BAB 2

LANDASAN TEORI

2.1 Sejarah Internet

Internet pada zaman sekarang bukan sebuah media atau alat yang modern lagi. Apalagi sekarang ini pemakaian internet sudah menjamur dimana-mana. Mulai dari anak-anak Sekolah Dasar sampai pekerja kantoran sangat membutuhkan informasi yang ada di internet tersebut. Hanya membuka situs-situs yang diinginkan maka kita langsung mendapatkan informasi dengan cepat dan mudah. Informasi yang didapat bukan hanya yang terjadi didaerah lokal saja tetapi dari luar negeri pun dapat kita temukan. Hampir seluruh kehidupan manusia modern tidak bisa lepas dari internet, karena mereka tidak mau ketinggalan berita lokal maupun internasional. Apalagi teknologi yang semakin modern mendukung mereka untuk mengakses internet. Bukan itu saja bahkan dengan internet para pekerja kantoran bisa bertemu kliennya disini dengan cepat dan mudah. Maka dengan itu penulis akan membahas mengenai sejarah dan pengertian internet.

Kehadiran internet diawali dengan adanya Lembaga Riset Departemen Pertahanan Amerika Serikat (*Advanced Research Projects Agency* (ARPA) merupakan tonggak sejarah bagi perkembangan teknologi informasi dan komunikasi masa depan, dimana misi utamanya adalah menerapkan teknologi canggih di lembaga pertahanan Amerika Serikat tersebut. ARPA menjadi pusat para pemikir teknologi canggih lembaga pertahanan Amerika Serikat yang melibatkan ratusan para ilmuwan terkemuka. Saat itu, Lembaga tersebut

memfokuskan pada ruang angkasa, senjata balistik, dan monitoring tes nuklir. Bahkan berikutnya berkembang pada teknologi komunikasi melalui jaringan langsung komputer antara basis operasional dengan sub kontraktornya.

Pada tahun 1962, ARPA membuka program riset komputer yang bekerja sama dengan seorang ilmuwan MIT, John Licklider. Ia yang pertama kali mempublikasikan memorandum pada jaringan Galatic (*Galatic Networks*) yang menjelaskan bahwa di masa depan, komputer akan menjadi suatu jaringan yang dapat diakses oleh siapa saja.

Pada tahun 1965 pernah dilakukan suatu penelitian pemanfaatan jaringan telepon untuk pengiriman data melalui komputer di Berkely dan MIT dengan kecepatan *dial-up* yang rendah, selanjutnya menjadi *" Wide Area Network"* (WAN). WAN memberikan peluang jangkauan lebih luas bagi penyampaian pesan-pesan bisnis.

Pada tahun 1966/1967 telah dilakukan riset komputer dipimpin oleh Leonard roberts untuk merencanakan sistem jaringan komputer *(computer network systems)* yang disebut ARPANET. Pada akhir tahun 1969, para ilmuwan ARPANET dengan empat unit komputer mengembangkan risetnya di pusat riset Santa Barbara dan Utah untuk memperbaiki kemampuan akses lewat sistem jaringan. Pada bulan Oktober 1972, dalam suatu konferensi internasional pertama tentang komputer dan komunikasi di Washington DC, para ilmuwan ARPANET telah mendemonstrasikan sistem jaringan komputer yang menghubungkan komputer di 40 lokasi yang berbeda. Konferensi di Washington juga telah

membentuk suatu asosiasi *Internet Working Group (IWG)* untuk melakukan koordinasi riset yang telah dilakukan.

Para ilmuwan ARPANET terus melakukan pembenahan sistem jaringan yang ada sejak tahun 1972 sampai tahun 1974, yang menghasilkan suatu sistem yang mampu mengkomunikasikan jaringan yang berbeda antara komputer satu dengan komputer lainnya, yang dikenal dengan *Transmission Control Protocol (TCP/IP)*. Pengembangan TCP/IP merupakan tahapan yang paling krusial dalam pengembangan sistem jaringan komputer dewasa.

Pada tahun 1982, akhirnya internet lahir dengan mengadopsi TCP/IP yang dapat menghubungkan seperangkat jaringan ke berbagai belahan dunia. Pengembangan internet merupakan babak baru dalam era komunikasi, yang memungkinkan setiap individu melakukan komunikasi ke berbagai belahan dunia dalam waktu yang sangat singkat. Pengembangan TCP/IP merupakan tahapan yang paling kristal dalam sistem jaringan komputer (Drs.Djoko Purwanto, M.B.A, 2003: 294).

2.2 Pengertian Internet

Internet adalah jaringan komputer yang saling terhubung ke seluruh dunia tanpa mengenal batas teritorial, hukum dan budaya. Secara fisik dianalogikan sebagai jaring laba-laba (The web) yang menyelimuti bola dunia dan terdiri dari titik-titik (node) yang saling berhubungan. Didalam internet sendiri terdapat beberapa fasilitas yang dapat digunakan atau dimanfaatkan sesuai dengan kebutuhan. Dimana mereka dapat mencari informasi berita atau gosip terbaru, mengirim email ke teman atau relasi bisnis, *chatting* dengan teman atau orang tua

yang berada jauh dari tempat tinggal kita. Dengan adanya internet akan memudahkan kita untuk mendapatkan informasi bahkan biaya yang dikeluarkan tidak begitu mahal jika dibandingkan yang kita dapatkan tergolong *up to date.*

Internet dapat diakses siapapun melalui segala jenis komputer seperti *Mac*, *PC*, *Notebook*, *Palmtop*, *PDA*, Mini komputer. Semua sistem operasi *UNIX*, *BSD*, *Linux*, *Windows*, *OS2*, *SUN* atau *MacOS*. Singkatnya hampir semua jenis komputer dan sistem operasi, bahkan kini internet dapat diakses lewat telepon seluler.

2.3 Manfaat Internet

Secara umum ada banyak manfaat yang dapat diperoleh apabila seseorang akses ke internet. Berikut ini sebagian dari apa yang tersedia di internet :

1. Informasi untuk kehidupan pribadi, yaitu: kesehatan, rekreasi, *hobby*, pengembangan pribadi, rohani dan sosial.
2. Informasi untuk kehidupan professional atau pekerja, yaitu: *sains*, teknologi, perdagangan, saham, komoditas, berita bisnis, asosiasi profesi, asosiasi bisnis, berbagai forum komunikasi.

Satu hal yang paling menarik adalah keanggotan internet tidak mengenal batas negara, ras, kelas ekonomi, ideologi atau faktor-faktor lain yang biasanya dapat menghambat pertukaran pikiran. Internet adalah suatu komunitas dunia yang sifatnya sangat demokratis serta memiliki kode etik yang dihormati segenap anggotanya.

Manfaat internet terutama diperoleh melalui kerjasama antar pribadi atau kelompok tanpa mengenal batas jarak dan waktu. Untuk lebih meningkatkan

kualitas sumber daya manusia di Indonesia, sudah waktunya para profesional Indonesia memanfaatkan jaringan internet dan menjadi bagian dari masyarakat informasi dunia (http://arema.cjb.net).

2.4 Keunggulan dan Kelemahan Internet

Keunggulan yang dapat ditemui di internet antara lain: (Tjiptono, 2000 dalam Anastasia Diana, 2001: 100-106):

1. Konektivitas dan jangkauan global, dapat mengakses data dari berbagai sumber di belahan dunia.
2. Akses 24 jam, dapat melakukan aktivitas, transaksi, akses data kapan saja tidak lagi dibatasi oleh waktu.
3. Kecepatan dan karakteristik *real-time* internet lebih atraktif dibandingkan sumber data tradisional. Pencarian informasi melalui *search engines* sangat menghemat waktu, apalagi bila dibandingkan dengan pencarian melalui buku.
4. Kenyamanan, yakni bahwa peneliti lewat internet tidak harus menghadapi masalah birokratis, seperti ijin dari berbagai instansi untuk keperluan pengumpulan data, 'kerahasian' informasi dan keharusan datang sendiri ke instansi bersangkutan. Banyak situs yang menyajikan data-data secara gratis yang tinggal *download* sehingga sangat memudahkan peneliti dalam mengakses berbagai situs internet.
5. Kemudahan akses, terutama didukung dengan menjamurnya bisnis warnet di Indonesia sehingga memudahkan untuk mengakses data-data.

6. Biaya yang relatif murah jika dibandingkan dengan berlangganan setiap majalah, koran, maupun jurnal secara reguler.
7. Interaktivitas dan flexibilitas, terutama berkaitan dengan diskusi mengenai topik dan hasil riset tertentu melalui sarana *mailing list* dan *chatting*.

Sedangkan kelemahan yang terdapat pada internet adalah:

1. Faktor anonimitas menyebabkan peneliti internet sulit mengidentifikasi identitas responden, karena setiap orang (termasuk yang bukan target responden) bisa mengisi kuesioner secara *on-line* tanpa bisa dicegah atau dibatasi.
2. Bila tidak dibarengi dengan strategi yang kreatif, pencarian informasi di *interent* bisa menjadi pengalaman yang membuat frustasi.
3. Resiko penyebaran virus komputer lewat e-mail maupun *file-file* yang di *download* dari internet.
4. Realibilitas dan validitas sumber acuan atau hasil riset kadang patut dipertanyakan, karena setiap orang bebas membuka *homepage* sendiri dan menampilkan berbagai informasi di sana.
5. Infrastruktur jaringan telepon dan *Internet Service Provider* (ISP) di Indonesia masih sangat lambat, sehingga www (World Wide Web) sering diplesetkan menjadi *World Wait Web*.

2.5 Sejarah Hotspot

Pada zaman sekarang ini pemakaian internet untuk berbagai keperluan sudah menjamur dimana-mana. Di Indonesia sendiri, penggunaan internet berbasis *Wi-Fi* sudah mulai menggejala di beberapa kota besar. Di Jakarta,

misalnya, para maniak internet yang sedang berselancar sambil menunggu pesawat *take off* di ruang tunggu bandara, sudah bukan merupakan hal yang asing. Fenomena yang sama terlihat diberbagai kafe seperti kafe *Starbuck* dan *La Moda* cafe di Plaza Indonesia, *Coffe Club* Senayan, dan *Mister Bean Coffe* di Cilandak *Town Square* dimana pengunjung dapat membuka internet untuk melihat berita politik atau gosip artis terbaru sembari minum *cappuccino* panas. Tidak di Jakarta saja hotspot mewabah tetapi di Yogjakarta hotspot pun juga banyak peminatnya. Buktinya yaitu banyaknya kafe-kafe yang ada telah dilengkapi dengan fasilitas hotspot dan hampir tiap hari kafe tersebut penuh dengan pengunjung. Apalagi setiap *weekend* pengunjung akan memadati kafe yang menyediakan fasilitas lebih seperti hotspot itu sendiri.

Dengan semakin meluasnya penggunaan internet dan kebutuhan bisa mengakses internet sewaktu-waktu menjadikan hotspot sebagai sesuatu yang dicari. Orang-orang pada saat ini membutuhkan informasi dengan cepat. Hotspot sekarang ini sudah bukan hal baru lagi. Pada saat orang harus sibuk dengan aktivitasnya mereka tetap diharuskan mendapatkan informasi dengan cepat. Maka dengan itu fasilitas hotspot sangat diperlukan bagi orang yang haus akan informasi. Di Indonesia sendiri fasilitas hotspot sudah banyak tetapi masih pada area publik misalnya, kafe, mall, bandara, hotel dan universitas-universitas yang digunakan untuk menambah fasilitas kampus itu sendiri.

Wi-Fi sebenarnya merupakan merek dagang *wireless* LAN yang diperkenalkan dan distandarisasi oleh *Wi-Fi Alliance*. Standar *Wi-Fi* didasarkan pada standar 802.11. *Wi-Fi Alliance* pertama kali membentuk *Wireless Ethernet*

Compatibility Alliance (WECA), sebuah organisasi nonprofit yang mempunyai fokus pada pemasaran serta mengurusi interoperabilitas pada produk *wireless* LAN 802.11. *Wi-Fi Alliance* juga memprakarsai standar keamanan pada 802.11i yang disebut *Wi-Fi Protected Acces (WPA)*.

Awalnya hotspot atau bisa disebut juga *Wi-Fi* (*Wireless Fidelity*) ditujukan untuk penggunaan perangkat nirkabel dan Jaringan Lokal (LAN), namun saat ini lebih banyak digunakan untuk mengakses internet. Hal ini memungkinkan seseorang dengan media komputer yang dilengkapi kartu nirkabel (*wireless card*) atau *Personal Digital Asisstant* (PDA) untuk terhubung pada internet dengan menggunakan hotspot terdekat. (www.wikipedia.com).

Jaringan Lokal Nirkabel atau WLAN adalah suatu jaringan lokal nirkabel yang menggunakan gelombang radio sebagai kariernya, *link* terakhir yang digunakan adalah nirkabel, untuk memberi sebuah koneksi jaringan ke seluruh pengguna dalam area sekitar. Area dapat berjarak dari ruangan tunggal keseluruh area kampus misalnya. Tulang punggung jaringan biasanya menggunakan kabel dengan satu atau lebih titik akses jaringan menyambungkan pengguna nirkabel ke jaringan berkabel.

WLAN (*Wireless Local Area Networks*) diharapkan menjadi sebuah teknologi yang banyak di sambungkan pada area bisnis. Frost dan Sullivan mengestimasikan pasar WLAN akan menjadi 0,3 milyar dolar AS dalam tahun 1998 dan 1,6 milyar dolar di tahun 2005. Sejauh ini WLAN sudah di *install* di berbagai universitas-universitas, bandara, dan tempat-tempat umum lainnya. Di Inggris pemakaian WLAN dibatasi dikarenakan biaya yang sangat tinggi dalam

penggunaannya, terutama di tempat-tempat umum seperti ruang tunggu dibandara kelas bisnis misalnya. Komponen WLAN sangat cukup mudah digunakan dirumah tentunya yang sudah di *set-up* sedemikian rupa, maka satu PC dapat digunakan untuk disambungkan langsung ke internet pada PC yang lainnya dimana masih dalam satu lingkup. Pengembangan utama meliputi solusi spesifik industri dan *protocol proprietary*, tetapi pada akhir tahun 1990-an digantikan dengan standar versi jenis utama dari IEEE 802.11 (Wi-Fi) dan HomeRF (2 Mbit/s, disarankan untuk rumah).

Wi-Fi (hotspot) dirancang berdasarkan spesifikasi IEEE 802.11. Sekarang ini ada empat variasi dari 802.11, yaitu 802.11a, 802.11b, 802.11g, dan 802.11n. Spesifikasi b merupakan produk pertama *Wi-Fi*. Variasi g dan n merupakan salah satu produk yang memiliki penjualan terbanyak pada tahun 2005.

Tabel 2.1 Spesifikasi Wi-Fi

Spesifikasi	**Kecepatan**	**Frekuensi band**	**Cocok dengan**
802.11b	11Mb/s	2.4 GHz	b
802.11a	54 Mb/s	5 GHz	a
802.11g	54 Mb/s	2.4 GHz	b, g
802.11n	100 Mb/s	2.4 GHz	b, g, n

Sumber: www.wikipedia.com, 6 Juni 2006

Di bagian banyak dunia, frekuensi yang digunakan oleh *Wi-Fi*, pengguna tidak diperlukan untuk mendapatkan ijin dari pengatur lokal, (misal, Komisi

Komunikasi Federal di A.S.). 802.11a menggunakan frekuensi yang lebih tinggi dan oleh sebab itu daya jangkaunya sangat sempit, untuk yang lainnya sama.

Teknologi Internet berbasis *Wi-Fi* (hotspot) dibuat dan dikembangkan sekelompok insinyur Amerika Serikat yang bekerja pada *Institute of Electrical and Electronis Engineers* (IEEE) berdasarkan standar teknis perangkat bernomor 802.11b, 802.11a, dan 802.16. Perangkat *Wi-Fi* sebenarnya tidak mampu bekerja dijaringan WLAN, tetapi juga dijaringan *Wireless Metropolitan Area Network* (WMAN). (www.wikipedia.com).

2.6 Pengertian Hotspot

Tanpa disadari sebenarnya kehidupan manusia tidak dapat terlepas dari kebutuhan untuk saling berbagi dalam segala hal. Kemampuan teknologi telah menjawab berbagai tantangan manusia untuk saling berinteraksi secara *real time* , dimana batas antara jarak, waktu, dan ruang bukanlah penghalang bagi keinginan manusia untuk saling berkomunikasi.

Era digital telah merambah ke segala bidang, sehingga hampir tidak ada celah dalam kehidupan manusia yang tidak berhubungan dengan teknologi digital. Keinginan manusia untuk menyadari keberadaannya secara relatif dengan manusia yang lain menjadi obsesi yang tidak berlebihan, di mana sinergi dari kesadaran untuk saling berbagi pakai tersebut akan dapat memberikan kemudahan dalam menjalani kehidupan.

Tingginya animo masyarakat khususnya di kalangan komunitas internet menggunakan teknologi *Wi-Fi* dikarenakan paling tidak dua faktor. Pertama, karena kemudahan akses. Artinya, para pengguna dalam satu area dapat

mengakses internet secara bersamaan tanpa perlu direpotkan dengan kabel. Konsekuensinya, pengguna yang ingin melakukan *surfing* atau *browsing* berita dan informasi di internet cukup membawa PDA (Personal Digital Asisstant) atau laptop berkemampuan *Wi-Fi* ke tempat dimana terdapat *access point* atau hotspot. Menjamurnya hotspot di tempat-tempat tersebut baik bagi penyedia internet bahkan orang perorangan dipicu oleh factor kedua, yaitu karena biaya pembangunannya yang relatif murah atau hanya berkisar 300 dollar Amerika Serikat.

Pengertian hotspot adalah sebuah area publik dengan akses poin nirkabel yang memungkinkan *users* untuk mengakses internet dengan mempergunakan standar teknologi jaringan nirkabel. Hanya saja, agar dapat mengakses internet di hotspot, *users* perlu melengkapi komputer dengan alat khusus (SOLOPOS, 10/9/2006 hal 2). Definisi yang lain hotspot adalah merupakan kawasan di mana orang awam boleh mendapat capaian tanpa bayar ke internet dengan menggunakan komputer atau PDA menggunakan teknologi piawai WLAN (*Wi-Fi*) (www.wikipedia.com). Selain itu, perkembangan teknologi tepatnya *information technology* (IT) menyumbangkan definisi baru buat istilah hotspot, yaitu hotspot merupakan area publik yang telah dipasangi jaringan internet *wireless* atau nirkabel. Jaringan *wireless fidelity* (*Wi-Fi*) ini memakai standar teknologi IEEE 802.11 dengan frekuensi 2,4 Gigahertz. Teknologi tersebut juga dikenal dengan nama WLAN (Wireless Local Area Network).

Beberapa komponen dalam hotspot adalah:

1. Station yang mobile
2. Access Point
3. Switch, Router, Network Access Controller
4. Web server atau server yang lain
5. Koneksi Internet kecepatan tinggi
6. Internet Service Provider
7. Wireless ISP

Dalam beberapa tahun ini, hotspot mulai marak dipasang oleh beberapa ISP (Internet Server Provider), meski dilihat dari pangsa pasar penggunanya masih kecil, tetapi layanan koneksi komunikasi nirkabel ini bisa menjadi tren yang positif. Dilihat dari kegunaannya sangat jelas bahwa layanan semacam ini (hotspot) sangat membantu dalam berinternet. Jadi kita tidak perlu untuk mencolokkan kabel jaringan ke dalam *notebook* atau komputer jinjing, selama ada sinyal *wireless* ada kita langsung koneksi ke internet maka kita bisa mengakses secara cepat (www.komputeraktif.com).

Metode dalam penyelenggaran hotspot ada dua jenis yaitu, metode *free paid* atau gratis dalam pemakainnya dan *pre paid* alias konsumen harus membayar dalam pemakainnya. Untuk metode gratis biasanya bisa ditemukan di publik area seperti bandara, atau dikafe yang memang dimaksudkan penyelanggaranya atau pemilik kafe tersebut digunakan sebagai media promosi. Biaya akses internet pada metode *free paid* biasanya ditanggung oleh penyelenggara, sehingga pengguna sama sekali tak dikenai biaya. Sedangkan sistem *pree paid* mengharuskan *users*

membayar sejumlah uang untuk memperoleh semacam kode akses. Setelah memperoleh kode akses tersebut barulah *users* bisa masuk ke hotspot. Tanpa kode tersebut mustahil *users* bisa mengakses internet di area hotspot.

Uniknya, pemakaian hotspot kini tak lagi terbatas di area publik, lobi hotel atau kafe semata. Melainkan juga sudah mulai merambah ke perusahaan hingga ke rumah pribadi. Ini diperuntukkan bagi konsumen yang tidak mau direpotkan dalam hal pemasangan kabel-kabel, maka dari itu hotspot yang paling praktis dalam penggunaannya. Maka tidak heran kalau sekarang banyak perusahaan bahkan pemilik rumah pribadi memilih hotspot agar bisa akses internet (SOLOPOS, 10/9/2006 hal 2).

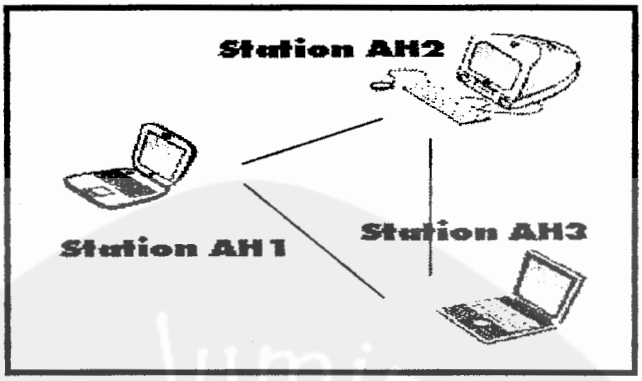
2.6.1 Topologi Jaringan *Wireless*

Jaringan *wireless* atau hotspot mempunyai sedikit perbedaan pada tipe topologinya, yaitu:

1. Independent Basic Service Set (IBSS)

Topologi paling sederhana adalah tipe Ad Hoc dimana *node-node* yang independen akan saling berkomunikasi secara *peer to peer* atau *point to point*. Standar ini merujuk pada topologi *independent basic service set* (IBSS) dimana salah satu *node* akan ditunjukkan sebagai proksi untuk melakukan koordinasi antarnode dalam sebuah grup.

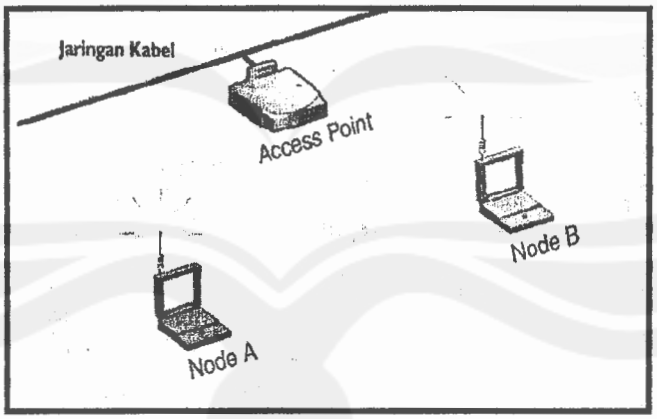
Proksi ini bertindak sebagai *access point* atau *base station* dalam sebuah jaringan yang kompleks. Topologi Ad Hoc sangat murah diterapkan dan sangat efektif serta mudah dalam pembangunan lingkungan *wireles* seperti pada ruangan konferensi, kelas, atau bahkan lingkungan kerja yang relatif kecil.



Gambar 2.1 Komunikasi *Peer to Peer* pada Jaringan *Ad Hoc*

2. Basic Service Set (BSS)

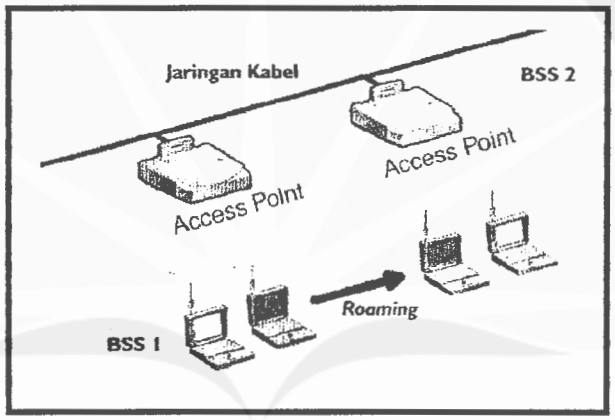
Topologi yang lebih kompleks adalah topologi infrastruktur, di mana paling sedikit ada satu *access point* yang bertindak sebagai *base station. Access point* akan menyediakan fungsi sinkronisasi dan koordinasi, melakukan *forwading* serta *broadcasting* paket data. Fungsi ini hampir sama dengan teknologi *bridge* pada metode jaringan *wired* (dengan kabel).



Gambar 2.2 Topologi *Basic Service Set* (BSS)

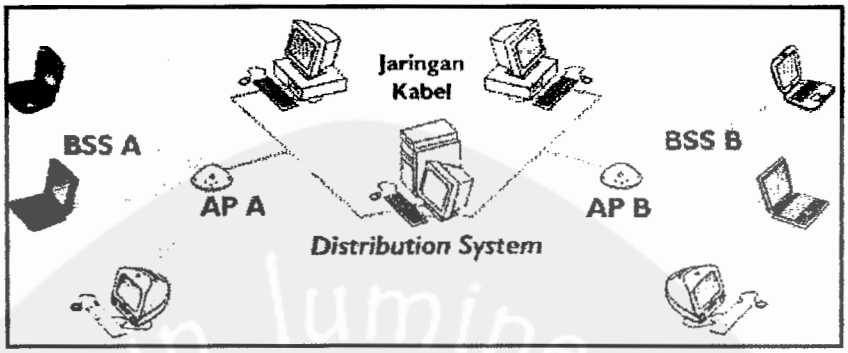
3. Extended Service Set (ESS)

Pada topologi ini, beberapa *access point* dapat digunakan untuk *mengcover range area* yang lebih luas, sehingga membentuk *extended service set* (ESS). Metode ini terdiri dari dua atau lebih *basic service set* yang terkoneksi pada satu jaringan kabel. Setiap *access point* diatur dalam *channel* yang berlainan untuk menghindari terjadinya interferensi. Metode ini akan membentuk sel-sel seperti pada jaringan seluler. *User* dapat melakukan *roaming* ke sel yang lain dengan cukup mudah tanpa kehilangan sinyal.



Gambar 2.3 *Extended Service Set* (ESS)

Extended service set (ESS) memperkenalkan kemungkinan melakukan *forwading* dari sebuah sel radio ke sel yang lain melalui jaringan kabel. Kombinasi *access point* dengan jaringan kabel akan membentuk *distribution system* (DS).



Gambar 2.4 *Extended Service Set* (ESS) dengan *Distribution System*

2.7 Fasilitas Hotspot

2.7.1 Kecepatan Akses

Hotspot sebenarnya seiring dengan kebutuhan konsumen yang ingin bisa berkomunikasi di mana saja. Penggunaannya pun masih diarahkan untuk kepentingan *personal*. Namun dalam perkembangannya, WLAN mulai digunakan untuk kepentingan publik. Biasanya WLAN publik disediakan di lobi hotel, ruang tunggu bandara dan kafe. Dengan demikian, kita dapat berinternet sembari rileks, ngobrol santai, dan minum kopi hangat.

Teknologi ini mulai diperkenalkan di tanah air oleh sejumlah ISP (Internet Service Provider) dan operator seperti Millenia Net (www.millenia.com), CBN (www.cbn.net.id), Biznet (www.Biznet.net.id) dan Telkomsel (www.Telkomsel.com). Sayangnya, teknologi nirkabel yang sering digunakan sebagai penghubung (*bridge*) antara ISP dan pelanggannya kadang menimbulkan interferensi gelombang. Ini disebabkan teknologi WLAN menggunakan frekuensi ISM yang *free-lisence*. Padahal, frekuensi ini pada mulanya hanya digunakan sebagai akses internet *indoor* pengganti kabel UTP.

Sebenarnya ada dua jenis konfigurasi WLAN yang digunakan dalam hotspot. Jenis pertama disebut dengan Mode Infrastruktur, yang memerlukan adanya sebuah *access point* atau titik akses, konfigurasi yang cocok untuk layanan publik. Secara teoritis, sebuah *access point* dapat melayani maksimal 255 pengguna. Access point digunakan untuk melakukan pengaturan lalu lintas jaringan dari *mobile* radio ke jaringan kabel atau dari *backbone* jaringan *wireless client/server*. Pengaturan ini digunakan untuk melakukan koordinasi dari semua node jaringan dalam mempergunakan layanan dasar jaringan serta memastikan penangganan lalu lintas data dapat berjalan dengan sempurna. *Access point* akan merutekan aliran data antara ~~pusat~~ jaringan pusat dengan jaringan *wireless* yang lain. Dalam sebuah WLAN pengaturan jaringan akan dilakukan oleh *access point* pusat yang mempunyai performa *throughput* yang lebih baik (Edi S. Mulyanta, S.Si, 2005: 54).

Mode kedua adalah Mode Ad Hoc yang tidak memerlukan titik akses, tetapi pengguna dapat berhubungan lewat adaptor nirkabel. Jaringan Ad Hoc merupakan jaringan sederhana dimana komunikasi terjadi antara dua perangkat atau lebih pada cakupan area tertentu tanpa harus memerlukan sebuah *access point* atau *server*. Standarisasi ini semacam etiket pada setiap perangkat jaringan dalam melakukan akses media *wireless*. Metode ini meliputi penentuan pemberian permintaan koneksi pada sebuah media untuk memastikan *throughput* yang dimaksimalkan untuk pengguna dalam menerima layanan (Edi S. Mulyanta, S.Si, 2005: 53).

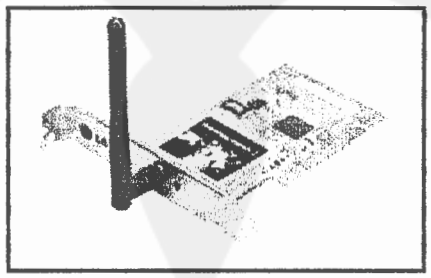
Selama mengakses jaringan WLAN di area hotspot, pengguna bisa mendapatkan akses koneksi internet dengan kecepatan sampai dengan 11 Mbps (*megabits per second*), kecepatan ini bisa ditingkatkan hingga 54 Mbps tergantung standar yang dipakai. Namun, rata-rata operator hotspot di dalam negeri memberi kecepatan akses internet sebesar 2 Mbps bagi penggunanya. Dari *access point* yang ada di area hotspot, bisa dipancarkan sinyal sejauh 100-400 meter. Sementara untuk terhubung ke NOC ISP, kebanyakan area hotspot dihubungkan dengan koneksi ADSL dan *wireless*.

2.7.2 Infrastruktur Jaringan Fisik *Wireless*

Ada beberapa hal yang diperlukan dan dapat dijadikan pegangan dalam mengembangkan serta melakukan instalasi WLAN pada jaringan di lingkungan kita, antara lain:

1. *Adapter Wireless*

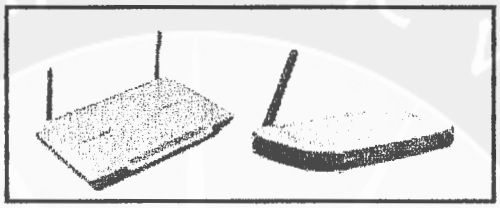
WLAN terdiri dari dua blok bangunan dasar, yaitu *access point* yang akan melakukan koneksi ke jaringan, dan *adapter wireless* yang terkoneksi pada peralatan komputer. *Adapter wireless* mempunyai fungsi yang sama dengan *network interface card* (NIC) pada jaringan *wired* tradisional.



Gambar 2.5 *Adapter wireless* berbentuk *Card PCI*

2. *Access Point*

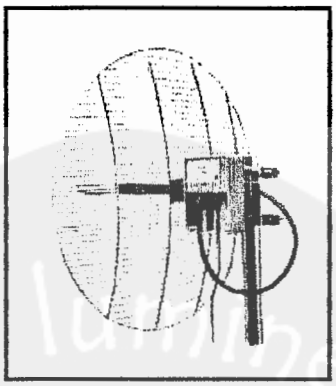
Biasanya berbentuk kotak kecil terkadang dilengkapi satu atau dua antena. Peralatan ini merupakan *radio based*, berupa *receiver* dan *transmitter* yang akan terkoneksi dengan LAN *wired* (kabel) atau dapat pula terkoneksi pada *broadband* menggunakan *ethernet*.



Gambar 2.6 *Acces Point*

3. *Antenna and Bridge*

Antena mempunyai fungsi utama untuk memperluas cakupan area dari frekuensi radio dalam *range* 802.11 WLAN. *Bridge* akan menyediakan koneksi *wireless point to point* antara dua LAN atau koneksi yang menghubungkan jaringan yang berbeda lokasi pada gedung bertingkat, misalnya berbeda lantai dalam satu gedung perkantoran (Edi S. Mulyanta, S.Si, 2005: 56-58).



Gambar 2.7 Antena

2.8 Keamanan Jaringan Wireless

Ada anggapan bahwa mengakses internet di area publik lewat hotspot sangat berisiko alias tidak aman. *Users* lain yang berniat jahat bisa memasukkan virus atau bahkan mengintip file yang tengah kita buka. Sama persis dengan kejahatan yang dilakukan oleh sejumlah oknum pada pengguna telepon seluler berteknologi *bluetooth*. Sang oknum biasanya akan memasukkan virus atau mengintip *file* lewat fasilitas *bluetooth* tersebut. Ada kode etik tersendiri di kalangan penyelenggara hotspot untuk melindungi *users*.

Apabila antar *users* dapat membuka *file* maka berarti pihak penyelenggara yang ceroboh. Termasuk untuk menghindari akses *spam* atau serangan *virus* dari *users* lain, biasanya penyelenggara sudah mengenakan filter-filter tersendiri (SOLOPOS, 10/9/2006 hal 2).

Namun meningkatnya pertumbuhan *Wi-Fi* perlu dibarengi kewaspadaan akan ancaman keamanan lewat jalur nirkabel. Pihak yang berniat jahat bisa saja

mendirikan sebuah menara pemancar pada lokasi yang berdekatan dengan menara pemancar *Wi-Fi* tertentu. Apabila pemancar palsu tersebut memancarkan sinyal yang lebih kuat, pengguna atau *users* bisa jadi terkecoh dan berusaha *log in* di jaringan palsu tersebut. Saat *users* memasuki jaringan tersebut, semua informasi yang dipertukarkan bisa disadap oleh pemilik pemancar. Data penting seperti nomor rekening, *password* bahkan nomor kartu kredit bisa saja dicuri. Agar aman berkoneksi di hotspot adalah melakukan proteksi terhadap komputer dari serangan virus (www.detikinet.com).

Teknologi yang masih banyak digunakan sekarang yaitu, *wired equivalent privacy* (WEP), tidak memungkinkan apabila digunakan pada hotspot. WEP mengisyaratkan satu kunci (*key*) dipakai oleh semua pengguna. Sehingga apabila digunakan akan percuma, karena bagaimana pun juga kunci ini akan dipublikasikan alias tidak ada yang dirahasiakan.

Walaupun sekarang teknologi lain seperti *Wi-Fi Protected Access* (WPA) sudah memungkinkan penggunaan kunci dinamik dan dapat diasosiasikan dengan *users name* atau *password* pelanggan hotspot tetapi masih banyak kartu *wireless* yang belum mendukung teknologi ini. Sehingga, karena tujuan penyelenggara hotspot kemudahan akses, maka WPA masih belum dalam waktu dekat ini.

Sertifikasi *Wi-Fi* adalah proses untuk memastikan interoperabilitas antar peralatan *wireless* LAN 802.11, termasuk *acces point* dan kartu-kartu jaringan radio *wireless* yang biasanya mempunyai beberapa *form factor* yang sangat

beragam. Perusahaan-perusahaan produsen peralatan *wireless* harus menjadi anggota *Wi-Fi Alliance*.

Perusahaan-perusahaan tersebut memerlukan sertifikasi *Wi-Fi* untuk menjaga kualitas produk. Sertifikasi ini juga digunakan untuk menjaga interoperabilitas beberapa produk *Wi-Fi*. Setelah produk tersebut melalui beberapa tes, pabrikan akan diberikan hak untuk menempatkan logo sertifikasi *Wi-Fi*, sehingga *user* akan mendapatkan beberapa kemudahan dalam hal standarisasi dan interoperabilitas (Edi S. Mulyanta, S.Si, 2005: 52-53).

Wi-Fi merupakan pembebasan dari jeratan kabel, sehingga pengguna jaringan dapat melakukan koneksi jaringan di manapun, baik *indoor* maupun *outdoor* dalam *range* tertentu. Akan tetapi, kebebasan tersebut tidak seluruhnya benar karena harus mengonfigurasi dan menyertifikasi perangkat yang anda gunakan dengan *Wi-Fi CERTIFIED*. Sertifikasi tersebut berarti dapat melakukan koneksi dimanapun jika peralatan kita kompatibel dengan produk-produk yang mempunyai logo sertifikasi *Wi-Fi CERTIFIED*. Pengembangan jaringan *Wi-Fi* (hotspot) telah merambah pada area-area seperti universitas-universitas, bandara, hotel, dan area publik lainnya yang telah berlomba-lomba mengembangkan kawasan hotspot.

Sertifikasi *Wi-Fi* digunakan untuk menjamin produk dengan interoperabilitas yang baik karena telah melalui pengujian standar produk yang telah kompatibel dengan produk yang dikeluarkan oleh beberapa *vendor* (Edi S. Mulyanta, S.Si, 2005: 147-148).

Gambar 2.8 Logo sertifikasi Wi-Fi

WPA dan protocol 802.11i akan mengurangi masalah penyadapan diarea hotspot maupun mencegah orang yang tidak mempunyai hak (bukan pelanggan hotspot misalnya) mengakses ke fasilitas hotspot (*access point*). Tetapi, WPA hanya akan memberikan solusi keamanan pada jalur data jaringan nirkabel, bukan solusi keamanan komputer dari ancaman pemakai hotspot yang lain.

Selain itu, WPA atau protocol 802.11i hanya akan memberikan solusi enkripsi pada jaringan nirkabel hotspot. Sehingga kalau pemakai hotspot akan mengakses *server* yang ada dikantornya, maka kemungkinan penyadapan akan tetap terjadi. Maka dari itu komputer harus diproteksi sedemikian saat mengakses hotspot. Selain itu teknologi keamanan juga dapat membantu meningkatkan keamanan komputer klien yang menggunakan jaringan publik seperti hotspot. Teknologi sistem keamanan komputer klien yang dapat digunakan adalah *personal firewall* atau *personal intrusion prevention system*, program VPN, dan tentunya program anti virus (www.eBizzAsia.com).

Masalah keamanan jaringan selalu menjadi prioritas penting dalam pengembangan jaringan baik *wired* maupun *wireless*. WLAN mempunyai kemampuan fleksibilitas pengembangan yang sangat tinggi. Akan tetapi, fitur ini

justru menimbulkan beberapa keterbukaan yang potensial terhadap adanya akses-akses yang tidak diinginkan. Akses *illegal* terhadap jaringan *wireless access point* dapat dilakukan apabila tidak mempersiapkan proteksi data yang lebih baik. Untuk itu, beberapa teknologi keamanan jaringan telah dikembangkan dengan berbagai tingkatan proteksi untuk keperluan jaringan *wireless* dari *home user* hingga bisnis skala besar.

Saat ini, spesifikasi produk 802.11b telah dilengkapi dengan keamanan standar dengan jenis proteksi:

a. **Service Set Identifier *(SSID)***

Merupakan kunci identitas WLAN yang telah umum digunakan. Klien harus dikonfigurasikan dengan menggunakan SSID yang benar untuk dapat melakukan akses jaringan WLAN. Kunci ini harus dapat di *share* hanya pada mereka yang telah sah untuk melakukan akses jaringan. SSID harus dapat diubah-ubah secara periodik untuk lebih meningkatkan keamanan.

b. **Media Access Control (MAC)**

Filtering pada alamat-alamat tertentu untuk membatasi akses WLAN ke daftar komputer yang dapat dibuat pada setiap *access point.*

c. **Wired Equivalent Privacy (WEP)**

Skema enkripsi yang melindungi aliran data WLAN antara klien dan *access point* yang telah ditentukan oleh standar 802.11. Fitur ini harus diaktifkan

walaupun fitur ini terkadang mengalami kerusakan atau ketidakefisienan keamanan (Edi S. Mulyanta, S.Si, 2005: 62-63).

Beberapa organisasi dan perusahaan semakin gencar mengembangkan jaringan *wireless* karena kemudahan, kenyamanan, dan harga peralatan yang semakin terjangkau. Di pasaran, peralatan-peralatan *wireless* ini secara *default* tidak mempunyai fitur keamanan yang memadai, sehingga keberadaan perlatan *wireless* menjadi target utama para *hacker* untuk mencoba memanfaatkan berbagai kelemahannya. Hal ini didukung lagi dengan dokumen-dokumen peralatan *wireless* yang dengan mudah diperoleh di *web site* secara bebas, baik dari segi teknis detail hingga operasionalnya.

Tidak seperti pada jairngan kabel tradisional, WLAN mengirimkan datanya melalui udara bebas dan sangat memungkinkan diakses di luar batas fisik sebuah kelompok jaringan yang berhak. Sinyal komunikasi secara alami tersedia secara terbuka dan merambat melalui udara.

Banyak pengembang jaringan *wireless* yang menyatakan bahwa WLAN mempunyai risiko keamanan yang sangat tinggi dan tidak ada jaminan keamanan yang dapat diberikan, kecuali hanya melakukan *mitigasi* risiko keamanan WLAN yang mungkin dapat dilakukan. Secara garis besar terdapat beberapa isu keamanan jaringan *wireless* serta risiko pengembangannya yang telah dipublikasikan, antara lain serangan terhadap kerahasiaan, integritas data serta ketersediaan jaringan.

Ada dua serangan dalam jaringan *wireless*, yaitu:

1. Serangan pasif

Biasanya menggunakan akses yang bukan haknya dan tidak melakukan perubahan *content* atau isi paket data. Serangan pasif biasanya berupa penyadapan atau penganalisaan lalu lintas jaringan (*traffic*) yang sering disebut *traffic flow analysis*.

Terdapat dua serangan pasif, antara lain:

a. Penyadapan atau *eavesdropping*, di mana penyerang melakukan pemonitoran transmisi serta isi dari pesan.
b. Analisa *traffic*, penyerang menggunakan cara yang tidak dirasakan pihak yang diserang dengan menggunakan metode pemonitoran yang lebih canggih untuk membuat pola komunikasi pihak yang diserang. Sejumlah informasi dapat dirangkai dan didapatkan melalui aliran pesan di antara bagian-bagian yang saling berkomunikasi.

2. Serangan aktif

Penyerang yang sebenarnya tidak berhak atas akses jaringan akan melakukan modifikasi data, aliran data, atau *file*. Serangan ini mudah sekali dideteksi, akan tetapi tipe ini sangat sulit untuk dihindari. Serangan aktif dapat berupa kombinasi dari keempat serangan aktif, yaitu *masquerading*, *replay*, modifikasi pesan, dan DoS.

a. *Masquerading*, penyerang akan menyamar sebagai user yang mempunyai hak untuk menggunakan jaringan, sehingga dapat memanfaatkan *resource* jaringan pihak yang diserang.

b. *Replay*, penyerang akan memonitor transmisi (serangan pasif) terlebih dahulu, kemudian akan melakukan transmisi ulang pesan tersebut selayaknya *user* yang berhak memanfaatkan jaringan.

c. Modifikasi pesan, penyerang akan mengubah pesan asli dengan cara menghapus, menambah dan melakukan penyusunan ulang pesan.

d. *Denial of Service* (DoS), Penyerang akan mencegah bahkan menghalangi penggunaan jaringan secara normal hingga menghalangi pengaturan fasilitas komunikasi (Edi S. Mulyanta, S.Si, 2005: 174-175).

2.9 Keunggulan dan Kelemahan Hotspot

Ada beberapa keunggulan atau kelebihan yang ada di hotspot yaitu:

1. Pemeliharaan murah
2. Infrastruktur berdimensi kecil
3. Pembangunan cepat
4. Mudah dan murah untuk direlokasi dan mendukung portabilitas
5. Koneksi internet 24 jam
6. Akses internet yang cepat
7. Bebas tanpa pulsa telepon

Ada pun hotspot juga mempunyai kelemahan, yaitu:

1. Biaya peralatan mahal
2. Delay yang sangat besar

3. Coverage area sangat terbatas
4. Kesulitan karena masalah propagasi radio
5. Keamanan data belum tentu terjamin
6. Kapasitas jaringan karena kapasitas *bandwith* (http://angin.com)