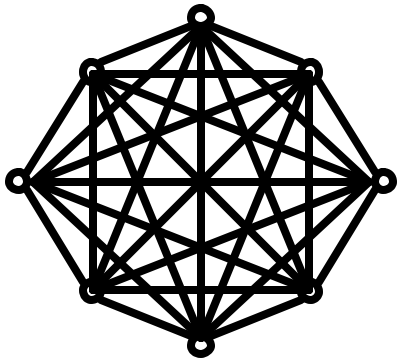
BAB IV
ASPEK-ASPEK STANDAR *IEEE 802.11b*

4.1. Arsitektur Jaringan Komputer *802.11b*

Karena karakteristik dari medium udara yang digunakan, pada dasarnya jaringan komputer nirkabel *802.11b* hanya dapat memiliki dua bentuk topologi jaringan, yaitu *ad-hoc* and *infrastructure*.

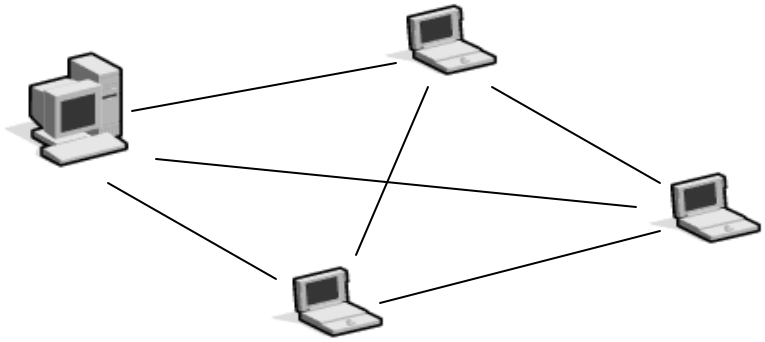
4.1.1. Topologi *Ad-Hoc* [11]

Pada jaringan *Ad-Hoc* seluruh terminal komputer terhubung secara langsung ke jaringan, sehingga setiap komputer dapat berkomunikasi secara langsung satu sama lain tanpa harus melalui sentral (dalam hal ini *Access Point*). Topologi jaringan seperti ini dapat disetarakan dengan topologi jaringan *mesh* pada *ethernet*.



Gambar 4.1. Topologi *mesh*

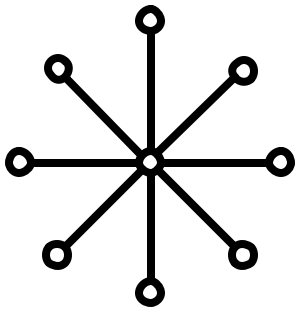
Topologi jaringan nirkabel dimana didalamnya tidak terdapat *access point* juga disebut dengan *Peer-to-Peer mode* atau *Independent Basic Service Set (IBSS).*



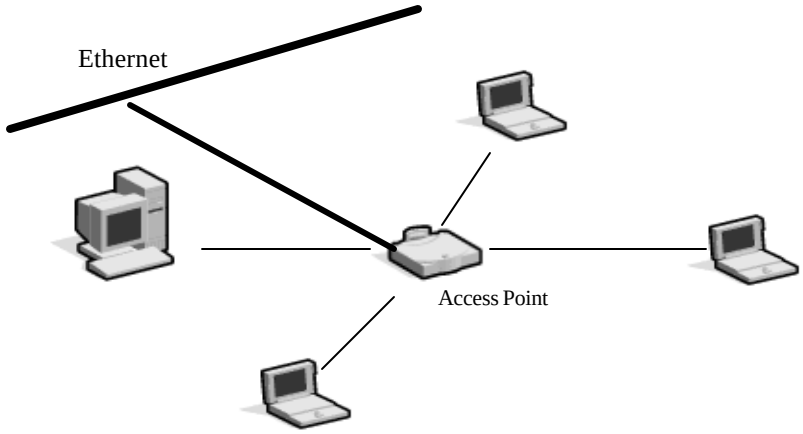
Gambar 4.2. *Independent Basic Service Set*

4.1.2. Topologi *Infrastructure* [11]

Pada jaringan Infrastuktur digunakan *Access Point* yang terhubung pada jaringan tetap/*fixed network* dan berfungsi sebagai sentral yang mengatur semua komunikasi antar terminal-terminal komputer nirkabel. *Access Point* dalam hal ini memiliki banyak fungsi, selain sebagai sentral jaringan nirkabel juga dapat berfungsi sebagai jembatan penghubung dengan jaringan *ethernet* biasa, sebagai *gateway* dengan jaringan internet (biasanya dilengkapi dengan *modem*), ataupun sebagai penghubung darat untuk memperluas jangkauan jaringan komputer nirkabel. Topologi jaringan seperti ini dapat disetarakan dengan topologi jaringan *star* pada *ethernet*.



Gambar 4.3. Topologi *star*



Gambar 4.4. *Basic Service Set*

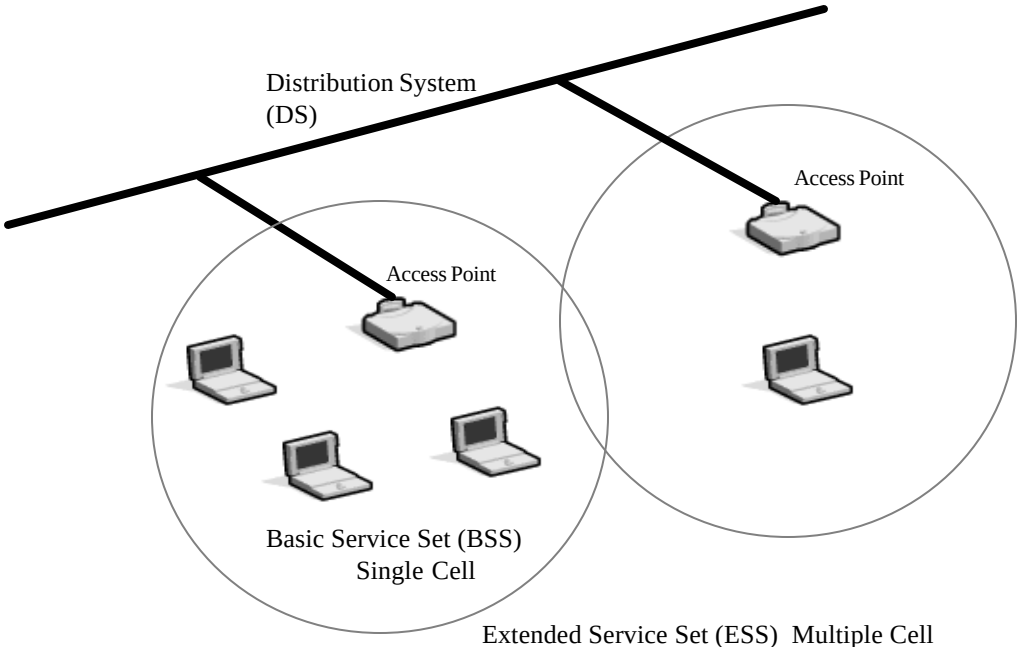
4.2. Pengembangan Arsitektur Jaringan Nirkabel [12]

Arsitektur jaringan komputer *802.11b* yang lebih kompleks dan luas sebenarnya berbasiskan pada arsitektur selular dimana suatu sistem besar dibagi-bagi menjadi sel-sel dimana setiap sel dikontrol oleh sebuah *access point*.

Suatu sel yang memiliki beberapa terminal *client* dengan sebuah *access point* sebagai pusatnya disebut dengan *Basic Service Set (BSS).*

Setiap *access point* dari setiap sel dapat dihubungkan dengan tulang punggung jaringan/*backbone*, ini disebut dengan *Distribution System (DS),* yang biasanya berupa *ethernet* biasa, ataupun dapat berupa sambungan lainnya (*fiber optic, laser, microwave).*

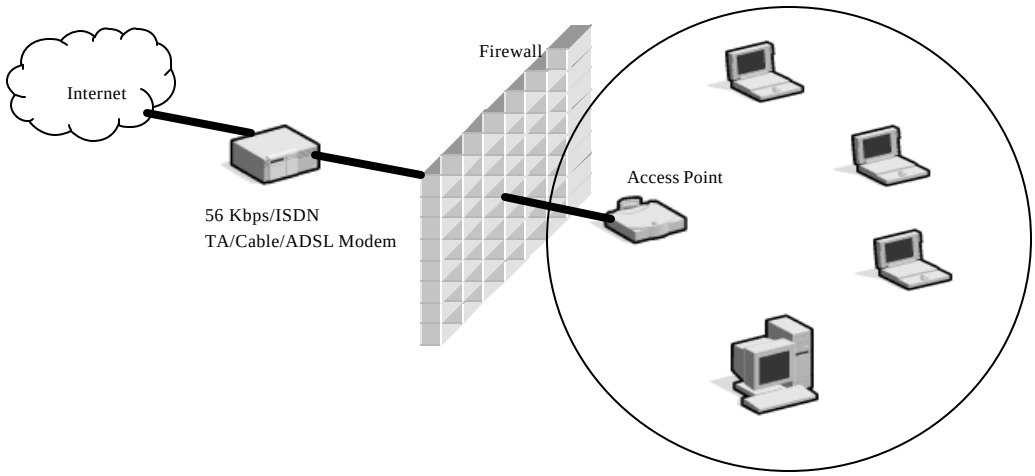
Secara keseluruhan, jaringan komputer nirkabel dengan beberapa sel yang masing-masing sel terhubung oleh *Distribution System* disebut dengan *Extended Service Set (ESS).*



Gambar 4.5. *Extended Service Set*

Selain *ESS* diatas, standar *802.11b* juga mendefinisikan apa yang disebut dengan konsep portal, Portal adalah suatu alat yang menghubungkan jaringan *802.11* dengan jaringan jenis lainnya, sering juga disebut dengan jembatan*/"translation bridge".*

Sebagai contoh dari konsep portal ialah penggunaan jaringan ini pada perumahan, dimana *access point* terhubung pada internet melalui *modem (56Kbps/ISDN/Cable/ADSL)*, sehingga selain sebagai sentral, *access point* juga berfungsi sebagai *gateway* internet, *Network Address Translation (NAT),* dan sering pula disertakan fungsi-fungsi *firewall* dan bahkan *router* pada *access point*.



Gambar 4.6. Portal

4.3. *Hand Over*, *Roaming*, dan *Channel Reuse* [11]

Pada jaringan komputer nirkabel yang kompleks dan luas sehingga harus terdiri atas beberapa sel yang saling tumpang tindih dapat mengakibatkan terjadinya keadaan dimana suatu terminal komputer berpindah dari satu sel ke sel yang lainnya, ini yang kemudian membutuhkan fungsi *hand over* dan *roaming* seperti yang terjadi pada jaringan telepon seluler.

Standar *802.11b* mendefinisikan bagaimana terminal berhubungan dengan *access point*, namun tidak mendefinisikan bagaimana *access point* melacak terminal saat berpindah sel, baik antar *access point* pada subnet jaringan yang sama atau saat terminal berpindah melewati batas *router* antar subnet jaringan yang barlainan.

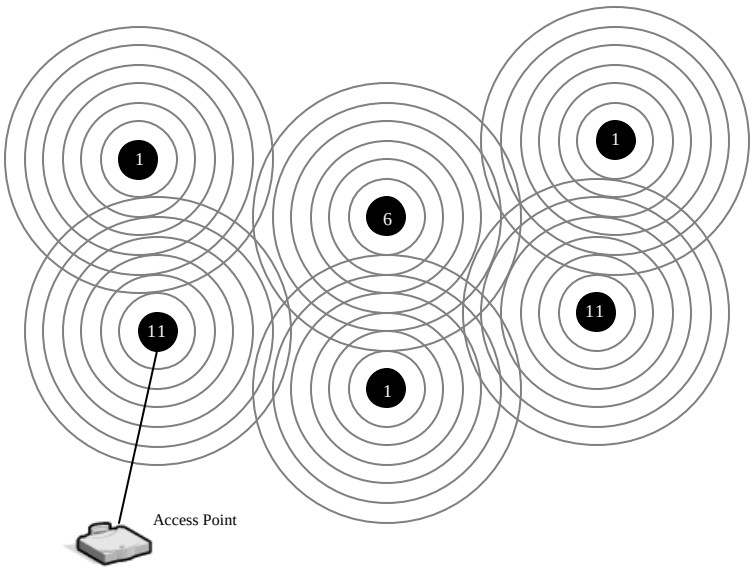
Masalah pertama, yaitu *roaming* antar *access point* dalam subnet yang sama untuk saat ini diatasi dengan jalan protokol inter *access point* dari masing-masing *vendor*, ini mengakibatkan performa yang bervariasi pada setiap merk produk *Wireless LAN*, dan jika protokol tersebut tidak efisien dapat terjadi hilangnya paket saat terminal melakukan *roaming* antar *access point*.

Karena itu *WECA* dan *IEEE* membentuk grup kerja *IEEE 802.11*f untuk mengatasi masalah interoperabilitas *access point* antar *vendor*, sebab meskipun banyak *hardware* dari *vendor* yang berlainan telah dapat berkomunikasi dengan standar *802.11b* namun ternyata masih terjadi kesulitan proses *roaming* dan *hand over* antar *access point* yang berlainan merk. Pengaturan fungsi *hand over* dan *roaming* antar *access point* ini dilakukan pada *layer* 2 dari *ISO OSI*, yaitu *layer data link*.

Sedangkan untuk masalah *roaming* yang telah melampaui batas *router* antar subnet jaringan diatasi dengan teknik *mobile IP* yang dibahas pada sub bab selanjutnya (4.4).

Fungsi *roaming* juga dapat digunakan untuk mendukung fungsi *"load balancing"* dari jaringan, yaitu untuk mendistribusikan kapasitas dari jaringan seefisien mungkin. Sehingga bila terdapat satu sel yang terlalu penuh dengan *client access point* dapat meminta *access point* di sel yang bersebelahan untuk ikut menangani beberapa *client* dengan fungsi *roaming*.

Untuk dapat membuat jaringan komputer nirkabel yang mencakup daerah yang luas, perlu digunakan teknik pengaturan sel pada jaringan *Base Transceiver Station (BTS)* telepon selular yaitu *"channel reuse"* seperti pada Gambar 4.7., teknik dimana *access point* yang saling berdampingan atau *overlapping* tidak boleh menggunakan frekuensi kanal yang sama karena akan menyebabkan terjadinya interferensi dan mengurangi *bandwidth* dari daerah *overlap*. Sedangkan pada daerah lainnya yang tidak berdampingan frekuensi kanal tersebut dapat digunakan lagi.



Gambar 4.7. *Channel Reuse*

4.4. Mobile Internet Protocol Address

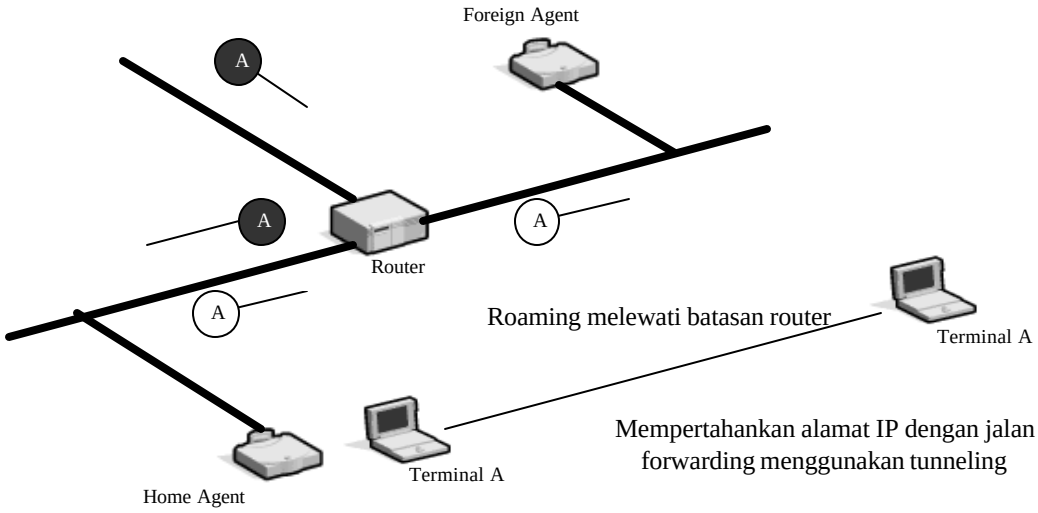
Masalah *roaming* terminal yang melampaui batas *router* antar subnet jaringan diatasi dengan penggunaan mekanisme *roaming* pada *network layer (layer 3) ISO OSI,* mekanisme ini disebut dengan *"mobile IP",* yang juga dikenal dengan *"RFC 2002"* di *Internet Engineering Task Force (IETF).*

Mobile IP bekerja dengan jalan menjadikan *access point* sebagai *"home agent"* bagi setiap terminal di selnya, begitu terminal meninggalkan *"home area"* dan memasuki area baru/*"foreign area", access point* di area baru/*"foreign agent"* meminta keterangan terminal tentang *home agent*-nya, setelah diketahui barulah mekanisme *"packet forwarding"* digunakan secara otomatis antara dua *access point* untuk menjamin bahwa alamat *IP* terminal bergerak dipertahankan dan terminal tetap dapat menerima/mengirim data.

Alamat *IP* bergerak bertujuan untuk mempertahankan jaringan komputer nirkabel. *Mobile IP address* difokuskan pada *layer network* dan dapat berkerja sama dengan teknologi *IP* yang ada saat ini *(IP version 4).* Pada protokol ini alamat *IP*

terminal yang bergerak tidak berubah saat terminal berpindah dari satu sel ke sel yang lainnya.

Saat sebuah terminal bergerak meninggalkan sel A dan masuk ke sel B, terminal tersebut memberitahu sel A kemana harus meneruskan data-data yang ditujukan untuknya, dan kemudian terminal mendaftarkan dirinya sebagai anggota dari sel B. Sehingga setiap data untuk terminal bergerak diteruskan oleh sel A ke sel B dimana terminal bergerak berada. Saat terminal bergerak kembali ke sel awalnya/sel A, terminal memberitahu sel A dan Sel B bahwa konfigurasi jaringan telah berubah lagi. Teknik *packet forwarding* ini sering disebut juga dengan *"tunneling"* yang diperlihatkan pada Gambar 4.8. dibawah*.* Alamat *access point* terakhir/Sel B, dimana paket data di-*forward* disebut dengan *Care of Address (COA).*



Gambar 4.8. *Packet forwarding*

Teknik alamat *IP* ini masih memiliki beberapa kekurangan. Tergantung pada seberapa jauh terminal berpindah, diperlukan beberapa kali penyimpanan dan penerusan paket bila terminal tidak berada pada jangkauan sel sama sekali, sebagai akibatnya mobile *IP* hanya berkerja pada *IPv4* dan tidak dapat menggunakan keuntungan dari *IPv6* yang lebih baru.

Karena teknik mobile *IP* ini belum distandarkan maka *vendor-vendor* masih menyediakan protokol mereka sendiri dengan teknik yang hampir sama untuk mempertahankan alamat *IP* agar selalu mengikuti pengguna yang melewati jaringan yang dipisahkan oleh *router*.

Alternatif lainnya selain penggunaan *mobile IP* untuk mengatasi masalah *roaming* di *layer* 3 adalah dengan mengimplementasikan *Dynamic Host Configuration Protocol (DHCP)* pada jaringan. *DHCP* membuat pengguna yang mematikan atau men-*suspend laptop* miliknya secara otomatis memperoleh alamat IP baru saat meneruskan ataupun menyalakan *laptop* di sel jaringan yang baru.

4.5. Pengaruh Paparan Energi Gelombang Elektromagnetik (GEM) pada Kesehatan [5]

Sama seperti teknologi nirkabel lainnya, *Wireless LAN* harus memenuhi standar kesehatan yang ketat dari pemerintah dan industri, telah banyak sorotan publik diberikan kepada beberapa teknologi nirkabel tentang resiko penggunaannya terhadap kesehatan.

Hingga saat penulisan tugas akhir ini penelitian ilmiah belum mampu menemukan hubungan yang merugikan antara kesehatan dengan transmisi gelombang *Wireless LAN*, begitu pula bukti yang mengatakan bahwa tidak ada hubungan antara kesehatan dan paparan GEM. Namun itu bukan merupakan alasan untuk tidak melakukan tindakan pencegahan terhadap kemungkinan gangguan kesehatan yang dapat terjadi.

Tindakan pencegahan yang dilakukan adalah dengan membatasi radiasi tenaga keluaran dari peralatan *Wireless LAN* sesuai dengan peraturan *FCC*, yaitu dibawah 100 mW, jauh lebih kecil daripada radiasi yang ada di telepon selular, dan diharapkan bahwa resiko kesehatan yang terjadi diminimalisir

dengan memperkecil tenaga dan memperbesar jarak dengan transmitternya.

4.6. Keamanan Jaringan Komputer *IEEE 802.11* [17]

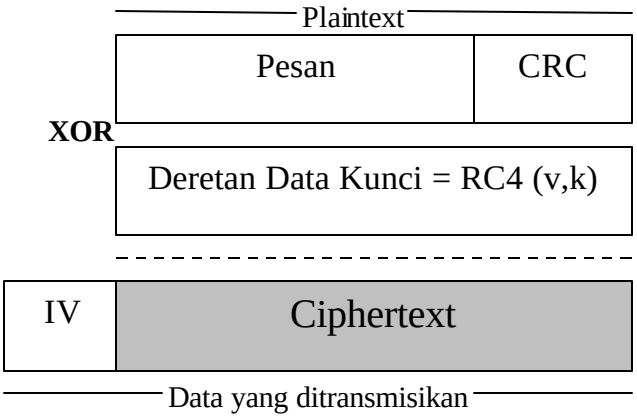
Karakteristik medium yang hanyalah berupa udara bebas membuat teknologi jaringan nirkabel ini membutuhkan teknik pengamanan yang lebih tinggi untuk mencegah akses jaringan bagi yang tidak berhak dan mengamankan data yang ditransmisikan dari penyadapan, karena itu digunakan teknik algoritma enkripsi data dan otentikasi terminal yang disebut dengan *Wired Equivalent Privacy (WEP).*

WEP menggunakan kunci rahasia yang hanya dimiliki oleh *access point* dan *NIC* terminal bergerak jaringan untuk mengenkripsi data sebelum ditransmisikan disertai dengan pengecekan integritas data untuk memastikan bahwa data tidak dimodifikasi selama transmisi. Dalam prakteknya ini dilakukan pada saat perancangan/pembuatan suatu jaringan, setiap *access point* dan *adapter NIC Wireless LAN* telah diset oleh administrator jaringan dengan menggunakan kunci rahasia yang sama.

WEP menggunakan algoritma enkripsi *RC4* yang dikenal dengan *"stream cipher"*, teknik ini dilakukan dengan jalan mengembangkan suatu kunci kecil menjadi aliran data kunci *pseudo random* yang tak terhingga/*Pseudo Random Generation Algorithm (PRGA)*, detil algoritma *RC4* [19] sendiri tertutup dan tidak untuk umum. Pengirim meng-*XOR*-kan aliran/deretan data kunci dengan *"plaintext"* data untuk menghasilkan *"ciphertext",* sedangkan penerima yang juga memiliki kunci yang sama menggunakannya untuk membangkitkan deretan data kunci yang sama di pengirim untuk kemudian di-*XOR*-kan dengan data *ciphertext* yang diterima dan diperoleh data aslinya.

Untuk meningkatkan keamanan dan menghindari adanya dua atau lebih *ciphertext* dienkripsi menggunakan deretan kunci yang sama digunakan *Initialization Vector (IV), IV* digunakan untuk memperluas kemungkinan variasi penggunaan kunci rahasia dan menghasilkan algoritma *RC4* yang berbeda untuk setiap paket data, teknik ini disebut juga dengan *Key Scheduling Algorithm (KSA)*, *IV* sendiri juga disertakan didalam paket data.

Sedangkan untuk meyakinkan bahwa paket data tidak dimodifikasi selama transmisi, *WEP* menggunakan *Integrity Check (IC)* yang disebut *CRC 16 checksum*, *CRC* dari paket data dihitung sebelum dienkripsi dan disertakan dalam bagian yang terenkripsi.



Gambar 4.9. Paket data yang dienkripsi menggunakan *WEP*

Gambar 4.9. menunjukkan diagram enkripsi paket data, sedangkan langkah-langkah enkripsi dan pengiriman data dituliskan secara matematis sebagai berikut:

Diketahui: k : Kunci rahasia
M : Pesan atau data
P : *Plaintext*
v : *Initialization Vector (IV)*
c(x) : Fungsi *checksum* x
C : *Chippertext*

1. *Checksum*

   Menghitung *checksum* dari pesan atau data untuk diperoleh *plaintext*

   P = (M, c(M))

2. Enkripsi

   Dihasilkan *keystream* dari kunci rahasia dengan algoritma *RC4*, kemudian di *XOR*-kan dengan *plaintext* yang kemudian diperoleh *ciphertext*.

   C = P *XOR RC4*(v,k)

3. Transmisi

   Secara matematik transmisi datanya:

   A ? B : v,(P *XOR RC4*(v,k))

Sedangkan langkah-langkah dekripsi *WEP* dan penerimaan data terenkripsi dapat dituliskan secara matematis sebagai berikut:

1. Dekripsi

   Penerima membangkitkan deretan kunci rahasia dan meng-*XOR*-kan-nya dengan *ciphertext* untuk memperoleh *plaintext*.

   P’ = C *XOR RC4*(v,k)
   = (P *XOR RC4*(v,k)) *XOR RC4*(v,k)
   = P

2. Pengecekan

   Penerima mencocokkan *checksum* **P’** dengan jalan membaginya menjadi bentuk **(M’,c’)**, menghitung ulang *checksum* **c(M’)**, dan mencocokkannya dengan **c’**.

   P’ = (M’,c’(M’))

Bila *checksum* **c(M’)** sama dengan *checksum* yang disertakan **c’**, maka proses enkripsi dan dekripsi dikatakan telah berhasil.

4.6.1. Kelemahan *WEP* [18]

Teknik keamanan *WEP* yang dijelaskan diatas memiliki beberapa kelemahan mendasar, yaitu:

1. *RC4* dan *CRC 16* bersifat *linear*, yang dirumuskan:

   c(x *XOR* y) = c(x) *XOR* c(y)

   yang artinya dimungkinkan untuk memperhitungkan perbedaan dua *CRC* berdasarkan pada perbedaan bit tempat mereka diambil, atau dengan kata lain membalik sebuah bit pada data dapat diketahui bit-bit mana pada *checksum* yang juga harus dibalik untuk memperoleh paket data yang dianggap sah/belum dimodifikasi.

   Karena membalik bit berpengaruh juga pada dekripsi *RC4*, penyerang bisa membalik bit manapun dari data dan menyesuaikan *checksum*-nya sehingga data tetap terlihat valid/belum dimodifikasi, ini dijelaskan secara matematis dibawah ini:

   Pengiriman paket data, **A ? (B) : (v,C)**

   Diasumsikan **C** berisi data **M** yang tidak diketahui isinya,

   C = *RC4*(v,k) *XOR* (M, c(M))

   Dimungkinkan membuat *ciphertext* **C’** baru yang berisi **M’**, dimana **M’ = M *XOR* ?** , dan **?** merupakan modifikasi yang dapat dipilih sesukanya oleh penyerang, sehingga paket data dimodifikasi menjadi **(A) ? B : (v,C’)** yang saat dekripsi, penerima **B** akan menerima pesan **M’** dengan *checksum* yang benar.

   Untuk memperoleh **C’** dari **C** yang asli agar **C’** mendekripsi ke **M’**, bukan ke **M** digunakan cara meng-*XOR*-kan **(?,c(?))** dengan **C = *RC4*(v,k) *XOR* (M, c(M))** , sehingga diperoleh **C’**.

C’ = C *XOR* (?,c(?))
= *RC4*(v,k) *XOR* (M,c(M)) *XOR* (?,c(?))
= *RC4*(v,k) *XOR* (M *XOR* ?, c(M) *XOR* c(?))
= *RC4*(v,k) *XOR* (M’,c(M *XOR* ?))
= *RC4*(v,k) *XOR* (M’,c(M’))

Pada penurunan diatas terlihat bahwa *checksum* dan *RC4* dari *WEP* adalah *linear*, **c(M) *XOR* c(?) = c(M *XOR* ?),** akibatnya **C** dapat dimodifikasi menjadi **C’** yang akan didekripsi menjadi **P *XOR* ?**.

Teknik modifikasi ini dapat dilakukan tanpa harus mengetahui isi dari data **M**, yang diperlukan hanya *ciphertext* **C** yang asli dan data modifikasi **?.** Sebagai contoh, untuk membalik bit pertama dari pesan penyerang dapat menggunakan **?** yang berisi : **10000…0**.

2. Sifat alami dari fungsi *XOR* yang apabila dijalankan pada dua buah data terenkripsi dengan *keystream* yang sama akan diperoleh informasi dari kedua data tersebut, dirumuskan:
   Jika **C1 = P1 *XOR* *RC4*(v,k)** dan **C2 = P2 *XOR* *RC4*(v,k)**
   maka
   C1 *XOR* C2 = (P1 *XOR* *RC4*(v,k)) *XOR* (C2 = P2 *XOR* C4(v,k))
   = P1 *XOR* P2
   Dengan kata lain, meng-*XOR*-kan kedua *ciphertext* (**C1** dan **C2**) bersama-sama membuat kegunaan dari enkripsi *RC4* sia-sia, baik menggunakan enkripsi sepanjang 64, 128, atau bahkan 256 bit pun tetap hasilnya adalah *XOR* dari kedua *plaintext* tersebut.
3. *Initialization Vector* yang digunakan di *WEP* sepanjang 24 bit yang dikirim tanpa dienkripsi pada paket data. *IV* yang sedemikian pendek menjamin terjadinya penggunaan ulang deretan data kunci yang sama. Sebuah *access point* yang sibuk, katakanlah mengirimkan 1500 *bytes* paket pada kecepatan 11 Mbps akan kekurangan variasi *IV* setelah:

$$1500 * 8 / (11 * 10^6) * 2^{24} = \sim 18000 \text{ detik}$$

atau lima jam, lamanya waktu yang dibutuhkan bahkan bisa lebih pendek karena banyak paket yang lebih kecil dari 1500 *bytes*. Ini membuat penyerang bisa mengumpulkan dua *ciphertext* yang dienkripsi menggunakan dua deretan data kunci yang sama dan melakukan analisa statistik untuk memperoleh *plaintext* data asli.

Kelemahan ini semakin parah karena standar *802.11b* hanya menspesifikasikan penggunaan acak *IV* untuk setiap paket hanyalah fitur tambahan.

4.6.2. Jenis-jenis Serangan Terhadap *WEP*

Kelemahan-kelemahan *WEP* yang dijelaskan diatas dapat menyebabkan jaringan nirkabel diakses ataupun diserang oleh orang yang tidak berhak.

Digolongkan menurut tekniknya, jaringan *Wireless LAN* dapat diakses/diserang menggunakan empat cara:

a. Serangan pasif untuk mendekripsi lalu lintas data menggunakan analisa statistik.
b. Serangan aktif untuk menginjeksikan lalu lintas data tambahan dari terminal ilegal menggunakan *plaintext* yang telah diketahui.
c. Serangan aktif untuk mendekripsi lalu lintas data dengan jalan menipu *access point*.
d. Serangan dengan jalan mengumpulkan sebanyak mungkin analisa lalu lintas data selama beberapa waktu/hari untuk mendekripsikan lalu lintas data secara *realtime*.

Serangan-serangan diatas dapat dilakukan dengan menggunakan *adapter NIC Wireless LAN* biasa dengan bantuan tambahan *software* dan dapat dilakukan baik pada *WEP* dengan enkripsi berapapun, ini yang menjadi kekhawatiran terbesar

karena serangan bisa dilakukan dengan mudah tanpa melakukan banyak modifikasi dan biaya sehingga sangat dianjurkan bahwa pada pengguna *Wireless LAN* menambahkan sistem keamanan dari pihak ketiga yang akan dibahas di sub bab selanjutnya.

4.6.2.1. Serangan Pasif untuk Mendekripsi Lalu Lintas Data

Serangan ini didasarkan pada kelemahan point 2 yang dijelaskan diatas, seorang penyerang pasif ikut mendengarkan lalu lintas data hingga terjadi pengulangan penggunaan *IV* (seringkali disebut dengan "tabrakan *IV*"), setelah diperoleh dua paket data yang menggunakan *IV* yang sama dapat diketahui hasil *XOR* dari keduanya yang kemudian digunakan untuk menduga isinya.

Lalu lintas protokol internet, dalam hal ini bisa berupa *beacon frame, control frame,* ataupun paket lainnya yang hanya digunakan oleh jaringan sering sekali mudah untuk diduga dan lebih menonjol sehingga paket dapat diabaikan bila isinya bukan data, dengan semakin banyak latihan akan lebih mudah menebak isi paket data sebenarnya melalui analisa statistik untuk memperkecil kemungkinan yang ada, bahkan pada beberapa kasus isi paket dapat ditebak dengan tepat.

Jika dengan teknik analisa statistik yang hanya menggunakan dua paket saja seperti diatas kurang meyakinkan, penyerang dapat menunggu dan mendengarkan apabila terjadi pengulangan *IV* lagi, dan bila itu terjadi keberhasilan analisa statistik akan meningkat dengan cepat. Setelah dimungkinkan untuk mendekripsi seluruh *plaintext* dari satu data, *plaintext* dari data yang lainnya dengan *IV* yang sama dapat langsung diketahui, karena semua pasangan variasi *XOR* telah diketahui.

Pengembangan dari teknik serangan ini bisa dilakukan dengan menggunakan sebuah terminal yang berada di internet untuk mengirimkan data ke dalam terminal bergerak target yang

isinya telah diketahui oleh penyerang. Saat penyerang memindai data terenkripsi yang dikirimkannya pada lalu lintas jaringan nirkabel, penyerang akan dapat mendekripsi semua paket yang menggunakan *IV* yang sama.

4.6.2.2. Serangan Aktif untuk Menginjeksikan Lalu Lintas Data Tambahan

Jika penyerang mengetahui *plaintext* yang tepat untuk sebuah pesan yang terenkripsi, penyerang dapat menggunakannya untuk menghasilkan paket terenkripsi baru yang isinya telah diubah sehingga terlihat sebagai paket yang sah, ini dilakukan dengan pembalikan bit *plaintext* pada paket data, membuat data baru, menghitung *CRC 16*, yang dirumuskan:

Untuk mengetahui *keystream*, **P *XOR* C = P *XOR* (P *XOR* *RC4*(v,k))**

= *RC4*(v,k)

Kemudian dibuat pesan **M'** baru **A ? B : (v,C')**,

dimana: **C' = (M',c(M')) *XOR* *RC4*(v,k)**

Bila dituliskan secara matematis, garis besar penggantian datanya: ***RC4*(X) *xor* X *xor* Y = *RC4*(Y)**

Dimana **X** adalah data asli, dan **Y** adalah data yang baru.

Paket yang baru tersebut jika dikirimkan ke *access point* atau terminal bergerak akan diterima sebagai paket yang sah.

Bila serangan ini dilakukan untuk mengubah perintah yang dikirimkan pada *shell* melalui *telnet* ataupun interaksi dengan *file server* akan dapat mengakibatkan kerusakan/kesalahan serius.

4.6.2.3. Serangan dengan Jalan Menipu *Access Point*

Serangan-serangan diatas dapat ditingkatkan menjadi mendekripsi lalu lintas data sewenang-wenang, dalam hal ini penyerang tidak menerka isi data dari paket, namun menerka *header* dari paket. Informasi ini biasanya lebih mudah untuk

diterka dan diperoleh, umumnya yang dibutuhkan hanya alamat *IP* tujuan. Dengan pengetahuan ini penyerang membalik bit-bit tertentu paket data untuk mengubah alamat *IP* tujuan (menggunakan kelemahan point 1) menjadi alamat *IP* terminal di internet yang telah dipersiapkan dan mentransmisikannya dengan menggunakan terminal bergerak yang ilegal.

Kebanyakan instalasi jaringan nirkabel memiliki akses internet, dan paket termodifikasi itu akan didekripsi di *access point* dan diteruskan tanpa dienkripsi ke terminal penyerang melalui *gateway* dan *router*, sehingga penyerang memperoleh *plaintext* yang data. Bahkan jika penyerang dapat menebak isi dari *header TCP* dari paket, dimungkinkan untuk mengubah *port* tujuan paket menjadi *port* 80 yang boleh digunakan/diteruskan pada kebanyakan *firewall*.

4.6.2.4. Serangan dengan Membangun Tabel Database Dekripsi

Ukuran *field IV* yang kecil sehingga pengembangan variasinya terbatas seperti yang dijelaskan di kelemahan point 3 diatas membuat penyerang dapat membangun tabel database dekripsi. Setelah penyerang memperoleh *plaintext* dari beberapa paket, penyerang dapat memperhitungkan aliran/deretan data kunci *RC4* yang dihasilkan dan digunakan oleh *IV*. Deretan data kunci ini dapat digunakan untuk mendekripsi paket lainnya yang menggunakan *IV* yang sama. Sejalan dengan waktu dan dengan menggunakan teknik diatas, penyerang dapat membangun tabel database tentang semua variasi *IV* yang ada dan semua deretan data kunci yang berhubungan dengannya. Tabel database ini hanya membutuhkan tempat yang relatif kecil di media penyimpan (~15 Gb), dan begitu tabel database selesai dibangun penyerang dapat mendekripsi secara *realtime* semua paket yang dikirimkan melalui jaringan *Wireless LAN*.

4.6.3. Teknik Memindai Jaringan Nirkabel

Disamping sulitnya mendekoder sinyal digital 2.4 GHz, perangkat keras yang digunakan untuk memonitor/memindai transmisi *802.11b* telah tersedia dengan luas bagi penyerang dalam bentuk produk *adapter 802.11b* itu sendiri. Produk-produk ini memiliki semua kemampuan memonitor yang dibutuhkan, dan yang tinggal dibutuhkan oleh penyerang adalah meyakinkan *hardware* untuk dapat bekerja sama.

Semua peralatan *802.11b* didesain untuk mengabaikan isi dari paket terenkripsi yang kuncinya tidak diketahui, namun dengan memodifikasi konfigurasi *driver* dan *firmware* dapat membuat peralatan *802.11b* menerima semua transmisi data *ciphertext WEP* untuk kemudian dianalisa. Pada umumnya modifikasi ini dilakukan di *platform* yang terbuka seperti *Linux* yang diketahui *source code*-nya.

Serangan aktif, yang juga memerlukan transmisi, tidak hanya mendengarkan, lebih sulit dilakukan namun bukan tidak mungkin. Banyak sekali produk *802.11b* yang *firmware*-nya dapat diprogram ulang sehingga dengan modifikasi dan *reverse engineered* dapat diperoleh kemampuan untuk menginjeksi lalu lintas data. Dengan metode seperti ini akan sangat memakan waktu, namun perlu diingat bahwa ini hanyalah biaya untuk sekali waktu saja, begitu ada yang dapat melakukannya dan kemudian mendistribusikan secara gelap *firmware* yang telah dimodifikasi atau bahkan menjualnya untuk kepentingan ilegal akan menjadi bisnis yang menguntungkan dan investasi waktu yang hilang tergantikan.

Ini yang merupakan kelemahan terbesar dari teknologi baru ini, dimana serangan bisa dilakukan tanpa menggunakan peralatan khusus, karena itu jaringan nirkabel *802.11b* bisa dikatakan tidak aman.

4.6.4. Antisipasi yang Dapat Dilakukan Terhadap Kelemahan Keamanan *Wireless LAN*

Terdapat beberapa antisipasi yang dapat dilakukan untuk mencegah terjadinya serangan, atau paling tidak mengurangi resiko jaringan *Wireless LAN* disadap:

a. Selalu asumsikan bahwa *layer data link* dari standar *802.11b* tidak aman.
b. Jangan mempercayakan keamanan hanya pada *WEP*, tapi gunakan mekanisme keamanan yang memiliki level lebih tinggi seperti *Internet Protocol Security (IPSec)* dan *Secure Shell (SSH).*
c. Perlakukan semua terminal komputer pada jaringan nirkabel *802.11b* sebagai sistem luar/eksternal, dan letakkan semua *access point* diluar *firewall*.
d. Asumsikan semua terminal yang ada dalam jangkauan jaringan *802.11b* adalah pengakses jaringan, dan perlu selalu diingat bahwa penyerang dapat menggunakan antena tambahan untuk meningkatkan jarak jangkauan *adapter Network Interface Card (NIC) Wireless LAN*.

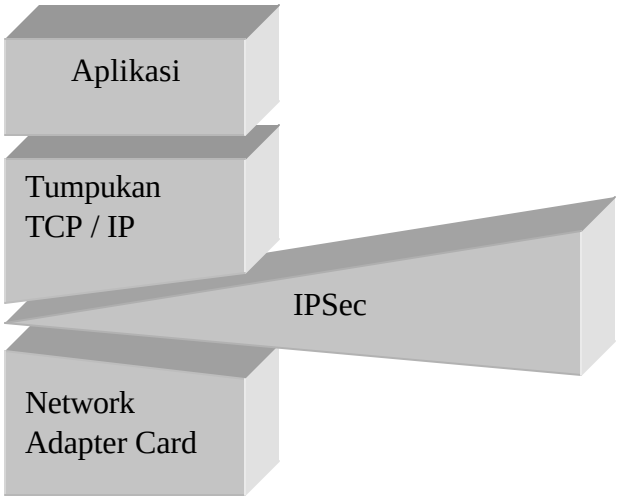
Dengan adanya kelemahan pada sistem keamanan WEP dari *802.11b* ini menunjukkan bahwa sangat sukar untuk membuat sistem keamanan yang ideal, selalu terdapat kekurangan pada setiap tingkat, termasuk juga desain protokol, implementasi, dan dalam penggunaannya yang dapat membuat sistem secara keseluruhan menjadi rentan terhadap serangan. Saat sebuah sistem yang rentan menjadi popular untuk menjadi target serangan, biasanya tidak lama kemudian sistem tersebut akan kalah bersaing.

Grup kerja *IEEE 802.11* sendiri saat ini sedang dalam proses merevisi sistem keamanan *Wireless LAN* yang disebut dengan kelompok kerja *802.11*i.

4.7. *Internet Protocol Security (IPSec), Secure Shell (SSH),* dan *Virtual Private Network (VPN)* [20]

Teknologi *Internet Address (IP)* yang ada sekarang *(IPv4)* terbukti sangat efisien, efektif, dan fleksible, namun *IPv4* yang ada sekarang selain mulai tidak mencukupi juga relatif tidak aman dari berbagai macam serangan, ini yang menyebabkan banyaknya halangan dalam implementasi aplikasi yang membutuhkan tingkat keamanan tinggi seperti *electronic commerce/E-commerce.* Untuk mengatasinya *Internet Engineering Task Force (IETF)* mengembangkan *IPSec* yang merupakan versi *IP* yang lebih aman.

Pemecahan *IPSec* untuk masalah kerahasiaan, integritas, dan otentikasi di internet adalah dengan mengenkripsi setiap paket data komunikasi dan otentikasi dari ujung ke ujung. Protokol *IPSec* bekerja pada level *network* (dibawah *physical layer*) sehingga tidak tergantung pada aplikasi yang digunakan. Letak posisi *IPSec* dalam tumpukan *layer* diperlihatkan pada Gambar 4.10. *IPSec* merupakan tambahan/*add-on* bagi *IPv4,* namun akan diintegrasikan dalam *IPv6* yang lebih baru.



Gambar 4.10. *IPSec* pada tumpukan *TCP/IP*

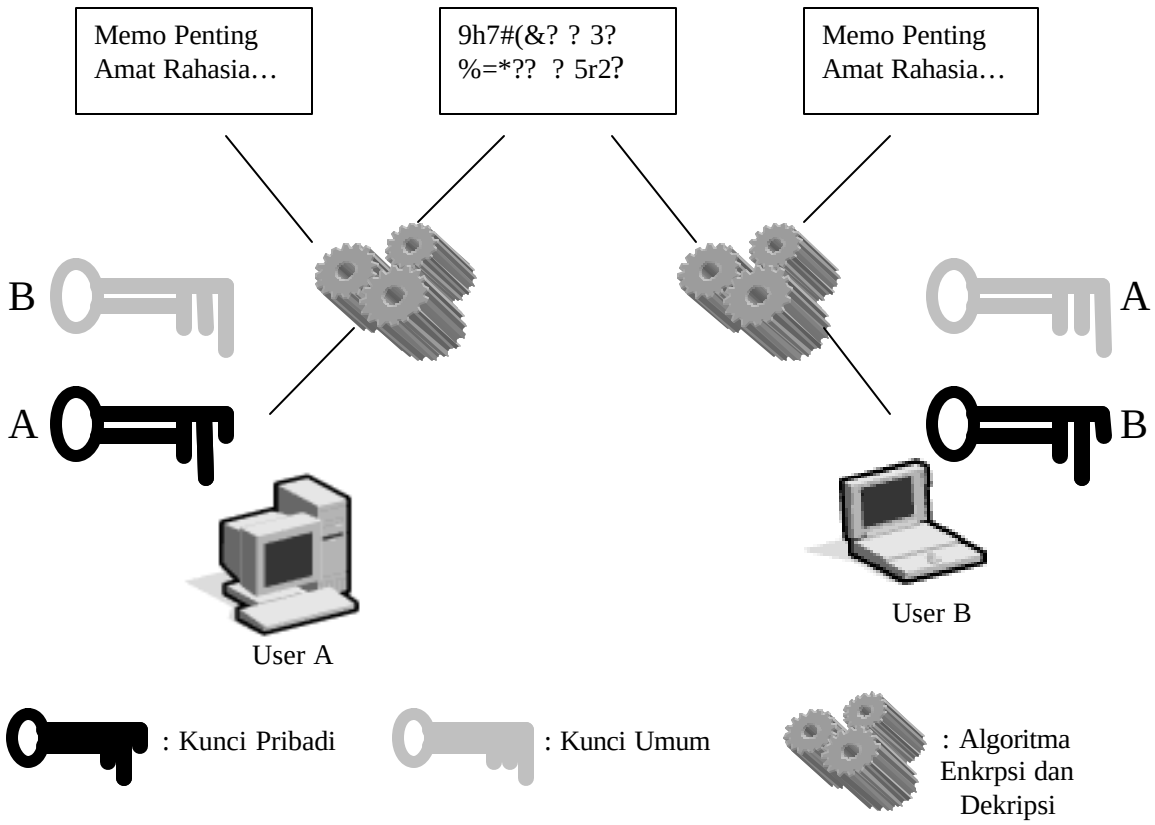
IPv6 sendiri merupakan versi pengalamatan yang lebih baru dengan memiliki panjang alamat 128 bit (*IPv4* hanya 32 bit), memiliki 3 jenis pengalamatan *(Unicast, Anycast, Multicast),* memiliki *header* dua kali lebih banyak namun lebih efisien dan efektif, dan tentunya sistem keamanan baru.

4.7.1. Otentikasi [21]

Terdapat dua macam teknik otentikasi yang disediakan oleh *IPSec*, yang paling sederhana adalah dengan kunci rahasia yang hanya diketahui oleh dua pihak yang berkomunikasi.

Cara otentikasi yang lebih canggih dilakukan dengan menggunakan sertifikat, menggunakan konsep pasangan kunci yaitu kunci pribadi *(private key)* dan kunci umum *(public key).* Seperti namanya, kunci pribadi hanya diketahui oleh setiap pengguna, sedangkan kunci umum diketahui oleh semua orang didalam jaringan. Kedua kunci tersebut secara matematis bergantung satu sama lain, tetapi tidak dapat diperoleh satu dari yang lainnya. Selain itu kedua kunci tersebut memiliki fungsi yang jelas, sehingga apa yang dienkripsi oleh salah satu kunci hanya bisa didekripsi oleh kunci yang lainnya.

Untuk otentikasi, pengirim menggunakan kunci pribadinya untuk mengenkripsi/memberi tanda tangan digital, kemudian sertifikat yang berisi kunci umum dan identitas pengirim ikut dikirimkan ke penerima. Karena pesan hanya dapat didekripsi menggunakan kunci umum pengirim dan kunci pribadi penerima tersebut, maka identitas pengguna terotentikasi. Proses otentikasi diilustrasikan pada Gambar 4.11.



Gambar 4.11. Enkripsi dan otentikasi *IPSec*

4.7.2. Enkripsi

Setelah mengotentikasi kedua belah pihak yang berkomunikasi, yang tertinggal adalah masalah untuk membuat saluran komunikasi yang aman. Kerahasiaan dan keutuhan komunikasi dicapai dengan mengenkripsi data dan memperhitungkan *checksum.* Dalam hal ini *IPSec* memiliki banyak sekali algoritma enkripsi yang dapat digunakan, antara lain *Data Encryption Standard (DES), 3 DES, CAST, Blowfish, Twofish,* dll. Untuk membahas lebih jauh akan menyimpang dari tujuan dan spesifikasi skripsi ini.

4.7.3. *Secure Shell (SSH)*

Secure shell merupakan teknologi yang berfungsi untuk mengamankan koneksi *remote access* yang melalui jaringan *IP* dengan jalan mengenkripsi semua data yang ditransmisikan, termasuk *password, file* biner, dan perintah administrasi, *SSH secure shell* didesain dan dikembangkan oleh *SSH Communications Security.* Versi kedua dari *SSH* didesain untuk sepenuhnya menjadi pengganti program-program *FTP, telnet*, dengan perintah-perintahnya seperti *rlogin, rsh, rcp,* dll.

4.7.4. *Virtual Private Network (VPN)*

Sebelumnya, jika suatu perusahaan ingin memperluas jaringan komputernya ke kantor cabang, partner kerja, atau *remote user*, perusahaan harus membuat jaringan pribadi dengan berlangganan *leased line* yang menggunakan peralatan yang mahal. Tetapi dengan lahirnya teknologi *Virtual Private Network (VPN),* kebutuhan untuk membangun jaringan tersendiri dengan *hardware* yang mahal tidak diperlukan lagi.

VPN dapat diartikan sebagai pembuatan jaringan komputer pribadi dengan menggunakan internet sebagai medium yang aksesnya dibatasi hanya untuk yang berhak dengan menggunakan enkripsi, bisa juga dikatakan dengan *VPN* dimungkinkan membuat hubungan yang aman pada internet, ini didukung juga dengan teknologi *IPSec* yang diterangkan diatas.