diharapkan adanya penambahan kapasitas *bandwidth* untuk mempercepat dan memperlancar koneksi internet pada Pengadilan Tinggi Palembang.
2. Diharapkan adanya penambahan *Hardwere Wireless Card* pada setiap Komputer agar dapat mengakses internet tanpa harus koneksi ke kabel UTP.
3. Peningkatan spesifikasi *server wireless* agar dapat lebih optimal untuk menjalankan fungsinya sebagai penyedia lanyanan *hotspot* Pengadilan Tinggi Palembang.
4. Perlunya penataan ulang kabel jaringan dan penempatan server di tempat yang aman agar aman dan terlihat rapi.
5. Sosialisasi kepada pegawai agar penggunaan fasilitas *hotspot* Pengadilan Tinggi Palembang lebih maksimal. Hal ini dapat di lakukan dengan pemasangan tanda area *hotspot* pada tempat-tempat tertentu.

DAFTAR PUSTAKA

Deris Stiawan, *Wireless Fundamental, Instalation & Implemetations*, 2008 http://www.ilkom.unsri.ac.id/deris.

Febyatmoko,Gesit Singgih, Hidayat Taufiq, Mukhammad Andri S, 2008, **Sistem Otentikasi,Otorisasi dan Pelaporan Koneksi *User* Pada Jaringan *Wireless* menggunakan Chillipspot dan Radius Server.** Universitas Islam Indonesia.

Goldman, James E. 2001, **Aplikasi Data Communications, A Business-Oriented Approach**. :John Wiley & Sons.

Hantoro, Dwi. 2009. ***Wi-Fi Jaringan Komputer Tanpa Kabel***. Bandung: Informatika

Kuntoro, Tri. 2005. ***Jaringan Wi-Fi Teori dan Implementasi*.** Yogyakarta: Andi Offset.

Kunang, Yesi Novaria, Yadi Ilman Zuhri, 2008. **Sistem Autentikasi Pengguna *Wireless* LAN Berbasis Radius Server**. Universitas Bina Darma Palembang.

Purbo, Onno W. 2006. ***Internet Wireless dan HotSpot***. Jakarta: Elex Media Komputindo.

Sofana, Iwan.2011. ***Tiori dan Module Pratikum Jaringan Komputer.*** Bandung Module.

Sopandi, Dede. 2010. ***Installasi dan Konfigurasi Jaringan Komputer.*** Informatika Bandung.Bandung.

Siregar, Edison. 2010. ***Langsung Praktik Mengelolah Jaringan Lebih Efektif dan Efesien.*** Yogyakarta:Andi.

Umar, 2007, ***Metode untuk Skripsi dan Tesis Bisnis***, Jakarta: Raja Garfindo Persada.

Varamita, *2008*. ***Remote Authentication Dial-In User Service***, http://ilkom.unsri.ac.id

Wagito. 2007. ***Jaringan Komputer Tiori dan Implementasi Berbasis Linux***. Gava Media : Yogyakarta.

Wahana Komputer, 2006, ***Pengelolaan Jaringan Komputer di Linux.*** Jakarta: Salemba Infotek.

Wirawan DEA, ***Mata Kuliah Jaringan Nirkabel Pita Lebar***, http://oc.its.ac.id, 2008.