# BAB 2

# LANDASAN TEORI

## 2.1 JARINGAN KOMPUTER

Dengan berkembangnya teknologi komputer dan komunikasi suatu model komputer tunggal yang melayani seluruh tugas-tugas komputasi suatu organisasi kini telah diganti dengan sekumpulan komputer yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya, sistem seperti ini disebut jaringan komputer (*computer network*) ( Tannenbaum 1997 , p.1 ).

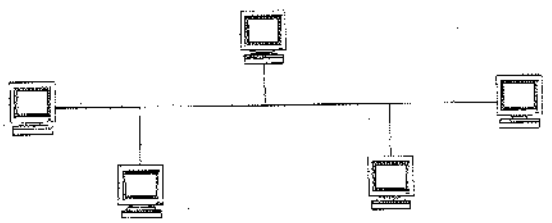
### 2.1.1 LOCAL AREA NETWORK ( LAN )

*Local Area Network* (LAN) merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer. ( Tannenbaum 1997, p.8)

. LAN bekerja pada kecepatan 10 sampai 100 Mbps (mega bit/detik) dengan delay rendah (puluhan mikro detik) dan mempunyai faktor kesalahan yang kecil. Saat ini LAN mampu beroperasi pada kecepatan yang lebih tinggi, sampai Gigabit ( 1000 Mega ) / detik. Dalam LAN , dikenal istilah topologi jaringan. Topologi jaringan didefinisikan sebagai suatu denah / peta mengenai bagaimana cara menghubungkan komputer satu dengan yang lain ( wijaya 2003. p.13 ) . Ada beberapa macam topologi jaringan, diantaranya :

1. Topologi Bus

Dengan topologi bus ini, komputer dihubungkan secara berantai ( *daisy – chain* ) satu dengan yang lain dengan perantara suatu kabel yang pada umumnya berupa kabel jenis koaksial

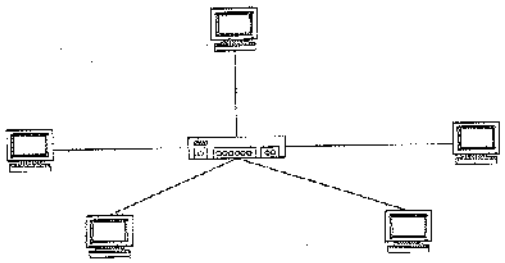


**Gambar 2.1 Topologi Bus**

Topologi ini umumnya tidak menggunakan suatu peralatan aktif untuk menghubungkan komputer, oleh sebab itu ujung – ujung kabel koaksial harus ditutup dengan tahanan ( terminator resistor ) untuk menghindari pantulan yang dapat menimbulkan gangguan yang menyebabkan kemacetan jaringan.

2. Topologi Star

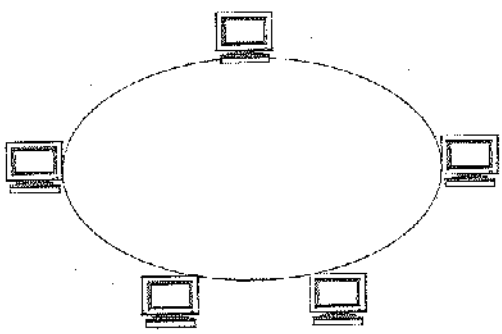
Pada topologi *Star*, masing-masing *workstation* dihubungkan secara langsung ke *server* atau *hub*. Keunggulan dari topologi tipe *Star* ini adalah bahwa dengan adanya kabel tersendiri untuk setiap *workstation* ke *server*, maka *bandwidth* atau lebar jalur komunikasi dalam kabel akan semakin lebar sehingga akan meningkatkan unjuk kerja jaringan secara keseluruhan. Dan juga bila terdapat gangguan di suatu jalur kabel maka gangguan hanya akan terjadi dalam komunikasi antara *workstation* yang bersangkutan dengan *server*, jaringan secara keseluruhan tidak mengalami gangguan. Kelemahan dari topologi Star adalah kebutuhan kabel yang lebih besar dibandingkan dengan topologi lainnya



**Gambar 2.2 Topologi Star**

3. Topologi Ring

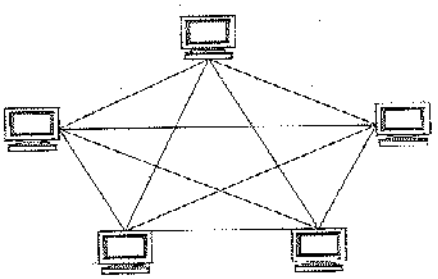
Di dalam topologi *Ring* semua *workstation* dan *server* dihubungkan sehingga terbentuk suatu pola lingkaran atau cincin. Tiap *workstation* ataupun *server* akan menerima dan melewatkan informasi dari satu komputer ke komputer lain, bila alamat- alamat yang dimaksud sesuai maka informasi akan diterima dan bila tidak informasi akan dilewatkan. Kelemahan dari topologi ini adalah setiap *node* dalam jaringan akan selalu ikut serta mengelola informasi yang dilewatkan dalam jaringan, sehingga bila terdapat gangguan di suatu *node* maka seluruh jaringan akan terganggu. Keunggulan topologi *Ring* adalah tidak terjadinya *collision* atau tabrakan pengiriman data seperti pada topologi *Bus*, karena hanya satu *node* dapat mengirimkan data pada suatu saat.



**Gambar 2.3 Topologi Ring**

4. Topologi Mesh

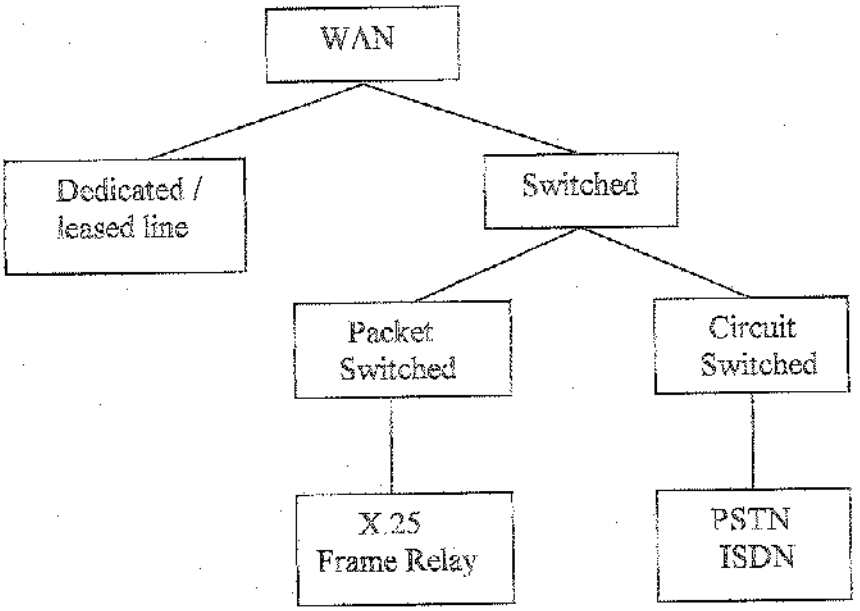
Topologi ini mempunyai jalur ganda dari setiap peralatan di jaringan. Semakin banyak jumlah komputer di jaringan, semakin sulit pemasangan kabel – kabel jaringannya karena jumlah kabel yang harus dipasang menjadi berlipat ganda. Oleh sebab itu jaringan mesh yang murni di mana setiap peralatan jaringan dihubungkan satu dengan yang lainnya jarang digunakan. Yang sering dipakai adalah pembuatan jalur ganda untuk hubungan – hubungan utama sebagai jalur cadangan jika terjadi kesulitan di jalur utama



**Gambar 2.4 Topologi Mesh**

### 2.1.2 WIDE AREA NETWORK ( WAN )

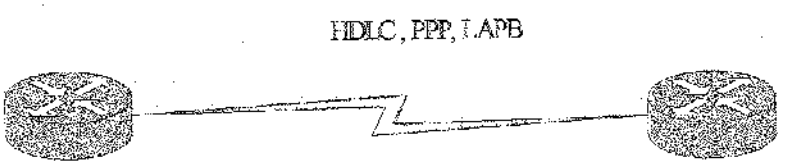
WAN menghubungkan sekelompok jaringan dengan kelompok jaringan yang lain yang terdapat di kota lain atau di pulau lain bahkan di negara lain ( Hayri 2003, p.108 ). Secara umum , teknologi WAN dapat dikategorikan kedalam 2 bagian , yaitu *Dedicated* dan *Switched* ( CNAP , 4th semester)




**Gambar 2.5 Teknologi WAN**

1. Dedicated

Jenis layanan ini biasanya menggunakan biaya tetap. Maksudnya, digunakan maupun tidak biaya yang dibayar kepada provider jaringan setiap bulannya sama. Besarnya biaya tergantung bandwidth yang disewa dan jarak. *Dedicated* atau *Leased Line* menggunakan koneksi point-to-point yang menghubungkan satu area lokasi dengan lokasi lainnya.




**Gambar 2.6 Dedicated WAN**

2. Switched

A. Circuit Switched

*Circuit-switched* merupakan koneksi yang menggunakan metode WAN *switching* di mana koneksi antar kedua titik jaringan dibangun, dipelihara, dan diputuskan setiap melakukan sesi komunikasi. Pada jaringan perusahaan telepon, *circuit-switched* beroperasi layaknya operasi telepon biasa.. Pada saat ini, koneksi yang biasa digunakan hanya mampu memperoleh bandwidth maksimum 56Kbps. Salah satu keuntungan menggunakan jaringan *circuit-switched* adalah biaya penggunaannya yang relatif murah dan dapat dikontrol

B. Packet Switched

*Packet Switched* merupakan metode *switching* , dimana suatu perangkat jaringan dapat membagi – bagi satu koneksi fisikal menjadi beberapa koneksi yang bersifat logikal. Contoh dari *packet switching* adalah *frame relay* dan X.25.

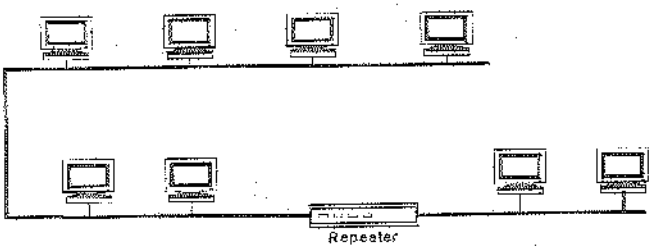
## 2.2 KOMPONEN JARINGAN

Komponen atau peralatan jaringan dapat digolongkan atas beberapa jenis yaitu :

### 2.2.1 REPEATER

*Repeater* adalah komponen dari suatu jaringan yang bertugas untuk menguatkan data / sinyal yang dilewatkan pada jalur tersebut. Dapat digunakan untuk sinyal analog maupun digital, biasanya digunakan untuk transmisi data jarak jauh. Repeater diperlukan karena misalnya sebuah *Ethernet Card* dengan kabel UTP CAT5 hanya mampu untuk menjangkau sampai jarak tertentu saja ( 100 meter ). *Repeater* akan

meneruskan dengan menguatkan sinyalnya untuk mendukung integritas data yang dilewatkan tersebut.




**Gambar 2.7 Repeater**

### 2.2.2 HUB dan SWITCH

Hub adalah komponen dalam jaringan yang menghubungkan beberapa komputer sekaligus. Tipe dari hub antara lain:

- Aktif, juga menguatkan sinyal (*repeater*)
- Pasif, tidak menguatkan sinyal hanya meneruskan
- *Intelegent*, mempunyai fungsi tambahan contohnya *switch*.

Hub akan mengirim paket ke semua komputer yang dihubungkan ke hub tersebut tetapi switch hanya akan melewatkan paket ke alamat yang dituju. Karena *switch* mempunyai kemampuan mendeteksi alamat komputer yang akan dituju. Jelas disini *switch* lebih aman dan lebih cepat. *Switch* pada saat yang sama dapat menangani lebih dari satu koneksi.

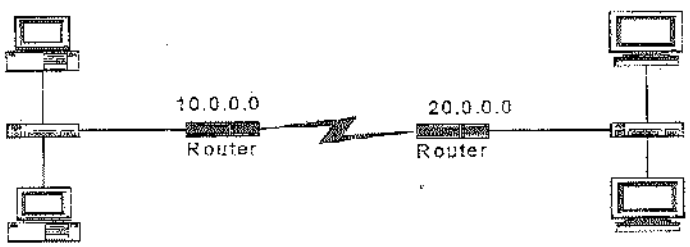
### 2.2.3 BRIDGE

Komponen yang menghubungkan dua LAN. Bisa membagi dua jaringan besar menjadi 2 jaringan yang lebih kecil. Ciri khusus dari jaringan itu adalah menggunakan protokol yang sama. Manfaat adanya bridge juga meningkatkan kinerja jaringan karena

dapat mengatur trafik jaringan dalam segmen yang kecil. Dibandingkan dengan *router*, *bridge* mempunyai kecepatan yang lebih tinggi.

### 2.2.4 ROUTER

*Router* adalah komponen jaringan yang bertugas *routing* paket dari suatu jaringan ke jaringan lain. Tugasnya memberi jalan paket antara network yang berbeda.




**Gambar 2.8 Router**

### 2.2.5 GATEWAY

*Gateway* adalah komputer yang bertugas pengkonversi protokol antara tipe jaringan yang berbeda ataupun aplikasi yang berbeda. Contohnya *gateway* dapat mengkonversi paket *TCP/IP* ke pakct *IPX* pada *Netware* . *Gateway* sebagai pintu gerbang kita untuk ke dunia luar (internet), maka semua paket yang keluar dari jaringan intern kita akan melalui gateway ini. Karena gateway sebagai pintu gerbang, maka untuk melindungi jaringan didalamnya dari ancaman luar dapat dipasang *firewall*.

## 2.3 KEAMANAN JARINGAN

Keamanan jaringan didefinisikan sebagai sebuah perlindungan dari sumber daya daya terhadap upaya penyingkapan, modifikasi, utilisasi, pelarangan, perusakan oleh pihak - pihak yang tidak diijinkan . ( Stalling 2000, p.5 )

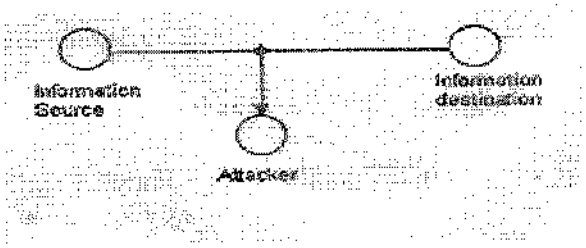
### 2.2.1 TIPE – TIPE SERANGAN PADA JARINGAN

Pada dasarnya, ada dua tipe serangan ( stalling , p.8 ) , yaitu :

1. Serangan yang bersifat pasif ( *passive attack* )

Serangan yang bersifat pasif dilakukan dengan cara melakukan pemantauan dan atau perekaman data selama data ditransmisikan lewat fasilitas komunikasi. Tujuan penyerang adalah untuk mendapatkan informasi yang sedang dikirimkan. Kategori ini memiliki dua tipe *yaitu* ***Release of message contain*** dan ***Traffic Analysis.***

Tipe *Release of message contain* memungkinan penyusup utnuk mendengar pesan, sedangkan tipe *traffic analysis* memungkinan penyusup untuk membaca *header* dari suatu paket sehingga bisa menentukan arah atau alamat tujuan paket dikirimkan. Penyusup dapat pula menentukan panjang dan frekuensi pesan.




**Gambar 2.9 Serangan pasif ( Passive attack )**

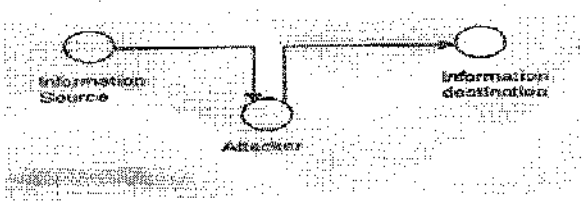
2. Serangan yang bersifat aktif ( *active attack* )

Serangan yang bersifat aktif menggunakan suatu peralatan yang terhubung ke fasilitas komunikasi untuk mengubah transmisi data atau mengubah isyarat kendali atau memunculkan data atau isyarat kendali palsu. Untuk kategori ini terdapat tiga tipe yaitu : *message-stream modification, denial of service* dan *masquerade*.

Tipe ***message-stream modification*** memungkinan pelaku untuk memilih untuk menghapus, memodifikasi, menunda, melakukan re-order dan menduplikasi pesan asli. Pelaku juga mungkin untuk menambahkan pesan-pesan palsu.

Tipe ***denial of service ( DoS )*** merupakan usaha ( dalam bentuk serangan ) untuk melumpuhkan sistem yang dijadikan target sehingga sistem tersebut tidak dapat menyediakan servis – servisnya ( *denial of service* ) atau tingkat servis menurun secara drastis. *Denial of service* dapat dilakukan dengan cara mematikan atau membanjiri saluran komunikasi dengan pesan – pesan ( yang dapat berupa pesan apa saja karena yang diutamakan adalah banyaknya pesan ) ( rahardjo 2002. p.13 ).

Tipe ***masquerade*** memungkinkan pelaku untuk menyamar sebagi host atau switch asli dan berkomunikasi dengan yang host yang lain atau switch untuk mendapatkan data atau pelayanan




**Gambar 2.10 Serangan Aktif ( Active Attack )**

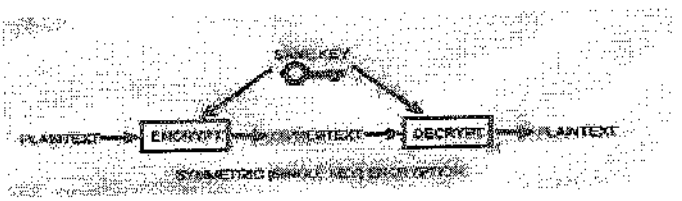
### 2.3.2 METODE – METODE PENGAMANAN PADA JARINGAN

Salah satu hal yang penting dalam komunikasi menggunakan komputer untuk menjamin kerahasian data adalah enkripsi. Enkripsi dapat didefinisikan sebagai proses konversi suatu informasi dalam bentuk yang dapat dibaca ( *plaintext* ) ke dalam bentuk yang tidak dapat dimengerti oleh pihak lain ( *ciphertext* ) ( Purbo 2002, p.97 ). Bila penerima data yang sudah dienkrip ingin membaca data semula, maka penerima data tersebut harus mengkonversikannya kembali ke bentuk semula melalui proses dekripsi .

Dekripsi adalah proses kebalikan dari enkripsi yaitu proses mengubah dari *ciphertext* menjadi *plaintext* . Terdapat dua kategori dari enkripsi yaitu :

1. Enkripsi Konvensional

Metode enkripsi ini juga dkenal dengan *private key* atau *symetric key* . Proses enkripsi pada metode ini dapat digambarkan sebagai berikut :



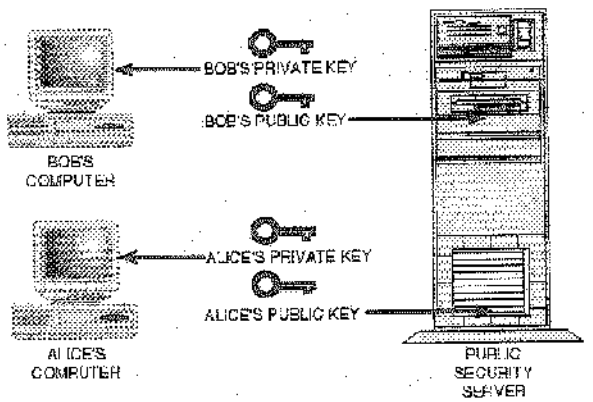

**Gambar 2.11 Enkripsi Konvensional**

Keamanan dari enkripsi konvensional bergantung pada beberapa faktor. Pertama algoritma enkripsi harus cukup kuat sehingga menjadikan sangat sulit untuk mendekripsi *cipher* teks tersebut. Lebih jauh dari itu keamanan dari algoritma enkripsi konvensional bergantung pada kerahasian dari kuncinya bukan algoritmanya. Atau dengan kata lain, kita tidak perlu menjaga kerahasiaan dari algoritma tetapi cukup dengan kerahasiaan kuncinya. Manfaat dari konvensional enkripsi algoritma adalah kemudahan dalam penggunaan secara luas.

2. Enkripsi *Public-Key*

Salah satu yang menjadi kesulitan utama dari enkripsi konvensional adalah perlunya untuk mendistribusikan kunci yang digunakan dalam keadaan aman. Sebuah metode yang lain telah ditemukan untuk mengatasi kelemahan ini dengan suatu model enkripsi yang tidak memerlukan sebuah kunci untuk didistribusikan. Metode ini dikenal dengan nama enkripsi *public-key* yang juga disebut dengan *asymmetric encryption* dan pertama kali

diperkenalkan pada tahun 1976 oleh ahli masalah keamanan bernama Whitfield Diffie dan Martin Hellman




**Gambar 2.12 Enkripsi Publik-key**

- Seperti terlihat pada gambar , masing-masing orang mempunyai sepasang kunci, kunci privat dan kunci publik, yang secara teori sama tetapi beda dalam fungsi.
- Dari dua kunci tersebut, satu buah disimpan secara pribadi (kunci privat) dan yang satunya dipublikasikan (kunci publik)

Kunci pribadi dijaga kerahasiaanya oleh pemiliknya atau diberikan pada server kunci publik apabila dihendaki. Apabila kita menginginkan untuk mengirimkan sebuah pesan terenkripsi, maka kunci publik dari penerima pesan harus diberitahukan untuk mengenkripsi pesan. Saat pesan tersebut sampai, maka penerima akan mendekripsi pesan dengan kunci pribadinya..Yang menjadi kelemahan dari metode enkripsi *public key* adalah jika dibandingkan dengan metode enkripsi konvensional algoritma enkripsi ini mempunyai algoritma yang lebih komplek, sehingga akan menghasilkan performa yang lebih rendah

**FIREWALL**

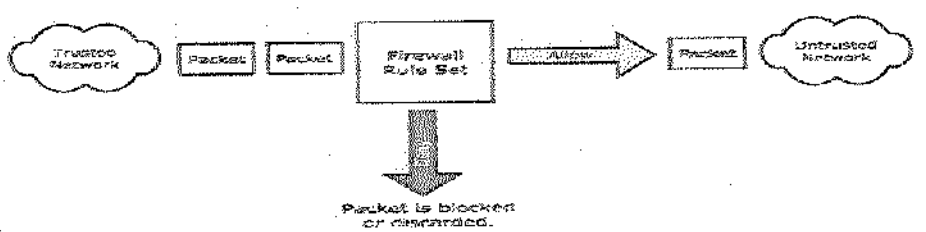
Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan / kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah *workstation, server, router* atau *local area network* (LAN) ( Muammar 2001, p.1 )

**2.3.3.1 TIPE FIREWALL**

Ada beberapa tipe dari firewall yaitu *Packet Filtering Router, Application Level-Gateway dan Statefull packet-inspection engine*

1. Packet Filtering Router

*Packet Filtering* diaplikasikan dengan cara mengatur semua paket IP baik yang menuju, melewati atau akan dituju oleh paket tersebut. Pada tipe ini paket tersebut akan diatur apakah akan di terima dan diteruskan atau di tolak. Penyaringan paket ini di konfigurasikan untuk menyaring paket yang akan di transfer secara dua arah (baik dari dan ke jaringan lokal). Kelebihan dari tipe ini adalah mudah untuk di implementasikan, transparan untuk pemakai, relatif lebih cepat. Adapun kelemahannya adalah cukup rumitnya untuk men-setting paket yang akan difilter secara tepat, serta lemah dalam hal otentifikasi.



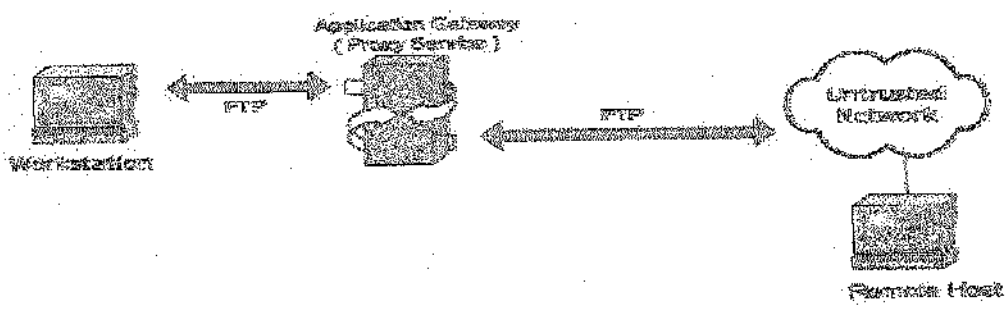

**Gambar 2.13 Packet Filtering Router**

2. Application – Level Gateway

*Application-level Gateway* yang biasa juga di kenal sebagai *proxy server* yang berfungsi untuk memperkuat/menyalurkan arus aplikasi. Tipe ini akan mengatur semua hubungan yang menggunakan layer aplikasi , misal *FTP* dan *HTTP*.Cara kerjanya adalah apabila ada pengguna yang menggunakan salah satu aplikasi semisal *FTP* untuk mengakses secara *remote*, maka *gateway* akan meminta user memasukkan alamat *remote host* yang akan di akses. Saat pengguna mengirimkan user ID serta informasi lainnya yang sesuai maka *gateway* akan melakukan hubungan terhadap aplikasi tersebut yang terdapat pada *remote host*, dan menyalurkan data diantara kedua titik. apabila data tersebut tidak sesuai maka *firewall* tidak akan meneruskan data tersebut atau menolaknya.

Kelebihannya adalah relatif lebih aman daripada tipe *packet filtering router* serta lebih mudah untuk memeriksa (audit) dan mendata (log) semua aliran data yang masuk pada level aplikasi.

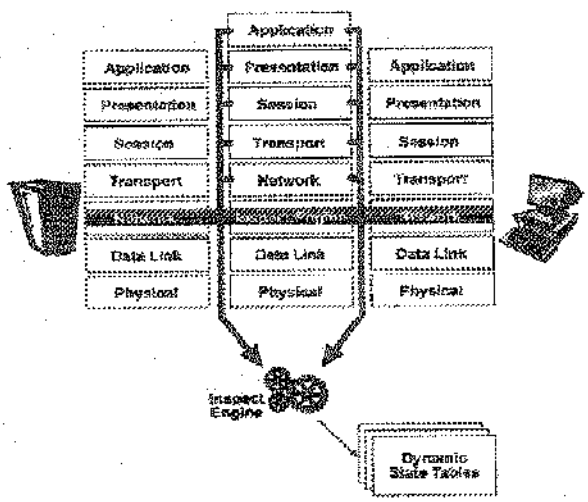
Kekurangannya adalah pemrosesan tambahan yang berlebih pada setiap hubungan. yang akan mengakibatkan terdapat dua buah sambungan koneksi antara pemakai dan gateway, dimana gateway akan memeriksa dan meneruskan semua arus dari dua arah.




Gambar 2.14 Application Level-Gateway

3. Stateful packet – inspection engine

Teknologi ini menggabungkan beragam fitur terbaik dari teknologi *Packet Filtering* dan teknologi *Application Gateway*. Teknologi ini dioperasikan diantara *layer Datalink* dan *layer Network* yang dalam kasus ini diletakkan antara kartu interface jaringan dengan *driver TCP/IP*. Teknologi ini membutuhkan sedikit lebih besar memori dan siklus CPU daripada teknologi penyaringan paket karena ia harus melakukan lebih banyak aktivitas. Akan tetapi, secara substansi tetap membutuhkan lebih sedikit pemakaian memori dan siklus CPU daripada teknologi gateway layer aplikasi.




**Gambar 2.15 Stateful packet – inspection engine**

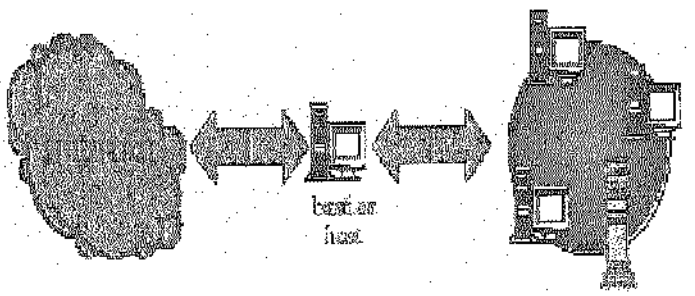
### 2.3.3.2 KONFIGURASI FIREWALL

Pada *firewall* , ada beberapa cara yang bisa dilakukan untuk melakukan konfigurasi firewall yaitu *Dual Homed Host / Dual Homed Gateway* , *Screened Host Gateway* serta *Screened Subnet Gateway*

1. Dual Homed Gateway ( DHG )

Sistem DHG menggunakan sebuah komputer dengan paling sedikit 2 kartu jaringan ( *network card interface* / NIC ). Interface pertama dihubungkan ke jaringan

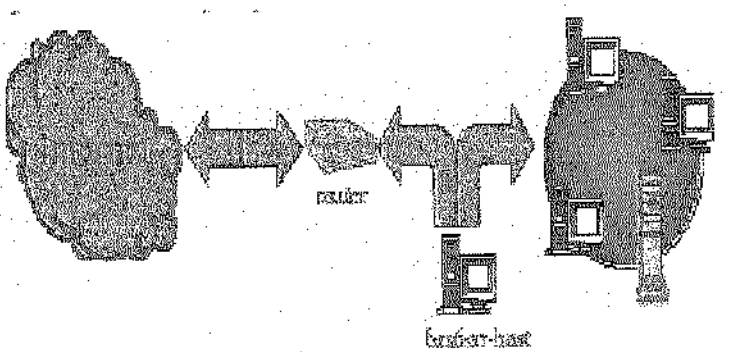
internal dan yang lainnya ke internet. Komputer ini juga berfungsi sebagai *bastion host* (bagian terdepan dan terpenting dari jaringan)



**Gambar 2.16 Dual Home Gateway**

2. Screened Host Gateway

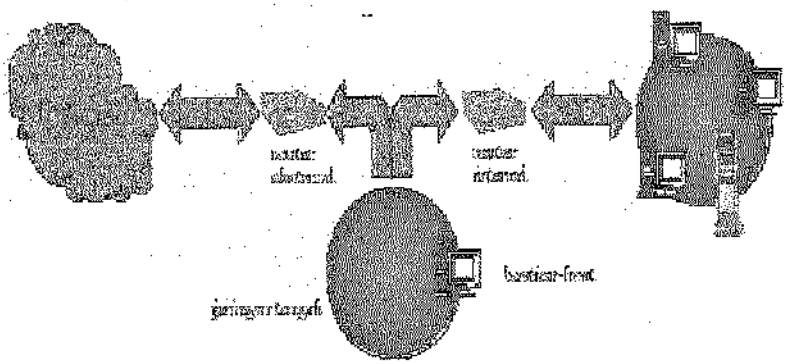
Pada topologi ini , fungsi *firewall* dilakukan oleh sebuah *router* dan *bastion host. Router* ini dikonfigurasi sehingga akan menolak semua trafik dari internet kecuali yang ditujukan ke *bastion host.* Sedangkan untuk trafik keluar dari jaringan internal hanya dari IP bastion host yang diijinkan



**Gambar 2.17 Screened Host Gateway**

3. Screened Subnet Gateway

*Firewall* dengan arsitektur ini menggunakan dua router dan jaringan tengah ( *perimeter network* ) antara kedua *router* tersebut ditempatkan sebuah *bastion host*



Gambar 2.18 Screened Subnet Gateway

### 2.3.3.3 LANGKAH MEMBANGUN FIREWALL

Ada beberapa tahapan yang harus dilakukan bila ingin menerapkan firewall pada jaringan ( Muammar 2001 p.6 ). Langkah tersebut antara lain :

1. Mengidentifikasikan bentuk jaringan yang dimiliki

   Dengan mengetahui bentuk jaringan yang dimiliki khususnya topologi yang digunakan serta protokol jaringan , akan memudahkan dalam mendesain suatu *firewall*

2. Menentukan *policy* atau kebijakan

   Penentuan kebijakan atau *policy* merupakan hal yang harus dilakukan, baik buruknya sebuah *firewall* yang dibangun sangat ditentukan oleh *policy* / kebijakan yang diterapkan . Diantaranya :

   - Menentukan apa saja yang perlu di layani. Artinya, apa saja yang akan dikenai *policy* atau kebijakan yang akan kita buat
   - Menentukan individu atau kelompok-kelompok yang akan dikenakan *policy* atau kebijakan tersebut
   - Menentukan layanan-layanan yang di butuhkan oleh tiap tiap individu atau kelompok yang menggunakan jaringan

- Berdasarkan setiap layanan yang di gunakan oleh individu atau kelompok tersebut akan ditentukan bagaimana konfigurasi terbaik yang akan membuatnya semakin aman
- Menerapkankan semua *policy* atau kebijakan tersebut

3. Menyiapkan *software* atau *hardware* yang digunakan

Baik itu sistem operasi yang mendukung atau *software-software* khusus pendukung *firewall* seperti *ipchains*, atau *iptables* pada linux, dsb. Serta konfigurasi *hardware* yang akan mendukung *firewall* tersebut.

4. Melakukan tes konfigurasi

Pengujian terhadap *firewall* yang telah selesai di bangun haruslah dilakukan, terutama untuk mengetahui hasil yang akan kita dapatkan, caranya dapat menggunakan *tool* yang biasa dilakukan untuk mengaudit.

### 2.3.4 RADIUS

RADIUS ( *Remote Autentication Dial In User Service* ) adalah suatu sistem sentralisasi dari proses otentifikasi , otorisasi dan perhitungan ( akunting ) pada client server di jaringan. Proses otentikasi , otorisasi dan perhitungan inilah yang dikenal dengan AAA ( *Authentication , Autorization , Accounting* ).

1. Authentication

Authentication adalah proses verifikasi terhadap pemakai untuk diketahui identitasnya. *Authentication* menggunakan kombinasi dari logon ID dan password yang merepresentasikan bahwa keberadaan pemakai tersebut adalah asli ( otentik )

2. Authorization

   Authorization menentukan hak akses pemakai ke dalam suatu sistem. Sebagai contoh dalam sistem penyedia jasa internet ( ISP ). Proses *authorization* akan menentukan alamat IP yang dapat diberikan kepada client , apakah statik atau dinamik

3. Accounting

   Accounting merupakan sebuah proses yang mengukur dan menginformasikan jumlah waktu atau jumlah data yang diterima atau dikirmkan oleh pemakai selama sesi pemakaian. Informasi yang diberikan dalam proses ini diterima melalui statistik dari sebuah sesi , informasi pemakaian dan digunakan untuk pengaturan otorisasi billing , analisis dan pemakaian sumber daya ( *resources* )

RADIUS mempunyai 2 keunggulan yaitu dalam hal keamanan dan kemudahan manajemen *user*

a. Keamanan

   Dengan menggunakan RADIUS , semua informasi tentang pengguna ( *user* ) dapat disimpan di satu komputer , sehingga dapat mengurangi celah kemanan. Semua otentifikasi serta akses ke jaringan diatur oleh sebuah *server* RADIUS

b. Kemudahan Manajemen

   Radius server menyimpan semua data mengenai *user* dalam bentuk *textfile* di satu tempat. Admin jaringan dapat menambah user baru atau memodifikasi user lama hanya dengan mengubah textfile tersebut

## 2.4 SECURITY POLICY

Security Policy pada dasarnya adalah sebuah rancangan dan daftar yang berisi mengenai apa saja aset perusahaan yang penting serta bagaimana aset tersebut harus dilindungi ( Danchev 2003, p.4 ). Secara umum, sebuah *security policy* mencakup hal – hal sebagai berikut ( onno 2002, p.5 ) :

- Deskripsi secara detail tentang lingkungan teknis dari jaringan, hukum yang berlaku, otoritas dari *policy* tersebut, dan aturan dasar yang digunakan pada saat mengaplikasikan *policy* tersebut
- Analisis resiko yang mengidentifikasikan aset – aset jaringan perusahaan, ancaman yang dihadapi aset tersebut, dan biaya yang harus dikeluarkan untuk kerusakan / kehilangan atas aset – aset tersebut.
- Petunjuk bagi administrator sistem untuk mengelola sistem
- Definisi bagi user tentang hal – hal yang boleh dilakukan

Sebelum menyusun *security policy*, perusahaan harus terlebih dahulu mengidentifikasi hal – hal yang diperlukan yaitu identifikasi aset ( *Risk Analysis* ) dan identifikasi ancaman ( *Risk Management* ) ( Danchev 2000 , p4 )

### 2.4.1 RISK ANALYSIS

*Risk analysis* adalah proses identifikasi mengenai apa saja aset informasi perusahaan yang penting ( *critical* ) serta manfaat dan cara menggunakannya. Pada intinya, *risk analysis* mendefinisikan mengenai *WHAT* ( apa saja yang harus kita lindungi ), *WHOM* ( dari siapa kita harus melindungi ), dan *HOW* ( bagaimana cara kita melindungi ). Dalam

*risk analysis*, point – point yang harus diperhatikan adalah :

1. *Hardware* , mencakup semua *server, workstation , personal computer ( pc )*, laptop, *removable media ( disk, cd, tape )*, dll.
2. *Software*, mencakup identifikasi mengenai *software update* dan *patches*
3. Personnel, mengenai siapa saja yang bisa mengakses data perusahaan yang bersifat rahasia ( *confidential* ) maupun *database* perusahaan

### 2.4.2 RISK MANAGEMENT

*Risk management* adalah proses identifikasi mengenai apa saja yang berpotensi sebagai ancaman keamanan data perusahaan.Hal – hal yang mencakup dalam *risk management* adalah :

1. Password , meliputi pemilihan password ( *password creation* ), jangka waktu pemakaian ( *password aging* ) dan panjang password.( *password length* )
2. Perlindungan dari virus , meliputi perlindungan dari kode berbahaya ( *malicious code* ), kapan harus dilakukan *scanning* , dan kapan harus dilakukan *update* anti virus
3. Instalasi *software* , meliputi software apa saja yang boleh di-install di komputer
4. *Removable* media, meliputi penggunaan disket , *USB drive* , dll.

## 2.5 WIRELESS LAN ( WLAN )

Wireless Local Area Network adalah suatu sistem komunikasi data yang bersifat fleksibel yang menggunakan infra merah ( infrared ) maupun gelombang radio untuk memancarkan dan menerima informasi di medium udara. ( Barnes 2002, p.2 )

### 2.5.1 KOMPONEN WLAN

Komponen yang dibutuhkan dalam WLAN adalah :

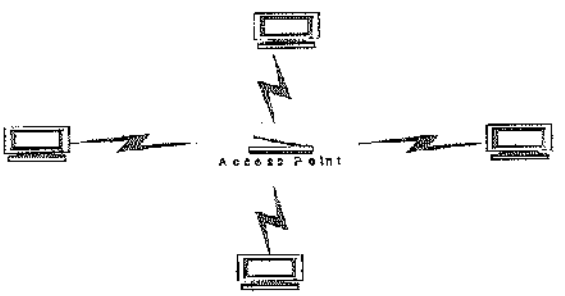
a. *LAN card / NIC* khusus untuk *wireless*

b. Access Point

Access Point ( AP ) memiliki fungsi yang sama dengan hub pada jaringan *wireline*. AP memiliki dua bentuk, yaitu dalam bentuk hardware dan software

- Hardware Access Point

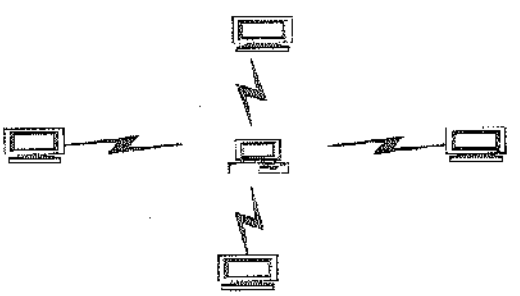
AP yang berbentuk *hardware* memiliki cara kerja yang sama dengan hub dalam jaringan kabel , namun memiliki kapasitas yang terbatas. AP hardware dapat menampung 100 komputer. AP dalam bentuk ini memiliki jangkauan yang lebih baik dibandingkan dengan AP dalam bentuk software




**Gambar 2.19 Hardware Access Point**

- Software Access Point

AP dalam bentuk *software* menggunakan suatu komputer yang akan digunakan sebagai AP. AP *software* memiliki fitur yang lebih baik dibandingkan dengan AP hardware, salah satunya adalah fitur file dan *printer sharing*. Kelemahan AP software adalah daya jangkau yang dimilikinya



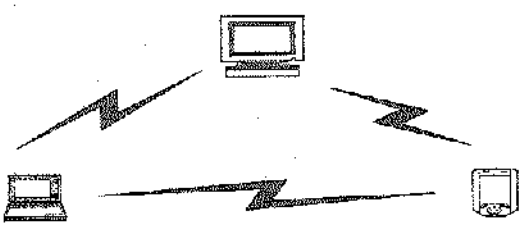
**Gambar 2.20 Software Access Point**

## 2.5.2 ARSITEKTUR WLAN

Semua komponen WLAN yang disebutkan diatas , dihubungkan dengan menggunakan konfigurasi tertentu. Ada dua arsitektur dari WLAN , yaitu *independent ( peer to peer )* dan *infrastructure*

A. Independent / Ad Hoc

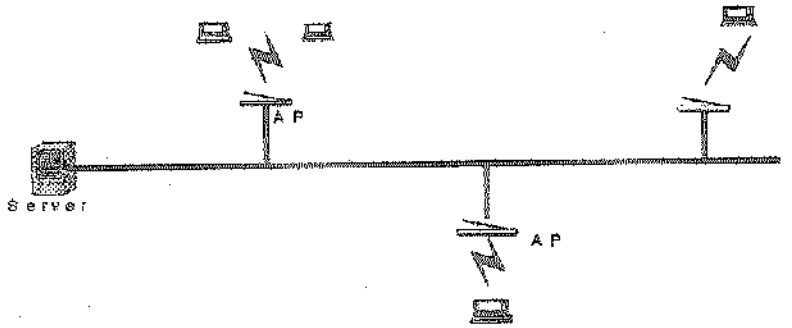
Jaringan Ad Hoc terbentuk bila antara terminal (*Notebook, Desktop* atau *PDA*) yang telah dilengkapi *Wireless LAN card* saling tersambung tanpa melalui *Access Point.* Contoh dari jaringan *ad hoc,* adalah jaringan yang memiliki konfigurasi *peer to peer. Ad Hoc* pada *wireless* LAN hanya membutuhkan *wireless NIC* di dalam setiap device yang terhubung ke jaringan.



**Gambar 2.21 Arsitektur Independent / Ad Hoc**

B. Infrastructure

*Infrastructure wireless LAN* adalah sebuah konfigurasi jaringan dimana jaringan *wireless* tidak hanya berhubungan dengan sesama jaringan *wireless* saja. Akan tetapi , terhubung juga dengan jaringan *wired.* Agar jaringan *wirelesss* dapat berhubungan dengan jaringan *wired* , maka disini digunakan *access point.*




**Gambar 2.22 Arsitektur Infrastucture**

### 2.5.3 STANDAR WLAN

Ada berbagai macam standar yang digunakan dalam *wireless LAN*. Masing – masing standar memiliki beberapa perbedaan mendasar seperti frekuensi yang digunakan , kecepatan serta daya jangkau dari setiap standar. Standar yang umum digunakan adalah 802.11 a , 802.11 b, dan 802.11 g.

1. 802.11 a

   Secara umum, 802.11 a bekerja pada frekuensi 5 GHz serta memiliki kecepatan maksimal hingga 54 Mbps. Standar ini dapat menampung hingga 64 *node* ( *user* ) per *access point*. Dari segi keamanan, standar ini mendukung enkripsi 64 bit dan 128 bit WEP. Karena standar ini bekerja pada frekuensi 5 GHz, maka standar ini tidak akan mengalami interferensi dari alat elektronik seperti *cordless phone* dan *Bluetooth* yang bekerja pada 2,4 GHz. Standar 802.11a sangat cocok digunakan untuk aplikasi yang membutuhkan bandwith yang besar seperti layanan aplikasi suara dan video serta transfer file dalam jumlah besar. Namun, standar ini hanya memiliki jarak jangkauan 50 m dari setiap point

2. 802.11 b

Standar b bekerja pada frekuensi yang lebih kecil yaitu 2,4 GHz. Dengan frekuensi ini, standar b memiliki daya jangkau yang lebih jauh dari standar a, yaitu hingga 300 m . Standar b hanya memiliki kecepatan maksimal sebesar 6Mbps; walaupun pada teorinya bisa ditentukan hingga 11 Mbps. Tingkat kecepatan ini jarang tercapai, karena banyak parameter dan *bandwidth* yang digunakan juga kadang tidak melakukan komunikasi secara sempurna. Standar ini banyak digunakan untuk *hotspot* ( layanan WLAN di tempat umum ) seperti hotel , bandara, dan kafe. Untuk keamanan, standar ini juga mendukung enkripsi WEP hingga 128 bit.

3. 802.11 g

Standar ini merupakan standar terbaru yang ditetapkan oleh IEEE ( *Institute of Electrical and Electronics Engineers* ). 802.11 g bekerja pada frekuensi yang sama dengan 802.11 b sehingga memiliki daya jangkau yang luas. Namun, dari kecepatan, standar ini mampu disejajarkan dengan standar a yang mampu bekerja hingga 54 Mbps.

4. Perbandingan ke-tiga standar WLAN

Setiap standar memiliki kelemahan dan kelebihan masing – masing yang berbeda. Berikut adalah kelebihan dan kelemahan masing – masing standar :

a. 802.11a

Kelebihan :

- Bekerja pada frekuensi 5 GHz sehingga bebas dari interfrensi peralatan elektronik seperti *cordless phone, microwave* dan *Bluetooth.*

- Mampu bekerja dengan kecepatan maksimal hingga 54 Mbps

Kekurangan :

- Harga relatif lebih mahal
- Memiliki jarak jangkauan yang lebih pendek ( sekitar 50 meter )
- Belum digunakan untuk kepentingan publik
- Tidak kompatibel dengan standar yang lain

b. 802.11b

Kelebihan :

- Standar yang paling banyak digunakan saat ini.
- Harga yang lebih terjangkau
- Memliki jangkauan yang lebih jauh ( hingga 300 m )
- *hotspot* yang menggunakan standar ini berkembang dengan cepat , sehingga memudahkan terjadinya komunikasi secara wireless.di area public

Kekurangan

- Hanya mampu bekerja hingga kecepatan 6 MBps, walaupun pada standarnya bisa ditingkatkan hingga 11 MBps
- Karena bekerja pada frekuensi 2,4 GHz, maka sangat rentan dengan gangguan frekuensi dari peralatan elektronik seperti *cordless phone* maupun *Bluetooth*

c. 802.11g

Kelebihan

- Memiliki kecepatan maksimal hingga 54 Mbps

- Jarak jangkauan hingga 300 m
- Harga yang relatif lebih terjangkau
- Kompatibel dengan standar 802.11b sehingga bisa juga digunakan pada layanan *hotspot*

Kekurangan

- Sama seperti standar 802.11b yang bekerja pada 2,4 GHz, standar ini juga rentan atas gangguan frekuensi dari peralatan elektronik yang bekerja pada frekuensi yang sama

### 2.5.4 KEUNTUNGAN WLAN

Secara umum, penerapan WLAN dapat memberikan keuntungan antara lain ( barnes 2002 , p.16 ).

1. Kenyamanan

Aspek kenyamanan merupakan alasan utama bagi para profesional IT dan *user* ( pengguna ) jika menggunakan WLAN. Aspek ini dapat dibagi lagi menjadi beberapa sub - aspek , yaitu :

- Fleksibilitas

  WLAN menawarkan fleksibilitas dalam hal pemasangan dan pemakaian jaringan. Pengguna ( *user* ) bisa membuat WLAN sederhana untuk kepentingan sementara seperti konferensi maupun rapat.

- Mobility

  Pengguna WLAN dapat mengakses file , sumber daya jaringan maupun internet tanpa harus terhubung dengan kabel ke jaringan

2. Harga terjangkau

Dengan berkembangnya trend teknologi ke arah teknologi yang lebih murah, lebih cepat dan lebih handal, maka WLAN telah mencapai titik harga yang kompetitif baik dalam hal biaya komponen WLAN maupun biaya instalasi.

3. Kecepatan

Dalam hal kecepatan, WLAN mampu bekerja dengan kecepatan hingga 54 Mbps , dan hal ini akan terus bertambah melalui penelitian teknologi di masa yang akan datang

4. Produktivitas

Dengan meningkatnya kenyamanan , *mobility*, dan fleksibilitas dari para pengguna, maka akan juga meningkatkan produktivitas dari para pengguna itu sendiri.

### 2.5.5 KEAMANAN WLAN

1. SSID

Pada setiap *access point* , terdapat sebuah identitas yang dikenal dengan SSID ( Server Set ID ). SSID adalah suatu identifikasi terhadap konfigurasi yang memungkinkan *client* berkomunikasi dengan *access point* yang tepat dan benar menggunakan konfigurasi tertentu. Hanya *client* dengan SSID yang benar dapat melakukan komunikasi. SSID bekerja sebagai suatu " single set password " antara *access point* dengan *client*. Demi keamanan , sebaiknya SSID tidak dikonfigurasi secara default

2. WEP

Wired Equivalent Privacy ( WEP ) adalah standar enkripsi data untuk *wireless* LAN. WEP memberikan otentifikasi pengguna ( *user authentification* ) dan juga sistem

enkripsi data dari standar IEEE 802.11 yang banyak digunakan saat ini. WEP termasuk dalam *symetric encryption*. WEP menggunakan algoritma RC4 dengan enkripsi 64 bit dan 128 bit. WEP terdiri atas dua bagian yaitu 24 bit *Initialitation Vector ( IV )* yang berada pada *packet header* 802.11 dan sebuah *secret key*. WEP memiliki kelemahan dalam hal algoritma enkripsi serta *key management*.( Barnes 2002 , p.202 ). Salah satu penyebabnya adalah sistem enkripsi WEP yang statis , sehingga belum cukup aman . Karena seorang penyerang dengan perlengkapan wireless serta software untuk mengumpulkan dan menganalisa data, dapat mengetahui kunci yang digunakan. Kelemahan lainnya adalah, bila fitur WEP diaktifkan , maka dapat menurunkan throughput sebanyak 50 persen.

3. WPA

Dengan enkripsi WEP yang memiliki kelemahan seperti yang telah disebutkan, maka telah dikembangkan teknik pengamanan baru yang dikenal dengan WPA ( *Wi-Fi Protected Access* ). Teknik WPA adalah model kompatibel dengan spesifikasi standar draft IEEE 802.11. Teknik ini mempunyai beberapa tujuan dalam desainnya, yaitu kokoh, interoperasi, mampu digunakan untuk menggantikan WEP, dapat diimplementasikan pada pengguna rumahan atau corporate, dan tersedia untuk publik secepat mungkin. Teknik WPA didesain menggantikan metode keamanan WEP, yang menggunakan kunci keamanan statik, dengan menggunakan TKIP (*Temporal Key Integrity Protocol*) yang mampu secara dinamis berubah setelah 10.000 paket data ditransmisikan. Protokol TKIP akan mengambil kunci utama sebagai starting point yang kemudian secara reguler berubah sehingga tidak ada kunci enkripsi yang digunakan dua kali. Dengan kelebihan ini, WPA bukan berarti tidak memiliki kelemahan. Dengan WPA yang diaktifkan, *througput* yang dihasilkan tetap mengalami penurunan seperti halnya WEP. Dari sisi *hardware, wireless*

AP dan *NIC* harus mengenali standar WPA. Sedangkan dari sisi software, belum ada sistem operasi *windows* yang mengenali WPA secara default sehingga harus menginstall WPA *client.*

4. IEEE 802.1X Authentication

802.1X merupakan mekanisme otentifikasi pada WLAN yang dikembangkan oleh *Internet Community untuk* link protokol PPP LCP ( *Point to Point Link Control Protocol* ) sebagai suatu pengembangan dari RADIUS ( *Remote Authentication Dial-in User Service* ) ( http://www.airmagnet.com/) . Ada 3 bagian yang dibutuhkan dalam protokol 802.1X , antara lain :

a. Supplicant ( client )

b. Authenticator ( access point )

c. Authentication Server ( pada umumnya RADIUS server )

802.1X menggunakan *Extensible Authentication Protocol* ( EAP ) sebagai protokol otentifikasi. Ada beberapa macam dari EAP , antara lain :

a. MD5

MD5 adalah metode EAP tingkat dasar yang paling sederhana. MD5 memiliki tingkat keamanan yang yang paling rendah dibandingkan metode EAP lainnya.

b. TLS ( Transport Level Security )

TLS menggunakan suatu sertifikat untuk memvalidasi baik dari *authentication server* ke *supplicant* maupun sebaliknya.

c. PEAP ( Protected EAP )

PEAP adalah solusi keamanan tingkat tinggi dari EAP. Metode ini menggunakan suatu terowongan ( *tunnel* ) antara *supplicant* dan *authenticator*

sebagai bagian dari proses otentifikasi. Data akan melewati tunnel tersebut. Selanjutnya proses koneksi ke jaringan dapat dilakukan.