

BAB II

KOMUNIKASI WIRELESS

2.1. Media Wifi Radio

Wireless menggunakan *unguided medium* untuk menyampaikan suatu data, pada umumnya udara namun ada juga yang melewatkan datanya melalui *medium* air. Ada 2 metode yang digunakan oleh *Wireless* untuk menyampaikan data, yaitu:

1. *Infra Red* (IR)
2. *Radio Frequency* (RF)

IR adalah metode yang mudah di-implementasikan, tidak ada regulasi pemerintah yang mengatur penggunaannya sehingga IR tidak memerlukan ijin. IR bisa digunakan dalam 3 cara yaitu:

1. *Direct Beam* – *Sender* langsung diarahkan ke *receiver*.
2. *Omnidirectional* – *Sender* mengirimkan sinyal infra ke kolektor untuk kemudian dipantulkan ke *receiver*.
3. *Diffused* – Sinyal infra dari sebuah *Sender* akan dipantulkan oleh kolektor ke semua *node* dalam jangkauan.

IR tidak mampu memberikan mobilitas yang memadai bagi penggunaannya, ada batasan-batasan yang menghambat penggunaan IR yaitu: pemisah ruangan dan adanya cahaya lain.

Gelombang yang digunakan oleh metode RF adalah *Microwave*. *Microwave Band* dibagi menjadi 3 bagian yaitu:

1. 902 – 928 MHz (915 MHz *Band*)
2. 2.4 – 2.4835 GHz (2.4 GHz *Band*)

3. 5.725 – 5.825 GHz (5.8 GHz Band)

Di Amerika Serikat, ketiga *Band* diatas memerlukan lisensi kecuali penggunaan untuk ISM (Industrial, Scientific dan Medical) dengan daya hingga 1 Watt. Di Indonesia regulasi belum diatur kecuali untuk *Band* 915MHz yang biasa digunakan untuk telepon selular.

Banyak peralatan yang beroperasi pada *Band* sekitar 900MHz yaitu: telepon selular, telepon *Cordless*, mikrofon *Wireless* dan radio amatir; sehingga banyak gangguan pada *Band* ini. *Band* 2.4GHz dimanfaatkan oleh lebih sedikit peralatan, yang umum adalah oven *Microwave*. Pada *Band* 5.8GHz, hampir tidak ada saingan kecuali *Wireless LAN* lain yang beroperasi di *Band* ini. Jadi *Band* 900MHz akan lebih banyak mengalami gangguan dari *Band* 2.4GHz dan *Band* 2.4GHz akan lebih banyak mengalami gangguan dari *Band* 5.8GHz.

2.2. Standarisasi Wireless Lan

Sebelum lebih jauh berbicara mengenai Wireless LAN, ada baiknya dikenal dahulu beberapa standar Wireless LAN yang beredar saat ini. Beberapa standar yang dikenal dan diterapkan pada produk – produk Wireless LAN saat ini adalah 802.11a, 802.11b, dan 802.11g. Dalam sejarah dan perkembangannya, standarisasi Wireless LAN dimulai dengan standar 802.11. Standar ini dicetuskan tahun 1997 oleh IEEE (Institute of Electrical and Electronic Engineers). Kecepatan transfer data pada standar 802.11 adalah sekitar 2 Mbps. Selanjutnya pada tahun 1999 muncul 2 standar baru untuk teknologi ini, yakni standar 802.11a dan 802.11b.

Perbedaan antara standar 802.11a dan 802.11b terletak pada frekuensi radio tempat standar ini bekerja dan pada kecepatan transfer datanya. 802.11a bekerja pada frekuensi radio 5,15 dan 5,875 GHz. Kecepatan transfer data pada 802.11a mencapai 54 Mbps.

Namun pemanfaatan standar ini tidak terlalu menggembirakan, karena sedikitnya produk yang mengadopsi teknologi dengan standar ini.

Berbeda dengan standar 802.11a, standar 802.11b justru lebih banyak dipakai. 802.11b bekerja pada frekuensi radio 2,4 GHz, namun sayangnya kecepatan transfer data pada 802.11b hanya 11 Mbps. Jauh dibawah standar 802.11a.

Pada tahun 2003 muncul lagi standar baru yang menggabungkan kemampuan 802.11a dan 802.11b. Standar ini diberi nama 802.11g yang bekerja pada frekuensi radio yang sama dengan 802.11b dan kecepatan transfer data mencapai 54 Mps, sama dengan standar 802.11a. Sampai saat ini standar 802.11b dan 802.11g merupakan standar yang paling banyak digunakan. Hampir semua produk Wireless LAN menggunakan kedua standar ini. Bahkan 802.11g digunakan sebagai standar umum pada komputer jinjing (laptop) yang dilengkapi dengan teknologi wireless. Untuk lebih jelasnya, bisa melihat perbedaan masing – masing standar pada tabel ini :

Tabel 2.1. 802.11x protokol

Standar	802.11b	802.11g	802.11a
Kompatibilitas	IEEE 802.11b	IEEE 802.11b dan 802.11g	IEEE 802.11b
Frekuensi	2,4 GHz	2,4 GHz	5 GHz
Data rate	11,5,5,2 dan 1 Mbps	54, 48, 36, 24, 18, 12, 9 dan 6 Mbps	54, 48, 36, 24, 18, 12, 9 dan 6 Mbps
Jumlah Channel	3 non-overlapping	3 non-overlapping	8 non-overlapping
Jangkauan dalam ruangan	30 m @ 11 Mbps; 91 m @ 1 Mbps	30 m @ 54 Mbps; 91 m @ 1 Mbps	12 m @ 54 Mbps; 91 m @ 6 Mbps
Jangkauan diuar ruangan	120 m @ 11 Mbps; 460 m @ 1 Mbps	120 m @ 54 Mbps; 460 m @ 1 Mbps	30 m @ 54 Mbps; 305 m @ 6 Mbps
Modulasi & Frekuensi	Direct sequence Spread	Orthogonal Frequency Division Multiplexing	Orthogonal Frequency Division Multiplexing
Kelebihan	Biaya Murah	Data rate tinggi dan biaya murah	Data rate tinggi

2.3. Sistem Kerja Wireless Lan

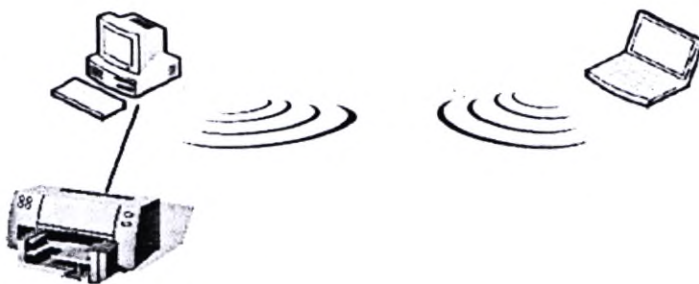
Wireless LAN beroperasi dengan menggunakan protokol yang sama seperti *LAN* biasa yaitu menggunakan IPv4. Komponen-komponen dari *Wireless LAN* juga sama dengan *LAN* biasa (*Client, Hub, Server*). Perbedaannya terletak pada *Wireless LAN* memanfaatkan *forwarding* routine dari *Network Layer*.

Forwarding routine dilaksanakan ketika seorang user atau perangkatnya (*agent*) meninggalkan original *network*nya dan masuk ke dalam *network* lainnya (*foreign network*). Ketika *agent* masuk ke dalam *foreign network*, *agent* akan memberitahu ke *network* mana data yang diterima harus *diforward*. *Forwarding* Routine akan *forward* data untuk *agent* dari original *network* ke *foreign network*, dan ketika *agent* kembali ke original *network*nya maka original dan *foreign network* akan diberitahu bahwa konfigurasi original telah *direstore*. *Network* lain di luar kedua *network* ini tidak perlu tahu bahwa *agent* berpindah.

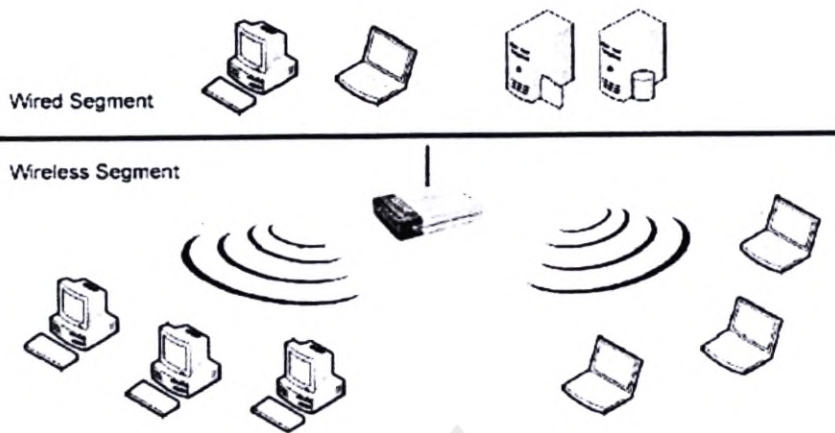
WiFi radio menggunakan teknik *encoding* data yang lebih efisien sehingga ikut memberikan kontribusi bagi data *rate* yang lebih tinggi. *Coding* yang digunakan 802.11a dan 802.11g adalah *orthogonal Frequency-division multiplexing* (OFDM), sedangkan 802.11b menggunakan *Complementary Code Keying* (CCK).

Ada 2 model struktur *network* pada *Wireless LAN* yaitu:

1. *Ad-Hoc*
2. *Infrastructured*



Gambar 2.1. Ad-Hoc Structure



Gambar 2.2. *Infrastructure*

Pada struktur *Ad-Hoc*, tidak ada *Infrastructure point*. *Network* terbentuk secara "on the fly" masing-masing *node* bisa berhubungan dengan *node* yang lainnya secara langsung. Contoh struktur *Ad-Hoc* adalah pada saat meeting dimana misalnya masing-masing anggota meeting membawa *laptop* dan melakukan *sharing design* atau *financial planning*. Walaupun tampaknya struktur *Ad-Hoc* tidak beraturan, namun algoritma *Ad-Hoc* selalu menunjuk satu *node* sebagai *master* dan mengatur *node* mana menjadi *master node* mana.

Jaringan komputer nirkabel menggunakan gelombang (radio atau infrared) elektromagnetik untuk bertukar informasi dari satu titik ke titik lain tanpa harus menggunakan alat koneksi secara fisik (mis. kabel). Gelombang radio seringkali disebut juga radio carrier (penghantar) karena secara sederhana melakukan fungsi menghantarkan energi ke alat penerima yang terpisah. Data yang dikirimkan telah "dibebankan" pada radio carrier sehingga dapat dipilah kembali oleh alat penerima (receiver). Hal ini secara umum digambarkan sebagai modulasi penghantar dengan informasi yang telah dikirimkan. Ketika gelombang radio berisi data telah dikirimkan

(modulated), signal radio menempati lebih dari satu frekwensi, karena frekwensi atau bit rate dari hasil modulasi informasi sudah ditambahkan pada carrier.

Dalam konfigurasi jaringan komputer nirkabel umumnya, sebuah alat yang berfungsi sekaligus sebagai transmitter/receiver (transceiver), disebut sebagai access point (Titik Akses), menghubungkan jaringan computer tradisional (berkabel) dari sebuah lokasi statis menggunakan topologi kabel standar. Secara minimum, Titik Akses (alat transceiver) menerima, menghubungkan dan mengirimkan data antara Jaringan Komputer Nirkabel dan infrastruktur jaringan yang menggunakan kabel. Sebuah Titik Akses (alat transceiver) dapat mendukung sebuah group kecil pengguna komputer dan beroperasi dalam jarak mulai dari seratus sampai beberapa ratus kaki. Titik Akses (atau antenna yang terpasang pada Titik Akses) biasanya dipasang pada ketinggian tapi juga bisa dipasang di mana saja sesuai kebutuhan asalkan dapat menangkap signal radio yang diharapkan. Para pengguna mengakses jaringan komputer nirkabel menggunakan adapter Jaringan Komputer Nirkabel (berupa PC expansion card) yang dipasang dalam palmtop, notebook, komputer desktop biasa atau komputer genggam, adapter Jaringan Komputer Nirkabel menyediakan interface antara client network operating system (NOS) dan gelombang radio melalui sebuah antenna.

2.4. Topologi Wireless Lan

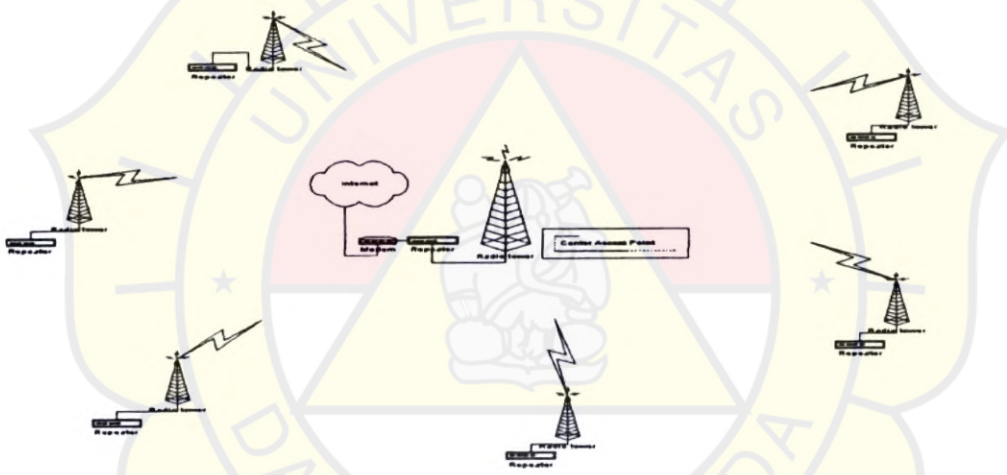
a. Wireless peer-to-peer network (ad-hoc)



Gambar 2.3. *Peer to Peer Network*

Jaringan komputer nirkabel bisa disebut sederhana sekaligus rumit. Pada dasarnya, dua unit komputer dilengkapi dengan kartu adapter Jaringan Komputer Nirkabel sudah cukup untuk membuat sebuah jaringan independent walaupun keduanya terpisah jarak. Hal ini disebut jaringan peert-to-peer. Jaringan on-demand dalam contoh ini tidak membutuhkan administrasi atau pra-konfigurasi. Dalam kasus ini setiap klien hanya memiliki akses terhadap klien lain tanpa mengakses sebuah server pusat.

b. Client and Access Point (Point to Multipoint)



Gambar 2.4. *Point to Multipoint Network*

Menginstal sebuah Titik Akses dapat menambah jangkauan network yang sudah ada, secara efektif menggandakan wilayah jangkauan di mana komputer-komputer dapat saling berhubungan. Karena Titik Akses (transceiver) dihubungkan dengan kabel ke jaringan komputer berkabel maka setiap klien nirkabel akan memiliki akses ke sumberdaya server sama seperti klien lain (berkabel). Setiap Titik Akses (transceiver) dapat mengakomodasi banyak klien; jumlah klien tergantung dari jumlah dan kemampuan transmisi yang digunakan.

c. Multiple access points and roaming

Titik Akses (transceiver) memiliki jangkauan yang terbatas, kira-kira 500 kaki dalam ruangan dan 1000 kaki di luar ruangan. Dalam lingkungan yang luas seperti gudang, atau pada kampus mungkin diperlukan lebih dari satu Titik Akses. Penempatan Titik Akses (alat transceiver) ditentukan melalui survey lokasi. Tujuannya adalah untuk meliputi wilayah seluas mungkin secara overlapping (menjangkau wilayah liputan Titik Akses yang lain) sehingga klien dapat berpindah dari satu wilayah liputan ke wilayah liputan berikutnya tanpa harus kehilangan kontak dengan jaringan (roaming). Sebuah Titik Akses harus dapat "mengoper" klien kepada Titik Akses lainnya tanpa harus disadari oleh si klien, tanpa hubungan yang terputus.

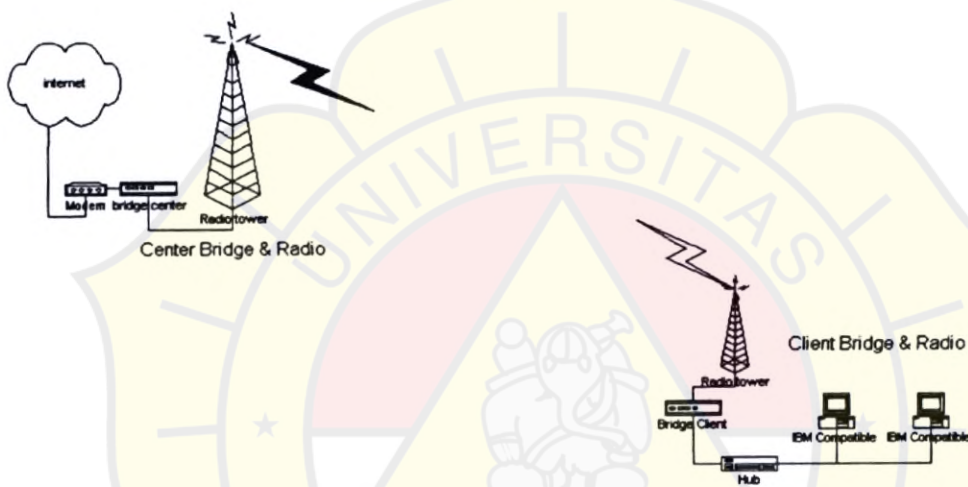
d. Use of an extension point

Untuk memecahkan masalah tersebut dalam topologi, perancang jaringan harus memilih untuk menggunakan Titik Tambahan (Extension Point) untuk menambah Titik Akses jaringan. Titik Tambahan kelihatan dan berfungsi seperti Titik Akses (transceiver), tapi Titik Tambahan tidak terikat pada jaringan berkabel seperti halnya Titik Akses. Fungsi Titik Tambahan seperti yang diimplikasikan oleh namanya; alat ini memperluas jangkauan jaringan dengan cara merelay signal dari sebuah klien ke Titik Akses atau Titik Tambahan. Beberapa Titik Tambahan bisa dijejarkan untuk menghubungkan pesan dari sebuah Titik Akses ke sebuah klien yang terletak jauh, seperti sebuah barisan manusia yang berdiri berjejer saling mengoperkan ember berisi air ke sumber kebakaran.

e. Directional Antenna (Point To Point)

Ada lagi sebuah alat untuk Jaringan Komputer Nirkabel yang patut dipertimbangkan, yaitu Directional Antenna. Seandainya anda memiliki sebuah

Jaringan Komputer Nirkabel pada Gedung A dan ingin menghubungkan jaringan tersebut ke sebuah Gedung B, yang jaraknya kira-kira satu mil. Solusinya adalah memasang sebuah Directional Antenna pada setiap gedung. Antenna di Gedung A terhubung dengan jaringan komputer di dalam Gedung A melalui sebuah Titik Akses (transceiver). Antenna di gedung B juga terhubung pada sebuah Titik Akses (transceiver) dalam Gedung B sehingga memungkinkan tercipta Jaringan Komputer Nirkabel antara Gedung A dan Gedung B.



Gambar 2.5. Point to Point Network

2.5. Modulasi Cck (Compelementary Code Keying)

Wireless radio menghasilkan 2.4 GHz gelombang pembawa (2.4 s/d 2.4835 GHz) dimana modulasi untuk tiap gelombang menggunakan teknik yang beragam. Untuk transmisi 1 Mbps menggunakan BPSK, untuk menghasilkan 2 Mbps menggunakan QPSK. QPSK menggunakan 4 rotasi (0,90,180 dan 270 derajat) untuk mengkodekan 2 bit informasi dalam ruang yang sama seperti BPSK mengkodekan 1.

IEEE 802.11b menggunakan 64 CCK (compelementary code keying) chipping sequence untuk mencapai 11 Mbps. CCK adalah variasi dari M-ary Orthogonal Keying modulation, dimana menggunakan arsitektur modulasi I/Q dengan struktur simbol yang

kompleks. CCK mengizinkan multi-channel yang bekerja pada 2.4 GHz menggunakan struktur channel pada DSSS. Teknik spreading ini memakai chipping rate yang sama dan spectrum shape seperti 802.11 Barker code word. Fungsi spreading mengizinkan 3 non-interfering channel pada band 2.4 sampai 2.4835 GHz.

2.6. Dsss (Direct Sequence Spread Spectrum)

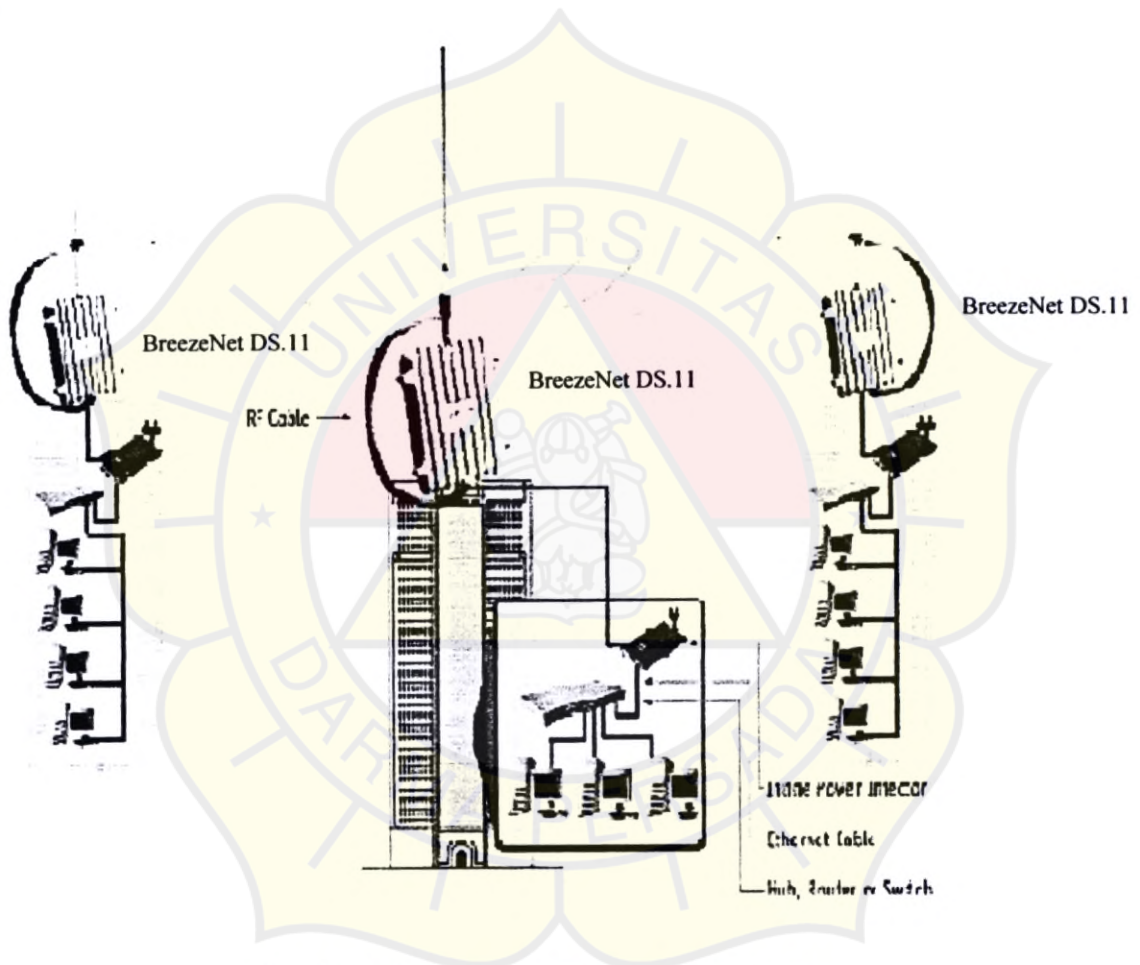
DS-SS adalah salah satu teknik akses *spread spectrum* yang mempunyai kelebihan kebal terhadap interferensi dan *jamming*. Teknologi ini pertama kali digunakan pada militer dan kemudian dikembangkan ke komunikasi selular angkasa. Pada tahun 1995, DS-SS mulai digunakan secara komersial terutama sesudah diperkenalkannya standard IS-95 pada tahun 1992 oleh QUALCOMM.

Sistem DS-SS tidak mengalokasikan frekuensi ataupun waktu dalam slot user, tetapi memberikan hak kepada semua user untuk menggunakan keduanya secara simultan. Untuk melakukan hal ini, sistem DS-SS menggunakan suatu sistem komunikasi yang dikenal dengan nama Spread Spectrum. Setiap user diberikan kode yang menyebar bandwidth sinyalnya dalam suatu cara sehingga hanya kode yang sama saja yang dapat *recover* sinyal pada receiver. Metode ini memiliki properti dimana sinyal yang tidak diinginkan dengan kode yang berbeda yang ikut disebar, akan terlihat seperti noise di receiver. Keuntungan DS-SS untuk Personal Communication Service (PCS) adalah kemampuannya untuk mengakomodasi banyak user pada waktu dan frekuensi yang sama.

2.7. Perangkat Keras Wlan

Di pasaran saat ini banyak sekali perangkat – perangkat dengan berbagai merek dengan kelebihan – kelebihan yang ditawarkan yang dibutuhkan dalam membuat sebuah

Wireless LAN. Begitu banyaknya produk yang ditawarkan dalam membangun sebuah Wireless LAN tetapi pada penulisan ini hanya mengangkat salah satu dari produk – produk tersebut yaitu BreezeNet DS.11. Untuk membangun sebuah jaringan Wireless LAN dibutuhkan perangkat – perangkat keras, seperti : Antennas, Bridge / Router, Cables, Power over Ethernet, Hub / Switches, Access Point, Personal Computer, WLAN Card.



Gambar 2.6. Perangkat Keras Wireless LAN

2.7.1. Antenna

Biasanya menggunakan external antenna untuk mendapatkan daerah cakupan. Banyak sekali variasi dari antenna di pasaran yang bisa digunakan, tergantung dari lokasi serta aplikasi di lapangan.

- Pada client side, bisa menggunakan directional antenna, seperti parabolic antenna, yagi antenna, tin can antenna dll.
- Pada Access Point, bisa menggunakan omni-directional antenna atau sectoral antenna



Gambar 2.7. Omnidirectional Antenna

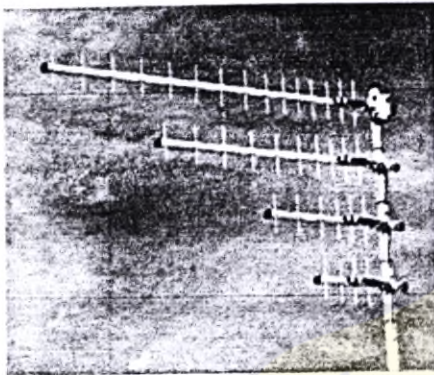
Untuk omnidirectional antenna memiliki cakupan 360 derajat, dimana memiliki antenna gain berkisar antara 3 sampai 12 dBi. Antenna omni biasa digunakan untuk komunikasi Point to Multipoint (P2MP) dan memiliki daerah coverage dari 1 sampai 5 km.



Gambar 2.8. Sectoral Antenna

Sectoral antenna hampir sama dengan antenna omni dimana digunakan untuk komunikasi Point to Multipoint (P2MP). Daerah cakupannya hanya berkisar antara 45 sampai 180 derajat dan memiliki gain yang lebih besar dari omni yaitu berkisar antara 10

- 19 dBi. Dalam komunikasi P2MP antenna sectoral mampu melayani jarak hingga 6-8 km.



Gambar 2.9. Yagi Antenna



Gambar 2.10. Parabolic Antenna

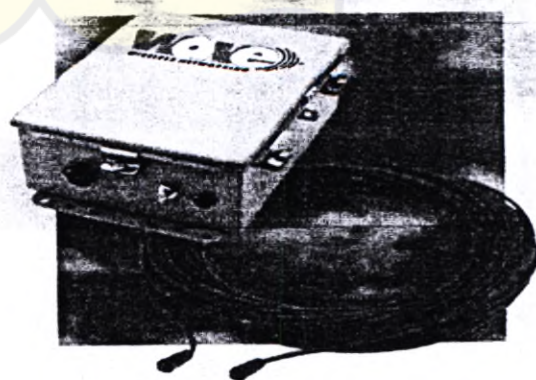
Pada client side bisa menggunakan directional antenna seperti yagi, flat panel, ataupun parabolic antenna. Untuk menaikkan gain antenna bisa menggunakan parabolic antenna yang memiliki gain antara 18 - 28 dBi. Namun jarak yang tercover oleh antenna ini terbatas.

2.7.2. Wireless Bridge / Router

Salah satu dari perangkat Wireless LAN adalah Wireless Bridge/ Router. Kebanyakan Wireless Bridge/Router dapat dijadikan sebagai Central ataupun sebagai Remote.



Gambar 2.11. Breezenet DS.11

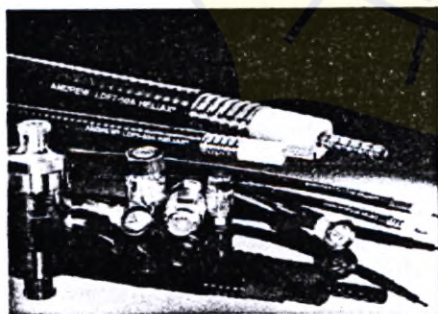


Gambar 2. 12 Speedland 8100/8200

Wireless Bridge/router memenuhi standard 802.11 dimana jangkauan operasinya lebih luas, juga menyediakan teknologi WLAN dengan kecepatan 11 Mbps dimana pengguna dapat akses ke Internet atau jaringan organisasi. Wireless outdoor memiliki casing yang permanen, tahan air, tahan cuaca dan dibuat dengan lightning protector untuk melindungi dari kondisi lingkungan yang berubah, termasuk dengan perubahan suhu yang ekstrim. Untuk melihat lebih jelas mengenai spesifikasi dari Breezenet DS.11 dapat dilihat pada Lampiran.

2.7.3. Pigtail, Kabel

Banyak kabel coaxial yang bisa digunakan, salah satu contohnya adalah kabel heliax $\frac{1}{2}$ LDF, dimana kabel heliax $\frac{1}{2}$ memiliki loss yang sangat kecil dan harganya tidak terlalu mahal dan disamping itu pula kabel tersebut sangat gampang didapat di Indonesia, disamping kabel heliax dibutuhkan pula konektornya, konektor memakai konektor Andrew. Gambar kabel heliax dan konektor Andrew bisa dilihat pada gambar 2.13. Disamping pemilihan kabel heliax dibutuhkan pula kabel Pigtail yang menghubungkan akses point ke kabel heliax, jenisnya ada beberapa macam tergantung dari jenis konektor Andrew yang dipakai pada sisi kabel heliax, gambar pigtail bisa dilihat pada gambar 2.14.



Gambar 2.13. Kabel heliax dan konektor Andrew



Gambar 2.14. Pigtail

2.7.4 .Surge Protector

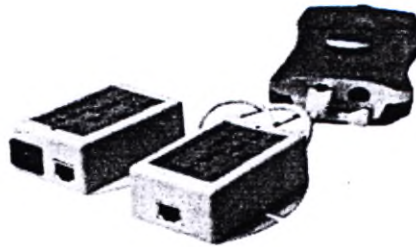
Surge protector sangat diperlukan untuk mencegah terjadinya kebakaran pada perangkat radio bridge jika antenna terkena petir, gambar Surge Protector bisa dilihat pada gambar 3.10, dan untuk jenisnya bisa disesuaikan dengan jenis konektor yang terpakai. Surge Protector bisanya digunakan antara antenna ke wireless bridge.



Gambar 2.15. Surge Protector

2.7.5. PoE (Power over Ethernet)

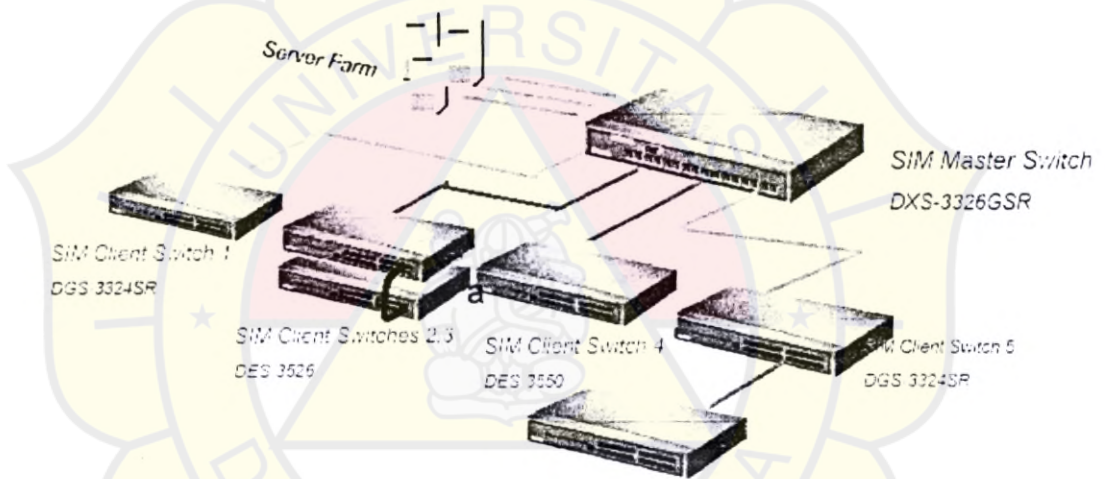
Untuk memudahkan dan efisiensi distribusi sumber listrik keatas menara sebagai sumber listrik dari perangkat radio bridge maka kami memakai PoE (power over ethernet), alat ini sangat berguna untuk menggantikan kabel listrik keatas menara, listrik telah dikonversi ke tegangan rendah dan dilewatkan ke kabel ethernet RJ45, hal ini dilakukan jika perangkat Radio Bridge dipasang diatas menara. Gambar PoE bisa dilihat pada gambar 3.16.



Gambar 2.16. Power Over Ethernet dan DC Power Supply

2.7.6. Hub / Switches

Hub / Switches pada dasarnya berfungsi sebagai penghubung antara server dengan beberapa komputer yang tergabung dalam satu jaringan. Satu hub / switches memiliki jumlah port komputer yang bervariasi. Tetapi dengan berkembangnya teknologi jumlah komputer bisa ditambah tanpa harus memakai jaringan tambahan, hanya tinggal mempararel hub / switches secara bertumpuk. Hub / switches memuat alamat IP address untuk masing – masing komputer dan pengendalian ataupun pengontrolan jaringan bisa dilakukan melalui server.



Gambar 2.7. Hub / Switches

2.7.7. Access Point

Access Point (AP) adalah perangkat penting yang akan selalu digunakan jika hendak membangun Wireless LAN. Sesuai dengan namanya Access Point berfungsi sebagai titik akses yang menghubungkan komputer – komputer ke dalam sebuah jaringan. Singkatnya, fungsi Access Point sama dengan fungsi Hub pada jaringan komputer konvensional. Sebuah Access Point biasanya dilengkapi dengan antenna dan port RJ45/Ethernet. Gambar access point terlihat seperti pada gambar 2.18.

Saat ini ada beberapa jenis Access Point yang beredar di pasaran, yakni Access Point 802.11b, 802.11g, serta Access Point dual band yakni Access Point yang mendukung standar 802.11a dan 802.11g.



Gambar 2.18. Access Point

Setiap Access Point biasanya memiliki beberapa mode operasi. Pada mode terbaru, dapat diatur berbagai fungsi dan melakukan proses monitoring melalui web browser. Saat hendak memilih Access Point sebaiknya diperhatikan mode yang didukung oleh Access Point tersebut. Beberapa Access Point yang beredar ada yang memberikan fasilitas mode operasi ekstra seperti Multi Point Bridge dan Repeater. Selain itu, juga harus memperhatikan bentuk dan jenis antenna yang digunakan pada Access Point tersebut. Biasanya antenna eksternal memiliki jangkauan yang lebih baik dibandingkan dengan antenna internal. Perhatikan apakah Access Point memiliki fitur untuk mengupgrade ke antenna luar yang lebih besar.

Access Point yang beredar saat ini biasanya sudah dilengkapi dengan fitur – fitur seperti:

- Sudah dilengkapi dengan proteksi firewall dan fitur untuk mengontrol access
- Mendukung protokol PPPoE/PPTP untuk ADSL
- Konfigurasi web based
- Security WEP dengan enkripsi 64/128 bit

Jika pada jaringan komputer konvensional (LAN) jumlah komputer yang dapat terhubung tergantung pada jumlah port yang tersedia pada hub atau switch, untuk Wireless LAN, jumlah komputer yang dapat terhubung sangat tergantung dengan Access Point yang digunakan. Ada Access Point yang hanya mendukung jumlah koneksi hingga 10 koneksi, ada juga yang lebih. Namun ada hal lain yang juga berpengaruh terhadap koneksi ke Access Point, yakni lalu lintas data pada Access Point tersebut. Semakin besar lalu lintas data yang beredar, kemungkinan tingkat koneksi semakin kecil.

2.7.8. *Wireless LAN Card*

Wireless LAN Card adalah Ethernet Card Wireless yang dipasang di slot PCI pada komputer. Jadi agar sebuah komputer dapat terhubung ke sebuah jaringan wireless, pada komputer harus terpasang kartu ini. Seperti halnya Access Point, saat ini jenis Wireless LAN Card yang beredar di pasaran adalah jenis dengan standar 802.11b, 802.11g dan dual band (802.11a – 802.11g). Ada beberapa bentuk Wireless LAN Card. Pada Gambar 3.19 bisa melihat sebuah Wireless LAN Card dengan internal antenna sedangkan pada gambar 3.20. adalah PCI Wireless LAN Card dengan SMA connector untuk dihubungkan dengan external antenna



Gambar 2.19. WLAN Card with antenna



Gambar 2.20. PCI Wireless LAN Card

Dalam memilih wireless LAN Card, ada baiknya dipilih Wireless LAN Card yang dapat diupgrade agar dapat menjangkau jarak yang lebih jauh. Kebanyakan Wireless LAN

Card, yang diproduksi vendor saat ini ditujukan untuk penggunaan dalam ruangan. Namun di pasaran masih dapat ditemui Wireless LAN Card yang dapat menjangkau jarak yang lebih jauh. Pada Wireless LAN Card seperti itu biasanya terdapat konektor untuk antena eksternal.

2.7.9. Wireless PCMCIA

Wireless PCMCIA adalah kartu wireless yang digunakan pada komputer jinjing (notebook). Jadi kartu ini dipasang pada slot PCMCIA notebook. Beberapa notebook keluaran terbaru sudah tidak memerlukan Wireless PCMCIA karena dilengkapi dengan perangkat Wireless LAN yang terintegrasi ke dalam notebook tersebut. Bentuk Wireless PCMCIA terlihat seperti pada Gambar 3.21.



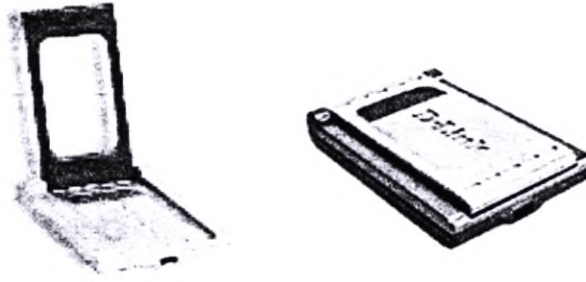
Gambar 2.21. PCMCIA DWL-G650+



Gambar 2.22. PCMCIA DWL-AG660

2.7.10. Wireless USB

Dewasa ini perkembangan perangkat yang memanfaatkan port USB semakin marak. Hal ini tidak lepas dari mudahnya pemasangan perangkat pada port USB. Dalam dunia wireless juga tersedia perangkat wireless yang dikenal dengan sebutan Wireless USB. Wireless USB adalah perangkat alternatif untuk Wireless LAN. Wireless USB dapat digunakan sebagai pengganti Wireless LAN Card atau Wireless PCMCIA. Perangkat ini dipasang pada port USB yang terdapat pada komputer notebook.



Gambar 2.23. Wireless USB

2.8. Radio Link Calculation

Tidak seperti penggunaan dalam rumah, kemampuan untuk mengkalkulasi radio link budget dan jarak adalah sangat penting jika seseorang ingin menggunakan perlengkapan Wireless LAN untuk mem-bypass jarak yang jauh. Sayangnya, mereka yang memiliki sedikit pengetahuan mengenai radio akan mempunyai kesulitan untuk melakukannya. Tetapi semenjak teknologi Wireless LAN telah berkembang pesat maka telah banyak informasi yang bisa didapat melalui Internet. Sebagai contoh bisa di-download kalkulasi radio link melalui www.ydi.com. atau www.gemesis.net/wlan/.

Ada beberapa parameter yang dibutuhkan sebagai kalkulasi untuk memastikan bahwa system telah berjalan dengan benar, yaitu :

- System Operating Margin (SOM), hal ini berhubungan dengan transmitter power, type antenna, panjang coaxial kable. Pastikan jika system yang dipakai memiliki power margin yang cukup untuk mencapai jarak tertentu.
- Free Space Loss (FSL), loss pada radio power setelah melewati jarak yang jauh.
- Fresnel Zone Clearance (FZC), untuk melihat ketinggian antenna yang dibutuhkan untuk melewati obstacle yang ada.

Penghitungan konversi power sangat dibutuhkan untuk mengubah dBm ke Watt, konversi dBm ke Watt atau sebaliknya dapat dilihat di bawah ini :

dBm – a relative power level referencing 1 milliwatt

W – a linear power level referencing Watts

$$\text{dBm} = 10 \times \log[\text{Power in Watts} / 0.001\text{W}]$$

$$\text{W} = 0.001 \times 10^{[\text{Power in dBm} / 10 \text{ dBm}]}$$

Kalkulasi pada YDI.COM menggunakan miles and feet, lalu kemudian pasti dibutuhkan suatu konversi menjadi meter atau kilometer jika dibutuhkan, berikut adalah konversi ke meter, feet, km, ataupun miles.

$$\text{Meter} = \text{Feet} * 0,3048$$

$$\text{Km} = \text{Miles} * 1.609344$$

Rx Sensitivity

Semua radio tentunya memiliki “*point of no return*”, yaitu ketika penerimaan sinyanya kurang dari Rx sensitivity, maka radio tidak akan mampu untuk melihat data. ‘Point of no return’ dari Rx sensitivity memiliki satuan dBm atau W. Pada semua radio, Rx sensitivity memiliki Bit error Rate (BER) antara 10 – 5 (99,999%).

Radiated Power

Pada wireless system, antenna digunakan untuk mengubah gelombang elektrik ke gelombang elektromagnetik. Antenna gain mengacu kepada jumlah energy yang bisa dikirim dan diterima. Antenna gain memiliki satuan ::

dB_i: relative to an isotropic radiator

dB_d: relative to a dipole radiator

Hubungan antara dB_d dengan dB_i adalah :

$$0 \text{ dBd} = 2.15 \text{ dBi}$$

Biasanya pada kalkulasi antenna gain menggunakan dBi

2.8.1. Energy Losses

Pada semua sistem komunikasi wireless ada beberapa faktor yang mempengaruhi hilangnya kekuatan sinyal, kabel, konektor, penahan petir semua dapat mempengaruhi performance dari sistem jika tidak dipasang dengan baik.

Pada sistem “daya kecil” setiap dB yang bisa kamu pakai akan sangat berarti, ingat aturan “3dB”

“For every 3 dB gain/loss you will either double your power (gain) or lose half your power (loss).”

“Untuk setiap 3 dB gain/loss kamu akan mendapatkan daya 2x dari daya awal (gain) atau kehilangan setengah dari daya awal (loss)”

$$-3 \text{ dB} = 1/2 \text{ daya}$$

$$-6 \text{ dB} = 1/4 \text{ daya}$$

$$+3 \text{ dB} = 2x \text{ daya}$$

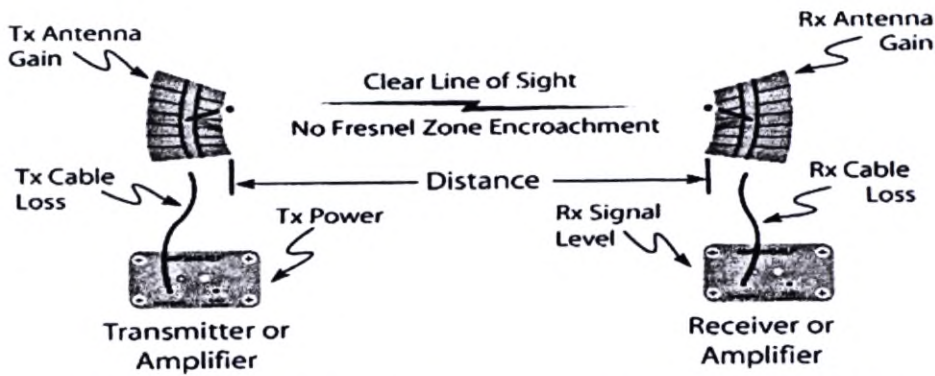
$$+6 \text{ dB} = 4x \text{ daya}$$

sumber dari loss pada sistem wireless adalah : free space (udara), kabel, penghubung, jumper, halangan (gedung-gedung, pohon-pohon, hujan)

2.8.2. Free Space Loss (FSL) Calculation

Sinyal yang keluar dari antenna akan menyebar, atau beredar ke angkasa. Pemilihan antenna akan menentukan seberapa banyak penyebaran yang terjadi. Karena melewati udara maka akan banyak loss pada dinyal radio.

Pada 2.4 GHz sangatlah penting untuk memastikan bahwa lintasan (lorong) antara dua antenna bersih dari segala halangan. Jika sinyal penyebaran bertemu dengan beberapa halangan pada lintasan, sinyal akan mengalami penurunan.



$$\text{Free Space Loss} = 20\text{Log}_{10}(\text{MHz}) + 20\text{Log}_{10}(\text{Distance in Miles}) + 36.6$$

Gambar 2.24. Free Space Loss

Seperti yang dilihat pada gambar diatas, Free Space Loss memiliki 2 parameter yaitu :

- Operating Frequency (in MHz)
- Jarak antara dua antenna (in Miles)

Sedangkan output dari Free Space Loss dalam dB. Free Space Loss dapat diprediksi dan diberikan dengan rumus :

$$FSL (dB) = 36.6 + 20 \text{Log}_{10} F(\text{MHz}) + 20 \text{Log}_{10} D(\text{Miles})$$

Atau menggunakan rumus lain :

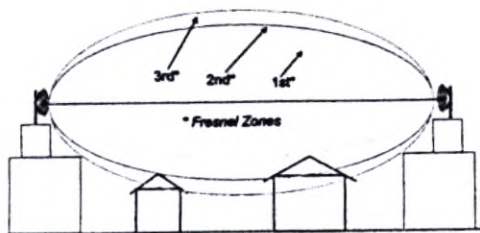
$$FSL(dB) = 32.45 + 20\text{Log}_{10}F(\text{MHz}) + 20\text{Log}_{10}D(\text{km})$$

Sebagai contoh untuk melihat Free Space Loss pada jarak 1 km dengan menggunakan sistem 2.4 GHz adalah 100 dB.

2.8.3. Fresnel Zone

Pencapaian Line of Sight (LOS) yang bagus antara antenna pemancar dan penerima sangatlah penting untuk perencanaan dan instalasi jaringan wireless Point to Point atau Point to Multipoint. Secara umum ada dua jenis LOS yang dipakai selama proses instalasi :

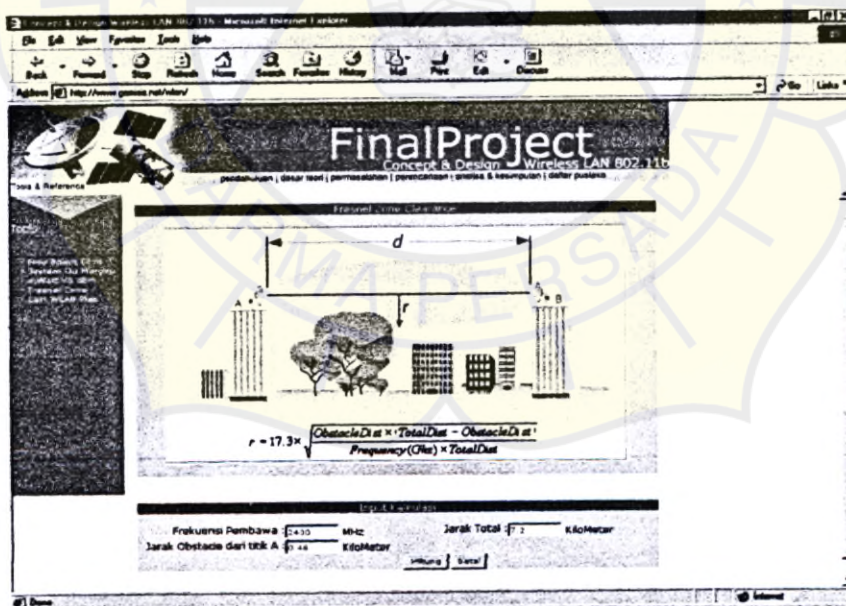
Fresnel Zones



Gambar 2.25. Fresnel Zone

1. Optical LOS, berhubungan pada kemampuan untuk melihat dari satu sisi ke sisi yang lain
2. Radio LOS, berhubungan pada kemampuan radio penerima untuk melihat sinyal yang ditransmisikan.

Optical Loss dapat dengan mudah dimengerti, sedangkan Radio loss membutuhkan sedikit kalkulasi untuk memastikan bahwa tidak ada distraction pada propagasi radio signal. Fresnel Zone adalah area dimana tidak obstacle yang bisa menghalangi transmisi sinyal radio. Pada gambar diatas dilihat Fresnel Zone 1st, 2nd, 3rd, dimana berbentuk suatu lingkaran elliptical yang menghubungkan dua stasiun. Biasanya menggunakan 80 % dari Fresnel Zone pertama sebagai daerah bebas. Sebagai contoh, Waverider menggunakan 60 % dari Fresnel Zone pertama ditambah 3 meter sebagai daerah bebas.

Gambar 2.26. Line of Sight ¹⁾

Rumus untuk mengkalkulasi radius dari Fresnel Zone adalah :

1) *Fresnel Zone*, www.gemesis.net/wlan/

$$r = 17.3 \times \sqrt{\frac{d(d-d_1)}{F(\text{GHz}) \cdot d}}$$

dimana :

r = radius dari Fresnel Zone (meter)

d = jarak antara dua titik (km) dan

d_1 = jarak obstacle (km)

f = frekuensi (GHz).

2.8.4. System Operating Margin (SOM) Calculation

System Operating Margin membutuhkan banyak parameter input dengan tiga output, yaitu :

RX Signal Level (dBm)

Free space Loss (dB)

Theoretical System Operating Margin (dB)

Pastikan bahwa system memiliki SOM antara 10 – 15 dB untuk memberikan ruang kepada fading dan multipath dalam penerimaan radio signal. Untuk dapat mengkalkulasi 3 parameter diatas, dibutuhkan beberapa input antara lain :

Frequency (MHz) yang digunakan

Distance (Miles) antara dua titik

TX Power (dBm), WLAN Card transmitter memiliki power biasanya antara 30 – 100 mW

TX Cable Loss (dB), loss pada cable dari transmitter ke antenna, tergantung dari type kabel dan panjangnya. Akan lebih baik jika panjang kabel kurang dari 10 meter untuk menghindari loss yang lebih besar.

TX Antenna Gain (dBi)

Free Space Loss (FSL)

RX Antenna Gain (dBi)

RX Cable Loss (dB), loss dari antenna ke receiver.

RX Sensitivity

Banyak data diatas dapat ditemukan pada buku manual dari setiap perlengkapan. Banyak WLAN card memiliki TX Power antara 15 – 20 dBm (antara 30-100 mW). Pada IEEE 802.11b, receiver sensitivity antara –80 sampai 85 dBm. Gain antenna tergantung dari jenis antena yang digunakan. Setelah didapatkan data yang dibutuhkan maka kemudian tinggal mencari SOM dengan rumus :

$$\text{FSL (dB)} = 36.6 + 20 \text{ Log}_{10} \text{ F(MHz)} + 20 \text{ Log}_{10} \text{ D(Miles)}$$

$$\text{Rx Signal Level} = \text{Tx Power} - \text{Tx Cable Loss} + \text{Tx Antenna Gain} - \text{FSL} + \text{Rx Antenna Gain} - \text{Rx Cable Loss}$$

$$\text{SOM} = \text{Rx Signal Level} - \text{Rx Sensitivity}$$

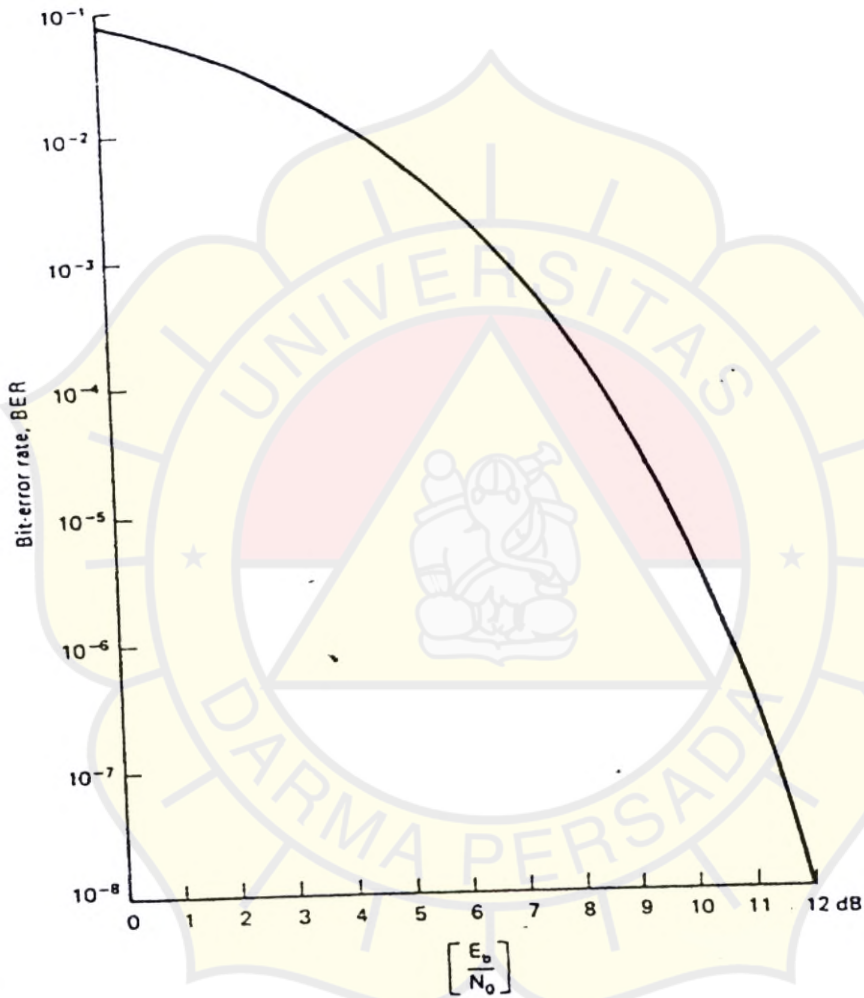
2.8.5. *Effective Isotropic Radiated Power (EIRP)*

Di dalam Wireless Wide Area Network , adalah sangat penting dimana frequency dapat direuse setelah melewati jarak tertentu. Untuk memastikan frequency reuse dapat diimplementasikan dalam suatu area, maka diperlukan maximum power. Effective Isotropics Radiated Power (EIRP) pada dasarnya adalah power dari radio signal pada ujung antenna sebelum diradiasikan ke udara, rumus dari EIRP adalah :

$$\text{EIRP (dBm)} = \text{TX Power} - \text{TX Cable Loss} + \text{TX Antenna Gain}$$

2.8.6. Bit Error Rate (BER), Carrier to Noise (C/N)

Kesalahan pensinyalan data pada transmisi dikenal dengan istilah *Bit Error Rate* (BER). Pada alat Breezenet DS.11 memiliki standar BER 10^{-5} yang artinya setiap 100.000 memiliki satu bit kesalahan. Dengan melihat gambar 2.7. maka bisa ditentukan BER dari E_b/E_o yang didapat.



Gambar 2.27. BER versus E_b/N_o

Karena *Wireless LAN* bekerja dengan kecepatan transmisi 11 Mbps. Maka dapat dicari

C/N_o dengan rumus :

$$\left[\frac{C}{N_o} \right] = \left[\frac{E_b}{N_o} \right] + [R_b]$$

dimana : C = Rx Signal Level (dBm)

N_o = $K T$

K = 1.38×10^{-23} J/K

T = 300^0 K

E_b/N_o = Energi to Noise Power (dB)

R_b = Bit Rate (dBbps)

2.9. Keamanan Wireless Lan

Sampai saat ini, masalah keamanan (security) masih dianggap sebagai salah satu kelemahan peneapan Wireless LAN. Hal ini terjadi karena perkembangan masalah keamanan pada Wireless LAN tidak sepesat penerapan dan perkembangan teknologi Wireless LAN itu sendiri. Secara umum masalah keamanan pada Wireless LAN timbul karena :

1. Masalah bentuk fisik Wireless LAN

Seperti yang diketahui, komunikasi pada Wireless LAN terjadi dengan memanfaatkan gelombang radio. Jadi di sekitar jaringan akan terdapat sinyal gelombang radio yang dipancarkan. Sinyal Wireless LAN secara normal dapat mencapai radius 200 meter. Oleh karena jauhnya radius sinyal ini, kemungkinan masih bisa tertangkap dari luar kantor atau rumah. Jika seseorang memiliki perangkat yang sesuai, orang tersebut dapat dengan mudah terhubung ke jaringan yang ada.

Hal ini berbeda dengan jaringan konvensional yang menggunakan media kabel untuk berkomunikasi. Untuk dapat mengakses ke sebuah jaringan, seseorang harus terhubung dengan kabel ke jaringan yang ada.

2. Lemahnya keamanan pada Wireless LAN juga sering diakibatkan karena lalainya administrator jaringan yang membiarkan perangkat Wireless LAN terpasang pada konfigurasi default. Konfigurasi default yang dimaksudkan adalah konfigurasi yang tidak mengaktifkan fungsi – fungsi dasar perlindungan, terhadap Wireless LAN, seperti enkripsi, membiarkan Access Point menggunakan nama SSID defaultnya, dan lainnya.

Untuk mengantisipasi masalah keamanan yang mungkin muncul, pada saat ini telah dibuat berbagai sistem untuk memproteksi Wireless LAN. Beberapa sistem keamanan yang saat ini dapat diterapkan pada Wireless LAN adalah pengesahan MAC Address, enkripsi dengan WEP (Wired Equivalent Privacy) atau WPA (WiFi Protected Access), serta proteksi menggunakan SSID (Service Set Identifier).

Perangkat Wireless yang beredar saat ini biasanya dilengkapi dengan sistem keamanan yang disebutkan di atas. Jadi sebagai administrator hanya tinggal memilih sistem keamanan mana yang akan digunakan. Juga dapat menggunakan beberapa sistem keamanan secara bersamaan sehingga jaringan yang ada dapat lebih terlindungi.

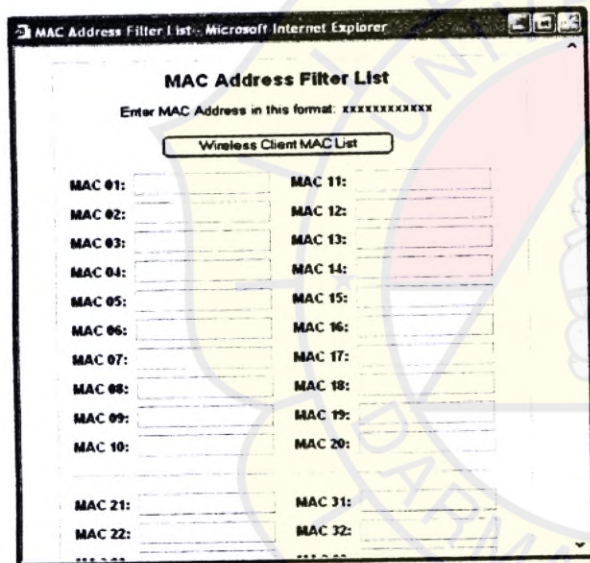
Semua konfigurasi sistem keamanan dapat diakses langsung pada Access Point yang digunakan seperti yang telah disebutkan sebelumnya pada perangkat keras Wireless LAN.

2.9.1. Proteksi dengan MAC Address

Dalam setiap kartu jaringan / NIC (Network Interface Card) pasti terdapat sebuah nomor yang unik yang dikenal dengan istilah MAC (Medium Access Control) Address. MAC Address disebut juga Physical Address. Sama halnya dengan NIC, pada setiap Wireless LAN Card juga terdapat MAC Address.

Salah satu sistem keamanan pada Wireless LAN memanfaatkan keunikan nomor MAC Address sebagai sarana untuk mengesahkan boleh atau tidaknya sebuah komputer mengakses jaringan. Pengesahan terhadap MAC Address ini dilakukan oleh Access Point. Biasanya dalam sebuah Access Point tersedia tabel yang dapat diisi dengan MAC Address untuk melarang atau mengizinkan komputer mengakses jaringan. Jadi dengan sistem keamanan ini, MAC Address komputer yang diberikan hak untuk mengakses jaringan akan didaftarkan terlebih dahulu pada Access Point.

Pada Access Point yang digunakan pada contoh ini, jumlah MAC Address yang didaftarkan pada Access Point mencapai 50 MAC Address. Lihat Gambar 2.27. MAC



Address sebuah Wireless LAN Card biasanya tercetak pada bagian depan Wireless LAN Card bersangkutan.

Jika tidak menemukannya, cara lain untuk mengetahui MAC Address adalah dengan mengetikkan perintah `ipconfig/all` pada command prompt.

Gambar 2.28. MAC Address

2.9.2. SSID

SSID mungkin merupakan sistem proteksi yang paling rendah tingkat keamanannya. Dalam jaringan konvensional SSID dapat disamakan dengan nama jaringan (Workgroup Name). Pada jaringan Wireless, SSID adalah identitas yang terdapat pada Access Point.

Untuk dapat mengakses sebuah jaringan Wireless, mutlak harus diketahui SSID yang ada. Jadi jika nama SSID tidak diketahui, sebuah komputer tidak akan terhubung ke

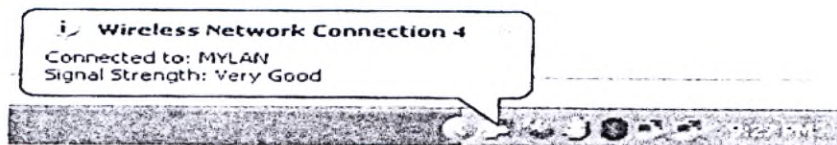
jaringan yang ada. Namun, untuk saat ini perangkat wireless yang beredar biasanya sudah dilengkapi dengan fitur yang dapat mendeteksi SSID yang berada di sekitarnya.

Sebagai contoh, jika memiliki sebuah notebook yang dilengkapi dengan kartu Wireless, pada saat berada pada ruangan yang dilengkapi dengan Access Point, kartu Wireless akan dengan mudah mendeteksi SSID yang ada pada Access Point tersebut. Gambar 2.28. menunjukkan sebuah wireless LAN Card mendeteksi adanya Access Point di sekitarnya.



Gambar 2.29. Wireless LAN Card mendeteksi Access Point di sekitarnya

Dari gambar diatas terdapat keterangan mengenai nama SSID Access Pointnya yakni **default**, serta keterangan mengenai kuatnya sinyal. Jika Access Point dijalankan dengan fitur DHCP, dengan sangat mudah akan mendapatkan IP Address dan masuk ke dalam jaringan yang ada. Jika SSID dinonaktifkan (Disable), Wireless LAN Card tidak akan mendeteksi adanya Access Point di sekitarnya. Agar komputer dapat terhubung ke jaringan yang ada, harus memasukkan identitas SSID Access Point secara manual. Tentunya hal ini dapat dilakukan jika diketahui nama SSID-nya. Setelah itu memasukkan nama SSID pada computer, maka Wireless LAN Card akan langsung mengenal Access Point yang ada. Pada komputer akan melihat pesan seperti yang tampak pada gambar 2.29.



Gambar 2.30 Koneksi berhasil dilakukan

2.9.3. Enkripsi WEP & WPA

Sistem keamanan WEP menggunakan teknologi enkripsi algoritma untuk mengotorisasi user dan melindungi komunikasi data yang terjadi pada jaringan. Pada sistem ini, sebelum data dikirimkan, data akan dienkripsi terlebih dahulu, dan setelah sampai pada penerima, data akan didekripsi kembali. Terdapat beberapa teknologi enkripsi yang digunakan, yakni 64 bit dan 128 bit. Semakin tinggi teknologi enkripsi yang digunakan, tingkat keamanan akan semakin baik, namun semakin tinggi tingkat enkripsi akan berdampak pada penggunaan bandwidth jaringan, dengan kata lain jaringan dapat menjadi lambat.

Pada perkembangan dan pemanfaatannya, sistem keamanan menggunakan WEP masih dianggap rentan karena masih dapat ditembus oleh penyusup. Oleh karena itu dikembangkanlah sistem keamanan WPA (WiFi Protected Access). Jika pada sistem WEP menggunakan static key untuk proses enkripsi, pada sistem WPA enkripsi dilakukan menggunakan rapid keying yang dikenal dengan istilah TKIP (Temporal Key Integrity Protocol). Sampai saat ini proteksi dengan sistem WEP dan WPA masih dianggap sebagai sistem proteksi yang paling aman.