BAB IV

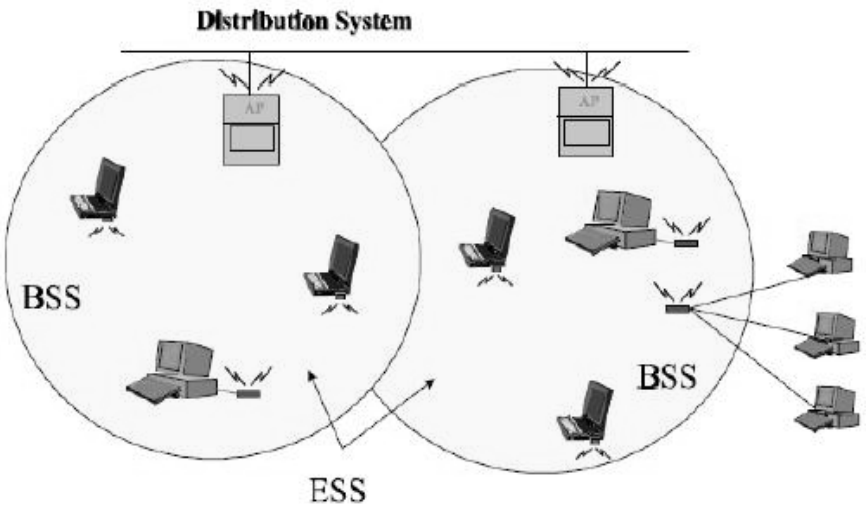
IMPLEMENTASI TEKNOLOGI WI-FI DAN HOTSPOT AREA

4.1. Konsep Implementasi Teknologi Wi-Fi di Komplek PTJ

4.1.1. Arsitektur Jaringan Wi-Fi

Untuk dapat mengimplementasikan teknologi jaringan nirkabel (Wi-Fi), terlebih dahulu harus dipahami tentang arsitektur dasarnya, sebagai mana telah dijelaskan pada landasan teori di BAB II dan sesuai dengan perencanaan yang telah digambarkan di BAB III yang pada kenyataannya sangat tergantung dilapangan (Komplek PTJ) dan sangat potensial akan keberhasilan pada implementasi teknologi Wi-Fi tersebut, terutama pada kekuatan sinyal dan jarak jangkauan (hotspot area) khususnya dalam akses free internet hotspot.

Wi-Fi (atau Wi- fi, WiFi, Wifi, wifi) merupakan kependekan dari *Wireless Fidelity*, memiliki pengertian yaitu sekumpulan standar yang digunakan untuk Jaringan Lokal Nirkabel (*Wireless Local Area Network,* WLAN) yang didasari pada spesifikasi The Institute of Electrical and Electronics Engineer (IEEE) 802.11. Fungsinya menghubungkan jaringan dalam satu area lokal secara nirkabel. Awalnya Wi-Fi digunakan untuk penggunaan perangkat nirkabel dan jaringan area lokal (LAN), namun saat ini lebih banyak digunakan untuk mengakses internet. Hal ini memungkinkan seseorang dengan komputer, dengan kartu nirkabel (*wireless card*) atau *personal digital assistant* (PDA) untuk terhubung dengan internet dengan menggunakan titik akses (hotspot) terdekat.



Gambar 4.1. Arsitektur Dasar Jaringan Wi-Fi

Arsitektur 802.11 LAN mirip arsitektur seluler di mana sistem ini dibagi-bagi menjadi beberapa sel. Tiap sel (yang disebut dengan *Basic Service Set* atau BSS) dikontrol oleh *Base Station* (yang disebut dengan *Access Point* atau biasa disingkat AP). Terdapat 2 jenis BSS, yaitu :

1. *Independent* BSS (IBSS), yaitu sistem BSS apabila *Wireless Station* (WS) tidak dihubungkan menggunakan AP.
2. *Infrastructure* BSS, yaitu sistem BSS apabila terdapat AP yang menghubungkan WS.

Walaupun WLAN dapat berupa sel tunggal, dengan sebuah AP, kebanyakan instalasi WLAN terdiri dari beberapa sel, di mana AP terhubung melalui suatu *backbone* (disebut dengan *Distribution System* atau DS). *Backbone* ini biasanya berupa *Ethernet* dan dalam beberapa kasus juga dapat berupa *wireless*. Jaringan WLAN yang telah terinterkoneksi secara utuh, termasuk dengan sel-sel yang berbeda, seluruh AP dan DS dipandang sebagai satu jaringan

802.11 bagi *layer* di atasnya dan jaringan ini disebut dengan *Extended Service Set* (ESS).

4.1.2. Metode Akses Jaringan Wi-Fi

Metode untuk akses koneksi ke jaringan nirkabel (Wi-Fi) dapat dilakukan dengan 2 cara menghubungkan antar PC dengan sistem Wi-Fi yaitu adhoc dan infrastruktur. Kedua cara ini memiliki keuntungan dan kelemahan masing masing sesuai dengan kondisi yang dihadapi saat melakukan pemasangan jaringan wireless sesuai kebutuhan.



Gambar 4.2. Mede Jaringan Adhoc

1. *Sistem adhoc* adalah sistem *peer* to *peer*, dalam arti satu komputer dihubungkan ke satu komputer dengan saling mengenal SSID. Bila digambarkan mungkin lebih mudah membayangkan sistem *direct connection* dari satu komputer ke satu komputer lainnya dengan menggunakan twist pair cable tanpa perangkat HUB.

   Jadi terdapat dua komputer dengan perangkat Wi-Fi dapat langsung berhubungan tanpa alat yang disebut *access point mode*. Pada sistem adhoc

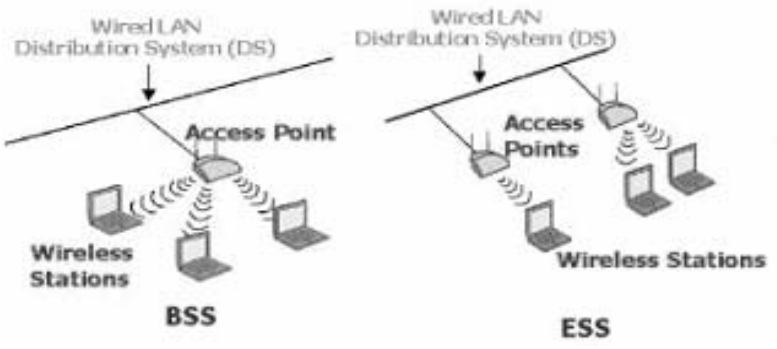
tidak lagi mengenal sistem central (yang biasanya difungsikan pada Access Point). Sistem adhoc hanya memerlukan satu buah komputer yang memiliki nama SSID atau sederhananya nama sebuah network pada sebuah card/komputer.

Dapat juga mengunakan MAC address dengan sistem BSSID (*Basic Service Set IDentifier* - cara ini tidak umum digunakan), untuk mengenal sebuah nama komputer secara langsung. MAC address umumnya sudah diberikan tanda atau nomor khusus tersendiri dari masing-masing card atau perangkat network termasuk network wireless. Sistem adhoc menguntungkan untuk pemakaian sementara misalnya hubungan network antara dua komputer walaupun disekitarnya terdapat sebuah alat Access Point yang sedang bekerja.

SSID adalah nama sebuah network card atau USB card atau PCI card atau Router Wireless. SSID hanyalah sebuah nama untuk memberikan tanda dimana nama sebuah perangkat berada. BSSID adalah nama lain dari SSID, SSID diberikan oleh pemakai misalnya ’antonetwork’ pada komputer yang sedang digunakan dan komputer lainnya dibuatkan nama ’apanetwork’. Sedangkan BSSID menggunakan basis MAC address. Bila sebuah koneksi wireless ingin saling berhubungan, keduanya harus menggunakan setup adhoc. Bila disekitar ruangan terdapat perangkat Access Point, perlu diingatkan untuk mengubah band frekuensi agar tidak saling adu kuat signal yang memancar didalam suatu ruangan.

2. *Sistem infrastruktur* membutuhkan sebuah perangkat khusus atau dapat difungsikan sebagai Access Point melalui software bila menggunakan jenis

wireless network dengan perangkat PCI card. Mirip seperti HUB Network yang menyatukan sebuah network tetapi didalam perangkat Access Point menandakan sebuah central network dengan memberikan signal (melakukan broadcast) radio untuk diterima oleh komputer lain. Untuk menggambarkan koneksi pada infrastruktur dengan Access Point minimal sebuah jaringan wireless network memiliki satu titik pada sebuah tempat dimana komputer lain yang mencari / menerima signal dapat masuk ke dalam network agar saling berhubungan. Sistem Access Point (AP) ini paling banyak digunakan karena setiap komputer yang ingin terhubung ke dalam network dapat dengan mudah mendengar transmisi dari Access Point tersebut. Access Point inilah yang memberikan tanda apakah di suatu tempat memiliki jaringan Wi-Fi dan secara terus menerus mentransmisikan namanya (SSID) dan dapat diterima oleh komputer lain untuk dikenal. Bedanya dengan HUB network cable, HUB menggunakan kabel tetapi tidak memiliki nama (SSID). Sedangkan Access Point tidak mengunakan kabel network tetapi harus memiliki sebuah nama yaitu nama untuk SSID.



Gambar 4.3. Mede Jaringan Infrastruktur

Adapun keuntungan pada sistem infrastruktur ini antara lain :

a. Untuk sistem AP dalam melayani banyak PC tentu lebih mudah pengaturannya. Komputer klien dapat mengetahui bahwa disuatu ruang ada sebuah hardware atau komputer yang memancarkan sinyal Access Point sehingga dapat masuk ke dalam sebuah network .
b. Keuntungan kedua bila menggunakan hardware khusus, maka tidak diperlukan sebuah PC berjalan 24 jam untuk melayani network. Banyak hardware Access Point yang dapat dihubungkan ke sebuah HUB atau sebuah jaringan LAN. Dan komputer pemakai Wi-Fi dapat masuk kedalam sebuah jaringan network.
c. Sistem security pada model AP lebih terjamin. Untuk fitur pengaman sebuah hardware Access Point memiliki beberapa fitur seperti melakukan block IP, membatasi pemakai pada port dan lainnya.

Jaringan Wireless memiliki beberapa kelebihan atau keunggulan jika dibandingkan dengan jaringan menggunakan kabel sebagai media untuk berkomunikasi, antara lain dalam hal :

1. Pengkabelan

   Pada jaringan wireless, sistem pengkabelan dapat diminimalkan bahkan dapat dihilangkan. Hal ini tidak akan dapat dilakukan oleh jaringan yang menggunakan kabel sebagai media komunikasi. Karena pada jaringan tersebut kabel adalah hal yang utama.

2. Pemeriksaan pada saat terjadi masalah

   Pada jaringan konvensional, jika salah satu komputer tidak dapat terhubung ke jaringan, salah satu penyebabnya adalah kabel. Tentunya jika hal tersebut terjadi kita harus memeriksa kabel tersebut sampai menemukan bagian yang rusak dan tentunya menuntut kerja ekstra, namun hal tersebut tidak akan terjadi pada jaringan wireless.

3. Jarak

   Jarak merupakan kendala bagi jaringan konvensional. Karena jarak maksimum yang dapat dijangkau hanya sekitar 10 0 meter. Sedangkan untuk jaringan wireless jangkauannya lebih luas, bahkan dapat mencapai antar negara.

4. Mobilitas

   Dengan jaringan wireless, seorang user tidak perlu bingung bila akan berpindah tempat selama ia masih dalam daerah jangkauan, karena tidak per lu memikirkan tersedia atau tidaknya kabel yang digunakan untuk media komunikasi.

Meski jaringan wireless memiliki beberapa kelebihan, namun dalam berkomunikasi dengan jaringan wireless mempunyai beberapa aturan yang harus dipenuhi oleh user/client yang ingin berkomunikasi secara wireless, antara lain :

- Seluruh perangkat keras wireless yang digunakan harus bekerja pada frekuensi dan system modulasi yang sama.
- Hendaknya menggunakan perangkat wireless yang menggunakan standart wireless yang sama meskipun perangkat keras tersebut berasal dar i vendor yang ber beda.

4.1.3. Komponen Jaringan Wi-Fi

Ada empat komponen utama dalam sistem Wireless LAN (Wi-Fi) adalah sebagai berikut :

1. Access Point

   Merupakan perangkat yang menjadi sentral koneksi dari pengguna (user) ke ISP, atau dari kantor cabang ke kantor pusat jika jaringannya adalah milik sebuah perusahaan. Access-Point berfungsi mengkonversikan sinyal frekuensi radio (RF) menjadi sinyal digital yang akan disalurkan melalui kabel, atau disalurkan ke perangkat WLAN yang lain dengan dikonversikan ulang menjadi sinyal frekuensi radio.



Gambar 4.4. Access Point Router

2. Wireless LAN Interface

   Merupakan peralatan yang dipasang di Mobile/Desktop PC, peralatan yang dikembangkan secara massal adalah dalam bentuk PCMCIA (Personal Computer Memory Card International Association) card, PCI card maupun melalui port USB (Universal Serial Bus).



Gambar 4.5. Wireless Adapter

3. Mobile/Desktop PC

   Merupakan perangkat akses untuk pengguna, mobile PC pada umumnya sudah terpasang port PCMCIA sedangkan desktop PC harus ditambahkan wireless adapter melalui PCI (Peripheral Component Interconnect) card atau USB (Universal Serial Bus).

4. Antena external (optional)

   Antena external ini digunakan untuk memperkuat daya pancar. Antena ini dapat dirakit sendiri oleh user. contoh : antena kaleng, wajan bolik, dll.

Secara relatif perangkat Access-Point ini mampu menampung beberapa sampai ratusan pengguna secara bersamaan. Beberapa vendor hanya merekomendasikan belasan sampai sekitar 40-an pengguna untuk satu Access Point. Meskipun secara teorinya perangkat ini bisa menampung banyak namun akan terjadi kinerja yang menurun karena faktor sinyal RF itu sendiri dan kekuatan sistem operasi Access Point.

Komponen logic dari Access Point adalah ESSID (Extended Service Set IDentification) yang merupakan standar dari IEEE 802.11. Pengguna harus mengkoneksikan wireless adapter ke Access Point dengan ESSID tertentu supaya

transfer data bisa terjadi. ESSID menjadi autentifikasi standar dalam komunikasi wireless. Dalam segi keamanan beberapa vendor tertentu membuat kunci autentifikasi tertentu untuk proses autentifikasi dari klien ke Access Point. Rawannya segi keamanan ini membuat IEEE mengeluarkan standarisasi Wireless Encryption Protocol (WEP), sebuah aplikasi yang sudah ada dalam setiap PCMCIA card. WEP ini berfungsi meng-encrypt data sebelum ditransfer ke sinyal Radio Frequency (RF), dan men-decrypt kembali data dari sinyal RF.

4.2. Implementasi Wi-Fi di Komplek PTJ

4.2.1. Prosedur Instalasi Wi-Fi

Masa depan teknologi tanpa kabel (nirkabel) sudah semakin nyata di depan mata. Perannya di dunia jaringan komputer pun semakin tak tergantikan. Internet, yang notabene telah menjadi kebutuhan hampir semua orang di dunia, kini dapat diperoleh lebih mudah tanpa menggunakan kabel. Hal ini pula yang membuat komplek PTJ merasa perlu untuk mempelajari dan mengimplementasikan teknologi Wi-Fi ini.

Berdasarkan hasil analisa perancangan dan survey site, maka teknologi Wi-Fi dapat di implementasikan sebagai bentuk pengembangan wired LAN yang sudah ada di SMK 2 Triple “J” dan sesuai dengan hasil studi kasus di Unit Kerja Lab. TKJ (Tahap I, rintisan Wired LAN ke Wireless LAN) dan Unit Kerja Sekretariat SMK 2 Triple “J” (Tahap II).

Baik secara hardware maupun software sesuai dengan konsep perancangan dan survey site yang telah dijelaskan pada BAB sebelumnya, prosedur instalasi Wi-Fi adalah sebagai berikut :

a. Fasilitas Peralatan
    1. Kompas dan peta topografi
    2. Penggaris dan busur derajat
    3. Pensil, penghapus, alat tulis
    4. GPS, altimeter, klinometer
    5. Kaca pantul dan teropong
    6. Radio komunikasi (HT)
    7. USB Wireless, pigtail dan Access Point
    8. Multimeter, SWR, cable tester, solder, timah, tang potong kabel
    9. Peralatan panjat, harness, carabiner, webbing, cows tail, pulley
    10. Kunci pas, kunci ring, kunci inggris, tang (potong, buaya, jepit), obeng set, tie rap, isolator gel, TBA, unibell
    11. Kabel power roll, kabel UTP straight/cross, crimping tools, konektor RJ45
    12. Software AP Manager, Net scrambler
b. Survey Lokasi
    1. Tentukan koordinat letak kedudukan station, jarak udara terhadap BTS dengan GPS dan kompas pada peta
    2. Perhatikan dan tandai titik potensial penghalang sepanjang path
    3. Hitung SOM, path dan acessories loss, EIRP, freznel zone, ketinggian antena

4. Perhatikan posisi terhadap station lain, kemungkinan potensi hidden station, over shoot dan test noise serta interferensi
5. Tentukan posisi ideal tower, elevasi, panjang kabel dan alternatif seandainya ada kesulitan dalam instalasi
6. Rencanakan sejumlah alternatif metode instalasi, pemindahan posisi dan alat

c. Pemasangan Konektor

1. Kuliti kabel coaxial dengan penampang melintang, spesifikasi kabel minimum adalah RG 8 9913 dengan perhitungan losses 10 db setiap 30 m
2. Jangan sampai terjadi goresan berlebihan karena perambatan gelombang mikro adalah pada permukaan kabel
3. Pasang konektor dengan cermat dan memperhatikan penuh masalah kerapian
4. Solder pin ujung konektor dengan cermat dan rapi, pastikan tidak terjadi short
5. Perhatikan urutan pemasangan pin dan kuncian sehingga dudukan kabel dan konektor tidak mudah bergeser
6. Tutup permukaan konektor dengan aluminium foil untuk mencegah kebocoran dan interferensi, posisi harus menempel pada permukaan konektor
7. Lapisi konektor dengan aluminium foil dan lapisi seluruh permukaan sambungan konektor dengan isolator TBA (biasa untuk pemasangan pipa saluran air atau kabel listrik instalasi rumah)

8. Tutup seluruh permukaan dengan isolator karet untuk mencegah air
9. Untuk perawatan, ganti semua lapisan pelindung setiap 6 bulan sekali
10. Konektor terbaik adalah model hexa tanpa solderan dan drat sehingga sedikit melukai permukaan kabel, yang dipasang dengan menggunakan crimping tools, disertai karet bakar sebagai pelindung pengganti isolator karet

d. Pembuatan POE

1. Power over ethernet (POE) diperlukan untuk melakukan injeksi catu daya ke perangkat Wireless In A Box yang dipasang di atas tower, POE bermanfaat mengurangi kerugian power (losses) akibat penggunaan kabel dan konektor
2. POE menggunakan 2 pair kabel UTP yang tidak terpakai, 1 pair untuk injeksi + (positif) power dan 1 pair untuk injeksi – (negatif) power, digunakan kabel pair (sepasang) untuk menghindari penurunan daya karena kabel loss
3. Perhatikan bahwa permasalahan paling krusial dalam pembuatan POE adalah bagaimana cara mencegah terjadinya short, karena kabel dan konektor power penampangnya kecil dan mudah bergeser atau tertarik, tetesi dengan lilin atau isolator gel agar setiap titik sambungan terlindung dari short
4. Sebelum digunakan uji terlebih dahulu semua sambungan dengan multimeter

e. Instalasi Antena

1. Pasang pipa dengan metode stack minimum sampai ketinggian 1st freznel zone terlewati terhadap obstructure terdekat
2. Perhatikan stabilitas dudukan pipa dan kawat strenght, pasang dudukan kaki untuk memanjat dan anker cows tail
3. Cek semua sambungan kabel dan konektor termasuk penangkal petir bila ada
4. Pasang antena dengan rapi dan benar, arahkan dengan menggunakan kompas dan GPS sesuai tempat kedudukan BTS di peta
5. Pasang kabel dan rapikan sementara, jangan sampai berat kabel menjadi beban sambungan konektor dan mengganggu gerak pointing serta kedudukan antena
6. Perhatikan dalam memasang kabel di tower / pipa, jangan ada posisi menekuk yang potensial menjadi akumulasi air hujan, bentuk sedemikian rupa sehingga air hujan bebas jatuh ke bawah

f. Instalasi Perangkat Radio

1. Instal PC Card dan Orinoco dengan benar sampai dikenali oleh OS tanpa konflik dan pastikan semua driver serta utility dapat bekerja sempurna
2. Instalasi pada OS W2K memerlukan driver terbaru dari web site dan ada di CD utility kopian, tidak diperlukan driver PCMCIA meskipun PNP W2K melakukannya justru deteksi ini menimbulkan konflik, hapus driver ini dari Device Manager

3. Instalasi pada NT memerlukan kecermatan alokasi alamat IO, IRQ dan DMA, pada BIOS lebih baik matikan semua device (COM, LPT dll.) dan peripheral (sound card, mpeg dll.) yang tidak diperlukan
4. Semua prosedur ini bisa diselesaikan dalam waktu kurang dari 30 menit tidak termasuk instalasi OS, lebih dari waktu ini segera jalankan prosedur selanjutnya
5. Apabila terus menerus terjadi kesulitan instalasi, untuk sementara demi efisiensi lakukan instalasi dibawah OS Win98 / ME yang lebih mudah dan sedikit masalah
6. Pada instalasi perangkat radio jenis Wireless In A Box (Mtech, Planet, Micronet, dlll.), terlebih dahulu lakukan update firmware dan utility
7. Kemudian uji coba semua fungsi yang ada (AP, Inter Building, SAI Client, SAA2, SAA Ad Hoc dll.) termasuk bridging dan IP Addressing dengan menggunakan antena helical, pastikan semua fungsi berjalan baik dan stabil
8. Pastikan bahwa perangkat Power Over Ethernet (POE) berjalan sempurna

g. Pengujian Noise

1. Bila semua telah berjalan normal, install semua utility yang diperlukan dan mulai lakukan pengujian noise / interferensi, pergunakan setting default
2. Tanpa antena perhatikan apakah ada signal strenght yang tertangkap dari station lain disekitarnya, bila ada dan mencapai good (sekitar 40% – 60%) atau bahkan lebih, maka dipastikan station tersebut beroperasi melebihi EIRP dan potensial menimbulkan gangguan bagi station yang sedang kita

bangun, pertimbangkan untuk berunding dengan operator BTS / station eksisting tersebut

3. Perhatikan berapa tingkat noise, bila mencapai lebih dari tingkat sensitifitas radio (biasanya adalah sekitar –83 dbm, baca spesifikasi radio), misalnya –100 dbm maka di titik station tersebut interferensinya cukup tinggi, tinggal apakah signal strenght yang diterima bisa melebihi noise
4. Perhitungan standar signal strenght adalah 0% – 40% poor, 40% – 60% good, 60% – 100% excellent, apabila signal strenght yang diterima adalah 60% akan tetapi noisenya mencapai 20% maka kondisinya adalah poor connection (60% – 20% – 40% poor), maka sedapat mungkin signal strenght harus mencapai 80%
5. Koneksi poor biasanya akan menghasilkan PER (packet error rate – bisa dilihat dari persentasi jumlah RTO dalam continous ping) diatas 3 % – 7% (dilihat dari utility Planet maupun Wave Rider), good berkisar antara 1% – 3 % dan excellent dibawah 1%, PER antara BTS dan station client harus seimbang
6. Perhitungan yang sama bisa dipergunakan untuk memperhatikan station lawan atau BTS kita, pada prinsipnya signal strenght, tingkat noise, PER harus imbang untuk mendapatkan stabilitas koneksi yang diharapkan
7. Pertimbangkan alternatif skenario lain bila sejumlah permasalahan di atas tidak bisa diatasi, misalkan dengan memindahkan station ke tempat lain, memutar arah pointing ke BTS terdekat lainnya atau dengan metode 3 titik (repeater) dll.

h. Perakitan Antena

1. Antena microwave jenis grid parabolic dan loop serta yagi perlu dirakit karena terdiri dari sejumlah komponen, berbeda dengan jenis patch panel, panel sector maupun omni directional
2. Rakit antena sesuai petunjuk (manual) dan gambar konstruksi yang disertakan
3. Kencangkan semua mur dan baut termasuk konektor dan terutama reflektor
4. Perhatikan bahwa antena microwave sangat peka terhadap perubahan fokus, maka pada saat perakitan antena perhatikan sebaik-baiknya fokus reflektor terhadap horn (driven antena), sedikit perubahan fokus akan berakibat luas seperti misalnya perubahan gain (db) antena
5. Beberapa tipe antena grid parabolic memiliki batang extender yang bisa merubah letak fokus reflektor terhadap horn sehingga bisa diset gain yang diperlukan

i. Pointing Antena

1. Secara umum antena dipasang dengan polarisasi horizontal
2. Arahkan antena sesuai arah yang ditunjukkan kompas dan GPS, arah ini kita anggap titik tengah arah (center beam)
3. Geser antena dengan arah yang tetap ke kanan maupun ke kiri center beam, satu per satu pada setiap tahap dengan perhitungan tidak melebihi ½ spesifikasi beam width antena untuk setiap sisi (kiri atau kanan), misalkan

antena 24 db, biasanya memiliki beam width 12 derajat maka, maksimum pergeseran ke arah kiri maupun kanan center beam adalah 6 derajat

4. Beri tanda pada setiap perubahan arah dan tentukan skornya, penentuan arah terbaik dilakukan dengan cara mencari nilai average yang terbaik, parameter utama yang harus diperhatikan adalah signal strenght, noise dan stabilitas
5. Karena kebanyakan perangkat radio Wireless In A Box tidak memiliki utility grafis untuk merepresentasikan signal strenght, noise dsb (kecuali statistik dan PER) maka agar lebih praktis, untuk pointing gunakan perangkat radio standar 802.11b yang memiliki utility grafis seperti Orinoco atau gunakan Wave Rider
6. Selanjutnya bila diperlukan lakukan penyesuaian elevasi antena dengan klino meter sesuai sudut antena pada station lawan, hitung berdasarkan perhitungan kelengkungan bumi dan bandingkan dengan kontur pada peta topografi
7. Ketika arah dan elevasi terbaik yang diperkirakan telah tercapai maka apabila diperlukan dapat dilakukan pembalikan polarisasi antena dari horizontal ke vertical untuk mempersempit beam width dan meningkatkan fokus transmisi, syaratnya kedua titik mempergunakan antena yang sama (grid parabolic) dan di kedua titik polarisasi antena harus sama (artinya di sisi lawan polarisasi antena juga harus dibalik menjadi vertical)

j. Pengujian Koneksi Radio

1. Lakukan pengujian signal, mirip dengan pengujian noise, hanya saja pada saat ini antena dan kabel (termasuk POE) sudah dihubungkan ke perangkat radio
2. Sesuaikan channel dan nama SSID (Network Name) dengan identitas BTS/AP tujuan, demikian juga enkripsinya, apabila dipergunakan otentikasi MAC Address maka di AP harus didefinisikan terlebih dahulu MAC Address station tersebut
3. Bila menggunakan otentikasi Radius, pastikan setting telah sesuai dan cobalah terlebih dahulu mekanismenya sebelum dipasang
4. Perhatikan bahwa kebanyakan perangkat radio adalah berfungsi sebagai bridge dan bekerja berdasarkan pengenalan MAC Address, sehingga IP Address yang didefinisikan berfungsi sebagai interface utility berdasarkan protokol SNMP saja, sehingga tidak perlu dimasukkan ke dalam tabel routing
5. Tabel routing didefinisikan pada (PC) router dimana perangkat radio terpasang, untuk Wireless In A Box yang perangkatnya terpisah dari (PC) router, maka pada device yang menghadap ke perangkat radio masukkan pula 1 IP Address yang satu subnet dengan IP Address yang telah didefinisikan pada perangkat radio, agar utility yang dipasang di router dapat mengenali radio
6. Lakukan continuos ping untuk menguji stabilitas koneksi dan mengetahui PER

7. Bila telah stabil dan signal strenght minimum good (setelah diperhitungkan noise) maka lakukan uji troughput dengan melakukan koneksi FTP (dengan software FTP client) ke FTP server terdekat (idealnya di titik server BTS tujuan), pada kondisi ideal average troughput akan seimbang baik saat download maupun up load, maksimum troughput pada koneksi radio 1 mbps adalah sekitar 600 kbps dan per TCP connection dengan MTU maksimum 1500 bisa dicapai 40 kbps
8. Selanjutnya gunakan software mass download manager yang mendukung TCP connection secara simultan (concurrent), lakukan koneksi ke FTP server terdekat dengan harapan maksimum troughput 5 kbps per TCP connection, maka dapat diaktifkan sekitar 120 session simultan (concurrent), asumsinya 5 x 120 = 600
9. Atau dengan cara yang lebih sederhana, digunakan skala yang lebih kecil, 12 concurrent connection dengan trouhput per session 5 kbps, apa total troughput bisa mencapai 60 kbps (average) ? bila tercapai maka stabilitas koneksi sudah dapat dijamin berada pada level maksimum
10. Pada setiap tingkat pembebanan yang dilakukan bertahap, perhatikan apakah RRT ping meningkat, angka mendekati sekitar 100 ms masih dianggap wajar

4.2.2. Konfigurasi Perangkat Wi-Fi

4.2.2.1. Access Point Linksys WAP54G

Dalam perancangan WLAN di Komplek PTJ ini menggunakan access point Linksys WAP54G dengan berbagai pertimbangan dan kebutuhan serta keadaan lokasi kemampuan coverage area dari hasil site survey.



Gambar 4.6. Access Point Linksys WAP54G

Spesifikasi lebih lengkap dari access point Linksys WAP54G dapat dilihat pada tabel 4.1.

4.2.2.2. Deskripsi Access Point Linksys WAP54G

Berikut ini adalah gambaran umum dan keterangan dari access point Linksys WAP54G yang digunakan untuk perancangan WLAN di komplek PTJ.

a. Panel Depan

Pada panel depan terdapat beberapa LED yang mengindikasikan aktivitas dan status dari access point, spesifikasi panel depan dapat dilihat pada tabel 4.2.



Gambar 4.7. Panel Depan AP Linksys WAP54G

b. Panel Belakang

Port Ethernet network, power, dan tombol reset terletak di panel belakang access point yang merupakan port interspaces antar perangkat, spesifikasi panel belakang dapat dilihat pada tabel 4.3.



Gambar 4.8. Panel Belakang AP Linksys WAP54G

Tabel 4.1. Spesifikasi AP Linksys WAP54G

Spesifikasi Linksys WAP54G	WAP54G
Standards	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u
Ports/Buttons	One 10/100 Auto-Cross Over (MDI/MDI-X) port, power port, reset and SES button
Cabling Type	RJ-45
LEDs	Power, Activity, Link, Secure Easy Setup
Transmit Power	802.11g: Typ. 13.5 +/- 2dBm @ Normal Temp Range 802.11b: Typ: 16.5 +/- 2dBm @ Normal Temp Range
Security Features	WPA, Linksys Wireless Guard, WEP Encryption, MAC Filtering SSID Broadcast enable/disable
WEP Key Bits	64/128-bit
Dimensions (W x H x D)	7.32" x 1.89" x 6.65" (186 mm x 48 mm x 169 mm)
Unit Weight	16.23 oz. (0.46 kg)
Power	External, 12V DC
Certifications	FCC

Tabel 4.2. Spesifikasi Panel Depan AP Linksys WAP54G

Spesifikasi Linksys WAP54G Model	Fungsi
Panel Depan (Logo Cisco)	Jingga/Putih. Logo Cisco adalah tombol Secure Easy Setup access point yang akan menyala bila access point dihidupkan. Logo Cisco berwarna jingga bila fitur Secure Easy Setup tidak digunakan, dan akan berwarna putih bila sedang digunakan. Tombol logo cisco juga dapat digunakan untuk mereset SSID dan WPA-PSK key dengan cara menekannya selama 10 detik.
Power	Merah. LED Power akan menyala bila access point dihidupkan (powered on).
Act	Hijau. LED Act akan menyala untuk mengindikasikan bahwa wireless siap digunakan. Dan akan berkedip bila ada transfer data (transmit atau receive).
Link	Jingga. LED Link akan menyala bila berhasil terhubung ke jaringan LAN. Dan akan berkedip bila ada transfer data yang melalui jaringan LAN.

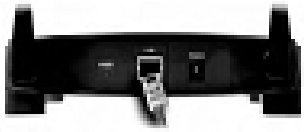
Tabel 4.3. Spesifikasi Panel Belakang AP Linksys WAP54G

Spesifikasi Linksys WAP54G Model	Fungsi
Panel Belakang LAN Port	Port ethernet network yang menghubungkan ke perangkat jaringan LAN seperti switch atau router.
Reset Button	Dengan menekan tombol reset ini selama 10 detik, maka seluruh konfigurasi access point akan terhapus dan kembali ke default.
Power Port	Port Power menghubungkan access point ke adaptor.

4.2.2.3. Menghubungkan Access Point ke Jaringan LAN

Langkah pertama yang harus dilakukan sebelum mengkonfigurasi access point adalah menghubungkan access point tersebut ke jaringan LAN yang ada. Berikut adalah langkah-langkahnya :

1. Hubungkan ujung kabel ethernet network ke switch atau router dan ujung yang satunya lagi ke port LAN yang ada di belakang access point



Gambar 4.9. Menghubungkan port LAN

2. Hubungkan power adapter ke port power access point



Gambar 4.10. Menghubungkan power adapter

Jika access point sudah menyala dan terhubung ke dalam jaringan LAN maka access point telah siap untuk dikonfigurasi.

4.2.2.4. Konfigurasi Access Point Menggunakan Setup Wizard

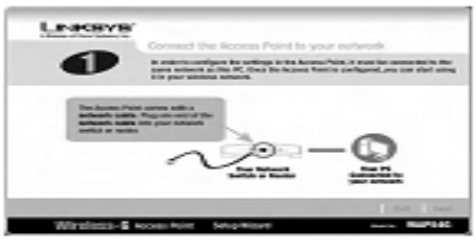
Untuk mengkonfigurasi access point bisa menggunakan komputer yang terhubung dalam satu jaringan LAN yang sama dengan access point tersebut. Cara termudah adalah dengan menggunakan Setup Wizard yang terdapat pada CD setup yang disertakan dalam produk tersebut. Langkah-langkah cara mengkonfigurasi access point dapat dijelaskan sebagai berikut :

1. Masukkan CD setup
2. Setelah itu akan muncul Welcome Screen Setup Wizard



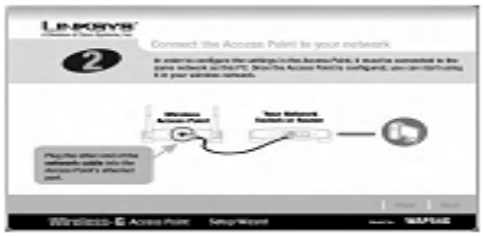
Gambar 4.11. Welcome Screen Setup Wizard AP

3. Untuk memulai konfigurasi tekan tombol Click Here to Start atau tombol Setup.
4. Pastikan jika ujung kabel ethernet network telah terhubung ke switch atau router pada jaringan LAN. Setelah itu tekan next.



Gambar 4.12. Menghubungkan AP ke Jaringan LAN

5. Pastikan juga jika ujung kabel ethernet network yang satu lagi telah tehubung ke port LAN yang terdapat pada access point. Kemudian tekan next.



Gambar 4.13. Menghubungkan ke port LAN Access Point

6. Lalu pastikan bahwa access point telah dihidupkan dengan menghubungkan kabel power adapter yang tersedia. Lalu tekan next.



Gambar 4.14. Menghubungkan Power Adapter Access Point

7. Periksa status access point dengan melihat lampu indikator yang terdapat pada panel depan access point. Bila LED indikator Power, Act dan Link sudah menyala, kemudian tekan next.



Gambar 4.15. Status Aktif Access Point

8. Setelah itu sistem akan mendeteksi access point yang terpasang pada jaringan, dan menampilkan nama dari access point tersebut di kolom sebelah kiri. Bila ada lebih dari satu access point yang terpasang pada jaringan silakan pilih access point yang akan dikonfigurasi, kemudian tekan next.



Gambar 4.16. Memilih Access Point yang Akan Dikonfigurasi

9. Masukkan password yang diminta. Secara default, password-nya adalah “admin”. Setelah itu tekan enter.



Gambar 4.17. Tampilan Password

10. Selanjutnya akan terlihat tampilan konfigurasi dasar secara default. Isikan Device Name, ubah password supaya aman, dan masukkan IP address. Bila telah diisi, lalu tekan next.



Gambar 4.18. Tampilan Konfigurasi Dasar AP

11. Berikut adalah tampilan konfigurasi untuk access point yang diletakkan di perpustakaan.



Gambar 4.19. Tampilan Konfigurasi Dasar Untuk Access Point

12. Setelah itu akan tampil pengaturan konfigurasi wireless



Gambar 4.20. Tampilan Pengaturan Konfigurasi Wireless

13. Masukkan konfigurasi SSID, Channel, dan Network Mode untuk jaringan wireless yang digunakan. Setelah itu tekan next.



Gambar 4.21. Konfigurasi SSID, Channel, dan Network Mode Access Point

14. Atur konfigurasi keamanan yang akan digunakan pada access point yang terpasang. Disini penulis men-disable pengaturan keamanannya. Jika telah dipilih kemudian tekan next.



Gambar 4.22. Tampilan Pengaturan Keamanan

15. Setelah konfigurasi selesai dilakukan, maka akan tampil layar konfirmasi yang akan menanyakan apakah konfigurasi tersebut akan disimpan. Bila sudah yakin silakan tekan Yes.



Gambar 4.23. Tampilan Konfirmasi Pengaturan

16. Lalu akan terlihat proses penyimpanan konfigurasi baru.



Gambar 4.24. Proses Penyimpanan Konfigurasi

17. Selanjutnya layar Congratulations akan tampil yang menandakan bahwa konfigurasi yang baru telah berhasil dilakukan.



Gambar 4.25. Tampilan layar Congratulations

4.2.3. Menghubungkan Komputer Client ke WLAN

Komputer client baik laptop maupun PC yang sudah terpasang wireless LAN card dapat terhubung ke dalam jaringan WLAN yang tersedia. Cara mengkoneksikannya pun cukup mudah. Berikut adalah caranya, menggunakan laptop dengan sistem operasi Windows XP, yaitu :

1. Pastikan bahwa wi-fi pada laptop dalam keadaan ON (aktif).
2. Klik kanan pada icon Network Wireless Connection pada taskbar, lalu pilih View Available Wireless Networks.



Gambar 4.26. Icon Wireless Network

3. Kemudian akan tampil Wireless Network Connection yang tersedia.
4. Pilih jaringan WLAN dengan sinyal yang paling baik, lalu klik Connect.



Gambar 4.27. Wireless Network Connection

5. Langkah selanjutnya adalah mengkonfigurasi alamat proxy pada browser yang digunakan.

4.2.4. Konfigurasi Proxy pada Browser

Agar jaringan dapat mengakses Internet maka harus melakukan konfigurasi alamat proxy terlebih dahulu pada browser yang digunakan.

4.2.4.1. Internet Explorer

Langkah untuk konfigurasi proxy pada browser Internet Explorer adalah sebagai berikut :

1. Masuk ke menu Tools
2. Pilih Internet Options
3. Pilih Connection
4. Pilih LAN Settings
5. Pilih Advanced, lalu masukkan konfigurasi proxy



Gambar 4.28. Konfigurasi Proxy Internet Explorer

4.2.4.2. Mozilla Firefox

Langkah untuk konfigurasi proxy pada browser Mozilla Firefox adalah sebagai berikut :

1. Masuk ke menu Tools
2. Pilih Options
3. Pilih Connection Setting
4. Lalu masukkan konfigurasi proxy



Gambar 4.29. Konfigurasi Proxy Mozilla Firefox

4.2.4.3. Opera

Langkah untuk konfigurasi proxy pada browser Opera adalah sebagai berikut :

1. Masuk ke menu Tools
2. Pilih Preferences
3. Pilih Advanced
4. Pilih Network
5. Pilih Proxy servers, lalu masukkan konfigurasi proxy



Gambar 4.30. Konfigurasi Proxy Opera

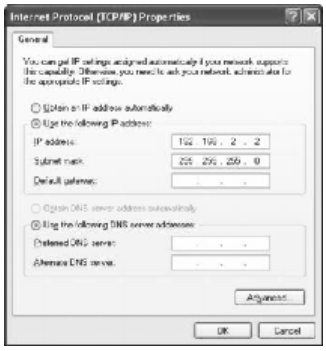
Jika semua konfigurasi telah dilakukan dengan benar, maka browser akan menampilkan SSO-TJ (Single Sign-On TJ), yang berarti bahwa jaringan komputer telah berhasil terhubung ke proxy dan bisa mengakses Internet. Tapi tentu saja harus memiliki sebuah account terlebih dahulu untuk bisa login ke dalam SSO-TJ ini.

4.3. Pengujian Jaringan Wi-Fi

Setelah proses penyetingan dan konfigurasi telah dilakukan dengan baik, sebelum menggunakan jaringan wireless sebagai media penghubung antar jaringan atau antar wireless station, terlebih dahulu harus dilakukan pengujian atau testing jaringan.

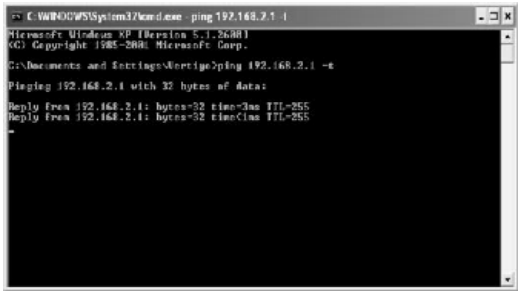
Langkah-langkah pengujian jaringan wireless atau Access point adalah sebagai berikut :

1. Setting komputer yang akan dipakai untuk pengujian Access Point agar IP Address komputer tersebut sekelas dengan Access Point. Karena IP Address Default dari Access Point adalah 192.168.2.1/24, maka IP Address Komputer di setting sekelas dengan IP Address Access Point yaitu 192.168.2.2/24.



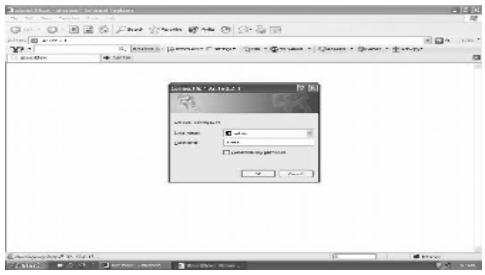
Gambar 4.31. Konfigurasi Setting IP Address

2. Kemudian melakukan tes koneksi dengan Access Point dengan cara melakukan perintah “ping” ke IP Address dari Access Point. Apabila muncul tulisan Reply from 192.168.2.1 berarti koneksi komputer dengan Access Point berhasil dan dilanjutkan tes ping untuk 192.168.2.2.



Gambar 4.32 Tes Ping ke IP Address Default Access Point

3. Kemudian mengakses IP Address dari Access Point tersebut menggunakan web browser yang ada dan melakukan login dengan username dan password default yang sudah ada dibuku manual AP



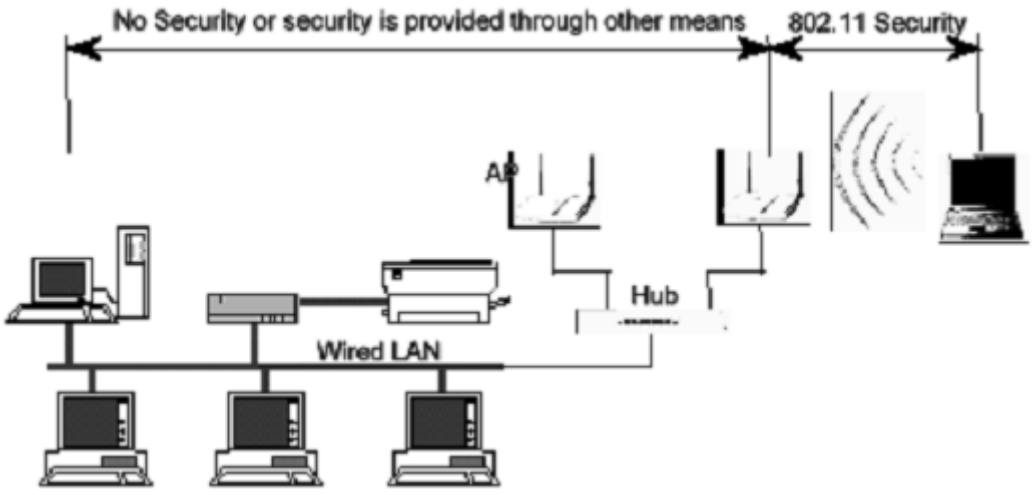
Gambar 4.33. Login untuk melakukan konfigurasi Access Point

4. Setelah melakukan login dengan benar, kemudian memilih Basic Setting pada untuk memilih mode dari Access Point yang akan digunakan, memilih Spesifikasi dan Frekuensi Band dan setting ESSID. Setelah semua setting selesai, pilihan Apply untuk proses saving. Kemudian siap melakukan tes koneksi dengan Access Point Client dan Access Point Server dengan melakukan ping ke IP Address dari masing-masing Access Point tersebut.

5. Jika hasil tes ping menunjukkan tampilan tulisan, misalnya : Reply from 192.168.2.11 dan Reply from 192.168.2.1, berarti kedua Access Point yang sudah disetting berhasil dan siap untuk digunakan sebagai media penghubung.
6. Selanjutnya lakukan juga tes ping IP Address media penghubung lainnya sesuaikan dengan jenis kelas IP dan urutan host atau clientnya, dan jaringan wireless siap untuk di akses dengan baik (internet hotspot).

4.4. Keamanan Wi-Fi Hotspot

Spesifikasi IEEE 802.11 menunjukkan beberapa layanan yang menyediakan lingkungan operasi yang aman. Layanan keamanan disediakan sebagian besar oleh protocol Wired Equivalent Privacy (WEP) untuk melindungi link level data selama transmisi wireless antara klien dan access point. WEP tidak menyediakan keamanan end-to-end, tapi hanya untuk bagian wireless dari koneksi seperti ditunjukkan pada Gambar 4.34.



Gambar 4.34. Sistem Keamanan Wi-Fi 802.11

Fitur Keamanan Wi-Fi 802.11

Tiga layanan kemanan dasar yang ditentukan oleh IEEE untuk lingkungan WLAN (WiFi Hotspot) adalah sebagai berikut :

1. Otentifikasi

   Tujuan utama dari WEP adalah menyediakan layanan keamanan untuk memastikan identitas lokasi klien yang berkomunikasi. Ini menyediakan kontrol bagi jaringan dengan menolak akses ke stasion klien yang tidak dapat memberika otentifikasi secara benar. Layanan ini menangani pertanyaan, ”Apakah hanya orang-orang yang berhak yang diijinkan untuk mendaptkan akses ke jaringan saya ?”

2. Kerahasiaan

   Kerahasiaan, atau privasi, adalah tujuan kedua WEP. Ini dibuat untuk menyediakan “privasi yang diperoleh pada jaringan kabel.” Maksudnya adalah untuk mencegah bocornya informasi dengan cara menguping (serangan pasif). Layanan ini, secara umum, menangani pertanyaan,”Apakah hanya orang-orang yang berhak yang diijinkan melihat data saya ?”

3. Integritas

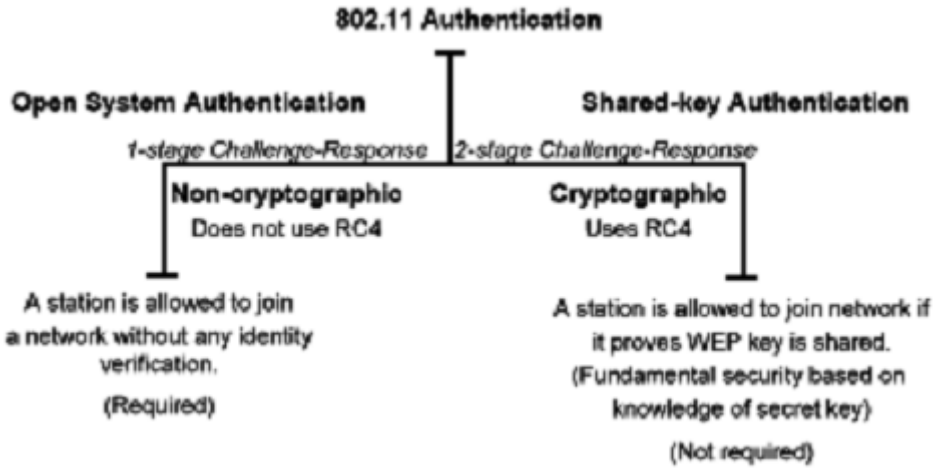
   Tujuan lain dari WEP adalah layanan keamanan yang dibuat untuk memastikan bahwa pesan tidak dirubah sewaktu pengiriman antara klien wireless dan access point dalam serangan aktif. Layanan ini menangani pertanyaan, ”Apakah data yang datang ke jaringan atau keluar jaringan dapat dipercaya ? Apakah data ini telah dirusak ?”

Penting untuk dicatat bahwa standar tidak menangani layanan keamanan lain seperti audit, otorisasi, dan pengakuan.

Otentifikasi

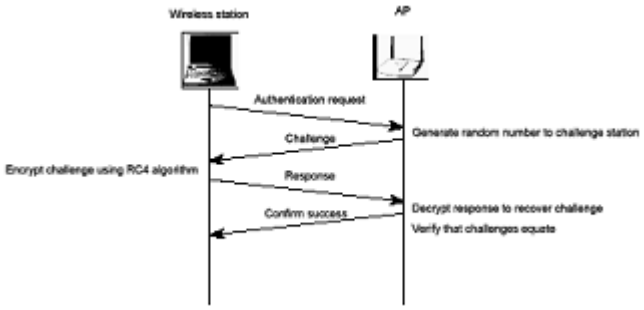
Spesifikasi IEEE 802.11 menentukan dua cara untuk memvalidasi pengguna wireless yang mencoba untuk mendapatkan akses ke jaringan kabel, yaitu otentifikasi open-system dan otentifikasi shared-key.

Otentifikasi shared-key didasarkan pada kriptografi, dan yang lainnya tidak. Teknik otentifikasi open-system bukan benar-benar otentifikasi, access point menerima stasion bergerak tanpa memverifikasi identitas stasion. Harus juga dicatat bahwa otentifikasi hanya satu arah yaitu hanya stasion bergerak yang di otentifikasi. Stasion bergerak harus percaya bahwa sistem sedang berkomunikasi dengan AP nyata. Sistem klasifikasi (taksonomi) teknik ini untuk 802.11 digambarkan pada gambar 4.35.



Gambar 4.35. Taksonomi Teknik Otentifikasi 802.11

Dengan otentifikasi open system, klien diotentifikasi jika dapat merespon dengan alamat MAC selama keduanya bertukar pesan dengan access point. selama pertukaran, klien tidak divalidasi tapi hanya merespon dengan kolom yang benar pada saat pertukaran pesan. Nyatanya, tanpa validasi kriptografis, otentifikasi open-system sangat rentan terhadap serangan dan mengundang akses yang tidak berhak. Otentifikasi open-system adalah satu-satunya bentuk otentifikasi yang dibutuhkan oleh spesifikasi 802.11.



Gambar 4.36. Aliran Pesan Otentifikasi Shared-key

Otentifikasi shared-key adalah teknik kriptografis untuk otentifikasi. Ini adalah skema “challenge-response” sederhana berdasarkan pada apakah klien mempunyai pengetahuan tentang rahasia shared. Pada skema, seperti digambarkan pada gambar 4.36., teguran acak dihasilkan oleh access point dan dikirimkan ke klien wireless. Klien, dengan menggunakan kunci kriptografis yang di shared dengan AP, mengenkrip teguran ini (atau disebut “nonce” dalam bahasa keamanan) dan mengembalikan hasilnya ke AP. Kemudian AP mendekrip hasil yang dikirimkan oleh klien dan memungkinkan akses hanya jika nilai yang didekrip sama dengan teguran acak yan dikirimkan. Algoritma yang digunakan

dalam perhitungan kriptografi dan untuk pembuatan teks teguran 128 bit adalah RC4 stream chipher yang dibuat oleh Ron Rivest dari MIT. Harus dicatat bahwa metoda otentifikasi yang dijelaskan diatas adalah teknik kriptografi yang belum sempurna, dan ini tidak menyediakan otentifikasi dua arah. Yaitu, klien tidak mengotentifikasi AP, dan karena itu tidak ada keyakinan bahwa klien sedang berkomunikasi dengan AP dan jaringan wireless yang sah. Juga penting dicatat bahwa skema challenge-response sepihak dan sederhana diketahui lemah. Hal ini mengalami banyak serangan dari user yang tidak berpengalaman. Spesifikasi IEEE 802.11 tidak memerlukan otentifikasi shared-key.

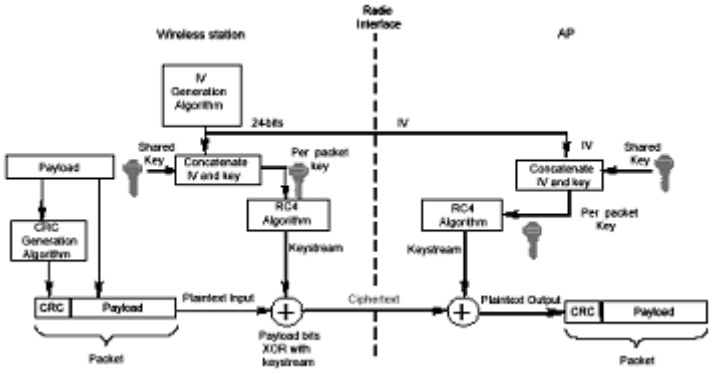
Privasi

Standar 802.11 mendukung privasi (kerahasiaan) melalui penggunaan teknik kriptografis untuk interface wireless. Teknik kriptografis WEP untuk kerahasiaan juga menggunakan algoritma RC4 symmetric-key, stream chipper untuk membuat urutan data semi acak. “Key stream” ini cukup dengan ditambah modulo 2 (eksklusif OR) ke data yang akan dikirmkan. Melalui teknik WEP, data dapat dilindungi dari pengungkapan selama pengiriman melalui hubungan wireless. WEP diterapkan ke semua data diatas lapisan WLAN 802.11 untuk melindungi lalulintas seperti Transmission Control Protocol/Internet Protocol (TCP/IP), Internet Packet Exchange (IPX), dan Hyper Text Transfer Protocol (HTTP).

Seperti ditentukan pada standar 802.11, WEP mendukung hanya ukuran kunci kriptografis 40 bit untuk shared key. Tapi, banyak vendor menawarkan

ekstensi WEP yang tidak standar yang mendukung panjang key dari 40 bit hingga 104 bit. Setidaknya satu vendor mendukung ukuran key 128 bit. Kunci WEP 104 bit, misalnya, dengan Initialization Vector (IV) 24 bit menjadi key RC4 128 bit. Secara umum, semuanya sama, kenaikan ukuran key meningkatkan keamanan dari teknik kriptografis. Tapi, selalu dimungkinkan bahwa kekurangan penerapan atau kekurangan rancangan menjadikan key yang panjang menurun keamanannya. Penelitian telah menunjukkan bahwa ukuran key lebih besar dari 80 bit, membuat pemecahan kode menjadi hal yang tidak mungkin.

Untuk key 80 bit, jumlah key yang mungkin dengan ruang key lebih dari 10-melampaui daya perhitungan. Pada pelaksanaannya, sebagian besar penggunaan WLAN tergantung pada key 40 bit. Lebih lanjut, serangan baru-baru ini telah menunjukkan bahwa pendekatan WEP untuk privasi rentan terhadap serangan tertentu tanpa memandang ukuran key. Tapi, komunitas standar kriptografis dan vendor WLAN telah membuat WEP yang telah ditingkatkan, yang tersedia sebagai penerapan pra standar vendor tertentu. Privasi WEP digambarkan secara konsep pada gambar 4.37.



Gambar 4.37. Privasi WEP Menggunakan Algoritma RC4

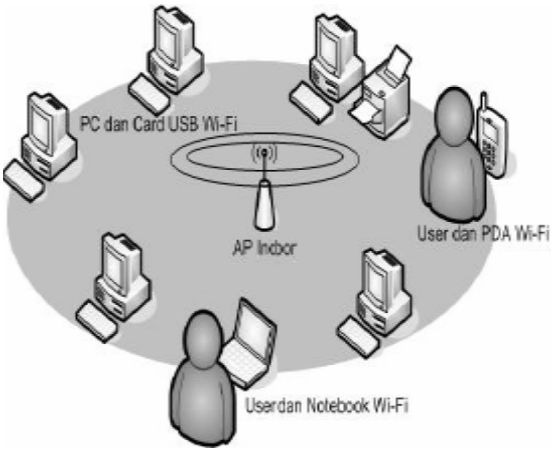
Integritas

Spesifikasi IEEE 802.11 juga menguraikan alat untuk menyediakan integritas data pada pesan yang dikirimkan antara klien wireless dan access point. Layanan keamanan ini dirancang untuk menolak setiap pesan yang telah dirubah oleh musuh aktif “ditengah”. Teknik ini menggunakan pendekatan Cyclic Redundancy Check terenkripsi sederhana. Seperti digambarkan pada Gambar 4.37. CRC-32, atau urutan pengecekan frame, dihitung pada masing-masing payload sebelum transmisi. Paket yang dibungkus integritas kemudian dienkripsi menggunakan key stream RC4 untuk menyediakan cipher-text message. Pada bagian penerima, dekripsi dilakukan dan CRC dihitung ulang pada pesan yang diterima. CRC yang dihitung pada bagian penerima dibandingkan dengan yang dihitung pada pesan asli. Jika CRC tidak sama, yaitu, “diterima dengan kesalahan”, ini akan mengindikasikan pelanggaran integritas dan paket akan dibuang. Seperti dengan layanan privasi, integritas 802.11 rentan terhadap serangan tertentu tanpa memandang ukuran kunci. Kekurangan mendasar dalam skema integritas WEP adalah CRC sederhana bukan mekanisme aman secara kriptografis seperti hash atau kode otentifikasi pesan. Sayangnya, spesifikasi IEEE 802.11 tidak menentukan alat apapun untuk manajemen key (penanganan daur hidup dari key kriptografis dan materi terkait). Oleh karena itu, pembuatan, pendistribusian, penyimpanan, loading, escrowing, pengarsipan, auditing, dan pemusnahan materi itu diserahkan pada WLAN yang dipakai. Manajemen key pada 802.11 diserahkan sebagai latihan bagi pengguna jaringan 802.11. Sebagai hasilnya, banyak kerentanan dapat dimasukkan ke lingkungan WLAN.

Kerentanan ini termasuk kunci WEP yang tidak unik, tidak pernah berubah, default pabrik, atau kunci lemah (semua nol, semua satu, berdasarkan pada password yang mudah ditebak, atau pola-pola lain yang mudah). Sebagai tambahan, karena manajemen key bukan merupakan bagian dari spesifikasi 802.11 asli, karena distribusi key tidak terselesaikan, maka WLAN yang diamankan dengan WEP tidak terjaga dengan baik. Jika sebuah perusahaan mengetahui kebutuhan untuk sering merubah key dan membuatnya acak, maka ini merupakan tugas berat pada lingkungan WLAN yang besar. Sebagai contoh, kampus besar bisa mempunyai AP sebanyak 15.000. Pembuatan, pendistribusian, loading, dan pengaturan key untuk lingkungan seukuran ini merupakan tantangan yang cukup berat. Sudah disarankan bahwa satu-satunya cara untuk mendistribusikan key pada lingkungan dinamis yang besar adalah dengan mengumumkannya. Tapi, teknet kriptografi dasar adalah bahwa key kriptografis tetap rahasia. Karena itu mempunyai dikotomi, dikotomi ini ada untuk setiap teknologi yang menolak untuk menangani masalah distribusi key.

4.5. Internet Hotspot

Hotspot adalah lokasi dimana user dapat mengakses melalui mobile computer (seperti laptop atau PDA) tanpa menggunakan koneksi kabel dengan tujuan suatu jaringan seperti internet. Jaringan nirkabel menggunakan radio frekuensi untuk melakukan komunikasi antara perangkat komputer dengan akses point dimana pada dasarnya berupa penerima dua arah yang bekerja pada frekuensi 2.4 GHz (802.11b, 802.11g) dan 5.4 GHz (802.11a).



Gambar 4.38. Internet Hotspot Area

Pada umumnya peralatan Wi-Fi Hotspot menggunakan standarisasi IEEE 802.11b atau IEEE 802.11g dengan menggunakan beberapa level keamanan seperti WEP dan/atau WPA. Perangkat laptop sudah banyak yang dilengkapi dengan adapter IEEE 802.11b atau IEEE 802.11g. Akan tetapi dapat juga digunakan peralatan wireless dalam bentuk PCMCIA atau USB.

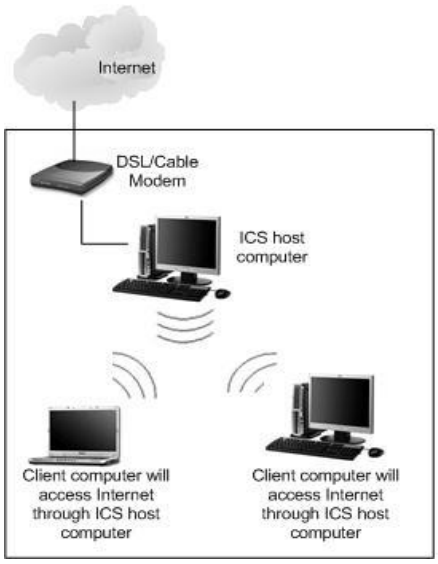
Internet (*Inter-Network*) adalah sebutan untuk sekumpulan jaringan komputer yang menghubungkan situs akademik, pemerintahan, komersial, organisasi, maupun perorangan. Internet menyediakan akses untuk layanan telekomnunikasi dan sumber daya informasi untuk jutaan pemakainya yang tersebar di seluruh dunia. Layanan internet meliputi komunikasi langsung (email, chat), diskusi (Usenet News, email, milis), sumber daya informasi yang terdistribusi (World Wide Web, Gopher), remote login dan lalu lintas file (Telnet, FTP), dan aneka layanan lainnya.

Jaringan yang membentuk internet bekerja berdasarkan suatu set protokol standar yang digunakan untuk menghubungkan jaringan komputer dan

mengalamati lalu lintas dalam jaringan. Protokol ini mengatur format data yang diijinkan, penanganan kesalahan (*error handling*), lalu lintas pesan, dan standar komunikasi lainnya. Protokol standar pada internet dikenal sebagai TCP/IP (*Transmission Control Protocol / Internet Protocol*). Protokol ini memiliki kemampuan untuk bekerja diatas segala jenis komputer, tanpa terpengaruh oleh perbedaan perangkat keras maupun sistem operasi yang digunakan.

Sebuah sistem komputer yang terhubung secara langsung ke jaringan memiliki nama domain dan alamat IP (*Internet Protocol*) dalam bentuk numerik dengan format tertentu sebagai pengenal. Internet juga memiliki gateway ke jaringan dan layanan yang berbasis protokol lainnya.

Dalam komunikasi internet secara wireless, sistem akses internet hotspot seperti ditunjukkan pada Gambar 4.39.



Gambar 4.39. Sistem Komunikasi Wireless Internet

Wireless internet merupakan koneksi internet yang menggunakan frekuensi radio dan bekerja pada kecepatan tinggi yaitu 11–54 Mbps, jauh lebih cepat dari pada layanan internet melalui telepon (kabel) yang hanya kecepatan maksimum 56 Kbps (milik telkom). Pemakaian wireless internet memungkinkan akses internet selama 24 jam dengan biaya sangat murah karena wireless internet tidak akan dikenakan pulsa, sehingga pemakai hanya digunakan biaya pembayaran kepada Internet Service Provider (ISP) saja.

4.6. Rencana Pengembangan Teknologi Wi-Fi

4.6.1. Pengembangan Jangkauan Area Hotspot dengan Wajanbolik

Teknik yang paling hemat dan sederhana untuk dapat menambah jangkauan wireless LAN (hotspot area) adalah dengan memanfaatkan antena outdor buatan sendiri, yaitu yang biasa disebut wajanbolic. Dalam teknik pembuatan wajan bolik dapat menggunakan wajanbolic hasil buatan e-goen.

Teknik wajanbolic e-goen (http://pg.photos.yahoo.com/) sangat kreatif dengan menggunakan USB WLAN, yang dimasukkan ke antenna kaleng, dan dt-extend kabel USB-nya menggunakan ka-bel UTP dan sebuah wajan sebagai reflector.

Detail material yang dibutuhkan untuk membuat waianbolic e-goen adalah:

a. Tutup panci atau wajan penggorengan yang cukup besar dengan diameter 70+ cm (lebih besar daya pancarnya lebih baik daya tangkapnya).
b. USB

c. Tutup pralon 1": 1 buah.

d. Baut besar:1buah.

e. Baut kecil:1buah.

f. Aluminum tape, untuk melapisi pralon 3" yg dipakai buat feeder

g. Rubber Tape, untuk menutup pipa listrik

h. Pipa listrik yg kecil (diameter 1 cm), untuk pelindung sambungan kabel UTP.

i. Hardware yang butuhkan:

    1. USB WLAN
    2. USB 2.0 Extender
    3. Pipa Pralon 3" untuk feeder

Beberapa ukuran yang perlu di perhatikan dalam pembuatan wajanbolic adalah sebagai berikut:

a. Untuk wajan dengan kedalaman 20 cm, diameter 70 cm, maka titik fokus parabola kira-kira berada pada 15,3 cm. Untuk wajan yang berbeda ukuran diameternya maka titik fokus akan berbeda.

b. Panjang pralon 3" yang harus ditutup rubber tape adalah 25cm

c. Total panjang pralon 3" yang dibutuhkan adalah panjang fokus ditambah pralon yang ditutup rubber tape, jadi total sekitar 41 cm. Titik fokus lebih kritis, jadi harus tepat di 15,3 cm, sementara rubber tape tidak kritis, jadi dapat lebih panjang.

d. Posisi lubang untuk USB WLAN di pralon 3" adalah 8.3 cm dari ujung pralon yang ber-rubber tape.

File spreadsheet untuk menghitung berbagai dimensi ant€na ini dapat diambil di http://www.telkomspeedy.com. Gain antena wajanbolic e-goen ini cukup tinggi, sekitar 21-23dBi, dapat digunakan untuk menyambungkan sebuah rumah ke access point wireless dalam jarak 2-3 km dengan relatif mudah.

4.6.2. Pengembangan Teknologi Wi-Fi ke Wimax

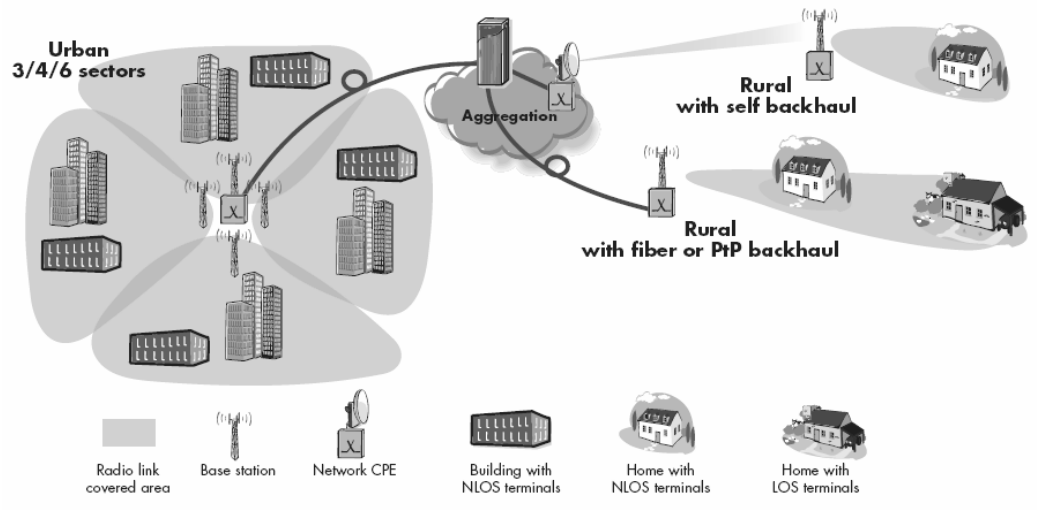
Sekarang ini, penggunaan teknologi wireless atau jaringan tanpa kabel (nirkabel) dirasa cukup efektif dan efisien untuk mencukupi kebutuhan masyarakat akan akses internet maupun kebutuhan lainnya. Untuk itu, salah satu teknologi berbasis wireless yang cukup berhasil dikembangkan adalah WiFi (Wireless Fidelity). Teknologi WiFi ini menggunakan standar IEEE 802.11 dan ETSIHiperLAN. Akan tetapi karena kebutuhan masyarakat, khususnya dunia pendidikian (Komplek PTJ) yang semakin bertambah, khusunya kebutuhan akan akses internet dan ditunjang dengan semakin berkembangnya dunia teknologi, maka teknologi WiFi mulai dirasa kurang dapat memenuhi kebutuhan tersebut. Hal ini dikarenakan ditemukannya beberapa kekurangan pada teknologi WiFi tersebut.

Untuk itu, ditemukan teknologi baru berbasis wireless juga yang mirip dengan Wi-Fi dan juga merupakan pengembangan dari teknologi Wi-Fi. Teknologi tersebut adalah teknologi WiMax (Worldwide Interoperability for Microwave Access). Teknologi WiMax menggunakan standar IEEE 802.16 dan ETSIHiperMAN. Dengan segala keunggulan yang dimilikinya, diharapkan

teknologi WiMax ini dapat memberikan manfaat bagi semua orang khususnya masyarakat Indonesia, dimana teknologi ini masih dalam tahap pembangunan di Indonesia.

Dan khususnya lembaga pendidikan dibawah naungan Yayasan Pendidikan Triple “J” (Komplek PTJ) yang komitmen dengan pengembangan dibidang teknologi pendidikan akan terus berupaya untuk bisa berperan aktif dalam memberdayakan dan memasyarakatkan Ilmu Pengetahuan dan Teknologi (IPTEK) khususnya Teknologi Informasi dan Komunikasi dalam hal ini Teknologi Nirkabel (Wi-Fi dan Wimax).

Menurut James A. Johnson (Vice President, Intel Communications Group/General Manager, Wireless Networking Group), istilah WiMax berasal dari singkatan wireless (disingkat Wi) Microwave Access (disingkat MAX). WiMax menyerupai Wi-Fi dalam hal penggunaan teknologi modulasi yang sama. Teknologi ini disebut OFDM (Orthogonal Frequency Division Multiplexing). OFDM merupakan sebuah sistem modulasi digital di mana sebuah sinyal dibagi menjadi beberapa kanal dengan pita frekuensi yang sempit dan saling berdekatan, dengan setiap kanal menggunakan frekuensi yang berbeda. Teknologi tersebut dikembangkan dalam tahun 1960-an - 1970-an. Teknologi ini dikembangkan pada saat dilakukannya penelitian untuk mengurangi terjadinya interferensi frekuensi di antara berbagai kanal yang jaraknya saling berdekatan.



Gambar 4.40. Sistem Komunikasi WiMax

Pada frekuensi non-WiMax, sebuah gelombang radio biasanya akan saling mengganggu gelombang radio lain, khususnya jika frekuensi tersebut memiliki siklus getaran yang berdekatan. Jadi apabila frekuensi yang dipakai untuk membawa data (carrier) seperti pada komunikasi data nirkabel mengalami hal yang demikian, gangguan tersebut bias menimbulkan aneka kerugian, seperti terjadinya kerusakan data yang dibawa frekuensi tersebut, terjadinya kegagalan pengiriman data, atau terjadinya kesalahan dalam pengalihan data. Namun, dengan adanya teknologi baru, yaitu teknologi WiMax, maka semua kendala tersebut akan dapat ditangani.

Teknologi WiMax memungkinkan kita memancarkan berbagai sinyal dalam jarak yang sangat berdekatan, tanpa harus cemas bahwa aneka sinyal tersebut akan saling mengganggu/berinterferensi. Dengan demikian, kita bias menumpangkan lalu lintas data dengan kepadatan tinggi dalam berbagai kanal tersebut. Dengan banyaknya kanal yang bisa ditumpangi oleh data yang berlimpah

dalam satu waktu, ISP atau penyedia layanan broadband bisa menghadirkan layanan berbasis kabel atau DSL untuk banyak pelanggan sebagai ganti media kabel tembaga.

WiMax juga merupakan penggabungan antara standar IEEE 802.16 dengan standar ETSI HiperMAN. Kedua standar yang disatukan ini merupakan standar teknis yang memiliki spesifikasi yang sangat cocok untuk menyediakan koneksi berjenis broadband lewat media wireless atau BWA. Jadi di masa mendatang, segala sesuatu yang berhubungan dengan teknologi BWA mungkin saja akan diberi semacam sertifikat WiMax seperti halnya Wi-Fi untuk perangkat wireless LAN. WiMax digunakan untuk jaringan yang luas, yaitu wireless MAN (WMAN).

Meskipun WiMax maupun Wi-Fi menggunakan salah satu frekuensi tidak berlisensi (yakni frekuensi 5,8GHz), akan tetapi WiMax juga diarahkan untuk bisa memanfaatkan dua frekuensi lain yang berlisensi, yakni 2,5GHz and 3,5GHz. Hal ini memungkinkan meningkatkan daya keluaran perangkat WiMax sehingga bisa menjangkau jarak yang lebih jauh. Dengan demikian, WiMax bisa beroperasi pada kisaran kilometer. Selain itu, WiMax dirancang dalam tataran teknologi carrier-grade. Hal ini membuat WiMax memiliki kehandalan dan kualitas pelayanan yang lebih baik dibandingkan Wi-Fi. Dengan jangkauan jarak yang lebih jauh, dan kemampuan untuk melewati aneka penghalang seperti gedung atau pohon, WiMax sesuai untuk diterapkan di daerah perkotaan yang memiliki gedung perkantoran dan pemukiman. Perhatikan Tabel 4.4. tentang perbedaan Teknologi Wi-Fi dan WiMax.

Tabel 4.4. Perbedaan Teknologi Wi-Fi dan WiMax

Perbedaan	IEEE 802.11 Wi-Fi	IEEE 802.16 WiMax	Perbedaan Teknis
Jarak	Dibawah 9 Km	Hingga 50 Km signalingnya menciptakan	Teknik 256 FFT sistem signalingnya menciptakan fitur ini.
Coverage	Optimal jika bekerja di dalam ruangan	Dirancang untuk penggunaan diluar ruangan dengan kondisi NLOS	IEEE 802.16 memiliki sistem gain yang lebih tinggi, mengakibatkan sinyal lebih kebal terhadaphalangan dalam jarak yang lebih jauh.
Skalabilitas	Skala penggunaannya hanya dalam tingkat LAN. Ukuran frekuensi kanalnya dibuat fix (20 MHz)	Dibuat untuk mendukung sampai 100 pengguna. kuran frekuensi kanal dapat bervariasi mulai dari 1,5 sampai dengan 20 MHz.	Sistem TDMA dan pengaturan slot komunikasi, sehingga semua frekuensi yang termasuk dalam range IEEE 802.16 dapat dipakai serta jumlah pengguna dapat bertambah.
Bit Rate	2,7 bps/Hz hingga 54Mbps dalam kanal 20 MHz Teknik modulasi yang lebih canggih disertai koreksi error lebih fleksibel, sehingga penggunaan frekuensi kanal lebih effisien.	5 bps/Hz hingga 100 Mbps dalam kanal 20 MHz.	Teknik modulasi yang lebih canggih disertai koreksi error yang lebih fleksibel, sehingga penggunaan frekuensi kanal lebih effisien.
QoS	Tidak mendukung QoS	QoS dibuat dalam layer MAC	Adanya pengaturan secara otomatis terhadap slot-slot TDMA, sehingga dimanfaatkan untuk peng-aturan QoS.